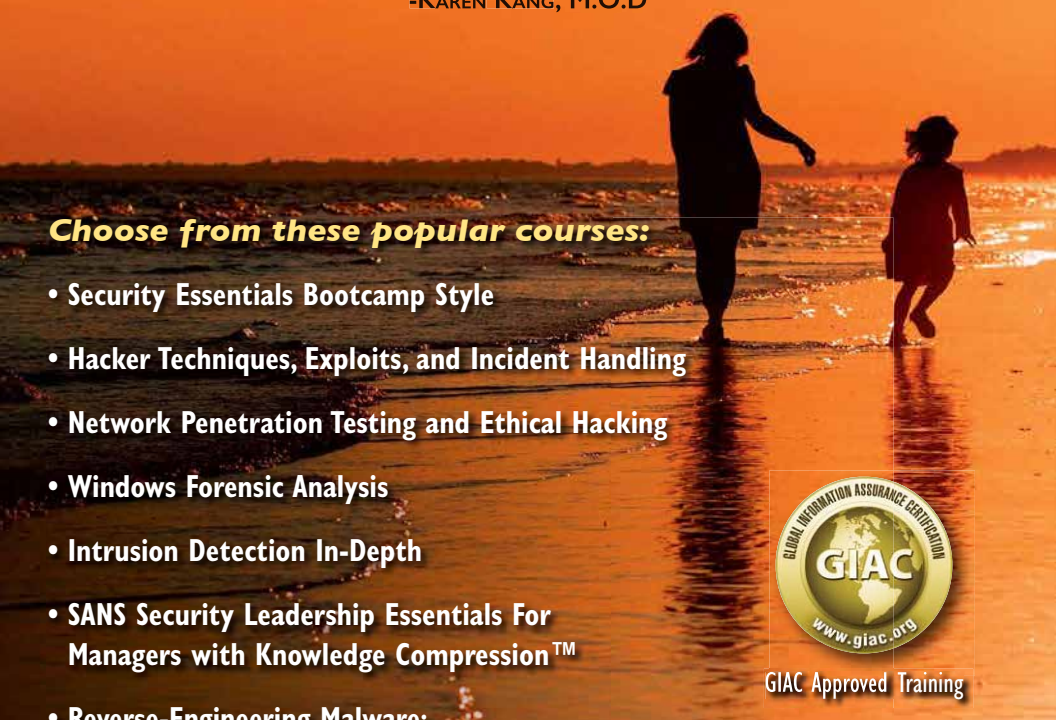
THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS Virginia Beach 2014

Virginia Beach, VA August 18-29

"This information is valuable not just for corporate use, but also for personal home security. Anyone and everyone should attend SANS courses. If you have a computer, laptop, tablet, or phone, you need this knowledge!"

-Karen Kang, M.O.D



Choose from these popular courses:

- Security Essentials Bootcamp Style
- Hacker Techniques, Exploits, and Incident Handling
- Network Penetration Testing and Ethical Hacking
- Windows Forensic Analysis
- Intrusion Detection In-Depth
- SANS Security Leadership Essentials For Managers with Knowledge Compression™
- Reverse-Engineering Malware: Malware Analysis Tools and Techniques
- Advanced Computer Forensic Analysis and Incident Response
- Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
- Virtualization and Private Cloud Security

GIAC Approved Training

FEATURING

NETWARS

Register at www.sans.org/event/virginia-beach-2014

Save $400 by registering early!

See page 17 for more details.

We are once again offering the opportunity to take two weeks of back-to-back courses at **SANS Virginia Beach 2014**, **August 18-29**. This event has been a hit year after year at this popular beach location, so don't miss the chance for a late-summer family vacation with two weeks of SANS training!

Attend one or two of our 10 courses from three disciplines – IT security, security management, and computer 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 some much needed relaxation! This is a great opportunity to take courses with some of our top instructors and the lineup includes Stephen Northcutt and David Hoelzer, Rob Lee, Ed Skoudis, Paul A. Henry, Mike Poor, Stephen Sims, Kevin Fiscus, Keith Palmgren, Mike Pilkington, and Anuj Soni. See this brochure for a complete schedule, course descriptions, instructor bios, and also information about earning your master's degree in Information Security through the **SANS Technology Institute** (STI), the only accredited graduate institution focused solely on cybersecurity. Nine of our Virginia Beach courses offer a **GIAC Certification** so be sure to look at that information as well.

Don't miss our bonus evening talks with keynote presentations. These unique, late-breaking sessions, presented by our instructors and other industry experts, will add to your learning experience at no additional cost. Offered for the first time in Virginia Beach, our popular **NetWars – Tournament Competition** to be held on August 21-22 and August 27-28! NetWars is a hands-on, interactive learning environment designed to represent real-world security concerns, weaknesses and their resolutions. See page 11 for details.

Located on the three-mile long Virginia Beach boardwalk and the ocean front, the **Hilton Virginia Beach Oceanfront** is right next to Neptune's Park and the Shoppes at 31 Ocean. With 35 miles of beaches nearby, this campus offers the perfect end-of-summer destination. The beach and boardwalk activities are endless! Rent a bike and cycle along the Boardwalk, watch street performers, ride carnival rides, walk the hub, try stand-up paddle boarding in secluded waters, or observe the dolphins in their natural habitat.

