SANS Security East 2013

January 16-23, 2013

The Most Trusted Source for Information and Software Security Training

Hands-on immersion training programs, including:

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

Network Penetration Testing and Ethical Hacking

Intrusion Detection In-Depth

Security Leadership Essentials for Managers with Knowledge Compression™

***NEW!* Virtualization and Private Cloud Security**

And more!

"I said it back in 2004 and it still holds true today; SANS offers the best training in the industry."
-Brian Hughes, USDA

Register at www.sans.org/security-east-2013

GIAC Approved Training

Dear Colleague,

SANS will return to the "Big Easy" for **SANS Security East 2013 on January 16-23**. Start the year off right with our top-rated instructors and outstanding course offerings. New Orleans is a very special destination this year as the Mardi Gras parade season begins January 19th. Three parades are scheduled during our conference dates. In addition, New Orleans is the city where you can dine on some of the finest cuisine in the world and *laissez les bons temps rouler!*

The SANS Technology Institute (STI) has chosen our New Orleans campus to kick off its first cohort of the year! Join the STI Cohort 2013-1 and start your Master's Degree in Information Security Management (MSISM) or Master's Degree in Information Security Engineering (MSISE). Apply by December 14, 2012 date and save 30% off tuition by going to the STI homepage (**www.sans.edu**) and clicking the Learn More button.

Our lineup of ten full courses will provide a great training experience. For instance, we will be offering our new Security 575: Mobile Device Security and Ethical Hacking and Security 579: Virtualization and Private Cloud Security courses, which have been selling out at other events.

Visit our GIAC page for more information and register for your certification attempt today. Don't miss our bonus evening presentations and Vendor events where we'll share the latest threats and discuss the best solutions.

Our SANS Security East 2013 campus is once again the Sheraton New Orleans, in the heart of the Big Easy. The Canal Street location borders the French Quarter, where the city's major attractions and the Mississippi River are literally right outside the hotel's door. Close to the Sheraton you can tour the Mississippi, walk Bourbon Street, visit a plantation, shop at Riverwalk Marketplace or Canal Place, take a swamp tour, see the Aquarium of the Americas, and learn about New Orleans rich and unique history. This city is a fabulous destination with something of interest for everyone!

A special discounted rate of $189 S/D will be honored based on space availability through December 23. Register today for SANS Security East 2013 – we are looking forward to meeting you in New Orleans!

Best regards,

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

Stephen Northcutt

Here is what past attendees had to say about their SANS training experience:

"Got SANS? SANS always is one of the first places I look for information. Not only because of the quantity – but also the quality."
-Bill Coffey, Shaw AFB

"I've been to 3 previous SANS events, they are always well done and always valuable."
-Charles Higgins, Northwest Hospital Corp.

"SANS courses and instructors are the best I have ever experienced."
-Diane Matt, Department of National Defence

"Great course. This is the best training I have attended; this is my first SANS course, and I can't wait to attend more."
-Leonard Crull, MI ANG

Courses-at-a-Glance

		WED 1/16	THU 1/17	FRI 1/18	SAT 1/19	SUN 1/20	MON 1/21	TUE 1/22	WED 1/23
SEC401	SANS Security Essentials Bootcamp Style	PAGE 1							
SEC503	Intrusion Detection In-Depth	PAGE 2							
SEC504	Hacker Techniques, Exploits & Incident Handling	PAGE 3							
SEC542	Web App Penetration Testing and Ethical Hacking	PAGE 4							
SEC560	Network Penetration Testing and Ethical Hacking	PAGE 5							
SEC575	Mobile Device Security and Ethical Hacking	PAGE 6							
SEC579	Virtualization and Private Cloud Security *NEW!*	PAGE 7							
FOR408	Computer Forensic Investigations - Windows In-Depth	PAGE 8							
MGT414	SANS® +S™ Training Program for the CISSP® Cert Exam	PAGE 9							
MGT512	SANS Security Leadership Essentials for Managers with Knowledge Compression™	PAGE 10							
SEC524	Cloud Security Fundamentals							PG 11	

Security 401

Security Essentials Bootcamp Style

Six-Day Program • Wed, Jan 16 - Mon, Jan 21 • 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 to know is Why? Why do some organizations get broken into and others do 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.

