THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS Boston 2013

August 5-10, 2013

Hands-on immersion training programs, including:

Securing Windows and Resisting Malware *NEW!*

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

Network Penetration Testing and Ethical Hacking

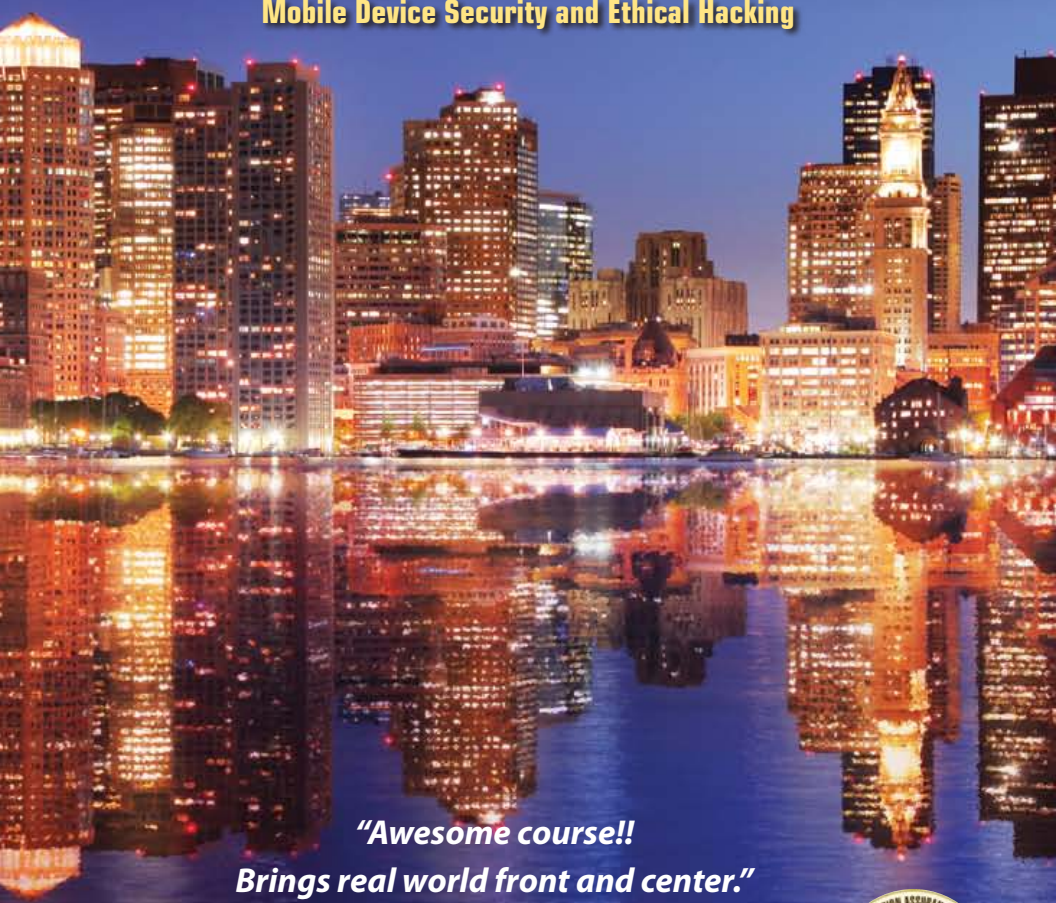
Security Leadership Essentials For Managers with Knowledge Compression™

SANS +S Training Program for the CISSP® Certification Exam

Advanced Computer Forensic Analysis and Incident Response

Virtualization and Private Cloud Security

Mobile Device Security and Ethical Hacking



"Awesome course!!
Brings real world front and center."

-Brian Howard, Grand River Dam Authority

Register at
www.sans.org/event/boston-2013

GIAC Approved Training

Dear Colleague,

Please join us in Boston this summer for one of SANS' best line-ups in cutting-edge cybersecurity training! Don't miss the chance to gain in-depth knowledge that you will use the minute you get back to your office. We will be offering our new Security 505: Securing Windows and Resisting Malware taught by James Tarala along with eight more 5- and 6-day courses in security management, IT security, and computer forensics. Come to Boston this August 5-10 to learn from SANS and soak in the great historic culture of this fascinating city.

SANS Boston 2013 offers top-rated courses brought to you by Dr. Eric Cole, Stephen Northcutt, Rob Lee, Paul A. Henry, Dave Shackleford, James Tarala, Seth Misenar, Christopher Crowley, and Tim Medin. See the course descriptions and the instructor bios inside. Seven courses are associated with the prestigious GIAC Certification. To turbo-charge your career, check which courses can help you earn your Master's Degree at the SANS Technology Institute (STI). Find out about GIAC and STI in this brochure.

Join us at the Hilton Boston Back Bay campus, which is just five blocks from the Boston Common. Take a walk to experience historic downtown Boston with its shopping, theaters, and Chinatown. For a wealth of information about Boston and things to do there, check out our Insider's Guide to Boston at http://www.sans.edu/research/security-musings/group/insider-guide-boston

Add depth to your training experience with unique evening events, including:

- **Welcome to SANS with Dr. Eric Cole; a great intro for SANS first-timers!**
- **Keynote: "APT: It is Time to Act" with Dr. Eric Cole**
- **GIAC Program Overview**
- **SANS Technology Institute Open House**
- **"Practical, Efficient Unix Auditing (with Scripts)" with James Tarala**
- **Vendor Showcase events – August 6**

Register and pay by June 19 and save up to $500! Start making your training and travel plans now; let your colleagues and friends know about SANS Boston 2013. We look forward to seeing you there.