This event has a history of filling up fast, so register and book your room as early as possible. A discounted room rate of $199 S/D is available to SANS students based on space availability. This rate includes high-speed Internet in your room and is only available through July 25, 2014. Government per diem rooms are available with proper ID. See our website for full details.

Register and pay for any course by June 25 to receive a $400 tuition fee discount! Start making your training and travel plans now and let your colleagues and friends know about SANS Virginia Beach 2014.

Here's what SANS alumni have said about the value of SANS training:

"SANS instructors are the best in the IT world. Their field knowledge plus delivery makes SANS the premier certification organization."
-Dave Dalton, Sentara Healthcare

"Excellent course, and excellent instructor. I'm getting a lot of relevant information."
-Paul White, WUSAO

SC MAGAZINE AWARDS 2014 WINNER
Honored in the U.S.

Courses-at-a-Glance

	MON 8/18	TUE 8/19	WED 8/20	THU 8/21	FRI 8/22	SAT 8/23	SUN 8/24	MON 8/25	TUE 8/26	WED 8/27	THU 8/28	FRI 8/29
SEC401 Security Essentials Bootcamp Style	Page 1											
SEC503 Intrusion Detection In-Depth							Page 2					
SEC504 Hacker Techniques, Exploits, and Incident Handling							Page 3					
SEC560 Network Penetration Testing and Ethical Hacking	Page 4											
SEC579 Virtualization and Private Cloud Security	Page 5											
SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking							Page 6					
FOR408 Windows Forensic Analysis	Page 7											
FOR508 Advanced Computer Forensic Analysis and Incident Response							Page 8					
FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques	Page 9											
MGT512 SANS Security Leadership Essentials For Managers with Knowledge Compression™								Page 10				

@SANSInstitute *Join the conversation:* #SANSVABeach

SECURITY 401

Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Aug 18 - Sat, Aug 23
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPE/CMU Credits
Instructor: Keith Palmgren

- GIAC Cert: GSEC
- Masters Program
- Cyber Guardian
- DoDD 8570

It seems wherever you turn organizations are being broken into, and the fundamental question that everyone wants answered is: Why? Why is it that some organizations get broken into and others do not? Organizations are spending millions of dollars on security and are still compromised. The problem is they are doing good things but not the right things. Good things will lay a solid foundation, but the right things will stop your organization from being headline news in the *Wall Street Journal*. SEC401's focus is to teach individuals the essential skills, methods, tricks, tools and techniques needed to protect and secure an organization's critical information assets and business systems.

This course teaches you the right things that need to be done to keep an organization secure. The focus is not on theory but practical hands-on tools and methods that can be directly applied when a student goes back to work in order to prevent all levels of attacks, including the APT (advanced persistent threat). In addition to hands-on skills, we will teach you how to put all of the pieces together to build a security roadmap that can scale today and into the future. When you leave our training we promise that you will have the techniques that you can implement today and tomorrow to keep your organization at the cutting edge of cyber security. Most importantly, your organization will be secure because students will have the skill sets to use the tools to implement effective security.

Who Should Attend

- Security professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Operations personnel who do not have security as their primary job function but need an understanding of security to be effective
- IT engineers and supervisors who need to know how to build a defensible network against attacks

"Keith injected a fair amount of humor into his lecture, and this definitely helped keep my attention."
-Keith Nelson, Honeywell

"SEC401 is a MUST for all sys admins who want to keep a job."
-Jaid Keenan, U.S. Navy

Before your organization spends a dollar of its IT budget or allocates any resources or time to anything in the name of cyber security, three questions must be answered:

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

Security is all about making sure you are focusing on the right areas of defense. By attending SEC401, you will learn the language and underlying theory of computer security. In addition, you will gain the essential, up-to-the-minute knowledge and skills required for effective security if you are given the responsibility for securing systems and/or organizations.

www.giac.org

www.sans.edu

www.sans.org/
cyber-guardian


www.sans.org/8570

"SEC401 is a great place to start for a wide range of topics. It IS in-depth, and leaves you wanting more."
-Todd Condit, Samaritan Health

Keith Palmgren *SANS Certified Instructor*

Keith Palmgren is an IT Security professional with 26 years of experience in the field. He began his career with the U.S. Air Force working with cryptographic keys & codes management. He also worked in, what was at the time, the newly-formed computer security department. Following the Air Force, Keith worked as an MIS director for a small company before joining AT&T/Lucent as a senior security architect working on engagements with the DoD and the National Security Agency. As security practice manager for both Sprint and Netigy, Keith built and ran the security consulting practice – responsible for all security consulting world-wide and for leading dozens of security professionals on many consulting engagements across all business spectrums. For the last several years, Keith has run his own company, NetIP, Inc. He divides his time between consulting, training, and freelance writing projects. As a trainer, Keith has satisfied the needs of nearly 5,000 IT professionals and authored a total of 17 training courses. Keith currently holds the CISSP, GSEC, CEH, Security+, Network+, A+, and CTT+ certifications.

