SANS Information Security Training

Offered in Texas

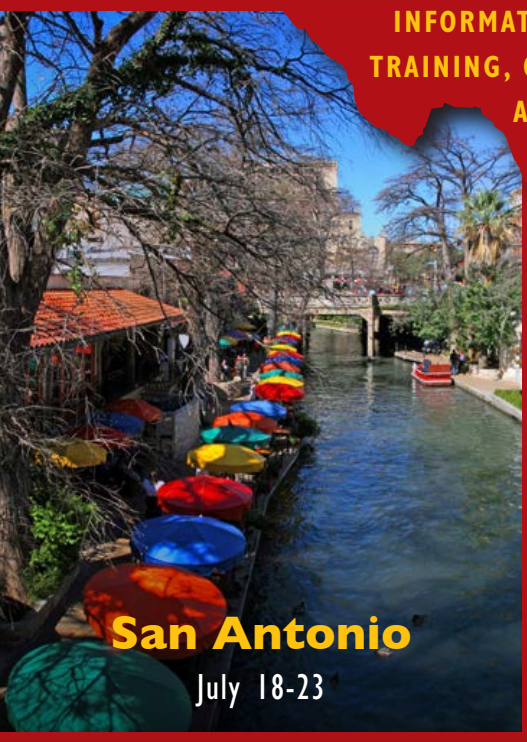
Pen Test Austin

April 18-23

Houston

May 9-14

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



San Antonio

July 18-23

Dallas

August 8-13

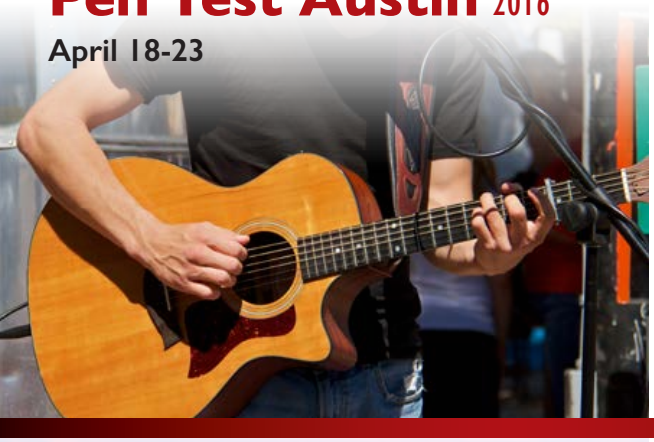
Get local information security training this spring/summer from SANS:

17 courses on cyber defense, pen testing, incident response, digital forensics, security management, and more!

sans.org/texas

Pen Test Austin 2016

April 18-23



COURSES:	INSTRUCTORS:
SEC401	*Paul A. Henry*
SEC504	*Kevin Fiscus*
SEC560	*Ed Skoudis*
SEC642	*Adrien de Beaupre*
SEC660	*Stephen Sims*
HOSTED	*The CORE Group*
The SANS NetWars Experience	

sans.org/pentest2016

Houston 2016

May 9-14

COURSES:	INSTRUCTORS:
SEC401	*Ted Demopoulos*
SEC503	*Dr. Johannes Ullrich*
SEC504	*Bryce Galbraith*
SEC511	*Jonathan Ham*
SEC560	*Adrien de Beaupre*
FOR408	*David Cowen*
MGT525	*Jeff Frisk*
LEG523	*Benjamin Wright*

sans.org/houston-2016

San Antonio 2016

July 18-23

COURSES:	INSTRUCTORS:
SEC301	*My-Ngoc Nguyen*
SEC401	*Keith Palmgren*
SEC503	*Kevin Fiscus*
SEC504	*BJ Gleason*
SEC550	*Bryce Galbraith*
FOR578	*Robert M. Lee*
MGT512	*G. Mark Hardy*
The SANS NetWars Experience	

sans.org/san-antonio-2016

Dallas 2016

August 8-13

COURSES:	INSTRUCTORS:
SEC401	*Paul A. Henry*
SEC504	*Christopher Crowley*
SEC560	*Kevin Fiscus*
FOR572	*Philip Hagen*
FOR610	*Anuj Soni*
AUD507	*David Hoelzer*

