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

SANS

Security West 2017

San Diego, CA | May 9-18

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

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

SAVE $400

Register and pay by March 15th – Use code **EarlyBird17**

30+ courses in:

CYBER DEFENSE

DETECTION & MONITORING

PENETRATION TESTING

INCIDENT RESPONSE

DIGITAL FORENSICS

ETHICAL HACKING

MANAGEMENT | AUDIT

SECURE DEVELOPMENT

GIAC

GIAC-Approved Training

SANS NETWARS EXPERIENCE

"For those considering the cybersecurity field, SANS training is a must."

-David First, Chevron

REGISTER AT **www.sans.org/security-west**

Dear Colleague,

Frank Kim

Cybersecurity skills and knowledge are in high demand. Cyber attacks and data breaches are more frequent and sophisticated than ever, and organizations are grappling with how to best defend themselves. As a result, cybersecurity is more vital, crucial, and important to the growth of your organization than ever before. Now is the perfect time to take the next step to protect your organization and advance your career. Join us at **Security West 2017** (May 9-18) in beautiful San Diego, CA to gain the skills and knowledge to help your organization succeed.

SANS is recognized around the world as the best place to develop the deep, hands-on cybersecurity skills most in need right now. Security West 2017 brings you 31 information security courses taught by SANS' world-class instructors. You will learn cutting-edge content about the hottest information security topics across penetration testing, digital forensics and incident response (DFIR), security operations, audit, application security, and security management.

At Security West 2017, you'll get the best hands-on, immersion training and learn what it takes to stop cyber threats. The course schedule features a full lineup of SANS' classic courses as well as new courses including: **DEV531: Defending Mobile Applications Security Essentials**; **DEV534: Secure DevOps: A Practical Introduction**; **SEC579: Virtualization and Software-Defined Security**; and **MGT517: Managing Security Operations: Detection, Response, and Intelligence**.

Many of these courses prepare you for a prestigious ***GIAC certification***. And you can also bundle four months of OnDemand online training with your live course at a discounted rate to extend your study. Enhance your credentials by signing up for a corresponding GIAC certification and OnDemand bundle when registering for your SANS course.

Don't forget the ***Core NetWars Experience*** and ***DFIR NetWars Tournament*** scheduled for the evenings of May 14 and 15. The Core NetWars Experience is an interactive, Internet-based environment for computer attacks and the analysis of defenses. The DFIR NetWars Tournament is an incident simulator packed with a vast amount of forensic and incident response challenges for individual or team-based "firefights." Professionals at all skill levels will gain valuable knowledge by participating.

There will be numerous opportunities to learn new skills and techniques at the keynote presentation on Emerging Trends in Cybersecurity and other SANS@Night talks, lunch and learns, and by networking with your peers. Hear about the latest and most important issues from SANS practitioners who are leading the global conversation on cybersecurity.

Our award-winning faculty has proven that they understand the challenges you face on a daily basis and they are eager to help you learn the vital skills needed to secure your environment. Visit **www.sans.org/security-west** to review the full course list and conference details. **Register and pay by March 15 to receive an early-bird discount!** We look forward to seeing you in San Diego!

Frank Kim
Chief Information Security Officer
Curriculum Lead, Management & Application Security

SANS

INFORMATION SECURITY TRAINING AND YOUR CAREER ROADMAP

CORE COURSES

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

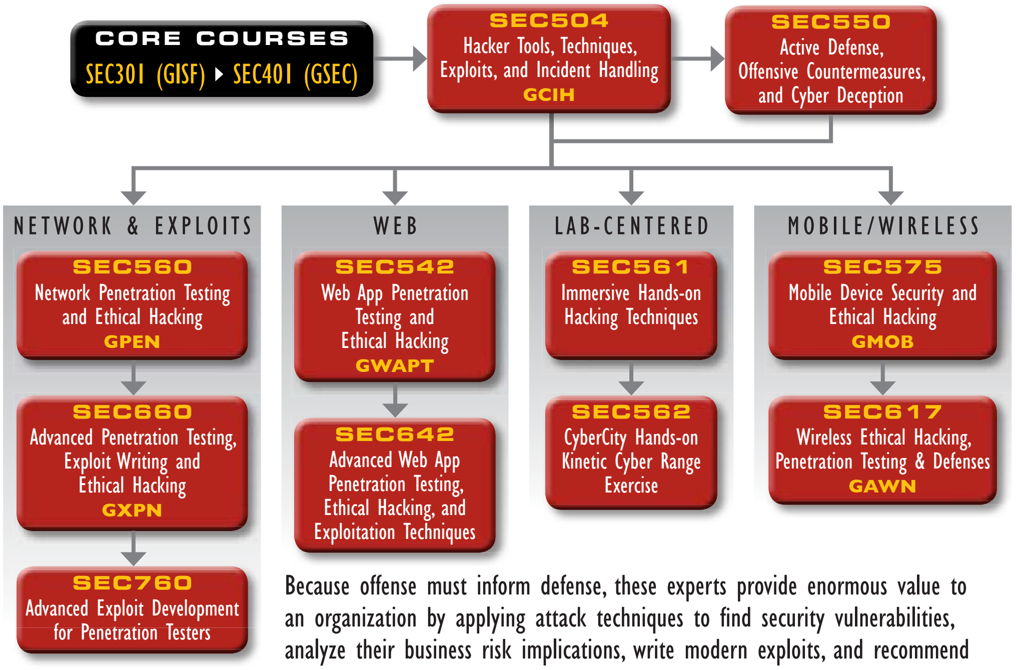
CORE

SEC401
Security Essentials Bootcamp Style
GSEC

IN-DEPTH

SEC501
Advanced Security Essentials — Enterprise Defender
GCED

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

NETWORK & EXPLOITS

SEC560
Network Penetration Testing and Ethical Hacking
GPEN

SEC660
Advanced Penetration Testing, Exploit Writing and Ethical Hacking
GXPN

SEC760
Advanced Exploit Development for Penetration Testers

WEB

SEC542
Web App Penetration Testing and Ethical Hacking
GWAPT

SEC642
Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques

LAB-CENTERED

SEC561
Immersive Hands-on Hacking Techniques

SEC562
CyberCity Hands-on Kinetic Cyber Range Exercise

MOBILE/WIRELESS

SEC575
Mobile Device Security and Ethical Hacking
GMOB

SEC617
Wireless Ethical Hacking, Penetration Testing & Defenses
GAWN

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

SAMPLE JOB TITLES

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

SPECIALIZATION

SEC567
Social Engineering for Penetration Testers

SEC573
Automating Information Security for Python
GPYC

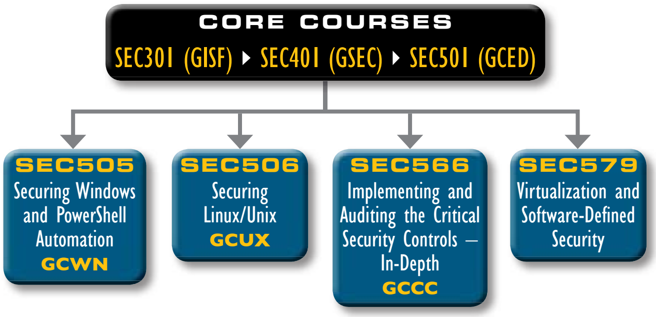
SEC580
Metasploit Kung Fu for Enterprise Pen Testing

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
GCUX

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

SEC579
Virtualization and Software-Defined Security

Security Operations Center/Intrusion Detection

SAMPLE JOB TITLES

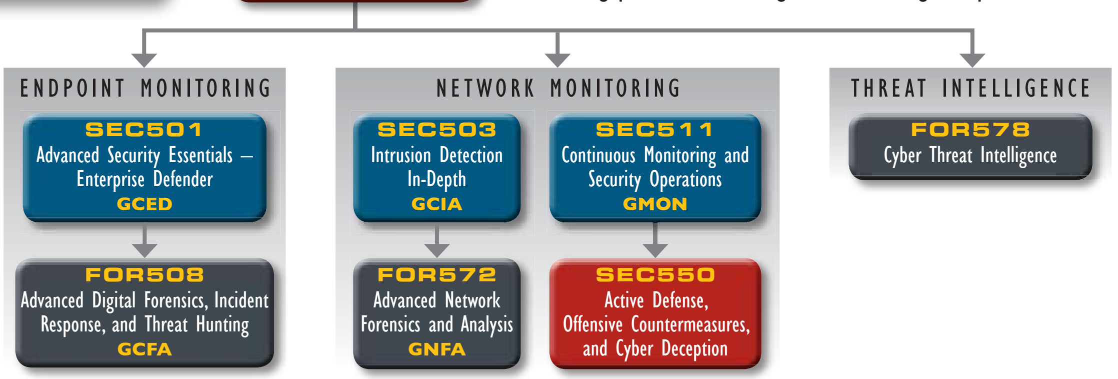
- Intrusion detection analyst
- Security Operations Center analyst/engineer
- CERT member
- Cyber threat analyst

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, Incident Response, and Threat Hunting
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.

