



The most trusted source for information security training, certification, and research.

INFORMATION SECURITY TRAINING

Fall 2016 Course Catalog

70+

Extraordinary SANS certified instructors

200+

Live events globally, plus multiple online/distance options



Curricula

Cyber Defense
Detection and Monitoring
Penetration Testing
Incident Response
Digital Forensics

Ethical Hacking
Management, Audit, Legal
Secure Development
ICS/SCADA Security

“Best training I’ve attended. Great material that you can apply immediately.”

- Nik Whitis, AFG

www.sans.org

YOUR SOURCE FOR INFORMATION SECURITY EDUCATION



SANS is the most trusted and by far the largest source of information security training in the world. We offer training through several delivery methods: live and virtual, classroom-style; online at your own pace or webcast with live instruction; guided study with a local mentor, or privately (onsite) at your workplace, where even your most remote colleagues can join in via Simulcast. Our computer security courses are developed by industry leaders in numerous fields, including network security, forensics, audit, security leadership, and application security. Courses are taught by real-world practitioners who are the best at ensuring you not only learn the material, but that you can apply it immediately to your work. In addition to top-notch training, we offer certification through GIAC, an affiliate of the SANS Institute. GIAC is a certification body featuring more than 20 hands-on, technical certifications in information security. We also offer optional Master's Degree programs through SANS Technology Institute graduate school, as well as numerous free security resources including newsletters, whitepapers and webcasts.

Why SANS is the best training and educational investment

- Intensive, hands-on immersion training with the highest-quality courseware in the industry.
- Incomparable course instructors and authors who are industry experts and practitioners fighting the same cyber battles as you and discovering new ways to thwart attacks.
- Training that strengthens a student's ability to achieve a GIAC certification, which is unique in the field of information security certifications because it not only tests a candidate's knowledge, but also the candidate's ability to put that knowledge into practice in the real world.

Course Disciplines

More than 50 courses in the following disciplines:

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

Career Paths

Areas of study:

- Computer Forensics Analyst
- Computer Crime Investigator
- Incident Responder
- Intrusion Analyst
- Malware Analyst
- Penetration Tester
- Security Auditor
- Security Analyst
- Developer
- Security Director

Higher Education

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

- Master of Science Degrees
- Graduate Certificate Programs

Learn more about STI at www.sans.edu

Global Information Assurance Certification (GIAC)

Offers more than 20 certifications in:

- Security
- Software Security
- Management
- Penetration Testing
- Forensics
- Audit
- ICS
- Legal

Learn more about GIAC at www.giac.org

SANS INFORMATION SECURITY TRAINING AND YOUR CAREER ROADMAP

Information Security

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

SAMPLE JOB TITLES

- Cybersecurity analyst
- Cybersecurity engineer
- Cybersecurity architect

TECHNICAL INTRODUCTORY

SEC301
Intro to
Information Security
GISF

CORE

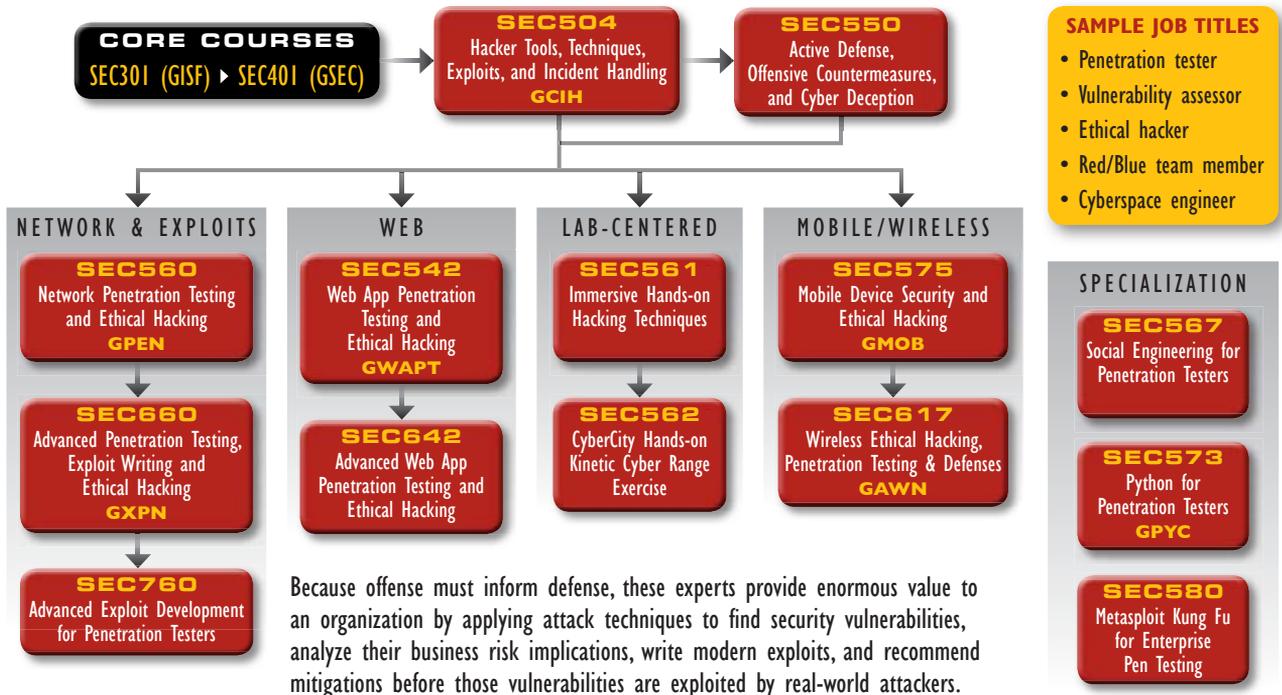
SEC401
Security Essentials
Bootcamp Style
GSEC

IN-DEPTH

SEC501
Advanced Security Essentials
— Enterprise Defender
GCED

CORE COURSES

Penetration Testing/Vulnerability Assessment

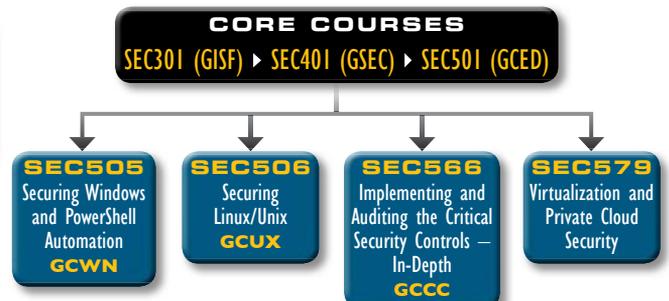


Network Operations Center, System Admin, Security Architecture

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



Security Operations Center/Intrusion Detection

SAMPLE JOB TITLES

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

CORE COURSES

SEC301 (GISF) ▶ SEC401 (GSEC)

SEC504

Hacker Tools, Techniques,
Exploits, and Incident Handling
GCIH

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

ENDPOINT MONITORING

SEC501

Advanced Security Essentials –
Enterprise Defender
GCEd

FOR508

Advanced Digital Forensics
and Incident Response
GCFA

NETWORK MONITORING

SEC503

Intrusion Detection
In-Depth
GCIA

FOR572

Advanced Network
Forensics and Analysis
GNFA

SEC511

Continuous Monitoring and
Security Operations
GMON

SEC550

Active Defense,
Offensive Countermeasures,
and Cyber Deception

THREAT INTELLIGENCE

FOR578

Cyber Threat Intelligence

Risk and Compliance/Auditing/Governance

SEC566

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

AUD507

Auditing &
Monitoring
Networks,
Perimeters, and
Systems
GSNA

LEG523

Law of Data Security
and Investigations
GLEG

MGT433

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

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

SAMPLE JOB TITLES

- Auditor
- Compliance officer

Development – Secure Development

CORE

Securing The Human for Developers

Application Security
Awareness Modules

DEV522

Defending Web Applications
Security Essentials
GWEB

DEV531

Defending Mobile Applications
Security Essentials

DEV534

Secure DevOps:
A Practical Introduction

SECURE CODING

DEV541

Secure Coding
in Java/JEE
GSSP-JAVA

DEV544

Secure Coding
in .NET
GSSP-.NET

DEV543

Secure Coding
in C/C++

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

SPECIALIZATION

SEC542

Web App Pen Testing
and Ethical Hacking
GWAPT

SEC642

Advanced Web App
Pen Testing and
Ethical Hacking

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

ICS456

Essentials for NERC
Critical Infrastructure
Protection

ICS515

ICS Active Defense and
Incident Response

HOSTED

Assessing and
Exploiting Control
Systems

HOSTED

Critical Infrastructure
and Control System
Cybersecurity

Cyber or IT Security Management

SAMPLE JOB TITLES

- CISO
- Cybersecurity manager/officer
- Security director

FOUNDATIONAL

MGT512

SANS Security Leadership Essentials for Managers with Knowledge Compression™
GSLC

MGT525

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

MGT414

SANS Training Program for CISSP® Certification
GISP

CORE

MGT514

IT Security Strategic Planning, Policy, and Leadership

LEG523

Law of Data Security and Investigations
GLEG

MGT415

A Practical Introduction to Cybersecurity Risk Management

MGT535

Incident Response Team Management

SPECIALIZATION

AUD507

Auditing & Monitoring Networks, Perimeters, and Systems
GSNA

SEC566

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

MGT433

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

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.

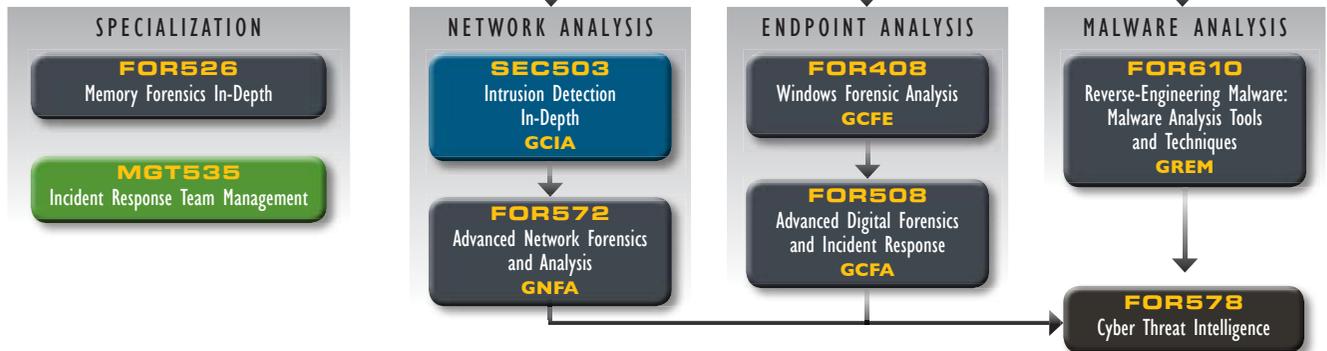
PMP is registered mark of the Project Management Institute, Inc.

Incident Response and Threat Hunting

SAMPLE JOB TITLES

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

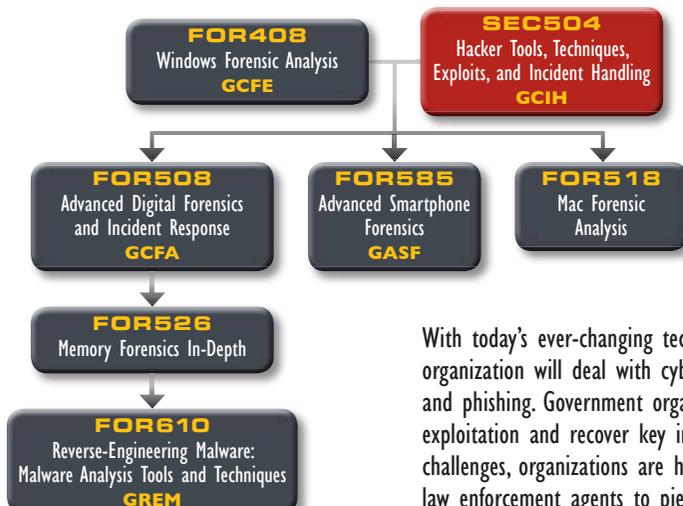
When the security of a system or network has been compromised, the incident responder is the first-line defense during the breach. The responders not only have to be technically astute, they must be able to handle stress under fire while navigating people, processes, and technology to help respond to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



Digital Forensic Investigations and Media Exploitation

SAMPLE JOB TITLES

- Computer crime investigator
- Law enforcement
- Digital investigations analyst
- Media exploitation analyst
- Information technology litigation consultant
- Insider threat analyst



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

The Value of SANS Training and YOU



EXPLORE

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

RELATE

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

VALIDATE

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

SAVE

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

ADD VALUE

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

ALTERNATIVES

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

ACT

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

Return on Investment

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

REMEMBER

the SANS promise:

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

TABLE OF CONTENTS

SANS Information Security Training and Your Career Roadmap.....	Inside Front Cover
The Value of SANS Training and YOU.....	2
SANS World-Class Instructors.....	4
SEC301 Intro to Information Security	6
SEC401 Security Essentials Bootcamp Style	8
SEC501 Advanced Security Essentials – Enterprise Defender	10
SEC503 Intrusion Detection In-Depth	14
SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	16
SEC505 Securing Windows and PowerShell Automation	18
SEC506 Securing Linux/Unix	20
SEC511 Continuous Monitoring and Security Operations	22
SEC542 Web App Penetration Testing and Ethical Hacking	24
SEC550 Active Defense, Offensive Countermeasures, and Cyber Deception	26
SEC562 CyberCity Hands-on Kinetic Cyber Range Exercise	27
SEC560 Network Penetration Testing and Ethical Hacking	28
SEC561 Immersive Hands-On Hacking Techniques	30
SEC566 Implementing and Auditing the Critical Security Controls – In-Depth	32
SEC573 Python for Penetration Testers	34
SEC575 Mobile Device Security and Ethical Hacking <i>NEW!</i>	36
SEC579 Virtualization and Private Cloud Security	38
SEC617 Wireless Ethical Hacking, Penetration Testing, and Defenses	40
SEC642 Advanced Web App Penetration Testing and Ethical Hacking	42
SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	44
SEC760 Advanced Exploit Development for Penetration Testers	46
FOR408 Windows Forensic Analysis	48
FOR508 Advanced Digital Forensics and Incident Response	50
FOR518 Mac Forensic Analysis	52
FOR526 Memory Forensics In-Depth	54
FOR572 Advanced Network Forensics and Analysis	56
FOR578 Cyber Threat Intelligence <i>NEW!</i>	58
FOR585 Advanced Smartphone Forensics	60
FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques	62
MGT414 SANS Training Program for CISSP® Certification	64
MGT512 SANS Security Leadership Essentials for Managers with Knowledge Compression™	66
MGT514 IT Security Strategic Planning, Policy, and Leadership	68
MGT525 IT Project Management, Effective Communication, and PMP® Exam Prep	70
LEG523 Law of Data Security and Investigations	72
AUD507 Auditing & Monitoring Networks, Perimeters, and Systems	73
DEV522 Defending Web Applications Security Essentials	74
DEV541 Secure Coding in Java/JEE: Developing Defensible Applications	76
DEV544 Secure Coding in .NET: Developing Defensible Applications	77
ICS410 ICS/SCADA Security Essentials	78
ICS515 ICS Active Defense and Incident Response	80
ICS456 Essentials for NERC Critical Infrastructure Protection <i>NEW!</i>	82
Hosted Courses.....	83
Additional Training Courses.....	84
SANS NetWars.....	86
Global Information Assurance Certification (GIAC) ..	87
SANS Technology Institute.....	88
Department of Defense Directive 8140.....	89
SANS Cyber Guardian.....	89
SANS Voucher Program.....	90
SANS Securing The Human.....	91
SANS CyberTalent Immersion Academy.....	91
SANS Training Formats (Live & Online).....	92
SANS Training Events.....	93
SANS Curriculum Roadmap.....	Inside Back Cover
SANS Resources.....	Back Cover

SANS WORLD-CLASS INSTRUCTORS

At SANS, we are privileged to have an instructor corps considered to be the best in the world. Not only do our instructors meet SANS' stringent requirements for excellence, they are all real-world practitioners. What you learn in class will be up to date and relevant to your job.



Dr. Eric Cole
Fellow
@drrericcole

TEACHES
MGT414 SEC401 SEC501

"Dr. Cole was excellent! I've had several similar courses and by far he kept the course interesting, entertaining, and relevant."
-JOSEPH R., U.S. AIR FORCE



Jason Fossen
Fellow
@JasonFossen

TEACHES
SEC401 SEC440 SEC505 SEC566

"Jason Fossen's Windows expertise is a clear asset to the SANS team!"
-ERNE H., U.S. NAVY



David Hoelzer
Fellow
@it_audit

TEACHES
AUD507 MGT305 MGT512 SEC503

"David Hoelzer is an excellent instructor with fantastic communication skills. He's able to provide real-world examples that are relatable for most people."
-APRIL EARLEY, N. MANHATTAN IMPROVEMENT CORP.



Tanya Baccam
Senior Instructor
@tbaccam

TEACHES
MGT414 SEC401 SEC502
SEC542 AUD507

"Tanya is an excellent instructor and does a great job of explaining difficult topics."
PAUL WHITE, WEST VIRGINIA STATE
AUDITOR'S OFFICE



Mark Baggett
Senior Instructor
@MarkBaggett

TEACHES
SEC504 SEC560 SEC561
SEC573

"Mark's teaching style is very relevant and sets an atmosphere where you are excited to learn."
-JEFF TURNER,
LEXIS NEXIS RISK SOLUTIONS



Eric Conrad
Senior Instructor
@eric_conrad

TEACHES
SEC542 SEC511 SEC560
SEC580 MGT414

"Eric is fantastic and does an excellent job relating the material to real-life examples."
-ROBBY CROFT,
BROWN-FORMAN CORPORATION



Paul A. Henry
Senior Instructor
@phenrycissp

TEACHES
FOR408 ICS410 MGT414
SEC401 SEC501 SEC502 SEC579

"Paul Henry was amazing and really made this course worth taking. His knowledge, insight, and experience were invaluable."
-KRIS CARR, VIRGINIA-FARM BUREAU



Frank Kim
Certified Instructor
@fykim

TEACHES
MGT514 DEV541

"Frank provided great real-world examples of attacks, course material, and quality."
-ANDREAS HEGNA, STOREBRAND



Stephen Sims
Senior Instructor
@Steph3nSims

TEACHES
SEC401 SEC560 SEC660 SEC760

"I am very impressed at how well Stephen conveyed the information. This is a hard topic and I feel like I have a lot I can take home with me and practice."