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
- Anyone new to information security with some background in information systems and networking

SANS SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast.
www.sans.org/virtual-training/event-simulcast

Test your security knowledge with our SANS Security Essentials Assessment Test. Get your free test at **www.sans.org/assessments**

SPECIAL NOTE: This course is endorsed by the Committee on National Security Systems (CNSS) NSTISSI 4013 Standard for Systems Administrators in Information Systems Security (INFOSEC).

Bootcamp

This program has extended hours.
Evening Bootcamp Sessions: 5:15pm - 7:00pm (Days 1-5)

Dr. Eric Cole *SANS Faculty Fellow*

Dr. Cole is an industry-recognized security expert with over 20 years of hands-on experience. Dr. Cole currently performs leading-edge security consulting and works in research and development to advance the state of the art in information systems security. Dr. Cole has experience in information technology with a focus on perimeter defense, secure network design, vulnerability discovery, penetration testing, and intrusion detection systems. Dr. Cole has a master's degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. Dr. Cole is the author of several books, including ***Hackers Beware***, ***Hiding in Plain Site***, ***Network Security Bible***, 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 founder of Secure Anchor Consulting in which he provides state of the art security services and expert witness work. He also served as CTO of McAfee and Chief Scientist for Lockheed Martin. Dr. Cole is actively involved with the SANS Technology Institute (STI) and SANS working with students, teaching, and maintaining and developing courseware. He is a SANS Faculty Fellow and course author.

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Cyber Guardian Program
www.sans.org/cyber-guardian

Security 503
Intrusion Detection In-Depth

Six-Day Program • Wed, Jan 16 - Mon, Jan 21 • 9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Mike Poor

Learn practical hands-on intrusion detection and traffic analysis from top practitioners/authors in the field. This challenging track methodically progresses from understanding the theory of TCP/IP, examining packets, using Snort to analyze traffic, becoming familiar with the tools and techniques for traffic and intrusion analysis, to reinforcing what you've learned with a hands-on challenge of investigating an incident. Students should be able to "hit the ground running" once returning to a live environment where traffic analysis is required.

Who Should Attend:

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

This is a fast-paced course, and students are expected to have a basic working knowledge of TCP/IP (**www.sans.org/security-training/tcpip_quiz.php**) in order to fully understand the topics that will be discussed. Although others may benefit from this course, it is most appropriate for students who are or who will become intrusion detection/prevention analysts. Students generally range from novices with some TCP/IP background all the way to seasoned analysts. The challenging hands-on exercises are specially designed to be valuable for all experience levels. We strongly recommend that you spend some time getting familiar with tcpdump before coming to class.

A Sampling of Topics

TCP/IP
- Tcpdump Overview and TCP/IP concepts
- ICMP
- Fragmentation
- Stimulus - Response
- Microsoft Protocols
- Domain Name System (DNS)
- IPv6

Hands-On tcpdump Analysis
- Mechanics of running tcpdump
- General network traffic analysis

Hands-On Snort Usage
- Various modes of running Snort
- Writing Snort rules

Intrusion Analysis
- Intrusion Detection Architecture
- Intrusion Detection/Prevention Analysis

Mike Poor *SANS Senior Instructor*

Mike is a founder and senior security analyst for the DC firm InGuardians, Inc. In the past he has worked for Sourcefire as a research engineer and for SANS leading their intrusion analysis team. As a consultant Mike conducts incident response, breach analysis, penetration tests, vulnerability assessments, security audits, and architecture reviews. His primary job focus, however, is in intrusion detection, response, and mitigation. Mike currently holds the GCIA certification and is an expert in network engineering and systems and network and Web administration. Mike is an author of the international best selling Snort series of books from Syngress, a member of the Honeynet Project, and a handler for the SANS Internet Storm Center.

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Cyber Guardian Program
www.sans.org/cyber-guardian

Security 504
Hacker Techniques, Exploits, and Incident Handling

Six-Day Program • Wed, Jan 16 - Mon, Jan 21 • 9:00am - 5:00pm • 37 CPE/CMU Credits
Laptop Required • Instructor: Bryce Galbraith

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.

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

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 and 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.

SANS SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast.
www.sans.org/virtual-training/event-simulcast

Notice: It is imperative that you get written permission from the proper authority in your organization before using these tools and techniques on your company's system and also that you advise your network and computer operations teams of your testing.

