THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS Virginia Beach 2013

Virginia Beach, VA | August 19-30

"This was an awesome and informative experience. My organization will benefit as a result. Thanks!"

-Far'd Thomas, Lockheed Martin

Hands-on immersion training programs, including:

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

Network Penetration Testing and Ethical Hacking

Computer Forensic Investigations - Windows In-Depth

Intrusion Detection In-Depth

SANS Security Leadership Essentials For Managers

REM: Malware Analysis Tools and Techniques

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

Advanced Security Essentials – Enterprise Defender

Virtualization and Private Cloud Security

Register at
www.sans.org/event/virginia-beach-2013

GIAC Approved Training

Please join us at the shore for **SANS Virginia Beach 2013 on August 19-30**. This event has been a hit every year, so we are again offering the opportunity to take two full back-to-back courses in this popular beach location. Don't miss the chance for a late-summer family beach vacation with two weeks of SANS training!

Attend one or two of 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 beautiful additions to your seashell collection! Our hand-picked instructor lineup includes Paul A. Henry teaching two classes and Dr. Eric Cole, Stephen Northcutt, Mike Poor, Dave Shackleford, Christopher Crowley, Seth Misenar, Kevin Fiscus, and Jake Williams each teaching one. See this brochure for a complete schedule, course descriptions, instructor bios, GIAC cert availability for nine of our courses, and information about earning your Master of Science in Information Security through the SANS Technology Institute (STI).

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

Located on the three-mile long Virginia Beach boardwalk, the **Hilton Virginia Beach Oceanfront** is right next to Neptune's Park and the Shoppes at 31 Ocean. With 35 miles of beaches right nearby, this campus offers a perfect destination with endless activities. The beach and boardwalk activities are endless! Rent a bike or roller blades and explore the Boardwalk, tune in to a variety of live music, feast on great food, experience the aquarium, shop until you drop, take flight by parasailing, go sportfishing on a charter boat, 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 until July 26. This great rate includes high-speed Internet access. Government per diem rooms are available with proper ID. Please note that when you call the hotel for a reservation, you will need to ask for the "SANS INSTITUTE GOVERNMENT ROOM BLOCK, Group CODE: **SNG**."

Register by July 3rd to receive a $500 tuition fee discount! Start making your training and travel plans now and let your colleagues and friends know about SANS Virginia Beach 2013. We look forward to seeing you there.

Best regards,

Stephen Northcutt
SANS Faculty Fellow

Stephen Northcutt

Here's what past Virginia Beach attendees had to say:

"SANS is the gold standard in information security training, plain and simple."
-Scott Hilts, Bruce Power

"The fact that the curriculum is updated every 3 months is a huge plus. Security is an ever-changing environment, and consistent updates are an example of why I choose SANS."
-Richard Mascolo, U. S. Navy

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

Courses-at-a-Glance

SECURITY 401

Security Essentials Bootcamp Style

Six-Day Program • Mon, Aug 19 - Sat, Aug 24
9:00am - 7:00pm (Days 1-5) • 9:00am - 5:00pm (Day 6)
46 CPE/CMU Credits • Laptop Required
Instructor: Dr. Eric Cole

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

Who Should Attend:

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

With the APT (advanced persistent threat), organizations are going to be targeted. Whether the attacker is successful penetrating an organization's network depends on the organization's defense. While defending against attacks is an ongoing challenge with new threats emerging all of the time, including the next generation of threats, organizations need to understand what works in cyber security. What has worked and will always work is taking a risk-based approach to cyber defense. Before your organization spends a dollar of its IT budget or allocates any resources or time 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. Since all jobs today require an understanding of security, this course will help you understand why security is important and how it applies to your job. In addition, you will gain the essential, up-to-the-minute knowledge and skills required for effective security so that you will be prepared if you are given the responsibility for securing systems and/or organizations. This course meets both of the key promises SANS makes to our students: (1) You will gain cutting-edge knowledge you can put into practice immediately upon returning to work; and, (2) You will be taught by the best security instructors in the industry.

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

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

Dr. Eric Cole *SANS Faculty Fellow*

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

SECURITY 501

Advanced Security Essentials – Enterprise Defender

Six-Day Program • Sun, Aug 25 - Fri, Aug 30
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Dave Shackleford

Cybersecurity continues to be a critical area for organizations and will continue to increase in importance as attacks become stealthier, have a greater financial impact on an organization, and cause reputational damage. Security Essentials lays a solid foundation for the security practitioner to engage the battle.

