SANS

CDI

THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

CYBER DEFENSE INITIATIVE 2015

Washington, DC
December 12-19

POWERED BY

NETWARS

INCLUDING THE
4TH ANNUAL
Tournament of Champions

GIAC Approved Training

"SANS has the best instructors available. Other training never comes close."

-Steve Sauro,
McDermott Will & Emery

Attend CDI with 1,000+ colleagues from around the world.

30+ Courses
Digital Forensics
Penetration Testing
Network & Software Security
Industrial Control Systems
Cybersecurity Management

2 NetWars Tournaments

15 Bonus Sessions

Register at
sans.org/cdi

Dear Colleagues,

Ed Skoudis

I'm Ed Skoudis and honored to extend a warm invitation to you to attend the magnificent **2015 SANS Cyber Defense Initiative** (CDI) event in Washington, DC December 12-19.

As you know, SANS is recognized around the world as the best place to develop the deep, hands-on cybersecurity skills most in need right now. Every year, SANS hosts the CDI event as a showcase for exceptional courses and evening events that you can't find anywhere else.

An impressive list of 33 information security courses will be taught by SANS' top instructors at CDI this year, and many of those courses can prepare you for a prestigious **GIAC** certification. You can also bundle four months of **OnDemand** with your live course at a discounted rate to extend your study. Review the full course and event details inside this catalog to realize what you'll gain from attending, and then visit **sans.org/cdi** to register as soon as possible to receive an earlybird discount!

Your CDI 2015 course registration will also give you special access to a full spectrum of evening **NetWars Tournaments!** The event is powered not only by a CORE NetWars challenge, but also a DFIR (digital forensics and incident response) NetWars challenge and the 4th annual **NetWars Tournament of Champions**. Be there live to test your skills, to battle your fellow students in a seriously fun and engaging environment, and to see who claims the title of 2015 NetWars Champion!

Multiple hot-topic talks each night will round out your agenda for the week, along with many opportunities to mingle with instructors, mentors, fellow students, and vendors.

Your CDI dance card will be full and we guarantee that you'll benefit from each super relevant and hyper-engaging component of this training event. Our award-winning faculty has proven that they understand the challenges you face on a daily basis and they are eager to be there to help you learn the vital skills needed to secure your environment. We're going to have an awesome time together at CDI, and I sincerely hope that you'll join us.

I look forward to welcoming you to CDI 2015!

Ed Skoudis
SANS Fellow
sans.org/cdi

PS – Don't forget that your live, hands-on SANS training experience can also count as progress towards a Graduate Certificate or Masters Degree in Information Security Management or Engineering via the **SANS Technology Institute**. See page 57 for more details about this opportunity.

Information Security

Information security professionals are responsible for research and analysis of security threats that may affect an organization's assets, products, or technical specifications. These security professionals will dig deeper into technical protocols and specifications related to security threats than most of their peers, identifying strategies to defend against attacks by gaining an intimate knowledge of the threats.

SAMPLE JOB TITLES
- Cybersecurity analyst
- Cybersecurity engineer
- Cybersecurity architect

CORE COURSES

TECHNICAL INTRODUCTORY	CORE	IN-DEPTH
SEC301 Intro to Information Security **GISF**	**SEC401** Security Essentials Bootcamp Style **GSEC**	**SEC501** Advanced Security Essentials – Enterprise Defender **GCED**

Penetration Testing/Vulnerability Assessment

CORE COURSES SEC301 (GISF) ▸ SEC401 (GSEC)

SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling **GCIH**

NETWORK & EXPLOITS	WEB	LAB-CENTERED	MOBILE/WIRELESS
SEC560 Network Penetration Testing and Ethical Hacking **GPEN**	**SEC542** Web App Penetration Testing and Ethical Hacking **GWAPT**	**SEC561** Immersive Hands-on Hacking Techniques	**SEC575** Mobile Device Security and Ethical Hacking **GMOB**
SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking **GXPN**	**SEC642** Advanced Web App Penetration Testing and Ethical Hacking	**SEC562** CyberCity Hands-on Kinetic Cyber Range Exercise	**SEC617** Wireless Ethical Hacking, Penetration Testing & Defenses **GAWN**
SEC760 Advanced Exploit Development for Penetration Testers			

SPECIALIZATION

SEC573 Python for Penetration Testers

SEC580 Metasploit Kung Fu for Enterprise Pen Testing

Because offense must inform defense, these experts provide enormous value to an organization by applying attack techniques to find security vulnerabilities, analyze their business risk implications, write modern exploits, and recommend mitigations before those vulnerabilities are exploited by real-world attackers.

SAMPLE JOB TITLES
- Penetration tester
- Vulnerability assessor
- Ethical hacker
- Red/Blue team member
- Cyberspace engineer

Risk and Compliance/Auditing/Governance

SEC566 Implementing and Auditing the Critical Security Controls – In-Depth **GCCC**

AUD507 Auditing & Monitoring Networks, Perimeters, and Systems **GSNA**

These experts assess and report risks to the organization by measuring compliance with policies, procedures, and standards. They recommend improvements to make the organization more efficient and profitable through continuous monitoring of risk management.

SAMPLE JOB TITLES
- Auditor
- Compliance officer

Security Operations Center/Intrusion Detection

SAMPLE JOB TITLES
- Intrusion detection analyst
- Security Operations Center analyst/engineer
- CERT member
- Cyber threat analyst

CORE COURSES
SEC301 (GISF) ▸ SEC401 (GSEC)

SEC504
Hacker Tools, Techniques, Exploits, and Incident Handling
GCIH

The Security Operations Center (SOC) is the focal point for safeguarding against cyber-related incidents, monitoring security, and protecting assets of the enterprise network and endpoints. SOC analysts are responsible for enterprise situational awareness and continuous surveillance, including monitoring traffic, blocking unwanted traffic to and from the Internet, and detecting any type of attack. Point solution security technologies are the starting point for hardening the network against possible intrusion attempts.

ENDPOINT MONITORING

SEC501
Advanced Security Essentials – Enterprise Defender
GCED

FOR508
Advanced Digital Forensics and Incident Response
GCFA

NETWORK MONITORING

SEC502
Perimeter Protection In-Depth
GPPA

SEC503
Intrusion Detection In-Depth
GCIA

FOR572
Advanced Network Forensics and Analysis
GNFA

SEC511
Continuous Monitoring and Security Operations
GMON

SEC550
Active Defense, Offensive Countermeasures, and Cyber Deception

THREAT INTELLIGENCE

FOR578
Cyber Threat Intelligence

Network Operations Center, System Admin, Security Architecture

SAMPLE JOB TITLES
- System/IT administrator
- Security administrator
- Security architect/engineer

A Network Operations Center (NOC) is where IT professionals supervise, monitor, and maintain the enterprise network. The NOC is the focal point for network troubleshooting, software distribution and updating, router and system management, performance monitoring, and coordination with affiliated networks. The NOC analysts work hand-in-hand with the Security Operations Center, which safeguards the enterprise and continuously monitors threats against it.

CORE COURSES
SEC301 (GISF) ▸ SEC401 (GSEC) ▸ SEC501 (GCED)

SEC505
Securing Windows with PowerShell and the Critical Security Controls
GCWN

SEC506
Securing Linux/Unix
GCUX

SEC566
Implementing and Auditing the Critical Security Controls – In-Depth
GCCC

SEC579
Virtualization and Private Cloud Security

Development – Secure Development

Securing the Human for Developers – STH.Developer
Application Security Awareness Modules

DEV522
Defending Web Applications Security Essentials
GWEB

DEV541
Secure Coding in Java/JEE: Developing Defensible Applications
GSSP-JAVA

DEV544
Secure Coding in .NET: Developing Defensible Applications
GSSP-.NET

SAMPLE JOB TITLES
- Developer
- Software architect
- QA tester
- Development manager

The security-savvy software developer leads all developers in creating secure software and implementing secure programming techniques that are free from logical design and technical implementation flaws. This expert is ultimately responsible for ensuring customer software is free from vulnerabilities that can be exploited by an attacker.

SPECIALIZATION

SEC542
Web App Penetration Testing and Ethical Hacking
GWAPT

SEC642
Advanced Web App Penetration Testing and Ethical Hacking

Industrial Control Systems

ICS-focused courses are designed to equip both security professionals and control system engineers with the knowledge and skills they need to safeguard critical infrastructure.

SAMPLE JOB TITLES
- IT & OT support staff
- IT & OT cybersecurity
- ICS engineer

ICS410
ICS/SCADA Security Essentials
GICSP

ICS515
ICS Active Defense and Incident Response

HOSTED
Assessing and Exploiting Control Systems

HOSTED
Critical Infrastructure and Control System Cybersecurity

Cyber or IT Security Management

FOUNDATIONAL

MGT512
SANS Security Leadership Essentials For Managers with Knowledge Compression™
GSLC

MGT525
IT Project Management, Effective Communication, and PMP® Exam Prep
GCPM

MGT414
SANS Training Program for CISSP® Certification
GISP

CORE

MGT514
IT Security Strategic Planning, Policy, and Leadership

MGT535
Incident Response Team Management

LEG523
Law of Data Security and Investigations
GLEG

SPECIALIZATION

MGT433
Securing The Human: How to Build, Maintain & Measure a High-Impact Awareness Program

AUD507
Auditing & Monitoring Networks, Perimeters, and Systems
GSNA

HOSTED
Health Care Security Essentials

SAMPLE JOB TITLES
- CISO
- Cybersecurity manager/officer
- Security director

Management of people, processes, and technologies is critical for maintaining proactive enterprise situational awareness and for the ongoing success of continuous monitoring efforts. These managers must have the leadership skills, current knowledge, and best practice examples to make timely and effective decisions that benefit the entire enterprise information infrastructure.

Incident Response

When the security of a system or network has been compromised, the incident responder is the first-line defense during the breach. The responders not only have to be technically astute, they must be able to handle stress under fire while navigating people, processes, and technology to help respond to and mitigate a security incident.

CORE COURSES
SEC301 (GISF) ▸ SEC401 (GSEC)

SEC504
Hacker Tools, Techniques, Exploits, and Incident Handling
GCIH

SPECIALIZATION

FOR526
Memory Forensics In-Depth

MGT535
Incident Response Team Management

NETWORK ANALYSIS

SEC503
Intrusion Detection In-Depth
GCIA

FOR572
Advanced Network Forensics and Analysis
GNFA

ENDPOINT ANALYSIS

FOR408
Windows Forensic Analysis
GCFE

FOR508
Advanced Digital Forensics and Incident Response
GCFA

MALWARE ANALYSIS

FOR610
Reverse-Engineering Malware: Malware Analysis Tools and Techniques
GREM

SAMPLE JOB TITLES
- Security analyst/engineer
- SOC analyst
- Cyber threat analyst
- CERT member
- Malware analyst

Digital Forensic Investigations and Media Exploitation

FOR408
Windows Forensic Analysis
GCFE

SEC504
Hacker Tools, Techniques, Exploits, and Incident Handling
GCIH

FOR508
Advanced Digital Forensics and Incident Response
GCFA

FOR585
Advanced Smartphone Forensics

FOR518
Mac Forensic Analysis

FOR526
Memory Forensics In-Depth

FOR610
Reverse-Engineering Malware: Malware Analysis Tools and Techniques
GREM

SAMPLE JOB TITLES
- Computer crime investigator
- Law enforcement
- Digital investigations analyst
- Media exploitation analyst
- Information technology litigation support and consultant
- Insider threat analyst

With today's ever-changing technologies and environments, it is inevitable that every organization will deal with cybercrime, including fraud, insider threats, industrial espionage, and phishing. Government organizations also need skilled personnel to perform media exploitation and recover key intelligence available on adversary systems. To help solve these challenges, organizations are hiring digital forensic professionals and relying on cybercrime law enforcement agents to piece together a comprehensive account of what happened.

Participate in either the CORE or DFIR NetWars Tournament at SANS Cyber Defense Initiative 2015 for FREE!

NETWARS

CORE NETWARS TOURNAMENT

DFIR NETWARS TOURNAMENT

CORE NetWars

The CORE NetWars Tournament 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

In-Depth, Hands-On InfoSec Skills – Embrace the Challenge – CORE NetWars

DFIR NetWars

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

Challenge Yourself Before the Enemy Does – DFIR NetWars

Both NetWars competitions will be played over two evenings: December 17-18, 2015

Prizes will be awarded at the conclusion of the games.

REGISTRATION IS LIMITED AND IS FREE

for students attending any long course at SANS CDI 2015 *(NON-STUDENT ENTRANCE FEE IS $1,450).*

Register at sans.org/event/cyber-defense-initiative-2015/courses

Courses-at-a-Glance

For an up-to-date course list please check the website at sans.org/event/cyber-defense-initiative-2015/schedule

		SAT 12/12	SUN 12/13	MON 12/14	TUE 12/15	WED 12/16	THU 12/17	FRI 12/18	SAT 12/19
SEC301	Intro to Information Security			PAGE 8					
SEC401	Security Essentials Bootcamp Style *SIMULCAST*			PAGE 10					
SEC440	Critical Security Controls: Planning, Implementing and Auditing	PAGE 52							
SEC501	Advanced Security Essentials – Enterprise Defender			PAGE 12					
SEC503	Intrusion Detection In-Depth			PAGE 14					
SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling			PAGE 16					
SEC505	Securing Windows with PowerShell and the Critical Security Controls *SIMULCAST*			PAGE 18					
SEC511	Continuous Monitoring and Security Operations			PAGE 20					
SEC550	Active Defense, Offensive Countermeasures and Cyber Deception **NEW!**			PAGE 6					
SEC560	Network Penetration Testing and Ethical Hacking *SIMULCAST*			PAGE 22					
SEC566	Implementing and Auditing the Critical Security Controls – In-Depth			PAGE 24					
SEC575	Mobile Device Security and Ethical Hacking			PAGE 26					
SEC579	Virtualization and Private Cloud Security			PAGE 28					
SEC580	Metasploit Kung Fu for Enterprise Pen Testing	PAGE 52							
SEC660	Advanced Penetration Testing, Exploit Writing, and Ethical Hacking			PAGE 30					
FOR408	Windows Forensic Analysis			PAGE 32					
FOR508	Advanced Digital Forensics and Incident Response *SIMULCAST*			PAGE 34					
FOR572	Advanced Network Forensics and Analysis			PAGE 36					
FOR578	Cyber Threat Intelligence **NEW!**			PAGE 7					
FOR610	Reverse-Engineering Malware: Malware Analysis Tools and Techniques			PAGE 38					
MGT414	SANS Training Program for CISSP® Certification			PAGE 40					
MGT415	A Practical Introduction to Cyber Security Risk Management **NEW!**	PAGE 53							
MGT433	Securing The Human: How to Build, Maintain, and Measure a High-Impact Awareness Program *SIMULCAST*	PAGE 53							
MGT512	SANS Security Leadership Essentials for Managers with Knowledge Compression™			PAGE 42					
MGT514	IT Security Strategic Planning, Policy, and Leadership **NEW!**			PAGE 44					
MGT535	Incident Response Team Management	PAGE 53							
AUD507	Auditing & Monitoring Networks, Perimeters, and Systems			PAGE 46					
DEV544	Secure Coding in .NET: Developing Defensible Applications			PAGE 48					
LEG523	Law of Data Security and Investigations *SIMULCAST*			PAGE 49					
ICS410	ICS/SCADA Security Essentials *SIMULCAST*			PAGE 50					
ICS515	ICS Active Defense and Incident Response **NEW!**			PAGE 5					
HOSTED	(ISC)²® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Training Seminar			PAGE 51					
HOSTED	Physical Penetration Testing	PAGE 51							
	NetWars Tournaments (CORE & DFIR)						PAGE 2		

CONTENTS

The Value of SANS Training and *YOU*

EXPLORE

- Read this brochure and note the courses that will enhance your role in your organization
- Use the *Career Roadmap* in this brochure (sans.org/media/security-training/roadmap.pdf) to plan your growth in your chosen career path

RELATE

- Consider how security needs in your workplace will be met with the knowledge you'll gain in a SANS course
- Know that the education you receive will make you an expert resource for your team

VALIDATE

- Pursue a GIAC Certification after your training to validate your new expertise
- Add a NetWars challenge to your SANS experience to prove your hands-on skills

SAVE

- Register early to pay less using early-bird specials
- Consider group discounts or bundled course packages to make the most of your training budget

ADD VALUE

- Network with fellow security experts in your industry
- Prepare thoughts and questions before arriving to share with the group
- Attend SANS@Night talks and activities to gain even more knowledge and experience from instructors and peers alike

ALTERNATIVES

- If you cannot attend a live training event in person, attend the courses virtually via SANS Simulcast
- Use SANS OnDemand or vLive to complete the same training online from anywhere in the world, at any time

ACT

- Bring the value of SANS training to your career and organization by registering for a course today, or contact us at 301-654-SANS with further questions

Return on Investment

SANS live training is recognized as the best resource in the world for information security education. With SANS, you gain significant returns on your InfoSec investment. Through our intensive immersion classes, our training is designed to help your staff master the practical steps necessary for defending systems and networks against the most dangerous threats – the ones being actively exploited.

