THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH

SANS FIRE 2017

Washington, DC | July 22-29

EXCLUSIVE EVENT POWERED BY THE INTERNET STORM CENTER

GET THE WORLD'S LEADING HANDS-ON, IMMERSION-STYLE

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

45+ courses in:

- CYBER DEFENSE
- DETECTION & MONITORING
- PENETRATION TESTING
- INCIDENT RESPONSE
- CYBER THREAT INTELLIGENCE
- ETHICAL HACKING
- SECURITY MANAGEMENT
- AUDIT | LEGAL
- SECURE DEVELOPMENT
- ICS/SCADA SECURITY

GIAC CERTIFICATIONS

GIAC-Approved Training

"This has been the best training I have ever taken. Between the knowledge of the instructor and the course material, everything was run to perfection!"

-Joe Lordi, Wawa

SANS NETWARS EXPERIENCE

SAVE $400

Register and pay by May 31st – Use code **EarlyBird17**

REGISTER AT **www.sans.org/sansfire**

Dear Colleague,


Johannes Ullrich, PhD

Now is the time to advance your career and develop skills to better protect your organization. Join us at **SANSFIRE 2017** in Washington DC from July 22-29 to learn directly from the world's top cybersecurity practitioners. Through hands-on immersion training, our courses will provide you with the cutting-edge skills to defend your organization against security breaches and prevent future attacks.

SANSFIRE 2017 also gives you a unique opportunity to meet and exchange ideas with some of the people behind the Internet Storm Center (ISC). You can attend our always popular "State of the Internet" panel as well as individual talks highlighting some of the extraordinary talent you can access via the ISC. Presentations by ISC handlers will cover some of the latest problems facing the industry, such as attacks against NoSQL Databases, as well as issues fresh in our minds, such as countermeasures for DDoS attacks. The presentations will be made by real-world practitioners who face the same challenges you do on a daily basis.

Why is SANSFIRE 2017 the best training and education investment?

SANS' immersion training is intensive and hands-on, and our courseware is unrivaled in the industry. Our instructors and course authors are leading industry experts and practitioners. With 45+ courses to choose from at this event, all types of professionals can learn valuable skills applicable to their security roles that they will be able to implement immediately. Learn cutting-edge content across a diverse set of practice areas, including Cyber Defense, Digital Forensics & Incident Handing, Threat Hunting, Audit, Management, Pen Testing, Cyber Threat Intelligence, Industrial Control Systems Security, and Secure Software Development. The courses will prepare you to meet today's threats and tomorrow's challenges.

Which courses will be offered?

The SANSFIRE 2017 schedule offers a full lineup of classic SANS courses as well as new ones, including:

- SEC573: Automating Information Security with Python
- SEC579: Virtualization and Software-Defined Security
- FOR572: Advanced Network Forensics and Analysis
- MGT517: Managing Security Operations: Detection, Response, and Intelligence
- DEV531: Defending Mobile Applications Security Essentials
- DEV534: Secure DevOps: A Practical Introduction

Many of these courses prepare you for a GIAC certification, one of the most prestigious security certifications in the field. You can also bundle four months of OnDemand online training with your live course at a discounted rate to extend your study. Add the corresponding GIAC certification and OnDemand bundle when registering for your course to receive the discounted rates (subject to availability).

Bonus Experiences

In addition to SANS classroom training and development, you can also test your security defense skills at the Core NetWars Experience, DFIR NetWars Tournament, and all-new Cyber Defense NetWars Competition scheduled for the evenings of July 27 and 28. The Core NetWars Experience is an interactive, Internet-based environment for computer attacks and analyzing defenses. The DFIR NetWars Tournament is an incident simulator, packed with a vast amount of forensic and incident response challenges, for individual or team-based "firefights." The Cyber Defense NetWars Competition is a defense-focused challenge aimed at testing your ability to solve problems and secure your systems from compromise. Professionals from all skill levels will gain valuable knowledge and experience from participating.

We look forward to seeing you at SANSFIRE 2017, and to proving why SANS is recognized around the world as the leader in information security training. Visit **www.sans.org/event/sansfire** to learn more, to review the course list and event details, and to find out how our training can help you reach your professional goals.

Don't forget – register and pay by May 31 to save $400.

See you in Washington DC!

Johannes Ullrich, Ph.D.
SANS Senior Instructor
Dean of Research for the SANS Technology Institute and Director of the Internet Storm Center

Courses at a Glance

For an up-to-date course list, please check the website at www.sans.org/event/sansfire-2017/schedule

		SAT 7-22	SUN 7-23	MON 7-24	TUE 7-25	WED 7-26	THU 7-27	FRI 7-28	SAT 7-29
SEC301	Intro to Information Security			PAGE 12					
SEC401	Security Essentials Bootcamp Style SIMULCAST			PAGE 8					
SEC440	Critical Security Controls: Planning, Implementing, and Auditing	P 87							
SEC501	Advanced Security Essentials – Enterprise Defender			PAGE 14					
SEC503	Intrusion Detection In-Depth SIMULCAST			PAGE 16					
SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling			PAGE 10					
SEC505	Securing Windows and PowerShell Automation			PAGE 18					
SEC506	Securing Linux/Unix			PAGE 20					
SEC511	Continuous Monitoring and Security Operations			PAGE 22					
SEC524	Cloud Security Fundamentals	P 86							
SEC542	Web App Penetration Testing and Ethical Hacking			PAGE 30					
SEC546	IPv6 Essentials	P 86							
SEC550	Active Defense, Offensive Countermeasures, and Cyber Deception			PAGE 32					
SEC560	Network Penetration Testing and Ethical Hacking			PAGE 28					
SEC561	Immersive Hands-On Hacking Techniques			PAGE 34					
SEC566	Implementing and Auditing the Critical Security Controls – In-Depth			PAGE 62					
SEC567	Social Engineering for Penetration Testers	P 87							
SEC573	Automating Information Security with Python			PAGE 36 NEW!					
SEC575	Mobile Device Security and Ethical Hacking			PAGE 38					
SEC579	Virtualization and Software-Defined Security			PAGE 24 NEW!					
SEC580	Metasploit Kung Fu for Enterprise Pen Testing	P 87							
SEC642	Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques			PAGE 40					
SEC660	Advanced Penetration Testing, Exploit Writing, and Ethical Hacking			PAGE 42					
FOR408	Windows Forensic Analysis SIMULCAST			PAGE 46					
FOR508	Advanced Digital Forensics, Incident Response, and Threat Hunting SIMULCAST			PAGE 48					
FOR526	Memory Forensics In-Depth			PAGE 50					
FOR572	Advanced Network Forensics and Analysis SIMULCAST			PAGE 52 NEW!					
FOR578	Cyber Threat Intelligence SIMULCAST			PAGE 54					
FOR585	Advanced Smartphone Forensics			PAGE 56					
FOR610	Reverse-Engineering Malware: Malware Analysis Tools and Techniques			PAGE 58					
MGT305	Technical Communication and Presentation Skills for Security Professionals		P 88						
MGT414	SANS Training Program for CISSP® Certification			PAGE 66					
MGT415	A Practical Introduction to Cybersecurity Risk Management	P 88							
MGT433	Securing The Human: How to Build, Maintain, and Measure a High-Impact Awareness Program	P 88							
MGT512	SANS Security Leadership Essentials for Managers with Knowledge Compression™			PAGE 64					
MGT514	IT Security Strategic Planning, Policy, and Leadership			PAGE 68					
MGT517	Managing Security Operations: Detection, Response, and Intelligence			PAGE 70 NEW!					
MGT525	IT Project Management, Effective Communication, and PMP® Exam Prep			PAGE 72					
AUD507	Auditing & Monitoring Networks, Perimeters, and Systems			PAGE 74					
LEG523	Law of Data Security and Investigations			PAGE 76					
DEV522	Defending Web Applications Security Essentials			PAGE 78					
DEV531	Defending Mobile Applications Security Essentials	P 89 NEW!							
DEV534	Secure DevOps: A Practical Introduction	P 89 NEW!							
DEV541	Secure Coding in Java/JEE: Developing Defensible Applications			PAGE 80					
DEV544	Secure Coding in .NET: Developing Defensible Applications			PAGE 82					
ICS410	ICS/SCADA Security Essentials			PAGE 84					
	Core NetWars, DFIR NetWars, and Cyber Defense NetWars						PAGE 26		

PMP® is a registered trademark of the Project Management Institute, Inc.

CONTENTS

SANS WORLD-CLASS INSTRUCTORS

SANS instructors are real-world practitioners who specialize in the subjects they teach. All instructors undergo rigorous training and testing in order to teach SANS courses. This guarantees that what you learn in class will be up to date and relevant to your job. The lineup of instructors for SANSFIRE 2017 includes:

For instructor bios, visit:
www.sans.org/event/sansfire-2017/instructors

Mark Baggett
Senior Instructor
@MarkBaggett
Teaching SEC573

Eric Conrad
Senior Instructor
@eric_conrad
Teaching SEC511

Eric Cornelius
Certified Instructor
Teaching ICS410

Christopher Crowley
Principal Instructor
@CCrowMontance
Teaching MGT517 & SEC580

Adrien de Beaupre
Certified Instructor
@adriendb
Teaching SEC642

Ted Demopoulos
Principal Instructor
@TedDemop
Teaching MGT512

Kevin Fiscus
Certified Instructor
@kevinbfiscus
Teaching SEC561

Jason Fossen
Faculty Fellow
@JasonFossen
Teaching SEC505

Jeff Frisk
Certified Instructor
Teaching MGT525

Bryce Galbraith
Principal Instructor
@brycegalbraith
Teaching SEC550

Philip Hagen
Certified Instructor
@PhilHagen
Teaching FOR572

Paul A. Henry
Senior Instructor
@phenrycissp
Teaching SEC501

David Hoelzer
Faculty Fellow
@it_audit
Teaching SEC503 & MGT305

Micah Hoffman
Certified Instructor
@WebBreacher
Teaching SEC567

Eric Johnson
Certified Instructor
@emjohn20
Teaching DEV544

Frank Kim
Certified Instructor
@fykim
Teaching DEV534 & MGT514

Jason Lam
Certified Instructor
@jasonlam_sec
Teaching DEV522

Rob Lee
Faculty Fellow
@robtlee, @sansforensics
Teaching FOR408

Gregory Leonard
Instructor
Teaching DEV531 & DEV541

Heather Mahalik
Senior Instructor
@HeatherMahalik
Teaching FOR585

Randy Marchany
Certified Instructor
@randymarchany
Teaching SEC440

Tim Medin
Certified Instructor
@timmedin
Teaching SEC660

David R. Miller
Certified Instructor
@DRM_CyberDude
Teaching MGT414

Seth Misenar
Senior Instructor
@sethmisenar
Teaching SEC542

Keith Palmgren
Senior Instructor
@kpalmgren
Teaching SEC301

Hal Pomeranz
Faculty Fellow
@hal_pomeranz
Teaching SEC506

Clay Risenhoover
Certified Instructor
@AuditClay
Teaching AUD507

Dave Shackleford
Senior Instructor
@daveshackleford
Teaching SEC524 & SEC579

Bryan Simon
Certified Instructor
@BryanOnSecurity
Teaching SEC401

Ed Skoudis
Faculty Fellow
@edskoudis
Teaching SEC560

Lance Spitzner
Certified Instructor
@lspitzner
Teaching MGT433

John Strand
Senior Instructor
@strandjs
Teaching SEC504

Peter Szczepankiewicz
Certified Instructor
@_s14
Teaching SEC575

James Tarala
Senior Instructor
@isaudit
Teaching SEC566 & MGT415

Chad Tilbury
Senior Instructor
@chadtilbury
Teaching FOR508

Alissa Torres
Certified Instructor
@sibertor
Teaching FOR526

Johannes Ullrich, PhD
Senior Instructor
@johullrich
Teaching SEC546

Jake Williams
Certified Instructor
@MalwareJake
Teaching FOR578

Benjamin Wright
Senior Instructor
@benjaminwright
Teaching LEG523

Lenny Zeltser
Senior Instructor
@lennyzeltser
Teaching FOR610

Training Roadmap | Choose Your Path

Baseline Skills

1 **You are** experienced in technology, but need to learn hands-on, essential security skills and techniques

Core Security Techniques
Defend & Maintain

Every security professional should know the defense-in-depth techniques taught in SEC401, and SEC504 completes the "offense informs defense" preparation that teaches defense specialists how attacks occur and how to respond. If you've got the core defense skills, start with SEC504.

SEC401 Security Essentials Bootcamp Style — **GSEC** Certification Security Essentials (p. 8)

SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling — **GCIH** Certification Certified Incident Handler (p. 10)

1b **You** will be responsible for managing security teams or implementations, but you do not require hands-on skills

Security Management

MGT512 SANS Security Leadership Essentials for Managers with Knowledge Compression™ — **GSLC** Certification Security Leadership (p. 64)

SEC566 Implementing and Auditing the Critical Security Controls – In-Depth — **GCCC** Certification Critical Security Controls (p. 62)

New to Cybersecurity?

SEC301 — **GISF** Certification

Intermediate Job Roles

2 **You are** experienced in security, preparing for a specialized job role or focus

Security Monitoring & Detection

SEC503 Intrusion Detection In-Depth — **GCIA** Certification Certified Intrusion Analyst (p. 16)

SEC511 Continuous Monitoring and Security Operations — **GMON** Certification Continuous Monitoring (p. 22)

Penetration Testing & Vulnerability Analysis

SEC560 Network Penetration Testing and Ethical Hacking — **GPEN** Certification Penetration Tester (p. 28)

SEC542 Web App Penetration Testing and Ethical Hacking — **GWAPT** Certification Web Application Penetration Tester (p. 30)

Incident Response and Enterprise Forensics

FOR508 Advanced Digital Forensics, Incident Response, and Threat Hunting — **GCFA** Certification Forensic Analyst (p. 48)

FOR572 Advanced Network Forensics and Analysis — **GNFA** Certification Network Forensic Analyst (p. 52)

MGT414 SANS Training Program for CISSP® Certification — **GISP** Certification Information Security Professional (p. 66)

Crucial Skills, Specialized Roles

SANS' comprehensive course offerings enable professionals to deepen their technical skills in key practice areas. The courses also address other topics and audiences, such as security training for software developers, industrial control engineers, and non-technical personnel in management, legal, and audit.

3 **You are** a candidate for specialized or advanced training

Cyber Defense Operations

- SEC**501** Advanced Security Essentials – Enterprise Defender **GCED** (p. 14)
- SEC**505** Securing Windows and PowerShell Automation **GCWN** (p. 18)
- SEC**506** Securing Linux/Unix | **GCUX** (p. 20)
- SEC**566** Implementing and Auditing the Critical Security Controls – In-Depth | **GCCC** (p. 62)
- SEC**579** Virtualization and Software-Defined Security (p. 24)

Industrial Control Systems Security

- ICS**410** ICS/SCADA Security Essentials | **GICSP** (p. 84)
- ICS**456** Essentials for NERC Critical Infrastructure Protection
- ICS**515** ICS Active Defense and Incident Response | **GIAD**

Penetration Testing & Ethical Hacking

- SEC**550** Active Defense, Offensive Countermeasures and Cyber Deception (p. 32)
- SEC**561** Immersive Hands-On Hacking Techniques (p. 34)
- SEC**562** CyberCity Hands-on Kinetic Cyber Range Exercise
- SEC**573** Automating Information Security with Python **GPYC** (p. 36)
- SEC**575** Mobile Device Security and Ethical Hacking **GMOB** (p. 38)
- SEC**617** Wireless Ethical Hacking, Penetration Testing, and Defenses | **GAWN**
- SEC**642** Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques (p. 40)
- SEC**660** Advanced Penetration Testing, Exploit Writing, and Ethical Hacking | **GXPN** (p. 42)
- SEC**760** Advanced Exploit Development for Penetration Testers

Digital Forensics and Incident Response

- FOR**408** Windows Forensic Analysis | **GCFE** (p. 46)
- FOR**518** Mac Forensic Analysis
- FOR**526** Memory Forensics In-Depth (p. 50)
- FOR**578** Cyber Threat Intelligence (p. 54)
- FOR**585** Advanced Smartphone Forensics | **GASF** (p. 56)
- FOR**610** Reverse-Engineering Malware: Malware Analysis Tools and Techniques | **GREM** (p. 58)

Software Security

- DEV**522** Defending Web Applications Security Essentials **GWEB** (p. 78)
- DEV**541** Secure Coding in Java/JEE: Developing Defensible Applications | **GSSP-JAVA** (p. 80)
- DEV**544** Secure Coding in .NET: Developing Defensible Applications | **GSSP-.NET** (p. 82)

Management

- MGT**514** IT Security Strategic Planning, Policy, and Leadership (p. 68)
- MGT**517** Managing Security Operations: Detection, Response, and Intelligence (p. 70)
- MGT**525** IT Project Management, Effective Communication, and PMP® Exam Prep | **GCPM** (p. 72)

Audit | Legal

- AUD**507** Auditing & Monitoring Networks, Perimeters, and Systems | **GSNA** (p. 74)
- SEC**566** Implementing and Auditing the Critical Security Controls – In-Depth | **GCCC** (p. 62)
- LEG**523** Law of Data Security and Investigations | **GLEG** (p. 76)

PMP® is a registered trademark of the Project Management Institute, Inc.

Securing **Approval** and **Budget** for Training

Packaging matters

Write a formal request

- All organizations are different, but because training requires a significant investment of both time and money, most successful training requests are made via a written document (short memo and/or a few powerpoint slides) that justifies the need and benefit. Most managers will respect and value the effort.
- Provide all the necessary information in one place. In addition to your request, provide all the right context by including the summary pages on Why SANS?, the Training Roadmap, the instructor bio, and additional benefits available at our live events or online.

Clearly state the benefits

Be specific

- How does the course relate to the job you need to be doing? Place the particular course you wish to take into the context on the SANS Career Roadmap. Are you establishing baseline skills? Transitioning to a more focused role? Decision-makers need to understand the plan and context for the decision.
- Highlight specifics of what you will be able to do afterwards. Each SANS course description includes a section titled "You Will Be Able To." Be sure to include these in your request so that you make the benefits clear. The clearer the match between the training and what you need to do at work, the better.

Set the context

Establish longer-term expectations

- Information security is a specialized career path within IT, with practices that evolve as attacks change. Because of this, organizations should expect to spend 6%-10% of salaries to keep professionals current and improve their skills. Training for such a dynamic field is an annual, per-person expense, and not a once-and-done item.
- Take a GIAC Certification exam to prove the training worked. Employers value the validation of learning that passing a GIAC exam offers. Exams are psychometrically designed to establish competency for related job tasks.
- Consider offering trade-offs for the investment. Many professionals build annual training expense into their employment agreements even before joining a company. Some offer to stay for a year after they complete the training.

SANS Baseline Skills

Core Security Techniques | Security Management

The foundation of a successful career in information security – whether technical or managerial – should be comprehensive and rooted in real-world expertise. Learn more about the SANS courses and certifications recommended for baseline skills below and on the pages that follow in this catalog.

Core Security Techniques
Defend & Maintain

SEC**401** Security Essentials Bootcamp Style	**GSEC** Certification Security Essentials
SEC**504** Hacker Tools, Techniques, Exploits and, Incident Handling	**GCIH** Certification Certified Incident Handler

Summary: Every hands-on technical professional should possess the baseline set of knowledge and skills taught in **SEC401** and **SEC504**. These courses cover the essentials of defense-in-depth, the mental model for how attacks work, and the proven methods for handling incidents when they occur.

Who This Path Is for: Hands-on technical professionals such as network administrators and engineers, security analysts, and consultants who need well-rounded and effective baseline security skills.

Why This Training Is Important: This training gives you essential knowledge and understanding about how a variety of attacks occur and how to respond to them.

"The focus on methodologies was superb because the techniques taught are applicable to every environment regardless of the tools utilized."

-Conrad Bovell, DSS

"This is great training that shows you potential indicators of compromise and the tools and techniques to look for and identify potentially compromised systems."

-Stephen Larkin, Exekib Corporation

SEC401

GSEC Certification
Security Essentials

www.giac.org/gsec

Security Essentials Bootcamp Style

Six-Day Program
Mon, July 24 - Sat, July 29
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Bryan Simon

This course has evening Bootcamp Sessions

Who Should Attend

- Security professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Operations personnel who do not have security as their primary job function but need an understanding of security to be effective
- IT engineers and supervisors who need to know how to build a defensible network against attacks
- Administrators responsible for building and maintaining systems that are being targeted by attackers
- Forensic specialists, penetration testers, and auditors who need a solid foundation of security principles to be as effective as possible at their jobs
- Anyone new to information security with some background in information systems and networking

This course will teach you the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. You'll learn tips and tricks from the experts so that you can win the battle against the wide range of cyber adversaries that want to harm your environment.

See page 96 for details.

STOP and ask yourself the following questions:

- **Do you fully understand why some organizations get compromised and others do not?**
- **If there were compromised systems on your network, are you confident that you would be able to find them?**
- **Do you know the effectiveness of each security device and are you certain that they are all configured correctly?**
- **Are proper security metrics set up and communicated to your executives to drive security decisions?**

If you do not know the answers to these questions, SEC401 will provide the information security training you need in a bootcamp-style format that is reinforced with hands-on labs.

SEC401: Security Essentials Bootcamp Style is focused on teaching you the essential information security skills and techniques you need to protect and secure your organization's critical information assets and business systems. Our course will show you how to prevent your organization's security problems from being headline news in the *Wall Street Journal*!

Prevention is Ideal but detection is a must.

With the rise in advanced persistent threats, it is almost inevitable that organizations will be targeted. Whether the attacker is successful in penetrating an organization's network depends on the effectiveness of the organization's defense. Defending against attacks is an ongoing challenge, with new threats emerging all of the time, including the next generation of threats. Organizations need to understand what really works in cybersecurity. What has worked, and will always work, is taking a risk-based approach to cyber defense. Before your organization spends a dollar of its IT budget or allocates any resources or time to anything in the name of cybersecurity, three questions must be answered:

- **What is the risk?**
- **Is it the highest priority risk?**
- **What is the most cost-effective way to reduce the risk?**

Security is all about making sure you focus on the right areas of defense. In SEC401 you will learn the language and underlying theory of computer and information security. You will gain the essential and effective security knowledge you will need if you are given the responsibility for securing systems and/or organizations. This course meets both of the key promises SANS makes to our students: (1) You will learn up-to-the-minute skills you can put into practice immediately upon returning to work; and (2) You will be taught by the best security instructors in the industry.

Bryan Simon *SANS Certified Instructor*

Bryan Simon is an internationally recognized expert in cybersecurity who has been working in the information technology and security field since 1991. Over the course of his career, Bryan has held various technical and managerial positions in the education, environmental, accounting, and financial services sectors. Bryan speaks on a regular basis at international conferences and with the press on matters of cybersecurity. He has instructed individuals from the FBI, NATO, and the UN in matters of cybersecurity, on two continents. Bryan has specialized expertise in defensive and offensive capabilities. He has received recognition for his work in IT security, and was most recently profiled by McAfee (part of Intel Security) as an IT Hero. Bryan holds 12 GIAC Certifications including GSEC, GCWN, GCIH, GCFA, GPEN, GWAPT, GAWN, GISP, GCIA, GCED, GCUX, and GISF. Bryan's scholastic achievements have resulted in the honor of sitting as a current member of the SANS Institute Advisory Board, and in his acceptance into the prestigious SANS Cyber Guardian program. Bryan teaches SEC401: Security Essentials Bootcamp Style; SEC501: Advanced Security Essentials – Enterprise Defender; SEC505: Securing Windows and Powershell Automaton; and SEC511: Continuous Monitoring and Security Operations. **@BryanOnSecurity**

401.1 HANDS ON: Networking Concepts

A key way that attackers gain access to a company's resources is through a network connected to the Internet. A company wants to try to prevent as many attacks as possible, but in cases where it cannot prevent an attack, it must detect it in a timely manner. Therefore, an understanding of how networks and the related protocols like TCP/IP work is critical to being able to analyze network traffic and determine what is hostile. It is just as important to know how to protect against these attacks using devices such as routers and firewalls. These essentials, and more, will be covered during this course day in order to provide a firm foundation for the consecutive days of training.

Topics: Setting Up a Lab with Virtual Machines; Network Fundamentals; IP Concepts; IP Behavior; Virtual Machines

401.2 HANDS ON: Defense In-Depth

To secure an enterprise network, you must have an understanding of the general principles of network security. In this course, you will learn about six key areas of network security. The day starts with information assurance foundations. Students look at both current and historical computer security threats, and how they have impacted confidentiality, integrity, and availability. The first half of the day also covers creating sound security policies and password management, including tools for password strength on both Unix and Windows platforms. The second half of the day is spent on understanding the information warfare threat and the six steps of incident handling. The day draws to a close by looking at attack strategies and how the offense operates.

Topics: Information Assurance Foundations; Computer Security Policies; Contingency and Continuity Planning; Access Control; Password Management; Incident Response; Offensive and Defensive Information Warfare; Attack Strategies and Methods

401.3 HANDS ON: Internet Security Technologies

Military agencies, banks, and retailers offering electronic commerce services, as well as dozens of other types of organizations, are striving to understand the threats they are facing and what they can do to address those threats. On day 3, you will be provided with a roadmap to help you understand the paths available to organizations that are considering deploying or planning to deploy various security devices and tools such as intrusion detection systems and firewalls. When it comes to securing your enterprise, there is no single technology that is going to solve all your security issues. However, by implementing an in-depth defense strategy that includes multiple risk-reducing measures, you can go a long way toward securing your enterprise.

Topics: Firewalls and Perimeters; Honeypots; Host-based Protection; Network-based Intrusion Detection and Prevention; Vulnerability Scanning and Remediation; Web Security

401.4 HANDS ON: Secure Communications

There is no silver bullet when it comes to security. However, there is one technology that would help solve a lot of security issues, though few companies deploy it correctly. This technology is cryptography. Concealing the meaning of a message can prevent unauthorized parties from reading sensitive information. Day 4 looks at various aspects of encryption and how it can be used to secure a company's assets. A related area called steganography, or information hiding, is also covered. The day finishes by looking at using the Critical Security Controls for metrics-based dashboards and performing risk assessment across an organization.

Topics: Cryptography; Steganography; Critical Security Controls; Risk Assessment and Auditing

401.5 HANDS ON: Windows Security

Windows is the most widely-used and hacked operating system on the planet. At the same time, the complexities of Active Directory, PKI, BitLocker, AppLocker, and User Account Control represent both challenges and opportunities. This section will help you quickly master the world of Windows security while showing you the tools that can simplify and automate your work. You will complete the day with a solid grounding in Windows security by looking at automation, auditing, and forensics.

Topics: Security Infrastructure; Service Packs, Patches, and Backups; Permissions and User Rights; Security Policies and Templates; Securing Network Services; Auditing and Automation

401.6 HANDS ON: Unix/Linux Security

While organizations do not have as many Unix/Linux systems, for those that do have them, these systems are often among the most critical systems that need to be protected. Day 6 provides step-by-step guidance to improve the security of any Linux system by combining practical how-to instructions with background information for Linux beginners, as well as security advice and best practices for administrators with all levels of expertise.

Topics: Linux Landscape; Permissions and User Accounts; Linux OS Security; Maintenance, Monitoring, and Auditing Linux; Linux Security Tools

You Will Be Able To

- Design and build a network architecture using VLANs, NAC and 802.1x based on an APT indicator of compromise
- Run Windows command line tools to analyze the system looking for high-risk items
- Run Linux command line tools (ps, ls, netstat, etc.) and basic scripting to automate the running of programs to perform continuous monitoring of various tools
- Install VMWare and create virtual machines to operate a virtual lab to test and evaluate the tools/security of systems
- Create an effective policy that can be enforced within an organization and prepare a checklist to validate security, creating metrics to tie into training and awareness
- Identify visible weaknesses of a system utilizing various tools including dumpsec and OpenVAS, and once vulnerabilities are discovered cover ways to configure the system to be more secure
- Build a network visibility map that can be used for hardening of a network – validating the attack surface and covering ways to reduce it through hardening and patching
- Sniff open protocols like telnet and ftp and determine the content, passwords and vulnerabilities utilizing WireShark
- Apply what you learned directly to your job when you go back to work

"This course has given me a great start on truly understanding the fundamentals of security and applying it every day."

-John Houser, First Citizens Bank

SEC504

GCIH Certification
Incident Handler

www.giac.org/gcih

Hacker Tools, Techniques, Exploits, and Incident Handling

Six-Day Program
Mon, July 24 - Sat, July 29
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: John Strand

This course has extended hours

Who Should Attend

- Incident handlers
- Leaders of incident handling teams
- System administrators who are on the front lines defending their systems and responding to attacks
- Other security personnel who are first responders when systems come under attack

"John Strand opened my eyes and helped me understand how to approach the concepts of offensive security and incident handling. He is one of the very best."

-Stephen Ellis, CB&I

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection or one or two disgruntled employees (and whose does not!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth. As defenders, it is essential we understand these hacking tools and techniques.

"If you love cybersecurity and learning how exploits work, you NEED this course."

-Jaid K., U.S. Navy

This course enables you to turn the tables on computer attackers by helping you to understand their tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan. It addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course provides a time-tested, step-by-step process for responding to computer incidents, and a detailed description of how attackers undermine systems so you can prepare for, detect, and respond to them. In addition, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence. Finally, students will participate in a hands-on workshop that focuses on scanning, exploiting, and defending systems. **It will enable you to discover the holes in your system before the bad guys do!**

The course is particularly well-suited to individuals who lead or are a part of an incident handling team. General security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, detect, and respond to attacks.

"[This course is a] good foundation for security incidents.
It's a must-have for security incident handlers/managers."

-Wu Peihui, Citibank

John Strand *SANS Senior Instructor*

Along with SEC504, John Strand also teaches SEC560: Network Penetration Testing and Ethical Hacking and SEC464: Hacker Detection for System Administrators. John is the course author for SEC464. When not teaching for SANS, John co-hosts PaulDotCom Security Weekly, the world's largest computer security podcast. He also is the owner of Black Hills Information Security, specializing in penetration testing and security architecture services. He has presented for the FBI, NASA, the NSA, and at DefCon. In his spare time he writes loud rock music and makes various futile attempts at fly fishing. **@strandjs**

504.1 Incident Handling Step-by-Step and Computer Crime Investigation

The first part of this section looks at the invaluable Incident Handling Step-by-Step Model, which was created through a consensus process involving experienced incident handlers from corporations, government agencies, and educational institutes, and has been proven effective in hundreds of organizations. This section is designed to provide students a complete introduction to the incident handling process, using the six steps (preparation, identification, containment, eradication, recovery, and lessons learned) necessary to prepare for and deal with a computer incident. The second part of this section examines from-the-trenches case studies to understand what does and does not work in identifying computer attackers. This section provides valuable information on the steps a systems administrator can take to improve the chances of catching and prosecuting attackers.

Topics: Preparation; Identification; Containment; Eradication; Recovery; Special Actions for Responding to Different Types of Incidents; Incident Record-Keeping; Incident Follow-Up

504.2 HANDS ON: Computer and Network Hacker Exploits – PART 1

Seemingly innocuous data leaking from your network could provide the clue needed by an attacker to blow your systems wide open. This day-long course covers the details associated with reconnaissance and scanning, the first two phases of many computer attacks.

Topics: Reconnaissance; Scanning; Intrusion Detection System Evasion; Hands-on Exercises for a List of Tools

504.3 HANDS ON: Computer and Network Hacker Exploits – PART 2

Computer attackers are ripping our networks and systems apart in novel ways while constantly improving their techniques. This course covers the third step of many hacker attacks – gaining access. Attackers employ a variety of strategies to take over systems from the network level up to the application level. This section covers the attacks in depth, from the details of buffer overflow and format string attack techniques to the latest in session hijacking of supposedly secure protocols.

Topics: Network-Level Attacks; Gathering and Parsing Packets; Operating System and Application-Level Attacks; Netcat: The Attacker's Best Friend; Hands-on Exercises with a List of Tools

504.4 HANDS ON: Computer and Network Hacker Exploits – PART 3

This course starts out by covering one of the attackers' favorite techniques for compromising systems: worms. We will analyze worm developments over the last two years and project these trends into the future to get a feel for the coming Super Worms we will face. Then the course turns to another vital area often exploited by attackers: web applications. Because most organizations' homegrown web applications do not get the security scrutiny of commercial software, attackers exploit these targets using SQL injection, cross-site scripting, session cloning, and a variety of other mechanisms discussed in detail.

Topics: Password Cracking; Web Application Attacks; Denial of Service Attacks; Hands-on Exercises with a List of Tools

504.5 HANDS ON: Computer and Network Hacker Exploits – PART 4

This day-long course covers the fourth and fifth steps of many hacker attacks: maintaining access and covering their tracks. Computer attackers install backdoors, apply Rootkits, and sometimes even manipulate the underlying kernel itself to hide their nefarious deeds. Each of these categories of tools requires specialized defenses to protect the underlying system. In this course, we will analyze the most commonly used malicious code specimens, as well as explore future trends in malware, including BIOS-level and combo malware possibilities.

Topics: Maintaining Access; Covering the Tracks; Putting It All Together; Hands-on Exercises with a List of Tools

504.6 HANDS ON: Hacker Tools Workshop

Over the years, the security industry has become smarter and more effective in stopping hackers. Unfortunately, hacker tools are becoming smarter and more complex. One of the most effective methods to stop the enemy is to actually test the environment with the same tools and tactics an attacker might use against you. This workshop lets you put what you have learned over the past week into practice.

Topics: Hands-on Analysis

You Will Be Able To

- Apply incident handling processes in-depth, including preparation, identification, containment, eradication, and recovery, to protect enterprise environments
- Analyze the structure of common attack techniques in order to evaluate an attacker's spread through a system and network, anticipating and thwarting further attacker activity
- Utilize tools and evidence to determine the kind of malware used in an attack, including rootkits, backdoors, and trojan horses, choosing appropriate defenses and response tactics for each
- Use built-in command-line tools such as Windows tasklist, wmic, and reg as well as Linux netstat, ps, and lsof to detect an attacker's presence on a machine
- Analyze router and system ARP tables along with switch CAM tables to track an attacker's activity through a network and identify a suspect
- Use memory dumps and the Volatility tool to determine an attacker's activities on a machine, the malware installed, and other machines the attacker used as pivot points across the network
- Gain access to a target machine using Metasploit, and then detect the artifacts and impacts of exploitation through process, file, memory, and log analysis
- Analyze a system to see how attackers use the Netcat tool to move files, create backdoors, and build relays through a target environment
- Run the Nmap port scanner and Nessus vulnerability scanner to find openings on target systems, and apply tools such as tcpdump and netstat to detect and analyze the impacts of the scanning activity
- Apply the tcpdump sniffer to analyze network traffic generated by a covert backdoor to determine an attacker's tactics
- Employ the netstat and lsof tools to diagnose specific types of traffic-flooding denial-of-service techniques and choose appropriate response actions based on each attacker's flood technique
- Analyze shell history files to find compromised machines, attacker-controlled accounts, sniffers, and backdoors

SEC301

GISF Certification
Information Security Fundamentals

www.giac.org/gisf

Intro to Information Security

Five-Day Program
Mon, July 24 - Fri, July 28
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Keith Palmgren

Who Should Attend

- People who are new to information security and in need of an introduction to the fundamentals of security
- Those who feel bombarded with complex technical security terms they don't understand, but want to understand
- Non-IT security managers who deal with technical issues and understand them and who worry their company will be the next mega-breach headline story on the 6 o'clock news
- Professionals with basic computer and technical knowledge in all disciplines who need to be conversant in basic security concepts, principles, and terms, but who don't need "deep in the weeds" detail
- Those who have decided to make a career change to take advantage of the job opportunities in information security and need formal training/certification

To determine if the SANS SEC301 course is right for you, ask yourself five simple questions:

- **Do you have basic computer knowledge, but are new to information security and in need of an introduction to the fundamentals?**
- **Are you bombarded with complex technical security terms that you don't understand?**
- **Are you a non-IT security manager (with some technical knowledge) who lays awake at night worrying that your company will be the next mega-breach headline story on the 6 o'clock news?**
- **Do you need to be conversant in basic security concepts, principles, and terms, even if you don't need "deep in the weeds" detail?**
- **Have you decided to make a career change to take advantage of the job opportunities in information security and need formal training/certification?**

If you answer yes to any of these questions, the **SEC301: Intro to Information Security** training course is for you. Jump-start your security knowledge by receiving insight and instruction from real-world security experts on critical introductory topics that are fundamental to information security. This completely revised five-day comprehensive course covers everything from core terminology to the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles.

This course is designed for students who have a basic knowledge of computers and technology but no prior knowledge of cybersecurity. The hands-on, step-by-step teaching approach will enable you to grasp all of the information presented even if some of the topics are new to you. You'll learn the fundamentals of information security that will serve as the foundation of your InfoSec skills and knowledge for years to come.

Written by a security professional with over 30 years of experience in both the public and private sectors, SEC301 provides uncompromising real-world insight from start to finish. The course prepares you for the Global Information Security Fundamentals (GISF) certification test, as well as for the next course up the line, **SEC401: Security Essentials Bootcamp Style**. It also delivers on the SANS promise: ***You will be able to use the knowledge and skills you learn in SEC301 as soon as you return to work.***

"Labs reinforced the security principles in a real-world scenario."
-Tyler Moore, Rockwell

Keith Palmgren *SANS Senior Instructor*

Keith Palmgren is an IT security professional with over 30 years of experience specializing in the field. He began his career with the U.S. Air Force working with cryptographic keys and codes management. He also worked in what was at the time the newly-formed Air Force computer security department. Following the Air Force, Keith worked as an MIS director for a small company before joining AT&T/Lucent as a Senior Security Architect working on engagements with the DoD and the National Security Agency. Later, as Security Consulting Practice Manager for both Sprint and Netigy, Keith built and ran the security consulting practice. He was responsible for all security consulting world-wide and for leading dozens of security professionals on many consulting engagements across all business spectrums. For the last several years, Keith has run his own company, NetIP, Inc. He divides his time between consulting, training, and freelance writing projects. In his career, Keith has trained over 10,000 IT professionals and authored more than 20 IT security training courses including the SANS SEC301 course. Keith currently holds 10 computer security certifications (CISSP, GSEC, GCIH, GCED, GISF, CEH, Security+, Network+, A+, CTT+). **@kpalmgren**

301.1 HANDS ON: Security's Foundation

Every good security practitioner and every good security program begins with the same mantra: learn the fundamentals. SEC301 starts by instilling familiarity with core security terms and principles. By the time you leave the classroom after the first day, you will fully understand the Principle of Least Privilege and the Confidentiality, Integrity, and Availability (CIA) Triad, and you'll see why those principles drive all security discussions. You will be conversant in the fundamentals of risk management, security policy, and authentication/authorization/accountability.

301.2 HANDS ON: Computer Functions and Networking

This course day begins with an explanation of how computers handle numbers using decimal, binary, and hexadecimal numbering systems. It also provides an understanding of how computers encode letters using ASCII (American Standard Code for Information Interchange). We then spend the remainder of the day on networking. All attacks or exploits have one thing in common: they take something that exists for perfectly valid reasons and misuse it in malicious ways. Always! So as security practitioners, to grasp what is invalid we must first understand what is valid – that is, how things like networks are supposed to work. Only once we have that understanding can we hope to understand the mechanics of malicious misuse of those networks – and only with that knowledge can we understand how security devices such as firewalls seek to thwart those attacks. Day two begins with a non-technical explanation of how data move across a network. From there we move to fundamental terminology dealing with network types and standards. You'll learn about common network hardware such as switches and routers, and you'll finally grasp what is meant by terms like "protocol" and "encapsulation." We'll give a very basic introduction to network addressing and port numbers and then work our way up the Open Systems Interconnection (OSI) protocol stack, introducing more detail only as we proceed to the next layer. In other words, we explain networking starting in non-technical terms and gradually progress to more technical detail as students are ready to take the next step. By the end of our discussions, you'll have a fundamental grasp of any number of critical technical networking acronyms that you've often heard and never quite understood: TCP/IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP, and DNS.

301.3 HANDS ON: An Introduction to Cryptography

One of the most complex issues faced by security practitioners, cryptography is not a topic you can explain in passing, so we will spend some time on it. Not to worry, we won't take you through the math behind cryptography, but we'll look at basic crypto terminology and processes. What is steganography? What is substitution and transposition? What is a "work factor" in cryptography and why does it matter? What do we mean by symmetric and asymmetric key cryptography and "cryptographic hash", and why do you need to know? How are those concepts used together in the real world to create cryptographic systems?

301.4 HANDS ON: Cybersecurity Technologies – PART 1

Our fourth day in the classroom begins our exploration of cybersecurity technologies. We begin with wireless network security (WiFi and Bluetooth), and mobile device security (i.e., cell phones). We follow that with a brief look at some common attacks. We then move into a discussion of malware and anti-malware technologies. From there, we move into a discussion of network security technologies and methods including compartmentalization, firewalls, intrusion detection and prevention systems, sniffers, content filters, and so on. We end the day with an examination of several data protection protocols used for email encryption, secure remote access, secure web access, secure file transfer, and Virtual Private Network technologies.

301.5 HANDS ON: Cybersecurity Technologies – PART 2

The final day of our SEC301 journey continues the discussion of cybersecurity technologies. The day begins by looking at the system security to include hardening operating systems, patching, virtual machines, cloud computing, and backup. We move to application security to learn about browser security and web security, as well as email and instant messaging concerns. We discuss competitive intelligence gathering methods and how you can defend against them. We close the course with an explanation of awareness training and social engineering so that students understand what it is and why it's so difficult to defend against.

You Will Be Able To

- Communicate with confidence regarding information security topics, terms, and concepts
- Understand and apply the Principles of Least Privilege
- Understand and apply the Confidentiality, Integrity, and Availability (CIA) Triad
- Build better passwords that are more secure while also being easier to remember and type
- Grasp basic cryptographic principles, processes, procedures, and applications
- Gain an understanding of computer network basics
- Have a fundamental grasp of any number of critical technical networking acronyms: TCP/IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP, and DNS
- Utilize built-in Windows tools to see your network settings
- Recognize and discuss various security technologies including anti-malware, firewalls, and intrusion detection systems
- Determine your "Phishing IQ" to more easily identify SPAM email messages
- Understand physical security issues and how they support cybersecurity
- Understand incident response, business continuity, and disaster recovery planning at an introductory level
- Access a number of websites to better understand password security, encryption, phishing, browser security, etc.

"SEC301 is the perfect blend of technical and practical information for someone new to the field, and I would recommend it to a friend."

-Steve Mecco, Draper

SEC501

GCED Certification
Certified Enterprise Defender

www.giac.org/gced

Advanced Security Essentials – Enterprise Defender

Six-Day Program
Mon, July 24 - Sat, July 29
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Paul A. Henry

Who Should Attend

- Incident response and penetration testers
- Security Operations Center engineers and analysts
- Network security professionals
- Anyone who seeks technical in-depth knowledge about implementing comprehensive security solutions

"SEC501 is the perfect course to immerse enterprise security staff into essential skills. Failing to attend this course is done at the peril of your organization."

-John N. Johnson,
Houston Police Department

Effective cybersecurity is more important than ever as attacks become stealthier, have a greater financial impact, and cause broad reputational damage. **SEC501: Advanced Security Essentials – Enterprise Defender** builds on a solid foundation of core policies and practices to enable security teams to defend their enterprise.

It has been said of security that "prevention is ideal, but detection is a must." However, detection without response has little value. Network security needs to be constantly improved to prevent as many attacks as possible and to swiftly detect and respond appropriately to any breach that does occur. This PREVENT - DETECT - RESPONSE strategy must be in place both externally and internally. As data become more portable and networks continue to be porous, there needs to be an increased focus on data protection. Critical information must be secured regardless of whether it resides on a server, in a robust network architecture, or on a portable device.

"The hands-on lab approach is a great way to make sense of what is being taught, and working with other classmates helped expand our knowledge and brought cohesion."

-Rachel Weiss, UPS Inc.

Despite an organization's best efforts to prevent network attacks and protect its critical data, some attacks will still be successful. Therefore, organizations need to be able to detect attacks in a timely fashion. This is accomplished by understanding the traffic that is flowing on your networks, looking for indications of an attack, and performing penetration testing and vulnerability analysis against your organization to identify problems and issues before a compromise occurs.

Finally, once an attack is detected we must react quickly and effectively and perform the forensics required. Knowledge gained by understanding how the attacker broke in can be fed back into more effective and robust preventive and detective measures, completing the security lifecycle.

Paul A. Henry *SANS Senior Instructor*

Paul Henry is one of the world's foremost global information security and computer forensic experts, with more than 20 years of experience managing security initiatives for Global 2000 enterprises and government organizations worldwide. Paul is a principal at vNet Security, LLC and is keeping a finger on the pulse of network security as the security and forensic analyst at Lumension Security. Throughout his career, Paul has played a key strategic role in launching new network security initiatives to meet our ever-changing threat landscape. He also advises and consults on some of the world's most challenging and high-risk information security projects, including the National Banking System in Saudi Arabia, the Reserve Bank of Australia, the U.S. Department of Defense's Satellite Data Project, and both government as well as telecommunications projects throughout Southeast Asia. Paul is frequently cited by major and trade print publications as an expert on computer forensics, technical security topics, and general security trends and serves as an expert commentator for network broadcast outlets such as FOX, NBC, CNN, and CNBC. In addition, Paul regularly authors thought leadership articles on technical security issues, and his expertise and insight help shape the editorial direction of key security publications, such as the *Information Security Management Handbook*, to which he is a consistent contributor. Paul serves as a featured and keynote speaker at seminars and conferences worldwide, delivering presentations on diverse topics including anti-forensics, network access control, cyber crime, DDoS attack risk mitigation, firewall architectures, security architectures, and managed security services. **@phenrycissp**

501.1 HANDS ON: Defensive Network Infrastructure

Making your network secure from attack starts with designing, building, and implementing a robust network infrastructure. There are many aspects to implementing a defense-in-depth network that are often overlooked when companies focus only on functionality. Achieving the proper balance between business drivers and core information security requires that an organization build a secure network that is mission-resilient to a variety of potential attacks. On the first day students will learn how to design and implement a functionality-rich, secure network and how to maintain and update it as the threat landscape evolves.