"Great course! I'm disturbed/ impressed at how much the instructors know. Top-notch instructors are what makes SANS!"
-Chris Robinson, Sempra Energy

A key theme is that prevention is ideal, but detection is a must. We need to be able to ensure that we constantly improve our security to prevent as many attacks as possible. This prevention/protection occurs on two fronts - externally and internally. Attacks will continue to pose a threat to an organization as data become more portable and networks continue to be porous. Therefore a key focus needs to be on data protection, securing our critical information no matter whether it resides on a server, in a robust network architecture, or on a portable device.

Despite an organization's best effort at preventing attacks and protecting its critical data, some attacks will still be successful. Therefore we need to be able to detect attacks in a timely fashion. This is accomplished by understanding the traffic that is flowing on your networks and looking for indication of an attack. It also includes performing penetration testing and vulnerability analysis against an organization to identify problems and issues before a compromise occurs.

Finally, once an attack is detected we must react to it in a timely fashion and perform forensics. Understanding how the attacker broke in can be fed back into more effective and robust preventive and detective measures, completing the security lifecycle.

"The information taught is valuable and applicable. It does not matter what your job functions are at your company, you will definitely find value in this course."
-Leslie Morales, Southwest Research Institute

Who Should Attend:

- Students who have taken Security Essentials and want a more advanced 500-level course similar to SEC401
- People who have foundational knowledge covered in SEC401, do not want to take a specialized 500-level course, and still want a broad, advanced coverage of the core areas to protect their systems
- Anyone looking for detailed technical knowledge on how to protect against, detect, and react to the new threats that will continue to cause harm to an organization

Dave Shackleford *SANS Senior Instructor*

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

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

www.giac.org

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

www.sans.edu

SECURITY 503

Intrusion Detection In-Depth

Six-Day Program • Mon, Aug 19 - Sat, Aug 24
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Mike Poor

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.

Who Should Attend:

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

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.

"Mike Poor's ability to explain GCIA concepts is unmatched and will allow any junior analyst to hit the ground running."
-Erich Melcher, Sabre Systems, Inc.

"This course is valuable for anyone interested in IDS. Mike's knowledge and willingness to help you understand the material are unlike any other training I've been to. Great course and instructor."
-Dannie Arnold, U.S. Army

Hands-on exercises supplement the coursebook 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 to have a more challenging experience. Additionally, there is an "extra credit" stumper question for each exercise intended to challenge the most advanced student.

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

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

"This course provides a good basis of knowledge and presents important tools which will be at the core of any intrusion analysis."
-Thomas Kelly, DIA

www.sans.edu

Mike Poor *SANS Senior Instructor*

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

www.sans.org/cyber-guardian

"Course was designed around real-world intrusions and is highly needed for network security administrators and/or analysts."
-Hector Araiza, USAF

SECURITY 504

Hacker Techniques, Exploits, and Incident Handling

Six-Day Program • Mon, Aug 19 - Sat, Aug 24
9:00am - 6:30pm (Day 1) • 9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits • Laptop Required
Instructor: Kevin Fiscus

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.

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

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
- 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

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.

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

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

Kevin Fiscus *SANS 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 taught many of SANS most popular classes including SEC401, SEC504, SEC575, FOR508, and MGT414. In addition to his security work, he is a proud husband and father of two children.

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

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

SECURITY 560

Network Penetration Testing and Ethical Hacking

Six-Day Program • Sun, Aug 25 - Fri, Aug 30
9:00am - 6:30pm (Day 1) • 9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits • Laptop Required
Instructor: Christopher Crowley

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

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

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

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

Who Should Attend:

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

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

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

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

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

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

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

Christopher Crowley *SANS Certified Instructor*

Christopher Crowley has 15 years of industry experience managing and securing networks. He has GSEC, GCIA, GCIH (gold), GCFA, and CISSP certifications. His teaching experience includes GSEC, GCIA, and GCIH Mentor; Apache web server administration and configuration; and shell programming. He was awarded the SANS 2009 Local Mentor of the year award, which is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities.