REMEMBER

the SANS promise:

You will be able to apply our information security training the day you get back to the office!

INDUSTRIAL CONTROL SYSTEMS 515

ICS Active Defense and Incident Response

NEW

Five-Day Program
Mon, Dec 14 - Fri, Dec 18
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Robert M. Lee

"ICS environments are unique and require specialized skills and processes to effectively manage the threats and vulnerabilities."
-John Ballentine, EthosEnergy

"Awesome!! In this course, being my 6th SANS course, Robert M. Lee demonstrated and reiterated the fact that SANS has world's best instructors!! The course was like a catalyst. It boosted my knowledge about the threats facing ICS environments, and provided me with a framework to actively defend these threats."
-Srinath Kannan, Accenture

ICS515: ICS Active Defense and Incident Response will empower students to understand their networked industrial control system (ICS) environment, monitor it for threats, perform incident response against identified threats, and learn from interactions with the adversary to enhance network security. This process of monitoring, responding to, and learning from threats is known as "active defense." It is the approach needed to appropriately counter advanced adversaries targeting ICS, as has been seen with malware such as Stuxnet, HAVEX, and BlackEnergy2. Students can expect to come out of this course fully understanding how to to deconstruct targeted ICS attacks, with a focus on delivery methods and observable attributes. This knowledge demystifies adversary capabilities and gives actionable recommendations to defenders. The course uses a hands-on approach that shows real-world malware and breaks down cyber attacks on ICS from start to finish. Students will gain a practical and technical understanding of concepts such as generating and using threat intelligence, performing network security monitoring, and executing threat triage and incident response to ensure the safety and reliability of operations. The strategy presented in the course serves as a basis for ICS organizations looking to show that defense is doable.

Who Should Attend

- Information technology and operational technology (IT and OT) personnel
- Cybersecurity personnel
- IT- and OT-support personnel
- ICS incident responders
- ICS engineers
- Security Operations Center personnel

What You Will Receive

A fully functioning ICS515 CYBATIWorks Mini-Kit that students take with them after the class. The kit includes a Raspberry PI that functions as a PLC, physical components and attachments for I/O, a virtual machine with commercial control system demonstration software from Rex Controls and PeakHMI, and industrial protocols and software including OPC, ModbusTCP, DNP3, and more.

Author Statement

"This class was developed from my experiences in the U.S. intelligence community and within the control system community dealing with advanced adversaries targeting industrial control systems. It is the class I wish I would have had available to me while protecting infrastructure against these adversaries. It is exactly what you'll need to maintain secure and reliable operations in the face of determined threats. ICS515 will empower you to prove that defense is doable."
-Robert M. Lee

Robert M. Lee *SANS Certified Instructor*

Robert M. Lee is a co-founder at the critical infrastructure cybersecurity company Dragos Security LLC where he has a passion for control system packet analysis, digital forensics, and threat intelligence research. He is the course author of SANS ICS515 and the co-author of SANS FOR578. He is a passionate educator although he should not be confused with the other Rob Lee at SANS - that Rob Lee is cooler but has less hair. Robert obtained his start in cybersecurity in the U.S. Air Force where he currently serves as a Cyber Warfare Operations Officer. He has performed defense, intelligence, and attack missions in various government organizations including the establishment of a first-of-its-kind ICS/SCADA cyber threat intelligence and intrusion analysis mission. Robert routinely writes articles and journals in publications such as Control Engineering, Air and Space Power Journal, Wired, and Passcode. He is also a frequent speaker at conferences and is currently pursuing his PhD at Kings College London with research into the cybersecurity of control systems. Robert is also the author of the book *SCADA and Me* and the web-comic www.LittleBobbyComic.com. @RobertMLee

SECURITY 550

Active Defense, Offensive Countermeasures, and Cyber Deception

NEW

Five-Day Program
Mon, Dec 14 - Fri, Dec 18
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.

Who Should Attend

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

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.

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

"Bryce is an excellent instructor. His knowledge and delivery are exceptional."

-Chris Shipp,
DM Petroleum Operations Co.

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

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

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

FORENSICS 578

Cyber Threat Intelligence

NEW

Five-Day Program
Mon, Dec 14 - Fri, Dec 18
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Jake Williams

"This is an awesome course and long overdue. I like the way you have mixed the technical with the intelligence and this is the first time I've seen this done in a meaningful way. Amazing work!"

-Rowanne Mackie, Barclays

"Everyone claims to be doing and selling cyber threat intel – this course teaches what it actually is."

-Jeremy Quinn, Salesforce

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

FOR578: Cyber Threat Intelligence will help network defenders and incident responders:

- Construct and exploit threat intelligence to detect, respond, and defeat advanced persistent threats (APTs)
- Fully analyze successful and unsuccessful intrusions by advanced attackers
- Piece together intrusion campaigns, threat actors, and nation-state organizations
- Manage, share, and receive intelligence on APT adversary groups
- Generate intelligence from their own data sources and share it accordingly
- Identify, extract, and leverage intelligence from APT intrusions
- Expand upon existing intelligence to build profiles of adversary groups
- Leverage intelligence to better defend against and respond to future intrusions.

Who Should Attend

- Incident response team members
- Experienced digital forensic analysts who want to consolidate and expand their understanding of filesystem forensics, investigations of technically advanced adversaries, incident response tactics, and advanced intrusion investigations
- Security Operations Center Personnel and information security practitioners who support hunting operations that seek to identify attackers in their network environments
- Federal agents and law enforcement officials who want to master advanced intrusion investigations and incident response, and expand their investigative skills beyond traditional host-based digital forensics
- SANS FOR408, FOR572, FOR508, or FOR610 graduates looking to take their skills to the next level

Conventional network defenses such as intrusion detection systems and anti-virus tools focus on the vulnerability component of risk, and traditional incident response methodology pre-supposes a successful intrusion. However, the evolving sophistication of computer network intrusions has rendered these approaches insufficient to address the threats faced by modern networked organizations. Today's adversaries accomplish their goals using advanced tools and techniques designed to circumvent most conventional computer network defense mechanisms, go undetected during the intrusion, and then remain undetected on networks over long periods of time.

The collection, classification, and exploitation of knowledge about adversaries – collectively known as cyber threat intelligence – gives network defenders information superiority that can be 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. 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.

During a targeted attack, an organization needs a top-notch and cutting-edge incident response armed with the critical intelligence necessary to understand how adversaries operate and to combat the threat. **FOR578: Cyber Threat Intelligence** will train you and your team to determine, scope, and select resilient courses of action in response to such intrusions and data breaches.

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 performed by state-sponsored actors in 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

SECURITY 301

Intro to Information Security

Five-Day Program
Mon, Dec 14 - Fri, Dec 18
9:00am - 5:00pm
Laptop Required
30 CPEs
Instructor: Keith Palmgren

- GIAC Cert: GISF
- OnDemand Bundle

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

- Are you 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 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: Introduction 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 no prior knowledge of security and limited knowledge of technology. 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.***

"SANS teaches you the logic and how to apply it to the real world."
-Kyle Prather, Heartland Dental

"Excellent, fast-paced course – Keith is extremely knowledgeable. I'll coordinate my next training class for when he's the instructor!!"
-Rick Desnoyers, Flagstar Bank

"I very much appreciate the passion of the instructors. Their knowledge is incredible and the presentation of their knowledge is down-to-earth and helpful. SANS training is far better than privacy-related certification."
-Ron Hoffman, Mutual of Omaha

Keith Palmgren *SANS Certified Instructor*

Keith Palmgren is an IT Security professional with over 30 years of experience specializing in the IT security 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 11 computer security certifications (CISSP, GSEC, GCIH, GCED, GISF, CEH, Security+, Network+, A+, CTT+). @kpalmgren

301.1 HANDS ON: The Cornerstone of Security

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, authentication/authorization/accountability, and security awareness training.

301.2 HANDS ON: Cryptography & Wireless Security

Cryptography is one of the most complex issues faced by security practitioners. It 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? Finally, we take a brief look at several cryptographic applications. We won't get into the details of how Secure Shell (SSH) actually works, but you will leave the classroom knowing what that term means and what SSH is used for. In other words, you'll be able to discuss several crypto applications in a general sense and not be confused when someone brings them up. Following cryptography, we introduce the fundamentals of wireless security (WiFi and Bluetooth), and mobile device security (i.e., cell phones).

301.3 HANDS 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. Day three begins with a nontechnical 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 hubs, switches, and routers, and you'll finally grasp what is meant by terms like protocol, encapsulation, and tunneling. 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. We'll close out day three with a very simple explanation of common network attacks such as spoofing, man-in-the-middle, denial of service, and distributed denial of service.

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 "SPAM IQ" to more easily identify SPAM email messages
- Understand physical security issues and how they support cybersecurity
- Have an introductory level of knowledge regarding incident response, business continuity, and disaster recovery planning
- Install and use the following tools: Password Safe, Secunia PSI, Malwarebytes, and Syncback

301.4 HANDS ON: Security Technologies

Building on what we've learned about how networks function and common attacks against them, we start day four by introducing methods and technologies to manage, control, and secure those networks. Students will learn about the importance of configuration management on networks, the different types of malware, and how anti-malware works to protect us. Students will also gain an introductory knowledge of firewalls, intrusion detection and prevention, sniffers, and virtualization technologies. We will not deep dive into firewall technology, but students will become familiar with basic firewall terminology and techniques. We'll also look at methods for auditing network security and examine fundamental security techniques such as hardening operating systems.

301.5 HANDS ON: Protecting Assets

The final day of our SEC301 journey is all about protecting assets, mostly with a physical security theme but with some logical security included as well. We begin with the "meta security" discipline of operations security that looks at security issues throughout the organization, not just in the IT area. We then introduce the topic of safety and physical security. Students will become familiar with the concepts of data classification and data loss prevention. From there we move to an introductory look at incident response, including business continuity and disaster recovery planning. We'll close out with a brief discussion of social engineering so that students understand what it is and why it's so difficult to defend against.

SECURITY 401

Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Dec 14 - Sat, Dec 19
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Paul A. Henry

- GIAC Cert: GSEC
- Cyber Guardian
- STI Master's Program
- OnDemand Bundle
- DoDD 8570

ATTEND REMOTELY

SIMULCAST

If you are unable to attend this event, this course is also available via SANS Simulcast.

More info on page 59

"This was my first SANS course – I didn't know what to expect. Now that I've been through a course, I must say, the experience was fantastic!"
-Gary Hughes, Seagate Technology

Learn the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. 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.

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!

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

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

With the advanced persistent threat, 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.

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. Paul 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

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: 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 what can be done to test and protect a web server in your company.

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

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: Attack Methods; Firewalls and Perimeters; Honeypots; Host-based Protection; Network-based Intrusion Detection and Prevention; Risk Assessment and Auditing

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

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

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.

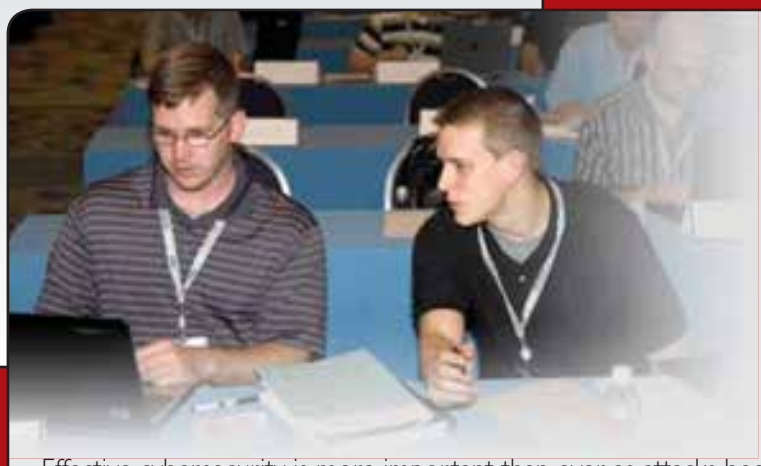
Topics: Linux Landscape; Permissions and User Accounts; Linux OS Security; Maintenance, Monitoring, and Auditing Linux; Linux Security Tools

SECURITY 501

Advanced Security Essentials – Enterprise Defender

Six-Day Program
Mon, Dec 14 - Sat, Dec 19
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Bryan Simon

- GIAC Cert: GCED
- STI Master's Program
- OnDemand Bundle
- DoDD 8570



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

"Great instructor with the ability to tie real-world threats to theory and practice."
-Bruce Henkel, Harris Corp.

"This course was most valuable. The demos and materials combined with the instructor's detailed explanation, experience, and recommendations, gave information I can apply immediately when I return to work."
-Rowley Molina, Altria

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.

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.

Bryan Simon *SANS Certified Instructor*

Bryan Simon is an internationally recognized expert in cybersecurity and 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 organizations such as 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 11 GIAC Certifications including GSEC, GCWN, GCIH, GCFA, GPEN, GWAPT, GAWN, GISP, GCIA, GCED, and GCUX. Bryan's scholastic achievements have resulted in the honor of sitting as a current member of the Advisory Board for the SANS Institute, and his acceptance into the prestigious SANS Cyber Guardian program. Bryan is a SANS Certified Instructor for SEC401: Security Essentials Bootcamp Style, SEC501: Advanced Security Essentials – Enterprise Defender, SEC505: Securing Windows with Powershell and the Critical Security Controls, and SEC511: Continuous Monitoring and Security Operations. @BryanOnSecurity

501.1 HANDS ON: Defensive Network Infrastructure

Protecting a network from attack starts with designing, building, and implementing a robust network infrastructure. Many aspects of implementing a defense-in-depth network are often overlooked because organizations focus on functionality. Achieving the proper balance between business drivers and core protection of information is difficult. 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

You Will Be Able To

- Identify the threats against network infrastructures and build defensible networks that minimize the impact of attacks
- Use the tools designed to analyze a network to both prevent 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
- Understand the six steps in the incident handling process and create and run an incident-handling capability
- 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

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)

SECURITY 503

Intrusion Detection In-Depth

SANS

Six-Day Program
Mon, Dec 14 - Sat, Dec 19
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Mike Poor

- GIAC Cert: GCIA
- Cyber Guardian
- STI Master's Program
- OnDemand Bundle
- DoDD 8570

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?

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 HTTP, so that you can intelligently examine network traffic for signs of an intrusion. You will get plenty of practice learning to configure and master different open-source tools like tcpdump, Wireshark, Snort, Bro, and many more. 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. In addition, most exercises include an "extra credit" stumper question intended to challenge even the most advanced student.