SECURITY 503

Intrusion Detection In-Depth

SANS

Six-Day Program
Sun, Aug 24 - Fri, Aug 29
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor:
Mike Poor

- GIAC Cert: GCIA
- Masters Program
- Cyber Guardian
- DoDD 8570

Who Should Attend

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

If you have an inkling of awareness of security (even my elderly aunt knows about the perils of the Interweb!), you often hear the disconcerting news about another high-profile company getting compromised. The security landscape is continually changing from what was once only perimeter protection to a current exposure of always-connected and often-vulnerable. Along with this is a great demand for security savvy employees who can help to detect and prevent intrusions. That is our goal in the **Intrusion Detection In-Depth** course – to acquaint you with the core knowledge, tools, and techniques to prepare you to defend your networks.

This course spans a wide variety of topics from foundational material such as TCP/IP to detecting an intrusion, building in breadth and depth along the way. It's kind of like the "soup to nuts" or bits to bytes to packets to flow of traffic analysis.

Hands-on exercises supplement the course book material, allowing you to transfer the knowledge in your head to your keyboard using the Packetrix VMware distribution created by industry practitioner and SANS instructor Mike Poor. As the Packetrix name implies, the distribution contains many of the tricks of the trade to perform packet and traffic analysis. All exercises have two different approaches. A more basic one that assists you by giving hints for answering the questions. Students who feel that they would like more guidance can use this approach. The second approach provides no hints, permitting a student who may already know the material or who has quickly mastered new material a more challenging experience. Additionally, there is an "extra credit" stumper question for each exercise intended to challenge the most advanced student.

By week's end, your head should be overflowing with newly gained knowledge and skills; and your luggage should be swollen with course book material that didn't quite get absorbed into your brain during this intense week of learning. This course will enable you to "hit the ground running" once returning to a live environment.

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8570

"What a fabulous class. Mike is an excellent instructor. Best training on the market."
-Rob McBee, SMUD

"Mike's knowledge and energy is infectious. Time really flies with his interesting style."
-Andy Weiser, Consumer Energy

"Mike is great, very patient and knowledgeable."
-Adam Hugoboom, Marine Corps

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 its 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. @Mike_Poor

SECURITY 504

Hacker Techniques, Exploits, and Incident Handling

SANS sans.org

Six-Day Program
Sun, Aug 24 - Fri, Aug 29
9:00am - 6:30pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits
Laptop Required
Instructor: Kevin Fiscus

- GIAC Cert: GCIH
- Masters Program
- Cyber Guardian
- DoDD 8570

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

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.

Who Should Attend

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

"The labs in SEC504 were great, and they were real-world activities that I will be able to use going forward."
-Larry Petty, Tribridge

"SEC504 will be beneficial in broadening my security career. The instructor was excellent."
-Christian Pernell, 1st IO Command

GCIH
www.giac.org

SANS INSTITUTE
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

www.sans.org/8570

Kevin Fiscus *SANS Certified Instructor*

Kevin Fiscus is the founder of and lead consultant for Cyber Defense Advisors where he performs security and risk assessments, vulnerability and penetration testing, security program design, policy development and security awareness with a focus on serving the needs of small and mid-sized organizations. Kevin has over 20 years of IT experience and has focused exclusively on information security for the past 12. Kevin currently holds the CISA, GPEN, GREM, GCFA-Gold, GCIA-Gold, GCIH, GAWN, GCWN, GCSC-Gold, GSEC, SCSA, RCSE, and SnortCP certifications and is proud to have earned the top information security certification in the industry, the GIAC Security Expert. Kevin has also achieved the distinctive title of SANS Cyber Guardian for both red team and blue team. Kevin has taught many of SANS most popular classes including SEC401, SEC464, SEC504, SEC542, SEC560, SEC575, FOR508, and MGT414. In addition to his security work, he is a proud husband and father of two children. @kevinbfiscus

SECURITY 560

Network Penetration Testing and Ethical Hacking

SANS sans.org

Six-Day Program
Mon, Aug 18 - Sat, Aug 23
9:00am - 6:30pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits
Laptop Required
Instructor: Ed Skoudis

- GIAC Cert: GPEN
- Masters Program
- Cyber Guardian

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

Who Should Attend

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

"Phenomenal speaking skills, Ed! Very engaging, excellent explanations and examples!"
-Travis Farral,
XTO Energy/ExxonMobile

"Ed Skoudis' dedication to preparation is demonstrated by the fact that all the labs work as described and directly complement the course content. Excellent!"
-Chris Shipp, DM Petroeum

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. 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.

