

SANS FIRE 2016

Washington, DC | June 11-18



Training You Can Implement Immediately!

Courses in:

CYBER DEFENSE OPERATIONS

PEN TESTING

DIGITAL FORENSICS

ETHICAL HACKING

INCIDENT RESPONSE

SECURITY MANAGEMENT

APPLICATION SECURITY

IT AUDIT

Top SANS Instructors:

ED SKOUDIS

ROB LEE

MIKE POOR

JASON FOSSEN

JOHN STRAND

DAVID HOELZER

FRANK KIM

ERIC CONRAD

*Choose from 45+ courses
taught by our
world-class instructors*

*"In-depth, cutting-edge,
real-world knowledge
provided!"*

-JAMES BAKER, PASS KEY



GIAC Approved Training

SAVE \$400

Register & pay early! SEE PAGE 80 FOR DETAILS.

www.sans.org/sansfire

Dear Colleagues,

SANSFIRE 2016 will showcase 47 cutting-edge courses for all experience levels, a variety of evening talks, and opportunities for serious discussions with the best leaders in the industry and your peers. Top-rated instructors reaching outstanding courses will show you everything there is to know RIGHT NOW.



Johannes Ullrich, PhD

We will put you in touch with the resources and people you need to stay current because the InfoSec world can change in the time it takes to have a lunch break. SSL is now called TLS, passwords are out, and your out-of-date malware-signature file just got a little bit more out of date.

Brad Duncan, who provides updates for the Internet Storm Center whenever an exploit kit changes, will talk about some of his latest tricks. If you are looking for updated traffic patterns, or indicators of compromise, Brad's diaries have you covered. How do you extract useful indicators of compromise from an Exploit Kit? How do Exploit Kits work? He will walk you through the lifecycle of an Exploit Kit step by step to teach you how they work.

Sometimes you are a bit too late and cannot prevent an infection. Kevin Liston deals with this for a living, and during his evening talk, Managing Large-Scale Incident Response, he will teach you how to manage a large-scale incident response. If you have bad guys in your network, Kevin will keep you calm and organized while teaching you how to respond.

And what do you do with all the malware you recover every day? Our Internet Storm Center handler John Bambenek will explain how to deal with malware at scale by creating databases of indicators of compromise and, of course, while using open-source software. The best feeds of indicators of compromise are usually not the ones you pay money for from a vendor, but the ones you pay for in sweat and tears by analyzing malware found on your own network

Over the last year, we added new data and features to the Internet Storm Center. We can now provide great context to your logs through such elements as the "color my logs" feature, <https://colormylogs.com>. As it does every year, SANSFIRE 2016 will feature our "State of the Internet" panel. This year is a must-see as we will reveal new features and initiatives to make the Internet Storm Center better than ever.

Now is the perfect time to take the next step in your career. Cybersecurity is more vital, crucial, and important to the growth of your organization than ever before. SANSFIRE 2016 is where you can learn the skills, tips, and tricks from the experts to help you win the battle against the wide range of cyber adversaries that want to harm your environment.

We hope to see you in Washington DC in June!

Johannes Ullrich, PhD

Dean of Research for the SANS Technology Institute

[@johullrich](https://twitter.com/johullrich) [@sans_isc](https://twitter.com/sans_isc)

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

TECHNICAL INTRODUCTORY

SEC301
Intro to
Information Security
GISF

CORE

SEC401
Security Essentials
Bootcamp Style
GSEC

IN-DEPTH

SEC501
Advanced Security Essentials
— Enterprise Defender
GCED

CORE COURSES

SANS
IT SECURITY
TRAINING
AND YOUR
CAREER
ROADMAP

Penetration Testing/Vulnerability Assessment

CORE COURSES
SEC301 (GISF) ► SEC401 (GSEC)

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

NETWORK & EXPLOITS

SEC560
Network Penetration Testing
and Ethical Hacking
GPEN

SEC660
Advanced Penetration Testing,
Exploit Writing & Ethical Hacking
GXPN

SEC760
Advanced Exploit Development for
Penetration Testers

SPECIALIZATION

SEC573
Python for
Penetration Testers
GPYC

SEC580
Metasploit Kung Fu
for Enterprise
Pen Testing

WEB

SEC542
Web App Penetration Testing
and Ethical Hacking
GWAPT

SEC642
Advanced Web App
Penetration Testing
and Ethical Hacking

LAB-CENTERED

SEC561
Immersive Hands-on
Hacking Techniques

SEC562
CyberCity Hands-on
Kinetic Cyber Range
Exercise

MOBILE/WIRELESS

SEC575
Mobile Device Security and
Ethical Hacking
GMOB

SEC617
Wireless Ethical Hacking,
Penetration Testing & Defenses
GAWN

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
GCMON

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

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

Development – Secure Development

Securing The Human
for Developers —
STH.Developer
Application Security Awareness
Modules

DEV522

Defending Web Applications
Security Essentials
GWEB

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.

SAMPLE JOB TITLES

- Developer
- Software architect
- QA tester
- Development manager

DEV541

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

DEV544

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

SPECIALIZATION

SEC542

Web App Penetration
Testing and Ethical Hacking
GWAPT

SEC642

Advanced Web App
Penetration Testing
and Ethical Hacking

Cyber or IT Security Management

FOUNDATIONAL

MGT512

SANS Security Leadership Essentials for Managers with Knowledge Compression™
GS LC

MGT525

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

MGT414

SANS Training Program for CISSP® Certification
GIS P

CORE

MGT514

IT Security Strategic Planning, Policy, and Leadership

LEG523

Law of Data Security and Investigations
GLE G

MGT415

A Practical Introduction to Cybersecurity Risk Management

MGT535

Incident Response Team Management

SPECIALIZATION

AUD507

Auditing & Monitoring Networks, Perimeters, and Systems
GS NA

SEC566

Implementing and Auditing the Critical Security Controls — In-Depth
GC CC

MGT433

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

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.

SAMPLE JOB TITLES

- Security analyst/engineer
- SOC analyst
- Cyber threat analyst
- CERT member
- Malware analyst

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
GCI A

FOR572

Advanced Network Forensics and Analysis
GNFA

ENDPOINT ANALYSIS

FOR408

Windows Forensic Analysis
GC FE

FOR508

Advanced Digital Forensics and Incident Response
GC FA

MALWARE ANALYSIS

FOR610

Reverse-Engineering Malware: Malware Analysis Tools and Techniques
GREM

Digital Forensic Investigations and Media Exploitation

FOR408

Windows Forensic Analysis
GC FE

SEC504

Hacker Tools, Techniques, Exploits, and Incident Handling
GCIH

FOR508

Advanced Digital Forensics and Incident Response
GC FA

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 cyber crime, 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 cyber crime law enforcement agents to piece together a comprehensive account of what happened.

**Participate in either the CORE or DFIR NetWars Tournament
at SANSFIRE 2016 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: June 16-17

Prizes will be awarded at the conclusion of the games.

REGISTRATION IS LIMITED AND IS FREE

for students attending any long course at SANSFIRE 2016 (NON-STUDENT ENTRANCE FEE IS \$1,450).

Courses-at-a-Glance

For an up-to-date course list please check the website at
sans.org/event/sansfire-2016/schedule

Courses-at-a-Glance		For an up-to-date course list please check the website at sans.org/event/sansfire-2016/schedule		SAT 6-11	SUN 6-12	MON 6-13	TUE 6-14	WED 6-15	THU 6-16	FRI 6-17	SAT 6-18
SEC301	Intro to Information Security					PAGE 6					
SEC401	Security Essentials Bootcamp Style	SIMULCAST				PAGE 8					
SEC440	Critical Security Controls: Planning, Implementing and Auditing			P 69							
SEC501	Advanced Security Essentials – Enterprise Defender					PAGE 10					
SEC503	Intrusion Detection In-Depth					PAGE 12					
SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling	SIMULCAST				PAGE 14					
SEC505	Securing Windows with PowerShell and the Critical Security Controls					PAGE 16					
SEC511	Continuous Monitoring and Security Operations					PAGE 18					
SEC524	Cloud Security Fundamentals			P 69							
SEC542	Web App Penetration Testing and Ethical Hacking					PAGE 20					
SEC546	IPv6 Essentials			P 69							
SEC550	Active Defense, Offensive Countermeasures, and Cyber Deception					PAGE 22					
SEC560	Network Penetration Testing and Ethical Hacking	NEW! SIMULCAST				PAGE 24					
SEC561	Immersive Hands-On Hacking Techniques					PAGE 26					
SEC562	CyberCity Hands-on Kinetic Cyber Range Exercise					PAGE 23					
SEC566	Implementing and Auditing the Critical Security Controls – In-Depth					PAGE 28					
SEC567	Social Engineering for Penetration Testers	NEW!		P 70							
SEC575	Mobile Device Security and Ethical Hacking					PAGE 30					
SEC579	Virtualization and Private Cloud Security					PAGE 32					
SEC580	Metasploit Kung Fu for Enterprise Pen Testing	SIMULCAST		P 70							
SEC617	Wireless Ethical Hacking, Penetration Testing, and Defenses					PAGE 34					
SEC642	Advanced Web App Penetration Testing and Ethical Hacking					PAGE 36					
SEC660	Advanced Penetration Testing, Exploit Writing, and Ethical Hacking					PAGE 38					
SEC760	Advanced Exploit Development for Penetration Testers					PAGE 40					
FOR408	Windows Forensic Analysis	SIMULCAST				PAGE 42					
FOR508	Advanced Digital Forensics and Incident Response	SIMULCAST				PAGE 44					
FOR518	Mac Forensic Analysis	SIMULCAST				PAGE 46					
FOR572	Advanced Network Forensics and Analysis	SIMULCAST				PAGE 48					
FOR578	Cyber Threat Intelligence	NEW! SIMULCAST				PAGE 4					
FOR585	Advanced Smartphone Forensics					PAGE 50					
FOR610	Reverse-Engineering Malware: Malware Analysis Tools and Techniques					PAGE 52					
MGT305	Technical Communication and Presentation Skills for Security Professionals			P 70							
MGT414	SANS Training Program for CISSP® Certification					PAGE 54					
MGT415	A Practical Introduction to Cybersecurity Risk Management	NEW!		P 71							
MGT433	Securing The Human: How to Build, Maintain, and Measure a High-Impact Awareness Program	SIMULCAST		P 71							
MGT512	SANS Security Leadership Essentials for Managers with Knowledge Compression™					PAGE 56					
MGT514	IT Security Strategic Planning, Policy, and Leadership					PAGE 58					
MGT525	IT Project Management, Effective Communication, and PMP® Exam Prep					PAGE 60					
MGT535	Incident Response Team Management			P 71							
AUD507	Auditing & Monitoring Networks, Perimeters, and Systems					PAGE 62					
DEV522	Defending Web Applications Security Essentials					PAGE 63					
DEV541	Secure Coding in Java/JEE: Developing Defensible Applications			PAGE 64							
DEV544	Secure Coding in .NET: Developing Defensible Applications							PAGE 65			
ICS410	ICS/SCADA Security Essentials					PAGE 66					
ICS515	ICS Active Defense and Incident Response	NEW!				PAGE 5					
LEG523	Law of Data Security and Investigations					PAGE 67					
HOSTED	Healthcare Security Essentials	NEW!		P 68							
HOSTED	Physical Penetration Testing			P 68							
	NetWars Tournaments (CORE & DFIR)									P 2	

CONTENTS

NetWars Tournaments	2
Bonus Sessions/Vendor-Sponsored Events	72-73
SANS CyberTalent	74
SANS Securing The Human Program	74
SANS Technology Institute	75
New GIAC Certifications	75

SANS Training Formats (Live & Online)	76
SANS Voucher Program	77
Future SANS Training Events	78-79
Hotel Information	80
Registration Information	80
Registration Fees	81



NEW!

Five-Day Program
Mon, Jun 13 - Fri, Jun 17
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Jake Williams



"I absolutely loved this class! [A] great framework for CTI that I will use to be more effective."

-NATE DEWITT, eBay, Inc.

"Jake Williams is very good. Enjoyed all the real-life stories/situations and awareness."

-RIAZ AHMED, ITT

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.

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.

Who Should Attend

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

THERE IS NO TEACHER BUT THE ENEMY!



Jake Williams SANS Certified Instructor

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

NEW!

Five-Day Program
 Mon, Jun 13 - Fri, Jun 17
 9:00am - 5:00pm
 30 CPEs
 Laptop Required
 Instructor: Robert M. Lee

► II
BUNDLE
ONDEMAND
 WITH THIS COURSE
sans.org/ondemand

“Very powerful tools
 and concepts!”

-RANDY WAGNER,
 BASIN ELECTRIC



ICS515: ICS Active Defense and Incident Response

will help you deconstruct ICS cyber attacks, leverage an active defense to identify and counter threats in your ICS, and use incident response procedures to maintain the safety and reliability of operations. This course will empower students to understand their networked industrial control system 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 internal to the network is known as active defense.

An active defense is the approach needed to 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 with the ability to deconstruct targeted ICS attacks and fight these adversaries and others. The course uses a hands-on approach and real-world malware to break down cyber attacks on ICS from start to finish. Students will gain a practical and technical understanding of leveraging active defense concepts such as using threat intelligence, performing network security monitoring, and utilizing malware analysis and incident response to ensure the safety and reliability of operations. The strategy and technical skills presented in this course serve as a basis for ICS organizations looking to show that defense is do-able.

You Will Be Able To

- Examine ICS networks and identify the assets and their data flows in order to understand the network baseline information needed to identify advanced threats
- Use active defense concepts such as threat intelligence consumption, network security monitoring, malware analysis, and incident response to safeguard the ICS
- Build your own Programmable Logic Controller using a CYBATIworks Kit and keep it after the class ends
- Gain hands-on experience with samples of Havex, BlackEnergy2, and Stuxnet through engaging labs while deconstructing these threats and others
- Leverage technical tools such as Shodan, Security Onion, TCPDump, NetworkMiner, Foremost, Wireshark, Snort, Bro, SGUIL, ELSA, Volatility, Redline, FTK Imager, PDF analyzers, malware sandboxes, and more
- Create indicators of compromise (IOCs) in OpenIOC and YARA while understanding sharing standards such as STIX and TAXII
- Take advantage of models such as the Sliding Scale of Cybersecurity, the Active Cyber Defense Cycle, and the ICS Cyber Kill Chain to extract information from threats and use it to encourage the long-term success of ICS network security

Who Should Attend

- ICS incident response team leads and members
- ICS and operations technology security personnel
- IT security professionals
- Security Operations Center (SOC) team leads and analysts
- ICS red team and penetration testers
- Active defenders

Robert M. Lee SANS Certified Instructor

Robert M. Lee is the CEO and founder of the critical infrastructure cybersecurity company Dragos Security LLC, where he has a passion for control system traffic analysis, incident response, and threat intelligence research. He is the course author of SANS ICS515: Active Defense and Incident Response and the co-author of SANS FOR578: Cyber Threat Intelligence. Robert is also a non-resident National Cyber Security Fellow at New America focusing on policy issues relating to the cybersecurity of critical infrastructure and a PhD candidate at Kings College London. For his research and focus areas, he was named one of Passcode's Influencers and awarded EnergySec's 2015 Cyber Security Professional of the Year. Robert obtained his start in cybersecurity in the U.S. Air Force, where he served 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 in publications such as Control Engineering and the Christian Science Monitor's Passcode and speaks at conferences around the world. He is also the author of *SCADA and Me* and the weekly web-comic (www.LittleBobbyComic.com)

@RobertMLee

Five-Day Program
Mon, Jun 13 - Fri, Jun 17
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Keith Palmgren



giac.org

► II
BUNDLE
OnDemand
WITH THIS COURSE
sans.org/ondemand



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

This course is designed for students who have 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.***

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

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.

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

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

-STEVE MECCO, DRAPER

"Good basic information for someone just coming into the field."

-BRYCE RICHERT, SUH

Six-Day Program

Mon, Jun 13 - Sat, Jun 18

9:00am - 7:00pm (Days 1-5)

9:00am - 5:00pm (Day 6)

46 CPEs

Laptop Required

Instructor: Jonathan Ham



giac.org



sans.edu



sans.org/cyber-guardian

MEETS DoDD 8140
(8570) REQUIREMENTS



sans.org/8140

**▶▶
BUNDLE
ONDEMAND
WITH THIS COURSE**

sans.org/ondemand



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*!