Industry expert Mike Poor has created a VMware distribution, Packetrix, specifically for this course. As the name implies, Packetrix contains many of the tricks of the trade to perform packet and traffic analysis. It is supplemented with demonstration "pcaps," which are files that contain network traffic. This allows students to follow along on their laptops with the class material and demonstrations. The pcaps also provide a good library of network traffic to use when reviewing the material, especially for certification.

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 often 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. The training will prepare you to put your new skills and knowledge to work immediately upon returning to a live environment.

Who Should Attend

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

"Today has been brilliant, bringing all of our skills together to achieve the challenge. I wish we could do this every day!"
-Hayley Roberts, MOD

"SEC503 covers the best processes for intrusion analysis and how to cut out most of the network noise and identify the important traffic. Mike Poor is a rock-star, and I look forward to learning more from him in the future."
-Mike Boya, Warner Bros.

Mike Poor *SANS Senior Instructor*

Mike Poor is a founder and senior security analyst for the Washington, DC firm InGuardians, Inc. In the past he has worked for Sourcefire as a research engineer and for SANS leading its intrusion analysis team. As a consultant Mike conducts incident response, breach analysis, penetration tests, vulnerability assessments, security audits, and architecture reviews. His primary job focus, however, is on intrusion detection, response, and mitigation. Mike currently holds the GCIA certification and is an expert in network engineering and systems and network and web administration. Mike is an author of the international best-selling "Snort" series of books from Syngress, a member of the Honeynet Project, and a handler for the SANS Internet Storm Center. @Mike_Poor

503.1 HANDS ON: Fundamentals of Traffic Analysis: PART 1

Day 1 provides a refresher or introduction to TCP/IP, depending on your background, covering the essential foundations such as the TCP/IP communication model, theory of bits, bytes, binary and hexadecimal, an introduction to Wireshark, the IP layer, and 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.

Topics: Concepts of TCP/IP; Introduction to Wireshark; Network Access/Link Layer: Layer 2; IP Layer: Layer 3, IPv4, and IPv6

503.2 HANDS ON: Fundamentals of Traffic Analysis: PART 2

Day 2 continues where Day1 ended in understanding TCP/IP. Two essential tools – Wireshark and tcpdump – are explored 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 culminates the examination of TCP/IP with an exploration of the application protocol layer. The concentration is on some of the most widely used, and sometimes vulnerable, crucial application protocols – HTTP, SMTP, DNS, and Microsoft communications. Our focus is on traffic analysis, a key skill in intrusion detection.

Topics: Advanced Wireshark; Detection Methods for Application Protocols; Microsoft Protocols; HTTP; SMTP; DNS; Packet Crafting and nmap OS Identification; IDS/IPS Evasion Theory; Real-World Traffic Analysis

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
- Synthesize disparate log files to widen and augment analysis
- 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

503.4 HANDS ON: Open-Source IDS: Snort and Bro

We take a unique approach of teaching both open-source IDS solutions by presenting them in their operational life-cycle phases from planning to updating. This will offer you a broader view of what is entailed for the production and operation of each of these open-source tools. This is more than just a step-by-step discussion of install, configure, and run the tools. This approach provides a recipe for a successful deliberated deployment, not just a haphazard "download and install the code and hope for the best."

Topics: Operational Lifecycle of Open-Source IDS; Introduction; Snort; Bro; Comparing Snort and Bro to Analyze Same Traffic

503.5 HANDS ON: Network Traffic Forensics and Monitoring

On the penultimate day, you'll become familiar with other tools in the "analyst toolkit" to enhance your analysis skills and give you alternative perspectives of traffic. The open-source network flow tool SiLK is introduced. It offers the capability to summarize network flows to assist in anomaly detection and retrospective analysis, especially at sites where the volume is so prohibitively large that full packet captures cannot be retained for very long, if at all.

Topics: Analyst Toolkit; SiLK; Network Forensics; Network Architecture for Monitoring; Correlation of Indicators

503.6 HANDS ON: IDS Challenge

The week culminates with a fun hands-on exercise that challenges you to find and analyze traffic to a vulnerable honeynet host using many of the same tools you mastered during the week. Students can work alone or in groups with or without workbook guidance. This is a great way to end the week because it reinforces what you've learned by challenging you to think analytically, gives you a sense of accomplishment, and strengthens your confidence to employ what you've learned in the Intrusion Detection In-Depth course in a real-world environment.

SECURITY 504

Hacker Tools, Techniques, Exploits, and Incident Handling

Six-Day Program
Mon, Dec 14 - Sat, Dec 19
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: John Strand

- GIAC Cert: GCIH
- Cyber Guardian
- STI Master's Program
- OnDemand Bundle
- DoDD 8570

"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

"Our organization has incident response pieces all over. This course is valuable in putting the pieces together and improving the plan and, more importantly, the mindset."
-Tyler Burwitz, TEEX

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.

By helping you understand attackers' 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, this course helps you turn the tables on computer attackers. 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.

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 *SANS Senior Instructor*

Along with SEC504, John Strand also teaches SEC560: Network Penetration Testing and Ethical Hacking; SEC580: Metasploit Kung Fu for Enterprise Pen Testing; and SEC464: Hacker Detection for System Administrators. John is the course author for SEC464 and the co-author for SEC580. 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) one needs to follow 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

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/ondemand

sans.org/8570

SECURITY 505

Securing Windows with PowerShell and the Critical Security Controls

Six-Day Program
Mon, Dec 14 - Sat, Dec 19
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jason Fossen

- GIAC Cert: GCWN
- Cyber Guardian
- STI Master's Program
- OnDemand Bundle

ATTEND REMOTELY

SIMULCAST

If you are unable to attend this event, this course is also available via SANS Simulcast.

More info on page 59

"SEC505 is very well structured and organized and provided me with an in-depth understanding of Windows security."
-Rochana Lahiri, BCBSLA

"I loved SEC505 and when I return to the office, I am recommending it to the rest of my team."
-Alex Fox,
Federal Home Loan Bank Chicago

What is Windows Hello in Windows 10? How can we defend against pass-the-hash attacks, administrator account compromise, and the lateral movement of hackers inside our networks? How do we actually implement the Critical Security Controls on Windows in a large environment? How can we significantly reduce the client-side exploits that lead to advanced persistent threat malware infections? We tackle these tough problems in **SEC505: Securing Windows with PowerShell and the Critical Security Controls**.

Understanding how penetration testers and hackers break into networks is not the same as knowing how to design defenses against them, especially when you work in a large and complex Active Directory environment. Knowing about tools like Metasploit, Cain, Netcat, and Poison Ivy is useful, but there is no simple patch against their abuse. The goal of this course is to show you ways to defend against both current Windows attack techniques and the likely types of attacks we can expect in the future. This requires more than just reactive patch management – we need to proactively design security into our systems and networks. That is what SEC505 is about.

Your adversaries want to elevate their privileges to win control over your servers and domain controllers, so a major theme of this course is controlling administrative powers through Group Policy and PowerShell scripting.

Learning PowerShell is probably the single best new skill for Windows administrators, especially with the trend toward cloud computing. Most of your competition in the job market lacks scripting skills, so knowing PowerShell is a great way to make your résumé stand out. This course devotes the entire first day to PowerShell, then we do more PowerShell exercises throughout the rest of the week. Don't worry, you don't need any prior scripting experience to attend.

SEC505 will also prepare you for the GIAC Certified Windows Security Administrator (GCWN) exam to certify your Windows security expertise. The GCWN certification counts toward getting a Master's Degree in information security from the SANS Technology Institute (**sans.edu**) and also satisfies the Department of Defense 8570 computing environment requirement.

This is a fun course and a real eye-opener, even for Windows administrators with years of experience. Come have fun learning PowerShell and Windows security!

Who Should Attend

- Anyone who wants to learn PowerShell
- Windows security engineers and system administrators
- Anyone implementing the Critical Security Controls
- Those who must enforce security policies on Windows hosts
- Those deploying or managing a PKI or smart cards
- Anyone who needs to reduce APT malware infections

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: Windows PowerShell Scripting

Today's course covers everything you need to know to get started using PowerShell. You don't need to have any prior scripting or programming experience. After today, we will look at PowerShell examples throughout the week as we work with our regular graphical tools to manage security. Ideally, we want to be able to manage security using either graphical tools or PowerShell (and usually both). In fact, some Microsoft graphical management tools are already built on top of PowerShell, and Microsoft is building more administrative tools this way.

Topics: Overview and Security; Getting Around Inside PowerShell; Example Commands; Write Your Own Scripts

505.2 HANDS ON: Windows Operating System and Applications Hardening

The trick is hardening Windows in a way that is cost-effective, scalable, and has a minimal impact on users. We will look at tools like EMET and Group Policy to make that process easier. As throughout the week, today's section will also look at how to implement many of the Critical Security Controls. The day begins with a continuation of the PowerShell material on the first day. In PowerShell, we will see how to interact with the Windows Management Instrumentation (WMI) service on remote computers. By talking to the WMI service, we can search event logs, start or stop processes, manage DNS records, reboot systems, and do hundreds of other tasks. PowerShell and WMI are tightly integrated, and learning WMI is very important for honing your PowerShell skills as a cyber-defense operator.

Topics: PowerShell and Windows Management Instrumentation (WMI); Going Beyond Just Anti-Virus Scanning; OS Hardening with Security Templates; Hardening with Group Policy

505.3 HANDS ON: High-Value Targets and Restricting Administrative Compromise

Hackers love it when "regular" users are members of the local Administrators group on their computers because it makes it easier to compromise those computers and then to move laterally to other machines. We will talk about what is so dangerous about the Administrators group, how to get users out of that group while still allowing them to get their work done, and, if we just cannot get users out of Administrators, then how to make User Account Control (UAC) less annoying to them...and to us. We will also see how to delegate authority in Active Directory. Like almost everything else, Active Directory can be managed through PowerShell. In today's PowerShell section, we will see how to create, delete, and edit objects in Active Directory, such as user accounts and passwords.

Topics: Compromise of Administrative Powers; PowerShell for Active Directory; Active Directory Permissions and Delegation

You Will Be Able To

- Use Group Policy to harden Windows and applications, deploy Microsoft EMET, do AppLocker whitelisting, apply security templates, and write your own PowerShell scripts.
- Implement Dynamic Access Control (DAC) permissions, file tagging, and auditing for Data Loss Prevention (DLP).
- Use Active Directory permissions and Group Policy to safely delegate administrative authority in a large enterprise to better cope with token abuse, pass-the-hash, service/task account hijacking, and other advanced attacks.
- Install and manage a full Windows PKI, including smart cards, certificate auto-enrollment, and detection of spoofed root CAs.
- Harden SSL, RDP, DNS, and other dangerous protocols.
- Deploy Windows Firewall and IPSec rules through Group Policy and PowerShell.
- Automate security tasks on local and remote systems with the PowerShell scripting language and remoting framework.

505.4 HANDS ON: Windows PKI, Smart Cards, and Managing Cryptography

PowerShell management of PKI and cryptography can be a challenge, but there are tricks to making it easier. In this course, we will see how PowerShell can access certificates, audit our lists of trusted certification authorities, perform file hashing, and encrypt secret data, such as user passwords being sent over the wire. In fact, one of the scripts we use during the week does exactly that – it resets an administrator's password, and the password is encrypted with our public key, and then sent securely over the network for archival. This sounds complex, but PowerShell makes it relatively easy.

Topics: Why Have Public Key Infrastructure?; How to Install the Windows PKI; How to Manage Your PKI; Deploying Smart Cards

505.5 HANDS ON: Server Hardening, IPSec, and Critical Protocols

IPSec is not just for VPNs. IPSec can authenticate users in Active Directory to implement share permissions for TCP and UDP ports based on the user's global group memberships. IPSec can also encrypt packet payloads to keep data secure. Imagine configuring the Windows Firewall on your servers and tablets to only permit access to your RPC or SMB ports if (1) the client has a local IP address, (2) the client is authenticated by IPSec to be a member of the domain, and (3) the packets are all encrypted with 256-bit AES. This is not only possible, it is actually relatively easy to deploy with Group Policy and can be scripted in PowerShell. This course section will show exactly how to do this.

Topics: Creating IPSec Policies; Windows Firewall; Dangerous Server Protocols; Server Hardening

505.6 HANDS ON: Dynamic Access Control and Hardening DNS

Today's course also continues the server hardening theme from the previous day with coverage of DNS security. DNS is mandatory on our networks, but the protocol itself is horrible – hackers love it! There are several things we can do to make DNS less insecure. We can use DNSSEC to digitally sign DNS records to prevent spoofing and man-in-the-middle attacks, do DNS secure dynamic updates with Kerberos, set permissions on DNS records in Active Directory, use the DNS sinkhole technique to frustrate malware, and apply IPSec to DNS packets. DNS was not designed for security to begin with, so security has to be bolted on afterward. Finally, it is no surprise that PowerShell can be used to manage DNS and Dynamic Access Control (DAC) settings. We will see plenty of examples, such as a PowerShell script for DNS sinkholing and PowerShell commands to manage DAC claims and file classifications.

Topics: Dynamic Access Control (DAC); Hardening DNS

SECURITY 511

Continuous Monitoring and Security Operations

Covers NIST SP800-137: Continuous Monitoring

SANS

Six-Day Program
Mon, Dec 14 - Sat, Dec 19
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Seth Misenar

- GIAC Cert: GMON
- OnDemand Bundle

Who Should Attend

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

"I work in net security with a lot of tools. Seth provided a great perspective on the state of cyber defense and how we should be approaching it."
-Kevin South, Navient

We continue to underestimate the tenacity of our adversaries! Organizations are investing a significant amount of 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 would 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!

With your training journey now complete and your skills enhanced and honed, it is time to go back to work and deliver on the SANS promise that you will be able to apply what you learn in this course the day you return to the office.

Seth Misenar *SANS Senior Instructor*

Seth Misenar serves as lead consultant and founder of 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 HIPAA and as information security officer for a state government agency. Prior to becoming a security geek, Seth received a BS 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, but are not limited to, the following: CISSP, GPEN, GWAPT, GSEC, GCIA, GCIH, GCWN, GCFA, and MCSE. @sethmisenar

511.1 HANDS ON: Current State Assessment, SOCs & 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 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 and 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 Architecture – Design Tools/Strategies; 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

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)
- Determine requisite monitoring capabilities for a SOC environment
- Determine capabilities required to support continuous monitoring of key Critical Security Controls
- Utilize tools to support implementation of Continuous Monitoring per NIST guidelines SP 800-137

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 insists on proactively and repeatedly assessing and reassessing 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, and Defend

The course culminates in a team-based Capture-the-Flag challenge that is a full day of hands-on work applying the principles taught throughout the week.

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

giac.org

WITH THIS COURSE

sans.org/ondemand

SECURITY 560

Network Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Mon, Dec 14 - Sat, Dec 19
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Ed Skoudis

- GIAC Cert: GPEN
- Cyber Guardian
- STI Master's Program
- OnDemand Bundle
- DoDD 8570

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.

This course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks and wireless and web apps, with over 30 detailed hands-on labs throughout.

Who Should Attend

- Security personnel whose job involves assessing networks and systems to find and remediate vulnerabilities
- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Red team members
- Blue team members

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

Chock full of practical, real-world tips from some of the world's best penetration testers, SEC560 prepares you to perform detailed reconnaissance by examining a target's infrastructure and mining blogs, search engines, social networking sites and other Internet and intranet infrastructure. You will be equipped to scan target networks using best-of-breed tools. We will not just cover run-of-the-mill options and configurations, we will also go over the less-known but highly useful capabilities of the best pen test toolsets available today. After scanning, you will learn dozens of methods for exploiting target systems to gain access and measure real business risk, then examine post-exploitation, password attacks, wireless and web apps, pivoting through the target environment to model the attacks of real-world bad guys.

