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

SANS Houston, TX

June 5-10, 2017

PROTECT YOUR COMPANY AND ADVANCE YOUR CAREER
WITH HANDS-ON, IMMERSION-STYLE

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

Eight courses in:

- CYBER DEFENSE
- DETECTION & MONITORING
- PENETRATION TESTING
- INCIDENT RESPONSE
- ETHICAL HACKING
- MANAGEMENT

GIAC CERTIFICATIONS
GIAC-Approved Training

"SANS courses provide training that helps you sharpen your skill set or obtain a new set of skills that you can apply right away."

-Todd Russell, Magellan LP

SAVE $400

Register and pay by April 12th – Use code **EarlyBird17**

www.sans.org/houston

SANS Instructors

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 SANS Houston 2017 lineup of instructors includes:

Ted Demopoulos
Principal Instructor
@TedDemop

Kevin Fiscus
Certified Instructor
@kevinbfiscus

Jonathan Ham
Certified Instructor
@jhamcorp

Ronald Hamann
Instructor
@airforceteacher

Paul A. Henry
Senior Instructor
@phenrycissp

Moses Hernandez
Instructor
@mosesrenegade

David R. Miller
Certified Instructor
@DRM_CyberDude

Bryan Simon
Certified Instructor
@BryanOnSecurity

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 9.

KEYNOTE: ***Look Before You Leap – Oops! Too Late***
David R. Miller

Infosec Rock Star: Geek Will Only Get You So Far
Ted Demopoulos

Shell Is Only the Beginning: Understanding Metasploit Post-Exploitation Modules
Kevin Fiscus

Save $400 when you register and pay by April 12th using code EarlyBird17

Courses at a Glance

	MON 6-5	TUE 6-6	WED 6-7	THU 6-8	FRI 6-9	SAT 6-10
SEC401 Security Essentials Bootcamp Style	Page 1					
SEC501 Advanced Security Essentials – Enterprise Defender	Page 2					
SEC503 Intrusion Detection In-Depth	Page 3					
SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	Page 4					
SEC542 Web App Penetration Testing and Ethical Hacking	Page 5					
SEC560 Network Penetration Testing and Ethical Hacking	Page 6					
MGT414 SANS Training Program for CISSP® Certification	Page 7					
MGT514 IT Security Strategic Planning, Policy, and Leadership	Page 8					

SEC401:
Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, June 5 - Sat, June 10
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Bryan Simon

www.giac.org/gsec

www.sans.edu


www.sans.org/8140

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

"Between knowledge of the instructor and the application of course material, everything was run to perfection!"
-Joe Lordi, Wawa, Inc.

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

Learn to build a security roadmap that can scale today and into the future!

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. This course will show you how to prevent your organization's security problems from being headline news in the *Wall Street Journal*!

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

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

Security is all about making sure you focus on the right areas of defense. In SEC401 you will learn the language and underlying theory of computer and information security. You will gain the essential and effective security knowledge you'll 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.

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

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 analysts, penetration testers, and auditors who need a solid foundation of security principles so they can be as effective as possible at their jobs
- Anyone new to information security with some background in information systems and networking

Bryan Simon *SANS Certified Instructor*

Bryan Simon is an internationally recognized expert in cybersecurity and has been working in the information technology and security field since 1991. Over the course of his career, Bryan has held various technical and managerial positions in the education, environmental, accounting, and financial services sectors. Bryan speaks on a regular basis at international conferences and with the press on matters of cybersecurity. He has instructed individuals from organizations such as the FBI, NATO, and the UN in matters of cybersecurity, on two continents. Bryan has specialized expertise in defensive and offensive capabilities. He has received recognition for his work in IT security, and was most recently profiled by McAfee (part of Intel Security) as an IT Hero. Bryan holds 12 GIAC certifications including the GSEC, GCWN, GCIH, GCFA, GPEN, GWAPT, GAWN, GISP, GCIA, GCED, GCUX, and GISF. Bryan's scholastic achievements have resulted in the honor of sitting as a current member of the Advisory Board for the SANS Institute, and his acceptance into the prestigious SANS Cyber Guardian program. Bryan is a SANS instructor for SEC401, SEC501, SEC505, and SEC511. @BryanOnSecurity