www.giac.org

www.sans.edu

www.sans.org/
cyber-guardian

Ed Skoudis *SANS Faculty Fellow*

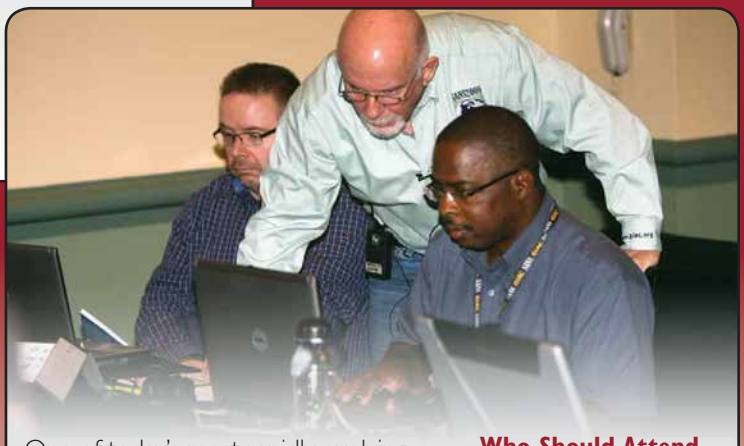
Ed Skoudis is the founder of Counter Hack, an innovative organization that designs, builds, and operates popular infosec challenges and simulations including CyberCity, NetWars, Cyber Quests, and Cyber Foundations. As director of the CyberCity project, Ed oversees the development of missions which help train cyber warriors in how to defend the kinetic assets of a physical, miniaturized city. Ed's expertise includes hacker attacks and defenses, incident response, and malware analysis, with over fifteen years of experience in information security. Ed authored and regularly teaches the SANS courses on network penetration testing (Security 560) and incident response (Security 504), helping over three thousand information security professionals each year improve their skills and abilities to defend their networks. He has performed numerous security assessments; conducted exhaustive anti-virus, anti-spyware, Virtual Machine, and IPS research; and responded to computer attacks for clients in government, military, financial, high technology, healthcare, and other industries. Previously, Ed served as a security consultant with InGuardians, International Network Services (INS), Global Integrity, Predictive Systems, SAIC, and Bell Communications Research (Bellcore). Ed also blogs about command line tips and penetration testing. @edskoudis

SECURITY 579

Virtualization and Private Cloud Security

Six-Day Program
Mon, Aug 18 - Sat, Aug 23
9:00am - 5:00pm
Laptop Required
36 CPE/CMU Credits
Instructor: Paul A. Henry

SANS
sans.org



"SEC579 gives a great overview of the virtual environments and how I, as an admin or security professional, can secure it."
-Josh Wickern, Overstock.com

"Paul Henry is an excellent instructor and I was never bored on any of the class days. Lots of hands-on and the instructor had real-world experiences! Excellent use of my time."
-Colleen Bolan, HP

"SEC579 provided extensive insight into the security problems faced in virtual infrastructure."
-Jarred House, Dillard's

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.

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

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

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

Paul A. Henry *SANS Senior Instructor*

Paul Henry is a Senior Instructor with the SANS Institute and one of the world's foremost global information security and computer forensic experts with more than 20 years' experience managing security initiatives for Global 2000 enterprises and government organizations worldwide. Paul is a principal at vNet Security, LLC and is keeping a finger on the pulse of network security as the security and forensic analyst at Lumension Security. Throughout his career, Paul has played a key strategic role in launching new network security initiatives to meet our ever-changing threat landscape. Paul also advises and consults on some of the world's most challenging and high-risk information security projects, including the National Banking System in Saudi Arabia, the Reserve Bank of Australia, the Department of Defense's Satellite Data Project (USA), and both government as well as telecommunications projects throughout Southeast Asia. @phenrycissp

SECURITY 660

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

SANS
sans.org

Six-Day Program
Sun, Aug 24 - Fri, Aug 29
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPE/CMU Credits
Instructor: Stephen Sims
- GIAC Cert: GXPN
- Masters Program

Who Should Attend

- Network and systems penetration testers
- Incident handlers
- Application developers
- IDS engineers

This course is designed as a logical progression point for those who have completed **SANS SEC560: Network Penetration Testing and Ethical Hacking**, or for those with existing penetration testing experience. Students with the prerequisite knowledge to take this course will walk through dozens of real-world attacks used by the most seasoned penetration testers. The methodology of a given attack is discussed, followed by exercises in a real-world lab environment to solidify advanced concepts and allow for the immediate application of techniques in the workplace. Each day includes a two-hour evening bootcamp to allow for additional mastery of the techniques discussed and even more hands-on exercises. A sample of topics covered include weaponizing Python for penetration testers, attacks against network access control (NAC) and VLAN manipulation, network device exploitation, breaking out of Linux and Windows restricted environments, IPv6, Linux privilege escalation and exploit-writing, testing cryptographic implementations, fuzzing, defeating modern OS controls such as ASLR and DEP, Return Oriented Programming (ROP), Windows exploit-writing, and much more!

It is well-known that attackers are becoming cleverer and their attacks more complex. In order to keep up with the latest attack methods, one must have a strong desire to learn, the support of others, and the opportunity to practice and build experience. SEC660 engages attendees with in-depth knowledge of the most prominent and powerful attack vectors and an environment to perform these attacks in numerous hands-on scenarios. This course goes far beyond simple scanning for low-hanging fruit, and shows penetration testers how to model the abilities of an advanced attacker to find significant flaws in a target environment and demonstrate the business risk associated with these flaws.

www.giac.org

www.sans.edu

"Stephen gave an awesome presentation that makes the course so interesting. He gave very good examples to explain difficult terms."
-Alex, IDA

"SEC660 has been nothing less than excellent. The instructor had extensive knowledge covering all aspects of the topics covered and then some."
-Brian Anderson, Northrop Grumman Corporation

"Stephen Sims is super skilled! SANS has the brightest!!!"
-Mike Evans, Alaska Airlines

Stephen Sims *SANS Senior Instructor*

Stephen Sims is an industry expert with over 15 years of experience in information technology and security. Stephen currently works out of San Francisco as a consultant. He has spent many years performing security architecture, exploit development, reverse engineering, and penetration testing. Stephen has an MS in information assurance from Norwich University. He is the author of SANS' only 700-level course, SEC760: Advanced Exploit Development for Penetration Testers, which concentrates on complex heap overflows, patch diffing, and client-side exploits. Stephen is also the lead author on SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking. He holds the GIAC Security Expert (GSE) certification as well as the CISSP, CISA, Immunity NOP, and many other certifications. In his spare time Stephen enjoys snowboarding and writing music.