SECURITY 579

Virtualization and Private Cloud Security

Six-Day Program • Sun, Aug 25 - Fri, Aug 30
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop provided during class • Instructor: Paul A. Henry

Who Should Attend:

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

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

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

Server virtualization vulnerabilities

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

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

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

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

Paul A. Henry *SANS Senior Instructor*

Paul Henry is one of the world's foremost global information security and computer forensic experts with more than 20 years experience managing security initiatives for Global 2000 enterprises and government organizations worldwide. Paul is a principle at vNet Security, LLC and is keeping a finger on the pulse of network security as the security and forensic analyst at Lumension Security. Throughout his career, Paul has played a key strategic role in launching new network security initiatives to meet our ever-changing threat landscape. Paul also advises and consults on some of the world's most challenging and high-risk information security projects, including the National Banking System in Saudi Arabia, the Reserve Bank of Australia, the Department of Defense's Satellite Data Project (USA), and both government as well as telecommunications projects throughout Southeast Asia. Paul is frequently cited by major and trade print publications as an expert in computer forensics, technical security topics, and general security trends and serves as an expert commentator for network broadcast outlets, such as FOX, NBC, CNN, and CNBC. In addition, Paul regularly authors thought leadership articles on technical security issues, and his expertise and insight help shape the editorial direction of key security publications, such as the ***Information Security Management Handbook***, where he is a consistent contributor. Paul serves as a featured and keynote speaker at seminars and conferences worldwide, delivering presentations on diverse topics including anti-forensics, network access control, cyber crime, DDoS attack risk mitigation, firewall architectures, security architectures, and managed security services.

FORENSICS 408

Computer Forensic Investigations – Windows In-Depth

Six-Day Program • Mon, Aug 19 - Sat, Aug 24
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Paul A. Henry

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

FOR408: Computer Forensic Investigations – Windows In-Depth focuses on the critical knowledge of the Windows OS that every digital forensic analyst must know to investigate computer incidents successfully. You will learn how computer forensic analysts focus on collecting and analyzing data from computer systems to track user-based activity that could be used internally or in civil/criminal litigation.

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

Who Should Attend:

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

"This is a very high-intensity course with extremely current course material that is not available anywhere else in my experience."

-Alexander Applegate, Auburn University

What you will receive with this course

- **Windows version of the SIFT Workstation Virtual Machine**
- **Windows 8 Standard Full Version License and Key for the Windows SIFT Workstation**
- **Full License to AccessData FTK and Guidance Software EnCase for a 3 month trial**
- **Full License to MagnetForensics Internet Evidence Finder for a 15 day trial**
- **Two full real-world cases to examine during class**
- **Course DVD loaded with case examples, tools, and documentation**
- **Wiebetech Ultradock v5 Write Blocker Kit**

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

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

Paul A. Henry *SANS Senior Instructor*

Paul Henry is one of the world's foremost global information security and computer forensic experts with more than 20 years experience managing security initiatives for Global 2000 enterprises and government organizations worldwide. Paul is a principle at vNet Security, LLC and is keeping a finger on the pulse of network security as the security and forensic analyst at Lumension Security. Throughout his career, Paul has played a key strategic role in launching new network security initiatives to meet our ever-changing threat landscape. Paul also advises and consults on some of the world's most challenging and high-risk information security projects, including the National Banking System in Saudi Arabia, the Reserve Bank of Australia, the Department of Defense's Satellite Data Project (USA), and both government as well as telecommunications projects throughout Southeast Asia. Paul is frequently cited by major and trade print publications as an expert in computer forensics, technical security topics, and general security trends and serves as an expert commentator for network broadcast outlets, such as FOX, NBC, CNN, and CNBC. In addition, Paul regularly authors thought leadership articles on technical security issues, and his expertise and insight help shape the editorial direction of key security publications, such as the ***Information Security Management Handbook***, where he is a consistent contributor. Paul serves as a featured and keynote speaker at seminars and conferences worldwide, delivering presentations on diverse topics including anti-forensics, network access control, cyber crime, DDoS attack risk mitigation, firewall architectures, security architectures, and managed security services.

www.giac.org

www.sans.edu

FORENSICS 610

Reverse-Engineering Malware: Malware Analysis Tools and Techniques

Five-Day Program • Mon, Aug 19 - Fri, Aug 23
9:00am - 5:00pm • 30 CPE/CMU Credits
Laptop Required • Instructor: Jake Williams

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!

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. The course 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.

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**

"This class gave me essential tools that I can immediately apply to protect my organization."
-Don Lopez, Valley National Bank