SEC501:

Advanced Security Essentials – Enterprise Defender

SANS

Six-Day Program
Mon, June 5 - Sat, June 10
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor: Paul A. Henry

www.giac.org/gced

www.sans.edu

www.sans.org/8140

Bundle OnDemand
with this course
www.sans.org/ondemand

"This has been one of the best courses I have taken! It was highly job relevant, and incorporated ground-breaking material."
-Jonathan C., CDSA Dam Neck

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.

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

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

"We aren't just learning how to use the tools, we also have real-world examples to avoid possible pitfalls. There is cloud-based analysis that is so useful, but I would never have thought of using it had Paul not covered it."
-Stuart Long, Bank of England

Of course, 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 prevention and detection measures, completing the security lifecycle.

Paul A. Henry *SANS Senior Instructor*

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

SEC503:
Intrusion Detection In-Depth

SANS

Six-Day Program
Mon, June 5 - Sat, June 10
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jonathan Ham

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

Who Should Attend

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

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

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.

"This course was very valuable for me because I had the opportunity to understand in-depth what bad guys do and how. I really enjoy the course and the challenge was very amazing!" -Daniele L., Accenture

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.

www.giac.org/gcia

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

Bundle OnDemand
with this course
www.sans.org/ondemand

"This course allows analysts to not only understand what to look for in packets, but why they are doing so."
-Katie Kelley, Great River Energy

Jonathan Ham *SANS Certified Instructor*

Jonathan is an independent consultant who specializes in large-scale enterprise security issues, from policy and procedure, through staffing and training, to scalable prevention, detection, and response technology and techniques. With a keen understanding of ROI and TCO (and an emphasis on process over products), he has helped his clients achieve greater success for over 20 years, advising in both the public and private sectors, from small upstarts to the Fortune 500. He's been commissioned to teach NCIS investigators how to use Snort, performed packet analysis from a facility more than 2000 feet underground, and chartered and trained the CIRT for one of the largest U.S. civilian federal agencies. He has held the CISSP, GSEC, GCIA, and GCIH certifications, and is a member of the GIAC Advisory Board. A former combat medic, Jonathan still spends some of his time practicing a different kind of emergency response, volunteering and teaching for both the National Ski Patrol and the American Red Cross. @jhamcorp

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Mon, June 5 - Sat, June 10
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Ronald Hamann

www.giac.org/gcih

SANS Technology Institute
www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

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

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

Who Should Attend

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

"If you love cybersecurity and learning how exploits work, you NEED this course!" -JAID, U.S. NAVY

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

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

"In cybersecurity it can often feel like you don't know what you are protecting the infrastructure from. This course paints the picture of specific types of attacks in a manner that is useful to cybersecurity professionals." -AKYL P., U.S. MARINES

Ronald Hamann *SANS Instructor*

Ron is a retired U.S. Air Force officer and enlisted person with over 20 years of experience in information technology and information assurance, from software development and system administration to security analysis and security operations. Ron is currently a senior security analyst for Rackspace Managed Security in San Antonio, working in their customer Security Operations Center hunting for attacker activity and responding to attacks daily. Ron has been a security instructor since 2010, sharing his experiences at multiple security operations centers, both military and commercial, and various consulting clients including NASA, oil and gas, and construction industry companies. Ron teaches the three core classes for the GSE and the STI Masters program: SEC401, SEC503 and SEC504. When not thinking about attackers and defenses, Ron spends his time looking for yet another craft cider he hasn't tried and apologizing to his dance partners. @airforceteacher

SEC542:
Web App Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Mon, June 5 - Sat, June 10
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Moses Hernandez

www.giac.org/gwapt

www.sans.edu

www.sans.org/cyber-guardian

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

"The SEC542 tools and course presentation are top-notch. I will be using this material extensively."
-Jeremy Pierson, Academy Mortgage

Web applications play a vital role in every modern organization. But if your organization does not 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.

