SANS

The Most Trusted Source for Information and Software Security Training

Virginia Beach 2012

Virginia Beach, VA | August 20-31, 2012

The right security training for your staff, at the right time, in the right location.

"The material was spot on and timely for immediate action when I return to work next week."

-Scott Finke USSA-ARS

Hands-on immersion training programs, including

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

Network Penetration Testing and Ethical Hacking

Security Leadership Essentials For Managers

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

Intrusion Detection In-Depth

Implementing and Auditing the Twenty Critical Security Controls - In-Depth

Advanced Computer Forensic Analysis and Incident Response

Auditing Networks, Perimeters, and Systems

NEW! **Mobile Device Security and Ethical Hacking**

Register at www.sans.org/virginia-beach-2012

GIAC Approved Training

Dear Colleague,

Stephen Northcutt

I am pleased to invite you to **SANS Virginia Beach 2012, August 20-31**. Don't miss the chance for a late-summer, family beach vacation with two weeks of SANS training! This event was a hit last year, so we are repeating the opportunity to take two full back-to-back courses in this popular location.

Attend one or two of our 10 courses from four of our disciplines - audit, security, management, and forensics, then relax at the beach with your family in your off time. You will return home with valuable, hands-on, security skills and maybe even a sock full of seashells! Our hand-picked instructor lineup includes Dr. Eric Cole, John Strand, David Hoelzer, James Tarala, Mike Poor, Joshua Wright, Michael Murr, Christopher Crowley, and me. See this brochure for a complete schedule, course descriptions, instructor bios, GIAC cert availability for eight of our courses, and information about earning your Master's Degree in Information Security through the SANS Technology Institute (STI).

Don't miss our bonus evening talks. These hot, late-breaking sessions are presented by our instructors and will add to your experience at no additional cost.

With 35 miles of beaches right nearby, the new Hilton Virginia Beach Oceanfront offers the perfect end-of-summer destination. Located on the Virginia Beach boardwalk and ocean front, the hotel is right next to Neptune's Park and the Shoppes at 31 Ocean. A discounted room rate of $199 S/D is available to SANS students until July 27, including complimentary high-speed Internet in the guest room rate! Government per diem rooms are available with proper ID. Please note that when you call the hotel for a reservation you will need to ask for the "SANS Government Per Diem Block." We also recommend you call the hotel directly during business hours. This event has a history of filling up fast, so register and book your room as early as possible.

"Where else could you get a compressed course from a fun instructor? Here at SANS. I'm coming back!" - Faye Higdon, Naval Sea Systems Command

Register by July 11 to receive a $500 tuition fee discount! Start making your training and travel plans now and let your colleagues and friends know about SANS Virginia Beach 2012. We look forward to seeing you there.

Best regards,

Stephen Northcutt

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

Courses-at-a-Glance

		MON 8/20	TUE 8/21	WED 8/22	THU 8/23	FRI 8/24	SAT 8/25
AUD507	Auditing Networks, Perimeters, and Systems	PAGE 12					
FOR508	Advanced Computer Forensic Analysis & Incident Response	PAGE 9					
SEC401	SANS Security Essentials Bootcamp Style	PAGE 3					
SEC504	Hacker Techniques, Exploits & Incident Handling	PAGE 5					
SEC575	Mobile Device Security and Ethical Hacking ***NEW!***	PAGE 8					
		SUN 8/26	MON 8/27	TUE 8/28	WED 8/29	THU 8/30	FRI 8/31
MGT414	SANS® +S™ Training Program for the CISSP® Cert Exam	PAGE 10					
MGT512	SANS Security Leadership Essentials For Managers with Knowledge Compression™		PAGE 11				
SEC503	Intrusion Detection In-Depth	PAGE 4					
SEC560	Network Penetration Testing and Ethical Hacking	PAGE 6					
SEC566	Implementing and Auditing the Twenty Critical Security Controls - In-Depth		PAGE 7				

Special Events

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.

