10 Great Courses – 2 Convenient Locations

Crystal City 2012

Arlington, VA

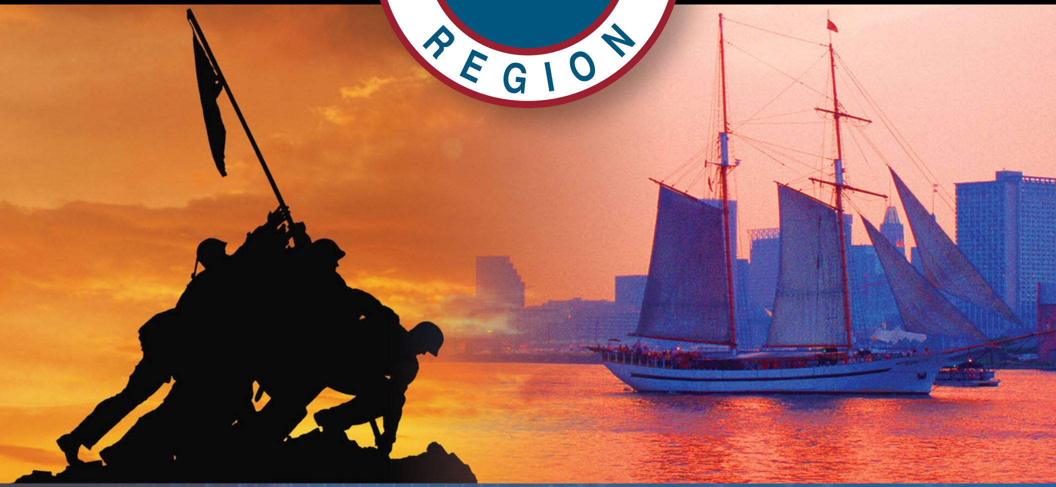
September 6-11, 2012

CAPITAL SANS REGION

Baltimore 2012

Baltimore, MD

October 15-20, 2012



Hands-on immersion training – Fall 2012:

Arlington, VA September 6-11

Intro to Information Security

Hacker Techniques, Exploits, and Incident Handling

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

Advanced Computer Forensic Analysis and Incident Response

Register at www.sans.org/crystal-city-2012

Baltimore, MD October 15-20

SANS Security Essentials Bootcamp Style

Network Penetration Testing and Ethical Hacking

SANS Security Leadership Essentials For Managers
with Knowledge Compression™

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

Mobile Device Security and
Ethical Hacking *NEW!*

Virtualization and Private
Cloud Security *NEW!*

Register at
www.sans.org/baltimore-2012

GLOBAL INFORMATION ASSURANCE CERTIFICATION GIAC www.giac.org

GIAC Approved Training

Dear Colleague,

Allow me to invite you to **SANS Capital Region Fall 2012**. SANS is presenting two weeks of training on two campuses near DC. The two events are **SANS Crystal City 2012** in Arlington, Virginia from September 6-11 and **SANS Baltimore 2012** in Baltimore, Maryland on October 15-20. Both are full SANS training events with *SANS @ Night* evening talks and *Vendor* events, which will enhance your training as part of your tuition.

Stephen Northcutt

SANS Crystal City 2012 has a unique lineup of four hands-on technical training courses from some of the best instructors in the industry. Start with the basics in Security 301 or choose our Advanced Computer Forensics course. The campus is Crystal City Marriott at Reagan National Airport, which is a short Metro ride from Washington DC and steps away from Pentagon City shopping, theaters, and some great, hip restaurants.

SANS Baltimore 2012 offers two courses in Security Management and four IT Security courses including our hot, new Security 575: Mobile Device Security and Ethical Hacking and Security 579: Virtualization and Private Cloud Security courses. The courses offered in Baltimore will follow on perfectly with those offered at Crystal City. The Hilton Baltimore serves as our campus for this event. It is located in the Inner Harbor in downtown Baltimore and is close to many of Baltimore's leading tourist attractions.

Both events include courses that will prepare you or your technical staff for *DoD Directive 8570* and *GIAC* approved certification exams along with counting toward your *STI Master's Degree*.

