

SANS CDI

POWERED BY

SANS
NETWARS
EXPERIENCE

INCLUDING THE
5TH ANNUAL

**Tournament
of Champions**



GIAC-Approved Training

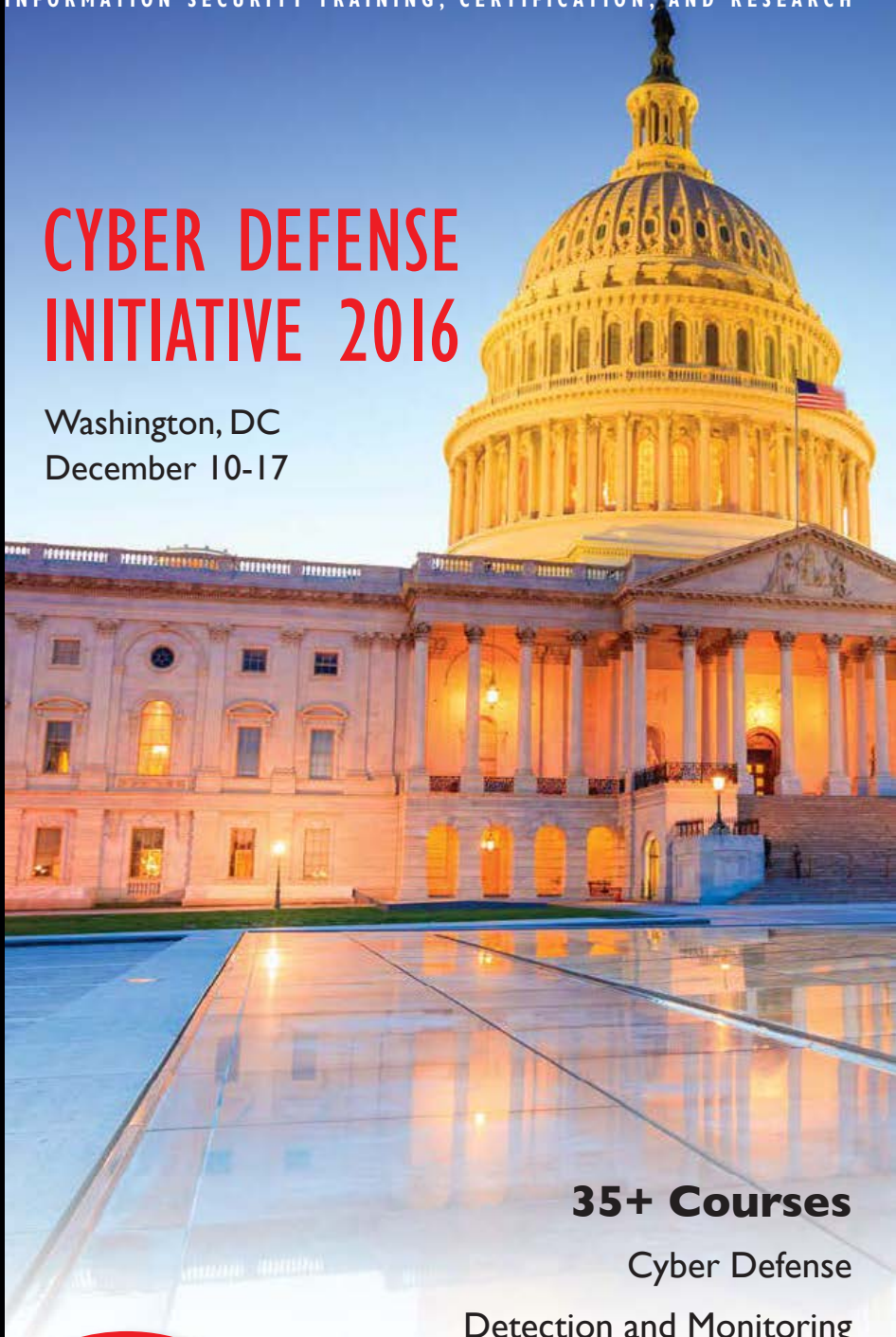
*"SANS is educational
Nirvana. No other training
today is capable of giving
such in-depth information
on a consistently
well-delivered schedule."*

-ROBERT WANGER, TRANSUNION

Register at
www.sans.org/cdi

CYBER DEFENSE INITIATIVE 2016

Washington, DC
December 10-17



35+ Courses

Cyber Defense
Detection and Monitoring
Pen Testing
Incident Response
Digital Forensics
Ethical Hacking
Management, Audit, Legal
Secure Development
ICS/SCADA Security

**SAVE
\$400**

when you register and
pay by October 19th
using code
EarlyBird2016

Ed Skoudis here. We've got something really cool for you to check out! An incredible training event coming is soon: **SANS Cyber Defense Initiative 2016** in Washington DC, December 10-17. This unique event features more than THIRTY of the best cybersecurity courses the industry has to offer; dozens of evening sessions full of late-breaking, must-have skills, and so much more. CDI covers the gamut of today's most needed cybersecurity skillsets, including cyber defense, digital forensics and incident response (DFIR), penetration testing, audit, application security, industrial control systems, and security management!



Ed Skoudis

What's more, we'll be running our brand-new **Core NetWars Experience** free for all students attending a five- or six-day course, giving you an amazing opportunity to apply the hands-on skills you learn in class in these interactive evening sessions. You can participate in the NetWars EXPERIENCE solo or in a team, completely up to you, offering additional opportunities for networking and fun. At CDI, we'll also host a fantastic **DFIR NetWars Tournament**, and the fifth annual **NetWars Tournament of Champions**.

Our course lineup at CDI is unmatched, featuring SANS immersive learning in five- and six-day courses, along with a series of additional one- and two-day courses to augment your skills. Of particular note is one of SANS' newest courses, ICS515, where you'll learn vital skills in industrial control system active defense and incident response. CDI's must-see evening talks include lessons learned from the Ukrainian power grid attack, continuous monitoring of large-scale networks, building an effective enterprise security program, and much more, all presented by some of the very best minds in our field.

Many SANS courses at the CDI event are closely aligned with well-known and highly respected GIAC certifications. By mastering the skills in your course and passing the associated GIAC exam, you can show your employer that you've developed the much-needed skills so essential in protecting against today's cyber attacks.

If you can't travel to CDI, you can still attend our most popular courses being held there from the comfort of your own office or home using the SANS Simulcast system. Students who register for a Simulcast course at CDI will attend remotely by logging into a virtual classroom and joining the live class. No travel budget? You can still join us and learn! With Simulcast, the SANS team focuses on bringing you all the in-class action and learning, no matter where you are located.

It's an exciting time to work in the cybersecurity industry, and CDI can help you build the vital skills needed to protect your organization from the latest attacks. With attackers growing more brazen and exploiting mission-critical computer systems, it's more important now than ever to ensure you are ready with the latest skills and techniques to excel. That's what CDI is all about. I urge you to reserve some time on your calendar and register for CDI today.

I look forward to seeing you at CDI in Washington DC!

Ed Skoudis

SANS Fellow and Curriculum Lead, Penetration Testing

SANS INFORMATION SECURITY TRAINING AND YOUR CAREER ROADMAP

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

Penetration Testing/Vulnerability Assessment

CORE COURSES

SEC301 (GISF) ► SEC401 (GSEC)

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

SEC550
Active Defense,
Offensive Countermeasures,
and Cyber Deception

SAMPLE JOB TITLES

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

NETWORK & EXPLOITS

SEC560
Network Penetration Testing
and Ethical Hacking
GPEN

SEC660
Advanced Penetration Testing,
Exploit Writing and
Ethical Hacking
GXPEN

SEC760
Advanced Exploit Development
for Penetration Testers

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

SPECIALIZATION

SEC567
Social Engineering for
Penetration Testers

SEC573
Python for
Penetration Testers
GPYC

SEC580
Metasploit Kung Fu
for Enterprise
Pen Testing

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

Network Operations Center, System Admin, Security Architecture

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.

SAMPLE JOB TITLES

- System/IT administrator
- Security administrator
- Security architect/engineer

CORE COURSES

SEC301 (GISF) ► SEC401 (GSEC) ► SEC501 (GCED)

SEC505
Securing Windows
and PowerShell
Automation
GCWN

SEC506
Securing
Linux/Unix
Automation
GCUX

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

SEC579
Virtualization and
Private Cloud
Security

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

SEC503

Intrusion Detection
In-Depth
GCIA

FOR572

Advanced Network
Forensics and Analysis
GNFA

SEC511

Continuous Monitoring and
Security Operations
GMON

SEC550

Active Defense,
Offensive Countermeasures,
and Cyber Deception

THREAT INTELLIGENCE

FOR578

Cyber Threat Intelligence

Risk and Compliance/Auditing/Governance

SEC566

Implementing and
Auditing
the Critical Security
Controls —
In-Depth
GCCC

AUD507

Auditing &
Monitoring
Networks,
Perimeters, and
Systems
GSNA

LEG523

Law of Data Security
and Investigations
GLEG

MGT433

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

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

Development – Secure Development

CORE

**Securing The
Human for
Developers**
Application Security
Awareness Modules

DEV522

Defending Web Applications
Security Essentials
GWEB

DEV531

Defending Mobile Applications
Security Essentials

DEV534

Secure DevOps:
A Practical Introduction

SECURE CODING

DEV541

Secure Coding
in Java/JEE
GSSP-JAVA

DEV544

Secure Coding
in .NET
GSSP-.NET

DEV543

Secure Coding
in C/C++

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

SPECIALIZATION

SEC542

Web App Pen Testing
and Ethical Hacking
GWAPT

SEC642

Advanced Web App
Pen Testing and
Ethical Hacking

Industrial Control Systems

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

SAMPLE JOB TITLES

- IT & OT support staff
- IT & OT cybersecurity
- ICS engineer

ICS410

ICS/SCADA Security
Essentials
GICSP

ICS456

Essentials for NERC
Critical Infrastructure
Protection

ICS515

ICS Active Defense and
Incident Response

HOSTED

Assessing and
Exploiting Control
Systems

HOSTED

Critical Infrastructure
and Control System
Cybersecurity

Cyber or IT Security Management

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.

FOUNDATIONAL

MGT512

SANS Security Leadership Essentials for Managers with Knowledge Compression™
GSLC

MGT525

IT Project Management, Effective Communication & PMP® Exam Prep
GCPM

MGT414

SANS Training Program for CISSP® Certification
GISP

CORE

MGT514

IT Security Strategic Planning, Policy, and Leadership

LEG523

Law of Data Security and Investigations
GLEG

MGT415

A Practical Introduction to Cybersecurity Risk Management

MGT535

Incident Response Team Management

SPECIALIZATION

AUD507

Auditing & Monitoring Networks, Perimeters, and Systems
GSNA

SEC566

Implementing and Auditing the Critical Security Controls — In-Depth
GCCC

MGT433

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

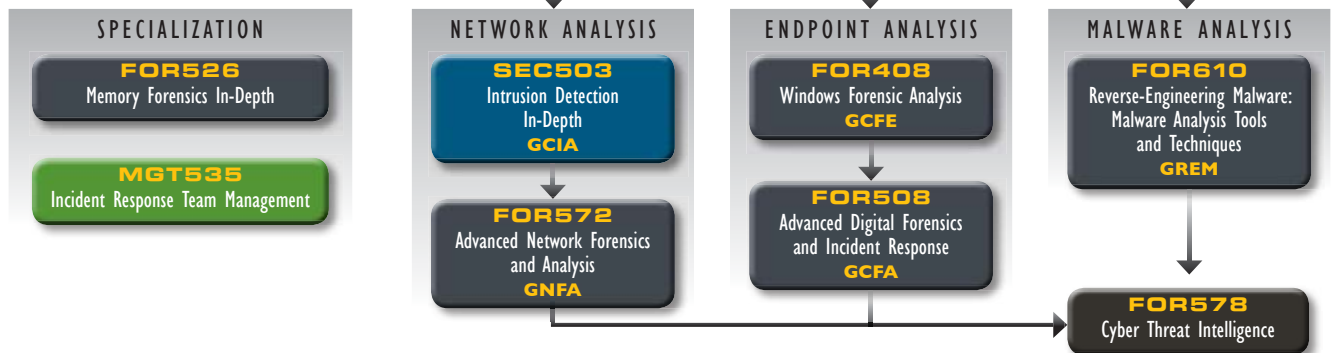
PMP is registered mark of the Project Management Institute, Inc.

Incident Response and Threat Hunting

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

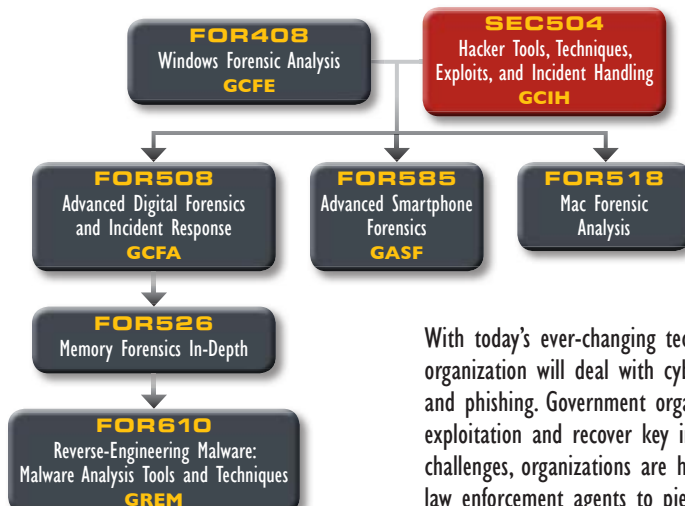
- Security analyst/engineer
- SOC analyst
- Cyber threat analyst
- CERT member
- Malware analyst



Digital Forensic Investigations and Media Exploitation

SAMPLE JOB TITLES

- Computer crime investigator
- Law enforcement
- Digital investigations analyst
- Media exploitation analyst
- Information technology litigation 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 SANS CDI 2016 for FREE!***



SANS NETWARS EXPERIENCE

CORE NETWARS EXPERIENCE

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

Who Should Attend

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

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



DFIR NETWARS TOURNAMENT

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

Who Should Attend

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

***Challenge Yourself
Before the Enemy Does –
DFIR NetWars***

Both NetWars competitions will be played over two evenings: December 15-16

Prizes will be awarded at the conclusion of the games.