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

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

Jake Williams *SANS Instructor*

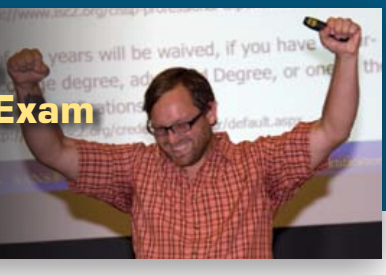
Jake Williams is a technical analyst with the Department of Defense (DoD) where he has over a decade of experience in systems engineering, computer security, forensics, and malware analysis. Jake has been providing technical instruction for years, primarily with HBGary, where he was the principal courseware developer and instructor for their products. He also maintains malware reverse engineering courses for CSRgroup Computer Security Consultants. Recently, he has been researching the application of digital forensic techniques to public and private cloud environments. Jake has been involved in numerous incident response events with industry partners in various consulting roles. Jake led the winning government team for the 2011 and 2012 DC3 Digital Forensics Challenge. He has spoken at numerous events, including the ISSA events, SANS @Night, the DC3 conference, Shmoocon, and Blackhat. Jake holds a Bachelor's degree in CIS, a Master's Degree in Information Assurance, and is currently pursuing a PhD in Computer Science. His research interests include protocol analysis, binary analysis, malware RE methods, and methods for identifying malware Command and Control (C2) techniques. He holds numerous certifications, including GREM, GCFE, GSNA, GCIA, GCIH, GCWN, GPEN, RHCSA, and CISSP.

www.giac.org

www.sans.edu

MANAGEMENT 414

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



Six-Day Program • Sun, Aug 25 - Fri, Aug 30
9:00am - 7:00pm (Day 1) • 8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6) • 46 CPE/CMU Credits
Laptop NOT Required • Instructor: Seth Misenar

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

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

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

Obtaining your CISSP® certification consists of:

- **Fulfilling minimum requirements for professional work experience**
- **Completing the Candidate Agreement**
- **Review of résumé**
- **Passing the CISSP® 250 multiple-choice question exam with a scaled score of 700 points or greater**
- **Submitting a properly completed and executed Endorsement Form**
- **Period Audit of CPEs to maintain the credential**

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

"This course breaks the huge CISSP study books down into manageable chunks, and helped me focus and identify weaknesses. The instructor's knowledge and teaching skills are excellent."
-Jeff Jones, Constellation Energy Group

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

Who Should Attend:

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

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

Seth Misenar *SANS Certified Instructor*

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

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

GIAC INFORMATION SECURITY PROFESSIONAL
GISP
www.giac.org

MANAGEMENT 512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program • Mon, Aug 26 - Fri, Aug 30
9:00am - 6:00pm (Course Days 1-4) • 9:00am - 4:00pm (Course Day 5)
33 CPE/CMU Credits • Laptop NOT Required • Instructor: Stephen Northcutt

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

Who Should Attend:

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

Essential security topics covered in this management track include: network fundamentals and applications, power, cooling and safety, architectural approaches to defense in depth, cyber attacks, vulnerability assessment and management, security policies, contingency and continuity planning, awareness management, risk management analysis, incident handling, web application security, and offensive and defensive information warfare, culminating with our management practicum. The material uses Knowledge Compression™, special charts, and other proprietary SANS techniques to help convey the key points of critical slides and keep the information flow rate at a pace senior executives demand every teaching hour of the course. The course has been evaluated and approved by CompTIA's CAQC program for Security+ 2008 to ensure that managers and their direct reports have a common baseline for security terminology and concepts. You will be able to put what you learn into practice the day you get back into the office.

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

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

Stephen Northcutt *SANS Faculty Fellow*

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

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

www.giac.org

www.sans.edu

Bonus Sessions

SANS@Night Evening Talks

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

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

In this engaging talk, one of the experts on APT, Dr. Cole, will outline an action plan for building a defensible network that focuses on the key motto that "Prevention is Ideal but Detection is a Must". Better understand what the APT really is and what organizations can do to be better prepared. The threat is not going away, so the more organizations can realign their thinking with solutions that actually work, the safer the world will become.

Thanks for Recovering... Now I can Hack You! *Charles Greene*

Why do disaster recovery (DR) exercises fail? Is it a lack of planning or a lack of testing? Both of these would cause an exercise to fail, but is this really a failure? Attend this session to learn more about the risks involved with data recovery exercises.

Everything I Know is Wrong! *Stephen Northcutt*

Join Stephen Northcutt in a myriad of topics including: Strong cryptography done correctly cant be defeated! Wrong – You have to have anti-virus! Well, fine, but it no longer works in a world that generates 30k new variations of malware some days – What about blades and virtualization? Data centers must have raised floors; funny, ours uses risers instead – and much more.

Evolving VoIP Threats *Paul A. Henry*

VoIP is thriving in an otherwise down economy. VoIP implementations are growing, driven by cost savings. Cost is typically the only consideration in the implementation of VoIP – it is all about saving money. Security, if considered at all, is clearly an afterthought. Too many still dismiss VoIP threats as theoretical. VoIP can afford significant costs savings while not sacrificing an organizations security. Recognizing the threats and implementing the compensating and technical controls can make all the difference in a successful VoIP implementation.