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.



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

Jonathan Ham SANS Certified Instructor

Jonathan is an independent consultant who specializes in large-scale enterprise security issues from policy and procedure to staffing and training, scalable prevention, detection, and response technology and techniques. With a keen understanding of ROI and TCO (and an emphasis on process over products), he has helped his clients achieve greater success for over 12 years, advising in both the public and private sectors, from small startups to the Fortune 500. He's been commissioned to teach NCIS investigators how to use Snort, performed packet analysis from a facility more than 2000 feet underground, and chartered and trained the CIRT for one of the largest U.S. government agencies. He has held the CISSP, GSEC, GCIA, and GCIH certifications, and is a member of the GIAC Advisory Board. A former combat medic, Jonathan still spends some of his time practicing a different kind of emergency response, volunteering and teaching for both the National Ski Patrol and the American Red Cross. @jhamcorp

Course Day Descriptions

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 attack strategies and how the offense operates.

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

401.3 HANDS ON: Internet Security Technologies

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

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

401.4 HANDS ON: Secure Communications

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

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

401.5 HANDS ON: Windows Security

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

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

401.6 HANDS ON: Unix/Linux Security

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

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

You Will Be Able To

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

“This 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

Six-Day Program
Mon, Jun 13 - Sat, Jun 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Bryan Simon



giac.org



sans.edu

MEETS DoDD 8140
(8570) REQUIREMENTS



sans.org/8140

► II
BUNDLE
ONDEMAND
WITH THIS COURSE
sans.org/ondemand

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.

“Great instructor with the ability to tie real-world threats to theory and practice.”

-BRUCE HENKEL, HARRIS CORP.

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.

“SEC501 is the perfect course to immerse enterprise security staff into essential skills.

Failing to attend this course is done at the peril of your organization.”

-JOHN N. JOHNSON, HOUSTON POLICE DEPARTMENT



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 I.T. 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 teaches 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](https://twitter.com/BryanOnSecurity)

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

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

501.3 HANDS ON: Pentest

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

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

501.4 HANDS ON: First Responder

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

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

501.5 HANDS ON: Malware

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

Topics: Malware; Microsoft Malware; External Tools and Analysis

501.6 HANDS ON: Data Loss Prevention

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

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

You Will Be Able To

- ▶ Identify the threats against network infrastructures and build defensible networks that minimize the impact of attacks
- ▶ 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
- ▶ Apply the six-step incident handling process
- ▶ Use various tools to identify and remediate malware across your organization
- ▶ Create a data classification program and deploy data loss prevention solutions at both a host and network level

"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

"Best course ever taken in InfoSec or any other subject!"

-J. COFER, DSS

Six-Day Program
Mon, Jun 13 - Sat, Jun 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Mike Poor



giac.org



sans.edu



sans.org/cyber-guardian

MEETS DoDD 8140
(8570) REQUIREMENTS



sans.org/8140

► II
BUNDLE
ONDEMAND
WITH THIS COURSE
sans.org/ondemand



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?

Who Should Attend

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

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.

“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

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.

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 GCIAC 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](https://twitter.com/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 Day 1 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; IDS/IPS Evasion Theory; Real-World Traffic Analysis

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; Packet Crafting

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.

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

“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 is beyond excellent. He is a great presenter/instructor and keeps it interesting with real-world examples willing to go above and beyond sessions before and after class. Awesome guy!”

-STACE McRAE, PARSONS

Six-Day Program

Mon, Jun 13 - Sat, Jun 18

9:00am - 7:15pm (Day 1)

9:00am - 5:00pm (Days 2-6)

37 CPEs

Laptop Required

Instructor: John Strand



giac.org



sans.edu



sans.org/cyber-guardian

MEETS DoD 8140
(8570) REQUIREMENTS

sans.org/8140

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



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.



sans.org/simulcast

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

“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, TEEEX

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!

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

-STEPHEN ELLIS, CB&I

The 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.

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) necessary to prepare for and deal with a computer incident. The second part of this section examines from-the-trenches case studies to understand what does and does not work in identifying computer attackers. This section provides valuable information on the steps a systems administrator can take to improve the chances of catching and prosecuting attackers.

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

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

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

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

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

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

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

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

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

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

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

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

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

504.6 HANDS ON: Hacker Tools Workshop

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

Topics: Hands-on Analysis

You Will Be Able To

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

Six-Day Program
Mon, Jun 13 - Sat, Jun 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jason Fossen



giac.org



sans.edu



sans.org/cyber-guardian

MEETS DoDD 8140
(8570) REQUIREMENTS



sans.org/8140

► II
**BUNDLE
ONDEMAND**
WITH THIS COURSE
sans.org/ondemand



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.

“SEC505 is very well structured and organized and provided me with an in-depth understanding of Windows security.” -ROCHANA LAHIRI, BCBSLA

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, we will learn PowerShell as we go along together.

“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

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](https://twitter.com/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

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

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.

Six-Day Program
Mon, Jun 13 - Sat, Jun 18
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Seth Misenar



giac.org



sans.edu

► II
BUNDLE
ONDEMAND
WITH THIS COURSE
sans.org/ondemand



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

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

The Defensible Security Architecture, Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Security Monitoring (CSM) taught in this course will best position your organization or Security Operations Center (SOC) to analyze threats and detect anomalies that could indicate cybercriminal behavior. The payoff for this new proactive approach 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!

Who Should Attend

- Security architects
- Senior security engineers
- Technical security managers
- Security Operations Center (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)

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, SOC's & 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, SOC's, and Security Architecture; Modern Security Architecture Principles; Frameworks and Enterprise Security Architecture; Security Architecture — Key Techniques/Practices; Security Operations Center

511.2 HANDS ON: Network Security Architecture

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

Topics: SOC's/Security Architecture — Key Infrastructure Devices; Segmented Internal Networks; Defensible Network Security Architecture Principles Applied

511.3 HANDS ON: Network Security Monitoring

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

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

511.4 HANDS ON: Endpoint Security Architecture

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

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

511.5 HANDS ON: Automation and Continuous Security Monitoring

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

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

Covers NIST
SP800-137:
Continuous
Monitoring

"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

"I run SOC's and this course provides a gut check against what we are doing today."

-TIM HOUSMAN,

GENERAL DYNAMICS IT

Six-Day Program
Mon, Jun 13 - Sat, Jun 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Eric Conrad



giac.org



sans.edu



sans.org/cyber-guardian

► II
BUNDLE
ONDEMAND
WITH THIS COURSE
sans.org/ondemand



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

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

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

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

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

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

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

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

Who Should Attend

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

Eric Conrad SANS Senior Instructor

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

Course Day Descriptions

542.1 HANDS ON: Introduction and Information Gathering

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

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

542.2 HANDS ON: Configuration, Identity, and Authorization Testing

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

Topics: Discovering the Infrastructure Within the Application; Identifying the Machines and Operating Systems; Secure Sockets Layer (SSL) Configurations and Weaknesses; Exploring Virtual Hosting and Its Impact on Testing; Learning Methods to Identify Load Balancers; Software Configuration Discovery; Exploring External Information Sources; Google Hacking; Learning Tools to Spider a Website; Scripting to Automate Web Requests and Spidering; Application Flow Charting; Relationship Analysis Within an Application; JavaScript for the Attacker

542.3 HANDS ON: Injection

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

Topics: Vulnerability Discovery Overview; Creating Custom Scripts for Penetration Testing; Python for Penetration Testing; Web App Vulnerabilities and Manual Verification Techniques; Interception Proxies; Fiddler; Zed Attack Proxy (ZAP); Burp Suite; Information Leakage, and Directory Browsing; Username Harvesting; Command Injection; Directory Traversal; SQL Injection; Blind SQL Injection

542.4 HANDS ON: JavaScript and XSS

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

Topics: Cross-Site Scripting (XSS); Cross-Site Scripting Discovery; Cross-Site Request Forgery (CSRF); Session Flaws; Session Fixation; AJAX; Logic Attacks; API Attacks; Data Binding Attacks; patproxy; Automated Web Application Scanners; skipfish; w3af

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

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

Topics: Exploring Methods to Zombify Browsers; Discussing Using Zombies to Port Scan or Attack Internal Networks; Exploring Attack Frameworks; Browser Exploitation Framework (BeEF); Walking Through an Entire Attack Scenario; Exploiting the Various Vulnerabilities Discovered; Leveraging Attacks to Gain Access to the System; How to Pivot Our Attacks Through a Web Application; Understanding Methods of Interacting with a Server Through SQL Injection; Exploiting Applications to Steal Cookies; Executing Commands Through Web Application Vulnerabilities

542.6 HANDS ON: Capture the Flag

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

You Will Be Able To

- ▶ Apply a detailed, four-step methodology to your web application penetration tests, including Recon, Mapping, Discovery and Exploitation
- ▶ Analyze the results from automated web testing tools to remove false positives and validate findings
- ▶ Use python to create testing and exploitation scripts during a penetration test
- ▶ Create configurations and test payloads within other web attacks
- ▶ Use FuzzDB to generate attack traffic to find flaws such as Command Injection and File Include issues
- ▶ Assess the logic and transaction flaw within a target application to find logic flaws and business vulnerabilities
- ▶ Use the rerelease of Durzosploit to obfuscate XSS payloads to bypass WAFs and application filtering
- ▶ Analyze traffic between the client and the server application using tools such as Ratproxy and Zed Attack Proxy to find security issues within the client-side application code
- ▶ Use BeEF to hook victim browsers, attack the client software and network and evaluate the potential impact XSS flaws have within an application
- ▶ Perform a complete web penetration test during the Capture the Flag exercise to pull all of the techniques and tools together into a comprehensive test

“The content in SEC542 is very relevant as it features recently discovered vulnerabilities. It also effectively, from my view, caters to various experience levels.”

-MALCOLM KING, MORGAN STANLEY

“SEC542 is a step-by-step introduction to testing and penetrating web applications — a must for anyone who builds, maintains, or audits web systems.”

-BRAD MILHORN, i12P LLC

Five-Day Program
Mon, Jun 13 - Fri, Jun 17
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

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

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 Be Able To

- Track bad guys with callback Word documents
- Use Honeybadger to track web attackers
- Block attackers from successfully attacking servers with honeypots
- 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

"It's hard to imagine a better instructor than Bryce.

He is obviously very skilled and experienced — his teaching skill and personality is a perfect fit."

-PATRICK GUSTAFSON,

ALLIANZ LIFE INSURANCE



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](https://twitter.com/brycegalbraith)

Six-Day Program
Mon, Jun 13 - Sat, Jun 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Tim Medin

The main objectives of CyberCity are to:

- > Teach cyber warriors and their leaders the potential kinetic impacts of cyber attacks
- > Provide a hands-on, realistic kinetic cyber range with engaging missions to conduct defensive and offensive actions
- > Develop capabilities for defending and controlling critical infrastructure components to mitigate or respond to cyber attacks
- > Demonstrate to senior leaders and planners the potential impacts of cyber attacks and cyber warfare



Computers, networks, and programmable logic controllers operate most of the physical infrastructure of our modern world, ranging from electrical power grids, water systems, and traffic systems all the way down to HVAC systems and industrial automation. Increasingly, security professionals need the skills to assess and defend this important infrastructure. In this innovative and cutting-edge course based on the SANS CyberCity kinetic range, you will learn how to analyze and assess the security of control systems and related infrastructure, finding vulnerabilities that could result in significant kinetic impact.

NetWars CyberCity

NetWars CyberCity, our most in-depth and ambitious offering, is designed to teach warriors and InfoSec pros that cyber action can have significant kinetic impact in the physical world. As computer technology, networks, and industrial control systems permeate nearly every aspect of modern life, military, government, and commercial organizations have an increasing need for skilled defenders to protect critical infrastructure. We engineered and built CyberCity to help organizations grow these capabilities in their teams.

CyberCity is a 1:87 scale miniaturized physical city that features SCADA-controlled electrical power distribution, as well as water, transit, hospital, bank, retail, and residential infrastructure. CyberCity engages participants to defend the city's components from terrorist cyber attacks, as well as to utilize offensive tactics to retake or maintain control of critical assets.

"Very very very excellent course! I would like to take this course again." -MASASHI FUJIWARA, HITACHI LTD

Participants engage in missions, with specific operation orders, describing the defensive or offensive goal they need to achieve. In some missions, participants prevent attackers from undermining the CyberCity infrastructure and wreaking havoc, with all the kinetic action captured through streaming video cameras mounted around the physical city. In offensive missions, participants must seize control of CyberCity assets, retaking them from adversaries and using them to achieve a kinetic impact specified in their operation orders. Each mission includes not only a list of goals to be achieved, but also specific sensitive city assets that are out of bounds for the engagement, requiring additional tactical planning to adhere to the rules of engagement.

To achieve mission objectives, participants work as a team, engaging in effective mission planning, devising overall strategies and particular tactics, and exercising detailed technical skills. Furthermore, some participants will be charged as leaders of their teams, helping to build and assess leadership skills, decision-making capabilities, and the ability to brief senior leadership. Multiple realistic defensive and offensive missions test the cyberspace engineers' ability to thwart the best efforts of a well-funded terrorist organization or other cyber attacker trying to control city assets.

Who Should Attend

- ▶ Red and blue team members
- ▶ Cyber warriors
- ▶ Incident handlers
- ▶ Penetration testers
- ▶ Ethical hackers
- ▶ Other security personnel who are first responders when systems come under attack

Tim Medin SANS Certified Instructor

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

NEW!



sans.org/simulcast

Who Should Attend

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

Six-Day Program

Mon, Jun 13 - Sat, Jun 18

9:00am - 7:15pm (Day 1)

9:00am - 5:00pm (Days 2-6)

37 CPEs

Laptop Required

Instructor: Ed Skoudis



giac.org



sans.edu



sans.org/cyber-guardian

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

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

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

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

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

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

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

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



Ed Skoudis SANS Faculty Fellow

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

Course Day Descriptions

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

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

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

560.2 HANDS ON: In-Depth Scanning

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

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

560.3 HANDS ON: Exploitation

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

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

560.4 HANDS ON: Post-Exploitation and Merciless Pivoting

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

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

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

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

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

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

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

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

You Will Be Able To

- ▶ Develop tailored scoping and rules of engagement for penetration testing projects to ensure the work is focused, well defined, and conducted in a safe manner
- ▶ Conduct detailed reconnaissance using document metadata, search engines, and other publicly available information sources to build a technical and organizational understanding of the target environment
- ▶ Utilize a scanning tool such as Nmap to conduct comprehensive network sweeps, port scans, OS fingerprinting, and version scanning to develop a map of target environments
- ▶ Choose and properly execute Nmap Scripting Engine scripts to extract detailed information from target systems
- ▶ Configure and launch a vulnerability scanner such as Nessus so that it safely discovers vulnerabilities through both authenticated and unauthenticated scans, and customize the output from such tools to represent the business risk to the organization
- ▶ Analyze the output of scanning tools to eliminate false positive reduction with tools including Netcat and Scapy
- ▶ Utilize the Windows PowerShell and Linux bash command lines during post-exploitation 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
- ▶ Evade anti-virus tools using powerful frameworks designed to hide executables
- ▶ Conduct comprehensive password attacks against an environment, including automated password guessing (while avoiding account lockout), traditional password cracking, rainbow table password cracking, and pass-the-hash attacks
- ▶ Launch web application vulnerability scanners and then manually exploit Cross-Site Request Forgery, Cross-Site Scripting, Command Injection, and SQL Injection to understand the business risk faced by an organization

"I learned more in one class than in years of self study!"

-BRADLEY MILHORN, COMPUCOM INC.