FORENSICS 408

Windows Forensic Analysis

SANS

Six-Day Program
Mon, Aug 18 - Sat, Aug 23
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Mike Pilkington
- GIAC Cert: GCFE
- Masters Program

Master Windows Forensics – What Do You Want to Uncover Today?

Every organization will deal with cyber crime occurring on the latest Windows operating systems. Analysts will investigate crimes including fraud, insider threats, industrial espionage, traditional crimes, and computer hacking. Government agencies use media exploitation of Windows systems to recover key intelligence available on adversary systems. To help solve these cases, organizations are hiring digital forensic professionals, investigators, and agents to uncover what happened on a system.

Who Should Attend

- Information technology professionals
- Incident response team members
- Law enforcement officers, federal agents, or detectives
- Media exploitation analysts
- Information security managers
- Information technology lawyers and paralegals
- Anyone interested in computer forensic investigations

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

FOR408: Windows Forensic Analysis focuses on the critical digital forensics knowledge of the Microsoft Windows operating system. You will learn how computer forensic analysts focus on collecting and analyzing data from computer systems to track user-based activity that can be used in internal investigations or civil/criminal litigation.

Proper analysis requires real data for students to examine. The completely updated FOR408 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 8.1, Office365, Skydrive, Sharepoint, Exchange Online, and Windows Phone). This will ensure that students are prepared to investigate the latest trends and capabilities they might encounter. In addition, students will have labs that cover both Windows XP and Windows 7 artifacts.

This course utilizes a brand-new Windows 8.1 based case exercise that took over 6 months to create the data. Realistic example case data takes months to create in real time correctly. The example case is a Windows 8.1 based image that has the subject utilize Windows Phone, Office 365, Sharepoint, MS Portal Online, Skydrive/ Onedrive, Dropbox, and USB external devices. Our development team spent months creating an incredibly realistic scenario. The case demonstrates the latest technologies an investigator would encounter analyzing a Windows operating system. The brand new case workbook, will detail the step-by-step each investigator could follow to examine the latest technologies including Windows 8.1.

www.giac.org

www.sans.edu

"Mike was amazing. His knowledge and helpful attitude made it a great week. I look forward to taking a class from him again in the future."
-Matt Edmondson, DHS

"I enjoyed understanding the legal aspects of FOR408 and the 'why we do what we do' preparation steps."
-Matt Campbell, Honeywell International Inc.

"As a member of the IR team, this course will aid in investing compromised hosts."
-Mike Pichler -URS Corp.

Mike Pilkington *SANS Instructor*

Mike Pilkington is a senior security consultant for a Fortune 500 company in the oil & gas industry. He has been an IT professional since graduating in 1996 from the University of Texas with a B.S. in Mechanical Engineering. Since joining his company in 1997, he has been involved in software quality assurance, systems administration, network administration, and information security. Outside of his normal work schedule, Mike has also been involved with the SANS Institute as a mentor and instructor in the digital forensics program. @mikepilkington

FORENSICS 508

Advanced Computer Forensic Analysis and Incident Response

SANS
sans.org

Six-Day Program
Sun, Aug 24 - Fri, Aug 29
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Rob Lee

- GIAC Cert: GCFA
- Masters Program
- Cyber Guardian
- DoDD 8570

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

What you will receive with this course

- SIFT Workstation Virtual Machine
- F-Response TACTICAL Edition with a 2 year license
- Best-selling book "File System Forensic Analysis" by Brian Carrier
- Course DVD loaded with case examples, additional tools, and documentation

"I've taken other network intrusion classes but nothing this in depth. FOR508 is outstanding!"
-Craig Goldsmith, OCRCFL

This course focuses on providing incident responders with the necessary skills to hunt down and counter a wide range of threats within enterprise networks, including economic espionage, hactivism, and financial crime syndicates. The completely updated FOR508 addresses today's incidents by providing real-life, hands-on response tactics.

Who Should Attend

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

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

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

FOR508 will help you determine:

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

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

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

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8570

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 crime investigations and an incident response team. 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. @robtlee,sansforensics

FORENSICS 610

Reverse-Engineering Malware: Malware Analysis Tools and Techniques

SANS sans.org

Six-Day Program
Mon, Aug 18 - Sat, Aug 23
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Anuj Soni
- GIAC Cert: GREM
- Masters Program

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

This popular malware analysis course has helped forensic investigators, malware specialists, incident responders, and IT administrators assess malware threats. The course teaches a practical approach to examining malicious programs—spyware, bots, trojans, etc.—that target or run on Microsoft Windows. This training also looks at reversing web-based malware, such as JavaScript and Flash files, as well as malicious document files. By the end of the course, you'll learn how to reverse-engineer malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and other tools for turning malware inside-out!