SPECIALIZATION

SEC542
Web App Pen Testing and Ethical Hacking
GWAPT

SEC642
Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques

SAMPLE JOB TITLES

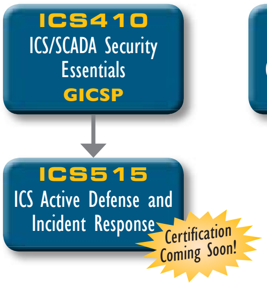
- Developer
- Software architect
- QA tester
- Development manager

Industrial Control Systems

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

SAMPLE JOB TITLES

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



ICS410
ICS/SCADA Security Essentials
GICSP

ICS515
ICS Active Defense and Incident Response

Certification Coming Soon!

ICS456
Essentials for NERC Critical Infrastructure Protection

HOSTED
Assessing and Exploiting Control Systems

HOSTED
Critical Infrastructure and Control System Cybersecurity

Cyber or IT Security Management

FOUNDATIONAL

- **MGT512** SANS Security Leadership Essentials for Managers with Knowledge Compression™ **GSLC**
- **MGT525** IT Project Management, Effective Communication & PMP® Exam Prep **GCPM**
- **MGT414** SANS Training Program for CISSP® Certification **GISP**

CORE

- **MGT514** IT Security Strategic Planning, Policy, and Leadership
- **MGT517** Managing Security Operations: Detection, Response, and Intelligence
- **LEG523** Law of Data Security and Investigations **GLEG**

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 a registered trademark of the Project Management Institute, Inc.

SAMPLE JOB TITLES

- CISO
- Cybersecurity manager/officer
- Security director

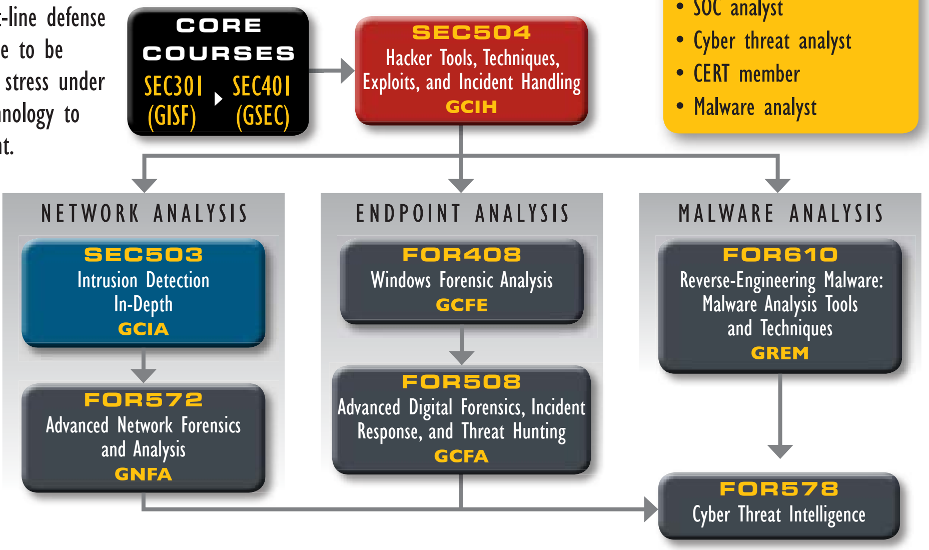
Management of people, processes, and technologies is critical for maintaining proactive enterprise situational awareness and for the ongoing success of continuous monitoring efforts. These managers must have the leadership skills, current knowledge, and best-practice examples to make timely and effective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

Incident Response 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

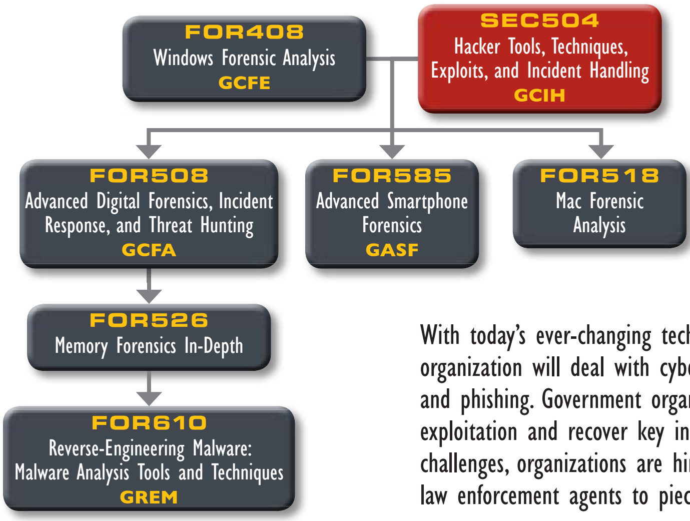


CORE COURSES
SEC301 (GISF)
SEC401 (GSEC)
SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling GCIH
NETWORK ANALYSIS
SEC503 Intrusion Detection In-Depth GCIA
FOR572 Advanced Network Forensics and Analysis GNFA
ENDPOINT ANALYSIS
FOR408 Windows Forensic Analysis GCFE
FOR508 Advanced Digital Forensics, Incident Response, and Threat Hunting GCFA
MALWARE ANALYSIS
FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques GREM
FOR578 Cyber Threat Intelligence

SPECIALIZATION

- **FOR526** Memory Forensics In-Depth
- **MGT535** Incident Response Team Management

Digital Forensic Investigations and Media Exploitation



FOR408 Windows Forensic Analysis GCFE
SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling GCIH
FOR508 Advanced Digital Forensics, Incident Response, and Threat Hunting GCFA
FOR585 Advanced Smartphone Forensics GASF
FOR518 Mac Forensic Analysis
FOR526 Memory Forensics In-Depth
FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques GREM

SAMPLE JOB TITLES

- Computer crime investigator
- Law enforcement
- Digital investigations analyst
- Media exploitation analyst
- Information technology litigation 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.

SANS NETWARS EXPERIENCE

Earn up to 6 CPEs!

*Three Ways to Participate at SANS Security West 2017 for FREE!**

DFIR NETWARS TOURNAMENT

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

Who Should Attend

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

CORE NETWARS EXPERIENCE

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

Who Should Attend

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

NEW! CYBER DEFENSE NETWARS COMPETITION

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

Who Should Attend

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

All three NetWars competitions will be played over two evenings: May 14-15

Prizes will be awarded at the conclusion of the games.

***REGISTRATION IS LIMITED AND IS FREE**

for students attending any long course at SANS Security West 2017 *(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/security-west-2017/schedule