"The quick pace is awesome! Moving forward and actively covering topics is invigorating!" -Steven Park, Boeing

GIAC Certification
www.giac.org

Bryce Galbraith *SANS Certified Instructor*

As a contributing author of the internationally best-selling book ***Hacking Exposed: Network Security Secrets & Solutions***, Bryce helped bring the secret world of hacking out of the darkness and into the public eye. Bryce has held security positions at global ISPs and Fortune 500 companies, he was a member of Foundstone's renowned penetration testing team and served as a senior instructor and co-author of Foundstone's ***Ultimate Hacking: Hands-On*** course series. Bryce is currently the owner of Layered Security where he and his team provide specialized vulnerability assessment and penetration testing services for clients. He teaches several of The SANS Institute's most popular courses and develops curriculum around current topics. He has taught the art of ethical hacking and countermeasures to thousands of IT professionals from a who's who of top companies, financial institutions, and government agencies around the globe. Bryce is an active member of several security-related organizations, he speaks at numerous conferences, and holds several security certifications and blogs about security issues at **http://blog.layeredsec.com**.

STI Graduate School
www.sans.edu

Cyber Guardian Program
www.sans.org/cyber-guardian

Security 542
Web App Penetration Testing and Ethical Hacking

Six-Day Program • Wed, Jan 16 - Mon, Jan 21 • 9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Seth Misenar

Web applications are a major point of vulnerability in organizations today. Web app holes have resulted in the theft of millions of credit cards, major financial and reputational damage for hundreds of enterprises, and even the compromise of thousands of browsing machines that visited Web sites altered by attackers. In this intermediate to advanced level class, you'll learn the art of exploiting Web applications so you can find flaws in your enterprise's Web apps before the bad guys do. Through detailed, hands-on exercises and training from a seasoned professional, you will be taught the four-step process for Web application penetration testing. You will inject SQL into back-end databases, learning how attackers exfiltrate sensitive data. You will utilize cross-site scripting attacks to dominate a target infrastructure in our unique hands-on laboratory environment. And you will explore various other Web app vulnerabilities in depth with tried-and-true techniques for finding them using a structured testing regimen. You will learn the tools and methods of the attacker, so that you can be a powerful defender.

Who Should Attend:

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

Throughout the class, you will learn the context behind the attacks so that you intuitively understand the real-life applications of our exploitation. In the end, you will be able to assess your own organization's Web applications to find some of the most common and damaging Web application vulnerabilities today.

By knowing your enemy, you can defeat your enemy. General security practitioners, as well as Web site designers, architects, and developers, will benefit from learning the practical art of Web application penetration testing in this class.

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.

"Outstanding course!! It is great to have an opportunity to learn the material from someone who is extremely relevant in the field and is able to impart the value of his experiences."
-Bobby Bryant, DoD

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Cyber Guardian Program
www.sans.org/cyber-guardian

Security 560
Network Penetration Testing and Ethical Hacking

Six-Day Program • Wed, Jan 16 - Mon, Jan 21 • 9:00am - 5:00pm • 37 CPE/CMU Credits
Laptop Required • Instructor: Ed Skoudis

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.

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

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.

"Can't overemphasize the value in getting wisdom from a seasoned, experienced penetration tester."

-Sean Verity, MSUFCU

Ed Skoudis *SANS Faculty Fellow*

Ed Skoudis is a founder and senior security consultant with InGuardians. He is also the founder of Counter Hack Challenges, an innovative organization that designs, builds, and operates popular infosec challenges and simulations including NetWars, Cyber Quests, and Cyber Foundations. Ed's expertise includes hacker attacks and defenses, the information security industry, and computer privacy issues, with over fifteen years of experience in information security. Ed authored and regularly teaches the SANS courses on network penetration testing (SEC560) and incident response (SEC504), helping over three thousand information security professionals each year improve their skills and abilities to defend their networks. He has performed numerous security assessments; conducted exhaustive anti-virus, anti-spyware, Virtual Machine, and IPS research; and responded to computer attacks for clients in financial, high technology, healthcare, and other industries. Ed conducted a demonstration of hacker techniques against financial institutions for the United States Senate and is a frequent speaker on issues associated with hacker tools and defenses. He has published numerous articles on these topics as well as the Prentice Hall best sellers ***Counter Hack Reloaded*** and ***Malware: Fighting Malicious Code***. Ed was also awarded 2004-2009 Microsoft MVP awards for Windows Server Security and is an alumnus of the Honeynet Project. Previous to InGuardians, Ed served as a security consultant with International Network Services (INS), Global Integrity, Predictive Systems, SAIC, and Bell Communications Research (Bellcore). Ed also blogs about command line tips. **http://blog.commandlinekungfu.com**

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Cyber Guardian Program
www.sans.org/cyber-guardian

Security 575
Mobile Device Security and Ethical Hacking

Six-Day Program • Wed, Jan 16 - Mon, Jan 21 • 9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Provided for Class use • Instructor: Joshua Wright

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 ERP 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.

