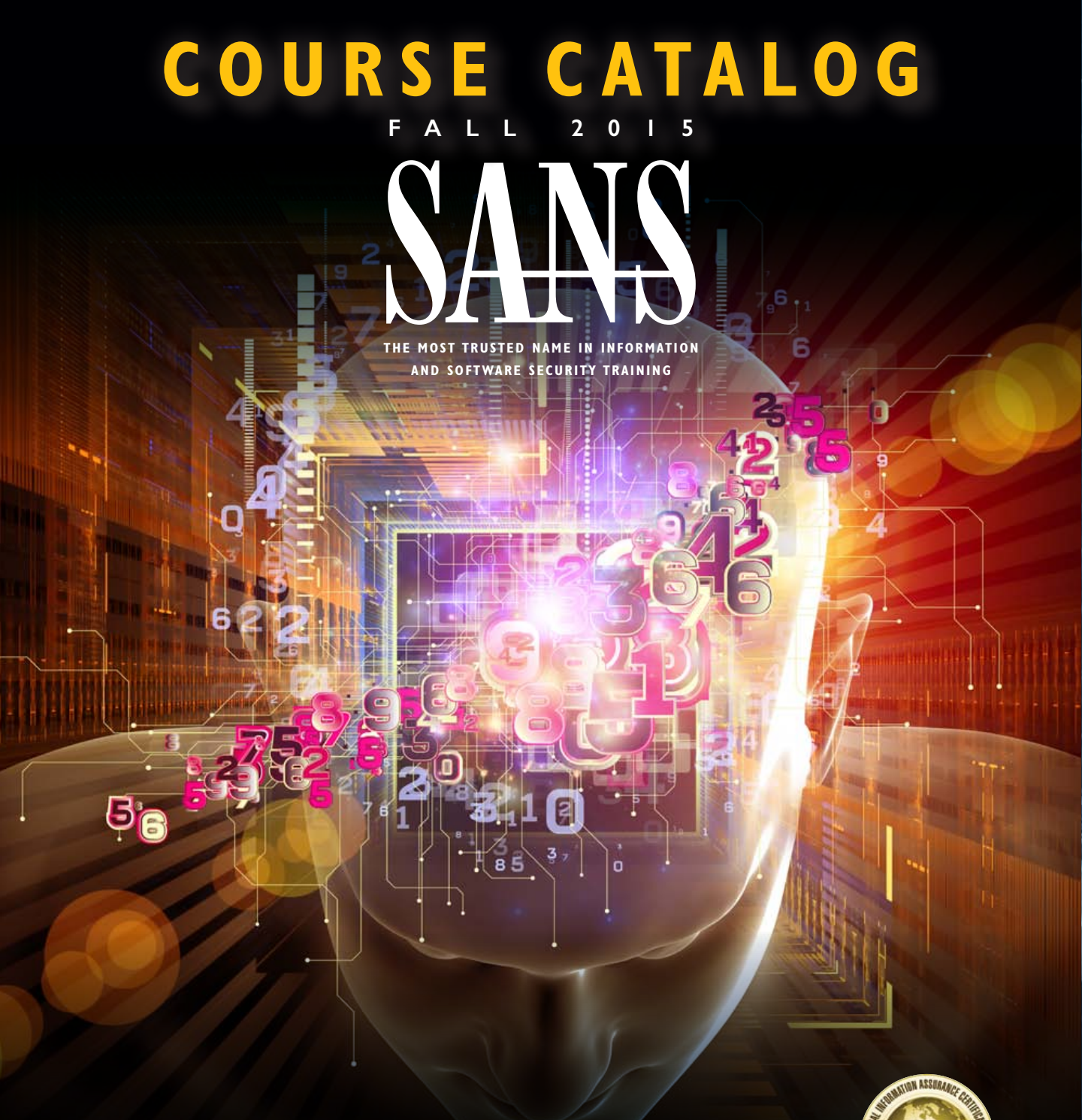
COURSE CATALOG

FALL 2015

SANS

THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING



Continuing Education

Over 50 courses across all skill levels:

- Cyber Defense
- Pen Testing
- Incident Response
- Digital Forensics
- Management, Audit, Legal
- Secure Development
- Industrial Control Systems

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

GIAC Certification

SANS Technology Institute Higher Education

sans.org

Information Security

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

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

CORE COURSES

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

Penetration Testing/Vulnerability Analysis

CORE COURSES: SEC301 (GISF) ▸ SEC401 (GSEC) → SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling GCIH

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

SPECIALIZATION: SEC573 Python for Penetration Testers; SEC580 Metasploit Kung Fu for Enterprise Pen Testing

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

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

Risk and Compliance/Auditing/Governance

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

AUD507 Auditing & Monitoring Networks, Perimeters, and Systems GSNA

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

SAMPLE JOB TITLES
- Auditor
- Compliance officer

Security Operations Center/Intrusion Detection

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

CORE COURSES: SEC301 (GISF) ▸ SEC401 (GSEC) → SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling GCIH

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

ENDPOINT MONITORING	NETWORK MONITORING		THREAT INTELLIGENCE
SEC501 Advanced Security Essentials — Enterprise Defender GCED	SEC502 Perimeter Protection In-Depth GPPA	SEC503 Intrusion Detection In-Depth GCIA	SEC511 Continuous Monitoring and Security Operations GMON	FOR578 Cyber Threat Intelligence
FOR508 Advanced Digital Forensics and Incident Response GCFA		FOR572 Advanced Network Forensics and Analysis GNFA	SEC550 Active Defense, Offensive Countermeasures, and Cyber Deception	

Network Operations Center, System Admin, Security Architecture

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

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

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

SEC505 Securing Windows with PowerShell and the Critical Security Controls GCWN

SEC506 Securing Linux/Unix GCUX

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

SEC579 Virtualization and Private Cloud Security

Development – Secure Development

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

DEV522 Defending Web Applications Security Essentials GWEB

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

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

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

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

SPECIALIZATION: SEC542 Web App Penetration Testing and Ethical Hacking GWAPT → SEC642 Advanced Web App Penetration Testing and Ethical Hacking

Industrial Control Systems

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

SAMPLE JOB TITLES
- IT & OT Support
- IT & OT Cybersecurity
- ICS Engineer

ICS410 ICS/SCADA Security Essentials GICSP

ICS515 ICS Active Defense and Incident Response

HOSTED Assessing and Exploiting Control Systems

HOSTED Critical Infrastructure and Control System Cybersecurity

Cyber or IT Security Management

FOUNDATIONAL	CORE	SPECIALIZATION
MGT512 SANS Security Leadership Essentials For Managers with Knowledge Compression™ GSLC	MGT514 IT Security Strategic Planning, Policy, and Leadership	MGT433 Securing The Human: How to Build, Maintain & Measure a High-Impact Awareness Program
MGT525 IT Project Management, Effective Communication, and PMP® Exam Prep GCPM	MGT535 Incident Response Team Management	AUD507 Auditing & Monitoring Networks, Perimeters, and Systems GSNA
MGT414 SANS Training Program for CISSP® Certification GISP	LEG523 Law of Data Security and Investigations GLEG	HOSTED Health Care Security Essentials

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

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

Incident Response

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

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

CORE COURSES: SEC301 (GISF) ▸ SEC401 (GSEC) → SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling GCIH

SPECIALIZATION	NETWORK ANALYSIS	ENDPOINT ANALYSIS	MALWARE ANALYSIS
FOR526 Memory Forensics In-Depth	SEC503 Intrusion Detection In-Depth GCIA	FOR408 Windows Forensic Analysis GCFE	FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques GREM
MGT535 Incident Response Team Management	FOR572 Advanced Network Forensics and Analysis GNFA	FOR508 Advanced Digital Forensics and Incident Response GCFA	FOR578 Cyber Threat Intelligence

Digital Forensic Investigations and Media Exploitation

FOR408 Windows Forensic Analysis GCFE

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

FOR508 Advanced Digital Forensics and Incident Response GCFA

FOR585 Advanced Smartphone Forensics

FOR518 Mac Forensic Analysis

FOR526 Memory Forensics In-Depth

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

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

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

SANS IT SECURITY TRAINING AND YOUR CONTINUING EDUCATION ROADMAP

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**

NETWORK & EXPLOITS
- **SEC560** Network Pen Testing and Ethical Hacking **GPEN**
- **SEC660** Advanced Penetration Testing, Exploit Writing, and Ethical Hacking **GXPN**
- **SEC760** Advanced Exploit Development for Penetration Testers

WEB
- **SEC542** Web App 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** Intense Hands-on Pen Testing Skill Development (with SANS NetWars)
- **SEC562** CyberCity Hands-on Kinetic Cyber Range Exercise

SPECIALIZATION
- **SEC573** Python for Penetration Testers
- **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 with PowerShell and the Critical Security Controls **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**

NETWORK MONITORING
- **SEC502** Perimeter Protection In-Depth **GPPA**
- **SEC503** Intrusion Detection In-Depth **GCIA**
- **SEC511** Continuous Monitoring and Security Operations **GMON**
- **FOR572** Advanced Network Forensics and Analysis **GNFA**
- **SEC550** Active Defense, Offensive Countermeasures, and Cyber Deception

THREAT INTELLIGENCE
- **FOR578** Cyber Threat Intelligence

MANAGEMENT CURRICULUM

- **SEC301** Intro to Information Security **GISF**
- **SEC401** Security Essentials Bootcamp Style **GSEC**
- **MGT512** SANS Security Leadership Essentials For Managers with Knowledge Compression™ **GSLC**
- **MGT525** IT Project Management, Effective Communication, and PMP® Exam Prep **GCPM**
- **MGT535** Incident Response Team Management
- **MGT414** SANS Training Program for CISSP® Certification **GISP**
- **MGT433** Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Program
- **MGT514** IT Security Strategic Planning, Policy, and Leadership

DEVELOPER CURRICULUM

CORE
- **Securing the Human for Developers** Application Security Awareness Modules
- **DEV522** Defending Web Applications Security Essentials **GWEB**
- **DEV541** Secure Coding in Java/JEE **GSSP-JAVA**
- **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

FORENSICS CURRICULUM

Incident Response

SEC401 Security Essentials Bootcamp Style **GSEC**

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

NETWORK ANALYSIS
- **SEC503** Intrusion Detection In-Depth **GCIA**
- **FOR572** Advanced Network Forensics and Analysis **GNFA**

ENDPOINT ANALYSIS
- **FOR408** Windows Forensic Analysis **GCFE**
- **FOR508** Advanced Digital Forensics & Incident Response **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 **GCFE**

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
- **FOR610** Reverse Engineering Malware: Malware Analysis Tools and Techniques **GREM**
- **FOR518** Mac Forensic Analysis

AUDIT CURRICULUM

- **SEC480** Top 4 Mitigation Strategies: Implementing and Auditing
- **SEC566** Implementing and Auditing the Critical Security Controls – In-Depth **GCCC**
- **AUD507** Auditing & Monitoring Networks, Perimeters, and Systems **GSNA**

LEGAL CURRICULUM

- **SEC401** Security Essentials Bootcamp Style **GSEC**
- **LEG523** Law of Data Security and Investigations **GLEG**

ICS CURRICULUM

- **ICS410** ICS/SCADA Security Essentials **GICSP**
- **ICS515** ICS Active Defense and Incident Response

For information on all of SANS' courses, visit sans.org/courses

GIAC certification available for courses indicated with GIAC acronyms

YOUR SOURCE FOR IT 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 the GIAC, an affiliate of the SANS Institute, a certification body featuring over 20 hands-on, technical certifications in information security, and 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 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. See pages 6 and 7 for more information about GIAC.

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

Continuing Education

Over 50 courses in the following disciplines:

- Security
- Management
- Forensics
- Audit
- Software Security
- Legal
- Industrial Control Systems

Higher Education

The SANS Technology Institute is the only accredited institution offering master's degree and graduate certificate programs focused solely on cybersecurity.

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

Learn more about STI at sans.edu

Global Information Assurance Certification (GIAC)

Offers 30 certifications in:

- Security
- Software Security
- Management
- Penetration Testing
- Forensics
- Audit
- Legal
- Industrial Control Systems

Learn more about GIAC at giac.org

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* (front and back inside covers) to plan your growth in your chosen career path

RELATE

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

VALIDATE

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

SAVE

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

ADD VALUE

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

ALTERNATIVES

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

ACT

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

Return on Investment

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

REMEMBER

the SANS promise:

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

TABLE OF CONTENTS

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
@drericcole

TEACHES
MGT414 SEC401 SEC501

"Dr. Cole has superb communication skills. He breaks down complex subjects into ways that are easier to understand. I never thought I would learn so much in such a short amount of time."
-Jote Aga, Department of Veterans Affairs

Jason Fossen

Fellow
@JasonFossen

TEACHES
SEC401 SEC440 SEC505 SEC566

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

Tanya Baccam

Senior Instructor
@tbaccam

TEACHES
MGT414 SEC401 SEC502 SEC542 AUD507

"Tanya is excellent. Her skill and experience show and add to the content richly."
-Jeff Reed, Cambia Health Solutions

Eric Conrad

Senior Instructor
@eric_conrad

TEACHES
SEC542 SEC511 SEC560 SEC580 MGT414

"Eric is a great instructor and I plan to take future classes that he teaches!"
-Jason Thompson, North Island Credit Union

"This is the opportunity to learn from instructors that are at the top of the food chain."

-Jeff Boggio,
South Oakland Systems

Paul A. Henry

Senior Instructor
@phenrycissp

TEACHES
FOR408 ICS410 MGT414 SEC401 SEC501 SEC502 SEC579

"Paul was great and shared so much of his experience with us during the class which helps solidify the concepts."
-Stephanie Padilla, Intel Security

John Strand

Senior Instructor
@strandjs

TEACHES
SEC504

"John Strand opened my eyes and helped me understand how to approach the concepts of offensive security and incident handling. He is one of the very best."
-Stephen Ellis, CB&I

James Tarala

Senior Instructor
@isaudit

TEACHES
AUD507 SEC440 SEC504 SEC505 SEC566

"James is an amazing presenter, fun to listen to on top of being very knowledgeable."
-Mike Pildher, URS Corp

Chad Tilbury

Senior Instructor
@chadtilbury

TEACHES
FOR408 FOR508

"The best educator I have ever learned from. His knowledge and presentation are superb."
-R. Ross, FDA

Johannes Ullrich, PhD

Senior Instructor
@johullrich

TEACHES
SEC546 DEV522 FOR572 SEC503

"Johannes has an excellent teaching style, very knowledgeable, listens to questions, and will keep explaining with different examples until you understand."
-Lori Stockdale, NYISO

SANS WORLD-CLASS INSTRUCTORS

David Hoelzer
Fellow
@it_audit

TEACHES
AUD507 MGT305 MGT512 SEC503

"David was awesome, very interactive, and engaging."
-Christopher Hills, Charles Schwab

Rob Lee
Fellow
@robtlee @sansforensics

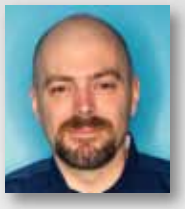
TEACHES
FOR408 FOR508

"Rob Lee takes forensics to the highest level. It's not just about forensics, it's about forensic methodically."
-Thomas C., Army Cyber Institute

Hal Pomeranz
Fellow
@hal_pomeranz

TEACHES
FOR508 FOR518 FOR572 FOR610
SEC506

"Great intro to malware analysis. Hal Pomeranz was extremely knowledgeable on the subject."
-Jonathon Hinson, Duke Energy



Ed Skoudis
Fellow
@edskoudis

TEACHES
SEC560

"Ed is one of the best instructors I have ever had. It's no secret why he is such a world-class pen tester!"
-Patrick McCoy, KEYW Corporation

Seth Misenar
Senior Instructor
@sethmisenar

TEACHES
MGT414 SEC511 SEC542

"Seth did an amazing job presenting the course material. He is very passionate about security and it shows."
-James Harding, WEMS

Mike Poor
Senior Instructor
@Mike_Poor

TEACHES
SEC503

"Mike is outstanding! Many claim to have the background he does when they don't. It's nice to learn from a pro!"
-Jeremy Glass, Molina Healthcare

Dave Shackleford
Senior Instructor
@daveshackleford

TEACHES
SEC501 SEC504 SEC560 SEC579

"Real-world tools and examples from a real-world professional. Dave is an absolute subject-matter expert!"
-Harry Lohse, Centric Group

Stephen Sims
Senior Instructor
@Steph3nSims

TEACHES
SEC401 SEC560 SEC660 SEC760

"Stephen is an excellent instructor. It's very rare to find an instructor who is so adept yet still makes the material approachable."
-Don Bailey, Blackbird Technologies

Benjamin Wright
Senior Instructor
@benjaminwright

TEACHES
LEG523

"Benjamin Wright knows the material very well. He has excellent flow and is right on target with the course description."
-Sharon O'Bryan, DeVry Inc.