<table>
<tr><th></th><th></th><th></th><th>TUE
5-9</th><th>WED
5-10</th><th>THU
5-11</th><th>FRI
5-12</th><th>SAT
5-13</th><th>SUN
5-14</th><th>MON
5-15</th><th>TUE
5-16</th><th>WED
5-17</th><th>THU
5-18</th></tr>
<tr><td>SEC301</td><td>Intro to Information Security</td><td>SIMULCAST</td><td></td><td></td><td colspan="5">PAGE 6</td><td></td><td></td><td></td></tr>
<tr><td>SEC401</td><td>Security Essentials Bootcamp Style</td><td></td><td></td><td></td><td colspan="6">PAGE 8</td><td></td><td></td></tr>
<tr><td>SEC440</td><td>Critical Security Controls: Planning, Implementing, and Auditing</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="2">P 50</td></tr>
<tr><td>SEC501</td><td>Advanced Security Essentials – Enterprise Defender</td><td></td><td></td><td></td><td colspan="6">PAGE 10</td><td></td><td></td></tr>
<tr><td>SEC503</td><td>Intrusion Detection In-Depth</td><td></td><td></td><td></td><td colspan="6">PAGE 12</td><td></td><td></td></tr>
<tr><td>SEC504</td><td>Hacker Tools, Techniques, Exploits, and Incident Handling</td><td>SIMULCAST</td><td></td><td></td><td colspan="6">PAGE 14</td><td></td><td></td></tr>
<tr><td>SEC505</td><td>Securing Windows and PowerShell Automation</td><td></td><td></td><td></td><td colspan="6">PAGE 16</td><td></td><td></td></tr>
<tr><td>SEC511</td><td>Continuous Monitoring and Security Operations</td><td></td><td></td><td></td><td colspan="6">PAGE 18</td><td></td><td></td></tr>
<tr><td>SEC524</td><td>Cloud Security Fundamentals</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="2">P 50</td></tr>
<tr><td>SEC542</td><td>Web App Penetration Testing and Ethical Hacking</td><td>SIMULCAST</td><td></td><td></td><td colspan="6">PAGE 20</td><td></td><td></td></tr>
<tr><td>SEC546</td><td>IPv6 Essentials</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="2">P 51</td></tr>
<tr><td>SEC560</td><td>Network Penetration Testing and Ethical Hacking</td><td>SIMULCAST</td><td></td><td></td><td colspan="6">PAGE 22</td><td></td><td></td></tr>
<tr><td>SEC566</td><td>Implementing and Auditing the Critical Security Controls – In-Depth</td><td></td><td></td><td></td><td colspan="5">PAGE 24</td><td></td><td></td><td></td></tr>
<tr><td>SEC575</td><td>Mobile Device Security and Ethical Hacking</td><td></td><td></td><td></td><td colspan="6">PAGE 26</td><td></td><td></td></tr>
<tr><td>SEC579</td><td>Virtualization and Software-Defined Security <b><i>NEW!</i></b></td><td></td><td></td><td></td><td colspan="5">PAGE 28</td><td></td><td></td><td></td></tr>
<tr><td>SEC580</td><td>Metasploit Kung Fu for Enterprise Pen Testing</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="2">P 51</td></tr>
<tr><td>SEC660</td><td>Advanced Penetration Testing, Exploit Writing, and Ethical Hacking</td><td></td><td></td><td></td><td colspan="6">PAGE 30</td><td></td><td></td></tr>
<tr><td>FOR408</td><td>Windows Forensic Analysis</td><td></td><td></td><td></td><td colspan="6">PAGE 32</td><td></td><td></td></tr>
<tr><td>FOR508</td><td>Advanced Digital Forensics, Incident Response, and Threat Hunting</td><td></td><td></td><td></td><td colspan="6">PAGE 34</td><td></td><td></td></tr>
<tr><td>FOR518</td><td>Mac Forensic Analysis</td><td></td><td></td><td></td><td colspan="6">PAGE 36</td><td></td><td></td></tr>
<tr><td>FOR578</td><td>Cyber Threat Intelligence</td><td></td><td></td><td></td><td colspan="5">PAGE 38</td><td></td><td></td><td></td></tr>
<tr><td>MGT305</td><td>Technical Communication and Presentation Skills for Security Professionals</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>P 52</td><td></td></tr>
<tr><td>MGT414</td><td>SANS Training Program for CISSP® Certification</td><td></td><td></td><td></td><td colspan="6">PAGE 40</td><td></td><td></td></tr>
<tr><td>MGT415</td><td>A Practical Introduction to Cybersecurity Risk Management</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="2">P 52</td></tr>
<tr><td>MGT433</td><td>Securing The Human: How to Build, Maintain, and Measure a High-Impact Awareness Program</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="2">P 52</td></tr>
<tr><td>MGT512</td><td>SANS Security Leadership Essentials for Managers with Knowledge Compression™</td><td></td><td></td><td></td><td colspan="5">PAGE 42</td><td></td><td></td><td></td></tr>
<tr><td>MGT514</td><td>IT Security Strategic Planning, Policy, and Leadership</td><td></td><td></td><td></td><td colspan="5">PAGE 44</td><td></td><td></td><td></td></tr>
<tr><td>MGT517</td><td>Managing Security Operations: Detection, Response, and Intelligence <b><i>NEW!</i></b></td><td></td><td></td><td></td><td colspan="5">PAGE 46</td><td></td><td></td><td></td></tr>
<tr><td>DEV522</td><td>Defending Web Applications Security Essentials</td><td></td><td></td><td></td><td colspan="6">PAGE 48</td><td></td><td></td></tr>
<tr><td>DEV531</td><td>Defending Mobile Applications Security Essentials <b><i>NEW!</i></b></td><td></td><td colspan="2">P 53</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>DEV534</td><td>Secure DevOps: A Practical Introduction <b><i>NEW!</i></b></td><td></td><td colspan="2">P 53</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>Core NetWars, DFIR NetWars, and Cyber Defense NetWars</td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="2">P 2</td><td></td><td></td><td></td></tr>
</table>

CONTENTS

Core NetWars Experience 2
DFIR NetWars Tournament 2
Cyber Defense NetWars Competition 2
The Value of SANS Training and You 4
SANS World-Class Instructors. 5
Bonus Sessions 54-55
Vendor-Sponsored Events. 55
DoD Directive 8140 56
SANS Securing The Human. 57
SANS Cyber Guardian Program 57
SANS Technology Institute 58
SANS VetSuccess Immersion Academy 58
SANS Training Formats (Live & Online) . . .59
Future SANS Training Events 60-61
SANS Voucher Program. 62
Hotel Information. 63
Registration Information 64
Registration Fees 65

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. The roadmap is 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

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!

SANS WORLD-CLASS INSTRUCTORS

Chris Christianson
Instructor

@cchristianson

Teaching SEC440

Eric Conrad
Senior Instructor

@eric_conrad

Teaching SEC542

David Cowen
Certified Instructor

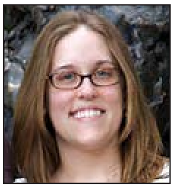
@hecfblog

Teaching FOR408

Christopher Crowley
Principal Instructor

@CCrowMontance

Teaching MGT517



Sarah Edwards
Certified Instructor

@iamevltwin

Teaching FOR518

Jason Fossen
Faculty Fellow

@JasonFossen

Teaching SEC505

Bryce Galbraith
Principal Instructor

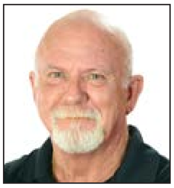
@brycegalbraith

Teaching SEC560 & SEC580

G. Mark Hardy
Certified Instructor

@g_mark

Teaching MGT512



Paul A. Henry
Senior Instructor

@phenrycissp

Teaching SEC501

David Hoelzer
Faculty Fellow

@it_audit

Teaching SEC503 & MGT305

Eric Johnson
Certified Instructor

@emjohn20

Teaching DEV531

Frank Kim
Certified Instructor

@fykim

Teaching MGT514 & DEV534

Rob Lee
Faculty Fellow

@robtlee @sansforensics

Teaching FOR508

David R. Miller
Certified Instructor

@DRM_CyberDude

Teaching MGT414

Seth Misenar
Senior Instructor

@sethmisenar

Teaching SEC511

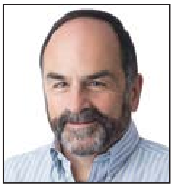
Jorge Orchilles
Instructor

Teaching SEC524

Keith Palmgren
Senior Instructor

@kpalmgren

Teaching SEC301



John Pescatore
Instructor

@john_pescatore

Bonus Session Keynote

Dave Shackleford
Senior Instructor

@daveshackleford

Teaching SEC579

Bryan Simon
Certified Instructor

@BryanOnSecurity

Teaching SEC401

Stephen Sims
Senior Instructor

@Steph3nSims

Teaching SEC660

Lance Spitzner
Certified Instructor

@lspitzner

Teaching MGT433

John Strand
Senior Instructor

@strandjs

Teaching SEC504

James Tarala
Senior Instructor

@isaudit

Teaching SEC566 & MGT415

Johannes Ullrich, PhD
Senior Instructor

@johullrich

Teaching SEC546 & DEV522

Jake Williams
Certified Instructor

@MalwareJake

Teaching FOR578

Joshua Wright
Senior Instructor

@joswr1ght

Teaching SEC575

SEC301

Intro to Information Security

ALSO AVAILABLE VIA SIMULCAST

See page 64 for details.

SANS

Five-Day Program
Thu, May 11 - Mon, May 15
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Keith Palmgren

GIAC INFORMATION SECURITY FUNDAMENTALS GISF

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
- Understand incident response, business continuity, and disaster recovery planning at an introductory level
- Access a number of websites to better understand password security, encryption, phishing, browser security, etc.