Best regards,

Stephen Northcutt
The SANS Technology Institute, a postgraduate computer security college

Stephen Northcutt

Here's what past Boston attendees had to say:

"Stephen is a very engaging instructor and the content is relevant to today's security challenges."
-Joy Randels, Applied G2

"SANS courses are the best there is, this one is no exception."
-Scott Hilts, Bruce Power

"Sec401 is an extremely valuable training tool to establish a baseline for common core security knowledge. SANS maintains its standards of excellence by attracting top-notch instructors. You will not have a poor learning experience, period."
-John Lindsay, Department of National Defense

Courses-at-a-Glance

SECURITY 401

Security Essentials Bootcamp Style

Six-Day Program • Mon, Aug 5 - Sat, Aug 10
9:00am - 7:00pm (Days 1-5) • 9:00am - 5:00pm (Day 6)
46 CPE/CMU Credits • Laptop Required
Instructor: Dr. Eric Cole

It seems wherever you turn organizations are being broken into and the fundamental question that everyone wants answered is: Why? Why do some organizations get broken into and others not? SEC401 Security Essentials is focused on teaching you the right things that need to be done to keep an organization secure. Organizations are spending millions of dollars on security and are still compromised. The problem is they are doing good things but not the right things. Good things will lay a solid foundation but the right things will stop your organization from being headline news in the *Wall Street Journal*. SEC401's focus is to teach individuals the essential skills and techniques needed to protect and secure an organization's critical information assets and business systems. We also understand that security is a journey and not a destination. Therefore we will teach you how to build a security roadmap that can scale today and into the future. When you leave our training we promise that you will be given techniques that you can implement today and tomorrow to keep your organization at the cutting edge of cyber security. Most importantly, your organization will be secure.

With the APT (advanced persistent threat), organizations are going to be targeted. Whether the attacker is successful penetrating an organization's network depends on the organization's defense. While 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 works in cyber security. 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 on anything in the name of cyber security, three questions must be answered:

1. **What is the risk?**
2. **Is it the highest priority risk?**
3. **Is it the most cost-effective way of reducing the risk?**

Security is all about making sure you are focusing on the right areas of defense. By attending SEC401 you will learn the language and underlying theory of computer security. Since all jobs today require an understanding of security, this course will help you understand why security is important and how it applies to your job. In addition, you will gain the essential, up-to-the-minute knowledge and skills required for effective security 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 gain cutting-edge knowledge you can put into practice immediately upon returning to work; and, (2) You will be taught by the best security instructors in the industry.

Who Should Attend:

- **Security professionals who want to fill the gaps in their understanding of technical information security**
- **Managers who want to understand information security beyond simple terminology and concepts**
- **Operations personnel who do not have security as their primary job function but need an understanding of security to be effective**
- **IT engineers and supervisors who need to know how to build a defensible network against attacks**
- **Administrators responsible for building and maintaining systems that are being targeted by attackers**
- **Forensic, penetration testers, auditors who need a solid foundational of security principles so they can be effective as possible at their jobs**
- **Anyone new to information security with some background in information systems and networking**

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/boston-2013.

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

Dr. Eric Cole *SANS Faculty Fellow*

Dr. Cole is an industry-recognized security expert with over 20 years of hands-on experience. Dr. Cole has experience in information technology with a focus on helping customers focus on the right areas of security by building out a dynamic defense. Dr. Cole has a master's degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. He served as CTO of McAfee and Chief Scientist for Lockheed Martin. Dr. Cole is the author of several books, including ***Advanced Persistent Threat***, ***Hackers Beware***, ***Hiding in Plain Site***, ***Network Security Bible*** 2nd Edition, and ***Insider Threat***. He is the inventor of over 20 patents and is a researcher, writer, and speaker. He is also a member of the Commission on Cyber Security for the 44th President and several executive advisory boards. Dr. Cole is the founder and an executive leader at Secure Anchor Consulting where he provides leading-edge cyber security consulting services, expert witness work, and leads research and development initiatives to advance the state-of-the-art in information systems security. Dr. Cole is actively involved with the SANS Technology Institute (STI) and is a SANS faculty fellow and course author who works with students, teaches, and develops and maintains courseware.

SECURITY 504

Hacker Techniques, Exploits, and Incident Handling

Six-Day Program • Mon, Aug 5 - Sat, Aug 10
9:00am - 6:30pm (Day 1) • 9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits • Laptop Required
Instructor: Dave Shackleford

If your organization has an Internet connection or one or two disgruntled employees (and whose doesn't!), 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.

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, the in-depth information in this course helps you turn the tables on computer attackers. This course addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still so prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course includes a time-tested, step-by-step process for responding to computer incidents; a detailed description of how attackers undermine systems so you can prepare, detect, and respond to them; and a hands-on workshop for discovering holes before the bad guys do. Additionally, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence.