Joshua Wright
Senior Instructor
@joswr1ght

TEACHES
SEC561 SEC562 SEC575

"Joshua is very knowledgeable and is great presenting the material."
-Tara Larson, Medtronic

Lenny Zeltser
Senior Instructor
@lennyzeltser

TEACHES
FOR610

"Lenny is a great instructor. He is patient, precise, quick to help, and motivating. Thanks! "
-Joona Airamo, StoneSoft

"Best training I've ever had – instructor and SANS altogether!"

-Duran Ochoa,
Fox Entertainment Group

For a complete instructor list and bios: sans.org/instructors

PROVE YOUR SKILLS
STAY COMPETITIVE
GET GIAC CERTIFIED!

"GIAC defines a higher level of mastery and skill that is required in order to earn the credential. GIAC really stands out among other security certifications." -JOSH RINGER, BENFIS HEALTH SYSTEM

As an information security professional, it is critical to stay abreast of the latest techniques and demonstrate you have the skills to protect vital systems, data, and infrastructure.

GIAC is the leading provider and developer of Information Security Certifications. GIAC tests and validates the ability of practitioners in information security, forensics, and software security. GIAC certification holders are recognized as experts in the IT industry and are sought after globally by governments, militaries, and industries to protect their cyber environment.

Broad certifications don't cover hands-on technical skills like GIAC. There are over 30 certifications in cyber defense, forensics, penetration testing and ethical hacking, and management.

Save over $400 when you register for a GIAC cetification attempt with your SANS training course!

Featured GIAC Certifications

COMING SOON!

GIAC Continuous Monitoring Certification (GMON)

Preventing all intrusions is impossible, but early detection is a must for the security of your enterprise. The proper use of Defensible Security Architecture, Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/ Continuous Security Monitoring will support the hindrance of intrusions and allow for early detection of anomalous activity.

The GMON is targeted towards security architects, engineers, analysts, and managers who want to demonstrate their ability to assess and implement defensible security architecture and continuous security monitoring. Successful GMON candidates will demonstrate the ability to securely architect a network resistant to breaches and that lends itself to monitoring. They will also demonstrate their ability to monitor, analyze detect threats and anomalies on the network.

For more information: **giac.org/certification/gmon**

GIAC Critical Controls Certification (GCCC)

GIAC Critical Controls Certification (GCCC) is the only certification based on the Critical Security Controls, a prioritized, risk-based approach to security. This certification ensures that candidates have the knowledge and skills to implement and execute the Critical Security Controls recommended by the Council on Cybersecurity, and perform audits based on the standard.

Successful candidates must have a solid understanding of the philosophies and driving forces behind the creation of the Critical Security Controls, their scope, and how these controls can be used to prioritize information security controls based on community risk assessment efforts. Candidates must also understand how the Critical Security Controls relate to other information assurance standards (such as ISO 27000, NIST 800-53, the NIST Core Framework, and others) and how the controls can be used to meet the goals of those standards. GCCC holders will make a practical and real difference in the security posture of any organization from a small- to medium-sized business to a multi-national corporation or governmental agency.

For more information: **giac.org/certification/gccc**

NEW

FOR578: Cyber Threat Intelligence

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

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

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

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

The collection, classification, and exploitation of knowledge about adversaries – collectively known as cyber threat intelligence – gives network defenders information superiority that can be used to reduce the adversary's likelihood of success with each subsequent intrusion attempt. Responders need accurate, timely, and detailed information to monitor new and evolving attacks, as well as methods to exploit this information to put in place an improved defensive posture. Threat intelligence thus represents a force multiplier for organizations looking to update their response and detection programs to deal with increasingly sophisticated advanced persistent threats.

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

THERE IS NO TEACHER BUT THE ENEMY!

digital-forensics.sans.org

Who Should Attend

- Incident response team members who regularly respond to complex security incidents and intrusions from APT groups and other advanced adversaries, and who need to know how to detect, investigate, remediate, and recover from compromised systems across an enterprise
- Experienced digital forensic analysts who want to consolidate and expand their understanding of filesystem forensics, investigations of technically advanced adversaries, incident response tactics, and advanced intrusion investigations
- Security Operations Center Personnel and Information Security Practitioners who support hunting operations that seek to identify attackers in their network environments
- Federal agents and law enforcement officials who want to master advanced intrusion investigations and incident response, and expand their investigative skills beyond traditional host-based digital forensics
- SANS FOR408, FOR572, FOR508, or FOR610 graduates looking to take their skills to the next level

***FOR578** is available via* (subject to change):

Featured Training Events

FOR578 CTI . . . . . Tysons Corner, VA . . Aug 31-Sep 4
CDI. . . . . Washington, DC . . . . . Dec 12-19

Summit Events

DFIR . . . . . Austin, TX . . . . . Jul 7-14

Private Training

All SANS courses are available through Private Training.

Custom Simulcast

Customized training for distributed workforces

"Since I am fresh out of college, this was a definite eye opener. This course was very valuable in that it gives a view of most tools available for auditing networks."

-Ryan Awai

NEW

ICS515: ICS Active Defense & Incident Response

This course is designed to empower students with the ability to understand and utilize active defense mechanisms in concert with incident response for industrial control system networks in order to respond to and deny cyber threats. This class uses a hands-on approach to give students a technical understanding of concepts such as generating and using threat intelligence, communicating control system needs to information technology personnel to deploy appropriate defenses, detecting malicious actors or threats on control system networks, and performing threat triage and incident response to ensure the safety and reliability of operations technology.

Author Statement

"In taking this course you will leave with the skills to identify and understand your networked infrastructure, monitor it for advanced threats, quickly respond to identified threats while keeping operations running, and extract lessons learned from interactions with the adversary to incorporate in your team's defense efforts or share with others in the form of threat intelligence."
-Robert M. Lee

What You Will Receive

- This course provides the student with a full functioning Cybati Works Mini-Kit
- The ICS515 kit includes a Raspberry PI with PiFace Digital, Snap-Circuit components, Wireless and Magnetic I/O, USB cables (with Volt/Amp meter), memory, and the Virtual Machine with OPC, HMI, PLC, RTU, I/O, industrial protocols, commercial control system demonstration software from Rex Controls and PeakHMI
- This course also makes use of numerous Virtual Machine environments throughout the hands-on labs

Who Should Attend

- IT and OT support
- IT and OT cybersecurity
- ICS engineers

You Will Be Able To

Participants will gain hands-on experience with the following tools:

- CYBATIWorks Kit and Virtual Machine with PeakHMI
- Snort and Bro for tailoring and tuning Intrusion Detection System rules
- Wireshark and TCPDump for network traffic capturing and packet analysis
- FTK Imager and MD5Deep for forensic data acquisition and validation
- OpenIOC and YARA for developing Indicators of Compromise
- Xplico and NetworkMiner for network flow and data analysis

***ICS515** is available via* (subject to change):

Featured Training Events

San Antonio . . . . . San Antonio, TX . . . . . Aug 17-22
CDI. . . . . Washington, DC . . . . . Dec 12-19

Private Training

All SANS courses are available through Private Training.

Custom Simulcast

Customized training for distributed workforces

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

NEW

SEC550: Active Defense, Offensive Countermeasures, and Cyber Deception

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.

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

Who Should Attend

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

You Will Be Able To

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

***SEC550** is available via* (subject to change):

Featured Training Events

San Jose	San Jose, CA	Jul 20-25
Network Security	Las Vegas, NV	Sep 12-21
Baltimore	Baltimore, MD	Sep 21-26
Cyber Defense San Diego		Oct 19-24
CDI	Washington, DC	Dec 12-19

Private Training

All SANS courses are available through Private Training.

Custom Simulcast

Customized training for distributed workforces

NEW

SEC562: CyberCity Hands-on Kinetic Cyber Range Exercise

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 these important infrastructures. 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 infrastructures, 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 are realizing an increasing need for skilled defenders of critical infrastructures. 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 infrastructures. 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.

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

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

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

Who Should Attend

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

You Will Be Able To

- Scan for and discover the details associated with 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

***SEC562** is available via* (subject to change):

Featured Training Events

Network Security . . Las Vegas, NV . . . . . Sep 12-21

Summit Events

Pen Test Hackfest. . . . Washington, DC . . . Nov 16-23

Private Training

All SANS courses are available through Private Training.

Custom Simulcast

Customized training for distributed workforces

DEV522: Defending Web Applications Security Essentials

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

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

"What you don't know about web app defense is most likely killing you and you wouldn't know it."
-Michael Malarkey, Bank of America

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

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

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

"The current security landscape is rapidly changing. The course content is relevant and important to software security and compliance software."
-Scott Hoof, Tripwire Inc.

The course will cover the topics outlined by OWASP's Top 10 risks document as well as additional issues the authors have found to be important in their day-to-day web application development practice. 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 will conclude with a large defensive exercise, reinforcing the lessons learned throughout the week.

"In-depth, cutting edge, real world knowledge provided in this course!"
-James Baker, Pass Key

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

***DEV522** is available via* (subject to change):

Featured Training Events

Capital City . . . . . Washington, DC . . . . . Jul 6-11
Network Security . . Las Vegas, NV . . . . . Sep 12-21

Private Training

All SANS courses are available through Private Training.

vLive Events

Live Virtual Training . . . . . .Aug 3-Sep 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

giac.org

sans.edu

DEVELOPER 541

Hands On | Four Days | Laptop Required | 24 CPEs | GIAC Cert: GSSP-JAVA

DEV541: Secure Coding in Java/JEE: Developing Defensible Applications

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

Who Should Attend

- Developers who want to build more secure apps
- Java EE programmers
- Software engineers
- Software architects
- 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

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** is available via* (subject to change):

Featured Training Events

Chicago . . . . . Chicago, IL. . . . . Aug 30-Sep 4
Network Security . . Las Vegas, NV . . . . . Sep 12-21
CDI. . . . . Washington, DC . . . . . Dec 12-19

Private Training

All SANS courses are available through Private Training.

vLive Events

Live Virtual Training . . . . . Oct 26-Nov 18

Custom Simulcast

Customized training for distributed workforces

OnDemand

E-learning available anytime, anywhere, at your pace

This course is available in SANS SelfStudy

giac.org

sans.edu

DEVELOPER 544

Hands On | Four Days | Laptop Required | 24 CPEs | GIAC Cert: GSSP-.NET

DEV544: Secure Coding in .NET: Developing Defensible Applications

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

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

Who Should Attend

This class is focused specifically on software development but is accessible enough for anyone who's comfortable working with code and has an interest in understanding the developer's perspective:

- Software developers and architects
- Senior software QA specialists
- System and security administrators
- Penetration testers

DEV544: Secure Coding in .NET: Developing Defensible Applications will help students leverage built-in and custom defensive technologies to integrate security into their applications. This comprehensive course covers a huge set of skills and knowledge. It is not a high-level theory course. It is about real programming. Students examine actual code, work with real tools, build applications, and gain confidence in the resources they need to improve the security of .NET applications.

***DEV544** is available via* (subject to change):

Featured Training Events

Network Security . . Las Vegas, NV . . . . . Sep 12-21
CDI. . . . . Washington, DC . . . . . Dec 12-19

Private Training

All SANS courses are available through Private Training.

vLive Events

Live Virtual Training . . . . . Oct 27-Nov 19

Custom Simulcast

Customized training for distributed workforces

OnDemand

E-learning available anytime, anywhere, at your pace

This course is available in SANS SelfStudy

giac.org

sans.edu

FOR408: Windows Forensic Analysis

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.

"This is a very high-intensity course with extremely current course material that is not available anywhere else in my experience."
-Alexander Applegate, Auburn University

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.

"I've been doing forensic investigations for several years, but would highly recommend this course for both new and old forensic investigations."
-Galarza, JP Morgan Chase

Proper analysis requires real data for students to examine. The completely updated FOR408 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7, Windows 8/8.1, Office and Office365, cloud storage, Sharepoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Nothing is left out – attendees learn to analyze everything from legacy Windows XP systems to just-discovered Windows 8.1 artifacts.

FOR408 is continually updated: This course utilizes a brand-new intellectual property theft and corporate espionage case that took over 6 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 can encounter while analyzing Windows systems. The incredibly detailed workbook details the tools and techniques step-by-step that each investigator should follow to solve a forensic case.

digital-forensics.sans.org

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

giac.org

sans.edu

Who Should Attend

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

You Will Be Able To

- Perform proper Windows forensic analysis by applying key analysis techniques covering Windows XP through Windows 8
- Use full-scale forensic tools and analysis methods to detail every action a suspect accomplished on a Windows system, including how and who placed an artifact on the system, 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 analysis, Windows artifact analysis, and email 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), email 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 to accomplish 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 via a remote session, at the keyboard, or simply by unlocking their 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 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; FAT and NTFS File System Overview; Key Word Searching and Forensics Suites (FTK, EnCase, and Autopsy); Document and File Metadata; File Carving

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

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

Topics: Registry Basics; Profile Users and Groups; Core System Information; User Forensic Data; External and Bring Your Own Device (BYOD) Forensic Examinations; Tools Utilized

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

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

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

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

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

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

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

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

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

408.6 HANDS ON: Windows Forensic Challenge

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

Topics: Digital Forensic Case; Mock Trial

***FOR408** is available via* (subject to change):

Featured Training Events

Minneapolis . . . . Minneapolis, MN . . . . . Jul 20-25
Virginia Beach . . . Virginia Beach, VA . . . .Aug 24-29
Crystal City . . . . . Crystal City, VA . . . . . .Sep 8-13
Network Security . . Las Vegas, NV . . . . . .Sep 12-21
CDI. . . . . Washington, DC . . . . .Dec 12-19

Summit Events

DFIR . . . . . Austin, TX . . . . . Jul 7-14

Mentor Program Events

Cartersville, GA . . . . . Jul 16-Oct 15

Private Training

All SANS courses are available through Private Training.

vLive Events

Live Virtual Training . . . . . Dec 1-Jan 21

Event Simulcast

Virtual/Online . . . . . Jul 9-14

Custom Simulcast

Customized training for distributed workforces

OnDemand

E-learning available anytime, anywhere, at your pace

SelfStudy

This course is available in SANS SelfStudy

FOR508: Advanced Digital Forensics and Incident Response

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

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

"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

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

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

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.