***REGISTRATION IS LIMITED AND IS FREE**

for students attending any long course at SANS CDI 2016 (NON-STUDENT ENTRANCE FEE IS \$1,520).

Courses-at-a-Glance

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

			SAT 12-10	SUN 12-11	MON 12-12	TUE 12-13	WED 12-14	THU 12-15	FRI 12-16	SAT 12-17
SEC301	Intro to Information Security	<i>SIMULCAST</i>			PAGE 6					
SEC401	Security Essentials Bootcamp Style				PAGE 8					
SEC440	Critical Security Controls: Planning, Implementing, and Auditing		P 64							
SEC501	Advanced Security Essentials – Enterprise Defender				PAGE 10					
SEC503	Intrusion Detection In-Depth				PAGE 12					
SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling	<i>SIMULCAST</i>			PAGE 14					
SEC505	Securing Windows and PowerShell Automation	<i>SIMULCAST</i>			PAGE 16					
SEC511	Continuous Monitoring and Security Operations	<i>SIMULCAST</i>			PAGE 18					
SEC542	Web App Penetration Testing and Ethical Hacking				PAGE 20					
SEC550	Active Defense, Offensive Countermeasures, and Cyber Deception				PAGE 22					
SEC560	Network Penetration Testing and Ethical Hacking				PAGE 24					
SEC561	Immersive Hands-On Hacking Techniques				PAGE 26					
SEC566	Implementing and Auditing the Critical Security Controls – In-Depth				PAGE 28					
SEC567	Social Engineering for Penetration Testers NEW!		P 64							
SEC575	Mobile Device Security and Ethical Hacking	<i>SIMULCAST</i>			PAGE 30					
SEC579	Virtualization and Private Cloud Security				PAGE 32					
SEC580	Metasploit Kung Fu for Enterprise Pen Testing	<i>SIMULCAST</i>	P 65							
SEC660	Advanced Penetration Testing, Exploit Writing, and Ethical Hacking				PAGE 34					
SEC760	Advanced Exploit Development for Penetration Testers				PAGE 36					
FOR408	Windows Forensic Analysis	<i>SIMULCAST</i>			PAGE 38					
FOR508	Advanced Digital Forensics and Incident Response	<i>SIMULCAST</i>			PAGE 40					
FOR518	Mac Forensic Analysis				PAGE 42					
FOR572	Advanced Network Forensics and Analysis				PAGE 44					
FOR578	Cyber Threat Intelligence NEW!				PAGE 46					
FOR610	Reverse-Engineering Malware: Malware Analysis Tools and Techniques	<i>SIMULCAST</i>			PAGE 48					
MGT305	Technical Communication and Presentation Skills for Security Professionals		P 65							
MGT414	SANS Training Program for CISSP® Certification				PAGE 50					
MGT415	A Practical Introduction to Cybersecurity Risk Management		P 66							
MGT433	Securing The Human: How to Build, Maintain, and Measure a High-Impact Awareness Program	<i>SIMULCAST</i>	P 66							
MGT512	SANS Security Leadership Essentials for Managers with Knowledge Compression™				PAGE 52					
MGT514	IT Security Strategic Planning, Policy, and Leadership				PAGE 54					
MGT535	Incident Response Team Management		P 66							
DEV522	Defending Web Applications Security Essentials				PAGE 56					
DEV534	Secure DevOps: A Practical Introduction NEW!		P 67							
ICS456	Essentials for NERC Critical Infrastructure Protection NEW!				PAGE 58					
ICS515	ICS Active Defense and Incident Response				PAGE 60					
AUD507	Auditing & Monitoring Networks, Perimeters, and Systems				PAGE 62					
HOSTED	Health Care Security Essentials NEW!		P 67							
HOSTED	Physical Access Control Systems: Elements of Design, Offense, and Defense NEW!		P 67							
	Core NetWars Experience & DFIR NetWars Tournament								PAGE 2	

CONTENTS

Core NetWars Experience	2	GIAC	71	SANS Training Formats (Live & Online)	75
DFIR NetWars Tournament	2	SANS Technical Institute	72	Future SANS Training Events	76-77
SANS Instructors	4-5	SANS CyberTalent Immersion Academy	72	Hotel Information.	78-79
Bonus Sessions	68-69	DoD Directive 8140	73	Registration Information	80
Vendor-Sponsored Events.	69	SANS Cyber Guardian Program	73	Registration Fees	81
The Value of SANS Training and You	70	SANS Voucher Program	74		



SANS instructors are real-world practitioners who specialize in the subjects they teach. All instructors undergo rigorous training and testing in order to teach SANS courses. This guarantees that what you learn in class will be up to date and relevant to your job. The line-up of instructors for SANS CDI 2016 includes:



Ben Allen
SANS Instructor
@mr_secure
Teaching DEV534



Ovie Carroll
Certified Instructor
Teaching FOR408



Eric Conrad
Senior Instructor
@eric_conrad
Teaching SEC542



Tim Conway
SANS Instructor
Teaching ICS456



Christopher Crowley
Certified Instructor
@CCrowMontance
Teaching SEC575 & MGT535



Sarah Edwards
Certified Instructor
@iamevltwin
Teaching FOR518



Kevin Fiscus
Certified Instructor
@kevinbfiscus
Teaching SEC561



Jason Fossen
Faculty Fellow
@JasonFossen
Teaching SEC505



Bryce Galbraith
Principal Instructor
@brycegalbraith
Teaching SEC550 & SEC580



Philip Hagen
Certified Instructor
@PhilHagen
Teaching FOR572



Paul A. Henry
Senior Instructor
@phenrycissp
Teaching SEC501



Frank Kim
Certified Instructor
@fykim
Teaching MGT514 & DEV534

For instructor bios, visit: www.sans.org/event/cyber-defense-initiative-2016/instructors



Robert M. Lee
 Certified Instructor
 @RobertMLee
 Teaching ICS515



James Lyne
 Certified Instructor
 @jameslyne
 Teaching SEC660



Randy Marchany
 Certified Instructor
 @randymarchany
 Teaching SEC440



David R. Miller
 Certified Instructor
 @DRM_CyberDude
 Teaching MGT414



Seth Misenar
 Senior Instructor
 @sethmisenar
 Teaching SEC511



Michael Murr
 Principal Instructor
 @mikemurr
 Teaching SEC560



Stephen Northcutt
 Faculty Fellow
 @StephenNorthcutt
 Teaching MGT512



Keith Palmgren
 Senior Instructor
 @kpalmgren
 Teaching SEC301



Mike Poor
 Senior Instructor
 @Mike_Poor
 Teaching SEC503



Greg Porter
 SANS Instructor
 Teaching HOSTED: Health Care



Clay Risenhoover
 Certified Instructor
 Teaching AUD507



Dave Shackleford
 Senior Instructor
 @daveshackleford
 Teaching SEC567 & SEC579



Bryan Simon
 Certified Instructor
 @BryanOnSecurity
 Teaching MGT305 & SEC401



Stephen Sims
 Senior Instructor
 @Steph3nSims
 Teaching SEC760



Lance Spitzner
 Certified Instructor
 @lspitzner
 Teaching MGT433



John Strand
 Senior Instructor
 @strandjs
 Teaching SEC504



James Tarala
 Senior Instructor
 @isaudit
 Teaching SEC566 & MGT415



Chad Tilbury
 Senior Instructor
 @chadtilbury
 Teaching FOR508



Johannes Ullrich, PhD
 Senior Instructor
 @johullrich
 Teaching DEV522



Jake Williams
 Certified Instructor
 @MalwareJake
 Teaching FOR578



Lenny Zeltser
 Senior Instructor
 @lennyzeltser
 Teaching FOR610

For instructor bios, visit: www.sans.org/event/cyber-defense-initiative-2016/instructors



Five-Day Program
Mon, Dec 12- Fri, Dec 16
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Keith Palmgren



www.giac.org/gisf

► II
**BUNDLE
ONDEMAND**
WITH THIS COURSE

www.sans.org/ondemand



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

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

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

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

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

*"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 Senior Instructor

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

301.1 HANDS ON: Security's Foundation

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

301.2 HANDS ON: Computer Numbers and Cryptography

This course day begins with an explanation of how computers handle numbers using decimal, binary, and hexadecimal numbering systems. It also provides an understanding of how computers encode letters using ASCII (American Standard Code for Information Interchange). We then spend the remainder of the day on cryptography – 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?

301.3 HANDS ON: Networking and Network Security

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 learning how to secure those networks using firewalls, intrusion detection systems, intrusion prevention systems, and others.

301.4 HANDS ON: Host Security

Our fourth day in the classroom is devoted primarily to securing host computers and similar devices. We begin with wireless network security (WiFi and Bluetooth), and mobile device security (i.e., cell phones). We follow that with a brief look at some common attacks. We then move into a discussion of malware and anti-malware technologies. From there we move into several data protection technologies and look at email encryption, secure remote access, secure web access, secure file transfer, and Virtual Private Network technologies. We will then look into the basics of securing endpoint computers via Operating System hardening, patch management, and application security. Of course, we spend some time on the critical topic of backups as well. We end the day with a look at web and browser security, one of the most common attack vectors.

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 "Phishing 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
- ▶ Access a number of websites to better understand password security, encryption, phishing, browser security, etc.

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

-STEVE MECCO, DRAPER

"This course is very valuable as I start my new position in IT security. There is so much to learn and many good ideas."

-AMY SWANSON, TRUVEN HEALTH ANALYTICS

Six-Day Program

Mon, Dec 12- Sat, Dec 17

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

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

46 CPEs

Laptop Required

NEW LAPTOP REQUIREMENTS

Instructor: Bryan Simon



www.giac.org/gsec



www.sans.edu



www.sans.org/cyber-guardian

MEETS DoDD 8140
(8570) REQUIREMENTS



www.sans.org/8140



BUNDLE

ONDEMAND

WITH THIS COURSE

www.sans.org/ondemand



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

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

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

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

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 the FBI, NATO, and the UN in matters of cybersecurity, on two continents. Bryan has specialized expertise in defensive and offensive capabilities. He has received recognition for his work in IT security, and was most recently profiled by McAfee (part of Intel Security) as an IT Hero. Bryan holds 12 GIAC certifications including GISE, 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 SANS Institute Advisory Board, and in his acceptance into the prestigious SANS Cyber Guardian program. Bryan teaches SEC401: Security Essentials Bootcamp Style, SEC501: Advanced Security Essentials — Enterprise Defender, SEC505: Securing Windows and Powershell Automaton, and SEC511: Continuous Monitoring and Security Operations.

@BryanOnSecurity

401.1 HANDS ON: Networking Concepts

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

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

401.2 HANDS ON: Defense In-Depth

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

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

401.3 HANDS ON: Internet Security Technologies

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

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

401.4 HANDS ON: Secure Communications

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

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

401.5 HANDS ON: Windows Security

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

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

401.6 HANDS ON: Unix/Linux Security

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

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

You Will Be Able To

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

“This course is brilliant. It addresses almost every area of IT security.”

-ADNAN SYE, TAFE NSW

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

-JOHN HOUSER, FIRST CITIZENS BANK

Six-Day Program
Mon, Dec 12- Sat, Dec 17
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Paul A. Henry



www.giac.org/gced



www.sans.edu

MEETS DoDD 8140
(8570) REQUIREMENTS



www.sans.org/8140

► II
**BUNDLE
ONDEMAND**
WITH THIS COURSE
www.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.

“Paul is a 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

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

Paul A. Henry SANS Senior Instructor

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

501.1 HANDS ON: Defensive Network Infrastructure

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

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

501.2 HANDS ON: Packet Analysis

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

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

501.3 HANDS ON: Pentest

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

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

501.4 HANDS ON: First Responder

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

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

501.5 HANDS ON: Malware

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

Topics: Malware; Microsoft Malware; External Tools and Analysis

501.6 HANDS ON: Data Loss Prevention

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

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

You Will Be Able To

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

“Best course ever taken in InfoSec or any other subject!”

-J. COFER, DSS

“This has been one of the best courses I have taken, highly job relevant, ground-breaking material!”

-JONATHAN COPELAND, CDSA DAM NECK

“The time has flown by. There is some stuff like cloud-based analysis that is so useful but I would have never thought of using it had Paul not covered it.”

-STUART LONG, BANK OF ENGLAND

Six-Day Program
Mon, Dec 12- Sat, Dec 17
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Mike Poor



www.giac.org/gcia



www.sans.edu



www.sans.org/cyber-guardian

MEETS DoDD 8140
(8570) REQUIREMENTS



www.sans.org/8140

► II
**BUNDLE
ONDEMAND**
WITH THIS COURSE
www.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.

“This course directly covers the necessary knowledge and skill set I use day to day for my job. The added insight is worth the price of the course.” -MICHAEL GARRETT, FEDERAL RESERVE BANK OF SAN FRANCISCO

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

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; 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; Command and Control (C2)

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.

“This course gives rookies and the experienced great tools and techniques to go with the knowledge.”