4 -ADAM LOGUE, SPECTRUM HEALTH



John Strand
Senior Instructor
@strandjs

TEACHES
SEC504 SEC550

"John Strand opened my eyes and helped me understand how to approach the concepts of offensive security and incident handling."
-STEPHEN ELLIS, CB&I



James Tarala
Senior Instructor
@isaudit

TEACHES
AUD507 SEC440 SEC504 SEC505
SEC560 SEC566

"James makes the class very interesting by providing real-world examples that help me to remember the concepts."

-SRINATH KANNAN, ACCENTURE



Chad Tilbury
Senior Instructor
@chadtilbury

TEACHES
FOR408 FOR508

"Chad's real-world examples are a key part of the training. It really helps to have a knowledgeable instructor who currently works in the industry."

-ROGER S., MISSILE DEFENSE AGENCY

SANS WORLD-CLASS INSTRUCTORS



Rob Lee

Fellow

@robtleee @sansforensics

TEACHES
FOR408 FOR508

"Rob Lee takes forensics to the highest level! It's not just about forensics, it's about forensic methodically and properly."

-THOMAS COOK, ARMY CYBER INSTITUTE



Stephen Northcutt

Fellow

@StephenNorthcut

TEACHES
MGT512

"Stephen is a very engaging instructor and the content is relevant to today's security challenges."

-JOY RANDELS, APPLIED G2



Hal Pomeranz

Fellow

@hal_pomeranz

TEACHES
FOR508 FOR518 FOR572
FOR610 SEC506

"Great intro to malware analysis. Hal Pomeranz was extremely knowledgeable on the subject. He is highly recommended!"

-JONATHAN HINSON, DUKE ENERGY CORPORATION



Ed Skoudis

Fellow

@edskoudis

TEACHES
SEC560

"Ed Skoudis successfully combines expertise, real-world experiences, and even humor to deliver an incredibly effective learning experience...Thank you!"

-GEORGE HUANG, NATIONWIDE INSURANCE



Heather Mahalik

Senior Instructor
@HeatherMahalik

TEACHES
FOR408 FOR585

"Heather did a great job introducing and explaining concepts without dwelling on those subjects too long. Very well-balanced!"

-STEPHANIE KURTZ, DELOITTE



Seth Misener

Senior Instructor
@sethmisener

TEACHES
MGT414 SEC511 SEC542

"Seth's experience and expertise in the subject domain are especially useful for me to understand the customers' requirements."

-RYAN WONG, ACCEL SYSTEMS



Keith Palmgren

Senior Instructor
@kpalmgren

TEACHES
SEC301 SEC401 SEC501

"Best explanation of cryptography I've heard yet. Keith took a difficult subject and made it understandable."

-TED ANTONUCCI, MACY'S



Mike Poor

Senior Instructor
@Mike_Poor

TEACHES
SEC503

"Mike Poor is a rock star and excellent instructor. I look forward to learning more from him in the future."

-MIKE BOYA, WARNER BROS. ENTERTAINMENT



Dave Shackelford

Senior Instructor
@daveshackelford

TEACHES
SEC501 SEC504 SEC560
SEC579

"Dave is an awesome and talented instructor!"

-MICHAEL OLDRIGHT, PRAESIDIO, INC.



Johannes Ullrich, PhD

Senior Instructor
@johullrich

TEACHES
SEC546 DEV522 FOR572 SEC503

"Dr. Ullrich has the subject matter and teaching down to a science."

-DAVID EDSTROM, MOSIAC451



Benjamin Wright

Senior Instructor
@benjaminwright

TEACHES
LEG523

"Mr. Wright is the best instructor I have had at SANS to date – great delivery of content!"

-KEITH WALTON, BB&T CORPORATION



Joshua Wright

Senior Instructor
@joswrIght

TEACHES
SEC561 SEC575 SEC617

"Joshua's awesome organized methodical style, combined with his knowledge and experience was a seamless learning experience for me."

-M. JAUREGUI, INTEL CORPORATION



Lenny Zeltser

Senior Instructor
@lennyzeltser

TEACHES
FOR610

"Lenny presented a wealth of knowledge, tied it together smoothly, and I am leaving with exponentially more knowledge."

-DAVID WARDEN, NGIS

Five-Day Program
30 CPEs
Laptop Required



www.giac.org/gisf

“SANS teaches you the logic and how to apply it to the real world.”

-KYLE PRATHER, HEARTLAND DENTAL

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.

“Very engaging course. I was on the edge of my seat the entire time!”

-CAROL FLAMER, VANGUARD

You Will Be Able To

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

“This course is very engaging. Although I have a security background, I found the information presented very informative, and 100% correct on SCADA risks and vulnerabilities.”

-TYLER MOORE, ROCKWELL AUTOMATION

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.**

“A really interesting course! I feel as if I'm getting a great overview of security, and I now know the areas where I need more training to best get my job done.”

-RACHEL SHAW, QUALCOMM INCORPORATED

Course Day Descriptions

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, IPTCP, 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.



SEC301 is available via (subject to change):



Featured Training Events

Crystal City	Crystal City, VA.	Sep 6-10
Network Security	Las Vegas, NV.	Sep 12-16
Seattle	Seattle, WA.	Oct 3-7
San Diego	San Diego, CA	Oct 23-27
Miami	Miami, FL	Nov 7-11
CDI.	Washington, DC	Dec 12-16
Security East	New Orleans, LA.	Jan 9-13



Community SANS Events

Denver, CO	Aug 1-5
San Jose, CA.	Aug 15-19
New York, NY	Aug 22-26
Dallas, TX	Oct 3-7
Atlanta, GA	Oct 3-7
Chantilly, VA	Oct 24-28
Salt Lake City, UT	Oct 31-Nov 4
New York, NY	Nov 7-11
Chantilly, VA	Dec 12-16



Summit Events

Security Awareness	San Francisco, CA.	Aug 5-9
------------------------------	----------------------------	---------



Private Training

All SANS courses are available through Private Training.



vLive Events

Virtual/Online.	Aug 16-Sep 15
-------------------------	-----------	---------------



Event Simulcast

Virtual/Online.	Dec 12-16
-------------------------	-----------	-----------



Custom Simulcast

Customized training for distributed workforces



OnDemand

E-learning available anytime, anywhere, at your pace



SelfStudy

This course is available in SANS SelfStudy

Six-Day Program
46 CPEs

Laptop Required

NEW LAPTOP REQUIREMENTS



www.giac.org/gsec



www.sans.edu



www.sans.org/cyber-guardian

MEETS DoDD 8140
(8570) REQUIREMENTS



www.sans.org/8140

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

STOP and ask yourself the following questions:

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

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

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

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

With the rise in advanced persistent threats, it is almost inevitable that organizations will be

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

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

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

"This course is an eye opener for everyone who cares about securing their information!" -DON CERVONE, BRIDGEWATER ASSOCIATES

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

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

Course Day Descriptions

401.1 HANDS ON: Networking Concepts

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

Topics: 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; Honey pots; Host-based Protection; Network-based Intrusion Detection and Prevention; Vulnerability Scanning and Remediation; Web Security

401.4 HANDS ON: Secure Communications

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

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

401.5 HANDS ON: Windows Security

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

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

401.6 HANDS ON: Unix/Linux Security

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

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

SEC401 is available via (subject to change):



Featured Training Events

Boston	Boston, MA	Aug 1-6
Portland	Portland, OR	Aug 8-13
Dallas	Dallas, TX	Aug 8-13
Chicago	Chicago, IL	Aug 22-27
Virginia Beach	Virginia Beach, VA	Aug 28-Sep 2
Crystal City	Crystal City, VA	Sep 6-11
Network Security	Las Vegas, NV	Sep 12-17
Seattle	Seattle, WA	Oct 3-8
Baltimore	Baltimore, MD	Oct 10-15
San Diego	San Diego, CA	Oct 23-28
Tysons Corner	Tysons Corner, VA	Oct 24-29
Miami	Miami, FL	Nov 7-12
San Francisco	San Francisco, CA	Nov 27-Dec 2
CDI	Washington, DC	Dec 12-17
Security East	New Orleans, LA	Jan 9-14
Las Vegas	Las Vegas, NV	Jan 16-21



Community SANS Events

Omaha, NE	Aug 15-20
Atlantic City, NJ	Aug 15-20
Columbus, OH	Aug 15-20
Raleigh-Cary, NC	Aug 22-27
Columbia, MD	Sep 12-17
Sacramento, CA	Sep 12-17
Albuquerque, NM	Sep 12-17
Detroit, MI	Sep 12-17
San Antonio, TX	Sep 12-17
Augusta, GA	Sep 19-24
San Francisco, CA	Sep 24-Oct 29
Chantilly, VA	Sep 26-Oct 1
Lakewood, WA	Sep 26-Oct 1
St Louis, MO	Oct 10-15
Richmond, VA	Oct 17-22
Ottawa, ON	Oct 24-29
San Diego, CA	Dec 5-10



Summit Events

Security Leadership	Dallas, TX	Sep 29-Oct 4
Healthcare Cybersecurity	Houston, TX	Nov 16-21



Mentor Classes

New York, NY	Aug 15-Sep 22
Louisville, KY	Aug 22-Oct 24
Des Moines, IA	Sep 13-Oct 25
Riverside, CA	Oct 12-14



Private Training

All SANS courses are available through Private Training.



vLive Events

Virtual/Online	Dec 13-Feb 2
--------------------------	--------------



Event Simulcast

Virtual/Online	Sep 12-17
Virtual/Online	Oct 23-28



Custom Simulcast

Customized training for distributed workforces



OnDemand

E-learning available anytime, anywhere, at your pace



SelfStudy

This course is available in SANS SelfStudy

Six-Day Program
36 CPEs
Laptop Required



www.giac.org/gced



www.sans.edu

MEETS DoDD 8140
(8570) REQUIREMENTS



www.sans.org/8140

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

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

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

-RACHEL WEISS, UPS INC.

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

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

“A very good thoughtful and practical understanding of security – something everyone in IT should have.”

-PAUL GODARD, OPC

“This training is valuable to my company because it allows me to learn about aspects of security I normally don't get exposed to on a daily basis.”

-BRENDON RAGER, TALQUIN ELECTRIC COOPERATIVE

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

Course Day Descriptions

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)



SEC501 is available via (subject to change):



Featured Training Events

Chicago	Chicago, IL	Aug 22-27
Virginia Beach . . .	Virginia Beach, VA . . .	Aug 22-27
Network Security . .	Las Vegas, NV	Sep 12-17
Baltimore	Baltimore, MD	Oct 10-15
San Diego	San Diego, CA	Oct 23-28
Tysons Corner . . .	Tysons Corner, VA . . .	Oct 24-29
CDI	Washington, DC	Dec 12-17



Community SANS Events

Columbia, MD	Sep 19-24
Ottawa, ON	Dec 12-17



Summit Events

Security Awareness . . .	San Francisco, CA . .	Aug 5-10
--------------------------	-----------------------	----------



Private Training

All SANS courses are available through Private Training.



Event Simulcast

Virtual/Online	Oct 23-28
--------------------------	-----------



Custom Simulcast

Customized training for distributed workforces



OnDemand

E-learning available anytime, anywhere, at your pace



SelfStudy

This course is available in SANS SelfStudy

Six-Day Program
36 CPEs
Laptop Required



www.giac.org/gcia



www.sans.edu



www.sans.org/cyber-guardian

MEETS DoDD 8140
(8570) REQUIREMENTS



www.sans.org/8140

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

Who Should Attend

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

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

“SEC503 directly covers the necessary knowledge and skill set I use day to day at my job. The added insight is worth the price of the course.” -MICHAEL GARRETT, FEDERAL RESERVE BANK OF SAN FRANCISCO

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

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

“The threats to our businesses and government agencies are ever increasing. We need to focus our IDS/IPS on our critical data and SEC503 helps us achieve that.”

-ED BREWSTER, SAIC INC.

You Will Be Able To

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

503.1 HANDS ON: Fundamentals of Traffic Analysis: PART 1

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

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

503.2 HANDS ON: Fundamentals of Traffic Analysis: PART 2

Day 2 continues where Day 1 ended in understanding TCP/IP. Two essential tools – Wireshark and tcpdump – are explored to give you the skills to analyze your own traffic. The focus of these tools on Day 2 is filtering traffic of interest in Wireshark using display filters and in tcpdump using Berkeley Packet Filters. We proceed with our exploration of the TCP/IP layers covering TCP, UDP, and ICMP. Once again, we describe the layers and analyze traffic not just in theory and function, but from the perspective of an attacker and defender.

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

503.3 HANDS ON: Application Protocols and Traffic Analysis

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

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

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

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

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

503.5 HANDS ON: Network Traffic Forensics and Monitoring

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

Topics: Analyst Toolkit; SILK; Network Forensics; Network Architecture for Monitoring; Correlation of Indicators; Packet Crafting; Command and Control (C2)

503.6 HANDS ON: IDS Challenge

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



SEC503 is available via (subject to change):

 **Featured Training Events**

- Boston Boston, MA Aug 1-6
- Virginia Beach . . . Virginia Beach, VA . . . Aug 28-Sep 2
- Network Security . . Las Vegas, NV Sep 12-17
- San Diego San Diego, CA Oct 23-28
- CDI Washington, DC Dec 12-17
- Security East New Orleans, LA Jan 9-14

 **Community SANS Events**

- Marina Del Rey, CA Aug 15-20
- Seattle, WA Sep 19-24
- Houston, TX Sep 26-Oct 1
- Chicago, IL Oct 17-22
- Las Vegas, NV Oct 31-Nov 5
- Indianapolis, IN Nov 14-19
- Tysons Corner, VA Nov 14-19
- Albany, NY Dec 12-17

 **Private Training**

All SANS courses are available through Private Training.

 **vLive Events**

Virtual/Online Sep 19-Oct 26

 **Event Simulcast**

Virtual/Online Oct 23-28

 **Custom Simulcast**

Customized training for distributed workforces

 **OnDemand**

E-learning available anytime, anywhere, at your pace

 **SelfStudy**

This course is available in SANS SelfStudy

Six-Day Program
37 CPEs
Laptop Required



www.giac.org/gcih



www.sans.edu



www.sans.org/cyber-guardian

MEETS DoDD 8140
(8570) REQUIREMENTS



www.sans.org/8140

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.

“After taking SEC504, I feel prepared to face the unknown threats and my voice of reason is better than ever!” -AARON WILLIAMS, DAF

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

law enforcement, and handling evidence. Finally, students will participate in a hands-on workshop that focuses on scanning, exploiting, and defending systems. **It will enable you to discover the holes in your system before the bad guys do!**

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

“This training gives you knowledge to think like an attacker, and better equips you to defend your network.”

-SHERYLL TIAUZON, COCA-COLA COMPANY

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

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

SEC504 is available via (subject to change):

 **Featured Training Events**

Boston	Boston, MA	Aug 1-6
Dallas	Dallas, TX	Aug 8-13
Alaska	Anchorage, AK	Aug 22-27
Chicago	Chicago, IL	Aug 22-27
Virginia Beach	Virginia Beach, VA	Aug 28-Sep 2
Crystal City	Crystal City, VA	Sep 6-11
Network Security	Las Vegas, NV	Sep 12-17
Seattle	Seattle, WA	Oct 3-8
Baltimore	Baltimore, MD	Oct 10-15
San Diego	San Diego, CA	Oct 23-28
Tysons Corner	Tysons Corner, VA	Oct 24-29
Miami	Miami, FL	Nov 7-12
San Francisco	San Francisco, CA	Nov 27-Dec 2
CDI	Washington, DC	Dec 12-17
Security East	New Orleans, LA	Jan 9-14
Las Vegas	Las Vegas, NV	Jan 16-21

 **Community SANS Events**

Tampa, FL	Aug 8-13
Columbia, MD	Aug 8-13
Marina del Rey, CA	Aug 15-20
St Louis, MO	Aug 22-27
Toronto, ON	Sep 12-17
Albany, NY	Sep 19-24
Miami, FL	Sep 19-24
Pittsburgh, PA	Oct 3-8
Omaha, NE	Oct 10-15
San Antonio, TX	Oct 17-22
Woodlawn, MD	Oct 17-22
Augusta, GA	Oct 24-29
Seattle, WA	Oct 31-Nov 5
Richmond, VA	Dec 5-10
Detroit, MI	Dec 5-10

 **Summit Events**

HackFest	Crystal City, VA	Nov 4-9
Healthcare Cybersecurity	Houston, TX	Nov 16-21

 **Mentor Classes**

Cleveland, OH	Aug 23-Oct 25
Denver, CO	Sep 9-Nov 11
Watertown, MA	Oct 4-Nov 15
Columbia, MD	Oct 5-Dec 7
Dayton, OH	Oct 20-Dec 1

 **Private Training**

All SANS courses are available through Private Training.

 **vLive Events**

Virtual/Online	Nov 1-Dec 8
--------------------------	-------------

 **Event Simulcast**

Virtual/Online	Sep 12-17
Virtual/Online	Dec 12-17

 **Custom Simulcast**

Customized training for distributed workforces

 **OnDemand**

E-learning available anytime, anywhere, at your pace

 **SelfStudy**

This course is available in SANS SelfStudy

Six-Day Program
36 CPEs
Laptop Required



www.giac.org/gcwn



www.sans.edu

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.

Who Should Attend

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

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

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

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

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

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

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

“This course was an excellent balance between theory and practical applications, extremely relevant to current trends, concepts, and technologies.”