"Final challenge is excellent – really brought home all lessons learned."
-Alexandros Papadopoulos, Dell SecureWorks

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.

"FOR508 gives you the skills necessary to work effectively on a high performing security team, and the timeline analysis is extremely useful and interesting."
-Manny Ortiz, AT&T

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

giac.org | sans.org/cyber-guardian | sans.edu | sans.org/8570 | digital-forensics.sans.org

Who Should Attend

- Information security professionals
- Incident response team members
- Security Operations Center (SOC) personnel
- System administrators
- Experienced digital forensic analysts
- Federal agents and law enforcement
- Red team members, penetration testers, and exploit developers
- 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 hackivists
- Discover every system compromised in your enterprise utilizing incident response tools such as F-Response and digital forensic analysis capabilities in the SIFT Workstation to identify APT beach head 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 it has collected to exfiltrate as you track your adversary's movements in your network via timeline analysis using the log2timeline toolset
- Begin recovery and remediation of the compromise via the use of Indicators of Compromise (IOC), Threat Intelligence, and IR/Forensics key scanning techniques to identify active malware and all enterprise systems affected by the breach
- Perform filesystem surgery using the sleuthkit tool to discover how filesystems work and uncover powerful forensic artifacts such as NTFS $I30 directory file indexes, journal parsing, and detailed Master File Table analysis
- Use volume shadow snapshot examinations, XP restore point analysis, and NTFS examination tools in the SIFT Workstation, and recover artifacts hidden by anti-forensic techniques such as timestomping, file wiping, rootkit hiding, and privacy cleaning
- Discover an adversary's persistence 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

508.1 HANDS ON: Enterprise Incident Response

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

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

508.2 HANDS ON: Memory Forensics in Incident Response

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

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

508.3 HANDS ON: Timeline Analysis

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

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

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

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, Server 2008 Shadow Volume Copy Analysis; Deep Dive Malware and Anti-Forensic Detection; Data Layer Analysis; Stream-Based Data Carving; File-Based Data Carving; NTFS Filesystem Analysis; Anti-Forensic Detection Methodologies

508.5 HANDS ON: Adversary and Malware Hunting

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

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

508.6 HANDS ON: The APT Incident Response Challenge

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

***FOR508** is available via* (subject to change):

Featured Training Events

Boston	Boston, MA	Aug 3-8
Virginia Beach	Virginia Beach, VA	Aug 30-Sep 4
Network Security	Las Vegas, NV	Sep 12-21
Seattle	Seattle, WA	Oct 5-10
Tysons Corner	Tysons Corner, VA	Oct 12-17
South Florida	Ft. Lauderdale, FL	Nov 9-14
CDI	Washington, DC	Dec 12-19

Summit Events

DFIR	Austin, TX	Jul 7-14
Cyber Crime	Dallas, TX	Sep 21-26

Private Training

All SANS courses are available through Private Training.

vLive Events

Live Virtual Training . . . . . Sep 22-Oct 29

Event Simulcast

Virtual/Online . . . . . Jul 9-14

Custom Simulcast

Customized training for distributed workforces

OnDemand

E-learning available anytime, anywhere, at your pace

SelfStudy

This course is available in SANS SelfStudy

FOR518: Mac Forensic Analysis

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

"This course gives a top-to-bottom approach to forensic thinking that is quite needed in the profession."
-Naveel Koya, AC-DAC – Trivandrum

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

FORENSICATE DIFFERENTLY!

FOR518: Mac Forensic Analysis will teach you:

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

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

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

Who Should Attend

- Experienced digital forensic analysts
- Law enforcement officers, federal agents, and detectives
- Media exploitation analysts
- Incident response team members
- Information security professionals
- SANS FOR408, FOR508, FOR526, FOR610, and FOR585 alumni looking to round out their forensic skills

You Will Be Able To

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

DFIR
digital-forensics.sans.org

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

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

518.4 HANDS ON: Advanced Analysis Topics

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

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

518.5 HANDS ON: iOS Forensics

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

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

518.6 HANDS ON: The Mac Forensics Challenge

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

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

***FOR518** is available via* (subject to change):

Featured Training Events

Virginia Beach . . . Virginia Beach, VA . . . . Aug 24-29
Network Security . . Las Vegas, NV . . . . . Sep 12-21
San Francisco . . . . San Francisco . . . . Nov 30-Dec 4

OnSite

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

FOR526: Memory Forensics In-Depth

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.

"Thank you for all the content and I can't wait to do the exercises and the challenges again."
-Nick Christian, TBI

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.

MALWARE CAN HIDE, BUT IT MUST RUN

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.

"This course is totally awesome, relevant, and eye opening. I want to learn more every day."
-Matthew Britton, Blue Cross Blue Shield of Louisiana

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

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 forensic 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

DFIR

digital-forensics.sans.org

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 Workstation; 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

Day 4 focuses on introducing some 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, "Spotting Rootkit Behaviors" and "Extracting Suspicious Binaries," it is important to emphasize again the rootkit paradox. 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, the 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: Final Day 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 12-21
Baltimore . . . . . Baltimore, MD . . . . . Sep 21-26

Summit Events

DFIR . . . . . Austin, TX . . . . . Jul 7-14

Private Training

All SANS courses are available through Private Training.

Event Simulcast

Virtual/Online . . . . . Jul 9-14

Custom Simulcast

Customized training for distributed workforces

OnDemand

E-learning available anytime, anywhere, at your pace

SelfStudy

This course is available in SANS SelfStudy

FOR572: Advanced Network Forensics & Analysis

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

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

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

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

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

What You Will Receive

- Custom distribution of the Linux SANS SIFT Workstation Virtual Machine with over 500 digital forensics and incident response tools prebuilt into the environment, including network forensic tools added just for this course
- Realistic case data to examine during class, from multiple sources including:
  - NetFlow data
  - Web proxy, firewall, and intrusion detection system logs
  - Network captures in pcap format
  - Network service logs
- 64GB USB disk loaded with case examples, tools, and documentation

Who Should Attend

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

You Will Be Able To

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

572.1 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 go hands-on to find and extract stolen data from the proxy. 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; High-level Analysis Tools and Utilities

572.2 HANDS ON: NetFlow Analysis, Commerical 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. Findings supported by 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); 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 look at a broad range of protocols, including the Dynamic Host Configuration Protocol, which "glues" together layers two and three on the OSI model, and Microsoft's Remote Procedure Call Protocol, which provides all manners of file, print, name resolution, authentication, and other services.

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

572.4 HANDS ON: Logging, OPSEC, and Footprint

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

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

572.5 HANDS ON: Encryption, Protocol Reversing, and Automation

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

Topics: Introduction to Encryption; Man-in-the-Middle; Encrypted Traffic Flow Analysis; Payload Reconstruction; 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 prior to and 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

San Jose	San Jose, CA	Jul 20-25
San Antonio	San Antonio, TX	Aug 17-22
Virginia Beach	Virginia Beach, VA	Aug 24-29
Network Security	Las Vegas, NV	Sep 12-21
South Florida	Ft. Lauderdale, FL	Nov 9-14
San Francisco	San Francisco, CA	Nov 30-Dec 5
CDI	Washington, DC	Dec 12-19

Summit Events

DFIR . . . . . Austin, TX . . . . . Jul 7-14

Private Training

All SANS courses are available through Private Training.

vLive Events

Live Virtual Training . . . . . Oct 20-Nov 25

Event Simulcast

Virtual/Online . . . . . Jul 9-14

Custom Simulcast

Customized training for distributed workforces

OnDemand

E-learning available anytime, anywhere, at your pace

SelfStudy

This course is available in SANS SelfStudy

giac.org

sans.edu

FOR585: Advanced Smartphone Forensics

It is almost impossible today to conduct a digital forensic investigation that does not include a smartphone or mobile device. Smartphones are replacing the need for a personal computer, and almost everyone owns at least one. The smartphone may be the only source of digital evidence tracing an individual's movements and motives, and thus can provide the who, what, when, where, why, and how behind a case. **FOR585: Advanced Smartphone Forensics** teaches real-life, hands-on skills that help digital forensic examiners, law enforcement officers, and information security professionals handle investigations involving even the most complex smartphones currently available.

The course focuses on smartphones as sources of evidence, providing students with the skills needed to handle mobile devices in a forensically sound manner, manipulate locked devices, understand the different technologies, discover malware, and analyze the results for use in digital investigations by diving deeper into the file systems of each smartphone. Students will be able to obtain actionable intelligence and recover and analyze data that commercial tools often miss for use in internal investigations, criminal and civil litigation, and security breach cases. Students will walk away with knowledge they can immediately put to use on their next smartphone investigation.

YOUR TEXTS AND APPS CAN AND WILL BE USED AGAINST YOU!

The hands-on exercises in this course cover the best commercial and open-source tools available to conduct smartphone and mobile device forensics, and provide detailed instructions on how to manually decode data that tools sometimes overlook. The course will prepare you to recover and reconstruct events relating to illegal or unauthorized activities, determine if a smartphone has been compromised with malware or spyware, and provide your organization with the capability to use evidence from smartphones.

This intensive six-day course will take your mobile device forensics knowledge and abilities to the next level. Smartphone technologies are constantly changing, and most forensics professionals are unfamiliar with the data formats. It is 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!

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

You Will Be Able To

- Extract and use information from smartphones and mobile devices, including Android, iOS, Blackberry, Windows Phone, Symbian, and Chinese knock-off devices
- Understand how to detect hidden malware and spyware on smartphones and extract information related to security breaches, cyber espionage, and advanced threats involving smartphones
- Prevent loss or destruction of valuable data on smartphones by learning proper handling of these devices
- Learn a variety of acquisition methods for smartphones with an understanding of the advantages and limitations of each acquisition approach
- Interpret file systems on smartphones and locate information that is not generally accessible to users
- Recover artifacts of user activities from third-party applications on smartphones
- Recover location-based and GPS information from smartphones
- Perform advanced forensic examinations of data structures on smartphones by diving deeper into underlying data structures that many tools do not interpret
- Analyze SQLite databases and raw data dumps from smartphones to recover deleted information
- Perform advanced data-carving techniques on smartphones to validate results and extract missing or deleted data
- Reconstruct events surrounding a crime using information from smartphones, including timeline development and link analysis (who communicated with whom, locations at particular times)
- Decrypt locked backup file and bypass smartphone locks
- Apply the knowledge you acquire during the course to conduct a full-day smartphone capstone event involving multiple devices and modeled after real-world smartphone investigations

"FOR585 course content is extremely valuable for use in real-world application and directly pertinent to analysis conducted at my lab."
-H. Polend, Virginia Dept. of Forensic Science

digital-forensics.sans.org

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.

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

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; Android File System Structures; Android Evidentiary Locations; Handling Locked Android Devices; Traces of User Activity on Android Devices

585.3 HANDS ON: iOS Forensics

Apple iOS devices are no longer restricted to the United States, they are now in use worldwide. 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 forensics investigation.

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

585.4 HANDS ON: Backup File and BlackBerry Forensics

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 file systems are commonly found on external media and can be the only forensics 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; Creating and Parsing Backup Files; Evidentiary Locations on Backup Files; Locked Backup Files; Blackberry Forensics Overview; Blackberry Forensic Acquisition and Best Practices; Blackberry File System and Evidentiary Locations; Blackberry Forensic Analysis

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

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. Nokia smartphones running the Symbian operating system may no longer be manufactured, but they still exist in the wild. You must acquire skills for handling and parsing data from uncommon smartphone devices. This day of instruction 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.

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 Forensic Capstone Exercise

This section 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 forensics 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

Boston . . . . . Boston, MA. . . . . Aug 3-8
Network Security . . Las Vegas, NV . . . . . Sep 12-21
Tysons Corner . . . Tysons Corner, VA . . . . Oct 12-17
South Florida . . . . Ft. Lauderdale, FL. . . . Nov 9-14

Community SANS Events

Chantilly, VA . . . . . Dec 7-12

Private Training

All SANS courses are available through Private Training.

vLive Events

Live Virtual Training . . . . . Aug 11-Sep 17

Event Simulcast

Virtual/Online . . . . . Sep 14-19

Custom Simulcast

Customized training for distributed workforces

OnDemand

E-learning available anytime, anywhere, at your pace

SelfStudy

This course is available in SANS SelfStudy

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

This popular malware analysis course helps forensic investigators, incident responders, security engineers and IT administrators acquire practical skills for examining malicious programs that target and infect Windows systems. Understanding the capabilities of malware is critical to an organization's ability to derive the threat intelligence it needs to respond to information security incidents and fortify defenses. This 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.

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

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

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

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

"This course touches on the most novel, up-to-date malware challenges in today's world, and the instructor is great!"
-Morgan Harris, Booz Allen Hamilton

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

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

Who Should Attend

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

You Will Be Able To

- Build an isolated laboratory environment for analyzing code and behavior of malicious programs
- Employ network and system-monitoring tools to examine how malware interacts with the file system, the registry, the network and other processes on Microsoft Windows
- Uncover and analyze malicious JavaScript, VB Script and ActionScript components of web pages, which are often used as part of drive-by attacks
- Control some aspect of the malicious program's behavior through network traffic interception and code patching
- Use a disassembler and a debugger to examine inner workings of malicious Windows executables
- Bypass a variety of 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
- 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 contain and recover from the incident
- Utilize practical memory forensics techniques to examine capabilities of rootkits

digital-forensics.sans.org

giac.org

sans.edu

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 then 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 will learn how to examine this aspect of attacks. As with the other topics covered throughout the course, you will be able to experiment with such techniques during hands-on exercises.

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

610.5 HANDS ON: Malicious Documents and Memory Forensics

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

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

610.6 HANDS ON: Malware Analysis Tournament

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

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

***FOR610** is available via* (subject to change):

Featured Training Events

Virginia Beach . . . Virginia Beach, VA . . Aug 30-Sep 4
Network Security . . Las Vegas, NV . . . . . Sep 12-21
CDI. . . . . Washington, DC . . . . . Dec 12-19

Summit Events

DFIR . . . . . Austin, TX . . . . . Jul 7-14

Private Training

All SANS courses are available through Private Training.

vLive Events

Live Virtual Training . . . . . Jul 14-Aug 20
Live Virtual Training . . . . . Nov 10-Dec 17

Event Simulcast

Virtual/Online . . . . . Jul 9-14

Custom Simulcast

Customized training for distributed workforces

OnDemand

E-learning available anytime, anywhere, at your pace

SelfStudy

This course is available in SANS SelfStudy

MGT414: SANS Training Program for CISSP® Certification

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

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

MGT414 focuses solely on the 8 domains of knowledge as determined by (ISC)² that form a critical part of 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.

"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

"It was extremely valuable to have an experienced information security professional teaching the course as he was able to use experimental knowledge in examples and explanations."
-Sean Hoar, Davis Wright Tremaine

You Will Receive With This Course:

- Course books for each of the 8 domains
- 320 questions to test knowledge and preparation for each domain

Take advantage of SANS' CISSP® Get Certified Program currently being offered.
sans.org/special/cissp-get-certified-program

giac.org

MEETS DoDD 8570 REQUIREMENTS
sans.org/8570

Over the past 4 years, 98% of all surveyed students who took SANS MGT414 and then took the CISSP® Certification Exam passed, compared to a national average of around 70% for other prep courses.