This challenging course is particularly well-suited to individuals who lead or are a part of an incident handling team. Furthermore, 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.

"When I get back to the office, I will use the knowledge I gained here to better defend my organization's network."
-Joshua Anthony, West Virginia Army National Guard

Who Should Attend:

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

SANS SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast. *More info on page 11.*

"The course covers almost every corner of attack and defense areas. It's a very helpful handbook for a network security analysis job. It upgrades my knowledge in IT security and keeps pace with the trend."
-Anthony Liu, Scotia Bank

Dave Shackleford *SANS Senior Instructor*

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

"Fantastic class! Fantastic Instructor! I have taken six SANS classes, I have not had a bad experience yet, they are just so professionally done!"
-Rafael Cabrera, Air Force

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/boston-2013.

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

SECURITY 505

Securing Windows and Resisting Malware

Six-Day Program • Mon, Aug 5 - Sat, Aug 10
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: James Tarala

New Course!

In April of 2014, Microsoft will stop releasing any new security patches for Windows XP. Like it or not, migrating off Windows XP is no longer optional, the clock is counting down. The Securing Windows and Resisting Malware course is fully updated for Windows Server 2012, Windows 8, Server 2008-R2, and Windows 7.

This course is about the most important things to do to secure Windows and how to minimize the impact on users of these changes. You'll see the instructor demo the important steps live, and you can follow along on your laptop. The manuals are filled with screenshots and step-by-step exercises, so you can do the steps alongside the instructor in seminar or later on your own time if you prefer.

We've all got anti-virus scanners, but what else needs to be done to combat malware and intruders using Advanced Persistent Threat (APT) techniques? Today's weapon of choice for hackers is stealthy malware with remote control channels, preferably with autonomous worm capabilities, installed through client-side exploits. While other courses focus on detection or remediation, the goal of this course is to prevent the infection in the first place (after all, first things first).

Especially in Server 2012 and beyond, PowerShell dominates Windows scripting and automation. It seems everything can be managed through PowerShell now. And if there's a needed skill that will most benefit the career of a Windows specialist, it's being able to write PowerShell scripts, because most of your competition will lack scripting skills, so it's a great way to make your resume stand out. This course devotes an entire day to PowerShell scripting, but you don't need any prior scripting experience.

This course will also prepare you for the GIAC Certified Windows Security Administrator (GCWN) certification exam to help prove your security skills and Windows expertise.

Who Should Attend:

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

SANS SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast. *More info on page 11.*

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/boston-2013.

"You will know and be confident on how to enable Windows PK1 after taking this course. I had no practical experience, but plenty of theory. The instructor broke down the pros and cons of the whole process. Excellent!!"
-Othello Swanston, DTRA-DOD

James Tarala *SANS Senior Instructor*

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

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

SECURITY 560

Network Penetration Testing and Ethical Hacking

Six-Day Program • Mon, Aug 5 - Sat, Aug 10
9:00am - 6:30pm (Day 1) • 9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits • Laptop Required
Instructor: Tim Medin

As cyber attacks increase, so does the demand for information security professionals who possess true network penetration testing and ethical hacking skills. There are several ethical hacking courses that claim to teach these skills, but few actually do. SANS SEC560: Network Penetration Testing and Ethical Hacking truly prepares you to conduct successful penetration testing and ethical hacking projects. The course starts with proper planning, scoping and recon, and then dives deep into scanning, target exploitation, password attacks, and wireless and web apps with detailed hands-on exercises and practical tips for doing the job safely and effectively. You will finish up with an intensive, hands-on Capture the Flag exercise in which you'll conduct a penetration test against a sample target organization, demonstrating the knowledge you mastered in this course.

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

-Mark Hamilton, McAfee

Equipping Security Organizations with Advanced Penetration Testing and Ethical Hacking Know-How

Security vulnerabilities, such as weak configurations, unpatched systems, and botched architectures, continue to plague organizations. Enterprises need people who can find these flaws in a professional manner to help eradicate them from our infrastructures. Lots of people claim to have penetration testing, ethical hacking, and security assessment skills, but precious few can apply these skills in a methodical regimen of professional testing to help make an organization more secure. This class covers the ingredients for successful network penetration testing to help attendees improve their enterprise's security stance.

Who Should Attend:

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

We address detailed pre-test planning, including setting up an effective penetration testing infrastructure and establishing ground rules with the target organization to avoid surprises and misunderstanding. Then, we discuss a time-tested methodology for penetration and ethical hacking across the network, evaluating the security of network services and the operating systems behind them.

"The skills taught and demonstrated in this class are perfect for new pen testers and veterans alike." -Roy Luongo, Dept of Defense

Attendees will learn how to perform detailed reconnaissance, learning about a target's infrastructure by mining blogs, search engines, and social networking sites. We'll then turn our attention to scanning, experimenting with numerous tools in hands-on exercises. Our exploitation phase will include the use of exploitation frameworks, stand-alone exploits, and other valuable tactics, all with hands-on exercises in our lab environment. The class also discusses how to prepare a final report, tailored to maximize the value of the test from both a management and technical perspective. The final portion of the class includes a comprehensive hands-on exercise, conducting a penetration test against a hypothetical target organization, following all of the steps.