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

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

SEC401 Security Essentials Bootcamp Style

SANS

Six-Day Program
Thu, May 11 - Tue, May 16
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
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

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

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 who has been working in the information technology and security field since 1991. Over the course of his career, Bryan has held various technical and managerial positions in the education, environmental, accounting, and financial services sectors. Bryan speaks on a regular basis at international conferences and with the press on matters of cybersecurity. He has instructed individuals from the FBI, NATO, and the UN in matters of cybersecurity, on two continents. Bryan has specialized expertise in defensive and offensive capabilities. He has received recognition for his work in IT security, and was most recently profiled by McAfee (part of Intel Security) as an IT Hero. Bryan holds 12 GIAC certifications including GISF, 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

You Will Be Able To

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

"This course has been the best training I have ever taken from an instructor with the knowledge and ability to teach the material."

-Joe Lordi, Wawa

"This course is an eye opener for anyone who cares about securing their information today!"

-Don Cervone, Bridgewater Associates

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

SEC501 Advanced Security Essentials – Enterprise Defender

SANS

Six-Day Program
Thu, May 11 - Tue, May 16
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Paul A. Henry

GIAC CERTIFIED ENTERPRISE DEFENDER GCED

www.giac.org/gced

SANS Technology Institute

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.

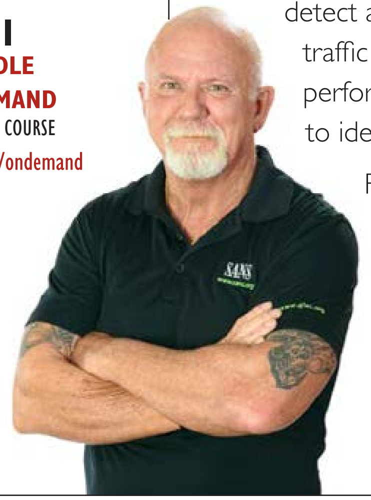
It has been said of security that "prevention is ideal, but detection is a must." However, detection without response has little value. Network security needs to be constantly improved to prevent as many attacks as possible and to swiftly detect and respond appropriately to any breach that does occur. 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.

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 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

Paul A. Henry *SANS Senior Instructor*

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

501.1 HANDS ON: Defensive Network Infrastructure

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

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

501.2 HANDS ON: Packet Analysis

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

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

501.3 HANDS ON: Pentest

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

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

501.4 HANDS ON: First Responder

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

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

501.5 HANDS ON: Malware

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

Topics: Malware; Microsoft Malware; External Tools and Analysis

501.6 HANDS ON: Data Loss Prevention

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

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

You Will Be Able To

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

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

-Brett Smetanka, KeyBank

"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

SEC503 Intrusion Detection In-Depth

SANS

Six-Day Program
Thu, May 11 - Tue, May 16
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: David Hoelzer

www.giac.org/gcia

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

Who Should Attend

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

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

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

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

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

David Hoelzer *SANS Faculty Fellow*

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

503.1 HANDS ON: Fundamentals of Traffic Analysis: PART 1

Day 1 provides a refresher or introduction to TCP/IP, depending on your background, covering the essential foundations such as the TCP/IP communication model, theory of bits, bytes, binary and hexadecimal, an introduction to Wireshark, the IP layer, and both IPv4 and IPv6 and packet fragmentation in both. We describe the layers and analyze traffic not just in theory and function, but from the perspective of an attacker and defender.

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

503.2 HANDS ON: Fundamentals of Traffic Analysis: PART 2

Day 2 continues where Day1 ended in understanding TCP/IP. Two essential tools – Wireshark and tcpdump – are explored to give you the skills to analyze your own traffic. The focus of these tools on Day 2 is filtering traffic of interest in Wireshark using display filters and in tcpdump using Berkeley Packet Filters. We proceed with our exploration of the TCP/IP layers covering TCP, UDP, and ICMP. Once again, we describe the layers and analyze traffic not just in theory and function, but from the perspective of an attacker and defender.

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

503.3 HANDS ON: Application Protocols and Traffic Analysis

Day 3 culminates the examination of TCP/IP with an exploration of the application protocol layer. The concentration is on some of the most widely used, and sometimes vulnerable, crucial application protocols – HTTP, SMTP, DNS, and Microsoft communications. Our focus is on traffic analysis, a key skill in intrusion detection.

Topics: Advanced Wireshark; Detection Methods for Application Protocols; Microsoft Protocols; HTTP; SMTP; DNS; 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

> "This course has really given me a deep insight into the mindset of an analyst."
>
> -Seth Phillips, Alert Logic

> "The concepts learned in SEC503 helped me bridge a gap in knowledge of what we need to better protect our organization."
>
> -Greg Thys, Mary Greeley Medical Center

> "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

SEC504

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Thu, May 11 - Tue, May 16
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

ALSO AVAILABLE VIA SIMULCAST

See page 64 for details.

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

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

"If you love cybersecurity and learning how exploits work, you NEED this course." -Jaid K., U.S. Navy

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

"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.

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

John Strand *SANS Senior Instructor*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

504.6 HANDS ON: Hacker Tools Workshop

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

Topics: Hands-on Analysis

You Will Be Able To

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

SEC505

Securing Windows and PowerShell Automation

SANS

Six-Day Program
Thu, May 11 - Tue, May 16
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jason Fossen

GIAC CERTIFIED WINDOWS SECURITY ADMINISTRATOR GCWN
www.giac.org/gcwn

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

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

▶❙❙ **Bundle OnDemand** WITH THIS COURSE
www.sans.org/ondemand

Who Should Attend

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

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.

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

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

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

If you are an IT manager or CIO, the aim for this course is to have it pay for itself 10 times over within two years, because automation isn't just good for SecOps/DevOps, it can save money, too. 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 the NSA Top 10 Mitigations and the CIS Critical Security Controls related to Windows, especially the ones that are difficult to implement in large environments.

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

"Really great course for anyone involved in the administration or securing of Windows environments." -David Hazar, Oracle

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

SEC511

Continuous Monitoring and Security Operations

New Extended Bootcamp Hours to Enhance Your Skills

Six-Day Program
Thu, May 11 - Tue, May 16
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Seth Misenar

www.giac.org/gmon

www.sans.edu

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

Who Should Attend

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

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

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

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

> "This [course] is a must for anyone responsible for monitoring networks for security."
>
> -Brad Milhorn, CompuCom

SEC542 Web App Penetration Testing and Ethical Hacking

SANS

ALSO AVAILABLE VIA SIMULCAST

See page 64 for details.

Six-Day Program
Thu, May 11 - Tue, May 16
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Eric Conrad

GIAC WEB APPLICATION PENETRATION TESTER GWAPT
www.giac.org/gwapt

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

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

Who Should Attend

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

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

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

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

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

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

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

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

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

"The best content and best training I have attended!" -Viswanath.S.Ch., GEMALTO

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

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

> "SEC542 is a step-by-step introduction to testing and penetrating web applications — a must for anyone who builds, maintains, or audits web systems."
>
> -Brad Milhorn, ii2P LLC

SEC560

Network Penetration Testing and Ethical Hacking

Six-Day Program
Thu, May 11 - Tue, May 16
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Bryce Galbraith

www.giac.org/gpen

www.sans.edu

www.sans.org/cyber-guardian

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

ALSO AVAILABLE VIA SIMULCAST

See page 64 for details.

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.

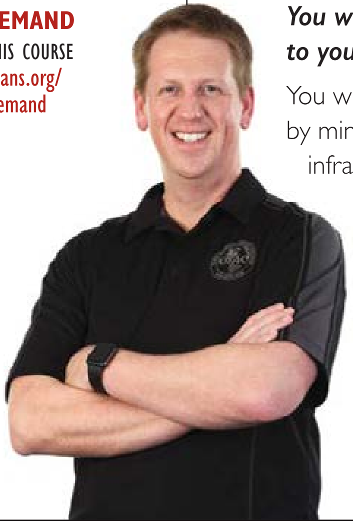
SEC560 is designed to get you ready to conduct a full-scale, high-value penetration test – and on the last day of the course you'll do just that. After building your skills in comprehensive and challenging labs over five days, the course culminates with a final full-day, real-world penetration test scenario. 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.

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



"I am relatively new to the field. This is hands down the best training I have seen."
-Brandon, Stalwart Systems

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

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 love the technical depth and breadth of the material."
>
> -Eric Robinson, Premera Blue Cross

SEC566

Implementing and Auditing the Critical Security Controls – In-Depth

SANS

Five-Day Program
Thu, May 11 - Mon, May 15
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: James Tarala

GIAC CRITICAL CONTROLS CERTIFICATION
GCCC

www.giac.org/gccc

SANS Technology Institute

www.sans.edu

▶❚❚ **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.