Six-Day Program
Mon, Jun 13 - Sat, Jun 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Joshua Wright

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



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

Topics addressed in the course include:

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

“This course really forces you to think and the format rewards your hard work and dedication to finding the solutions.” -MICHAEL NUTBROWN, SOLERS, INC

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

Joshua Wright SANS Senior Instructor

Joshua Wright is a senior technical analyst with Counter Hack, a company devoted to the development of information security challenges for education, evaluation, and competition. Through his experiences as a penetration tester, Josh has worked with hundreds of organizations on attacking and defending mobile devices and wireless systems, ethically disclosing significant product and protocol security weaknesses to well-known organizations. As an open-source software advocate, Josh has conducted cutting-edge research resulting in several software tools that are commonly used to evaluate the security of widely deployed technology targeting WiFi, Bluetooth, and ZigBee wireless systems, smart grid deployments, and the Android and Apple iOS mobile device platforms. As the technical lead of the innovative CyberCity, Josh also oversees and manages the development of critical training and educational missions for cyber warriors in the U.S. military, government agencies, and critical infrastructure providers. @joshwrlght

Who Should Attend

- Security professionals
- Systems and network administrators
- Incident response analysts
- Forensic analysts
- Penetration testers
- Red and blue team members

561.1 HANDS ON: Security Platform Analysis

The first day of the course prepares students for real-world security challenges by giving them hands-on practice with essential Linux and Windows server and host management tools. Students will start by leveraging built-in and custom Linux tools to evaluate the security of host systems and servers, inspecting and extracting content from rich data sources such as image headers, browser cache content and system logging resources. Students will then turn their attention to performing similar analysis against remote Windows servers using built-in Windows system management tools to detect misconfigured services, identify password guessing attempts and track down the user performing the attack, evaluate the impact of malware attacks and analyze packet capture data. By completing these tasks, students build their systems management skills (applicable to post-compromise system host analysis) as well as their defensive skills (defending targeted systems from persistent attack threats). By adding new tools and techniques to their arsenal, students are better prepared to complete the analysis of complex systems with greater accuracy in less time.

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

561.2 HANDS ON: Enterprise Security Assessment

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

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

561.3 HANDS ON: Web Application Assessment

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

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

561.4 HANDS ON: Mobile Device and Application Analysis

With the rapidly increasing use of mobile devices in enterprise networks, organizations have a growing need to identify expertise in security assessment and penetration testing of mobile devices and their supporting infrastructure. This section will examine the practical vulnerabilities introduced by mobile devices and applications, as well as how they relate to the security of the enterprise. Students will look at the common vulnerabilities and attack opportunities against Android and Apple iOS devices, examining data remnants from lost or stolen mobile devices, the exposure introduced by common weak application developer practices, and the threat introduced by popular cloud-based mobile applications found in many networks today.

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

561.5 HANDS ON: Advanced Penetration Testing

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

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

561.6 HANDS ON: Capture-the-Flag Challenge

This lively session is the culmination of the course, giving students the opportunity to apply the skills they have mastered throughout all the other sections in a hands-on workshop. The Capture-the-Flag Challenge is an expanded version of the exercises conducted in the previous sections. The aim is to independently reinforce skills learned throughout the course. Students will apply their newly developed skills to scan for flaws, use exploits, unravel technical challenges and dodge firewalls, all while guided by the challenges presented to them by the SANS NetWars Scoring Server. By practicing the skills in a challenging workshop that combines multiple focus areas, participants will be able to explore, exploit, pillage and reinforce skills in a realistic target environment.

You Will Be Able To

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

Five-Day Program
Mon, Jun 13 - Fri, Jun 17
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: James Tarala



giac.org



sans.edu

► II
BUNDLE
OnDemand
WITH THIS COURSE
sans.org/ondemand



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

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

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

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

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

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

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

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 developing large enterprise IT security and infrastructure architectures, specifically working with many Microsoft-based directory services, e-mail, terminal services, and wireless technologies. He has also spent a large amount of time consulting with organizations to assist them 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: Controlled Use of Administrative Privileges

Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs

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

Topics: Critical Control 7: Email and Web Browser Protections

Critical Control 8: Malware Defenses

Critical Control 9: Limitation and Control of Network Ports, Protocols, and Services

Critical Control 10: Data Recovery Capability (validated manually)

Critical Control 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

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

Topics: Critical Control 12: Boundary Defense

Critical Control 13: Data Protection

Critical Control 14: Controlled Access Based on the Need to Know

Critical Control 15: Wireless Device Control

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

Topics: Critical Control 16: Account Monitoring and Control

Critical Control 17: Security Skills Assessment and Appropriate Training to Fill Gaps (validated manually)

Critical Control 18: Application Software Security

Critical Control 19: Incident Response and Management (validated manually)

Critical Control 20: Penetration Tests and Red Team Exercises

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

"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

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

-JEFF EVENSON, AGSTAR FINANCIAL SERVICES

"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

Six-Day Program
 Mon, Jun 13 - Sat, Jun 18
 9:00am - 5:00pm
 36 CPEs
 Laptop Required
 Instructor: Christopher Crowley



giac.org



sans.edu

► II
BUNDLE
ONDEMAND
 WITH THIS COURSE
sans.org/ondemand



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.

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.

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

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 MGT535: Incident Response Team Management and holds the GSEC, GCIA, GCIH (gold), GCFA, GPEN, GREM, GMOB, and CISSP certifications. His teaching experience includes SEC401, SEC503, SEC504, SEC560, SEC575, SEC580, FOR585, and MGT535; Apache web server administration and configuration; and shell programming. He was awarded the SANS 2009 Local Mentor of the year award, which is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities.

@CCrowMontance

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 developing our own skills to analyze 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

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.

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

“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.

Six-Day Program
Mon, Jun 13 - Sat, Jun 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Dave Shackelford

► II
**BUNDLE
ONDEMAND**
WITH THIS COURSE
sans.org/ondemand

**"I will be recommending
this course to all my
peers and friends."**

-ANA MARIE SOLAS, CYBERNET ASSOCIATES



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.

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

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.

"Great course! Anyone involved with managing virtual system environments will benefit from taking SEC579." -RANDALL R., DEFENSE SECURITY SERVICES

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.

"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.

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

Dave Shackelford SANS Senior Instructor

Dave Shackelford 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.

@daveshackelford

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

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 we 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.

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

“SEC579 is the absolute best virtualization security information available! And it is immediately usable.”

-LEONARD LYONS, NORTHROP GRUMMAN

Six-Day Program
Mon, Jun 13 - Sat, Jun 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Larry Pesce



giac.org



sans.edu



sans.org/cyber-guardian



Despite the security concerns many of us share regarding wireless technology, it is here to stay. In fact, not only is wireless here to stay, it is growing in deployment and utilization with wireless LAN technology and WiFi as well as other applications, including cordless telephones, smart homes, embedded devices, and more. Technologies like ZigBee and Z-Wave offer new methods of connectivity to devices, while other wireless technology, including WiFi, Bluetooth, Bluetooth Low Energy, and DECT, continue their massive growth rate, each introducing its own set of security challenges and attacker opportunities.

“The detailed cryptographic explanations made it easier to understand how various encryption algorithms work.” -JONATHAN WILHOIT, FLUOR

To be a wireless security expert, you need to have a comprehensive understanding of the technology, threats, exploits, and defensive techniques along with hands-on experience in evaluating and attacking wireless technology. Not limiting your skill-set to WiFi, you'll need to evaluate the threat from other standards-based and proprietary wireless technologies as well. This course takes an in-depth look at the security challenges of many different wireless technologies, exposing you to wireless security threats through the eyes of an attacker. Using readily available and custom-developed tools, you'll navigate your way through the techniques attackers use to exploit WiFi networks, including attacks against WEP, WPA/WPA2, PEAP, TTLS, and other systems. You'll also develop attack techniques leveraging Windows 7 and Mac OS X. We'll examine the commonly overlooked threats associated with Bluetooth, ZigBee, DECT, and proprietary wireless systems. As part of the course, you'll receive the SWAT Toolkit, which will be used in hands-on labs to back up the course content and reinforce wireless ethical hacking techniques.

“I will use this knowledge to apply the best possible security to wireless guest networks where access is mandated to be easy.” -JUAN REYNOSO, FOX

Using assessment and analysis techniques, this course will show you how to identify the threats that expose wireless technology and build on this knowledge to implement defensive techniques that can be used to protect wireless systems.

Who Should Attend

- ▶ Ethical hackers and penetration testers
- ▶ Network security staff
- ▶ Network and system administrators
- ▶ Incident response teams
- ▶ Information security policy decision-makers
- ▶ Technical auditors
- ▶ Information security consultants
- ▶ Wireless system engineers
- ▶ Embedded wireless system developers

Larry Pesce SANS Certified Instructor

Larry is a Senior Security Analyst with InGuardians after a long stint in security and disaster recovery in healthcare, performing penetration testing, wireless assessments, and hardware hacking. He also diverts a significant portion of his attention to co-hosting the PaulDotCom Security Weekly podcast and likes to tinker with all things electronic and wireless, much to the disappointment of his family, friends, warranties, and his second Leatherman Multi-tool. Larry co-authored Linksys WRT54G Ultimate Hacking and Using Wireshark and Ethereal from Syngress. Larry is an Extra Class Amateur Radio operator (KB1TNF) and enjoys developing hardware and real-world challenges for the Mid-Atlantic Collegiate Cyber Defense Challenge. @haxorthematrix

617.1 HANDS ON: Wireless Data Collection and WiFi MAC Analysis

Students will identify the risks associated with modern wireless deployments as well as the characteristics of physical layer radio frequency systems, including 802.11 a/b/g systems. Students will leverage open-source tools for analyzing wireless traffic and mapping wireless deployments.

Topics: Understanding the Wireless Threat; Wireless LAN Organizations and Standards; Using the SANS Wireless Auditing Toolkit; Sniffing Wireless Networks: Tools, Techniques and Implementation; IEEE 802.11 MAC: In-Depth

617.2 HANDS ON: Wireless Tools and Information Analysis

Students will develop an in-depth treatise on the IEEE 802.11 MAC layer and operating characteristics. Using passive and active assessment techniques, students will evaluate deployment and implementation weaknesses, auditing against common implementation requirements including PCI and the DoD Directive 8100.2. Security threats introduced with rogue networks will be examined from a defensive and penetration-testing perspective. Threats present in wireless hotspot networks will also be examined, identifying techniques attackers can use to manipulate guest or commercial hotspot environments.

Topics: Wireless LAN Assessment Techniques; Rogue AP Analysis; Wireless Hotspot Networks; Attacking WEP

617.3 HANDS ON: Client, Crypto, and Enterprise Attacks

Students will continue their assessment of wireless security mechanisms, such as the identification and compromise of static and dynamic WEP networks and the exploitation of weak authentication techniques, including the Cisco LEAP protocol. Next-generation wireless threats will be assessed, including attacks against client systems such as network impersonation attacks and traffic manipulation. Students will evaluate the security and threats associated with common wireless MAN technology, including proprietary and standards-based solutions.

Topics: Cisco LEAP Attacks; Wireless Client Attacks; Attacking WPA2-PSK Networks; Assessing Enterprise WPA2

617.4 HANDS ON: Advanced WiFi Attack Techniques

This section covers the evaluation of modern wireless encryption and authentication systems, identifying the benefits and flaws in WPA/WPA2 networks and common authentication systems. Upper-layer encryption strategies for wireless security using IPSec are evaluated with in-depth coverage of denial-of-service attacks and techniques.

Topics: Deficiencies in TKIP Networks; Leveraging WiFi DoS Attacks; Wireless Fuzzing for Bug Discovery; Bridging the Airgap: Remote WiFi Pentesting; Framework and Post-Exploitation Modules

617.5 HANDS ON: Bluetooth, DECT, and ZigBee Attacks

Advanced wireless testing and vulnerability discovery systems will be covered, including 802.11 fuzzing techniques. A look at other wireless technology, including proprietary systems, cellular technology, and an in-depth coverage of Bluetooth risks, will demonstrate the risks associated with other forms of wireless systems and their impact on organizations.

Topics: DECT Attacks; Exploiting ZigBee; Enterprise Bluetooth Threats; Advanced Bluetooth Threats

617.6 HANDS ON: Wireless Security Strategies and Implementation

The final day of the course evaluates strategies and techniques for protecting wireless systems. Students will examine the benefits and weaknesses of WLAN IDS systems while gaining insight into the design and deployment of a public key infrastructure (PKI). Students will also examine critical secure network design choices, including the selection of an EAP type, selection of an encryption strategy, and the management of client configuration settings.

Topics: WLAN IDS Analyst Techniques; Evaluating Proprietary Wireless Technology; Deploying a Secure Wireless Infrastructure; Configuring and Securing Wireless Clients

You Will Be Able To

- ▶ Identify and locate malicious rogue access points using free and low-cost tools
- ▶ Conduct a penetration test against low-power wireless including ZigBee to identify control system and related wireless vulnerabilities
- ▶ Identify vulnerabilities and bypass authentication mechanisms in Bluetooth networks using Ubertooth, CarWhisperer, and btatrap to collect sensitive information from headsets, wireless keyboards and Bluetooth LAN devices
- ▶ Utilize wireless capture tools to extract audio conversations and network traffic from DECT wireless phones to identify information disclosure threats exposing the organization
- ▶ Implement an enterprise WPA2 penetration test to exploit vulnerable wireless client systems for credential harvesting
- ▶ Utilize wireless fuzzing tools including Metasploit file2air, and Scapy to identify new vulnerabilities in wireless devices

“The labs were great and provided a good means to practice the material. An excellent course for all levels of professionals who are dealing with wireless in their organization. Not knowing this information is like having your head in the sand. Easy to follow, but difficult to master... the instructor has stretched me and my skills this week and I am better for it!”

-JOHN FRUGE, B&W TECHNICAL SERVICES

Six-Day Program
Mon, Jun 13 - Sat, Jun 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Justin Searle

**“Best web app
class ever!”**

-JOHN CARTRETT,

TORCHMARK CORPORATIONS



This course is designed to teach you the advanced skills and techniques required to test today's web applications. This advanced pen testing course uses a combination of lecture, real-world experiences, and hands-on exercises to educate you in the techniques used to test the security of enterprise applications.

“SEC642 is the perfect course for someone who has a background in web app pen testing, but wants to really gain advanced skills.”

-MATTHEW SULLIVAN, WEBFILINGS

We will begin by exploring specific techniques and attacks to which applications are vulnerable. These techniques and attacks use advanced ideas and skills to exploit the system through various controls and protections. This learning will be accomplished through lectures and exercises using real-world applications.

We will then explore encryption as it relates to web applications. You will learn how encryption works as well as techniques to identify the type of encryption in use within the application. Additionally, you will learn methods for exploiting or abusing this encryption, again through lecture and labs.

**“I like this training because it is very hands on and not just focused on slides.
Very helpful for the real world.”**

-ZACH MORENO, CHICO SECURITY

The next day of class will focus on how to identify web application firewalls, filtering, and other protection techniques. You will then learn methods to bypass these controls in order to exploit the system. You'll also gain skills in exploiting the control itself to further the evaluation of the security within the application.

Following these general exploits, you will learn techniques that target specific enterprise applications. You will attack systems such as content management and ticketing systems.

We will explore the risks and flaws found within these systems and how to better exploit them. This part of the course will also include web services and mobile applications due to their prevalence within modern organizations.

This information-packed advanced pen testing course will wrap up with a full-day Capture-the-Flag event that will target an imaginary organization's web applications and include both Internet and intranet applications of various technologies. This event is designed to allow you to put the pieces together from the previous five days reinforcing the information and learning you will have gained.

Who Should Attend

- ▶ Web penetration testers
- ▶ Security consultants
- ▶ Developers
- ▶ QA testers
- ▶ System administrators
- ▶ IT managers
- ▶ System architects

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. He co-leads prominent open-source projects including the Samurai Web Testing Framework (SamuraiWTF), the Samurai Security Testing Framework for Utilities (SamuraiSTFU), Middled, 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

642.1 HANDS ON: Advanced Discovery and Exploitation

As applications and their vulnerabilities become more complex, penetration testers have to be able to handle these targets. We will begin the class by exploring how Burp Suite works and more advanced ways to use it within your penetration-testing processes. The exploration of Burp Suite will focus on its ability to work within the traditional web penetration testing methodology and assist in manually discovering the flaws within the target applications.