The course also describes the limitations of penetration testing techniques and other practices that can be used to augment penetration testing to find vulnerabilities in architecture, policies, and processes. We also address how penetration testing should be integrated as a piece of a comprehensive enterprise information security program.

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/boston-2013.

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

Tim Medin *SANS Instructor*

Tim Medin currently works at Counter Hack Challenges, a company devoted to the development of information security challenges for education, evaluation, and competition. Prior to Counter Hack Challenges, Tim was a Senior Security Consultant for FishNet Security where the majority of his focus was on penetration testing. He gained information security experience in a variety of industries including previous positions in control systems, higher education, financial services, and manufacturing. He currently holds a number of GIAC certifications including GPEN, GCIH, GWEPT, and GCED. Tim regularly contributes to the Command Line Kung Fu Blog and is a project lead for the Laudanum Project, a collection of injectable scripts designed to be used in penetration testing.

SECURITY 575

Mobile Device Security and Ethical Hacking

Six-Day Program • Mon, Aug 5 - Sat, Aug 10
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Christopher Crowley

Mobile phones and tablets have become essential to enterprise and government networks, from small organizations to Fortune 500 companies and large-scale agencies. Often, mobile phone deployments grow organically, adopted by multitudes of end-users for convenient email access as well as managers and executives who need access to sensitive organizational resources from their favored personal mobile devices. In other cases, mobile phones and tablets have become critical systems for a wide variety of production applications from enterprise resource planning to project management. With increased reliance on these devices, organizations are quickly recognizing that mobile phones and tablets need greater security implementations than a simple screen protector and clever password.

"Wow! This course is everything you need to know about mobile device deployment, risks and more. Don't deploy your mobile devices without taking this course first."
-Bryan Simon, INTEGRIS Credit Union

The security risks of mobile phone and tablet device use in the workplace

Whether the device is an Apple iPhone or iPad, a Windows Phone, an Android or BlackBerry phone or tablet, the ubiquitous mobile device has become a hugely attractive and vulnerable target for nefarious attackers. The use of mobile devices introduces a vast array of new risks to organizations, including:

- **distributed sensitive data storage and access mechanisms**
- **lack of consistent patch management and firmware updates**
- **the high probability of device loss or theft, and more.**

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

Who Should Attend:

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

From mobile device security policy development, to design and deployment, and more

This course was designed to help organizations struggling with mobile device security by equipping personnel with the skills needed to design, deploy, operate, and assess a well-managed secure mobile environment. From practical policy development to network architecture design and deployment, and mobile code analysis to penetration testing and ethical hacking, this course will help you build the critical skills necessary to support the secure deployment and use of mobile phones and tablets in your organization.

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/boston-2013.

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

Christopher Crowley *SANS Certified Instructor*

Mr. Crowley has 10 years of industry experience managing and securing networks. He has GSEC, GCIA, GCIH (gold), GCFA, and CISSP certifications. His teaching experience includes GSEC, GCIA, and GCIH Mentor; Apache web server administration and configuration; and shell programming. He was awarded the SANS 2009 Local Mentor of the year award. "The Mentor of the Year Award is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities."

"Don't walk, run to this course if your life has anything to do with mobility. Don't go anywhere else, all other courses are pretenders, this is the best."
-Aamir Lakhani,
World Wide Technology

SECURITY 579

Virtualization and Private Cloud Security

Six-Day Program • Mon, Aug 5 - Sat, Aug 10
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop provided during class • Instructor: Paul A. Henry

Who Should Attend:

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

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

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/boston-2013.

Server virtualization vulnerabilities

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

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

The class starts out with two days of architecture and security design for both virtualization and private cloud infrastructure. The entire gamut of components will be covered ranging from hypervisor platforms to virtual networking, storage security to locking down the individual virtual machine files. The next two days we'll go into detail on offense and defense - how can we assess virtualized environment using scanning and pen testing tools and techniques, and how do things change when we move to a cloud model? During day 5, we will help you adapt your existing security policies and practices to the new virtualized or cloud-based infrastructure. On day 6, we'll cover the top virtualization configuration and hardening guides from DISA, CIS, Microsoft, and VMware, and talk about the most important and critical things to take away from these to implement.

"I plan to (eventually) send everyone in my Net Ops and Cyber Security shops to this course. It seems indispensable."
-Keil Hubert, 136th Comm. Flight

Paul A. Henry *SANS Senior Instructor*

Paul Henry is one of the world's foremost global information security and computer forensic experts with more than 20 years experience managing security initiatives for Global 2000 enterprises and government organizations worldwide. Paul is a principle 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. Paul 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 Department of Defense's Satellite Data Project (USA), and both government as well as telecommunications projects throughout Southeast Asia. Paul is frequently cited by major and trade print publications as an expert in computer forensics, technical security topics, and general security trends and serves as an expert commentator for network broadcast outlets, such as FOX, NBC, CNN, and CNBC. In addition, Paul regularly authors thought leadership articles on technical security issues, and his expertise and insight help shape the editorial direction of key security publications, such as the ***Information Security Management Handbook***, where he is a consistent contributor. Paul serves as a featured and keynote speaker at seminars and conferences worldwide, delivering presentations on diverse topics including anti-forensics, network access control, cyber crime, DDoS attack risk mitigation, firewall architectures, security architectures, and managed security services.