Topics: Introducing Network Infrastructure as Targets for Attack; Implementing the Cisco Gold Standard to Improve Security; Advanced Layer 2 and 3 Controls

501.2 HANDS ON: Packet Analysis

Packet analysis and intrusion detection are at the core of timely detection. Detecting attacks is becoming more difficult as attacks become more stealthy and more difficult to find. Only by understanding the core principles of traffic analysis can one become a skilled analyst and distinguish normal traffic from attack traffic. Security professionals must be able to detect new, advanced zero-day attacks before they compromise a network. Prevention, detection, and reaction must all be closely knit so that once an attack is detected, defensive measures can be adapted, proactive forensics implemented, and the organization can continue to operate.

Topics: Architecture Design & Preparing Filters; Detection Techniques and Measures; Advanced IP Packet Analysis; Intrusion Detection Tools

501.3 HANDS ON: Pentest

An organization must understand the changing threat landscape and compare that against its own vulnerabilities. On day three students will be shown the variety of tests that can be run and how to perform penetration testing in an effective manner. Students will learn about external and internal penetration testing and the methods of black, gray, and white box testing. Penetration testing is critical to identify an organization's exposure points, but students will also learn how to prioritize and fix these vulnerabilities to increase the overall security of an organization.

Topics: Variety of Penetration Testing Methods; Vulnerability Analysis; Key Tools and Techniques; Basic Pen Testing; Advanced Pen Testing

501.4 HANDS ON: First Responder

Any organization connected to the Internet or with employees is going to have attacks launched against it. Security professionals need to understand how to perform incident response, analyze what is occurring, and restore their organization back to a normal state as soon as possible. Day four will equip students with a proven six-step process to follow in response to an attack – prepare, identify, contain, eradicate, recover, and learn from previous incidents. Students will learn how to perform forensic investigations and find indications of an attack. This information will be fed into the incident response process to ensure that the attack is prevented from occurring again in the future.

Topics: Incident Handling Process and Analysis; Forensics and Incident Response

501.5 HANDS ON: Malware

As security professionals continue to build more proactive security measures, attackers' methods will continue to evolve. A common way for attackers to target, control, and break into as many systems as possible is through the use of malware. Therefore it is critical that students understand what type of malware is currently available to attackers as well as the future trends and methods of exploiting systems. With this knowledge students can then learn how to analyze, defend, and detect malware on systems and minimize the impact to the organization.

Topics: Malware; Microsoft Malware; External Tools and Analysis

501.6 HANDS ON: Data Loss Prevention

Cybersecurity is all about managing, controlling, and mitigating risk to critical assets, which in almost every organization are composed of data or information. Perimeters are still important, but we are moving away from a fortress model and moving towards a focus on data. This is based on the fact that information no longer solely resides on servers where properly configured access control lists can limit access and protect our information; it can now be copied to laptops and plugged into networks. Data must be protected no matter where it resides.

Topics: Risk Management; Data Classification; Digital Rights Management; Data Loss Prevention (DLP)

You Will Be Able To

- Identify the threats against network infrastructures and build defensible networks that minimize the impact of attacks
- Access tools that can be used to analyze a network to prevent attacks and detect the adversary
- Decode and analyze packets using various tools to identify anomalies and improve network defenses
- Understand how the adversary compromises networks and how to respond to attacks
- Perform penetration testing against an organization to determine vulnerabilities and points of compromise
- Apply the six-step incident handling process
- Use various tools to identify and remediate malware across your organization
- Create a data classification program and deploy data loss prevention solutions at both a host and network level

"Best SANS course I've taken. The content is relevant and the labs were interactive. Strongly recommended for SOC analysts and IR professionals."

-Brett Smetanka, KeyBank

SEC503

Intrusion Detection In-Depth

GCIA Certification
Certified Intrusion Analyst

www.giac.org/gcia

Six-Day Program
Mon, July 24 - Sat, July 29
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: David Hoelzer

Who Should Attend

- Intrusion detection (all levels), system, and security analysts
- Network engineers/administrators
- Hands-on security managers

"This course directly covers the necessary knowledge and skill set I use day to day for my job. The added insight is worth the price of the course."

-Michael Garrett,
Federal Reserve Bank of San Francisco

"Thank you SANS! I have doubled my security knowledge."

-Jerome Joseph, Nationwide Insurance

Reports of prominent organizations being hacked and suffering irreparable reputational damage have become all too common. How can you prevent your company from becoming the next victim of a major cyber attack?

ALSO AVAILABLE VIA SIMULCAST

See page 96 for details.

Preserving the security of your site in today's threat environment is more challenging than ever before. The security landscape is continually changing from what was once only perimeter protection to protecting exposed and mobile systems that are almost always connected and sometimes vulnerable. Security-savvy employees who can help detect and prevent intrusions are therefore in great demand. Our goal in **SEC503: Intrusion Detection In-Depth** is to acquaint you with the core knowledge, tools, and techniques to defend your networks with insight and awareness. The training will prepare you to put your new skills and knowledge to work immediately upon returning to a live environment.

Mark Twain said, "It is easier to fool people than to convince them that they've been fooled." Too many IDS/IPS solutions provide a simplistic red/green, good/bad assessment of traffic and too many untrained analysts accept that feedback as the absolute truth. This course emphasizes the theory that a properly trained analyst uses an IDS alert as a starting point for examination of traffic, not as a final assessment. SEC503 imparts the philosophy that the analyst must have access and the ability to examine the alerts to give them meaning and context. You will learn to investigate and reconstruct activity to deem if it is noteworthy or a false indication.

SEC503: Intrusion Detection In-Depth delivers the technical knowledge, insight, and hands-on training you need to defend your network with confidence. You will learn about the underlying theory of TCP/IP and the most used application protocols, such as DNS and HTTP, so that you can intelligently examine network traffic for signs of an intrusion. You will get plenty of practice learning to master different open source tools like tcpdump, Wireshark, Snort, Bro, tshark, and SiLK. Daily hands-on exercises suitable for all experience levels reinforce the course book material so that you can transfer knowledge to execution. Basic exercises include assistive hints while advanced options provide a more challenging experience for students who may already know the material or who have quickly mastered new material.

David Hoelzer *SANS Faculty Fellow*

David Hoelzer is a high-scoring SANS instructor and author of more than 20 sections of SANS courseware. He is an expert in a variety of information security fields, having served in most major roles in the IT and security industries over the past 25 years. Recently, David was called upon to serve as an expert witness for the Federal Trade Commission for ground-breaking GLBA Privacy Rule litigation. David has been highly involved in governance at the SANS Technology Institute, serving as a member of the Curriculum Committee as well as Audit Curriculum Lead. As a SANS instructor, David has trained security professionals from organizations including NSA, DHHS, Fortune 500 companies, various Department of Defense sites, national laboratories, and many colleges and universities. David is a Research Fellow at the Center for Cybermedia Research as well as the Identity Theft and Financial Fraud Research Operations Center (ITFF/ROC). He also is an Adjunct Research Associate for the UNLV Cybermedia Research Lab and a Research Fellow with the Internet Forensics Lab. David has written and contributed to more than 15 peer-reviewed books, publications, and journal articles. Currently, David serves as the principal examiner and director of research for Enclave Forensics, a New York/Las Vegas based incident response and forensics company. He also serves as the chief information security officer for Cyber-Defense, an open-source security software solution provider. In the past, David served as the director of the GIAC Certification program, bringing the GIAC Security Expert certification to life. David holds a BS in IT, Summa Cum Laude, having spent time either attending or consulting for Stony Brook University, Binghamton University, and American Intercontinental University. **@it_audit**

503.1 HANDS ON: Fundamentals of Traffic Analysis – PART 1

Day 1 provides a refresher or introduction, depending on your background, to TCP/IP. It describes the need to understand packet structure and content. It covers the essential foundations such as the TCP/IP communication model, theory of bits, bytes, binary and hexadecimal, an introduction. We introduce the use of open source Wireshark and tcpdump for analysis.We begin our exploration of the TCP/IP communication model with the study of the link layer, the IP layer, both IPv4 and IPv6 and packet fragmentation in both. We describe the layers and analyze traffic not just in theory and function, but from the perspective of an attacker and defender. All traffic is discussed and displayed using the two open-source tools, Wireshark and tcpdump.

Topics: Concepts of TCP/IP; Introduction to Wireshark; Network Access/Link Layer: Layer 2; IP Layer: Layer 3

503.2 HANDS ON: Fundamentals of Traffic Analysis – PART 2

Day 2 continues where the previous day ended in understanding the TCP/IP model. Two essential tools, Wireshark and tcpdump, are further explored, using their advanced features to give you the skills to analyze your own traffic. The focus of these tools on Day 2 is filtering traffic of interest in Wireshark using display filters and in tcpdump using Berkeley Packet Filters. We proceed with our exploration of the TCP/IP layers covering TCP, UDP, and ICMP. Once again, we describe the layers and analyze traffic not just in theory and function, but from the perspective of an attacker and defender.

Topics: Wireshark Display Filters; Writing tcpdump Filters; TCP; UDP; ICMP

503.3 HANDS ON: Application Protocols and Traffic Analysis

Day 3 introduces the versatile packet crafting tool Scapy. It is a very powerful Python-based tool that allows the manipulation, creation, reading, and writing packets. Scapy can be used to craft packets to test the detection capability of an IDS/IPS, especially important when a new user-created IDS rule is added, for instance for a recently announced vulnerability. The examination of TCP/IP culminates with an exploration of the application protocol layer. The concentration is on some of the most widely used, and sometimes vulnerable, crucial application protocols: DNS, HTTP(S), SMTP, and Microsoft communications. Our focus is on protocol analysis, a key skill in intrusion detection. IDS/IPS evasions are the bane of the analyst, so the theory and possible implications of evasions at different protocol layers are examined.

Topics: Scapy; Advanced Wireshark; Detection Methods for Application Protocols; DNS; Microsoft Protocols; HTTP(2)/TLS; SMTP; IDS/IPS Evasion Theory

503.4 HANDS ON: Network Monitoring: Snort and Bro

The fundamental knowledge gained from the first three days provides a fluid progression into one of the most popular days SEC503. Snort and Bro are widely deployed open source IDS/IPS solutions that have been industry standards for many years. The day begins with a discussion on network architecture including the features of intrusion detection and prevention devices along with a discussion about options and requirement of devices that can sniff and capture the traffic for inspection. Next, the topic of the analyst's role in the detection process is examined. Before Snort and Bro are discussed, the capabilities and limitations are considered. Snort detection flow, running Snort, and rules are explored with an emphasis on writing efficient rules. It is likely that false positives and negatives will occur and tips for dealing with them are presented. Bro's unique capability to use its own scripting language to write code to analyze patterns of event-driven behavior is one of the most powerful detection tools available to the analyst. We discuss how this enables monitoring and correlating activity and demonstrate with examples.

Topics: Network Architecture; Introduction to IDS/IPS Analysis; Snort; Bro

503.5 HANDS ON: Network Traffic Forensics

The penultimate day continues the format of less instruction and more hands-on training using three separate incidents that must be analyzed. The three incident scenarios are introduced with some new material to be used in the related hands-on analysis. This material includes an introduction to network forensics analysis for the first scenario. It continues with using network flow records to assist in analysis of the traffic from the second scenario. It concludes with the third scenario where Command and Control channels are discussed and managing analysis when very large packet capture files are involved.

Topics: Introduction to Network Forensics Analysis; Using Network Flow Records; Examining Command and Control Traffic; Analysis of Large pcaps

503.6 HANDS ON: NetWars: IDS Version

The week culminates with a fun hands-on NetWars: IDS Version challenge. Students compete on teams to answer many questions that require using tools and theory covered in the first five days. This is a great way to end the week because it reinforces what was learned by challenging the student to think analytically and strengthens confidence to employ what was learned in in a real-world environment.

You Will Be Able To

- Configure and run open-source Snort and write Snort signatures
- Configure and run open-source Bro to provide a hybrid traffic analysis framework
- Understand TCP/IP component layers to identify normal and abnormal traffic
- Use open-source traffic analysis tools to identify signs of an intrusion
- Comprehend the need to employ network forensics to investigate traffic to identify and investigate a possible intrusion
- Use Wireshark to carve out suspicious file attachments
- Write tcpdump filters to selectively examine a particular traffic trait
- Craft packets with Scapy
- Use the open-source network flow tool SiLK to find network behavior anomalies
- Use your knowledge of network architecture and hardware to customize placement of IDS sensors and sniff traffic off the wire

"This training directly correlates to my agency's mission of conducting network forensics/intrusion investigations."

-Chris G., AFOSI

"I would recommend this to network/security people who have some experience already but need to sharpen their skills."

-M.S., AOL

SEC505

GCWN Certification
Windows Security Administrator

www.giac.org/gcwn

Securing Windows and PowerShell Automation

Six-Day Program
Mon, July 24 - Sat, July 29
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jason Fossen

Who Should Attend

- Security Operations engineers
- Windows endpoint and server administrators
- Anyone who wants to learn PowerShell automation
- Anyone implementing the NSA Top 10 Mitigations
- Anyone implementing the CIS Critical Security Controls
- Those deploying or managing a Public Key Infrastructure or smart cards
- Anyone who needs to reduce malware infections

"Really great course for anyone involved in the administration or securing of Windows environments."

-David Hazar, Oracle

Hackers know how to use PowerShell for evil. Do you know how to use it for good? In SEC505 you will learn PowerShell and Windows security hardening at the same time. SecOps requires automation, and Windows automation means PowerShell.

You've run a vulnerability scanner and applied patches – *now what?* A major theme of this course is defensible design: we have to assume that there will be a breach, so we need to build in damage control from the beginning. Whack-a-mole incident response cannot be our only defensive strategy – we'll never win, and we'll never get ahead of the game. By the time your monitoring system tells you a Domain Admin account has been compromised, IT'S TOO LATE.

For the assume breach mindset, we must carefully delegate limited administrative powers so that the compromise of one administrator account is not a total catastrophe. Managing administrative privileges is a tough problem, so this course devotes an entire day to just this one critical task.

"I loved the course! When I return to the office, I am recommending it to the rest of my team."

-Alex Fox, Federal Home Loan Bank Chicago

Learning PowerShell is also useful for another kind of security: *job security*. Employers are looking for people with these skills. You don't have to know any PowerShell to attend the course, we will learn it together. About half the labs during the week are PowerShell, while the rest use graphical security tools. PowerShell is free and open source on GitHub for Linux and Mac OS, too.

This course is not a vendor show to convince you to buy another security appliance or to install yet another endpoint agent. The idea is to use built-in or free Windows and Active Directory security tools when we can (especially PowerShell and Group Policy) and then purchase commercial products only when absolutely necessary.

If you are an IT manager or CIO, the aim for this course is to have it pay for itself 10 times over within two years, because automation isn't just good for SecOps/DevOps, it can save money, too.

This course is designed for systems engineers, security architects, and the Security Operations (SecOps) team. The focus of the course is on how to automate the NSA Top 10 Mitigations and the CIS Critical Security Controls related to Windows, especially the ones that are difficult to implement in large environments.

This is a fun course and a real eye-opener, even for Windows administrators with years of experience. We don't cover patch management, share permissions, or other such basics – the aim is to go far beyond that. Come have fun learning PowerShell and agile Windows security at the same time!

Jason Fossen *SANS Faculty Fellow*

Jason Fossen is a principal security consultant at Enclave Consulting LLC, a published author, and a frequent public speaker on Microsoft security issues. He is the sole author of the SANS week-long Securing Windows course (SEC505), maintains the Windows day of Security Essentials (SEC401.5), and has been involved in numerous other SANS projects since 1998. He graduated from the University of Virginia, received his master's degree from the University of Texas at Austin, and holds a number of professional certifications. He currently lives in Dallas, Texas. **@JasonFossen**

505.1 HANDS ON: PowerShell Automation and Security

PowerShell is made for Security Operations (SecOps) automation on Windows. Today's course covers what you need to know to get started using PowerShell. You don't need to have any prior scripting experience. We will do PowerShell labs throughout the week, so today is not the only PowerShell content. Don't worry, you won't be left behind, the PowerShell labs will walk you through every step. Learning PowerShell is not only good for network security, it's also good for job security.

Topics: Overview and Security; Getting Around Inside PowerShell; What Can We Do With It?; Write Your Own Scripts

505.2 HANDS ON: Continuous Secure Configuration Enforcement

Running a vulnerability scanner is easy; remediating vulnerabilities across a large number of systems is what can be difficult. Most vulnerabilities are fixed by applying patches, but this course does not talk about patch management, you're doing that already. What about the other vulnerabilities, the ones not fixed by applying patches? These vulnerabilities are, by definition, remediated by configuration changes. That's the hard part. We need a secure architecture designed for SecOps.

Topics: Continuous Secure Configuration Enforcement; Group Policy Precision Targeting; Server Hardening for SecOps/DevOps; PowerShell Desired State Configuration (DSC)

505.3 HANDS ON: Windows PKI and Smart Cards

Don't believe what you hear on the street: Public Key Infrastructure (PKI) is not that hard to manage on Windows! You'll be pleasantly surprised at how much Group Policy, Active Directory, and PowerShell can help you manage your PKI. And we don't really have a choice anymore: having a PKI is pretty much mandatory for Microsoft security and cloud computing. The labs in today's course mostly use graphical PKI tools, but there are also PowerShell labs to delete unwanted certificates installed by malware, audit our lists of trusted CAs, perform file hashing, compare thousands of recorded file hashes at two different times (similar to Tripwire), and encrypt secret data in our own PowerShell applications, such as for encrypting admin passwords.

Topics: Why Is A PKI Necessary?; How to Install the Windows PKI; How to Manage Your PKI; Deploying Smart Cards

505.4 HANDS ON: Administrative Compromise and Privilege Management

Is there a Windows version of sudo, like on Linux? Yes, it's called Just Enough Admin (JEA) for PowerShell. JEA allows non-admin users to remotely execute commands with administrative privileges, but without exposing any administrative credentials to them (kind of like setuid root on Linux). With JEA, all PowerShell commands are blocked by default except those you explicitly allow, and you can even use regular expression patterns to limit the arguments to those commands. And for less-technical users who'd prefer a graphical interface, don't forget that graphical applications can be built on top of PowerShell JEA too. In this course, we will see how to set up JEA and PowerShell Remoting.

Topics: You Don't Know The Power!; Compromise of Administrative Powers; PowerShell Just Enough Admin (JEA); Active Directory Permissions and Delegation

505.5 HANDS ON: Endpoint Protection and Pre-Forensics

Despite our best efforts, we must still assume breach. Pre-forensics describes what we should configure on Windows to prepare for a security incident. It's not about the response itself, it's about the preparations, such as enabling centralized logging. Preparation is half the battle. Pre-forensics also means gathering ongoing operational data to give to the Hunt Team and incident responders while they look for indicators of compromise. When the Hunt Team has a baseline of what is "normal" on a server to compare against, identifying what is new and out of place is vastly easier. PowerShell makes creating these scheduled baseline snapshots easy.

Topics: Anti-Exploitation; IPSec Port Permissions; Host-Based Firewalls; Pre-Forensics

505.6 HANDS ON: Defensible Networking and Blue Team WMI

Hackers love Windows Management Instrumentation (WMI), and so should we! SecOps automation uses the WMI service a lot, so today's course has PowerShell for WMI. Beyond WMI, there are several other network services or protocols that we cannot live without, but which are targeted by hackers. To move laterally inside the LAN, hackers go after SSL/TLS, DNS, Kerberos, Remote Desktop Protocol (RDP), PowerShell Remoting, or the File and Print Sharing protocol (SMB/CIFS). As more virtual machines are moved up to the networks of cloud providers, RDP use over the Internet will increase. But with PKI, IPSec encryption, and proper hardening, RDP can be made safe enough to use, even for administrators.

Topics: PowerShell and WMI; Hardening DNS; Dangerous Protocols We Can't Live Without

You Will Be Able To

- Execute PowerShell commands on remote systems and begin to write your own PowerShell scripts
- Harden PowerShell itself against abuse, and enable transcription logging
- Use Group Policy to execute PowerShell scripts on an almost unlimited number of hosts, while using Group Policy Object permissions, organizational units, and Windows Management Instrumentation (WMI) to target just the systems that need the scripts run
- Use PowerShell Desired State Configuration (DSC) and Server Manager scripting for the sake of SecOps/DevOps automation of server hardening
- Assuming a breach will occur, use Group Policy and PowerShell to grant administrative privileges in a way that reduces the harm if an attack succeeds
- Configure PowerShell remoting to use Just Enough Admin (JEA) policies to create a Windows version of Linux sudo and setuid root
- Configure mitigations against attacks such as pass-the-hash, Kerberos golden tickets, Remote Desktop Protocol (RDP) man-in-the-middle, Security Access Token abuse, and others
- Use PowerShell and Group Policy to manage the Microsoft Enhanced Mitigation Experience Toolkit (EMET), AppLocker whitelisting rules, INF security templates, Windows Firewall rules, IPSec rules, and many other security-related settings
- Install and manage a full Windows Public Key Infrastructure (PKI), including smart cards, certificate auto-enrollment, Online Certificate Status Protocol (OCSP) web responders, and detection of spoofed root Certification Authorities (CAs)
- Harden SSL/TLS, RDP, DNS, and SMB against attacks. This includes deploying DNSSEC, DNS sinkholes for malware, SMB encryption, and TLS cipher suite optimization
- Use PowerShell with the WMI service, such as remote command execution, searching event logs, and doing a remote inventory of user applications

"The good guys are way behind on PowerShell and the bad guys are catching up. This course will close that knowledge gap."

-Jason Vasquez, Bloomberg L.P.

SEC506

Securing Linux/Unix

GCUX Certification
UNIX Security Administrator

www.giac.org/gcux

Six-Day Program
Mon, July 24 - Sat, July 29
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Hal Pomeranz

Who Should Attend

- Security professionals looking to learn the basics of securing Unix operating systems
- Experienced administrators looking for in-depth descriptions of attacks on Unix systems and how they can be prevented
- Administrators needing information on how to secure common Internet applications on the Unix platform
- Auditors, incident responders, and InfoSec analysts who need greater visibility into Linux and Unix security tools, procedures, and best practices

"Best of any course I've ever taken. I love the idea of being able to bring the material home to review."

-Eric Koebelen, Incident Response US

SEC506: Securing Linux/Unix provides in-depth coverage of Linux and Unix security issues that includes specific configuration guidance and practical, real-world examples, tips, and tricks. We examine how to mitigate or eliminate general problems that apply to all Unix-like operating systems, including vulnerabilities in the password authentication system, file system, virtual memory system, and applications that commonly run on Linux and Unix.

The course will teach you the skills to use freely available tools to handle security issues, including SSH, AIDE, sudo, lsof, and many others. SANS' practical approach uses hand-on exercises every day to ensure that you will be able to use these tools as soon as you return to work. We will also put these tools to work in a special section that covers simple forensic techniques for investigating compromised systems.

Topics

- **Memory Attacks, Buffer Overflows**
- **File System Attacks, Race Conditions**
- **Trojan Horse Programs and Rootkits**
- **Monitoring and Alerting Tools**
- **Unix Logging and Kernel-Level Auditing**
- **Building a Centralized Logging Infrastructure**
- **Network Security Tools**
- **SSH for Secure Administration**
- **Server Lockdown for Linux and Unix**
- **Controlling Root Access with sudo**
- **SELinux and chroot() for Application Security**
- **DNSSEC Deployment and Automation**
- **mod_security and Web Application Firewalls**
- **Secure Configuration of BIND, Sendmail, Apache**
- **Forensic Investigation**

Course Author Statement

"A wise man once said, 'How are you going to learn anything if you know everything already?' And yet there seems to be a quiet arrogance in the Unix community that we have figured out all of our security problems, as if to say, 'Been there, done that.' All I can say is that what keeps me going in the Unix field, and the security industry in particular, is that there is always something new to learn, discover, or invent. In 20 plus years on the job, what I have learned is how much more there is that I can learn. I think this is also true for the students in my courses. I regularly get comments back from students who say things like, 'I have been using Unix for 20 years, and I still learned a lot in this class.' That is really rewarding."

- Hal Pomeranz

Hal Pomeranz *SANS Faculty Fellow*

Hal Pomeranz is an independent digital forensic investigator who has consulted on cases ranging from intellectual property theft to employee sabotage, organized cybercrime, and malicious software infrastructures. He has worked with law enforcement agencies in the United States and Europe and with global corporations. Equally at home in the Windows or Mac environment, Hal is recognized as an expert in the analysis of Linux and Unix systems. His research on EXT4 file system forensics provided a basis for the development of open-source forensic support for this file system. His EXT3 file recovery tools are used by investigators worldwide. Hal is a SANS Lethal Forensicator, and is the creator of the SANS Linux/Unix Security track (GCUX). He holds the GCFA and GREM certifications and teaches the related courses in the SANS Forensics curriculum. He is a respected author and speaker at industry gatherings worldwide. Hal is a regular contributor to the SANS Computer Forensics blog and co-author of the Command Line Kung Fu blog.
@hal_pomeranz

506.1 HANDS ON: Hardening Linux/Unix Systems – PART 1

This course tackles some of the most important techniques for protecting your Linux/Unix systems from external attacks. But it also covers what those attacks are so that you know what you're defending against. This is a full-disclosure course with in-class demos of actual exploits and hands-on exercises to experiment with various examples of malicious software, as well as different techniques for protecting Linux/Unix systems.

Topics: Memory Attacks and Overflows; Vulnerability Minimization; Boot-Time Configuration; Encrypted Access; Host-Based Firewalls

506.2 HANDS ON: Hardening Linux/Unix Systems – PART 2

Continuing our exploration of Linux/Unix security issues, this course focuses on local exploits and access control issues. What do attackers do once they gain access to your systems? How can you detect their presence? How do you protect against attackers with physical access to your systems? What can you do to protect against mistakes (or malicious activity) by your own users?

Topics: Rootkits and Malicious Software; File Integrity Assessment; Physical Attacks and Defenses; User Access Controls; Root Access Control with sudo; Warning Banners; Kernel Tuning For Security

506.3 HANDS ON: Hardening Linux/Unix Systems – PART 3

Monitoring your systems is critical for maintaining a secure environment. This course digs into the different logging and monitoring tools available in Linux/Unix, and looks at additional tools for creating a centralized monitoring infrastructure such as Syslog-NG. Along the way, the course introduces a number of useful SSH tips and tricks for automating tasks and tunneling different network protocols in a secure fashion.

Topics: Automating Tasks With SSH; AIDE via SSH; Linux/Unix Logging Overview; SSH Tunneling; Centralized Logging with Syslog-NG

506.4 HANDS ON: Application Security – PART 1

This course examines common application security tools and techniques. The SCP-Only Shell will be presented as an example of using an application under chroot() restriction, and as a more secure alternative to file-sharing protocols like anonymous FTP. The SELinux application whitelisting mechanism will be examined in depth. Tips for troubleshooting common SELinux problems will be covered and students will learn how to craft new SELinux policies from scratch for new and locally developed applications. Significant hands-on time will be provided for students to practice these concepts.

Topics: chroot() for Application Security; The SCP-Only Shell; SELinux Basics; SELinux and the Reference Policy

506.5 HANDS ON: Application Security – PART 2

This course is a full day of in-depth analysis on how to manage some of the most popular application-level services securely on a Linux/Unix platform. We will tackle the practical issues involved with securing three of the most commonly used Internet servers on Linux and Unix: BIND, Sendmail, and Apache. Beyond basic security configuration information, we will take an in-depth look at topics like DNSSec and Web Application Firewalls with mod_security and the Core Rules.

Topics: BIND; DNSSec; Apache; Web Application Firewalls with mod_security

506.6 HANDS ON: Digital Forensics for Linux/Unix

This hands-on course is designed to be an information-rich introduction devoted to basic forensic principles and techniques for investigating compromised Linux and Unix systems. At a high level, it introduces the critical forensic concepts and tools that every administrator should know and provides a real-world compromise for students to investigate using the tools and strategies discussed in class.

Topics: Tools Throughout; Forensic Preparation and Best Practices; Incident Response and Evidence Acquisition; Media Analysis; Incident Reporting

You Will Be Able To

- Significantly reduce the number of vulnerabilities in the average Linux/Unix system by disabling unnecessary services
- Protect your systems from buffer overflows, denial-of-service, and physical access attacks by leveraging OS configuration settings
- Configure host-based firewalls to block attacks from outside.
- Deploy SSH to protect administrative sessions, and leverage SSH functionality to securely automate routine administrative tasks
- Use sudo to control and monitor administrative access
- Create a centralized logging infrastructure with Syslog-NG, and deploy log monitoring tools to scan for significant events
- Use SELinux to effectively isolate compromised applications from harming other system services
- Securely configure common Internet-facing applications such as Apache, BIND
- Investigate compromised Unix/Linux systems with the Sleuthkit, lsof, and other open-source tools
- Understand attacker rootkits and how to detect them with AIDE and rkhunter/chkrootkit

"This course is painting a big picture of how various system tools can be used together to support security, and I like how the labs are continuing to build upon each other."

-Chris H., U.S. Naval Academy

SEC511

GMON Certification
Continuous Monitoring

www.giac.org/gmon

Continuous Monitoring and Security Operations

Six-Day Program
Mon, July 24 - Sat, July 29
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Eric Conrad

This course has evening Bootcamp Sessions

Who Should Attend

- Security architects
- Senior security engineers
- Technical security managers
- Security Operations Center (SOC) analysts, engineers, and managers
- CND analysts
- Individuals working to implement Continuous Diagnostics and Mitigation (CDM), Continuous Security Monitoring (CSM), or Network Security Monitoring (NSM)

We continue to underestimate the tenacity of our adversaries! Organizations are investing significant time and financial and human resources trying to combat cyber threats and prevent cyber attacks, but despite this tremendous effort organizations are still getting compromised. The traditional perimeter-focused, prevention-dominant approach to security architecture has failed to prevent intrusions. No network is impenetrable, a reality that business executives and security professionals alike have to accept. Prevention is crucial, and we can't lose sight of it as the primary goal. However, a new proactive approach to security is needed to enhance the capabilities of organizations to detect threats that will inevitably slip through their defenses.

The underlying challenge for organizations victimized by an attack is timely incident detection. Industry data suggest that most security breaches typically go undiscovered for an average of seven months. Attackers simply have to find one way into most organizations, because they know that the lack of visibility and internal security controls will then allow them to methodically carry out their mission and achieve their goals.

The Defensible Security Architecture, Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Security Monitoring (CSM) taught in this course will best position your organization or Security Operations Center (SOC) to analyze threats and detect anomalies that could indicate cybercriminal behavior. The payoff for this new proactive approach will be early detection of an intrusion, or successfully thwarting the efforts of attackers altogether. The National Institute of Standards and Technology (NIST) developed guidelines described in NIST SP 800-137 for Continuous Monitoring (CM), and this course will greatly increase your understanding and enhance your skills in implementing CM utilizing the NIST framework.

SEC511 will take you on quite a journey. We start by exploring traditional security architecture to assess its current state and the attacks against it. Next, we discuss and discover modern security design that represents a new proactive approach to such architecture that can be easily understood and defended. We then transition to how to actually build the network and endpoint security, and then carefully navigate our way through automation, NSM/CDM/CSM. For timely detection of potential intrusions, the network and systems must be proactively and continuously monitored for any changes in the security posture that might increase the likelihood that attackers will succeed.

Your SEC511 journey will conclude with one last hill to climb! The final day (Day 6) features a Capture-the-Flag competition that challenges you to apply the skills and techniques learned in the course to detect and defend the modern security architecture that has been designed. Course authors Eric Conrad and Seth Misenar have designed the Capture-the-Flag competition to be fun, engaging, comprehensive, and challenging. You will not be disappointed!

Eric Conrad *SANS Senior Instructor*

Eric Conrad is lead author of the book The CISSP® Study Guide. Eric's career began in 1991 as a UNIX systems administrator for a small oceanographic communications company. He gained information security experience in a variety of industries, including research, education, power, Internet, and healthcare. He is now president of Backshore Communications, a company focusing on intrusion detection, incident handling, information warfare, and penetration testing. He is a graduate of the SANS Technology Institute with a master of science degree in information security engineering. In addition to the CISSP®, he holds the prestigious GIAC Security Expert (GSE) certification as well as the GIAC GPEN, GCIH, GCIA, GCFA, GAWN, and GSEC certifications. Eric also blogs about information security at ericconrad.com. **@eric_conrad**

511.1 HANDS ON: Current State Assessment, SOCs, and Security Architecture

We begin with the end in mind by defining the key techniques and principles that will allow us to get there. An effective modern Security Operations Center (SOC) or security architecture must enable an organization's ability to rapidly find intrusions to facilitate containment and response. Both significant knowledge and a commitment to continuous monitoring are required to achieve this goal.

Topics: Current State Assessment, SOCs, and Security Architecture; Modern Security Architecture Principles; Frameworks and Enterprise Security Architecture; Security Architecture – Key Techniques/Practices; Security Operations Center

511.2 HANDS ON: Network Security Architecture

Understanding the problems with the current environment and realizing where we need to get to is far from sufficient: we need a detailed roadmap to bridge the gap between the current and desired state. Day 2 introduces and details the components of our infrastructure that become part of a defensible network security architecture and SOC. We are long past the days when a perimeter firewall and ubiquitous antivirus were sufficient security. There are many pieces and moving parts that make up a modern defensible security architecture.

Topics: SOCs/Security Architecture – Key Infrastructure Devices; Segmented Internal Networks; Defensible Network Security Architecture Principles Applied

511.3 HANDS ON: Network Security Monitoring

Designing a SOC or security architecture that enhances visibility and detective capabilities represents a paradigm shift for most organizations. However, the design is simply the beginning. The most important element of a modern security architecture is the emphasis on detection. The network security architecture presented in days one and two emphasized baking visibility and detective capabilities into the design. Now we must figure out how to look at the data and continuously monitor the enterprise for evidence of compromise or changes that increase the likelihood of compromise.

Topics: Continuous Monitoring Overview; Network Security Monitoring (NSM); Practical NSM Issues; Cornerstone NSM

511.4 HANDS ON: Endpoint Security Architecture

One of the hallmarks of modern attacks is an emphasis on client-side exploitation. The days of breaking into networks via direct frontal assaults on unpatched mail, web, or DNS servers are largely behind us. We must focus on mitigating the risk of compromise of clients. Day four details ways in which endpoint systems can be both more resilient to attack and also enhance detective capabilities.

Topics: Security Architecture – Endpoint Protection; Dangerous Endpoint Applications; Patching

511.5 HANDS ON: Automation and Continuous Security Monitoring

Network Security Monitoring (NSM) is the beginning: we need to not only detect active intrusions and unauthorized actions, but also to know when our systems, networks, and applications are at an increased likelihood for compromise. A strong way to achieve this is through Continuous Security Monitoring (CSM) or Continuous Diagnostics and Mitigation (CDM). Rather than waiting for the results of a quarterly scan or an annual penetration test to determine what needs to be addressed, continuous monitoring proactively and repeatedly assesses and reassesses the current security posture for potential weaknesses that need be addressed.

Topics: CSM Overview; Industry Best Practices; Winning CSM Techniques; Maintaining Situational Awareness; Host, Port and Service Discovery; Vulnerability Scanning; Monitoring Patching; Monitoring Applications; Monitoring Service Logs; Monitoring Change to Devices and Appliances; Leveraging Proxy and Firewall Data; Configuring Centralized Windows Event Log Collection; Monitoring Critical Windows Events; Scripting and Automation

511.6 HANDS ON: Capstone: Design, Detect, Defend

The course culminates in a team-based design, detect, and defend-the-flag competition that is a full day of hands-on work applying the principles taught throughout the week.

Topics: Security Architecture; Assess-Provided Architecture; Continuous Security Monitoring; Using Tools/Scripts Assessing the Initial State; Quickly/Thoroughly Find All Changes Made

You Will Be Able To

- Analyze a security architecture for deficiencies
- Apply the principles learned in the course to design a defensible security architecture
- Understand the importance of a detection-dominant security architecture and Security Operations Center (SOC)
- Identify the key components of Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Monitoring (CM)
- Determine appropriate security monitoring needs for organizations of all sizes
- Implement robust Network Security Monitoring/Continuous Security Monitoring (NSM/CSM)
- Utilize tools to support implementation of Continuous Monitoring per NIST guidelines SP800-137
- Determine requisite monitoring capabilities for a SOC environment
- Determine capabilities required to support continuous monitoring of key Critical Security Controls

"This course has been awesome at teaching me how to use tools and existing architecture in ways I haven't thought of before!"

-John Hubbard, GlaxoSmithKline

"Keep on giving real-life scenarios to spice up the class. This class was perfect."

-Genevieve Opaye-Tetteh, eProcess Int SA

SEC579

Virtualization and Software-Defined Security *NEW!*

Five-Day Program
Mon, July 24 - Fri, July 28
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Dave Shackleford

Who Should Attend

- Security personnel who are tasked with securing virtualization and private cloud infrastructure
- Network and systems administrators who need to understand how to architect, secure, and maintain virtualization and cloud technologies
- Technical auditors and consultants who need to gain a deeper understanding of VMware virtualization from a security and compliance perspective

"SEC579 was one of the best-produced SANS courses I have taken. The blend of ops and security was extremely valuable."

-Scott Towery, Visions

One of today's most rapidly evolving and widely deployed technologies is server virtualization. **SEC579: Virtualization and Software-Defined Security** is intended to help security, IT operations, and audit and compliance professionals build, defend, and properly assess both virtual and converged infrastructures, as well as understand software-defined networking and infrastructure security risks.

Many organizations are already realizing cost savings from implementing virtualized servers, and systems administrators love the ease of deployment and management of virtualized systems. More and more organizations are deploying desktop, application, and network virtualization as well. There are even security benefits of virtualization: easier business continuity and disaster recovery, single points of control over multiple systems, role-based access, and additional auditing and logging capabilities for large infrastructure.

With these benefits comes a dark side, however. Virtualization technology is the focus of many new potential threats and exploits, and it presents new vulnerabilities that must be managed. There are also a vast number of configuration options that security and system administrators need to understand, with an added layer of complexity that has to be managed by operations teams. Virtualization technologies also connect to network infrastructure and storage networks, and require careful planning with regard to access controls, user permissions, and traditional security controls.

In addition, many organizations are evolving virtualized infrastructure into private clouds using converged infrastructure that employs software-defined tools and programmable stack layers to control large, complex data centers. Security architecture, policies, and processes will need to be adapted to work within a converged infrastructure, and there are many changes that security and operations teams will need to accommodate to ensure that assets are protected.

This course will cover core operational functions like secure network design and segmentation, building secure systems, and secure virtualization implementation and controls. Cutting-edge topics like software-defined networking and container technology will also be covered in detail with an emphasis on security techniques and controls. Security-focused virtualization, integration, and monitoring will be covered at length. Attacks and threats to virtual environments will be discussed, and students will learn how to perform vulnerability assessments and penetration tests in their virtual environments. We'll also look at how to implement network intrusion detection and access controls, implement log and event management, and perform forensics and incident handling in virtual and converged data centers. Finally, students will learn how to perform technical audits and assessments of their in-house and public cloud environments, creating reports and documenting technical controls. This instruction will heavily emphasize automation and scripting techniques.

Dave Shackleford *SANS Senior Instructor*

Dave Shackleford is the owner and principal consultant of Voodoo Security and a SANS analyst and course author. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering, and is a VMware vExpert with extensive experience designing and configuring secure virtualized infrastructures. He has previously worked as CSO for Configuresoft, CTO for the Center for Internet Security, and as a security architect, analyst, and manager for several Fortune 500 companies. Dave is the author of the Sybex book *Virtualization Security: Protecting Virtualized Environments*, as well as the coauthor of *Hands-On Information Security* from Course Technology. Recently Dave coauthored the first published course on virtualization security for the SANS Institute. Dave currently serves on the Board of Directors at the SANS Technology Institute and helps lead the Atlanta chapter of the Cloud Security Alliance. **@daveshackleford**

579.1 HANDS ON: Core Concepts of Virtualization Security

The first day of class will cover the foundations of virtualization infrastructure and different types of technology. We will define and clarify the differences between server, desktop, application, and storage virtualization, and dissect the various virtualization elements that make up the architecture one by one, with a focus on the security configurations that will help you create or revise your virtualization design to be as secure as possible.

Topics: **Virtualization Components and Architecture Designs; Different Types of Virtualization, Ranging from Desktops to Servers and Applications; Hypervisor Lockdown Controls for VMware, Microsoft Hyper-V, and Citrix Xen; Virtual Machine Security Configuration Options, with a Focus on VMware VMX Files; Storage Security and Design Considerations; Locking Down Management Servers and Clients for vCenter, XenServer, and Microsoft SCVMM; Security Design Considerations for VDI**

579.2 HANDS ON: Virtualization and Software-Defined Security Architecture and Design

Day 2 starts with several topics that round out our discussions on virtualization and infrastructure components, delving into container technology and converged infrastructure platforms and tools (along with security considerations for both). We'll then begin our discussion of virtualization and software-defined architecture and networking. We'll cover design concepts and models, network capabilities and models in virtual environments, with time devoted to virtual switches and other platforms, and look at how network security adapts to fit into a virtual infrastructure.

Topics: **Container Technology Security Considerations; Converged Infrastructure Security Considerations; Defining Software-Defined Components and Architectural Models; Designing Security for Software-Defined Environments; Virtual Network Design Cases with Pros and Cons of Each; Virtual Switches and Port Groups, with Security Options Available; Commercial and Open-Source Virtual Switches Available, with Configuration Options; Segmentation Techniques, Including VLANs and PVLANs; Software-Defined Networking and Architecture; Network Isolation and Access Control; Adapting Firewalls, IPS, Proxies, and More to Virtual Environments; Products and Capabilities Available Today**

You Will Be Able To

- Lock down and maintain a secure configuration for all components of a virtualization environment
- Design a secure virtual network architecture
- Evaluate virtual firewalls, intrusion detection and prevention systems, and other security infrastructure
- Evaluate security for converged and software-defined environments
- Perform vulnerability assessments and pen tests in virtual and private cloud environments, and acquire forensic evidence
- Perform audits and risk assessments within a virtual or private cloud environment

"This is the future of IT and security. Knowledge is power!"

-Joe Marshall, Exelon

579.3 HANDS ON: Virtualization Threats, Vulnerabilities, and Attacks

This session will delve into the offensive side of security specific to virtualization and cloud technologies. We will first examine a number of specific attack scenarios, then we will go through the entire penetration testing and vulnerability assessment lifecycle, with an emphasis on virtualization tools and technologies. We'll progress through scanners and how to use them to assess virtual systems, then turn to virtualization exploits and attack toolkits that can be easily added into existing penetration test regimens. We will also cover some specific techniques that may help in cloud environments, providing examples of scenarios where certain tools and exploits are less effective or more risky to use than others.

Topics: **Threats and Attack Research Related to Virtualization Infrastructure; Attack Models That Pertain to Virtualization and Cloud Environments; Threat Modeling for Virtualization and Software-Defined Technology; Specific Virtualization Platform Attacks and Exploits; Pen Testing Cycles with a Focus on Virtualization Attack Types; Password Attacks Against Virtualization and Software-Defined Platforms; How to Modify Vulnerability Management Processes and Scanning Configuration to Get the Best Results in Virtualized Environments; How to Use Attack Frameworks Like VASTO to Exploit Virtualization Systems**

579.4 HANDS ON: Defending Virtualization and Software-Defined Technologies

We will start off with an analysis of anti-malware techniques, looking at traditional antivirus, whitelisting, and other tools and techniques to combat malware, with a specific eye toward virtualization and converged environments. Then we will turn to intrusion detection, monitoring traffic and learning about logs and log management in virtual environments. The second half of this session will focus on incident response and forensics in a virtualized or converged infrastructure and how students can adapt forensics processes and tools to work in virtual environments.

Topics: **Data Protection in Virtual and Converged Environments; Identity and Access Management in Virtual and Software-Defined Environments; How to Implement Intrusion Detection Tools and Processes in a Virtual Environment; What Kinds of Logs and Logging are Most Critical for Identifying Attacks and Live Incidents in Virtual Environments?; How Anti-Malware Tools Function in Virtual Environments; How the Six-Step Incident Response Process Can Be Modified and Adapted to Work with Virtual Infrastructure; What Kinds of Incidents to Look for Within Virtual Environments, and What the Warning Signs Are; Processes and Procedures to Build and Grow Incident Response Capabilities for Virtual Environments; How Forensics Processes and Tools Should Be Used and Adapted for Virtual Systems; What Tools Are Best to Get the Most Accurate Results From Virtual Machine System Analysis?; How to Most Effectively Capture Virtual Machines for Forensic Evidence Analysis; What Can Be Done to Analyze Hypervisor Platforms, and What Does the Future Hold for VM Forensics?**

579.5 HANDS ON: Virtualization Operations, Auditing, and Monitoring

Today's session will start off with a lively discussion on virtualization assessment and auditing. We will cover the top virtualization configuration and hardening guides from DISA, CIS, Microsoft, and VMware, and talk about the most critical information to take away from these guides and implement. Students will learn to implement audit and assessment techniques by scripting with the VI CLI, as well as some general shell scripting! We will look at automation and orchestration tools and techniques that can help to streamline and manage configuration and auditing (examples include Chef, Puppet, and more), as well as monitoring techniques that provide a feedback loop.