Who Should Attend

- Professionals with responsibilities in the areas of incident response, forensic investigation, Windows security, and system administration
- Professionals who deal with incidents involving malware and would like to learn how to understand key aspects of malicious programs
- Individuals who attended the course have experimented with aspects of malware analysis prior to the course and were looking to formalize and expand their malware forensics expertise

The malware analysis process taught in this class helps incident responders assess the severity and repercussions of a situation that involves malicious software. It also assists in determining how to contain the incident and plan recovery steps. Forensics investigators also learn how to understand key characteristics of malware present on compromised systems, including how to establish indicators of compromise (IOCs) for scoping and containing the intrusion.

The course begins by covering fundamental aspects of malware analysis and continues by discussing essential x86 assembly language concepts. Towards the end of the course, you'll learn to analyze malicious document files that take the form of Microsoft Office and Adobe PDF documents.

Hands-on workshop exercises are a critical aspect of this course and allow you to apply reverse-engineering techniques by examining malware in a controlled environment. When performing the exercises, you'll study the supplied specimen's behavioral patterns and examine key portions of its code. You'll examine malware on a Windows virtual machine that you'll infect during the course and will use the supplied Linux virtual machine (REMnux) that includes tools for examining and interacting with malware.

While the field of reverse-engineering malware is in itself advanced, the course begins by covering this topic from an introductory level and quickly progresses to discuss malware analysis tools and techniques of intermediate complexity. Neither programming experience nor the knowledge of assembly is required to benefit from the course. However, you should have a general idea about core programming concepts, such as variables, loops, and functions. The course spends some time discussing essential aspects of x86 assembly to allow malware analysts to navigate through malicious executables using a debugger and a disassembler.

"FOR610 should be required training for all forensic investigators. It is necessary for awareness, analysis, and reporting threats."

-Paul Gunnerson, U.S. Army

www.giac.org

www.sans.edu

Anuj Soni *SANS Instructor*

Anuj Soni is a senior incident responder at a DC-based consulting firm. Anuj manages and executes specialized incident response techniques to detect, respond to, and mitigate sophisticated threat actors across commercial and government networks. He uses his skills in conducting host-based forensics, malicious code analysis, and advanced threat risk assessments to help clients improve their security posture. He has over 8 years of experience in incident response, forensics, malware analysis, penetration testing, and steganalysis. Anuj received his Bachelors and Masters from Carnegie Mellon University and holds the following certifications: GIAC Reverse Engineering Malware (GREM), EnCase Certified Examiner (EnCE), and Certified Information Systems Security Professional (CISSP). @asoni

MANAGEMENT 512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

SANS
sans.org

Five-Day Program
Mon, Aug 25 - Fri, Aug 29
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPE/CMU Credits
Laptop NOT Needed
Instructors: Stephen Northcutt
David Hoelzer

- GIAC Cert: GSLC
- Masters Program
- DoDD 8570

This completely updated course is designed to empower advancing managers who want to get up to speed quickly on information security issues and terminology. You won't just learn about security, you will learn how to manage security. Lecture sections are intense; the most common student comment is that it's like drinking from a fire hose. The diligent manager will gain vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. Additionally, the course has been engineered to incorporate the NIST Special Publication 800 (series) guidance so that it can be particularly useful to US government managers and supporting contractors.

Who Should Attend

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

Essential security topics covered in this management track include: network fundamentals and applications, power, cooling and safety, architectural approaches to defense in depth, cyber attacks, vulnerability assessment and management, security policies, contingency and continuity planning, awareness management, risk management analysis, incident handling, Web application security, 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.

David Hoelzer

SANS Faculty Fellow

David Hoelzer is a high-scoring SANS Fellow 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. 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. @david_hoelzer

www.giac.org

www.sans.edu

www.sans.org/8570

Knowledge Compression™

Knowledge Compression™ is an optional add-on feature to a SANS class which aims to maximize the absorption and long-term retention of large amounts of data over a relatively short period of time. Through the use of specialized training materials, in-class reviews, examinations and test-taking instruction, Knowledge Compression™ ensures students have a solid understanding of the information presented to them. By attending classes that feature this advanced training product, you will experience some of the most intense and rewarding training programs SANS has to offer, in ways that you never thought possible!

Stephen Northcutt *SANS Faculty Fellow*

Stephen Northcutt founded the GIAC certification and served as president of the SANS Technology Institute. 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. @StephenNorthcut

SANS

CORE NETWARS TOURNAMENT

In-Depth, Hands-On InfoSec Skills

—

Embrace the Challenge

—

Core NetWars Tournament

Core NetWars is a computer and network security challenge designed to test a participant's experience and skills in a safe, controlled environment while having a little fun with your fellow IT security professionals. Many enterprises, government agencies, and military bases are using NetWars OnSites to help identify skilled personnel and as part of extensive hands-on training. With Core NetWars, you'll build a wide variety of skills while having a great time.

Who Should Attend:

- **Security professionals**
- **System administrators**
- **Network administrators**
- **Ethical hackers**
- **Penetration testers**
- **Incident handlers**
- **Security auditors**
- **Vulnerability assessment personnel**
- **Security Operations Center staff members**

There will be two NetWars events:
Aug 21-22 & Aug 27-28 | 6:30-9:30pm

Prizes will be awarded at the conclusion of the games.