A look through this brochure will reveal our comprehensive course descriptions, our instructor bios, our evening events and talks that enhance your training. I think you will find the two events interesting and inviting. Select a course from each event to maximize your training in a location convenient to you! If I can help you select the course that will best boost your career, please drop me a line at **Stephen@sans.edu**.

Kind regards,

Stephen Northcutt

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

> *"Best technical SANS course I've been to."*
> -Will Stott,
> Raytheon Company

> *"Up-to-date hands-on content left me feeling confident I could start to apply my new skills back in the office."*
> -Rafe Pilling,
> Dell SecureWorks

> *"Excellent strategies to help me improve my influence at all levels of my organization."*
> -Clare Elliott, Huawei

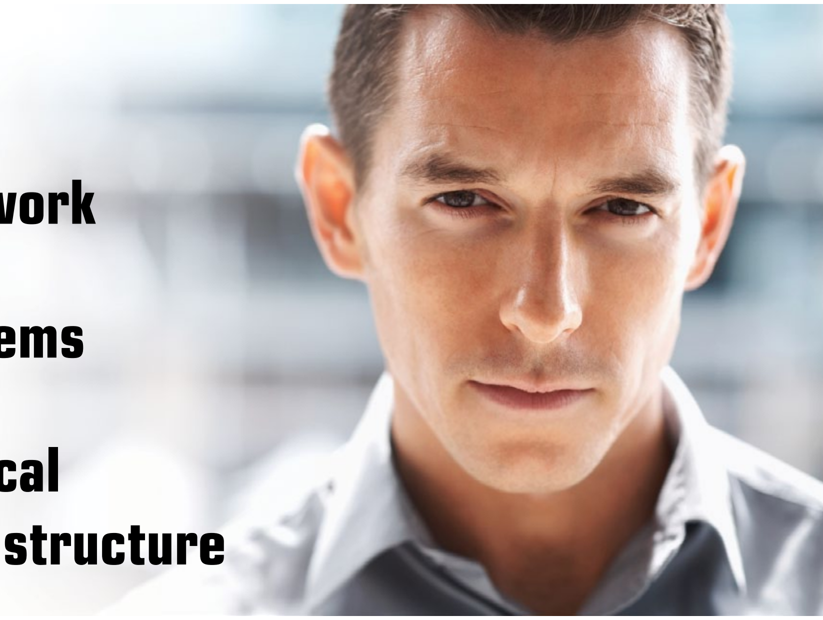
SANS Crystal City Courses (Arlington)

		THU 9/6	FRI 9/7	SAT 9/8	SUN 9/9	MON 9/10	TUE 9/11
FOR508	Advanced Computer Forensic Analysis & Incident Response	PAGE 11					
SEC301	Intro to Information Security	PAGE 4					
SEC504	Hacker Techniques, Exploits & Incident Handling	PAGE 6					
SEC566	Implementing and Auditing the Twenty Critical Security Controls - In-Depth	PAGE 8					

SANS Baltimore Courses (Baltimore)

		MON 10/15	TUE 10/16	WED 10/17	THU 10/18	FRI 10/19	SAT 10/20
MGT414	SANS® +S™ Training Program for the CISSP® Cert Exam	PAGE 12					
MGT512	SANS Security Leadership Essentials For Managers with Knowledge Compression™	PAGE 13					
SEC401	SANS Security Essentials Bootcamp Style	PAGE 5					
SEC560	Network Penetration Testing and Ethical Hacking	PAGE 7					
SEC575	Mobile Device Security and Ethical Hacking *NEW!*	PAGE 9					
SEC579	Virtualization and Private Cloud Security *NEW!*	PAGE 10					

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**

GLOBAL INFORMATION ASSURANCE CERTIFICATION
GIAC
www.giac.org

DoD 8570 Required Certifications

Come to SANS and take the training with the HIGHEST pass rate on 8570 required certifications including CISSP, GSLC, GSEC, GCIH, GCIA, GCFA, and more!