Topics: **Key Configuration Controls from the Leading DISA, CIS, VMware, and Microsoft Hardening Guides; Sound Configuration Management and Patching in Virtual Infrastructure; Scripting Techniques in VI CLI and PowerShell for Automating Audit and Assessment Processes; Sample Scripts That Help Implement Key Audit Functions; Automation and Orchestration with Puppet, Chef, ManageEngine, etc.; Full Hardening-Guide-Scripted Audit**

SANS NETWARS EXPERIENCE

Earn up to 6 CPEs!

*Three Ways to Participate at SANSFIRE 2017 for FREE!**

DFIR NETWARS TOURNAMENT

The DFIR NetWars Tournament is an incident simulator packed with a vast amount of forensic and incident response challenges covering host forensics, network forensics, and malware and memory analysis. It is developed by incident responders and analysts who use these skills daily to stop data breaches and solve crimes. Sharpen your team's skills prior to being involved in a real incident.

Who Should Attend

- Digital forensic analysts
- Forensic examiners
- Reverse-engineering and malware analysts
- Incident responders
- Law enforcement officers, federal agents, or detectives
- Security Operations Center analysts
- Cyber crime investigators
- Media exploitation analysts

Core NETWARS EXPERIENCE

The Core NetWars Experience is a computer and network security challenge designed to test a participant's experience and skills in a safe, controlled environment while having a little fun with your fellow IT security professionals. Many enterprises, government agencies, and military bases are using NetWars to help identify skilled personnel and as part of extensive hands-on training. With Core NetWars, you'll build a wide variety of skills while having a great time.

Who Should Attend

- Security professionals
- System administrators
- Network administrators
- Ethical hackers
- Penetration testers
- Incident handlers
- Security auditors
- Vulnerability assessment personnel
- Security Operations Center staff

Introducing Experience 5.0 "A Whole New Experience!"

NEW! CYBER DEFENSE NETWARS COMPETITION

The all-new Cyber Defense NetWars Competition is a defense-focused challenge aimed at testing your ability to solve problems and secure your systems from compromise. With so much focus on offense, Cyber Defense NetWars is a truly unique experience and opportunity to test your skills in architecture, operations, threat hunting, log analysis, packet analysis, cryptography, and much more!

Who Should Attend

- System administrators
- Enterprise defenders
- Architects
- Network engineers
- Incident responders
- Security operations specialists
- Security analysts
- Security auditors
- Builders and breakers

All three NetWars competitions will be played over two evenings: July 27-28

Prizes will be awarded at the conclusion of the games.

***REGISTRATION IS LIMITED AND IS FREE**

for students attending any long course at SANSFIRE 2017 *(NON-STUDENT ENTRANCE FEE IS $1,520).*

Register at **www.sans.org/sansfire**

SANS Intermediate and Specialized Skills

Penetration Testing & Vulnerability Analysis

Penetration Testing & Vulnerability Analysis

SEC**560** Network Penetration Testing and Ethical Hacking	**GPEN** Certification Penetration Tester
SEC**542** Web App Penetration Testing and Ethical Hacking	**GWAPT** Certification Web Application Penetration Tester

Summary: High-performing security organizations need specially trained professionals who can continuously challenge the defenses and monitoring systems set up by the cyber defense operations teams, and discover vulnerabilities to be addressed that might otherwise be exploited by attackers. Professionals focusing on this career path must be able to test both network and wireless vulnerabilities and understand these environments before advancing to additional areas.

SEC560 and **SEC542** teach you the skills that are core to this type of role. An additional nine SANS penetration testing courses in advanced and specialized topics allow you to mold your career into a particular practice area or task. Review the following pages for detailed information about all of these courses and the certifications that validate your acquired skills.

Who This Path Is for: Information Security Engineers, Analysts, and Risk Consultants need to master this coursework in particular to hone their penetration testing, ethical hacker, and vulnerability analysis skills.

Why This Training Is Important: These courses teach proper planning, scoping, and recon, and dive deep into scanning, target exploitation, password attacks, web app configuration, identity, and authentication; custom scripting as well as the workings of interception proxies. Together with dozens of detailed, hands-on labs, this training allows you to go back to work with the practical, real-world examples and practice needed to do your job efficiently and masterfully.

> **"I was pleasantly humbled, challenged, encouraged and trained. I feel 100% more qualified to defend my company's network after taking this training."**
>
> -Ivan Dominguez, NWCU.com

SEC560

GPEN Certification
Penetration Tester

www.giac.org/gpen

Network Penetration Testing and Ethical Hacking

Six-Day Program
Mon, July 24 - Sat, July 29
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Ed Skoudis

This course has extended hours

Who Should Attend

- Security personnel whose job involves assessing networks and systems to find and remediate vulnerabilities
- Penetration testers
- Ethical hackers
- Defenders who want to better understand offensive methodologies, tools, and techniques
- Auditors who need to build deeper technical skills
- Red and blue team members
- Forensics specialists who want to better understand offensive tactics

"Ed is an excellent instructor! Best training by far in 30 years in IT."

-Bruce Perrin, State of Texas

As a cybersecurity professional, you have a unique responsibility to find and understand your organization's vulnerabilities, and to work diligently to mitigate them before the bad guys pounce. Are you ready? SANS SEC560, our flagship course for penetration testing, fully arms you to address this task head-on.

SEC560 is the must-have course for every well-rounded security professional.

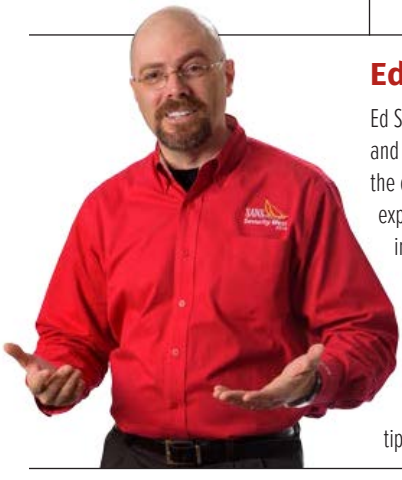
With comprehensive coverage of tools, techniques, and methodologies for network penetration testing, SEC560 truly prepares you to conduct high-value penetration testing projects step-by-step and end-to-end. Every organization needs skilled information security personnel who can find vulnerabilities and mitigate their effects, and this entire course is specially designed to get you ready for that role. The course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks, and web app manipulation, with more than 30 detailed hands-on labs throughout. The course is chock-full of practical, real-world tips from some of the world's best penetration testers to help you do your job safely, efficiently...and masterfully.

Learn the best ways to test your own systems before the bad guys attack.

SEC560 is designed to get you ready to conduct a full-scale, high-value penetration test – and on the last day of the course you'll do just that. After building your skills in comprehensive and challenging labs over five days, the course culminates with a final full-day, real-world penetration test scenario. You'll conduct an end-to-end pen test, applying knowledge, tools, and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization, demonstrating the knowledge you've mastered in this course.

You will bring comprehensive penetration testing and ethical hacking know-how back to your organization.

You will learn how to perform detailed reconnaissance, studying a target's infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. Our hands-on labs will equip you to scan target networks using best-of-breed tools. We won't just cover run-of-the-mill options and configurations, we'll also go over the lesser known but super-useful capabilities of the best pen test toolsets available today. After scanning, you'll learn dozens of methods for exploiting target systems to gain access and measure real business risk. You'll dive deep into post-exploitation, password attacks, and web apps, pivoting through the target environment to model the attacks of real-world bad guys to emphasize the importance of defense in depth.



Ed Skoudis *SANS Faculty Fellow*

Ed Skoudis is the founder of Counter Hack, an innovative organization that designs, builds, and operates popular InfoSec challenges and simulations including CyberCity, NetWars, Cyber Quests, and Cyber Foundations. As director of the CyberCity project, Ed oversees the development of missions that help train cyber warriors in how to defend the kinetic assets of a physical, miniaturized city. Ed's expertise includes hacker attacks and defenses, incident response, and malware analysis, with over 15 years of experience in information security. Ed authored and regularly teaches the SANS courses on network penetration testing (SEC560) and incident response (SEC504), helping over 3,000 information security professionals each year improve their skills and abilities to defend their networks. He has performed numerous security assessments; conducted exhaustive anti-virus, anti-spyware, Virtual Machine, and IPS research; and responded to computer attacks for clients in government, military, financial, high technology, healthcare, and other industries. Previously, Ed served as a security consultant with InGuardians, International Network Services (INS), Global Integrity, Predictive Systems, SAIC, and Bell Communications Research (Bellcore). Ed also blogs about command line tips and penetration testing. **@edskoudis**

560.1 HANDS ON: Comprehensive Pen Test Planning, Scoping, and Recon

In this section of the course, you will develop the skills needed to conduct a best-of-breed, high-value penetration test. We will go in-depth on how to build penetration testing infrastructure that includes all the hardware, software, network infrastructure, and tools you will need to conduct great penetration tests, with specific low-cost recommendations for your arsenal. We will then cover formulating a pen test scope and rules of engagement that will set you up for success, including a role-play exercise. We'll also dig deep into the reconnaissance portion of a penetration test, covering the latest tools and techniques, including hands-on document metadata analysis to pull sensitive information about a target environment, as well as a lab using Recon-ng to plunder a target's DNS infrastructure for information such as the anti-virus tools the organization relies on.

Topics: **The Mindset of the Professional Pen Tester; Building a World-Class Pen Test Infrastructure; Creating Effective Pen Test Scopes and Rules of Engagement; Detailed Recon Using the Latest Tools; Effective Pen Test Reporting to Maximize Impact; Mining Search Engine Results; Document Metadata Extraction and Analysis**

560.2 HANDS ON: In-Depth Scanning

We next focus on the vital task of mapping the target environment's attack surface by creating a comprehensive inventory of machines, accounts, and potential vulnerabilities. We will look at some of the most useful scanning tools freely available today and run them in numerous hands-on labs to help hammer home the most effective way to use each tool. We will also conduct a deep dive into some of the most useful tools available to pen testers today for formulating packets: Scapy and Netcat. We finish the day covering vital techniques for false-positive reduction so you can focus your findings on meaningful results and avoid the sting of a false positive. And we will examine the best ways to conduct your scans safely and efficiently.

Topics: **Tips for Awesome Scanning; Tcpdump for the Pen Tester; Nmap In-Depth; Version Scanning with Nmap; Vulnerability Scanning with Nessus; False-Positive Reduction; Packet Manipulation with Scapy; Enumerating Users; Netcat for the Pen Tester; Monitoring Services During a Scan**

560.3 HANDS ON: Exploitation

In this section, we look at the many kinds of exploits that penetration testers use to compromise target machines, including client-side exploits, service-side exploits, and local privilege escalation. We'll see how these exploits are packaged in frameworks like Metasploit and its mighty Meterpreter. You'll learn in-depth how to leverage Metasploit and the Meterpreter to compromise target environments. We'll also analyze the topic of anti-virus evasion to bypass the target organization's security measures, as well as methods for pivoting through target environments, all with a focus on determining the true business risk of the target organization.

Topics: **Comprehensive Metasploit Coverage with Exploits/Stagers/Stages; Strategies and Tactics for Anti-Virus Evasion; In-Depth Meterpreter Analysis, Hands-On; Implementing Port Forwarding Relays for Merciless Pivots; How to Leverage Shell Access of a Target Environment**

560.4 HANDS ON: Post-Exploitation and Merciless Pivoting

Once you've successfully exploited a target environment, penetration testing gets extra exciting as you perform post-exploitation, gathering information from compromised machines and pivoting to other systems in your scope. This section of the course zooms in on pillaging target environments and building formidable hands-on command line skills. We'll cover Windows command line skills in-depth, including PowerShell's awesome abilities for post-exploitation. We'll see how we can leverage malicious services and the incredible WMIC toolset to access and pivot through a target organization. We'll then turn our attention to password guessing attacks, discussing how to avoid account lockout, as well as numerous options for plundering password hashes from target machines including the great Mimikatz Kiwi tool. Finally, we'll look at Metasploit's fantastic features for pivoting, including the msfconsole route command.

Topics: **Windows Command Line Kung Fu for Penetration Testers; PowerShell's Amazing Post-Exploitation Capabilities; Password Attack Tips; Account Lockout and Strategies for Avoiding It; Automated Password Guessing with THC-Hydra; Retrieving and Manipulating Hashes from Windows, Linux, and Other Systems; Pivoting through Target Environments; Extracting Hashes and Passwords from Memory with Mimikatz Kiwi**

560.5 HANDS ON: In-Depth Password Attacks and Web App Pen Testing

In this section of the course, we'll go even deeper in exploiting one of the weakest aspects of most computing environments: passwords. You'll custom-compile John the Ripper to optimize its performance in cracking passwords. You'll look at the amazingly full-featured Cain tool, running it to crack sniffed Windows authentication messages. We'll see how Rainbow Tables really work to make password cracking much more efficient, all hands-on. And we'll cover powerful "pass-the-hash" attacks, leveraging Metasploit, the Meterpreter, and more. We then turn our attention to web application pen testing, covering the most powerful and common web app attack techniques with hands-on labs for every topic we address. We'll cover finding and exploiting cross-site scripting (XSS), cross-site request forgery (XSRF), command injection, and SQL injection flaws in applications such as online banking, blog sites, and more.

Topics: **Password Cracking with John the Ripper; Sniffing and Cracking Windows Authentication Exchanges Using Cain; Using Rainbow Tables to Maximum Effectiveness; Pass-the-Hash Attacks with Metasploit and More; Finding and Exploiting Cross-Site Scripting; Cross-Site Request Forgery; SQL Injection; Leveraging SQL Injection to Perform Command Injection; Maximizing Effectiveness of Command Injection Testing**

560.6 HANDS ON: Penetration Test and Capture-the-Flag Workshop

This lively session represents the culmination of the network penetration testing and ethical hacking course. You'll apply all of the skills mastered in the course so far in a full-day, hands-on workshop during which you'll conduct an actual penetration test of a sample target environment. We'll provide the scope and rules of engagement, and you'll work with a team to achieve your goal of finding out whether the target organization's Personally Identifiable Information (PII) is at risk. As a final step in preparing you for conducting penetration tests, you'll make recommendations about remediating the risks you identify.

Topics: **Applying Penetration Testing and Ethical Hacking Practices End-to-End; Scanning; Exploitation; Post-Exploitation; Merciless Pivoting; Analyzing Results**

You Will Be Able To

- Develop tailored scoping and rules of engagement for penetration testing projects to ensure the work is focused, well defined, and conducted in a safe manner
- Conduct detailed reconnaissance using document metadata, search engines, and other publicly available information sources to build a technical and organizational understanding of the target environment
- Utilize a scanning tool such as Nmap to conduct comprehensive network sweeps, port scans, OS fingerprinting, and version scanning to develop a map of target environments
- Choose and properly execute Nmap Scripting Engine scripts to extract detailed information from target systems
- Configure and launch a vulnerability scanner such as Nessus so that it safely discovers vulnerabilities through both authenticated and unauthenticated scans, and customize the output from such tools to represent the business risk to the organization
- Analyze the output of scanning tools to manually verify findings and perform false positive reduction using Netcat and the Scapy packet crafting tools
- Utilize the Windows and Linux command lines to plunder target systems for vital information that can further overall penetration test progress, establish pivots for deeper compromise, and help determine business risks
- Configure an exploitation tool such as Metasploit to scan, exploit, and then pivot through a target environment
- Conduct comprehensive password attacks against an environment, including automated password guessing (while avoiding account lockout), traditional password cracking, rainbow table password cracking, and pass-the-hash attacks
- Launch web application vulnerability scanners and then manually exploit Cross-Site Request Forgery, Cross-Site Scripting, Command Injection, and SQL Injection to understand the business risk faced by an organization

SEC542

GWAPT Certification
Web Application Penetration Tester

www.giac.org/gwapt

Web App Penetration Testing and Ethical Hacking

Six-Day Program
Mon, July 24 - Sat, July 29
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Seth Misenar

Who Should Attend

- General security practitioners
- Penetration testers
- Ethical hackers
- Web application developers
- Website designers and architects

"This training boosted my thoughts and perspective on IT. Taught me how to think outside of the box."
-Ephraim P., U.S. Air Force

"SEC542 is a step-by-step introduction to testing and penetrating web applications – a must for anyone who builds, maintains, or audits web systems."
-Brad Milhorn, i12P LLC

Web applications play a vital role in every modern organization. However, if your organization doesn't properly test and secure its web apps, adversaries can compromise these applications, damage business functionality, and steal data. Unfortunately, many organizations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems.

SEC542 helps students move beyond push-button scanning to professional, thorough, and high-value web application penetration testing.

Customers expect web applications to provide significant functionality and data access. Even beyond the importance of customer-facing web applications, internal web applications increasingly represent the most commonly used business tools within any organization. Unfortunately, there is no "patch Tuesday" for custom web applications, and major industry studies find that web application flaws play a major role in significant breaches and intrusions. Adversaries increasingly focus on these high-value targets either by directly abusing public-facing applications or by focusing on web apps as targets after an initial break-in.

Modern cyber defense requires a realistic and thorough understanding of web application security issues. Anyone can learn to sling a few web hacks, but effective web application penetration testing requires something deeper.

SEC542 enables students to assess a web application's security posture and convincingly demonstrate the impact of inadequate security that plagues most organizations.

In this course, students will come to understand major web application flaws and their exploitation. Most importantly, they'll learn a field-tested and repeatable process to consistently find these flaws and convey what they have learned to their organizations. Even technically gifted security geeks often struggle with helping organizations understand risk in terms relatable to business. Much of the art of penetration testing has less to do with learning how adversaries are breaking in than it does with convincing an organization to take the risk seriously and employ appropriate countermeasures. The goal of SEC542 is to better secure organizations through penetration testing, and not just show off hacking skills. This course will help you demonstrate the true impact of web application flaws through exploitation.

In addition to high-quality course content, SEC542 focuses heavily on in-depth, hands-on labs to ensure that students can immediately apply all they learn.

In addition to having more than 30 formal hands-on labs, the course culminates in a web application pen test tournament, powered by the SANS NetWars Cyber Range. This Capture-the-Flag event on the final day brings students into teams to apply their newly acquired command of web application penetration testing techniques in a fun way that hammers home lessons learned.

Seth Misenar *SANS Senior Instructor*

Seth Misenar is the founder of and now the lead consultant for Jackson, Mississippi-based Context Security, which provides information security thought leadership, independent research, and security training. Seth's background includes network and web application penetration testing, vulnerability assessment, regulatory compliance efforts, security architecture design, and general security consulting. He has previously served as both physical and network security consultant for Fortune 100 companies as well as the Health Insurance Portability and Accountability Act and as information security officer for a state government agency. Prior to becoming a security geek, Seth received a bachelor's degree in philosophy from Millsaps College, where he was twice selected for a Ford Teaching Fellowship. Also, Seth is no stranger to certifications and thus far has achieved credentials that include CISSP, GPEN, GWAPT, GSEC, GCIA, GCIH, GCWN, GCFA, and MCSE. **@sethmisenar**

542.1 HANDS ON: Introduction and Information Gathering

Understanding the attacker's perspective is key to successful web application penetration testing. The course begins by thoroughly examining web technology, including protocols, languages, clients and server architectures, from the attacker's perspective. We will also examine different authentication systems, including Basic, Digest, Forms and Windows Integrated authentication, and discuss how servers use them and attackers abuse them.

Topics: Overview of the Web from a Penetration Tester's Perspective; Exploring the Various Servers and Clients; Discussion of the Various Web Architectures; Discovering How Session State Works; Discussion of the Different Types of Vulnerabilities; Defining a Web Application Test Scope and Process; Defining Types of Penetration Testing; Heartbleed Exploitation; Utilizing the Burp Suite in Web App Penetration Testing

542.2 HANDS ON: Configuration, Identity, and Authentication Testing

The second day starts the actual penetration testing process, beginning with the reconnaissance and mapping phases. Reconnaissance includes gathering publicly available information regarding the target application and organization, identifying the machines that support our target application, and building a profile of each server, including the operating system, specific software and configuration. The discussion is underscored through several practical, hands-on labs in which we conduct reconnaissance against in-class targets.

Topics: Discovering the Infrastructure Within the Application; Identifying the Machines and Operating Systems; Secure Sockets Layer (SSL) Configurations and Weaknesses; Exploring Virtual Hosting and Its Impact on Testing; Learning Methods to Identify Load Balancers; Software Configuration Discovery; Exploring External Information Sources; Learning Tools to Spider a Website; Scripting to Automate Web Requests and Spidering; Brute Forcing Unlinked Files and Directories; Discovering and Exploiting Shellshock

542.3 HANDS ON: Injection

This section continues to explore our methodology with the discovery phase. We will build on the information started the previous day, exploring methods to find and verify vulnerabilities within the application. Students will also begin to explore the interactions between the various vulnerabilities.

Topics: Python for Web App Penetration Testing; Web App Vulnerabilities and Manual Verification Techniques; Interception Proxies; Zed Attack Proxy (ZAP); Burp Suite; Information Leakage, and Directory Browsing; Username Harvesting; Command Injection; Directory Traversal; SQL Injection; Blind SQL Injection; Local File Inclusion (LFI); Remote-File Inclusion (RFI); JavaScript for the Attacker

542.4 HANDS ON: JavaScript and XSS

On day four, students continue exploring the discovery phase of the methodology. We cover methods to discover key vulnerabilities within web applications, such as Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF/XSRF). Manual discovery methods are employed during hands-on labs.

Topics: Cross-Site Scripting (XSS); Cross-Site Request Forgery (CSRF); Session Flaws; Session Fixation; AJAX; Logic Attacks; Data Binding Attacks; Automated Web Application Scanners; w3af; XML and JSON

542.5 HANDS ON: CSRF, Logic Flaws, and Advanced Tools

On the fifth day, we launch actual exploits against real-world applications, building on the previous three steps, expanding our foothold within the application, and extending it to the network on which it resides. As penetration testers, we specifically focus on ways to leverage previously discovered vulnerabilities to gain further access, highlighting the cyclical nature of the four-step attack methodology.

Topics: Metasploit for Web Penetration Testers; The sqlmap Tool; Exploring Methods to Zombify Browsers; Browser Exploitation Framework (BeEF); Walking Through an Entire Attack Scenario; Leveraging Attacks to Gain Access to the System; How to Pivot Our Attacks Through a Web Application; Understanding Methods of Interacting with a Server Through SQL Injection; Exploiting Applications to Steal Cookies; Executing Commands Through Web Application Vulnerabilities

542.6 HANDS ON: Capture the Flag

On day six, students form teams and compete in a web application penetration testing tournament. This NetWars-powered Capture-the-Flag exercise provides students an opportunity to wield their newly developed or further-honed skills to answer questions, complete missions, and exfiltrate data, applying skills gained throughout the course. The style of challenge and integrated-hint system allows students of various skill levels to both enjoy a game environment and solidify the skills learned in class.

You Will Be Able To

- Apply a detailed, four-step methodology to your web application penetration tests: reconnaissance, mapping, discovery, and exploitation
- Analyze the results from automated web testing tools to validate findings, determine their business impact, and eliminate false positives
- Manually discover key web application flaws
- Use Python to create testing and exploitation scripts during a penetration test
- Discover and exploit SQL Injection flaws to determine true risk to the victim organization
- Create configurations and test payloads within other web attacks
- Fuzz potential inputs for injection attacks
- Explain the impact of exploitation of web application flaws
- Analyze traffic between the client and the server application using tools such as the Zed Attack Proxy and Burp Suite to find security issues within the client-side application code
- Manually discover and exploit Cross-Site Request Forgery (CSRF) attacks
- Use the Browser Exploitation Framework (BeEF) to hook victim browsers, attack client software and the network, and evaluate the potential impact that XSS flaws have within an application
- Perform a complete web penetration test during the Capture the Flag exercise to bring techniques and tools together into a comprehensive test

SEC550

Active Defense, Offensive Countermeasures, and Cyber Deception

Five-Day Program
Mon, July 24 - Fri, July 28
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Bryce Galbraith

The current threat landscape is shifting. Traditional defenses are failing us. We need to develop new strategies to defend ourselves. Even more importantly, we need to better understand who is attacking us and why. You may be able to immediately implement some of the measures we discuss in this course, while others may take a while. Either way, consider what we discuss as a collection of tools that will be at your disposal when you need them to annoy attackers, determine who is attacking you, and, finally, attack the attackers.

SEC550: Active Defense, Offensive Countermeasures, and Cyber Deception is based on the Active Defense Harbinger Distribution live Linux environment funded by the Defense Advanced Research Projects Agency (DARPA). This virtual machine is built from the ground up for defenders to quickly implement Active Defenses in their environments. The course is very heavy with hands-on activities – we won't just talk about Active Defenses, we will work through labs that will enable you to quickly and easily implement what you learn in your own working environment.

Who Should Attend

- General security practitioners
- Penetration testers
- Ethical hackers
- Web application developers
- Website designers and architects

"It's hard to imagine a better instructor than Bryce. He is obviously very skilled and experienced – his teaching skill and personality is a perfect fit."

-Patrick Gustafson, Allianz Life Insurance

You Will Learn:

- **How to force an attacker to take more moves to attack your network – moves that in turn may increase your ability to detect that attacker**
- **How to gain better attribution as to who is attacking you and why**
- **How to gain access to a bad guy's system**
- **Most importantly, you will find out how to do the above legally**

What You Will Receive

- **A fully functioning Active Defense Harbinger Distribution ready to deploy**
- **Class books and a DVD with the necessary tools and the OCM virtual machine, which is a fully functional Linux system with the OCM tools installed and ready to go for the class and for the students' work environments**

"SEC550 is the next step in the evolution of cyber defense – learning to make the hacker's job harder, track their movement, and get attribution."

-Mick Leach, Nationwide

Bryce Galbraith *SANS Principal Instructor*

As a contributing author of the internationally bestselling book *Hacking Exposed: Network Security Secrets & Solutions*, Bryce helped bring the secret world of hacking out of the darkness and into the public eye. Bryce has held security positions at global ISPs and Fortune 500 companies, he was a member of Foundstone's renowned penetration testing team, and he served as a senior instructor and co-author of Foundstone's Ultimate Hacking: Hands-On course series. Bryce is currently the owner of Layered Security, where he provides specialized vulnerability assessment and penetration testing services for clients. He teaches several of the SANS Institute's most popular courses and develops curriculum around current topics. He has taught the art of ethical hacking and countermeasures to thousands of IT professionals from a who's who of top companies, financial institutions, and government agencies around the globe. Bryce is an active member of several security-related organizations, holds several security certifications, and speaks at conferences around the world. **@brycegalbraith**

550.1 HANDS ON: Setup and Baseline

Day 1 topics:

- Setup
- Mourning Our Destiny, Leaving Youth and Childhood Behind
- Bad Guy Defenses
- Basics and Fundamentals (Or, Don't Get Owned Doing This)
- Playing With Advanced Backdoors
- Software Restriction Policies
- Legal Issues
- Venom and Poison

550.2 HANDS ON: Annoyance

Day 2 topics:

- How to Connect to Evil Servers (Without Getting Shot)
- Remux.py
- Recon on Bad Servers and Bad People
- Honeypots
- Honeyports
- Kippo
- Deny Hosts
- Artillery
- More Evil Web Servers
- Cryptolocked

542.3 HANDS ON: Attribution

Day 3 topics:

- Dealing with TOR
- Decloak
- Word Web Bugs (Or Honeydocs)
- More Evil Web Servers
- Cryptolocked

550.4 HANDS ON: More Attribution and Attack

Day 4 topics:

- Nova
- Infinitely Recursive Windows Directories
- Web Application Street Fighting with BeEF!
- Wireless and Brotherly Love
- Evil Java Applications with SET
- AV Bypass (for the Good Guys!)
- Arming Word Documents
- Python Injection
- Ghostwriting
- HoneyBadger
- Let's Try to Trojan Some Java Applications

550.5 HANDS ON: Capture the Flag

The Capture-the-Flag challenge draws on what you have learned over the previous four days of the course.

"Great training – very helpful to better understand analysis and offensive security and also how to improve protection."

-Stefania Iannelli, Palo Alto Networks

You Will Be Able To

- Track bad guys with callback Word documents
- Use Honeybadger to track web attackers
- Block attackers from successfully attacking servers with honeyports
- Block web attackers from automatically discovering pages and input fields
- Understand the legal limits and restrictions of Active Defense
- Obfuscate DNS entries
- Create non-attributable Active Defense Servers
- Combine geolocation with existing Java applications
- Create online social media profiles for cyber deception
- Easily create and deploy honeypots

Course Author Statement

"I wrote this course to finally make defense fun, to finally add some confusion to the attackers, and to change the way we all look at defense. One of the most frequent questions I get is why offensive countermeasures are so important. Many people tell me that we cannot ignore patching, firewalls, policies, and other security management techniques. I could not agree more. The techniques presented in this course are intended for organizations that have gone through the process of doing things correctly and want to go further. Get your house in order, and then play. Of course, there will be challenges for anyone trying to implement offensive countermeasures in their organization. However, they can all be faced and overcome."

-John Strand

SEC561

Immersive Hands-on Hacking Techniques

Six-Day Program
Mon, July 24 - Sat, July 29
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Kevin Fiscus

Who Should Attend

- Security professionals who want to expand their hands-on technical skills in new analysis areas such as packet analysis, digital forensics, vulnerability assessment, system hardening, and penetration testing
- Systems and network administrators who want to gain hands-on experience in information security skills to become better administrators
- Incident response analysts who want to better understand system attack and defense techniques
- Forensic analysts who need to improve their analysis through experience with real-world attacks
- Penetration testers seeking to gain practical experience for use in their own assessments
- Red team members who want to build their hands-on skills and blue team members who want to better understand attacks and defend their environments

To be a top penetration testing professional, you need fantastic hands-on skills for finding, exploiting and resolving vulnerabilities. Top instructors at SANS engineered **SEC561: Immersive Hands-On Hacking Techniques** from the ground up to help you get good fast. The course teaches in-depth security capabilities through 80%+ hands-on exercises, maximizing keyboard time during in-class labs and making this SANS' most hands-on course ever. With over 30 hours of intense labs, students experience a leap in their capabilities, as they come out equipped with the practical skills needed to handle today's pen test and vulnerability assessment projects in enterprise environments. Throughout the course, an expert instructor coaches students as they work their way through solving increasingly demanding real-world information security scenarios using skills that they will be able to apply the day they get back to their jobs.

People often talk about these concepts, but this course teaches you how to actually do them hands-on and in-depth. SEC561 shows penetration testers, vulnerability assessment personnel, auditors, and operations personnel how to leverage in-depth techniques to get powerful results in every one of their projects. The course is overflowing with practical lessons and innovative tips, all with direct hands-on application. Throughout the course, students interact with brand new and custom-developed scenarios built just for this course on the innovative NetWars challenge infrastructure, which guides them through the numerous hands-on labs providing questions, hints, and lessons learned as they build their skills.

Topics addressed in the course include:

- **Applying network scanning and vulnerability assessment tools to effectively map out networks and prioritize discovered vulnerabilities for effective remediation.**
- **Manipulating common network protocols to reconfigure internal network traffic patterns, as well as defenses against such attacks.**
- **Analyzing Windows and Linux systems for weaknesses using the latest enterprise management capabilities of the operating systems, including the super-powerful Windows Remote Management (WinRM) tools.**
- **Applying cutting-edge password analysis tools to identify weak authentication controls leading to unauthorized server access.**
- **Scouring through web applications and mobile systems to identify and exploit devastating developer flaws.**
- **Evading anti-virus tools and bypassing Windows User Account Control to understand and defend against these advanced techniques.**
- **Honing phishing skills to evaluate the effectiveness of employee awareness initiatives and your organization's exposure to one of the most damaging attack vectors widely used today.**

Kevin Fiscus *SANS Certified Instructor*

Kevin Fiscus is the founder of and lead consultant for Cyber Defense Advisors, where he performs security and risk assessments, vulnerability and penetration testing, security program design, policy development and security awareness with a focus on serving the needs of small and mid-sized organizations. Kevin has over 20 years of IT experience and has focused exclusively for the past 12 years on information security. Kevin currently holds the CISA, GPEN, GREM, GMOB, GCED, GCFA-Gold, GCIA-Gold, GCIH, GAWN, GPPA, GCWN, GCSC-Gold, GSEC, SCSA, RCSE, and SnortCP certifications and is proud to have earned the top information security certification in the industry, the GIAC Security Expert. Kevin has also achieved the distinctive title of SANS Cyber Guardian for both red team and blue team. **@kevinbfiscus**

561.1 HANDS ON: Security Platform Analysis

The first day of the course prepares students for real-world security challenges by giving them hands-on practice with essential Linux and Windows server and host management tools. First, students will leverage built-in and custom Linux tools to evaluate the security of host systems and servers, inspecting and extracting content from rich data sources such as image headers, browser cache content, and system logging resources. Next, students will turn their focus to performing similar analysis against remote Windows servers using built-in Windows system management tools to identify misconfigured services, scrutinize historical registry entries for USB devices, evaluate the impact of malware attacks, and analyze packet capture data. By completing these tasks, students build their skills in managing systems, applicable to post-compromise system host analysis, or defensive tasks such as defending targeted systems from persistent attack threats. By adding new tools and techniques to their arsenal, students are better prepared to complete the analysis of complex systems with greater accuracy in less time.

Topics: Linux Host and Server Analysis; Windows Host and Server Analysis

561.2 HANDS ON: Enterprise Security Assessment

In this section of the class, students investigate the critical tasks for a high-quality penetration test. We'll look at the safest, most efficient ways to map a network and discover target systems and services. Once the systems are discovered, we look for vulnerabilities and reduce false positives with manual vulnerability verification. We'll also look at exploitation techniques, including the use of the Metasploit Framework to exploit these vulnerabilities, accurately describing risk and further reducing false positives. Of course, exploits are not the only way to access systems, so we also leverage password-related attacks, including guessing and cracking techniques to extend our reach for a more effective and valuable penetration test.

Topics: Network Mapping and Discovery; Enterprise Vulnerability Assessment; Network Penetration Testing; Password and Authentication Exploitation

561.3 HANDS ON: Web Application Assessment

This section of the course will look at the variety of flaws present in web applications and how each of them is exploited. Students will solve challenges presented to them by exploiting web applications hands-on with the tools used by professional web application penetration testers every day. The websites students attack mirror real-world vulnerabilities including Cross-Site Scripting (XSS), SQL Injection, Command Injection, Directory Traversal, Session Manipulation and more. Students will need to exploit the present flaws and answer questions based on the level of compromise they are able to achieve.

Topics: Recon and Mapping; Server-side Web Application Attacks; Client-side Web Application Attacks; Web Application Vulnerability Exploitation

561.4 HANDS ON: Mobile Device and Application Analysis

With the accelerated growth of mobile device use in enterprise networks, organizations find an increasing need to identify expertise in the security assessment and penetration testing of mobile devices and the supporting infrastructure. In this component of the course, we examine the practical vulnerabilities introduced by mobile devices and applications, and how they relate to the security of the enterprise. Students will look at the common vulnerabilities and attack opportunities against Android and Apple iOS devices, examining data remnants from lost or stolen mobile devices, the exposure introduced by common weak application developer practices, and the threat introduced by popular cloud-based mobile applications found in many networks today.

Topics: Mobile Device Assessment; Mobile Device Data Harvesting; Mobile Application Analysis

561.5 HANDS ON: Advanced Penetration Testing

This portion of the class is designed to teach the advanced skills required in an effective penetration test to extend our reach and move through the target network. This extended reach will provide a broader and more in-depth look at the security of the enterprise. We'll utilize techniques to pivot through compromised systems using various tunneling/pivoting techniques, bypass anti-virus and built-in commands to extend our influence over the target environment, and find issues that lesser testers may have missed. We'll also look at some of the common mistakes surrounding poorly or incorrectly implemented cryptography and ways to take advantage of those weaknesses to access systems and data that are improperly secured.

Topics: Anti-Virus Evasion Techniques; Advanced Network Pivoting Techniques; Exploiting Network Infrastructure Components

561.6 HANDS ON: Capture the Flag Challenge

This lively session represents the culmination of the course, where attendees will apply the skills they have mastered throughout all the other sessions in a hands-on workshop. Students will participate in a larger version of the exercises presented in the class to independently reinforce skills learned throughout the course. They will then apply their newly developed skills to scan for flaws, use exploits, unravel technical challenges, and dodge firewalls, all while guided by the challenges presented by the NetWars Scoring Server. By practicing the skills in a combination workshop in which multiple focus areas are combined, participants will have the opportunity to explore, exploit, pillage, and continue to reinforce skills against a realistic target environment.

You Will Be Able To

- Use network scanning and vulnerability assessment tools to effectively map out networks and prioritize discovered vulnerabilities for effective remediation
- Use password analysis tools to identify weak authentication controls leading to unauthorized server access
- Evaluate web applications for common developer flaws leading to significant data loss conditions
- Manipulate common network protocols to maliciously reconfigure internal network traffic patterns
- Identify weaknesses in modern anti-virus signature and heuristic analysis systems
- Inspect the configuration deficiencies and information disclosure threats present on Windows and Linux servers
- Bypass authentication systems for common web application implementations
- Exploit deficiencies in common cryptographic systems
- Bypass monitoring systems by leveraging IPv6 scanning and exploitation tools
- Harvest sensitive mobile device data from iOS and Android targets

"Hands down, one of the best SANS courses I have taken. I learned cutting-edge pentesting techniques in a hands-on environment that challenged my abilities and increased my overall knowledge."

-Dave Odom, Bechtel

"80% hands-on is intense and the best way to build on previous pen testing-focused SANS courses."

-Timothy McKenzie, DELL/Secureworks

SEC573

GPYC Certification
Python Coder

www.giac.org/gpyc

Automating Information Security with Python *NEW!*

Six-Day Program
Mon, July 24 - Sat, July 29
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Mark Baggett

Who Should Attend

- Security professionals who want to learn how to develop Python applications
- Penetration testers who want to move from being a consumer of security tools to being the creator of security tools
- Technologists who need custom tools to test their infrastructure and who want to create those tools themselves

"Excellent class for beginners and advanced alike. It has something for everyone."
-Mike Perez, Disney

"SEC573 gave me exposure to tools and techniques I wouldn't have normally considered, but now are part of my arsenal."
-Allen C., DoD

All security professionals, including Penetration Testers, Forensics Analysts, Network Defenders, Security Administrators, and Incident Responders, have one thing in common: CHANGE. Change is constant. Technology, threats, and tools are constantly evolving. If we don't evolve with them, we'll become ineffective and irrelevant, unable to provide the vital defenses our organizations increasingly require.

Maybe your chosen Operating System has a new feature that creates interesting forensics artifacts that would be invaluable for your investigation, if only you had a tool to access it. Often for new features and forensics artifacts, no such tool has yet been released. You could try moving your case forward without that evidence or hope that someone creates a tool before the case goes cold... **or you can write a tool yourself.**

Or, perhaps an attacker bypassed your defenses and owned your network months ago. If existing tools were able to find the attack, you wouldn't be in this situation. You are bleeding sensitive data and the time-consuming manual process of finding and eradicating the attacker is costing you money and hurting your organization big time. The answer is simple if you have the skills: Write a tool to automate your defenses.

Or, as a Penetration tester, you need to evolve as quickly as the threats you are paid to emulate. What do you do when "off-the-shelf" tools and exploits fall short? If you're good, you write your own tool.

Writing a tool is easier said than done, right? Not really. Python is a simple, user-friendly language that is designed to make automating tasks that security professionals perform quick and easy. Whether you are new to coding or have been coding for years, **SEC573: Automating Information Security with Python** will have you creating programs to make your job easier and make you more efficient. This self-paced class starts from the very beginning assuming you have no prior experience or knowledge of programming. We cover all of the essentials of the language up front. If you already know the essentials, you will find that the pyWars lab environment allows advanced developers to quickly accelerate to more advanced material in the class. The self-paced style of the class will meet you where you are to let you get the most out of the class. Beyond the essentials we discuss file analysis, packet analysis, forensics artifact carving, networking, database access, website access, process execution, exception handling, object-oriented coding and more.

This course is designed to give you the skills you need for tweaking, customizing, or outright developing your own tools. We put you on the path of creating your own tools, empowering you in automating the daily routine of today's information security professional, and achieving more value in less time. Again and again, organizations serious about security emphasize their need for skilled tool builders. There is a huge demand for people who can understand a problem and then rapidly develop prototype code to attack or defend against it. **Join us and learn Python in-depth and fully weaponized.**

Mark Baggett *SANS Senior Instructor*

Mark Baggett is the owner of Indepth Defense, an independent consulting firm that offers incident response and penetration testing services. Mark has more than 28 years of commercial and government experience ranging from Software Developer to Chief Information Security Officer and is the author of SEC573: Automating Information Security for Python. Mark has a master's degree in information security engineering and many industry certifications, including being 15th person in the world to receive the prestigious GIAC Security Expert certification (GSE). Mark is very active in the information security community. He is the founding president of The Greater Augusta ISSA (Information Systems Security Association) chapter that has been extremely successful in bringing networking and educational opportunities to Augusta information technology workers. Since January 2011, Mark has served as the Technical Advisor to the DoD for SANS, assisting various government agencies in the development of information security capabilities. **@MarkBaggett**

573.1 HANDS ON: Essentials Workshop with pyWars

The course begins with a brief introduction to Python and the pyWars Capture-the-Flag game. We set the stage for students to learn at their own pace in the 100% hands-on pyWars lab environment. As more advanced students take on Python-based Capture-the-Flag challenges, students who are new to programming will start from the very beginning with Python essentials.

Topics: Python Syntax; Variables; Math Operators; Strings; Functions; Modules; Control Statements; Introspection

573.2 HANDS ON: Essentials Workshop with MORE pyWars

You will never learn to program by staring at PowerPoint slides. The second day continues the hands-on, lab-centric approach established on day one. This section covers data structures and more detailed programming concepts. Next, we focus on invaluable tips and tricks to make you a better Python programmer and on how to debug your code.

Topics: Lists; Loops; Tuples; Dictionaries; The Python Debugger; Coding Tips, Tricks, and Shortcuts; System Arguments; ArgParser Module

573.3 HANDS ON: Defensive Python

Day three includes in-depth coverage about how defenders can use Python automation as we cover Python modules and techniques that everyone can use. Forensicators and offensive security professionals will also learn essential skills they will apply to their craft. We will play the role of a network defender who needs to find the attackers on their network. We will discuss how to analyze network logs and packets to discover where the attackers are coming from and what they are doing. We will build scripts to empower continuous monitoring and disrupt the attackers before they exfiltrate your data.

Topics: File Operations; Python Sets; Regular Expressions; Log Parsing; Data Analysis Tools and Techniques; Long Tail/Short Tail Analysis; Geolocation Acquisition; Blacklists and Whitelists; Packet Analysis; Packet Reassembly; Payload Extraction

573.4 HANDS ON: Forensics Python

On day four we will play the role of a forensics analyst who has to carve evidence from artifacts when no tool exists to do so. Even if you don't do forensics you will find that these skills covered on day four are foundational to every security role. We will discuss the process required to carve binary images, find appropriate data of interest in them, and extract that data. Once you have the artifact isolated, there is more analysis to be done. You will learn how to extract metadata from image files. Then we will discuss techniques for finding artifacts in other locations such as SQL databases and interacting with web pages.

Topics: Acquiring Images from Disk, Memory, and the Network; File Carving; The STRUCT Module; Raw Network Sockets and Protocols; Image Forensics and PIL; SQL Queries; HTTP Communications with Python Built-In Libraries; Web Communications with the Requests Module

573.5 HANDS ON: Offensive Python

On day five we play the role of penetration testers whose normal tricks have failed. Their attempts to establish a foothold have been stopped by modern defenses. To bypass these defenses, you will build an agent to give you access to a remote system. Similar agents can be used for incident response or systems administration, but our focus will be on offensive operations.

Topics: Network Socket Operations; Exception Handling; Process Execution; Blocking and Non-blocking Sockets; Asynchronous Operations; The Select Module; Python Objects; Argument Packing and Unpacking

573.6 HANDS ON: Capture the Flag

In this final section you will be placed on a team with other students. Working as a team, you will apply the skills you have mastered in a series of programming challenges. Participants will exercise the skills and code they have developed over the previous five days as they exploit vulnerable systems, break encryption cyphers, analyze packets, parse logs, and automate code execution on remote systems. Test your skills! Prove your might!

"Best class ever! After just 2 days I'm getting comfortable with the nuances of Python. I never thought that would happen."

-Jay Wilson, Navient

You Will Be Able To

- Write a backdoor that uses Exception Handling, Sockets, Process execution, and encryption to provide you with your initial foothold in a target environment. The backdoor will include features such as a port scanner to find an open outbound port, techniques for evading antivirus software and network monitoring, and the ability to embed payload from tools such as Metasploit.
- Write a SQL injection tool that uses standard Python libraries to interact with target websites. You will be able to use different SQL attack techniques for extracting data from a vulnerable target system.
- Develop a password-guessing attack tool with features like multi-threading, cookie handlers, support for application proxies such as Burp, and much more.
- Write a network reconnaissance tool that uses SCAPY, StringsIO, and PIL to reassemble TCP packet streams, extract data payloads such as images, display images, extract metadata such as GPS coordinates, and link those images with GPS coordinates to Google maps.