-BRIAN NICHOLS, COUNTY OF MIDLAND, MI

Six-Day Program

Mon, Dec 12- Sat, Dec 17

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

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

37 CPEs

Laptop Required

Instructor: John Strand


www.giac.org/gcih

www.sans.edu

www.sans.org/cyber-guardian
MEETS DoDD 8140
(8570) REQUIREMENTS
www.sans.org/8140

►►
**BUNDLE
ONDEMAND**
WITH THIS COURSE

www.sans.org/ondemand

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.


www.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

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

-JAID K., U.S. NAVY

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

504.6 HANDS ON: Hacker Tools Workshop

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

Topics: Hands-on Analysis

You Will Be Able To

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

Six-Day Program
Mon, Dec 12- Sat, Dec 17
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jason Fossen



www.giac.org/gcwn



www.sans.edu



www.sans.org/cyber-guardian

MEETS DoDD 8140
(8570) REQUIREMENTS



www.sans.org/8140

► II
**BUNDLE
ONDEMAND**
WITH THIS COURSE

www.sans.org/ondemand



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

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

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

“On day one, I am already seeing ways to use this training at my job.” -NICK PAPA, CHEMICAL BANK

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

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

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

This course is designed for systems engineers, security architects, and the Security Operations (SecOps) team. The focus of the course is on how to automate those Windows-related Critical Security Controls that are the most effective, but also the most difficult to implement, especially in large environments.

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

“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



www.sans.org/simulcast

Who Should Attend

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

Jason Fossen SANS Faculty Fellow

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

505.1 HANDS ON: PowerShell Automation and Security

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

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

505.2 HANDS ON: Continuous Secure Configuration Enforcement

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

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

505.3 HANDS ON: Windows PKI and Smart Cards

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

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

505.4 HANDS ON: Administrative Compromise and Privilege Management

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

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

505.5 HANDS ON: Endpoint Protection and Pre-Forensics

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

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

505.6 HANDS ON: Defensible Networking and Blue Team WMI

Hackers love Windows Management Instrumentation (WMI), and so should we! SecOps automation uses the WMI service a lot, so today's course has PowerShell for WMI. Beyond WMI, there are several other network services or protocols that we cannot live without, but which are targeted by hackers. To move laterally inside the LAN, hackers go after DNS, Remote Desktop Protocol (RDP), SMB, NTLM, Kerberos, SSL and IPv6. We must assume there will be a breach, so we will learn how to harden, eliminate, or encrypt these protocols, and we will do it with little or no user disruption. We can't keep hackers and malware out entirely, but with PKI, IPSec encryption, and proper hardening, RDP can be made safe enough to use, even for administrators.

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

You Will Be Able To

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



www.sans.org/simulcast

Who Should Attend

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

Six-Day Program

Mon, Dec 12- Sat, Dec 17

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

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

46 CPEs

Laptop Required

Instructor: Seth Misenar

**New Extended
Bootcamp Hours to
Enhance Your Skills**



www.giac.org/gmcn



www.sans.edu

**▶ II
BUNDLE
ONDEMAND
WITH THIS COURSE**

www.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!

Seth Misenar SANS Senior Instructor

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

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

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

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

511.2 HANDS ON: Network Security Architecture

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

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

511.3 HANDS ON: Network Security Monitoring

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

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

511.4 HANDS ON: Endpoint Security Architecture

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

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

511.5 HANDS ON: Automation and Continuous Security Monitoring

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

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

Topics: Security Architecture; 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)
- ▶ Utilize tools to support implementation of Continuous Monitoring per NIST guidelines SP800-137
- ▶ Determine requisite monitoring capabilities for a SOC environment
- ▶ Determine capabilities required to support continuous monitoring of key Critical Security Controls

Covers NIST
SP800-137:
Continuous
Monitoring

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

-JOHN HUBBARD, GLAXOSMITHKLINE

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

-TIM HOUSMAN,

GENERAL DYNAMICS IT

Six-Day Program
Mon, Dec 12- Sat, Dec 17
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Eric Conrad



www.giac.org/gwapt



www.sans.edu



www.sans.org/cyber-guardian

► II
BUNDLE
ONDEMAND
WITH THIS COURSE
www.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 countermeasures. 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

542.1 HANDS ON: Introduction and Information Gathering

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

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

542.2 HANDS ON: Configuration, Identity, and Authentication Testing

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

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

542.3 HANDS ON: Injection

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

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

542.4 HANDS ON: JavaScript and XSS

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

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

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

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

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

542.6 HANDS ON: Capture the Flag

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

You Will Be Able To

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

"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, i!2P LLC

Five-Day Program
Mon, Dec 12- Fri, Dec 16
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Bryce Galbraith

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

Who Should Attend

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

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

You Will Learn:

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

What You Will Receive

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

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

**Bryce Galbraith** SANS Principal Instructor

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

Course Day Descriptions

550.1 HANDS ON: Setup and Baseline

Day 1 topics:

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

550.2 HANDS ON: Annoyance

Day 2 topics:

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

542.3 HANDS ON: Attribution

Day 3 topics:

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

550.4 HANDS ON: More Attribution and Attack

Day 4 topics:

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

550.5 HANDS ON: Capture the Flag

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

Author Statement

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

-John Strand

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

"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

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

-STEFANIA IANNELLI,

PALO ALTO NETWORKS

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, Dec 12- Sat, Dec 17

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

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

37 CPEs

Laptop Required

Instructor: Michael Murr



www.giac.org/gpen



www.sans.edu



www.sans.org/cyber-guardian

▶ II
**BUNDLE
ONDEMAND**

WITH THIS COURSE

[www.sans.org/
ondemand](http://www.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 more than **30 detailed hands-on labs** throughout. The course is chock-full of practical, real-world tips from some of the world's best penetration testers to help you do your job safely, efficiently...and masterfully.

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

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

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

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

"This class pulls together all of the tools needed for pen testing in a very clear and logical manner. Excellent and highly valuable training." -BILL HINDS, PMI



Michael Murr SANS Principal Instructor

Michael has been a forensic analyst with Code-X Technologies for over five years, has conducted numerous investigations and computer forensic examinations, and has performed specialized research and development. Michael has taught SANS SEC504 (Hacker Techniques, Exploits, and Incident Handling), SANS FOR508 (Computer Forensics, Investigation, and Response), and SANS FOR610 (Reverse-Engineering Malware); has led SANS@Home courses; and is a member of the GIAC Advisory Board. Currently, Michael is working on an open-source framework for developing digital forensics applications. Michael holds the GCIA, GCFA, and GREM certifications and has a degree in computer science from California State University at Channel Islands. Michael also blogs about digital forensics on his forensic computing blog (www.forensicblog.org). @mikemurr

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; 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
- ▶ 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, Dec 12- Sat, Dec 17
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Kevin Fiscus

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

-DAVE ODOM, BECHTEL

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

-TIMOTHY MCKENZIE, DELL/SECUREWORKS

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

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

Topics addressed in the course include:

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

Who Should Attend

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



Kevin Fiscus SANS Certified Instructor

Kevin Fiscus is the founder of and lead consultant for Cyber Defense Advisors, where he performs security and risk assessments, vulnerability and penetration testing, security program design, policy development and security awareness with a focus on serving the needs of small and mid-sized organizations. Kevin has over 20 years of IT experience and has focused exclusively on information security for the past 12. Kevin currently holds the CISA, GPEN, GREM, GMOB, GCED, GCFA-Gold, GCIA-Gold, GCIH, GAWN, GPPA, GCWN, GCSC-Gold, GSEC, SCSA, RCSE, and SnortCP certifications and is proud to have earned the top information security certification in the industry, the GIAC Security Expert. Kevin has also achieved the distinctive title of SANS Cyber Guardian for both red team and blue team. Kevin has taught many of SANS most popular classes including SEC401, SEC464, SEC503, SEC504, SEC542, SEC560, SEC561, SEC575, FOR508, and MGT414. @kevinbfiscus

561.1 HANDS ON: Security Platform Analysis

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

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

561.2 HANDS ON: Enterprise Security Assessment

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

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

561.3 HANDS ON: Web Application Assessment

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

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

561.4 HANDS ON: Mobile Device and Application Analysis

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

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

561.5 HANDS ON: Advanced Penetration Testing

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

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

561.6 HANDS ON: Capture the Flag Challenge

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

You Will Be Able To

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

Five-Day Program
Mon, Dec 12- Fri, Dec 16
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: James Tarala



www.giac.org/gccc



www.sans.edu

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

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

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

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

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

Topics: Critical Control 1: Inventory of Authorized and Unauthorized Devices

Critical Control 2: Inventory of Authorized and Unauthorized Software

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

Topics: Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers

Critical Control 4: Continuous Vulnerability Assessment and Remediation

Critical Control 5: Controlled Use of Administrative Privileges

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

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

Topics: Critical Control 7: Email and Web Browser Protections

Critical Control 8: Malware Defenses

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

Critical Control 10: Data Recovery Capability (validated manually)

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

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

Topics: Critical Control 12: Boundary Defense

Critical Control 13: Data Protection

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

Critical Control 15: Wireless Device Control

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

Topics: Critical Control 16: Account Monitoring and Control

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

Critical Control 18: Application Software Security

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

Critical Control 20: Penetration Tests and Red Team Exercises (validated manually)

You Will Be Able To

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

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

-JEFF EVENSON, AGSTAR FINANCIAL SERVICES

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

"I'm leaving the class with a great mindset aimed at evaluating the current environment and controls."

SEC566 was good information with a great instructor!" -TOM KOZELSKY, NEXEO SOLUTIONS

"I will be recommending that our whole security team take this course."

-MATTHEW MORRIS, DHS/OBIM

Six-Day Program
Mon, Dec 12- Sat, Dec 17
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Christopher Crowley



www.giac.org/gmob



www.sans.edu

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



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

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

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

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

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

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



www.sans.org/simulcast

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

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 Device Platform Analysis; Wearable Platforms; Mobile Device Lab Analysis Tools; Mobile Device Malware Threats

575.2 HANDS ON: Mobile Platform Access and Application Analysis

With an understanding of the threats, architectural components and desired security methods, we 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: Static Application Analysis; Unlocking, Rooting, Jailbreaking Mobile Devices; Mobile Phone Data Storage and Filesystem Architecture; Network Activity Monitoring

575.3 HANDS ON: Mobile Application Reverse Engineering

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

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

575.4 HANDS ON: Penetration Testing Mobile Devices – PART I

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

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

575.5 HANDS ON: Penetration Testing Mobile Devices – PART 2

Continuing our look at ethical hacking 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: SSL/TLS Attacks; Client Side Injection (CSI) Attacks; Web Framework Attacks; Back-end Application Support Attacks

575.6 HANDS ON: Capture the Flag

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

You Will Be Able To

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

“This is a great course for getting skilled at pen testing mobile applications.”

-BEN BRUCKER, MADISON GURKHA

“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, Dec 12- Sat, Dec 17
9:00am - 5:00pm
36 CPEs
LAPTOP PROVIDED
Instructor: Dave Shackelford

► II
**BUNDLE
ONDEMAND**
WITH THIS COURSE

www.sans.org/ondemand

**“This is the future of
IT and security.**

Knowledge is power!”

-JOE MARSHALL, EXELON



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 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; Different Types of Virtualization; Hypervisor Lockdown Controls for VMware; Microsoft Hyper-V, and Citrix Xen; Virtual Network Design Cases; Virtual Switches and Port Groups; Available Commercial and Open-source Virtual Switches; 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. Days 2-6 do not list any topics.

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, NORTHPROP GRUMMAN

Six-Day Program

Mon, Dec 12- Sat, Dec 17

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

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

46 CPEs

Laptop Required

Instructor: James Lyne



www.giac.org/gxpn



www.sans.edu



www.sans.org/cyber-guardian

► II
**BUNDLE
ONDEMAND**
WITH THIS COURSE
www.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.**

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 the 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 he 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; Custom Network Protocol Manipulation with Ettercap and Custom Filters; Multiple Techniques for Gaining Man-in-the-Middle Network Access; Exploiting OSPF Authentication to Inject Malicious Routing Updates; Using Evilgrade to Attack Software Updates; Overcoming SSL Transport Encryption Security with Sslstrip; Remote Cisco Router Configuration File Retrieval; IPv6 for Penetration Testers

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

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

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

660.3 HANDS ON: Python, Scapy, and Fuzzing

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

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

660.4 HANDS ON: Exploiting Linux for Penetration Testers

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

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

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

-MICHAEL HORKEN, ROCKWELL AUTOMATION

"This material puts me at that next level."

-ADAM LOGUE, SPECTRUM HEALTH

Six-Day Program

Mon, Dec 12- Sat, Dec 17

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.

“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 KITACHIT, 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: www.sans.org/sec760/quiz

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



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 a master's of science degree in information assurance from Norwich University. 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 DarunGrim4; 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 7/8 Kernels and Drivers; 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

FOR408

Six-Day Program
Mon, Dec 12- Sat, Dec 17
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Ovie Carroll



www.giac.org/gcfe



www.sans.edu

► II
BUNDLE
ONDEMAND
WITH THIS COURSE

www.sans.org/ondemand



Windows Forensic Analysis



www.sans.org/simulcast

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.

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

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

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

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

Who Should Attend

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

Ovie Carroll SANS Certified Instructor

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

408.1 HANDS ON: Windows Digital Forensics and Advanced Data Triage

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

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

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

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

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

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

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

Topics: Shell Item Forensics; USB and Bring Your Own Device (BYOD); 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; Examination of Browser Artifacts; Tools Used

408.6 HANDS ON: Windows Forensic Challenge

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

Topics: Digital Forensic Case; Windows 7 Forensic Challenge

You Will Be Able To

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

"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

Six-Day Program
Mon, Dec 12- Sat, Dec 17
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Chad Tilbury



www.giac.org/gcfa



www.sans.edu



www.sans.org/cyber-guardian

MEETS DoDD 8140
(8570) REQUIREMENTS



www.sans.org/8140

▶▶
**BUNDLE
ONDEMAND**
WITH THIS COURSE

www.sans.org/ondemand

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

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.

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.

“So far this is the best course I've taken in 20 years.” -MAURICIO BELLIDO JR., USG

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



Chad Tilbury SANS Senior Instructor

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



www.sans.org/simulcast

Who Should Attend

- ▶ System administrators
- ▶ 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

508.1 HANDS ON: Advanced Incident Response and Digital Forensics

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 hundreds of systems.