Who Should Attend

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

"This course has been well worth it! I can't wait to take the advanced pen testing course." -Ben Johnson, Time Inc.

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.

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 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.**

Moses Hernandez *SANS Instructor*

Moses Hernandez is a seasoned security professional with over 15 years in the IT industry. He has held positions as a network engineer, network architect, security architect, platform engineer, site reliability engineer, and consulting sales engineer. He has a background in complex network systems, systems administration, forensics, penetration testing, and development. He has worked with some of the largest companies in the nation as well as fast-growing, bootstrap startups. Moses has developed information security regimens safeguarding some of the most sensitive personal data in the nation. He creates custom security software to find and mitigate unknown threats, and works on continually evolving his penetration testing skills. He enjoys building software, networks, systems, and working with business-minded individuals. Moses's current passions include offensive forensics, building secure systems, finance, economics, history, and music. @mosesrenegade

SEC560:

Network Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Mon, June 5 - Sat, June 10
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Kevin Fiscus

www.giac.org/gpen

www.sans.edu

www.sans.org/cyber-guardian

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

"Learning how attackers profile and exploit allows me to understand how to tailor our product offerings to provide real value."
-Travis Smith, Tripwire

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.

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.

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

Who Should Attend

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

Kevin Fiscus *SANS Certified Instructor*

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

MGT414:

SANS Training Program for CISSP® Certification

SANS

Six-Day Program
Mon, June 5 - Sat, June 10
9:00am - 7:00pm (Day 1)
8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6)
46 CPEs
Laptop NOT Needed
Instructor: David R. Miller

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

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

Who Should Attend

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

You Will Be Able To:

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

Note:
The CISSP® exam itself is not hosted by SANS. You will need to make separate arrangements to take the CISSP® exam. Please note as well that the GISP exam offered by GIAC is NOT the same as the CISSP® exam offered by (ISC)^2.

Obtaining Your CISSP® Certification Consists of:

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

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

www.giac.org/gisp

www.sans.org/8140

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

"The instructor was excellent and truly an expert! I'm getting depth in my understanding and David explained some topics better than several books I've read."
-Freda Lurdy, Raytheon

David R. Miller *SANS Certified Instructor*

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

MGT514:

IT Security Strategic Planning, Policy, and Leadership

SANS

Five-Day Program
Mon, June 5 - Fri, June 9
9:00am - 5:00pm
30 CPEs
Laptop NOT Needed
Instructor: Ted Demopoulos

GIAC
CERTIFICATION COMING SOON!

SANS Technology Institute
www.sans.edu

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

"Ted is a great instructor – very animated with relevant real-world stories."
-Errol H., Naval Sea Systems Command

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

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:

Who Should Attend

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

Develop Strategic Plans

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

Create Effective Information Security Policy

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

Develop Management and Leadership Skills

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

Ted Demopoulos *SANS Principal Instructor*

Ted Demopoulos' first significant exposure to computers was in 1977 when he had unlimited access to his high school's PDP-11 and hacked at it incessantly. He consequently almost flunked out but learned he liked playing with computers a lot. His business pursuits began in college and have been ongoing ever since. His background includes over 25 years of experience in information security and business, including 20+ years as an independent consultant. Ted helped start a successful information security company, was the CTO at a "textbook failure" of a software startup, and has advised several other businesses. Ted is a frequent speaker at conferences and other events, quoted often by the press. He also has written two books on social media, has an ongoing software concern in Austin, Texas in the virtualization space, and is the recipient of a Department of Defense Award of Excellence. In his spare time, he is also a food and wine geek, enjoys flyfishing, and plays with his children. @TedDemop

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.