You Will Receive

- A virtual machine with sample code and working examples
- A copy of the book *Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers*, which shows how to forge your own weapons using the Python programming language
- MP3 audio files of the complete course lecture

SANS Technology Institute

www.sans.edu

SEC575

GMOB Certification
Mobile Device Security Analyst

www.giac.org/gmob

Mobile Device Security and Ethical Hacking

Six-Day Program
Mon, July 24 - Sat, July 29
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Peter Szczepankiewicz

Who Should Attend

- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Security personnel whose job involves assessing, deploying or securing mobile phones and tablets
- Network and system administrators supporting mobile phones and tablets

"Outstanding course material and instructor presentation. It truly drills in the analytic process, while remaining technical. I highly recommend this course to anyone performing any level of intelligence support to defensive cyber operations."

-Thomas L, U.S. Air Force

Imagine an attack surface spread throughout your organization and in the hands of every user. It moves from place to place regularly, stores highly sensitive and critical data, and sports numerous different wireless technologies all ripe for attack. You don't need to imagine any further because this already exists today: **mobile devices**. These devices are the biggest attack surface in most organizations, yet these same organizations often don't have the skills needed to assess them.

Mobile devices are no longer a convenience technology: they are an essential tool carried or worn by users worldwide, often displacing conventional computers for everyday enterprise data needs. You can see this trend in corporations, hospitals, banks, schools, and retail stores throughout the world. Users rely on mobile devices more today than ever before – we know it, and the bad guys do too.

This course is designed to give you the skills you need to understand the security strengths and weaknesses in Apple iOS, Android, and wearable devices including Apple Watch and Android Wear. With these skills, you will evaluate the security weaknesses of built-in and third-party applications. You'll learn how to bypass platform encryption, and how to manipulate Android apps to circumvent obfuscation techniques. You'll leverage automated and manual mobile application analysis tools to identify deficiencies in mobile app network traffic, file system storage, and inter-app communication channels. You'll safely work with mobile malware samples to understand the data exposure and access threats affecting Android and iOS devices, and you'll exploit lost or stolen devices to harvest sensitive mobile application data.

Understanding and identifying vulnerabilities and threats to mobile devices is a valuable skill, but it must be paired with the ability to communicate the associated risks. Throughout the course, you'll review the ways in which we can effectively communicate threats to key stakeholders. You'll leverage tools including Mobile App Report Cards to characterize threats for management and decision-makers, while identifying sample code and libraries that developers can use to address risks for in-house applications as well.

You'll then use your new skills to apply a mobile device deployment penetration test in a step-by-step fashion. Starting with gaining access to wireless networks to implement man-in-the-middle attacks and finishing with mobile device exploits and data harvesting, you'll examine each step in conducting such a test with hands-on exercises, detailed instructions, and tips and tricks learned from hundreds of successful penetration tests. By building these skills, you'll return to work prepared to conduct your own test, and you'll be better informed about what to look for and how to review an outsourced penetration test.

Mobile device deployments introduce new threats to organizations including advanced malware, data leakage, and the disclosure of enterprise secrets, intellectual property, and personally identifiable information assets to attackers. Further complicating matters, there simply are not enough people with the security skills needed to identify and manage secure mobile phone and tablet deployments. By completing this course, you'll be able to differentiate yourself as being prepared to evaluate the security of mobile devices, effectively assess and identify flaws in mobile applications, and conduct a mobile device penetration test – all critical skills to protect and defend mobile device deployments.

Peter Szczepankiewicz *SANS Certified Instructor*

Formerly working with the military, Peter responded to network attacks, and worked with both defensive and offensive red teams. Currently, Peter is a Senior Security Engineer with IBM. People lead technology, not the other way around, so Peter works daily to bring actionable intelligence out of disparate security devices for customers, making systems interoperable. Peter expounds, "Putting together networks only to tear them apart is just plain fun," he explains. "And it allows students to take the information learned from books and this hands-on experience back to their particular work place." **@_s14**

575.1 HANDS ON: Device Architecture and Common Mobile Threats

The first section of the course quickly looks at the significant threats affecting mobile device deployments, highlighted with a hands-on exercise evaluating network traffic from a vulnerable mobile banking application. As a critical component of a secure deployment, we will examine the architectural and implementation differences and similarities in Android (including Android Marshmallow), Apple iOS 10, and the Apple Watch and Google Wear platforms. We will also look at the specific implementation details of popular platform features such as iBeacon, AirDrop, App Verification, and more. Hands-on exercises will be used to interact with mobile devices running in a virtualized environment, including low-level access to installed application services and application data.

Topics: Mobile Problems and Opportunities; Mobile Device Platform Analysis; Wearable Platforms: Mobile Device Lab Analysis Tools; Mobile Device Malware Threats

575.2 HANDS ON: Mobile Platform Access and Application Analysis

With an understanding of the threats, architectural components and desired security methods, we dig deeper into iOS and Android mobile platforms focusing on sandboxing and data isolation models, and on the evaluation of mobile applications. This section is designed to help build skills in analyzing mobile device data and applications through rooting and jailbreaking Android and iOS devices and using that access to evaluate file system artifacts.

Topics: Static Application Analysis; Unlocking, Rooting, Jailbreaking Mobile Devices; Mobile Phone Data Storage and Filesystem Architecture; Network Activity Monitoring

575.3 HANDS ON: Mobile Application Reverse Engineering

One of the critical decisions you will need to make in supporting a mobile device deployment is to approve or disapprove of unique application requests from end-users in a corporate device deployment. With some analysis skills, we can evaluate applications to determine the type of access and information disclosure threats they represent. In this section we will use automated and manual application assessment tools to evaluate iOS and Android apps. We'll build upon the static application analysis skills covered in day 2 to manipulate application components, including Android intents and iOS URL extensions. We'll also learn and practice techniques for manipulating iOS and Android applications: method swizzling on iOS, and disassembly, modification, and reassembly of iOS apps. The day ends with a look at a standard system for evaluating and grading the security of mobile applications in a consistent method through the application report card project.

Topics: Application Report Cards; Automated Application Analysis Systems; Manipulating App Behavior

575.4 HANDS ON: Penetration Testing Mobile Devices – Part 1

An essential component of developing a secure mobile phone deployment is to perform an ethical hacking assessment. Through ethical hacking or penetration testing, we examine the mobile devices and infrastructure from the perspective of an attacker, identifying and exploiting flaws that deliver unauthorized access to data or supporting networks. Through the identification of these flaws we can evaluate the mobile phone deployment risk to the organization with practical, useful risk metrics.

Topics: Fingerprinting Mobile Devices; Wireless Network Probe Mapping; Weak Wireless Attacks; Enterprise Wireless Security Attacks; Network Manipulation Attacks; Sidejacking Attacks

575.5 HANDS ON: Penetration Testing Mobile Devices – Part 2

Continuing our look at ethical hacking and penetration testing, we turn our focus to exploiting weaknesses on iOS and Android devices. We will also examine platform-specific application weaknesses and look at the growing use of web framework attacks in mobile application exploitation.

Topics: SSL/TLS Attacks; Client-Side Injection (CSI) Attacks; Web Framework Attacks; Back-end Application Support Attacks

575.6 HANDS ON: Capture the Flag

On the last day of class we'll pull in all the concepts and technology we've covered in the week for a comprehensive Capture-the-Flag (CTF) challenge. During the CTF event, you'll have the option to participate in multiple roles, designing a secure infrastructure for the deployment of mobile phones, monitoring network activity to identify attacks against mobile devices, extracting sensitive data from a compromised iPad, and attacking a variety of mobile phones and related network infrastructure components. In the CTF, you'll use the skills you've built to practically evaluate systems and defend against attackers, simulating the realistic environment you'll be prepared to protect when you get back to the office.

You Will Be Able To

- Use jailbreak tools for Apple iOS and Android systems
- Conduct an analysis of iOS and Android filesystem data to plunder compromised devices and extract sensitive mobile device use information
- Analyze Apple iOS and Android applications with reverse-engineering tools
- Change the functionality of Android and iOS apps to defeat anti-jailbreaking or circumvent in-app purchase requirements
- Conduct an automated security assessment of mobile applications
- Use wireless network analysis tools to identify and exploit wireless networks used by mobile devices
- Intercept and manipulate mobile device network activity
- Leverage mobile-device-specific exploit frameworks to gain unauthorized access to target devices
- Manipulate the behavior of mobile applications to bypass security restrictions

"Mobile hacking is developing at an increasing rate. This course is a great way to get the skills and knowledge."

-Tim Grech, Pfizer

SEC642

Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques

Six-Day Program
Mon, July 24 - Sat, July 29
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Adrien de Beaupre

Who Should Attend

- Web penetration testers
- Red team members
- Vulnerability assessment personnel
- Network penetration testers
- Security consultants
- Developers
- QA testers
- System administrators
- IT managers
- System architects

"SEC642 helps sharpen the pen testing mindset and to be more creative when performing pen tests."
-Jesper Pettersson, Klarna

Can Your Web Apps Withstand the Onslaught of Modern Advanced Attack Techniques?

Modern web applications are growing more sophisticated and complex as they utilize exciting new technologies and support ever more critical operations. Long gone are the days of basic HTML requests and responses. Even in the age of Web 2.0 and AJAX, the complexity of HTTP and modern web applications is progressing at breathtaking speed. With the demands of highly available web clusters and cloud deployments, web applications are looking to deliver more functionality in smaller packets, with a decreased strain on backend infrastructure. Welcome to an era that includes tricked-out cryptography, WebSockets, HTTP/2, and a whole lot more. Are your web application assessment and penetration testing skills ready to evaluate these impressive new technologies and make them more secure?

"SEC642 is the perfect course for someone who has a background in web app pen testing, but wants to really gain advanced skills." -Matthew Sullivan, Webfilings

Are You Ready to Put Your Web Apps to the Test with Cutting-Edge Skills?

This pen testing course is designed to teach you the advanced skills and techniques required to test modern web applications and next-generation technologies. The course uses a combination of lecture, real-world experiences, and hands-on exercises to teach you the techniques to test the security of tried-and-true internal enterprise web technologies, as well as cutting-edge Internet-facing applications. The final course day culminates in a Capture-the-Flag competition, where you will apply the knowledge you acquired during the previous five days in a fun environment based on real-world technologies.

Hands-on Learning of Advanced Web App Exploitation Skills

We begin by exploring advanced techniques and attacks to which all modern-day complex applications may be vulnerable. We'll learn about new web frameworks and web backends, then explore encryption as it relates to web applications, digging deep into practical cryptography used by the web, including techniques to identify the type of encryption in use within the application and methods for exploiting or abusing it. We'll look at alternative front ends to web applications and web services such as mobile applications, and examine new protocols such as HTTP/2 and WebSockets. The final portion of the class will focus on how to identify and bypass web application firewalls, filtering, and other protection techniques.

Adrien de Beaupre *SANS Certified Instructor*

Adrien de Beaupre works as an independent consultant in beautiful Ottawa, Ontario. His work experience includes technical instruction, vulnerability assessment, penetration testing, intrusion detection, incident response and forensic analysis. He is a member of the SANS Internet Storm Center (isc.sans.edu). He is actively involved with the information security community, and has been working with SANS since 2000. Adrien holds a variety of certifications including the GXPN, GPEN, GWAPT, GCIH, GCIA, GSEC, CISSP, OPST, and OPSA. When not geeking out he can be found with his family, or at the dojo. **@adriendb**

642.1 HANDS ON: Advanced Attacks

As applications and their vulnerabilities become more complex, penetration testers have to be able to handle advanced targets. We'll start the course with a warm-up pen test of a small application. After our review of this exercise, we will explore some of the more advanced techniques for LFI/RFI and SQLi server-based flaws. We will then take a stab at combined XSS and XSRF attacks, where we leverage the two vulnerabilities together for even greater effect. After discovering the flaws, we will then work through various ways to exploit these flaws beyond the typical means exhibited today. These advanced techniques will help penetration testers find ways to demonstrate these vulnerabilities to their organization through advanced and custom exploitation.

Topics: Review of the Testing Methodology; Using Burp Suite in a Web Penetration Test; Exploiting Local and Remote File Inclusions; Exploring Advanced Discovery Techniques for SQL Injection and Other Server-Based Flaws; Exploring Advanced Exploitation of XSS and XSRF in a Combined Attack; Learning Advanced Exploitation Techniques

642.2 HANDS ON: Web Frameworks

We'll continue exploring advanced discovery and exploitation techniques for today's complex web applications. We'll look at vulnerabilities that could affect web applications written in any backend language, then examine how logic flaws in applications, especially in Mass Object Assignments, can have devastating effects on security. We'll also dig into assumptions made by core development teams of backend programming languages and learn how even something as simple as handling the data types in variables can be leveraged through the web with Type Juggling and Object Serialization. Next we'll explore various popular applications and frameworks and how they change the discovery techniques within a web penetration test. Part of this discussion will lead us to cutting-edge technologies like the MEAN stack, where JavaScript is leveraged from the browser, web server, and backend NoSQL storage. The final section of the class examines applications in content management systems such as SharePoint and WordPress, which have unique needs and features that make testing them both more complex and more fruitful for the tester.

Topics: Web Architectures; Web Design Patterns; Languages and Frameworks; Java and Struts; PHP-Type Juggling; Logic Flaws; Attacking Object Serialization; The MEAN Stack; Content Management Systems; SharePoint; WordPress

You Will Be Able To

- Perform advanced Local File Include (LFI)/ Remote File Include (RFI), Blind SQL injection (SQLi), and Cross-Site Scripting (XSS) combined with Cross-Site Request Forger (XSRF) discovery and exploitation
- Exploit advanced vulnerabilities common to most backend language like Mass Assignments, Type Juggling, and Object Serialization
- Perform JavaScript-based injection against ExpressJS, Node.js, and NoSQL
- Understand the special testing methods for content management systems such as SharePoint and WordPress
- Identify and exploit encryption implementations within web applications and frameworks
- Discover XML Entity and XPath vulnerabilities in SOAP or REST web services and other datastores
- Use tools and techniques to work with and exploit HTTP/2 and Web Sockets
- Identify and bypass Web Application Firewalls and application filtering techniques to exploit the system

642.3 HANDS ON: Web Cryptography

Cryptographic weaknesses are common, yet few penetration testers have the skill to investigate, attack and exploit these flaws. When we investigate web application crypto attacks, we typically target the implementation and use of cryptography in modern web applications. Many popular web programming languages or development frameworks make encryption services available to the developer, but do not inherently protect encrypted data from being attacked, or only permit the developer to use cryptography in a weak manner. These implementation mistakes are going to be our focus in this section, as opposed to the exploitation of deficiencies in the cryptographic algorithms themselves. We will also explore the various ways applications use encryption and hashing insecurely. Students will learn techniques ranging from identifying what the encryption technique is to exploiting various flaws within the encryption or hashing.

Topics: Identifying the Cryptography Used in the Web Application; Analyzing and Attacking the Encryption Keys; Exploiting Stream Cipher IV Sollisions; Exploiting Electronic Codebook (ECB) Mode Ciphers with Block Shuffling; Exploiting Cipher Block Chaining (CBC) Mode with Bit Flipping; Vulnerabilities in PKCS#7 Padding Implementations

642.4 HANDS ON: Alternative Web Interfaces

Web applications are no longer limited to the traditional HTML-based interfaces. Web services and mobile applications have become more common and are regularly being used to attack clients and organizations. As such, it has become very important that penetration testers understand how to evaluate the security of these systems. We will examine Flash, Java, Active X, and Silverlight flaws. We will explore various techniques to discover flaws within the applications and backend systems. These techniques will make use of tools such as Burp Suite and other automated toolsets. We'll use lab exercises to explore the newer protocols of HTTP/2 and WebSockets, exploiting flaws exposed within each of them.

Topics: Intercepting Traffic to Web Services and from Mobile Applications; Flash, Java, ActiveX, and Silverlight Vulnerabilities; SOAP and REST Web Services; Penetration Testing of Web Services; WebSocket Protocol Issues and Vulnerabilities; New HTTP/2 Protocol Issues and Penetration Testing

642.5 HANDS ON: Web Application Firewall and Filter Bypass

Applications today are using more security controls to help prevent attacks. These controls, such as Web Application Firewalls and filtering techniques, make it more difficult for penetration testers during their testing. The controls block many of the automated tools and simple techniques used to discover flaws. On this day we'll explore techniques used to map the control and how that control is configured to block attacks. You'll be able to map out the rule sets and determine the specifics of how the Web Application Firewall detects attacks. This mapping will then be used to determine attacks that will bypass the control. You'll use HTML5, UNICODE, and other encodings that will enable your discovery techniques to work within the protected application.

Topics: Understanding of Web Application Firewalling and Filtering Techniques; Determining the Rule Sets Protecting the Application; Fingerprinting the Defense Techniques Used; Learning How HTML5 Injections Work; Using UNICODE, CTYPEs, and Data URIs to Bypass Restrictions; Bypassing a Web Application Firewall's Best-Defended Vulnerabilities, XSS and SQLi

642.6 HANDS ON: Capture the Flag

On this final course day you will be placed on a network and given the opportunity to complete an entire penetration test. The goal of this exercise is for you to explore the techniques, tools, and methodology you will have learned over the last five days. You'll be able to use these skills against a realistic extranet and intranet. At the end of the day, you will provide a verbal report of the findings and methodology you followed to complete the test. Students will be provided with a virtual machine that contains the Samurai Web Testing Framework (SamuraiWTF). You will be able to use this both in the class and after leaving and returning to your jobs.

SEC660

GXPN Certification

Exploit Researcher and Advanced Penetration Tester

www.giac.org/gxpn

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Six-Day Program
Mon, July 24 - Sat, July 29
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Tim Medin

This course has evening Bootcamp Sessions

Who Should Attend

- Network and systems penetration testers
- Incident handlers
- Application developers
- IDS engineers

"The SEC660 course was hands-on, packed with content, and current to today's technology!"

-Michael Horken, Rockwell Automation

"This material puts me at that next level."

-Adam Logue, Spectrum Health

This course is designed as a logical progression point for those who have completed **SEC560: Network Penetration Testing and Ethical Hacking**, or for those with existing penetration testing experience. Students with the prerequisite knowledge to take this course will walk through dozens of real-world attacks used by the most seasoned penetration testers. **The methodology of a given attack is discussed, followed by exercises in a real-world lab environment to solidify advanced concepts and allow for the immediate application of techniques in the workplace.** Each day includes a two-hour evening bootcamp to allow for additional mastery of the techniques discussed and even more hands-on exercises. A sample of topics covered includes weaponizing Python for penetration testers, attacks against network access control (NAC) and VLAN manipulation, network device exploitation, breaking out of Linux and Windows restricted environments, IPv6, Linux privilege escalation and exploit-writing, testing cryptographic implementations, fuzzing, defeating modern OS controls such as ASLR and DEP, return-oriented programming (ROP), Windows exploit-writing, and much more!

Attackers are becoming more clever and their attacks more complex. In order to keep up with the latest attack methods, you need a strong desire to learn, the support of others, and the opportunity to practice and build experience. **SEC660 provides attendees with in-depth knowledge of the most prominent and powerful attack vectors and an environment to perform these attacks in numerous hands-on scenarios.** This course goes far beyond simple scanning for low-hanging fruit, and shows penetration testers how to model the abilities of an advanced attacker to find significant flaws in a target environment and demonstrate the business risk associated with these flaws.

SEC660 starts off by introducing the advanced penetration concept, and provides an overview to help prepare students for what lies ahead. The focus of day one is on network attacks, an area often left untouched by testers. Topics include accessing, manipulating, and exploiting the network. **Attacks are performed against NAC, VLANs, OSPF, 802.1X, CDP, IPv6, VOIP, SSL, ARP, SNMP, and others.** Day two starts off with a technical module on performing penetration testing against various cryptographic implementations. The rest of the day is spent on network booting attacks, escaping Linux restricted environments such as chroot, and escaping Windows restricted desktop environments. Day three jumps into an introduction of Python for penetration testing, Scapy for packet crafting, product security testing, network and application fuzzing, and code coverage techniques. Days four and five are spent exploiting programs on the Linux and Windows operating systems. You will learn to identify privileged programs, redirect the execution of code, reverse-engineer programs to locate vulnerable code, obtain code execution for administrative shell access, and defeat modern operating system controls such as ASLR, canaries, and DEP using ROP and other techniques. Local and remote exploits, as well as client-side exploitation techniques, are covered. **The final course day is dedicated to numerous penetration testing challenges requiring you to solve complex problems and capture flags.**

Tim Medin *SANS Certified Instructor*

Tim Medin is a senior technical analyst at Counter Hack, a company devoted to the development of information security challenges for education, evaluation, and competition. Through the course of his career, Tim has performed penetration tests on a wide range of organizations and technologies. Prior to Counter Hack, Tim was a Senior Security Consultant for FishNet Security, where the majority of his focus was on penetration testing. He gained information security experience in a variety of industries, including previous positions in control systems, higher education, financial services, and manufacturing. Tim regularly contributes to the SANS Penetration Testing Blog (**pen-testing.sans.org/blog**) and the Command Line Kung Fu Blog (**blog.commandlinekungfu.com**). He is also project lead for the Laudanum Project, a collection of injectable scripts designed to be used in penetration testing. **@timmedin**

660.1 HANDS ON: Network Attacks for Penetration Testers

Day one serves as an advanced network attack module, building on knowledge gained from SEC560. The focus will be on obtaining access to the network; manipulating the network to gain an attack position for eavesdropping and attacks, and for exploiting network devices; leveraging weaknesses in network infrastructure; and taking advantage of client frailty.

Topics: **Bypassing Network Admission Control; Impersonating Devices with Admission Control Policy Exceptions; Exploiting EAP-MD5 Authentication; Custom Network Protocol Manipulation with Ettercap and Custom Filters; Multiple Techniques for Gaining Man-in-the-Middle Network Access; Exploiting OSPF Authentication to Inject Malicious Routing Updates; Using Evilgrade to Attack Software Updates; Overcoming SSL Transport Encryption Security with Sslstrip; Remote Cisco Router Configuration File Retrieval; IPv6 for Penetration Testers**

660.2 HANDS ON: Crypto, Network Booting Attacks, and Escaping Restricted Environments

Day two starts by taking a tactical look at techniques penetration testers can use to investigate and exploit common cryptography mistakes. We finish the module with lab exercises that allow you to practice your new-found crypto attack skill set against reproduced real-world application vulnerabilities.

Topics: **Pen Testing Cryptographic Implementations; Exploiting CBC Bit Flipping Vulnerabilities; Exploiting Hash Length Extension Vulnerabilities; Delivering Malicious Operating Systems to Devices Using Network Booting and PXE; PowerShell Essentials; Enterprise PowerShell; Post-Exploitation with PowerShell and Metasploit; Escaping Software Restrictions; Two-hour Evening Capture-the-Flag Exercise Using PXE, Network Attacks, and Local Privilege Escalation**

660.3 HANDS ON: Python, Scapy, and Fuzzing

Day three starts with a focus on how to leverage Python as a penetration tester. It is designed to help people unfamiliar with Python start modifying scripts to add their own functionality while helping seasoned Python scripters improve their skills. Once we leverage the Python skills in creative lab exercises, we move on to leveraging Scapy for custom network targeting and protocol manipulation. Using Scapy, we examine techniques for transmitting and receiving network traffic beyond what canned tools can accomplish, including IPv6.

Topics: **Becoming Familiar with Python Types; Leveraging Python Modules for Real-World Pen Tester Tasks; Manipulating Stateful Protocols with Scapy; Using Scapy to Create a Custom Wireless Data Leakage Tool; Product Security Testing; Using Taof for Quick Protocol Mutation Fuzzing; Optimizing Your Fuzzing Time with Smart Target Selection; Automating Target Monitoring While Fuzzing with Sulley; Leveraging Microsoft Word Macros for Fuzzing .docx files; Block-Based Code Coverage Techniques Using Paimei**

660.4 HANDS ON: Exploiting Linux for Penetration Testers

Day four begins by walking through memory from an exploitation perspective as well as introducing x86 assembler and linking and loading. Processor registers are directly manipulated by testers and must be intimately understood. Disassembly is a critical piece of testing and will be used throughout the remainder of the course. We will take a look at the Linux OS from an exploitation perspective and discuss the topic of privilege escalation.

Topics: **Stack and Dynamic Memory Management and Allocation on the Linux OS; Disassembling a Binary and Analyzing x86 Assembly Code; Performing Symbol Resolution on the Linux OS; Identifying Vulnerable Programs; Code Execution Redirection and Memory Leaks; Return-Oriented Programming (ROP); Identifying and Analyzing Stack-Based Overflows on the Linux OS; Performing Return-to-libc (ret2libc) Attacks on the Stack; Defeating Stack Protection on the Linux OS; Defeating ASLR on the Linux OS**

You Will Be Able To

- Perform fuzz testing to enhance your company's SDL process
- Exploit network devices and assess network application protocols
- Escape from restricted environments on Linux and Windows
- Test cryptographic implementations
- Model the techniques used by attackers to perform 0-day vulnerability discovery and exploit development
- Develop more accurate quantitative and qualitative risk assessments through validation
- Demonstrate the needs and effects of leveraging modern exploit mitigation controls
- Reverse-engineer vulnerable code to write custom exploits

SANS Technology Institute

www.sans.edu

www.sans.org/cyber-guardian

660.5 HANDS ON: Exploiting Windows for Penetration Testers

On day five we start with covering the OS security features (ALSR, DEP, etc.) added to the Windows OS over the years, as well as Windows-specific constructs, such as the process environment block (PEB), structured exception handling (SEH), thread information block (TIB), and the Windows API. Differences between Linux and Windows will be covered. These topics are critical in assessing Windows-based applications. We then focus on stack-based attacks against programs running on the Windows OS.

Topics: **The State of Windows OS Protections on Windows 7, 8, 10, Server 2008 and 2012; Understanding Common Windows Constructs; Stack Exploitation on Windows; Defeating OS Protections Added to Windows; Creating a Metasploit Module; Advanced Stack-Smashing on Windows; Using ROP; Building ROP Chains to Defeat DEP and Bypass ASLR; Windows 7 and 8; Porting Metasploit Modules; Client-side Exploitation; Windows Shellcode**

660.6 HANDS ON: Capture the Flag Challenge

This day will serve as a real-world challenge for students by requiring them to utilize skills they have learned throughout the course, think outside the box, and solve a range of problems from simple to complex. A web server scoring system and Capture-the-Flag engine will be provided to score students as they capture flags. More difficult challenges will be worth more points. In this offensive exercise, challenges range from local privilege escalation to remote exploitation on both Linux and Windows systems, as well as networking attacks and other challenges related to the course material.

Department of Defense Directive 8140

(DoDD 8570)

www.sans.org/dodd-8140

Department of Defense Directive 8570 has been replaced by the DoD CIO and is now DoDD 8140. DoDD 8570 is now part of a larger initiative that falls under the guidelines of DoDD 8140. DoDD 8140 provides guidance and procedures for the training, certification, and management of all government employees who conduct Information Assurance functions in assigned duty positions. These individuals are required to carry an approved certification for their particular job classification. GIAC certifications are among those required for Technical, Management, CND, and IASAE classifications.

Compliance/Recertification:

To stay compliant with DoDD 8140 requirements, you must maintain your certifications. GIAC certifications are renewable every four years.

Go to www.giac.org to learn more about certification renewal.

DoD Baseline IA Certifications

IAT Level I	IAT Level II	IAT Level III	IAM Level I	IAM Level II	IAM Level III
A+CE Network+CE SSCP	**GSEC** Security+CE SSCP	**GCED** **GCIH** **CISSP** (or Associate) CISA, CASP	**GSLC** CAP Security+CE	**GSLC** **CISSP** (or Associate) CAP, CASP CISM	**GSLC** **CISSP** (or Associate) CISM

Computer Network Defense (CND) Certifications

CND Analyst	CND Infrastructure Support	CND Incident Responder	CND Auditor	CND Service Provider Manager
GCIA **GCIH** CEH	SSCP CEH	**GCIH** **GCFA** CSIH, CEH	**GSNA** CISA CEH	CISSP - ISSMP CISM

Information Assurance System Architecture & Engineering (IASAE) Certifications

IASAE I	IASAE II	IASAE III
CISSP (or Associate) CASP, CSSCP	**CISSP** (or Associate) CASP, CSSLP	CISSP - ISSEP CISSP - ISSAP

Computer Environment (CE) Certifications

GCWN	**GCUX**

SANS Training Courses for DoDD Approved Certifications

SANS TRAINING COURSE		DoDD APPROVED CERT
SEC401	**Security Essentials Bootcamp Style**	**GSEC**
SEC501	**Advanced Security Essentials – Enterprise Defender**	**GCED**
SEC503	**Intrusion Detection In-Depth**	**GCIA**
SEC504	**Hacker Tools, Techniques, Exploits, and Incident Handling**	**GCIH**
SEC505	**Securing Windows and PowerShell Automation**	**GCWN**
SEC506	**Securing Linux/Unix**	**GCUX**
AUD507	**Auditing & Monitoring Networks, Perimeters, and Systems**	**GSNA**
FOR508	**Advanced Digital Forensics, Incident Response, and Threat Hunting**	**GCFA**
MGT414	**SANS Training Program for CISSP® Certification**	**CISSP**
MGT512	**SANS Security Leadership Essentials for Managers with Knowledge Compression™**	**GSLC**

SANS Intermediate and Specialized Skills

Incident Response and Enterprise Forensics

Incident Response and Enterprise Forensics

FOR508 Advanced Digital Forensics, Incident Response, and Threat Hunting

GCFA Certification Forensic Analyst

FOR572 Advanced Network Forensics and Analysis

GNFA Certification Network Forensic Analyst

Summary: Properly trained incident responders can hunt for and identify compromised systems, provide effective containment during a breach, and rapidly remediate an incident. They must have in-depth digital forensics knowledge of both host and network systems within the enterprise as well as knowing how to apply proactive threat intelligence – skills taught by SANS in **FOR508**, **FOR572**, and **FOR578**.

Specialized incident response and forensics skills are taught in six additional SANS courses, covering everything from Windows forensics to reverse engineering malware. Review the following pages for detailed information about all of these courses.

Who This Path Is for: Incident responders, cyber threat analysts, forensic examiners, security analysts and engineers all utilize this training path to advance their threat hunting and responding skills.

Why This Training Is Important: This training will teach you to detect compromised and affected systems, how and when a breach occurred, what attackers took or changed, and how to contain and remediate incidents. Upon completing your focus path in incident response and enterprise forensics, you will be able to incorporate evidence from different sources such as networks, mobile devices, and more into your investigations, provide better findings and get the job done faster.

> **"This material is directly relevant to what our analysts are doing daily. Highly useful."**
>
> -Tom L., U.S. Air Force

> **"This training gave me immediately applicable skills from active professionals in the field."**
>
> -Abe Jones, Spectrum Health

FOR408

Windows Forensic Analysis

GCFE Certification
Forensic Examiner

www.giac.org/gcfe

Six-Day Program
Mon, July 24 - Sat, July 29
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Rob Lee

Who Should Attend

- Information security professionals
- Incident response team members
- Law enforcement officers, federal agents, and detectives
- Media exploitation analysts
- Anyone interested in a deep understanding of Windows forensics

"It's the best Windows forensic class in the world."
-Bob A. Akin, SALC

"This is a fantastic course! Rob is a fantastic instructor with real-world application experience. This is a must for any investigator."
-Eddie Sky, Forsythe

ALSO AVAILABLE VIA SIMULCAST

See page 96 for details.

All organizations must prepare for cyber crime occurring on their computer systems and within their networks. Demand has never been higher for analysts who can investigate crimes like fraud, insider threats, industrial espionage, employee misuse, and computer intrusions. Government agencies increasingly require trained media exploitation specialists to recover key intelligence from Windows systems. To help solve these cases, SANS is training a new cadre of the world's best digital forensic professionals, incident responders, and media exploitation masters capable of piecing together what happened on computer systems second by second.

FOR408: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of the Microsoft Windows operating systems. You can't protect what you don't understand, and understanding forensic capabilities and artifacts is a core component of information security. You'll learn to recover, analyze, and authenticate forensic data on Windows systems. You'll understand how to track detailed user activity on your network and how to organize findings for use in incident response, internal investigations, and civil/criminal litigation. You'll be able to use your new skills to validate security tools, enhance vulnerability assessments, identify insider threats, track hackers, and improve security policies. Whether you know it or not, Windows is silently recording an unimaginable amount of data about you and your users. FOR408 teaches you how to mine this mountain of data.

Proper analysis requires real data for students to examine. The completely updated FOR408 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7/8/10, Office and Office365, cloud storage, Sharepoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Nothing is left out – attendees learn to analyze everything from legacy Windows XP systems to just-discovered Windows 10 artifacts.

FOR408 is continually updated. This course utilizes a brand-new intellectual property theft and corporate espionage case that took over six months to create. You work in the real world and your training should include real practice data. Our development team used incidents from their own experiences and investigations and created an incredibly rich and detailed scenario designed to immerse students in a true investigation. The case demonstrates the latest artifacts and technologies an investigator might encounter while analyzing Windows systems. The incredibly detailed step-by-step workbook details the tools and techniques that each investigator should follow to solve a forensic case.

MASTER WINDOWS FORENSICS – YOU CAN'T PROTECT WHAT YOU DON'T KNOW ABOUT

Rob Lee *SANS Faculty Fellow*

Rob Lee is an entrepreneur and consultant in the Washington, DC area and currently the Curriculum Lead and author for digital forensic and incident response training at the SANS Institute in addition to owning his own firm. Rob has more than 15 years' experience in computer forensics, vulnerability and exploit development, intrusion detection/prevention, and incident response. Rob graduated from the U.S. Air Force Academy and earned his MBA from Georgetown University. He served in the U.S. Air Force as a member of the 609th Information Warfare Squadron (IWS), the first U.S. military operational unit focused on information warfare. Later, he was a member of the Air Force Office of Special Investigations (AFOSI), where he led crime investigations and an incident response team. Over the next seven years, he worked directly with a variety of government agencies in the law enforcement, U.S. Department of Defense, and intelligence communities as the technical lead for vulnerability discovery and exploit development teams, lead for a cyber-forensics branch, and lead for a computer forensic and security software development team. Most recently, Rob was a Director for MANDIANT, a commercial firm focusing on responding to advanced adversaries such as the APT. Rob co-authored the book *Know Your Enemy*, 2nd Edition. Rob is also co-author of the MANDIANT threat intelligence report "M-Trends: The Advanced Persistent Threat." **@robtlee** & **@sansforensics**

408.1 HANDS ON: Windows Digital Forensics and Advanced Data Triage

The Windows forensics course starts with an examination of digital forensics in today's interconnected environments and discusses challenges associated with mobile devices, tablets, cloud storage, and modern Windows operating systems. We will discuss how modern hard drives, such as Solid State Devices (SSD), can affect the digital forensics acquisition process and how analysts need to adapt to overcome the introduction of these new technologies.

Topics: Windows Operating System Components; Core Forensic Principles; Live Response and Triage-Based Acquisition Techniques; Acquisition Review with Write Blocker; Advanced Acquisition Challenges; Windows Image Mounting and Examination; NTFS File System Overview; Document and File Metadata; File Carving; Custom Carving Signatures; Memory, Pagefile, and Unallocated Space Analysis

408.2 HANDS ON: CORE WINDOWS FORENSICS PART 1 – Windows Registry Forensics and Analysis

Our journey continues with the Windows Registry, where the digital forensic investigator will learn how to discover critical user and system information pertinent to almost any investigation. Each examiner will learn how to navigate and examine the Registry to obtain user-profile data and system data. The course teaches forensic investigators how to prove that a specific user performed key word searches, ran specific programs, opened and saved files, perused folders, and used removable devices.

Topics: Registry Basics; Profile Users and Groups; Core System Information; User Forensic Data; Tools Utilized

408.3 HANDS ON: CORE WINDOWS FORENSICS PART 2 – USB Devices, Shell Items, and Key Word Searching

Being able to show the first and last time a file was opened is a critical analysis skill. Utilizing shortcut (LNK) and jumplist databases, we are able to easily pinpoint which file was opened and when. We will demonstrate how to examine the pagefile, system memory, and unallocated space – all difficult-to-access locations that can offer the critical data for your case.

Topics: Shell Item Forensics; USB and Bring Your Own Device (BYOD) Forensic Examinations; Key Word Searching and Forensics Suites (AccessData's FTK, Guidance Software's EnCase)

408.4 HANDS ON: CORE WINDOWS FORENSICS PART 3 – Email, Key Additional Artifacts, and Event Logs

This section discusses what types of information can be relevant to an investigation, where to find email files, and how to use forensic tools to facilitate the analysis process. We will find that the analysis process is similar across different types of email stores, but the real work takes place in the preparation – finding and extracting the email files from a variety of different sources. The last part of the section will arm each investigator with the core knowledge and capability to maintain this crucial skill for many years to come.

Topics: Email Forensics; Forensicating Additional Windows OS Artifacts; Windows Event Log Analysis

408.5 HANDS ON: CORE WINDOWS FORENSICS PART 4 – Web Browser Forensics: Firefox, Internet Explorer, and Chrome

Throughout the section, investigators will use their skills in real hands-on cases, exploring evidence created by Chrome, Firefox, and Internet Explorer along with Windows Operating System artifacts.

Topics: Browser Forensics: History, Cache, Searches, Downloads, Understanding of Browser Timestamps, Internet Explorer; Firefox; Chrome; Examination of Browser Artifacts; Tools Used

408.6 HANDS ON: Windows Forensic Challenge

This complex case will involve an investigation into one of the most recent versions of the Windows Operating System. The evidence is real and provides the most realistic training opportunity currently available. Solving the case will require that students use all of the skills gained from each of the previous sections.

Topics: Digital Forensic Case; Windows 7 Forensic Challenge

SANS Technology Institute
www.sans.edu

www.sans.org/ondemand

You Will Be Able To

- Perform proper Windows forensic analysis by applying key techniques focusing on Windows 7/8/10
- Use full-scale forensic tools and analysis methods to detail nearly every action a suspect accomplished on a Windows system, including who placed an artifact on the system and how, program execution, file/folder opening, geo-location, browser history, profile USB device usage, and more
- Uncover the exact time that a specific user last executed a program through Registry and Windows artifact analysis, and understand how this information can be used to prove intent in cases such as intellectual property theft, hacker-breached systems, and traditional crimes
- Determine the number of times files have been opened by a suspect through browser forensics, shortcut file analysis (LNK), e-mail analysis, and Windows Registry parsing
- Identify keywords searched by a specific user on a Windows system in order to pinpoint the files and information the suspect was interested in finding and accomplish detailed damage assessments
- Use Windows shellbags analysis tools to articulate every folder and directory that a user opened up while browsing local, removable, and network drives
- Determine each time a unique and specific USB device was attached to the Windows system, the files and folders that were accessed on it, and who plugged it in by parsing key Windows artifacts such as the Registry and log files
- Use event log analysis techniques to determine when and how users logged into a Windows system, whether via a remote session, at the keyboard, or simply by unlocking a screensaver
- Determine where a crime was committed using registry data to pinpoint the geo-location of a system by examining connected networks and wireless access points
- Use free browser forensic tools to perform detailed web browser analysis, parse raw SQLite and ESE databases, and leverage session recovery artifacts and flash cookies to identify the web activity of suspects, even if privacy cleaners and in-private browsing are used

"This is a great look at forensic tools, acquiring data, and how they pertain to real-world scenarios."

-Rick Schroeder, Penn Medicine

FOR508

GCFA Certification
Forensic Analyst

www.giac.org/gcfa

Advanced Digital Forensics, Incident Response, and Threat Hunting

Six-Day Program
Mon, July 24 - Sat, July 29
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Chad Tilbury

Who Should Attend

- Incident response team members
- Threat hunters
- Experienced digital forensic analysts
- Information security professionals
- Federal agents and law enforcement
- Red team members, penetration testers, and exploit developers
- SANS FOR408 and SEC504 graduates

"This is, by far, the best training I have ever had. My forensic knowledge increased more in the last five days than in the last year."
-Vito Rocco, UNLV

FOR508: Advanced Digital Forensics, Incident Response, and Theat Hunting will help you to:

- **Detect how and when a breach occurred**
- **Identify compromised and affected systems**
- **Determine what attackers took or changed**
- **Contain and remediate incidents**
- **Develop key sources of threat intelligence**
- **Hunt down additional breaches using knowledge of the adversary**

See page 96 for details.

DAY 0: A 3-letter government agency contacts you to say an advanced threat group is targeting organizations like yours, and that your organization is likely a target. They won't tell how they know, but they suspect that there are already several breached systems within your enterprise. An advanced persistent threat, aka an APT, is likely involved. This is the most sophisticated threat that you are likely to face in your efforts to defend your systems and data, and these adversaries may have been actively rummaging through your network undetected for months or even years.

This is a hypothetical situation, but the chances are very high that hidden threats already exist inside your organization's networks. Organizations can't afford to believe that their security measures are perfect and impenetrable, no matter how thorough their security precautions might be. Prevention systems alone are insufficient to counter focused human adversaries who know how to get around most security and monitoring tools.

This in-depth incident response and threat hunting course provides responders and threat hunting teams with advanced skills to hunt down, identify, counter, and recover from a wide range of threats within enterprise networks, including APT nation-state adversaries, organized crime syndicates, and hactivism. Constantly updated, **FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting** addresses today's incidents by providing hands-on incident response and threat hunting tactics and techniques that elite responders and hunters are successfully using to detect, counter, and respond to real-world breach cases.

GATHER YOUR INCIDENT RESPONSE TEAM – IT'S TIME TO GO HUNTING!

Chad Tilbury *SANS Senior Instructor*

Chad Tilbury has been responding to computer intrusions and conducting forensic investigations since 1998. His extensive law enforcement and international experience stems from working with a broad cross-section of Fortune 500 companies and government agencies around the world. During his service as a Special Agent with the U.S. Air Force Office of Special Investigations, he investigated and conducted computer forensics for a variety of crimes, including hacking, abduction, espionage, identity theft, and multi-million-dollar fraud cases. He has led international forensic teams and was selected to provide computer forensic support to the United Nations Weapons Inspection Team. Chad has worked as a computer security engineer and forensic lead for a major defense contractor and as the Vice President of Worldwide Internet Enforcement for the Motion Picture Association of America. In that role, he managed Internet anti-piracy operations for the seven major Hollywood studios in over 60 countries. Chad is a graduate of the U.S. Air Force Academy and holds bachelor's and master's of science degrees in computer science as well as GCFA, GCIH, GREM, and ENCE certifications. He is currently a consultant specializing in incident response, corporate espionage, and computer forensics. **@chadtilbury**

508.1 HANDS ON: Advanced Incident Response and Threat Hunting

Incident responders and threat hunters should be armed with the latest tools, memory analysis techniques, and enterprise methodologies to identify, track, and contain advanced adversaries and to remediate incidents. Incident response and threat hunting analysts must be able to scale their analysis across thousands of systems in their enterprise. This section examines the six-step incident response methodology as it applies to an enterprise's response to a targeted attack.

Topics: **Real Incident Response Tactics; Threat Hunting; Cyber Threat Intelligence; Threat Hunting in the Enterprise; Malware Persistence Identification; Remote and Enterprise Incident Response**

508.2 HANDS ON: Memory Forensics in Incident Response & Threat Hunting

Now a critical component of many incident response and threat hunting teams that detect advanced threats in their organization, memory forensics has come a long way in just a few years. Memory forensics can be extraordinarily effective at finding evidence of worms, rootkits, and advanced malware used by an APT group of attackers. This extremely popular section will introduce some of the most capable tools available and give you a solid foundation to add core and advanced memory forensic skills to your incident response and forensics capabilities.

Topics: **Memory Acquisition; Memory Forensics Analysis Process for Response and Hunting; Memory Forensics Examinations; Memory Analysis Tools**

508.3 HANDS ON: Intrusion Forensics

Cyber defenders have a wide variety of tools and artifacts available to identify, hunt, and track adversary activity in a network. Each attacker's action leaves a corresponding artifact, and understanding what is left behind as footprints can be critical to both red and blue team members. Attacks follow a predictable pattern, and we focus our detective efforts on immutable portions of that pattern. In this section, we cover common attacker tradecraft and discuss the various data sources and forensic tools you can use to identify malicious activity in the enterprise.

Topics: **Advanced Evidence of Execution Detection; Window Shadow Volume Copy Analysis; Lateral Movement Adversary Tactics, Techniques, and Procedures (TTPs); Event Log Analysis for Incident Responders and Hunters**

508.4 HANDS ON: Timeline Analysis

Learn advanced incident response and hunting techniques uncovered via timeline analysis directly from the authors who pioneered timeline analysis tradecraft. This section will step you through the two primary methods of building and analyzing timelines created during advanced incident response, threat hunting, and forensic cases. Exercises will show analysts how to create a timeline and also how to introduce the key methods to help you use those timelines effectively in your cases.

Topics: **Timeline Analysis Overview; Memory Analysis Timeline Creation; Filesystem Timeline Creation & Analysis; Super Timeline Creation & Analysis**

508.5 HANDS ON: Incident Response and Hunting Across the Enterprise – Advanced Adversary and Anti-Forensics Detection

Over the years, we have observed that many incident responders and threat hunters have a challenging time finding threats without pre-built indicators of compromise or threat intelligence gathered before a breach. This is especially true in APT adversary intrusions. This advanced session will demonstrate techniques used by first responders to identify malware or forensic artifacts when very little information exists about their capabilities or hidden locations. We will discuss techniques to help funnel possibilities down to the candidates most likely to be evil malware trying to hide on the system.

Topics: **Evolution of Incident Response Scripting; Malware and Anti-Forensic Detection; Anti-Forensic Detection Methodologies; Identifying Compromised Hosts without Active Malware**

508.6 HANDS ON: The APT Incident Response Challenge

This incredibly rich and realistic enterprise intrusion exercise is based on a real-world advanced persistent threat (APT) group. It brings together techniques learned earlier in the week and tests your newly acquired skills in a case that simulates an attack by an advanced adversary. The challenge brings it all together using a real intrusion into a complete Windows enterprise environment. You will be asked to uncover how the systems were compromised in the initial intrusion, find other systems the adversary moved to laterally, and identify intellectual property stolen via data exfiltration. You will walk out of the course with hands-on experience investigating realistic attacks, curated by a cadre of instructors with decades of experience fighting advanced threats from attackers ranging from nation-states to financial crime syndicates and hactivist groups.