Topics: Real Incident Response Tactics; Threat and Adversary Intelligence; 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; Memory Analysis Timeline Creation

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

In digital forensics, many tools simply require a few mouse clicks to automatically recover data. However, this “push button” mentality has led to many inaccurate results in the past few years. It is also very difficult to identify a skilled attacker solely using antiquated and slow commercial toolsets. This section will free you from relying on “push button” forensic techniques by showing you how the engines of digital forensic tools really work. To understand how to carve out data, it is best to understand how to do it by hand and then show how automated tools should be able to recover the same data.

Topics: Advanced “Evidence of Execution” Artifacts; Windows 7/8 Server 2008/2012 Shadow Volume Copy Analysis; Deep Dive Malware and Anti-Forensics Detection; File-Based Data Carving; NTFS Filesystem Analysis; Anti-Forensic Detection Methodologies

508.5 HANDS ON: Threat 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: APT Intrusion 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, Dec 12- Sat, Dec 17
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Sarah Edwards

► II
**BUNDLE
ONDEMAND**
WITH THIS COURSE
www.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

“Best of any course I’ve ever taken. I love the idea of being able to bring the material home to review.”

-ERIC KOEBELEN, INCIDENT RESPONSE US



Sarah Edwards SANS Certified Instructor

A self-described Mac nerd, Sarah Edwards is a forensic analyst, author, speaker, and both author and instructor of SANS FOR518: Mac Forensic Analysis. She has been a devoted user of Apple devices for many years and has worked specifically in Mac forensics since 2004, carving out a niche for herself when this area of forensics was still new. Although Sarah appreciates digital forensics in all platforms, she has a passion for working within Apple environments and is well known for her work with cutting-edge Mac OS X and iOS, and for her forensic file system expertise. Sarah has more than 12 years of experience in digital forensics, and her passion for teaching is fueled by the ever-increasing presence of Mac devices in today’s digital forensic investigations. Sarah has worked with federal law enforcement agencies on a variety of high-profile investigations in such areas as computer intrusions, criminal cases, counter-intelligence, counter-narcotics, and counter-terrorism. Her research and analytical interests include Mac forensics, mobile device forensics, digital profiling, and malware reverse engineering. @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 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, Dec 12- Sat, Dec 17
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Philip Hagen



www.giac.org/gnfa



www.sans.edu

► II
**BUNDLE
OnDemand**
WITH THIS COURSE

www.sans.org/ondemand



The network IS the new investigative baseline.

There is simply no incident response action that doesn't include a communications component any more – whether you conduct threat hunting operations, traditional casework, or post-mortem incident response, understanding the nature of how systems have communicated is critical to success. Even in disk- and memory-based incident response work, artifacts that clarify a subject's network actions can be keystone findings you can't afford to miss. Whether you are handling a data breaches, intrusion scenario, employee misuse, or threat hunting (proactively trawling your organization's data stores for evidence of an undiscovered compromise), the need to effectively examine and interpret network artifacts is here to stay.

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

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

Whether you are a consultant responding to a client's site, a law enforcement professional assisting victims of 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.

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. In the same vein, presenting concise findings from extremely large data sources is an important skill. A network forensicator should be able to aggregate and visually present findings, especially when faced with a years-long compromise incident. Expressing findings supported with visualizations can provide a much clearer picture than words alone.

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 Eventing; 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

“The labs — practice towards excellence — and the instructor's real-world stories provide valuable experiences and insight.”

-NATE DEWITT, eBAY, INC.

NEW!

Five-Day Program
 Mon, Dec 12- Fri, Dec 16
 9:00am - 5:00pm
 30 CPEs
 Laptop Required
 Instructor: Jake Williams

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

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

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

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

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

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

Who Should Attend

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

"I absolutely loved this class! The instructor provided a great framework for CTI that I will use to be more effective."

-NATE DeWITT, eBay, Inc.



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

THERE IS NO TEACHER BUT THE ENEMY!

578.1 HANDS ON: Cyber Threat Intelligence

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

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

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

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

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

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

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

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

578.4 HANDS ON: Operational Threat Intelligence: Sharing Intelligence

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

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

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

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

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

“Jake Williams is very good. I enjoyed all of the real-life stories/situations and awareness.”

-RIAZ AHMED, ITT

Six-Day Program
Mon, Dec 12- Sat, Dec 17
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Lenny Zeltser



www.giac.org/grem



www.sans.edu

► II
BUNDLE
ONDEMAND
WITH THIS COURSE

www.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.

"This material is something you can use to build or enhance your company's playbook in terms of incident response and detection" -CHRIS BAILEY, CALIFORNIA LOTTERY

This 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.



www.sans.org/simulcast

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 a master's degree in business administration from MIT Sloan and a computer science degree from the University of Pennsylvania. @lennyzeltser

610.1 HANDS ON: Malware Analysis Fundamentals

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

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

610.2 HANDS ON: Malicious Code Analysis

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

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

610.3 HANDS ON: In-Depth Malware Analysis

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

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

610.4 HANDS ON: Self-Defending Malware

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

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

610.5 HANDS ON: Malicious Documents and Memory Forensics

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

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

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, Dec 12- Sat, Dec 17

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

8:00am - 7:00pm (Days 2-5)

8:00am - 5:00pm (Day 6)

46 CPEs

Laptop NOT Needed

Instructor: David R. Miller


www.giac.org/gisp

 MEETS DoDD 8140
(8570) REQUIREMENTS

www.sans.org/8140
**► II
BUNDLE
ONDEMAND**
WITH THIS COURSE

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

“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.

www.sans.org/cissp

“The instructor is truly an expert! I feel very honored to be in this class. He's explained some topics better than several books I've read.” -FREDA LURDY, RAYTHEON

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® eight domains
- ▶ Security professionals and managers looking for practical ways the eight 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

David R. Miller SANS Certified Instructor

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

414.1 Introduction; Security and Risk Management

On the first day of training for the CISSP® exam, MGT414 introduces the specific requirements needed to obtain certification. The 2016 exam update will be discussed in detail. We will cover the general security principles needed to understand the eight domains of knowledge, with specific examples for each domain. The first of the eight domains, Security and Risk Management, is discussed using real-world scenarios to illustrate the critical points.

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

"Dave is a great instructor for this course. He has a good teaching style and he knows the test."

-TOM YERGEAU, THOMSON REUTERS

Five-Day Program

Mon, Dec 12- Fri, Dec 16

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

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

33 CPEs

Laptop Recommended

Instructor: Stephen Northcutt


www.giac.org/gslc

www.sans.edu
MEETS DoDD 8140
(8570) REQUIREMENTS
www.sans.org/8140

► II
BUNDLE
ONDEMAND
WITH THIS COURSE

www.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.

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!

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

**Stephen Northcutt** SANS Faculty Fellow

Stephen Northcutt founded the GIAC certification and served as the founding president of the SANS Technology Institute, an accredited graduate school focused on cybersecurity. Stephen is author/coauthor of *Incident Handling Step-by-Step*, *Intrusion Signatures and Analysis*, *Inside Network Perimeter Security* 2nd Edition, *IT Ethics Handbook*, and *Network Intrusion Detection* 3rd Edition. He was the original author of the Shadow Intrusion Detection system before accepting the position of chief for information warfare at the Ballistic Missile Defense Organization. Stephen is a graduate of Mary Washington College. Before entering the field of computer security, he worked as a Navy helicopter search and rescue crewman, white water raft guide, chef, martial arts instructor, cartographer, and network designer. Since 2007 Stephen has conducted over 40 in-depth interviews with leaders in the security industry, from CEOs of security product companies to the most well-known practitioners, in order to research the competencies required to be a successful leader in the security field. He maintains the SANS Leadership Laboratory, where research on these competencies is posted, as well as SANS Security Musings. He leads the MGT512 Alumni Forum, where hundreds of security managers post questions. He is the lead author for MGT512: SANS Security Leadership Essentials for Managers, a prep course for the GSLC certification that meets all levels of requirements for DoD Security Managers per DoDD 8140. He also is the lead author/instructor for MGT514: IT Security Strategic Planning, Policy, and Leadership. Stephen blogs at the SANS Security Laboratory and is on the NewsBites and SANS Analyst teams. He has been involved in a number of security startups including SourceFire, Tenable, Savant Protection and Zimperium, and currently serves as director of academic advising for SANS.EDU. @StephenNorthcutt

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

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

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

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

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

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

512.3 Secure Communications

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

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

512.4 The Value of Information

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

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

512.5 Management Practicum

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

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

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

You Will Be Able To

- ▶ 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 MGT512, 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.

"Perfect fit for my management role. Good balance of tech and management topics."

-MICHAEL MADDOX, CITY OF AUSTIN

"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.

Five-Day Program
Mon, Dec 12- Fri, Dec 16
9:00am - 5:00pm
30 CPEs
Laptop NOT Needed
Instructor: Frank Kim



www.sans.edu

► II
BUNDLE
ONDEMAND
WITH THIS COURSE
www.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 responsibility for delivering innovative security solutions to meet the unique needs of the nation's largest not-for-profit health plan and integrated health care provider with annual revenue of \$55 billion, 9.5 million members, and 175,000 employees. In recognition of his work, Frank was a two-time recipient of the CIO Achievement Award for business-enabling thought leadership. Frank holds degrees from the University of California at Berkeley and is the author of popular SANS courseware on strategic planning, leadership, and application security. @fykim

514.1 Strategic Planning Foundations

Creating 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

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

-ALEXIS BROWNINGS, CERT-UK

“This is a great foundational course as we realize the importance of bringing a business perspective to security.”

-NAIROBI KIM, WELLS FARGO

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

-DJ, ZOETIS

Six-Day Program
Mon, Dec 12- Sat, Dec 17

9:00am - 5:00pm

36 CPEs

Laptop Required

Instructor: Johannes Ullrich, Ph.D.



www.giac.org/gweb



www.sans.edu

► II
BUNDLE
OnDemand
WITH THIS COURSE
www.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.

Who Should Attend

- Application developers
- Application security analysts or managers
- Application architects
- Penetration testers who are interested in learning about defensive strategies
- Security professionals who are interested in learning about web application security
- Auditors who need to understand defensive mechanisms in web applications
- Employees of PCI compliant organizations who need to be trained to comply with PCI requirements

Johannes Ullrich, PhD SANS Senior Instructor

As Dean of Research for the SANS Technology Institute, Johannes is currently responsible for the SANS Internet Storm Center (ISC) and the GIAC Gold program. In 2000, he founded DShield.org, which is now the data collection engine behind the ISC. His work with the ISC has been widely recognized, and in 2004, Network World named him one of the 50 most powerful people in the networking industry. Prior to working for SANS, Johannes worked as a lead support engineer for a web development company and as a research physicist. Johannes holds a PhD in physics from SUNY Albany and is based in Jacksonville, Florida. His daily podcast summarizes current security news in a concise format. @johullrich

522.1 HANDS ON: Web Basics and Authentication Security

We begin day one with an overview of recent web application attack and security trends, then follow up by examining the essential technologies that are at play in web applications. You cannot win the battle if you do not understand what you are trying to defend. We arm you with the right information so you can understand how web applications work and the security concepts related to them.

Topics: HTTP Basics; Overview of Web Technologies; Web Application Architecture; Recent Attack Trends; Authentication Vulnerabilities and Defense; Authorization Vulnerabilities and Defense

522.2 HANDS ON: Web Application Common Vulnerabilities and Mitigations

Since the Internet does not guarantee the secrecy of information being transferred, encryption is commonly used to protect the integrity and secrecy of information on the web. This course day covers the security of data in transit or on disk and how encryption can help with securing that information in the context of web application security.

Topics: SSL Vulnerabilities and Testing; Proper Encryption Use in Web Application; Session Vulnerabilities and Testing; Cross-site Request Forgery; Business Logic Flaws; Concurrency; Input-related Flaws and Related Defenses; SQL Injection Vulnerabilities, Testing, and Defense

522.3 HANDS ON: Proactive Defense and Operation Security

Day three begins with a detailed discussion on cross-site scripting and related mitigation and testing strategies, as well as HTTP response splitting. The code in an application may be totally locked down, but if the server setting is insecure, the server running the application can be easily compromised. Locking down the web environment is essential, so we cover this basic concept of defending the platform and host. To enable any detection of intrusion, logging and error handling must be done correctly. We will discuss the correct approach to handling incidents and logs, then dive even further to cover the intrusion detection aspect of web application security. In the afternoon we turn our focus to the proactive defense mechanism so that we are ahead of the bad guys in the game of hack and defend.

Topics: Cross-site Scripting Vulnerability and Defenses; Web Environment Configuration Security; Intrusion Detection in Web Applications; Incident Handling; Honeytoken

522.4 HANDS ON: AJAX and Web Services Security

Day four is dedicated to the security of asynchronous JavaScript and XML (AJAX) and web services, which are currently the most active areas in web application development. Security issues continue to arise as organizations dive head first into insecurely implementing new web technologies without first understanding them. We will cover security issues, mitigation strategies, and general best practices for implementing AJAX and web services. We will also examine real-world attacks and trends to give you a better understanding of exactly what you are protecting against. Discussion focuses on the web services in the morning and AJAX technologies in the afternoon.

Topics: Web Services Overview; Security in Parsing of XML; XML Security; AJAX Technologies Overview; AJAX Attack Trends and Common Attacks; AJAX Defense

522.5 HANDS ON: Cutting-Edge Web Security

Day five focuses on cutting-edge web application technologies and current research areas. Topics such as clickjacking and DNS rebinding are covered. These vulnerabilities are difficult to defend and multiple defense strategies are needed for their defense to be successful. Another topic of discussion is the new generation of single-sign-on solutions such as OpenID. We cover the implications of using these authentication systems and the common "gotchas" to avoid. With the Web2.0 adoption, the use of Java applet, Flash, ActiveX, and Silverlight are on the increase. The security strategies of defending these technologies are discussed so that these client-side technologies can be locked down properly.