Topics: Review of the Testing Methodology; Using Burp Suite in a Web Penetration Test; Examining How to Use Burp Intruder to Effectively Fuzz Requests; Exploring Advanced Discovery Techniques for SQL Injection and Other Server-Based Flaws; Learning Advanced Exploitation Techniques

642.2 HANDS ON: Discovery and Exploitation for Specific Applications

We will continue the exploration of advanced discovery and exploitation techniques. We'll start by exploring client-side flaws such as cross-site scripting (XSS) and cross-site request forgery (XSRF). We will explore some of the more advanced methods for discovering these issues. After finding the flaws, you will learn some of the more advanced methods of exploitation, such as scriptless attacks and building web-based worms using XSRF and XSS flaws within an application.

Topics: Discovering XSRF Flaws Within Complex Applications; Learning About DOM-based XSS Flaws and How to Find Them Within Applications; Exploiting XSS Using Scriptless Injections; Bypassing Anti-XSRF Controls Using XSS/XSRF Worms; Attacking SharePoint Installations; How to Modify Your Test Based on the Target Application

642.3 HANDS ON: Web Application Encryption

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

Topics: Exploring How to Identify the Cryptography in Use; Discovering How to Attack the Encryption Keys; Learning How to Attack Electronic Codebook (ECB) Mode Ciphers; Exploit Padding Oracles and Cipher Block Chaining (CBC) Bit Flipping

642.4 HANDS ON: Mobile Applications and Web Services

Web applications are no longer limited to the traditional HTML-based interface. Web services and mobile applications have become more common and are regularly being used to attack clients and organizations. As such, it has become very important that penetration testers understand how to evaluate the security of these systems. After finishing up our discussion on cryptography attacks, we will look at how to build a test environment for testing web services used by mobile applications. We will also explore various techniques to discover flaws within the applications and backend systems. These techniques will make use of tools such as Burp Suite and other automated toolsets.

Topics: Attacking CBC Chosen Plaintext; Exploiting CBC with Padding Oracles; Understanding the Mobile Platforms and Architectures; Intercepting Traffic to Web Services and from Mobile Applications; Building a Test Environment; Penetration Testing of Web Services

642.5 HANDS ON: Web Application Firewall and Filter Bypass

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

Topics: Understanding of Web Application Firewalling and Filtering Techniques; Exploring How to Determine the Rule Sets Protecting the Application; Learning How HTML5 Injections Work; Discovering the Use of UNICODE and Other Encodings

642.6 HANDS ON: Capture the Flag

During day six of the class, you will be placed on a network and given the opportunity to complete an entire penetration test. The goal of this Capture-the-Flag event is for you to explore the techniques, tools, and methodology you learned over the last five days. You'll be able to use these ideas and methods against a realistic extranet and intranet attack. At the end of the day, you will provide a verbal report of the findings and methodology you followed to complete the test. Students will be provided with a virtual machine that contains the Samurai Web Testing Framework web penetration-testing environment. Students will be able to use this both in the class and after leaving and returning to their jobs.

You Will Be Able To

- ▶ Assess and attack complex modern applications
- ▶ Understand the special testing and exploits available against content management systems such as SharePoint and WordPress
- ▶ Use techniques to identify and attack encryption within applications
- ▶ Identify and bypass web application firewalls and application filtering techniques to exploit the system
- ▶ Use exploitation techniques learned in class to perform advanced attacks against web application flaws such as XSS, SQL injection and CSRF

Six-Day Program

Mon, Jun 13 - Sat, Jun 18

9:00am - 7:00pm (Days 1-5)

9:00am - 5:00pm (Day 6)

46 CPEs

Laptop Required

Instructor: James Lyne



giac.org



sans.edu



sans.org/cyber-guardian



BUNDLE
ONDEMAND
WITH THIS COURSE

sans.org/ondemand



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

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

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

Who Should Attend

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

James Lyne SANS Certified Instructor

James is the Director of EMEA at SANS and Director of Technology Strategy at security firm Sophos. He comes from a background in cryptography but over the years has worked in a wide variety of security problem domains including anti-malware and hacking. James spent many years as a hands-on analyst dealing with deep technical issues and is a self-professed "massive geek." Eventually James escaped dark rooms and learned some social skills, and today is a keen presenter at conferences and industry events. He has a wide range of experience working in a technical and a strategic capacity from incident response to forensics with some of the world's largest and most paranoid organizations. James participates in industry panels and policy groups, and is a frequently-called-upon expert advisor all over the world. He is a frequent guest lecturer and often appears in the media including national TV. As a young spokesperson for the industry James is extremely passionate about talent development and participates in initiatives to identify and develop new talent. Ask James to show you his best geek party trick. @jameslyne

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; IPv6 for Penetration Testers

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

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

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

660.3 HANDS ON: Python, Scapy, and Fuzzing

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

Topics: Becoming Familiar with Python Types; Leveraging Python Modules for Real-World Pen Tester Tasks; Manipulating Stateful Protocols with Scapy; Using Scapy to Create a Custom Wireless Data Leakage Tool; Product Security Testing; Using Taof for Quick Protocol Mutation Fuzzing; 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 with covering the OS security features (ALSR, DEP, etc.) added to the Windows OS over the years, as well as Windows-specific constructs, such as the process environment block (PEB), structured exception handling (SEH), thread information block (TIB), and the Windows API. Differences between Linux and Windows will be covered. These topics are critical in assessing Windows-based applications. We then focus on stack-based attacks against programs running on the Windows OS.

Topics: The State of Windows OS Protections on Windows 7, 8, 10, Server 2008 and 2012; Understanding Common Windows Constructs; Stack Exploitation on Windows; Defeating OS Protections Added to Windows; Creating a Metasploit Module; Advanced Stack-Smashing on Windows; Return-Oriented Programming (ROP); Windows 7 and 8; Porting Metasploit Modules; Client-side Exploitation; Windows and Linux Shellcode

660.6 HANDS ON: Capture-the-Flag Challenge

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

“The SEC660 course was a very eye-opening experience. The theory and concepts were equally covered in the practical exercises which I have never seen in other courses.”

-FAISAL AL MANSOUR, SAUDI ARAMCO

Six-Day Program

Mon, Jun 13 - Sat, Jun 18

9:00am - 7:00pm (Days 1-5)

9:00am - 5:00pm (Day 6)

46 CPEs

Laptop Required

Instructor: Stephen Sims

Vulnerabilities in modern operating systems such as Microsoft Windows 7/8, Server 2012, and the latest Linux distributions are often very complex and subtle. Yet these vulnerabilities could expose organizations to significant attacks, undermining their defenses when attacked by very skilled adversaries. Few security professionals have the skillset to discover let alone even understand at a fundamental level why the vulnerability exists and how to write an exploit to compromise it. Conversely, attackers must maintain this skillset regardless of the increased complexity. **SEC760: Advanced Exploit Development for**

Penetration Testers teaches the skills required to reverse-engineer 32- and 64-bit applications, perform remote user application and kernel debugging, analyze patches for one-day exploits, and write complex exploits, such as use-after-free attacks, against modern software and operating systems.

Who Should Attend

- ▶ Senior network and system penetration testers
- ▶ Secure application developers (C & C++)
- ▶ Reverse-engineering professionals
- ▶ Senior incident handlers
- ▶ Senior threat analysts
- ▶ Vulnerability researchers
- ▶ Security researchers

What You Will Receive

- Various preconfigured *NIX virtual machines
- Various tools on a course USB that are required for use in class
- Access to the in-class Virtual Training Lab with many in-depth labs
- Access to recorded course audio to help hammer home important network penetration testing lessons



**“SEC760 is a kind of training we could not get anywhere else.
It is not a theory, we got to implement and to exploit everything we learned.”**

-JENNY KITAICHT, INTEL

Some of the skills you will learn in SEC760 include:

- ▶ How to write modern exploits against the Windows 7/8/10 operating systems
- ▶ How to perform complex attacks such as use-after-free, Kernel exploit techniques, one-day exploitation through patch analysis, and other advanced topics
- ▶ The importance of utilizing a Security Development Lifecycle (SDL) or Secure SDLC, along with Threat Modeling
- ▶ How to effectively utilize various debuggers and plug-ins to improve vulnerability research and speed
- ▶ How to deal with modern exploit mitigation controls aimed at thwarting success and defeating determination

**“No one can teach the material as clearly as Steve does.
He is awesome.”**

WALLY STRZELEC, TEXAS A&M UNIVERSITY

Not sure if you are ready for SEC760?

Take this 10 question quiz: sans.org/sec760/quiz

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 of 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

760.1 HANDS ON: Threat Modeling, Reversing and Debugging with IDA

Many penetration testers, incident handlers, developers, and other related professionals lack reverse-engineering and debugging skills. This is a different skill than reverse-engineering malicious software. As part of the Security Development Lifecycle (SDL) and Secure-SDLC, developers and exploit writers should have experience using IDA Pro to debug and reverse their code when finding bugs or when identifying potential risks after static code analysis or fuzzing.

Topics: Security Development Lifecycle (SDL); Threat Modeling; Why IDA Is the #1 Tool for Reverse Engineering; IDA Navigation; IDA Python and the IDA IDC; IDA Plug-ins and Extensibility; Local Application Debugging with IDA; Remote Application Debugging with IDA

760.2 HANDS ON: Advanced Linux Exploitation

The ability to progress into more advanced reversing and exploitation requires an expert-level understanding of basic software vulnerabilities, such as those covered in SEC660. Heap overflows serve as a rite of passage into modern exploitation techniques. This day is aimed at bridging this gap of knowledge in order to inspire thinking in a more abstract manner, necessary for continuing further with the course. Linux can sometimes be an easier operating system to learn these techniques, serving as a productive gateway into Windows.

Topics: Linux Heap Management, Constructs, and Environment; Navigating the Heap; Abusing Macros such as `unlink()` and `frontlink()`; Function Pointer Overwrites; Format String Exploitation; Abusing Custom Doubly-Linked Lists; Defeating Linux Exploit Mitigation Controls; Using IDA for Linux Application Exploitation; Using Format String Bugs for ASLR Bypass

760.3 HANDS ON: Patch Diffing, One-Day Exploits, and Return-Oriented Shellcode

Attackers often download patches as soon as they are distributed by vendors such as Microsoft in order to find newly patched vulnerabilities. Vulnerabilities are usually disclosed privately, or even discovered in-house, allowing the vendor to more silently patch the vulnerability. This also allows the vendor to release limited or even no details at all about a patched vulnerability. Attackers are well aware of this and quickly work to find the patched vulnerability in order to take control of unpatched systems. This technique is also performed by incident handlers, IDS administrators and vendors, vulnerability and penetration testing framework companies, government entities, and others. You will use the material covered in this day to identify bugs patched by vendors and take them through to exploitation.

Topics: The Microsoft Patch Management Process and Patch Tuesday; Obtaining Patches and Patch Extraction; Binary Diffing with BinDiff, patchdiff2, turbodiff, and darungrm3; Visualizing Code Changes and Identifying Fixes; Reversing 32-bit and 64-bit Applications and Modules; Triggering Patched Vulnerabilities; Writing One-Day Exploits; Handling Modern Exploit Mitigation Controls; Using ROP to Compiled Shellcode on the Fly (Return-Oriented Shellcode)

760.4 HANDS ON: Windows Kernel Debugging and Exploitation

The Windows Kernel is very complex and intimidating. This day aims to help you understand the Windows kernel and the various exploit mitigations added into recent versions. You will perform kernel debugging on various versions of the Windows OS, such as Windows 7 and 8, and learn to deal with its inherent complexities. Exercises will be performed to analyze vulnerabilities, look at exploitation techniques, and get a working exploit.

Topics: Understanding the Windows Kernel; Navigating the Windows Kernel; Modern Kernel Protections; Debugging the Windows Kernel; WinDbg; Analyzing Kernel Vulnerabilities and Kernel Vulnerability Types; Kernel Exploitation Techniques; Token Stealing and HAL Dispatch Table Overwrites

760.5 HANDS ON: Windows Heap Overflows and Client-Side Exploitation

The focus of this section is primarily on Windows browser and client-side exploitation. You will learn to analyze C++ vtable overflows, one of the most common mechanisms used to compromise a modern Windows system. Many of these vulnerabilities are discovered in the browser; so browser techniques will also be taught, including modern heap spraying to deal with IE 8/9/10 and other browsers such as FireFox and Chrome. You will work towards writing exploits in the Use-After-Free/Dangling Pointer vulnerability class.

Topics: Windows Heap Management, Constructs, and Environment; Understanding the Low Fragmentation Heap (LFH); Browser-based and Client-side Exploitation; Remedial Heap Spraying; Understanding C++ vtable/vtable Behavior; Modern Heap Spraying to Determine Address Predictability; Use-after-free Attacks and Dangling Pointers; Using Custom Flash Objects to Bypass ASLR; Defeating ASLR, DEP, and Other Common Exploit Mitigation Controls

760.6 HANDS ON: Capture-the-Flag Challenge

Day 6 will serve as a Capture-the-Flag event with different types of challenges taken from material taught throughout the week.

You Will Be Able To

- ▶ Discover zero-day vulnerabilities in programs running on fully-patched modern operating systems
- ▶ Create exploits to take advantage of vulnerabilities through a detailed penetration testing process
- ▶ Use the advanced features of IDA Pro and write your own IDC and IDA Python scripts
- ▶ Perform remote debugging of Linux and Windows applications
- ▶ Understand and exploit Linux heap overflows
- ▶ Write return-oriented shellcode
- ▶ Perform patch diffing against programs, libraries, and drivers to find patched vulnerabilities
- ▶ Perform Windows heap overflows and use-after-free attacks
- ▶ Use precision heap sprays to improve exploitability
- ▶ Perform Windows Kernel debugging up through Windows 8 64-bit
- ▶ Jump into Windows kernel exploitation

Six-Day Program
Mon, Jun 13 - Sat, Jun 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Chad Tilbury



giac.org



sans.edu

▶ II
**BUNDLE
ONDEMAND**
WITH THIS COURSE
sans.org/ondemand



sans.org/simulcast

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

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

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

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

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

MASTER WINDOWS FORENSICS – YOU CAN'T PROTECT WHAT YOU DON'T UNDERSTAND

Chad Tilbury SANS Senior Instructor

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

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; Forensically 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

"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

You Will Be Able To

- ▶ Perform proper Windows forensic analysis by applying key techniques focusing on Windows 7/8/10
- ▶ Use full-scale forensic tools and analysis methods to detail nearly every action a suspect accomplished on a Windows system, including who placed an artifact on the system and how, program execution, file/folder opening, geo-location, browser history, profile USB device usage, and more
- ▶ Uncover the exact time that a specific user last executed a program through Registry and Windows artifact analysis, and understand how this information can be used to prove intent in cases such as intellectual property theft, hacker-breached systems, and traditional crimes
- ▶ Determine the number of times files have been opened by a suspect through browser forensics, shortcut file analysis (LNK), e-mail analysis, and Windows Registry parsing
- ▶ 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

Six-Day Program
Mon, Jun 13 - Sat, Jun 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Rob Lee



giac.org



sans.edu



sans.org/cyber-guardian

MEETS DoDD 8140
(8570) REQUIREMENTS



sans.org/8140

► II
**BUNDLE
ONDEMAND**
WITH THIS COURSE
sans.org/ondemand



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

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.

“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

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!**



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

Rob Lee SANS Faculty Fellow

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

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 hacktivists
- ▶ 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 \$I30 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 timestamping, 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 autoruns, psexec, jobparser, group policy, triage-ir, and IOCFinder

Six-Day Program
Mon, Jun 13 - Sat, Jun 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Sarah Edwards



sans.org/simulcast

► II
BUNDLE
ONDEMAND
WITH THIS COURSE
sans.org/ondemand



"Sarah is an incredible instructor — her knowledge far surpasses anything I've ever experienced, especially regarding the file system."