Why Do Organizations Get Compromised? *Dr. Eric Cole*

The number one question people ask with regards to security is... "Why?".

Why do some organizations get compromised and others do not? Fifteen years ago, when an organization was compromised, it was pretty easy to understand why. The organization spent minimal energy and effort on security, did not protect their systems and it was pretty obvious why they were compromised. Today, organizations are spending significant resources on cyber security and still being compromised. Many executives and technical staff are getting very frustrated because on the surface it looks like they are doing the right things, but they are still compromised. This talk will focus on why organizations are compromised and what checks you can perform to determine your likelihood of being compromised. Trends and solutions will also be examined to understand what needs to be done to build an effective program.

Information Assurance Metrics: Practical Steps to Measurement

James Tarala

In this presentation, James Tarala, a senior instructor with the SANS Institute, will be presenting on making specific plans for information assurance metrics in an organization. Learn what efforts are currently underway in the industry to create consensus metrics guides and what initial steps an organization can take to start measuring the effectiveness of their security program. Small steps are better than no steps, and by the end of this presentation, students will have a start integrating metrics into their information assurance program.

Everything They Told Me About Security Was Wrong *John Strand*

In this presentation we will cover many of the common misconceptions about computer security. We will have multiple live demonstrations including: hacking a Mac, and hacking a Linux system and bypassing AV. However, the most important thing about this presentation is that we will cover how we need to change our defensive mindset. After all, if information security was easy it would not take six days to cover the essentials.

Who's Watching the Watchers *Mike Poor*

We have instrumented our networks to the Nth degree. We have firewalls, IDS, IPS, Next Gen Firewalls, Log correlation, and aggregation... but do we know if we have it right? Will we detect the NextGen™ attackers? In this talk we will explore ways that we improve the signal/noise ratio in our favor, and help identify the needle in the needlestack.

Failure to Operate *Chris Crowley*

An organization with a well run operations department tends to also have good security. Even though this is well known, some organizations still fail to maintain operational excellence. These failures manifest in myriad minor failures, and combine to produce at times spectacular failures.

Assessing Deception *Mike Murr*

This talk departs from the traditional aspects of information security, and focuses on the human element of deception. Join us as we examine the *process* and the mechanics behind assessing deception, and dispel some of the common myths that pervade today's society. So if you are interested in learning the signs and clues that someone may be lying to you, make sure to attend this talk.

For dates, times, and complete information, please visit www.sans.org/virginia-beach/night.php

SANS Virginia Beach 2012

Vendor Expo

Tuesday, August 21 & Tuesday, August 28
12:00pm - 1:30pm and 5:00pm - 7:00pm

Given that (virtually) everything in security is accomplished with a tool, exposure to those tools is a very important part of the SANS Training Event learning experience. Leading solutions providers will be on-hand for two vendor expos, an added bonus to registered training event attendees.

PROTECT

Prove you have the skills, training and experience to be an IT security expert. GIAC Certification holders possess comprehensive security skills to protect critical IT infrastructure.

Top Four Reasons to Get GIAC Certified

1. **Promotes** hands-on technical skills and improves knowledge retention
2. **Provides** proof that you possess hands-on technical skills
3. **Positions** you to be promoted and earn respect among your peers
4. **Proves** to hiring managers that you are technically qualified for the job

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

GLOBAL INFORMATION ASSURANCE CERTIFICATION
GIAC
www.giac.org

Security 401

SANS Security Essentials Bootcamp Style

Six-Day Program • Mon, Aug 20 - Sat, Aug 25
9:00am - 7:00pm (Days 1-5) • 9:00am - 5:00pm (Day 6)
46 CPE/CMU Credits • Laptop Required
Instructor: Dr. Eric Cole

Maximize your training time and turbo-charge your career in security by learning the full SANS Security Essentials curriculum needed to qualify for the GSEC certification. In this course you will learn the language and underlying theory of computer security. At the same time you will learn the essential, up-to-the-minute knowledge and skills required for effective performance 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 up-to-the-minute 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. As always, great teaching sets SANS courses apart, and SANS ensures this by choosing instructors who have ranked highest in a nine-year competition among potential security faculty.