DoD Baseline IA Certifications

TECH II: GSEC   TECH III: GCIH • GCED • CISSP • CISA

MGT I: GSLC • GISF   MGT II: GSLC • CISSP   MGT III: GSLC • CISSP

Computer Environment (CE) Certifications

SEC505: GCWN   SEC506: GCUX

Information Assurance System Architecture & Engineering (IASAE) Certifications

IASAE I: CISSP   IASAE II: CISSP

By the end of 2011, all personnel performing CND-SP and IASAE roles must be certified. These courses will prepare you for the required certifications:

Computer Network Defense (CND) Certifications

CND Analyst: GCIA • GCIH   CND Incident Responder: GCIH

CND Auditor: GSNA • CISA

Training for Certifications

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

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.

CRYSTAL CITY ONLY

SIFT Workstation – The Art of Incident Response *Rob Lee*

An international team of forensics experts helped create the SANS Investigative Forensic Toolkit (SIFT) Workstation and made it available to the whole community as a public service. The free SIFT toolkit, that can match any modern forensic tool suite, is also featured in SANS' Advanced Computer Forensic Analysis and Incident Response course (FOR 508). 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. The SANS Investigative Forensic Toolkit has become the most popular download on the SANS website. Over the past year, 20,000 individuals have downloaded the SIFT workstation and has become a staple in many organizations key tools to perform investigations.

Learn how to use the SIFT workstation during Incident response in an real case where APT-like adversaries have compromised an enterprise network. This session will demonstrate some of the key tools and capabilities of the suite. You will learn how to leverage this powerful tool in your incident response capability in your organizations.

CRYSTAL CITY ONLY

Why our Defenses are Failing us. One Click is All it Takes... *Bryce Galbraith*

Organizations are spending unprecedented amounts of money in an attempt to defend their assets... yet all too often, one click is all it takes for it all to come toppling down around them. Every day we read in the news about national secrets, intellectual property, financial records & personal details being exfiltrated from the largest organizations on Earth. How is this being done? How are they bypassing our defenses (e.g. strong passwords, non-privileged accounts, anti-virus, firewalls/proxies, IDS/IPS, logging, etc.). And most importantly, what can we do about it? A keen understanding of the "true" risks we face in today's threatscape is paramount to our success.

CRYSTAL CITY & BALTIMORE

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

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

CRYSTAL CITY & BALTIMORE

GIAC Program Overview & SANS Technology Overview

For dates, times, and complete information, please visit
www.sans.org/crystal-city-2012/night.php or www.sans.org/baltimore-2012/night.php

Vendor Expo

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 a one-day vendor showcase, an added bonus to registered training event attendees.

- **Welcome Reception**
- **Tabletop Exhibits**

SANS CRYSTAL CITY 2012
September 7, 2012

SANS BALTIMORE 2012
October 16, 2012

Security 301

Intro to Information Security

Five-Day Program • Thu, Sept 6 - Mon, Sept 10
9:00am - 5:00pm • 30 CPE/CMU Credits
Laptop Required • Instructor: Dr. Eric Cole

SANS CRYSTAL CITY — Arlington, VA

This introductory certification course is the fastest way to get up to speed in information security. Written and taught by battle-scarred security veterans, this entry-level course covers a broad spectrum of security topics and is liberally sprinkled with real-life examples. A balanced mix of technical and managerial issues makes this course appealing to attendees who need to understand the salient facets of information security and risk management. Organizations often tap someone who has no information security training and say, "Congratulations, you are now a security officer." If you need to get up to speed fast, SEC301 rocks!

What Students Are Saying

"This class is great for IT professionals looking for their first step towards security awareness. I have been in IT for 17 years and I learned a lot on this first day of class." -Paul Beninati, EMC

We begin by covering basic terminology and concepts and then move to the basics of computers and networking, discussing Internet Protocol, routing Domain Name Service, and network devices. We cover the basics of cryptography and wireless networking; then we look at policy as a tool to effect change in your organization. In the final day of the course, we put it all together with an introduction to defense in depth.

If you're a newcomer to the field of information security, this is the course for you! You will develop the skills to bridge the gap that often exists between managers and system administrators and learn to communicate effectively with personnel in all departments and at all levels within your organization.

This is the course SANS offers for the professional just starting out in security. If you have experience in the field, please consider our more advanced offerings, such as SEC401: SANS Security Essentials Bootcamp Style.