-CHRIS S., NAVAL SURFACE WARFARE CENTER



www.sans.org/cyber-guardian

MEETS DoDD 8140 (8570) REQUIREMENTS



www.sans.org/8140

Course Day Descriptions

505.1 HANDS ON: PowerShell Automation and Security

Today's course covers what you need to know to get started using PowerShell. You don't need to have any prior scripting or programming experience. We have PowerShell labs throughout the week, so today is not the only PowerShell material. We start with the essentials, then go more in depth as the week progresses. Don't worry, you won't be left behind, the PowerShell labs walk you through every step.

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! We are the linebackers on the Blue Team and the WMI service was made for us, not them. 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



SEC505 is available via (subject to change):



Featured Training Events

Network Security . . . Las Vegas, NV Sep 12-17
San Diego San Diego, CA Oct 23-28
CDI Washington, DC Dec 12-17



Private Training

All SANS courses are available through Private Training.



Event Simulcast

Virtual/Online Oct 23-28
Virtual/Online Dec 12-17



Custom Simulcast

Customized training for distributed workforces



OnDemand

E-learning available anytime, anywhere, at your pace



SelfStudy

This course is available in SANS SelfStudy

Six-Day Program
36 CPEs
Laptop Required



www.giac.org/gcux



www.sans.edu



www.sans.org/cyber-guardian

MEETS DoDD 8140
(8570) REQUIREMENTS



www.sans.org/8140

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

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

Topics

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

Who Should Attend

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

You Will Be Able To

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

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

-CHRIS H., U.S. NAVAL ACADEMY

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

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

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

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

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

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

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

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

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

506.4 HANDS ON: Application Security – PART 1

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

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

506.5 HANDS ON: Application Security – PART 2

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

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

506.6 HANDS ON: Digital Forensics for Linux/Unix

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

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

“This course gave me a lot of tips and big chunks of knowledge that I missed during my Unix upbringing.”

-LUCAS SWEANY, QUALYS



SEC506 is available via (subject to change):



Featured Training Events

Network Security . . . Las Vegas, NV. Sep 12-17



Private Training

All SANS courses are available through Private Training.



Custom Simulcast

Customized training for distributed workforces



OnDemand

E-learning available anytime, anywhere, at your pace



SelfStudy

This course is available in SANS SelfStudy

New Extended
Bootcamp Hours to
Enhance Your Skills

Six-Day Program
46 CPEs
Laptop Required



www.giac.org/gmon



www.sans.edu

“SEC511 delivers the practical methodologies and granular information that can help bridge the communications gap that may exist between analysts, engineers, and operations.”

-KEVIN SOUTH, NAVIENT

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!

“SEC511 is a practical approach to continue security monitoring using free and open-source tools either alone or in conjunction with existing tools and devices. This is a must for anyone responsible for monitoring networks for security.”

-BRAD MILHORN, COMPUCOM

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)

You Will Be Able To

- ▶ Analyze a security architecture for deficiencies
- ▶ Apply the principles learned in the course to design a defensible security architecture
- ▶ Understand the importance of a detection-dominant security architecture and Security Operations Center (SOC)
- ▶ Identify the key components of Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Monitoring (CM)
- ▶ Determine appropriate security monitoring needs for organizations of all sizes
- ▶ Implement robust Network Security Monitoring/Continuous Security Monitoring (NSM/CSM)
- ▶ Determine requisite monitoring capabilities for a SOC environment
- ▶ Determine capabilities required to support continuous monitoring of key Critical Security Controls
- ▶ Utilize tools to support implementation of Continuous Monitoring per NIST guidelines SP 800-137

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

We begin with the end in mind by defining the key techniques and principles that will allow us to get there. An effective modern 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



SEC511 is available via (subject to change):

 **Featured Training Events**

- Boston Boston, MA Aug 1-6
- Virginia Beach . . . Virginia Beach, VA . . . Aug 22-27
- Network Security . . Las Vegas, NV. Sep 12-17
- San Diego San Diego, CA Oct 23-28
- CDI Washington, DC Dec 12-17
- Security East New Orleans, LA. Jan 9-14

 **Community SANS Events**

- Atlanta, GA Aug 1-6
- Minneapolis, MN. Sep 12-17
- Portland, OR Oct 17-22
- Richardson, TX Oct 17-22
- Phoenix, AZ Nov 7-12

 **Mentor Classes**

- Raleigh, NC Aug 18-29

 **Private Training**

All SANS courses are available through Private Training.

 **vLive Events**

- Virtual/Online Sep 26-Nov 2

 **Event Simulcast**

- Virtual/Online Oct 23-28
- Virtual/Online Dec 12-17

 **Custom Simulcast**

Customized training for distributed workforces

 **OnDemand**

E-learning available anytime, anywhere, at your pace

 **SelfStudy**

This course is available in SANS SelfStudy

Six-Day Program
36 CPEs
Laptop Required



www.giac.org/gwapt



www.sans.edu



www.sans.org/cyber-guardian

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.

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

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

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

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

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

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

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

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

You Will Be Able To

- ▶ 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
- ▶ 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
- ▶ Apply a detailed, four-step methodology to your web application penetration tests: reconnaissance, mapping, discovery, and exploitation
- ▶ Discover and exploit SQL Injection flaws to determine true risk to the victim organization

Who Should Attend

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

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.

SEC542 is available via (subject to change):



Featured Training Events

- Boston Boston, MA Aug 1-6
- Crystal City Crystal City, VA Sep 6-11
- Network Security Las Vegas, NV Sep 12-17
- Baltimore Baltimore, MD Oct 10-15
- San Francisco San Francisco, CA Nov 27-Dec 2
- CDI Washington, DC Dec 12-17



Community SANS Events

- Denver, CO Aug 8-13
- Indianapolis, IN Aug 22-27
- Anaheim, CA Nov 7-12
- Seattle, WA Nov 7-12



Summit Events

- HackFest Crystal City, VA Nov 4-9



Private Training

All SANS courses are available through Private Training.



vLive Events

- Virtual/Online Dec 5-Jan 25



Event Simulcast

- Virtual/Online Sep 12-17
- Virtual/Online Nov 4-9



Custom Simulcast

Customized training for distributed workforces



OnDemand

E-learning available anytime, anywhere, at your pace



SelfStudy

This course is available in SANS SelfStudy

“This course gave me a thorough understanding of how web app vulnerabilities can actually be exploited, and therefore why that needs to be fixed.”

-ANNA CANNING, CANNON IT SERVICES LLC

Five-Day Program
30 CPEs
Laptop Required

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

SEC550: Active Defense, Offensive Countermeasures, and Cyber Deception is based on the Active Defense Harbinger Distribution live Linux environment funded by the Defense Advanced Research Projects Agency (DARPA).

This virtual machine is built from the ground up for defenders to quickly implement Active Defenses in their environments. The course is very heavy with hands-on activities – we won't just talk about Active Defenses, we will work through labs that will enable you to quickly and easily implement what you learn in your own working environment.

You Will Learn:

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

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

-MICK LEACH, NATIONWIDE

You Will Be Able To

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

“The instructor is obviously very skilled and experienced – his teaching skill and personality is a perfect fit.”

**-PATRICK GUSTAFSON,
ALLIANZ LIFE INSURANCE**

Who Should Attend

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

SEC550 is available via (subject to change):



Featured Training Events

Chicago Chicago, IL Aug 22-27
Network Security . . Las Vegas, NV. Sep 12-17
Tysons Corner. . . . Tysons Corner, VA Oct 24-29
CDI. Washington, DC Dec 12-17
Security East New Orleans, LA. . . . Jan 9-13



Private Training

All SANS courses are available through Private Training.

What You Will Receive

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



Six-Day Program
36 CPEs
Laptop Required

The main objectives of CyberCity are to:

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

You Will Be Able To

- Scan for and discover the details associated computer, network, and ICS assets.
- Analyze and manipulate commonly used, very powerful, but often less-well-understood protocols such as Profinet, DNP3, Modbus, and more.
- Work as part of a team analyzing attacker actions and preventing kinetic impacts against industrial control systems.
- Look for vulnerabilities in systems associated with electrical power distribution, water systems, traffic systems, and other infrastructures.
- Use a variety of hands-on tools for analyzing and interacting with target systems, including Wireshark, tcpdump, Nmap, Metasploit, and much more.
- Control various Human Machine Interfaces and Operator Interface Terminals widely used by SCADA and other Industrial Control Systems (ICSs)
- Prevent attackers from wreaking havoc by manipulating computers that control physical infrastructures

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

NetWars CyberCity

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

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

“This course is the greatest! I’ve taken over 14 SANS training courses and have been waiting for this type of course. I would like to take this course again in a few years.” -MASASHI FUJIMARA, HITACHI LTD

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

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

Who Should Attend

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

SEC562 is available via (subject to change):



Featured Training Events

Network Security . . . Las Vegas, NV. Sep 12-17



Summit Events

Pen Test Hackfest. Crystal City, VA. . . Nov 4-9



Private Training

All SANS courses are available through Private Training.

Six-Day Program
37 CPEs
Laptop Required



www.giac.org/gpen



www.sans.edu



www.sans.org/cyber-guardian

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

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

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

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

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

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

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

"This course content is excellent and coherently organized. It will provide high value to my job." -MARGARITA JAUREGUI, INTEL CORPORATION

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

You Will Be Able To

- ▶ Develop tailored scoping and rules of engagement for penetration testing projects to ensure the work is focused, well defined, and conducted in a safe manner
- ▶ Conduct detailed reconnaissance using document metadata, search engines, and other publicly available information sources to build a technical and organizational understanding of the target environment
- ▶ Utilize the Nmap scanning tool to conduct comprehensive network sweeps, port scans, Operating System fingerprinting and version scanning to develop a map of target environments
- ▶ Configure and launch a vulnerability scanner such as Nessus so that it discovers vulnerabilities through both authenticated and unauthenticated scans in a safe manner, and customize the output from such tools to represent the business risk to the organization
- ▶ Analyze the output of scanning tools to manually verify findings and perform false positive reduction using connection-making tools such as Netcat and packet crafting tools such as Scapy
- ▶ Utilize the Windows and Linux command lines to plunder target systems for vital information that can further the overall penetration test progress, establish pivots for deeper compromise, and help determine business risks
- ▶ Configure an exploitation tool such as Metasploit to scan, exploit, and then pivot through a target environment
- ▶ Conduct comprehensive password attacks against an environment, including automated password guessing (while avoiding account lockout), traditional password cracking, rainbow table password cracking, and pass-the-hash attacks
- ▶ Utilize wireless attack tools for Wifi networks to discover access points and clients (actively and passively), crack WEP/WPA/WPA2 keys, and exploit client machines included within a project's scope
- ▶ Launch web application vulnerability scanners such as ZAP and then manually exploit Cross-Site Request Forgery, Cross-Site Scripting, Command Injection, and SQL Injection vulnerabilities to determine the business risk faced by an organization

Course Day Descriptions

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

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

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

560.2 HANDS ON: In-Depth Scanning

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

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

560.3 HANDS ON: Exploitation

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

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

560.4 HANDS ON: Post-Exploitation and Merciless Pivoting

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

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

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

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

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

560.6 HANDS ON: Penetration Test and Capture the Flag Workshop

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

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

SEC560 is available via (subject to change):



Featured Training Events

Portland	Portland, OR	Aug 8-13
Dallas	Dallas, TX	Aug 8-13
Virginia Beach . . .	Virginia Beach, VA . . .	Aug 22-27
Network Security . .	Las Vegas, NV	Sep 12-17
Baltimore	Baltimore, MD	Oct 10-15
CDI	Washington, DC	Dec 12-17
Security East	New Orleans, LA	Jan 9-14



Community SANS Events

Columbia, MD	Aug 1-6
Ottawa, ON	Sep 12-17
Des Moines, IA	Nov 14-19
Tampa, FL	Dec 5-10



Summit Events

HackFest	Crystal City, VA . . .	Nov 4-9
--------------------	------------------------	---------



Mentor Classes

Philadelphia, PA	Sep 14-Nov 16
----------------------------	---------------



Private Training

All SANS courses are available through Private Training.



vLive Events

Virtual/Online	Aug 16-Sep 22
Virtual/Online	Dec 6-Jan 26



Event Simulcast

Virtual/Online	Sep 12-17
Virtual/Online	Nov 4-9



Custom Simulcast

Customized training for distributed workforces



OnDemand

E-learning available anytime, anywhere, at your pace



SelfStudy

This course is available in SANS SelfStudy

Six-Day Program
36 CPEs
Laptop Required

“The course really forces you to think and the format rewards your hard work and dedication to finding the solutions.”

-MICHAEL NUTBROWN, SOLERS, INC

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

-TIMOTHY MCKENZIE, DELL/SECUREWORKS

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

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

on the innovative **NetWars** challenge infrastructure, which guides them through the numerous hands-on labs providing questions, hints, and lessons learned as they build their skills.

Who Should Attend

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

You Will Be Able To

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

Topics addressed in the course include:

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

Course Day Descriptions

561.1 HANDS ON: Security Platform Analysis

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

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

561.2 HANDS ON: Enterprise Security Assessment

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

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

561.3 HANDS ON: Web Application Assessment

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

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

561.4 HANDS ON: Mobile Device and Application Analysis

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

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

561.5 HANDS ON: Advanced Penetration Testing

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

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

561.6 HANDS ON: Capture the Flag Challenge

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



SEC561 is available via (subject to change):



Featured Training Events

Virginia Beach . . . Virginia Beach, VA . . . Aug 22-27
CDI Washington, DC Dec 12-17



Private Training

All SANS courses are available through Private Training.

Five-Day Program
30 CPEs
Laptop Required



www.giac.org/gccc



www.sans.edu

“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

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

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

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

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

“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

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

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

Who Should Attend

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

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

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)

“I’m leaving the class with a great mindset aimed at evaluating the current environment and controls. SEC566 was good information with a great instructor!”

-TOM KOZELSKY, NEXEO SOLUTIONS

“SEC566 is a very comprehensive course, and the collections of lists are useful, informative tools that can be moved in the real day-to-day job.”

-HENRY JIANG, GENWORTH FINANCIAL



SEC566 is available via (subject to change):



Featured Training Events

Network Security . . . Las Vegas, NV Sep 12-17

San Francisco San Francisco, CA . . . Nov 27-Dec 1

CDI Washington, DC Dec 12-17

Security East New Orleans, LA Jan 9-12



Summit Events

Security Awareness . . . San Francisco, CA . . Aug 5-10

Security Leadership Dallas, TX . . Sep 29-Oct 3



Community SANS Events

Long Beach, CA Sep 26-30

New York, NY Sep 26-30

New Orleans, LA Oct 3-7



Private Training

All SANS courses are available through Private Training.



Custom Simulcast

Customized training for distributed workforces



OnDemand

E-learning available anytime, anywhere, at your pace



SelfStudy

This course is available in SANS SelfStudy

Five-Day Program
30 CPEs
Laptop Required



www.giac.org/gpyc



www.sans.edu

You Will Receive

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

You Will Be Able To

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

Your target has been well hardened. So far, your every attempt to compromise their network has failed. You did find evidence of vulnerability, a break in their defensive posture. Unfortunately, all of your tools have failed to successfully exploit it. Your employers demand results. You want to model the actions of an advanced adversary and take advantage of that discovered flaw your tools can't seem to address. What do you do when off-the-shelf tools fall short? You write your own tool!

SEC573: Python for Penetration Testers will teach you the skills needed not only to tweak or customize tools, but to even develop your own tools from scratch. The course is designed to meet you at your current skill level and appeal to a wide variety of backgrounds. Whether you have absolutely no coding experience or are a skilled Python developer looking to apply your coding skills to penetration testing, this course has something for you.

You cannot become a world-class tool builder by merely listening to lectures, so this course is chock full of hands-on labs. Every day we will teach you the skills you need to develop serious Python programs and show you how to apply those skills in penetration testing engagements.

The course begins with an introduction to SANS pyWars, which is a four-day Capture-the-Flag competition that runs parallel to the course material. It will challenge your existing programming skills and help you develop new skills at your own pace. Experienced programmers can quickly progress to more advanced concepts while novice programmers spend time building a strong foundation.

We then cover the essential skills required to get the most out of the Python language. The essentials workshop labs will teach you the concepts and techniques required to develop your own

tools. The workshop focuses on essential programming skills and how to apply them in real-world scenarios, but it also shows you shortcuts that will make even experienced developers more deadly. Once everyone understands the essentials, we apply those skills by developing tools to help you in your next penetration test. You will develop a port-scanning, anti-virus-evading, client-infecting backdoor for placement on target systems, as well as a SQL injection tool to extract data from websites that are immune to off-the-shelf tools. You will learn the concepts required to build a multi-threaded password guessing tool and a packet assembling network reconnaissance tool. The course concludes with a capstone one-day Capture-the-Flag event that complements the pyWars challenge and tests your ability to apply your new tools and coding skills in a penetration testing challenge.

The ability to read, write, and customize software is what distinguishes the good penetration tester from the great one. The best penetration testers can customize existing open-source tools or develop their own tools. Unfortunately, even though organizations serious about security continually emphasize their need for skilled tool builders, many testers do not have these skills. Developing these skills is not beyond your reach. So when you are ready to fully weaponize your penetration testing skillset and build and use your own tools to automate your penetration testing skills, join us for **SEC573: Python for Penetration Testers**.

Who Should Attend

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

Course Day Descriptions

573.1 HANDS ON: Essentials Workshop – PART 1

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

Topics: Variables; Math Operators; Strings; Functions; Modules; Compound Statements; Introspection

573.2 HANDS ON: Essentials Workshop – PART 2

You will never learn to program by staring at Powerpoint slides. The second day continues the hands-on lab-centric approach established on day one. This section continues covering the essentials of the language, including data structures and programming concepts. With the essentials of the language under your belt, the pyWwars challenges and the in-class labs start to cover more complex subjects.