Who Should Attend

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

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

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

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

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

James Tarala *SANS Senior Instructor*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

"Practical priorities for real IT security."

-Zak Jones, Bloomberg LP

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

"This course provides direction and metrics for evaluating an organization's system." -Anthony Clarke, Marion County Public Schools

"Amazing course. Learn about what you need to do to secure your organization."

-Mike Rinkel, Calgary Board of ED

SEC575

Mobile Device Security and Ethical Hacking

SANS

Six-Day Program
Thu, May 11 - Tue, May 16
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Joshua Wright

GMOB

www.giac.org/gmob

SANS Technology Institute

www.sans.edu

▶❚❚ **BUNDLE ONDEMAND** WITH THIS COURSE

www.sans.org/ondemand

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

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.

Joshua Wright *SANS Senior Instructor*

Joshua Wright is a senior technical analyst with Counter Hack, a company devoted to the development of information security challenges for education, evaluation, and competition. Through his experiences as a penetration tester, Josh has worked with hundreds of organizations on attacking and defending mobile devices and wireless systems, ethically disclosing significant product and protocol security weaknesses to well-known organizations. As an open-source software advocate, Josh has conducted cutting-edge research resulting in several software tools that are commonly used to evaluate the security of widely deployed technology targeting WiFi, Bluetooth, and ZigBee wireless systems, smart grid deployments, and the Android and Apple iOS mobile device platforms. As the technical lead of the innovative CyberCity, Josh also oversees and manages the development of critical training and educational missions for cyber warriors in the U.S. military, government agencies, and critical infrastructure providers. @joshwr1ght

575.1 HANDS ON: Device Architecture and Common Mobile Threats

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

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

575.2 HANDS ON: Mobile Platform Access and Application Analysis

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

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

575.3 HANDS ON: Mobile Application Reverse Engineering

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

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

575.4 HANDS ON: Penetration Testing Mobile Devices – PART 1

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

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

575.5 HANDS ON: Penetration Testing Mobile Devices – PART 2

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

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

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

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

> "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.

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.

SEC579

Virtualization and Software-Defined Security

SANS

NEW!

Five-Day Program
Thu, May 11 - Mon, May 15
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Dave Shackleford

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

-Scott Towery, Visions

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

-Joe Marshall, Exelon

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

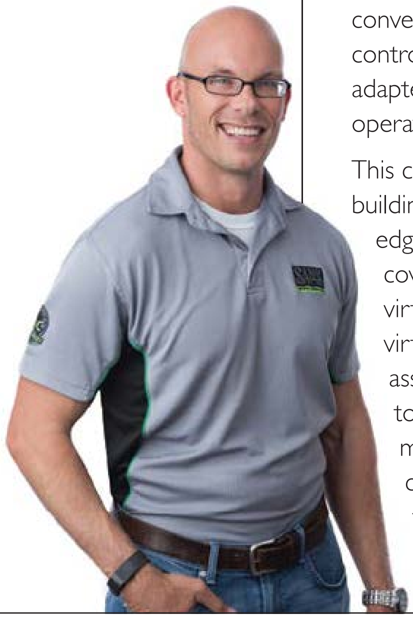
One of today's most rapidly evolving and widely deployed technologies is server virtualization. **SEC579: Virtualization and Software-Defined Security** is intended to help security, IT operations, and audit and compliance professionals build, defend, and properly assess both virtual and converged infrastructures,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

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

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

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

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



Dave Shackleford *SANS Senior Instructor*

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

579.1 HANDS ON: Core Concepts of Virtualization Security

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

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

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

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

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

You Will Be Able To

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

579.3 HANDS ON: Virtualization Threats, Vulnerabilities, and Attacks

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

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

579.4 HANDS ON: Defending Virtualization and Software-Defined Technologies

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

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

579.5 HANDS ON: Virtualization Operations, Auditing, and Monitoring

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

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

> "SEC579 is the absolute best virtualization security information available! And it is immediately usable."
>
> -Leonard Lyons, Northrop Grumman

SEC660

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Six-Day Program
Thu, May 11 - Tue, May 16
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Stephen Sims

www.giac.org/gxpn

www.sans.edu

www.sans.org/cyber-guardian

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

Who Should Attend

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

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.**

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

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

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

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; Using ROP; Building ROP Chains to Defeat DEP and Bypass ASLR; Windows 7 and 8; Porting Metasploit Modules; Client-side Exploitation; Windows Shellcode

660.6 HANDS ON: Capture the Flag Challenge

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

FOR408

Windows Forensic Analysis

Six-Day Program
Thu, May 11 - Tue, May 16
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: David Cowen

GCFE
www.giac.org/gcfe

SANS Technology Institute
www.sans.edu

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

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

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

David Cowen *SANS Certified Instructor*

David Cowen is a Partner at G-C Partners, LLC, where his team of expert digital forensics investigators pushes the boundaries of what is possible on a daily basis. He has been working in digital forensics and incident response since 1999 and has performed investigations covering thousands of systems in the public and private sector. Those investigations have involved everything from revealing insider threats to serving as an expert witness in civil litigation and providing the evidence to put cyber criminals behind bars. David has authored three series' of books on digital forensics: *Hacking Exposed Computer Forensics* (1st-3rd editions); *Infosec Pro Guide to Computer Forensics*; and the *Anti Hacker Toolkit* (3rd Edition). His research into file system journaling forensics has created a new area of analysis that is changing the industry. Combined with Triforce products, David's research enables examiners to go back in time to find previously unknown artifacts and system interactions. David is a Certified Information Systems Security Professional (CISSP) and a GIAC Certified Forensic Examiner. He is the winner of the first SANS DFIR NetWars and a SANS Lethal Forensicator whose passion for digital forensics can be seen in everything he does. He started in 1996 as a penetration tester and has kept up his information security knowledge by acting as the Red Team captain for the National Collegiate Cyber Defense Competition for the last nine years. @hecfblog

408.1 HANDS ON: Windows Digital Forensics and Advanced Data Triage

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

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

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

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

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

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

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

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

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

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

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

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

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

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

408.6 HANDS ON: Windows Forensic Challenge

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

Topics: Digital Forensic Case; Windows 7 Forensic Challenge

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

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

FOR508 Advanced Digital Forensics, Incident Response, and Threat Hunting

SANS

NEWLY UPDATED!

Six-Day Program
Thu, May 11 - Tue, May 16
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Rob Lee

GIAC CERTIFIED FORENSIC ANALYST GCFA
www.giac.org/gcfa

SANS Technology Institute
www.sans.edu

sapere aude
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, Incident Response, and Theat Hunting will help you to:

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

Who Should Attend

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

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

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

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

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

"Excellent course and delivery. I have learned a great deal and look forward to using these skills at my job." -Helen B., Royal Navy

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

Rob Lee *SANS Faculty Fellow*

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

508.1 HANDS ON: Advanced Incident Response and Threat Hunting

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

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

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

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

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

508.3 HANDS ON: Intrusion Forensics

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

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

508.4 HANDS ON: Timeline Analysis

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

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

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

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

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

You Will Be Able To

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

508.6 HANDS ON: The APT Incident Response Challenge

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

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

FOR518 Mac Forensic Analysis

SANS

Six-Day Program
Thu, May 11 - Tue, May 16
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

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."

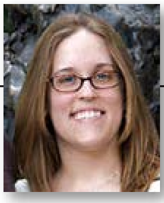
-Kevin J. Ripa, Computer Evidence Recovery, Inc.

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, and FOR585 alumni looking to round out their forensic skills



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

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

> "Best Mac forensics course available."
>
> -David Klopp, JPMorgan Chase

FOR578

Cyber Threat Intelligence

SANS

Five-Day Program
Thu, May 11 - Mon, May 15
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Jake Williams

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

-Thomas L., USAF

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

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.

"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.

THERE IS NO TEACHER BUT THE ENEMY!