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).

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

Bootcamp

This program has extended hours.
Security 401 PARTICIPANTS ONLY
Evening Bootcamp Sessions:
5:15pm - 7:00pm (Days 1-5)

Attendance is required for the evening bootcamp sessions as the information presented appears on the GIAC exams. These daily bootcamps give you the opportunity to apply the knowledge gained throughout the course in an instructor-led environment. It helps fill your toolbox with valuable tools you can use to solve problems when you go back to work. The material covered is based on Dr. Eric Cole's "Cookbook for Geeks," and most students find it to be one of the highlights of their Security Essentials experience! Students will have the opportunity to install, configure, and use the tools and techniques they have learned. CDs containing the software required will be provided for each student. Students should arrive with a laptop properly configured. A working knowledge of each operating system is recommended but not required. For students who do not wish to build a dual boot machine, SANS will provide a bootable Linux CD for the Linux exercises.

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.

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

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/virginia-beach-2012/event.php.

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 • Sun, Aug 26 - Fri, Aug 31
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 is the most advanced program in network intrusion detection that has ever been taught. This course is jam-packed with network traces and analysis tips.

The emphasis of this course is on improving students' understanding of the workings of TCP/IP, methods of network traffic analysis, and one specific intrusion detection/prevention system (IDS/IPS) - Snort. This is not a comparison or demonstration of multiple IDS/IPS solutions. Instead, the knowledge provided here enables students to better understand the qualities that go into a sound IDS/IPS so they are better equipped to make a wise selection for a site's particular needs.

This is a fast-paced course, and students are expected to have a basic working knowledge of TCP/IP (see www.sans.org/conference/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 or windump before coming to class.

Who Should Attend:

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

From the Author

Guy Bruneau, Mike Poor, and I have worked as intrusion analysts for many years. Over the years, we have seen our fair share of attacks and suspicious traffic often leading to intrusions. Over time, we have developed various analysis techniques that work on new detects that we have learned to pass on to the students. Attendees will learn how TCP/IP really works from instructors that have spent thousands of hours analyzing, researching and categorizing suspicious traffic with a variety of security tools. You will learn from hundreds of old and current examples of detects that were captured in the real world and be able to apply these real world examples to analyze known and new intrusion patterns. We are confident that students will put the training they receive from this course into practice the day they get back to the office.
- Judy Novak, Guy Bruneau, and Mike Poor

What Students Are Saying

"This class heightens your security awareness on protecting your network and provides excellent examples, in detail, on how to accomplish this." -Laura Freeman, DND

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.

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/virginia-beach-2012/event.php.

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

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

Security 504

Hacker Techniques, Exploits & Incident Handling

Six-Day Program • Mon, Aug 20 - Sat, Aug 25
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: John Strand

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.

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.

What Students Are Saying

"This course will open your eyes wider than you thought they could open. Great class."

-Migeul Escobedo, USMC

John Strand *SANS Senior Instructor*

John Strand is a senior instructor with the SANS Institute. He teaches SEC504: Hacker Techniques, Exploits, and Incident Handling; SEC560: Network Penetration Testing and Ethical Hacking; SEC580: Metasploit Kung Fu for Enterprise Pen Testing; and SEC464: Hacker Detection for System Administrators. John is the course author for SEC464 and the co-author for SEC580. When not teaching for SANS, John co-hosts PaulDotCom Security Weekly, the world's largest computer security podcast. He also is the owner of Black Hills Information Security, specializing in penetration testing and security architecture services. He has presented for the FBI, NASA, the NSA, and at DefCon. In his spare time he writes loud rock music and makes various futile attempts at fly-fishing.

Who Should Attend:

- Incident handlers
- Leaders of incident handling teams
- Penetration Testers
- Ethical Hackers
- 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

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/virginia-beach-2012/event.php.