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

After building your skills in challenging labs over five days, the course culminates with a full-day, real-world network penetration test scenario. You will conduct an end-to-end penetration test, applying the knowledge, tools and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization.

"Ed's presentation style is very effective. He creates a comfortable atmosphere and does a wonderful job delivering the material while checking the students' comprehension. This course was well worth the investment of time and money."

-Mike Williams, Lancaster-Lebanon IU 13

"This course was tremendously timely and super relevant for my career."

-James Miller, SRA

ATTEND REMOTELY

SIMULCAST

If you are unable to attend this event, this course is also available via SANS Simulcast.

More info on page 59

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'll develop the skills needed to conduct a best-of-breed, high-value penetration test. We'll go in-depth on how to build a penetration testing infrastructure that includes all the hardware, software, network infrastructure, and tools you'll need for conducting great penetration tests, with specific low-cost recommendations for your arsenal. We'll then cover formulating a pen test scope and rules of engagement that will set you up for success, with a role-playing exercise where you'll build an effective scope and rules of engagement. We 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.

Topics: The Mindset of the Professional Pen Tester; Building a World-Class Pen Test Infrastructure; Creating Effective Pen Test Scopes and Rules of Engagement; Effective Reporting; Detailed Recon Using the Latest Tools; 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 attack surface by creating a comprehensive inventory of machines, accounts, and potential vulnerabilities. We'll 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'll 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, as well as how to conduct your scans safely and efficiently.

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

560.3 HANDS ON: Exploitation and Post-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, search them for information to advance the penetration test, and pivot to other systems, all with a focus on determining the true business risk of the target organization. We'll also look at post-exploitation analysis of machines and pivoting to find new targets, finishing the section with a lively discussion of how to leverage the Windows shell to dominate target environments.

Topics: Comprehensive Metasploit Coverage with Exploits/Stagers/Stages; In-Depth Meterpreter Hands-On Labs; Implementing Port Forwarding Relays for Merciless Pivots; Bypassing the Shell vs. Terminal Dilemma; Installing VNC/RDP/SSH with Only Shell Access; Windows Command Line Kung Fu for Penetration Testers

560.4 HANDS ON: Password Attacks and Merciless Pivoting

This component of the course turns our attention to password attacks, analyzing password guessing, password cracking, and pass-the-hash techniques in depth. We'll go over numerous tips based on real-world experience to help penetration testers and ethical hackers maximize the effectiveness of their password attacks. You'll patch and 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. You'll also perform multiple types of pivots to move laterally through our target lab environment, and pluck hashes and cleartext passwords from memory using the Mimikatz tool. We'll see how Rainbow Tables really work to make password cracking much more efficient, all hands-on. And, we'll finish the day with an exciting discussion of powerful "pass-the-hash" attacks, leveraging Metasploit, the Meterpreter, and SAMBA client software.

Topics: 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; Massive Pivoting Through Target Environments; Extracting Hashes and Passwords from Memory with Mimikatz; Password Cracking with John the Ripper & Cain; Using Rainbow Tables to Maximum Effectiveness; Pass-the-Hash Attacks with Metasploit and More

560.5 HANDS ON: Wireless and Web Apps Penetration Testing

This in-depth section of the course is focused on helping you become a well-rounded penetration tester. Augmenting your network penetration testing abilities, we turn our attention to methods for finding and exploiting wireless weaknesses, including identifying misconfigured access points, cracking weak wireless protocols, and exploiting wireless clients. We then turn our attention to web application pen testing, with detailed hands-on exercises that involve 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: Wireless Attacks; Discovering Access; Attacking Wireless Crypto Flaws; Client-Side Wireless Attacks; 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 Testing Workshop and Capture the Flag Event

This lively session represents the culmination of the network penetration testing and ethical hacking course, where you'll apply all of the skills mastered in the course so far in a full-day, hands-on workshop. 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. And, 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; 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 the Nmap scanning tool to conduct comprehensive network sweeps, port scans, Operating System fingerprinting, and version scanning to develop a map of target environments
- Configure and launch a vulnerability scanner such as Nessus so that it discovers vulnerabilities through both authenticated and unauthenticated scans in a safe manner, 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 connection-making tools such as Netcat and packet crafting tools such as Scapy
- Utilize the Windows and Linux command 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
- Utilize wireless attack tools for WiFi networks to discover access points and clients (actively and passively), crack WEP/WPA/WPA2 keys, and exploit client machines included within a project's scope
- Launch web application vulnerability scanners such as ZAP and then manually exploit Cross-Site Request Forgery, Cross-Site Scripting, and Command Injection

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/ondemand

SECURITY 566

Implementing and Auditing the Critical Security Controls – In-Depth

SANS

Five-Day Program
Mon, Dec 14 - Fri, Dec 18
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: James Tarala
- GIAC Cert: GCCC
- STI Master's Program
- OnDemand Bundle

"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

"I'm leaving the class with a great mindset aimed at evaluating the current environment and controls. SEC566 was good information with a great instructor!"
-Tom Kozelsky, Nexeo Solution

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?

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.

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

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. Specifically, by the end of the course students will know how to:

- Create a strategy to successfully defend their data
- Implement controls to prevent data from being compromised
- Audit systems to ensure compliance with Critical Control standards.

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 and senior instructor with 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 architecting 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 in 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: Malware Defenses
Critical Control 6: Application Software Security

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

Topics: Critical Control 7: Wireless Device Control
Critical Control 8: Data Recovery Capability (validated manually)
Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps (validated manually)
Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services

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

Topics: Critical Control 12: Controlled Use of Administrative Privileges
Critical Control 13: Boundary Defense
Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs
Critical Control 15: Controlled Access Based on Need to Know

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

Topics: Critical Control 16: Account Monitoring and Control
Critical Control 17: Data Loss Prevention
Critical Control 18: Incident Response Capability (validated manually)
Critical Control 19: Secure Network Engineering (validated manually)
Critical Control 20: Penetration Tests and Red Team Exercises (validated manually)

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

"Topics addressed real-world and current threats – gives great suggestions to assist an organization to better protect their IP space."
-Bill Coffey, Shaw AFB

giac.org

sans.edu

sans.org/ondemand

SECURITY 575

Mobile Device Security and Ethical Hacking

Six-Day Program
Mon, Dec 14 - Sat, Dec 19
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Christopher Crowley

- GIAC Cert: GMOB
- STI Master's Program
- OnDemand Bundle

"Taking this course was a great opportunity to ask an expert all my questions, good broad overview and mobile threats background!"
-Tom G., GovCert UK

"Once again, SANS has exceeded my expectations and successfully re-focused my view of threats and risks. I recommend this course because it is very enlightening."
-Charles Allen,
EM Solutions, Inc.

Mobile phones and tablets have become essential to enterprise and government networks ranging from small organizations to Fortune 500 companies and large agencies. Often, mobile phone deployments grow organically, adopted by multitudes of end-users for convenient email access, as well as by managers and executives who need access to sensitive organizational resources from their favored personal mobile devices. In other cases, mobile phones and tablets have become critical systems for a wide variety of production applications from enterprise resource planning (ERP) to project management.

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

For all of its convenience, however, the ubiquitous use of mobile devices in the work place and beyond has brought new security risks. As reliance on these devices has grown exponentially, organizations have quickly recognized that mobile phones and tablets need greater security implementations than a simple screen protector and clever password. Whether an Apple iPhone or iPad, a Windows Phone, or an Android or BlackBerry phone or tablet, these devices have become hugely attractive and vulnerable targets for nefarious attackers. The use of such devices poses an array of new risks to organizations, including:

- Distributed sensitive data storage and access mechanisms
- Lack of consistent patch management and firmware updates
- The high probability of device loss or theft, and more

Mobile code and apps are also introducing new avenues for malware and data leakage, exposing critical enterprise secrets, intellectual property, and personally identifiable information assets to attackers. To further complicate matters, today there simply are not enough people with the security skills needed to manage mobile phone and tablet deployments.

SEC575: Mobile Device Security and Ethical Hacking is designed to help organizations secure their mobile devices by equipping personnel with the knowledge to design, deploy, operate, and assess a well-managed and safe mobile environment. The course will help you build the critical skills to support your organization's secure deployment and use of mobile phones and tablets. You will learn how to capture and evaluate mobile device network activity, disassemble and analyze mobile code, recognize weaknesses in common mobile applications, and conduct full-scale mobile penetration tests.

You will gain hands-on experience in designing a secure mobile phone network for local and remote users and learn how to make critical decisions to support devices effectively and securely. You will also be able to analyze and evaluate mobile software threats, and learn how attackers exploit mobile phone weaknesses so you can test the security of your own deployment. With these skills, you will be a valued mobile device security analyst, fully able to guide your organization through the challenges of securely deploying mobile devices.

Christopher Crowley *SANS Certified Instructor*

Christopher Crowley 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. Mr. Crowley is the course author for SANS Management 535 - 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, 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

575.1 HANDS ON: Device Architecture and Common Mobile Threats

The first part of the course looks at the significant threats affecting mobile phone deployments and how organizations are being attacked through these systems. As a critical component of a secure deployment, we'll examine the architectural and implementational differences between Android, Apple, BlackBerry, and Windows Phone systems, including platform software defenses and application permission management. We'll also look at the specific implementation details of popular platform features such as iBeacon, AirDrop, App Verification and more. We'll apply hands-on exercises to interact with mobile device emulator features including low-level access to installed application services.

Topics: Mobile Problems and Opportunities; Mobile Devices and Infrastructure; Mobile Device Security Models; 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 can design incident response processes to mitigate the effect of common threat scenarios, including device loss. We'll look at building such a program, while building our own skills at analyzing mobile device data and applications through rooting and jailbreaking, filesystem data analysis, and network activity analysis techniques.

Topics: Mitigating Stolen Devices; Unlocking, Rooting, Jailbreaking Mobile Devices; Mobile Phone Data Storage and Filesystem Architecture; Network Activity Monitoring

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
- 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

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. We'll examine the techniques for reverse-engineering iOS and Android applications, obtaining source code for applications from public app stores. For Android applications we'll look at opportunities to change the behavior of applications as part of our analysis process by decompiling, manipulating, and recompiling code, and adding new code to existing applications without prior source code access. For iOS we'll extract critical app definition information available in all apps to examine and manipulate app behavior through the Cycript tool.

Topics: Static Application Analysis; 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

575.5 HANDS ON: Penetration Testing Mobile Devices – PART 2

Continuing our look at ethical hacking or penetration testing, we turn our focus to exploiting weaknesses on individual mobile devices, including iPhones, iPads, Android phones and tablets, Windows Phones, and BlackBerry devices. We'll also examine platform-specific application weaknesses and look at the growing use of web framework attacks.

Topics: Network Manipulation Attacks; Mobile Application 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.

giac.org

SANS Technology Institute

sans.edu

BUNDLE ONDEMAND WITH THIS COURSE

sans.org/ondemand

SECURITY 579

Virtualization and Private Cloud Security

SANS

Six-Day Program
Mon, Dec 14 - Sat, Dec 19
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Dave Shackleford
- OnDemand Bundle

One of today's most rapidly evolving and widely deployed technologies is server virtualization. Many organizations are already realizing the cost savings from implementing virtualized servers, and systems administrators love the ease of deployment and management of virtualized systems. 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 presents new vulnerabilities that must be managed. In addition, there are 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 – internal shared services running on virtualized infrastructure. Security architecture, policies, and processes will need to adapt to work within a cloud infrastructure, and there are many changes that security and operations teams will need to accommodate to ensure assets are protected.

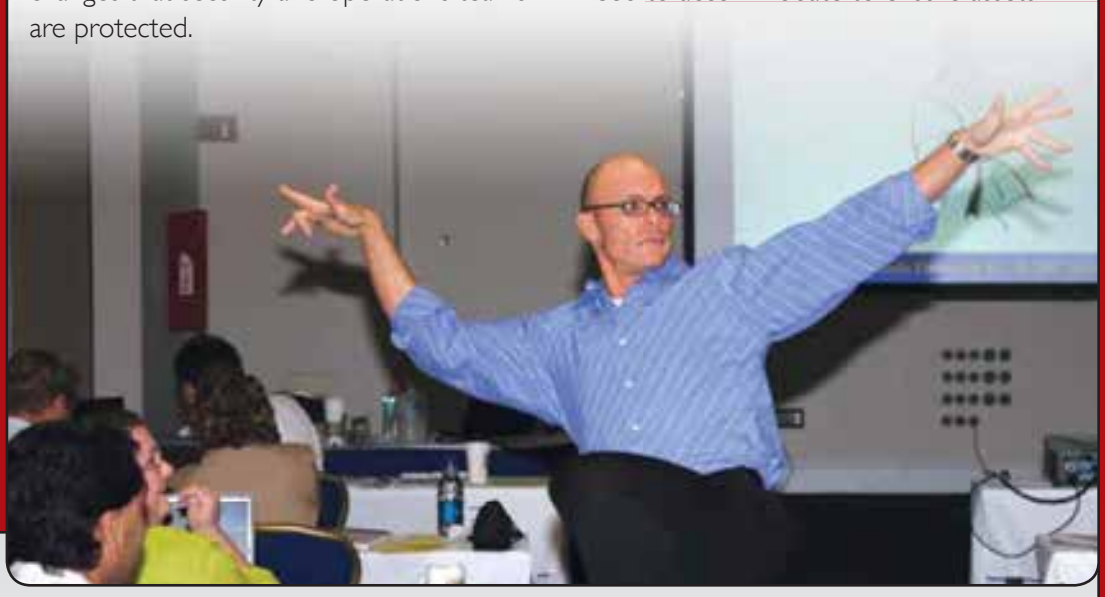
Who Should Attend

- 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

"Great course! Anyone involved with managing virtual system environments will benefit from taking SEC579."
-Randall R.,
Defense Security Services

"Dave is an excellent teacher and communicator. He made a highly technical course interesting and the overall experience was thoroughly enjoyable!"
-Wayne Rosen, Adnet Systems, Inc.



Dave Shackleford *SANS Senior Instructor*

Dave Shackleford is the owner and principal consultant of Voodoo Security and a SANS analyst, senior instructor, 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: Virtualization Security Architecture and Design

We'll cover the foundations of virtualization infrastructure and clarify the differences between server virtualization, desktop virtualization, application virtualization, and storage virtualization. We'll start with hypervisor platforms, covering the fundamental controls that should be set within VMware ESX and ESXi, Microsoft Hyper-V, and Citrix XenServer. You'll spend time analyzing virtual networks. We'll compare designs for internal networks and DMZs. Virtual switch types will be discussed, along with VLANs and PVLANs. We will cover virtual machine settings, with an emphasis on VMware VMX files.

Topics: Virtualization Components and Architecture Designs; Hypervisor Lockdown Controls for VMware; Microsoft Hyper-V, and Citrix Xen; Virtual Network Design Cases; Virtual Switches and Port Groups; Segmentation Techniques; Virtual Machine Security Configuration Options

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 private cloud 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

579.2 HANDS ON: Virtualization and Private Cloud Infrastructure Security

Today starts with virtualization management. VMware vCenter, Microsoft System Center Virtual Machine Manager (SCVMM), and Citrix XenCenter will be covered. Virtual Desktop Infrastructure (VDI) will be covered with an emphasis on security principles. Specific security-focused use cases for VDI, such as remote access and network access control, will be reviewed. We will take an in-depth look at virtual firewalls. Students will build a virtualized intrusion detection model; integrate promiscuous interfaces and traffic capture methods into virtual networks; and then set up and configure a virtualized IDS sensor. Attention will be paid to host-based IDS, with considerations for multitenant platforms.