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.**

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**

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.

SANS SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast.
www.sans.org/virtual-training/event-simulcast

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.

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.

Joshua Wright *SANS Senior Instructor*

Joshua Wright is an independent information security analyst and senior instructor with the SANS Institute. A widely recognized expert in the wireless security field, Josh has worked with private and government organizations to evaluate the threat surrounding wireless technology and evolving threats. As an open-source enthusiast, Josh has developed a variety of tools that can be leveraged for penetration testing and security analysis. Josh publishes his tools, papers and techniques for effective security analysis on his website at **www.willhackforsushi.com**.

Security 579
Virtualization and Private Cloud Security

Six-Day Program • Wed, Jan 16 - Mon, Jan 21 • 9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Dave Shackleford

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.

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.

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

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, as well, 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 next two days will help you adapt your existing security policies and practices to the new virtualized or cloud-based infrastructure. The final two days 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?

Dave Shackleford *SANS Senior Instructor*

Dave Shackleford is the owner and principal consultant at Voodoo Security; senior vice president of research and CTO at IANS; and a SANS analyst, instructor, and course author. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. He is a VMware vExpert and has 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 coauthor of Hands-On Information Security from Course Technology as well as the Managing Incident Response chapter in the Course Technology book Readings and Cases in the Management of Information Security. 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.

Forensics 408

Computer Forensic Investigations – Windows In-Depth

Six-Day Program • Wed, Jan 16 - Mon, Jan 21 • 9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Rob Lee

Master computer forensics. Learn critical investigation techniques. With today's ever-changing technologies and environments, it is inevitable that every organization will deal with cybercrime including fraud, insider threat, industrial espionage, and phishing. In addition, government agencies are now performing media exploitation to recover key intelligence kept on adversary systems. In order to help solve these cases, organizations are hiring digital forensic professionals and calling cybercrime law enforcement agents to piece together what happened in these cases.

Who Should Attend:

- Information technology professionals
- Incident Response Team Members
- Law enforcement officers, federal agents, or detectives
- Media Exploitation Analysts
- Information security managers
- Information technology lawyers and paralegals
- Anyone interested in computer forensic investigations

This course covers the fundamental steps of the in-depth computer forensic and media exploitation methodology so that each student will have the complete qualifications to work as a computer forensic investigator in the field helping solve and fight crime. In addition to in-depth technical digital forensic knowledge on Windows Digital Forensics (Windows XP through Windows 7 and Server 2008), you will be exposed to well-known computer forensic tools such as Access Data's Forensic Toolkit (FTK), Guidance Software's EnCase, Registry Analyzer, FTK Imager, Prefetch Analyzer, and much more.

FOR408: COMPUTER FORENSIC INVESTIGATIONS – WINDOWS IN-DEPTH is the first course in the SANS Computer Forensic Curriculum. If this is your first computer forensics course with SANS we recommend that you start here.

FIGHT CRIME. UNRAVEL INCIDENTS...ONE BYTE AT A TIME.

GIAC Certification
www.giac.org

You will receive with this course: Free SANS Investigative Forensic Toolkit (SIFT) Essentials

As a part of this course you will receive a SANS Investigative Forensic Toolkit (SIFT) Essentials with a Tableau Write Block Acquisition Kit.

- **One Tableau T35es Write Blocker (Read-Only)**
- **IDE Cable/Adapters**
- **SATA Cable/Adapters**
- **FireWire and USB Cable Adapters**
- **Forensic Notebook Adapters (IDE/SATA)**

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

Rob Lee *SANS Faculty Fellow*

Rob Lee is an entrepreneur and consultant in the Washington D.C. area and 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' experience in computer forensics, vulnerability and exploit development, intrusion detection/prevention, and incident response. Rob graduated from the U.S. Air Force Academy and earned his MBA from Georgetown University. He served in the U.S. Air Force as a member of the 609th Information Warfare Squadron (IWS), 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 computer crime investigations and incident response. Over the next 7 years, he worked directly 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. Most recently, Rob was a Director for MANDIANT, a commercial firm focusing on responding to advanced adversaries such as the APT. 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**.