sans.org/dallas-2016

COURSES and TRAINING EVENTS	Austin April 18-23	Houston May 9-14	San Antonio July 18-23	Dallas August 8-13
SEC301 Intro to Information Security			SEC301	
SEC401 Security Essentials Bootcamp Style	SEC401	SEC401	SEC401	SEC401
SEC503 Intrusion Detection In-Depth		SEC503	SEC503	
SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	SEC504	SEC504	SEC504	SEC504
SEC511 Continuous Monitoring and Security Operations		SEC511		
SEC550 Active Defense, Offensive Countermeasures, and Cyber Deception			SEC550	
SEC560 NEW Network Penetration Testing and Ethical Hacking	SEC560	SEC560		SEC560
SEC642 Advanced Web App Penetration Testing and Ethical Hacking	SEC642			
SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	SEC660			
FOR408 Windows Forensic Analysis		FOR408		
FOR572 Advanced Network Forensics and Analysis				FOR572
FOR578 NEW Cyber Threat Intelligence			FOR578	
FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques				FOR610
MGT512 SANS Security Leadership Essentials for Managers with Knowledge Compression™			MGT512	
MGT525 IT Project Management, Effective Communication, and PMP® Exam Prep		MGT525		
LEG523 Law of Data Security and Investigations		LEG523		
AUD507 Auditing & Monitoring Networks, Perimeters, and Systems				AUD507
HOSTED NEW Physical Security Specialist – Facilities Edition	HOSTED			

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

David Cowen
SANS Instructor
@hecfblog

FOR408 – Houston

Christopher Crowley
Certified Instructor
@CCrowMontance

SEC504 – Dallas

Adrien de Beaupre
Certified Instructor
@adriendb

SEC642 – Pen Test Austin
SEC560 – Houston

Ted Demopoulos
Certified Instructor
@TedDemop

SEC401 – Houston

Kevin Fiscus
Certified Instructor
@kevinbfiscus

SEC504 – Pen Test Austin
SEC503 – San Antonio
SEC560 – Dallas

Jeff Frisk
Certified Instructor

MGT525 – Houston

Bryce Galbraith
Principal Instructor
@brycegalbraith

SEC504 – Houston
SEC550 – San Antonio

BJ Gleason
SANS Instructor
@bjgSANS

SEC504 – San Antonio

Philip Hagen
Certified Instructor
@PhilHagen
FOR572 – Dallas

Jonathan Ham
Certified Instructor
@jhamcorp
SEC511 – Houston

G. Mark Hardy
Certified Instructor
@jg_mark
MGT512 – San Antonio

Paul A. Henry
Senior Instructor
@phenrycissp
SEC401 – Pen Test Ausin
SEC401 – Dallas

David Hoelzer
Faculty Fellow
@it_audit
AUD507 – Dallas

Robert M. Lee
Certified Instructor
@RobertMLee
FOR578 – San Antonio

My-Ngoc Nguyen
Certified Instructor
@MenopN
SEC301 – San Antonio

Keith Palmgren
Certified Instructor
@kpalmgren
SEC401 – San Antonio

Stephen Sims
Senior Instructor
@Steph3nSims
SEC660 – Pen Test Austin

Ed Skoudis
Faculty Fellow
@edskoudis
SEC560 –Pen Test Austin

Anuj Soni
Certified Instructor
@asoni
FOR610 – Dallas

Dr. Johannes Ullrich
Senior Instructor
@johullrich
SEC503 – Houston

Benjamin Wright
Senior Instructor
@benjaminwright
LEG523 – Houston

Bios on all instructors can be found at:
sans.org/event/**pentest2016**/instructors
sans.org/event/**houston-2016**/instructors
sans.org/event/**san-antonio-2016**/instructors
sans.org/event/**dallas-2016**/instructors

SANS SEC301

Intro to Information Security

Five-Day Program
30 CPEs
Laptop Required

TRAINING EVENT

San Antonio
July 18-22 | My-Ngoc Nguyen

giac.org

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

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

"Good basic information for someone just coming into the field."
-Bryce Richert, SUH

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

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

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

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

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

"I very much appreciate the passion of the instructors. Their knowledge is incredible and the presentation of their knowledge is down-to-earth and helpful. SANS training is far better than privacy-related certification."
-Ron Hoffman, Mutual of Omaha