579.3 HANDS ON: Virtualization Offense and Defense – PART 1

In this session, we'll delve into the offensive side of security specific to virtualization and cloud technologies. While many key elements of vulnerability management and penetration testing are similar to traditional environments, there are many differences that we will cover. First, we'll cover a number of specific attack scenarios and models that represent the different risks organizations face in their virtual environments. Then we'll go through the entire penetration testing and vulnerability assessment lifecycle, with an emphasis on virtualization tools and technologies. Students will then learn about monitoring traffic and looking for malicious activity within the virtual network, and numerous network-based and host-based tools will be covered and implemented in class. Finally, students will learn about logs and log management in virtual environments.

579.4 HANDS ON: Virtualization Offense and Defense – PART 2

This session is all about defense! We'll start off with an analysis of anti-malware techniques. We'll look at traditional antivirus, whitelisting, and other tools and techniques for combating malware, with a specific eye toward virtualization and cloud environments. New commercial offerings in this area will also be discussed to provide context. Most of this session will focus on incident response and forensics in a virtualized or cloud-based infrastructure. We'll walk students through the six-step incident response cycle espoused by NIST and SANS, and highlight exactly how virtualization fits into the big picture. Students will discuss and analyze incidents at each stage, again with a focus on virtualization and cloud. We'll finish the incident response section with processes and procedures organizations can put to use right away to improve their awareness of virtualization-based incidents.

579.5 HANDS ON: Virtualization and Cloud Integration: Policy, Operations, and Compliance

This session will explore how traditional security and IT operations change with the addition of virtualization and cloud technology in the environment. Our first discussion will be a lesson in contrast! First, we'll present an overview of integrating existing security into virtualization. Then, we'll take a vastly different approach and outline how virtualization actually creates new security capabilities and functions! This will really provide a solid grounding for students to understand just what a paradigm shift virtualization is, and how security can benefit from it, while still needing to adapt in many ways.

579.6 HANDS ON: Auditing and Compliance for Virtualization and Cloud

Today's session will start off with a lively discussion on virtualization assessment and audit. You may be asking – how will you possibly make a discussion on auditing lively? Trust us! We'll cover the top virtualization configuration and hardening guides from DISA, CIS, Microsoft, and VMware, and talk about the most important and critical things to take away from these to implement. We'll really put our money where our mouth is next – students will learn to implement audit and assessment techniques by scripting with the VI CLI, as well as some Powershell and general shell scripting! Although not intended to be an in-depth class on scripting, some key techniques and ready-made scripts will be discussed to get students prepared for implementing these principles in their environments as soon as they get back to work.

SECURITY 660

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

SANS

Six-Day Program
Mon, Dec 14 - Sat, Dec 19
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Stephen Sims

- GIAC Cert: GXPN
- Cyber Guardian
- STI Master's Program
- OnDemand Bundle

"The SEC660 course was a very eye opening experience. The theory and concepts were equally covered as the practical exercises which I have never seen in other courses."
-Faisal Al Mansour, Saudi Aramco

"Great instruction with the right mix of lecture and labs. The Capture The Flag brought everything together for the week."
-Chris Fortune, Vectren Corp.

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!

Who Should Attend

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

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 engages 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.

Stephen Sims *SANS Senior Instructor*

Stephen Sims is an industry expert with over 15 years of experience in information technology and security. Stephen currently works out of San Francisco as a consultant performing reverse engineering, exploit development, threat modeling, and penetration testing. Stephen has an MS in information assurance from Norwich University and is a course author and senior instructor for the SANS Institute. He is the author of SANS' only 700-level course, SEC760: Advanced Exploit Development for Penetration Testers, which concentrates on complex heap overflows, patch diffing, and client-side exploits. Stephen is also the lead author on SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking. He holds the GIAC Security Expert (GSE) certification as well as the CISSP, CISA, Immunity NOP, and many other certifications. In his spare time Stephen enjoys snowboarding and writing music. @Steph3nSims

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; IEEE 802.1X 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

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; IDAPro; 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

660.5 HANDS ON: Exploiting Windows for Penetration Testers

On day five we start off 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. We look at fuzzing skills, which are required to test remote services, such as TFTP and FTP, for faults.

Topics: The State of Windows OS Protections on XP, Vista, 7, Server 2003 and 2008; Understanding Common Windows Constructs; Stack Exploitation on Windows; Defeating OS Protections Added to Windows; Dynamic and Static Fuzzing on Windows Applications or Processes; Creating a Metasploit Module; Advanced Stack-Smashing on Windows; Return-Oriented Programming (ROP); Windows 7 and Windows 8; Porting Metasploit Modules; Client-side Exploitation; Windows and Linux Shellcode

660.6 HANDS ON: Capture the Flag

This day will serve as a real-world challenge for students, requiring them to utilize skills learned throughout the course, think outside the box, and solve simple-to-complex problems. 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.

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

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/ondemand

FORENSICS 408

Windows Forensic Analysis

SANS

Six-Day Program
Mon, Dec 14 - Sat, Dec 19
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Ovie Carroll

- GIAC Cert: GCFE
- STI Master's Program
- OnDemand Bundle

"The methods taught and the tools introduced will be very beneficial to me as an analyst performing examinations. I have really enjoyed the classes and I feel I have learned a great deal of valuable knowledge and skills."
-Joseph Selph, IBM

"I have been doing forensic investigations for several years, but would highly recommend this course (FOR408) for both new and old forensic investigations."
-Robert Galarza, JP Morgan Chase

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.

Who Should Attend

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

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, Windows 8/8.1, 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 8.1 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 UNDERSTAND

Ovie Carroll *SANS Certified Instructor*

Ovie Carroll has over 20 years of federal law enforcement experience. Ovie was a special agent for the Air Force Office of Special Investigations (AFOSI) and Chief of the Washington Field Office Computer Investigations and Operations Branch responsible for investigating all national-level computer intrusions into USAF computer systems. Following his career with the AFOSI he was the Special Agent in Charge of the Postal Inspector General's computer crimes unit, where he was responsible for all computer intrusion investigations and for providing all computer forensic analysis in support of USPS-OIG investigations. Ovie is currently the Director for the Cybercrime Lab at the Department of Justice, Computer Crime and Intellectual Property Section (CCIPS) and an adjunct professor at George Washington University teaching computer crime investigations. In addition to his career fighting computer crime, Ovie has conducted investigations into a variety of offenses including murder, fraud, bribery, theft, gangs and narcotics.

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; FAT and NTFS File System Overview; Key Word Searching and Forensics Suites (FTK, EnCase, and Autopsy); Document and File Metadata; File Carving

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; External and Bring Your Own Device (BYOD) Forensic Examinations; 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); 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

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; Mock Trial

You Will Be Able To

- Perform proper Windows forensic analysis by applying key techniques focusing on Windows 7/8/8.1
- 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
- Use automated analysis techniques via AccessData's Forensic ToolKit (FTK), Nuix, and Internet Evidence Finder (IEF)
- 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

FORENSICS 508

Advanced Digital Forensics and Incident Response

Six-Day Program
Mon, Dec 14 - Sat, Dec 19
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Alissa Torres

- GIAC Cert: GCFA
- Cyber Guardian
- STI Master's Program
- DoDD 8570
- OnDemand Bundle

"FOR508 has been the best DFIR course I've taken so far. All the material is recent and it shows a lot of time went into the material. "
-Louise Cheung, Stroz Friedberg

"FOR508 is an extremely valuable course overall. It brings essential topics into one class and covers an extensive amount of topics along with excellent reference material."
-Edgar Zayas, U.S. Securities and Exchange Commission

DAY 0: A 3-letter government agency contacts you to say critical information was stolen through a targeted attack on your organization. They won't tell how they know, but they identify several breached systems within your enterprise. An Advanced Persistent Threat adversary, aka an APT, is likely involved – the most sophisticated threat you are likely to face in your efforts to defend your systems and data.

FOR508: Advanced Digital Forensics and Incident Response will help you determine:

- How the breach occurred
- How systems were affected and compromised
- What attackers took or changed
- How to contain and mitigate the incident

Who Should Attend

- Information security professionals
- Incident response team members
- Experienced digital forensic analysts
- Federal agents and law enforcement
- Red team members, penetration testers, and exploit developers
- Security Operations Center (SOC) personnel and Information Security Practitioners
- SANS FOR408 and SEC504 graduates

ATTEND REMOTELY

SIMULCAST

If you are unable to attend this event, this course is also available via SANS Simulcast.

More info on page 59

Over 80% of all breach victims learn of a compromise from third-party notifications, not from internal security teams. In most cases, adversaries have been rummaging through your network undetected for months or even years.

Incident response tactics and procedures have evolved rapidly over the past several years. Data breaches and intrusions are growing more complex. Adversaries are no longer compromising one or two systems in your enterprise; they are compromising hundreds. Your team can no longer afford antiquated incident response techniques that fail to properly identify compromised systems, provide ineffective containment of the breach, and ultimately fail to rapidly remediate the incident.

This in-depth incident response course provides responders with advanced skills to hunt down, counter, and recover from a wide range of threats within enterprise networks, including APT adversaries, organized crime syndicates, and hactivism. Constantly updated, FOR508 addresses today's incidents by providing hands-on incident response tactics and techniques that elite responders are successfully using in real-world breach cases.

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

Alissa Torres *SANS Certified Instructor*

Alissa Torres is a certified SANS instructor, specializing 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 Bachelors degree from the University of Virginia and a Masters from the University of Maryland in Information Technology. Alissa has taught as an instructor 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

508.1 HANDS ON: Enterprise Incident Response

Incident responders should be armed with the latest tools, memory analysis techniques, and enterprise scanning methodologies in order to identify, track and contain advanced adversaries and remediate incidents. Incident response and forensic analysts must be able to scale their examinations from the traditional one analyst per system toward one analyst per 1,000 or more systems. Enterprise scanning techniques are now a requirement to track targeted attacks by APT groups or crime syndicate groups that propagate through thousands of systems.

Topics: Real Incident Response Tactics; Threat and Adversary Intelligence; Intrusion Digital Forensics Methodology; Remote and Enterprise IR System Analysis; Windows Live Incident Response

508.2 HANDS ON: Memory Forensics in Incident Response

Now a critical component of many incident response teams that detect advanced threats in their organization, memory forensics has come a long way in just a few years. It can be extraordinarily effective at finding evidence of worms, rootkits, and advanced malware used by an APT group of attackers. Memory analysis traditionally was solely the domain of Windows internals experts, but the recent development of new tools makes it accessible today to anyone, especially incident responders. Better interfaces, documentation, and built-in detection heuristics have greatly leveled the playing field. This section will introduce some of the newest free tools available and give you a solid foundation in adding core and advanced memory forensic skills to your incident response and forensics capabilities.

Topics: Memory Acquisition; Memory Forensics Analysis Process; Memory Forensics Examinations; Memory Analysis Tools

508.3 HANDS ON: Timeline Analysis

Learn advanced incident response techniques uncovered via timeline analysis directly from the developers who pioneered timeline analysis tradecraft. Temporal data are located everywhere on a computer system. File system modified/access/creation/change times, log files, network data, registry data, and Internet history files all contain time data that can be correlated into critical analysis to successfully solve cases. Pioneered by Rob Lee in 2001, timeline analysis has become a critical incident response and forensics technique to solve complex cases. New timeline analysis frameworks provide the means to conduct simultaneous examinations of a multitude of time-based artifacts. Analysis that once took days now takes minutes.

Topics: Timeline Analysis Overview; Filesystem Timeline Creation and Analysis; Windows Time Rules (File Copies vs. File Moves); Filesystem Timeline Creation Using Sleuthkit and fls; Super Timeline Creation and Analysis; Super Timeline Artifact Rules; Timeline Creation with log2timeline; Super Timeline Analysis

508.4 HANDS ON: Deep Dive Forensics and Anti-Forensics Detection

A major criticism of digital forensic professionals is that they use tools that simply require a few mouse clicks to automatically recover data for evidence. This "push button" mentality has led to inaccurate case results in the past few years in high-profile cases such as the Casey Anthony murder trial. You will stop being reliant on "push button" forensic techniques as we cover how the engines of digital forensic tools really work. To understand how to carve out data, it is best to understand how to accomplish it by hand and show how automated tools should be able to recover the same data.

Topics: Advanced "Evidence of Execution" Artifacts; Windows 7, Server 2008 Shadow Volume Copy Analysis; Deep Dive Forensics Analysis; Data Layer Analysis; Stream-Based Data Carving; File-Based Data Carving; NTFS Filesystem Analysis; Anti-Forensic Detection Methodologies

508.5 HANDS ON: Adversary and Malware Hunting

Over the years, we have observed that many incident responders have a challenging time finding malware without pre-built indicators of compromise or threat intelligence gathered prior to a breach. This is especially true in APT group 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. The section concludes with a step-by-step approach to handling some of the most difficult types of investigations.

Topics: Adversary and Malware Hunting; Methodology to Analyze and Solve Challenging Cases

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.

You Will Be Able To

- Apply incident response processes, threat intelligence, and digital forensics to investigate breached enterprise environments from Advanced Persistent Threat (APT) groups, organized crime syndicates, or hackivists
- Discover every system compromised in your enterprise utilizing incident response tools such as F-Response and digital forensic analysis capabilities in the SIFT Workstation to identify APT beachhead and spear phishing attack mechanisms, lateral movement, and data exfiltration techniques
- Use the SIFT Workstation's capabilities, and perform forensic analysis and incident response on any remote enterprise hard drive or system memory without having to image the system first, allowing for immediate response and scalable analysis to take place across the enterprise
- Use system memory and the Volatility toolset to discover active malware on a system, determine how the malware was placed there, and recover it to help develop key threat intelligence to perform proper scoping activities during incident response
- Detect advanced capabilities such as Stuxnet, TDSS, or APT command and control malware immediately through memory analysis using Redline's Malware Rating Index (MRI) to quickly ascertain the threat to your organization and aid in scoping the true extent of the data breach
- Track the exact footprints of an attacker crossing multiple systems and observe data the attacker has collected to exfiltrate as you track your adversary's movements in your network via timeline analysis using the log2timeline toolset
- Begin recovery and remediation of the compromise via the use of Indicators of Compromise (IOC), Threat Intelligence, and IR/Forensics key scanning techniques to identify active malware and all enterprise systems affected by the breach
- Perform filesystem surgery using the sleuthkit tool to discover how filesystems work and uncover powerful forensic artifacts such as NTFS $130 directory file indexes, journal parsing, and detailed Master File Table analysis
- Use volume shadow snapshot examinations, XP restore point analysis, and NTFS examination tools in the SIFT Workstation, and recover artifacts hidden by anti-forensic techniques such as timestomping, file wiping, rootkit hiding, and privacy cleaning
- Discover an adversary's persistent mechanisms to allow malware to continue to run on a system after a reboot using command-line tools such as autorunsc, psexec, jobparser, group policy, triage-ir, and IOCFinder

FORENSICS 572

Advanced Network Forensics and Analysis

SANS

Six-Day Program
Mon, Dec 14 - Sat, Dec 19
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Philip Hagen

- GIAC Cert: GNFA
- STI Master's Program
- OnDemand Bundle

"FOR572 was an excellent course that kept my attention and it will be immediately useful when I get back to work."
-John Ives, UC Berkeley

"The instructor was very knowledgeable with relevant and interesting examples to illustrate key points."
-Everett Sherlock, Kapstone Paper

Forensic casework that does not include a network component is a rarity in today's environment. Performing disk forensics will always be a critical and foundational skill for this career, but overlooking the network component of today's computing architecture is akin to ignoring security camera footage of a crime as it was committed. Whether you handle an intrusion incident, data theft case, or employee misuse scenario, the network often has an unparalleled view of the incident. Its evidence can provide the proof necessary to show intent, or even definitively prove that 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.***

Who Should Attend

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

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, or an on-staff forensic practitioner, this course offers hands-on experience with real-world scenarios that will help take your work to the next level. Previous SANS security 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 any convenient hard drive or memory images.