FORENSICS 508

Advanced Computer Forensic Analysis and Incident Response

Six-Day Program • Mon, Aug 5 - Sat, Aug 10
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Rob Lee

This course focuses on providing incident responders with the necessary skills to hunt down and counter a wide range of threats within enterprise networks, including economic espionage, hactivism, and financial crime syndicates. The completely updated FOR508 addresses today's incidents by providing real-life, hands-on response tactics. Don't miss the NEW FOR508!

DAY 0: A 3-letter government agency contacts you to say that critical information was stolen from a targeted attack on your organization. Don't ask how they know, but they tell you that there are several breached systems within your enterprise. You are compromised by an Advanced Persistent Threat, aka an APT – the most sophisticated threat you are likely to face in your efforts to defend your systems and data.

Who Should Attend:

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

Over 90% of all breach victims learn of a compromise from third party notification, not from internal security teams. In most cases, adversaries have been rummaging through your network undetected for months or even years. Gather your team—it's time to go hunting.

This course will help you determine:

- **How did the breach occur?**
- **What systems were compromised?**
- **What did they take? What did they change?**
- **How do we remediate the incident?**

SANS SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast. ***More info on page 11.***

The updated FOR508 trains digital forensic analysts and incident response teams to identify, contain, and remediate sophisticated threats—including APT groups and financial crime syndicates. A hands-on lab—developed from a real-world targeted attack on an enterprise network—leads you through the challenges and solutions. You will identify where the initial targeted attack occurred and which systems an APT group compromised. The course will prepare you to find out which data was stolen and by whom, contain the threat, and provide your organization the capabilities to manage and counter the attack.

During a targeted attack, an organization needs the best incident responders and forensic analysts in the field. FOR508 will train you and your team to be ready to do this work.

"The SANS FOR508 course exceeded my expectations in every way. It provided me the skills, knowledge, and tools to effectively respond to any handle apts and other enterprise-wide threats."
-Josh Moulin, NSTEC/NNSA/DOE

Rob Lee *SANS Faculty Fellow*

Rob Lee is an entrepreneur and consultant in the Washington, DC area, specializing in information security, incident response, and digital forensics. Rob is currently the curriculum lead and author for digital forensic and incident response training at the SANS Institute in addition to owning his own firm. Rob has more than 15 years of experience in computer forensics, vulnerability and exploit discovery, intrusion detection/prevention, and incident response. Rob graduated from the U.S. Air Force Academy and served in the U.S. Air Force as a founding member of the 609th Information Warfare Squadron, the first U.S. military operational unit focused on information warfare. Later, he was a member of the Air Force Office of Special Investigations (AFOSI) where he led a team conducting computer crime investigations, incident response, and computer forensics. Prior to starting his own firm, he directly worked with a variety of government agencies in the law enforcement, U.S. Department of Defense, and intelligence communities as the technical lead for a vulnerability discovery and an exploit development team, lead for a cyber forensics branch, and lead for a computer forensic and security software development team. Rob was also a director for MANDIANT, a company focused on investigating advanced adversaries, such as the APT, for four years prior to starting his own business. Rob co-authored the book ***Know Your Enemy***, 2nd Edition. Rob is also co-author of the MANDIANT threat intelligence report ***M-Trends: The Advanced Persistent Threat***. Rob frequently contributes articles at the SANS Blog **http://computer-forensics.sans.org**.

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/boston-2013.

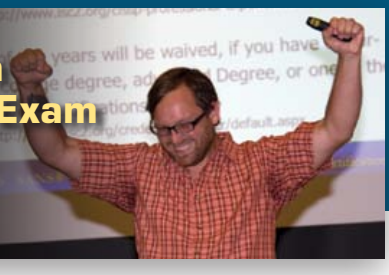
Digital Forensics and Incident Response
http://computer-forensics.sans.org

www.giac.org

www.sans.edu

MANAGEMENT 414

SANS® +S™ Training Program for the CISSP® Certification Exam



Six-Day Program • Mon, Aug 5 - Sat, Aug 10
9:00am - 7:00pm (Day 1) • 8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6) • 46 CPE/CMU Credits
Laptop NOT Required • Instructor: Seth Misenar

The SANS® +S™ Training Program for the CISSP® Certification Exam will cover the security concepts needed to pass the CISSP® exam. This is an accelerated review course that assumes the student has a basic understanding of networks and operating systems and focuses solely on the 10 domains of knowledge of the CISSP®:

- **Domain 1: Access Controls**
- **Domain 2: Telecommunications and Network Security**
- **Domain 3: Information Security Governance & Risk Management**
- **Domain 4: Software Development Security**
- **Domain 5: Cryptography**
- **Domain 6: Security Architecture and Design**
- **Domain 7: Security Operations**
- **Domain 8: Business Continuity and Disaster Recovery Planning**
- **Domain 9: Legal, Regulations, Investigations and Compliance**
- **Domain 10: Physical (Environmental) Security**

Each domain of knowledge is dissected into its critical components. Every component is discussed in terms of its relationship to other components and other areas of network security. After completion of the course, the student will have a good working knowledge of the 10 domains of knowledge and, with proper preparation, be ready to take and pass the CISSP® exam.