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 • Sun, Aug 26 - Fri, Aug 31
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Christopher Crowley

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.

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.

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, following all of the steps to conduct a penetration test against a hypothetical target organization.

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.

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**

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/virginia-beach-2012/event.php.

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

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

What Students Are Saying

"This course taught me how to become a GIAC-certified professional! The instructor's professionalism and the layout/material of the course has opened up a whole new paradigm and career opportunity for me." -Gene Wikle, SAIC, Inc.

Christopher Crowley *SANS Instructor*

Mr. Crowley has 10 years 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."

Security 566

Implementing and Auditing the Twenty Critical Security Controls - In-Depth

Five-Day Program • Mon, Aug 27 - Fri, Aug 31 • 9:00am - 5:00pm
30 CPE/CMU Credits • Laptop Required • Instructor: James Tarala

In the last couple of years it has become obvious that in the world of information security, the offense is outperforming the defense. Even though budgets increase and management pays more attention to the risks of data loss and system penetration, data is still being lost and systems are still being penetrated. Over and over people are asking, "What can we practically do to protect our information?" The answer has come in the form of 20 information assurance controls known as the Consensus Audit Guidelines (CAG).

This course has been written to help those implementing or deploying a strategy for information assurance in their agency or organization by enabling them to better understand these guidelines. Specifically the course has been designed in the spirit of the offense teaching the defense to help security practitioners understand not only what to do to stop a threat, but why the threat exists and how later to audit to ensure that the organization is indeed in compliance with their standards.

At the end of Security 566, students should better understand:

- **How to create a strategy for successfully defending their data**
- **How to implement controls to prevent data from being compromised**
- **How to audit systems to ensure compliance with the standard**

And in SANS style, this course will not only provide a framework for better understanding, but will give you a hands-on approach to learning these objectives to ensure that what you learn today, you'll be able to put into practice in your organization tomorrow.

This course helps you master specific, proven techniques and tools needed to implement and audit the Top Twenty Most Critical Security Controls. These Top 20 Security Controls, listed below, are rapidly becoming accepted as the highest priority list of what must be done and proven before anything else at nearly all security conscious organizations.

The US military and other government and private organizations, including the National Security Agency (NSA), Department of Homeland Security (DHS), the U.S. Government Accountability Office (GAO) defined these top 20 controls as their consensus for the best way to block the known attacks and help find and mitigate damage from the attacks that get through.

For security professionals, the course enables you to see how to put the controls in place in your existing network though the effective and widespread use of cost-effective automation. For auditors, CIOs, and risk officers the course is the best way to understand how you will measure whether the Top 20 controls are effectively implemented. It closely reflects the Top 20 Critical Security Controls. **www.sans.org/critical-security-controls/guidelines.php**

Who Should Attend:

- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense (DoD) personnel or contractors
- Federal agencies or clients
- Private sector organizations looking to improve information assurance processes and secure their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/virginia-beach-2012/event.php.

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 times performs independent security audits and assists internal audit groups to develop 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.

Security 575 NEW COURSE!

Mobile Device Security and Ethical Hacking

Six-Day Program • Mon, Aug 20 - Sat, Aug 25
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • 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.**

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**

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/virginia-beach-2012/event.php.

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**.

Forensics 508

Advanced Computer Forensic Analysis and Incident Response

Six-Day Program • Mon, Aug 20 - Sat, Aug 25
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Michael Murr

Over the past two years, we have seen a dramatic increase in sophisticated attacks against organizations. Cyber-attacks originating from China named the Advanced Persistent Threat (APT) have proved difficult to suppress. Financial attacks from Eastern Europe and Russia obtain credit card, and financial data resulting in millions of dollars stolen. Hackivist groups attacking government and Fortune500 companies are becoming bolder.