-BEN KECK, CIENA



Sarah Edwards SANS Certified Instructor

Sarah is a senior digital forensic analyst who has worked with various federal law enforcement agencies. She has performed a variety of investigations including computer intrusions, criminal cases, counter-intelligence, counter-narcotics, and counter-terrorism. Sarah's research and analytical interests include Mac forensics, mobile device forensics, digital profiling, and malware reverse engineering. Sarah has presented at the following industry conferences; Shmoocon, CEIC, BsidenOLA, TechnoSecurity, HTCIA, and the SANS DFIR Summit. She has a Bachelor of Science in Information Technology from Rochester Institute of Technology and a Master's in Information Assurance from Capitol College. @iamevltwin

Digital forensic investigators have traditionally dealt with Windows machines, but what if they find themselves in front of a new Apple Mac or iDevice? The increasing popularity of Apple devices can be seen everywhere, from coffee shops to corporate boardrooms, yet most investigators are familiar with Windows-only machines.

"This course gives a top-to-bottom approach to forensic thinking that is quite needed in the profession."

-NAVEEL KOYA, AC-DAC — TRIVANDRUM

Times and trends change and forensic investigators and analysts need to change with them. The new **FOR518: Mac Forensic Analysis** course provides the tools and techniques necessary to take on any Mac case without hesitation. The intense hands-on forensic analysis skills taught in the course will enable Windows-based investigators to broaden their analysis capabilities and have the confidence and knowledge to comfortably analyze any Mac or iOS system.

FOR518: Mac Forensic Analysis will teach you:

- **Mac Fundamentals:** How to analyze and parse the Hierarchical File System (HFS+) by hand and recognize the specific domains of the logical file system and Mac-specific file types.
- **User Activity:** How to understand and profile users through their data files and preference configurations.
- **Advanced Analysis and Correlation:** How to determine how a system has been used or compromised by using the system and user data files in correlation with system log files.
- **Mac Technologies:** How to understand and analyze many Mac-specific technologies, including Time Machine, Spotlight, iCloud, Versions, FileVault, AirDrop, and FaceTime.

"Pound for pound, dollar for dollar, there is no other forensic training I have seen, from FTK to EnCase to anything private, that holds a candle to what was presented in this course."

-KEVIN J. RIPA, COMPUTER EVIDENCE RECOVERY, INC.

FOR518: Mac Forensic Analysis aims to form a well-rounded investigator by introducing Mac forensics into a Windows-based forensics world. This course focuses on topics such as the HFS+ file system, Mac-specific data files, tracking user activity, system configuration, analysis and correlation of Mac logs, Mac applications, and Mac exclusive technologies. A computer forensic analyst who successfully completes the course will have the skills needed to take on a Mac forensics case.

FORENSICATE DIFFERENTLY!

Who Should Attend

- Experienced digital forensic analysts who want to solidify and expand their understanding of file system forensics and advanced Mac analysis
- Law enforcement officers, federal agents, or detectives who want to master advanced computer forensics and expand their investigative skill set
- Media exploitation analysts who need to know where to find the critical data they need from a Mac system
- Incident response team members who are responding to complex security incidents/intrusions from sophisticated adversaries and need to know what to do when examining a compromised system
- Information security professionals who want to become knowledgeable with Mac OS X and iOS system internals
- SANS FOR408, FOR508, FOR526, FOR610, FOR585 alumni looking to round out their forensic skills

518.1 HANDS ON: Mac Essentials and the HFS+ File System

This section introduces the student to Mac system fundamentals such as acquisition, the Hierarchical File System (HFS+), timestamps, and logical file system structure. Acquisition fundamentals are the same with Mac systems, but there are a few Mac-specific tips and tricks that can be used to successfully and easily collect Mac systems for analysis. The building blocks of Mac Forensics start with a thorough understanding of the HFS+. Utilizing a hex editor, the student will learn the basic principles of the primary file system implemented on Mac OS X systems. Students comfortable with Windows forensic analysis can easily learn the slight differences on a Mac system: the data are the same, only the format differs.

Topics: Mac Fundamentals; Mac Acquisition; Incident Response; HFS+ File System; Volumes; Mac Basics

518.2 HANDS ON: User Domain File Analysis

The logical Mac file system is made up of four domains; User, Local, System, and Network. The User Domain contains most of the user-related items of forensic interest. This domain consists of user preferences and configurations, e-mail, Internet history, and user-specific application data. This section contains a wide array of information that can be used to profile and understand how individuals use their computers.

Topics: User Home Directory; User Account Information; User Data Analysis; Internet & E-mail; Instant Messaging; Native Mac Applications

518.3 HANDS ON: System and Local Domain File Analysis

The System and Local Domains contain system-specific information such as application installation, system settings and preferences, and system logs. This section details basic system information, GUI preferences, and system application data. A basic analysis of system logs can give a good understanding of how a system was used or abused. Timeline analysis tells the story of how the system was used. Each entry in a log file has a specific meaning and may be able to tell how the user interacted with the computer. The log entries can be correlated with other data found on the system to create an in-depth timeline that can be used to solve cases quickly and efficiently. Analysis tools and techniques will be used to correlate the data and help the student put the story back together in a coherent and meaningful way.

Topics: System Information; System Applications; Log Analysis; Timeline Analysis & Correlation

518.4 HANDS ON: Advanced Analysis Topics

Mac systems implement some technologies that are available only to those with Mac devices. These include data backup with Time Machine, Versions, and iCloud; extensive file metadata with Extended Attributes and Spotlight; and disk encryption with FileVault. Other advanced topics include data hidden in encrypted containers, Mac intrusion and malware analysis, Mac Server, and Mac memory analysis.

Topics: Extended Attributes; Time Machine; Spotlight; Cracking Passwords & Encrypted Containers; iCloud; Document Versions; Malware & Antivirus; Memory Acquisition & Analysis; Portable OS X Artifacts; Mac OS X Server

518.5 HANDS ON: iOS Forensics

From iPods to iPhones to iPads, it seems everyone has at least one of these devices. Apple iDevices are seen in the hands of millions of people. Much of what goes on in our lives is often stored on them. Forensic analysis of these iOS devices can provide an investigator with an incredible amount of information. Data on these iOS devices will be explored to teach the student what key files exist on them and what advanced analysis techniques can be used to exploit them for investigations.

Topics: History of iOS Devices; iOS Acquisition; iOS Analytical Tool Overview; iOS Artifacts Recovered from OS X Systems; iOS File System; iOS Artifacts & Areas of Evidentiary Value; Third-Party Applications

518.6 HANDS ON: The Mac Forensics Challenge

Students will put their new Mac forensics skills to the test by completing the following tasks:

- In-Depth HFS+ File System Examination
- File System Timeline Analysis
- Advanced Computer Forensics Methodology
- Mac Memory Analysis
- File System Data Analysis
- Metadata Analysis
- Recovering Key Mac Files
- Volume and Disk Image Analysis
- Analysis of Mac Technologies including Time Machine, Spotlight, and FileVault
- Advanced Log Analysis and Correlation
- iDevice Analysis and iOS Artifacts

You Will Be Able To

- ▶ Parse the HFS+ file system by hand, using only a cheat sheet and a hex editor
- ▶ Determine the importance of each file system domain
- ▶ Conduct temporal analysis of a system by correlating data files and log analysis
- ▶ Profile an individuals' usage of the system, including how often they used it, what applications they frequented, and their personal system preferences
- ▶ Determine remote or local data backups, disk images, or other attached devices
- ▶ Find encrypted containers and FileVault volumes, understand keychain data, and crack Mac passwords
- ▶ Analyze and understand Mac metadata and their importance in the Spotlight database, Time Machine, and Extended Attributes
- ▶ Develop a thorough knowledge of the Safari Web Browser and Apple Mail applications
- ▶ Identify communication with other users and systems through iChat, Messages, FaceTime, Remote Login, Screen Sharing, and AirDrop
- ▶ Conduct an intrusion analysis of a Mac for signs of compromise or malware infection
- ▶ Acquire and analyze memory from Mac systems
- ▶ Acquire iOS and analyze devices in-depth

“Very comprehensive in-depth coverage of the course topic. Excellent reference materials as a takeaway.”

-JENNIFER BARNES, INDIANA STATE POLICE

Six-Day Program
Mon, Jun 13 - Sat, Jun 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Philip Hagen



giac.org



sans.edu

► II
BUNDLE
ONDEMAND
WITH THIS COURSE
sans.org/ondemand



digital-forensics.sans.org



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.

"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

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 cyber crime 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, tcpextract, 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.



sans.org/simulcast

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
- Anyone interested in computer network intrusions and investigations
- Security Operations Center personnel and information security practitioners

Philip Hagen SANS Certified Instructor

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

572.1 HANDS ON: Off the Disk and Onto the Wire

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

Topics: Web Proxy Server Examination, 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

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

You Will Be Able To

- ▶ Extract files from network packet captures and proxy cache files, allowing follow-on malware analysis or definitive data loss determination
- ▶ Use historical NetFlow data to identify relevant past network occurrences, allowing accurate incident scoping
- ▶ Reverse-engineer custom network protocols to identify an attacker's command-and-control abilities and actions
- ▶ Decrypt captured SSL traffic to identify attackers' actions and what data they extracted from the victim
- ▶ Use data from typical network protocols to increase the fidelity of the investigation's findings
- ▶ Identify opportunities to collect additional evidence based on the existing systems and platforms within a network architecture
- ▶ Examine traffic using common network protocols to identify patterns of activity or specific actions that warrant further investigation
- ▶ Incorporate log data into a comprehensive analytic process, filling knowledge gaps that may be far in the past
- ▶ Learn how attackers leverage man-in-the-middle tools to intercept seemingly secure communications
- ▶ Examine proprietary network protocols to determine what actions occurred on the endpoint systems
- ▶ Analyze wireless network traffic to find evidence of malicious activity
- ▶ 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

Six-Day Program
Mon, Jun 13 - Sat, Jun 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Heather Mahalik

► **BUNDLE**
ONDEMAND
WITH THIS COURSE
sans.org/ondemand



"FOR585 course content is extremely valuable for use in real-world application and directly pertinent to analysis conducted at my lab."

-H. POLEND, VIRGINIA DEPT.
OF FORENSIC SCIENCE



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

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

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

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

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

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

Who Should Attend

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

Heather Mahalik SANS Senior Instructor

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

585.1 HANDS ON: Smartphone Overview and Malware Forensics

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

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

585.2 HANDS ON: Android Forensics

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

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

585.3 HANDS ON: iOS Forensics

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

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

585.4 HANDS ON: Backup File and BlackBerry Forensics

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

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

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

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

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

585.6 HANDS ON: Smartphone Forensics Capstone Exercise

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

You Will Be Able To

- ▶ Understand where key evidence is located on a smartphone
- ▶ Determine how the data got onto the smartphone
- ▶ Recover deleted mobile device data that most forensic tools miss
- ▶ Decode evidence stored in third-party applications
- ▶ Detect, decompile, and analyze mobile malware and spyware
- ▶ Handle locked or encrypted devices, applications, and containers

A smartphone lands on your desk and you are tasked with determining if the user was at a specific location at a specific date and time. You rely on your forensic tools to dump and parse the data. The tools show location information tying the device to the place of interest. Are you ready to prove the user was at that location? Do you know how to take this further to place the subject at the location of interest at that specific date and time? Tread carefully, because the user may not have done what the tools are showing!

SMARTPHONES HAVE MINDS OF THEIR OWN

DON'T MAKE THE MISTAKE OF REPORTING SYSTEM EVIDENCE AS USER ACTIVITY

IT'S TIME TO GET SMARTER!

Six-Day Program
Mon, Jun 13 - Sat, Jun 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Lenny Zeltser



giac.org



sans.edu

► II
BUNDLE
ONDEMAND
WITH THIS COURSE

sans.org/ondemand



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

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

"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 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.

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

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

610.4 HANDS ON: Self-Defending Malware

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

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

610.5 HANDS ON: Malicious Documents and Memory Forensics

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

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

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

You Will Be Able To

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

Six-Day Program

Mon, Jun 13 - Sat, Jun 18

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: Paul A. Henry



giac.org

MEETS DoDD 8140
(8570) REQUIREMENTS

sans.org/8140

BUNDLE
ONDEMAND
WITH THIS COURSE

sans.org/ondemand



SANS MGT414: SANS Training Program for CISSP®

Certification is an accelerated review course that has been specifically updated to prepare you to pass the 2016 version of the CISSP® exam.

Course authors Eric Conrad and Seth Misenar have revised MGT414 to take into account the 2016 updates to the CISSP® exam and prepare students to navigate all types of questions included in the new version.

"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

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.

"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

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

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

Who Should Attend

- ▶ Security professionals who are interested in understanding the concepts covered on the CISSP® exam as determined by (ISC)²
- ▶ Managers who want to understand the critical areas of 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

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

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 2016 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

414.2 Asset Security and Security Engineering (PART 1)

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

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

414.3 Security Engineering (PART 2); Communication and Network Security

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

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

414.4 Identity and Access Management

Controlling access to data and systems is one of the primary objectives of information security. Domain 5, Identity and Access Management, strikes at the heart of access control by focusing on identification, authentication, and authorization of accounts. Password-based authentication represents a continued weakness, so Domain 5 stresses multi-factor authentication, biometrics, and secure credential management. The 2016 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 2016 CISSP® exam update will be discussed, including DevOps. We will wrap up this course section by discussing security vulnerabilities, secure coding strategies, and testing methodologies.

Topics: Domain 8: Software Development Security

You Will Be Able To

- ▶ Understand the 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

Five-Day Program

Mon, Jun 13 - Fri, Jun 17

9:00am - 6:00pm (Days 1-4)

9:00am - 4:00pm (Day 5)

33 CPEs

Laptop NOT Needed

Instructor: G. Mark Hardy



giac.org



sans.edu

MEETS DoD 8140
(8570) REQUIREMENTS

sans.org/8140

► II
BUNDLE
ONDEMAND
WITH THIS COURSE
sans.org/ondemand



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

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

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

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

512.4 The Value of Information

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

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

512.5 Management Practicum

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

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

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

"MGT512 has great info for newly assigned managers to cybersecurity."

-KERRY T., U.S. ARMY CORPS OF ENGINEERS

"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.

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.

Five-Day Program
Mon, Jun 13 - Fri, Jun 17
9:00am - 5:00pm
30 CPEs
Laptop NOT Needed
Instructor: Frank Kim



sans.edu

► II
BUNDLE
ONDEMAND
WITH THIS COURSE
sans.org/ondemand

"I loved the enthusiasm
and life experience that
was brought into class."

-SANS SCOTTSDALE 2015 STUDENT



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

This course teaches security professionals how to do three things:

► Develop Strategic Plans

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

► Create Effective Information Security Policy

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

► Develop Management and Leadership Skills

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

How the Course Works

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

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

Who Should Attend

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

Frank Kim SANS Certified Instructor

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

514.1 Strategic Planning Foundations

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

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

514.2 Strategic Roadmap Development

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

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

514.3 Security Policy Development and Assessment

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

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

514.4 Leadership and Management Competencies

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

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

514.5 Strategic Planning Workshop

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

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

You Will Be Able To

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

"The instructor not only provided relevant content, he delivered it in an engaging way."

-BRIAN COOK, SANS 2015 STUDENT

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

-ERIC BURGAN, IDAHO NATIONAL LABS

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

-ALEXIS BROWNING, CERT-UK

Six-Day Program
Mon, Jun 13 - Sat, Jun 18
9:00am - 5:00pm
36 CPEs
Laptop NOT Needed
Instructor: Jeff Frisk



giac.org



sans.edu



Recently updated to fully prepare you for the 2016 PMP® Exam, **SANS MGT525: IT Project Management, Effective Communication, and PMP® Exam Prep** is a PMI Registered Education Provider (R.E.P.). R.E.P.s provide the training necessary to earn and maintain the Project Management Professional (PMP®) and other professional credentials. During this class you will learn how to improve your project planning methodology and project task scheduling to get the most out of your critical IT resources. We will utilize project case studies that highlight information technology services as deliverables. MGT525 follows the basic project management structure from the *PMBOK® Guide* (Fifth Edition) and also provides specific techniques for success with information assurance initiatives. Throughout the week, we will cover all aspects of IT project management – from initiating and planning projects through managing cost, time, and quality while your project is active, to completing, closing, and documenting as your project finishes. A copy of the *PMBOK® Guide* (Fifth Edition) is provided to all participants. You can reference the guide and use your course material along with the knowledge you gain in class to prepare for the 2016 updated PMP® Exam and the GIAC Certified Project Manager Exam.