Who Should Attend:

- **Persons new to information technology (IT) who need to understand the basics of information assurance, computer networking, cryptography, and risk evaluation**
- **Managers and information security officers who need a basic understanding of risk management and the tradeoffs between confidentiality, integrity, and availability**
- **Managers, administrators, and auditors who need to draft, update, implement, or enforce policy**

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/crystal-city-2012/event.php.

GIAC Certification
www.giac.org

Security 401

SANS Security Essentials Bootcamp Style

Six-Day Program • Mon, Oct 15 - Sat, Oct 20
9:00am - 7:00pm (Days 1-5) • 9:00am - 5:00pm (Day 6)
46 CPE/CMU Credits • Laptop Required
Instructor: Dr. Eric Cole

SANS BALTIMORE Baltimore, MD

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**

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**

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.

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/baltimore-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 • Thu, Sept 6 - Mon, Sept 11
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Bryce Galbraith

SANS CRYSTAL CITY Arlington, VA

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.

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**

What Students Are Saying

"This course will open your eyes wider than you thought they could open. Great class." -Migeul Escobedo, USMC

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.

Bryce Galbraith *SANS Certified Instructor*

As a contributing author of the internationally bestselling 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**.

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/crystal-city-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 • Mon, Oct 15 - Sat, Oct 20
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Christopher Crowley

SANS BALTIMORE Baltimore, MD

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.

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."

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/ baltimore-2012/event.php.

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

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

Security 566

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

Five-Day Program • Thu, Sept 6 - Mon, Sept 10 • 9:00am - 5:00pm
30 CPE/CMU Credits • Laptop Required • Instructor: James Tarala

SANS CRYSTAL CITY Arlington, VA

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/crystal-city-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, Oct 15 - Sat, Oct 20
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Joshua Wright

SANS BALTIMORE Baltimore, MD

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/baltimore-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**.

Security 579 NEW COURSE!

Virtualization and Private Cloud Security

Six-Day Program • Mon, Oct 15 - Sat, Oct 20
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Provided • Instructor: James Tarala

SANS BALTIMORE Baltimore, MD

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.

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 entire gamut of components will be covered ranging from hypervisor platforms to virtual networking, storage security to locking down the individual virtual machine files. We'll describe how to secure the management interfaces and servers, delve into virtual desktop infrastructure (VDI), and go in-depth on what to consider when building a private cloud from existing virtualization architecture. Finally, we'll look at integrating virtual firewalls and intrusion detection systems into the new architecture for access control and network monitoring.

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

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

The next two days will help you adapt your existing security policies and practices to the new virtualized or cloud-based infrastructure. We'll show you how to design a foundational risk assessment program, and then build on this with policies, governance, and compliance considerations within your environment. We'll cover auditing and assessment of your virtualized assets, with a session on scripting that will help you put this into practice right away. Then we'll go in-depth into data security within a private cloud environment, discussing encryption and data lifecycle management techniques that will help you keep up with data that is much more mobile than ever before. Identity and Access Management (IAM) within a virtualized/cloud environment will be touched on, and we'll wrap up with a thorough session on disaster recovery and business continuity planning that leverages and benefits from virtualization and cloud-based technology.

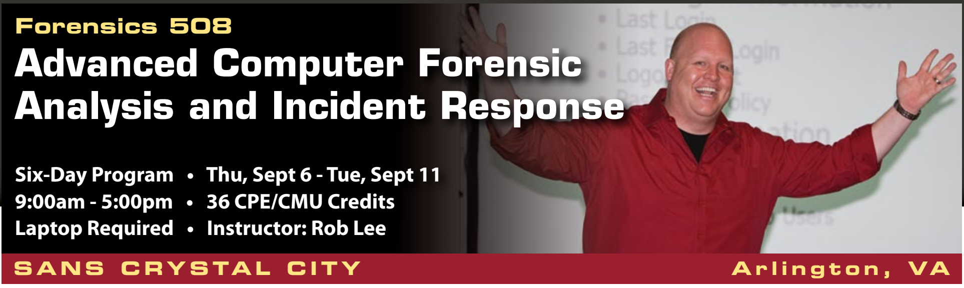
The final two days go into detail on offense and defense - how can we assess virtualized environment using scanning and pen testing tools and techniques, and how do things change when we move to a cloud model? We'll cover a variety of scanners and vulnerability management tools and practices, and then take a hard look at virtualization vulnerabilities, exploits, and toolkits for pen testing that we can put to use in class. Once we cover the offense, we'll take the opposite approach and go into detail on performing intrusion detection and logging within the virtual environment, as well as covering anti-malware advances and changes within virtual infrastructure. We'll wrap up the session with coverage of incident handling within virtual and cloud environments, as well as adapting forensics processes and tools to ensure we can maintain chain-of-custody and perform detailed analysis of virtualized assets.