Who Should Attend

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

You Will Be Able To

- Understand the 8 domains of knowledge that are covered on the CISSP® exam
- Analyze questions on the exam and be able to select the correct answer
- Apply the knowledge and testing skills learned in class to pass the CISSP® exam
- Understand and explain all of the concepts covered in the 8 domains of knowledge
- Apply the skills learned across the 8 domains to solve security problems when you return to work

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

414.1 Introduction; Security and Risk Management

On the first day of training for the CISSP® exam, MGT414 introduces the specific requirements needed to obtain certification. The 2015 exam update will be discussed in detail. We will cover the general security principles needed to understand the 8 domains of knowledge, with specific examples for each domain. The first of the 8 domains, Security and Risk Management, is discussed using real-world scenarios to illustrate the critical points.

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

414.2 Asset Security and Security Engineering (PART 1)

Understanding asset security is critical to building a solid information security program. The Asset Security domain, the initial focus of today's course section, describes data classification programs, including those used by both governments/militaries and the private sector. We will also discuss ownership, covering owners ranging from business/mission owners to data and system owners. We will examine data retention and destruction in detail, including secure methods for purging data from electronic media. We then turn to the first part of the Security Engineering domain, including new topics for the 2015 exam such as the Internet of Things, Trusted Platform Modules, Cloud Security, and much more.

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

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

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

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

414.4 Identity and Access Management

Controlling access to data and systems is one of the primary objectives of information security. Domain 5, Identity and Access Management, strikes at the heart of access control by focusing on identification, authentication, and authorization of accounts. Password-based authentication represents a continued weakness, so Domain 5 stresses multi-factor authentication, biometrics, and secure credential management. The 2015 CISSP® exam underscores the increased role of external users and service providers, and mastery of Domain 5 requires an understanding of federated identity, SSO, SAML, and third-party identity and authorization services like Oauth and OpenID.

Topics: Domain 5: Identity and Access Management

414.5 Security Assessment and Testing; Security Operations

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

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

414.6 Software Development Security

Domain 8 (Software Development Security) describes the requirements for secure software. Security should be "baked in" as part of network design from day one, since it is always less effective when it is added later to a poor design. We will discuss classic development models, including waterfall and spiral methodologies. We will then turn to more modern models, including agile software development methodologies. New content for the 2015 CISSP® exam update will be discussed, including DevOps. We will wrap up 414.6 by discussing security vulnerabilities, secure coding strategies, and testing methodologies.

Topics: Domain 8: Software Development Security

***MGT414** is available via* (subject to change):

Featured Training Events

Capital City	Washington, DC	Jul 6-11
San Jose	San Jose, CA	Jul 20-25
Boston	Boston, MA	Aug 3-8
San Antonio	San Antonio, TX	Aug 17-22
Chicago	Chicago, IL	Aug 30-Sep 4
Network Security	Las Vegas, NV	Sep 12-21
Tysons Corner	Tysons Corner, VA	Oct 12-17
Cyber Defense San Diego		Oct 19-24
CDI	Washington, DC	Dec 12-19

Community SANS Events

Chantilly, VA	Jul 20-25
Dallas, TX	Jul 27-Aug 1
St Louis, MO	Jul 27-Aug 1
Ft Lauderdale, FL	Aug 10-15
Rockville, MD	Aug 17-22
Austin, TX	Oct 5-10
Boston, MA	Nov 2-7

Summit Events

Security Leadership	Dallas, TX	Dec 3-10

Mentor Program Events

Chantilly, VA	Sep 9-Nov 11
Lansing, MI	Sep 9-Nov 11
Salt Lake City, UT	Sep 17-Nov 19

Private Training

All SANS courses are available through Private Training.

vLive Events

Live Virtual Training	Sep 8-Oct 14
Live Virtual Training	Dec 7-Jan 27

Custom Simulcast

Customized training for distributed workforces

OnDemand

E-learning available anytime, anywhere, at your pace

SelfStudy

This course is available in SANS SelfStudy

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

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.

"MGT512 is hard hitting – it goes directly to the heart of the issue and is totally management focused."
-Tim Hoffman, Alida Connection

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.

"Breadth and depth is incredible! Very comprehensive. MGT512 is worth your time!"
-Steve McGee, Curaspan Health Group

Knowledge Compression™

Maximize your learning potential!

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

Who Should Attend

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

You Will Be Able To

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

"This course provides you with the right technical knowledge needed by an executive and business knowledge to lead the security organization."
-Warren R. Bituin, SGN

giac.org

SANS Technology Institute
sans.edu

MEETS DoDD 8570 REQUIREMENTS

sans.org/8570

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; The Total Cost of Ownership; Negotiations; Fraud; Legal Liability; Technical People

Security Leaders and Managers earn the highest salaries (well into six figures) in information security and are near the top of the IT industry. 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

Minneapolis . . . . . Minneapolis, MN . . . . . Jul 20-25
San Jose . . . . . San Jose, CA . . . . . Jul 20-25
San Antonio . . . . . San Antonio, TX . . . . . Aug 17-22
Virginia Beach . . . Virginia Beach, VA . . . . Aug 24-28
Chicago . . . . . Chicago, IL . . . . . Aug 30-Sep 4
Crystal City . . . . . Crystal City, VA . . . . . Sep 8-13
Network Security . . Las Vegas, NV . . . . . Sep 12-21
CDI . . . . . Washington, DC . . . . . Dec 12-19

Community SANS Events

New York, NY . . . . . Jul 13-17

Summit Events

Security Leadership . . . Dallas, TX . . . . . Dec 3-10

Private Training

All SANS courses are available through Private Training.

vLive Events

Live Virtual Training . . . . . Nov 3-Dec 3

Custom Simulcast

Customized training for distributed workforces

OnDemand

E-learning available anytime, anywhere, at your pace

SelfStudy

This course is available in SANS SelfStudy

MGT514: IT Security Strategic Planning, Policy, and Leadership

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.

"MGT514 provided applicable and actionable knowledge for my InfoSec program. This was an invaluable experience."
-Jeremy Edson, Butler University

Create Effective Information Security Policy

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

Develop Management and Leadership Skills

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

How the Course Works

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

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

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

- Calculate the half-life of information
- Establish a strategic planning horizon appropriate for your organization
- Conduct any of the well-known environmental scans (SWOT, Porters 5, Pest and many others)
- Facilitate out-of-the-box thinking (brainstorming, reverse brainstorming, synergetics)
- Select between candidate initiatives and perform back-of-the-envelope planning
- Understand how policy is used and when it is needed or not needed
- Manage the policy creation process
- Develop policy for difficult topics such as social media
- Evaluate policy using using the SMART methodology

"MGT514 contained good practical information, and both professional and personal value."
-Keith Turpin, Boeing

"I find that courses such as MGT514 will allow me to plan and lead the organization forward."
-Eric Burgan, Idaho National Labs

SANS Technology Institute
sans.edu

514.1 Strategic Planning Foundations

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

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

514.2 Strategic Roadmap Development

With a firm understanding of business drivers as well as the threats facing the organization you will develop a plan to analyze the current state, identify the target state, 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 pioneers of the case study method, and focus specifically on information security management and leadership competencies. The Strategic Planning Workshop serves as a capstone exercise for the course, allowing students to synthesize and apply concepts, management tools, and methodologies learned in class.

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

***MGT514** is available via* (subject to change):

Featured Training Events

Network Security . . Las Vegas, NV . . . . . Sep 12-21
Tysons Corner . . . Tysons Corner, VA . . . . Oct 12-17
San Francisco . . . . San Francisco, CA . . Nov 30-Dec 5
CDI . . . . . Washington, DC . . . . . Dec 12-19

Summit Events

Security Leadership . . . Dallas, TX . . . . . Dec 3-10

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

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

Recently updated to fully prepare you for the 2015 PMP® Exam, **SANS MGT525: IT Project Management, Effective Communication, and PMP® Exam Prep** is a PMI Registered Education Provider (R.E.P.). R.E.P.s provide the training necessary to earn and maintain the Project Management Professional (PMP®) and other professional credentials. During this class you will learn how to improve your project planning methodology and project task scheduling to get the most out of your critical IT resources. We will utilize project case studies that highlight information technology services as deliverables. MGT525 follows the basic project management structure from the *PMBOK® Guide* (Fifth Edition) and also provides specific techniques for success with information assurance initiatives. Throughout the week, we will cover all aspects of IT project management – from initiating and planning projects to managing cost, time, and quality while your project is active, completing, closing, and documenting as your project finishes. A copy of the *PMBOK® Guide* (Fifth Edition) is provided to all participants. You can reference the guide and use your course material along with the knowledge you gain in class to prepare for the 2015 updated PMP® Exam and the GIAC Certified Project Manager Exam.

"Best way to prepare top project managers for the real world and certification!"
-Rob Ashworth, Barling Bay

"I think this is an awesome course that provides the knowledge and tools that I can use right when I get back to work."
-Johnny Matamoros Jr., Freeman

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.

Project Management Institute
Registered Education Provider

Who Should Attend

- Individuals who need to prepare 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

GCPM
giac.org

SANS Technology Institute
sans.edu

525.1 Project Management Structure & 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 from the onset your project is well defined. 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, the project activity sequence, and resource constraints. We will use milestones to set project timelines and task dependencies along with learning methods for 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 costs 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 Baselining; 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, quality assurance, and quality control methodologies. You'll also learn about 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 using and understanding 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 12-21

Private Training

All SANS courses are available through Private Training.

Custom Simulcast

Customized training for distributed workforces

SEC301: Intro to Information Security

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

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

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

"This course is crucial in today's world, and at a minimum, makes you aware of security issues, threats, and fixes."
-Cyd Allred, MGM Resorts International

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

"Good introductory course for someone whose organization is in need of implementing or rewriting security policies."
-Brad Ackerman, Victory Electric Cooperative

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**. It also delivers on the SANS promise: ***You will be able to use the knowledge and skills you learn in SEC301 as soon as you return to work.***

"I would recommend this course to anyone entering information security. I wish every security professional will be able to build the foundation of their career in security by taking SEC301! This was a basic review for me personally but good, solid information to newbies."
-Kimberly Hawkins, Scottrade

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
- Fundamentally understand 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 be able to discuss various security technologies including anti-malware, firewalls, and intrusion detection systems.
- Determine your "SPAM IQ" to more easily identify SPAM email messages
- Understand physical security issues and how they support cybersecurity
- Have an introductory level of knowledge regarding incident response, business continuity, and disaster recover planning
- Install and use the following tools: Password Safe, Secunia PSI, Malwarebytes, and Syncback

"I very much appreciate the passion of the instructors. Their knowledge is incredible and the presentation of their knowledge is down-to-earth and helpful."
-Ron Hoffman, Mutual of Omaha

giac.org

301.1 HANDS ON: The Cornerstone of Security

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

301.2 HANDS ON: Cryptography & Wireless Security

Cryptography is one of the most complex issues faced by security practitioners. It is not a topic you can explain in passing, so we will spend some time on it. Not to worry, we won't take you through the math behind cryptography, but we'll look at basic crypto terminology and processes. What is steganography? What is substitution and transposition? What is a "work factor" in cryptography and why does it matter? What do we mean by symmetric and asymmetric key cryptography and "cryptographic hash," and why do you need to know? How are those concepts used together in the real world to create cryptographic systems? Finally, we take a brief look at several cryptographic applications. We won't get into the details of how Secure Shell (SSH) actually works, but you will leave the classroom knowing what that term means and what SSH is used for. In other words, you'll be able to discuss several crypto applications in a general sense and not be confused when someone brings them up. Following cryptography, we introduce the fundamentals of wireless security (WiFi and Bluetooth), and mobile device security (i.e., cell phones).

301.3 HANDS ON: Networking

All attacks or exploits have one thing in common: they take something that exists for perfectly valid reasons and misuse it in malicious ways. Always! So as security practitioners, to grasp what is invalid we must first understand what is valid – that is, how things like networks are supposed to work. Only once we have that understanding can we hope to understand the mechanics of malicious misuse of those networks. Day three begins with a nontechnical explanation of how data move across a network. From there we move to fundamental terminology dealing with network types and standards. You'll learn about common network hardware such as hubs, switches, and routers, and you'll finally grasp what is meant by terms like protocol, encapsulation, and tunneling. We'll give a very basic introduction to network addressing and port numbers and then work our way up the Open Systems Interconnection (OSI) protocol stack, introducing more detail only as we proceed to the next layer. In other words, we explain networking starting in non-technical terms and gradually progress to more technical detail as students are ready to take the next step. By the end of our discussions, you'll have a fundamental grasp of any number of critical technical networking acronyms that you've often heard and never quite understood: TCP/IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP, and DNS. We'll close out day three with a very simple explanation of common network attacks such as spoofing, man-in-the-middle, denial of service, and distributed denial of service.

301.4 HANDS ON: Security Technologies

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

301.5 HANDS ON: Protecting Assets

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

***SEC301** is available via* (subject to change):

Featured Training Events

Capital City . . . . . Washington, DC . . . . . Jul 6-11
Crystal City . . . . . Crystal City, VA . . . . . Sep 8-13
Network Security . . Las Vegas, NV . . . . . Sep 12-21
CDI. . . . . Washington, DC . . . . . Dec 12-19

Community SANS Events

New Orleans, LA . . . . . Jul 13-17
Philadelphia, PA. . . . . Jul 13-17
Indianapolis, IN . . . . . Jul 20-24
Chantilly, VA . . . . . Aug 3-7
Cupertino, CA . . . . . Aug 10-14
Minneapolis, MN. . . . . Sep 21-25
Memphis, TN . . . . . Nov 9-13

Summit Events

Security Awareness . . . Philadelphia, PA . . . Aug 17-25
Cyber Crime. . . . . Dallas, TX . . . . . Sep 21-26

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

SEC401: Security Essentials Bootcamp Style

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.

"This course is a must for anyone who is responsible for managing security in a enterprise."
-Bradley Hoover, Exxonmobil

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.