Topics: Clickjacking; DNS Rebinding; Flash Security; Java Applet Security; Single-Sign-On Solution and Security; IPv6 Impact on Web Security

522.6 HANDS ON: Capture and Defend the Flag Exercise

Day six starts with an introduction to the secure software development life cycle and how to apply it to web development. But the focus is a large lab that will tie together the lessons learned during the week and reinforce them with hands-on applications. Students will be provided with a virtual machine to implement a complete database-driven dynamic website. In addition, they will use a custom tool to enumerate security vulnerabilities and simulate a vulnerability assessment of the website. Students will then have to decide which vulnerabilities are real and which are false positives, and then mitigate the vulnerabilities. The scanner will score the student as vulnerabilities are eliminated or checked off as false positives. Advanced students will be able to extend this exercise and find vulnerabilities not presented by the scanner. Students will learn through these hands-on exercises how to secure the web application, starting with the operating system, the web server; finding configuration problems in the application language setup, and finding and fixing coding problems in the site.

Topics: Mitigation of Server Configuration Errors; Discovering and Mitigating Coding Problems; Testing Business Logic Issues and Fixing Problems; Web Services Testing and Security Problem Mitigation

You Will Be Able To

- ▶ Understand the major risks and common vulnerabilities related to web applications through real-world examples
- ▶ Mitigate common security vulnerabilities in web applications using proper coding techniques, software components, configurations, and defensive architecture
- ▶ Understand the best practices in various domains of web application security such as authentication, access control, and input validation
- ▶ Fulfill the training requirement as stated in PCI DSS 6.5
- ▶ Deploy and consume web services (SOAP and REST) in a more secure fashion
- ▶ Proactively deploy cutting-edge defensive mechanisms such as the defensive HTTP response headers and Content Security Policy to improve the security of web applications
- ▶ Strategically roll out a web application security program in a large environment
- ▶ Incorporate advanced web technologies such as HTML5 and AJAX cross-domain requests into applications in a safe and secure manner
- ▶ Develop strategies to assess the security posture of multiple web applications

NEW!

Five-Day Program
Mon, Dec 12- Fri, Dec 16
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Tim Conway

ICS456: Essentials for NERC Critical Infrastructure

Protection is a five-day course that empowers students with knowledge of the “what” and the “how” of the Version 5/6 standards. The course addresses the role of the Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC), and the regional entities. It provides multiple approaches to identifying and categorizing BES Cyber Systems and helps asset owners determine the specific implementations applicable to the requirements. Additionally, the course covers implementation strategies for the Version 5/6 standards with a balanced practitioner approach to both cybersecurity benefits and regulatory compliance. This course also contains 24 hands-on labs ranging from securing workstations to digital forensics and lock picking.

Who Should Attend

- ▶ IT and OT (ICS) cybersecurity
- ▶ Field support personnel
- ▶ Security operations personnel
- ▶ Incident response personnel
- ▶ Compliance staff
- ▶ Team leaders
- ▶ Governance officials
- ▶ Vendors/Integrators
- ▶ Auditors

Author Statement

“The **SANS ICS456: Essentials for NERC Critical Infrastructure Protection** course was developed by SANS ICS team members with extensive electric industry experience including former Registered Entity Primary Contacts, a former NERC officer, and a Co-Chair of the NERC CIP Interpretation Drafting Team. Together the authors bring real-world, practitioner experience gained from developing and maintaining NERC CIP and NERC 693 compliance programs and actively participating in the standards development process.”

“Best CIP training I’ve ever had in all my years of the CIP program.”

-MICHAEL VEILLON, CLECO



Tim Conway SANS Instructor

Tim is the Technical Director of ICS and SCADA programs at SANS. He is responsible for developing, reviewing, and implementing technical components of the SANS ICS and SCADA product offerings. He previously served as the Director of CIP Compliance and Operations Technology at Northern Indiana Public Service Company (NIPSCO), where he was responsible for Operations Technology, NERC CIP Compliance, and the NERC training environments for the operations departments within NIPSCO Electric. Tim was also an EMS Computer Systems Engineer at NIPSCO for eight years, with responsibility over the control system servers and the supporting network infrastructure. He was the chair of the RFC CIPC, and is the current chair of the NERC CIP Interpretation Drafting Team, member of the NESCO advisory board, chair of the NERC CIPC GridEx Working Group, and chair of the NBISE Smart Grid Cyber Security panel.

456.1 HANDS ON: Asset Identification and Governance

A transition is under way from NERC CIP programs that are well defined and understood to a new CIP paradigm that expands its scope into additional environments and adds significantly more complexity. In day one, students will develop an understanding of the electric sector regulatory structure and history as well as an appreciation for how the CIP Standards fit into the overall framework of the reliability standards. Key NERC terms and definitions related to NERC CIP are reviewed using realistic concepts and examples that prepare students to better understand their meaning. We will explore multiple approaches to BES Cyber Asset identification and learn the critical role of strong management and governance controls. The day will examine a series of architectures, strategies, and difficult compliance questions in a way that highlights the reliability and cybersecurity strengths of particular approaches. Unique labs will include a scenario-based competition that helps bring the concepts to life and highlights the important role we play in defending “the grid.”

Topics: Regulatory History and Overview; NERC Functional Model; NERC Reliability Standards; CIP History; Terms and Definitions; CIP-002: BES Cyber System Categorization; CIP-003: Security Management Controls

456.2 HANDS ON: Access Control and Monitoring

Strong physical and cyber access controls are at the heart of any good cybersecurity program. During day two, we move beyond the “what” of CIP compliance to understanding the “why” and the “how.” Firewalls, proxies, gateways, IDS, and more – learn where and when they help and learn practical implementations to consider and designs to avoid. Physical protections include more than fences and you’ll learn about the strengths and weaknesses of common physical controls and monitoring schemes. Labs will reinforce the learnings throughout the day and will introduce architecture review and analysis, firewall rules, IDS rules, compliance evidence demonstration, and physical security control reviews.

Topics: CIP-005: Electronic Security Perimeter(s); Interactive Remote Access; External Routable Communication and Electronic Access Points; CIP-006: Physical Security of BES Cyber Systems; Physical Security Plan; Visitor Control Programs; PACS Maintenance and Testing; CIP-014: Physical Security

456.3 HANDS ON: System Management

CIP-007 has consistently been one of the most violated Standards going back to CIP version 1. With the CIP Standards moving to a systematic approach with varying requirement applicability based on system impact rating, the industry now has new ways to design and architect system management approaches. Throughout day three, students will dive into CIP-007. We’ll examine various Systems Security Management requirements with a focus on implementation examples and the associated compliance challenges. This day will also cover the CIP-010 requirements for configuration change management and vulnerability assessments that ensure systems are in a known state and under effective change control. We’ll move through a series of labs that reinforce the topics covered from the perspective of the CIP practitioner responsible for implementation and testing.

Topics: CIP-007: System Management; Physical and Logical Ports; Patch Management; Malicious Code Prevention; Account Management; CIP-010: Configuration Change Management and Vulnerability Assessments; Change Management Program; Baseline Configuration Methodology; Change Management Alerting/Prevention

456.4 HANDS ON: Information Protection and Response

Education is key to every organization’s success with NERC CIP, and the students in ICS456 will be knowledgeable advocates for CIP when they return to their place of work. Regardless of their role, students can be a valued resource to their organization’s CIP-004 training program, the CIP-011 information protection program. Students will be ready with resources for building and running strong awareness programs that reinforce the need for information protection and cybersecurity training. In day four, we’ll examine CIP-008 and CIP-009 covering identification, classification communication of incidents as well as the various roles and responsibilities needed in an incident response or a disaster recovery event. Labs in day four will introduce tools for ensuring file integrity and sanitization of files to be distributed, how to best utilize and communicate with the E-ISAC, and how to preserve incident data for future analysis.

Topics: CIP-004: Personnel & Training; Security Awareness Program; CIP Training Program; PRA Evaluation Process; CIP-011: Information Protection; Information Protection Program; Data Sanitization; CIP-008: Incident Reporting and Response Planning; Incident Response Plan/Testing; Reporting Requirements; CIP-009: Recovery Plans for BES Cyber Systems; Recovery Plans; System Backup

456.5 CIP Process

On the final day students will learn the key components for running an effective CIP Compliance program. We will review the NERC processes for standards development, violation penalty determination, requests for interpretation, and recent changes stemming from the Reliability Assurance Initiative. Additionally, we’ll identify recurring and audit-related processes that keep a CIP compliance program on track: culture of compliance, annual assessments, gap analysis, TFEs, and self-reporting. We’ll also look at the challenge of preparing for NERC audits and provide tips to be prepared to demonstrate the awesome work your team is doing. Finally, we’ll look at some real-life CIP violations and discuss what happened and the lessons we can take away. At the end of day five, students will have a strong call-to-action to participate in the on-going development of CIP within their organization and in the industry overall as well as a sense that CIP is doable! Labs in day five will cover DOE C2M2, audit tools, and an audit-focused take on the “blue team – red team” exercise.

Topics: CIP Processes for Maintaining Compliance; Preparing for an Audit; Audit Follow-up; CIP Industry Activities; Standards Process; CIP of the Future

Five-Day Program
Mon, Dec 12- Fri, Dec 16
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Robert M. Lee

► II
BUNDLE
ONDEMAND
WITH THIS COURSE

www.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.

What You Will Receive

- 64Gb USB packed with ICS lab data such as packet captures and memory images
 - Protocol samples of OPC, ModbusTCP, DNP3, BACnet, ISO-TSAP, and more
 - System files from infected DCS and HMI systems
- A fully functioning CYBATIworks Mini-kit that students will keep following the class
 - A Raspberry PI that functions as a PLC
 - Physical components and attachments for I/O
 - Commercial control system demonstration software from Rex Controls
 - Commercial control system demonstration software from PeakHMI
 - Commercial control system demonstration software from CyberLens
- Samples of Stuxnet, Havex, and BlackEnergy2 in a safe Virtual Machine environment
- CYBATI Virtual Machine tailored for continued ICS education
- REMnux Virtual Machine for malware analysis
- Security Onion Virtual Machine for monitoring the network and detecting threats

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

**"Awesome!! This course
was my sixth SANS
course, and Robert M.
Lee demonstrated and
reiterated the fact that
SANS has the world's best
instructors."**

-SRINATH KANNAN, ACCENTURE

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, and he established 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

515.1 HANDS ON: Threat Intelligence

Industrial control system (ICS) security professionals must be able to leverage internal and external threat intelligence to critically analyze threats, extract indicators of compromise (IOCs), and guide security teams to find threats in the environment. Today you will learn how threat intelligence is generated, how to critically analyze reports, and the basic tenets of active defense functions. Students will become better analysts and critical thinkers by learning skills useful in day-to-day operations, regardless of their jobs and roles. This day features four hands-on labs that include building a Programmable Logic Controller (PLC), identifying information available about assets online through Shodan, completing an analysis of competing hypotheses, and ingesting threat intelligence reports to guide their practices over the rest of the labs in the course.

Topics: Case Study: Havex; Introduction to ICS Active Defense and Incident Response; Intelligence Life Cycle and Threat Intelligence; ICS Information Attack Surface; External ICS Threat Intelligence; Internal ICS Threat Intelligence; Sharing and Consuming ICS Threat Intelligence

515.2 HANDS ON: Asset Identification and Network Security Monitoring

Understanding the networked environment is the only way to fully defend it: you cannot defend what you do not know. This course section will teach students to use tools such as Wireshark, TCPDump, SGUIL, ELSA, CyberLens, Bro, NetworkMiner, and Snort to map their ICS network, collect data, detect threats, and analyze threats to drive incident response procedures. During this section, students will be introduced to the lab network and an advanced persistent threat (APT) that is present on it. Drawing on threat intelligence from the previous course section, students will have to discover, identify, and analyze the threat using their new active defense skills to guide incident responders to the affected Human Machine Interface (HMI).

Topics: Case Study: BlackEnergy2; ICS Asset and Network Visibility; Identifying and Reducing the Threat Landscape; ICS Network Security Monitoring — Collection; ICS Network Security Monitoring — Detection; ICS Network Security Monitoring — Analysis

515.3 HANDS ON: Incident Response

The ability to prepare for and perform ICS incident response is vital to the safety and reliability of control systems. ICS incident response is a core concept in an ICS active defense and requires that analysts safely acquire digital evidence while scoping the environment for threats and their impact on operations. ICS incident response is a young field with many challenges, but students in this section will learn effective tactics and tools to collect and preserve forensic-quality data. Students will then use this data to perform timely forensic analysis and create IOCs. In the previous section's labs, APT malware was identified in the network. In this section, the labs will focus on identifying which system is impacted and gathering a sample of the threat that can be analyzed.

Topics: Case Study: Stuxnet; Incident Response and Digital Forensics Overview; Preparing an ICS Incident Response Team; Evidence Acquisition; Sources of Forensic Data in ICS Networks; Time-Critical Analysis; Maintaining and Restoring Operations

515.4 HANDS ON: Threat and Environment Manipulation

Understanding the threat is key to discovering its capabilities and its potential to affect the ICS. The information extracted from threats through processes such as malware analysis is also critical to being able to make the necessary changes to the environment to reduce the effectiveness of the threat. The information obtained is vital to an ICS active defense, which requires internal data collection to create and share threat intelligence. In this section, students will learn how to analyze initial attack vectors such as spearphishing emails, perform timely malware analysis techniques, analyze memory images, and create Indicators of Compromise in YARA. The previous section's labs identified the infected HMI and gathered a sample of the APT malware. In this section's labs, students will analyze the malware, extract information, and develop YARA rules to complete the active defense model introduced in the class and maintain operations.