Who Should Attend

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

“Best way to prepare top project managers for the real world and certification!”

-ROB ASHWORTH, BARLING BAY

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

“Honestly, this is one of the best courses I have had to date. I feel like I have thousands of things to take back to my job.” -RYAN SPENCER, REED ELSEVIER INC.



Jeff Frisk SANS Certified Instructor

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

525.1 Project Management Structure and Framework

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

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

525.2 Project Charter and Scope Management

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

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

525.3 Time and Cost Management

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

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

525.4 Communications and Human Resources

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

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

525.5 Quality and Risk Management

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

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

525.6 Procurement, Stakeholder Management, and Project Integration

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

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

You Will Be Able To

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

Six-Day Program
Mon, Jun 13 - Sat, Jun 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: David Hoelzer



giac.org



sans.edu

MEETS DoDD 8140
(8570) REQUIREMENTS



sans.org/8140

► II
BUNDLE
ONDEMAND
WITH THIS COURSE
sans.org/ondemand



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. Students are invited to bring a Windows XP Professional or higher laptop for use during class. Macintosh computers running OS X may also be used with VMWare Fusion.

A great audit is more than marks on a checklist; it is the understanding of what the underlying controls are, what the best practices are, and why. Sign up for this course and gain the mix of theoretical, hands-on, and practical knowledge to conduct a great audit.

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 agencies such as the NSA and 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, he 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

Six-Day Program
Mon, Jun 13 - Sat, Jun 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jason Lam



giac.org



sans.edu

► II
BUNDLE
ONDEMAND
WITH THIS COURSE
sans.org/ondemand

This is the course to take if you have to defend web applications!

The quantity and importance of data entrusted to web applications is growing, and defenders need to learn how to secure them. Traditional network defenses, such as firewalls, fail to secure web applications. DEV522 covers the OWASP Top 10 Risks and will help you better understand web application vulnerabilities, thus enabling you to properly defend your organization's web assets.

Mitigation strategies from an infrastructure, architecture, and coding perspective will be discussed alongside real-world applications that have been proven to work. The testing aspect of vulnerabilities will also be covered so that you can ensure your application is tested for the vulnerabilities discussed in class.

To maximize the benefit for a wider range of audiences, the discussions in this course will be programming language agnostic. Focus will be maintained on security strategies rather than coding-level implementation.

"The current security landscape is rapidly changing and the course content is relevant and important to software security and compliance software." -SCOTT HOOF, TRIPWIRE, INC.

DEV522: Defending Web Applications Security Essentials is intended for anyone tasked with implementing, managing, or protecting web applications. It is particularly well suited to application security analysts, developers, application architects, pen testers, auditors who are interested in recommending proper mitigations for web security issues, and infrastructure security professionals who have an interest in better defending their web applications.

The course will also cover additional issues the authors have found to be important in their day-to-day web application development practices. The topics that will be covered include:

- Infrastructure security
- Server configuration
- Authentication mechanisms
- Application language configuration
- Application coding errors like SQL injection and cross-site scripting
- Cross-site request forging
- Authentication bypass
- Web services and related flaws
- Web 2.0 and its use of web services
- XPATH and XQUERY languages and injection
- Business logic flaws
- Protective HTTP headers

The course will make heavy use of hands-on exercises and conclude with a large defensive exercise that reinforces the lessons learned throughout the week.



Jason Lam SANS Certified Instructor

Jason is a senior security analyst at a major financial institution in Canada. His recent SANS Institute courseware development includes Defending Web Application Security Essentials and Web Application Pen Testing Hands-On Immersion. Jason started his career as a programmer before moving on to ISP network administration, where he handled network security incidents, which sparked his interest in information security. Jason specializes in Web application security, penetration testing, and intrusion detection. He holds a BA in computer science from York University in Toronto, Ontario, as well as the CISSP, GCIA, GCFW, GCUX, GCWN, and GCIH certifications.

@jasonlam_sec

Four-Day Program
Sat, Jun 11 - Tue, Jun 14
9:00am - 5:00pm
24 CPEs
Laptop Required
Instructor: Gregory Leonard



giac.org



sans.edu

► II
**BUNDLE
ONDEMAND**
WITH THIS COURSE
sans.org/ondemand

This secure coding course will teach students how to build secure Java applications and gain the knowledge and skills to keep a website from getting hacked, counter a wide range of application attacks, prevent critical security vulnerabilities that can lead to data loss, and understand the mindset of attackers.

The course teaches you the art of modern web defense for Java applications by focusing on foundational defensive techniques, cutting-edge protection, and Java EE security features you can use in your applications as soon as you return to work. This includes learning how to:

- Identify security defects in your code
- Fix security bugs using secure coding techniques
- Utilize secure HTTP headers to prevent attacks
- Secure your sensitive representational state transfer (REST) services
- Incorporate security into your development process
- Use freely available security tools to test your applications

Great developers have traditionally distinguished themselves by the elegance, effectiveness and reliability of their code. That is still true, but the security of the code now needs to be added to those other qualities. This unique SANS course allows you to hone the skills and knowledge required to prevent your applications from getting hacked.

“This course provided a great review in Java development practices to ensure secure and defensible applications.” -JOHN DAVIS, LOCKHEED MARTIN CORPORATION

DEV541: Secure Coding in Java/JEE: Developing Defensible Applications is a comprehensive course covering a wide set of skills and knowledge. It is not a high-level theory course – it is about real-world, hands-on programming. You will examine actual code, work with real tools, build applications and gain confidence in the resources you need to improve the security of Java applications.

Rather than teaching students to use a given set of tools, the course covers concepts of secure programming. This involves looking at a specific piece of code, identifying a security flaw and implementing a fix for flaws found on the OWASP Top 10 and CWE/SANS Top 25 Most Dangerous Programming Errors.

The course culminates in a Secure Development Challenge in which students perform a security review of a real-world open-source application. You will conduct a code review, perform security testing to actually exploit real vulnerabilities, and implement fixes for these issues using the secure coding techniques that you have learned in the course.

PCI Compliance

Section 6.5 of the Payment Card Industry (PCI) Data Security Standard (DSS) instructs auditors to verify processes that require training in secure coding techniques for developers. If you are responsible for developing applications that process cardholder data and are therefore required to be PCI compliant, then this is the course for you.

Who Should Attend

- Developers who want to build more secure applications
- Java Enterprise Edition (JEE) programmers
- Software engineers
- Software architects
- Developers who need to be trained in secure coding techniques to meet PCI compliance requirements
- Application security auditors
- Technical project managers
- Senior software QA specialists
- Penetration testers who want a deeper understanding of target applications or who want to provide more detailed vulnerability remediation options

“DEV541 will help change the way the developers in my organization code. We have not placed a high amount of emphasis on secure coding before.”

-BRETT HANSON, AGRIUM



Gregory Leonard SANS Instructor

Gregory Leonard has over 16 years of experience in software development, with an emphasis on writing large-scale enterprise applications. Greg's responsibilities have included application architecture and security, performing infrastructure design and implementation, security analysis, code reviews, and evaluating performance diagnostics. Greg is currently focusing on overseeing the integration of secure development practices for his company.

Four-Day Program
Wed, Jun 15 - Sat, Jun 18
9:00am - 5:00pm
24 CPEs
Laptop Required
Instructor: Eric Johnson



giac.org



sans.edu

▶ II
**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?

“This is a must-have for all applications and must-know for all developers.

I recommend it to my colleagues.” -PRAVEEN PALEY, WESTERN UNION BUSINESS SOLUTIONS

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.

“It is shocking to see how much we are missing in our code.

I am going back to change the code immediately.” -RUOJIE WANG, NEW JERSEY HOSPITAL ASSOCIATION

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.

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 requirements
- ▶ Application security auditors
- ▶ Technical project managers
- ▶ Senior software QA specialists
- ▶ Penetration testers



Eric Johnson SANS Certified Instructor

Eric Johnson is a Senior Security Consultant at Cypress Data Defense and the Application Security Curriculum Product Manager at SANS. He is the lead author and instructor for DEV544 Secure Coding in .NET, as well as an instructor for DEV541 Secure Coding in Java/JEE. Eric serves on the advisory board for the SANS Securing the Human Developer Awareness Training Program and is a contributing author for the developer security awareness modules. His experience includes web and mobile application penetration testing, secure code review, risk assessment, static source code analysis, security research, and developing security tools. Eric completed a Bachelor of Science degree in computer engineering and a Master of Science in information assurance at Iowa State University, and currently holds the CISSP, GWAPT, GSSP-.NET, and GSSP-Java certifications. He is based in West Des Moines, IA and outside the office enjoys spending time with his wife and daughter, attending Iowa State athletic events, and golfing on the weekends. @emjohn20

Five-Day Program
Mon, Jun 13 - Fri, Jun 17
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Eric Cornelius



giac.org



sans.edu

▶▶
BUNDLE
OnDemand
WITH THIS COURSE

sans.org/ondemand



SANS has joined forces with industry leaders to equip security professionals and control system engineers with the cybersecurity skills they need to defend national critical infrastructure. **ICS410: ICS/SCADA Security Essentials** provides a foundational set of standardized skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

The course will provide you with:

- ▶ An understanding of industrial control system components, purposes, deployments, significant drivers, and constraints
- ▶ Hands-on lab learning experiences to control system attack surfaces, methods, and tools
- ▶ Control system approaches to system and network defense architectures and techniques
- ▶ Incident-response skills in a control system environment
- ▶ Governance models and resources for industrial cybersecurity professionals

When examining the greatest risks and needs in critical infrastructure sectors, the course authors looked carefully at the core security principles necessary for the range of tasks involved in supporting control systems on a daily basis. While other courses are available for higher-level security practitioners who need to develop specific skills such as industrial control system penetration testing, vulnerability analysis, malware analysis, forensics, secure coding, and red team training, most of these courses do not focus on the people who operate, manage, design, implement, monitor, and integrate critical infrastructure production control systems.

With the dynamic nature of industrial control systems, many engineers do not fully understand the features and risks of many devices. 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.

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

Eric Cornelius SANS Instructor

Eric Cornelius is the Director of Critical Infrastructure and Industrial Control Systems (ICS) at Cylance, Inc. where he is responsible for thought leadership, architecture, and consulting. Eric brings a wealth of ICS knowledge and his leadership keeps organizations safe, secure, and resilient against advanced attackers. Previously, Eric served as the Deputy Director and Chief Technical Analyst for the Control Systems Security Program at the U.S. Department of Homeland Security. Eric earned a bachelor's degree from the New Mexico Institute of Mining and Technology, where he was the recipient of many scholarships and awards including the National Science Foundation's Scholarship for Service. Eric went on to work at the Army Research Laboratory's Survivability/Lethality Analysis Directorate, where he worked to secure field deployable combat technologies. It was at ARL that Cornelius became interested in non-traditional computing systems, an interest that ultimately led him to the Idaho National Laboratory where he participated in deep-dive vulnerability assessments of a wide range of ICS systems. Eric is the co-author of "Recommended Practice: Creating Cyber Forensics Plans for Control Systems" as part of the DHS National Cyber Security Division's 2008 Control Systems Security Program and is also a frequent speaker and instructor at ICS events across the globe.

Five-Day Program
 Mon, Jun 13 - Fri, Jun 17
 9:00am - 5:00pm
 30 CPEs
 Laptop NOT Needed
 Instructor: Benjamin Wright



► II
BUNDLE
OnDemand
 WITH THIS COURSE
sans.org/ondemand



- **The European Union's invalidation of the Privacy Safe Harbor for transferring data to the United States.**
- **Cyber insurer's lawsuit against hospital to deny coverage after data breach and \$4.1 million legal settlement with patients.**
- **Target's and Home Depot's legal and public statements about payment card breaches.**
- **New legal tips on confiscating and interrogating mobile devices.**
- **Lawsuit by credit card issuers against Target's QSA and alleged security vendor, Trustwave.**

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.

"I have gained many valuable ideas and tools to support and defend my organization and to strengthen security overall. I wish I'd taken LEG523 3-4 years ago."

-Tom S., CASE WESTERN RESERVE UNIVERSITY

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.

Who Should Attend

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

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

SANS Hosted is a series of courses presented by other educational providers at SANSFIRE 2016 to complement your needs for training outside of our current course offerings.



HOSTED



Healthcare Security Essentials

Two-Day Course | Sat, Jun 11 - Sun, Jun 12 | 9:00am - 5:00pm | 12 CPEs | Laptop Required | Instructor: Greg Porter

Healthcare Security Essentials is designed to provide SANS students with an introduction to current and emerging issues in healthcare information security and regulatory compliance. The class provides a foundational set of skills and knowledge for healthcare security professionals by integrating case studies, hands-on labs, and tips for securing and monitoring electronic Protected Health Information. Administrative insights for those managing the many aspects of healthcare security operations will also be discussed. The goal of the course is to present a substantive overview and analysis of relevant information security subject matter that is having a direct and material impact on the U.S. healthcare system.

MODULE 1: Overview of Healthcare Information Security

The first module of the class focuses on current threats to healthcare information systems and data. We will examine the how and why patient information is being targeted as well as key trends, including, but not limited to, the commercialization of malicious software, medical identity theft, insider threats, mobile device proliferation, cloud computing, and poor operational governance. The module will conclude with a discussion on common sources of healthcare data breaches and practical countermeasures.

MODULE 2: HIPAA Security 2.0

Module 2 will provide attendees with an overview of the HIPAA Security Rule and its context, with close attention paid to the rules structure, safeguards, and implementation specifications governing electronic Protected Health Information. Students will also examine breach notification requirements and conclude the module by reviewing the security implications of Electronic Medical Records and Meaningful Use.

MODULE 3: Risk Analysis & Management

Module 3 discusses the risk-based guidance framework to assist healthcare-based organizations and other custodians of personal health information with developing an effective risk assessment program specifically designed to identify risks to the confidentiality, integrity, and availability of ePHI while meeting Office for Civil Rights expectations.

MODULE 4: Medical Device Security

The course will conclude by taking the lessons learned from previous modules and attempting to understand their applicability to medical device management. Medical devices, large and small alike, continue to play an essential and growing role in patient care. Today's security professional must understand the risks medical devices may present to wired and/or wireless networks, patient data, and end users and how those risks should be appropriately managed.

HOSTED

Physical Penetration Testing

Two-Day Course | Sat, Jun 11 - Sun, Jun 12 | 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.

SEC440

Critical Security Controls: Planning, Implementing, and Auditing

Two-Day Course | Sat, Jun 11 - Sun, Jun 12 | 9:00am - 5:00pm | 12 CPEs | Laptop NOT Needed | Instructor: Randy Marchany

This course will help you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS). 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. The controls 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 through 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.**

SEC524

Cloud Security Fundamentals

Two-Day Course | Sat, Jun 11 - Sun, Jun 12 | 9:00am - 5:00pm | 12 CPEs | Laptop Required | Instructor: Paul A. Henry

SEC524 starts out with a detailed introduction to the various delivery models of cloud computing, ranging from Software as a Service (SaaS) to Infrastructure as a Service (IaaS) and everything in between. Each of these delivery models represents an entirely separate set of security conditions to consider, especially when coupled with various cloud types, including public, private and hybrid. An overview of security issues within each of these models will be covered with an in-depth discussion of the risks involved. This cloud security training course will go in-depth on architecture and infrastructure fundamentals for private, public and hybrid clouds, including a wide range of topics such as patch and configuration management, virtualization security, application security and change management. Policy, risk assessment, and governance within cloud environments will also be covered, with recommendations for both internal policies and contract provisions. This path leads to a discussion of compliance and legal concerns. The first day will wrap up with disaster recovery and business continuity planning using cloud models and architecture.

Day 2 of this course will start with the challenges of identity and access management in cloud environments. Next, more businesses are utilizing the cloud to store critical data, so we will cover how to protect your critical data in the cloud. New approaches for data encryption, network encryption, key management and data lifecycle concerns will be covered in detail, followed by a deep dive into risk assessments and risk management. Intrusion detection and incident response in cloud environments will also be covered, along with how best to manage these critical security processes and the technologies that support them given that most controls are managed by the CSP.