FOR508: ADVANCED COMPUTER FORENSIC ANALYSIS AND INCIDENT RESPONSE will give you help you start to become a master of advanced incident response and computer forensics tools and techniques to investigate data breach intrusions, tech-savvy rogue employees, the advanced persistent threat, and complex digital forensic cases.

This course utilizes as uses the popular SIFT Workstation to teach investigators how to investigate sophisticated crimes. The free SIFT Workstation can match any modern forensic tool suite. It demonstrates that advanced investigations and responding to intrusions can be accomplished using cutting-edge open-source tools that are freely available and frequently updated.

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

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

The SIFT Advanced Toolkit consists of:

- **F-Response Tactical**
  - **Tactical enables investigators to access remote system via the network**
  - **Perfect for incident response investigating compromised systems**
- **SANS VMware based Forensic Analysis Workstation (SIFT Workstation)**
- **Best-selling book "File System Forensic Analysis" by Brian Carrier**
- **Bootable Forensic Distribution**
- **Course DVD loaded with case examples, tools, and documentation**

Michael Murr *SANS Certified Instructor*

Michael has been a forensic analyst with Code-X Technologies for over five years, has conducted numerous investigations and computer forensic examinations, and has performed specialized research and development. Michael has taught SANS Security 504 (Hacker Techniques, Exploits, and Incident Handling), SANS Security 508 (Computer Forensics, Investigation, and Response), and SANS Security 601 (Reverse-Engineering Malware); has led SANS@Home courses; and is a member of the GIAC Advisory Board. Currently, Michael is working on an open-source framework for developing digital forensics applications. Michael holds the GCIH, GCFA, and GREM certifications and has a degree in computer science from California State University at Channel Islands. Michael also blogs about Digital forensics on his Forensic Computing blog. **www.forensicblog.org**

Who Should Attend:

- **Incident response team members**
- **Experienced digital forensic analysts**
- **Law Enforcement Officers, Federal agents, or detectives**
- **Media exploitation analysts**
- **Red team members, penetration testers, and exploit developers**
- **Information security professionals**

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/virginia-beach-2012/event.php.

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

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

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

Management 414

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

Six-Day Program • Sun, Aug 26 - Fri, Aug 31
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: Dr. Eric Cole

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

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.**

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)

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.

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/virginia-beach-2012/event.php.

GIAC INFORMATION SECURITY PROFESSIONAL GISP

GIAC Certification
www.giac.org

Management 512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program • Mon, Aug 27 - Fri, Aug 31
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.

Knowledge Compression™

uses specialized material, in-class reviews, examinations, and test-taking training to ensure that students have a solid understanding of the material that has been presented to them.

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**

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/virginia-beach-2012/event.php.

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

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.

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 Executbytes, 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**

Audit 507

Auditing Networks, Perimeters, and Systems

Six-Day Program • Mon, Aug 20 - Sat, Aug 25
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: David Hoelzer

A great audit is more than marks on a checklist; it is the understanding of what the underlying controls are, what the best practices are, and why. This course provides a risk-driven method for tackling the enormous task of designing an enterprise security validation program. After covering a variety of high-level audit issues and general audit best practices, you will have the opportunity to dive deep into the technical how-to for determining the key controls that can be used to provide a level of assurance to any organization. Tips on how to repeatedly verify these controls and techniques for automatic compliance validation will be given from real-world examples.

While the primary audience for this course is auditors, system and security administrators will find very powerful techniques and processes for building continuous monitoring of systems and networks. Throughout the course, time is spent exploring how to determine what the correct "settings" are for an organization, how to abstract those settings into an automated process and how to ensure that the processes in the organization select and manage those settings correctly.

Every day of this course includes hands-on exercises. A variety of tools will be discussed and demonstrated during the lecture sections. These examples are then put into practice during labs so that you will leave knowing how to verify each and every control described in the class and know what to expect as audit evidence. Five of the hands-on days will give you the chance to perform a thorough technical audit of the technology being considered by applying the checklists provided in class to sample audit problems in a virtualized environment. Each student is invited to bring a Windows XP Professional or higher laptop for use during class. Macintosh computers running OS X may also be used with VMWare Fusion.