Topics: Case Study: German Steelworks; ICS Threat and Environment Manipulation Goals and Considerations; Establishing a Safe Working Environment; Analyzing Acquired Evidence; Memory Forensics; Malware Analysis Methodologies; Case Study: BlackEnergy2 Automated Analysis; Indicators of Compromise; Environment Manipulation

515.5 HANDS ON: Active Defense and Incident Response Challenge

This section focuses on reinforcing the strategy, methodologies, skillsets, and tools introduced in the first four sections of the course. This entirely hands-on section will present students with two different scenarios. The first involves data collected from an intrusion into SANS Cyber City. The second involves data collected from a Distributed Control System (DCS) infected with malware. This section will truly challenge students to utilize their ICS active defense and incident response skills and test themselves.

Topics:

Scenario One: Identify the Assets and Map the ICS Networks; Perform ICS Network Security Monitoring to Identify the Abnormalities; Execute ICS Incident Response Procedures Into the SANS Cyber City Data Files; Analyze the Malicious Capability and Determine if the Threat is an Insider Threat or a Targeted External Threat

Scenario Two: Identify the Software and Information Present on the DCS; Leverage ICS Active Defense Concepts to Identify the Real-World Malware; Determine the Impact on Operations and Remediation Needs

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 CYBATworks Kit and keep it after the class ends
- ▶ Gain hands-on experience with samples of Havex, BlackEnergy2, and Stuxnet through engaging labs while de-constructing 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

Six-Day Program
Mon, Dec 12- Sat, Dec 17
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Clay Risenhoover



www.giac.org/gсна



www.sans.edu

MEETS DoDD 8140
(8570) REQUIREMENTS



www.sans.org/8140

► II
**BUNDLE
ONDEMAND**
WITH THIS COURSE

www.sans.org/ondemand

"I can't wait to put
everything I learned
into practice!
What a great course!"

-T. BOZEMAN EHRENFRIED,
STINGER GHAFARIAN



Clay Risenhoover *SANS Certified Instructor*

Clay is the president of Risenhoover Consulting, Inc., an IT management consulting firm based in Durant, Oklahoma. Founded in 2003, RCI provides IT audit and IT management consulting services to clients in multiple sectors. Clay's past experience includes positions in software development, technical training, LAN and WAN operations, and IT management in both the private and public sector. He has a master's degree in computer science and holds a number of technical and security certifications, including GPEN, GSNA, CISA, CISM, GWEB and CISSP.

One of the most significant obstacles facing many auditors today is how exactly to go about auditing the security of an enterprise. What systems really matter? How should the firewall and routers be configured? What settings should be checked on the various systems under scrutiny? Is there a set of processes that can be put into place to allow an auditor to focus on the business processes rather than the security settings? How do we turn this into a continuous monitoring process? All of these questions and more will be answered by the material covered in this course.

This course is specifically organized to provide a risk-driven method for tackling the enormous task of designing an enterprise security validation program. After covering a variety of high-level audit issues and general audit best practices, the students will have the opportunity to dive deep into the technical how-to for determining the key controls that can be used to provide a level of assurance to an organization. Tips on how to repeatedly verify these controls and techniques for automatic compliance validation are taken from real-world examples.

One of the struggles that IT auditors face today is helping management understand the relationship between the technical controls and the risks to the business that these controls address. In this course these threats and vulnerabilities are explained based on validated information from real-world situations. The instructor will take the time to explain how this can be used to raise the awareness of management and others within the organization to build an understanding of why these controls specifically and auditing in general are important. From these threats and vulnerabilities, we will explain how to build the ongoing compliance monitoring systems and automatically validate defenses through instrumentation and automation of audit checklists.

You'll be able to use what you learn immediately. Five of the six days in the course will either produce or provide you directly with a general checklist that can be customized for your audit practice. Each of these days includes hands-on exercises with a variety of tools discussed during the lecture sections so that you will leave knowing how to verify each and every control described in the class. Each of the five hands-on days gives you the chance to perform a thorough technical audit of the technology being considered by applying the checklists provided in class to sample audit problems in a virtualized environment. Students are invited to bring a Windows XP Professional or higher laptop for use during class. Macintosh computers running OS X may also be used with VMWare Fusion.

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

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

507.1 Effective Auditing, Risk Assessment, and Reporting

After laying the foundation for the role and function of an auditor in the information security field, this day's material will give you two extremely useful risk assessment methods that are particularly effective for measuring the security of enterprise systems, identifying control gaps and risks, and gaining the knowledge to be able to recommend additional compensating controls to address the risk. Nearly a third of the day is spent covering important audit considerations and questions dealing with virtualization and cloud computing.

Topics: Auditor's Role in Relation to Policy Creation, Policy Conformance, and Incident Handling; Basic Auditing and Assessing Strategies; Risk Assessment; The Six-Step Audit Process; Virtualization and Cloud Computing

507.2 Effective Network and Perimeter Auditing/Monitoring

On this day we will build from the ground up dealing with security controls, proper deployment, and effective auditing continuous monitoring of configuration from Layer 2 all the way up the stack. Students will learn how to identify insecurely configured VLANs, determine perimeter firewall requirements, examine enterprise routers, and much more.

Topics: Secure Layer 2 Configurations; Router and Switch Configuration Security; Firewall Auditing, Validation, and Monitoring; Wireless; Network Population Monitoring; Vulnerability Scanning

507.3 Web Application Auditing

Web applications have consistently been rated for the past several years as one of the top five vulnerabilities that enterprises face. Unlike the other top vulnerabilities, however, enterprises continue to accept this risk, since most modern corporations need an effective web presence to do business today. One of the most important lessons that we are learning as an industry is that installing an application firewall is not enough!

Topics: Identifying Controls Against Information Gathering Attacks; Processing Controls to Prevent Hidden Information Disclosures; Control Validation of the User Sign-on Process; Examining Controls Against User Name Harvesting; Validating Protections Against Password Harvesting; Best Practices for OS and Web Server Configuration; How to Verify Session Tracking and Management Controls; Identification of Controls to Handle Unexpected User Input; Server-side Techniques for Protecting Your Customers and Their Sensitive Data

507.4 Advanced Windows Auditing and Monitoring

Microsoft's business-class system makes up a large part of the typical IT infrastructure. Quite often, these systems are also the most difficult to effectively secure and control because of the enormous number of controls and settings within the operating system. This course day will provide you with the techniques and tools to build an effective long-term audit program for your Microsoft Windows environment. More importantly, during the course a continuous monitoring and reporting system is built out, allowing you to easily and effectively scale the testing discussed within your enterprise when you return home.

Topics: Progressive Construction of a Comprehensive Audit Program; Automating the Audit Process; Windows Security Tips and Tricks; Maintaining a Secure Enterprise

507.5 Advanced Unix Auditing and Monitoring

Students will gain a deeper understanding of the inner workings and fundamentals of the Unix operating system as applied to the major Unix environments in use in business today. Students will have the opportunity to explore, assess and audit Unix systems hands-on. Lectures describe the different audit controls that are available on standard Unix systems, as well as access controls and security models.

Topics: Auditing to Create a Secure Configuration; Auditing to Maintain a Secure Configuration; Auditing to Determine What Went Wrong

507.6 Audit the Flag: A NetWars Experience

This final day of the course presents a capstone experience with additional learning opportunities. Leveraging the well-known NetWars engine, students have the opportunity to connect to a simulated enterprise network environment. Building on the tools and techniques learned throughout the week, each student is challenged to answer a series of questions about the enterprise network, working through various technologies explored during the course.

Topics: Network Devices; Servers; Applications; Workstations

You Will Be Able To

- ▶ Understand the different types of controls (e.g., technical vs. non-technical) essential to perform a successful audit
- ▶ Conduct a proper risk assessment of a network to identify vulnerabilities and prioritize what will be audited
- ▶ Establish a well-secured baseline for computers and networks, constituting a standard against which one can conduct audits
- ▶ Perform a network and perimeter audit using a seven-step process
- ▶ Audit firewalls to validate that rules/settings are working as designed, blocking traffic as required
- ▶ Utilize vulnerability assessment tools effectively to provide management with the continuous remediation information necessary to make informed decisions about risk and resources
- ▶ Audit web applications configuration, authentication, and session management to identify vulnerabilities attackers can exploit
- ▶ Utilize scripting to build a system to baseline and automatically audit Active Directory and all systems in a Windows domain

“AUD507 provided me additional insight to the technical side of security auditing. Great course and a super instructor!”

-CARLOS E., U.S. ARMY

“AUD507 not only prepares you to perform a comprehensive audit but also provides excellent information to operations for an improved network security posture.”

-RIFAT I., STATE DEPT FCU

SEC440

Critical Security Controls: Planning, Implementing, and Auditing

Two-Day Course | Sat, Dec 10 - Sun, Dec 11 | 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, other government agencies (including the NSA, DHS, GAO, and many others), and private organizations that are the most respected experts on how attacks actually work and what can be done to stop them. 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 provides an excellent prioritized approach to IT security.” -DARRELL BATEMAN, TEXAS TECH

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

You will find the full document describing the Critical Security Controls posted at the Center for Internet Security at www.cisecurity.org/critical-controls.cfm.

Notice: Please note SEC440 does not contain any labs. Students looking for hands-on labs involving the Critical Controls should take SEC566.

SEC567

Social Engineering for Penetration Testers

Two-Day Course | Sat, Dec 10 - Sun, Dec 11 | 9:00am - 5:00pm | 12 CPEs | Laptop Required | Instructor: Dave Shackleford

NEW!

SEC567: Social Engineering for Penetration Testers 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 during the authors' 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 up 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.

Who Should Attend

- ▶ Staff or consultant penetration testers looking to increase their testing breadth and effectiveness
- ▶ Security defenders looking to enhance their understanding of attack techniques to improve their defenses
- ▶ Staff responsible for security awareness and education campaigns who want to understand how cyber criminals persuade their way through their defenses

SEC580

Metasploit Kung Fu for Enterprise Pen Testing

Two-Day Course | Sat, Dec 10 - Sun, Dec 11 | 9:00am - 5:00pm | 12 CPEs | Laptop Required | Instructor: Bryce Galbraith



www.sans.org/simulcast

Many enterprises today face regulatory or compliance requirements that mandate regular penetration testing and vulnerability assessments. Commercial tools and services for performing such tests can be expensive. While really solid free tools such as Metasploit are available, many testers do not understand the comprehensive feature sets of such tools and how to apply them in a professional-grade testing methodology. Metasploit was designed to help testers with confirming vulnerabilities using an open-source and easy-to-use framework. This course will help students get the most out of this free tool.

This class will show students how to apply the incredible capabilities of the Metasploit Framework in a comprehensive penetration testing and vulnerability assessment regimen according to a thorough methodology for performing effective tests. Students who complete the course will have a firm understanding of how Metasploit can fit into their penetration testing and day-to-day assessment activities. The course will provide an in-depth understanding of the Metasploit Framework far beyond simply showing attendees how to exploit a remote system. **The class will cover exploitation, post-exploitation reconnaissance, token manipulation, spear-phishing attacks, and the rich feature set of the Meterpreter, a customized shell environment specially created for exploiting and analyzing security flaws.**

The course will also cover many of the pitfalls that a tester may encounter when using the Metasploit Framework and how to avoid or work around them, making tests more efficient and safe.

“This is one of SANS’ best courses. Practical labs are a big part of this course, which is awesome.”

-CAMILO DO CARMO PINTO, DELOITTE

MGT305

Technical Communication and Presentation Skills for Security Professionals

One-Day Course | Sun, Dec 11 | 9:00am - 5:00pm | 6 CPEs | Laptop Required | Instructor: Bryan Simon

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.



www.sans.edu

MGT415

A Practical Introduction to Cybersecurity Risk Management

Two-Day Course | Sat, Dec 10 - Sun, Dec 11 | 9:00am - 5:00pm | 12 CPEs | Laptop Required | Instructor: James Tarala

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

You Will Learn:

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

MGT433

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

Two-Day Course | Sat, Dec 10 - Sun, Dec 11 | 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.



www.sans.org/simulcast



www.sans.edu

MGT535

Incident Response Team Management

Two-Day Course | Sat, Dec 10 - Sun, Dec 11 | 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 because it is their 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

NEW!

DEV534

Secure DevOps: A Practical Introduction

Two-Day Course | Sat, Dec 10 - Sun, Dec 11 | 9:00am - 5:00pm | 12 CPEs | Laptop Required | Instructors: Frank Kim, Ben Allen

DEV534: Secure DevOps: A Practical Introduction explains the fundamentals of DevOps, and how DevOps teams can build and deliver secure software. It will explain the principles and practices and tools in DevOps and how they can be leveraged to improve the reliability, integrity and security of systems.

What Does the Course Cover?

This course will introduce students to DevOps principles, practices and tools and explain how Secure DevOps can be implemented, using lessons from successful DevOps security programs. Students will build up a DevOps CI/CD toolchain, understand how code is automatically built, tested and deployed, using popular open source tools including git, Puppet, Jenkins and Docker. In a series of labs they will inject security into a CI/CD toolchain, and learn about the tools, patterns and techniques to do this. The course will make extensive use of open source materials and tooling for automated configuration management ("Infrastructure as Code"), Continuous Integration, Continuous Delivery and Continuous Deployment, containerization and micro-segmentation, and automated compliance ("Compliance as Code") and monitoring.

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



NEW!

HOSTED

Health Care Security Essentials

Two-Day Course | Sat, Dec 10 - Sun, Dec 11 | 9:00am - 5:00pm
12 CPEs | Laptop Required | Instructor: Greg Porter

Health Care Security Essentials is designed to provide SANS students with an introduction to current and emerging issues in health care information security and regulatory compliance. The class provides a foundational set of skills and knowledge for health care 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 health care 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. health care system.

MODULE 1: Overview of Healthcare Information Security

MODULE 2: HIPAA Security 2.0

MODULE 3: Risk Analysis & Management

MODULE 4: Medical Device Security

NEW!