"This class focuses like a laser on the key concepts you'll need to understand the CISSP exam. Don't struggle with thousand page textbooks – let this course be your guide!"
-Carl Williams, Harris Corporation

Who Should Attend:

- Security professionals who are interested in understanding the concepts covered in the CISSP® exam as determined by $(ISC)^2$
- Managers who want to understand the critical areas of network security
- System, security, and network administrators who want to understand the pragmatic applications of the CISSP® 10 Domains
- Security professionals and managers looking for practical ways the 10 domains of knowledge can be applied to the current job

Obtaining your CISSP® certification consists of:

- Fulfilling minimum requirements for professional work experience
- Completing the Candidate Agreement
- Review of 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
- Period Audit of CPEs to maintain the credential

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

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

Seth Misenar *SANS Certified Instructor*

Seth Misenar is a certified SANS instructor and also serves as lead consultant and founder of Jackson, Mississippi-based Context Security, which provides information security though leadership, independent research, and security training. Seth's background includes network and Web application penetration testing, vulnerability assessment, regulatory compliance efforts, security architecture design, and general security consulting. He has previously served as both physical and network security consultant for Fortune 100 companies as well as the HIPAA and information security officer for a state government agency. Prior to becoming a security geek, Seth received a BS in philosophy from Millsaps College, where he was twice selected for a Ford Teaching Fellowship. Also, Seth is no stranger to certifications and thus far has achieved credentials which include, but are not limited to, the following: CISSP, GPEN, GWAPT, GSEC, GCIA, GCIH, GCWN, GCFA, and MCSE. Beyond his security consulting practice, Seth is a regular instructor for SANS. He teaches numerous SANS classes, including SEC401: SANS Security Essentials Bootcamp Style, SEC504: Hacker Techniques, Exploits, and Incident Handling, and SEC542: Web App Penetration Testing and Ethical Hacking. Seth has also served as both virtual mentor and technical director for SANS OnDemand, the online course delivery arm of the SANS Institute.

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/boston-2013.

SANS SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast.
More info on page 11.

GIAC INFORMATION SECURITY PROFESSIONAL GISP
www.giac.org

MANAGEMENT 512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program • Mon, Aug 5 - Fri, Aug 9
9:00am - 6:00pm (Course Days 1-4) • 9:00am - 4:00pm (Course Day 5)
33 CPE/CMU Credits • Laptop NOT Required • Instructor: Stephen Northcutt

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 gain vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. Additionally, the course has been engineered to incorporate the NIST Special Publication 800 (series) guidance so that it can be particularly useful to U.S. government managers and supporting contractors.

Who Should Attend:

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

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.

"Tremendously valuable experience!! Learned a lot and also validated a lot of our current pratices. Thank you!!"
-Chad Gray, Booz Allen Hamilton

"Every IT security professional should attend no matter what their position. This information is important to everyone."
-John Flood, NASA

Stephen Northcutt *SANS Faculty Fellow*

Stephen Northcutt founded the GIAC certification and served as president of the SANS Technology Institute (**www.sans.edu**). Stephen is author/coauthor of ***Incident Handling Step-by-Step***, ***Intrusion Signatures and Analysis***, ***Inside Network Perimeter Security 2nd Edition***, ***IT Ethics Handbook***, ***SANS Security Essentials***, ***SANS Security Leadership Essentials***, and ***Network Intrusion Detection 3rd Edition***. He was the original author of the Shadow Intrusion Detection system before accepting the position of chief for information warfare at the Ballistic Missile Defense Organization. Stephen is a graduate of Mary Washington College. Before entering the field of computer security, he worked as a Navy helicopter search and rescue crewman, white water raft guide, chef, martial arts instructor, cartographer, and network designer. Since 2007 Stephen has conducted over 40 in-depth interviews with leaders in the security industry, from CEOs of security product companies to the most well-known practitioners, in order to research the competencies required to be a successful leader in the security field. He maintains the SANS Leadership Laboratory, where research on these competencies is posted, as well as SANS Security Musings (**www.sans.edu/research/security-musings**). He leads the Management 512 Alumni Forum, where hundreds of security managers post questions. He is the lead author/instructor for Management 512: SANS Security Leadership Essentials for Managers, a prep course for the GSLC certification that meets all levels of requirements for DoD Security Managers per DoD 8570. He also is the lead author/instructor for Management 514: IT Security Strategic Planning, Policy, and Leadership. Stephen blogs at the SANS Security Laboratory. **www.sans.edu/research/security-laboratory**

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at **www.sans.org/event/boston-2013**.

www.giac.org

www.sans.edu

Bonus Sessions

SANS@Night Evening Talks

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

Keynote: APT: It is Time to Act *Dr. Eric Cole*

Albert Einstein said "We cannot solve our problems with the same thinking we used when we created them." With the new advanced and emerging threat vectors that are breaking into networks with relative ease, a new approach to security is required. The myth that these attacks are so stealthy they cannot be stopped is just not true. There is no such thing as an unstoppable adversary. It is time to act. In this engaging talk one of the experts on APT, Dr. Cole, will outline an action plan for building a defensible network that focuses on the key motto that "Prevention is Ideal but Detection is a Must". Better understand what the APT really is and what organizations can do to be better prepared. The threat is not going away, so the more organizations can realign their thinking with solutions that actually work, the safer the world will become.