Security Essentials Bootcamp Style

SANS SEC401

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

STOP and ask yourself the following questions:

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

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

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

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

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

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

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

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

Six-Day Program
46 CPEs
Laptop Required

TRAINING EVENTS

Pen Test Austin
April 18-23 | Paul A. Henry

Houston
May 9-14 | Ted Demopoulos

San Antonio
July 18-23 | Keith Palmgren

Dallas
August 8-13 | Paul A. Henry

giac.org

sans.edu

sans.org/cyber-guardian

MEETS DoDD 8140
(8570) REQUIREMENTS

sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

Who Should Attend

- Security professionals
- Managers
- Operations personnel
- IT engineers and supervisors
- Administrators
- Forensic specialists, penetration testers, and auditors
- Anyone new to information security with some background in information systems and networking

SANS SEC503

Intrusion Detection In-Depth

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENTS

Houston
May 9-14 | Dr. Johannes Ullrich

San Antonio
July 18-23 | Kevin Fiscus

Dallas
August 8-13 | Jonathan Ham

giac.org

sans.edu

sans.org/cyber-guardian

MEETS DoDD 8140
(8570) REQUIREMENTS

sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

Who Should Attend

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

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

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

"Today has been brilliant, bringing all of our skills together to achieve the challenge. I wish we could do this every day!"
-Hayley Roberts, MOD

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

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

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS SEC504

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.

"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

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

"Excellent course. I've learned about the techniques and tools used by the bad guys and I have a greater understanding of how to protect our network."
-Howard Duck, Schools Financial Credit Union

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.

"The course was a real eye opener and I now realize the wide range of attacks available. This should be mandatory for all in IT development."
-Andrew Tolhurst, ABC

"Best course I've ever taken."
-Edward D., Norwegian Defence Logistics Organisation

Six-Day Program
37 CPEs
Laptop Required

TRAINING EVENTS

Pen Test Austin
April 18-23 | Kevin Fiscus

Houston
May 9-14 | Bryce Galbraith

San Antonio
July 18-23 | BJ Gleason

Dallas
August 8-13 | Chris Crowley

giac.org

sans.edu

sans.org/cyber-guardian

MEETS DoDD 8140 (8570) REQUIREMENTS

sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

Who Should Attend

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

SANS SEC511

Continuous Monitoring and Security Operations

New Extended Bootcamp Hours to Enhance Your Skills

Six-Day Program
46 CPEs
Laptop Required

TRAINING EVENT

Houston
May 9-14 | Jonathan Ham

giac.org

sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

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)

"I run SOCs and this course provides a gut check against what we are doing today."
-Tim Housman, General Dynamics IT

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

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

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

SEC511 will take you on quite a journey. We start by exploring traditional security architecture to assess its current state and the attacks against it. Next, we discuss and discover modern security design that represents a new proactive approach to such architecture that can be easily understood and defended. We then transition to how to actually build the network and endpoint security, and then carefully navigate our way through automation, NSM/CDM/CSM. For timely detection of potential intrusions, the network and systems must be proactively and continuously monitored for any changes in the security posture that might increase the likelihood that attackers will succeed.

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

Active Defense, Offensive Countermeasures & Cyber Deception

SANS SEC550

Five-Day Program
9:00am - 5:00pm
30 CPEs
Laptop Required

TRAINING EVENT
San Antonio
July 18-22 | Bryce Galbraith

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

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

You Will 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

Author Statement

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

"SEC550 is the next step in the evolution of cyber defense, learning to make the hackers' job harder, track their movement, and get attribution."
-Mick Leach, Nationwide

"It's hard to imagine a better instructor than Bryce. He is obviously very skilled and experienced – his teaching skill and personality is a perfect fit."
-Patrick Gustafson, Allianz Life Insurance

Who Should Attend

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

SANS
SEC560

NEW!

Network Penetration Testing and Ethical Hacking

Six-Day Program
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required

TRAINING EVENTS

Pen Test Austin
April 18-23 | Ed Skoudis

Houston
May 9-14 | Adrien de Beaupre

Dallas
August 8-13 | Kevin Fiscus

giac.org

sans.edu

sans.org/cyber-guardian

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

Who Should Attend

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

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

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

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

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

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

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

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

"I learned more in one class then in years of self study!"
-Bradley Milhorn, Compucom Inc.