Management 414

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

Six-Day Program • Wed, Jan 16 - Mon, Jan 21 • 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: Paul A. Henry

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.

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
- In short, if you desire a CISSP® or your job requires it, MGT414 is the training for you to get GISP certified. Reinforce what you learned in training and prove your skills and knowledge with a GISP certification.

You Will Receive With This Course:

Free "CISSP® Study Guide" by Eric Conrad, Seth Misenar, and Joshua Feldman.

Obtaining your CISSP® certification consists of:

- Fulfilling minimum requirements for professional work experience
- Completing the Candidate Agreement
- Review of Resume
- 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

Bootcamp

This program has extended hours.
Evening Bootcamp Sessions: 5:00pm - 7:00pm (Days 1-5)
Morning Bootcamp Sessions: 8:00am - 9:00am (Days 2-6)

SANS SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast.
www.sans.org/virtual-training/event-simulcast

Paul A. Henry *SANS Certified 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. Henry has played a key strategic role in launching new network security initiatives to meet our ever-changing threat landscape. Paul 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. Henry is frequently cited 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. 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. Paul serves as a 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.

GIAC Certification
www.giac.org

Management 512

SANS Security Leadership Essentials for Managers with Knowledge Compression™

Five-Day Program • Wed, Jan 16 - Sun, Jan 20 • 9:00am - 6:00pm (Days 1-4) • 9:00am - 5:00pm (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 learn vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. Additionally, the course has been engineered to incorporate the NIST Special Publication 800 (series) guidance so that it can be particularly useful to US government managers and supporting contractors.

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, 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.

Who Should Attend:

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

There are three goals for this course and certification:

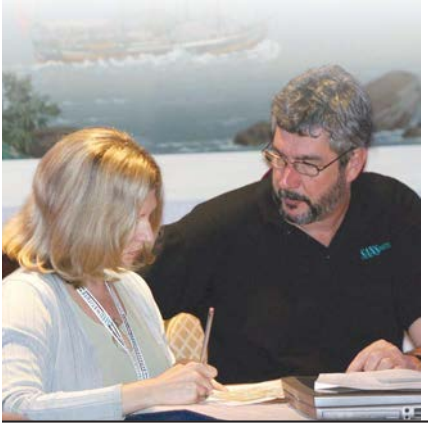
1) Establish a minimum standard for IT security knowledge, skills, and abilities.
2) Establish a minimum standard for IT management knowledge, skills, and abilities.
3) Save the up-and-coming generation of senior and rapidly advancing managers a world of pain by sharing the things we wish someone had shared with us.

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Stephen Northcutt *SANS Faculty Fellow*

Stephen Northcutt founded the GIAC certification and currently serves as president of the SANS Technology Institute, a postgraduate level IT security college (**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 34 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. He is the lead author for Execubytes, a monthly newsletter that covers both technical and pragmatic information for security managers. He leads the MGT512 Alumni forum, where hundreds of security managers post questions. He is the lead author/instructor for MGT512, a prep course for the GSLC certification that meets all levels of requirements for DoD Security Managers per DoD 8570, and he also is the lead author/instructor for MGT421. Stephen also blogs at the SANS Security Leadership blog. **www.sans.edu/research/leadership-laboratory**

Security 524
Cloud Security Fundamentals

Two-Day Program • Tue, Jan 22 - Wed, Jan 23 • 9:00am - 5:00pm • 12 CPE/CMU Credits
Laptop Required • Instructor: Dave Shackleford

Many organizations today are feeling pressure to reduce IT costs and optimize IT operations. Cloud computing is rapidly emerging as a viable means to create dynamic, rapidly provisioned resources for operating platforms, applications, development environments, storage and backup capabilities, and many more IT functions. A staggering number of security considerations exist that information security professionals need to consider when evaluating the risks of cloud computing.

The first fundamental issue is the loss of hands-on control of system, application, and data security. Many of the existing best practice security controls that infosec professionals have come to rely on are not available in cloud environments, stripped down in many ways, or not able to be controlled by security teams. Security professionals must become heavily involved in the development of contract language and Service Level Agreements (SLAs) when doing business with Cloud Service Providers (CSPs). Compliance and auditing concerns are compounded. Control verification and audit reporting within CSP environments may be less in-depth and frequent as audit and security teams require.