Practical, Efficient Unix Auditing (with Scripts) *James Tarala*

Technical audits of Unix operating system controls can scare auditors especially if the scope is a flavor of Unix that the auditor is not 100% comfortable with the operating system. But operating system audits are the bread and butter of most IS auditors. In most every technical audit that an IS auditor will perform there will be some level of inspection thats performed at the operating system level. Auditors therefore need the skills be able to audit the technical components of an operating system, whether they have a strong background in that operating environment or not. In this presentation James Tarala, a senior instructor with the SANS Institute, will provide a practical, step-by-step approach to auditing Unix operating systems. Not only will students receive a better understanding of the audit process for these technical controls, but they will walk out of the presentation with access to an audit script to assist them in their efforts!

Certifiably Certifiable *Seth Misenar*

An alphabet soup of required certifications seems to follow every job posting, and yet for all these letters are our organizations becoming more secure? Are our security certifications failing us? Are we failing our security certifications? This talk will be a discussion on the past and current state of security certifications. Additionally, the future of security certifications and what modifications are needed will be discussed. Talk by Seth Misenar, GSE, CASP, CISSP, GSEC, GCIA, GCIH, GPEN, GWAPT, GCFA, GCWN, GCFW, MCSE, MCDBA, Cyber Guardian Red/Blue Team, etc., etc., etc.

Cloud IR & Forensics *Paul A. Henry*

The move to private and public cloud changes many things including how we respond for IR and forensics. As an example: traditionally in a physical realm we relied upon imaging a server's hard drive as well as RAM to perform a thorough analysis. Today in the cloud, creating a forensically sound image of an "instance" of a server to capture the server's abstracted hard disk and an image of its RAM brings new technical and legal complications. An additional issue to consider is that some vendor's platforms are simply not fully supported by our current IR & forensics tools; today's commercial tools lack the ability to perform any analysis at all on a VMware VMFS file system. Lastly, downloading a large server image may simply be cost prohibitive due to the high bandwidth costs associated with moving data out of the cloud environment. The best course of action may be to perform your analysis within the cloud - however, the methods used in the analysis within the cloud must be forensically sound and as always in computer forensics, they must be repeatable and the result must be the same findings. In this session we will begin to explore the changes that simply must be made to your IR and forensics procedures to properly address IR & forensics in the cloud.

An Incident Response and Forensics Analysis of an APT Attack *Rob Lee*

Is host-based detection dead? No one has been able to see the APT circumvent common defenses because victims rarely share specific attack details. Until now. A real-world APT attack reveals how surprisingly ineffective sophisticated host-based defenses are. Starting from an initial attack through data exfiltration, this presentation will cover several of the tactics and techniques used by attackers to bypass host-based controls used in numerous organizations today.

For dates, times, and complete information, visit www.sans.org/event/boston-2013/bonus-sessions

Vendor Showcase

Tuesday, August 6 | 10:30am-10:50am • 12:30pm-1:15pm • 3:00pm-3:20pm

Our events incorporate external vendor partners showcasing some of the best security solutions available. Take advantage of the opportunity to interact with the people behind the products and learn what they have to offer you and your organization.

You don't have to miss out on SANS' top-rated training. Attend select SANS Boston 2013 courses remotely via SANS Simulcast!

How SANS Simulcast Works

Cutting-edge webcast technology and live instruction combine to deliver a fun and engaging remote learning experience. Remote students will also receive four months of access to an archived copy of the class to use as a reference tool or to catch up on a missed session. The platform is web-based so students simply need a solid internet connection to participate.

"This is the first web-based training course I have done and was wondering if it would actually be worthwhile. It surpassed my expectations! The software and technology worked really well, the presenter kept everything moving along nicely and was quick to pick up on participants' comments during the lecture segments. The IM component adds value – lots of good information/comments from the class."

-Jeremy Gay, Montana State University

The following SANS Boston 2013 courses will be available via SANS Simulcast:

SEC504

SEC505

FOR508

MGT414

SANS Event Simulcast classes are:

COST-EFFECTIVE – You can save thousands of dollars on travel costs, making Event Simulcast an ideal solution for students working with limited training budgets or travel bans.

ENGAGING – Event Simulcast classes are live and interactive, allowing you to ask questions and share experiences with your instructor and classmates.

CONDENSED – Complete your course quickly; all SANS Event Simulcast classes take no longer than six days to complete.

REPEATABLE – Event Simulcast classes are recorded and placed in an online archive in case you have to miss part of the class or just wish to view the material again at a later date.

COMPLETE – You will receive the same books, discs, and MP3 audio files that conference students receive, and you will see and hear the same information as it is presented at the live event.

To register for a SANS Boston 2013 Simulcast course, please visit www.sans.org/simulcasts

What's Your Next Career Move?