HOSTED

Physical Access Control Systems: Elements of Design, Offense, and Defense

Two-Day Course | Sat, Dec 10 - Sun, Dec 11 | 9:00am - 5:00pm
12 CPEs | Laptop Required | Instructor: The CORE Group

Topics:

- ▶ 125KHz Credentials:
 - AWID, Overview and Cloning
 - EM4102/EM4200, Overview and Cloning
 - HID Prox / ProxCard II, Overview and Cloning
 - Kantech ioProx / ioProx XSE, Overview and Cloning
 - Atmel T5555 / T5577 Tags, Emulation Overview and Cloning Capabilities
 - Motorola / HID Indala Overview, and Cloning
 - Overview of other uncommon credentials
- ▶ 125/134KHz Vehicle Transponder Overview
- ▶ 13.56MHz Credentials and Smart Cards:
 - HID iCLASS Analysis, Review, Cloning, and Weaknesses
 - NXP Mifare Classic Detailed Overview, Cracking, Cloning, Weaknesses
 - Overview of other common and uncommon credentials, with discussion of security implications and strengths of each
- ▶ Practical Cloning in the Field, Advanced Format Downgrade Attacks
- ▶ Backend Detailed Overview, Weaknesses, and Attacks:
 - Man in the Middle
 - Denial of Service
- ▶ Defeating Tamper Detection
- ▶ Defenses and Mitigation

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

Jason Fossen

Ubuntu Bash built into Windows? Microsoft open-source projects on GitHub? Free upgrades to Windows 10? It's a new Microsoft under CEO Satya Nadella, that's for sure. In this talk, Jason Fossen, a SANS Institute Fellow and author of the Securing Windows course (SEC505), will lay out what's new for security in Server 2016 and Windows 10. Come see how Docker containers, Credential Guard, Windows as a Service (WaaS), biometric facial scanning, Server Nano, PowerShell and Bash can all figure into your organization's IT security planning. Is it really a "New Microsoft" when it comes to security or just the same old thing wrapped in new buzzwords? Come to the event and see!

GIAC Program Presentation

Global Information Assurance Certification (GIAC) develops and administers the premier certifications for information security professionals. More than 30 GIAC certifications align with SANS training and ensure mastery in critical, specialized InfoSec domains. GIAC certifications provide the highest and most rigorous assurance of cybersecurity knowledge and skill available to industry, government, and military clients across the world. Join us for an informational presentation along with a Q and A session. We'll cover everything from why you should get certified, what testing looks like, how to keep certifications current and more. GIAC staff will be present to answer your questions before and after the presentation.

Women's CONNECT Event

Join SANS and ISSA International Women in Security Special Interest Group (WIS SIG) as we partner with local association chapters and groups to foster an evening of connections. Group representatives will be on hand to discuss their groups and activities and the benefits of membership. From Jean Jennings Bartik to Diane Greene, women have always been a driving force in the field of information technology. Their experiences have been filled not only with stories of overcoming challenges but also ones of innovation and inspiration. Join us to hear some of these stories and come share your own. After the discussions, stay and network with other attendees and with the various groups that will be featured at the event.

DLP FAIL!!! Using Encoding, Steganography, and Covert Channels to Evade DLP and Other Critical Controls

Kevin Fiscus

It's all about the information! Two decades after the movie Sneakers, the quote remains as relevant as ever, if not more so. The fact that someone hacks into an environment is interesting but not that relevant. What is important is what happens after the compromise. If the data are destroyed or modified, organizations are negatively impacted but the benefits to an attacker for destruction or alteration are somewhat limited. Stealing information, however, is highly profitable. Identity theft, espionage, and financial attacks involve the exfiltration of sensitive data. As a result, organizations deploy tools to detect and/or stop that data exfiltration. While these tools can be extremely valuable, many have serious weaknesses; attackers can encode, hide, or obfuscate the data, or can use secret communication channels. This session will talk about and demonstrate a range of these methods.

Security Awareness: Understanding and Managing Your Top Seven Human Risks

Lance Spitzner

A key step to managing your human risk is first identifying and then prioritizing those risks and then focusing on the top ones. After working with hundreds of organizations, Lance Spitzner will discuss what are the seven most common human risks he finds in organizations and what you can do to effectively manage and measure those specific risks. Key points you will learn include.

- Concepts of "cognitive overload" and how every behavior has a cost
- Key elements in a human risk analysis
- Determining the key behaviors that will mitigate your top human risks
- How to effectively communicate and measure those behaviors

Perception Management in Information Warfare

Stephen Northcutt

The change from "Information Warfare" to "Cyberwar" buried an important nuance. There is a war on information. As an example (which we will not use in the talk since the subject will be exhausted by then), 2016 is an election year. Each of us is bombarded by TV commercials, robocalls, emails, "news stories" and the like. We know that not all of these are fully accurate. But, we have less of an understanding of the impact on our perceptions. They would not spend that kind of money if it did not garner measurable results. The talks will focus on far smaller, far more subtle, events that successfully, unsuccessfully, intentionally and unintentionally influence our perceptions. Attendees will gain an increased understanding and awareness of perception management.

Current and Future Trends in Digital Investigative Analysis

Ovie Carroll

In this fun and fast-paced presentation, Ovie Carroll will discuss current and future trends in digital investigative analysis. Ovie will cover critical challenges digital investigative analysts (computer forensic examiners) face and cover some of the most interesting digital artifacts.

Analysis of the Cyber Attack on the Ukrainian Power Grid

Robert M. Lee

On December 23, 2015 a cyber attack caused a power outage that affected 230,000 people in Ukraine. The SANS ICS team immediately began investigating and reporting on the case. In this presentation the attack will be broken down with lessons learned and takeaways for organizations to secure their infrastructure.

The iOS of Sauron: How iOS Tracks Everything You Do

Sarah Edwards

iOS devices have the ability to track everything the user does — how many steps the user takes, where the user has been — and keeps track of how they use their devices. This presentation will dive into some of the protected files that keep track of every detail of a user's life that iOS tracks. These databases and files can be used to correlate user activity down to the smallest detail. Methods of analysis as well as some scripts will be shown to help analyze these files.

CISSP®: How to Get the Certification that Matters the Most

David R. Miller

See why the CISSP® certification is so important to your IT career. Companies are in great need of qualified security professionals. The positions are there. The budget is there. Many IT security positions remain available because there are too few certified IT security professionals. This means you can choose which position you want from many companies. This means companies are willing to pay higher salaries to get you. This presentation is offered by one of the most experienced CISSP® instructors on the planet.

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.

Open-Source Intelligence (OSINT) Tips for Malware Investigations

Lenny Zeltser

If you're responding to a malware incident, you need to quickly derive relevant and actionable information about the malicious program and the context within which it was employed. This involves not only examining the specimen in your lab, but also benefiting from relevant publicly-available details. Accomplishing this requires the right skills to locate and makes sense of the data. This engaging presentation will show several real-world examples, tools and data sources for gathering such open-source intelligence, so you can:

- Benefit from previously-discovered information to focus your time on new malware characteristics.
- Pivot around data points to progress with your analysis of the malware sample.
- Broaden and deepen your understanding of the security incident's context.

Attend this talk to expand your incident response and malware analysis skillset and learn how to turn publicly-available data about adversaries and their malicious programs into useful intelligence.

Quality Not Quantity: Continuous Monitoring's Deadliest Events

Eric Conrad

Most Security Operations Centers (SOCs) are built for compliance, not security. One well-known retail firm suffered the theft of over a million credit cards, and 60,000 true positive events were reported to its SOC during that missed breach, but they were lost in the noise of millions. If you are bragging about how many events your SOC handles each day, you are doing it wrong. During this talk, we will show you how to focus on quality instead of quantity, and provide an actionable list of the deadliest events that occur during virtually every successful breach.

How to Build a Cybersecurity Platform the Easy Way

Keith Palmgren

Building a cybersecurity program is easy. Building a cybersecurity program that is effective is seriously hard! When faced with a seemingly insurmountable task, prioritization is vital. Investing time and money in the right place at the right time is the difference between success and being the next cyberbreach headline. Whether you are new to cybersecurity or an old hand, you may feel lost in the storm. If so, this talk is for you. Cybersecurity's five historic and current pitfalls that prevent organizations from building an effective IT Security platform will be discussed: poor passwords, vulnerabilities, malware/crimeware, insider threat, and mismanagement. Every organization needs a cybersecurity strategy. An effective strategy requires that you understand the problems as well as the solutions to those problems. Only then can you prioritize your limited cybersecurity resources. Managers and technicians alike will gain valuable insight in this non-technical talk.

The Tap House

Philip Hagen

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

Vendor-Sponsored Events

Vendor Expo

Wednesday, December 14 | 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, December 14 | 12:00pm - 1:30pm

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

Lunch & Learn Presentations

Throughout SANS CDI 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, December 14 | 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.

The Value of SANS Training and YOU



EXPLORE

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

RELATE

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

VALIDATE

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

SAVE

- Register early to pay less using early-bird specials
- Consider the SANS Voucher Program to make the most of your training budget

ADD VALUE

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

ALTERNATIVES

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

ACT

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

Return on Investment

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

REMEMBER

the SANS promise:

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

.001%

GSE: The Certification Like No Other

Only the true security elite hold a GIAC Security Expert certification (GSE). In fact, it's about .001% of all GIAC certification holders. GSE is the most prestigious, most demanding certification in the information security industry. The GSE's performance based, hands-on nature sets it apart from any other certification in cybersecurity. Those who earn the GSE master the wide variety of skills, across multiple domains, required by top security professionals. They demonstrate expertise in applying knowledge in a hands-on environment.

GSEs are verified network packet ninjas with world-class incident response capabilities. In addition to superior technical skills, GSEs must have demonstrated a keen awareness of important business drivers and considerations, an exceptionally rare skill set among technology professionals.

GSE. For the very few, the very best, cybersecurity professionals.

SANS



DEEPER KNOWLEDGE. ADVANCED SECURITY.

INFO@GIAC.ORG WWW.GIAC.ORG

Global Information Assurance Certification (GIAC) develops and administers the premier certifications for information security professionals. More than 30 certifications align with SANS training and ensure mastery in critical, specialized InfoSec domains. GIAC certifications provide the highest and most rigorous assurance of cybersecurity knowledge and skill available to industry, government, and military clients across the world.

INFO@GIAC.ORG WWW.GIAC.ORG



Students earn industry-
recognized GIAC certifications
during most technical courses.

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

-John Hally, MSISE, EBSCO Information Services

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

Master of Science Degrees

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

Graduate Certificate Programs

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

Learn more at www.sans.edu

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



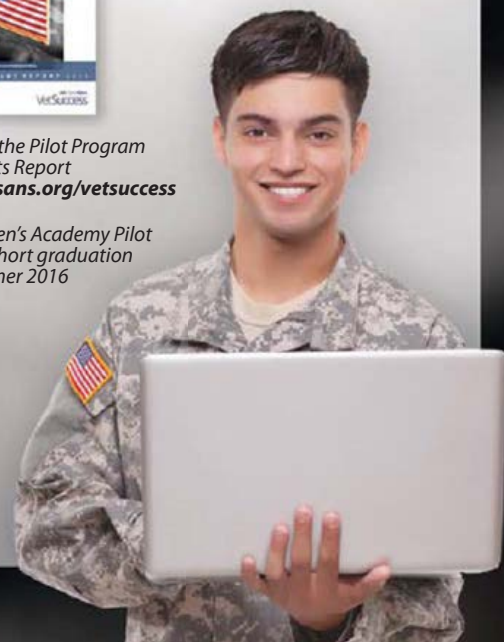
Read the Pilot Program
Results Report
Visit sans.org/vetsuccess

Women's Academy Pilot
1st cohort graduation
Summer 2016

VetSuccess

SANS

CyberTalent
IMMERSION ACADEMY



Department of Defense Directive 8140

(DoDD 8570)



www.sans.org/dodd-8140

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

Compliance/Recertification:

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

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

DoD Baseline IA Certifications

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

Computer Network Defense (CND) Certifications

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

Information Assurance System Architecture & Engineering (IASAE) Certifications

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

Computer Environment (CE) Certifications

GCWN	GCUX
-------------	-------------

SANS Training Courses for DoDD Approved Certifications

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



Real Threats
Real Skills
Real Success
Join Today!

SANS

CYBER GUARDIAN

PROGRAM

This program begins with hands-on core courses that will build and increase your knowledge and skills. These skills will be reinforced by taking and passing the associated GIAC certification exam. After completing the core courses, you will choose a course and certification from either the Red or Blue Team. The program concludes with participants taking and passing the GIAC Security Expert (GSE) certification.

Core Courses

SEC503 (GCIA) | SEC504 (GCIH) | SEC560 (GPEN) | FOR508 (GCFA)

After completing the core courses, students must choose one course and certification from either the Blue or Red Team

Blue Team Courses

SEC505 (GCWN)
SEC506 (GCUX)

Red Team Courses

SEC542 (GWAPT)
SEC617 (GAWN)
SEC660 (GXPN)

Contact us at onsite@sans.org to get started!
www.sans.org/cyber-guardian



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

www.sans.org/vouchers

VOUCHER PROGRAM



Training Investment & Bonus Funds

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

The investment and bonus funds:

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

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



Flexibility & Control

The online SANS Admin Tool allows the organization's Program Administrator to manage the account at anytime from anywhere.