Who Should Attend:

- Security personnel who are currently tasked with assessing the technical risks of cloud computing
- Network and systems administrators who currently manage private clouds or need to leverage hybrid and/or public cloud services
- Technical auditors and consultants who need to gain a deeper understanding of cloud computing and security concerns
- Security and IT managers who need to understand the risks of cloud computing and advise business management of the risks and various approaches to cloud computing

The SANS Cloud Security Fundamentals course starts out with a detailed introduction to the various delivery models of cloud computing ranging from Software as a Service (SaaS) to Infrastructure as a Service (IaaS) and everything in between. Attendees will start off the second day with coverage of audits and assessments for cloud environments. The day will include hands-on exercises for students to learn about new models and approaches for performing assessments, as well as evaluating audit and monitoring controls. Next the class will turn to protecting the data itself! New approaches for data encryption, network encryption, key management, and data lifecycle concerns will be covered in-depth.

Dave Shackleford *SANS Senior Instructor*

Dave Shackleford is the owner and principal consultant at Voodoo Security; senior vice president of research and CTO at IANS; and a SANS analyst, instructor, and course author. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. He is a VMware vExpert and has 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 coauthor of Hands-On Information Security from Course Technology as well as the Managing Incident Response chapter in the Course Technology book Readings and Cases in the Management of Information Security. 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.

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, get the most for your training dollar, and hear from the voices that matter in computer security.

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

Future Trends in Network Security 2013 *Dr. Eric Cole*

Malicious code and other attacks are increasing in intensity and the damage that they cause. With little time to react, organizations have to become more proactive in their security stance. Reactive security will no longer work. Therefore, organizations need to better understand what the future trends, risks, and threats are so that they can be better prepared to make their organizations as secure as possible. Dr. Cole's in-depth, cross-industry experience allows him to give relevant examples in every instance. This presentation covers security issues that are relevant to IT managers and administrators alike.

Hacking Your Friends and Neighbors For Fun *Joshua Wright*

I regularly see my neighbors trying to connect to open wireless APs I run in my house. A while back, I setup a special open AP to give them Internet access. The cost? My entertainment. My neighbor-hack AP is setup to manipulate the web traffic of its users, randomly redirecting people to websites of my choosing, manipulating the format and content of pictures they download and more. All it takes is an inexpensive AP, a Linux box and an Internet connection. In this talk, I'll show you how to setup your own neighbor-hack AP and, in the process, you'll learn just how scary (or fun) an open wireless AP can be.

The Next Wave - Data Center Consolidation *Paul A. Henry*

Many of the physical server to virtual server projects have long been been completed. The next wave is to consolidate those early entries to improve data center density and performance. This presentation looks at Federal, State and commercial consolidation efforts. Of critical importance is that an organization's Wide-Area Network (WAN) is the foundation of their globally connected enterprise, enabling collaboration, communication, business productivity, and risk mitigation. The performance of the WAN is critical to everything organizations do. This engaging workshop, led by expert, Paul Henry, will begin here and branch out to help you navigate trends and challenges driving change in IT and discuss best practices that every organization can employ.

Top Threats to Cloud for 2013 *Dave Shackleford*

One of the major research projects that the Cloud Security Alliance (CSA) publishes is the "Top Threats to Cloud" report. As one of the co-chairs of this working group and research project, as well as the author of the SANS cloud security class and curriculum, Dave Shackleford has worked to update the latest CSA documents and gather input from the industry at large regarding the top threats to today's cloud providers and infrastructure. In this session, Dave will provide an update on what's new with the CSA working group, what the latest research has uncovered, and delve into some of the latest attacks, vulnerabilities, and threat vectors facing cloud infrastructure today.

Vendor Showcase

Thursday, January 17, 2013 | 12:00pm - 1:30pm and 5:00pm - 7:00pm

How Are You Protecting Your

- Data
- Network
- Systems
- Critical Infrastructure

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, audit, and management.

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

-Christina Ford,
Department of Commerce

Learn more about GIAC and how to *Get Certified* at **www.giac.org**

What's Your Next Career Move?

The information security field is growing and maturing rapidly; are you positioned to win? A Master's Degree in Information Security from the SANS Technology Institute will help you build knowledge and skills in management or technical engineering.