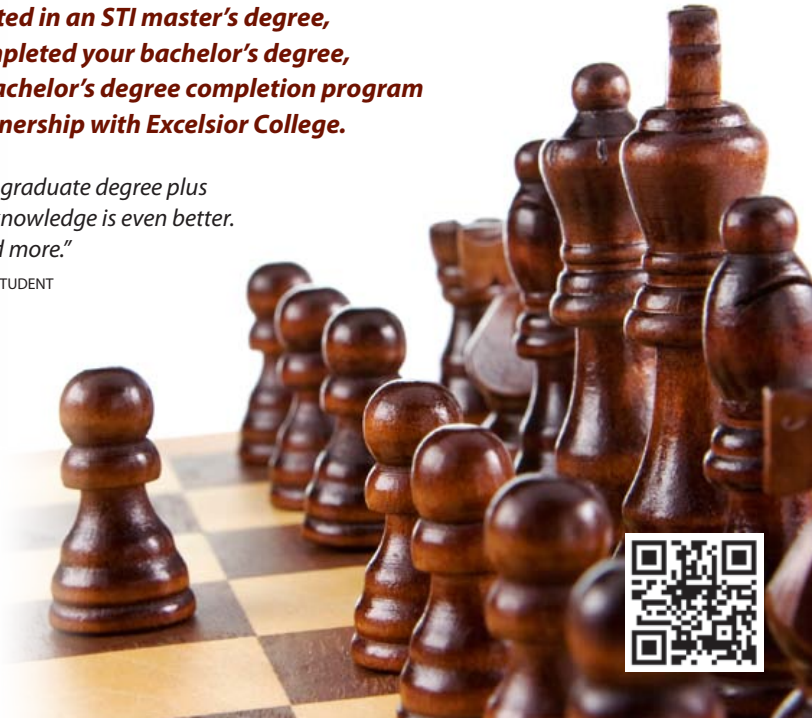
The SANS Technology Institute (STI) offers two unique master's degree programs:

Master of Science in Information Security Engineering

Master of Science in Information Security Management

If you are interested in an STI master's degree, but have not completed your bachelor's degree, we now offer a bachelor's degree completion program through our partnership with Excelsior College.

"A degree is great. A graduate degree plus current actionable knowledge is even better. STI provides this and more."
-Seth Misenar, MSISE Student



SANS TECHNOLOGY INSTITUTE
KNOWLEDGE FOR PEACE
SCIENTIA PRO PACE

www.sans.edu
info@sans.edu

How Are You Protecting Your

Risk management is a top priority. The security of these assets depends on the skills and knowledge of your security team. Don't take chances with a one-size-fits-all security certification.
Get GIAC certified!

GIAC offers over 20 specialized certifications in security, forensics, penetration testing, web application security, IT audit, management, and IT security law.

"GIAC is the only certification that proves you have hands-on technical skills."
-Christina Ford, Department of Commerce

"GIAC Certification demonstrates an applied knowledge versus studying a book."
-Alan C, USMC

GLOBAL INFORMATION ASSURANCE CERTIFICATION
GIAC
www.giac.org

Get Certified at
www.giac.org

SANS Boston 2013

Hotel Information

Training Campus
Hilton Boston Back Bay

40 Dalton Street | Boston, MA
Phone: 617-236-1100
www.hilton.com

Special Hotel Rates Available

A special discounted rate of $209.00 S/D will be honored based on space availability. Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room, and they are only available through July 21, 2013. To make reservations please call (800) HILTONS (800-445-8667) or call the hotel directly at (617) 236-1100 and ask for the SANS group rate.

Located in the picturesque neighborhood of Back Bay, the Hilton Boston Back Bay hotel is steps away from everything downtown Boston has to offer. This Back Bay hotel in Boston, Massachusetts is directly across the street from the Hynes Convention Center, is only four miles from Boston Logan International Airport, and is within walking distance of world-class shopping and dining.

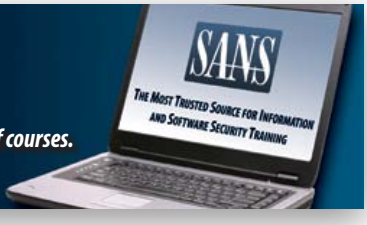
Top 5 reasons to stay at the Hilton Boston Back Bay

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 Hilton Boston Back Bay, 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 Hilton Boston Back Bay that you won't want to miss!
5. Everything is in one convenient location!

SANS Boston 2013

Registration Information

We recommend you register early to ensure you get your first choice of courses.
Register online at www.sans.org/event/boston-2013



To register, go to www.sans.org/event/boston-2013

Select your course or courses and indicate whether you plan to test for GIAC certification.

How to tell if there is room available in a course:

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.

Look for E-mail Confirmation – It Will Arrive Soon After You Register

We recommend you register and pay early to ensure you get your first choice of courses. An immediate e-mail confirmation is sent to you when the registration is submitted properly. If you have not received e-mail confirmation within two business days of registering, please call the SANS Registration office at 301-654-7267 9am - 8pm ET.

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 July 10, 2013 – processing fees may apply.

To register for a SANS Boston 2013 Simulcast course, please visit www.sans.org/simulcasts

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	**6/19/13**	**$500.00**	**7/3/13**	**$250.00**

Some restrictions apply.

Group Savings (Applies to tuition only)

15% discount if 12 or more people from the same organization register at the same time
10% discount if 8 - 11 people from the same organization register at the same time
5% discount if 4 - 7 people from the same organization register at the same time

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

SANS Voucher Credit Program

Expand your Training Budget! Extend your Fiscal Year. The SANS Voucher Discount Program pays you credits and delivers flexibility.

www.sans.org/vouchers