REGISTRATION IS LIMITED AND IS FREE
for students attending any course at SANS Virginia Beach 2014
(NON-STUDENTS ENTRANCE FEE IS $1,249).

Learn more at sans.org/netwars

VIRGINIA BEACH BONUS SESSIONS

SANS@Night Evening Talks

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

(AUG 18) KEYNOTE: Cloud IR & Forensics *Paul A. Henry*

The move to private and public cloud changes many things, including how we respond for IR and forensics. As an example, traditionally in a physical realm we relied upon imaging a server's hard drive as well as RAM to perform a thorough analysis. Today in the cloud, creating a forensically sound image of an "instance" of a server to capture the server's abstracted hard disk and an image of its RAM brings new technical and legal complications. An additional issue to consider is that some vendors' platforms are simply not fully supported by our current IR & forensics tools; today's commercial tools lack the ability to perform any analysis at all on a VMware VMFS file system. Lastly, downloading a large server image may simply be cost prohibitive due to the high bandwidth costs associated with moving data out of the cloud environment.

The best course of action may be to perform your analysis within the cloud – however, the methods used in the analysis within the cloud must be forensically sound and as always in computer forensics, they must be repeatable and the result must be the same findings. In this session we will begin to explore the changes that simply must be made to your IR and forensics procedures to properly address IR & forensics in the cloud.

(AUG 19) How to Build a Completely Hackable City in Five Steps (And Why You Should Build Your Own Skills in this Arena) *Ed Skoudis*

The NetWars CyberCity project involves an entire, and entirely functional, city in miniature. There's a real power grid, real water systems, real traffic lights, and real systems to hack. Cyber warriors build skills and develop strategies and contingency plans by running missions in CyberCity. This talk will present an overview of the creation of CyberCity, step by step: concept, funding, architecture and design, implementation, testing, and finally, lessons learned.

But so what? You're not about to construct your own CyberCity – or are you? The border between the cyber and kinetic worlds is eroding, and some of the most interesting (and dangerous) hacks are in the interstitial space between software and hardware. The very cornerstones of society – the power grid, water treatment plants, medical devices, military equipment, and more – are at risk, and ideas such as air gaps and pressure valves are antiquated. The talk will also explore avenues for building your own skills in these various areas so you can help improve the security of our kinetic infrastructures. Find out what CyberCity teaches us about getting our act together in securing the cyber/kinetic space – and how you can build your own skills in this burgeoning arena.

(AUG 19) Privileged Domain Account Protection: How to Limit Credentials Exposure *Mike Pilkington*

In most enterprise networks, there are a number of privileged accounts that are used for maintaining the Windows domain, including accounts for domain administration, configuration management, patch management, vulnerability analysis, and of course incident response. In all of these cases, the accounts have the ability to logon to most, if not all, Windows hosts in the environment. These accounts therefore become high-value targets for attackers.

In order to protect these privileged domain accounts, it is important to have a solid understanding of the various circumstances that can expose domain account credentials. In this presentation, I will discuss what you can and cannot do safely with domain accounts. In particular, I will cover attacks against password hashes, security support providers, access tokens, and network authentication protocols. I will then provide a set of recommendations that you can follow to mitigate the risks and protect those privileged domain account credentials in your environment.

(AUG 20) The 13 Absolute Truths of Security *Keith Palmgren*

Keith Palmgren has identified thirteen "Absolute Truths" of security – things that remain true regardless of circumstance, network topology, organizational type, or any other variable. Recognizing these thirteen absolute truths and how they affect a security program can lead to the success of that program. Failing to recognize these truths will spell almost certain doom. Here we will take a non-technical look at each of the thirteen absolute truths in turn, examine what they mean to the security manager, what they mean to the security posture, and how understanding them will lead to a successful security program.

VIRGINIA BEACH BONUS SESSIONS

(AUG 21) Debunking the Complex Password Myth *Keith Palmgren*

Perhaps the worst advice you can give a user is "choose a complex password." The result is the impossible-to-remember password requiring the infamous sticky note on the monitor. In addition, that password gets used at a dozen sites at home, AND the very same password gets used at work. The final result ends up being the devastating password compromise. In this one-hour talk, we will look at the technical and non-technical (human nature) issues behind passwords. Attendees will gain a more complete understanding of passwords and receive solid advice on creating more easily remembered AND significantly stronger passwords at work and at home, for their users, for themselves and even for their children.

(AUG 22) Closing the Door on Web Shells *Anuj Soni*

While many attackers install malware on end-user workstations to accomplish their goals, external-facing servers continue to be prime targets of attack. In many of these cases, web shell backdoors are utilized by the adversary to download/upload files, execute arbitrary commands, and access back-end databases and other resources. Web shells are often heavily customized and obfuscated to evade detection. They may be only several lines of code, and they can be deployed on a variety of platforms. Every incident responder should be familiar with this dangerous category of malware so it is not overlooked during an investigation. This talk will discuss how web shells work, dive deep into several specimens, discuss approaches to detect related activity, and touch on some best practices to reduce the likelihood of seeing them on your systems.