Advanced Web App Penetration Testing and Ethical Hacking

SANS SEC642

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENT

Pen Test Austin
April 18-23 | Adrien de Beaupre

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

"SEC642 is the perfect course for someone who has a background in web app pen testing, but wants to really gain advanced skills."
-Matthew Sullivan, Webfilings

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

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

"I like this training because it is very hands on and not just focused on slides. Very helpful for the real world."
-Zach Moreno, Chico Security

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

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

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

"Best web app class ever!"
-John Cartrett, Torchmark Corporations

"This has been the best SANS course that I have had the privilege to participate in!"
-Tom Moore, Lowe's Companies, Inc.

Who Should Attend

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

SANS SEC660

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Six-Day Program
46 CPEs
Laptop Required

TRAINING EVENT

Pen Test Austin
April 18-23 | Stephen Sims

giac.org

sans.edu

sans.org/cyber-guardian

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

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

Who Should Attend

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

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

Attackers are becoming more clever and their attacks more complex. In order to keep up with the latest attack methods, you need a strong desire to learn, the support of others, and the opportunity to practice and build experience. SEC660 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.

Windows Forensic Analysis

SANS FOR408

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENT
Houston
May 9-14 | David Cowen

giac.org

sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

DFIR
digital-forensics.sans.org

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

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

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

"I have been doing forensic investigations for several years, but would highly recommend this course (FOR408) for both new and old forensic investigations." -Robert Galarza, JP Morgan Chase

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

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

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

SANS FOR572

Advanced Network Forensics and Analysis

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENT
Dallas
August 8-13 | Philip Hagen

giac.org

sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

digital-forensics.sans.org

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

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

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

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

The hands-on exercises in this class cover a wide range of tools, including the venerable tcpdump and Wireshark for packet capture and analysis; commercial tools from Splunk, NetworkMiner, and SolarWinds; and open-source tools including nfdump, 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.

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

Cyber Threat Intelligence

SANS FOR578

NEW!

Five-Day Program
30 CPEs
Laptop Required

TRAINING EVENT

San Antonio
July 18-22 | Robert M. Lee

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

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

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

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

"I absolutely loved this class! [A] great framework for CTI that I will use to be more effective."
-Nate DeWitt, eBay, Inc.

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

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

DFIR
digital-forensics.sans.org

THERE IS NO TEACHER BUT THE ENEMY!

"This is exactly what I need for my job."
-Daniel, BKAmt

Who Should Attend

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

SANS FOR610

Reverse-Engineering Malware: Malware Analysis Tools & Techniques

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENT

Dallas
August 8-13 | Anuj Soni

giac.org

sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

digital-forensics.sans.org

Who Should Attend

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

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

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

"For those considering the cybersecurity field, this is a must."
-David First, Chevron

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

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

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

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

SANS Security Leadership Essentials for Managers with Knowledge Compression™

SANS MGT512

Five-Day Program
33 CPEs
Laptop NOT Needed

TRAINING EVENT

San Antonio
July 18-22 | G. Mark Hardy

giac.org

sans.edu

MEETS DoDD 8140 (8570) REQUIREMENTS

sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

This completely updated course is designed to empower advancing managers who want to get up to speed quickly on information security issues and terminology. You won't just learn about security, you will learn how to *manage* security. Lecture sections are intense; the most common student comment is that it's like drinking from a fire hose. The diligent manager will learn vital, up-to-date information 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 has great info for newly assigned managers to cybersecurity."
-Kerry T., U.S. Army Corps of Engineers

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

Knowledge Compression™

Maximize your learning potential!

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

"MGT512 is one of the most valuable courses I've taken with SANS. It really did help bridge the gap from security practitioner to security orchestrator. Truly a gift!" -John Madick, Epiq Systems, Inc.

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

SANS MGT525

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

Six-Day Program
36 CPEs
Laptop NOT Needed

TRAINING EVENT

Houston
May 9-14 | Jeff Frisk

giac.org

sans.edu

Who Should Attend

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

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

"Taking this course is the best way to prepare top project managers for the real world and certification!"
-Rob Ashworth, Barling Bay

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

"Honestly, this is one of the best courses I have had to date. I feel like I have thousands of things to take back to my job."
-Ryan Spencer, Reed Elsevier Inc.