STI offers two master's degree programs:

Master of Science in Information Security Engineering

Master of Science in Information Security Management

The Master of Science degree programs of study leading to proficiency in Information Security Engineering (MSISE) and Management (MSISM) are developed and delivered for you using a scholar-practitioner philosophy. *Scholar-practitioner* means they are designed to provide a sound theoretical experience delivered through practitioner's lens. The focus of the programs is solutions at the enterprise level, meaning you will be able to make an impact at on an organization, total system or sovereign entity.

www.sans.edu
info@sans.edu
720.941.4932

Department of Defense

Come to SANS and take the training with the highest pass rate on 8570 required certifications.

www.sans.org/8570

DoD Approved Baseline Certifications

IAT Level I	IAT Level II	IAT Level III
A+-CE	**GSEC**	**GCIH**
Network+CE	Security+CE	**GSE**
SSCP	SSCP	CISA
		CISSP (or Associate)

IAM Level I	IAM Level II	IAM Level III
GISF	**GSLC**	**GSLC**
GSLC	CAP	CISM
CAP	CISM	**CISSP** (or Associate)
Security+CE	**CISSP** (or Associate)	

IASAE I	IASAE II	IASAE III
CISSP (or Associate)	**CISSP** (or Associate)	CISSP - ISSEP
		CISSP - ISSAP

CND Analyst	CND Infrastructure Support
GCIA	SSCP
GCIH	CEH
CEH	

CND Incident Responder	CND Auditor
GCIH	**GSNA**
CSIH	CSIA
CEH	CEH

CN-SP Manager
CISSP - ISSMP
CISM

SANS Training Courses for DoD Approved Certifications

SANS TRAINING COURSE	DoD APPROVED CERT
SEC301: Intro to Information Security	GISF
SEC401: SANS Security Essentials Bootcamp Style	GSEC
SEC503: Intrusion Detection In-Depth	GCIA
SEC504: Hacker Techniques, Exploits & Incident Handling	GCIH
AUD507: Auditing Networks, Perimeters and Systems	GSNA
MGT414: SANS® +S™ Training Program for the CISSP® Certification Exam	CISSP
MGT512: SANS Security Essentials for Managers with Knowledge Compression™	GSLC

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

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

SANS CYBER GUARDIAN PROGRAM

www.sans.org/cyber-guardian

Stay ahead of cyber threats!

Join the SANS Cyber Guardian program today.

How the Program Works

This program begins with hands-on core courses that will build and increase your knowledge and skills. These skills will be reinforced by taking and passing the associated GIAC certification exam. After completing the core courses, you will choose a course and certification from either the Red or Blue Team. The program concludes with participants taking and passing the GIAC Security Expert (GSE) certification.

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

Program Prerequisites

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

Core Courses

SEC503 Intrusion Detection In-Depth (GCIA)

SEC504 Hacker Techniques, Exploits, and Incident Handling (GCIH)

SEC560 Network Penetration Testing and Ethical Hacking (GPEN)

FOR508 Advanced Computer Forensic Analysis & Incident Response (GCFA)

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

Blue Team Courses

SEC502 Perimeter Protection In-Depth (GCFW)

SEC505 Securing Windows & Resisting Malware (GCWN)

SEC506 Securing Linux/Unix (GCUX)

Red Team Courses

SEC542 Web App Penetration Testing & Ethical Hacking (GWAPT)

SEC617 Wireless Ethical Hacking, Penetration Testing, and Defenses (GAWN)

SEC660 Advanced Penetration Testing, Exploits, and Ethical Hacking (GXPN)

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

SECURITY AWARENESS

FOR THE 21st CENTURY

- Go beyond compliance and focus on changing behaviors.
- Training is mapped against the 20 Critical Controls framework.
- Create your own program by choosing from over 25 different training modules.
- Meets mandated compliance requirements.
- Translated into 20 languages.
- Host on the SANS Virtual Learning Environment (VLE)
- For a free trial account contact us at info@securingthehuman.org

SANS SECURING THE HUMAN

www.securingthehuman.org

Future SANS

SANS **San Diego** 2012
San Diego, CA
November 12-17, 2012
www.sans.org/san-diego-2012

SANS **San Antonio** 2012
San Antonio, TX
November 27 - December 2, 2012
www.sans.org/san-antonio-2012