James Tarala *SANS Senior Instructor*

James Tarala's bio can be found on page 8.

Forensics 508

Advanced Computer Forensic Analysis and Incident Response



Six-Day Program • Thu, Sept 6 - Tue, Sept 11
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Rob Lee

SANS CRYSTAL CITY Arlington, VA

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**

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**.

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/crystal-city-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 • Mon, Oct 15 - Sat, Oct 20
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: Ted Demopoulos

SANS BALTIMORE Baltimore, MD

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.

Note: The CISSP® exam is NOT provided as part of the training.

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)

Ted Demopoulos *SANS Certified Instructor*

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

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/baltimore-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, Oct 15 - Fri, Oct 19
9:00am - 6:00pm (Days 1-4) • 9:00am - 5:00pm (Day 5)
33 CPE/CMU Credits • Laptop NOT Required
Instructor: Stephen Northcutt

SANS BALTIMORE Baltimore, MD

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/baltimore-2012/event.php.

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 40 in-depth interviews with leaders in the security industry, from CEOs of security product companies to the most well-known practitioners in order to research the competencies required to be a successful leader in the security field. He maintains the SANS Leadership Laboratory, where research on these competencies is posted as well as SANS Security Musings. 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**

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 STI program prepares me in both technical aptitude and leadership skills. The instructors have extensive real-world experience - you walk out of every class with skills you can use immediately."*
>
> -Courtney Imbert, MSISE Student

Five of the courses being offered at SANS Crystal City 2012 and SANS Baltimore 2012 may be applied towards an STI Master's Degree.

SANS Technology Institute
Knowledge for Peace
Scientia Pro Pace

www.sans.edu

info@sans.edu

720.941.4932

SANS CYBER GUARDIAN PROGRAM

www.sans.org/cyber-guardian

Become a SANS Cyber Guardian and stay one step ahead of the threats as well as know what to do when a breach occurs.

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.

How the Program Works

This program begins with hands-on core courses that will build and increase your knowledge and skills with each course. 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

- **A 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 and 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 (GCWN)

SEC506: Securing Linux/Unix (GCUX)

Red Team Courses

SEC542: Web App Penetration Testing and Ethical Hacking (GWAPT)

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

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

Learn more about the SANS Cyber Guardian Program at www.sans.org/cyber-guardian

SANS Training Formats

Training

Training Events

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

Community

Community

Community SANS

www.sans.org/community

OnSite

OnSite

Live Training at Your Location

www.sans.org/onsite

Mentor

Mentor

Intimate Live Instruction

www.sans.org/mentor

Summit

Summit Series

Live IT Security Summits and Training

www.sans.org/summit

OnDemand

OnDemand

All the Course Content at Your Own Pace

www.sans.org/ondemand

vLive

vLive

Virtual Live Training from Your Home or Office

www.sans.org/virtual-training/vlive

Simulcast

Simulcast

Attend Event Training From Your Location

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

SelfStudy

SelfStudy

Independent Study with Books and MP3s

www.sans.org/selfstudy

Future SANS Training Events

SANSFIRE 2012

Washington, DC | July 6-15, 2012
www.sans.org/sansfire-2012

Plus: Security Impact of IPv6 Summit 2012
www.sans.org/ipv6-summit-2012

SANS San Francisco 2012

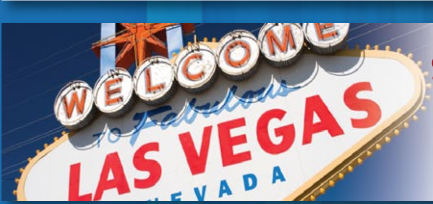
San Francisco, CA
July 30 - August 6, 2012
www.sans.org/san-francisco-2012