Jake Williams *SANS Certified Instructor*

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

578.1 HANDS ON: Cyber Threat Intelligence

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

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

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

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

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

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

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

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

578.4 HANDS ON: Operational Threat Intelligence: Sharing Intelligence

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

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

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

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

MGT414

SANS Training Program for CISSP® Certification

SANS

Six-Day Program
Thu, May 11 - Tue, May 16
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

GIAC Information Security Professional GISP

www.giac.org/gisp

MEETS DoDD 8140
(8570) REQUIREMENTS

www.sans.org/8140

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

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

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

Who Should Attend

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

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

> "This course teaches you everything you need to prepare and defend your network. A must-do for all blue teams."
>
> -Brad Milhorn, CompuCom

> "This course will open eyes by sharing real experiences and ways to defend."
>
> -Jeff Fiser, Symc

> "SANS does it again. An excellent course for those looking to lead their companies through the next stage of security evolution."
>
> -Travis Anderson, PGE

Take advantage of SANS' CISSP® Get Certified Program currently being offered.
www.sans.org/cissp

David R. Miller *SANS Certified Instructor*

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

414.1 Introduction; Security and Risk Management

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

Topics: Overview of CISSP® Certification; Introductory Material; Overview of the 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)

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

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

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

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

414.4 Identity and Access Management

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

Topics: Domain 5: Identity and Access Management

414.5 Security Assessment and Testing; Security Operations

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

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

414.6 Software Development Security

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

Topics: Domain 8: Software Development Security

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

-Eric Pavlov, Innomark

MGT512

SANS Security Leadership Essentials for Managers with Knowledge Compression™

SANS

Five-Day Program
Thu, May 11 - Mon, May 15
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop Recommended
Instructor: G. Mark Hardy

GIAC Security Leadership Certification GSLC

www.giac.org/gslc

SANS Technology Institute

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.

Who Should Attend

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

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

Knowledge Compression™

Maximize your learning potential!

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

G. Mark Hardy *SANS Certified Instructor*

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

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

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

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

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

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

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

512.3 Secure Communications

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

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

You Will Be Able To

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

512.4 The Value of Information

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

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

512.5 Management Practicum

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

Topics: The Mission; Globalization; IT Business and Program Growth; Security and Organizational Structure; 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.

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

-David Stewart, ADM

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

-Manuel M., U.S. Army

"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.

MGT514

IT Security Strategic Planning, Policy, and Leadership

SANS

Five-Day Program
Thu, May 11 - Mon, May 15
9:00am - 5:00pm
30 CPEs
Laptop NOT Needed
Instructor: Frank Kim

SANS Technology Institute
www.sans.edu

▶❚❚ **Bundle OnDemand**
WITH THIS COURSE
www.sans.org/ondemand

"Excellent training with encyclopedia coverage of the topic.

-Alexander Kotkov, Ernst and Young

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

This course teaches security professionals how to do three things:

Develop Strategic Plans

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

Create Effective Information Security Policy

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

Develop Management and Leadership Skills

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

Who Should Attend

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

How the Course Works

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

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

Frank Kim *SANS Certified Instructor*

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

514.1 Strategic Planning Foundations

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

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

514.2 Strategic Roadmap Development

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

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

514.3 Security Policy Development and Assessment

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

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

514.4 Leadership and Management Competencies

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

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

514.5 Strategic Planning Workshop

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

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

> "This training was valuable because it helped me examine myself from an outside point of view."
>
> -DJ, Zoetis

You Will Be Able To

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

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

> "Really good case studies and examples which prompted useful class discussion."
>
> -Alexis Brownings, CERT-UK

> "This is a great foundational course as we realize the importance of bringing a business perspective to security."
>
> -Nairobi Kim, Wells Fargo

MGT517 Managing Security Operations: Detection, Response, and Intelligence

SANS

NEW!

Five-Day Program
Thu, May 11 - Mon, May 15
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Christopher Crowley

> "Chris is a fantastic instructor – great pacing with engaging anecdotes and was very insightful."
>
> -Rich Savacool, Nixon Peabody

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

Who Should Attend

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

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

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

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

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

Christopher Crowley *SANS Principal Instructor*

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

517.1 HANDS ON: Design the Security Operations Center

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

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

517.2 HANDS ON: Build the Security Operations Center

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

Topics: Governance Structure; Process Engineering; Technical Components

517.3 HANDS ON: Operate and Mature the Security Operations Center

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

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

517.4 HANDS ON: Incident Response Management – PART I

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

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

517.5 HANDS ON: Incident Response Management – PART II

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

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

You Will Be Able To

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

Author Statement

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

-Chris Crowley

DEV522

Defending Web Applications Security Essentials

SANS

Six-Day Program
Thu, May 11 - Tue, May 16
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Johannes Ullrich, Ph.D.

GIAC CERTIFIED WEB APPLICATION DEFENDER
GWEB
www.giac.org/gweb

SANS Technology Institute
www.sans.edu

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

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

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

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

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

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

"DEV522 goes over security issues that every web developer and appsec employee needs."
-Allen Ott, Boeing

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.

Johannes Ullrich, Ph.D. *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. He founded DShield.org in 2000, 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

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

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

SEC440

Critical Security Controls: Planning, Implementing, and Auditing

Two-Day Course | Wed, May 17 - Thu, May 18 | 9:00am - 5:00pm | 12 CPEs | Laptop NOT Needed | Instructor: Chris Christianson

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. 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.

"SEC440 provides an excellent prioritized approach to IT security." -Darrell Bateman, Texas Tech

SEC524

Cloud Security Fundamentals

Two-Day Course | Wed, May 17 - Thu, May 18 | 9:00am - 5:00pm | 12 CPEs | Laptop Required | Instructor: Jorge Orchilles

Who Should Attend

- Security personnel
- Network and systems administrators
- Technical auditors and consultants
- Security and IT managers

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

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

SEC546
IPv6 Essentials

Two-Day Course | Wed, May 17 - Thu, May 18 | 9:00am - 5:00pm | 12 CPEs | Laptop Required | Instructor: Johannes Ullrich, Ph.D.

We are out of IPv4 addresses. ISPs worldwide will have to rapidly adopt IPv6 in the years ahead in order to grow, particularly because mobile devices require more and more address space. Already, modern operating systems implement IPv6 by default. Windows 7, for example, ships with Teredo enabled by default. This course is designed not just for implementers of IPv6, but also for those who just need to learn how to detect IPv6 and defend against threats unintentional IPv6 use may bring about.

IPv6 is currently being implemented rapidly in Asia in response to the exhaustion of IPv4 address space, which is most urgently felt in fast-growing networks in China and India. Even if you do not feel the same urgency of IP address exhaustion, you may have to connect to these IPv6 resources as they become more important to global commerce.

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

SEC580
Metasploit Kung Fu for Enterprise Pen Testing

Two-Day Course | Wed, May 17 - Thu, May 18 | 9:00am - 5:00pm | 12 CPEs | Laptop Required | Instructor: Bryce Galbraith

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

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

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

MGT305

Technical Communication and Presentation Skills for Security Professionals

One-Day Course | Wed, May 17 | 9:00am - 5:00pm | 6 CPEs | Laptop Required | Instructor: David Hoelzer

This course is designed for every IT professional in your organization. In this course we cover the top techniques that will show you how to research and write professional quality reports, and how to create outstanding presentation materials. Attendees will also get a crash course on advanced public speaking skills. Writing reports is a task that many IT professionals struggle with, sometimes from the perspective of writing the report and other times from the perspective of having to read someone else's report! In the morning material, we cover step by step how to work through the process of identifying critical ideas, how to properly research them, how to develop a strong argument in written form, and how to put it all down on paper. How do you transform an excellent report into a powerful presentation? We will work through a process that serves to either condense a report into a presentation or can even be used to write a presentation from scratch that communicates your important thoughts in a meaningful and interesting way.

SANS Technology Institute
www.sans.edu

MGT415

A Practical Introduction to Cybersecurity Risk Management

Two-Day Course | Wed, May 17 - Thu, May 18 | 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.

Who Should Attend:

- Security engineers, compliance directors, managers, and auditors — basically any SANS alumni
- Auditors
- Directors of security compliance
- Information assurance managers
- System administrators

MGT433

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

Two-Day Course | Wed, May 17 - Thu, May 18 | 9:00am - 5:00pm | 12 CPEs | Laptop NOT Needed | Instructor: Lance Spitzner

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

SANS Technology Institute
www.sans.edu

Who Should Attend:

- Security awareness officers
- Chief security officers and security management officials
- Security auditors, and governance and compliance officers
- Training, human resources, and communications staff
- Representatives from organizations regulated by industries such as HIPAA, FISMA, FERPA, PCI-DSS, ISO/IEC 27001 SOX, NERC, or any other compliance-driven standard
- Anyone involved in planning, deploying or maintaining a security awareness program

NEW!