"This course has been eye opening in the world of security and lets you see if there are other areas you want to explore."
-Ted Schuck, Vanguard

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

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

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

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

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

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.

giac.org | sans.org/cyber-guardian | sans.edu | sans.org/8570

MEETS DoDD 8570 REQUIREMENTS

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 tools/security of systems
- Create an effective policy that can be enforced within an organization and prepare a checklist to validate security, creating metrics to tie into training and awareness
- Identify visible weaknesses of a system utilizing various tools including dumpsec and OpenVAS, and once vulnerabilities are discovered cover ways to configure the system to be more secure
- Build a network visibility map that can be used for hardening of a network – validating the attack surface and covering ways to reduce it through hardening and patching
- Sniff open protocols like telnet and ftp and determine the content, passwords and vulnerabilities utilizing WireShark
- Apply what you learned directly to your job when you go back to work

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

Topics: Information Assurance Foundations; Computer Security Policies; Contingency and Continuity Planning; Access Control; Password Management; Incident Response; Offensive and Defensive Information Warfare; 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 three, 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: Vulnerability Scanning and Remediation; Web Security; Firewalls and Perimeters; Honeypots; Host-based Protection; Network-based Intrusion Detection and Prevention

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 four 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

Capital City	Washington, DC	Jul 6-11
Minneapolis	Minneapolis, MN	Jul 20-25
San Jose	San Jose, CA	Jul 20-25
Boston	Boston, MA	Aug 3-8
San Antonio	San Antonio, TX	Aug 17-22
Virginia Beach	Virginia Beach, VA	Aug 24-29
Chicago	Chicago, IL	Aug 30-Sep 4
Crystal City	Crystal City, VA	Sep 8-13
Network Security	Las Vegas, NV	Sep 12-21
Baltimore	Baltimore, MD	Sep 21-26
Seattle	Seattle, WA	Oct 5-10
Tysons Corner	Tysons Corner, VA	Oct 12-17
Cyber Defense San Diego		Oct 19-24
South Florida	Ft. Lauderdale, FL	Nov 9-14
San Francisco	San Francisco, CA	Nov 30-Dec 5
CDI	Washington, DC	Dec 12-19

Summit Events

Cyber Defense	Nashville, TN	Aug 11-18
Cyber Crime	Dallas, TX	Sep 21-26
Security Leadership	Dallas, TX	Dec 3-10

Community SANS Events

Baltimore, MD	Jul 20-25
Anaheim, CA	Aug 10-15
Charleston, SC	Aug 17-22
Milwaukee, WI	Sep 14-19
Kansas City, MO	Sep 28-Oct 3
Madison, WI	Oct 5-10
Jacksonville, FL	Oct 12-17
New York, NY	Nov 9-14
San Antonio, TX	Nov 9-14
Salt lake City, UT	Nov 16-21

Mentor Program Events

Charleston, SC	Jul 16-Sep 17
Chantilly, VA	Jul 20-Sep 21
Raleigh, NC	Aug 20-Oct 22
Downers Grove, IL	Oct 8-Dec 17
Philadelphia, PA	Oct 12-Nov 23

Private Training

All SANS courses are available through Private Training.

vLive Events

Live Virtual Training	Sep 1-Oct 8
Live Virtual Training	Nov 2-Dec 9

Event Simulcast

Virtual/Online	Aug 13-18
Virtual/Online	Sep 14-19

Custom Simulcast

Customized training for distributed workforces

OnDemand

E-learning available anytime, anywhere, at your pace

SelfStudy

This course is available in SANS SelfStudy

SEC501: Advanced Security Essentials – Enterprise Defender

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.

"I enjoyed real-life business cases that were discussed in SEC501 to make the material relevant."
-Lorelei Duff

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.

"Very knowledgeable. Top-tier training and industry leading."
-Herbert Monford, Regions Bank

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.

"After taking SEC401, this course is the perfect follow-up, going deep into attacking techniques while understanding the most-used vulnerabilities and how to defend your network against those attacks."
-Fawaz Alhomoud, Saudi Aramco

Who Should Attend

- Incident response and penetration testers
- Security Operations Center engineers and analysts
- Network security professionals
- Anyone who seeks technical in-depth knowledge about implementing comprehensive security solutions

You Will Be Able To

- Identify the threats against network infrastructures and build defensible networks that minimize the impact of attacks
- Learn the tools that can be used to analyze a network to both prevent and detect the adversary
- Decode and analyze packets using various tools to identify anomalies and improve network defenses
- Understand how the adversary compromises networks and how to respond to attacks
- Perform penetration testing against an organization to determine vulnerabilities and points of compromise
- Understand the six steps in the incident handling process and create and run an incident-handling capability
- Learn how to 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

GCED
giac.org

SANS Technology Institute
sans.edu

MEETS DoDD 8570 REQUIREMENTS
sans.org/8570

501.1 HANDS ON: Defensive Network Infrastructure

Protecting a network from attack starts with designing, building, and implementing a robust network infrastructure. Many aspects of implementing a defense-in-depth network are often overlooked because organizations focus on functionality. Achieving the proper balance between business drivers and core protection of information is difficult. On the first day students will learn how to design and implement a functionality-rich, secure network and how to maintain and update it as the threat landscape evolves.

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

501.2 HANDS ON: Packet Analysis

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

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

501.3 HANDS ON: Pentest

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

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

501.4 HANDS ON: First Responder

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

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

501.5 HANDS ON: Malware

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

Topics: Malware; Microsoft Malware; External Tools and Analysis

501.6 HANDS ON: Data Loss Prevention

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

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

***SEC501** is available via* (subject to change):

Featured Training Events

Minneapolis . . . . . Minneapolis, MN . . . . . Jul 20-25
Boston . . . . . Boston, MA. . . . . Aug 3-8
Virginia Beach . . . Virginia Beach, VA . . Aug 30-Sep 4
Chicago . . . . . Chicago, IL. . . . . Aug 30-Sep 4
Network Security . . Las Vegas, NV . . . . . Sep 12-21
Seattle . . . . . Seattle, WA. . . . . Oct 5-10
Tysons Corner. . . . Tysons Corner, VA . . . . Oct 12-17
Cyber Defense San Diego . . . . . Oct 19-24
CDI. . . . . Washington, DC . . . . . Dec 12-19

Summit Events

Security Awareness . . . Philadelphia, PA . . . Aug 17-25

Private Training

All SANS courses are available through Private Training.

Event Simulcast

Virtual/Online . . . . . Sep 14-19

Custom Simulcast

Customized training for distributed workforces

OnDemand

E-learning available anytime, anywhere, at your pace

SelfStudy

This course is available in SANS SelfStudy

SEC502: Perimeter Protection In-Depth

There is no single fix for securing your network. That's why this course is a comprehensive analysis of a wide breadth of technologies. In fact, this is probably the most diverse course in the SANS catalog, as mastery of multiple security techniques is required to defend your network from remote attacks. You cannot just focus on a single OS or security appliance. A proper security posture must be comprised of multiple layers. This course was developed to give you the knowledge and tools necessary at every layer to ensure your network is secure.

The course starts by looking at common problems we need to resolve. Is there traffic passing by my firewall I didn't expect? How did my system get compromised when no one can connect to it from the Internet? Is there a better solution than anti-virus for controlling malware? We'll dig into these questions and more and answer them.

We spend quite a bit of time learning about IP. Sure we all know how to assign an IP address, but to secure your network you really need to understand the idiosyncrasies of the protocol. We'll talk about how IP works and how to spot the abnormal patterns. If you can't hear yourself saying "Hmmm, there are no TCP options in that packet, it's probably forged," then you'll gain some real insight from this portion of the material.

Once you have an understanding of the complexities of IP, we'll get into how to control it on the wire. Rather than trying to tell you what are good and bad products, we focus on the underlying technology used by all of them. This is extremely practical information because a side-by-side product comparison is only useful for that specific moment in time. By gaining knowledge of what goes on under the hood, you will be empowered to make good product choices for years to come. Just because two firewalls are stateful inspection, do they really work the same on the wire? Is there really any difference between stateful inspection and network-based intrusion prevention, or is it just marketing? These are the types of questions we address in this portion of the course.

"As an analyst, these courses are the most relevant in the industry."
-Louis Robichaud, Atlantic Lottery Corp.

From there, it's a hands-on tour through how to perform a proper wire-level assessment of a potential product, as well as what options and features are available. We'll even get into how to deploy traffic control while avoiding some of the most common mistakes. Feel like your firewall is generating too many daily entries for you to review the logs effectively? We'll address this problem not by reducing the amount of critical data, but by streamlining and automating the backend process of evaluating it.

But you can't do it all on the wire. A proper layered defense needs to include each individual host – not just the hosts exposed to access from the Internet, but hosts that have any kind of direct or indirect Internet communication capability as well. We'll start with OS lockdown techniques and move on to third-party tools that can permit you to do anything from sandbox insecure applications to full-blown application policy enforcement.

"SEC502 opened my eyes so wide, it scared me!"
-George Scarborough, Defense Logistics Agency

Most significantly, the course material has been developed using the following guiding principles:

- Learn the process, not one specific product.
- You learn more by doing, so hands-on problem-solving is key.
- Always peel back the layers and identify the root cause.

While technical knowledge is important, what really matters are the skills to properly leverage that knowledge. This is why the course is heavily focused on problem-solving and root-cause analysis. While these are usually considered soft skills, they are vital to being effective in the role of security architect. So along with the technical training, you'll expand risk management capabilities and even gain a bit of Zen empowerment.

Who Should Attend

- Information security officers
- Intrusion analysts
- IT managers
- Network architects
- Network security engineers
- Network and system administrators
- Security managers
- Security analysts
- Security architects
- Security auditors

You Will Be Able To

- Apply perimeter security solutions in order to identify and minimize weaknesses to properly protect your perimeter
- Deploy and utilize multiple firewalls to understand the strengths and weaknesses that each presents
- Use built-in tools to audit and protect systems and to identify whether they have been compromised
- Utilize tcpdump to analyze network traffic in detail to understand what packets are communicating and how to identify potential covert channels
- Understand and utilize techniques to compromise and protect against application layer attacks such as XSS, CSRF, SQL injection and more
- Utilize tools to evaluate packets and identify legitimate and illegitimate traffic
- Use tools to evaluate and identify the risks related to Cloud Computing
- Inspect the intricate complexities of IP, including identifying malicious packets
- Evaluate and secure SSL, wireless networks, VPNs, applications and more
- Implement a logging solution that properly identifies risk and is manageable

giac.org

sans.org/cyber-guardian

SANS Technology Institute

sans.edu

502.1 HANDS ON: IP and Packet Decoding

On day one we start off with a 30,000 foot view of what needs to be addressed. However, this section is more than an executive overview as we dig down into the bits and bytes of the problem as well. What can be secured at the network level, and which protection needs to be pushed back to the hosts? What are my packet-level control devices really doing on the wire, and when can't I trust them?

Topics: Threat Vectors; OSI Layer 2; OSI Layer 3; OSI Layers 4 and 5; Packet Decoding

502.2 HANDS ON: Network Security – PART I

The only way to understand if a network traffic control device is going to meet your requirements is to understand the technology underneath the hood. Do all firewalls handle traffic the same way? What is the difference in solutions? In today's material we will cut through the vendor marketing slicks and look at what their products are really capable of doing. We will also start pulling together the pieces of a layered defense and discussing best practices for traffic control.

Topics: IPv6; Static and Stateful Packet Filtering; Stateful Inspection and NAT; Netfilter and Building a Rule Base; Network-based Intrusion Detection and Prevention; NIDS Hands-on

***SEC502** is available via* (subject to change):

Mentor Program Events

Columbia, MD . . . . . Aug 19-Oct 21

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

502.3 HANDS ON: Network Security – PART II

On day two we laid the foundation by discussing the technology under the hood of traffic control products. In today's material, we expand further by looking at additional solutions and how they work. We will also discuss how to test these products on the wire so we know exactly how they are impacting traffic. Can the product stop a source route attack? What about an application layer attack? These are the types of questions we will strive to answer in this material. We will also look at network access control (NAC), NextGen firewalls, virtual firewalls and much more.

Topics: Cisco Routers; Network Access Control; Packet Crafting; Perimeter Assessment; Virtual Firewalls and Proxies; Beyond Stateful

502.4 HANDS ON: Protecting the Endpoint – Host Security

In the early days of the Internet it was possible to secure a network right at the perimeter. Modern-day attacks, however, are far more advanced and require a multi-layered approach to security. This does not mean the traditional perimeter no longer serves a useful role, but just that it is only part of the equation – and the perimeter has changed. So in today's material, we will focus on the security posture of each of our individual hosts. We will look at endpoint protection solutions, and solutions to identify advanced malware. Additionally, we will look at applications and the huge vulnerabilities that can be present within applications and how to secure the issues identified.

Topics: Locking Down Hosts; Locking Down Web Applications; Application Firewalls; Endpoint Protection; Advanced Malware Protection

502.5 HANDS ON: Logging, Wireless, Encryption, and VPNs

The number one problem students have with managing their environment is dealing with the firewall logs. This is why we cover this topic in today's material. Not only will we discuss what to look for, but through practical exercises you will learn how to optimize the log review process into something that takes less time to finish than your morning coffee.

Topics: Security Information and Event Management; Firewall Log Analysis; Wireless Security; Authentication, Encryption and VPN Basics; VPN Options

502.6 HANDS ON: Assessments, Cloud Considerations, and Pulling It All Together

On the final day we will pull together everything we have learned. This day's material focuses greatly on problem resolution. The problems start off easy, like small organizations that need advice in order to make their environment more secure. The complexity quickly escalates, however, to where you need to combine security, functionality, and political issues into the design. A healthy dose of risk assessment is also thrown in for good measure.

Topics: Vulnerability Assessment and Auditing; Cloud Considerations; Pulling it All Together; Ettercap Labs; Useful Tools

SEC503: Intrusion Detection In-Depth

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

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

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

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.

"SEC503 covers the best processes for intrusion analysis and how to cut out most of the network noise and identify the important traffic."
-Mike Boya, Warner Brothers

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

Who Should Attend

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

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

"Anyone responsible for incident handling should attend this course. It is exactly what you need to do the job."
-Jamy Klein, Qualcomm, Inc.

giac.org

sans.org/cyber-guardian

sans.edu

MEETS DoDD 8570 REQUIREMENTS
sans.org/8570

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; Packet Crafting and nmap OS Identification; IDS/IPS Evasion Theory; Real-World Traffic Analysis

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

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

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

503.5 HANDS ON: Network Traffic Forensics and Monitoring

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

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

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 3-8
San Antonio . . . . . San Antonio, TX . . . . . Aug 17-22
Virginia Beach . . . Virginia Beach, VA . . . . Aug 24-29
Network Security . . Las Vegas, NV . . . . . Sep 12-21
Baltimore . . . . . Baltimore, MD . . . . . Sep 21-26
Tysons Corner . . . . Tysons Corner, VA . . . . Oct 12-17
Cyber Defense San Diego . . . . . Oct 19-24
CDI . . . . . Washington, DC . . . . . Dec 12-19

Summit Events

Cyber Defense . . . . . Nashville, TN . . . . Aug 11-18

Mentor Program Events

Evansville, IN . . . . . Sep 15-Nov 17

Private Training

All SANS courses are available through Private Training.

Event Simulcast

Virtual/Online . . . . . Aug 13-18

Custom Simulcast

Customized training for distributed workforces

OnDemand

E-learning available anytime, anywhere, at your pace

SelfStudy

This course is available in SANS SelfStudy

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

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.

"Incident handling is the baseline for cybersecurity. So having a course like this is great for the beginner and the expert alike. A good solid foundation leads to a great cybersecurity setup for a company."
-Robert Fredricks, Parkell, Inc.

By helping you understand attackers' tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan, this course helps you turn the tables on computer attackers. It addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course provides a time-tested, step-by-step process for responding to computer incidents, and a detailed description of how attackers undermine systems so you can prepare, 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 for, exploiting, and defending systems. It will enable you to discover the holes in your system before the bad guys do!

"This course is very beneficial and will sharpen your skills and then some."
-Robert Delizio, Federal Reserve Bank

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.