The hands-on exercises in this class cover a wide range of tools, including the venerable tcpdump and Wireshark for packet capture and analysis; commercial tools from Splunk, NetworkMiner, and SolarWinds; and open-source tools including nfdump, tcpxtract, ELSA, and more. Through all of these exercises, your shell scripting abilities will come in handy 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 has 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, Payload Reconstruction, Foundational Network Forensics Tools: tcpdump and Wireshark, Network Evidence Types and Sources, Network Architectural Challenges and Opportunities, Packet Capture Applications and Data

572.2 HANDS ON: NetFlow Analysis, Commercial Tools, and Visualization

In this section, you will learn what data items NetFlow can provide, and the various means of collecting those items. As with many such monitoring technologies, both commercial and open-source solutions exist to query and examine NetFlow data. We will review both categories and discuss the benefits and drawbacks of each. Finally, we will address the forensic aspects of wireless networking. We will cover similarities with and differences from traditional wired network examination, as well as what interesting artifacts can be recovered from wireless protocol fields. Some inherent weaknesses of wireless deployments will also be covered, including how attackers can leverage those weaknesses during an attack, and how they can be detected.

Topics: NetFlow Analysis and Collection; Open-Source Flow Tools, Commercial Network Forensics; Visualization Techniques and Tools; Dynamic Host Configuration Protocol (DHCP) and Domain Name Service (DNS)

572.3 HANDS ON: Network Protocols and Wireless Investigations

This section covers some of the most common and fundamental network protocols that you will likely face during an investigation. We will cover a broad range of protocols including the Dynamic Host Configuration Protocol, which glues together layers two and three on the OSI model, and Microsoft's Remote Procedure Call protocol, which provides all manners of file, print, name resolution, authentication, and other services.

Topics: Hypertext Transfer Protocol (HTTP); Network Time Protocol (NTP); File Transfer Protocol (FTP); Wireless Network Forensics; Simple Mail Transfer Protocol (SMTP); Microsoft Protocols

572.4 HANDS ON: Logging, OPSEC, and Footprint

In this section, you will learn about 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 will learn various solutions that accomplish this, from tactical to enterprise-scale.

Topics: Syslog; Microsoft Event Logging; HTTP Server Logs; Firewall and Intrusion Detection Systems; Log Data Collection, Aggregation, and Analysis; Investigation OPSEC and Footprint Considerations

You Will Be Able To

- Extract files from network packet captures and proxy cache files, allowing follow-on malware analysis or definitive data loss determinations
- 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
- Use visualization tools and techniques to distill vast, complex data sources into management-friendly reports
- 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

572.5 HANDS ON: Encryption, Protocol Reversing, and Automation

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: Dealing with Encoding and Encryption; Man-in-the-Middle; Encrypted Traffic Flow Analysis; Secure HTTP (HTTPS) and Secure Sockets Layer (SSL); Network Protocol Reverse Engineering; Automated Tools and Libraries

572.6 HANDS ON: Network Forensics Capstone Challenge

This section will combine all of what you have learned during this week. In groups, you will examine network evidence from a real-world compromise by an advanced attacker. Each group will independently analyze data, form and develop hypotheses, and present findings. No evidence from endpoint systems is available – only the network and its infrastructure.

Topics: Network Forensic Case

FORENSICS 610

Reverse-Engineering Malware: Malware Analysis Tools and Techniques

SANS

Six-Day Program
Mon, Dec 14 - Sat, Dec 19
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Lenny Zeltser

- GIAC Cert: GREM
- STI Master's Program
- OnDemand Bundle

"FOR610 should be required training for all forensic investigators. It is necessary for awareness, analysis, and reporting of threats."
-Paul G., U.S. Army

"The training is very well documented with lots of hands-on labs, in addition, all topics are discussed thoroughly and reinforced."
-Chaz Hobson, Deutsche Bank

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.

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

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 an MBA degree 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

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, the registry, the 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 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.

610.4 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 will 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

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

giac.org

sans.edu

sans.org/ondemand

digital-forensics.sans.org

MANAGEMENT 414

SANS Training Program for CISSP® Certification

Course Updated for New CISSP® Exam

SANS

Six-Day Program
Mon, Dec 14 - Sat, Dec 19
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: Eric Conrad

- GIAC Cert: GISP
- OnDemand Bundle
- DoDD 8570

"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

"This is a great way to refresh and review my knowledge before sitting for the CISSP exam. This course not only focused on the material at hand, but portrayed it with real-life examples that made it easy to relate to! One of the best classes and experiences I have had."
-Glenn C., Leidos

SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that has been specifically updated to prepare you to pass the 2015 version of the CISSP® exam.

Course authors Eric Conrad and Seth Misenar have revised MGT414 to take into account the 2015 updates to the CISSP® exam and prepare students to navigate all types of questions included in the new version.

MGT414 focuses solely on the 8 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.

Who Should Attend

- Security professionals who are interested in understanding the concepts covered in the CISSP® exam as determined by (ISC)^2
- Managers who want to understand the critical areas of network security
- System, security, and network administrators who want to understand the pragmatic applications of the CISSP® 8 domains
- Security professionals and managers looking for practical ways the 8 domains of knowledge can be applied to their current job

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

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 health care. 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

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 2015 exam update will be discussed in detail. We will cover the general security principles needed to understand the 8 domains of knowledge, with specific examples for each domain. The first of the 8 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 8 Domains; Domain 1: Security and Risk Management

You Will Be Able To

- Understand the 8 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 8 domains of knowledge.
- Apply the skills learned across the 8 domains to solve security problems when you return to work.

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/militaries and 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 2015 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 2015 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 2015 CISSP® exam update will be discussed, including DevOps. We will wrap up 414.6 by discussing security vulnerabilities, secure coding strategies, and testing methodologies.

Topics: Domain 8: Software Development Security

Note: CISSP® exams are not hosted by SANS. You will need to make separate arrangements to take the CISSP® exam.

giac.org

sans.org/ondemand

sans.org/8570

Take advantage of SANS' CISSP® Get Certified Program currently being offered.

sans.org/special/cissp-get-certified-program

MANAGEMENT 512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program
Mon, Dec 14 - Fri, Dec 18
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop NOT Needed
Instructor: G. Mark Hardy

- GIAC Cert: GSLC
- STI Master's Program
- OnDemand Bundle
- DoDD 8570

"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.

"MGT512 has great info for newly assigned managers to cybersecurity."
-Kerry T.,
U.S. Army Corps of Engineers

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.

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 their technical people are telling them

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!

G. Mark Hardy *SANS Certified Instructor*

G. Mark Hardy is founder and President of the National Security Corporation. He has been providing cybersecurity expertise to government, military, and commercial clients for over 30 years, and is an internationally recognized expert who has spoken at over 250 events world-wide. He serves on the Advisory Board of CyberWATCH, an Information Assurance/Information Security Advanced Technology Education Center of the National Science Foundation. A retired U.S. Navy Captain, he was privileged to serve in command nine times, including responsibility for leadership training for 70,000 sailors. He also served as wartime Director, Joint Operations Center for U.S. Pacific Command, and Assistant Director of Technology and Information Management for Naval Logistics in the Pentagon, with responsibility for INFOSEC, Public Key Infrastructure, and Internet security. Captain Hardy was awarded the Defense Superior Service Medal, the Legion of Merit, five Meritorious Service Medals, and 24 other medals and decorations. A graduate of Northwestern University, he holds a BS in Computer Science, BA in Mathematics, Masters in Business Administration, and a Masters in Strategic Studies, and holds the GSLC, CISSP, CISM, and CISA certifications. @g_mark

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

You Will Be Able To

- Establish a minimum standard for IT security knowledge, skills, and abilities. In a nutshell, this course covers all of the non-operating system topics that are in SANS Security Essentials, though not to the same depth. The goal is 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.

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; The 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.

NEW

MANAGEMENT 514

IT Security Strategic Planning, Policy, and Leadership

Five-Day Program
Mon, Dec 14 - Fri, Dec 18
9:00am - 5:00pm
30 CPEs
Laptop NOT Needed
Instructor: Mark Williams
- STI Master's Program
- OnDemand Bundle

"Excellent training with encyclopedia coverage of the topic. The instructor is fantastic with lots of wisdom and real-life examples."
-Alexander Kotkov, Ernst and Young

"As I progress in my career within cybersecurity, I find that courses such as MGT514 allow me to plan and lead my organization forward."
-Eric Burgan, Idaho National Labs

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:

Who Should Attend

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

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, case scenarios, 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.

Mark Williams *SANS Instructor*

Mark Williams currently holds the position of Principal Systems Security Officer at BlueCross BlueShield of Tennessee. Mark holds multiple certifications in security and privacy including the CISSP, CISA, CRISC, and CIPP/IT. He has authored and taught courses at undergraduate and graduate levels, as well as public seminars around the world. He has worked in public and private sectors in the Americas, Canada, and Europe in the fields of security, compliance, and management. Mark has more than 20 years of international high-tech business experience working with major multinational organizations, governments, and private firms. During his career Mark has consulted on issues of privacy and security, led seminars, and developed information security, privacy, and compliance programs.

514.1 Strategic Planning Foundations

Creating security strategic plans requires 1) a fundamental understanding of the business, and 2) 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

You Will Be Able To

- Develop security strategic plans
- Understand business and organization drivers
- Develop a stakeholder management strategy
- Conduct Porter's, PEST, and SWOT analysis
- Understand threat actors and their motivations
- Market and communicate your strategic plans
- Understand approaches for creating a security business case
- Develop and assess security policy
- Manage the policy creation process
- Understand the use of leadership competencies
- Motivate and inspire your teams
- Analyze case studies from leading universities

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 pioneers 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

"The instructor not only provided relevant content, he delivered it in an engaging way."
-Brian Cook, SANS 2015 student

SANS Technology Institute
sans.edu

Bundle OnDemand
with this course
sans.org/ondemand

"I loved the enthusiasm and life experience that was brought into class."
-SANS Scottsdale 2015 student

AUDIT 507

Auditing & Monitoring Networks, Perimeters, and Systems

SANS

Six-Day Program
Mon, Dec 14 - Sat, Dec 19
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: David Hoelzer

- GIAC Cert: GSNA
- STI Master's Program
- OnDemand Bundle
- DoDD 8570

"AUD507 provided me additional insight to the technical side of security auditing. Great course and a super instructor!"
-Carlos E., U.S. Army

"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

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? 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. Each student is 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.

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

David Hoelzer *SANS Faculty Fellow*

David Hoelzer is the 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 for the Center for Cybermedia Research and for 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. He 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. @david_hoelzer

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

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 applications 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

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

giac.org

sans.edu

sans.org/ondemand

sans.org/8570

DEVELOPER 544

Secure Coding in .NET: Developing Defensible Applications

SANS

Four-Day Program
Mon, Dec 14 - Thu, Dec 17
9:00am - 5:00pm
24 CPEs
Laptop Required
Instructors Aaron Cure

- GIAC Cert: GSSP-.NET
- STI Master's Program
- OnDemand Bundle

"DEV544 has useful information on static and dynamic analysis as well as code reviews."

-Daryl Webb, Highway Safety and Motor Vehicles

giac.org

sans.edu

Bundle OnDemand
with this course
sans.org/ondemand

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?

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

DEV544: Secure Coding in .NET: Developing Defensible Applications will help students leverage built-in and custom defensive technologies to integrate security into their applications. 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.

You Will Learn How To:

- Understand attackers' methodologies and how they will attack your web application
- Apply defensive coding techniques to prevent your application from being compromised
- Safeguard your sensitive information using approved cryptography standards
- Find vulnerabilities in your application using code review and basic penetration testing techniques
- Integrate security into your software development lifecycle

Aaron Cure *SANS Instructor*

Aaron is a senior security consultant at Cypress Data Defense and an instructor and contributing author for the DEV544 Secure Coding in .NET course. After 10 years in the U.S. Army as a Russian Linguist and a Satellite Repair Technician, he worked as a database administrator and programmer on the Iridium project, with subsequent positions as a telecommunications consultant, senior programmer, and security consultant. He also has experience developing security tools, performing secure code reviews, vulnerability assessments, and penetration testing, as well as risk assessments, static source code analysis, and security research. Aaron holds the GIAC GSSP-.NET, GWAPT, GMOB, and CISSP certifications and is located in Arvada, CO. Outside the office Aaron enjoys boating, travel, and playing hockey.

LEGAL 523

Law of Data Security and Investigations

SANS

Five-Day Program
Mon, Dec 14 - Fri, Dec 18
9:00am - 5:00pm
30 CPE/CMU Credits
Laptop NOT Needed
Instructor: Benjamin Wright

- GIAC Cert: GLEG
- STI Master's Program
- OnDemand Bundle

ATTEND REMOTELY

SIMULCAST

If you are unable to attend this event, this course is also available via SANS Simulcast.

More info on page 59

giac.org

sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

- **New for live delivery 2015: Sony Pictures' alleged denial of service attack on sites dumping its stolen corporate data.**
- **New for live delivery as of October 2014: Home Depot's legal and public statements about payment card breach.**
- **New legal tips on confiscating and interrogating mobile devices.**
- **New for live delivery as of April 2014: Course covers lawsuit by credit card issuers against Target's QSA and security vendor, Trustwave.**

Who Should Attend

- Investigators
- Security and IT professionals
- Lawyers
- Paralegals
- Auditors
- Accountants
- Technology managers
- Vendors
- Compliance officers
- Law enforcement
- Privacy officers
- Penetration testers

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 business, contracts, fraud, crime, IT security, liability and policy – 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.

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. We will cover recent stories ranging from Home Depot's legal and public statements about a payment card breach to the lawsuit by credit card issuers against Target's QSA and security vendor, Trustwave.

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.

"I have gained many valuable ideas and tools to support and defend my organization and to strengthen security over all. I wish I'd taken LEG523 3-4 years ago."
-Tom S., Case Western Reserve University

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. Mr. Wright 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

INDUSTRIAL CONTROL SYSTEMS 410

ICS/SCADA Security Essentials

SANS

Five-Day Program
Mon, Dec 14 - Fri, Dec 18
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Justin Searle
- GIAC Cert: GICSP
- OnDemand Bundle

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

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

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. In addition, 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.

ATTEND REMOTELY

SIMULCAST

If you are unable to attend this event, this course is also available via SANS Simulcast.

More info on page 59

GICSP

giac.org

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

Justin Searle *SANS Certified Instructor*

Justin Searle is a Managing Partner of UtiliSec, specializing in Smart Grid security architecture design and penetration testing. Justin led the Smart Grid Security Architecture group in the creation of NIST Interagency Report 7628 and played key roles in the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG). He currently leads the testing group at the National Electric Sector Cybersecurity Organization Resources (NESCOR). Justin has taught courses in hacking techniques, forensics, networking, and intrusion detection for multiple universities, corporations, and security conferences. In addition to electric power industry conferences, Justin frequently presents at top international security conferences such as Black Hat, DEFCON, OWASP, Nullcon, and AusCERT. Justin co-leads prominent open-source projects including the Samurai Web Testing Framework (SamuraiWTF), the Samurai Security Testing Framework for Utilities (SamuraiSTFU), Middler, Yokoso!, and Laudanum. Justin has an MBA in International Technology and is a CISSP and SANS GIAC certified Incident Handler (GCIH), Intrusion Analyst (GCIA), and Web Application Penetration Tester (GWAPT). @meeas

SANS Hosted is a series of courses presented by other educational providers at SANS Cyber Defense Initiative 2015 to complement your needs for training outside of our current course offerings.