Topics: Lists; Loops; Tuples; Dictionaries; The Python Debugger; System Arguments & OptParser; File Operations

573.3 HANDS ON: Pen Testing Applications – PART 1

Day 3 shifts gears. With a core set of skills established, we can begin developing penetration testing tools that you can use in your next engagement. You will develop a backdoor command shell that evades antivirus software and provides you with that critical initial foothold in the target environment. You will then develop a customizable SQL injection tool that you can use to extract all the data from a vulnerable database when off-the-shelf tools fail. Finally, we will discuss how to speed up your code with multi-threading.

Topics: Network Sockets; Exception Handling; Process Execution; Metasploit Integration; Antivirus; IDS Evasion; Introduction to SQL; Blind SQL Injection Techniques; Developing Web Clients; Multi-Threaded Applications; Mutexes and Semaphores; Message Queues; Thread Communications

573.4 HANDS ON: Pen Testing Applications – PART 2

In this section you will develop more tools that will make you a more lethal penetration tester. First, you will develop a custom web-based password guesser. This will teach you how to get the most out of Python's web-based libraries and interact with websites using cookies, proxies, and other features to p0wn the most difficult web-based authentication systems. Then, you'll write a network reconnaissance tool that will demonstrate the power of Python's third-party libraries.

Topics: HTTP Form Password Guessing; Advanced Web Client Techniques; HTTP Proxies/HTTP Cookies; Session Hijacking; TCP Packet Reassembly with Scapy; Extracting Images from TCP Streams; Analyzing Image Metadata

573.5 HANDS ON: Capture the Flag

The Capture-the-Flag event on the final day complements the pyWwars challenge and tests your ability to apply your new penetration testing tools and coding skills. Working in teams, students apply the skills they have mastered in a series of penetration testing challenges. Participants will exercise the skills and code they have developed over the previous four days as they exploit vulnerable systems, break encryption cyphers, and remotely execute code on target systems. Test your skills! Prove your might!

“SEC573 is a great course. Advanced thinking required and challenges are excellent!”

-KEVIN NICHOLSON, MOTOROLA SOLUTIONS

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

-JAY WILSON, NAVIENT



SEC573 is available via (subject to change):



Featured Training Events

Network Security . . Las Vegas, NV. Sep 12-16



Private Training

All SANS courses are available through Private Training.

“Excellent class for beginners and advanced alike. It has something for everyone.”

-MIKE PEREZ, DISNEY

“SEC573 gave me exposure to tools and techniques I wouldn't have normally considered, but now are part of my arsenal.”

-ALLEN C., DoD

NEW!

Six-Day Program
36 CPEs
Laptop Required



www.giac.org/gmob



www.sans.edu

“This course exposes you to a new world that complements all the information security backgrounds that I have learned in previous courses and work experiences.”

-FRED BEDRICH, BCI GROUP

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.

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

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

575.1 HANDS ON: Device Architecture and Common Mobile Threats

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

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

575.2 HANDS ON: Mobile Platform Access and Application Analysis

With an understanding of the threats, architectural components and desired security methods, we can design incident response processes to mitigate the effect of common threat scenarios, including device loss. We'll look at building such a program, while developing our own skills to analyze mobile device data and applications through rooting and jailbreaking, filesystem data analysis, and network activity analysis techniques.

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

575.3 HANDS ON: Mobile Application Reverse Engineering

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

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

575.4 HANDS ON: Penetration Testing Mobile Devices – PART 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 or penetration testing, we turn our focus to exploiting weaknesses on individual mobile devices, including iPhones, iPads, Android phones and tablets, Windows Phones, and BlackBerry devices. We'll also examine platform-specific application weaknesses and look at the growing use of web framework attacks.

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

575.6 HANDS ON: Capture the Flag

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



SEC575 is available via (subject to change):



Featured Training Events

Boston Boston, MA Aug 1-6
Virginia Beach . . . Virginia Beach, VA . . . Aug 22-27
Network Security . . Las Vegas, NV. Sep 12-17
CDI. Washington, DC Dec 12-17



Private Training

All SANS courses are available through Private Training.



Event Simulcast

Virtual/Online Dec 12-17



Custom Simulcast

Customized training for distributed workforces



OnDemand

E-learning available anytime, anywhere, at your pace



SelfStudy

This course is available in SANS SelfStudy

Six-Day Program
36 CPEs
Laptop Required

“Overall, it’s a great course! The Exploits and PoC are cutting edge! This is the future of IT and security knowledge is power!”

-JOE MARSHALL, EXELON

One of today’s most rapidly evolving and widely deployed technologies is server virtualization. Many organizations are already realizing the cost savings from implementing virtualized servers, and systems administrators love the ease of deployment and management of virtualized systems. There are even security benefits of virtualization: easier business continuity and disaster recovery, single points of control over multiple systems, role-based access, and additional auditing and logging capabilities for large infrastructure.

“This course was excellent! As always, SANS training is top notch.”

-JD LOVERING, GE CAPITAL

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

“There is lots of information to consume, and the instructor did an outstanding job with presentation.”

-KEVIN M., ARMY NATIONAL GUARD

In addition, many organizations are evolving virtualized infrastructure into private clouds, internal shared services running on virtualized infrastructure. Security architecture, policies, and processes will need to adapt to work within a cloud infrastructure, and there are many changes that security and operations teams will need to accommodate to ensure assets are protected.

Who Should Attend

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



You Will Be Able To

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

Author Statement

“Seeing the growth in virtualization technology over the past decade, I realized how important it was to educate security professionals on how the nature of their infrastructure is changing. We cannot keep securing systems the same way when the footprint of our data centers is radically different! As more organizations build private and hybrid clouds, we are changing trust models toward shared infrastructure as well. This course will help security, IT operations and audit team members develop a solid understanding of what is changing and how they can best secure these new technologies.”

-Dave Shackelford

579.1 HANDS ON: Virtualization Security Architecture and Design

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

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

579.2 HANDS ON: Virtualization and Private Cloud Infrastructure Security

Today starts with virtualization management. VMware vCenter, Microsoft System Center Virtual Machine Manager (SCVMM), and Citrix XenCenter will be covered. Virtual Desktop Infrastructure (VDI) will be covered with an emphasis on security principles. Specific security-focused use cases for VDI, such as remote access and network access control, will be reviewed. We will take an in-depth look at virtual firewalls. Students will build a virtualized intrusion detection model; integrate promiscuous interfaces and traffic capture methods into virtual networks; and then set up and configure a virtualized IDS sensor. Attention will be paid to host-based IDS, with considerations for multitenant platforms. Days 2-6 do not list any topics.

579.3 HANDS ON: Virtualization Offense and Defense – PART 1

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

579.4 HANDS ON: Virtualization Offense and Defense – PART 2

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

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

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

579.6 HANDS ON: Auditing and Compliance for Virtualization and Cloud

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

SEC579 is available via (subject to change):



Featured Training Events

Network Security . . . Las Vegas, NV. Sep 12-17
CDI. Washington, DC Dec 12-17



Private Training

All SANS courses are available through Private Training.



Custom Simulcast

Customized training for distributed workforces



OnDemand

E-learning available anytime, anywhere, at your pace



SelfStudy

This course is available in SANS SelfStudy

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

-LEONARD LYONS, NORTHROP GRUMMAN

Six-Day Program
36 CPEs
Laptop Required



www.giac.org/gawn



www.sans.edu



www.sans.org/cyber-guardian

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

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

To be a wireless security expert, you need to have a comprehensive understanding of the technology, threats, exploits, and defensive techniques along with hands-on experience in evaluating and attacking wireless technology. Not limiting your skill-set to WiFi, you'll need to evaluate the threat from other standards-based and proprietary wireless technologies as well. This course takes an in-depth look at the security challenges of many different wireless technologies, exposing you to wireless security threats through the eyes of an attacker. Using readily available and custom-developed tools, you'll navigate your way through the techniques attackers use to exploit WiFi networks, including attacks against WEP, WPA/WPA2, PEAP, TTLS, and other systems. You'll also develop

attack techniques leveraging Windows 7 and Mac OS X. We'll examine the commonly overlooked threats associated with Bluetooth, ZigBee, DECT, and proprietary wireless systems. As part of the course, you'll receive the SWAT Toolkit, which will be used in hands-on labs to back up the course content and reinforce wireless ethical hacking techniques.

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

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

“SEC617 is an excellent course to prepare you for wireless lecturing space.”

-GARY P., DEPARTMENT OF NATIONAL DEFENSE

Who Should Attend

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

You Will Be Able To

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

617.1 HANDS ON: Wireless Data Collection and WiFi MAC Analysis

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

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

617.2 HANDS ON: Wireless Tools and Information Analysis

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

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

617.3 HANDS ON: Client, Crypto, and Enterprise Attacks

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

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

617.4 HANDS ON: Advanced WiFi Attack Techniques

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

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

617.5 HANDS ON: Bluetooth, DECT, and ZigBee Attacks

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

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

617.6 HANDS ON: Wireless Security Strategies and Implementation

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

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



SEC617 is available via (subject to change):



Featured Training Events

Network Security . . . Las Vegas, NV. Sep 12-17



Summit Events

HackFest. Crystal City, VA. . . Nov 4-9



Community SANS Events

New York, NY. Nov 14-19



Private Training

All SANS courses are available through Private Training.



Custom Simulcast

Customized training for distributed workforces

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

-JOHN FRUGE, B&W TECHNICAL SERVICES

Six-Day Program
36 CPEs
Laptop Required

“Best web app
class ever!”

-JOHN CARTRETT,

TORCHMARK CORPORATIONS

“SEC642 helps sharpen the
pen testing mindset and
to be more creative when
performing pen tests.”

-JESPER PETERSSON, KLARNA



You Will Be Able To

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

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

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

-MATTHEW SULLIVAN, WEBFILINGS

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

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

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

Following these general exploits, you will learn techniques that target specific enterprise applications. You will attack systems such as content management and ticketing systems. We will explore the risks and flaws found within these systems and how to better exploit them. This part of the course will also include web services and mobile applications due to their prevalence within modern organizations.

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

Author Statement

“Students who have taken SEC542 have learned the benefits of applying hands-on, in-depth web application penetration testing techniques to take their assessments far beyond the limited push-button approach of purely automated scanners. But how do we take that to the next level? How can we dig deeper to find those vulnerabilities still hiding in our apps? In SEC642, I love seeing students get excited about taking SQLi, RFI/LFI, XSRF/XSS exploits to the next level, exploring the ins and outs of various web frameworks, testing for crypto flaws in cookies and parameter values that look like random characters to novice testers, working with alternate web interfaces like services and client-side binaries, and probing the effectiveness of their WAFs. In SEC642 we get to step away from the basics and dig into advanced topics that can be leveraged in our assessments, exploring parts of our apps that are often overlooked or not considered testable by less experienced penetration testers.” -Justin Searle

Who Should Attend

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

642.1 HANDS ON: Advanced Discovery and Exploitation

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

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

642.2 HANDS ON: Discovery and Exploitation for Specific Applications

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

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

642.3 HANDS ON: Web Application Encryption

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

Topics: Exploring How to Identify the Cryptography in Use; Discovering How to Attack the Encryption Keys; Exploiting Stream Cipher IV Collisions; Exploiting Electronic Codebook (ECB) Mode Ciphers with Block Suffling; Exploit Cipher Block Chaining (CBC) Bit Flipping

642.4 HANDS ON: Mobile Applications and Web Services

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

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

642.5 HANDS ON: Web Application Firewall and Filter Bypass

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

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

642.6 HANDS ON: Capture the Flag

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

SEC642 is available via (subject to change):



Featured Training Events

Network Security . . Las Vegas, NV. Sep 12-17



Private Training

All SANS courses are available through Private Training.



Custom Simulcast

Customized training for distributed workforces

“I like this training because it is very hands-on and not just focused on slides.

Very helpful for the real world.” -ZACH

MORENO, CHICO SECURITY

Six-Day Program
46 CPEs
Laptop Required



www.giac.org/gxpn



www.sans.edu



www.sans.org/cyber-guardian

“The SEC660 course was hands-on, packed with content, and current to today’s technology!”

-MICHAEL HORKEN, ROCKWELL AUTOMATION

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.**

**“Great instruction with the right mix of lecture and labs.
The capture-the-flag challenge brought everything together for the week.”**

-CHRIS FORTUNE, VECTREN CORPORATION

Who Should Attend

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

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

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 Paimeir

660.4 HANDS ON: Exploiting Linux for Penetration Testers

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

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

660.5 HANDS ON: Exploiting Windows for Penetration Testers

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

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

660.6 HANDS ON: Capture the Flag Challenge

This day will serve as a real-world challenge for students, requiring them to utilize skills learned throughout the course, think outside the box, and solve simple-to-complex problems. In this offensive exercise, challenges range from local privilege escalation to remote exploitation on both Linux and Windows systems, as well as networking attacks and other challenges related to the course material.



SEC660 is available via (subject to change):



Featured Training Events

Network Security . . . Las Vegas, NV Sep 12-17
San Francisco San Francisco, CA . . . Nov 27-Dec 2
CDI Washington, DC Dec 12-17



Private Training

All SANS courses are available through Private Training.



Custom Simulcast

Customized training for distributed workforces



OnDemand

E-learning available anytime, anywhere, at your pace



SelfStudy

This course is available in SANS SelfStudy

Six-Day Program
46 CPEs
Laptop Required

What You Will Receive

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

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

-JENNY KITACHIT, INTEL

Vulnerabilities in modern operating systems such as Microsoft Windows 7/8/10, Server 2012, and the latest Linux distributions are often very complex and subtle. Yet these vulnerabilities could expose organizations to significant attacks, undermining their defenses when attacked by very skilled adversaries. Few security professionals have the skillset to discover let alone even understand at a fundamental level why the vulnerability exists and how to write an exploit to compromise it. Conversely, attackers must maintain this skillset regardless of the increased complexity. **SEC760: Advanced Exploit Development for Penetration Testers** teaches the skills required to reverse-engineer 32- and 64-bit applications, perform remote user application and kernel debugging, analyze patches for one-day exploits, and write complex exploits, such as use-after-free attacks, against modern software and operating systems.

Some of the skills you will learn in SEC760 include:

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

Not sure if you are ready for SEC760?

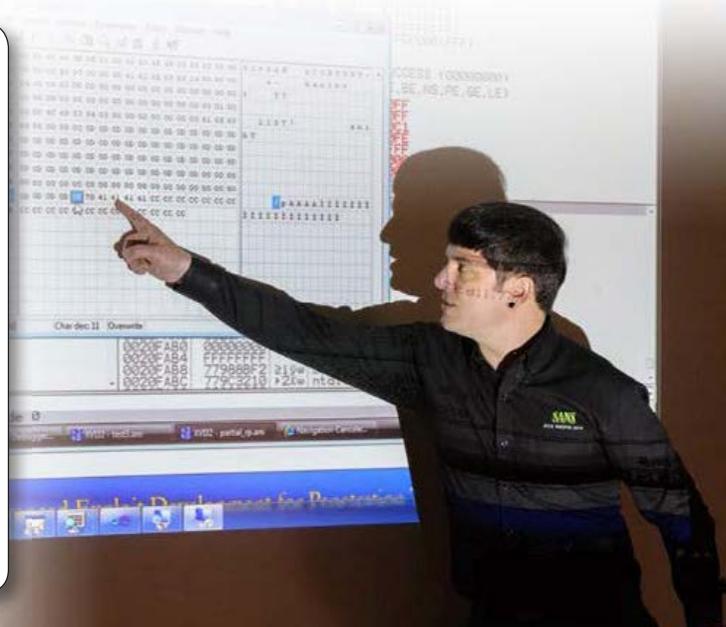
Take this 10 question quiz: www.sans.org/sec760/quiz

Who Should Attend

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

You Will Be Able To

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



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

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

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

760.2 HANDS ON: Advanced Linux Exploitation

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

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

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

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

Topics: The Microsoft Patch Management Process and Patch Tuesday; Obtaining Patches and Patch Extraction; Binary Diffing with BinDiff, patchdiff2, turbodiff, and DarunGrim4; Visualizing Code Changes and Identifying Fixes; Reversing 32-bit and 64-bit Applications and Modules; Triggering Patched Vulnerabilities; Writing One-Day Exploits; Handling Modern Exploit Mitigation Controls; Using ROP to Compiled Shellcode on the Fly (Return-Oriented Shellcode)

760.4 HANDS ON: Windows Kernel Debugging and Exploitation

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

Topics: Understanding the Windows Kernel; Navigating the Windows Kernel; Modern Kernel Protections; Debugging the Windows 7/8 Kernels and Drivers; WinDbg; Analyzing Kernel Vulnerabilities and Kernel Vulnerability Types; Kernel Exploitation Techniques; Token Stealing and HAL Dispatch Table Overwrites

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

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

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

760.6 HANDS ON: Capture the Flag Challenge

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

SEC760 is available via (subject to change):



Featured Training Events

Network Security . . . Las Vegas, NV. Sep 12-17
CDI. Washington, DC Dec 12-17



Summit Events

HackFest. Crystal City, VA. . . Nov 4-9



Private Training

All SANS courses are available through Private Training.

“This course is the challenge I was looking for. It will be overwhelming, but well worth it.”

-WILLIAM STOTT, RAYTHEON

“As always, SANS training is extremely valuable for any security professional. This course sits on top of the mountain of great SANS material.”

-DOUG RODGERS, WELLS FARGO

Six-Day Program
36 CPEs
Laptop Required



www.giac.org/gcfe



www.sans.edu

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

FOR408: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of the Microsoft Windows operating systems. You can't protect what you don't understand, and understanding forensic capabilities and artifacts is a core component of information security. You'll learn to recover, analyze, and authenticate forensic data on Windows systems. You'll understand

how to track detailed user activity on your network and how to organize findings for use in incident response, internal investigations, and civil/criminal litigation. You'll be able to use your new skills to validate security tools, enhance vulnerability assessments, identify insider threats, track hackers, and improve security policies. Whether you know it or not, Windows is silently recording an unimaginable amount of data about you and your users. FOR408 teaches you how to mine this mountain of data.