Topics: **Identification and Scoping; Containment and Threat Intelligence Gathering; Remediation and Recovery**

SANS Technology Institute
www.sans.edu

www.sans.org/cyber-guardian

MEETS DoDD 8140 (8570) REQUIREMENTS

www.sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

You Will Be Able To

- Learn and master the tools, techniques, and procedures necessary to effectively hunt, detect, and contain a variety of adversaries and to remediate incidents
- Detect and hunt unknown live, dormant, and custom malware in memory across multiple Windows systems in an enterprise environment
- Hunt through and perform incident response across hundreds of unique systems simultaneously using F-Response Enterprise and the SIFT Workstation
- Identify and track malware beaconing outbound to its command and control (C2) channel via memory forensics, registry analysis, and network connection residue
- Determine how the breach occurred by identifying the beachhead and spear phishing attack mechanisms
- Target advanced adversary anti-forensics techniques like hidden and time-stomped malware, along with utility-ware used to move in the network and maintain an attacker's presence
- Use memory analysis, incident response, and threat hunting tools in the SIFT Workstation to detect hidden processes, malware, attacker command lines, rootkits, network connections, and more
- Track user and attacker activity second-by-second on the system you are analyzing through in-depth timeline and super-timeline analysis
- Recover data cleared using anti-forensics techniques via Volume Shadow Copy and Restore Point analysis
- Identify lateral movement and pivots within your enterprise, showing how attackers transition from system to system without detection
- Understand how the attacker can acquire legitimate credentials – including domain administrator rights – even in a locked-down environment
- Track data movement as the attackers collect critical data and shift them to exfiltration collection points
- Recover and analyze archives and .rar files used by APT-like attackers to exfiltrate sensitive data from the enterprise network
- Use collected data to perform effective remediation across the entire enterprise

FOR526

Memory Forensics In-Depth

Six-Day Program
Mon, July 24 - Sat, July 29
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Alissa Torres

Who Should Attend

- Incident response team members
- Experienced digital forensic analysts
- Red team members, penetration testers, and exploit developers
- Law enforcement officers, federal agents, and detectives
- SANS FOR508 and SEC504 graduates
- Forensics investigators

"This course is totally awesome, relevant, and eye opening. I want to learn more every day."

-Matthew Britton,
Blue Cross Blue Shield of Louisiana

Digital Forensics and Incident Response (DFIR) professionals need Windows memory forensics training to be at the top of their game. Investigators who do not look at volatile memory are leaving evidence at the crime scene. RAM content holds evidence of user actions, as well as evil processes and furtive behaviors implemented by malicious code. It is this evidence that often proves to be the smoking gun that unravels the story of what happened on a system.

FOR526: Memory Forensics In-Depth provides the critical skills necessary for digital forensics examiners and incident responders to successfully perform live system memory triage and analyze captured memory images. The course uses the most effective freeware and open-source tools in the industry today and provides an in-depth understanding of how these tools work. FOR526 is a critical course for any serious DFIR investigator who wants to tackle advanced forensics, trusted insider, and incident response cases.

In today's forensics cases, it is just as critical to understand memory structures as it is to understand disk and registry structures. Having in-depth knowledge of Windows memory internals allows the examiner to access target data specific to the needs of the case at hand. For those investigating platforms other than Windows, this course also introduces OSX and Linux memory forensics acquisition and analysis using hands-on lab exercises.

There is an arms race between analysts and attackers. Modern malware and post-exploitation modules increasingly employ self-defense techniques that include more sophisticated rootkit and anti-memory analysis mechanisms that destroy or subvert volatile data. Examiners must have a deeper understanding of memory internals in order to discern the intentions of attackers or rogue trusted insiders. FOR526 draws on best practices and recommendations from experts in the field to guide DFIR professionals through acquisition, validation, and memory analysis with real-world and malware-laden memory images.

MALWARE CAN HIDE, BUT IT MUST RUN

FOR526:Memory Forensics In-Depth will teach you:

- **Proper Memory Acquisition: Demonstrate targeted memory capture ensuring data integrity and overcoming obstacles to acquisition/anti-acquisition behaviors**
- **How to Find Evil in Memory: Detect rogue, hidden, and injected processes, kernel-level rootkits, Dynamic Link Libraries (DLL) hijacking, process hollowing, and sophisticated persistence mechanisms**
- **Effective Step-by-Step Memory Analysis Techniques: Use process timelining, high-low level analysis, and walking the Virtual Address Descriptors (VAD) tree to spot anomalous behavior**
- **Best Practice Techniques: Learn when to implement triage, live system analysis, and alternative acquisition techniques and how to devise custom parsing scripts for targeted memory analysis**

Alissa Torres *SANS Certified Instructor*

Alissa specializes in advanced computer forensics and incident response. Her industry experience includes serving in the trenches as part of the Mandiant Computer Incident Response Team (MCIRT) as an incident handler and working on an internal security team as a digital forensic investigator. She has extensive experience in information security, spanning government, academic, and corporate environments and holds a bachelor's degree from the University of Virginia and a master's degree from the University of Maryland in information technology. Alissa has taught at the Defense Cyber Investigations Training Academy (DCITA), delivering incident response and network basics to security professionals entering the forensics community. She has presented at various industry conferences and numerous B-Sides events. In addition to being a GIAC Certified Forensic Analyst (GCFA), she holds the GCFE, GPEN, CISSP, EnCE, CFCE, MCT and CTT+ certifications. **@sibertor**

526.1 HANDS ON: Foundations in Memory Analysis and Acquisition

Simply put, memory analysis has become a required skill for all incident responders and digital forensics examiners. Regardless of the type of investigation, system memory and its contents often expose the first piece of the evidential thread that, when pulled, unravels the whole picture of what happened on the target system. Where is the malware? How did the machine get infected? Where did the attacker move laterally? Or what did the disgruntled employee do on the system? What lies in physical memory can provide answers to all of these questions and more.

Topics: Why Memory Forensics?; Investigative Methodologies; The Ubuntu SIFT and Windows 8.1 Workstations; The Volatility Framework; System Architectures; Triage versus Full Memory Acquisition; Physical Memory Acquisition

526.2 HANDS ON: Unstructured Analysis and Process Exploration

Structured memory analysis using tools that identify and interpret operating system structures is certainly powerful. However, many remnants of previously allocated memory remain available for analysis, and they cannot be parsed through structure identification. What tools are best for processing fragmented data? Unstructured analysis tools! They neither know nor care about operating system structures. Instead, they examine data, extracting findings using pattern matching. You will learn how to use Bulk Extractor to parse memory images and extract investigative leads such as email addresses, network packets, and more.

Topics: Unstructured Memory Analysis; Page File Analysis; Exploring Process Structures; List Walking and Scanning; Pool Memory; Exploring Process Relationships; Exploring DLLs; Kernel Objects

526.3 HANDS ON: Investigating the User via Memory Artifacts

An incident responder (IR) is often asked to triage a system because of a network intrusion detection system alert. The Security Operations Center makes the call and requires more information due to outbound network traffic from an endpoint and the IR team is asked to respond. In this section, we cover how to enumerate active and terminated TCP connections – selecting the right plugin for the job based on the OS version.

Topics: Network Connections; Virtual Address Descriptors; Detecting Injected Code; Analyzing the Registry via Memory Analysis; User Artifacts in Memory

526.4 HANDS ON: Internal Memory Structures

Day 4 focuses on introducing some internal memory structures (such as drivers), Windows memory table structures, and extraction techniques for portable executables. As we come to the final steps in our investigative methodology, "Spotting Rootkit Behaviors" and "Extracting Suspicious Binaries," it is important to emphasize again the rootkit paradox. The more malicious code attempts to hide itself, the more abnormal and seemingly suspicious it appears. We will use this concept to evaluate some of the most common structures in Windows memory for hooking, the IDTs and SSDTs.

Topics: Interrupt Descriptor Tables; System Service Descriptor Tables; Drivers; Direct Kernel Object Manipulation; Module Extraction; Hibernation Files; Crash Dump Files

526.5 HANDS ON: Memory Analysis on Platforms Other than Windows

Windows systems may be the most prevalent platform encountered by forensic examiners today, but most enterprises are not homogeneous. Forensic examiners and incident responders are best served by having the skills to analyze the memory of multiple platforms, including Linux and Mac – that is, platforms other than Windows.

Topics: Linux Memory Acquisition and Analysis; Mac Memory Acquisition and Analysis

526.6 HANDS ON: Memory Analysis Challenges

This final section provides students with a direct memory forensics challenge that makes use of the SANS NetWars Tournament platform. Your memory analysis skills are put to the test with a variety of hands-on scenarios involving hibernation files, Crash Dump files, and raw memory images, reinforcing techniques covered in the first five sections of the course. These challenges strengthen students' ability to respond to typical and atypical memory forensics challenges from all types of cases, from investigating the user to isolating the malware. By applying the techniques learned earlier in the course, students consolidate their knowledge and can shore up skill areas where they feel they need additional practice.

Topics: Malware and Rootkit Behavior Detection; Persistence Mechanism Identification; Code Injection Analysis; User Activity Reconstruction; Linux Memory Image Parsing; Mac OSX Memory Image Parsing; Windows Hibernation File Conversion and Analysis; Windows Crash Dump Analysis (Using Windows Debugger)

What You Will Receive

- SIFT Workstation 3
  This course extensively uses the SIFT Workstation 3 to teach incident responders and forensic analysts how to respond to and investigate sophisticated attacks. SIFT contains hundreds of free and open-source tools, easily matching any modern forensic and incident response commercial tool suite.
  - Ubuntu LTS base
  - 64 bit-based system
  - Better memory utilization
  - Auto-DFIR package update and customizations
  - Latest forensic tools and techniques
  - VMware Appliance ready to tackle forensics
  - Cross-compatibility between Linux and Windows
  - Expanded filesystem support (NTFS, HFS, EXFAT, and more)
- Windows 8.1 Workstation with license
  - 64 bit-based system
  - A licensed virtual machine loaded with the latest forensic tools
  - VMware Appliance ready to tackle forensics
- 32 GB Course USB 3.0
  - USB loaded with memory captures, SIFT workstation 3, tools, and documentation
- SANS Memory Forensics Exercise Workbook
  - Exercise book is over 200 pages long with detailed step-by-step instructions and examples to help you become a master incident responder
- SANS DFIR cheat sheets to help use the tools
- MP3 audio files of the complete course lecture

"An excellent course instructed by a very knowledgable GURU (Alissa Torres) with lots of real-world examples. Thanks!"

-Chip M., MoD

FOR572

GNFA Certification
Network Forensic Analyst

www.giac.org/gnfa

Advanced Network Forensics and Analysis *NEW!*

Six-Day Program
Mon, July 24 - Sat, July 29
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Philip Hagen

Who Should Attend

- Incident response team members and forensicators
- Hunt team members
- Law enforcement officers, federal agents, and detectives
- Information security managers
- Network defenders
- IT professionals
- Network engineers
- Anyone interested in computer network intrusions and investigations
- Security Operations Center personnel and information security practitioners

"Great training course that is exposing me to new networking concepts."

-John McDonald, Florida Department of Law Enforcement

Take your system-based forensic knowledge onto the wire. Incorporate network evidence into your investigations, provide better findings, and get the job done faster.

ALSO AVAILABLE VIA SIMULCAST

See page 96 for details.

It is exceedingly rare to work any forensic investigation that doesn't have a network component. Endpoint forensics will always be a critical and foundational skill for this career, but overlooking their network communications is akin to ignoring security camera footage of a crime as it was committed. Whether you handle an intrusion incident, data theft case, employee misuse scenario, or are engaged in proactive adversary discovery, the network often provides an unparalleled view of the incident. Its evidence can provide the proof necessary to show intent, uncover attackers that have been active for months or longer, or may even prove useful in definitively proving a crime actually occurred.

FOR572: Advanced Network Forensics and Analysis was built from the ground up to cover the most critical skills needed to mount efficient and effective post-incident response investigations. We focus on the knowledge necessary to expand the forensic mindset from residual data on the storage media from a system or device to the transient communications that occurred in the past or continue to occur. Even if the most skilled remote attacker compromised a system with an undetectable exploit, the system still has to communicate over the network. Without command-and-control and data extraction channels, the value of a compromised computer system drops to almost zero. Put another way: Bad guys are talking – we'll teach you to listen.

This course covers the tools, technology, and processes required to integrate network evidence sources into your investigations, with a focus on efficiency and effectiveness. You will leave this week with a well-stocked toolbox and the knowledge to use it on your first day back on the job. We will cover the full spectrum of network evidence, including high-level NetFlow analysis, low-level pcap exploration, ancillary network log examination, and more. We cover how to leverage existing infrastructure devices that may contain months or years of valuable evidence as well as how to place new collection platforms while an incident is already under way.

Whether you are a consultant responding to a client's site, a law enforcement professional assisting victims of cybercrime and seeking prosecution of those responsible, an on-staff forensic practitioner, or a member of the growing ranks of "threat hunters", this course offers hands-on experience with real-world scenarios that will help take your work to the next level. Previous SANS SEC curriculum students and other network defenders will benefit from the FOR572 perspective on security operations as they take on more incident response and investigative responsibilities. SANS Forensics alumni from FOR408 and FOR508 can take their existing knowledge and apply it directly to the network-based attacks that occur daily. In FOR572, we solve the same caliber of real-world problems without the use of disk or memory images.

The hands-on labs in this class cover a wide range of tools and platforms, including the venerable tcpdump and Wireshark for packet capture and analysis; NetworkMiner for artifact extraction; and open-source tools including nfdump, tcpxtract, tcpflow, and more. Newly added tools in the course include the SOF-ELK platform – a VMware appliance pre-configured with the ELK stack. This "big data" platform includes the Elasticsearch storage and search database, the Logstash ingest and parse utility, and the Kibana graphical dashboard interface. Together with the custom SOF-ELK configuration files, the platform gives forensicators a ready-to-use platform for log and NetFlow analysis. For full-packet analysis and hunting at scale, the Moloch platform is also used. Through all of the in-class labs, your shell scripting abilities will also be used to make easy work of ripping through hundreds and thousands of data records.

Philip Hagen *SANS Certified Instructor*

Philip Hagen has been working in the information security field since 1998, running the full spectrum including deep technical tasks, management of an entire computer forensic services portfolio, and executive responsibilities. Currently, Phil is an Evangelist at Red Canary, where he engages with current and future customers of Red Canary's managed threat detection service to ensure their use of the service is best aligned for success in the face of existing and future threats. Phil started his security career while attending the U.S. Air Force Academy, with research covering both the academic and practical sides of security. He served in the Air Force as a communications officer at Beale AFB and the Pentagon. In 2003, Phil became a government contractor, providing technical services for various IT and information security projects. These included systems that demanded 24x7x365 functionality. He later managed a team of 85 computer forensic professionals in the national security sector. He provided forensic consulting services for law enforcement, government, and commercial clients prior to joining the Red Canary team. Phil is the course lead and co-author of FOR572: Advanced Network Forensics and Analysis. **@PhilHagen**

572.1 HANDS ON: Off the Disk and Onto the Wire

Network data can be preserved, but only if captured directly from the wire. Whether tactical or strategic, packet capture methods are quite basic. You will re-acquaint yourself with tcpdump and Wireshark, the most common tools used to capture and analyze network packets, respectively. However, since long-term full-packet capture is still uncommon in most environments, many artifacts that can tell us about what happened on the wire in the past come from devices that manage network functions. You will learn about what kinds of devices can provide valuable evidence and at what level of granularity. We will walk through collecting evidence from one of the most common sources of network evidence, a web proxy server, then you'll go hands-on to find and extract stolen data from the proxy yourself. The Linux SIFT virtual machine, which has been specifically loaded with a set of network forensic tools, will be your primary toolkit for the week.

Topics: Web Proxy Server Examination; Foundational Network Forensics Tools: tcpdump and Wireshark; Network Evidence Acquisition; Network Architectural Challenges and Opportunities

572.2 HANDS ON: Core Protocols & Log Aggregation/Analysis

Understanding log data and how it can guide the investigative process is an important network forensicator skill. Examining network-centric logs can also fill gaps left by an incomplete or nonexistent network capture. In this section, you will learn various logging mechanisms available to both endpoint and network transport devices. You will also learn how to consolidate log data from multiple sources, providing a broad corpus of evidence in one location. As the volume of log data increases, so does the need to consider automated analytic tools. You'll use the SOF-ELK platform for post-incident log aggregation and analysis, bringing quick and decisive insight to a compromise investigation.

Topics: Hypertext Transfer Protocol (HTTP): Protocol and Logs; Domain Name Service (DNS): Protocol and Logs; Firewall, Intrusion Detection System, and Network Security Monitoring Logs; Logging Protocol and Aggregation; ELK Stack and the SOF-ELK Platform

572.3 HANDS ON: NetFlow and File Access Protocols

In this section, you will learn the contents of typical NetFlow protocols, as well as common collection architectures and analysis methods. You'll also learn how to distill full-packet collections to NetFlow records for quick initial analysis before diving into more cumbersome pcap files. You'll also examine the File Transfer Protocol, including how to reconstruct specific files from an FTP session. While FTP is commonly used for data exfiltration, it is also an opportunity to refine protocol analysis techniques, due to its multiple-stream nature. Lastly, you'll explore a variety of the network protocols unique to a Microsoft Windows or Windows-compatible environment. Attackers frequently use these protocols to "live off the land" within the victim's environment. By using existing and expected protocols, adversaries can hide in plain sight and avoid deploying malware that could tip off the investigators to their presence and actions.

Topics: NetFlow Collection and Analysis; Open-Source Flow Tools; File Transfer Protocol (FTP); Microsoft Protocols

572.4 HANDS ON: Commercial Tools, Wireless, and Full-Packet Hunting

Commercial tools hold clear advantages in some situations a forensicator may typically encounter. Most commonly, this centers on scalability. Many open-source tools are designed for tactical or small-scale use. Whether using them for large-scale deployments or for specific niche functionalities, these tools can immediately address many investigative needs. You'll look at the typical areas where commercial tools in the network forensic realm tend to focus, and discuss the value each may provide for your organizational requirements or those of your clients. Additionally, we will address the forensic aspects of wireless networking.

Topics: Simple Mail Transfer Protocol (SMTP); Commercial Network Forensics; Wireless Network Forensics; Automated Tools and Libraries; Full-Packet Hunting with Moloch

572.5 HANDS ON: Encryption, Protocol Reversing, OPSEC, and Intel

Encryption is frequently cited as the most significant hurdle to effective network forensics, and for good reason. When properly implemented, encryption can be a brick wall in between an investigator and critical answers. However, technical and implementation weaknesses can be used to our advantage. Even in the absence of these weaknesses, the right analytic approach to encrypted network traffic can still yield valuable information about the content. We will discuss the basics of encryption and how to approach it during an investigation. The section will also cover flow analysis to characterize encrypted conversations.

Topics: Encoding, Encryption, and SSL; Man in the Middle; Network Protocol Reverse Engineering; Investigation OPSEC and Threat Intel

572.6 HANDS ON: Network Forensics Capstone Challenge

Students will test their understanding of network evidence and their ability to articulate and support hypotheses through presentations made to the instructor and class. The audience will include senior-level decision-makers, so all presentations must include executive summaries as well as technical details. Time permitting, students should also include recommended steps that could help to prevent, detect, or mitigate a repeat compromise.

Topics: Network Forensic Case

You Will Be Able To

- Extract files from network packet captures and proxy cache files, allowing follow-on malware analysis or definitive data loss determination
- Use historical NetFlow data to identify relevant past network occurrences, allowing accurate incident scoping
- Reverse-engineer custom network protocols to identify an attacker's command-and-control abilities and actions
- Decrypt captured SSL traffic to identify attackers' actions and what data they extracted from the victim
- Use data from typical network protocols to increase the fidelity of the investigation's findings
- Identify opportunities to collect additional evidence based on the existing systems and platforms within a network architecture
- Examine traffic using common network protocols to identify patterns of activity or specific actions that warrant further investigation
- Incorporate log data into a comprehensive analytic process, filling knowledge gaps that may be far in the past
- Learn how attackers leverage man-in-the-middle tools to intercept seemingly secure communications
- Examine proprietary network protocols to determine what actions occurred on the endpoint systems
- Analyze wireless network traffic to find evidence of malicious activity
- Learn how to modify configuration on typical network devices such as firewalls and intrusion detection systems to increase the intelligence value of their logs and alerts during an investigation
- Apply the knowledge you acquire during the week in a full-day capstone exercise, modeled after real-world nation-state intrusions

FOR578

Cyber Threat Intelligence

Five-Day Program
Mon, July 24 - Fri, July 28
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Jake WIlliams

Who Should Attend

- Incident response team members
- Threat hunters
- Experienced digital forensic analysts
- Security Operations Center personnel and information security practitioners
- Federal agents and law enforcement officials
- SANS FOR408, FOR572, FOR508, or FOR610 graduates looking to take their skills to the next level

"Outstanding course material and instructor presentation! It truly drills into the analytic process, while remaining technical. I highly recommend this course to anyone performing any level of intelligence support to defensive cyber operations."

-Thomas L., U.S. Air Force

ALSO AVAILABLE VIA SIMULCAST

See page 96 for details.

Make no mistake: current network defense, threat hunting, and incident response practices contain a strong element of intelligence and counterintelligence that cyber analysts must understand and leverage in order to defend their networks, proprietary data, and organizations.

FOR578: Cyber Threat Intelligence will help network defenders, threat hunting teams, and incident responders to:

- **Understand and develop skills in tactical, operational, and strategic-level threat intelligence**
- **Generate threat intelligence to detect, respond to, and defeat advanced persistent threats (APTs)**
- **Validate information received from other organizations to minimize resource expenditures on bad intelligence**
- **Leverage open-source intelligence to complement a security team of any size**
- **Create Indicators of Compromise (IOCs) in formats such as YARA, OpenIOC, and STIX.**

The collection, classification, and exploitation of knowledge about adversaries – collectively known as cyber threat intelligence – gives network defenders information superiority that is used to reduce the adversary's likelihood of success with each subsequent intrusion attempt. Responders need accurate, timely, and detailed information to monitor new and evolving attacks, as well as methods to exploit this information to put in place an improved defensive posture.

Cyber threat intelligence thus represents a force multiplier for organizations looking to update their response and detection programs to deal with increasingly sophisticated advanced persistent threats. Malware is an adversary's tool but the real threat is the human one, and cyber threat intelligence focuses on countering those flexible and persistent human threats with empowered and trained human defenders.

During a targeted attack, an organization needs a top-notch and cutting-edge threat hunting or incident response team armed with the threat intelligence necessary to understand how adversaries operate and to counter the threat. **FOR578: Cyber Threat Intelligence** will train you and your team in the tactical, operational, and strategic-level cyber threat intelligence skills and tradecraft required to make security teams better, threat hunting more accurate, incident response more effective, and organizations more aware of the evolving threat landscape.

THERE IS NO TEACHER BUT THE ENEMY!

Jake Williams *SANS Certified Instructor*

Jake Williams is a Principal Consultant at Rendition Infosec. He has more than a decade of experience in secure network design, penetration testing, incident response, forensics, and malware reverse engineering. Before founding Rendition Infosec, Jake worked with various cleared government agencies in information security roles. He is well versed in cloud forensics and previously developed a cloud forensics course for a U.S. government client. Jake regularly responds to cyber intrusions by state-sponsored actors in the financial, defense, aerospace, and healthcare sectors using cutting-edge forensics and incident response techniques. He often develops custom tools to deal with specific incidents and malware-reversing challenges. Additionally, Jake performs exploit development and has privately disclosed a multitude of zero day exploits to vendors and clients. He found vulnerabilities in one of the state counterparts to healthcare.gov and recently exploited antivirus software to perform privilege escalation. Jake developed Dropsmack, a pentesting tool (okay, malware) that performs command and control and data exfiltration over cloud file sharing services. Jake also developed an anti-forensics tool for memory forensics, Attention Deficit Disorder (ADD). This tool demonstrated weaknesses in memory forensics techniques. **@MalwareJake**

578.1 HANDS ON: Cyber Threat Intelligence

Cyber threat intelligence is a rapidly growing field. However, intelligence was a profession long before the word "cyber" entered the lexicon. Understanding the key points regarding intelligence terminology, tradecraft, and impact is vital to understanding and using cyber threat intelligence. This section introduces students to the most important concepts of intelligence, analysis tradecraft, and levels of threat intelligence, and the value they can add to organizations. As with all sections, the day includes immersive hands-on labs to ensure that students have the ability to turn theory into practice.

Topics: Case-Study: Carbanak, "The Great Bank Robbery"; Understanding Intelligence; Understanding Cyber Threat Intelligence; Tactical Threat Intelligence Introduction; Operational Threat Intelligence Introduction; Strategic Threat Intelligence Introduction

578.2 HANDS ON: Tactical Threat Intelligence: Kill Chain for Intrusion Analysis

Tactical cyber threat intelligence requires that analysts extract and categorize indicators and adversary tradecraft from intrusions. These actions enable all other levels of threat intelligence by basing intelligence on observations and facts that are relevant to the organization. One of the most commonly used models for assessing adversary intrusions is the "kill chain." This model is a framework to understand the steps an adversary must accomplish to be successful. This section will help tactical threat intelligence develop the skills required to be successful by using the kill chain as a guide. Students will then pivot into open-source intelligence-gathering tradecraft to enrich their understanding of the analyzed intrusion. The section walks students through multi-phase intrusions from initial notification of adversary activity to the completion of analysis of the event. The section also highlights the importance of this process to structuring and defining adversary campaigns.

Topics: Kill Chain Courses of Action; Tactical Threat Intelligence Requirements; Kill Chain Deep Dive; Handling Multiple Kill Chains; Pivoting to Open-Source Intelligence

578.3 HANDS ON: Tactical/Operational Threat Intelligence: Campaigns and Open-Source Intelligence

Developing an understanding of adversary campaigns and tradecraft requires piecing together individual intrusions and data points. Organizations of any size will need to complement what they know from internal analysis with open-source intelligence (OSINT) to enrich and validate the information. This allows security personnel to understand dedicated adversaries more fully and consistently defend their environments. In this section, students learn what campaigns are, why they are important, and how to define them. From this baseline intelligence, gaps and collection opportunities are identified for fulfillment via open-source resources and methods. Common types and implementations of open-source data repositories, as well as their use, are explored in-depth through classroom discussion and exercises. These resources can produce an enormous volume of intelligence about intrusions, which may contain obscure patterns that further elucidate campaigns or actors. Tools and techniques to expose these patterns within the data through higher-order analysis will be demonstrated in narrative and exercise form. The application of the resulting intelligence will be articulated for correlation, courses of action, campaign assembly, and more.

Topics: Case Study: Axiom; OSINT Pivoting, Link Analysis, and Domains; OSINT From Malware; Case Study: GlassRAT; Intelligence Aggregation and Data Visualization; Defining Campaigns; Communicating About Campaigns

578.4 HANDS ON: Operational Threat Intelligence: Sharing Intelligence

Many organizations seek to share intelligence but often falter in understanding the value of shared intelligence, its limitations, and the right formats to choose for each audience. This section will focus on identifying both open-source and professional tools that are available for students as well as sharing standards for each level of cyber threat intelligence both internally and externally. Students will learn about YARA and generate YARA rules to help incident responders, security operations personnel, and malware analysts. They will gain hands-on experience with STIX and understand the CybOX and TAXII frameworks for sharing information between organizations. Finally, the section will focus on sharing intelligence at the strategic level in the form of reports, briefings, and analytical assessments in order to help organizations make required changes to counter persistent threats and safeguard business operations.

Topics: Storing Threat Intelligence; Sharing: Tactical; Case Study: Sony Attack; Sharing: Operational; Sharing: Strategic

578.5 HANDS ON: Strategic Threat Intelligence: Higher-Order Analysis

A core component of intelligence analysis at any level is the ability to defeat biases and analyze information. At the strategic level of cyber threat intelligence, the skills required to think critically are exceptionally important and can have organization-wide or national-level impact. In this section, students will learn about logical fallacies and cognitive biases as well as how to defeat them. They will also learn about nation-state attribution, when it can be of value, and when it is merely a distraction. Students will also learn about nation-state-level attribution from previously identified campaigns and take away a more holistic view of the cyber threat intelligence industry to date. The class will finish with a discussion on consuming threat intelligence and actionable takeaways for students to make significant changes in their organizations.

Topics: Logical Fallacies and Cognitive Biases; Analysis of Competing Hypotheses; Case Study: Stuxnet; Human Elements of Attribution; Nation-State Attribution; Case Study: Sofacy; A Look Backward; Case Study: Cyber Attack on the Ukrainian Power Grid; Active Defense

Statements From Our Authors

The author team of Mike Cloppert, Chris Sperry, and Robert M. Lee originally developed FOR578 with the understanding that the community was in need of a single concise collection of tradecraft. Cloppert and Sperry initiated the development of the course with the understanding that their schedules would not permit them to be able to constantly teach it. However, it was through their thought leadership that the class has become what it is today. Their influence on the course development remains, and SANS thanks them for their leadership.

"When considering the value of threat intelligence, most individuals and organizations ask themselves three questions: What is threat intelligence? When am I ready for it? How do I use it? This class answers these questions and more at a critical point in the development of the field of threat intelligence in the wider community. The course will empower analysts of any technical background to think more critically and be prepared to face persistent and focused threats."
-Robert M. Lee

"Threat intelligence is a powerful tool in the hands of a trained analyst. It can provide insight to all levels of a security program, from security analysts responding to tactical threats against the network to executives reporting strategic level threats to the Board of Directors. This course will give students an understanding of the role of threat intelligence in security operations and how it can be leveraged as a game-changing resource to combat an increasingly sophisticated adversary."
-Rebekah Brown

"Before threat intelligence was a buzzword, it was something we all used to just do as part of incident response. But I'll admit that most of us used to do it badly. Or more accurately, ad hoc at best. We simply lacked structured models for intrusion analysis, campaign tracking, and consistent reporting of threats. Today, we need analysts trained in intelligence analysis techniques ready to perform proper campaign modeling, attribution, and threat analysis. The Cyber Threat Intelligence course teaches students all of that, as well as how to avoid cognitive biases in reporting and the use of alternative competing hypothesis in intelligence analysis. These are critical skills that most in industry today absolutely lack."
-Jake Williams

FOR585

GASF Certification
Advanced Smartphone Forensics

www.giac.org/gasf

Advanced Smartphone Forensics

Six-Day Program
Mon, July 24 - Sat, July 29
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Heather Mahalik

Who Should Attend

- Experienced digital forensic analysts who want to extend their knowledge and experience to forensic analysis of mobile devices, especially smartphones
- Media exploitation analysts who need to master Tactical Exploitation or Document and Media Exploitation (DOMEX) operations on smartphones and mobile devices by learning how individuals used their smartphones, who they communicated with, and what files they accessed
- Information security professionals who respond to data breach incidents and intrusions
- Incident response teams tasked with identifying the role that smartphones played in a breach
- Law enforcement officers, federal agents, and detectives who want to master smartphone forensics and expand their investigative skills beyond traditional host-based digital forensics
- IT auditors who want to learn how smartphones can expose sensitive information
- SANS SEC575, FOR408, FOR508, FOR518, and FOR572 graduates looking to take their skills to the next level

Mobile devices are often a key factor in criminal cases, intrusions, IP theft, security threats, and other types of attacks. Understanding how to leverage the data from the device in a correct manner can make or break your case and your future as an expert. **FOR585: Advanced Smartphone Forensics** will teach you those skills.

Every time the smartphone "thinks" or makes a suggestion, the data are saved. It's easy to get mixed up in what the forensic tools are reporting. Smartphone forensics is more than pressing the "find evidence" button and getting answers. Your team cannot afford to rely solely on the tools in your lab. You have to understand how to use them correctly to guide your investigation, instead of just letting the tool report what it believes happened on the device. It is impossible for commercial tools to parse everything from smartphones and understand how the data were put on the device. Examining and interpreting the data is your job, and this course will provide you and your organization with the capability to find and extract the correct evidence from smartphones with confidence.

This in-depth smartphone forensics course provides examiners and investigators with advanced skills to detect, decode, decrypt, and correctly interpret evidence recovered from mobile devices. The course features 17 hands-on labs that allow students to analyze different datasets from smart devices and leverage the best forensic tools and custom scripts to learn how smartphone data hide and can be easily misinterpreted by forensic tools. Each lab is designed to teach you a lesson that can be applied to other smartphones. You will gain experience with the different data formats on multiple platforms and learn how the data are stored and encoded on each type of smart device. The labs will open your eyes to what you are missing by relying 100% on your forensic tools.

FOR585 is continuously updated to keep up with the latest malware, smartphone operating systems, third-party applications, and encryption. This intensive six-day course offers the most unique and current instruction available, and it will arm you with mobile device forensic knowledge you can apply immediately to cases you're working on the day you finish the course.

Smartphone technologies are constantly changing, and most forensic professionals are unfamiliar with the data formats for each technology. Take your skills to the next level: it's time for the good guys to get smarter and for the bad guys to know that their texts and apps can and will be used against them!

SMARTPHONE DATA CAN'T HIDE FOREVER – IT'S TIME TO OUTSMART THE MOBILE DEVICE!

Heather Mahalik *SANS Senior Instructor*

Heather Mahalik is a project manager for Ocean's Edge, where she uses her experience to manage projects focused on wireless cybersecurity and mobile application development. Heather has over 12 years of experience in digital forensics, vulnerability discovery of mobile devices, application reverse engineering and manual decoding. She is currently the course lead for FOR585: Advanced Smartphone Forensics. Previously, Heather headed the mobile device team for Basis Technology, where she led the mobile device exploitation efforts in support of the U.S. government. She also worked as a forensic examiner at Stroz Friedberg and the U.S. State Department Computer Investigations and Forensics Lab, where she focused on high-profile cases. Heather co-authored *Practical Mobile Forensics* and various white papers, and has presented at leading conferences and instructed classes focused on Mac forensics, mobile device forensics, and computer forensics to practitioners in the field. Heather blogs and hosts work from the digital forensics community at www.smarterforensics.com. **@HeatherMahalik**

585.1 HANDS ON: Smartphone Overview and Malware Forensics

Although smartphone forensics concepts are similar to those of digital forensics, smartphone file system structures require specialized decoding skills to correctly interpret the data acquired from the device. On the first course day students will apply what they already know to smartphone forensics handling, device capabilities, acquisition methods and data encoding concepts of smartphone components. Students will also become familiar with the forensics tools required to complete comprehensive examinations of smartphone data structures. Malware affects a plethora of smartphone devices. This section will examine various types of malware, how it exists on smartphones and how to identify it. Most commercial tools help you identify malware, but none of them will allow you to tear down the malware to the level we cover in class. Up to five labs will be conducted on this first day alone!

Topics: The SIFT Workstation; Malware and Spyware Forensics; Introduction to Smartphones; Smartphone Handling; Forensic Acquisition of Smartphones; Smartphone Forensics Tool Overview; JTAG Forensics; Smartphone Components

585.2 HANDS ON: Android Forensics

Android devices are among the most widely used smartphones in the world, which means they will surely be part of an investigation that will come across your desk. Android devices contain substantial amounts of data that can be decoded and interpreted into useful information. However, without honing the appropriate skills for bypassing locked Androids and correctly interpreting the data stored on them, you will be unprepared for the rapidly evolving world of smartphone forensics.

Topics: Android Forensics Overview; Handling Locked Android Devices; Android File System Structures; Android Evidentiary Locations; Traces of User Activity on Android Devices

585.3 HANDS ON: iOS Forensics

Apple iOS devices contain substantial amounts of data (including deleted records) that can be decoded and interpreted into useful information. Proper handling and parsing skills are needed for bypassing locked iOS devices and correctly interpreting the data. Without iOS instruction, you will be unprepared to deal with the iOS device that will likely be a major component in a forensic investigation.

Topics: iOS Forensics Overview and Acquisition; iOS File System Structures; iOS Evidentiary Locations; Handling Locked iOS Devices; Traces of User Activity on iOS Devices

585.4 HANDS ON: Backup File and BlackBerry Forensics

We realize that not everyone examines BlackBerry devices. However, this section highlights pieces of evidence that can be found on multiple smartphones. Most importantly, we cover encrypted data on SD cards and how those data need to be acquired and examined. BlackBerry smartphones are designed to protect user privacy, but techniques taught in this section will enable the investigator to go beyond what the tools decode and manually recover data residing in database files of BlackBerry device file systems. Backup smartphone images are commonly found on external media and the cloud, and may be the only forensic acquisition method for newer iOS devices that are locked. Learning how to access and parse data from encrypted backup files may be the only lead to smartphone data relating to your investigation.

Topics: Backup File Forensics Overview; Common File Formats For Smartphone Backups; Creating and Parsing Backup Files; Evidentiary Locations on Backup Files; Locked Backup Files; Blackberry Forensics Overview; BlackBerry File System, Evidentiary Locations and Forensic Analysis

585.5 HANDS ON: Third-Party Application and Other Smartphone Device Forensics

This day starts with third-party applications across all smartphones and is designed to teach students how to leverage third-party application data and preference files to support an investigation. Next, other smartphones not afforded a full day of instruction are discussed and labs for each are provided. Given the prevalence of other types of smartphones around the world, it is critical for examiners to develop a foundation of understanding about data storage on multiple devices. You must acquire skills for handling and parsing data from uncommon smartphone devices. This course day will prepare you to deal with "misfit" smartphone devices and provide you with advanced methods for decoding data stored in third-party applications across all smartphones. The day ends with the students challenging themselves using tools and methods learned throughout the week to recover user data from a wiped Windows Phone.

Topics: Third-Party Applications on Smartphones Overview; Third-Party Application Locations on Smartphones; Decoding Third-Party Application Data on Smartphones; Knock-off Phone Forensics; Nokia (Symbian) Forensics; Windows Phone/Mobile Forensics

585.6 HANDS ON: Smartphone Forensics Capstone Exercise

This final course day will test all that you have learned during the course. Working in small groups, students will examine three smartphone devices and solve a scenario relating to a real-world smartphone forensic investigation. Each group will independently analyze the three smartphones, manually decode data, answer specific questions, form an investigation hypothesis, develop a report, and present findings.

You Will Be Able To

- Select the most effective forensic tools, techniques, and procedures for critical analysis of smartphone data
- Reconstruct events surrounding a crime using information from smartphones, including timeline development and link analysis (e.g., who communicated with whom, where, and when)
- Understand how smartphone file systems store data, how they differ, and how the evidence will be stored on each device
- Interpret file systems on smartphones and locate information that is not generally accessible to users
- Identify how the evidence got onto the mobile device – we'll teach you how to know if the user created the data, which will help you avoid the critical mistake of reporting false evidence obtained from tools
- Incorporate manual decoding techniques to recover deleted data stored on smartphones and mobile devices
- Tie a user to a smartphone at a specific date/time and at various locations
- Recover hidden or obfuscated communication from applications on smartphones
- Decrypt or decode application data that are not parsed by your forensic tools
- Detect smartphones compromised by malware and spyware using forensic methods
- Decompile and analyze mobile malware using open-source tools
- Handle encryption on smartphones and bypass, crack, and/or decode lock codes manually recovered from smartphones, including cracking iOS backup files that were encrypted with iTunes
- Understand how data is stored on smartphone components (SD cards) and how encrypted data can be examined by leveraging the smartphone
- Extract and use information from smartphones and their components, including Android, iOS, BlackBerry, Windows Phone, Nokia (Symbian), Chinese knock-offs, SIM cards, and SD cards
- Perform advanced forensic examinations of data structures on smartphones by diving deeper into underlying data structures that many tools do not interpret
- Analyze SQLite databases and raw data dumps from smartphones to recover deleted information
- Perform advanced data-carving techniques on smartphones to validate results and extract missing or deleted data
- Apply the knowledge you acquire during the course to conduct a full-day smartphone capstone event involving multiple devices and modeled after real-world smartphone investigations

FOR610

GREM Certification
Reverse Engineering Malware

www.giac.org/grem

Reverse-Engineering Malware: Malware Analysis Tools and Techniques

Six-Day Program
Mon, July 24 - Sat, July 29
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Lenny Zeltser

Who Should Attend

- Individuals who have dealt with incidents involving malware and want to learn how to understand key aspects of malicious programs
- Technologists who have informally experimented with aspects of malware analysis prior to the course and are looking to formalize and expand their expertise in this area
- Forensic investigators and IT practitioners looking to expand their skillsets and learn how to play a pivotal role in the incident response process

"This material is something you can use to build or enhance your company's playbook in terms of incident response and detection."

-Chris Bailey, California Lottery

This popular malware analysis course helps forensic investigators, incident responders, security engineers and IT administrators acquire practical skills for examining malicious programs that target and infect Windows systems. Understanding the capabilities of malware is critical to an organization's ability to derive the threat intelligence it needs to respond to information security incidents and fortify defenses. The course builds a strong foundation for analyzing malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger and other tools useful for turning malware inside-out.

The course begins by covering fundamental aspects of malware analysis. You will learn how to set up an inexpensive and flexible laboratory to understand the inner workings of malicious software and uncover characteristics of real-world malware samples. Then you will learn to examine the specimens' behavioral patterns and code. The course continues by discussing essential x86 assembly language concepts. You will examine malicious code to understand its key components and execution flow. Additionally, you will learn to identify common malware characteristics by looking at suspicious Windows API patterns employed by bots, rootkits, keyloggers, downloaders, and other types of malware.

This course will teach you how to handle self-defending malware. You'll learn how to bypass the protection offered by packers, and other anti-analysis methods. In addition, given the frequent use of browser malware for targeting systems, you will learn practical approaches to analyzing malicious browser scripts and deobfuscating JavaScript and VBScript to understand the nature of the attack.

You will also learn how to analyze malicious documents that take the form of Microsoft Office and Adobe PDF files. Such documents act as a common infection vector and may need to be examined when dealing with large-scale infections as well as targeted attacks. The course also explores memory forensics approaches to examining malicious software, especially useful if it exhibits rootkit characteristics.

The course culminates with a series of Capture-the-Flag challenges designed to reinforce the techniques learned in class and provide additional opportunities to learn practical malware analysis skills in a fun setting.

Hands-on workshop exercises are a critical aspect of this course and allow you to apply malware analysis techniques by examining malware in a lab that you control. When performing the exercises, you will study the supplied specimens' behavioral patterns and examine key portions of their code. To support these activities, you will receive pre-built Windows and Linux virtual machines that include tools for examining and interacting with malware.

Lenny Zeltser *SANS Senior Instructor*

Lenny Zeltser is a seasoned business leader with extensive experience in information technology and security. As a product management director at NCR Corporation, he focuses on safeguarding IT infrastructure of small and midsize businesses world-wide. Before NCR, Lenny led the enterprise security consulting practice at a major IT hosting provider. In addition, Lenny is a member of the Board of Directors at SANS Technology Institute and a volunteer incident handler at the Internet Storm Center. Lenny's expertise is strongest at the intersection of business, technology and information security practices and includes incident response, cloud services and product management. He frequently speaks at conferences, writes articles and has co-authored books on network security and malicious software defenses. Lenny is one of the few individuals in the world who've earned the prestigious GIAC Security Expert designation. He has a master's degree in business administration from MIT Sloan and a computer science degree from the University of Pennsylvania. **@lennyzeltser**

610.1 HANDS ON: Malware Analysis Fundamentals

Section one lays the groundwork for malware analysis by presenting the key tools and techniques useful for examining malicious programs. You will learn how to save time by exploring Windows malware in two phases. Behavioral analysis focuses on the program's interactions with its environment, such as the registry, the network, and the file system. Code analysis focuses on the specimen's code and makes use of a disassembler and debugger tools such as IDA Pro and OllyDbg. You will learn how to set up a flexible laboratory to perform such analysis in a controlled manner, and set up such a lab on your laptop using the supplied Windows and Linux (REMnux) virtual machines. You will then learn how to use the key analysis tools by examining a malware sample in your lab – with guidance and explanations from the instructor – to reinforce the concepts discussed throughout the day.

Topics: **Assembling a Toolkit for Effective Malware Analysis; Examining Static Properties of Suspicious Programs; Performing Behavioral Analysis of Malicious Windows Executables; Performing Static and Dynamic Code Analysis of Malicious Windows Executables; Contributing Insights to the Organization's Larger Incident Response Effort**

610.2 HANDS ON: Malicious Code Analysis

Section two focuses on examining malicious Windows executables at the assembly level. You will discover approaches for studying inner workings of a specimen by looking at it through a disassembler and, at times, with the help of a debugger. The section begins with an overview of key code-reversing concepts and presents a primer on essential x86 Intel assembly concepts, such as instructions, function calls, variables, and jumps. You will also learn how to examine common assembly constructs, such as functions, loops, and conditional statements. The remaining part of the section discusses how malware implements common characteristics, such as keylogging and DLL injection, at the assembly level. You will learn how to recognize such characteristics in suspicious Windows executable files.

Topics: **Core Concepts for Analyzing Malware at the Code Level; x86 Intel Assembly Language Primer for Malware Analysts; Identifying Key x86 Assembly Logic Structures with a Disassembler; Patterns of Common Malware Characteristics at the Windows API Level (DLL Injection, Function Hooking, Keylogging, Communicating over HTTP, etc.)**

610.3 HANDS ON: In-Depth Malware Analysis

Section three builds upon the approaches to behavioral and code analysis introduced earlier in the course, exploring techniques for uncovering additional aspects of the functionality of malicious programs. You will learn about packers and the techniques that may help analysts bypass their defenses. Additionally, you will understand how to redirect network traffic in the lab to better interact with malware to understand its capabilities. You will also learn how to examine malicious websites and deobfuscate browser scripts, which often play a pivotal role in malware attacks.