SEC546

IPv6 Essentials

Two-Day Course | Sat, Jun 11 - Sun, Jun 12 | 9:00am - 5:00pm | 12 CPEs | Laptop Required | Instructor: Johannes Ullrich, PhD

Implementing IPv6 should not happen without carefully considering the security impact of the new protocol. Even if you haven't implemented it yet, the ubiquitous IPv6 support in modern operating systems easily leads to unintentional IPv6 implementation, which may put your network at risk. In this course, we will start out by introducing the IPv6 protocol, explaining in detail many of its features like the IPv6 header, extension headers and auto configuration. Only by understanding the design of the protocols in depth will it be possible to appreciate the various attacks and mitigation techniques. The course will address how to take advantage of IPv6 to re-think how to assign addresses in your network and how to cope with what some suggest is the biggest security problem in IPv6: no more NAT! IPv6 doesn't stop at the network layer. Many application layer protocols change in order to support IPv6, and we will take a close look at protocols like DNS, DHCPv6 and more.

The course covers various security technologies like firewalls and Intrusion Detection and Prevention Systems (IDS/IPS). It also addresses the challenges in adequately configuring these systems and makes suggestions as to how apply existing best practices to IPv6. Upcoming IPv6 attacks are discussed using tools like the THC IPv6 attack suite and others as an example.

SECURITY SKILL-BASED COURSES

SEC567

Social Engineering for Penetration Testers

NEW!

Two-Day Course | Sat, Jun 11 - Sun, Jun 12 | 9:00am - 5:00pm | 12 CPEs | Laptop Required | Instructor: James Lyne

This class provides the blend of knowledge required to add social engineering skills to your penetration testing portfolio. Successful social engineering utilizes psychological principles and technical methods to measure your success and manage the risk. SEC567 covers the principles of persuasion and the psychological foundations required to craft effective attacks and bolsters this with many examples of what works taken from the experiences of both cyber criminals and the authors. On top of these principles, the course offers a number of tools (produced in our engagements over the years and now available in the course) and labs centered around the key technical skills required to measure your social engineering success and report it to your company or client. You'll learn how to perform recon on targets using a wide variety of sites and tools, create and track phishing campaigns, and develop media payloads that effectively demonstrate compromise scenarios. You'll also learn how to conduct pretexting exercises, and we wrap the course with a fun "Capture the Human" exercise to put what you've learned into practice. This is the perfect course to open up new attack possibilities, better understand the human vulnerability in attacks, and let you practice snares that have proven themselves in tests time and time again.

SEC580

Metasploit Kung Fu for Enterprise Pen Testing

Two-Day Course | Sat, Jun 11 - Sun, Jun 12 | 9:00am - 5:00pm | 12 CPEs | Laptop Required | Instructor: Eric Conrad

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.



sans.org/simulcast

MANAGEMENT SKILL-BASED COURSES

MGT305

Technical Communication & Presentation Skills for Security Professionals

One-Day Course | Sun, Jun 12 | 9:00am - 5:00pm | 6 CPEs | Laptop Required | Instructor: David Hoelzer

This course is designed for every IT professional in your organization. In this course we cover the top techniques that will show any attendee how to research and write professional quality reports, and how to create outstanding presentation materials. Attendees will also get a crash course on advanced public speaking skills.

Writing reports is a task that many IT professionals struggle with, sometimes from the perspective of writing the report and other times from the perspective of having to read someone else's report! In the morning material, we cover step by step how to work through the process of identifying critical ideas, how to properly research them, how to develop a strong argument in written form, and how to put it all down on paper. We also discuss some of the most common mistakes that can negatively impact the reception of your work and show how to avoid them. Attendees can expect to see the overall quality of their reports improve significantly as a result of this exercise.

After writing a meaningful report, it is not uncommon to find that we must present the key findings from that report before an audience, whether that audience is our department, upper management, or perhaps even the entire organization. How do you transform an excellent report into a powerful presentation? We will work through a process that serves to either condense a report into a presentation or can even be used to write a presentation from scratch that communicates your important thoughts in a meaningful and interesting way.



sans.edu

MGT415

A Practical Introduction to Cyber Security Risk Management**NEW!**

Two-Day Course | Sat, Jun 11 - Sun, Jun 12 | 9:00am - 5:00pm | 12 CPEs | Laptop Required | Instructor: James Tarala

In this course students will learn the practical skills necessary to perform regular risk assessments for their organizations. The ability to perform a risk assessment is crucial for organizations hoping to defend their systems. There are simply too many threats, too many potential vulnerabilities, and not enough resources to create an impregnable security infrastructure. Therefore every organization, whether it does so in an organized manner or not, will make priority decisions on how best to defend its valuable data assets. Risk assessment should be the foundational tool used to facilitate thoughtful and purposeful defense strategies.

You Will Learn:

- ▶ Step by step how to perform a risk assessment
- ▶ How to map an organization's business requirements to implemented security controls
- ▶ The elements of risk assessment and the data necessary for performing an effective risk assessment
- ▶ What in-depth risk management models exist for implementing a deeper risk management program in their organization

MGT433

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

Two-Day Course | Sat, Jun 11 - Sun, Jun 12 | 9:00am - 5:00pm | 12 CPEs | Laptop NOT Needed | Instructor: Lance Spitzner

Organizations have invested a tremendous amount of money and resources into securing technology, but little if anything into securing their employees and staff. As a result, people, not technology, have become their weakest link in cybersecurity. The most effective way to secure the human element is to establish a high-impact security awareness program that goes beyond just compliance and changes behaviors. This intense two-day course will teach you the key concepts and skills needed to build, maintain and measure just such a program. All course content is based on lessons learned from hundreds of security awareness programs from around the world. You will learn not only from your instructor, but from extensive interaction with your peers, as well. Please bring example materials from your security awareness program that you can show and share with other students during the course. Finally, through a series of labs and exercises, you will develop your own custom security awareness plan that you can implement as soon as you return to your organization.

sans.org/simulcastsans.edu

MGT535

Incident Response Team Management

Two-Day Course | Sat, Jun 11 - Sun, Jun 12 | 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.

The course has been updated to address current issues such as the advanced persistent threat, incident response in the cloud, and threat intelligence.

You Will Learn:

- ▶ Fundamentals of incident response
- ▶ How to establish requirements
- ▶ How to set up operations
- ▶ Communications
- ▶ How to make operations work
- ▶ Legal and regulatory issues
- ▶ Training, education, and awareness

BONUS SESSIONS

Enrich your SANS training experience! Evening talks by our instructors and selected subject-matter experts help you broaden your knowledge, hear from the voices that matter in computer security, and get the most for your training dollar.



KEYNOTE: State of the Internet Panel Discussion
Dr. Johannes Ullrich and Marcus Sachs

SANSFIRE offers the greatest opportunity to meet ISC handlers from around the world. During this session, you will have the chance to hear from our handlers and ask their opinions and insights on current threats. This is a unique opportunity you will only have at SANSFIRE — a dozen of the industry's brightest minds at your disposal for two intriguing hours!

Data Mining Malware Like a Boss
John Bambenek, ISC Handler

With over 500,000 new samples of distinct malware seen per day just by Virustotal, relying on traditional anti-malware defenses is becoming a losing battle. This talk will focus on new techniques to statically mine configuration data from large malware datasets to create an in-depth malware database.

\$HOME Sweet \$HOME
Xavier Mertens, ISC Handler

With the rise of the mobile devices, the Internet of Things and all media devices, home networks become a critical environment for all family members. This presentation will explain how to improve the security of your home network based on simple free software tools.

Penetration Testing Mobile Banking Applications
Bojan Zdrnja, ISC Handler

This presentation will demonstrate how a penetration test of a mobile banking application is typically conducted, what tools are used and what specific attack vectors should be given extra attention.

Exploit Kits and Indicators of Compromise
Brad Duncan, ISC Handler

Criminal groups use many methods to spread malware, and some of these methods make use of exploit kits. This presentation reviews different examples of successful malware infections by criminals using exploit kits.

How to Make Sense of IOCs (or Automate it or Lose it!)
Pedro Bueno, ISC Handler

We are living in a time where every single security vendor (and security community) has its own IOC feeds. There are different products, both open-source and commercial flavors that promise to make the best use of these feeds. This presentation will share experiences with both worlds.

Managing Large-Scale Incident Response
Kevin Liston, ISC Handler

So you've discovered that someone has had unauthorized access to your network for a while. We'll be going over the answers to that burning question: Now what?

Homegrown AppSec: How to Build Your Team from the Inside *Frank Kim & Eric Johnson*

The application security space has nearly twice as many job openings as candidates. Job qualifications demand several years of experience, knowledge of many security tools, and industry certifications. Endless search efforts and recruiting have led placement agencies and human resource departments to conclude that the industry has a talent shortage. Rather than stand idle and wait for the perfect candidate to apply for open positions, what if we told you the talent already exists inside your organization? This talk will explore how leaders can train and develop their existing employees to build a homegrown application security team.

The Dizzy New World of Cyber Investigations: Law, Ethics and Evidence *Ben Wright*

Increasingly, employers and enterprises are engaged in cyber investigations. The explosion of cyber evidence (email, text, metadata, social media, etc.) about every little thing 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. Surprises abound. 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.

Continuous Opportunity: DevOps & Security
Ben Allen

With DevOps practices spreading throughout many organizations, development and operations teams are creating tools and gathering ongoing data to deliver features to end users at an ever-increasing rate. This can be an immense challenge when the security team is left out of the loop, and an even bigger opportunity when security can bring actionable ideas to the table. We will explore some concrete ways that security teams can gain visibility into a rapidly changing environment by adding value to the pipelines that power the DevOps practice.

How to Commit Card Fraud *G. Mark Hardy*

Well, we're not going to show you how to commit fraud, but we will show you how the bad guys do it and how you can protect yourself and your business. We'll take a look into the "dark web" and see how these big card heists are pulled off, why chip-and-pin won't solve the fraud problem, and why payment technologies like Apple Pay pose new risks. You'll learn the ecosystem of fraud, and how it's become a big business that costs banks and merchants over \$16 billion annually. We'll have a mag stripe card reader so you can really see what's in your wallet.

Making Awareness Stick
Lance Spitzner

One of the most common, long-term challenges faced by any awareness program is getting it to stick. How do you create an engaging program that people want to listen to, teaches them more, and ultimately changes behaviors? In this talk we explain effective efforts by organizations around the world to emotionally engage and communicate to their employees. Key points you will learn include behavior modeling, defining culture, developing an engagement strategy, ambassador programs and gamification.

How to Bring Some Advanced Persistent Trickery to Your Fight Against Advanced Persistent Threats *Bryce Galbraith*

You know you have intruders in your house...but this is your house and no one knows it better than you. Don't sit back and wait...it's game on! This presentation will explore ways that you can frustrate, annoy, and potentially reveal advanced persistent threats with active defense, offensive countermeasures and cyber deception (legally and ethically).

Playing with SCADA's Modbus Protocol

Justin Searle

Join Justin for a peek into one of SCADA's oldest and most deployed TCP/IP protocols. He'll take you through the modbus network protocol standard and walk you through some hands-on exercises, including analyzing modbus network captures, configuring modbus endpoint simulators, and generating your own modbus traffic to query PLCs, and a primer on fuzzing modbus endpoints.

CISO Success Strategies *Frank Kim*

The increased importance and visibility of cybersecurity as a vital component of business growth make it critical that security leaders understand how to connect with senior executives and business leaders. Join Frank Kim, seasoned security leader and CISO, as he explains three things that will make you a more effective security business leader.

Smartphone and Network Forensics Go Together Like Peas and Carrots

Heather Mahalik and Phil Hagen

There are strong ties between the smartphone and network aspects of the forensic process. In this talk, Heather Mahalik, will address the smartphone side of this investigative coin and Phil Hagen will look at things from the network side. As often identified in the forensic process, a comprehensive approach is necessary to conduct a thorough investigation.

Writing Tech: Stories from the Field *Joshua Wright*

Tech writing is a great way to differentiate you from your peers, opening up opportunities for career advancement and peer approbation. In the last decade, Josh has learned a thing or two about tech writing as the author or co-author of four books and six SANS courses. Come to this talk to learn about tech writing, and the opportunities it opens up for your career and leave with a sense of purpose, and approbation.

Securing Your Kids *Lance Spitzner*

Technology is an amazing tool. It allows our kids to access a tremendous amount of information, meet new people, and communicate with friends around the world. In addition, for them to be successful in the 21st century they have to know and understand how to leverage these new tools. However, with all these capabilities come a variety of new risks, risks that as parents you may not understand or even be aware of. In this one-hour presentation we cover the top three risks to kids online and the top steps you can take to protect them.

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 learn not only how to take action against attackers, but how to do it legally.

Executing an Active Defense Strategy in an ICS/SCADA Network *Robert M. Lee*

An active defense is a focus on analysts monitoring, responding to, and learning from threats internal to their networks. The application of that knowledge ensures that defenders get better over time. This talk will present an active defense strategy, how it aligns with ICS/SCADA networks, and a threat case-study to highlight the strengths of defenders in these types of networks.

Going Mobile: Are Your Apps Putting You at Risk?

Eric Johnson

With over 3 million apps now deployed in the Apple and Google Play app stores, the importance of mobile application security assessments is at an all-time high. Business critical mobile apps now handle payment card, healthcare, and financial information on end-user devices, so organizations are vulnerable to an entirely new class of mobile software vulnerabilities. As the bad guys shift their focus towards attacking mobile applications, defenders are struggling to keep up. We will discuss some common issues often found in mobile application vulnerability assessments, such as local data storage, inter-process communication, and broken cryptography. We'll then teach you the mitigation strategies to apply to your organization's mobile apps.

Vendor-Sponsored Events

Vendor Expo

Wednesday, June 15 | 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

Wednesday, June 15 | 12:00pm - 1:30pm

Join these sponsoring vendors and others on the expo floor for an introduction to leading solutions and services that showcase the best options in information security.

Lunch & Learn Presentations

Throughout SANSFIRE 2016, 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

Wednesday, June 15 | 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.

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

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

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

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

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

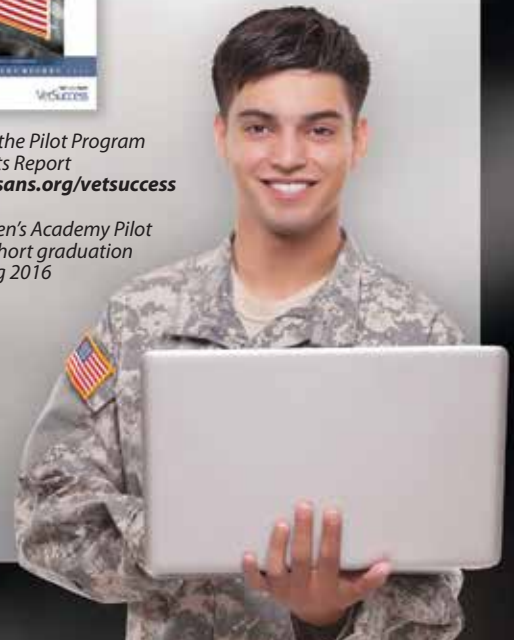
sans.org/cybertalent/immersion-academy

Email: immersionacademy@sans.org



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

Women's Academy Pilot
1st cohort graduation
Spring 2016



SANS | **CyberTalent**
IMMERSION ACADEMY

VetSuccess



Security Awareness Training by the Most Trusted Source

Computer-based Training for your Employees

End User
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

Visit SANS Securing The Human at
securingthehuman.sans.org



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



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

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

“Joining the SANS master’s program
was probably one of the best decisions I’ve ever made.”

-John Hally, MSISE, EBSCO Information Services

Earn a master’s degree or specialized certificate from SANS’ regionally accredited graduate school.

Master of Science Degrees

- Information Security Engineering (MSISE)
- Information Security Management (MSISM)

Graduate Certificates

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

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.

NEW GIAC CERTIFICATIONS!



www.giac.org

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

SANS TRAINING COURSE:

SEC511: Continuous Monitoring and Security Operations

“The demand for skilled analysts is growing as organizations refocus efforts on better monitoring capabilities. The GMON helps individuals demonstrate knowledge and ability in detecting modern adversary activities.”