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

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

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

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

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

408.1 HANDS ON: Windows Digital Forensics and Advanced Data Triage

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

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

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

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

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

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

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

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

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

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

Topics: Email Forensics; Forensics 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



FOR408 is available via (subject to change):



Featured Training Events

- Boston Boston, MA Aug 1-6
- Chicago Chicago, IL Aug 22-27
- Virginia Beach . . . Virginia Beach, VA . . . Aug 22-27
- Crystal City Crystal City, VA Sep 6-11
- Network Security . . Las Vegas, NV Sep 12-17
- Seattle Seattle, WA Oct 3-8
- CDI Washington, DC Dec 12-17
- Las Vegas Las Vegas, NV Jan 16-21



Private Training

All SANS courses are available through Private Training.



vLive Events

Virtual/Online Oct 11-Nov 17



Event Simulcast

Virtual/Online Sep 12-17
Virtual/Online Dec 12-17



Custom Simulcast

Customized training for distributed workforces



OnDemand

E-learning available anytime, anywhere, at your pace



SelfStudy

This course is available in SANS SelfStudy

“After years of imaging and analysis, I learned more in one day than six months in this field.”

-DON MALONE, BEYOND INC.

Six-Day Program
36 CPEs
Laptop Required



www.giac.org/gcfa



www.sans.edu

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

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

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

Who Should Attend

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

You Will Be Able To

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

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

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

-LOUISE CHEUNG, STROZ FRIEDBERG

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

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

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

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



www.sans.org/cyber-guardian

MEETS DoDD 8140
(8570) REQUIREMENTS



www.sans.org/8140

Course Day Descriptions

508.1 HANDS ON: Advanced Incident Response and Digital Forensics

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

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

508.2 HANDS ON: Memory Forensics in Incident Response

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

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

508.3 HANDS ON: Timeline Analysis

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

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

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

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

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

508.5 HANDS ON: Threat Hunting

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

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

508.6 HANDS ON: APT Intrusion Incident Response Challenge

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



FOR508 is available via (subject to change):



Featured Training Events

Portland	Portland, OR	Aug 8-13
Virginia Beach . . .	Virginia Beach, VA . .	Aug 28-Sep 2
Network Security . .	Las Vegas, NV	Sep 12-17
Baltimore	Baltimore, MD	Oct 10-15
Tysons Corner . . .	Tysons Corner, VA . . .	Oct 24-29
Miami	Miami, FL	Nov 7-12
CDI	Washington, DC	Dec 12-17
Security East	New Orleans, LA	Jan 9-14



Summit Events

Cyber Threat Intelligence . . . Arlington, VA . . .Jan 25-30



Community SANS Events

Columbia, MDSep 26-Oct 1
New York, NYOct 17-22



Private Training

All SANS courses are available through Private Training.



vLive Events

Virtual/Online Oct 3-Nov 9



Event Simulcast

Virtual/Online Dec 12-17



Custom Simulcast

Customized training for distributed workforces



OnDemand

E-learning available anytime, anywhere, at your pace



SelfStudy

This course is available in SANS SelfStudy

Six-Day Program
36 CPEs
Laptop Required

“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.

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.

Who Should Attend

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

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

-NAVEEL KOYA, AC-DAC — TRIVANDRUM

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

“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!

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
- Advanced Log Analysis and Correlation
- Analysis of Mac Technologies including Time Machine, Spotlight, and FileVault
- iDevice Analysis and iOS Artifacts

FOR518 is available via (subject to change):

 **Featured Training Events**

Virginia Beach . . . Virginia Beach, VA . . . Aug 28-Sep 2
 Network Security . . . Las Vegas, NV. Sep 12-17
 San Francisco . . . San Francisco, CA . . . Nov 27-Dec 2
 CDI. Washington, DC Dec 12-17

 **Summit Events**

Cyber Threat Intelligence . . . Arlington, VA . . . Jan 25-30

 **Private Training**

All SANS courses are available through Private Training.

 **Custom Simulcast**

Customized training for distributed workforces

 **OnDemand**

E-learning available anytime, anywhere, at your pace

 **SelfStudy**

This course is available in SANS SelfStudy

Six-Day Program
36 CPEs
Laptop Required

“Thank you for all the content and I can’t wait to do the exercises and the challenges again.”

-NICK CHRISTIAN, TBI

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

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

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

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

FOR526:Memory Forensics In-Depth will teach you:

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

MALWARE CAN HIDE, BUT IT MUST RUN

Who Should Attend

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

What You Will Receive

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

526.1 HANDS ON: Foundations in Memory Analysis and Acquisition

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

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

526.2 HANDS ON: Unstructured Analysis and Process Exploration

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

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

526.3 HANDS ON: Investigating the User via Memory Artifacts

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

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

526.4 HANDS ON: Internal Memory Structures

Section four focuses on introducing internal memory structures such as drivers, Windows memory table structures, and extraction techniques for portable executables. As we come to the final steps in our investigative methodology – steps that include spotting rootkit behaviors and extracting suspicious binaries – it is important to emphasize again the rootkit paradox, which is that the more malicious code attempts to hide itself, the more abnormal and seemingly suspicious it appears. We will use this concept to evaluate some of the most common structures in Windows memory for hooking, IDTs, and SSDTs.

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

526.5 HANDS ON: Memory Analysis on Platforms Other than Windows

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

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

526.6 HANDS ON: Memory Analysis Challenges

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

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



FOR526 is available via (subject to change):



Featured Training Events

Network Security . . . Las Vegas, NV. Sep 12-17
Security East New Orleans, LA. Jan 9-14



Private Training

All SANS courses are available through Private Training.



Event Simulcast

Virtual/Online Sep 12-17



Custom Simulcast

Customized training for distributed workforces



OnDemand

E-learning available anytime, anywhere, at your pace



SelfStudy

This course is available in SANS SelfStudy

Six-Day Program
36 CPEs
Laptop Required



www.giac.org/gnfa



www.sans.edu

The network IS the new investigative baseline.

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

FOR572: Advanced Network Forensics and Analysis was built from the ground up to cover the most critical skills needed to mount efficient and effective post-incident response investigations. We focus on the knowledge necessary to expand the forensic mindset from residual data on the storage media

from a system or device to the transient communications that occurred in the past or continue to occur. Even if the most skilled remote attacker compromised a system with an undetectable exploit, the system still has to communicate over the network. Without command-and-control and data extraction channels, the value of a compromised computer system drops to almost zero. Put another way: **Bad guys are talking – we'll teach you to listen.**

“FOR572 was an excellent course that kept my attention and it will be immediately useful when I get back to work.” -JOHN IVES, UC BERKELEY

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

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

The hands-on exercises in this class cover a wide range of tools, including the venerable tcpdump and Wireshark for packet capture and analysis; commercial tools from Splunk, NetworkMiner, and SolarWinds; and open-source tools including nfdump, tcpextract, ELSA, and more. Through all of these exercises, your shell scripting abilities will come in handy to make easy work of ripping through hundreds and thousands of data records.

Who Should Attend

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

You Will Be Able To

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

Course Day Descriptions

572.1 HANDS ON: Off the Disk and Onto the Wire

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

Topics: Web Proxy Server Examination, Payload Reconstruction, Foundational Network Forensics Tools: tcpdump and Wireshark, Network Evidence Types and Sources, Network Architectural Challenges and Opportunities, Packet Capture Applications and Data

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

In this section, you will learn what data items NetFlow can provide, and the various means of collecting those items. As with many such monitoring technologies, both commercial and open-source solutions exist to query and examine NetFlow data. We will review both categories and discuss the benefits and drawbacks of each. In the same vein, presenting concise findings from extremely large data sources is an important skill. A network forensicator should be able to aggregate and visually present findings, especially when faced with a years-long compromise incident. Expressing findings supported with visualizations can provide a much clearer picture than words alone.

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

572.3 HANDS ON: Network Protocols and Wireless Investigations

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

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

572.4 HANDS ON: Logging, OPSEC, and Footprint

In this section, you will learn about various logging mechanisms available to both endpoint and network transport devices. You will also learn how to consolidate log data from multiple sources, providing a broad corpus of evidence in one location. As the volume of log data increases, so does the need to consider automated analytic tools. You will learn various solutions that accomplish this, from tactical to enterprise-scale.

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

572.5 HANDS ON: Encryption, Protocol Reversing, and Automation

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

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

572.6 HANDS ON: Network Forensics Capstone Challenge

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

Topics: Network Forensic Case

FOR572 is available via (subject to change):



Featured Training Events

Boston Boston, MA Aug 1-6
Dallas Dallas, TX Aug 8-13
Virginia Beach . . . Virginia Beach, VA . . . Aug 28-Sep 2
Network Security . . Las Vegas, NV. Sep 12-17
San Francisco . . . San Francisco, CA . . . Nov 27-Dec 2
CDI Washington, DC Dec 12-17
Las Vegas Las Vegas, NV. Jan 16-21



Summit Events

Cyber Threat Intelligence . . . Arlington, VA . . . Jan 25-30



Community SANS Events

Columbia, MD Aug 15-20



Private Training

All SANS courses are available through Private Training.



vLive Events

Virtual/Online Nov 8-Dec 15



Custom Simulcast

Customized training for distributed workforces



OnDemand

E-learning available anytime, anywhere, at your pace



SelfStudy

This course is available in SANS SelfStudy

NEW!

Five-Day Program
30 CPEs
Laptop Required

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

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

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

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

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

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

THERE IS NO TEACHER BUT THE ENEMY!

Author Statement

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

Who Should Attend

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

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

-NATE DEWITT, eBay, Inc.

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

-RIAZ AHMED, ITT



What You Will Receive

- ▶ SIFT Workstation
- ▶ 64 GB Course USB
 - USB loaded with threat intel exercises data, memory captures, network captures, SIFT workstation 3, tools, and documentation
- ▶ Cyber Threat Intelligence Exercise Workbook
 - Exercise book with detailed step by step instructions and examples
- ▶ Cyber Threat Intelligence Poster
- ▶ MP3 audio files of the complete course lecture

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

FOR578 is available via (subject to change):



Featured Training Events

ChicagoChicago, IL Aug 22-27
 Network Security . . Las Vegas, NV. Sep 12-17
 BaltimoreBaltimore, MDOct 10-14
 San FranciscoSan Francisco, CA . . Nov 27-Dec 1
 CDI.Washington, DC Dec 12-17
 Security EastNew Orleans, LA. . . . Jan 9-13



Summit Events

Cyber Threat Intelligence Arlington, VA . .Jan 25-29



Private Training

All SANS courses are available through Private Training.



Custom Simulcast

Customized training for distributed workforces

Six-Day Program
36 CPEs
Laptop Required



www.giac.org/gasf



www.sans.edu

“This class exceeded my expectations. The material is cutting edge!”
-KEVIN McNAMARA,
SAN DIEGO POLICE DEPT.



SMARTPHONES HAVE MINDS OF THEIR OWN.

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

IT'S TIME TO GET SMARTER!

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

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

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

“The analyses methodologies taught in FOR585 will enable examiners to methodically locate files of interest and then quickly analyze them for evidence of interest.” -SANDY OSBORNE, SAVA WORKFORCE SOLUTIONS

You Will Be Able To

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

Who Should Attend

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

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

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

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

Course Day Descriptions

585.1 HANDS ON: Smartphone Overview and Malware Forensics

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

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

585.2 HANDS ON: Android Forensics

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

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

585.3 HANDS ON: iOS Forensics

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

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

585.4 HANDS ON: Backup File and BlackBerry Forensics

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

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

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

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

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

585.6 HANDS ON: Smartphone Forensics Capstone Exercise

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

FOR585 is available via (subject to change):



Featured Training Events

Virginia Beach . . . Virginia Beach, VA . . . Aug 22-27
Network Security . . Las Vegas, NV Sep 12-17
Baltimore Baltimore, MD Oct 10-15



Summit Events

Cyber Threat Intelligence Arlington, VA . . Jan 25-30



Community SANS Events

Madison, WI Sep 19-24



Private Training

All SANS courses are available through Private Training.



Event Simulcast

Virtual/Online Sep 12-17



Custom Simulcast

Customized training for distributed workforces



OnDemand

E-learning available anytime, anywhere, at your pace



SelfStudy

This course is available in SANS SelfStudy

Six-Day Program
36 CPEs
Laptop Required



www.giac.org/grem



www.sans.edu

“The training is very well documented with lots of hands-on labs, in addition, all topics are discussed thoroughly and reinforced.”

-CHAZ HOBSON, DEUTSCHE BANK

This popular course explores malware analysis tools and techniques in depth. FOR610 training has helped forensic investigators, incident responders, security engineers, and IT administrators acquire the practical skills to examine malicious programs that target and infect Windows systems. Understanding the capabilities of malware is critical to an organization's ability to derive the threat intelligence it needs to respond to information security incidents and fortify defenses. The course builds a strong foundation for analyzing malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger and other tools useful for turning malware inside-out.

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

“The course is highly advanced, and the instructor showed us how to perform behavior and code analysis to better understand how malware works.” -DAVID BERNAL, ALSTOM

You Will Be Able To

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

Who Should Attend

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

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

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

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

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

610.1 HANDS ON: Malware Analysis Fundamentals

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

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

610.2 HANDS ON: Malicious Code Analysis

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

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

610.3 HANDS ON: In-Depth Malware Analysis

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

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

610.4 HANDS ON: Self-Defending Malware

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

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

610.5 HANDS ON: Malicious Documents and Memory Forensics

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

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

610.6 HANDS ON: Malware Analysis Tournament

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

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

FOR610 is available via (subject to change):



Featured Training Events

Dallas Dallas, TX. Aug 8-13
 Network Security . . Las Vegas, NV. Sep 12-17
 CDI. Washington, DC Dec 12-17



Summit Events

Cyber Threat Intelligence Arlington, VA . . Jan 25-30



Private Training

All SANS courses are available through Private Training.



Event Simulcast

Virtual/Online Dec 12-17



Custom Simulcast

Customized training for distributed workforces



OnDemand

E-learning available anytime, anywhere, at your pace



SelfStudy

This course is available in SANS SelfStudy

Six-Day Program
46 CPEs
Laptop Not Needed



www.giac.org/gisp

MEETS DoDD 8140
(8570) REQUIREMENTS



www.sans.org/8140



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

SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that has been specifically updated to prepare you to pass the 2016 version of the CISSP® exam.

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

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

-TONY BARNES, UNITED STATES SUGAR CORP

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

Obtaining Your CISSP® Certification Consists of:

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

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

-SEAN HOAR, DAVIS WRIGHT TREMAINE

“I think the course material and the instructor are very relevant for the task of getting a CISSP.

The overall academic exercise is solid.”

-AARON LEWTER, AVAILITY

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

www.sans.org/cissp

Who Should Attend

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

414.1 Introduction; Security and Risk Management

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

Topics: Overview of CISSP® Certification; Introductory Material; Overview of the 8 Domains; Domain 1: Security and Risk Management

414.2 Asset Security and Security Engineering (PART 1)

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

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

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

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

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

414.4 Identity and Access Management

Controlling access to data and systems is one of the primary objectives of information security. Domain 5, Identity and Access Management, strikes at the heart of access control by focusing on identification, authentication, and authorization of accounts. Password-based authentication represents a continued weakness, so Domain 5 stresses multi-factor authentication, biometrics, and secure credential management. The 2016 CISSP® exam underscores the increased role of external users and service providers, and mastery of Domain 5 requires an understanding of federated identity, SSO, SAML, and third-party identity and authorization services like OAuth and OpenID.

Topics: Domain 5: Identity and Access Management

414.5 Security Assessment and Testing; Security Operations

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

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

414.6 Software Development Security

Domain 8 (Software Development Security) describes the requirements for secure software. Security should be "baked in" as part of network design from day one, since it is always less effective when it is added later to a poor design. We will discuss classic development models, including waterfall and spiral methodologies. We will then turn to more modern models, including agile software development methodologies. New content for the 2016 CISSP® exam update will be discussed, including DevOps. We will wrap up this course section by discussing security vulnerabilities, secure coding strategies, and testing methodologies.

Topics: Domain 8: Software Development Security

MGT414 is available via (subject to change):



Featured Training Events

Dallas	Dallas, TX.	Aug 8-13
Chicago	Chicago, IL	Aug 22-27
Virginia Beach . . .	Virginia Beach, VA . .	Aug 28-Sep 2
Network Security . .	Las Vegas, NV.	Sep 12-17
San Diego	San Diego, CA	Oct 23-28
Tysons Corner. . . .	Tysons Corner, VA . . .	Oct 24-29
CDI.	Washington, DC	Dec 12-17
Las Vegas	Las Vegas, NV.	Jan 16-21



Summit Events

Security Awareness . . .	San Francisco, CA. .	Aug 5-10
Healthcare Cybersecurity. .	Houston, TX . .	Nov 16-21



Mentor Classes

Houston, TX		Aug 23-Oct 25
Dallas, TX		Aug 31-Nov 2
Mayfield Village, OH.		Sep 7-16
Arlington, VA.		Sep 13-Nov 15



Private Training

All SANS courses are available through Private Training.



vLive Events

Virtual/Online.		Nov 7-Dec 14
-------------------------	--	--------------



Event Simulcast

Virtual/Online.		Sep 12-17
-------------------------	--	-----------



Custom Simulcast

Customized training for distributed workforces



OnDemand

E-learning available anytime, anywhere, at your pace



SelfStudy

This course is available in SANS SelfStudy

Five-Day Program
33 CPEs
Laptop NOT Needed



www.giac.org/gslc



www.sans.edu

MEETS DoDD 8140
(8570) REQUIREMENTS



www.sans.org/8140

“MGT512 has great info for newly assigned managers to cybersecurity.”

-KERRY T.,

U.S. ARMY CORPS OF ENGINEERS

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

Who Should Attend

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

“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.

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.

“SANS MGT512 has been instrumental in bridging the gaps in my knowledge and has prepared me to take on bigger responsibilities.”