KEYNOTE:

Look Before You Leap – Oops! Too Late

David R. Miller

As a security and compliance consultant, I'm often told "We just completed our move into the cloud, and management is thrilled. Now, how do we make sure our stuff is secure?" We all know and appreciate the massive benefits that an enterprise can recoup by migrating its IT assets and services into the cloud. Indeed, you can reduce the huge capital expenditures and ongoing operational expenses of building and maintaining your own datacenter by simply paying small monthly leasing fees to cloud service providers. And they give you everything you ever wanted in performance, reliability, high availability, highly elastic capacity, and disaster recovery. Who can resist? And how can this be a bad decision? Let's take a closer look and explore some of the many items overlooked and unconsidered BEFORE placing your most valuable information assets in the hands of people who don't love you like your momma does, and they never will.

Infosec Rock Star: Geek Will Only Get You So Far

Ted Demopoulos

This presentation is based on the recently published book of the same title. Some of us are so effective, and well known, that the term "Rock Stars" is entirely accurate. What kind of skills do Rock Stars have and wannabe Rock Stars need to develop? Although we personally may never be swamped by groupies, we can learn the skills to be more effective, well respected, and well paid. Obviously it's not just about technology; in fact most of us are very good at the technology part. And although the myth of the Geek with zero social skills is just that, a myth, the fact is that increasing our skills more on the social and business side will make most of us more effective at what we do than learning how to read hex better while standing on our heads, becoming "One with Metasploit," or understanding the latest hot technologies.

Shell Is Only the Beginning: Understanding Metasploit Post-Exploitation Modules

Kevin Fiscus

Metasploit is a fantastic hacking tool. Having a huge range of exploits and a collection of different payloads that are easy to use makes compromising vulnerable systems almost trivial. Many a penetration tester have been given the opportunity to do their "happy dance" by compromising a system and getting shell on the target system. Getting shell however, is only the beginning of the penetration test. When taking martial arts it is common to hear that becoming a blackbelt is only the beginning of the training. Penetration testing is similar. The test really begins when you get shell. Once you have access to the compromised system, what do you do? This talk will discuss the often overlooked post-exploitation modules in Metasploit. These are the components in Metasploit that allow you to capture keystrokes, identify new targets, grab credentials, identify users, determine what applications are installed and even identify if you have compromised a physical or virtual host. During this talk we will describe and demonstrate many of these modules, adding to your arsenal of penetration testing techniques.

Enhance Your Training Experience

Add an

OnDemand Bundle & GIAC Certification Attempt*

to your course within seven days of this event for just $689 each.

SPECIAL PRICING

Extend Your Training Experience with an 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.

Get Certified with GIAC Certifications

- Distinguish yourself as an information security leader
- 30+ GIAC cybersecurity certifications available
- 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

www.sans.org/ondemand/bundles www.giac.org

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

Securing **Approval** and **Budget** for Training

Packaging matters

Write a formal request

- All organizations are different, but because training requires a significant investment of both time and money, most successful training requests are made via a written document (short memo and/or a few powerpoint slides) that justify the need and benefit. Most managers will respect and value the effort.
- Provide all the necessary information in one place. In addition to your request, provide all the right context by including the summary pages on Why SANS?, the Training Roadmap, the instructor bio, and additional benefits available at our live events or online.

Clearly state the benefits

Be specific

- How does the course relate to the job you need to be doing? Place the particular course you wish to take into the context on the SANS Career Roadmap. Are you establishing baseline skills? Transitioning to a more focused role? Decision-makers need to understand the plan and context for the decision.
- Highlight specifics of what you will be able to do afterwards. Each SANS course description includes a section titled "You Will Be Able To." Be sure to include this in your request so that you make the benefits clear. The clearer the match between the training and what you need to do at work, the better.