DEV531

Defending Mobile Applications Security Essentials

Two-Day Course | Tue, May 9 - Wed, May 10 | 9:00am - 5:00pm | 12 CPEs | Laptop Required | Instructor: Eric Johnson

Mobile application development is growing exponentially year over year. As of late 2015, over 3 million apps were deployed in the Apple and Google app stores. These apps are consumed by over 700 million users world-wide and account for 33% of the traffic on the Internet. Average users have over 100 mobile apps installed on their device, many of which provide business-critical services to customers and employees.

Unfortunately, these apps are often rushed to market to gain a competitive advantage with little regard for security. As seen in web applications for the past 20 years, software vulnerabilities always exist where code is being written and mobile apps are no different. Mobile apps are vulnerable to a whole new class of vulnerabilities, as well as most traditional issues that have long plagued web and desktop applications. This problem will only continue to grow unless managers, architects, developers, and QA teams learn how to test and defend their mobile apps.

DEV531: Defending Mobile Applications Security Essentials covers the most prevalent mobile app risks, including those from the OWASP Mobile Top 10. Students will participate in numerous hands-on exercises available in both the Android and iOS platforms. Each exercise is designed to reinforce the lessons learned throughout the course, ensuring that you understand how to properly defend your organization's mobile applications.

Who Should Attend:

- Mobile application developers
- Mobile app development managers
- Mobile app architects
- Quality assurance testers
- Penetration testers who are interested in mobile app defensive strategies
- Auditors who need to understand mobile app risks and defensive controls
- Application security managers

NEW!

DEV534

Secure DevOps: A Practical Introduction

Two-Day Course | Tue, May 9 - Wed, May 10 | 9:00am - 5:00pm | 12 CPEs | Laptop Required | Instructor: Frank Kim

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

The course will explain how secure DevOps can be implemented, using lessons from successful DevOps security programs. Students will build up a DevOps CI/CD toolchain and learn how code is automatically built, tested, and deployed, using popular open-source tools including git, Puppet, Jenkins and Docker. In a series of labs, students will inject security into a CI/CD toolchain and learn about the tools, patterns, and techniques to do this.

The course will make extensive use of open-source materials and tooling for automated configuration management (Infrastructure as Code), Continuous Integration, Continuous Delivery and Continuous Deployment, containerization and micro-segmentation, and automated compliance (Compliance as Code) and monitoring.

Who Should Attend:

- Developers, software architects, operations engineers, and system admins working in a DevOps environment or transitioning to a DevOps environment who want to understand how and where to add security checks, testing and other controls
- Security analysts, security engineers, auditors and risk managers, security consultants, and pen testers who want to understand how to adapt security practices to DevOps and Continuous Delivery

You Will Learn:

- Foundations and principles of DevOps, Continuous Delivery, and Continuous Deployment
- The security risks and challenges that DevOps introduces
- The keys to successful DevOps security programs
- How to build security into Continuous Delivery and Continuous Deployment
- The tools, patterns, and techniques of security automation in DevOps
- How to secure your build and deployment environment and tool chain
- How to leverage Infrastructure as Code for secure configuration management and provisioning
- How manual security practices (risk assessments, audits and pen tests) can be adapted to continuously changing environments, and the important role that they still play
- Security risks and challenges that containers introduce — and how to secure container technology
- How to automate compliance in DevOps, using the DevOps Audit Defense Toolkit

BONUS SESSIONS

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

EMERGING TRENDS IN CYBERSECURITY

KEYNOTE:

Emerging Trends in Cybersecurity – 2020 Outlook

John Pescatore

SANS Director of Emerging Security will take a data- and analytics-based approach to forecasting the major security trends that will impact cybersecurity professionals over the remainder of this decade. SANS will solicit inputs on social media before the session, and the session will include audience participation to add a crowd-sourced element to the predictions. There may also be a surprise speaker or two. Come learn what changes in threats, technology, regulations, and job markets will impact your future in cybersecurity.

Stop Hitting Yourself: Common Mistakes in Security Operations

Jake Williams

Ever work in a security operation where it felt like you were constantly shooting yourself in the foot? I have, and I can't help but think of siblings torturing one another while saying "stop hitting yourself." But that's what we deal with regularly in infosec. Whether we realize it or not, we utilize intelligence in security operations every day – whether in incident response, intrusion detection, or hunt team operations. However, many in security are not formally trained in intelligence operations and don't properly understand gain/loss calculations. This lack of understanding leads to mistakes in how intelligence is used, often exposing our sensitive collection to the adversary and adversely impacting security operations. In this session, you will learn about how to maximize the value of your intelligence using real-world case studies. Armed with the knowledge of how to better use intelligence for security operations, you'll take your security operations to a whole new level.

How to Commit Card Fraud

G. Mark Hardy

Well, we're not going to show you how to commit fraud, but we will show you how the bad guys do it and how you can protect yourself and your business. We'll take a look into the "dark web" and see how these big card heists are pulled off, why chip-and-pin won't solve the fraud problem, and why payment technologies like Apple Pay pose new risks. You'll learn the ecosystem of fraud, and how it's become a big business that costs banks and merchants over $16 billion annually. See if your bank even bothers to use the security protections it could – we'll have a mag stripe card reader so you can really see what's in your wallet. Certified SANS Instructor G. Mark Hardy is the CEO and founder of CardKill Inc., a start-up that helps banks preemptively kill stolen cards BEFORE they are used in fraud.

Cyber-Hygiene and Standards of Care: Practical Defenses Against Advanced Attacks

James Tarala

There is no question that organizations are struggling to stop attacks. Yet hackers are not magic, though we pretend that they are and that special secret knowledge is required to stop them. In this presentation, James Tarala, contributor to the CIS Critical Security Controls, will discuss standards of cybersecurity care and why the CIS Critical Security Controls are quickly becoming the standard of cybersecurity care for organizations. He will also share practical tips for implementing these controls and overcoming the barriers to implementation. Attendees should expect to leave the presentation with practical advice for using these controls to stop even the most advanced attacks in their organization.

Sarah's Apple Orchard

Sarah Edwards

This talk series will feature freshly picked topics pertaining to Apple-specific digital forensics. Topics may be from the smallest seedling like a recent subject in current news to something that has been baking for a while that requires advanced forensic analysis. These talks will get at the core of many Apple technologies in a wide variety of areas within software and hardware. Any juicy and delicious topic is fair game in Sarah's Apple Orchard.

The 14 Absolute Truths of Security

Keith Palmgren

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

Ten Tenets of CISO Success

Frank Kim

The era of CISO-as-dictator is at an end. The increased importance of cybersecurity as a vital component of business growth requires security leaders to find new ways to work with executive leaders, business partners, and their own team members. Learn 10 tenets that CISOs and security leaders can utilize to go beyond technical skills, successfully lead organizations through change, and ultimately get to "yes" with the business.

A Hunting We Shall Go

John Strand

Lets build a threat hunting kit, for free!! In this presentation, John Strand will go through some tools and tactics we can all use to help find the bad guys who bypass all our shiny security tools. We will also cover some new techniques bad guys are using to bypass these traditional defenses.

Blue is the New Red

Panelists: Stephen Sims, Eric Conrad, Seth Misenar, Bryan Simon, and Bryce Galbraith

So much focus has been on penetration testing over the last few years that the world would have you believe that we're in desperate need of thousands of penetration testers to fill countless open job requisitions. Truth be told, the majority of professionals seeking to build their skills in offensive techniques are Enterprise Defenders! In this panel discussion we will talk to both offensive and defensive experts about this perception, where we are lacking in expertise, and techniques that can be used to improve your organization's defense.

Windows Exploratory Surgery with Process Hacker

Jason Fossen

In this talk we'll rummage around inside the guts of Windows while on the lookout for malware, using a free tool named Process Hacker (similar to Process Explorer). Understanding processes, threads, drivers, handles, and other OS internals is important for analyzing malware, doing forensics, troubleshooting, and hardening the OS. If you have a laptop, get Process Hacker from SourceForge.net and together we'll take a peek under the GUI to learn about Windows internals and how to use Process Hacker for combating malware (**http://processhacker.sourceforge.net**).

Vendor-Sponsored Events

Vendor Expo

Friday, May 12

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

Friday, May 12

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 Security West 2017, vendors will provide sponsored lunch presentations where attendees can interact with peers and learn about vendor solutions. Take a break and get up-to-date on security technologies!

Department of Defense Directive 8140

(DoDD 8570)

www.sans.org/dodd-8140

Department of Defense Directive 8570 has been replaced by the DoD CIO as DoDD 8140; DoDD 8570 is now a 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.