-MIR SHAJEE, ACCENTURE

You Will Be Able To

- ▶ Establish a minimum standard for IT security knowledge, skills, and abilities. In a nutshell, this course covers all of the non-operating system topics that are in MGT512, though not to the same depth. The goal is to enable managers and auditors to speak the same language as system, security, and network administrators.
- ▶ Establish a minimum standard for IT management knowledge, skills, and abilities. I keep running into managers who don't know TCP/IP, and that is OK; but then they don't know how to calculate total cost of ownership (TCO), leaving me quietly wondering what they do know.
- ▶ Save the up-and-coming generation of senior and rapidly advancing managers a world of pain by sharing the things we wish someone had shared with us. As the saying goes, it is OK to make mistakes, just make new ones.

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!

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

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

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

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

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

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

512.3 Secure Communications

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

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

512.4 The Value of Information

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

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

512.5 Management Practicum

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

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

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



MGT512 is available via (subject to change):



Featured Training Events

Boston	Boston, MA	Aug 1-5
Portland	Portland, OR	Aug 8-12
Virginia Beach	Virginia Beach, VA	Aug 22-26
Crystal City	Crystal City, VA	Sep 6-10
Network Security	Las Vegas, NV	Sep 12-16
Tysons Corner	Tysons Corner, VA	Oct 24-28
San Francisco	San Francisco, CA	Nov 27-Dec 1
CDI	Washington, DC	Dec 12-16
Las Vegas	Las Vegas, NV	Jan 16-20



Community SANS Events

Calgary, AB	Oct 27-Nov 24
Las Vegas, NV	Dec 5-9



Summit Events

Healthcare Cybersecurity	Houston, TX	Nov 16-21
------------------------------------	-----------------------	-----------



Mentor Classes

Chambersburg, PA	Aug 5-Sep 23
Minneapolis, MN	Sep 8-Nov 10



Private Training

All SANS courses are available through Private Training.



vLive Events

Virtual/Online	Aug 8-Sep 7
--------------------------	-------------



Custom Simulcast

Customized training for distributed workforces



OnDemand

E-learning available anytime, anywhere, at your pace



SelfStudy

This course is available in SANS SelfStudy

Five-Day Program
30 CPEs
Laptop NOT Needed



www.sans.edu

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

-DJ, ZOETIS

“The instructor did a great job engaging the students. This is a tough class, however, he pulls participation out of everyone.”

-TODD WAGNER, CATERPILLAR

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

-ERIC BURGAN, IDAHO NATIONAL LABS

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

This course teaches security professionals how to do three things:

› Develop Strategic Plans

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

› Create Effective Information Security Policy

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

› Develop Management and Leadership Skills

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

How the Course Works

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

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

Who Should Attend

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

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

514.1 Strategic Planning Foundations

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

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

514.2 Strategic Roadmap Development

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

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

514.3 Security Policy Development and Assessment

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

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

514.4 Leadership and Management Competencies

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

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

514.5 Strategic Planning Workshop

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

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



MGT514 is available via (subject to change):



Featured Training Events

Boston	Boston, MA	Aug 1-5
Crystal City	Crystal City, VA	Sep 6-10
Network Security	Las Vegas, NV	Sep 12-16
Seattle	Seattle, WA	Oct 3-7
Baltimore	Baltimore, MD	Oct 10-14
Miami	Miami, FL	Nov 7-11
CDI	Washington, DC	Dec 12-16
Security East	New Orleans, LA	Jan 9-13



Summit Events

Security Leadership Dallas, TX . . . Sep 29-Oct 4



Private Training

All SANS courses are available through Private Training.



Custom Simulcast

Customized training for distributed workforces



OnDemand

E-learning available anytime, anywhere, at your pace



SelfStudy

This course is available in SANS SelfStudy

Six-Day Program
36 CPEs
Laptop NOT Needed



www.giac.org/gcpm



www.sans.edu



SANS MGT525: IT Project Management, Effective Communication, and PMP® Exam Prep is offered by The SANS Institute, a PMI® Registered Education Provider (R.E.P.). R.E.P.s provide the training necessary to earn and maintain the Project Management Professional (PMP)® and other professional credentials. PMP is a registered mark of Project Management Institute, Inc.

This course has been recently updated to fully prepare you for the 2016 PMP® exam changes. During this class you will learn how to improve your project planning methodology and project task scheduling to get the most out of your critical IT resources. We will utilize project case studies that highlight information technology services as deliverables. MGT525 follows the basic project management structure from the *PMBOK® Guide - Fifth Edition* and also provides specific techniques for success with information assurance initiatives. Throughout the week, we will cover all aspects of IT project management from initiating and planning projects through managing cost, time, and quality while your project is active, to completing, closing, and documenting as your project finishes. A copy of the *PMBOK® Guide – Fifth Edition* is provided to all participants. You can reference the *PMBOK® Guide* and use your course material along with the knowledge you gain in class to prepare for the 2016 updated Project Management Professional (PMP)® Exam and the GIAC Certified Project Manager Exam.

Who Should Attend

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

You Will Be Able To

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

“This course introduced me to an aspect of IT interface that I was unfamiliar with and I now have a better understanding of the business side.”

-DALLAS HASELHORST, SICOR COMPUTER TECHNOLOGIES

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

“This is my 6th SANS training event and SANS continues to deliver. They offer relevant, practical, and highly informative courses that are taught by instructors who truly understand the content.”

-TYLER LEET, COMPUTER SERVICES INC.

PMP, PMBOK and the PMI Registered Education Provider logo are registered marks of the Project Management Institute, Inc.

525.1 Project Management Structure and Framework

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

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

525.2 Project Charter and Scope Management

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

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

525.3 Time and Cost Management

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

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

525.4 Communications and Human Resources

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

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

525.5 Quality and Risk Management

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

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

525.6 Procurement, Stakeholder Management, and Project Integration

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

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



MGT525 is available via (subject to change):



Featured Training Events

Network Security . . . Las Vegas, NV. Sep 12-17



Private Training

All SANS courses are available through Private Training.

Five-Day Program
30 CPEs
Laptop NOT Needed



www.giac.org/gleg



www.sans.edu

You Will Be Able To

- ▶ Work better with other professionals at your organization who make decisions about the law of data security and investigations
- ▶ Exercise better judgment on how to comply with technology regulations, both in the United States and in other countries
- ▶ Evaluate the role and meaning of contracts for technology, including services, software and outsourcing
- ▶ Help your organization better explain its conduct to the public and to legal authorities
- ▶ Anticipate technology law risks before they get out of control
- ▶ Implement practical steps to cope with technology law risk
- ▶ Better explain to executives what your organization should do to comply with information security and privacy law
- ▶ Better evaluate technologies, such as digital signatures, to comply with the law and serve as evidence
- ▶ Make better use of electronic contracting techniques to get the best terms and conditions
- ▶ Exercise critical thinking to understand the practical implications of technology laws and industry standards (such as the Payment Card Industry Data Security Standard)

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

New law on privacy, e-discovery and data security is creating an urgent need for professionals who can bridge the gap between the legal department and the IT department. SANS LEG523 provides this unique professional training, including skills in the analysis and use of contracts, policies and records management procedures.

"Outstanding instructor! Keep doing what you are doing."

-PAUL MOBLEY, FIS GLOBAL

This course covers the law of business, contracts, fraud, crime, IT security, liability and policy – all with a focus on electronically stored and transmitted records. It also teaches investigators how to prepare credible, defensible reports, whether for cyber crimes, forensics, incident response, human resource issues or other investigations.

Each successive day of this five-day course builds upon lessons from the earlier days in order to comprehensively strengthen your ability to help your enterprise (public or private sector) cope with illegal hackers, botnets, malware, phishing, unruly vendors, data leakage, industrial spies, rogue or uncooperative employees, or bad publicity connected with IT security.

Recent updates to the course address hot topics such as legal tips on confiscating and interrogating mobile devices, the retention of business records connected with cloud computing and social networks like Facebook and Twitter, and analysis and response to the risks and opportunities surrounding open-source intelligence gathering.

Over the years this course has adopted an increasingly global perspective. Non-U.S. professionals attend LEG523 because there is no training like it anywhere else in the world. For example, a lawyer from the national tax authority in an African country took the course because electronic filings, evidence and investigations have become so important to her work. International students help the instructor; U.S. attorney Benjamin Wright, constantly revise the course and include more content that crosses borders.

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

-TOM S., CASE WESTERN RESERVE UNIVERSITY

Who Should Attend

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

LEG523 is available via (subject to change):



Featured Training Events

Chicago Chicago, IL Aug 22-27
Network Security . . Las Vegas, NV Sep 14-17



Private Training

All SANS courses are available through Private Training.



Custom Simulcast

Customized training for distributed workforces



OnDemand

E-learning available anytime, anywhere, at your pace



SelfStudy

This course is available in SANS SelfStudy

Six-Day Program
36 CPEs
Laptop Required



www.giac.org/gсна



www.sans.edu

MEETS DoDD 8140
(8570) REQUIREMENTS



www.sans.org/8140

You Will Be Able To

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

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

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

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

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

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

Who Should Attend

- ▶ Auditors seeking to identify key controls in IT systems
- ▶ Audit professionals looking for technical details on auditing
- ▶ Managers responsible for overseeing the work of an audit or security team
- ▶ Security professionals newly tasked with audit responsibilities
- ▶ System and network administrators looking to better understand what an auditor is trying to achieve, how auditors think, and how to better prepare for an audit
- ▶ System and network administrators seeking to create strong change control management and detection systems for the enterprise

AUD507 is available via (subject to change):



Featured Training Events

Dallas Dallas, TX. Aug 8-13
Network Security . . Las Vegas, NV. Sep 12-17
Tysons Corner. . . Tysons Corner, VA . . . Oct 24-29
CDI. Washington, DC . . . Dec 12-17



Private Training

All SANS courses are available through Private Training.



Custom Simulcast

Customized training for distributed workforces



OnDemand

E-learning available anytime, anywhere, at your pace



SelfStudy

This course is available in SANS SelfStudy

Six-Day Program
36 CPEs
Laptop Required



www.giac.org/gweb



www.sans.edu

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

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

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

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

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

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

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

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

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

“This training has been very helpful in making me more aware. I have a better understanding of vulnerabilities and what can be done to minimize them in my future development projects.”

-LERMA WINCHELL, ViSTAR CREDIT UNION

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

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

Course Day Descriptions

522.1 HANDS ON: Web Basics and Authentication Security

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

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

522.2 HANDS ON: Web Application Common Vulnerabilities and Mitigations

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

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

522.3 HANDS ON: Proactive Defense and Operation Security

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

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

522.4 HANDS ON: AJAX and Web Services Security

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

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

522.5 HANDS ON: Cutting-Edge Web Security

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

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

522.6 HANDS ON: Capture and Defend the Flag Exercise

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

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

DEV522 is available via (subject to change):



Featured Training Events

Network Security . . . Las Vegas, NV. Sep 12-17
CDI. Washington, DC Dec 12-17



Community SANS Events

Salt Lake City, UT Sep 26-Oct 1
Detroit, MI. Oct 24-29



Private Training

All SANS courses are available through Private Training.



Custom Simulcast

Customized training for distributed workforces



OnDemand

E-learning available anytime, anywhere, at your pace



SelfStudy

This course is available in SANS SelfStudy

Four-Day Program
24 CPEs
Laptop Required



www.giac.org/gssp-java

You Will Be Able To

- ▶ Use a web application proxy to view and manipulate HTTP requests and responses
- ▶ Review and perform basic exploits of common web application vulnerabilities, such as those found among the SANS/CWE Top 25 Most Dangerous Software Errors and the OWASP Top 10:
 - Cross-site scripting (XSS)
 - Cross-site request forgery (CSRF)
 - SQL injection
 - Parameter manipulation
 - Open redirect
 - Session hijacking
 - Clickjacking
 - Authentication and access control bypass
- ▶ Mitigate common web application vulnerabilities using secure coding practices and Java libraries, including:
 - Input validation
 - Blacklist and whitelist validation
 - Regular expressions
 - Output encoding
 - Content Security Policy
 - Client-side security headers
- ▶ Build applications using:
 - Java Enterprise Edition authentication
 - Basic and form-based authentication
 - Client certificates
 - Secure Sockets Layer/Transport Layer Security (SSL/TLS)
 - Java Secure Sockets Extension
 - Secure password storage techniques
 - Java Cryptography Architecture
 - Security Manager
- ▶ Implement a secure software development lifecycle, including code review, static analysis and dynamic analysis techniques.

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

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

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

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

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

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

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

PCI Compliance

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

Who Should Attend

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

DEV541 is available via (subject to change):



Featured Training Events

Network Security . . . Las Vegas, NV. Sep 14-17
San Diego San Diego, CA Oct 23-26



Community SANS Events

Salt Lake City, UT Aug 29-Sep 1
Nashville, TN Sep 26-29



Private Training

All SANS courses are available through Private Training.



Event Simulcast

Virtual/Online Oct 23-26



Custom Simulcast

Customized training for distributed workforces



OnDemand

E-learning available anytime, anywhere, at your pace



SelfStudy

This course is available in SANS SelfStudy

Four-Day Program
24 CPEs
Laptop Required



www.giac.org/gssp-net

ASP.NET and the .NET framework have provided web developers with tools that allow them an unprecedented degree of flexibility and productivity. However, these sophisticated tools make it easier than ever to miss the little details that allow security vulnerabilities to creep into an application. Since ASP.NET 2.0, Microsoft has done a fantastic job of integrating security into the ASP.NET framework, but the responsibility is still on application developers to understand the limitations of the framework and ensure that their own code is secure.

You Will Be Able To

- ▶ Use a web application proxy to view and manipulate HTTP requests and responses
- ▶ Review and perform basic exploits of common web application vulnerabilities, such as those found among the SANS/CWE Top 25 Most Dangerous Software Errors and the OWASP Top 10:
 - Cross-Site Scripting
 - Parameter Manipulation
 - Open Redirect
 - Unvalidated Forwards
 - SQL Injection
 - Session Hijacking
 - Clickjacking
 - Cross-Site Request Forgery
 - Man-in-the-middle
- ▶ Mitigate common web application vulnerabilities using industry best practices in the .NET framework, including:
 - Input Validation
 - Blacklist and Whitelist Validation
 - Regular Expressions
 - Command Encoding
 - Output Encoding
 - Content Security Policy
 - Client-side Security Headers
- ▶ Understand built-in ASP .NET security mechanisms, including:
 - AntiForgeryToken
 - Data Annotations
 - Event Validation
 - Request Validation
 - View State
 - Entity Framework
 - ASP.NET Identity
 - Forms Authentication
 - Membership Provider
 - WCF
 - Web API
- ▶ Apply industry best practices (NIST, PCI) for cryptography and hashing in the .NET framework.
- ▶ Implement a secure software development lifecycle (SDLC) to include threat modeling, static analysis and dynamic analysis.

Have you ever wondered if the built-in ASP.NET validation is effective? Have you been concerned that Windows Communication Foundation (WCF) services might be introducing unexamined security issues into your application? Should you feel uneasy relying solely on the security controls built into the ASP.NET framework?

“It is shocking to see how much we are missing in our code. I am going back to change the code immediately.”

-RUOJIE WANG, NEW JERSEY HOSPITAL ASSOCIATION

This comprehensive course covers a huge set of skills and knowledge. It is not a high-level theory course. It is about real programming. Students examine actual code, work with real tools, build applications, and gain confidence in the resources they need to improve the security of .NET applications.

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

The class culminates with a security review of a real-world open-source application. Students will conduct a code review, review a penetration test report, perform security testing to actually exploit real vulnerabilities, and finally, using the secure coding techniques that they have learned in class, implement fixes for these issues.

PCI Compliance

Section 6.5 of the Payment Card Industry (PCI) Data Security Standard (DSS) instructs auditors to verify processes that require training in secure coding techniques for developers. This is the course for you if your application processes cardholder data and you are required to meet PCI compliance.

Who Should Attend

- ▶ ASP.NET developers who want to build more secure web applications
- ▶ .NET framework developers
- ▶ Software engineers
- ▶ Software architects
- ▶ Developers who need to be trained in secure coding techniques to meet PCI compliance
- ▶ Application security auditors
- ▶ Technical project managers
- ▶ Senior software QA specialists
- ▶ Penetration testers

DEV544 is available via (subject to change):



Featured Training Events

Network Security . . Las Vegas, NV. Sep 10-13



Private Training

All SANS courses are available through Private Training.



Custom Simulcast

Customized training for distributed workforces



OnDemand

E-learning available anytime, anywhere, at your pace



SelfStudy

This course is available in SANS SelfStudy

Five-Day Program
30 CPEs
Laptop Required



www.giac.org/gicsp



www.sans.edu

“This course was information packed, and a lot of invaluable instruction and knowledge to consume.”

-ROB RUEL, EDISON

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

The course will provide you with:

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

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

With the dynamic nature of industrial control systems, many engineers do not fully understand

the features and risks of many devices. In addition, IT support personnel who provide the communications paths and network defenses do not always grasp the systems' operational drivers and constraints. This course is designed to help traditional IT personnel fully understand the design principles underlying control systems and how to support those systems in a manner that ensures availability and integrity. In parallel, the course addresses the need for control system engineers and operators to better understand the important role they play in cybersecurity. This starts by ensuring that a control system is designed and engineered with cybersecurity built into it, and that cybersecurity has the same level of focus as system reliability throughout the system lifecycle.

When these different groups of professionals complete this course, they will have developed an appreciation, understanding, and common language that will enable them to work together to secure their industrial control system environments. The course will help develop cyber-secure-aware engineering practices and real-time control system IT/OT support carried out by professionals who understand the physical effects of actions in the cyber world.

“The real-world relationship was key to applying the information. The instructor relates his experiences with the attacks.”