SANS **Cyber Defense Initiative** 2012
Washington, DC
December 7-16, 2012
www.sans.org/cyber-defense-initiative-2012

SANS **Mobile Device Security**
Summit 2013
Anaheim, CA | January 7-14, 2013
www.sans.org/mobile-device-security-summit-2013

SANS **Virtualization and Cloud Computing**
Summit 2013
Anaheim, CA | January 7-14, 2013
www.sans.org/virtualization-cloud-summit-2013

SANS **North American SCADA and Process Control**
Summit 2013
Lake Buena Vista, FL | February 6-15, 2013
www.sans.org/north-american-scada-2013

SANS **Scottsdale** 2013
Scottsdale, AZ
February 18-23, 2013
www.sans.org/scottsdale-2013

SANS 2013
Orlando, FL
March 8-15, 2013
www.sans.org/sans-2013

SANS **Monterey** 2013
Monterey, CA
March 20-28, 2013
www.sans.org/monterey-2013

For a complete list of SANS events, visit www.sans.org/security-training/bylocation/index_all.php

Training Events

SANS **Northern Virginia** 2013
Reston, VA
April 14-20, 2013
www.sans.org/northern-virginia-2013

SANS **Cyber Guardian** 2013
Baltimore, MD
April 15-20, 2013
www.sans.org/cyber-guardian-2013

SANS **Austin** 2013
Austin, TX
April 22-27, 2013
www.sans.org/austin-2013

SANS **Security West** 2013
San Diego, CA
May 9-14, 2013
www.sans.org/security-west-2013

SANSFIRE 2013
Washington, DC
June 17-24, 2013
www.sans.org/sansfire-2013

SANS **Rocky Mountain** 2013
Denver, CO
July 15-22, 2013
www.sans.org/rocky-mountain-2013

SANS **San Francisco** 2013
San Francisco, CA
July 29 - August 6, 2013
www.sans.org/san-francisco-2013

SANS **Boston** 2013
Boston, MA
August 12-17, 2013
www.sans.org/boston-2013

SANS **Network Security** 2013
Las Vegas, NV
September 18-25, 2013
www.sans.org/network-security-2013

SANS Training Options

Multi-Course Training Events

Live instruction from SANS' top faculty, vendor showcase, bonus evening sessions, and networking.

www.sans.org/security-training/bylocation/index_all.php

Community SANS

Live Training in Your Local Region with Smaller Class Sizes

www.sans.org/community

OnSite

Live Training at Your Office Location

www.sans.org/onsite

Mentor

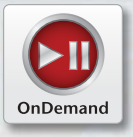
Live Multi-Week Training with a Mentor

www.sans.org/mentor

Summit

Live IT Security Summits and Training

www.sans.org/summit



OnDemand

All the Course Content at Your Own Pace

www.sans.org/ondemand

vLive

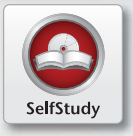
Virtual Live Training from Your Home or Office

www.sans.org/virtual-training/vlive

Simulcast

Attend Event Training From Your Location

www.sans.org/virtual-training/event-simulcast
www.sans.org/virtual-training/custom-simulcast



SelfStudy

Independent Study with Books and MP3s

www.sans.org/selfstudy

Hotel Information

SANS Security East 2013 will be located at

Sheraton New Orleans

500 Canal Street
New Orleans, LA 70130
Phone: 504-525-2500

Special 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; you will need to call reservations and ask for the SANS government rate. These rates include high speed Internet in your room and are only available through December 23, 2012. To make reservations please call 888-627-7033 and ask for the SANS group rate.

You must mention that you are attending the SANS Institute training event to get the discounted rate or special amenities.

The hotel will require a major credit card to guarantee your reservation. To cancel your reservation, you must notify the hotel at least 72 hours before your planned arrival date.

Top 5 reasons to stay at Sheraton New Orleans

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

Registration Information

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

Register online at www.sans.org/security-east-2013

To register, go to www.sans.org/security-east-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 9:00am - 8:00pm Eastern Time.

Cancellation

You may substitute another person in your place at any time by e-mail: **registration@sans.org** or faxing to 301-951-0140. There is a $300 cancellation fee per registration. Cancellation requests must be received by Wednesday, September 26 by fax or mail-in order to receive a refund.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	**11/28/12**	**$500.00**	**12/12/12**	**$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 Discount Program that pays you credits and delivers flexibility www.sans.org/vouchers