Law of Data Security and Investigations

SANS LEG523

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

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

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

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

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.

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.

Five-Day Program
30 CPEs
Laptop NOT Needed

TRAINING EVENT
Houston
May 9-13 | Benjamin Wright

giac.org

sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

Who Should Attend

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

SANS AUD507

Auditing & Monitoring Networks, Perimeters, and Systems

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENT

Dallas
August 8-13 | David Hoelzer

giac.org

sans.edu

MEETS DoDD 8140
(8570) REQUIREMENTS

sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

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

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

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

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

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

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

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

SANS HOSTED

Physical Security Specialist – Facilities Edition

NEW!

Five-Day Program
30 CPEs
Laptop Required

TRAINING EVENT

Pen Test Austin
April 18-22 | The CORE Group

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

The CORE Group is a firm with divisions that focus on penetration testing, physical defense, personal protection details, and law enforcement training. Those who attend this course will leave with a full awareness of how to best protect buildings and grounds from unauthorized access, as well as how to compromise most existing physical security in order to gain access themselves. Our subject-matter experts will immerse you in all the necessary components of a well-layered physical defense system and then teach you how to conduct a thorough site analysis of a facility.

This training is ideal for any individual who is tasked with making physical security decisions for existing or new facilities.

During days one and two of this course, 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 in order to assess their own company's security posture or to augment their career as a penetration tester.

On days three and four, students will learn to evaluate physical barriers, defensive lighting, doors, external and internal physical intrusion detection systems, camera placement, access controls, and standard operating procedures. They will also be exposed to best practice standards and a robust variety of adversarial methodologies used to compromise weak targets such as social engineering and the exploitation of a weak employee culture. Numerous in-depth case studies and practical hands-on demonstrations will be utilized to solidify the acquisition of knowledge.

The training concludes on day five with an intense specialization focus: safe-cracking. Students will all be issued a mounted safe dial and will learn the fundamentals of safe manipulation and attack. While many commercially-available safes offer high security, the majority of document safe and gun safes in the field at present do not. Most individuals can learn how to open a conventional safe dial with one day of instruction. Today is that day.

By the end of this course, students will be very prepared to make educated and fiscally-responsible security decisions not only for their respective organizations but also for themselves. Participants will be able to approach any target, site-unseen, and then either conduct a walk-through assessment highlighting attack vectors, or proceed directly with an attack, gaining physical access to critical areas and infrastructure. Additionally, these newly-minted professionals in our training will also be able to provide sound documentation while making recommendations to management or to their insurance providers...saving money for their companies.

Hosted by The CORE Group

The CORE Group provides specialized consulting that focuses on physical security solutions. It provides training, blended penetration testing, and innovative tools for clients who seek security on all surfaces. The senior team's combined experience in the physical security sector represents decades of hard knowledge and applied work.

The CORE Group finds innovative ways to augment typical security auditing, assessment, and training by approaching topics that others often fail to consider: mechanical locks, electronic locks, safes, alarm systems, elevator systems, and much more.

Twitter: @TCGsec

SANS@NIGHT EVENING TALKS

Enrich your SANS training experience!

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

Pen Test Austin

A Night of Hands-on Pen Testing of "Internet of Things" Devices – Stephen Sims

sans.org/event/pentest2016/bonus-sessions

Houston

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

Automating Correlation with DFIR, Python, and ElasticSearch – David Cowen

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

Complete Web Application Pwnage via Multi-POST XSRF – Adrien de Beaupre

Instant Expert: Legitimately and Ethically – Ted Demopoulos

sans.org/event/houston-2016/bonus-sessions

San Antonio

KEYNOTE: ***Lessons Learned from the Attack on the Ukrainian Power Grid*** – Robert M. Lee

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

How to Commit Card Fraud – G. Mark Hardy

The 14 Absolute Truths of Security – Keith Palmgren

Debunking the Complex Password Myth – Keith Palmgren

The Red Pill. Become Aware: Squashing Security Misconceptions and More – My-Ngoc Nguyen

Advanced Persistent Threats and You: What You Need to Know – BJ Gleason

sans.org/event/san-antonio-2016/bonus-sessions

Dallas

Evolving Threats – Paul A. Henry

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

Need for Speed: Malware Edition – Anuj Soni

The Tap House – Philip Hagen

SANS 8 Mobile Device Security Steps – Christopher Crowley

sans.org/event/dallas-2016/bonus-sessions

Build Your Best Career

WITH

SANS

Add an

OnDemand Bundle & GIAC Certification Attempt*

to your course within seven days of these events for just $659 each.