Topics: **Recognizing Packed Malware; Automated Malware Unpacking Tools and Approaches; Manual Unpacking of Using OllyDbg, Process Dumping Tools and Imports-Rebuilding Utilities; Intercepting Network Connections in the Malware Lab; Interacting with Malicious Websites to Examine their Nature; Deobfuscating Browser Scripts Using Debuggers and Runtime Interpreters; JavaScript Analysis Complications**

610.4 HANDS ON: Self-Defending Malware

Section four focuses on the techniques malware authors commonly employ to protect malicious software from being examined, often with the help of packers. You will learn how to recognize and bypass anti-analysis measures, such as tool detection, string obfuscation, unusual jumps, breakpoint detection and so on. We will also discuss the role that shellcode plays in the context of malware analysis and learn how to examine this aspect of attacks. As with the other topics covered throughout the course, you will be able to experiment with such techniques during hands-on exercises.

Topics: **Bypassing Anti-Analysis Defenses; Recovering Concealed Malicious Code and Data; Unpacking More Sophisticated Packers to Locate the Original Entry Point (OEP); Identifying and Disabling Methods Employed by Malware to Detect Analysts' Tools; Analyzing Shellcode to Assist with the Examination of Malicious Documents and other Artifacts**

610.5 HANDS ON: Malicious Documents and Memory Forensics

Section five starts by exploring common patterns of assembly instructions often used to gain initial access to the victim's computer. Next, we will learn how to analyze malicious Microsoft Office documents, covering tools such as OfficeMalScanner and exploring steps for analyzing malicious PDF documents with practical tools and techniques. Another major topic covered in this section is the reversing of malicious Windows executables using memory forensics techniques. We will explore this topic with the help of tools such as the Volatility Framework and associated plug-ins. The discussion of memory forensics will bring us deeper into the world of user and kernel-mode rootkits and allow us to use context of the infection to analyze malware more efficiently.

Topics: **Analyzing Malicious Microsoft Office (Word, Excel, PowerPoint) Documents; Analyzing Malicious Adobe PDF Documents; Analyzing Memory to Assess Malware Characteristics and Reconstruct Infection Artifacts; Using Memory Forensics to Analyze Rootkit Infections**

You Will Be Able To

- Build an isolated, controlled laboratory environment for analyzing code and behavior of malicious programs
- Employ network and system-monitoring tools to examine how malware interacts with the file system, registry, network, and other processes in a Windows environment
- Uncover and analyze malicious JavaScript and VBScript components of web pages, which are often used by exploit kits for drive-by attacks
- Control relevant aspects of the malicious program's behavior through network traffic interception and code patching to perform effective malware analysis
- Use a disassembler and a debugger to examine the inner-workings of malicious Windows executables
- Bypass a variety of packers and other defensive mechanisms designed by malware authors to misdirect, confuse and otherwise slow down the analyst
- Recognize and understand common assembly-level patterns in malicious code, such as DLL injection and anti-analysis measures
- Assess the threat associated with malicious documents, such as PDF and Microsoft Office files, in the context of targeted attacks
- Derive Indicators of Compromise (IOCs) from malicious executables to perform incident response triage
- Utilize practical memory forensics techniques to examine capabilities of rootkits and other malicious program types

610.6 HANDS ON: Malware Analysis Tournament

Section six assigns students to the role of a malware reverse engineer working as a member of an incident response and malware analysis team. Students are presented with a variety of hands-on challenges involving real-world malware in the context of a fun tournament. These challenges further a student's ability to respond to typical malware-reversing tasks in an instructor-led lab environment and offer additional learning opportunities. Moreover, the challenges are designed to reinforce skills covered in the first five sections of the course, making use of the hugely popular SANS NetWars tournament platform. By applying the techniques learned earlier in the course, students solidify their knowledge and can shore up skill areas where they feel they need additional practice. The students who score the highest in the malware reverse-engineering challenge will be awarded the coveted SANS' Digital Forensics Lethal Forensicator coin. Game on!

Topics: **Behavioral Malware Analysis; Dynamic Malware Analysis (Using a Debugger); Static Malware Analysis (Using a Disassembler); JavaScript Deobfuscation; PDF Document Analysis; Office Document Analysis; Memory Analysis**

ONLINE Training Options

FOR SANSFIRE 2017

WASHINGTON, DC JULY 22-29

Simulcast www.sans.org/simulcast

Six courses will be Simulcast from this event.
Attend SEC401, SEC503, FOR408, FOR508, FOR572, and FOR578 virtually!

OnDemand Bundle

Extend your SANSFIRE 2017 course online after the event with:

- Four months of online e-learning and review
- Subject-matter-expert support
- Additional quizzes and labs to reinforce your study

Learn more about your Online Training options at sans.org/online or contact us at ondemand@sans.org.

Employers need good talent. Veterans need good jobs. SANS VetSuccess Immersion Academy delivers both.

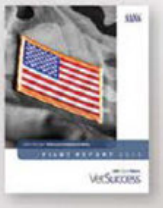
Introducing the SANS VetSuccess Immersion Academy, an intensive, accelerated program that provides the real-world training and certifications needed to fill critical jobs in cybersecurity.

For employers, the academy is a faster, more reliable, and less expensive way to find, train, certify, and employ highly qualified cybersecurity talent.

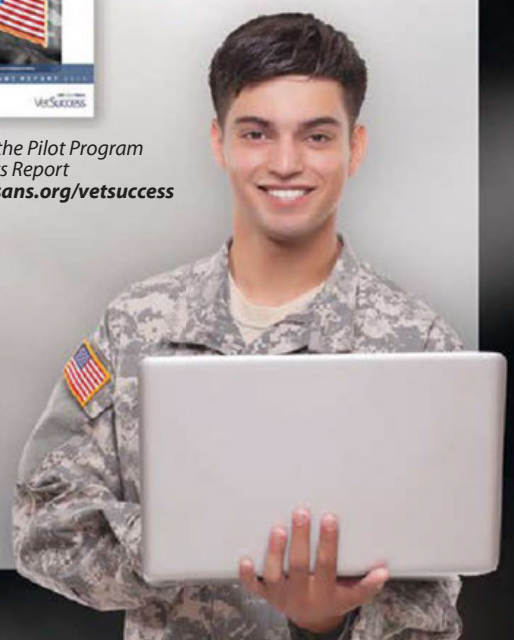
For transitioning veterans, the academy provides free accelerated training and certifications to quickly and effectively launch careers in cybersecurity.

Find out how your organization can benefit from hiring graduates or launching an academy to meet your specific talent needs.

2017 Immersion Academy information is available at:
www.sans.org/cybertalent/immersion-academy
or email: immersionacademy@sans.org



Read the Pilot Program Results Report
Visit sans.org/vetsuccess



VetSuccess

SANS CyberTalent IMMERSION ACADEMY

SANS Intermediate and Specialized Skills

Management | Audit | Legal

Summary: Professional security managers need broad and proven knowledge of policy, standards and practices in order to provide the greatest level of security to their organizations. They also need to speak their technicians' language, and design security plans that withstand attack from all angles. SANS' specialized management, audit, and legal courses deliver the tools and techniques required to lead with confidence.

More than 10 advanced and specialized training options in this practice area are detailed on the following pages.

Who This Path Is for: CISOs, IT directors, or others with responsibility for managing their organization's security operations benefit from the experience-rich instruction in SANS management, audit, and legal courses. Security, system, and network administrators who are pursuing a CISSP® or a new management role should also prepare themselves for this type of training.

Why This Training Is Important: Professionals who train and certify in these skills are the leaders of cybersecurity. They master the specific techniques and tools needed to implement and audit the Critical Security Controls, they have a firm understanding of the eight domains of knowledge covered in the CISSP®, they can communicate information security best practices to executives and technical teams, and they are designing the security operation centers of the future.

Software Security | Industrial Control System Security

Specialists in software security or industrial control system security can find detailed information about four additional SANS courses available for SANSFIRE 2017 on pages 78 – 85.

SEC566

GCCC Certification
Critical Controls

www.giac.org/gccc

Implementing and Auditing the Critical Security Controls – In-Depth

Five-Day Program
Mon, July 24 - Fri, July 28
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: James Tarala

Who Should Attend

- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense personnel or contractors
- Staff and clients of federal agencies
- Private sector organizations looking to improve information assurance processes and secure their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance
- Alumni of SEC/AUD440, SEC401, SEC501, SANS Audit classes, and MGT512

Cybersecurity attacks are increasing and evolving so rapidly that it is more difficult than ever to prevent and defend against them. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches? This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS).

As threats evolve, an organization's security should too. To enable your organization to stay on top of this ever-changing threat scenario, SANS has designed a comprehensive course on how to implement the Critical Security Controls, a prioritized, risk-based approach to security. Designed by private and public sector experts from around the world, the Controls are the best way to block known attacks and mitigate damage from successful attacks. They have been adopted by the U.S. Department of Homeland Security, state governments, universities, and numerous private firms.

The Controls are specific guidelines that CISOs, CIOs, IGs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defenses. They are designed to complement existing standards, frameworks, and compliance schemes by prioritizing the most critical threat and highest payoff defenses, while providing a common baseline for action against risks that we all face.

The Controls are an effective security framework because they are based on actual attacks launched regularly against networks. Priority is given to Controls that (1) mitigate known attacks (2) address a wide variety of attacks, and (3) identify and stop attackers early in the compromise cycle. The British government's Center for the Protection of National Infrastructure describes the Controls as the "baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence."

SANS' in-depth, hands-on training will teach you how to master the specific techniques and tools needed to implement and audit the Critical Controls. It will help security practitioners understand not only how to stop a threat, but why the threat exists, and how to ensure that security measures deployed today will be effective against the next generation of threats.

The course shows security professionals how to implement the Controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the Controls are effectively implemented.

James Tarala *SANS Senior Instructor*

James Tarala is a principal consultant with Enclave Security and is based in Venice, Florida. He is a regular speaker for the SANS Institute as well as a courseware author and editor for many SANS auditing and security courses. As a consultant, he has spent the past few years developing large enterprise IT security and infrastructure architectures, specifically working with many Microsoft-based directory services, e-mail, terminal services, and wireless technologies. He has also spent a large amount of time consulting with organizations to assist them with their security management, operational practices, and regulatory compliance issues, and he often performs independent security audits and assists internal audit groups in developing their internal audit programs. James completed his undergraduate studies at Philadelphia Biblical University and his graduate work at the University of Maryland. He holds numerous professional certifications. **@isaudit**

566.1 HANDS ON: Introduction and Overview of the 20 Critical Controls

Day 1 will introduce you to all of the Critical Controls, laying the foundation for the rest of the class. For each Control, we will follow the same outline covering the following information:

- **Overview of the Control**
- **How It Is Compromised**
- **Defensive Goals**
- **Quick Wins**
- **Visibility & Attribution**
- **Configuration & Hygiene**
- **Advanced**
- **Overview of Evaluating the Control**
- **Core Evaluation Test(s)**
- **Testing/Reporting Metrics**
- **Steps for Root Cause Analysis of Failures**
- **Audit/Evaluation Methodologies**
- **Evaluation Tools**
- **Exercise to Illustrate Implementation or Steps for Auditing a Control**

In addition, Critical Controls 1 and 2 will be covered in depth.

Topics: **Critical Control 1: Inventory of Authorized and Unauthorized Devices**
Critical Control 2: Inventory of Authorized and Unauthorized Software

566.2 HANDS ON: Critical Controls 3, 4, 5, and 6

Topics: **Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers**
Critical Control 4: Continuous Vulnerability Assessment and Remediation
Critical Control 5: Controlled Use of Administrative Privileges
Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs

566.3 HANDS ON: Critical Controls 7, 8, 9, 10, and 11

Topics: **Critical Control 7: Email and Web Browser Protections**
Critical Control 8: Malware Defenses
Critical Control 9: Limitation and Control of Network Ports, Protocols, and Services
Critical Control 10: Data Recovery Capability (validated manually)
Critical Control 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

566.4 HANDS ON: Critical Controls 12, 13, 14, and 15

Topics: **Critical Control 12: Boundary Defense**
Critical Control 13: Data Protection
Critical Control 14: Controlled Access Based on the Need to Know
Critical Control 15: Wireless Device Control

566.5 HANDS ON: Critical Controls 16, 17, 18, 19, and 20

Topics: **Critical Control 16: Account Monitoring and Control**
Critical Control 17: Security Skills Assessment and Appropriate Training to Fill Gaps (validated manually)
Critical Control 18: Application Software Security
Critical Control 19: Incident Response and Management (validated manually)
Critical Control 20: Penetration Tests and Red Team Exercises (validated manually)

"The 20 controls presented in the course are requirements found in most regulated industries. I found the format and layout of each control well explained and easy to follow."

-Josh Ellis, Iberdrola USA

You Will Be Able To

- Apply a security framework based on actual threats that is measurable, scalable, and reliable in stopping known attacks and protecting organizations' important information and systems
- Understand the importance of each Control, how it is compromised if ignored, and explain the defensive goals that result in quick wins and increased visibility of networks and systems
- Identify and utilize tools that implement Controls through automation
- Learn how to create a scoring tool for measuring the effectiveness of each Control
- Employ specific metrics to establish a baseline and measure the effectiveness of the Controls
- Understand how the Critical Controls map to standards such as NIST 800-53, ISO 27002, the Australian Top 35, and more
- Audit each of the Critical Controls with specific, proven templates, checklists, and scripts provided to facilitate the audit process

"This is a must-do course if you are looking to steer your company through some hefty controls to security."

-Jeff Evenson, AgStar Financial Services

"Good instruction and clear content!"

-Roy Hall, NASBA

www.sans.edu

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

MGT512

GSLC Certification
Security Leadership

www.giac.org/gslc

SANS Security Leadership Essentials for Managers with Knowledge Compression™

Five-Day Program
Mon, July 24 - Fri, July 28
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop Recommended
Instructor: Ted Demopoulos

This course has extended hours

Who Should Attend

- All newly appointed information security officers
- Technically skilled administrators who have recently been given leadership responsibilities
- Seasoned managers who want to understand what your technical people are telling you

"MGT512 is one of the most valuable courses I've taken with SANS. It really did help bridge the gap from security practitioner to security orchestrator. Truly a gift!"
-John Madick, Epiq Systems, Inc.

This completely updated course is designed to empower advancing managers who want to get up to speed quickly on information security issues and terminology. You won't just learn about security, you will learn how to manage security. Lecture sections are intense; the most common student comment is that it's like drinking from a fire hose. The diligent manager will learn vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. Additionally, the course has been engineered to incorporate the NIST Special Publication 800 (series) guidance so that it can be particularly useful to U.S. government managers and supporting contractors.

Essential security topics covered in this management track include network fundamentals and applications, power, cooling and safety, architectural approaches to defense in depth, cyber attacks, vulnerability assessment and management, security policies, contingency and continuity planning, awareness management, risk management analysis, incident handling, web application security, and offensive and defensive information warfare, culminating with our management practicum. The material uses Knowledge Compression,™ special charts, and other proprietary SANS techniques to help convey the key points of critical slides and keep the information flow rate at a pace senior executives demand every teaching hour of the course. The course has been evaluated and approved by CompTIA's CAQC program for Security+ 2008 to ensure that managers and their direct reports have a common baseline for security terminology and concepts. You will be able to put what you learn into practice the day you get back into the office.

Knowledge Compression™

Maximize your learning potential!

Knowledge Compression™ is an optional add-on feature to a SANS class that aims to maximize the absorption and long-term retention of large amounts of data over a relatively short period of time. Through the use of specialized training materials, in-class reviews, examinations and test-taking instruction, Knowledge Compression™ ensures students have a solid understanding of the information presented to them. By attending classes that feature this advanced training product, you will experience some of the most intense and rewarding training programs SANS has to offer, in ways that you never thought possible!

Ted Demopoulos *SANS Principal Instructor*

Ted Demopoulos' first significant exposure to computers was in 1977 when he had unlimited access to his high school's PDP-11 and hacked at it incessantly. He consequently almost flunked out but learned he liked playing with computers a lot. His business pursuits began in college and have been continuous ever since. His background includes over 25 years of experience in information security and business, including 20+ years as an independent consultant. Ted helped start a successful information security company, was the CTO at a "textbook failure" of a software startup, and has advised several other businesses. Ted is a frequent speaker at conferences and other events, quoted often by the press. He also has written two books on social media, has an ongoing software concern in Austin, Texas in the virtualization space, and is the recipient of a Department of Defense Award of Excellence. In his spare time, he is a food and wine geek, enjoys flyfishing, and likes to play with his children. **@TedDemop**

512.1 Managing the Enterprise, Planning, Network, and Physical Plant

The course starts with a whirlwind tour of the information an effective IT security manager must know to function in today's environment. We will cover safety, physical security, and how networks and the related protocols like TCP/IP work, and equip you to review network designs for performance, security, vulnerability scanning, and return on investment. You will learn more about secure IT operations in a single day than you ever thought possible.

Topics: **Budget Awareness and Project Management; The Network Infrastructure; Computer and Network Addressing; IP Terminology and Concepts; Vulnerability Management; Managing Physical Safety, Security, and the Procurement Process**

512.2 IP Concepts, Attacks Against the Enterprise, and Defense-in-Depth

You will learn about information assurance foundations, which are presented in the context of both current and historical computer security threats, and how they have impacted confidentiality, integrity, and availability. You will also learn the methods of the attack and the importance of managing attack surface.

Topics: **Attacks Against the Enterprise; Defense in Depth; Managing Security Policy; Access Control and Password Management**

512.3 Secure Communications

This course section examines various cryptographic tools and technologies and how they can be used to secure a company's assets. A related area called steganography, or information hiding, is also covered. Learn how malware and viruses often employ cryptographic techniques in an attempt to evade detection. We will learn about managing privacy issues in communications and investigate web application security.

Topics: **Cryptography; Wireless Network Security; Steganography; Managing Privacy; Web Communications and Security; Operations Security, Defensive and Offensive Methods**

512.4 The Value of Information

On this day we consider the most valuable resource an organization has: its information. You will learn about intellectual property, incident handling, and how to identify and better protect the information that is the real value of your organization. We will then formally consider how to apply everything we have learned, as well as practice briefing management on our risk architecture.

Topics: **Managing Intellectual Property; Incident Handling Foundations; Information Warfare; Disaster Recovery/Contingency Planning; Managing Ethics; IT Risk Management**

512.5 Management Practicum

On the fifth and final day, we pull it all together and apply the technical knowledge to the art of management. The management practicum covers a number of specific applications and topics concerning information security. We'll explore proven techniques for successful and effective management, empowering you to immediately apply what you have learned your first day back at the office.

Topics: **The Mission; Globalization; IT Business and Program Growth; Security and Organizational Structure; Total Cost of Ownership; Negotiations; Fraud; Legal Liability; Technical People**

Security Leaders and Managers earn the highest salaries (well into six figures) in information security and are near the top of IT. Needless to say, to work at that compensation level, excellence is demanded. These days, security managers are expected to have domain expertise as well as the classic project management, risk assessment, and policy review and development skills.

You Will Be Able To

- Enable managers and auditors to speak the same language as system, security, and network administrators.
- Establish a minimum standard for IT management knowledge, skills, and abilities. I keep running into managers who don't know TCP/IP, and that is OK; but then they don't know how to calculate total cost of ownership (TCO), leaving me quietly wondering what they do know.
- Save the up-and-coming generation of senior and rapidly advancing managers a world of pain by sharing the things we wish someone had shared with us. As the saying goes, it is OK to make mistakes, just make new ones.

"This was a great course that I feel all management should take. It helps managers understand not only security but also technical and business concepts and issues."

-David Stewart, ADM

"This course is a great foundation for those involved in an organization's info security."

-Manuel M., U.S. Army

MGT414

GISP Certification
Information Security Professional

www.giac.org/gisp

SANS Training Program for CISSP® Certification

Six-Day Program
Mon, July 24 - Sat, July 29
9:00am - 7:00pm (Day 1)
8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6)
46 CPEs
Laptop NOT Needed
Instructor: David R. Miller

This course has evening Bootcamp Sessions

Who Should Attend

- Security professionals who are interested in understanding the concepts covered on the CISSP® exam as determined by $(ISC)^2$
- Managers who want to understand the critical areas of information security
- System, security, and network administrators who want to understand the pragmatic applications of the CISSP® eight domains
- Security professionals and managers looking for practical ways the eight domains of knowledge can be applied to their current job

SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that is specifically designed to prepare students to successfully pass the CISSP® exam.

MGT414 focuses solely on the eight domains of knowledge as determined by $(ISC)^2$ that form a critical part of the CISSP® exam. Each domain of knowledge is dissected into its critical components, and those components are then discussed in terms of their relationship with one another and with other areas of information security.

Obtaining Your CISSP® Certification Consists of:

- **Fulfilling minimum requirements for professional work experience**
- **Completing the Candidate Agreement**
- **Review of your résumé**
- **Passing the CISSP® 250 multiple-choice question exam with a scaled score of 700 points or greater**
- **Submitting a properly completed and executed Endorsement Form**
- **Periodic audit of CPEs to maintain the credential**

"Best security training I have ever received and just the right amount of detail for each domain."

-Tony Barnes, United States Sugar Corporation

"It was extremely valuable to have an experienced information security professional teaching the course as he was able to use experiential knowledge in examples and explanations."

-Sean Hoar, Davis Wright Tremaine

"I think the course material and the instructor are very relevant for the task of getting a CISSP. The overall academic exercise is solid."

-Aaron Lewter, Availity

David R. Miller *SANS Certified Instructor*

David has been a technical instructor since the early 1980s and has specialized in consulting, auditing, and lecturing on information systems security, legal and regulatory compliance, and network engineering. David has helped many enterprises develop their overall compliance and security program, including through policy writing, network architecture design including security zones, development of incident response teams and programs, design and implementation of public key infrastructures, security awareness training programs, specific security solution designs like secure remote access and strong authentication architectures, disaster recovery planning and business continuity planning, and pre-audit compliance gap analysis and remediation. He serves as a security lead and forensic investigator on numerous enterprise-wide IT design and implementation projects for Fortune 500 companies, providing compliance, security, technology, and architectural recommendations and guidance. Projects include Microsoft Windows Active Directory enterprise designs, security information and event management systems, intrusion detection and protection systems, endpoint protection systems, patch management systems, configuration monitoring systems, and enterprise data encryption for data at rest, in transit, in use, and within email systems. David is an author, lecturer and technical editor of books, curriculum, certification exams, and computer-based training videos. **@DRM_CyberDude**

414.1 Introduction; Security and Risk Management

On the first day of training for the CISSP® exam, MGT414 introduces the specific requirements needed to obtain certification. The exam update will be discussed in detail. We will cover the general security principles needed to understand the eight domains of knowledge, with specific examples for each domain. The first of the eight domains, Security and Risk Management, is discussed using real-world scenarios to illustrate the critical points.

Topics: Overview of CISSP® Certification; Introductory Material; Overview of the Eight Domains; Domain 1: Security and Risk Management

414.2 Asset Security and Security Engineering – PART 1

Understanding asset security is critical to building a solid information security program. The Asset Security domain, the initial focus of today's course section, describes data classification programs, including those used by both governments and the military as well as the private sector. We will also discuss ownership, covering owners ranging from business/mission owners to data and system owners. We will examine data retention and destruction in detail, including secure methods for purging data from electronic media. We then turn to the first part of the Security Engineering domain, including new topics for the 2016 exam such as the Internet of Things, Trusted Platform Modules, Cloud Security, and much more.

Topics: Domain 2: Asset Security; Domain 3: Security Engineering (Part 1)

414.3 Security Engineering – PART 2; Communication and Network Security

This section continues the discussion of the Security Engineering domain, including a deep dive into cryptography. The focus is on real-world implementation of core cryptographic concepts, including the three types of cryptography: symmetric, asymmetric, and hashing. Salts are discussed, as well as rainbow tables. We will round out Domain 3 with a look at physical security before turning to Domain 4, Communication and Network Security. The discussion will cover a range of protocols and technologies, from the Open Systems Interconnection (OSI) model to storage area networks.

Topics: Domain 3: Security Engineering (Part 2); Domain 4: Communication and Network Security

414.4 Identity and Access Management

Controlling access to data and systems is one of the primary objectives of information security. Domain 5, Identity and Access Management, strikes at the heart of access control by focusing on identification, authentication, and authorization of accounts. Password-based authentication represents a continued weakness, so Domain 5 stresses multi-factor authentication, biometrics, and secure credential management. The CISSP® exam underscores the increased role of external users and service providers, and mastery of Domain 5 requires an understanding of federated identity, SSO, SAML, and third-party identity and authorization services like Oauth and OpenID.

Topics: Domain 5: Identity and Access Management

414.5 Security Assessment and Testing; Security Operations

This course section covers Domain 6 (Security Assessment) and Domain 7 (Security Operations). Security Assessment covers types of security tests, testing strategies, and security processes. Security Operations covers investigatory issues, including eDiscovery, logging and monitoring, and provisioning. We will discuss cutting-edge technologies such as cloud, and we'll wrap up day five with a deep dive into disaster recovery.

Topics: Domain 6: Security Assessment; Domain 7: Security Operations

414.6 Software Development Security

Domain 8 (Software Development Security) describes the requirements for secure software. Security should be "baked in" as part of network design from day one, since it is always less effective when it is added later to a poor design. We will discuss classic development models, including waterfall and spiral methodologies. We will then turn to more modern models, including agile software development methodologies. New content for the CISSP® exam update will be discussed, including DevOps. We will wrap up this course section by discussing security vulnerabilities, secure coding strategies, and testing methodologies.

Topics: Domain 8: Software Development Security

You Will Be Able To

- Understand the eight domains of knowledge that are covered on the CISSP® exam
- Analyze questions on the exam and be able to select the correct answer
- Apply the knowledge and testing skills learned in class to pass the CISSP® exam
- Understand and explain all of the concepts covered in the eight domains of knowledge
- Apply the skills learned across the eight domains to solve security problems when you return to work

"This course has been fantastic in terms of boiling down years of IT security trends and best practices into a week of learning."

-Eric Pavlov, Innomark

"I feel prepared for my exam after taking this course."

-Tom DiNunzio, Exelon

MEETS DoDD 8140 (8570) REQUIREMENTS

www.sans.org/8140

BUNDLE ONDEMAND

WITH THIS COURSE

www.sans.org/ondemand

MGT514

IT Security Strategic Planning, Policy and Leadership

CERTIFICATION COMING SOON!

Five-Day Program
Mon, July 24 - Fri, July 28
9:00am - 5:00pm
30 CPEs
Laptop NOT Needed
Instructor: Frank Kim

Who Should Attend

- CISOs
- Information security officers
- Security directors
- Security managers
- Aspiring security leaders
- Other security personnel who have team lead or management responsibilities

"Excellent training with encyclopedic coverage of the topic."

-Alexander Kotkov, Ernst and Young

As security professionals we have seen the landscape change. Cybersecurity is now more vital and relevant to the growth of your organization than ever before. As a result, information security teams have more visibility, more budget, and more opportunity. However, with this increased responsibility comes more scrutiny.

This course teaches security professionals how to do three things:

Develop Strategic Plans
Strategic planning is hard for people in IT and IT security because we spend so much time responding and reacting. We almost never get to practice until we get promoted to a senior position and then we are not equipped with the skills we need to run with the pack. Learn how to develop strategic plans that resonate with other IT and business leaders.

Create Effective Information Security Policy
Policy is a manager's opportunity to express expectations for the workforce, set the boundaries of acceptable behavior, and empower people to do what they ought to be doing. It is easy to get wrong. Have you ever seen a policy and your response was, "No way, I am not going to do that"? Policy must be aligned with an organization's culture. We will break down the steps to policy development so that you have the ability to develop and assess policy to successfully guide your organization.

Develop Management and Leadership Skills
Leadership is a capability that must be learned, exercised and developed to better ensure organizational success. Strong leadership is brought about primarily through selfless devotion to the organization and staff, tireless effort in setting the example, and the vision to see and effectively use available resources toward the end goal. Effective leadership entails persuading team members to accomplish their objectives while removing obstacles and maintaining the well-being of the team in support of the organization's mission. Learn to utilize management tools and frameworks to better lead, inspire, and motivate your teams.

How the Course Works

Using case studies from Harvard Business School, team-based exercises, and discussions that put students in real-world scenarios, students will participate in activities that they can then carry out with their own team members when they return to work.

The next generation of security leadership must bridge the gap between security staff and senior leadership by strategically planning how to build and run effective security programs. After taking this course you will have the fundamental skills to create strategic plans that protect your company, enable key innovations, and work effectively with your business partners.

Frank Kim *SANS Certified Instructor*

As CISO at the SANS Institute, Frank leads the security risk function for the most trusted source of computer security training, certification, and research in the world. He also helps shape, develop, and support the next generation of security leaders by teaching, developing courseware, and leading the management and software security curricula. Prior to the SANS Institute, Frank was Executive Director of Cyber Security at Kaiser Permanente with responsibility for delivering innovative security solutions to meet the unique needs of the nation's largest not-for-profit health plan and integrated health care provider with annual revenue of $55 billion, 9.5 million members, and 175,000 employees. In recognition of his work, Frank was a two-time recipient of the CIO Achievement Award for business-enabling thought leadership. Frank holds degrees from the University of California at Berkeley and is the author of popular SANS courseware on strategic planning, leadership, and application security. **@fykim**

514.1 Strategic Planning Foundations

Creating strategic plans for security requires a fundamental understanding of the business and a deep understanding of the threat landscape.

Topics: **Vision & Mission Statements; Stakeholder Management; PEST Analysis; Porter's Five Forces; Threat Actors; Asset Analysis; Threat Analysis**

514.2 Strategic Roadmap Development

With a firm understanding of business drivers as well as the threats facing the organization, you will develop a plan to analyze the current situation, identify the target situation, perform gap analysis, and develop a prioritized roadmap. In other words, you will be able to determine (1) what you do today, (2) what you should be doing in the future, (3) what you don't do, and (4) what you should do first. With this plan in place you will learn how to build and execute your plan by developing a business case, defining metrics for success, and effectively marketing your security program.

Topics: **Historical Analysis; Values and Culture; SWOT Analysis; Vision and Innovation; Security Framework; Gap Analysis; Roadmap Development; Business Case Development; Metrics and Dashboards; Marketing and Executive Communications**

514.3 Security Policy Development and Assessment

Policy is one of the key tools that security leaders have to influence and guide the organization. Security managers must understand how to review, write, assess, and support security policy and procedure. Using an instructional delivery methodology that balances lecture, exercises, and in-class discussion, this course section will teach techniques to create successful policy that users will read and follow and business leaders will accept. Learn key elements of policy, including positive and negative tone, consistency of policy bullets, how to balance the level of specificity to the problem at hand, the role of policy, awareness and training, and the SMART approach to policy development and assessment.

Topics: **Purpose of Policy; Policy Gap Analysis; Policy Development; Policy Review; Awareness and Training**

514.4 Leadership and Management Competencies

Learn the critical skills you need to lead, motivate, and inspire your teams to achieve the goal. By establishing a minimum standard for the knowledge, skills, and abilities required to develop leadership you will understand how to motivate employees and develop from a manager into a leader.

Topics: **Leadership Building Blocks; Creating and Developing Teams; Coaching and Mentoring; Customer Service Focus; Conflict Resolution; Effective Communication; Leading Through Change; Relationship Building; Motivation and Self-Direction; Teamwork; Leadership Development**

514.5 Strategic Planning Workshop

Using the case study method, students will work through real-world scenarios by applying the skills and knowledge learned throughout the course. Case studies are taken directly from Harvard Business School, the pioneer of the case-study method, and focus specifically on information security management and leadership competencies. The Strategic Planning Workshop serves as a capstone exercise for the course, allowing students to synthesize and apply concepts, management tools, and methodologies learned in class.

Topics: **Creating a Security Plan for the CEO; Understanding Business Priorities; Enabling Business Innovation; Working with BYOD; Effective Communication; Stakeholder Management**

"This training was valuable because it helped me examine myself from an outside point of view."

-DJ, Zoetis

You Will Be Able To

- Develop security strategic plans that incorporate business and organizational drivers
- Develop and assess information security policy
- Use management and leadership techniques to motivate and inspire your teams

"As I progress in my career within cybersecurity, I find that courses such as MGT514 allow me to plan and lead organizations forward."

-Eric Burgan, Idaho National Labs

"Really good case studies and examples which prompted useful class discussion."

-Alexis Brownings, CERT-UK

"I moved into management a few years ago and am currently working on a new security strategy/roadmap and this class just condensed the past two months of my life into a one week course and I still learned a lot!"

-Travis Evans, SiriusXM

SANS Technology Institute

www.sans.edu

Bundle OnDemand

WITH THIS COURSE

www.sans.org/ondemand

MGT517

Managing Security Operations: Detection, Response, and Intelligence *NEW!*

Five-Day Program
Mon, July 24 - Fri, July 28
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Christopher Crowley

Who Should Attend

- Information security managers
- SOC managers, analysts, and engineers
- Information security architects
- IT managers
- Operations managers
- Risk management professionals
- IT/System administration/Network administration professionals
- IT auditors
- Business continuity and disaster recovery staff

"Chris is a fantastic instructor – great pacing with engaging anecdotes and was very insightful."

-Rich Savacool, Nixon Peabody

Managing Security Operations covers the design, operation, and ongoing growth of all facets of the security operations capabilities in an organization. An effective Security Operations Center (SOC) has many moving parts and must be designed with the ability to adjust and work within the constraints of the organization. To run a successful SOC, managers need to provide tactical and strategic direction and inform staff of the changing threat environment as well as provide guidance and training for employees. This course covers design, deployment, and operation of the security program to empower leadership through technical excellence.

The course covers the functional areas of Communications, Network Security Monitoring, Threat Intelligence, Incident Response, Forensics, and Self-Assessment. We discuss establishing Security Operations governance for:

- **Business alignment and ongoing adjustment of capabilities and objectives**
- **Designing the SOC and the associated objectives of functional areas**
- **Software and hardware technology required for performance of functions**
- **Knowledge, skills, and abilities of staff as well as staff hiring and training**
- **Execution of ongoing operations**

You will walk out of this course armed with a roadmap to design and operate an effective SOC tailored to the needs of your organization.

"SANS coursework is the most thorough learning available, anywhere. What you learn is not only conceptual, but also hands-on, showing you what to do, why you do it, and how you can apply solutions that you learn to real-world problems."

-Duane Tucker, Barmark Partners

Christopher Crowley *SANS Principal Instructor*

Christopher has 15 years of industry experience managing and securing networks. He currently works as an independent consultant in the Washington, DC area. His work experience includes penetration testing, computer network defense, incident response, and forensic analysis. He is the course author for SANS MGT535: Incident Response Team Management and holds the GSEC, GCIA, GCIH (gold), GCFA, GPEN, GREM, GMOB, and CISSP certifications. His teaching experience includes SEC401, SEC503, SEC504, SEC560, SEC575, SEC580, FOR585, and MGT535; Apache web server administration and configuration; and shell programming. He was awarded the SANS 2009 Local Mentor of the Year Award, which is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities. **@CCrowMontance**

517.1 HANDS ON: Design the Security Operations Center

We will focus on how to align and deploy a Security Operations Center (SOC). This day lays the foundational aspects of the SOC by discussing the functional areas that form the basis of the build and operate days that follow. The first issue to address is how the SOC will serve the business. To understand what is to be built, we explore the business drivers for SOCs. Each company has its own circumstances and needs, but there are common drivers for setting out to build a SOC. From business alignment, systems analysis performed shows all the things that need to be done. This is an elaborate and substantial effort to undertake. Knowing what components are available and how the pieces fit together is critical. This analysis will be followed with design and build on day 2.

Topics: SOC Fundamentals; SOC Components; Sizing and Scoping; SOC Program

517.2 HANDS ON: Build the Security Operations Center

Once a clear picture of what should be done to secure the organization is produced from analysis of what the needs are, and what resources are available, we set out to build the SOC. The build-out starts with an operating plan decided on by the key stakeholders from the organization. The interactions, inputs, outputs, and actions within each of the process components are identified. Each functional area needs specific hardware and software to accomplish each process, so alternatives are discussed for all of these. Open-source, inexpensive, and enterprise-level solutions are presented for each need. We will discuss the available solutions in-depth, and help focus the budget available on the necessary tools. The output of this day is on all the procurement necessary for building out a SOC.

Topics: Governance Structure; Process Engineering; Technical Components

517.3 HANDS ON: Operate and Mature the Security Operations Center

Designing and building-out a SOC are considered projects. Operation is an ongoing and perpetual effort. If the design of the system is insufficient or short-sighted, then operating the system will be difficult and inefficient. The overriding challenge of management is discussed in terms of organizational dimensions. The analytical processes of competing hypotheses, the kill chain, and the diamond model are discussed to provide a context for the analytical currency of the SOC. We will evaluate the staffing structure, how to hire, and how to keep those staff continually trained and updated. A schedule of meetings, specific metrics to report, and specific metrics to use to measure the relationship within the functional areas of the SOC are shown. Specific processes and the data relationships when performing the processes are discussed to depict the standard operating procedures that the SOC must carry out.

Topics: People and Processes; Measurements and Metrics; Process Development

517.4 HANDS ON: Incident Response Management – PART 1

Further detail on incident response is developed to show the operation of the SOC. Since the response component is the action of defense, the operation of the incident response team is addressed in great detail. An examination of cloud-based systems shows a special case of incident response. The preparation of response capability in the cloud is insufficient because the contractual negotiations of the service rarely address incident response adequately. We discuss appropriate preparation and response action within cloud services. User training and awareness is developed as a basis for corrective action when incident response is required.

Topics: The Cloud; Incident Response Process; Creating Incident Requirements; Training, Education, and Awareness

517.5 HANDS ON: Incident Response Management – PART 2

Continuing the operation of incident response, we discuss the staffing requirements in detail. Common caveats of incidence response operations are discussed, and table top exercises are developed to mitigate those caveats. Communication requirements are laid out and incident tracking methods are discussed. We also look at how to make the most out of a response and damage control task. Tools for estimating and tracking costs associated with incidents are demonstrated, and overall recommendations are presented on how to interface with law enforcement. The final topic addressed is the development of appropriate response techniques for APT-style actors, including strategies for quickly differentiating APT-style compromise using threat intelligence, sufficient scope identification, and eradication of the current wave of compromise.

Topics: Staffing Considerations; Setting Up Operations; Managing Daily Operations; Cost Considerations; Legal and Regulatory Issues; Advanced Threat Response

You Will Be Able To

- Design security operations to address all needed functions for the organization
- Select technologies needed to implement the functions for a SOC
- Maintain appropriate business alignment with the security capability and the organization
- Develop and streamline security operations processes
- Strengthen and deepen capabilities
- Collect data for metrics, report meaningful metrics to the business, and maintain internal SOC performance metrics
- Hire appropriate SOC staff and keep existing SOC staff up to date

Course Author Statement

"The inclusion of all functional areas of security operations is intended to develop a standardized program for an organization and express all necessary capabilities. Admittedly ambitious, the intention of this course is to provide a unified picture of coordination among teams with different skillsets to help the business prevent loss due to poor security practices. I have encountered detrimental compartmentalization in most organizations. There is a tendency for specialists to look at their piece of the problem, without understanding the larger scope of information security within an organization. Organizations are likely to perceive a SOC as a tool, and not as the unification of people, processes, and technologies. This course provides a comprehensive picture of what a Cyber Security Operations Center (CSOC or SOC) is. After attending this course, the participant will have a roadmap for what needs to be done in the organization seeking to implement security operations."
-Chris Crowley

MGT525

GCPM Certification
Project Manager

www.giac.org/gcpm

IT Project Management, Effective Communication, and PMP® Exam Prep

Six-Day Program
Mon, July 24 - Sat, July 29
9:00am - 5:00pm
36 CPEs
Laptop NOT Needed
Instructor: Jeff Frisk

Who Should Attend

- Individuals interested in preparing for the Project Management Professional (PMP)® Exam
- Security professionals who are interested in understanding the concepts of IT project management
- Managers who want to understand the critical areas of making projects successful
- Individuals working with time, cost, quality, and risk-sensitive projects and applications
- Anyone who would like to utilize effective communication techniques and proven methods to relate better to people
- Anyone in a key or lead engineering/ design position who works regularly with project management staff

This course is offered by the SANS Institute as a PMI® Registered Education Provider (R.E.P.). R.E.P.s provide the training necessary to earn and maintain the Project Management Professional (PMP)® and other professional credentials. PMP® is a registered trademark of Project Management Institute, Inc.

This course has been recently updated to fully prepare you for the 2017 PMP® exam changes. During this class you will learn how to improve your project planning methodology and project task scheduling to get the most out of your critical IT resources. We will utilize project case studies that highlight information technology services as deliverables. MGT525 follows the basic project management structure from the *PMBOK® Guide – Fifth Edition* and also provides specific techniques for success with information assurance initiatives. Throughout the week, we will cover all aspects of IT project management from initiating and planning projects through managing cost, time, and quality while your project is active, and to completing, closing, and documenting as your project finishes. A copy of the *PMBOK® Guide – Fifth Edition* is provided to all participants. You can reference the *PMBOK® Guide* and use your course material along with the knowledge you gain in class to prepare for the 2017 updated Project Management Professional (PMP)® Exam and the GIAC Certified Project Manager Exam.

"Honestly, this is one of the best courses I have had to date. I feel like I have thousands of things to take back to my job."

-Ryan Spencer, Reed Elsevier Inc.

The project management process is broken down into core process groups that can be applied across multiple areas of any project, in any industry. Although our primary focus is the application to the InfoSec industry, our approach is transferable to any projects that create and maintain services as well as general product development. We cover in-depth how cost, time, quality, and risks affect the services we provide to others. We will also address practical human resource management as well as effective communication and conflict resolution. You will learn specific tools to bridge the communications gap between managers and technical staff.

Jeff Frisk *SANS Certified Instructor*

Jeff Frisk currently serves as the director of the GIAC certification program and is a member of the SANS Technology Institute Curriculum Committee. Jeff is a PMP® credential holder and a GIAC GSEC credential holder. He also is the course author for MGT525. He has worked on many projects for SANS and GIAC, including courseware, certification, and exam development. Jeff has an engineering degree from the Rochester Institute of Technology and more than 15 years of IT project management experience with computer systems, high-tech consumer products, and business development initiatives. Jeff has held various positions including managing operations, product development, and electronic systems/computer engineering. He has many years of international and high-tech business experience working with both big and small companies to develop computer hardware/software products and services.

525.1 Project Management Structure and Framework

This course offers insight and specific techniques that both beginner and experienced project managers can utilize. The structure and framework section lays out the basic architecture and organization of project management. We will cover the common project management group processes, the difference between projects and operations, project life cycles, and managing project stakeholders.

Topics: Definition of Terms and Process Concepts; Group Processes; Project Life Cycle; Types of Organizations; PDCA Cycle

525.2 Project Charter and Scope Management

During day two, we will go over techniques used to develop the project charter and formally initiate a project. The scope portion defines the important input parameters of project management and gives you the tools to ensure that your project is well defined from the outset. We cover tools and techniques that will help you define your project's deliverables and develop milestones to gauge performance and manage change requests.

Topics: Formally Initiating Projects; Project Charters; Project Scope Development; Work Breakdown Structures; Scope Verification and Control

525.3 Time and Cost Management

Our third day details the time and cost aspects of managing a project. We will cover the importance of correctly defining project activities, project activity sequence, and resource constraints. We will use milestones to set project timelines and task dependencies along with learning methods of resource allocation and scheduling. We introduce the difference between resource and product-related costs and go into detail on estimating, budgeting, and controlling costs. You will learn techniques for estimating project cost and rates as well as budgeting and the process for developing a project cost baseline.

Topics: Process Flow; Task Lead and Lag Dependencies; Resource Breakdown Structures; Task Duration Estimating; Critical Path Scheduling; Cost Estimating Tools; Cost vs. Quality; Cost Baselining; Earned Value Analysis and Forecasting

525.4 Communications and Human Resources

During day four, we move into human resource management and building effective communications skills. People are the most valuable asset of any project and we cover methods for identifying, acquiring, developing and managing your project team. Performance appraisal tools are offered as well as conflict management techniques. You will learn management methods to help keep people motivated and provide great leadership. The effective communication portion of the day covers identifying and developing key interpersonal skills. We cover organizational communication and the different levels of communication as well as common communication barriers and tools to overcome these barriers.

Topics: Acquiring and Developing Your Project Team; Organizational Dependencies and Charts; Roles and Responsibilities; Team Building; Conflict Management; Interpersonal Communication Skills; Communication Models and Effective Listening

525.5 Quality and Risk Management

On day five you will become familiar with quality planning, assurance, and control methodologies as well as learning the cost-of-quality concept and its parameters. We define quality metrics and cover tools for establishing and benchmarking quality control programs. We go into quality assurance and auditing as well as how to understand and use quality control charts. The risk section goes over known versus unknown risks and how to identify, assess, and categorize risk. We use quantitative risk analysis and modeling techniques so that you can fully understand how specific risks affect your project. You will learn ways to plan for and mitigate risk by reducing your exposure as well as how to take advantage of risks that could have a positive effect on your project.

Topics: Cost of Quality; Quality Metrics; Continual Process Improvement; Quality Baselines; Quality Control; Change Control; Risk Identification; Risk Assessment; Time and Cost Risks; Risk Probability and Impact Matrices; Risk Modeling and Response

525.6 Procurement, Stakeholder Management, and Project Integration

We close out the week with the procurement aspects of project and stakeholder management, and then integrate all of the concepts presented into a solid, broad-reaching approach. We cover different types of contracts and then the make-versus-buy decision process. We go over ways to initiate strong requests for quotations (RFQ) and develop evaluation criteria, then qualify and select the best partners for your project. Stakeholder communication and management strategies are reinforced. The final session integrates everything we have learned by bringing all the topics together with the common process groups. Using a detailed project management methodology, we learn how to finalize the project management plan and then execute and monitor the progress of your project to ensure success.