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

giac.org | sans.org/cyber-guardian | sans.edu | sans.org/8570

Who Should Attend

- Incident handlers
- Penetration testers
- Ethical hackers
- Leaders of incident handling teams
- System administrators who are on the front lines defending their systems and responding to attacks
- Other security personnel who are first responders when systems come under attack

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

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

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

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

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

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

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

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

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

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

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

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

This 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

Capital City	Washington, DC	Jul 6-11
Minneapolis	Minneapolis, MN	Jul 20-25
San Jose	San Jose, CA	Jul 20-25
Boston	Boston, MA	Aug 3-8
San Antonio	San Antonio, TX	Aug 17-22
Virginia Beach	Virginia Beach, VA	Aug 24-29
Chicago	Chicago, IL	Aug 30-Sep 4
Crystal City	Crystal City, VA	Sep 8-13
Network Security	Las Vegas, NV	Sep 12-21
Baltimore	Baltimore, MD	Sep 21-26
Seattle	Seattle, WA	Oct 5-10
Tysons Corner	Tysons Corner, VA	Oct 12-17
Cyber Defense San Diego		Oct 19-24
South Florida	Ft. Lauderdale, FL	Nov 9-14
CDI	Washington, DC	Dec 12-19

Summit Events

DFIR	Austin, TX	Jul 7-14
Cyber Defense	Nashville, TN	Aug 11-18
Cyber Crime	Dallas, TX	Sep 21-26
Pen Test Hackfest	Washington, DC	Nov 16-23

Community SANS Events

New Orleans, LA	Jul 13-18
Baltimore, MD	Jul 20-25
Columbus, OH	Aug 24-29
Colorado Springs, CO	Sep 21-26
Raleigh, NC	Oct 5-10
Alexandria, VA	Oct 26-31

Mentor Program Events

New Orleans, LA	Jul 21-Sep 22
St Louis, MO	Aug 12-Oct 14
Gainesville, FL	Sep 10-Nov 12

Private Training

All SANS courses are available through Private Training.

vLive Events

Virtual/Online	Sep 14-Oct 21
Virtual/Online	Dec 8-Jan 28

Event Simulcast

Virtual/Online	Jul 9-14
Virtual/Online	Aug 13-18
Virtual/Online	Oct 5-10

Custom Simulcast

Customized training for distributed workforces

OnDemand

E-learning available anytime, anywhere, at your pace

SelfStudy

This course is available in SANS SelfStudy

SEC505: Securing Windows with PowerShell and the Critical Security Controls

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

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

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

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

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

"SEC505 has a direct impact on windows IS Security and is a must for any system admin in this day and age."
-Chris Linville, Raytheon

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

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

giac.org | sans.org/cyber-guardian | sans.edu | sans.org/8570

Who Should Attend

- Windows security engineers and system administrators
- Anyone who wants to learn PowerShell
- Anyone who wants to implement the SANS Critical Security Controls
- Those who must enforce security policies on Windows hosts
- Anyone who needs a whole drive encryption solution
- Those deploying or managing a PKI or smart cards

You Will Be Able To

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

"As auditors, we are always being accused of not understanding the technology and not empathizing with our clients when we challenge the control decisions they make. This course allows me to communicate at the same level and understand."
-Susan Chiutsi, Canadian Imperial Bank of Commerce

505.1 HANDS ON: Windows PowerShell Scripting

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

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

505.2 HANDS ON: Windows Operating System and Applications Hardening

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

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

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

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

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

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

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

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

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

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

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

505.6 HANDS ON: Dynamic Access Control and Hardening DNS

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

Topics: Dynamic Access Control (DAC); Hardening DNS

***SEC505** is available via* (subject to change):

Featured Training Events

Network Security . . Las Vegas, NV . . . . . Sep 12-21
Seattle . . . . . Seattle, WA. . . . . Oct 5-10
CDI. . . . . Washington, DC . . . . . Dec 12-19

Private Training

All SANS courses are available through Private Training.

vLive Events

Live Virtual Training . . . . . Sep 21-Oct 28
Live Virtual Training . . . . . Oct 12-Nov 18

Custom Simulcast

Customized training for distributed workforces

OnDemand

E-learning available anytime, anywhere, at your pace

SelfStudy

This course is available in SANS SelfStudy

SEC506: Securing Linux/Unix

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

"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

"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 Magazine

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 ipfilter 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

giac.org

sans.org/cyber-guardian

sans.edu

MEETS DoDD 8570 REQUIREMENTS
sans.org/8570

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; Sendmail; 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 principals 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

"It sparked my interest to get a deeper understanding of how to secure my systems at work and at home. The instructor's experience as a forensics examiner is of great interest and a definite plus. Great experience!"

-Tim Horne, Honeywell Aerospace

***SEC506** is available via* (subject to change):

Featured Training Events

Network Security . . Las Vegas, NV . . . . . Sep 12-21

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

SEC511: Continuous Monitoring and Security Operations

Covers NIST SP800-137: Continuous Monitoring

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

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

The Defensible Security Architecture, Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/ Continuous Security Monitoring (CSM), taught in this course will best position your organization or Security Operations Center (SOC) to analyze threats and detect anomalies that could indicate cybercriminal behavior. The payoff for this new proactive approach would be early detection of an intrusion, or successfully thwarting the efforts of attackers altogether. The National Institute of Standards and Technology (NIST) developed guidelines described in NIST SP 800-137 for Continuous Monitoring (CM), and Day five (5) will greatly increase your understanding and enhance your skills in implementing Continuous Monitoring utilizing NIST framework.

SANS is uniquely qualified to offer this course. Course authors Eric Conrad (GSE #13) and Seth Misenar (GSE #28) hold the distinguished GIAC Security Expert Certification (GSE). Both are experienced, real-world, practitioners who apply the concepts and techniques they teach in this course on a daily basis. SEC511 will take you on quite a journey. We start by exploring traditional security architecture to assess its current state and the attacks against it. Next, we discuss and discover modern security design that represents a new proactive approach to such architecture that can be easily understood and defended. We then transition to how to actually build the network and endpoint security, and then carefully navigate our way through automation, NSM/CDM/CSM. For timely detection of potential intrusions, the network and systems must be proactively and continuously monitored for any changes in the security posture that might increase the likelihood that attackers will succeed.

Your SEC511 journey will conclude with one last hill to climb! The final day (Day 6) features a capture-the-flag competition that challenges you to apply the skills and techniques learned in the course to detect and defend the modern security architecture that has been designed. Course authors Eric Conrad and Seth Misenar have designed the capture-the-flag competition to be fun, engaging, comprehensive, and challenging. You will not be disappointed!

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

Who Should Attend

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

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

"The SEC511 material is excellent. I appreciated the background and pen test material to build up defense. Good defense understands offense."

-Kenneth Hall, BCBSMS

giac.org

sans.edu

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 and continuous monitoring are required to achieve this goal.

Topics: Modern Security Architecture Principles; Frameworks and Enterprise Security Architecture; Security Architecture – Key Techniques/Practices; Security Operations Center (SOC)

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 two 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)

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; SOCs and Defensible Endpoint Security Architecture; 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 know when our systems, networks, and applications are at an increased likelihood for compromise. A strong way to achieve this is through Continuous Security Monitoring (CSM) or Continuous Diagnostics and Mitigation (CDM). Rather than waiting for the results of a quarterly scan or an annual penetration test to determine what needs to be addressed, continuous monitoring insists on proactively and repeatedly assessing and reassessing the current security posture for potential weaknesses that need be addressed. The volume of data that must continuously be sought and mined is vast: the goal of continuous monitoring would be out of reach without scripting and automation. Naturally, there are vendors and tools to scratch this itch, but they will be incomplete and require their own care, feeding, and monitoring. Day five describes how to perform continuous monitoring with simple tools and scripts.

Topics: CSM Overview; Industry Best Practices; Winning CSM Techniques; Maintaining Situational Awareness; Host, Port and Service Discovery; Vulnerability Scanning; Monitoring Patching; Monitoring Applications; Monitoring Service Logs; Monitoring Change to Devices and Appliances; Leveraging Proxy and Firewall Data; Configuring Centralized Windows Event Log Collection; Monitoring Critical Windows Events; Scripting and Automation

511.6 HANDS ON: Capstone: Design, Detect, and Defend

The course culminates in a team-based design, detect, and defend the flag competition. Powered by NetWars, day six provides a full day of hands-on work applying the principles taught throughout the week. Your team will progress through multiple levels and missions designed to ensure mastery of the modern cyber defense techniques promoted all week long. From security architecture, network security monitoring, endpoint security, and continuous monitoring, this challenging exercise will reinforce key principles in a fun, hands-on, team-based challenge.

Topics: Security Architecture; Assess-provided Architecture; Continuous Security Monitoring; Using Tools/Scripts to Assess the Initial State; Quickly/Thoroughly Find All Changes Made

***SEC511** is available via* (subject to change):

Featured Training Events

Capital City . . . . . Washington, DC . . . . . Jul 6-11
Boston . . . . . Boston, MA. . . . . Aug 3-8
Virginia Beach . . . Virginia Beach, VA . . . . Aug 24-29
Network Security . . Las Vegas, NV . . . . . Sep 12-21
Cyber Defense San Diego . . . . . Oct 19-24
CDI. . . . . Washington, DC . . . . . Dec 12-19

Summit Events

Cyber Defense. . . . . Nashville, TN. . . . . Aug 11-18

Community SANS Events

Chicago, IL . . . . . Jul 13-18
Charlotte, NC . . . . . Jul 20-25

Private Training

All SANS courses are available through Private Training.

vLive Events

Live Virtual Training . . . . . Oct 6-Nov 12

Event Simulcast

Virtual/Online . . . . . Aug 13-18

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

SEC542: Web App Penetration Testing and Ethical Hacking

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

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

"Everything is very well thought out and organized. The URLs used for the labs work flawlessly. Course content and teaching skills are great."
-Stephan Hofacker, InfoTrust AG

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, so 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.

"SEC542 is a step-by-step introduction to testing and penetrating web applications, a must for anyone who builds, maintains, or audits web systems."
-Brad Milhorn, i2P LLC

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

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

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

Who Should Attend

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

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
- Attack Proxy 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

giac.org

sans.org/cyber-guardian

sans.edu

542.1 HANDS ON: The Attacker's View of the Web

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 pen testing

542.2 HANDS ON: Reconnaissance and Mapping

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

Topics: Discovering the Infrastructure Within the Application; Identifying the Machines and Operating Systems; Secure Sockets Layer (SSL) Configurations and Weaknesses; Exploring Virtual Hosting and Its Impact on Testing; Learning Methods to Identify Load Balancers; Software Configuration Discovery; Exploring External Information Sources; 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: Discovery

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; Local File Inclusion (LFI); Remote File Inclusion (RFI); SQL Injection; Blind SQL Injection; JavaScript for the Attacker

542.4 HANDS ON: Discovery (CONTINUED)

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

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

542.5 HANDS ON: Exploitation

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: The sqlmap Tool; Metasploit for Web Penetration Testers; Exploring Methods to Zombify Browsers; Browser Exploitation Framework (BeEF); 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; Walking Through an Entire Attack Scenario

542.6 HANDS ON: Web Penetration Testing Tournament: Powered by NetWars

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 the 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

Capital City	Washington, DC	Jul 6-11
San Jose	San Jose, CA	Jul 20-25
Boston	Boston, MA	Aug 3-8
Network Security	Las Vegas, NV	Sep 12-21
South Florida	Ft. Lauderdale, FL	Nov 9-14
San Francisco	San Francisco, CA	Nov 30-Dec 5

Community SANS Events

Tampa, FL	Jul 6-11
Atlanta, GA	Aug 3-8

Summit Events

Pen Test Hackfest	Washington, DC	Nov 16-23

Mentor Program Events

McKinney, TX	Aug 4-Oct 6
Salt Lake City, UT	Aug 20-Oct 22

Private Training

All SANS courses are available through Private Training.

vLive Events

Live Virtual Training	Aug 4-Sep 10
Live Virtual Training	Dec 15-Feb 4

Custom Simulcast

Customized training for distributed workforces

OnDemand

E-learning available anytime, anywhere, at your pace

SelfStudy

This course is available in SANS SelfStudy

SEC560: Network Penetration Testing and Ethical Hacking

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

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

"This course has a direct correlation to my job duties, and the insight and use of various tools will make it a lot easier. You will learn some of the ways your systems are vulnerable."
-Roland T., USAF

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

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

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

"I think if you genuinely want to learn how exploitation techniques work and how to properly think like a hacker, it would be silly not to attend."
-Mark Hamilton, McAfee

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

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

"This course was tremendously timely and super relevant for my career."
-James Miller, SRA

Who Should Attend

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

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 attacks 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

giac.org sans.org/cyber-guardian sans.edu

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

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

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

560.2 HANDS ON: In-Depth Scanning

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

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

560.3 HANDS ON: Exploitation and Post-Exploitation

In this section, we look at the many kinds of exploits that penetration testers use to compromise target machines, including client-side exploits, service-side exploits, and local privilege escalation. We'll see how these exploits are packaged in frameworks like Metasploit and its mighty Meterpreter. You'll learn in-depth how to leverage Metasploit and the Meterpreter to compromise target environments, search them for information to advance the penetration test, and pivot to other systems, all with a focus on determining the true business risk of the target organization. We'll also look at post-exploitation analysis of machines and pivoting to find new targets, finishing the section with a lively discussion of how to leverage the Windows shell to dominate target environments.

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

560.4 HANDS ON: Password Attacks & Merciless Pivoting

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

Topics: Password Attack Tips; Account Lockout and Strategies for Avoiding It; Automated Password Guessing with THC-Hydra; Retrieving and Manipulating Hashes from Windows, Linux, and Other Systems; Massive Pivoting Through Target Environments; Extracting Hashes and Passwords from Memory with Mimikatz; Password Cracking with John the Ripper & Cain; Using Rainbow Tables to Maximum Effectiveness; Pass-the-Hash Attacks with Metasploit and More

560.5 HANDS ON: Wireless and Web Apps Penetration Testing

This in-depth section of the course is focused on helping you become a well-rounded penetration tester. Augmenting your network penetration testing abilities, we turn our attention to methods for finding and exploiting wireless weaknesses, including identifying misconfigured access points, cracking weak wireless protocols, and exploiting wireless clients. We then turn our attention to web application pen testing, with detailed hands-on exercises that involve finding and exploiting cross-site scripting (XSS), cross-site request forgery (XSRF), command injection, and SQL injection flaws in applications such as online banking, blog sites, and more.

Topics: Wireless Attacks; Discovering Access; Attacking Wireless Crypto Flaws; Client-Side Wireless Attacks; Finding and Exploiting Cross-Site Scripting; Cross-Site Request Forgery; SQL Injection; Leveraging SQL Injection to Perform Command Injection; Maximizing Effectiveness of Command Injection Testing

560.6 HANDS ON: Penetration Testing Workshop and Capture-the-Flag Event

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

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

***SEC560** is available via* (subject to change):

Featured Training Events

Minneapolis . . . . . Minneapolis, MN . . . . . Jul 20-25
San Antonio . . . . . San Antonio, TX . . . . . Aug 17-22
Virginia Beach . . . Virginia Beach, VA . . Aug 30-Sep 4
Network Security . . Las Vegas, NV . . . . . Sep 12-21
CDI . . . . . Washington, DC . . . . . Dec 12-19

Summit Events

Pen Test Hackfest. . . . Washington, DC . . . Nov 16-23

Community SANS Events

Ottawa, ON . . . . . Oct 19-24
Portland, OR . . . . . Oct 26-31

Mentor Program Events

Rockville, MD . . . . . Aug 13-Sep 24
Manasquan, NJ . . . . . Aug 26-Oct 28
Denver, CO . . . . . Sep 17-Nov 19

Private Training

All SANS courses are available through Private Training.

vLive Events

Live Virtual Training . . . . . Jul 6-Aug 12
Live Virtual Training . . . . . Nov 9-Dec 16

Event Simulcast

Virtual/Online . . . . . Sep 14-19

Custom Simulcast

Customized training for distributed workforces

OnDemand

E-learning available anytime, anywhere, at your pace

SelfStudy

This course is available in SANS SelfStudy

SEC561: Intense Hands-on Pen Testing Skill Development (with SANS NetWars)

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

"Hands down one of the best SANS courses I have taken. We learned cutting-edge pen testing techniques in a hands-on environment that challenged my abilities and increased my overall knowledge."
-Dave Odom, Bechtel

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.

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

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

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.

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

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?

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

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 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

The British government's Center for the Protection of National Infrastructure describes the Controls as the "baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence."