Sign up for this course and experience the mix of theory, hands-on, and practical knowledge.

Who Should Attend:

- **Auditors seeking to identify key controls in IT systems**
- **Audit professionals looking for technical details on auditing**
- **Managers responsible for overseeing the work of an audit or security team**
- **Security professionals newly tasked with audit responsibilities**
- **System and network administrators looking to better understand what an auditor is trying to achieve, how they think, and how to better prepare for an audit**
- **System and network administrators seeking to create strong change control management and detection systems for the enterprise**

What Students Are Saying

"This is the best group of instructors I've ever been exposed to."

-Mark Jeanmougin, 53.com

David Hoelzer *SANS Faculty Fellow*

David Hoelzer is a high-scoring certified SANS instructor and author of more than twenty sections of SANS courseware. He is an expert in a variety of information security fields, having served in most major roles in the IT and security industries over the past twenty-five years. Recently, David was called upon to serve as an expert witness for the Federal Trade Commission for ground-breaking GLBA Privacy Rule litigation. David has been highly involved in governance at SANS Technology Institute, serving as a member of the Curriculum Committee as well as Audit Curriculum Lead. Currently, David serves as the principal examiner and director of research for Enclave Forensics, a New York/Las Vegas based incident response and forensics company. He also serves as the chief information security officer for Cyber-Defense, an open source security software solution provider. In the past, David served as the director of the GIAC Certification program, bringing the GIAC Security Expert certification to life. David holds a BS in IT, Summa Cum Laude, having spent time either attending or consulting for Stony Brook University, Binghamton University, and American Intercontinental University. David blogs about IT Audit issues at **https://blogs.sans.org/it-audit**.

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/virginia-beach-2012/event.php.

GIAC SYSTEMS AND NETWORK AUDITOR
GSNA

GIAC Certification
www.giac.org

SANS TECHNOLOGY INSTITUTE
KNOWLEDGE FOR PEACE
SCIENTIA PRO PACE

STI Graduate School
www.sans.edu

SANS Virginia Beach 2012

Hotel Information

Event Location

Hilton Virginia Beach Oceanfront
3001 Atlantic Avenue | Virginia Beach, VA 23451
Phone: 757-213-3000

Special Hotel Rates Available

A special discounted rate of $199.00 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 July 27, 2012. To make reservations please call (800) HILTONS (445-8667) and ask for the SANS Institute group rate.

Note: You must mention that you are attending the SANS Institute training event to get the discounted rate or special amenities (such as complimentary high-speed internet) in your room. If you book outside the SANS block or stay at another hotel SANS has no influence on the terms and conditions you agreed to when making a reservation.

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 the Hilton Virginia Beach Oceanfront

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 Virginia Beach Oceanfront, 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 Virginia Beach Oceanfront that you won't want to miss!

5 Everything is in one convenient location!

SANS Virginia Beach 2012

Registration Information

SANS
The Most Trusted Source for Information and Software Security Training

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

Register online at www.sans.org/virginia-beach-2012

To register, go to www.sans.org/virginia-beach-2012

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. Cancellation requests must be received by Wednesday, August 1 by fax or mail-in order to receive a refund.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	**7/11/12**	**$500.00**	**7/25/12**	**$250.00**

Discount applies to 5- or 6-day courses.

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**

Scan the QR code to register by July 11th and

SAVE $500

on Virginia Beach courses.

www.sans.org/info/104820

To download a free QR reader
www.mobile-barcodes.com/qr-code-software

SANS

5705 Salem Run Blvd.
Suite 105
Fredericksburg, VA 22407

PROMO CODE

Register using this
Promo Code

Save $500 when you register by July 11th
www.sans.org/virginia-beach-2012

To be removed from future mailings, please contact unsubscribe@sans.org or (301) 654-SANS (7267). Please include name and complete address.