HOSTED

(ISC)²® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Training Seminar

Five-Day Course | Mon, Dec 14 - Fri, Dec 18 | 9:00am - 5:00pm | 30 CPEs | Laptop NOT Needed | Instructor: Staff

This course will help you advance your software development expertise by ensuring you're properly prepared to take on the constantly evolving vulnerabilities exposed in the SDLC. It will train you on every phase of the software lifecycle detailing security measures and best practices for each phase. The CSSLP® Education Program is for all the stakeholders involved in software development. By taking this course, you will enhance your ability to develop software with more assurance and better understand how to build security within each phase of the software lifecycle.

The comprehensive (ISC)² CSSLP® CBK® Education program covers the following domains:

- **Secure Software Concepts** – know what constitutes secure software and what design aspects to take into consideration to architect hack-resilient software
- **Secure Software Requirements** – capturing all of the security requirements from various stakeholders and understanding the sources and processes needed to ensure a more effective design
- **Secure Software Design** – secure design elements, software architecture, secure design review, and conduct threat modeling
- **Secure Software Implementation/Coding** – secure coding practices, vulnerabilities to look for, and how to review the code to ensure that there are no errors in it or in the code or security controls
- **Secure Software Testing** – integrated software testing for security functionality, reliability, resiliency to attack, and recoverability
- **Software Acceptance** – security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria and methods of independent testing
- **Software Deployment, Operations, Maintenance and Disposal** – security issues around steady state operations and management of software. security measures that must be taken when a product reaches its end of life
- **Supply Chain and Software Acquisition** – provides a holistic outline of the knowledge and tasks required in managing risk for outsourced development, acquisition, and procurement of software and related services

HOSTED

Physical Penetration Testing

Two-Day Course | Sat, Dec 12 - Sun, Dec 13 | 9:00am - 5:00pm | 12 CPEs | Laptop NOT Needed | Instructor: The CORE Group

Physical security is an oft-overlooked component of data and system security in the technology world. While frequently forgotten, it is no less critical than timely patches, appropriate password policies, and proper user permissions. You can have the most hardened servers and network but that doesn't make the slightest difference if someone can gain direct access to a keyboard or, worse yet, march your hardware right out the door.

Those who attend this session will leave with a full awareness of how to best protect buildings and grounds from unauthorized access, as well as how to compromise most existing physical security in order to gain access themselves. Attendees will not only learn how to distinguish good locks and access controls from poor ones, but will also become well-versed in picking and bypassing many of the most common locks used in North America in order to assess their own company's security posture or to augment their career as a penetration tester.

SECURITY 440

Critical Security Controls: Planning, Implementing, and Auditing

Two-Day Course | Sat, Dec 12 - Sun, Dec 13 | 9:00am - 5:00pm | 12 CPEs | Laptop NOT Needed | Instructor: Jason Fossen

This course will help you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Council on CyberSecurity. The 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. They were selected and defined by the U.S. military and other government and private organizations (including NSA, DHS, GAO, and many others) that are the most respected experts on how attacks actually work and what can be done to stop them. These entities defined the 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. If you are looking for hands-on labs involving the Critical Controls, you should take SEC566.***

You will find the full document describing the Critical Security Controls posted on the Council on CyberSecurity at **http://www.cisecurity.org**

One of the best features of the course is that it uses offense to inform defense. In other words, you will learn about the actual attacks that you'll be stopping or mitigating. That makes the defenses very real, and it makes you a better security professional.

As a student of the Critical Security Controls two-day course, you'll learn important skills that you can take back to your workplace and use your first day back on the job in implementing and auditing each of the controls.

SECURITY 580

Metasploit Kung Fu for Enterprise Pen Testing

Two-Day Course | Sat, Dec 12 - Sun, Dec 13 | 9:00am - 5:00pm | 12 CPEs | Laptop Required | Instructor: Bryce Galbraith

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 with confirming 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.

MANAGEMENT 415

A Practical Introduction to Cyber Security Risk Management

NEW

Two-Day Course | Sat, Dec 12 - Sun, Dec 13 | 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 that could exist, 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.

MANAGEMENT 433

Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Program

Two-Day Course | Sat, Dec 12 - Sun, Dec 13 | 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.

ATTEND REMOTELY

SIMULCAST

If you are unable to attend this event, this course is also available via SANS Simulcast.

More info on page 59

MANAGEMENT 535

Incident Response Team Management

Two-Day Course | Sat, Dec 12 - Sun, Dec 13 | 9:00am - 5:00pm | 12 CPEs | Laptop Required | Instructor: Christopher Crowley

This course discusses the often-neglected topic of managing an incident response team. Given the frequency and complexity of today's cyber attacks, incident response is a critical function for organizations. Incident response is the last line of defense.

Detecting and efficiently responding to incidents requires strong management processes, and managing an incident response team requires special skills and knowledge. A background in information security management or security engineering is not sufficient for managing incidents. On the other hand, incident responders with strong technical skills do not necessarily become effective incident response managers. Special training is necessary.

This course was originally developed by Dr. Eugene Schultz, the founder of the first U.S. government incident response team and an information security professional with over 26 years of experience. The course has been updated to address current issues such as the advanced persistent threat, incident response in the cloud, and threat intelligence.

BONUS SESSIONS

SANS@Night Evening Talks

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: What's New for Security in Windows 10 and Server 2016?

Jason Fossen

Windows 8 was a flop, worse than Vista, so will Windows 10 be successful? The return of the Start Menu, touch screen integration, the faster Edge browser, and Cortana should make Windows 10 popular with users. Windows 10 also includes significant changes for security and manageability in large organizations, such as "Windows as a Service" rolling updates and deeper integration with Azure Active Directory. In this lively talk, Jason Fossen, author of the Securing Windows (SEC505) course at SANS, will lay out what to love and fear in Windows 10 and Windows Server 2016. We will also talk about some of the epic changes going on at Microsoft, now that CEO Steve Ballmer is gone. Is it really a new era for Microsoft? Come join the presentation and see what Microsoft is betting its future on!

The 14 Absolute Truths of Security

Keith Palmgren

Keith Palmgren has identified 14 "Absolute Truths" of security – things that remain true regardless of circumstance, network topology, organizational type, or any other variable. Recognizing these 14 absolute truths and how they affect a security program can lead to the success of that program. Failing to recognize these truths will spell almost certain doom. Here we will take a non-technical look at each of the fourteen absolute truths in turn, examine what they mean to the security manager, what they mean to the security posture, and how understanding them will lead to a successful security program.

The Crazy New World of Cyber Investigations: Law, Ethics and Evidence

Benjamin Wright

Increasingly, employers and enterprises are engaged in cyber investigations. The explosion of cyber evidence (email, text, meta data, social media, etc.) about every little thing that anyone does or says creates a massive need for HR departments, IT departments, internal audit departments and other investigators to find and sift through this evidence. These cyber investigations are guided, motivated and restricted by a blizzard of new laws and court cases. Increasingly enterprises need professionals with backgrounds in cyber forensics, cyber law and computer privacy.

The Tap House

Philip Hagen

Packets move pretty fast. The field of Network Forensics needs to move fast, too. Whether you are investigating a known incident, hunting unidentified adversaries in your environment, or enriching forensic findings from disk- and memory-based examinations, it's critical to stay abreast of the latest developments in the discipline. In this SANS@Night talk, Philip Hagen will discuss some of the latest technologies, techniques, and tools that you will want to know in pursuit of forensication nirvana. Philip is also an avid craft beer fan, so there's a good chance you will learn something about a new notable national or interesting local beer in the process. This presentation will be helpful for those that wish to keep up-to-date on the most cutting-edge facets of Network Forensics.

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 triage the incident to 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 evening talk will help you start learning how to turn malware inside out.

Debunking the Complex Password Myth

Keith Palmgren

Perhaps the worse advice you can give a user is "choose a complex password." The result is the impossible-to-remember password requiring the infamous sticky note on the monitor. In addition, that password gets used at a dozen sites at home, AND the very same password gets used at work. The final result ends up being the devastating password compromise. In this one-hour talk, we will look at the technical and non-technical (human nature) issues behind passwords. Attendees will gain a more complete understanding of passwords and receive solid advice on creating more easily remembered AND significantly stronger passwords at work and at home, for their users, for themselves, and even for their children.

The Plinko Board of Modern Persistence Techniques

Alissa Torres

No matter what techniques an attacker employs to hide and persist on compromised remote systems, we must be up for the challenge to detect, analyze and remediate. This session focuses on the latest techniques modern malware is using to ensure continued presence in your network. As detailed in recently released industry threat intelligence reports, these methods are increasing in sophistication and are often missed by forensics tools developed to only enumerate common autorun and service persistence methods. In this presentation, we will cover advanced detection techniques, pivoting from physical memory analysis to the examination of remnants found on the file system.

Offensive Countermeasures, Active Defenses, and Internet Tough Guys

John Strand

In this presentation John Strand will demonstrate the Active Defense Harbinger Distribution, a DARPA funded, free Active Defense virtual machine. He will debunk many of the myths, outright lies, and subtle confusions surrounding taking active actions against attackers. From this presentation, you will not only know how to take action against attackers, you will learn how to do it legally.

Automating Post-Exploitation with PowerShell

James Tarala

As organizations assess the security of their information systems, the need for automation has become more and more apparent. Not only are organizations attempting to automate their assessments, the need is becoming more pressing to perform assessments centrally against large numbers of enterprise systems. Penetration testers can use this automation to make their post-exploitation efforts more thorough, repeatable, and efficient. Defenders need to understand the techniques attackers are using once an initial compromise has occurred so they can build defenses to stop the attacks. Microsoft's PowerShell scripting language has become the de facto standard for many organizations looking to perform this level of distributed automation. In this presentation James Tarala, of Enclave Security, will describe to students the enterprise capabilities PowerShell offers and show practical examples of how PowerShell can be used to perform large scale penetration tests of Microsoft Windows systems.

Evolving Threats and Defenses

Paul A. 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 attacker's 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. This presentation will highlight recent/current developments in the evolution of both attacks and defenses.

ICS/SCADA Cyber Attacks – Fact vs. Fiction

Robert M. Lee

Industrial Control Systems (ICS) play a huge role in almost every aspect of modern day life. Supervisory control and data acquisition (SCADA) as an example play a large role in monitoring and controlling the power grid, oil pipelines, and more. It's understandable then that they gain attention in national headlines when they come under attack. Unfortunately, getting the technical details right is so difficult that these stories are often incorrect. The resulting hype and confusions drive the investment of resources into trying to solve the wrong problem. The threat is real, but plenty of the stories are not. In this presentation, Robert M. Lee, author of ICS515 and co-author of FOR578, will break down a number of high-profile stories that are fiction and then deconstruct real threats to show the actual issues in the community and what can be learned for defense.

Information Security Risk Management – No Exceptions!

Mark Williams

As a risk analyst or manager, it is likely that your days are filled with requests for exceptions to policy to permit people to do things wrong. I believe there is a better way. Permitting exceptions can be a valuable tool in developing a process life cycle. It can also become an easy way to avoid making decisions to upgrade or improve systems. We are all faced daily with decisions on whether to permit exceptions. Let me show you how I think that continuous risk assessment and risk management can actually avoid the need for exceptions. By using a logical approach to risk identification, categorization and decision making, you too can do the "impossible" and say: NO EXCEPTIONS!

Securing The Kids

Lance Spitzner

Technology 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 today's world they have to know how to leverage these new tools. However, with all these capabilities come new risks, risks that as parents we may not understand or even be aware of. In this interactive talk we discuss the top three risks to kids online and the steps parents are taking to educate and protect them.

Card Fraud 101

G. Mark Hardy

Ever get a call from your bank saying your credit card was stolen, yet it is still in your wallet? What's going on here? Card fraud costs $16 billion annually, and the problem is getting worse. Target, PF Changs, Michaels, Home Depot, who's next? Find out how these big card heists are pulled off, why chip-and-pin won't solve the fraud problem, and how crooks compromised Apple Pay. See if your bank even bothers to use the security protections it could – we'll have a mag stripe card reader so you can really see what's in your wallet. Certified SANS Instructor G. Mark Hardy is the CEO and founder of CardKill Inc., a start-up that helps banks preemptively kill stolen cards BEFORE they are used in fraud.

The Effectiveness of Microsoft's EMET

Stephen Sims

In this talk we will take a look at Microsoft's Enhanced Mitigation Experience Toolkit (EMET) and how it stops exploits from working. This free tool has a low adoption rate inside of companies, but has the ability to stop 0-day attacks from being successful. We will cover the effectiveness of the various controls, how they work, as well as techniques used to bypass the tool in targeted attacks.

Vendor-Sponsored Events

Vendor Expo

Wed, Dec 16 | 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 Lunch

Wed, Dec 16 | 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 SANS Cyber Defense Initiative 2015, 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!

Vendor Welcome Reception

Wed, Dec 16 | 5:30pm - 7:30pm

This informal reception allows you to visit exhibits and participate in some exciting activities. This is a great time to mingle with your peers and experience first-hand the latest in information security tools and solutions with interactive demonstrations. Enjoy appetizers and beverages while comparing experiences with other attendees regarding the solutions they are employing to address security threats in their organization.

ARE YOU GIAC CERTIFIED?

Risk management is a top priority. The security of your critical assets depend on the skills and knowledge of your security team.

Don't take chances with one-size-fits-all security certification.

Get GIAC certified!

GIAC offers over 30+ specialized certifications in cybersecurity, forensics, penetration testing, web application security, IT audit, management, cybersecurity law, and industrial control systems.

"GIAC is the only certification that proves you have hands-on technical skills."
-CHRISTINA FORD, DEPARTMENT OF COMMERCE

"GIAC Certification demonstrates an applied knowledge versus studying a book."
-ALAN C, USMC

Learn more about GIAC and how to *Get Certified* at www.giac.org

@CertifyGIAC

linkedin.com/company/GIAC

Bundle GIAC Certification with SANS training and *SAVE $330!*

NEW GIAC CERTIFICATION:

CONTINUOUS MONITORING (GMON)

Available December 2015

Successful **GMON** candidates will demonstrate the ability to securely architect a network resistant to breaches and that lends itself to monitoring. They will also demonstrate their ability to **monitor**, **analyze**, and **detect threats** and **anomalies** on the network.

The **GMON** is targeted towards **security architects**, **engineers**, **analysts**, and **managers** who want to demonstrate their ability to assess and implement defensible security architecture and continuous cyber-security monitoring.

www.giac.org/gmon

SANS Technology Institute

The SANS Technology Institute transforms the world's best cybersecurity training and certifications into a comprehensive, rigorous, graduate education experience.

"I was challenged by both the coursework and faculty. Earning a graduate degree from SANS had a direct and positive influence on my career."

-**Russ McRee, MSISE**
Director, Security Response & Investigations, Microsoft

POST-9/11 GI BILL

The SANS Technology Institute is approved to accept and/or certify Veterans for education benefits. Programs also typically qualify for corporate tuition reimbursement plans.

GIAC — Global Information Assurance Certification — www.giac.org

Students earn industry-recognized GIAC certifications during their course of studies.

Master of Science Degrees

- Master of Science in Information Security Engineering (MSISE)
- Master of Science in Information Security Management (MSISM)

Graduate Certificates

- Cybersecurity Engineering (Core)
- Cyber Defense Operations
- Penetration Testing and Ethical Hacking
- Incident Response

To learn more, visit **www.sans.edu** or email **info@sans.edu**

The SANS Technology Institute, an independent subsidiary of SANS, is accredited by The Middle States Commission on Higher Education (3624 Market Street, Philadelphia, PA 19104 – 267.284.5000), an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

Top 5 Reasons

why SANS customers use CyberTalent Assessments to manage their cyber talent.

SANS Leadership

SANS is the most trusted, and the largest source for information security training and certification in the world.