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

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

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

giac.org

sans.edu

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, AUD507, 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 Security 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 cover an introduction and overview of the 20 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**
- **Overview of Evaluating the Control**
- **Core Evaluation Test(s)**
- **Testing/Reporting Metrics**
- **Steps for Root Cause Analysis of Failures**
- **Audit/Evaluation Methodologies**
- **Evaluation Tools**
- **Exercise to Illustrate Implementation or Steps for Auditing a Control**

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

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

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

Topics: Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
Critical Control 4: Continuous Vulnerability Assessment and Remediation
Critical Control 5: Malware Defenses
Critical Control 6: Application Software Security

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

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

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

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

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

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

"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

***SEC566** is available via* (subject to change):

Featured Training Events

Crystal City . . . . . Crystal City, VA . . . . . .Sep 8-13
Network Security . . Las Vegas, NV . . . . . .Sep 12-21
San Francisco . . . . San Francisco, CA . . Nov 30-Dec 5
CDI. . . . . Washington, DC . . . . . .Dec 12-19

Community SANS Events

New York, NY . . . . . .October 5-9
Herndon, VA . . . . . .Nov 16-20

Summit Events

Cyber Defense. . . . . Nashville, TN. . . . .Aug 11-18
Security Awareness . . . Philadelphia, PA. . .Aug 17-25

Private Training

All SANS courses are available through Private Training.

Event Simulcast

Virtual/Online . . . . . .Aug 13-17

Custom Simulcast

Customized training for distributed workforces

OnDemand

E-learning available anytime, anywhere, at your pace

SelfStudy

This course is available in SANS SelfStudy

SEC573: Python for Penetration Testers

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!

"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: 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

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 tool to launch password guessing attacks. While developing this tool you will also make your code run faster by using multi-threading. You will handle a modern authentication system by finding cookies and bypassing CAPTCHAs. You will know how to enhance your program with local application proxies and how to create and use target customized password files.
- 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.

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

573.1 HANDS ON: Essentials Workshop – PART 1

The course begins with a brief introduction to Python and the pyWars Capture-the-Flag challenge. We set the stage for students to learn at their own pace in the 100% hands-on pyWars lab environment. More advanced students will take on Python-based Capture-the-Flag 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 pyWars 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 pyWars 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 available via* (subject to change):

Featured Training Events

Network Security . . Las Vegas, NV . . . . . Sep 12-21

Private Training

All SANS courses are available through Private Training.

Custom Simulcast

Customized training for distributed workforces

"SEC573 gave me exposure to tools and techniques I wouldn't have normally considered, but now are part of my arsenal."
-Allen C., DoD

"Great course – very advanced thinking required and the challenges are excellent."
-Kevin Nicholson, Motorola Solutions

SEC575: Mobile Device Security and Ethical Hacking

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

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

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

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

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

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

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

Who Should Attend

- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Security personnel whose job involves assessing, deploying or securing mobile phones and tablets
- Network and system administrators supporting mobile phones and tablets

You Will Be Able To

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

"Awesome course material. Day three really picked up the pace and demonstrated interesting techniques."
-Ted Moskalenko, University of Pennsylvania

giac.org

sans.edu

575.1 HANDS ON: Architecture and Management

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 implementation differences between Android, Apple, BlackBerry, and Windows Phone systems, including platform software defenses and application permission management. We'll also look at the specific implementation details of popular platform features such as iBeacon, AirDrop, App Verification and more. We'll apply hands-on exercises to interact with mobile device emulator features including low-level access to installed application services.

Topics: Mobile Problems and Opportunities; Mobile Devices and Infrastructure; Mobile Device Security Models; Mobile Device Lab Analysis Tools; Mobile Device Malware Threats

575.2 HANDS ON: Security Controls and Platform Access

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

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

575.3 HANDS ON: Application Analysis

One of the critical decisions you will need to make in supporting a mobile device deployment is to approve or disapprove of unique application requests from end-users in a corporate device deployment. With some analysis skills, we can evaluate applications to determine the type of access and information disclosure threats they represent. We'll examine the techniques for reverse-engineering iOS and Android applications, obtaining source code for applications from public app stores. For Android applications we'll look at opportunities to change the behavior of applications as part of our analysis process by decompiling, manipulating, and recompiling code, and adding new code to existing applications without prior source code access. For iOS we'll extract critical app definition information available in all apps to examine and manipulate app behavior through the Cycript tool.

Topics: Static Application Analysis; Automated Application Analysis Systems; Manipulating App Behavior

575.4 HANDS ON: Penetration Testing Mobile – PART 1

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

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

575.5 HANDS ON: Penetration Testing Mobile – PART 2

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

Topics: Network Manipulation Attacks; Mobile Application Attacks; Web Framework Attacks; Back-end Application Support Attacks

575.6 HANDS ON: Mobile Security Event

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 3-8
Virginia Beach . . . Virginia Beach, VA . . Aug 30-Sep 4
Network Security . . Las Vegas, NV . . . . . Sep 12-21
Seattle . . . . . Seattle, WA. . . . . .Oct 5-10
CDI. . . . . Washington, DC . . . . .Dec 12-19

Private Training

All SANS courses are available through Private Training.

Event Simulcast

Virtual/Online . . . . . Sep 14-19

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: Virtualization and Private Cloud Security

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

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

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

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.

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

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

"Class continues to be spot-on. I'm really enjoying class and taking a lot from it as it's forcing me to think about architectural items we hadn't considered as an organization."
-Glenn Galang, Lake Villa District Library

579.1 HANDS ON: Virtualization Security Architecture and Design

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

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

579.2 HANDS ON: Virtualization & Private Cloud Infrastructure Security

The next section will delve into network security adapted to fit into a virtual infrastructure. Do firewalls and network access controls work the same with virtual systems and cloud models? We will find out! Students will take an in-depth look at virtual firewalls and even set one up. Virtual switches will be revisited here, as they pertain to segmentation and access controls. Students will also build a virtualized intrusion detection model, integrating promiscuous interfaces and traffic capture methods into virtual networks, then setting up and configuring a virtualized intrusion detection system (IDS) sensor. Some attention will also be paid to host-based IDS, with considerations for multitenant platforms and the performance impact any agent-based product can have in a virtual environment.

579.3 HANDS ON: Virtualization Offense and Defense – PART 1

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

579.4 HANDS ON: Virtualization Offense and Defense – PART 2

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

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

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

579.6 HANDS ON: Auditing and Compliance for Virtualization and Cloud

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

***SEC579** is available via* (subject to change):

Featured Training Events

Capital City . . . . . Washington, DC . . . . . Jul 6-11
Chicago . . . . . Chicago, IL. . . . . Aug 30-Sep 4
Network Security . . Las Vegas, NV . . . . . Sep 12-21
CDI. . . . . Washington, DC . . . . . Dec 12-19

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

SEC617: Wireless Ethical Hacking, Penetration Testing, and Defenses

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 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 the 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

To be a wireless security expert, you need to have a comprehensive understanding of the technology, threats, exploits, and defense 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 was great! I am still impressed with the consistency from day one thru day six. The instructor keeps a high level of energy and knowledge throughout."
-Philip Mein, JCCC

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

giac.org

sans.org/cyber-guardian

sans.edu

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 802.11a/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

***SEC617** is available via* (subject to change):

Featured Training Events

Network Security . . Las Vegas, NV . . . . . Sep 12-21

Summit Events

Pen Test Hackfest. . . . Washington, DC . . . Nov 16-23

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

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 to 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

SEC642: Advanced Web App Penetration Testing and Ethical Hacking

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.

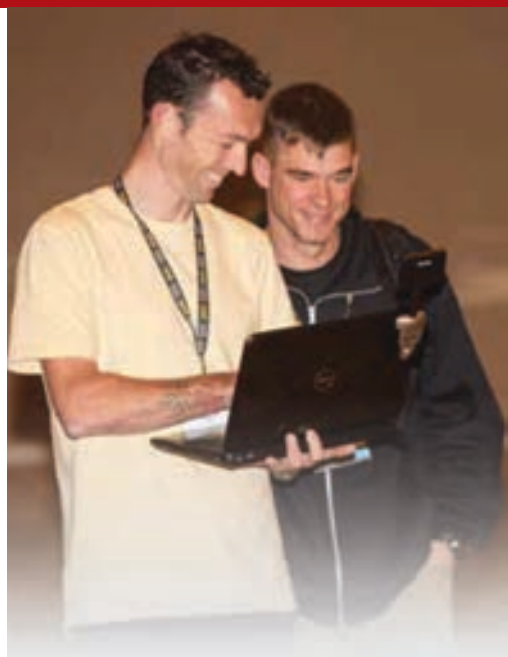
"The real-world examples presented will be useful when I go back to report to my executive management."
-Jason Balderann, County of Marin

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.

"I feel like I level-up every time I do a SANS course."
-Jake Evans, Oracle

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



Who Should Attend

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

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

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

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

642.4 HANDS ON: Mobile Applications and Web Services

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

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

642.5 HANDS ON: Web Application Firewall and Filter Bypass

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

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

642.6 HANDS ON: Capture the Flag

During day six of the class, you will be placed on a network and given the opportunity to complete an entire penetration test. The goal of this Capture-the-Flag event is for you to explore the techniques, tools, and methodology you will have 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 (SamuraiWTF) 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

Minneapolis . . . . . Minneapolis, MN . . . . . Jul 20-25
Network Security . . Las Vegas, NV . . . . . Sep 12-21

Private Training

All SANS courses are available through Private Training.

Event Simulcast

Virtual/Online . . . . . Sep 14-19

Custom Simulcast

Customized training for distributed workforces

OnDemand

E-learning available anytime, anywhere, at your pace

SelfStudy

This course is available in SANS SelfStudy

SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

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 engages attendees with in-depth knowledge of the most prominent and powerful attack vectors and an environment to perform these attacks in numerous hands-on scenarios. This course goes far beyond simple scanning for low-hanging fruit, and shows penetration testers how to model the abilities of an advanced attacker to find significant flaws in a target environment and demonstrate the business risk associated with these flaws.

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

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

"SEC660 course was hands-on, packed with content, and current to today's technology!"
-Michael Horken, Rockwell Automation

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

giac.org

sans.org/cyber-guardian

sans.edu

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

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

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

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

***SEC660** is available via* (subject to change):

Featured Training Events

Capital City . . . . . Washington, DC . . . . . Jul 6-11
Network Security . . Las Vegas, NV . . . . . Sep 12-21
CDI. . . . . Washington, DC . . . . . Dec 12-19

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

660.3 HANDS ON: Python, Scapy, and Fuzzing

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

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

660.4 HANDS ON: Exploiting Linux for Penetration Testers

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

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

660.5 HANDS ON: Exploiting Windows for Penetration Testers

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

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

660.6 HANDS ON: Capture the Flag

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

SEC760: Advanced Exploit Development for Penetration Testers

"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 Kitaichit, Intel

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

Some of the skills you will learn in SEC760 include:

- How to write modern exploits against the Windows 7 and 8 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

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

What You Will Receive

- Various preconfigured *NIX virtual machines; however, you are required to bring the Windows virtual machines discussed in the Laptop Requirements section
- 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

Not sure if you are ready for SEC760?

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

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 Exploitaiton

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 darungrim3; Visualizing Code Changes and Identifying Fixes; Reversing 32-bit and 64-bit Applications and Modules; Triggering Patched Vulnerabilities; Writing One-Day Exploits; Handling Modern Exploit Mitigation Controls; Using ROP to Compiled Shellcode on the Fly (Return-Oriented Shellcode)

760.4 HANDS ON: Windows Kernel Debugging and Exploitation

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

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

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

The focus of this section is primarily on Windows browser and client-side exploitation. You will learn to analyze C++ 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

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

***SEC760** is available via* (subject to change):

Summit Events

Pen Test Hackfest. . . . Washington, DC . . . Nov 16-23

Private Training

All SANS courses are available through Private Training.

Custom Simulcast

Customized training for distributed workforces

AUD507: Auditing & Monitoring Networks, Perimeters, and Systems

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

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

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 not only prepares you to perform a comprehensive audit but also provides excellent information to operations for an improved network security posture."
-Rifat I., State Dept. FCU

One of the 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 how to automatically validate defenses through instrumentation and automation of audit checklists.

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

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

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

You Will Be Able To

- Understand the different types of controls (e.g., technical vs. non-technical) essential to performing a successful audit
- Conduct a proper network risk assessment to identify vulnerabilities and prioritize what will be audited
- Establish a well-secured baseline for computers and networks—a standard to conduct an audit against
- 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 risks and resources.
- Audit configuration, authentication, and session management of a web application 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

***Audit 507** is available via* (subject to change):

Featured Training Events

Crystal City . . . . . Crystal City, VA . . . . . .Sep 8-13
Network Security . . Las Vegas, NV . . . . . .Sep 12-21
San Francisco . . . . San Francisco, CA . . .Nov 30-Dec 5
CDI. . . . . Washington, DC . . . . . .Dec 12-19

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

giac.org sans.edu MEETS DoDD 8570 REQUIREMENTS sans.org/8570

ICS410: ICS/SCADA Security Essentials

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.

"ICS410 really opens you up to possibilities and issues that otherwise you wouldn't really think about."
-Alfonso Barreiro, Panama Canal Authority

The course will provide you with:

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

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

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

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

Who Should Attend

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

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

giac.org

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, etc.) 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

***ICS410** is available via* (subject to change):

Featured Training Events

Minneapolis . . . . . Minneapolis, MN . . . . . Jul 20-25
Crystal City . . . . . Crystal City, VA . . . . . Sep 8-13
Network Security . . Las Vegas, NV . . . . . Sep 12-21
CDI. . . . . Washington, DC . . . . . Dec 12-19

Community SANS Events

Atlanta, GA . . . . . Sep 28-Oct 2

OnSite

All SANS courses are available through Private Training.

Event Simulcast

Live Virtual Training . . . . . Aug 28-Sep 1

OnDemand

E-learning available anytime, anywhere, at your pace

SelfStudy

This course is available in SANS SelfStudy

LEG523: Law of Data Security & Investigations

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

"I have gained many valuable ideas and tools to support and defend my organization and to strengthen security over all."
-Tom Siu, Case Western Reserve University

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

Each successive day of this five-day course builds upon lessons from the earlier days in order to comprehensively strengthen your ability to help your enterprise (public or private sector) cope with illegal hackers, botnets, malware, phishing, unruly vendors, data leakage, industrial spies, rogue or uncooperative employees, or bad publicity connected with IT security. We will cover recent stories ranging from Home Depot's legal and public statements about a payment card breach to the lawsuit by credit card issuers against Target's QSA and security vendor, Trustwave.

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

"This course provided depth of subject and firmly reinforced facts and theory with case history. Very high impact combination."
-Mike Bando, U.S. National Park Service

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

Who Should Attend

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

"LEG523 was an excellent use of time. [The course instructor] knows the material very well. He has excellent flow and is right on target with the course description."
-Sharon O'Bryan, DeVry Inc.

***LEG523** is available via* (subject to change):

Featured Training Events

Chicago . . . . . Chicago, IL . . . . . Aug 30-Sep 4
Network Security . . Las Vegas, NV . . . . . Sep 12-21
CDI . . . . . Washington, DC . . . . . Dec 12-19

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

giac.org

sans.edu

SANS Hosted is a series of courses presented by other educational providers to complement your needs for training outside of our current course offerings. A complete list of Hosted courses and descriptions is available at at sans.org/courses/hosted.