Set the context

Establish longer-term expectations

- Information security is a specialized career path within IT, with practices that evolve as attacks change. Because of this, organizations should expect to spend 6%-10% of salaries to keep professionals current and improve their skills. Training for such a dynamic field is an annual, per-person expense, and not a once-and-done item.
- Take a GIAC Certification exam to prove the training worked. Employers value the validation of learning that passing a GIAC exam offers. Exams are psychometrically designed to establish competency for related job tasks.
- Consider offering trade-offs for the investment. Many professionals build annual training expense into their employment agreements even before joining a company. Some offer to stay for a year after they complete the training.

Future Training Events

Tysons Corner Spring . . . . . McLean, VA . . . . . March 20-25
Pen Test Austin . . . . . Austin, TX . . . . . March 27 - April 1

Baltimore Spring . . . . . Baltimore, MD . . . . . April 24-29

Northern Virginia – Reston . . . . Reston, VA . . . . . May 21-26
Atlanta . . . . . Atlanta, GA . . . . . May 30 - June 4
Houston . . . . . Houston, TX . . . . . June 5-10
San Francisco Summer . . . . . San Francisco, CA . . . . . June 5-10
Rocky Mountain . . . . . Denver, CO . . . . . June 12-17
Charlotte . . . . . Charlotte, NC . . . . . June 12-17

Future Summit Events

ICS Security . . . . . Orlando, FL . . . . . March 19-27
Threat Hunting and IR . . . . . New Orleans, LA . . . . . April 18-25
Automotive Cybersecurity . . . . Detroit, MI . . . . . May 1-8
Security Operations Center . . . Washington, DC . . . . . June 5-12

SANS Training Options

LIVE CLASSROOM TRAINING

Multi-Course Training Events www.sans.org/security-training/by-location/all
Live Instruction from SANS' Top Faculty, Vendor Showcase, Bonus Evening Sessions, and Networking with Your Peers

Community SANS www.sans.org/community
Live Training in Your Local Region with Smaller Class Sizes

Private Training www.sans.org/private-training
Live Onsite Training at Your Office Location. Both In-person and Online Options Available

Mentor www.sans.org/mentor
Live Multi-Week Training with a Mentor

Summit www.sans.org/summit
Live IT Security Summits and Training

ONLINE TRAINING

OnDemand www.sans.org/ondemand
E-learning Available Anytime, Anywhere, at Your Own Pace

vLive www.sans.org/vlive
Online Evening Courses with SANS' Top Instructors

Simulcast www.sans.org/simulcast
Attend a SANS Training Event without Leaving Home

OnDemand Bundles www.sans.org/ondemand/bundles
Extend Your Training with an OnDemand Bundle Including Four Months of E-learning

SANS HOUSTON 2017

Hotel Information

Training Campus

Royal Sonesta Hotel Houston

2222 West Loop South
Houston, TX 77027
713-627-7600
www.sans.org/event/houston-2017/location

Located in the heart of the Galleria area, the newly renovated, AAA-rated Four Diamond Royal Sonesta Hotel Houston is in the shopping, dining and entertainment hub of Uptown Houston. It is conveniently positioned near key destinations including downtown Houston, the Museum and Theater districts, and Reliant Park.

Special Hotel Rates Available

A special discounted rate of $189.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID. These rates include high-speed Internet in your room and are only available through May 13, 2017. To book a room, please call 800-766-3782 and mention you are with SANS.

Top 5 reasons to stay at the Royal Sonesta Hotel Houston

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

SANS HOUSTON 2017

Registration Information

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

Register online at www.sans.org/houston

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

Use code **EarlyBird17** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**4-12-17**	**$400.00**	**5-3-17**	**$200.00**

Some restrictions apply.

SANS Voucher Program

Expand your training budget!

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

www.sans.org/vouchers

Cancellation

You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by May 17, 2017 – processing fees may apply.

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

WEBCASTS

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

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

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

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

NEWSLETTERS

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

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

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

OTHER FREE RESOURCES

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

www.sans.org/account