Reduce Hiring Costs

Cyber Talent Assessments provide more information and better insight which lower your risk of costly hiring mistakes.

Better Team Management

A simple, easy to use tool that helps you identify your team's specific needs, map your talent portfolio, and develop personalized training plans for each member of your team.

Ensure Contractor's Skills

CyberTalent Assessments provide a reliable, effective way to be sure your contractor support has the skills you need.

Prepare for Today's Threats

CyberTalent Assessments help ensure your team is ready for the changing threat landscape.

SANS CyberTalent offers three web-based assessments:

- Cyber Defense
- Penetration Testing
- Digital Forensics

Start improving your cyber talent management today. There's no reason to wait.

SANS | CyberTalent

sans.org/cybertalent

Contact: dbrown@sans.org or mshuftan@sans.org

Sign up for a FREE demo

sans.org/cybertalent/free-demo

SANS ONLINE TRAINING Gives You More Options

Simulcast sans.org/event/cyber-defense-initiative-2015/attend-remotely

The following courses will be Simulcast live from CDI 2015:

SEC401 | SEC505 | SEC560 | FOR508 | LEG523 | ICS410 | MGT433

OnDemand Bundles sans.org/ondemand/bundles

Bundle four months of online study with your live course for just $659 with an OnDemand Bundle. The additional study will reinforce your learning through quizzes, labs, access to subject-matter experts and more.

vLive sans.org/vlive

Train live and online in the evenings via SANS' vLive format, which also provides six months of online access to your course mp3s, presentations, and labs.

For more information about any of SANS' flexible online training formats, visit sans.org/online

SANS SECURING THE HUMAN

Security Awareness Training by the Most Trusted Source

Computer-based Training for your Employees

End User
Phishing
CIP v5
ICS Engineers
Developers
Healthcare

- Let employees train on their own schedule
- Tailor modules to address specific audiences
- Courses translated into many languages
- Test learner comprehension through module quizzes
- Track training completion for compliance reporting purposes
- Test employee behavior through phishing emails

Visit SANS Securing The Human at
securingthehuman.sans.org

Change Human Behavior | Manage Risk | Maintain Compliance | Protect Your Brand

FUTURE SANS TRAINING EVENTS

Information on all events can be found at sans.org/security-training/by-location/all

Baltimore
2015

Baltimore, MD
September 21-26

Seattle
2015

Seattle, WA
October 5-10

Tysons Corner
2015

Tysons Corner, VA
October 12-17

Cyber Defense San Diego
2015

San Diego, CA
October 19-24

South Florida
2015

Fort Lauderdale, FL
November 9-14

Pen Test Hackfest
SUMMIT & TRAINING 2015

Alexandria, VA
November 16-23

San Francisco
2015

San Francisco, CA
Nov 30 - Dec 5

Security Leadership
SUMMIT & TRAINING 2015

Dallas, TX
December 3-10

Las Vegas
2016

Las Vegas, NV
January 9-14

Security East
2016

New Orleans, LA
January 25-30

Scottsdale
2016

Scottsdale, AZ
February 8-13

McLean
2016

McLean, VA
February 15-20

Anaheim
2016

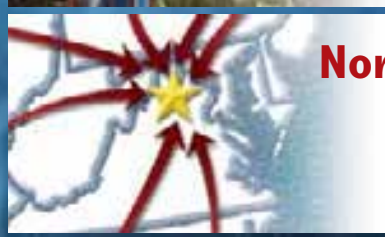
Anaheim, CA
February 22-27

Philadelphia
2016

Philadelphia, PA
Feb 29 - Mar 5

SANS 2016

Orlando, FL
March 12-21



Northern Virginia
2016

Reston, VA
April 4-9

FUTURE SANS TRAINING EVENTS

Information on all events can be found at sans.org/security-training/by-location/all

Threat Hunting & Incident Response
SUMMIT & TRAINING 2016

New Orleans, LA
April 12-19

Atlanta
2016

Atlanta, GA
April 18-23

Austin
2016

Austin, TX
April 18-23

Security West
2016

San Diego, CA
May 1-6

Houston
2016

Houston, TX
May 9-14

Baltimore
2016

Baltimore, MD
May 9-14

SANSFIRE
2016

Washington, DC
June 13-20

Salt Lake City
2016

Salt Lake City, UT
June 27 - July 1

Rocky Mountain
2016

Denver, CO
July 11-16

Minneapolis
2016

Minneapolis, MN
July 18-23

San Antonio
2016

San Antonio, TX
July 18-23

San Jose
2016

San Jose, CA
July 25-30

Boston
2016

Boston, MA
August 1-6

Private Training

Live Onsite Training at Your Office Location. Both In-person and Online Options Available.

sans.org/private-training

Community SANS

Live Training in Your Local Region with Smaller Class Sizes

sans.org/community

Mentor

Live Multi-Week Training with a Mentor

sans.org/mentor

BUILD YOUR BEST CAREER

WITH:

SANS

Add an

OnDemand Bundle & **GIAC Certification Attempt**

to your course within seven days of this event for just $659 each.

SPECIAL PRICING

OnDemand Bundle

- Four months of supplemental online review
- 24/7 online access to your course lectures, materials, quizzes, and labs
- Subject-matter expert support to help you increase your retention of course material

"The course content and OnDemand delivery method have both exceeded my expectations."

-Robert Jones, Team Jones, Inc.

GIAC Certification

- Distinguish yourself as an information security leader
- 30+ GIAC certifications to choose from
- Two practice exams included
- Four months of access to complete the attempt

"GIAC is the only certification that proves you have hands-on technical skills."

-Christina Ford, Department of Commerce

MORE INFORMATION

www.sans.org/ondemand/bundles www.giac.org

HOTEL INFORMATION

Training Campus

Grand Hyatt Washington

1000 H Street NW

Washington, DC 20001

sans.org/event/cyber-defense-initiative-2015/location

Experience the upscale elegance of Grand Hyatt Washington, a full-service Washington, DC hotel. Centrally located in the trendy Penn Quarter near popular local attractions, Grand Hyatt Washington is a welcoming destination with a host of world-class services and amenities, and with convenient Metro Center access directly from the lobby.

Special Hotel Rates Available

A special discounted rate of $215.00 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 are only available through November 17, 2015. To make reservations, please use the following links:

For rooms at the SANS group rate:
https://aws.passkey.com/event/12679833/owner/544/home

For rooms at the government rate:
https://resweb.passkey.com/go/SansGovernmentRooms

You can also make reservations by calling Central Reservations at 888-421-1442 and asking for the SANS group rate.

Weather Conditions

December in Washington, DC is mild with highs around 48° and lows near 28°. For the latest weather conditions and forecast, please consult weather.com.

Top 5 reasons to stay at the Grand Hyatt Washington:

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 Grand Hyatt Washington, you gain the opportunity to further network with your industry peers and remain at the center of activities surrounding the training event.
4. SANS schedules morning and evening events at the Grand Hyatt Washington that you won't want to miss!
5. Everything is in one convenient location!

REGISTRATION INFORMATION

We recommend you register early to ensure you get your first choice of courses.

How to Register

1. To register, go to sans.org/event/cyber-defense-initiative-2015/courses.

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. We do not take registrations by phone.

2. Provide payment information.

3. Print your invoice.

4. An email confirmation will arrive soon after you register.

Use code **EarlyBird15** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	10/21/15	$400.00	11/11/15	$200.00

Some restrictions apply.

Group Savings (Applies to tuition only)

10% discount if 10 or more people from the same organization register at the same time

5% discount if 5-9 people from the same organization register at the same time

To obtain a group discount, complete the discount code request form at sans.org/security-training/discounts prior to registering.

To register for a CDI 2015 Simulcast course, please visit sans.org/event/cyber-defense-initiative-2015/attend-remotely

Group Discounts for SANS Security Training

sans.org/vouchers

SANS Universal Voucher Credit Program

The ***SANS Universal Voucher Credit Program*** provides organizations of all sizes with a 12-month online account that is convenient and easy to manage. SANS will maximize your training investment by providing you with bonus credits. SANS Universal Voucher Credits can be used for any SANS live or online training format as well as GIAC certification exams. This will give you maximum flexibility and an easy one-time procurement process.

Get GIAC Certified!

- Only $659 when combined with SANS training
- Deadline to register at this price is the last day of SANS CDI 2015
- Price goes to $979 after deadline
- Register today at registration@sans.org

Frequently Asked Questions

Frequently asked questions about SANS Training and GIAC Certification are posted at giac.org/overview/faq.php.

Cancellation Policy

If an attendee must cancel, a substitution request may be made at any time. Processing fees will apply. All substitution requests must be submitted by e-mail to registration@sans.org.

If an attendee must cancel without substitution, a refund can be issued for any received payments. All cancellation requests must be submitted in writing by mail or fax and postmarked by November 18, 2014. Payments will be refunded by the method that they were submitted. Processing fees will apply. No refunds will be given after the stated deadline. Accessed online materials cannot be transferred to a substitute or have payments refunded.

Find complete details at sans.org/cdi

SANS CYBER DEFENSE INITIATIVE 2015 REGISTRATION FEES

Register online at sans.org/event/cyber-defense-initiative-2015/courses

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 10/21/15	Paid before 11/11/15	Paid after 11/11/15	Add GIAC Cert	Add OnDemand	Add NetWars Continuous
☐ SEC301	Intro to Information Security	$4,885	$5,085	$5,285	☐ $659	☐ $659	☐ $1,199
☐ SEC401	Security Essentials Bootcamp Style	$5,620	$5,820	$6,020	☐ $659	☐ $659	☐ $1,199
☐ SEC501	Advanced Security Essentials – Enterprise Defender	$5,620	$5,820	$6,020	☐ $659	☐ $659	☐ $1,199
☐ SEC503	Intrusion Detection In-Depth	$5,620	$5,820	$6,020	☐ $659	☐ $659	☐ $1,199
☐ SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling	$5,620	$5,820	$6,020	☐ $659	☐ $659	☐ $1,199
☐ SEC505	Securing Windows with PowerShell and the Critical Security Controls	$5,510	$5,710	$5,910	☐ $659	☐ $659	☐ $1,199
☐ SEC511	Continuous Monitoring and Security Operations	$5,620	$5,820	$6,020	☐ $659	☐ $659	☐ $1,199
☐ SEC550	Active Defense, Offensive Countermeasures and Cyber Deception **NEW!**	$4,885	$5,085	$5,285			☐ $1,199
☐ SEC560	Network Penetration Testing and Ethical Hacking	$5,620	$5,820	$6,020	☐ $659	☐ $659	☐ $1,199
☐ SEC566	Implementing and Auditing the Critical Security Controls – In-Depth	$4,885	$5,085	$5,285	☐ $659	☐ $659	☐ $1,199
☐ SEC575	Mobile Device Security and Ethical Hacking	$5,620	$5,820	$6,020	☐ $659	☐ $659	☐ $1,199
☐ SEC579	Virtualization and Private Cloud Security	$5,620	$5,820	$6,020		☐ $659	☐ $1,199
☐ SEC660	Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	$5,620	$5,820	$6,020	☐ $659	☐ $659	☐ $1,199
☐ AUD507	Auditing & Monitoring Networks, Perimeters, and Systems	$5,510	$5,710	$5,910	☐ $659	☐ $659	☐ $1,199
☐ DEV544	Secure Coding in .NET: Developing Defensible Applications	$4,420	$4,620	$4,820	☐ $659	☐ $659	☐ $1,199
☐ FOR408	Windows Forensic Analysis	$5,620	$5,820	$6,020	☐ $659	☐ $659	☐ $1,199
☐ FOR508	Advanced Digital Forensics and Incident Response	$5,620	$5,820	$6,020	☐ $659	☐ $659	☐ $1,199
☐ FOR572	Advanced Network Forensics and Analysis	$5,620	$5,820	$6,020	☐ $659	☐ $659	☐ $1,199
☐ FOR578	Cyber Threat Intelligence **NEW!**	$5,095	$5,295	$5,495			☐ $1,199
☐ FOR610	Reverse-Engineering Malware: Malware Analysis Tools and Techniques	$5,620	$5,820	$6,020	☐ $659	☐ $659	☐ $1,199
☐ ICS410	ICS/SCADA Security Essentials	$4,885	$5,085	$5,285	☐ $659	☐ $659	☐ $1,199
☐ ICS515	ICS Active Defense and Incident Response **NEW!**	$4,885	$5,085	$5,285			☐ $1,199
☐ LEG523	Law of Data Security and Investigations	$4,885	$5,085	$5,285	☐ $659	☐ $659	☐ $1,199
☐ MGT414	SANS Training Program for CISSP® Certification	$4,990	$5,190	$5,390	☐ $659	☐ $659	☐ $1,199
☐ MGT512	SANS Security Leadership Essentials for Managers with Knowledge Compression™	$5,265	$5,465	$5,665	☐ $659	☐ $659	☐ $1,199
☐ MGT514	IT Security Strategic Planning, Policy, and Leadership **NEW!**	$4,885	$5,085	$5,285		☐ $659	☐ $1,199
☐ HOSTED	(ISC)²® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Training Seminar	$3,415	$3,415	$3,415			☐ $1,199

Skill-Based Short Courses		Course fee if taking a 4-6 day course	Course fee
☐ SEC440	Critical Security Controls: Planning, Implementing, and Auditing	$1,450	$2,250
☐ SEC580	Metasploit Kung Fu for Enterprise Pen Testing	$1,350	$2,130
☐ MGT415	A Practical Introduction to Cyber Security Risk Assessment **NEW!**	$1,350	$2,130
☐ MGT433	Securing The Human: How to Build, Maintain & Measure a High-Impact Awareness Program	$1,350	$2,130
☐ MGT535	Incident Response Team Management	$1,350	$2,130
☐ HOSTED	Physical Penetration Testing		$2,000
☐ SPECIAL	CORE NetWars Tournament – Tournament Entrance Fee	FREE	$1,450
☐ SPECIAL	DFIR NetWars Tournament – Tournament Entrance Fee	FREE	$1,450

Pay for any long course using the code EARLYBIRD15 at checkout by:

10/21/15 to get $400 OFF

11/11/15 to get $200 OFF

SANS NewsBites

Join over 200,000 professionals who subscribe to this high-level, executive summary of the most important news and issues relevant to cybersecurity professionals. Delivered twice weekly. Read insightful commentary from expert SANS instructors.

InfoSec Reading Room

Computer security research and whitepapers

Security Policies

Templates for rapid information security policy development

Top 25 Software Errors

The most widespread and critical errors leading to serious vulnerabilities

OUCH!

OUCH! is the world's leading free security awareness newsletter designed for the common computer user. Published every month and in multiple languages, each edition is carefully researched and developed by the SANS Securing The Human team, SANS instructor subject-matter experts, and team members of the community. Each issue focuses on a specific topic and actionable steps people can take to protect themselves, their family, and their organization.

Open a SANS Portal Account

Receive free webcasts, newsletters, the latest news and updates, and many other free resources.

sans.org/account

Webcasts

SANS Information Security Webcasts are live broadcasts by knowledgeable speakers addressing key issues in cybersecurity, often in response to breaking news about risks. Gain valuable information on topics you tell us are most interesting!

Critical Security Controls

Consensus guidelines for effective cyber defense

Industry Thought Leadership

In-depth interviews with the thought leaders in information security and IT

Intrusion Detection FAQ

The Internet's most trusted site for vendor-neutral intrusion detection information

@RISK: The Consensus Security Alert

@RISK provides a reliable weekly summary of:

- Newly discovered attack vectors
- Vulnerabilities with active new exploits
- Insightful explanations of how recent attacks worked and other valuable data

A key purpose of @RISK is to provide data that will ensure that the Critical Controls continue to be the most effective defenses for all known attack vectors.