(ISC)²® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Education Program

Five Days | 30 CPEs

This course will help you advance your software development expertise by ensuring you're properly prepared to take on the constantly evolving vulnerabilities exposed in the SDLC. It will train you on every phase of the software lifecycle, detailing security measures and best practices for each phase. The CSSLP® Education Program is for all the stakeholders involved in software development. By taking this course, you will not only enhance your ability to develop software with more assurance, you will also understand how to build security within each phase of the software lifecycle.

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.

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. Some of the things we talk about you may implement immediately, others may take you a while to implement. Either way, consider what we discuss as a collection of tools at your disposal when you need them to annoy attackers, determine who is attacking you and, finally, attack the attackers.

This class is based on the DARPA-funded Active Defense Harbinger Distribution live Linux environment. This virtual machine is built from the ground up for defenders to quickly implement Active Defenses in their environments. This class is also very heavy with hands-on labs. We won't just talk about Active Defenses. We will be doing hands-on labs in a way that will enable you to quickly and easily implement what you learn in your working environment.

Physical Penetration Testing

Two Days | 12 CPEs

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

Those who attend this session will leave with a full awareness of how to best protect buildings and grounds from unauthorized access, as well as how to compromise most existing physical security in order to gain access themselves. Attendees will not only learn how to distinguish good locks and access 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.

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 ("ePHI"). Administrative insights for those managing the many aspects of health care security operations will also be discussed. The goal of the course is to present a substantive overview and analysis of relevant information security subject matter that is having a direct and material impact on the U.S. health care system.

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 Council on CyberSecurity. 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. If the student is looking for hands-on labs involving the Critical Controls, they should take SEC566.

SEC464: Cyber Security Training for IT Administrators (2 DAYS)
There are not enough well-trained IT administrators and operations staff to meet the daily onslaught of cyber criminal and cyber terrorist activities. Sandia National Labs, NASA, and the State of Texas recently demonstrated that we can address this issue by leveraging the large number of IT admins within an organization to act as a hacker guard to help thwart many of these attacks. As will be examined in this course, the goal is to have IT administrators in an organization serve as the first line of defense as human intrusion detectors.

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.

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.

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.

DEVELOPER

DEV536: Secure Coding: Developing Defensible Applications (2 DAYS)
The audit procedure documents for PCI 1.2 tell auditors that they should look for evidence that web application programmers in a PCI environment have had "training for secure coding techniques." The problem that many businesses are facing, however, is, "What is that and where can I get it?" This course packs a thorough explanation and examination of the OWASP top ten issues, which are the foundation of the PCI requirement, into a two-day course.

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.

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.

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 infrastructures 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 infrastructures and the dangers posed by the global Internet.

MGT415: A Practical Introduction to Risk Assessment (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 every organization, 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.

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.

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. 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. For security professionals, the course enables you to see how to put the controls in place in your existing network through effective and widespread use of cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how to measure if the 20 Critical Controls are effectively implemented. If the student is looking for hands-on labs involving the Critical Controls, they should take SEC566.

INDUSTRIAL CONTROL SYSTEMS

ICS515: Industrial Control System Active Defense and Incident Response *NEW!* (5 DAYS)
This course is designed to empower students to understand and utilize active defense mechanisms in concert with incident response for industrial control system networks in order to respond to and deny cyber threats.

For schedules, course updates, prerequisites, special notes, or laptop requirements, visit sans.org/courses

SECURITY AWARENESS

FOR THE 21ST CENTURY

End User - Utility - Engineer - Developer - Healthcare - Phishing

- Go beyond compliance and focus on changing behaviors.
- Create your own training program by choosing from a variety of computer based training modules:
  - STH.End User is mapped against the Critical Security Controls.
  - STH.Utility fully addresses NERC-CIP compliance.
  - STH.Engineer focuses on security behaviors for individuals who interact with, operate, or support Industrial Control Systems.
  - STH.Developer uses the OWASP Top 10 web vulnerabilities as a framework.
  - STH.Healthcare focuses on security behaviors for individuals who interact with Protected Health Information (PHI).
  - Compliance modules cover various topics including PCI DSS, Red Flags, FERPA, and HIPAA, to name a few.
- Test your employees and identify vulnerabilities through STH.Phishing emails.

SANS SECURING THE HUMAN

For a free trial visit us at:
www.securingthehuman.org

TWO NIGHTS OF
NETWARS
TOURNAMENT [CORE / DFIR]

= FREE

W/ PAID REGISTRATION OF A 4 - 6 DAY SANS COURSE
AT A PARTICIPATING SANS TRAINING EVENT
SEE WEBSITE FOR DETAILS - SANS.ORG/NETWARS

SANS

NETWARS

HANDS-ON | INTERACTIVE | ENGAGING | INFOSEC TRAINING

4 WAYS TO EXPERIENCE NETWARS

TOURNAMENT [CORE & DFIR]

LIVE | IN-PERSON | HANDS-ON | COMPETITIVE | EXCITING | EDUCATIONAL

AVAILABLE AS AN ADD-ON AT MOST SANS TRAINING EVENTS & AS A PRIVATE TRAINING EVENT FOR YOUR ORGANIZATION

CONTINUOUS

ONDEMAND | HANDS-ON | 4-MONTHS | IN-DEPTH | HINTS | TECHNICAL SUPPORT

AVAILABLE ONLINE, ANYTIME, WHEN YOU WANT TO TRAIN - EXTENSIONS AVAILABLE

TRAINING COURSES

6-DAY SANS TRAINING | IMMERSIVE | HANDS-ON | INSTRUCTOR SUPPORT

SEC561: INTENSE HANDS-ON PEN TESTING (pg 58-59) | SEC562: CYBERCITY HANDS-ON KINETIC CYBER RANGE EXERCISE (pg. 11)

CYBERCITY

ICS / SCADA | HANDS-ON | TEAM BASED | COLLABORATIVE | MISSION-ORIENTED

AVAILABLE AT SANS TRAINING EVENTS (SEC562) & AS A PRIVATE TRAINING EVENT FOR YOUR ORGANIZATION

"We were very impressed with SANS NetWars. The material is relevant and educational, and the tournament-style play is remarkably engaging. I really like the scoring system and scoreboard." - Adam Tice, Lockheed Center for Cyber Security

IN-DEPTH INFORMATION, PHOTOS, VIDEOS, AND TO REGISTER FOR NETWARS TRAINING - VISIT:

sans.org/NETWARS

Top 5 Reasons

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

SANS Leadership

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

Reduce Hiring Costs

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

Better Team Management

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

Ensure Contractor's Skills

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

Prepare for Today's Threats

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

SANS CyberTalent offers three web-based assessments:

- Cyber Defense
- Penetration Testing
- Digital Forensics

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

SANS | CyberTalent

sans.org/cybertalent

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

Sign up for a FREE demo

sans.org/cybertalent/free-demo

SANS CYBER GUARDIAN PROGRAM

www.sans.org/
cyber-guardian

Stay ahead of cyber threats!

Join the SANS Cyber Guardian program today.

How the SANS Cyber Guardian Program Works

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.

Contact us at onsite@sans.org to get started!

Program Prerequisites

- Five years of industry-related experience
- A GSEC certification (with a score of 80 or above) or CISSP certification

Core Courses

SEC503	Intrusion Detection In-Depth (GCIA)
SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling (GCIH)
SEC560	Network Penetration Testing and Ethical Hacking (GPEN)
FOR508	Advanced Digital Forensics and Incident Response (GCFA)

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

Blue Team Courses

SEC502	Perimeter Protection In-Depth (GPPA)
SEC505	Securing Windows with PowerShell and the Critical Security Controls (GCWN)
SEC506	Securing Linux/Unix (GCUX)

Red Team Courses

SEC542	Web App Penetration Testing & Ethical Hacking (GWAPT)
SEC617	Wireless Ethical Hacking, Penetration Testing, and Defenses (GAWN)
SEC660	Advanced Penetration Testing, Exploit Writing, and Ethical Hacking (GXPN)

The SANS Cyber Guardian program is a unique opportunity for information security individuals or organizational teams to develop specialized skills in incident handling, perimeter protection, forensics, and penetration testing.

Department of Defense Directive 8570
(DoDD 8570)

sans.org/8570

Department of Defense Directive 8570 (DoDD 8570) 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 provides the most options in the industry for meeting 8570 requirements.

DoD Baseline IA Certifications

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

Computer Network Defense (CND) Certifications

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

Information Assurance System Architecture & Engineering (IASAE) Certifications

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

Computer Environment (CE) Certifications

GCWN	**GCUX**

Compliance/Recertification:

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

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

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

For more information, contact us at 8570@sans.org or visit sans.org/8570

SANS Training Courses for DoDD Approved Certifications

SANS TRAINING COURSE		DoDD APPROVED CERT
SEC401	**Security Essentials Bootcamp Style**	**GSEC**
SEC501	**Advanced Security Essentials – Enterprise Defender**	**GCED**
SEC503	**Intrusion Detection In-Depth**	**GCIA**
SEC504	**Hacker Tools, Techniques, Exploits, and Incident Handling**	**GCIH**
SEC505	**Securing Windows with PowerShell and the Critical Security Controls**	**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**

Group Discounts for SANS Security Training

sans.org/vouchers

SANS Universal Voucher Credit Program

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

SANS Universal Voucher Credit Benefits

- **Valid for classroom, online learning, and GIAC certification**
- **Cost savings help you expand your training budget**
- **Extends your fiscal year**
- **Free Learning Management Tool featuring online enrollment and usage reports**
- **Online access to credits, orders, and GIAC certification results**
- **Fully transferable**
- **Only one procurement is needed for 12 months, but you can add funds to renew the account at any time**
- **Great way to motivate and retain your valued employees**

If your organization prefers online training, find out how you can earn an additional 5% bonus with a ***SANS Online Voucher Credit Program*** for OnDemand and vLive courses. To learn more, please contact onlinevoucher@sans.org or visit the SANS Voucher Credit Program. SANS Universal Credit allows you to invest today, earn instant credits, and decide later how to spend your training credits over the next 12 months to maximize your investment and extend your fiscal year.

Create an Account

Creating your SANS Universal or Online Voucher Credit Account is easy.

- Visit sans.org/vouchers for details
- Email Vouchers@sans.org for a proposal or questions
- Designate a "Voucher Administrator" responsible for allocating credits.

Questions?

E-mail
vouchers@sans.org

or call
301-654-SANS (7267)
[Mon-Fri, 9am-8pm EST]

SANS Voucher Credit Pricing and Savings

Minimum Investment	Maximum Investment	Bonus	Example
$35,000	$74,999	10%	$50,000 investment = $55,000
$75,000+		Call	Contact Your Account Manager vouchers@sans.org

SANS TRAINING FORMATS

LIVE TRAINING

Multi-Course Training Events

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

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

Summit

sans.org/summit

Live IT Security Summits and Training

Community SANS

sans.org/community

Live Training in Your Local Region with Smaller Class Sizes

Private Training

sans.org/private-training

Live Training at Your Office Location

Mentor

sans.org/mentor

Live Multi-Week Training with a Mentor

ONLINE TRAINING

OnDemand

sans.org/ondemand

Four Months of Self-Paced e-Learning

vLive

sans.org/vlive

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

Simulcast

sans.org/simulcast

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

SelfStudy

sans.org/selfstudy

Self-Paced Study with Lecture Audio

OnDemand Bundles

sans.org/ondemand/bundles

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

SANS TRAINING EVENTS

FEATURED EVENTS

Capital City | Washington, DC | July 6-11, 2015

Minneapolis | July 20-25, 2015

San Jose | July 20-25, 2015

Boston | August 3-8, 2015

San Antonio | August 17-22, 2015

Virginia Beach | August 24 - September 4, 2015

Chicago | August 30 - September 4, 2015

FOR578 Cyber Threat Intelligence
Tysons Corner, VA | August 31 - September 4

Crystal City | Crystal City, VA | September 8-13, 2015

Network Security | Las Vegas, NV | Sept 12-21, 2015

Baltimore | September 21-26, 2015

Seattle | October 5-10, 2015

Tysons Corner | Tysons Corner, VA | Oct 12-17, 2015

Cyber Defense San Diego | October 19-24, 2015

South Florida | Ft. Lauderdale, FL | November 9-14, 2015

San Francisco | November 30 - December 5, 2015

Cyber Defense Initiative
Washington, DC | December 12-19, 2015

SUMMIT EVENTS

Digital Forensics & Incident Response
Austin, TX | July 7-14, 2015

Cyber Defense
Nashville, TN | August 11-18, 2015

Security Awareness
Philadelphia, PA | August 17-25, 2015

Cyber Crime
Dallas, TX | September 21-26, 2015

Pen Test Hackfest
Washington, DC | November 16-23, 2015

Security Leadership
Dallas, TX | December 3-10, 2015

COMMUNITY SANS EVENTS

Tampa, FL	SEC542	July 6-11
New Orleans, LA	SEC301	July 13-17
New York, NY	MGT512	July 13-17
Philadelphia, PA	SEC301	July 13-17
New Orleans, LA	SEC504	July 13-18
Chicago, IL	SEC511	July 13-18
Baltimore, MD	SEC401	July 20-25
Baltimore, MD	SEC504	July 20-25
Chantilly, VA	MGT414	July 20-25
Charlotte, NC	SEC511	July 20-25
Indianapolis, IN	SEC301	July 20-24
Tucson, AZ	SEC440	July 23-24
Dallas, TX	MGT414	July 27 - August 1
St. Louis, MO	MGT414	July 27 - August 1
Chantilly, VA	SEC301	August 3-7
Atlanta, GA	SEC542	August 3-8
Anaheim, CA	SEC401	August 10-15
Cupertino, CA	SEC301	August 10-14
Ft. Lauderdale, FL	MGT414	August 10-15
Albuquerque, NM	SEC440	August 14-15
Charleston, SC	SEC401	August 17-22
Rockville, MD	MGT414	August 17-22
Columbus, OH	SEC504	August 24-29
Milwaukee, WI	SEC401	September 14-19
Minneapolis, MN	SEC301	September 21-25
Colorado Springs, CO	SEC504	September 21-26
Atlanta, GA	ICS410	Sep 28-Oct 2
Kansas City, MO	SEC401	Sep 28 - Oct 3
New York, NY	SEC566	October 5-9
Madison, WI	SEC401	October 5-10
Raleigh, NC	SEC504	October 5-10
Austin, TX	MGT414	October 5-10
Jacksonville, FL	SEC401	October 12-17
Alexandria, VA	SEC504	October 26-31
Portland, OR	SEC560	October 26-31
Boston, MA	MGT414	November 2-7
Memphis, TN	SEC301	November 9-13
Herndon-Reston, VA	SEC566	November 9-14
New York, NY	SEC401	November 9-14
San Antonio, TX	SEC401	November 9-14
Salt Lake City, UT	SEC401	Nov 16-21
Chantilly, VA	FOR585	December 7-12

For a complete list of all SANS training events, visit
sans.org/security-training/by-location/all

SANS NewsBites

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

InfoSec Reading Room

Computer security research and whitepapers

Security Policies

Templates for rapid information security policy development

Top 25 Software Errors

The most widespread and critical errors leading to serious vulnerabilities

OUCH!

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

Open a SANS Portal Account

Sign up for a **SANS Portal Account** and receive free webcasts, newsletters, the latest news and updates, and many other free resources.

sans.org/account

Webcasts

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

Critical Security Controls

Consensus guidelines for effective cyber defense

Industry Thought Leadership

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

Intrusion Detection FAQ

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

@RISK: The Consensus Security Alert

@RISK provides a reliable weekly summary of:

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

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