DoD Baseline IA Certifications

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

Computer Network Defense (CND) Certifications

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

Information Assurance System Architecture & Engineering (IASAE) Certifications

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

Computer Environment (CE) Certifications

GCWN	**GCUX**

Compliance/Recertification:

To stay compliant with DoDD 8570 requirements, you must maintain your certifications. GIAC certifications are renewable every four years.

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

DoDD 8570 certification requirements are subject to change, please visit http://iase.disa.mil/eta/iawip for the most updated version.

For more information, contact us at 8140@sans.org or visit www.sans.org/dodd-8140

SANS Training Courses for DoDD-Approved Certifications

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

Security Awareness Training by the Most Trusted Source

Computer-based Training for Your Employees

End User
CIP
ICS Engineers
Developers
Healthcare

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

Visit SANS Securing The Human at
securingthehuman.sans.org

Phishing | Knowledge Assessments | Culture and Behavior Change | Managed Services

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

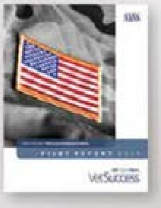
Blue Team Courses

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


SANS
VetSuccess

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

SOUTHERN CALIFORNIA **Anaheim** 2017

February 6-11

SANS ICS SECURITY ORLANDO SUMMIT & TRAINING

Orlando, FL

March 20-27

Scottsdale 2017

February 20-25

Pen Test Austin 2017

March 27-April 1

Dallas 2017

February 27-March 4

SANS 2017

Orlando, FL | April 7-14

San Jose 2017

March 6-11

SILICON VALLEY

Threat Hunting & **Incident Response**

SANS DFIR | Summit & Training

New Orleans, LA | April 18-25

Tysons Corner SPRING 2017

McLean, VA | March 20-25

Baltimore Spring 2017

April 24-29

FUTURE SANS TRAINING EVENTS

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

SANS

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

www.sans.org/vouchers

VOUCHER PROGRAM

Training Investment & Bonus Funds

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

The investment and bonus funds:

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

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

Flexibility & Control

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

With the SANS Admin Tool, the Administrator can:

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

Getting Started

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

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

By creating a Voucher Account, your organization can:

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

HOTEL INFORMATION

Training Campus

Manchester Grand Hyatt Hotel

One Market Place
San Diego, CA 92101
www.sans.org/event/sans-security-west-2017/location

Discover the vibrant culture and natural beauty of Southern California right outside your door at Manchester Grand Hyatt San Diego. Ideally situated on San Diego Bay between the San Diego Convention Center and the city's popular Seaport Village, this hotel offers a spectacular waterfront resort-like setting, complete with shopping, dining, and entertainment venues. The city comes to life at night – Manchester Grand Hyatt San Diego is within walking distance to restaurants, bars and nightclubs located in the ever popular Gaslamp District.

Hotel features include:

- Location in the heart of Downtown, near Seaport Village, Petco Park, the Convention Center and Gaslamp Quarter
- 4th floor pool deck, 25,000-square-foot rooftop with whirlpools, fire pits and a bay view sundeck
- Pools and StayFit™ Gym, two rooftop pools with private cabanas and a 24-hour fitness center
- A Marilyn Monroe™ Spa, facials, massages, reflexology, and body wraps
- Eight on-site dining options including three recently remodeled restaurants, Top of the Hyatt, Sally's Fish House & Bar, and MARKET | ONE
- Top of the Hyatt, 40th floor lounge with incredible views, cocktails, and light fare

Special Hotel Rates Available

A special discounted rate of $221.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through **April 17, 2017**. To make reservations, please call 619-232-1234 and ask for the SANS group rate or SANS government rate.

Top 5 reasons to stay at the Manchester Grand Hyatt Hotel

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 Manchester Grand Hyatt Hotel, 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 Manchester Grand Hyatt Hotel that you won't want to miss!

5 Everything is in one convenient location!

REGISTRATION INFORMATION

Register online at www.sans.org/security-west

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 **EarlyBird17** when registering early

Pay Early and Save*

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	3-15-17	$400.00	4-5-17	$200.00

*Some restrictions apply. Early-bird discounts do not apply to Hosted courses.

SANS SIMULCAST

To register for a SANS Security West 2017 Simulcast course, please visit www.sans.org/event/security-west-2017/attend-remotely

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, April 19, 2017** – processing fees may apply.

SANS SECURITY WEST 2017 REGISTRATION FEES

Register online at www.sans.org/security-west

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 3-15-17	Paid before 4-5-17	Paid after 4-5-17	Add GIAC Cert	Add OnDemand	Add NetWars Continuous
□ SEC301	Intro to Information Security	$4,730	$4,930	$5,130	□ $689	□ $689	□ $1,199
□ SEC401	Security Essentials Bootcamp Style	$5,510	$5,710	$5,910	□ $689	□ $689	□ $1,199
□ SEC501	Advanced Security Essentials – Enterprise Defender	$5,510	$5,710	$5,910	□ $689	□ $689	□ $1,199
□ SEC503	Intrusion Detection In-Depth	$5,510	$5,710	$5,910	□ $689	□ $689	□ $1,199
□ SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling	$5,510	$5,710	$5,910	□ $689	□ $689	□ $1,199
□ SEC505	Securing Windows and PowerShell Automation	$5,420	$5,620	$5,820	□ $689	□ $689	□ $1,199
□ 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
□ SEC560	Network Penetration Testing and Ethical Hacking	$5,510	$5,710	$5,910	□ $689	□ $689	□ $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 Software-Defined Security ***NEW!***	$4,730	$4,930	$5,130			□ $1,199
□ SEC660	Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	$5,510	$5,710	$5,910	□ $689	□ $689	□ $1,199
□ FOR408	Windows Forensic Analysis	$5,510	$5,710	$5,910	□ $689	□ $689	□ $1,199
□ FOR508	Advanced Digital Forensics, Incident Response, and Threat Hunting	$5,510	$5,710	$5,910	□ $689	□ $689	□ $1,199
□ FOR518	Mac Forensic Analysis	$5,510	$5,710	$5,910		□ $689	□ $1,199
□ FOR578	Cyber Threat Intelligence	$4,730	$4,930	$5,130			□ $1,199
□ MGT414	SANS Training Program for CISSP® Certification	$4,840	$5,040	$5,240	□ $689	□ $689	□ $1,199
□ MGT512	SANS Security Leadership Essentials for Managers with Knowledge Compression™	$5,130	$5,330	$5,530	□ $689	□ $689	□ $1,199
□ MGT514	IT Security Strategic Planning, Policy, and Leadership	$4,730	$4,930	$5,130		□ $689	□ $1,199
□ MGT517	Managing Security Operations: Detection, Response, and Intelligence ***NEW!***	$5,130	$5,330	$5,530			□ $1,199
□ DEV522	Defending Web Applications Security Essentials	$5,420	$5,620	$5,820	□ $689	□ $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	$1,770	$2,360
□ SEC524	Cloud Security Fundamentals	$1,770	$2,360
□ SEC546	IPv6 Essentials	$1,770	$2,360
□ SEC580	Metasploit Kung Fu for Enterprise Pen Testing	$1,770	$2,360
□ MGT305	Technical Communication and Presentation Skills for Security Professionals	$1,030	$1,370
□ MGT415	A Practical Introduction to Cybersecurity Risk Management	$1,770	$2,360
□ MGT433	Securing The Human: How to Build, Maintain & Measure a High-Impact Awareness Program	$1,770	$2,360
□ DEV531	Defending Mobile Applications Security Essentials ***NEW!***	$1,770	$2,360
□ DEV534	Secure DevOps: A Practical Introduction ***NEW!***	$1,770	$2,360
□ SPECIAL	Core NetWars Experience – Tournament Entrance Fee	FREE	$1,520
□ SPECIAL	DFIR NetWars Tournament – Tournament Entrance Fee	FREE	$1,520
□ SPECIAL	Cyber Defense NetWars Competition – Tournament Entrance Fee	FREE	$1,520

EARLY-BIRD DISCOUNTS

Pay for any long course using the code EarlyBird17 at checkout by:
3-15-17 to get $400 OFF* / 4-5-17 to get $200 OFF*

***Early-bird discounts do not apply to Hosted courses.**

Create a SANS Account today to enjoy these FREE resources:

WEBCASTS

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

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

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

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

NEWSLETTERS

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

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

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

OTHER FREE RESOURCES

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

www.sans.org/account

SAVE $400 on SANS Security West 2017 courses!

Register and pay by 3-15-17 (SAVE $400) or 4-5-17 (SAVE $200) – www.sans.org/security-west