(AUG 24) KEYNOTE: Gone in 60 Minutes: Have You Patched Your System Today? *David Hoelzer*

In our industry we hear about new vulnerabilities every day, but there can be a perception that moving from the discovery of a flaw to a workable exploit is very difficult. The result is that most organizations are perfectly happy operating with a 30-day patch-rollout cycle. Is this really fast enough? How hard is it really to exploit a vulnerability? How hard is it to scale a proof of concept into a working tool that can compromise thousands of hosts? This presentation demonstrates the entire process, walking through the process that a security researcher or hacker follows from research through proof of concept and working exploit... all in less than 60 minutes. While aspects of this presentation can be somewhat technical, the emphasis isn't on the technical but on the process and speed with which a working exploit can be developed. There's something for everyone to take away from this presentation!

(AUG 25) DLP FAIL!!! Using Encoding, Steganography, and Covert Channels to Evade DLP and Other Critical Controls *Kevin Fiscus*

It's all about the information! Two decades after the movie Sneakers, the quote remains as relevant, if not more so. The fact that someone hacks into an environment is interesting but not that relevant. What is important is what happens after the compromise. If the data is destroyed or modified, organizations are negatively impacted but the benefits to an attacker for destruction or alteration are somewhat limited. Stealing information however, is highly profitable. Identity theft, espionage, and financial attacks involve the exfiltration of sensitive data. As a result, organizations deploy tools to detect and/or stop that data exfiltration. While these tools can be extremely valuable, many have serious weaknesses; attackers can encode, hide, or obfuscate the data, or can use secret communication channels. This session will talk about and demonstrate a range of these methods.

(AUG 26) 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.

(AUG 27) Investing for Retirement *Stephen Northcutt*

When I turned 50 I joined AARP so I could get 20% off Regal Theaters popcorn and other swell discounts, but it seemed that every single issue of their magazine had an article on people not saving enough to retire. However, saving for retirement is silly, the best interest rate I have seen on a savings account is 0.7% and that is probably less than the true cost of living increases. If any of us are going to retire, we will need to invest and invest wisely. Since I am older than most of the SANS instructors, it occurred to me that I would probably be one of the first to go. For the last year, I have been looking at the options to generate enough monthly income to retire on and have found the results rather surprising. This talk summarizes my research, it will cover many of the financial vehicles that are available and for each we will cover the pitch, the catch, and my best assessment on how to use (or avoid) that vehicle. The talk is meant to encourage each member of the audience to begin thinking about their financial portfolio and retirement options. Best of all, I promise I will not try to sell anybody anything.

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

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

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

OnSite www.sans.org/onsite
Live Training at Your Office Location

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

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

ONLINE TRAINING

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

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

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

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

FUTURE SANS TRAINING EVENTS

Information on all events can be found at www.sans.org/security-training/by-location/all

SANSFIRE 2014

Baltimore, MD | June 21-30

SANS Capital City 2014

Washington, DC | July 7-12

SANS San Francisco 2014

San Francisco, CA | July 14-19

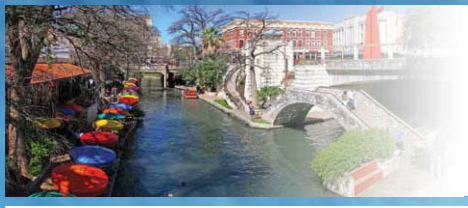
SANS ICS Industrial Control Systems

ICS Security TRAINING 2014 - HOUSTON

Houston, TX | July 21-25

SANS Boston 2014

Boston, MA | July 28 - August 2



SANS San Antonio 2014

San Antonio, TX | August 11-16

SANS Cyber Defense SUMMIT

Nashville, TN | August 13-20

SANS Chicago 2014

Chicago, IL | August 24-29

SANS Crystal City 2014

Crystal City, VA | September 8-13

SANS VIRGINIA BEACH 2014

Hotel Information

Training Campus
Hilton Virginia Beach Oceanfront

3001 Atlantic Avenue
Virginia Beach, VA 23451
www.sans.org/event/virginia-beach-2014/location

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 25, 2014. To make reservations please call 800-445-8667 and ask for the SANS group rate.

Refresh, work and relax at the Hilton Virginia Beach Oceanfront hotel, conveniently located just minutes from Norfolk International Airport and right on Virginia Beach. Wander along the boardwalk or experience great live music for free at Neptune's Park next to the hotel. Enjoy superior views of the Atlantic Ocean and surrounding areas from Sky Bar, located on the 21st floor of the hotel next to Virginia's first rooftop infinity pool. Indulge with gourmet cuisine at Salacia, Virginia's first AAA-4 diamond steakhouse, or be tempted by the freshest oysters at Catch 31.

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 2014

Registration Information

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

Register online at www.sans.org/event/virginia-beach-2014/courses

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

If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with Internet access must complete the online registration form. We do not take registrations by phone.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	**6/25/14**	**$400.00**	**7/9/14**	**$250.00**

Some restrictions apply.

Group Savings (Applies to tuition only)*

10% discount if 10 or more people from the same organization register at the same time
5% discount if 5-9 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 prior to registering.

**Early-bird rates and/or other discounts cannot be combined with the group discount.*

Cancellation

You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by July 30, 2014 – processing fees may apply.

SANS Voucher Credit Program

Expand your training budget! Extend your Fiscal Year. The SANS Voucher Discount Program pays you credits and delivers flexibility.
www.sans.org/vouchers