-TAYLOR A., MARFORCYBER

Who Should Attend

The course is designed for the range of individuals who work in, interact with, or can affect industrial control system environments, including asset owners, vendors, integrators, and other third parties. These personnel primarily come from four domains:

- IT (includes operational technology support)
- IT security (includes operational technology security)
- Engineering
- Corporate, industry, and professional standards

You Will Be Able To

- Run Windows command line tools to analyze the system looking for high-risk items
- Run Linux command line tools (ps, ls, netstat, ect) and basic scripting to automate the running of programs to perform continuous monitoring of various tools
- Install VMWare and create virtual machines to create a virtual lab to test and evaluate tools/security of systems
- Better understand various industrial control systems and their purpose, application, function, and dependencies on network IP and industrial communications
- Work with operating systems (system administration concepts for Unix/Linux and/or Windows operating systems)
- Work with network infrastructure design (network architecture concepts, including topology, protocols, and components)
- Better understand the systems' security lifecycle
- Better understand information assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)
- Use your skills in computer network defense (detecting host and network-based intrusions via intrusion detection technologies)
- Implement incident response and handling methodologies

410.1 ICS Overview

Students will develop and reinforce a common language and understanding of Industrial Control System (ICS) cybersecurity as well as the important considerations that come with cyber-to-physical operations within these environments. Each student will receive programmable logic controller (PLC) hardware to keep. The PLC contains physical inputs and outputs that will be programmed in class and mapped to an operator interface, or HMI, also created in class. This improved hardware-enabled approach provides the necessary cyber-to-physical knowledge that allows students to better understand important ICS operational drivers and constraints that require specific safety protection, communications needs, system management approaches, and cybersecurity implementations. Essential terms, architectures, methodologies, and devices are all covered to build a common language for students from a variety of different roles.

Topics: Global Industrial Cybersecurity Professional (GICSP) Overview; Overview of ICS; Field Components; Programming Controllers; Supervisory Components; Types of ICS Systems; IT & ICS Differences; Physical Security; ICS Network Architecture

410.2 ICS Attack Surface

If you know the adversary's approaches to attacking an ICS environment, you will be better prepared to defend that environment. Numerous attack vectors exist within an ICS environment. Some are similar to traditional IT systems, while others are more specific to ICS. During Day 2, defenders will develop a better understanding of where these specific attack vectors exist, as well as the tools to use to discover vulnerabilities and exploit them. Each student will use a vulnerable target virtual machine to further understand attacks targeting the types of web servers used on many ICS devices for management purposes. Simulators will be configured to allow students to conduct attacks against unauthenticated ICS protocols. A variety of data samples are used to examine additional attack vectors on remote devices.

Topics: ICS Attack Surface; Attacks on HMIs and UIs; Attacks on Control Servers; Attacks on Network Communications; Attacks on Remote Devices

410.3 Defending ICS Servers and Workstations

Students will learn essential ICS-related server and workstation operating system capabilities, implementation approaches, and system management practices. Students will receive and work with both Windows- and Linux-based virtual machines in order to understand how to monitor and harden these hosts from attack. Students will examine concepts that benefit ICS systems such as system hardening, log management, monitoring, alerting, and audit approaches, then look at some of the more common applications and databases used in ICS environments across multiple industries.

Topics: Windows in ICS; Linux/Unix in ICS; Updates and Patching; Processes and Services; Configuration Hardening; Endpoint Defenses; Automation and Auditing; Log Management; Databases and Historians

410.4 Defending ICS Networks and Devices

With an understanding of the ICS environment, the attack vectors that exist, and the defender-specific capabilities available on servers, workstations, and applications, students will now learn network-specific defense approaches. We'll first examine common IT protocols and network components used within ICS environments, then discuss ICS-specific protocols and devices. Technologies used to defend ICS networks will be reviewed along with implementation approaches. Students will interact with ICS traffic and develop skills to analyze it, then work through a number of tools to further explore a series of staged adversary actions conducted in a lab environment.

Topics: Network Fundamentals; Ethernet; TCP/IP Protocol Suite; ICS Protocols over TCP/IP; Enforcement Zone Devices; Honey pots; Wireless in Control Systems; Network Capture Forensics; Field and Plant Floor Equipment; Cryptography Fundamentals

410.5 ICS Security Governance

Students will learn about the various models, methodologies, and industry-specific regulations that are used to govern what must be done to protect critical ICS systems. Key business processes that consider risk assessments, disaster recovery, business impact analysis, and contingency planning will be examined from the perspective of ICS environments. On this final course day, students will work together on an incident response exercise that places them squarely in an ICS environment that is under attack. This exercise ties together key aspects of what has been learned throughout the course and presents students with a scenario to review with their peers. Specific incident-response roles and responsibilities are considered, and actions available to defenders throughout the incident response cycle are explored. Students will leave with a variety of resources for multiple industries and will be well prepared to pursue the GICSP, an important ICS-focused professional certification.

Topics: Information Assurance Foundations; Security Policies; Contingency and Continuity Planning; Risk Assessment and Auditing; Attack Tree Analysis; Password Management; Incident Handling; Incident Response; Resources

ICS410 is available via (subject to change):



Featured Training Events

AlaskaAlaska, AK Aug 22-26
 ChicagoChicago, IL Aug 22-26
 Network Security . .Las Vegas, NV. Sep 12-16
 SeattleSeattle, WA Oct 3-7
 Las VegasLas Vegas, NV.Jan 16-20



Private Training

All SANS courses are available through Private Training.



Custom Simulcast

Customized training for distributed workforces



OnDemand

E-learning available anytime, anywhere, at your pace



SelfStudy

This course is available in SANS SelfStudy

Five-Day Program
30 CPEs
Laptop Required

“Very powerful tools and concepts!”

-RANDY WAGNER, BASIN ELECTRIC



ICS515: ICS Active Defense and Incident Response

will help you deconstruct ICS cyber attacks, leverage an active defense to identify and counter threats in your ICS, and use incident response procedures to maintain the safety and reliability of operations. This course will empower students to understand their networked industrial control system environment, monitor it for threats, perform incident response against identified threats, and learn from interactions with the adversary to enhance network security. This process of monitoring, responding to, and learning from threats internal to the network is known as active defense. An active defense is the approach needed to counter advanced adversaries targeting ICS, as has been seen with malware such as Stuxnet, Havex, and BlackEnergy2. Students can expect to come out of this course with the ability to deconstruct targeted ICS attacks and fight these adversaries and others. The course uses a hands-on approach and real-world malware to break down cyber attacks on ICS from start to finish.

Students will gain a practical and technical understanding of leveraging active defense concepts such as using threat intelligence, performing network security monitoring, and utilizing malware analysis and incident response to ensure the safety and reliability of operations. The strategy and technical skills presented in this course serve as a basis for ICS organizations looking to show that defense is do-able.

“ICS environments are unique and require specialized skills and processes to effectively manage the threats and vulnerabilities.”

-JOHN BALLENTINE, ETHOSENERGY

Who Should Attend

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

What You Will Receive

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

This Course Will Prepare You To

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

515.1 Threat Intelligence

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

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

515.2 Asset Identification and Network Security Monitoring

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

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

515.3 Incident Response

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

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

515.4 Threat and Environment Manipulation

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

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

515.5 Active Defense and Incident Response Challenge

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

Topics:

Scenario One: Identify the assets and map the ICS networks; Perform ICS network security monitoring to identify the abnormalities; Execute ICS incident response procedures into the SANS Cyber City data files; Analyze the malicious capability and determine if the threat is an insider threat or a targeted external threat

Scenario Two: Identify the software and information present on the DCS; Leverage ICS active defense concepts to identify the real-world malware; Determine the impact on operations and remediation needs

ICS515 is available via (subject to change):



Featured Training Events

Virginia Beach . . . Virginia Beach, VA . . . Aug 29-Sep 2
 Network Security . . . Las Vegas, NV. Sep 12-16
 Baltimore Baltimore, MD Oct 10-14
 CDI. Washington, DC Dec 12-16
 Security East New Orleans, LA. Jan 9-13



Private Training

All SANS courses are available through Private Training.



Custom Simulcast

Customized training for distributed workforces



OnDemand

E-learning available anytime, anywhere, at your pace



SelfStudy

This course is available in SANS SelfStudy

“This course raised my awareness of incidents attacking ICS today, and broadened my knowledge of techniques and tools to manage them effectively.”

-STEVEN ROMERO, WGMI

NEW!

Five-Day Program
30 CPEs
Laptop Required

“SANS coursework is the most thorough learning available anywhere.

What you learn is not only conceptual, but it also is hands-on showing you what to do, why you do it, and how you can apply what you learn to real-world solutions to problems.”

-DUANE TUCKER, BAYMARK PARTNERS

Course Authorship

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

The Essentials for NERC Critical Infrastructure Protection course empowers students with knowledge of the “What” and the “How” of the Version 5/6 standards. The course addresses the role of the Federal Energy Regulatory Commission (FERC), North American Electric Reliability Corporation (NERC), and the Regional Entities, provides multiple approaches for identifying and categorizing BES Cyber Systems, and helps asset owners determine the requirements applicable to specific implementations. Additionally, the course covers implementation strategies for the Version 5/6 requirements with a balanced practitioner approach to both cybersecurity benefits, as well as regulatory compliance.

Course Day Descriptions

ICS456.1: Asset Identification and Governance

A transition is under way from NERC Critical Infrastructure Protection (CIP) programs that are well defined and understood to a new CIP paradigm that expands its scope into additional environments and adds significantly more complexity. On day one, students will develop an understanding of the electric sector regulatory structure and history as well as an appreciation for how the CIP standards fit into the overall framework of the reliability standards.

ICS456.2: Access Control and Monitoring Strong physical and cyber access controls are at the heart of any good cybersecurity program. On day two we move beyond the “what” of CIP compliance to understanding the “why” and the “how.”

ICS456.3: System Management CIP-007 has consistently been one of the most violated standards going back to CIP version 1. With the CIP standards moving to a systematic approach with varying requirement applicability based on system impact rating, the industry now has new ways to design and architect system management approaches. Throughout day three, students will dive into CIP-007.

ICS456.4: Information Protection and Response Education is key to every organization’s success with NERC CIP. After this session on information protection and response, ICS456 students will be knowledgeable advocates for CIP when they return to their place of work.

ICS456.5: CIP Process On the final day students will learn the key components for running an effective CIP compliance program. Topics will include CIP processes for maintaining compliance, preparing for an audit and following up on it, CIP industry activities, standards process, and the CIP of the future.

Who Should Attend

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

ICS456 is available via (subject to change):



Featured Training Events

Portland	Portland, OR	Aug 8-12
CDI	Washington, DC	Dec 12-16
Security East	New Orleans, LA	Jan 9-13



Private Training

All SANS courses are available through Private Training.

NEW! Physical Security Specialist – Full Comprehensive Edition

Six Days | 36 CPEs | Laptop Required

This course will leave with a full awareness of how to best protect buildings and grounds from unauthorized access, as well as how to compromise most existing physical security in order to gain access themselves. Our subject-matter experts will immerse you in all the necessary components of a well-layered physical defense system and then teach you how to conduct a thorough site analysis of a facility.

NEW! Health Care Security Essentials

Two Days | 12 CPEs | Laptop Required

Health Care Security Essentials is designed to provide SANS students with an introduction to current and emerging issues in health care information security and regulatory compliance. The class provides a foundational set of skills and knowledge for health care security professionals by integrating case studies, hands-on labs, and tips for securing and monitoring electronic protected health information.

NEW! Embedded Device Security Assessments for the Rest of Us

Two Days | 12 CPEs | Laptop Required

The challenge we all face is how to assess the security of these devices accurately, efficiently, and thoroughly. If you've wondered how much damage attackers can do with devices such as printers, wireless routers, thermostats, TVs, and even Wi-Fi-enabled treadmills, look no further than this course. The goal of this course is to enable you to uncover embedded system vulnerabilities as part of your duties as a security professional.

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

Two Days | 12 CPEs | Laptop Required

Topics

- ▶ 125KHz Credentials
- ▶ 125/134KHz Vehicle Transponder Overview
- ▶ 13.56MHz Credentials and Smart Cards
- ▶ Practical Cloning in the Field, Advanced Format Downgrade Attacks
- ▶ Backend Detailed Overview, Weaknesses, and Attacks
- ▶ Defeating Tamper Detection
- ▶ Defenses and Mitigation

NEW! Assessing and Exploiting Control Systems

Six Days | 36 CPEs | Laptop Required

This is not your traditional SCADA/ICS/IoT security course! This course teaches hands-on penetration testing techniques used to test embedded electronic field devices, network protocols, RF communications, and controlling servers of ICS and Smart Grid systems like PLCs, RTUs, smart meters, Home Area Networks (HAN), smart appliances, SCADA, substation automation, and synchrophasors.

Critical Infrastructure and Control System Cybersecurity

Five Days | 30 CPEs | Laptop Provided

This is an intermediate to advanced course covering control system cybersecurity vulnerabilities, threats and mitigating controls. This course will provide hands-on analysis of control system environments allowing students to understand the environmental, operational and economic impacts of attacks like Stuxnet and supporting mitigating controls.

Physical Penetration Testing

Two Days | 12 CPEs

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

Offensive Countermeasures: The Art of Active Defenses

Two Days | 12 CPEs | Laptop Required

Active Defenses have been capturing a large amount of attention in the media lately. There are those who thirst for vengeance and want to directly attack the attackers. There are those who believe that any sort of active response directed at an attacker is wrong. We believe the answer is somewhere in between. In this class you will learn how to force attackers to take more moves to attack your network – moves that can increase your ability to detect them. You will learn how to gain more knowledge about who is attacking you and why. You will also find out how to get access to a bad guy's system. And most importantly, you will find out how to do the above legally.

ADDITIONAL TRAINING COURSES

SECURITY

SEC440: Critical Security Controls: Planning, Implementing, and Auditing (2 DAYS)

This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS). These Critical Security Controls are rapidly becoming accepted as the highest priority list of what must be done and proven before anything else at nearly all serious and sensitive organizations. These controls were selected and defined by the U.S. military and other government and private organizations (including NSA, DHS, GAO, and many others) that are the most respected experts on how attacks actually work and what can be done to stop them. They defined these controls as their consensus for the best way to block known attacks and help find and mitigate damage from the attacks that get through.

SEC480: Top 4 Mitigation Strategies: Implementing & Auditing NEW! (3 DAYS)

Over the past three years, there has been an ever-increasing focus on preventing targeted cyber intrusions around the world. The Australian Signals Directorate (ASD) responded to the sharp increase in observed intrusion activity with the Strategies to Mitigate Targeted Cyber Intrusions. This is a list of 35 strategies ranked in order of effectiveness that organizations can implement to reduce the likelihood of a successful targeted cyber intrusion. After attending this hands-on course, individuals will be able to effectively implement and audit the Top 4 mitigation strategies in their own environments to achieve a significant level of security.

SEC524: Cloud Security Fundamentals (2 DAYS)

This 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.

SEC546: IPv6 Essentials (2 DAYS)

IPv6 is currently being implemented at a rapid pace in Asia in response to the exhaustion of IPv4 address space, which is most urgently felt in rapidly 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 and more important to global commerce. This course will introduce network administrators and security professionals to the basic concepts of IPv6.

SEC567: Social Engineering for Penetration Testers NEW! (2 DAYS)

This course covers the principles of persuasion and the psychological foundations required to craft effective attacks and bolsters this with many examples of what works, drawing on cyber criminal cases and on the experiences of the authors in combating cyber crime. On top of these principles we provide a number of tools and labs centered around the key technical skills required to measure your social engineering success and report it to your company or client.

SEC580: Metasploit Kung Fu for Enterprise Pen Testing (2 DAYS)

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.

IT AUDIT

AUD480: Top 4 Mitigation Strategies: Implementing & Auditing NEW! (3 DAYS)

Over the past three years, there has been an ever-increasing focus on preventing targeted cyber intrusions around the world. The Australian Signals Directorate (ASD) in Australia responded to the sharp increase in observed intrusion activity with the Strategies to Mitigate Targeted Cyber Intrusions. This is a list of 35 strategies ranked in order of effectiveness that organizations can implement to reduce the likelihood of a successful targeted cyber intrusion.

AUD440: Critical Security Controls: Planning, Implementing and Auditing (2 DAYS)

This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS). These Critical Security Controls are rapidly becoming accepted as the highest priority list of what must be done and proven before anything else at nearly all serious and sensitive organizations. These controls were selected and defined by the U.S. military and other government and private organizations (including NSA, DHS, GAO, and many others) that are the most respected experts on how attacks actually work and what can be done to stop them. They defined these controls as their consensus for the best way to block known attacks and help find and mitigate damage from the attacks that get through.

ADDITIONAL TRAINING COURSES

MANAGEMENT

MGT305: Technical Communication and Presentation Skills for Security Professionals (1 DAY)

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



www.sans.edu

MGT405: Critical Infrastructure Protection (2 DAYS)

This class is designed to give the student a full examination of the scope of critical infrastructure vulnerabilities, the dependence of critical infrastructure on the Internet, and Internet security problems. No laptop is required, but the subject material requires at least a working knowledge of computer networks and business decision-making. The ideal student is a manager, supervisor, senior engineer, or other professional with a strong working knowledge of plant operations or a government official with responsibilities for CIP policy development wanting to learn more about the interdependence of critical infrastructure and the dangers posed by the global Internet.

MGT415: A Practical Introduction to Cybersecurity Risk Management NEW! (2 DAYS)

There are simply too many threats, too many potential vulnerabilities that could exist, and simply not enough resources to create an impregnable security infrastructure. Therefore all organizations, whether they do so in an organized manner or not, will make priority decisions on how best to defend their valuable data assets. Risk management should be the foundational tool used to facilitate thoughtful and purposeful defense strategies.

MGT433: Securing The Human: How to Build, Maintain, and Measure a High-Impact Awareness Program (2 DAYS)

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.



www.sans.edu

MGT535: Incident Response Team Management (2 DAYS)

This course discusses the often-neglected topic of managing an incident response team. Given the frequency and complexity of today's cyber attacks, incident response is a critical function for organizations. Incident response is the last line of defense. Detecting and efficiently responding to incidents requires strong management processes, and managing an incident response team requires special skills and knowledge.

DEVELOPER

DEV531: Defending Mobile Applications Security Essentials NEW! (2 DAYS)

This course 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.