-Seth Misenar, co-author of SANS SEC511: Continuous Monitoring and Security Operations



The new **GPYC** certification focuses on applying core programming concepts and techniques to the Python programming language. Certified individuals can create simple Python-based tools to interact with network traffic, create custom executables, test and interact with databases and websites, and parse logs or sets of data.

SANS TRAINING COURSE:

SEC573: Python for Penetration Testers

SANS TRAINING FORMATS

LIVE TRAINING



Multi-Course Training Events

sans.org/security-training/by-location/all

Live Instruction from SANS' Top Faculty, Vendor Showcase, Bonus Evening Sessions, and Networking with Your Peers



Summit

sans.org/summit

Live IT Security Summits and Training



Community SANS

sans.org/community

Live Training in Your Local Region with Smaller Class Sizes



Private Training

sans.org/private-training

Live Training at Your Office Location



Mentor

sans.org/mentor

Live Multi-Week Training with a Mentor

ONLINE TRAINING



OnDemand

sans.org/ondemand

Four Months of Self-Paced e-Learning



vLive

sans.org/vlive

Live Online, Evening Sessions with Six Months of Online Course Access



Simulcast

sans.org/simulcast

Online, Daytime Access to a One-Week Live-Event Course



SelfStudy

sans.org/selfstudy

Self-Paced Study with Lecture Audio



OnDemand Bundles

sans.org/ondemand/bundles

Extend Your Training with an OnDemand Bundle Including Four Months of E-learning



The SANS Voucher Program allows an organization to manage its training budget from a single SANS Account, potentially receive bonus funds based on its investment level, and centrally administer its training.

CONTACT

vouchers@sans.org

www.sans.org/vouchers

VOUCHER PROGRAM



Training Investment & Bonus Funds

To open an Account, an organization makes an agreed-upon training investment. Based on the amount of the training investment, an organization could be eligible to receive additional bonus funds.

The investment and bonus funds:

- Can be applied to **any live or online SANS training course, SANS Summit, GIAC certification, or certification renewal***
- Can be increased at any time by making additional prepayments
- Need to be allocated within 12 months, although the term can be extended by re-investing additional funds before the end of the 12-month term



Flexibility & Control

The online SANS Admin tool allows the program administrator to manage the account at anytime from anywhere.

With the SANS Admin Tool, the Administrator can:

- Approve student enrollment and allocate funds
- View fund usage in real time
- View students' certification status and test results
- Monitor OnDemand course progress by student per course

By creating a SANS Account, your organization can:

- Simplify the procurement process with a single invoice and payment
- Easily change course attendees if previous plans change
- Lock-in your hard-fought training budget and allocate over time
- Control how, where, and for whom funds are spent
- Allow employees to register for training while managing approvals centrally

Getting Started

Complete and submit the form online (sans.org/vouchers) and a SANS representative in your region will contact you within 24 business hours.

Get started today and within as little as one week we can create your Account and your employees can begin their training.

*Current exceptions are the Partnership Program, Security Awareness Training, and SANS workshops hosted at events and conferences run by other companies.

FUTURE SANS TRAINING EVENTS

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



SANS 2016

Orlando, FL
Mar 12-21



Security Operations Center

SUMMIT & TRAINING 2016

Crystal City, VA
May 19-26



NORTHERN VIRGINIA Reston 2016

Reston, VA
April 4-9



Digital Forensics & Incident Response

SUMMIT & TRAINING 2016

Austin, TX
June 23-30



Atlanta 2016

Atlanta, GA
April 4-9



Salt Lake City 2016

Salt Lake City, UT
June 27 - July 2



Threat Hunting & Incident Response

SUMMIT & TRAINING 2016

New Orleans, LA
April 12-19



Rocky Mountain 2016

Denver, CO
July 11-16



Pen Test Austin 2016

Austin, TX
April 18-23



Minneapolis 2016

Minneapolis, MN
July 18-23



Security West 2016

San Diego, CA
April 29 - May 6



San Antonio 2016

San Antonio, TX
July 18-23



Baltimore Spring 2016

Baltimore, MD
May 9-14



ICS Security SUMMIT & TRAINING 2016

Houston, TX
Jul 25-30



Houston 2016

Houston, TX
May 9-14



San Jose 2016

San Jose, CA
July 25-30

FUTURE SANS TRAINING EVENTS

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



Boston 2016

Boston, MA
August 1-6



Seattle 2016

Seattle, WA
October 3-8



Security Awareness SUMMIT & TRAINING 2016

San Francisco, CA
August 1-10



Baltimore 2016

Baltimore, MD
October 10-15



Portland 2016

Portland, OR
August 8-13



Cyber Defense **San Diego** 2016

San Diego, CA
October 23-28



Dallas 2016

Dallas, TX
August 8-13



Tysons Corner 2016

Tysons Corner, VA
October 24-29



Chicago 2016

Chicago, IL
August 22-27



Pen Test Hackfest SUMMIT & TRAINING 2016

Crystal City, VA
November 2-9



Virginia Beach 2016

Virginia Beach, VA
August 22 - September 2



Miami 2016

Miami, FL
November 7-12



Crystal City 2016

Crystal City, VA
September 6-11



San Francisco 2016

San Francisco, CA
Nov 27 - Dec 2



Network Security 2016

Las Vegas, NV
September 10-17



Cyber Defense **Initiative** 2016

Washington, DC
December 9-18

Hotel Information

Training Campus
Washington Marriott Wardman Park

2660 Woodley Road, NW | Washington, DC 20008
202-328-2000

sans.org/event/sansfire-2016/location

When you arrive at the Washington Marriott Wardman Park, you'll find a charming neighborhood in the heart of Washington, DC filled with amazing restaurants and quaint shops. With a Metro stop just outside the doors and area airports close by, it's a premier city destination just two Metro stops from everything DC has to offer.

Special Hotel Rates Available

A special discounted rate of \$209.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through May 19, 2015.

Top 5 reasons to stay at the Washington Marriott Wardman Park

- 1 All SANS attendees receive complimentary high-speed Internet when booking in the SANS block.
- 2 No need to factor in daily cab fees and the time associated with travel to alternate hotels.
- 3 By staying at the Washington Marriott Wardman Park, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.
- 4 SANS schedules morning and evening events at the Washington Marriott Wardman Park that you won't want to miss!
- 5 Everything is in one convenient location!

SANSFIRE 2016

Registration Information

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



Register online at sans.org/event/sansfire-2016/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. Everyone with Internet access must complete the online registration form. We do not take registrations by phone.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	4-20-16	\$400.00	5-11-16	\$200.00
	Some restrictions apply.			

Use code
EarlyBird16
when registering

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.

*Early-bird rates and/or other discounts cannot be combined with the group discount.



SANS SIMULCAST

To register for a SANSFIRE 2016 Simulcast course, please visit sans.org/event/sansfire-2016/attend-remotely

SANS Voucher Credit Program

Expand your training budget! Extend your Fiscal Year. The SANS Voucher Discount Program pays you credits and delivers flexibility.
sans.org/vouchers

Cancellation

You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by Wed, May 25, 2016 — processing fees may apply.

SANSFIRE 2016 REGISTRATION FEES

Register online at sans.org/event/sansfire-2016/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 4-20-16	Paid before 5-11-16	Paid after 5-11-16	Add GIAC Cert	Add OnDemand	Add NetWars Continuous
<input type="checkbox"/> SEC301	Intro to Information Security	\$4,485	\$4,685	\$4,885	<input type="checkbox"/> \$659	<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> SEC401	Security Essentials Bootcamp Style	\$5,220	\$5,420	\$5,620	<input type="checkbox"/> \$659	<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> SEC501	Advanced Security Essentials — Enterprise Defender	\$5,220	\$5,420	\$5,620	<input type="checkbox"/> \$659	<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> SEC503	Intrusion Detection In-Depth	\$5,220	\$5,420	\$5,620	<input type="checkbox"/> \$659	<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling	\$5,220	\$5,420	\$5,620	<input type="checkbox"/> \$659	<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> SEC505	Securing Windows with PowerShell and the Critical Security Controls	\$5,110	\$5,310	\$5,510	<input type="checkbox"/> \$659	<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> SEC511	Continuous Monitoring and Security Operations	\$5,220	\$5,420	\$5,620	<input type="checkbox"/> \$659	<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> SEC542	Web App Penetration Testing and Ethical Hacking	\$5,220	\$5,420	\$5,620	<input type="checkbox"/> \$659	<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> SEC550	Active Defense, Offensive Countermeasures and Cyber Deception	\$4,485	\$4,685	\$4,885			<input type="checkbox"/> \$1,199
<input type="checkbox"/> SEC560	Network Penetration Testing and Ethical Hacking NEW!	\$5,220	\$5,420	\$5,620	<input type="checkbox"/> \$659	<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> SEC561	Immersive Hands-On Hacking Techniques	\$5,220	\$5,420	\$5,620			<input type="checkbox"/> \$1,199
<input type="checkbox"/> SEC562	CyberCity Hands-on Kinetic Cyber Range Exercise	\$6,180	\$6,380	\$6,580			<input type="checkbox"/> \$1,199
<input type="checkbox"/> SEC566	Implementing and Auditing the Critical Security Controls — In-Depth	\$4,485	\$4,685	\$4,885	<input type="checkbox"/> \$659	<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> SEC575	Mobile Device Security and Ethical Hacking	\$5,220	\$5,420	\$5,620	<input type="checkbox"/> \$659	<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> SEC579	Virtualization and Private Cloud Security	\$5,220	\$5,420	\$5,620		<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> SEC617	Wireless Ethical Hacking, Penetration Testing, and Defenses	\$4,740	\$4,940	\$5,140	<input type="checkbox"/> \$659		<input type="checkbox"/> \$1,199
<input type="checkbox"/> SEC642	Advanced Web App Penetration Testing and Ethical Hacking	\$5,220	\$5,420	\$5,620			<input type="checkbox"/> \$1,199
<input type="checkbox"/> SEC660	Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	\$5,220	\$5,420	\$5,620	<input type="checkbox"/> \$659	<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> SEC760	Advanced Exploit Development for Penetration Testers	\$4,950	\$5,150	\$5,350			<input type="checkbox"/> \$1,199
<input type="checkbox"/> AUD507	Auditing & Monitoring Networks, Perimeters, and Systems	\$5,110	\$5,310	\$5,510	<input type="checkbox"/> \$659	<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> DEV522	Defending Web Applications Security Essentials	\$5,110	\$5,310	\$5,510	<input type="checkbox"/> \$659	<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> DEV541	Secure Coding in Java/JEE: Developing Defensible Applications	\$4,020	\$4,220	\$4,420	<input type="checkbox"/> \$659	<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> DEV544	Secure Coding in .NET: Developing Defensible Applications	\$4,020	\$4,220	\$4,420	<input type="checkbox"/> \$659	<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> FOR408	Windows Forensic Analysis	\$5,220	\$5,420	\$5,620	<input type="checkbox"/> \$659	<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> FOR508	Advanced Digital Forensics and Incident Response	\$5,220	\$5,420	\$5,620	<input type="checkbox"/> \$659	<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> FOR518	Mac Forensic Analysis	\$5,220	\$5,420	\$5,620		<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> FOR572	Advanced Network Forensics and Analysis	\$5,220	\$5,420	\$5,620	<input type="checkbox"/> \$659	<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> FOR578	Cyber Threat Intelligence NEW!	\$4,695	\$4,895	\$5,095			<input type="checkbox"/> \$1,199
<input type="checkbox"/> FOR585	Advanced Smartphone Forensics	\$5,220	\$5,420	\$5,620		<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> FOR610	Reverse-Engineering Malware: Malware Analysis Tools and Techniques	\$5,220	\$5,420	\$5,620	<input type="checkbox"/> \$659	<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> ICS410	ICS/SCADA Security Essentials	\$4,785	\$4,985	\$5,185	<input type="checkbox"/> \$659	<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> ICS515	ICS Active Defense and Incident Response NEW!	\$5,035	\$5,235	\$5,435		<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> LEG523	Law of Data Security and Investigations	\$4,485	\$4,685	\$4,885	<input type="checkbox"/> \$659	<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> MGT414	SANS Training Program for CISSP® Certification	\$4,590	\$4,790	\$4,990	<input type="checkbox"/> \$659	<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> MGT512	SANS Security Leadership Essentials for Managers with Knowledge Compression™	\$4,865	\$5,065	\$5,265	<input type="checkbox"/> \$659	<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> MGT514	IT Security Strategic Planning, Policy, and Leadership	\$4,485	\$4,685	\$4,885		<input type="checkbox"/> \$659	<input type="checkbox"/> \$1,199
<input type="checkbox"/> MGT525	IT Project Management, Effective Communication, and PMP® Exam Prep	\$4,590	\$4,790	\$4,990	<input type="checkbox"/> \$659		<input type="checkbox"/> \$1,199

Skill-Based Short Courses

		Course fee if taking a 4-6 day course	Course fee
<input type="checkbox"/> SEC440	Critical Security Controls: Planning, Implementing, and Auditing	\$1,450	\$2,250
<input type="checkbox"/> SEC524	Cloud Security Fundamentals	\$1,350	\$2,130
<input type="checkbox"/> SEC546	IPv6 Essentials	\$1,350	\$2,130
<input type="checkbox"/> SEC567	Social Engineering for Penetration Testers NEW!	\$1,350	\$2,130
<input type="checkbox"/> SEC580	Metasploit Kung Fu for Enterprise Pen Testing	\$1,350	\$2,130
<input type="checkbox"/> MGT305	Technical Communication and Presentation Skills for Security Professionals	\$850	\$1,300
<input type="checkbox"/> MGT415	A Practical Introduction to Cyber Security Risk Management NEW!	\$1,350	\$2,130
<input type="checkbox"/> MGT433	Securing The Human: How to Build, Maintain & Measure a High-Impact Awareness Program	\$1,350	\$2,130
<input type="checkbox"/> MGT535	Incident Response Team Management	\$1,350	\$2,130
<input type="checkbox"/> HOSTED	Healthcare Security Essentials NEW!		\$2,130
<input type="checkbox"/> HOSTED	Physical Penetration Testing		\$2,000
<input type="checkbox"/> SPECIAL	CORE NetWars Tournament — Tournament Entrance Fee	FREE	\$1,450
<input type="checkbox"/> SPECIAL	DFIR NetWars Tournament — Tournament Entrance Fee	FREE	\$1,450

Pay for any long course using the code

EARLYBIRD16 at checkout by:

4-20-16 to get **\$400 OFF**


5-11-16 to get **\$200 OFF**

**EARLYBIRD
DISCOUNTS**


Open a **SANS Portal Account** today
to enjoy these FREE resources:

WEBCASTS


 **Ask The Expert Webcasts** — SANS experts bring current and timely information on relevant topics in IT Security.


 **Analyst Webcasts** — A follow-on to the SANS Analyst Program, Analyst Webcasts provide key information from our whitepapers and surveys.


 **WhatWorks Webcasts** — The SANS WhatWorks webcasts bring powerful customer experiences showing how end users resolved specific IT Security issues.

 **Tool Talks** — Tool Talks are designed to give you a solid understanding of a problem, and how a vendor's commercial tool can be used to solve or mitigate that problem.

NEWSLETTERS

 **NewsBites** — Twice-weekly high-level executive summary of the most important news relevant to cybersecurity professionals

 **OUCH!** — The world's leading monthly free security awareness newsletter designed for the common computer user

 **@RISK: The Consensus Security Alert**
— A reliable weekly summary of (1) newly discovered attack vectors, (2) vulnerabilities with active new exploits, (3) how recent attacks worked, and (4) other valuable data

OTHER FREE RESOURCES

- | | |
|----------------------------------|--|
| ■ InfoSec Reading Room | ■ Security Posters |
| ■ Top 25 Software Errors | ■ Thought Leaders |
| ■ 20 Critical Controls | ■ 20 Coolest Careers |
| ■ Security Policies | ■ Security Glossary |
| ■ Intrusion Detection FAQ | ■ SCORE (Security Consensus Operational Readiness Evaluation) |
| ■ Tip of the Day | |

sans.org/account

SAVE \$400 on SANSFIRE 2016 courses!

Register and pay by 4-20-16 (SAVE \$400) or 5-11-16 (SAVE \$200) – **sans.org/sansfire**