SPECIAL PRICING

OnDemand Bundle

- Four months of supplemental online review
- 24/7 online access to your course lectures, materials, quizzes, and labs
- Subject-matter expert support to help you increase your retention of course material

"The course content and OnDemand delivery method have both exceeded my expectations."

-Robert Jones, Team Jones, Inc.

GIAC Certification

- Distinguish yourself as an information security leader
- 30+ GIAC certifications to choose from
- Two practice exams included
- Four months of access to complete the attempt

"GIAC is the only certification that proves you have hands-on technical skills."

-Christina Ford, Department of Commerce

MORE INFORMATION

sans.org/ondemand/bundles giac.org

*OnDemand Bundles and GIAC Certifications only available for certain courses.

SANS VOUCHER PROGRAM

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

Training Investment & Bonus Funds

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

The investment and bonus funds:

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

Flexibility & Control

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

With the SANS Admin tool, the Administrator can:

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

By creating a SANS Account, your organization can:

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

Getting Started

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

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

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

CONTACT

vouchers@sans.org | www.sans.org/vouchers

HOTEL INFORMATION

PEN TEST AUSTIN 2016

Omni Austin Hotel Downtown

700 San Jacinto At 8th Street
Austin, TX 78701
512-476-3700
sans.org/event/pentest2016/location

Special Hotel Rates Available*

A special discounted rate of $213.00 S/D.

Government per diem rooms may be available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through 5:00 pm CST March 25, 2016.

HOUSTON 2016

Royal Sonesta Hotel Houston

2222 West Loop South
Houston, TX 77027
713-627-7600
sans.org/event/houston-2016/location

Special Hotel Rates Available*

A special discounted rate of $189.00 S/D.

Government per diem rooms may be available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through 5:00 pm CST April 18, 2016.

SAN ANTONIO 2016

Hilton Palacio del Rio

200 South Alamo Street
San Antonio, TX 78205
210-222-1400
sans.org/event/san-antonio-2016/location

Special Hotel Rates Available*

A special discounted rate of $169.00 S/D.

Government per diem rooms may be available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through 5:00 pm CST July 5, 2016.

DALLAS 2016

The Westin Dallas Downtown

1201 Main Street
Dallas, Texas 75202
972-584-6650
sans.org/event/dallas-2016/location

Special Hotel Rates Available*

A special discounted rate of $179.00 S/D.

Government per diem rooms may be available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through 5:00 pm CST July 14, 2016.

**Price will be honored based on space availability*

REGISTRATION INFORMATION

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

Register online at:

PEN TEST AUSTIN: sans.org/event/pentest2016/courses
HOUSTON: sans.org/event/houston-2016/courses
SAN ANTONIO: sans.org/event/san-antonio-2016/courses
DALLAS: sans.org/event/dallas-2016/courses

Select your course or courses and indicate whether you plan to test for GIAC certification.
If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with Internet access must complete the online registration form. We do not take registrations by phone.

Use code **EarlyBird16** when registering early

Pay Early and Save

Pay and enter code by the dates listed to the right for special discounts

EVENT	DATE	DISCOUNT	DATE	DISCOUNT
Pen Test Austin	2-24-16	$400.00	3-16-16	$200.00
Houston	3-16-16	$400.00	4-6-16	$200.00
San Antonio	5-25-16	$400.00	6-15-16	$200.00
Dallas	6-15-16	$400.00	7-13-16	$200.00

Group Savings (Applies to tuition only)

10% discount if 10 or more people from the same organization register at the same time
5% discount if 5-9 people from the same organization register at the same time

To obtain a group discount, complete the discount code request form at sans.org/security-training/discounts prior to registering.

Cancellation

You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by respective dates (see website for dates) – processing fees may apply.