DEV534: Secure DevOps: A Practical Introduction NEW! (2 DAYS)

This course explains the fundamentals of DevOps, and how DevOps teams can build and deliver secure software. It will explain the principles and practices and tools in DevOps and how they can be leveraged to improve the reliability, integrity and security of systems.

DEV543: Secure Coding in C & C++ (2 DAYS)

The C and C++ programming languages are the bedrock for most operating systems, major network services, embedded systems and system utilities. Even though C and, to a lesser extent, C++, are well understood languages, the flexibility of the language and inconsistencies in the standard C libraries have led to an enormous number of discovered vulnerabilities over the years. The unfortunate truth is that there are probably more undiscovered vulnerabilities than there are known vulnerabilities! This course will cover all of the most common programming flaws that affect C and C++ code.

For schedules, course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/courses

SANS NETWARS EXPERIENCE

Information Security Challenges

Exciting and Interactive
Designed for Novice to Advanced

Play in Teams or Solo

Free for All SANS Students
Taking a 5 or 6-Day Course



“NetWars takes the concepts in the class and gives you an opportunity to put them into action.”

– Kyle McDaniel, Lenovo

“Really great learning experience! Very challenging and educational!”

– Chad Eckles, Deloitte

Many ways to experience NetWars

LIVE

ONLINE

Core
NETWARS
EXPERIENCE

DFIR
NETWARS
EXPERIENCE

Free for SANS students at select SANS Training Events

Core
NETWARS
CONTINUOUS

DFIR
NETWARS
CONTINUOUS

Purchase Four Months of Online Access – New Challenges

To request a free seven day trial of Core NetWars Continuous, contact netwars@sans.org

www.sans.org/netwars

GIAC CERTIFICATION DOMAINS

APPLICATION
SECURITY

CYBER
DEFENSE

MANAGEMENT
LEGAL AND
AUDIT

PENETRATION
TESTING

DIGITAL
FORENSICS

"It's an awesome effort: great questions, excellent material and presentation throughout the (training event) week. I've really enjoyed it and will recommend it to many. Thank you GIAC/SANS!"

– Nicolas B., Intrasys,
GIAC Certified Incident Handler (GCIH)

"I think the exam was both fair and practical. These are the kind of real world problems I expect to see in the field."

– Carl Hallberg, Wells Fargo,
GIAC Reverse Engineering Malware (GREM)

"GIAC made the testing process much better than other organizations. The material is spot on with what I do at work, daily."

– Jason Pfister, EWEB,
GIAC Continuous Monitoring (GMON)

"It feels like SANS and GIAC are working with the candidates to help them to meet the required standards, which are achievable with hard work."

– Thomas Gurney,
GIAC Certified Intrusion Analyst (GCIA)

GIAC The Highest Standard in Cybersecurity Certification.

Job-Specific, Specialized Focus

Today's cyber attacks are highly sophisticated and exploit specific vulnerabilities. Broad and general InfoSec certifications are no longer enough. Professionals need the specific skills and specialized knowledge required to meet multiple and varied threats. That's why GIAC has more than 30 certifications, each focused on specific job skills and each requiring unmatched and distinct knowledge.

Deep, Real-World Knowledge

Theoretical knowledge is the ultimate security risk. Deep, real-world knowledge and hands-on skills are the only reliable means to reduce security risk. Nothing comes close to a GIAC certification to ensure that this level of real-world knowledge and skill has been mastered.

Most Trusted Certification Design

The design of a certification exam impacts the quality and integrity of a certification. GIAC exam content and question design are developed through a rigorous process led by GIAC's on-staff psychometrician and reviewed by experts in each area. More than 78,000 certifications have been issued since 1999. GIAC certifications meet ANSI standards.

SANS

GIAC



DEEPER KNOWLEDGE. ADVANCED SECURITY.

WWW.GIAC.ORG

SANS Technology Institute

Join the only graduate degree program designed and taught by SANS' world-class faculty.

"I chose the SANS graduate program because the technical content and faculty are unparalleled, and the mix of live and online instruction fit into my work life."

- Joshua Lewis, EY,
MSISE candidate



Industry-Recognized Certifications

Students earn GIAC certifications during most technical courses.



Tuition Reimbursement

The SANS Technology Institute is approved to accept and/or certify Veterans for education benefits.

Built on proven SANS courses and GIAC certification exams, and accessible through live classes around the country and online from work or home, our graduate programs transform the best of SANS training and faculty into an unparalleled educational experience that is custom designed for a working professional.

Master of Science Degrees

The master's programs of the SANS Technology Institute provide the foremost education for cyber professionals.

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

Graduate Certificates

The certificate programs offer individuals the opportunity to earn a post-baccalaureate, graduate-level credential by completing a series of three to four related technical courses.

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

Accreditation

The SANS Technology Institute is accredited by the Middle States Commission on Higher Education, 3624 Market Street, Philadelphia, PA 19104 (267-284-5000). The Middle States Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

GI Bill® is a registered trademark of the U.S. Department of Veterans Affairs (VA). More information about education benefits offered by VA is available at the official U.S. government Web site at www.benefits.va.gov/gjbill.

Visit sans.edu for complete information on courses, admissions, and tuition.

Department of Defense Directive 8140

(DoDD 8140)



www.sans.org/dodd-8140

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

Compliance/Recertification:

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

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

DoD Baseline IA Certifications

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

Computer Network Defense (CND) Certifications

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

Information Assurance System Architecture & Engineering (IASAE) Certifications

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

Computer Environment (CE) Certifications

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

SANS Training Courses for DoDD Approved Certifications

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



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 (GCIH) | 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

SEC502 (GPPA) | SEC505 (GCWN) | SEC506 (GCUX)

Red Team Courses

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

Real Threats
Real Skills
Real Success
Join Today!

Contact us at onsite@sans.org to get started!

www.sans.org/cyber-guardian

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

www.sans.org/vouchers

VOUCHER PROGRAM



Training Investment & Bonus Funds

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

The investment and bonus funds:

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

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



Flexibility & Control

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

With the SANS Admin Tool, the Administrator can:

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

By creating a Voucher Account, your organization can:

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

Getting Started

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

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



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



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

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

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

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

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

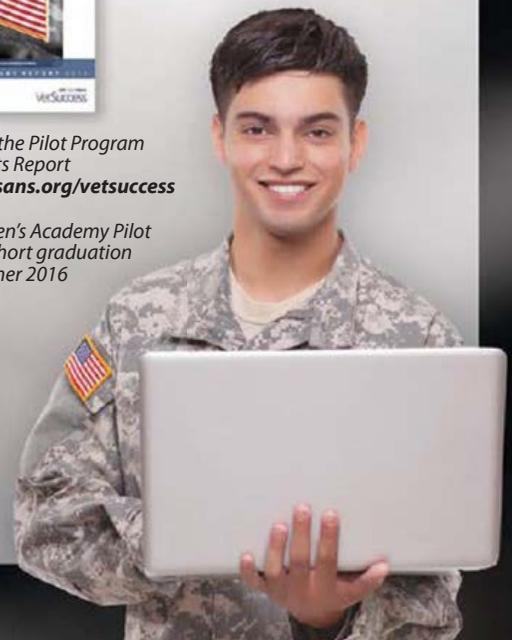
Find out how your organization can benefit from hiring graduates or launching an academy to meet your specific talent needs.

sans.org/cybertalent/immersion-academy
Email: immersionacademy@sans.org



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

Women's Academy Pilot
1st cohort graduation
Summer 2016



SANS | CyberTalent
IMMERSION ACADEMY

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

SANS TRAINING EVENTS

FEATURED EVENTS

Boston Boston, MA Aug 1-6	Virginia Beach Virginia Beach, VA Aug 22-Sep 2	Baltimore Baltimore, MD Oct 10-15	San Francisco San Francisco, CA Nov 27-Dec 2
Portland Portland, OR Aug 8-13	Crystal City Crystal City, VA Sep 6-11	Tysons Corner Tysons Corner, VA Oct 22-29	CDI Washington, DC Dec 10-17
Dallas Dallas, TX Aug 8-13	Network Security Las Vegas, NV Sep 10-19	San Diego San Diego, CA Oct 23-28	Security East New Orleans, LA Jan 9-14
Chicago Chicago, IL Aug 22-27	Seattle Seattle, WA Oct 3-8	Miami Miami, FL Nov 7-12	Las Vegas Las Vegas, NV Jan 16-21
Alaska Anchorage, AK Aug 22-27			

COMMUNITY SANS EVENTS

Atlanta, GA SEC511 Aug 1-6	Salt Lake City, UT DEV541 Aug 29-Sep 1	Long Beach, CA SEC566 Sep 26-30	Richmond, VA SEC401 Oct 17-22	Phoenix, AZ SEC511 Nov 7-12
Columbia, MD SEC560 Aug 1-6	Albuquerque, NM SEC401 Sep 12-17	New York, NY SEC566 Sep 26-30	San Antonio, TX SEC504 Oct 17-22	Baton Rouge, LA SEC440 Nov 14-15
Denver, CO SEC301 Aug 1-6	Columbia, MD SEC401 Sep 12-17	Chantilly, VA SEC401 Sep 26-Oct 1	Portland, OR SEC511 Oct 17-22	Des Moines, IA SEC560 Nov 14-19
Columbia, MD SEC504 Aug 8-13	Detroit, MI SEC401 Sep 12-17	Columbia, MD FOR508 Sep 26-Oct 1	Woodlawn, MD SEC504 Oct 17-22	Indianapolis, IN SEC503 Nov 14-19
Denver, CO SEC542 Aug 8-13	Minneapolis, MN SEC511 Sep 12-17	Houston, TX SEC503 Sep 26-Oct 1	Chantilly, VA SEC301 Oct 24-28	New York, NY SEC617 Nov 14-19
Tampa, FL SEC504 Aug 8-13	Ottawa, ON SEC560 Sep 12-17	Lakewood, WA SEC401 Sep 26-Oct 1	Augusta, GA SEC504 Oct 24-29	Tysons Corner, VA SEC503 Nov 14-19
San Jose, CA SEC301 Aug 15-19	Sacramento, CA SEC401 Sep 12-17	Salt Lake City, UT DEV522 Sep 26-Oct 1	Detroit, MI DEV522 Oct 24-29	Mississauga, ON SEC440 Nov 28-29
Atlantic City, NJ SEC401 Aug 15-20	San Antonio, TX SEC401 Sep 12-17	New Orleans, LA SEC566 Oct 3-7	Ottawa, ON SEC401 Oct 24-29	Las Vegas, NV MGT512 Dec 5-9
Columbia, MD FOR572 Aug 15-20	Toronto, ON SEC504 Sep 12-17	Dallas, TX SEC301 Oct 3-7	Calgary, AB MGT512 Oct 27-Nov 24	Detroit, MI SEC504 Dec 5-10
Columbus, OH SEC401 Aug 15-20	Augusta, GA SEC401 Sep 19-24	Atlanta, GA SEC301 Oct 3-7	Colorado Springs, CO SEC440 Oct 31-Nov 1	Richmond, VA SEC504 Dec 5-10
Marina del Rey, CA SEC503 Aug 15-20	Columbia, MD SEC501 Sep 19-24	Pittsburgh, PA SEC504 Oct 3-8	Las Vegas, NV SEC503 Oct 31-Nov 5	San Diego, CA SEC401 Dec 5-10
Marina del Rey, CA SEC504 Aug 15-20	Madison, WI FOR585 Sep 19-24	Omaha, NE SEC504 Oct 10-15	Salt Lake City, UT SEC301 Oct 31-Nov 4	Tampa, FL SEC560 Dec 5-10
Omaha, NE SEC401 Aug 15-20	Seattle, WA SEC503 Sep 19-24	St Louis, MO SEC401 Oct 10-15	Seattle, WA SEC504 Oct 31-Nov 5	New York, NY SEC580 Dec 12-13
New York, NY SEC301 Aug 22-26	Albany, NY SEC504 Sep 19-24	New York, NY SEC524 Oct 13-14	Minneapolis, MN SEC440 Nov 7-8	Chantilly, VA SEC301 Dec 12-16
Indianapolis, IN SEC542 Aug 22-27	Miami, FL SEC504 Sep 19-24	Chicago, IL SEC503 Oct 17-22	Seattle, WA SEC542 Nov 7-12	Albany, NY SEC503 Dec 12-17
Raleigh-Cary, NC SEC401 Aug 22-27	San Francisco, CA SEC401 Sep 24-Oct 29	New York, NY FOR508 Oct 17-22	New York, NY SEC301 Nov 7-11	Ottawa, ON SEC501 Dec 12-17
St Louis, MO SEC504 Aug 22-27	Nashville, TN DEV541 Sep 26-29	Richardson, TX SEC511 Oct 17-22	Anaheim, CA SEC542 Nov 7-12	

SUMMIT EVENTS

Security Awareness SUMMIT & TRAINING San Francisco, CA Aug 1-10	Security Leadership SUMMIT & TRAINING Dallas, TX Sep 27 - Oct 4	Healthcare Cybersecurity SUMMIT & TRAINING Houston, TX Nov 14-21
Data Breach SUMMIT Chicago, IL Aug 18	HackFest SUMMIT & TRAINING Crystal City, VA Nov 2-9	Cyber Threat Intelligence SUMMIT & TRAINING Crystal City, VA Jan 25 - Feb 1

For a complete list of all SANS training events, visit sans.org/security-training/by-location/all

SANS CURRICULUM ROADMAPS

SECURITY CURRICULUM

Beginners

SEC301 NOTE:

If you have experience in the field, please consider our more advanced course – SEC401.

SEC301

Intro to Information Security
GISF

Penetration Testing

SEC401

Security Essentials Bootcamp Style
GSEC

SEC504

Hacker Tools, Techniques, Exploits, and Incident Handling
GCIH

SEC550

Active Defense, Offensive Countermeasures, and Cyber Deception

NETWORK & EXPLOITS

SEC560

Network Pen Testing and Ethical Hacking
GPEN

SEC660

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
GXPEN

SEC760

Advanced Exploit Development for Penetration Testers

WEB

SEC542

Web App Pen Testing and Ethical Hacking
GWAPT

SEC642

Advanced Web App Pen Testing and Ethical Hacking

MOBILE/WIRELESS

SEC575

Mobile Device Security and Ethical Hacking
GMOB

SEC617

Wireless Ethical Hacking, Pen Testing, and Defenses
GAWN

LAB-CENTERED

SEC561

Immersive Hands-On Hacking Techniques

SEC562

CyberCity Hands-on Kinetic Cyber Range Exercise

SPECIALIZATION

SEC567

Social Engineering for Penetration Testers

SEC573

Python for Penetration Testers
GPYC

SEC580

Metasploit Kung Fu for Enterprise Pen Testing

Network Operations Center, System Admin, Security Architecture

SEC401

Security Essentials Bootcamp Style
GSEC

SEC501

Advanced Security Essentials – Enterprise Defender
GCED

SEC505

Securing Windows and PowerShell Automation
GCWN

SEC506

Securing Linux/Unix
GCUX

SEC566

Implementing and Auditing the Critical Security Controls
GCCC

SEC579

Virtualization and Private Cloud Security

Security Operations Center/Intrusion Detection

SEC401

Security Essentials Bootcamp Style
GSEC

SEC504

Hacker Tools, Techniques, Exploits, and Incident Handling
GCIH

ENDPOINT MONITORING

SEC501

Advanced Security Essentials – Enterprise Defender
GCED

FOR508

Advanced Digital Forensics and Incident Response
GCFA

THREAT INTELLIGENCE

FOR578

Cyber Threat Intelligence

NETWORK MONITORING

SEC503

Intrusion Detection In-Depth
GCIH

FOR572

Advanced Network Forensics and Analysis
GNFA

SEC511

Continuous Monitoring and Security Operations
GMON

SEC550

Active Defense, Offensive Countermeasures, and Cyber Deception

Industrial Control Systems

ICS410

ICS/SCADA Security Essentials
GICSP

ICS515

ICS Active Defense and Incident Response

ICS456

Essentials for NERC Critical Infrastructure Protection

FORENSICS CURRICULUM

Incident Response and Threat Hunting

SEC401

Security Essentials Bootcamp Style
GSEC

SEC504

Hacker Tools, Techniques, Exploits, and Incident Handling
GCIH

NETWORK ANALYSIS

SEC503

Intrusion Detection In-Depth
GCIH

FOR572

Advanced Network Forensics and Analysis
GNFA

ENDPOINT ANALYSIS

FOR408

Windows Forensic Analysis
GCFA

FOR508

Advanced Digital Forensics & Incident Response
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

FOR408

Windows Forensic Analysis
GCFA

SEC504

Hacker Tools, Techniques, Exploits, and Incident Handling
GCIH

FOR508

Advanced Digital Forensics and Incident Response
GCFA

FOR526

Memory Forensics In-Depth

FOR585

Advanced Smartphone Forensics
GASF

FOR610

Reverse Engineering Malware: Malware Analysis Tools and Techniques
GREM

FOR518

Mac Forensic Analysis

MANAGEMENT CURRICULUM

FOUNDATIONAL

MGT512

SANS Security Leadership Essentials for Managers with Knowledge Compression™
GSLC

MGT525

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

MGT414

SANS Training Program for CISSP® Certification
GISP

CORE

MGT514

IT Security Strategic Planning, Policy, and Leadership

LEG523

Law of Data Security and Investigations
GLEG

MGT535

Incident Response Team Management

SPECIALIZATION

AUD507

Auditing & Monitoring Networks, Perimeters, and Systems
GSNA

SEC566

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

MGT433

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

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

DEVELOPER CURRICULUM

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

DEV543

Secure Coding in C/C++

DEV544

Secure Coding in .NET
GSSP-.NET

SPECIALIZATION

SEC542

Web App Pen Testing and Ethical Hacking
GWAPT

SEC642

Advanced Web App Pen Testing and Ethical Hacking

For information on all of SANS' courses, visit www.sans.org/courses



GIAC certification available for courses indicated with GIAC acronyms

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 CIS Critical Security 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