SANS Boston 2012

Boston, MA | August 6-11, 2012
www.sans.org/boston-2012

SANS Virginia Beach 2012

Virginia Beach, VA
August 20-31, 2012
www.sans.org/virginia-beach-2012



SANS Network Security 2012

Las Vegas, NV | September 16-24, 2012
www.sans.org/network-security-2012

SANS CyberCon 2012

Virtual Conference | October 8-13, 2012
www.sans.org/cybercon-2012

SANS Seattle 2012

Seattle, WA | October 14-19, 2012
www.sans.org/seattle-2012

SANS Chicago 2012

Chicago, IL
October 27 - November 5, 2012
www.sans.org/chicago-2012

SANS CDI 2012

Washington, DC | December 7-16, 2012
www.sans.org/cyber-defense-initiative-2012

Community SANS Training Events

Raleigh, NC

July 16-21, 2012 | Course: SEC504

Atlanta , GA

July 30-31 | Course: SEC464

Fort Lauderdale, FL

July 30-31, 2012 | Course: SEC464

Pensacola, FL

August 6-11, 2012 | Course: SEC401

Baltimore, MD

August 6-10, 2012 | Course: FOR610

Toronto, ON

August 13-18, 2012 | Course: SEC401

Annapolis, MD

September 10-15, 2012 | Course: SEC560

Atlanta, GA

September 10-15, 2012 | Course: SEC401

Montreal, QC

September 24-29, 2012 | Course: SEC560

Quantico, VA

October 15-19, 2012 | Course: FOR558

Quantico, VA

October 22-27, 2012 | Course: FOR508

Boston, MA

November 12-17, 2012 | Course: MGT414

Reston, VA

November 12-17, 2012 | Course: FOR408

Ottawa, ON

November 19-23, 2012 | Course: SEC401

SANS Crystal City 2012

Hotel Information

Event Location:

Crystal City Marriott at Reagan National Airport
1999 Jefferson Davis Highway | Arlington, VA 22202-3526
Tel: 703-413-5500
Web: www.marriott.com/hotels/travel/wascc-crystal-city-marriott-at-reagan-national-airport

Special Hotel Rates Available

A special discount rate of $179 S/D will be honored based on space availability. This rate includes high-speed Internet in your room. Make your reservations now; this special rate is only available through Saturday, August 11, 2012. To make reservations, please call 703-413-5500 and ask for the SANS Crystal City 2012 group rate. A limited number of Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government 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 Crystal City Marriott

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 Crystal City Marriott, 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 Crystal City Marriott that you won't want to miss!
5. Everything is in one convenient location!

SANS Crystal City 2012

Registration Information

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

Register online at www.sans.org/crystal-city-2012

SANS
The Most Trusted Source for Information and Software Security Training

To register, go to www.sans.org/crystal-city-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 15 by fax or mail-in order to receive a refund.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	7/25/12	$500.00	8/8/12	$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**

SANS Baltimore 2012

Hotel Information

Event Location:
Hilton Baltimore
401 West Pratt Street | Baltimore, MD 21201
Tel: 443-573-8700
Web: http://www.roomstays.com/hotel/34552

Special Hotel Rates Available

A special discounted rate of $215.00 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 September 21, 2012. To make reservations please call (800) HILTONS (800-445-8667) and ask for the SANS 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 Baltimore

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 Baltimore, 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 Baltimore that you won't want to miss!
5. Everything is in one convenient location!

SANS Baltimore 2012

Registration Information

We recommend you register early to ensure you get your first choice of courses.
Register online at www.sans.org/baltimore-2012

SANS
The Most Trusted Source for Information and Software Security Training

To register, go to www.sans.org/baltimore-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, September 26 by fax or mail-in order to receive a refund.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	9/5/12	$500.00	9/19/12	$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 25th and

SAVE $500

on Crystal City 2012 courses.

www.sans.org/info/105910

And register by Sept. 5th and

SAVE $500

on Baltimore 2012 courses.

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

SANS
5705 Salem Run Blvd.
Suite 105
Fredericksburg, VA 22407

Save $500 when you register early!

PROMO CODE

Register using this Promo Code

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