With the SANS Admin Tool, the Administrator can:

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

By creating a Voucher Account, your organization can:

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

Getting Started

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

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

SANS TRAINING FORMATS

LIVE TRAINING



Multi-Course Training Events

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

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



Summit

www.sans.org/summit

Live IT Security Summits and Training



Community SANS

www.sans.org/community

Live Training in Your Local Region with Smaller Class Sizes



Private Training

www.sans.org/private-training

Live Training at Your Office Location



Mentor

www.sans.org/mentor

Live Multi-Week Training with a Mentor

ONLINE TRAINING



OnDemand

www.sans.org/ondemand

Four Months of Self-Paced e-Learning



vLive

www.sans.org/vlive

Live Online, Evening Sessions with Six Months of Archive Access



Simulcast

www.sans.org/simulcast

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



SelfStudy

www.sans.org/selfstudy

Self-Paced Study with Lecture Audio



OnDemand Bundles

www.sans.org/ondemand/bundles

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

FUTURE SANS TRAINING EVENTS

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

Network Security

Las Vegas, NV

September 10-19, 2016

48 courses in:

CYBER DEFENSE

PEN TESTING

DIGITAL FORENSICS

ETHICAL HACKING

INCIDENT RESPONSE

SECURITY MANAGEMENT

APPLICATION SECURITY

ICS SECURITY

Crystal City 2016

Crystal City, VA
September 6-11

Seattle 2016

Seattle, WA
October 3-8

Baltimore 2016

October 10-15

Tysons Corner 2016

October 22-29

San Diego 2016

October 23-28

SANS | HACKFEST

SUMMIT & TRAINING 2016

Crystal City, VA | November 2-9

FUTURE SANS TRAINING EVENTS

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



Miami 2016

Miami, FL
November 7-12



Health Care Cybersecurity

SUMMIT & TRAINING 2016

Houston, TX
November 14-21



Las Vegas 2017

Las Vegas, NV
January 23-28



Cyber Threat Intelligence

SUMMIT & TRAINING 2017

Arlington, VA
January 25 - February 1



San Francisco 2016

November 27 - December 2



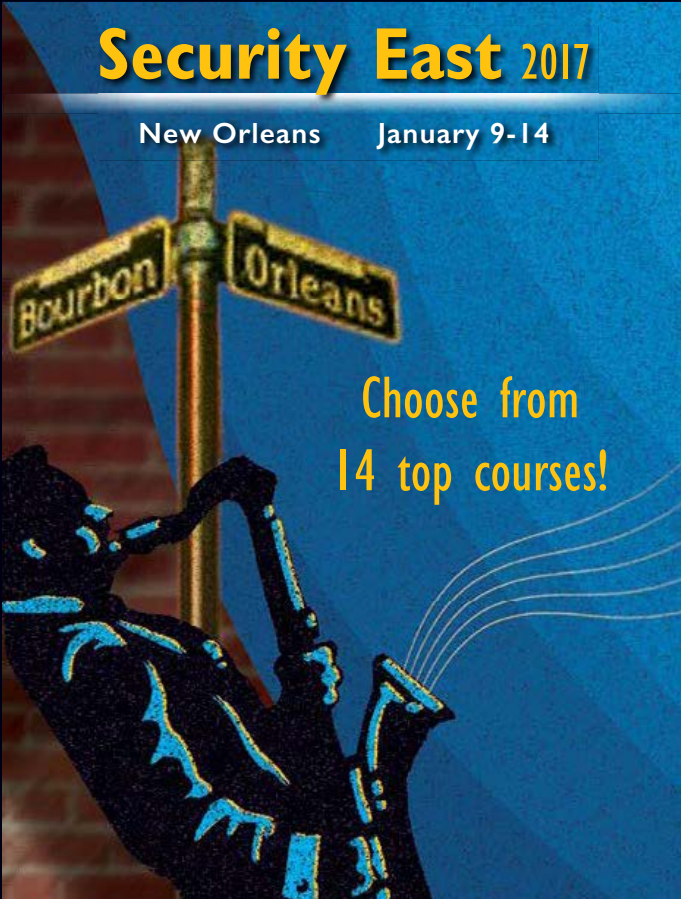
Anaheim 2017

Anaheim, CA
February 6-11



Scottsdale 2017

Scottsdale, AZ
February 20-25



Security East 2017

New Orleans January 9-14

Choose from
14 top courses!



Dallas 2017

February 27 - March 4



San Jose 2017

San Jose, CA
March 6-11



Tysons Corner Spring 2017

McLean, VA
March 20-25

Note: There are two host venues for Cyber Defense Initiative 2016.

Please see adjacent page for more information.

HOTEL INFORMATION

Training Campus
Grand Hyatt Washington

1000 H Street NW

Washington, DC 20001

202-582-1234

www.sans.org/event/cyber-defense-initiative-2016/location

Grand Hyatt Washington is happy to make available to our guests a host of first-class services and amenities. For your convenience, our Washington, DC City Center hotel offers valet parking, room service, laundry service and dry-cleaning. Use of our state-of-the-art Business Center is available daily with computer, print, and clerical services. Upgrade to our Business Plan room and enjoy complimentary breakfast and high-speed guestroom Internet access.

Innovative Hyatt services such as Fast Board™, E-Concierge, I-800-CHECK-IN®, Video Checkout and PDA Check-in will make your stay easy and seamless. Check emails, upload pictures or stay in touch with work with complimentary Wi-Fi access in our newly renovated lobby and your guestroom. Our fitness-minded guests will receive free access to the FIT Club at Washington Center located adjacent to the hotel. Relax and enjoy everything our upscale Metro Center hotel has to offer.

Special Hotel Rates Available

A special discounted rate of \$219.00 S/D will be honored based on space availability. The rate is only available through November 18, 2016.

To make reservations, use the following link:

<https://aws.passkey.com/event/14464942/owner/544/home>

You can also call **888-421-1442** and ask for the SANS group rate.

Top 5 reasons to stay at the Grand Hyatt Washington

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

Note: There are two host venues for Cyber Defense Initiative 2016.

Please see adjacent page for more information.

HOTEL INFORMATION

Training Campus

Washington Marriott at Metro Center

775 12th Street NW

Washington, DC 20005

202-737-2200

www.sans.org/event/cyber-defense-initiative-2016/location

*The Washington
Marriott at Metro
Center is one block
from the Grand Hyatt.*

Washington Marriott at Metro Center features convenient access to the best of Washington, DC area attractions, shopping and dining. Our premier location near the DC metro system provides guests easy access to the National Mall, Smithsonian Institution, CityCenterDC, Spy Museum and the National Portrait Gallery. Located within blocks of the Verizon Center and Walter E. Washington Convention Center, this Washington, DC hotel offers stylish surroundings for guests attending conferences, sporting events or concerts. Our hotel's location, engaging environment and dining options, including a Starbucks Café®, make us a great choice for business and leisure travelers. Meeting planners can explore the possibilities with over 14,000 square feet of event space and 15 breakout rooms, perfect for hosting a variety of gatherings and events. With easy access to the region's major airports, Union Station and the Convention Center, Washington Marriott at Metro Center is a top choice for travelers to DC.

Special Hotel Rates Available

A special discounted rate of \$179.00 S/D will be honored based on space availability. The rate is only available through November 13, 2016.

To make reservations, use the following link:

<https://resweb.passkey.com/go/b2c9fc31>

You can also call **800-393-2510** and ask for the SANS group rate.



Top 5 reasons to stay at the Washington Marriott

- 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, 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 that you won't want to miss!
- 5 Everything is in one convenient location!

REGISTRATION INFORMATION

Register online at
www.sans.org/cdi

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

Use code
EarlyBird16
when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	10-19-16	\$400.00	11-9-16	\$200.00

Some restrictions apply.



SANS SIMULCAST

To register for a SANS CDI 2016 Simulcast course, please visit
www.sans.org/event/cyber-defense-initiative-2016/attend-remotely

SANS Voucher Program

Expand your training budget!

Extend your fiscal year. The SANS Voucher Program provides flexibility and may earn you bonus funds for training.

www.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, November 23, 2016** – processing fees may apply.

SANS CDI 2016 REGISTRATION FEES

Register online at www.sans.org/cdi

If you don't wish to register online, please call 301-654-SANS (7267) 9:00am-8:00pm (Mon-Fri) EST and we will fax or mail you an order form.

Job-Based Long Courses

		Paid before 10-19-16	Paid before 11-9-16	Paid after 11-9-16	Add GIAC Cert	Add OnDemand	Add NetWars Continuous
☐ SEC301	Intro to Information Security	\$4,730	\$4,930	\$5,130	☐ \$689	☐ \$689	☐ \$1,199
☐ SEC401	Security Essentials Bootcamp Style	\$5,510	\$5,710	\$5,910	☐ \$689	☐ \$689	☐ \$1,199
☐ SEC501	Advanced Security Essentials — Enterprise Defender	\$5,510	\$5,710	\$5,910	☐ \$689	☐ \$689	☐ \$1,199
☐ SEC503	Intrusion Detection In-Depth	\$5,510	\$5,710	\$5,910	☐ \$689	☐ \$689	☐ \$1,199
☐ SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling	\$5,510	\$5,710	\$5,910	☐ \$689	☐ \$689	☐ \$1,199
☐ SEC505	Securing Windows and PowerShell Automation	\$5,420	\$5,620	\$5,820	☐ \$689	☐ \$689	☐ \$1,199
☐ SEC511	Continuous Monitoring and Security Operations	\$5,510	\$5,710	\$5,910	☐ \$689	☐ \$689	☐ \$1,199
☐ SEC542	Web App Penetration Testing and Ethical Hacking	\$5,510	\$5,710	\$5,910	☐ \$689	☐ \$689	☐ \$1,199
☐ SEC550	Active Defense, Offensive Countermeasures and Cyber Deception	\$4,730	\$4,930	\$5,130			☐ \$1,199
☐ SEC560	Network Penetration Testing and Ethical Hacking	\$5,510	\$5,710	\$5,910	☐ \$689	☐ \$689	☐ \$1,199
☐ SEC561	Immersive Hands-On Hacking Techniques	\$5,510	\$5,710	\$5,910			☐ \$1,199
☐ SEC566	Implementing and Auditing the Critical Security Controls — In-Depth	\$4,730	\$4,930	\$5,130	☐ \$689	☐ \$689	☐ \$1,199
☐ SEC575	Mobile Device Security and Ethical Hacking	\$5,510	\$5,710	\$5,910	☐ \$689	☐ \$689	☐ \$1,199
☐ SEC579	Virtualization and Private Cloud Security	\$5,510	\$5,710	\$5,910		☐ \$689	☐ \$1,199
☐ SEC660	Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	\$5,510	\$5,710	\$5,910	☐ \$689	☐ \$689	☐ \$1,199
☐ SEC760	Advanced Exploit Development for Penetration Testers	\$5,510	\$5,710	\$5,910			☐ \$1,199
☐ AUD507	Auditing & Monitoring Networks, Perimeters, and Systems	\$5,420	\$5,620	\$5,820	☐ \$689	☐ \$689	☐ \$1,199
☐ DEV522	Defending Web Applications Security Essentials	\$5,420	\$5,620	\$5,820	☐ \$689	☐ \$689	☐ \$1,199
☐ FOR408	Windows Forensic Analysis	\$5,510	\$5,710	\$5,910	☐ \$689	☐ \$689	☐ \$1,199
☐ FOR508	Advanced Digital Forensics and Incident Response	\$5,510	\$5,710	\$5,910	☐ \$689	☐ \$689	☐ \$1,199
☐ FOR518	Mac Forensic Analysis	\$5,510	\$5,710	\$5,910		☐ \$689	☐ \$1,199
☐ FOR572	Advanced Network Forensics and Analysis	\$5,510	\$5,710	\$5,910	☐ \$689	☐ \$689	☐ \$1,199
☐ FOR578	Cyber Threat Intelligence NEW!	\$4,730	\$4,930	\$5,130			☐ \$1,199
☐ FOR610	Reverse-Engineering Malware: Malware Analysis Tools and Techniques	\$5,510	\$5,710	\$5,910	☐ \$689	☐ \$689	☐ \$1,199
☐ ICS456	Essentials for NERC Critical Infrastructure Protection NEW!	\$4,730	\$4,930	\$5,130			☐ \$1,199
☐ ICS515	ICS Active Defense and Incident Response	\$5,310	\$5,510	\$5,710		☐ \$689	☐ \$1,199
☐ MGT414	SANS Training Program for CISSP® Certification	\$4,840	\$5,040	\$5,240	☐ \$689	☐ \$689	☐ \$1,199
☐ MGT512	SANS Security Leadership Essentials for Managers with Knowledge Compression™	\$5,130	\$5,330	\$5,530	☐ \$689	☐ \$689	☐ \$1,199
☐ MGT514	IT Security Strategic Planning, Policy, and Leadership	\$4,730	\$4,930	\$5,130		☐ \$689	☐ \$1,199

Skill-Based Short Courses

		Course fee if taking a 4-6 day course	Course fee
☐ SEC440	Critical Security Controls: Planning, Implementing, and Auditing	\$1,450	\$2,360
☐ SEC567	Social Engineering for Penetration Testers NEW!	\$1,350	\$2,240
☐ SEC580	Metasploit Kung Fu for Enterprise Pen Testing	\$1,350	\$2,240
☐ MGT305	Technical Communication and Presentation Skills for Security Professionals	\$850	\$1,370
☐ MGT415	A Practical Introduction to Cybersecurity Risk Management	\$1,350	\$2,240
☐ MGT433	Securing The Human: How to Build, Maintain & Measure a High-Impact Awareness Program	\$1,350	\$2,240
☐ MGT535	Incident Response Team Management	\$1,350	\$2,240
☐ DEV534	Secure DevOps: A Practical Introduction NEW!	\$1,350	\$2,130
☐ HOSTED	Health Care Security Essentials NEW!	\$2,235	\$2,235
☐ HOSTED	Physical Access Control Systems: Elements of Design, Offense, and Defense NEW!	\$2,140	\$2,140
☐ SPECIAL	Core NetWars Tournament — Tournament Entrance Fee	FREE	\$1,520
☐ SPECIAL	DFIR NetWars Tournament — Tournament Entrance Fee	FREE	\$1,520

**EARLYBIRD
DISCOUNTS**

Pay for any long course using the code **EARLYBIRD16** at checkout by:
10-19-16 to get **\$400 OFF** / 11-9-16 to get **\$200 OFF**

Create a **SANS Account** today
to enjoy these FREE resources:

WEBCASTS

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

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

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

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

NEWSLETTERS

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

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

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

OTHER FREE RESOURCES

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

www.sans.org/account

SAVE \$400 on SANS CDI 2016 courses!

Register and pay by 10-19-16 (SAVE \$400) or 11-9-16 (SAVE \$200) – **www.sans.org/cdi**