Topics: Contract Types; Make vs. Buy Analysis; Vendor Weighting Systems; Contract Negotiations; Stakeholder Communication and Stakeholder Management Strategies; Project Execution; Monitoring Your Project's Progress; Finalizing Deliverables; Forecasting and Integrated Change Control

You Will Be Able To

- Recognize the top failure mechanisms related to IT and InfoSec projects, so that your projects can avoid common pitfalls
- Create a project charter that defines the project sponsor and stakeholder involvement
- Document project requirements and create a requirements traceability matrix to track changes throughout the project lifecycle
- Clearly define the scope of a project in terms of cost, schedule and technical deliverables
- Create a work breakdown structure defining work packages, project deliverables and acceptance criteria
- Develop a detailed project schedule, including critical path tasks and milestones
- Develop a detailed project budget including cost baselines and tracking mechanisms
- Develop planned and earned value metrics for your project deliverables and automate reporting functions
- Effectively manage conflict situations and build communication skills with your project team
- Document project risks in terms of probability and impact, and assign triggers and risk response responsibilities
- Create project earned value baselines and project schedule and cost forecasts

"Over my 11-year relationship with SANS, they have continued to deliver the most complete education of any company across the board. This class is no exception."

-Murdoch, GSE #99, Wellpoint

SANS Technology Institute

www.sans.edu

PMI Registered Education Provider — Project Management Institute

AUD507

GSNA Certification
Systems and Network Auditor

www.giac.org/gsna

Auditing & Monitoring Networks, Perimeters, and Systems

Six-Day Program
Mon, July 24 - Sat, July 29
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Clay Risenhoover

Who Should Attend

- Auditors seeking to identify key controls in IT systems
- Audit professionals looking for technical details on auditing
- Managers responsible for overseeing the work of an audit or security team
- Security professionals newly tasked with audit responsibilities
- System and network administrators looking to better understand what an auditor is trying to achieve, how auditors think, and how to better prepare for an audit
- System and network administrators seeking to create strong change control management and detection systems for the enterprise

"The entire course has been fantastic – it far exceeded my expectations. I think SANS training is far superior to other training programs."

-Paul Petrasko, Bemis Company

One of the most significant obstacles facing many auditors today is how exactly to go about auditing the security of an enterprise. What systems really matter? How should the firewall and routers be configured? What settings should be checked on the various systems under scrutiny? Is there a set of processes that can be put into place to allow an auditor to focus on the business processes rather than the security settings? How do we turn this into a continuous monitoring process? All of these questions and more will be answered by the material covered in this course.

This course is specifically organized to provide a risk-driven method for tackling the enormous task of designing an enterprise security validation program. After covering a variety of high-level audit issues and general audit best practices, the students will have the opportunity to dive deep into the technical how-to for determining the key controls that can be used to provide a level of assurance to an organization. Tips on how to repeatedly verify these controls and techniques for automatic compliance validation are taken from real-world examples.

One of the struggles that IT auditors face today is helping management understand the relationship between the technical controls and the risks to the business that these controls address. In this course these threats and vulnerabilities are explained based on validated information from real-world situations. The instructor will take the time to explain how this can be used to raise the awareness of management and others within the organization to build an understanding of why these controls specifically and auditing in general are important. From these threats and vulnerabilities, we will explain how to build the ongoing compliance monitoring systems and automatically validate defenses through instrumentation and automation of audit checklists.

You'll be able to use what you learn immediately. Five of the six days in the course will either produce or provide you directly with a general checklist that can be customized for your audit practice. Each of these days includes hands-on exercises with a variety of tools discussed during the lecture sections so that you will leave knowing how to verify each and every control described in the class. Each of the five hands-on days gives you the chance to perform a thorough technical audit of the technology being considered by applying the checklists provided in class to sample audit problems in a virtualized environment. Students are invited to bring a Windows XP Professional or higher laptop for use during class. Macintosh computers running OS X may also be used with VMWare Fusion.

A great audit is more than marks on a checklist; it is the understanding of what the underlying controls are, what the best practices are, and why. Sign up for this course and gain the mix of theoretical, hands-on, and practical knowledge to conduct a great audit.

Clay Risenhoover *SANS Certified Instructor*

Clay is the president of Risenhoover Consulting, Inc., an IT management consulting firm based in Durant, Oklahoma. Founded in 2003, RCI provides IT audit and IT management consulting services to clients in multiple sectors. Clay's past experience includes positions in software development, technical training, LAN and WAN operations, and IT management in both the private and public sector. He has a master's degree in computer science and holds a number of technical and security certifications, including GPEN, GSNA, CISA, CISM, GWEB, and CISSP. **@AuditClay**

507.1 Effective Auditing, Risk Assessment, and Reporting

After laying the foundation for the role and function of an auditor in the information security field, this day's material will give you two extremely useful risk assessment methods that are particularly effective for measuring the security of enterprise systems, identifying control gaps and risks, and gaining the knowledge to be able to recommend additional compensating controls to address the risk. Nearly a third of the day is spent covering important audit considerations and questions dealing with virtualization and cloud computing.

Topics: Auditor's Role in Relation to Policy Creation, Policy Conformance, and Incident Handling; Basic Auditing and Assessing Strategies; Risk Assessment; The Six-Step Audit Process; Virtualization and Cloud Computing

507.2 Effective Network and Perimeter Auditing/Monitoring

On this day we will build from the ground up dealing with security controls, proper deployment, and effective auditing/continuous monitoring of configuration from Layer 2 all the way up the stack. Students will learn how to identify insecurely configured VLANs, determine perimeter firewall requirements, examine enterprise routers, and much more.

Topics: Secure Layer 2 Configurations; Router and Switch Configuration Security; Firewall Auditing, Validation, and Monitoring; Wireless; Network Population Monitoring; Vulnerability Scanning

507.3 Web Application Auditing

Web applications have consistently been rated for the past several years as one of the top five vulnerabilities that enterprises face. Unlike the other top vulnerabilities, however, enterprises continue to accept this risk, since most modern corporations need an effective web presence to do business today. One of the most important lessons that we are learning as an industry is that installing an application firewall is not enough!

Topics: Identifying Controls Against Information Gathering Attacks; Processing Controls to Prevent Hidden Information Disclosures; Control Validation of the User Sign-on Process; Examining Controls Against User Name Harvesting; Validating Protections Against Password Harvesting; Best Practices for OS and Web Server Configuration; How to Verify Session Tracking and Management Controls; Identification of Controls to Handle Unexpected User Input; Server-side Techniques for Protecting Your Customers and Their Sensitive Data

507.4 Advanced Windows Auditing and Monitoring

Microsoft's business-class system makes up a large part of the typical IT infrastructure. Quite often, these systems are also the most difficult to effectively secure and control because of the enormous number of controls and settings within the operating system. This course day will provide you with the techniques and tools to build an effective long-term audit program for your Microsoft Windows environment. More importantly, during the course a continuous monitoring and reporting system is built out, allowing you to easily and effectively scale the testing discussed within your enterprise when you return home.

Topics: Progressive Construction of a Comprehensive Audit Program; Automating the Audit Process; Windows Security Tips and Tricks; Maintaining a Secure Enterprise

507.5 Advanced Unix Auditing and Monitoring

Students will gain a deeper understanding of the inner workings and fundamentals of the Unix operating system as applied to the major Unix environments in use in business today. Students will have the opportunity to explore, assess and audit Unix systems hands-on. Lectures describe the different audit controls that are available on standard Unix systems, as well as access controls and security models.

Topics: Auditing to Create a Secure Configuration; Auditing to Maintain a Secure Configuration; Auditing to Determine What Went Wrong

507.6 Audit the Flag: A NetWars Experience

This final day of the course presents a capstone experience with additional learning opportunities. Leveraging the well-known NetWars engine, students have the opportunity to connect to a simulated enterprise network environment. Building on the tools and techniques learned throughout the week, each student is challenged to answer a series of questions about the enterprise network, working through various technologies explored during the course.

Topics: Network Devices; Servers; Applications; Workstations

You Will Be Able To

- Understand the different types of controls (e.g., technical vs. non-technical) essential to perform a successful audit
- Conduct a proper risk assessment of a network to identify vulnerabilities and prioritize what will be audited
- Establish a well-secured baseline for computers and networks, constituting a standard against which one can conduct audits
- Perform a network and perimeter audit using a seven-step process
- Audit firewalls to validate that rules/settings are working as designed, blocking traffic as required
- Utilize vulnerability assessment tools effectively to provide management with the continuous remediation information necessary to make informed decisions about risk and resources
- Audit web application configuration, authentication, and session management to identify vulnerabilities attackers can exploit
- Utilize scripting to build a system to baseline and automatically audit Active Directory and all systems in a Windows domain

"AUD507 not only prepares you to perform a comprehensive audit but also provides excellent information to operations for an improved network security posture."

-Rifat I., State Dept FCU

LEG523

GLEG Certification
Law of Data Security & Investigations

www.giac.org/gleg

Law of Data Security and Investigations

Five-Day Program
Mon, July 24 - Fri, July 28
9:00am - 5:00pm
30 CPEs
Laptop NOT Needed
Instructor: Benjamin Wright

Who Should Attend

- Investigators
- Security and IT professionals
- Lawyers
- Paralegals
- Auditors
- Accountants
- Technology managers
- Vendors
- Compliance officers
- Law enforcement
- Privacy officers
- Penetration testers

"Outstanding instructor! Keep doing what you are doing."

-Paul Mobley, FIS Global

NEW!

- **EU's new General Data Protection Regulation and its impact around the world.**
- **The impact of the Trump presidency and Brexit on data security law and regulatory enforcement.**
- **The EU's adoption of "Privacy Shield" to replace "Privacy Safe Harbor" for transferring data to the United States.**
- **Cyber insurer's lawsuit against hospital to deny coverage after data breach and $4.1 million legal settlement with patients.**

New law on privacy, e-discovery and data security is creating an urgent need for professionals who can bridge the gap between the legal department and the IT department. SANS LEG523 provides this unique professional training, including skills in the analysis and use of contracts, policies and records management procedures.

This course covers the law of fraud, crime, policy, contracts, liability, IT security and active defense – all with a focus on electronically stored and transmitted records. It also teaches investigators how to prepare credible, defensible reports, whether for cyber crimes, forensics, incident response, human resource issues or other investigations.

"I have gained many valuable ideas and tools to support and defend my organization and to strengthen security overall. I wish I'd taken LEG523 three or four years ago."

-Tom S., Case Western Reserve University

Each successive day of this five-day course builds upon lessons from the earlier days in order to comprehensively strengthen your ability to help your enterprise (public or private sector) cope with illegal hackers, botnets, malware, phishing, unruly vendors, data leakage, industrial spies, rogue or uncooperative employees, or bad publicity connected with IT security.

Recent updates to the course address hot topics such as legal tips on confiscating and interrogating mobile devices, the retention of business records connected with cloud computing and social networks like Facebook and Twitter, and analysis and response to the risks and opportunities surrounding open-source intelligence gathering.

Over the years this course has adopted an increasingly global perspective. Non-U.S. professionals attend LEG523 because there is no training like it anywhere else in the world. For example, a lawyer from the national tax authority in an African country took the course because electronic filings, evidence and investigations have become so important to her work. International students help the instructor, U.S. attorney Benjamin Wright, constantly revise the course and include more content that crosses borders.

Benjamin Wright *SANS Senior Instructor*

Benjamin Wright is the author of several technology law books, including *Business Law and Computer Security*, published by the SANS Institute. With 26 years in private law practice, he has advised many organizations, large and small, on privacy, e-commerce, computer security, and e-mail discovery and has been quoted in publications around the globe, from the *Wall Street Journal* to the *Sydney Morning Herald*. He is known for spotting and evaluating trends, such as the rise of whistleblowers wielding small video cameras. In 2010, Russian banking authorities tapped him for experience and advice on the law of cyber investigations and electronic payments. **@benjaminwright**

523.1 Fundamentals of IT Security Law and Policy

The first day is an introduction to law and IT that serves as the foundation for discussions during the rest of the course. We survey the general legal issues that must be addressed in establishing best information security practices, then canvass the many new laws on data security and evaluate information security as a field of growing legal liability. We will cover computer crime and intellectual property laws when a network is compromised, as well as emerging topics such as honeypots and active defenses, i.e., enterprises hacking back against illegal hackers. We will look at the impact of future technologies on law and investigations in order to help students factor in legal concerns when they draft enterprise IT security policies. For example, students will debate what the words of an enterprise policy would mean in a courtroom. The course also dives deep into the legal question of what constitutes a "breach of data security" for purposes of notifying others about it or for other purposes. The course includes a case study on the drafting of policy to comply with the Payment Card Industry Data Security Standard (PCI).

523.2 E-Records, E-Discovery, and Business Law

IT professionals can advance their careers by upgrading their expertise in the hot fields of e-discovery and cyber investigations. Critical facets of those fields come forward in course day two. We will focus on the use of computer records in disputes and litigation, with a view to teaching students how to manage requests to turn over e-records to adversaries (i.e., e-discovery), manage implementation of a "legal hold" over some records to prevent their destruction, and coordinate with legal counsel to develop workable strategies to legal challenges. The course is chock full of actual court case studies dealing with privacy, computer records, digital evidence, electronic contracts, regulatory investigations, and liability for shortfalls in security. The purpose of the case studies is to draw practical lessons that students can take back to their jobs.

523.3 Contracting for Data Security and Other Technology

Day three focuses on the essentials of contract law sensitive to the current legislative requirements for security. Compliance with many of the new data security laws requires contracts. Because IT pulls together the products and services of many vendors, consultants, and outsourcers, enterprises need appropriate contracts to comply with Sarbanes-Oxley, Gramm-Leach-Bliley, the Health Insurance Portability and Accountability Act, EU Data Directive, data breach notice laws and other regulations. Contracts covered include agreements for software, consulting, nondisclosure, application services, pen testing, and private investigation services. Special emphasis is given to cloud computing issues. Students will also learn how to exploit the surprising power of informal contract records and communications.

523.4 The Law of IT Compliance: How to Conduct Investigations

Information security professionals and cyber investigators operate in a world of ambiguity, rapid change, and legal uncertainty. To address these challenges, this course day presents methods to analyze a situation and then act in a way that is ethical and defensible and reduces risk. Lessons will be invaluable to the effective and credible execution of any kind of investigation, be it internal, government, consultant-related, a security incident, or any other. The lessons also include methods and justifications for maintaining the confidentiality of an investigation. Scattered through the course are numerous descriptions of actual fraud cases involving IT. The purpose is to acquaint the student with the range of modern business crimes, whether committed by executives, employees, suppliers or whole companies. More importantly, the course draws on the law of fraud and corporate misconduct to teach larger and broader lessons about legal compliance, ethical hacking and proper professional conduct in difficult case scenarios. Further, the course teaches how to conduct forensics investigations involving social, mobile and other electronic media.

523.5 Applying Law to Emerging Dangers: Cyber Defense

Knowing some rules of law is not the same as knowing how to deal strategically with real-world legal problems. This day is organized around extended case studies in security law: break-ins, investigations, piracy, extortion, rootkits, phishing, botnets, espionage and defamation. The studies lay out the chronology of events and critique what the good guys did right and what they did wrong. The goal is to learn to apply principles and skills to address incidents in your day-to-day work. The course includes an in-depth review of legal responses to the major security breaches at TJX, Target, and Home Depot, and looks at how to develop a Bring Your Own Device (BYOD) policy for an enterprise and its employees. LEG523 is increasingly global in its coverage, so although this course day centers around U.S. law, non-U.S. law and the roles of government authorities outside the United States will also be examined. At the end of this course section, the instructor will discuss a few sample questions to help students prepare for the GIAC exam associated with this course (GLEG).

You Will Be Able To

- Work better with other professionals at your organization who make decisions about the law of data security and investigations
- Exercise better judgment on how to comply with technology regulations, both in the United States and in other countries
- Evaluate the role and meaning of contracts for technology, including services, software and outsourcing
- Help your organization better explain its conduct to the public and to legal authorities
- Anticipate technology law risks before they get out of control
- Implement practical steps to cope with technology law risk
- Better explain to executives what your organization should do to comply with information security and privacy law
- Better evaluate technologies, such as digital signatures, to comply with the law and serve as evidence
- Make better use of electronic contracting techniques to get the best terms and conditions
- Exercise critical thinking to understand the practical implications of technology laws and industry standards (such as the Payment Card Industry Data Security Standard)

"This course changed the way I think about legal issues in the workplace and at home."

-Jon Mark Allen, Gamestop

SANS Technology Institute

www.sans.edu

Bundle OnDemand

with this course

www.sans.org/ondemand

DEV522

GWEB Certification
Web Application Defender

www.giac.org/gweb

Defending Web Applications Security Essentials

Six-Day Program
Mon, July 24 - Sat, July 29
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jason Lam

Who Should Attend

- Application developers
- Application security analysts or managers
- Application architects
- Penetration testers who are interested in learning about defensive strategies
- Security professionals who are interested in learning about web application security
- Auditors who need to understand defensive mechanisms in web applications
- Employees of PCI compliant organizations who need to be trained to comply with PCI requirements

"DEV522 goes over security issues that every web developer and appsec employee needs."

-Allen Ott, Boeing

This is the course to take if you have to defend web applications!

The quantity and importance of data entrusted to web applications is growing, and defenders need to learn how to secure them. Traditional network defenses, such as firewalls, fail to secure web applications. DEV522 covers the OWASP Top 10 Risks and will help you better understand web application vulnerabilities, thus enabling you to properly defend your organization's web assets.

Mitigation strategies from an infrastructure, architecture, and coding perspective will be discussed alongside real-world applications that have been proven to work. The testing aspect of vulnerabilities will also be covered so that you can ensure your application is tested for the vulnerabilities discussed in class.

To maximize the benefit for a wider range of audiences, the discussions in this course will be programming language agnostic. Focus will be maintained on security strategies rather than coding-level implementation.

DEV522: Defending Web Applications Security Essentials is intended for anyone tasked with implementing, managing, or protecting web applications. It is particularly well suited to application security analysts, developers, application architects, pen testers, auditors who are interested in recommending proper mitigations for web security issues, and infrastructure security professionals who have an interest in better defending their web applications.

The course will also cover additional issues the authors have found to be important in their day-to-day web application development practices. The topics that will be covered include:

- **Infrastructure security**
- **Server configuration**
- **Authentication mechanisms**
- **Application language configuration**
- **Application coding errors like SQL injection and cross-site scripting**
- **Cross-site request forging**
- **Authentication bypass**
- **Web services and related flaws**
- **Web 2.0 and its use of web services**
- **XPATH and XQUERY languages and injection**
- **Business logic flaws**
- **Protective HTTP headers**

The course will make heavy use of hands-on exercises and conclude with a large defensive exercise that reinforces the lessons learned throughout the week.

Jason Lam *SANS Certified Instructor*

Jason is accountable for cybersecurity at a large global financial company. He has over 15 years of experience in the information security industry progressing from hands-on research work to securing large-scale enterprise environments. His recent SANS Institute courseware development includes DEV522: Defending Web Application Security Essentials and SEC542: Web App Penetration Testing and Ethical Hacking. Jason started out as a programmer before moving on to an ISP as a network administrator. Handling security incidents for this ISP sparked his interest in information security. Over the years, Jason has performed and led intrusion detection, penetration testing, defense improvement programs and incident response in large enterprise environments. Recently, Jason has specialized in building large-scale security operations teams to handle the full cycle of threat identification, response and remediation, in parallel with his passion for directing enterprise web application security programs. **@jasonlam_sec**

522.1 HANDS ON: Web Basics and Authentication Security

We begin day one with an overview of recent web application attack and security trends, then follow up by examining the essential technologies that are at play in web applications. You cannot win the battle if you do not understand what you are trying to defend. We arm you with the right information so you can understand how web applications work and the security concepts related to them.

Topics: HTTP Basics; Overview of Web Technologies; Web Application Architecture; Recent Attack Trends; Authentication Vulnerabilities and Defense; Authorization Vulnerabilities and Defense

522.2 HANDS ON: Web Application Common Vulnerabilities and Mitigations

Since the Internet does not guarantee the secrecy of information being transferred, encryption is commonly used to protect the integrity and secrecy of information on the web. This course day covers the security of data in transit or on disk and how encryption can help with securing that information in the context of web application security.

Topics: SSL Vulnerabilities and Testing; Proper Encryption Use in Web Application; Session Vulnerabilities and Testing; Cross-site Request Forgery; Business Logic Flaws; Concurrency; Input-related Flaws and Related Defenses; SQL Injection Vulnerabilities, Testing, and Defense

522.3 HANDS ON: Proactive Defense and Operation Security

Day three begins with a detailed discussion on cross-site scripting and related mitigation and testing strategies, as well as HTTP response splitting. The code in an application may be totally locked down, but if the server setting is insecure, the server running the application can be easily compromised. Locking down the web environment is essential, so we cover this basic concept of defending the platform and host. To enable any detection of intrusion, logging and error handling must be done correctly. We will discuss the correct approach to handling incidents and logs, then dive even further to cover the intrusion detection aspect of web application security. In the afternoon we turn our focus to the proactive defense mechanism so that we are ahead of the bad guys in the game of hack and defend.

Topics: Cross-site Scripting Vulnerability and Defenses; Web Environment Configuration Security; Intrusion Detection in Web Applications; Incident Handling; Honeytoken

522.4 HANDS ON: AJAX and Web Services Security

Day four is dedicated to the security of asynchronous JavaScript and XML (AJAX) and web services, which are currently the most active areas in web application development. Security issues continue to arise as organizations dive head first into insecurely implementing new web technologies without first understanding them. We will cover security issues, mitigation strategies, and general best practices for implementing AJAX and web services. We will also examine real-world attacks and trends to give you a better understanding of exactly what you are protecting against. Discussion focuses on the web services in the morning and AJAX technologies in the afternoon.

Topics: Web Services Overview; Security in Parsing of XML; XML Security; AJAX Technologies Overview; AJAX Attack Trends and Common Attacks; AJAX Defense

522.5 HANDS ON: Cutting-Edge Web Security

Day five focuses on cutting-edge web application technologies and current research areas. Topics such as clickjacking and DNS rebinding are covered. These vulnerabilities are difficult to defend and multiple defense strategies are needed for their defense to be successful. Another topic of discussion is the new generation of single-sign-on solutions such as OpenID. We cover the implications of using these authentication systems and the common "gotchas" to avoid. With the Web2.0 adoption, the use of Java applet, Flash, ActiveX, and Silverlight are on the increase. The security strategies of defending these technologies are discussed so that these client-side technologies can be locked down properly.

Topics: Clickjacking; DNS Rebinding; Flash Security; Java Applet Security; Single-Sign-On Solution and Security; IPv6 Impact on Web Security

522.6 HANDS ON: Capture and Defend the Flag Exercise

Day six starts with an introduction to the secure software development life cycle and how to apply it to web development. But the focus is a large lab that will tie together the lessons learned during the week and reinforce them with hands-on applications. Students will be provided with a virtual machine to implement a complete database-driven dynamic website. In addition, they will use a custom tool to enumerate security vulnerabilities and simulate a vulnerability assessment of the website. Students will then have to decide which vulnerabilities are real and which are false positives, and then mitigate the vulnerabilities. The scanner will score the student as vulnerabilities are eliminated or checked off as false positives. Advanced students will be able to extend this exercise and find vulnerabilities not presented by the scanner. Students will learn through these hands-on exercises how to secure the web application, starting with the operating system, the web server, finding configuration problems in the application language setup, and finding and fixing coding problems in the site.

Topics: Mitigation of Server Configuration Errors; Discovering and Mitigating Coding Problems; Testing Business Logic Issues and Fixing Problems; Web Services Testing and Security Problem Mitigation

You Will Be Able To

- Understand the major risks and common vulnerabilities related to web applications through real-world examples
- Mitigate common security vulnerabilities in web applications using proper coding techniques, software components, configurations, and defensive architecture
- Understand the best practices in various domains of web application security such as authentication, access control, and input validation
- Fulfill the training requirement as stated in PCI DSS 6.5
- Deploy and consume web services (SOAP and REST) in a more secure fashion
- Proactively deploy cutting-edge defensive mechanisms such as the defensive HTTP response headers and Content Security Policy to improve the security of web applications
- Strategically roll out a web application security program in a large environment
- Incorporate advanced web technologies such as HTML5 and AJAX cross-domain requests into applications in a safe and secure manner
- Develop strategies to assess the security posture of multiple web applications

"The class helped me realize the importance of securing web app and applying secure coding rules for development efforts."

-Lerma Winchell, VyStar Credit Union

SANS Technology Institute

www.sans.edu

Bundle OnDemand

WITH THIS COURSE

www.sans.org/ondemand

DEV541

GSSP-JAVA Certification
Secure Software Programmer – Java

www.giac.org/gssp-java

Secure Coding in Java/JEE: Developing Defensible Applications

Four-Day Program
Mon, July 24 - Thu, July 27
9:00am - 5:00pm
24 CPEs
Laptop Required
Instructor: Gregory Leonard

Who Should Attend

- Developers who want to build more secure applications
- Java Enterprise Edition (JEE) programmers
- Software engineers
- Software architects
- Developers who need to be trained in secure coding techniques to meet PCI compliance
- Application security auditors
- Technical project managers
- Senior software QA specialists
- Penetration testers who want a deeper understanding of target applications or who want to provide more detailed vulnerability remediation options

This secure coding course will teach students how to build secure Java applications and gain the knowledge and skills to keep a website from getting hacked, counter a wide range of application attacks, prevent critical security vulnerabilities that can lead to data loss, and understand the mindset of attackers.

The course teaches you the art of modern web defense for Java applications by focusing on foundational defensive techniques, cutting-edge protection, and Java EE security features you can use in your applications as soon as you return to work. This includes learning how to:

- **Identify security defects in your code**
- **Fix security bugs using secure coding techniques**
- **Utilize secure HTTP headers to prevent attacks**
- **Secure your sensitive representational state transfer (REST) services**
- **Incorporate security into your development process**
- **Use freely available security tools to test your applications**

Great developers have traditionally distinguished themselves by the elegance, effectiveness and reliability of their code. That is still true, but the security of the code now needs to be added to those other qualities. This unique SANS course allows you to hone the skills and knowledge required to prevent your applications from getting hacked.

DEV541: Secure Coding in Java/JEE: Developing Defensible Applications is a comprehensive course covering a wide set of skills and knowledge. It is not a high-level theory course – it is about real-world, hands-on programming. You will examine actual code, work with real tools, build applications and gain confidence in the resources you need to improve the security of Java applications.

Rather than teaching students to use a given set of tools, the course covers concepts of secure programming. This involves looking at a specific piece of code, identifying a security flaw and implementing a fix for flaws found on the OWASP Top 10 and CWE/SANS Top 25 Most Dangerous Programming Errors.

The course culminates in a Secure Development Challenge in which students perform a security review of a real-world open-source application. You will conduct a code review, perform security testing to actually exploit real vulnerabilities, and implement fixes for these issues using the secure coding techniques that you have learned in course.

PCI Compliance

Section 6.5 of the Payment Card Industry (PCI) Data Security Standard (DSS) instructs auditors to verify processes that require training in secure coding techniques for developers. If you are responsible for developing applications that process cardholder data and are therefore required to be PCI compliant then this is the course for you.

Gregory Leonard *SANS Instructor*

Gregory Leonard has more than 17 years of experience in software development, with an emphasis on writing large-scale enterprise applications. Greg's responsibilities over the course of his career have included application architecture and security, performing infrastructure design and implementation, providing security analysis, conducting code reviews and evaluating performance diagnostics. He is currently employed as an application security consultant at Optiv Security, Inc.

541.1 HANDS ON: Data Validation

Improper data validation is the root cause of the most prevalent web application vulnerabilities today. On this first course day students will learn about some of the most prevalent web application vulnerabilities, including cross-site scripting (XSS), cross-site request forgery (CSRF), SQL injection, HTTP response splitting and parameter manipulation. You will learn how to find these issues and re-create them in a running application. Then you will use a variety of methods to actually fix the vulnerabilities in your Java code. The course is full of hands-on exercises where you can apply practical data validation techniques to prevent common attacks with defense, ranging from input validation, output encoding and use of new techniques like Content Security Policy.

Topics: Web Application Attacks; Cross-Site Scripting (XSS); Cross-Site Request Forgery (CSRF); SQL Injection; HTTP Response Splitting; Parameter Manipulation; Directory Traversal; Web Application Proxies; Validation Concerns; Character Encoding; Input Validation; Output Encoding; Blacklisting and Whitelisting; Validation Techniques; Regular Expressions; Servlet Filters; Output Encoding; Content Security Policy; Prepared Statements; CSRF Defense

541.2 HANDS ON: Authentication and Session Management

Broken authentication and session management are common issues that can compromise the integrity of your system. Weak authentication protection can allow an attacker to expose your most sensitive secrets: your data! In this session students will learn about these vulnerabilities and what you can do to design and code stronger authentication protections from the start. You will learn how to use Java Enterprise Edition (EE) container-based authentication and set up basic, form-based and client certificate authentication. You will also learn how to protect data in transit using SSL, and how to securely store passwords at rest. Various authorization attacks will be discussed, as well as unvalidated forwards and redirects. Session management attacks and defenses will also be covered along with Clickjacking and associated defenses.

Topics: Authentication Factors; Authentication Attacks; Java EE Authentication; Basic Authentication; Form-based Authentication; Client Certificates; Using SSL; Secure Password Storage; Authorization; Web and Enterprise JavaBean Access Control; Authorization Attacks; Access Control Bypass; Unvalidated Forwards and Redirects; State Management Attacks; Session Hijacking; Session Fixation; Clickjacking; Using X-Frame-Options

541.3 HANDS ON: Java Platform and API Security

Java is the language of choice for the development of many mission-critical applications. As such, it is vital to understand the security features and implications of using the Java language itself and the Java runtime environment (JRE). Through numerous hands-on exercises you will learn about Java Security Manager, how code privileges are managed, and how to sign jar files. You will also learn about exception handling and the importance of logging. With hands-on exercises you will write code to encrypt data both in transit and at rest using the Java Secure Socket Extension and the Java Cryptography Architecture, as well as integer and double overflows, and about numerous Java language features that you should consider while writing secure code. Organizations continue to expose critical representational state transfer (REST)-based web services that can be consumed by Ajax and mobile applications. You will learn how vulnerabilities like Cross-Site Request Forgery (CSRF) can be used by attackers to hack your JSON services. You will also learn how to develop applications that are resistant to such attacks and about the OAuth protocol for authentication and authorization.

Topics: Java Security Manager; Permissions; Policy File; Jar Signing; Class Security; Error Handling; Exceptions; Using Try/Catch/Finally; Logging; Logging Frameworks; ESAPI Logging; Encryption; Java Secure Sockets Extension (JSSE); Java Cryptography Architecture (JCA); Integer and Double Overflows; Thread Safety; Race Conditions; Web Service (JAX-RS) Security; REST Security; OAuth

541.4 HANDS ON: Secure Development Lifecycle

Using what you have learned about web application vulnerabilities, in this session you will conduct a security review of a real-world open-source application. You will see first hand how to integrate security in your software development life cycle (SDLC) by first conducting a code review of a large, widely used open-source application. Once you have identified various vulnerabilities in the code itself you will perform security testing and actually exploit these weaknesses. Once they have been exploited, you will fix the weaknesses using the secure coding techniques learned in class. The Secure Development Challenge introduces you to what is needed in a Secure SDLC and shows you how to do it first hand!

Topics: Security and the SDLC; Conducting a Secure Code Review; Manual Code Review; Using a Static Analysis Tool; Using FindBugs; Integrating Code Review into the SDLC; Security Testing; Exploiting XSS, CSRF, and SQL Injection; Secure Coding; Fixing Weaknesses in a Running Application

"This is my first SANS course and so far it is truly excellent.
I've learned valuable information from the very first hour. Great!"

-Francois Georgy, SecuLabs

You Will Be Able To

- Use a web application proxy to view and manipulate HTTP requests and responses
- Review and perform basic exploits of common web application vulnerabilities, such as those found among the SANS/CWE Top 25 Most Dangerous Software Errors and the OWASP Top 10:
  - Cross-site scripting (XSS)
  - Cross-site request forgery (CSRF)
  - SQL injection
  - Parameter manipulation
  - Open redirect
  - Session hijacking
  - Clickjacking
  - Authentication and access control bypass
- Mitigate common web application vulnerabilities using secure coding practices and Java libraries, including:
  - Input validation
  - Blacklist and whitelist validation
  - Regular expressions
  - Output encoding
  - Content Security Policy
  - Client-side security headers
- Build applications using:
  - Java Enterprise Edition authentication
  - Basic and form-based authentication
  - Client certificates
  - Secure Sockets Layer/Transport Layer Security (SSL/TLS)
  - Java Secure Sockets Extension
  - Secure password storage techniques
  - Java Cryptography Architecture
  - Security Manager
- Implement a secure software development lifecycle, including code review, static analysis and dynamic analysis techniques.

DEV544

GSSP-.NET Certification

Secure Software Programmer – .NET

www.giac.org/gssp-net

Secure Coding in .NET: Developing Defensible Applications

Four-Day Program
Mon, July 24 - Thu, July 27
9:00am - 5:00pm
24 CPEs
Laptop Required
Instructor: Eric Johnson

Who Should Attend

- ASP.NET developers who want to build more secure web applications
- .NET framework developers
- Software engineers
- Software architects
- Developers who need to be trained in secure coding techniques to meet PCI compliance
- Application security auditors
- Technical project managers
- Senior software QA specialists
- Penetration testers

"This class should be required for anyone in the field of software development."

-Chad Reuss, Meijer

ASP.NET and the .NET framework have provided web developers with tools that allow them an unprecedented degree of flexibility and productivity. However, these sophisticated tools make it easier than ever to miss the little details that allow security vulnerabilities to creep into an application. Since ASP.NET 2.0, Microsoft has done a fantastic job of integrating security into the ASP.NET framework, but the responsibility is still on application developers to understand the limitations of the framework and ensure that their own code is secure.

Have you ever wondered if the built-in ASP.NET validation is effective? Have you been concerned that Windows Communication Foundation (WCF) services might be introducing unexamined security issues into your application? Should you feel uneasy relying solely on the security controls built into the ASP.NET framework?

This comprehensive course covers a huge set of skills and knowledge. It is not a high-level theory course. It is about real programming. Students examine actual code, work with real tools, build applications, and gain confidence in the resources they need to improve the security of .NET applications.

Rather than teaching students to use a set of tools, the course teaches students concepts of secure programming. This involves looking at a specific piece of code, identifying a security flaw, and implementing a fix for flaws found on the OWASP Top 10 and CWE/SANS Top 25 Most Dangerous Programming Errors.

The class culminates with a security review of a real-world open-source application. Students will conduct a code review, review a penetration test report, perform security testing to actually exploit real vulnerabilities, and finally, using the secure coding techniques that they have learned in class, implement fixes for these issues.

PCI Compliance

Section 6.5 of the Payment Card Industry (PCI) Data Security Standard (DSS) instructs auditors to verify processes that require training in secure coding techniques for developers. This is the course for you if your application processes cardholder data and you are required to meet PCI compliance.

Eric Johnson *SANS Certified Instructor*

Eric Johnson is a Senior Security Consultant at Cypress Data Defense and the Application Security Curriculum Product Manager at SANS. He is the lead author and instructor for DEV544: Secure Coding in .NET, as well as an instructor for DEV541: Secure Coding in Java/JEE. Eric serves on the advisory board for the SANS Securing The Human Developer awareness training program and is a contributing author for the developer security awareness modules. His experience includes web and mobile application penetration testing, secure code review, risk assessment, static source code analysis, security research, and developing security tools. Eric completed a bachelor of science in computer engineering and a master of science in information assurance at Iowa State University, and currently holds the CISSP, GWAPT, GSSP-.NET, and GSSP-Java certifications. He is based in West Des Moines, Iowa and outside the office enjoys spending time with his wife and daughter, attending Iowa State athletic events, and golfing on the weekends. **@emjohn20**

544.1 HANDS ON: Data Validation

Improper data validation is the root cause of the most prevalent web application vulnerabilities today. Beginning on the first day, you will learn about some of the most prevalent web applications vulnerabilities such as XSS, SQL Injection, Open Redirects, and Parameter Manipulation. You will see how to find these issues and how to recreate them in a running application. Then you will use a variety of methods to actually fix these vulnerabilities in your C# code. The course is full of hands-on exercises where you can apply practical data validation techniques that you can use to prevent common attacks with defenses ranging from input validation to output encoding and the use of new techniques like Content Security Policy.

Topics: Web Application Attacks; Web Application Proxies; Parameter Manipulation; Cross-Site Scripting (XSS); Open Redirect; Unvalidated Forwards; SQL Injection; HTTP Response Splitting; Input Validation; Indirect Selection; Blacklists; Whitelists; Regular Expressions; Event Validation; Character Encoding; Command Encoding; Content Security Policy; LINQ & Entity Framework

544.2 HANDS ON: Authentication and Session Management

Authentication, authorization, and session management vulnerabilities are commonly exploited by attackers to gain unauthorized access to web applications. In this section, you will learn about various authentication and authorization attacks such as man-in-the-middle, cross-site request forgery, clickjacking, and session hijacking. Then, you will use a variety of techniques to fix these vulnerabilities in an ASP.NET web application.

Topics: Authentication Factors; Authentication Attacks; Authorization Attacks; Password Management; ASP.NET Identity; Forms Authentication & Membership Provider; Race Conditions; Session Identifiers; Man-in-the-middle (MITM) Attacks; Cross-Site Request Forgery (CSRF); Clickjacking; Session Hijacking; Session Fixation; Session Management; Cookie Security

544.3 HANDS ON: .NET Framework Security

A secure architecture is critical for mission-critical .NET applications. You will learn about various built-in .NET security features such as cryptography, password storage, web service security and many other .NET features you should consider while writing secure code. A number of hand-on exercises will guide you through writing a cryptography utility for storing sensitive data and user passwords, protecting data in memory, exploiting a running application using DLL Injection, and much more.

Topics: Cryptography; Password Storage; PCI Compliance; Threading; String Immutability; Numeric Overflow; Risks of Malicious Code; Exception Handling; Auditing and Logging; Web Services

544.4 HANDS ON: Secure Software Development Lifecycle (SDLC)

We will take a look at each phase of the SDLC and discuss how security fits into the process. Using what you have learned about application vulnerabilities, you will get the opportunity to write static analysis rules to identify insecure code. You will then perform security testing and actually exploit these weaknesses. Once they have been exploited, you will then fix them using the secure coding techniques you have learned in class.

Topics: Security Training; Security Requirements; Secure Design; Threat Modeling; Implementation; Static Analysis; Roslyn Diagnostic Analyzers; Peer Reviews; Secure Code Review; Verification; Dynamic Analysis; Penetration Test Reports; Release; Response

"It is shocking to see how much we are missing in our code. I am going back to change the code immediately."

-Ruojie Wang, New Jersey Hospital Association

You Will Be Able To

- Use a web application proxy to view and manipulate HTTP requests and responses
- Review and perform basic exploits of common web application vulnerabilities, such as those found among the SANS/CWE Top 25 Most Dangerous Software Errors and the OWASP Top 10:
  - Cross-Site Scripting
  - Parameter Manipulation
  - Open Redirect
  - Unvalidated Forwards
  - SQL Injection
  - Session Hijacking
  - Clickjacking
  - Cross-Site Request Forgery
  - Man-in-the-middle
- Mitigate common web application vulnerabilities using industry best practices in the .NET framework, including:
  - Input Validation
  - Blacklist and Whitelist Validation
  - Regular Expressions
  - Command Encoding
  - Output Encoding
  - Content Security Policy
  - Client-side Security Headers
- Understand built-in ASP .NET security mechanisms, including:
  - AntiForgeryToken
  - Data Annotations
  - Event Validation
  - Request Validation
  - View State
  - Entity Framework
  - ASP.NET Identity
  - Forms Authentication
  - Membership Provider
  - WCF
  - Web API
  - Roslyn Diagnostic Analyzers
- Apply industry best practices (NIST, PCI) for cryptography and hashing in the .NET framework.
- Implement a secure software development lifecycle (SDLC) to include threat modeling, static analysis and dynamic analysis.

ICS410

ICS/SCADA Security Essentials

GICSP Certification
Industrial Cyber Security Professional
www.giac.org/gicsp

Five-Day Program
Mon, July 24 - Fri, July 28
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Eric Cornelius

Who Should Attend

The course is designed for the range of individuals who work in, interact with, or can affect industrial control system environments, including asset owners, vendors, integrators, and other third parties. These personnel primarily come from four domains:

- IT (includes operational technology support)
- IT security (includes operational technology security)
- Engineering
- Corporate, industry, and professional standards

"Great introduction into ICS landscape and associated security concerns. The ICS material presented will provide immediate value relative to helping secure my company."
-Mike Poulos, Coca-Cola Enterprises

SANS has joined forces with industry leaders to equip security professionals and control system engineers with the cybersecurity skills they need to defend national critical infrastructure. **ICS410: ICS/SCADA Security Essentials** provides a foundational set of standardized skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

The course will provide you with:

- **An understanding of industrial control system components, purposes, deployments, significant drivers, and constraints**
- **Hands-on lab learning experiences to control system attack surfaces, methods, and tools**
- **Control system approaches to system and network defense architectures and techniques**
- **Incident-response skills in a control system environment**
- **Governance models and resources for industrial cybersecurity professionals**

When examining the greatest risks and needs in critical infrastructure sectors, the course authors looked carefully at the core security principles necessary for the range of tasks involved in supporting control systems on a daily basis. While other courses are available for higher-level security practitioners who need to develop specific skills such as industrial control system penetration testing, vulnerability analysis, malware analysis, forensics, secure coding, and red team training, most of these courses do not focus on the people who operate, manage, design, implement, monitor, and integrate critical infrastructure production control systems.

With the dynamic nature of industrial control systems, many engineers do not fully understand the features and risks of many devices. For their part, IT support personnel who provide the communications paths and network defenses do not always grasp the systems' operational drivers and constraints. This course is designed to help traditional IT personnel fully understand the design principles underlying control systems and how to support those systems in a manner that ensures availability and integrity. In parallel, the course addresses the need for control system engineers and operators to better understand the important role they play in cybersecurity. This starts by ensuring that a control system is designed and engineered with cybersecurity built into it, and that cybersecurity has the same level of focus as system reliability throughout the system lifecycle.

When these different groups of professionals complete this course, they will have developed an appreciation, understanding, and common language that will enable them to work together to secure their industrial control system environments. The course will help develop cyber-secure-aware engineering practices and real-time control system IT/OT support carried out by professionals who understand the physical effects of actions in the cyber world.

Eric Cornelius *SANS Certified Instructor*

Eric Cornelius is the Director of Critical Infrastructure and Industrial Control Systems (ICS) at Cylance, Inc., where he is responsible for thought leadership, architecture, and consulting. Eric brings a wealth of ICS knowledge and his leadership keeps organizations safe, secure, and resilient against advanced attackers. Previously, Eric served as the Deputy Director and Chief Technical Analyst for the Control Systems Security Program at the U.S. Department of Homeland Security. Eric earned a bachelor's degree from the New Mexico Institute of Mining and Technology, where he was the recipient of many scholarships and awards including the National Science Foundation's Scholarship for Service. Eric went on to work at the Army Research Laboratory's (ARL) Survivability/Lethality Analysis Directorate, where he worked to secure field deployable combat technologies. It was at ARL that Eric became interested in non-traditional computing systems, an interest that ultimately led him to the Idaho National Laboratory where he participated in deep-dive vulnerability assessments of a wide range of ICS systems. Eric is the co-author of "Recommended Practice: Creating Cyber Forensics Plans for Control Systems" as part of the DHS National Cyber Security Division's 2008 Control Systems Security Program and is also a frequent speaker and instructor at ICS events across the globe.

410.1 ICS Overview

Students will develop and reinforce a common language and understanding of industrial control system (ICS) cybersecurity as well as the important considerations that come with cyber-to-physical operations within these environments. Each student will receive programmable logic controller (PLC) hardware to keep. The PLC contains physical inputs and outputs that will be programmed in class and mapped to an operator interface, or HMI, also created in class. This improved hardware-enabled approach provides the necessary cyber-to-physical knowledge that allows students to better understand important ICS operational drivers and constraints that require specific safety protection, communications needs, system management approaches, and cybersecurity implementations. Essential terms, architectures, methodologies, and devices are all covered to build a common language for students from a variety of different roles.

Topics: **Global Industrial Cybersecurity Professional (GICSP) Overview; Overview of ICS; Field Components; Programming Controllers; Supervisory Components; Types of ICS Systems; IT & ICS Differences; Physical Security; ICS Network Architecture**

410.2 ICS Attack Surface

If you know the adversary's approaches to attacking an ICS environment, you will be better prepared to defend that environment. Numerous attack vectors exist within an ICS environment. Some are similar to traditional IT systems, while others are more specific to ICS. During Day 2, defenders will develop a better understanding of where these specific attack vectors exist, as well as the tools to use to discover vulnerabilities and exploit them. Each student will use a vulnerable target virtual machine to further understand attacks targeting the types of web servers used on many ICS devices for management purposes. Simulators will be configured to allow students to conduct attacks against unauthenticated ICS protocols. A variety of data samples are used to examine additional attack vectors on remote devices.