Certifiably Certifiable *Seth Misenar*

An alphabet soup of required certifications seems to follow every job posting, and yet for all these letters are our organizations becoming more secure? Are our security certifications failing us? Are we failing our security certifications? This talk will be a discussion on the past and current state of security certifications. Additionally, the future of security certifications and what modifications are needed will be discussed.

SANS 8 Mobile Device Security Steps *Chris Crowley*

Every organization is challenged to rapidly deploy mobile device security. The SANS 8 Mobile Device Security Steps is a community-driven project to provide the most up-to-date information on the most effective strategies for securing mobile infrastructure. Chris Crowley will discuss the guidance provided in the 8 Steps, including: user authentication and restricting unauthorized access, OS and application management, device monitoring, and key operational components for mobile device management.

So What? The Most Important Question in Information Security *Kevin Fiscus*

The world of information security is filled with sophisticated technical concepts and 0-day "sploits". Penetration testers ride high as the elite of the security community. Unfortunately, the business aspect of security often gets lost. Penetration testers sit confused when their boss or their client doesn't seem to care about getting "root" or domain admin access. The communication gaps widens when that boss or that client fails to fix identified problems or to follow sound recommendations. Fortunately, security professionals can solve these problems by simply asking a simple question – so what?

Code Injection *Jake Williams*

In this presentation, we'll talk about how code injection really works at a more technical level. We'll take a quick look at some malware that's performing code injection and discuss detection strategies for when your antivirus fails to detect it. Code injection is a huge topic and we can't cover every aspect in an hour, but the goal is for you to walk away understanding the basics of what's happening under the hood so you can speak intelligently to the topic.

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. 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.

Vendor Showcase

Tuesday, August 20 | 10:30am-10:50am • 3:00pm-3:20pm

What's Your Next Career Move?

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

Master of Science in Information Security Engineering

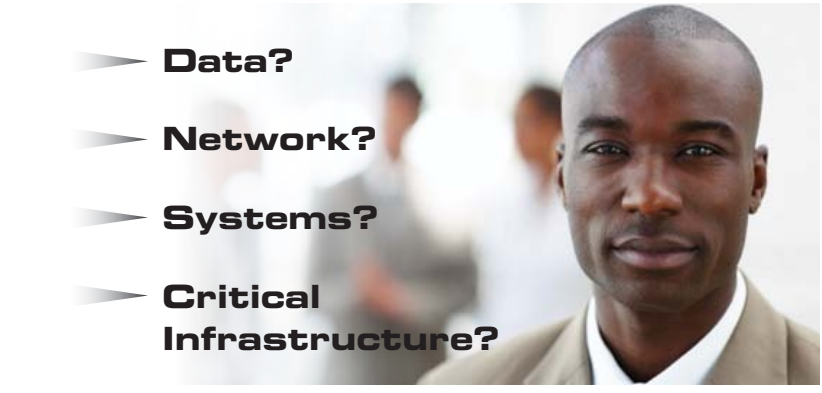
Master of Science in Information Security Management

Cohorts are forming now!
Apply now at www.sans.edu

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

www.sans.edu
info@sans.edu
855-672-6733

How Are You Protecting Your



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

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

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

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

Get Certified at
www.giac.org

SANS Virginia Beach 2013

Hotel Information

Training Campus
Hilton Virginia Beach Oceanfront

3001 Atlantic Ave. | Virginia Beach, VA 23451
Phone: 757-213-3000
www.sans.org/event/virginia-beach-2013/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 26, 2013. To make reservations please call (800) HILTONS (800-445-8667) and ask for the SANS group rate.

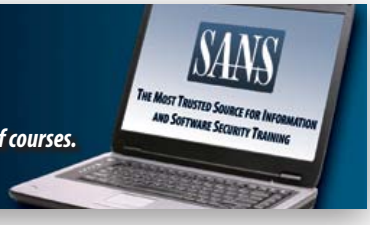
Refresh, work, and relax at the Hilton Virginia Beach Oceanfront hotel, conveniently located just minutes from Norfolk International Airport and right on Virginia Beach. Wander along the boardwalk or experience great live music for free at Neptune's Park next to the hotel. Enjoy superior views of the 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 2013

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-2013

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

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

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

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

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

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

Cancellation

You may substitute another person in your place at any time, at no charge, by e-mail: **registration@sans.org** or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail or fax, and postmarked by July 24, 2013 – processing fees may apply.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	**7/3/13**	**$500.00**	**7/17/13**	**$250.00**

Some restrictions apply.

Group Savings (Applies to tuition only)

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

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

SANS Voucher Credit Program

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

www.sans.org/vouchers