Topics: **ICS Attack Surface; Attacks on HMIs and UIs; Attacks on Control Servers; Attacks on Network Communications; Attacks on Remote Devices**

410.3 Defending ICS Servers and Workstations

Students will learn essential ICS-related server and workstation operating system capabilities, implementation approaches, and system management practices. Students will receive and work with both Windows- and Linux-based virtual machines in order to understand how to monitor and harden these hosts from attack. We'll examine concepts that benefit ICS systems such as system hardening, log management, monitoring, alerting, and audit approaches, then look at some of the more common applications and databases used in ICS environments across multiple industries.

Topics: **Windows in ICS; Linux/Unix in ICS; Updates and Patching; Processes and Services; Configuration Hardening; Endpoint Defenses; Automation and Auditing; Log Management; Databases and Historians**

410.4 Defending ICS Networks and Devices

With an understanding of the ICS environment, the attack vectors that exist, and the defender-specific capabilities available on servers, workstations, and applications, students will now learn network-specific defense approaches. We'll first examine common IT protocols and network components used within ICS environments, then discuss ICS-specific protocols and devices. Technologies used to defend ICS networks will be reviewed along with implementation approaches. Students will interact with ICS traffic and develop skills to analyze it, then work through a number of tools to further explore a series of staged adversary actions conducted in a lab environment.

Topics: **Network Fundamentals; Ethernet; TCP/IP Protocol Suite; ICS Protocols over TCP/IP; Enforcement Zone Devices; Honeypots; Wireless in Control Systems; Network Capture Forensics; Field and Plant Floor Equipment; Cryptography Fundamentals**

410.5 ICS Security Governance

Students will learn about the various models, methodologies, and industry-specific regulations that are used to govern what must be done to protect critical ICS systems. Key business processes that consider risk assessments, disaster recovery, business impact analysis, and contingency planning will be examined from the perspective of ICS environments. On this final course day, students will work together on an incident response exercise that places them squarely in an ICS environment that is under attack. This exercise ties together key aspects of what has been learned throughout the course and presents students with a scenario to review with their peers. Specific incident-response roles and responsibilities are considered, and actions available to defenders throughout the incident response cycle are explored. Students will leave with a variety of resources for multiple industries and will be well prepared to pursue the GICSP, an important ICS-focused professional certification.

Topics: **Information Assurance Foundations; Security Policies; Contingency and Continuity Planning; Risk Assessment and Auditing; Attack Tree Analysis; Password Management; Incident Handling; Incident Response; Resources**

You Will Be Able To

- Run Windows command line tools to analyze the system looking for high-risk items
- Run Linux command line tools (ps, ls, netstat, ect) and basic scripting to automate the running of programs to perform continuous monitoring of various tools
- Install VMWare and create virtual machines to create a virtual lab to test and evaluate tools/security of systems
- Better understand various industrial control systems and their purpose, application, function, and dependencies on network IP and industrial communications
- Work with operating systems (system administration concepts for Unix/Linux and/or Windows operating systems)
- Work with network infrastructure design (network architecture concepts, including topology, protocols, and components)
- Better understand the systems' security lifecycle
- Better understand information assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)
- Use your skills in computer network defense (detecting host and network-based intrusions via intrusion detection technologies)
- Implement incident response and handling methodologies

"Best training course I've taken in 25+ years."

-Curt Imanse, Accenture

SANS Technology Institute

www.sans.edu

Bundle OnDemand

WITH THIS COURSE

www.sans.org/ondemand

SEC524

Cloud Security Fundamentals

Two-Day Program
Sat, July 22 - Sun, July 23
9:00am - 5:00pm
12 CPEs
Laptop Required
Instructor: Dave Shackleford

Who Should Attend

- Security personnel
- Network and systems administrators
- Technical auditors and consultants
- Security and IT managers

SEC524 starts out with a detailed introduction to the various delivery models of cloud computing, ranging from Software as a Service (SaaS) to Infrastructure as a Service (IaaS) and everything in between. Each of these delivery models represents an entirely separate set of security conditions to consider, especially when coupled with various cloud types, including public, private and hybrid. An overview of security issues within each of these models will be covered with an in-depth discussion of the risks involved. This cloud security training course will go in depth on architecture and infrastructure fundamentals for private, public, and hybrid clouds, including a wide range of topics such as patch and configuration management, virtualization security, application security and change management. Policy, risk assessment, and governance within cloud environments will also be covered, with recommendations for both internal policies and contract provisions. This path leads to a discussion of compliance and legal concerns. The first day will wrap up with disaster recovery and business continuity planning using cloud models and architecture.

Day 2 of this cloud security training course will start with the challenges of identity and access management in cloud environments. Next, more businesses are utilizing the cloud to store critical data and we will cover how to protect your critical data in the cloud. New approaches for data encryption, network encryption, key management and data lifecycle concerns will be covered in detail, followed by a deep dive into risk assessments and risk management. Intrusion detection and incident response in cloud environments will also be covered, along with how best to manage these critical security processes and the technologies that support them given that most controls are managed by the CSP.

"One of the best courses I have been part of in my learning career." -Srinath Kamman, Accenture

---

SEC546

IPv6 Essentials

Two-Day Program
Sat, July 22 - Sun, July 23
9:00am - 5:00pm
12 CPEs
Laptop Required
Instructor:
Johannes Ullrich, Ph.D.

We are out of IPv4 addresses. ISPs worldwide will have to rapidly adopt IPv6 in the years ahead in order to grow, particularly because mobile devices require more and more address space. Already, modern operating systems implement IPv6 by default. Windows 7, for example, ships with Teredo enabled by default. This course is designed not just for implementers of IPv6, but also for those who just need to learn how to detect IPv6 and defend against threats that unintentional IPv6 use may bring about.

IPv6 is currently being implemented rapidly in Asia in response to the exhaustion of IPv4 address space, which is most urgently felt in fast-growing networks in China and India. Even if you do not feel the same urgency of IP address exhaustion, you may have to connect to these IPv6 resources as they become more important to global commerce.

Implementing IPv6 should not happen without carefully considering the security impact of the new protocol. Even if you haven't implemented it yet, the ubiquitous IPv6 support in modern operating systems easily leads to unintentional IPv6 implementation, which may put your network at risk. In this course, we will start out by introducing the IPv6 protocol, explaining in detail many of its features like the IPv6 header, extension headers and auto configuration. Only by understanding the design of the protocols in depth will it be possible to appreciate the various attacks and mitigation techniques. The course will address how to take advantage of IPv6 to re-think how to assign addresses in your network and how to cope with what some suggest is the biggest security problem in IPv6: no more NAT! IPv6 doesn't stop at the network layer. Many application layer protocols change in order to support IPv6, and we will take a close look at protocols like DNS, DHCPv6, and more.

The course covers various security technologies like firewalls and Intrusion Detection and Prevention Systems (IDS/IPS). It also addresses the challenges in adequately configuring these systems and makes suggestions as to how to apply existing best practices to IPv6. Upcoming IPv6 attacks are discussed using tools like the THC IPv6 attack suite and others as an example.

This course will introduce network administrators and security professionals to the basic concepts of IPv6. While it is an introduction to IPv6, it is not an introduction to networking concepts.

Cyber Defense **SHORT COURSES**

SEC**440**

Critical Security Controls: Planning, Implementing, and Auditing

Two-Day Program
Sat, July 22 - Sun, July 23
9:00am - 5:00pm
12 CPEs
Laptop Not Needed
Instructor: Randy Marchany

This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS). These Critical Security Controls are rapidly becoming accepted as the highest priority list of what must be done and proven before anything else at nearly all serious and sensitive organizations. These controls were selected and defined by the U.S. military and other government (including NSA, DHS, GAO, and many others) and private organizations that are the most respected experts on how attacks actually work and what can be done to stop them. They defined these controls as their consensus for the best way to block known attacks and find and mitigate damage from the attacks that get through. For security professionals, the course enables you to see how to put the controls in place in your existing network though effective and widespread use of cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the controls are effectively implemented. **SEC440 does not contain any labs. Students looking for hands-on labs involving the Critical Controls should take SEC566.**

Penetration Testing **SHORT COURSES**

SEC**567**

Social Engineering for Penetration Testers

Two-Day Program
Sat, July 22 - Sun, July 23
9:00am - 5:00pm
12 CPEs
Laptop Required
Instructor: Micah Hoffman

SEC567 provides the blend of knowledge required to add social engineering skills to your penetration testing portfolio. Successful social engineering utilizes psychological principles and technical techniques to measure your success and manage the risk. SEC567 covers the principles of persuasion and the psychological foundations required to craft effective attacks, then bolsters this with many examples of what works, drawing on the work of cyber criminals as well as the experience of the instructor in combating them. On top of these principles we provide a number of tools (produced in our engagements over the years and now available in the course) and also labs centered around the key technical skills required to measure your social engineering success and report it to your company or client.

You'll learn how to perform recon on targets using a wide variety of sites and tools, create and track phishing campaigns, and develop media payloads that effectively demonstrate compromise scenarios. You'll also learn how to conduct pretexting exercises, and we wrap the course with a fun "Capture the Human" exercise to put what you've learned into practice. This is the perfect course to open up new attack possibilities, to better understand the human vulnerability in attacks and to let you practice snares that have proven themselves in tests time and time again.

SEC**580**

Metasploit Kung Fu for Enterprise Pen Testing

Two-Day Program
Sat, July 22 - Sun, July 23
9:00am - 5:00pm
12 CPEs
Laptop Required
Instructor:
Christopher Crowley

Many enterprises today face regulatory or compliance requirements that mandate regular penetration testing and vulnerability assessments. Commercial tools and services for performing such tests can be expensive. While really solid free tools such as Metasploit are available, many testers do not understand the comprehensive feature sets of such tools and how to apply them in a professional-grade testing methodology. Metasploit was designed to help testers confirm vulnerabilities using an open-source and easy-to-use framework. This course will help students get the most out of this free tool.

This class will show students how to apply the incredible capabilities of the Metasploit Framework in a comprehensive penetration testing and vulnerability assessment regimen according to a thorough methodology for performing effective tests. Students who complete the course will have a firm understanding of how Metasploit can fit into their penetration testing and day-to-day assessment activities. The course will provide an in-depth understanding of the Metasploit Framework far beyond simply showing attendees how to exploit a remote system. The class will cover exploitation, post-exploitation reconnaissance, token manipulation, spear-phishing attacks, and the rich feature set of the Meterpreter, a customized shell environment specially created for exploiting and analyzing security flaws.

The course will also cover many of the pitfalls that a tester may encounter when using the Metasploit Framework and how to avoid or work around them, making tests more efficient and safe.

MGT305

Technical Communication and Presentation Skills for Security Professionals

One-Day Program
Sun, July 23
9:00am - 5:00pm
6 CPEs
Laptop Required
Instructor: David Hoelzer

This course is designed for every IT professional in your organization. In this course we cover the top techniques that will show you how to research and write professional quality reports, and how to create outstanding presentation materials. Attendees will also get a crash course on advanced public speaking skills. Writing reports is a task that many IT professionals struggle with, sometimes from the perspective of writing the report and other times from the perspective of having to read someone else's report! In the morning material, we cover step by step how to work through the process of identifying critical ideas, how to properly research them, how to develop a strong argument in written form, and how to put it all down on paper. How do you transform an excellent report into a powerful presentation? We will work through a process that serves to either condense a report into a presentation or can even be used to write a presentation from scratch that communicates your important thoughts in a meaningful and interesting way.

SANS Technology Institute
www.sans.edu

MGT415

A Practical Introduction to Cybersecurity Risk Management

Two-Day Program
Sat, July 22 - Sun, July 23
9:00am - 5:00pm
12 CPEs
Laptop Required
Instructor: James Tarala

In this course students will learn the practical skills necessary to perform regular risk assessments for their organizations. The ability to perform a risk assessment is crucial for organizations hoping to defend their systems. There are simply too many threats, too many potential vulnerabilities, and not enough resources to create an impregnable security infrastructure. Therefore every organization, whether it does so in an organized manner or not, will make priority decisions on how best to defend its valuable data assets. Risk assessment should be the foundational tool used to facilitate thoughtful and purposeful defense strategies.

You Will Learn:

- How to perform a risk assessment step by step
- How to map an organization's business requirements to implemented security controls
- The elements of risk assessment and the data necessary for performing an effective risk assessment
- In-depth risk management models for implementing a deeper risk management program in your organization

MGT433

Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Program

Two-Day Program
Sat, July 22 - Sun, July 23
9:00am - 5:00pm
12 CPEs
Laptop Not Needed
Instructor: Lance Spitzner

Organizations have invested a tremendous amount of money and resources into securing technology, but little if anything into securing their employees and staff. As a result, people, not technology, have become their weakest link in cybersecurity. The most effective way to secure the human element is to establish a high-impact security awareness program that goes beyond just compliance and changes behaviors. This intense two-day course will teach you the key concepts and skills needed to build, maintain, and measure just such a program. All course content is based on lessons learned from hundreds of security awareness programs from around the world. You will learn not only from your instructor, but from extensive interaction with your peers as well. Please bring example materials from your security awareness program that you can show and share with other students during the course. Finally, through a series of labs and exercises, you will develop your own custom security awareness plan that you can implement as soon as you return to your organization.

SANS Technology Institute
www.sans.edu

Who Should Attend

- Security awareness officers
- Chief security officers and security management officials
- Security auditors, and governance and compliance officers
- Training, human resources, and communications staff
- Representatives from organizations regulated by industries such as HIPAA, FISMA, FERPA, PCI-DSS, ISO/IEC 27001 SOX, NERC, or any other compliance-driven standard
- Anyone involved in planning, deploying or maintaining a security awareness program

DEV531

Defending Mobile Applications Security Essentials **NEW!**

Two-Day Program
Sat, July 22 - Sun, July 23
9:00am - 5:00pm
12 CPEs
Laptop Required
Instructor: Gregory Leonard

Mobile application development is growing exponentially from year to year. As of late 2015, over 3 million apps were deployed in the Apple and Google app stores. These apps are consumed by over 700 million users world-wide and account for 33% of the traffic on the Internet. Average users have over 100 mobile apps installed on their device, many of which provide business critical services to customers and employees.

Unfortunately, these apps are often rushed to market to gain a competitive advantage with little regard for security. As seen in web applications for the past 20 years, software vulnerabilities always exist where code is being written and mobile apps are no different. Mobile apps are vulnerable to a whole new class of vulnerabilities, as well as most traditional issues that have long plagued web and desktop applications. This problem will only continue to grow unless managers, architects, developers, and QA teams learn how to test and defend their mobile apps.

DEV531: Defending Mobile Applications Security Essentials covers the most prevalent mobile app risks, including those from the OWASP Mobile Top 10. Students will participate in numerous hands-on exercises available in both the Android and iOS platforms. Each exercise is designed to reinforce the lessons learned throughout the course, ensuring that you understand how to properly defend your organization's mobile applications.

To maximize the benefit for a wide range of audiences, the discussions in this course cover high-level mobile app defensive strategies, as well as risks specific to both the Android and iOS mobile operating systems. Students will walk away with the knowledge and skills to:

- **Understand mobile app risks and common vulnerabilities**
- **Find vulnerabilities in their mobile apps before an attacker does**
- **Apply defensive strategies to build secure mobile apps from the beginning**

DEV534

Secure DevOps: A Practical Introduction **NEW!**

Two-Day Program
Sat, July 22 - Sun, July 23
9:00am - 5:00pm
12 CPEs
Laptop Required
Instructor: Frank Kim

This course explains the fundamentals of DevOps and how DevOps teams can build and deliver secure software. It will explain the principles and practices and tools in DevOps and how they can be leveraged to improve the reliability, integrity and security of systems.

Drawing on lessons from successful DevOps security programs, students will build up a DevOps CI/CD toolchain and learn understand how code is automatically built, tested and deployed, using popular open-source tools including git, Puppet, Jenkins, and Docker.

In a series of labs students will inject security into a CI/CD toolchain, and learn about the tools, patterns and techniques to do this.

The course will make extensive use of open-source materials and tooling for automated configuration management ("Infrastructure as Code"), Continuous Integration, Continuous Delivery and Continuous Deployment, containerization and micro-segmentation, and automated compliance ("Compliance as Code") and monitoring.

You Will Learn:

- Foundations and principles of DevOps, Continuous Delivery and Continuous Deployment
- The security risks and challenges that DevOps introduces
- The keys to successful DevOps security programs
- How to build security into Continuous Delivery and Continuous Deployment, including tools, patterns and techniques of security automation in DevOps
- How to secure your build and deployment environment and tool chain
- How to leverage Infrastructure as Code for secure configuration management and provisioning
- How manual security practices (risk assessments, audits and pen tests) can be adapted to continuously changing environments, and the important role that they still play
- Security risks and challenges that containers introduce, and how to secure container technology
- How to automate compliance in DevOps, using the DevOps Audit Defense Toolkit

Bonus Sessions

Enrich your SANS training experience! Evening talks by our instructors and selected subject-matter experts help you broaden your knowledge, hear from the voices that matter in computer security, and get the most for your training dollar.

KEYNOTE: State of the Internet Panel Discussion

Internet Storm Center Handlers

SANSFIRE offers the greatest opportunity to meet Internet Storm Center handlers from around the world, and our most popular bonus session is their "State of the Internet" panel discussion. During this session, you will have the chance to hear from our handlers and ask their opinions and insights on current threats. This is a unique opportunity you will only have at SANSFIRE – a dozen of the industry's brightest minds at your disposal for two intriguing hours!

DOS-No-More: An Automation Toolset for Upstream Mitigation of DOS and DDOS Attacks

Rob Vandenbrink, ISC Handler

Recently we've been seeing DDOS attacks making a comeback. Or is it that they never left? In days gone by, when a DDOS attack involving hundreds or thousands of attackers occurred, we had to rely on a manual configuration on the upstream ISP to filter the attack traffic, usually by some mix of source and destination IP. More recently, we're now able to buy some really expensive hardware or upstream solutions that will automate some of this. In this presentation we will outline current methods of upstream mitigation of DDOS attacks, for zero or close to zero budget. DNM (Dos No More) uses a set of Python modules and ELK to query and interpret firewall and IPS logs to identify DOS and DDOS attacks, then characterizes "malicious traffic" using up to 12 different metrics. This is then used to update a table on the local router, which propagates that information to the ISP where the attack can be mitigated in any one of several ways, all dictated by the client to the ISP. The ruleset to identify attacks and specify how to deal with each attack type is held in a simple configuration file, so is easily customized. In the live demo, you will see attacks against production sites as well as amplification attacks. All attacks are identified in an automated fashion by the customer infrastructure, and then blocked, rate limited or otherwise mitigated at the ISP.

Espionage, Influence Operations, and Political Breaches: What Do High-Profile Attacks Teach Us About Enterprise Security?

John Bambenek, ICS Handler

The last 12 months have been filled with news of high-profile political targets being subjected to nation-state attacks. Stolen data are being used by non-friendly adversaries to manipulate and influence public opinion. It is easy to assume that skilled attackers are only interested in high-value targets, but the reality is that this is very much not the case. In a world of high-profile espionage attacks there are important lessons for enterprises to learn about their own security and what they should be doing. This talk will cover the tactics adversarial actors have used to establish their foothold in their victims and the similarity those same tactics have to more traditional cybercriminal actors. The surprising reality is that most of the techniques involve social engineering where, had the victims known what to look for, they would have been able to protect themselves. This talk will also cover how data was exfiltrated and detection strategies for enterprises to determine if they have data leakage occurring that requires response. The advent of defensive deception has also provided promising possibilities to protect enterprises (and high-value targets).

IR Awakens

Tom Webb, ICS Handler

Incident response at EDUs is a target rich environment; this allows for lots of opportunities to test tools and techniques. By analyzing your incidents statistics and your IR team's metrics, you can start to pinpoint gaps. We will review historical stats, incident details, and tools deployed. We will discuss how we reduced discovery time and investigation time at the University of South Carolina and what change was the most effective. These lessons can be applied to your environment to improve your IR program.

Performing Cyber Threat Intelligence in Power Infrastructure

Manuel Humberto Santander Palaez, ICS Handler

Effective cybersecurity requires companies to be one step ahead of hackers so their movements in the network can be effectively tracked before the cyberattack completely materializes. But in Operation Technology, how can this be done without any kind of affectation to the process? In this presentation we will review a practical case on implementation of cyber threat intelligence process for power generation, transmission and distribution, including tools used for Modbus, IEC 6087-5-104 and IEC 61850.

Pwning NoSQL Applications for Fun and Profit

Bojan Zdrnja, ICS Handler

In the last couple of years, NoSQL databases have become the main database used by many web developers. Together with popular stacks, such as the MEAN stack (MongoDB, Express.js, Angular.js and Node.js), NoSQL databases are increasingly popular, since such stacks support both client- and server-side programs written in JavaScript, allowing easy development. The core database used by the MEAN stack, MongoDB, is a NoSQL database program that uses JSON-like documents with dynamic schemas allowing huge flexibility. Although NoSQL databases are not vulnerable to standard SQL injection attacks, they can be exploited with various injection vulnerabilities depending on the creation of queries, which can even include user-defined JavaScript functions. This presentation will demonstrate how applications that use NoSQL databases can be exploited through NoSQL injection in order to retrieve data from the database and do even more.

Using Security Onion to Review Suspicious Network Traffic

Brad Duncan, ICS Handler

Malicious network traffic is often difficult for security professionals to recognize without the help of an intrusion detection system (IDS) or and other security tools. The Security Onion Linux distro is an outstanding resource that can help people analyze suspicious network traffic. In this presentation, ISC Handler Brad Duncan discusses how he first discovered Security Onion in 2013 and how he has used it since then. He covers how to use Security Onion in a lab environment to test traffic from exploit kits and links or attachments from malicious spam. Brad also covers how to set up Security Onion to monitor live traffic in a physical or virtual research environment. Such environments provide an excellent way to review network traffic or examine malware from infected Windows hosts.

So, You Wanna Be a Pentester?

Adrien de Beaupre

In this presentation, Adrien de Beaupre will discuss the education, background, aptitude,skills, and experience that are necessary to succeed as a penetration tester.

Quality Not Quantity: Continuous Monitoring's Deadliest Events

Eric Conrad

Most Security Operations Centers are built for compliance, not security. One well-known retail firm suffered the theft of over a million credit cards. Some 60,000 true positive events were reported to their SOC during that breach... and missed, lost in the noise of millions. If you are bragging about how many events your SOC "handles" each day: you are doing it wrong. During this talk we will show you how to focus on quality instead of quantity, and provide an actionable list of the deadliest events that occur during virtually every successful breach. We will also provide an overview of DeepBlueCLI, a PowerShell framework for automatically detecting the deadliest events.

Actionable Detects: Blue Team Cyber Defense Tactics

Seth Misenar

Organizations relying on third parties to detect breaches can go almost a full year before finding out they have been compromised. Detect the breach yourself, and on average you will find it within about a month of the initial occurrence. Considering detection and defense against modern adversaries too costly to perform yourself can be a very expensive miscalculation considering the substantially increased price of response and recovery with breach duration. This continually evolving presentation provides you thoughts, tactics, techniques, and procedures to once again take pride in your Blue Team Cyber capabilities. Not applying these lessons learned could prove costly in the face of adapting threat actors. Dig in and learn to hold your head high when talking about your defensive cyber operations capabilities.

The Cider Press: Extracting Forensic Artifacts from Apple Continuity

Heather Mahalik, Sarah Edwards, and Philip Hagen

Apple Continuity allows us to move between our devices without disruption in activity. Just think of the ultimate handoff where you can start browsing the Internet on your iPhone, continue on your Mac without the hassle of having to type a search a second time. Essentially, your devices work together enabling you to do less. Imagine how this looks on a Mac, iPhone, or Apple Watch. Will you be able to tell which device the user conducted an activity on? What will the on-device forensic artifacts look like? Continuity requires inter-device communications, so what artifacts will be present on the WiFi and Bluetooth fronts? What if this feature would make or break your investigation?

Infosec Rock Star: Geek Will Only Get You So Far

Ted Demopoulos

Some of us are so effective, and well known, that the term "Rock Stars" is entirely accurate. What kind of skills do Rock Stars have and wannabe Rock Stars need to develop? Although we personally may never be swamped by groupies, we can learn the skills to be more effective, well respected, and well paid. Obviously it's not just about technology; in fact most of us are very good at the technology part. The fact is that increasing our skills more on the social and business side will make most of us more effective at what we do than learning how to read hex better while standing on our heads, becoming "One with Metasploit," or understanding the latest hot technologies.

Securing Your Kids

Lance Spitzner

Technology is an amazing tool. It allows our kids to access a tremendous amount of information, meet new people, and communicate with friends around the world. In addition, for them to be successful in the 21st century they have to know and understand how to leverage these new tools. However, with all these capabilities come a variety of new risks, risks that as parents you may not understand or even be aware of. In this one-hour presentation we cover the top three risks to kids online and the top steps you can take to protect them.

Evolving Threats

Paul Henry

For nearly two decades defenders have fallen into the "Crowd Mentality Trap." They have simply settled on doing the same thing everyone else was doing, while at the same time attackers have clearly evolved both in terms of malware delivery vectors and attack methodology. Today our defenses focus primarily on the gateway and upon attempting to outwit attackers' delivery methods. This leaves us woefully exposed and according to a recent Data Breach Report has resulted in 3,765 incidents, 806 million records exposed, and $157 billion in data breach costs in only the past six years.

Offensive Digital Forensics

Alissa Torres

Network intruders are utilizing increasingly more sophisticated offensive forensic techniques in order to parse remote systems, obtain credentials, and locate and steal "target data," all while flying under the radar of modern detection systems. Incident responders and forensic examiners must be able to unravel the actions and intent of the adversary on their own networks in order to halt their progress, and anticipate future campaigns. From this session, attendees will gain a deeper understanding of today's offensive forensic strategies, how adversaries determine where key sensitive data and target individuals reside and, most importantly, how to detect these techniques utilizing Windows and file system artifacts.

Vendor-Sponsored Events

Vendor Expo

Wednesday, July 26

12:00pm - 1:30pm & 5:30pm - 7:30pm

Given that virtually everything in security is accomplished with a tool, exposure to those tools is a very important part of the SANS training event learning experience. Leading solution providers will be on hand for a one-day vendor expo, an added bonus to registered training event attendees. Attendees can visit sponsors during the lunch time and evening Vendor Expo hours to receive stamps on the Passport-to-Prizes form. Prize drawings will occur at the Vendor Welcome Reception.

VENDOR-SPONSORED

Networking Lunch

Wednesday, July 26

12:00pm - 1:30pm

Join these sponsoring vendors and others on the expo floor for an introduction to leading solutions and services that showcase the best options in information security.

Lunch & Learn Presentations

Throughout SANSFIRE 2017, vendors will provide sponsored lunch presentations where attendees can interact with peers and learn about vendor solutions. Take a break and get up-to-date on security technologies!

Bonus Sessions CONTINUED

10 Tenets of CISO Success

Frank Kim

The era of CISO-as-dictator is at an end. The increased importance of cybersecurity as a vital component of business growth requires security leaders to find new ways to work with executive leaders, business partners, and their own team members. Learn 10 tenets that CISOs and security leaders can utilize to go beyond technical skills, successfully lead organizations through change, and ultimately get to "yes" with the business.

The Three C's to Building a Mature Awareness Program

Lance Spitzner

After working with hundreds of organizations we have found three common obstacles to a successful awareness program, which we call the three Cs: Communication, Collaboration and Culture. Learn how the most effective organizations are overcoming these three challenges and how you can apply their lessons learned to your own security awareness program.

Making Sense of the Critical Security Controls in the Cloud

Eric Johnson

Is cloud security feeling a bit nebulous? A solid framework can help get you on stable footing. The CIS Critical Security Controls are publicly available (and free), and offer just such a framework. This talk will offer an in-depth examination of three of the Critical Security Controls and how they can be applied using Amazon Web Service (AWS) services and tools.

A Hunting We Will Go...

John Strand

In this talk we will discuss the RITA framework for detecting advanced beacons. It is free, it runs on top of Bro, and it rocks. We will walk through how it works and how you can set it up in your environment. Right now. In under 15 minutes.

Malware Analysis for Incident Responders: Getting Started

Lenny Zeltser

Knowing how to analyze malware has become a critical skill for incident responders and forensic investigators. A good way to get started with such efforts involves examining how malicious software behaves in a controlled laboratory environment. In this two-hour seminar briefing, Lenny Zeltser demonstrates key aspects of this process, walking you through behavioral analysis of a malware specimen by using several free tools and even peeking into the world of code analysis. You will see practical techniques in action and understand how malware analysis will help you to triage the incident and assess key capabilities of the malicious software. You will also learn how to determine ways of identifying this malware on systems in your environment by establishing indicators of compromise (IOCs). This seminar will help you start learning how to turn malware inside out.

You've Got Ransomeware! Managing the Legal Risk of Cyber Fraud

Benjamin Wright

Today most fraud has a cyber component, and most fraud investigations involve digital evidence. Cyber fraud like ransomware can trigger a legal crisis for your firm or your client. Mr. Wright will share insights on how to manage the legal risk. He will examine legal measures such as disclaimers, cyber insurance and invocation of attorney confidentiality rules.

Prioritizing Your Security Program

Keith Palmgren

Building a cybersecurity program is easy. Building a cybersecurity program that is effective is seriously hard! When faced with a seemingly insurmountable task, prioritization is vital. Investing time and money in the right place at the right time is the difference between success and being the next cyberbreach headline. Whether you are new to cybersecurity or an old hand, you may feel lost in the storm. If so, this talk is for you. Cybersecurity's five historic and current pitfalls that prevent organizations from building an effective IT Security platform will be discussed: poor passwords, vulnerabilities, malware/crimeware, insider threat, and mismanagement. Every organization needs a cybersecurity strategy. An effective strategy requires that you understand the problems as well as the solutions to those problems. Only then can you prioritize your limited cybersecurity resources. Managers and technicians alike will gain valuable insight in this non-technical talk.

Five Key Steps for Building an AppSec Program

Frank Kim & Eric Johnson

How do organizations take control of their application security? Chances are, at any given moment, your organization's applications are under attack. The bad guys see your applications as the front door, and a single bad line of code allows them entry. Through a mobile app, web application, or REST API, attackers can pivot to a backend database, your business partner's workstation, or even a payment processing vendor. As development teams continue to push new applications to web, mobile, and cloud environments, the need for an application security program is at an all-time high. Here's the problem: the application security space has nearly twice as many job openings as candidates. For every 100 developers, there are roughly 10 operations team members and only one security professional. Explore the real-world impact of application security breaches, discuss some alarming statistics and trends, and walk through a series of practical steps for building security into applications from the beginning. Attendees will walk away with actionable ideas and recommended practical tools to help improve their application security program.

GIAC Certifications

Jeff Frisk

GIAC certifications are the premier certifications for information security professionals. More than 30 GIAC certifications align with SANS training and ensure mastery in critical, specialized InfoSec domains. GIAC certifications provide the highest and most rigorous assurance of cybersecurity knowledge and skill available to industry, government, and military clients across the world. Join us for an informational presentation along with a Q&A session. We'll cover everything from why you should get certified to what testing looks like, how to keep certifications current, and more. GIAC staff will be present to answer your questions before and after the presentation.

Three Keys to Mobile Security: Are You Doing Everything You Can to Protect Your Apps?

Gregory Leonard

The threat landscape against mobile applications continues to grow. Malicious apps are still being discovered in the Apple and Google Play app stores, and questions continue to grow about how well protected mobile users really are. To combat this increasing threat landscape, mobile devices are providing new hardware and software features to help protect users from exploitation. We will discuss how developers can use features such as fingerprint scanning, on-device cryptography, and MDM/MAM to provide a secure environment for users and their data.

SANS

The SANS Voucher Program allows organizations to manage their training budget from a single SANS Account, potentially receive bonus funds based on their investment level, and centrally administer their training.

www.sans.org/vouchers

VOUCHER PROGRAM

Training Investment & Bonus Funds

To open a Voucher Account, an organization pays an agreed-upon training investment. Based on the amount of the training investment, an organization could be eligible to receive bonus funds.

The investment and bonus funds:

- Can be applied to **any live or online SANS training course, SANS Summit, GIAC certification, or certification renewal***
- Can be increased at any time by making additional investments
- Need to be utilized within 12 months, however, the term can be extended by investing additional funds before the end of the 12-month term

*Current exceptions are the Partnership Program, Security Awareness Training, and SANS workshops hosted at events and conferences run by other companies.

Flexibility & Control

The online SANS Admin Tool allows the organization's Program Administrator to manage the account at any time from anywhere.

With the SANS Admin Tool, the Administrator can:

- Approve student enrollment and manage fund usage
- View fund usage in real time
- View students' certification status and test results
- Obtain OnDemand course progress by student per course

Getting Started

Complete and submit the form online at **www.sans.org/vouchers** and a SANS representative in your region will contact you within 24 business hours.

Get started today and within as little as one week, we can create your Account and your employees can begin their training.

By creating a Voucher Account, your organization can:

- Simplify the procurement process with a single invoice and payment
- Easily change course attendees if previous plans change
- Lock-in your hard fought training budget and utilize it over time
- Control how, where, and for whom funds are spent
- Allow employees to register for training while managing approvals centrally

Future Training Events

Security West — San Diego, CA — May 9-18

Northern Virginia – Reston	Reston, VA	May 21-26
Atlanta	Atlanta, GA	May 30 - June 4
Houston	Houston, TX	June 5-10
San Francisco Summer	San Francisco, CA	June 5-10
Rocky Mountain	Denver, CO	June 12-17
Charlotte	Charlotte, NC	June 12-17
Minneapolis	Minneapolis, MN	June 19-24
Columbia	Columbia, MD	June 26 - July 1
Los Angeles - Long Beach	Long Beach, CA	July 10-15

SANSFIRE — Washington, DC — July 22-29

San Antonio	San Antonio, TX	Aug 6-11
Boston	Boston, MA	Aug 7-12
New York City	New York, NY	Aug 14-19
Salt Lake City	Salt Lake City, UT	Aug 14-19
Chicago	Chicago, IL	Aug 21-26
Virginia Beach	Virginia Beach, VA	Aug 21 - Sep 1
Tampa – Clearwater	Clearwater, FL	Sep 5-10
San Francisco	San Francisco, CA	Sep 5-10

Network Security — Las Vegas, NV — Sep 10-17

Future Summit Events

Automotive Cybersecurity	Detroit, MI	May 1-8
Security Operations Center	Washington, DC	June 5-12
Digital Forensics	Austin, TX	June 22-29
ICS & Energy	Houston, TX	July 10-15
Security Awareness	Nashville, TN	July 31 - Aug 9

Future Community SANS Events

Local, single-course events are also offered throughout the year via SANS Community. Visit **www.sans.org/community** for up-to-date Community course information.

Hotel Information

Washington Marriott Wardman Park
2660 Woodley Road, NW
Washington, DC 20008
Phone: 202-328-2000
www.sans.org/event/sansfire-2017/location

An uptown Washington DC hotel at the Woodley Park Metro

When you arrive at the Washington Marriott Wardman Park, you'll find a charming neighborhood in the heart of Washington, DC filled with amazing restaurants and quaint shops. Just a few steps away, you'll discover the funky stores and ethnic cuisine of Adams Morgan or the exciting night life of Dupont Circle. Head north to hear the sounds of animals coming from the National Zoo. Or venture into the hotel's natural surroundings to enjoy a quiet hike or invigorating run through Rock Creek Park. With a Metro stop just outside the doors and area airports close by, it's a premier city destination just two Metro stops from everything DC has to offer. We believe that brilliant meetings begin with brilliant space and we offer an astounding 195,000 square feet of versatile space that can be customized for groups of all sizes. It's an unmatched place to meet where accommodating venues and equally helpful planners can bring any group's unique ideas to life.

Special Hotel Rates Available

A special discounted rate of $209.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and fitness center access and are only available through June 30, 2017.

Top 5 reasons to stay at the Washington Marriott Wardman Park

1 All SANS attendees receive complimentary high-speed Internet when booking in the SANS block.

2 No need to factor in daily cab fees and the time associated with travel to alternate hotels.

3 By staying at the Washington Marriott Wardman Park, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.

4 SANS schedules morning and evening events at the Washington Marriott Wardman Park that you won't want to miss!

5 Everything is in one convenient location!

Register online at

www.sans.org/sansfire

We recommend you register early to ensure you get your first choice of courses.

Registration Information

Select your course or courses and indicate whether you plan to test for GIAC certification.

If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with Internet access must complete the online registration form. We do not take registrations by phone.

Pay Early and Save*

Use code **EarlyBird17** when registering early

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**5-31-17**	**$400.00**	**6-21-17**	**$200.00**

*Some restrictions apply. Early-bird discounts do not apply to Hosted courses.

SANS SIMULCAST

To register for a SANSFIRE 2017 Simulcast course, please visit **www.sans.org/event/sansfire-2017/attend-remotely**

Cancellation & Access Policy:

If an attendee must cancel, a substitute may attend instead. Substitution requests can be made at any time prior to the event start date. All substitution requests must be submitted by email to **registration@sans.org**. If an attendee must cancel and no substitute is available, a refund can be issued for any received payments by **June 28, 2017**. A credit memo can be requested up to the event start date. All cancellation requests must be submitted in writing by mail or fax and received by the stated deadlines. Payments will be refunded by the method that they were submitted. Processing fees will apply.

SANSFIRE 2017 REGISTRATION FEES

Register online at www.sans.org/sansfire

If you don't wish to register online, please call 301-654-SANS (7267) 9:00am-8:00pm (Mon-Fri) EST and we will fax or mail you an order form.

Job-Based Long Courses

		Paid before 5-31-17	Paid before 6-21-17	Paid after 6-21-17	Add GIAC Cert	Add OnDemand	Add NetWars Continuous
☐ SEC301	Intro to Information Security	$4,730	$4,930	$5,130	☐ $689	☐ $689	☐ $1,199
☐ SEC401	Security Essentials Bootcamp Style	$5,510	$5,710	$5,910	☐ $689	☐ $689	☐ $1,199
☐ SEC501	Advanced Security Essentials – Enterprise Defender	$5,510	$5,710	$5,910	☐ $689	☐ $689	☐ $1,199
☐ SEC503	Intrusion Detection In-Depth	$5,510	$5,710	$5,910	☐ $689	☐ $689	☐ $1,199
☐ SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling	$5,510	$5,710	$5,910	☐ $689	☐ $689	☐ $1,199
☐ SEC505	Securing Windows and PowerShell Automation	$5,420	$5,620	$5,820	☐ $689	☐ $689	☐ $1,199
☐ SEC506	Securing Linux/Unix	$5,510	$5,710	$5,910	☐ $689	☐ $689	☐ $1,199
☐ SEC511	Continuous Monitoring and Security Operations	$5,510	$5,710	$5,910	☐ $689	☐ $689	☐ $1,199
☐ SEC542	Web App Penetration Testing and Ethical Hacking	$5,510	$5,710	$5,910	☐ $689	☐ $689	☐ $1,199
☐ SEC550	Active Defense, Offensive Countermeasures, and Cyber Deception	$4,730	$4,930	$5,130			☐ $1,199
☐ SEC560	Network Penetration Testing and Ethical Hacking	$5,510	$5,710	$5,910	☐ $689	☐ $689	☐ $1,199
☐ SEC561	Immersive Hands-On Hacking Techniques	$5,510	$5,710	$5,910			☐ $1,199
☐ SEC566	Implementing and Auditing the Critical Security Controls – In-Depth	$4,730	$4,930	$5,130	☐ $689	☐ $689	☐ $1,199
☐ SEC573	Automating Information Security with Python ***NEW!***	$5,510	$5,710	$5,910	☐ $689		☐ $1,199
☐ SEC575	Mobile Device Security and Ethical Hacking	$5,510	$5,710	$5,910	☐ $689	☐ $689	☐ $1,199
☐ SEC579	Virtualization and Software-Defined Security ***NEW!***	$4,730	$4,930	$5,130			☐ $1,199
☐ SEC642	Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques	$5,510	$5,710	$5,910		☐ $689	☐ $1,199
☐ SEC660	Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	$5,510	$5,710	$5,910	☐ $689	☐ $689	☐ $1,199
☐ FOR408	Windows Forensic Analysis	$5,510	$5,710	$5,910	☐ $689	☐ $689	☐ $1,199
☐ FOR508	Advanced Digital Forensics, Incident Response, and Threat Hunting	$5,510	$5,710	$5,910	☐ $689	☐ $689	☐ $1,199
☐ FOR526	Memory Forensics In-Depth	$5,510	$5,710	$5,910			☐ $1,199
☐ FOR572	Advanced Network Forensics and Analysis ***NEW!***	$5,510	$5,710	$5,910	☐ $689	☐ $689	☐ $1,199
☐ FOR578	Cyber Threat Intelligence	$4,730	$4,930	$5,130		☐ $689	☐ $1,199
☐ FOR585	Advanced Smartphone Forensics	$5,510	$5,710	$5,910	☐ $689	☐ $689	☐ $1,199
☐ FOR610	Reverse-Engineering Malware: Malware Analysis Tools and Techniques	$5,510	$5,710	$5,910	☐ $689	☐ $689	☐ $1,199
☐ MGT414	SANS Training Program for CISSP® Certification	$4,840	$5,040	$5,240	☐ $689	☐ $689	☐ $1,199
☐ MGT512	SANS Security Leadership Essentials for Managers with Knowledge Compression™	$5,130	$5,330	$5,530	☐ $689	☐ $689	☐ $1,199
☐ MGT514	IT Security Strategic Planning, Policy, and Leadership	$4,730	$4,930	$5,130		☐ $689	☐ $1,199
☐ MGT517	Managing Security Operations: Detection, Response, and Intelligence ***NEW!***	$5,130	$5,330	$5,530			☐ $1,199
☐ MGT525	IT Project Management, Effective Communication, and PMP® Exam Prep	$4,840	$5,040	$5,240	☐ $689		☐ $1,199
☐ DEV522	Defending Web Applications Security Essentials	$5,420	$5,620	$5,820	☐ $689	☐ $689	☐ $1,199
☐ DEV541	Secure Coding in Java/JEE: Developing Defensible Applications	$4,240	$4,440	$4,640	☐ $689	☐ $689	☐ $1,199
☐ DEV544	Secure Coding in .NET: Developing Defensible Applications	$4,240	$4,440	$4,640	☐ $689	☐ $689	☐ $1,199
☐ AUD507	Auditing & Monitoring Networks, Perimeters, and Systems	$5,420	$5,620	$5,820	☐ $689	☐ $689	☐ $1,199
☐ LEG523	Law of Data Security and Investigations	$4,730	$4,930	$5,130	☐ $689	☐ $689	☐ $1,199
☐ ICS410	ICS/SCADA Security Essentials	$5,050	$5,250	$5,450	☐ $689	☐ $689	☐ $1,199

PMP® is a registered trademark of the Project Management Institute, Inc.

Skill-Based Short Courses

		Course fee if taking a 4-6 day course	Course fee
☐ SEC440	Critical Security Controls: Planning, Implementing, and Auditing	$1,770	$2,360
☐ SEC524	Cloud Security Fundamentals	$1,770	$2,360
☐ SEC546	IPv6 Essentials	$1,770	$2,360
☐ SEC567	Social Engineering for Penetration Testers	$1,770	$2,360
☐ SEC580	Metasploit Kung Fu for Enterprise Pen Testing	$1,770	$2,360
☐ MGT305	Technical Communication and Presentation Skills for Security Professionals	$1,030	$1,370
☐ MGT415	A Practical Introduction to Cybersecurity Risk Management	$1,770	$2,360
☐ MGT433	Securing The Human: How to Build, Maintain & Measure a High-Impact Awareness Program	$1,770	$2,360
☐ DEV531	Defending Mobile Applications Security Essentials ***NEW!***	$1,770	$2,360
☐ DEV534	Secure DevOps: A Practical Introduction ***NEW!***	$1,770	$2,360
☐ SPECIAL	Core NetWars Experience – Tournament Entrance Fee	FREE	$1,520
☐ SPECIAL	DFIR NetWars Tournament – Tournament Entrance Fee	FREE	$1,520
☐ SPECIAL	Cyber Defense NetWars Competition – Tournament Entrance Fee ***NEW!***	FREE	$1,520

Pay for any long course using the code EarlyBird17 at checkout by:
5-31-17 to get $400 OFF* / 6-21-17 to get $200 OFF*

***Some restrictions apply. Early-bird discounts do not apply to Hosted courses.**

Create a **SANS Account** today to enjoy these FREE resources:

WEBCASTS

Ask The Expert Webcasts – SANS experts bring current and timely information on relevant topics in IT Security.

Analyst Webcasts – A follow-on to the SANS Analyst Program, Analyst Webcasts provide key information from our whitepapers and surveys.

WhatWorks Webcasts – The SANS WhatWorks webcasts bring powerful customer experiences showing how end users resolved specific IT Security issues.

Tool Talks – Tool Talks are designed to give you a solid understanding of a problem, and how a vendor's commercial tool can be used to solve or mitigate that problem.

NEWSLETTERS

NewsBites – Twice weekly, high-level executive summary of the most important news relevant to cybersecurity professionals

OUCH! – The world's leading monthly, free security awareness newsletter designed for the common computer user

@RISK: The Consensus Security Alert – A reliable weekly summary of (1) newly discovered attack vectors, (2) vulnerabilities with active new exploits, (3) how recent attacks worked, and (4) other valuable data

OTHER FREE RESOURCES

- InfoSec Reading Room
- Top 25 Software Errors
- 20 Critical Controls
- Security Policies
- Intrusion Detection FAQs
- Tip of the Day
- Security Posters
- Thought Leaders
- 20 Coolest Careers
- Security Glossary
- SCORE (Security Consensus Operational Readiness Evaluation)

www.sans.org/account

NALT-BRO-SANSFIRE17-STD