16 Great Courses – 2 Convenient Locations

Cyber Guardian 2014

Baltimore, MD

March 3-8

CAPITAL SANS REGION

Northern Virginia 2014

Reston, VA

March 17-22

Hands-on immersion training:

Baltimore, MD | March 3-8

SEC503: Intrusion Detection In-Depth ***NEW!***

SEC401: Security Essentials Bootcamp Style

SEC560: Network Penetration Testing and Ethical Hacking

MGT512: SANS Security Leadership Essentials For Managers with Knowledge Compression™

FOR508: Advanced Computer Forensic Analysis and Incident Response

SEC501: Advanced Security Essentials – Enterprise Defender

Register at www.sans.org/event/cyber-guardian-2014

Reston, VA | March 17-22

SEC573: Python for Penetration Testers ***NEW!***

SEC760: Advanced Exploit Development for Penetration Testers ***BETA!***

SEC401: Security Essentials Bootcamp Style

SEC502: Perimeter Protection In-Depth

SEC504: Hacker Techniques, Exploits, and Incident Handling

SEC505: Securing Windows and Resisting Malware

SEC542: Web App Penetration Testing and Ethical Hacking

SEC575: Mobile Device Security and Ethical Hacking

SEC579: Virtualization and Private Cloud Security

FOR408: Computer Forensic Investigations – Windows In-Depth

MGT414: SANS® +S™ Training Program for the CISSP® Certification Exam

GIAC Approved Training

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

SANS Capital Region 2014 is made up of two training events in two cities near DC. Each is six days long and there is a week in between them. The two events and cities are: ***SANS Cyber Guardian 2014 in Baltimore from March 3-8***, and ***SANS Northern Virginia 2014 in Reston from March 17-22***. These two events feature SANS top instructors who are the best at ensuring you not only learn the material, but that you will be able to apply our information security training the day you get back to the office!

SANS Cyber Guardian 2014, will be held this year at the ***Sheraton Inner Harbor***. This is the SANS event that will put you on the path to becoming a ***Cyber Guardian*** and will provide the intense, immersion training you need for today's sophisticated cyber threats. All six courses are associated with a GIAC cert, and five are associated with the ***DOD Directive 8570***. This training is presented by some of our top-rated instructors who include: Dr. Eric Cole, Ed Skoudis, Mike Poor, Eric Conrad, G. Mark Hardy, and Jake Williams.

SANS Northern Virginia 2014 will be held at the ***Sheraton Reston*** with a unique lineup of ten comprehensive hands-on technical training courses—from our popular ***SEC401: Security Essentials Bootcamp*** to our new cutting-edge ***SEC760: Advanced Exploit Development for Penetration Testers***. Some of the courses at SANS Northern Virginia will count for either Baseline, Blue Team, or Red Team for the ***SANS Cyber Guardian Program***. Please refer to the Cyber Guardian page in the brochure to find out more about how select courses can apply to SANS Cyber Guardian Program.

Both events include courses that will prepare you or your technical staff for ***DoD Directive 8570*** and GIAC-approved certification exams. Earn your master's degree through ***SANS Technology Institute (STI)***. Take classes in Information Security Management (MSISM) or Engineering (MSISE). You can pick a course that may contribute to all of these options that are important to you!

Please take the time to look through the brochure, you will find the two events interesting and inviting. See our comprehensive course descriptions, our instructor bios, and our evening events and talks that enhance your training. Select a course from each event to maximize your training in a location convenient to you, and let your colleagues and friends know about SANS Capital Region 2014. We look forward to seeing you there!

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

"SANS has the best instructors!"
-Brian Houlihan,
National Credit Union Administration

"One of the most relevant and informational classes I've ever taken. I'll be back for more."
-Racheal Strider, Patelco Credit Union

"It's great to understand how hackers are exploiting a variety of systems, and learning how to prevent these as best as possible is imperative to protect key systems and resources."
-Samantha Hanagan, Texel Tek

"Keeping material relevant is what SANS has been doing. Keep up the good work!"
-B. Taylor, Navy

"I've been attending SANS for many years and there simply is no vendor that favorably compares."
-Curtis Overton, WA ARNG

COURSES-AT-A-GLANCE

SANS Cyber Guardian – Baltimore, MD	MON 3/3	TUE 3/4	WED 3/5	THU 3/6	FRI 3/7	SAT 3/8
SEC401: Security Essentials Bootcamp Style	Page 2					
SEC501: Advanced Security Essentials – Enterprise Defender	Page 3					
SEC503: Intrusion Detection In-Depth *NEW!*	Page 5					
SEC560: Network Penetration Testing and Ethical Hacking	Page 9					
FOR508: Advanced Computer Forensic Analysis and Incident Response	Page 15					
MGT512: SANS Security Leadership Essentials For Managers with Knowledge Compression™	Page 17					

SANS Northern Virginia – Reston, VA	MON 3/17	TUE 3/18	WED 3/19	THU 3/20	FRI 3/21	SAT 3/22
SEC401: Security Essentials Bootcamp Style	Page 2					
SEC502: Perimeter Protection In-Depth	Page 4					
SEC504: Hacker Techniques, Exploits & Incident Handling	Page 6					
SEC505: Securing Windows and Resisting Malware	Page 7					
SEC542: Web App Penetration Testing and Ethical Hacking	Page 8					
SEC573: Python for Penetration Testers *NEW!*	Page 10					
SEC575: Mobile Device Security and Ethical Hacking	Page 11					
SEC579: Virtualization and Private Cloud Security	Page 12					
SEC760: Advanced Exploit Development for Penetration Testers *BETA!*	Page 13					
FOR408: Computer Forensic Investigations – Windows In-Depth	Page 14					
MGT414: SANS® +S™ Training Program for the CISSP® Certification Exam	Page 16					

CONTENTS

SECURITY 401

Security Essentials Bootcamp Style

Six-Day Program
Mon, Mar 3 - Sat, Mar 8
&
Mon, Mar 17 - Sat, Mar 22
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPE/CMU Credits
Instructor: Eric Conrad (CG)
(Eric's bio - page 15)
Instructor: Keith Palmgren (NV)

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

OFFERED AT
SANS Cyber Guardian
&
SANS Northern Virginia

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.

With the APT, 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. 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.

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 analysts, penetration testers, and auditors who need a solid foundation of security principles so they can be as effective as possible at their jobs
- Anyone new to information security with some background in information systems and networking

www.giac.org

www.sans.edu

www.sans.org/
cyber-guardian


www.sans.org/8570

"The flagship SANS course, SEC401, has an exceptional blend of Security essential theory and hands-on experience."
-Ed Concepcion, USMC

"SEC401 is the best InfoSec training bar none. The value for the money is unbeatable!"
-Ron Foupht,
Sirius Computer Solutions

"SEC401 is an eye opener to the broader aspects of network/ Security admin roles. You see things from a different paradigm."
-Rod Campbell, CITEC

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 501

Advanced Security Essentials – Enterprise Defender

OFFERED AT
SANS Cyber Guardian

Six-Day Program
Mon, Mar 3 - Sat, Mar 8
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Dr. Eric Cole

- GIAC Cert: GCED
- Masters Program

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

"SEC501 gives a hands-on technical overview and hands-on approach for admins, but also added value to non-admin personnel (analysts)."
-Stephen Pastore, GE

"Eric made this course and made the content real-world and relevant."
-Dana Ormerod, DuPont

"Dr. Cole is very engaging and a high-energy instructor."
-Colin Gallagher, U.S. Navy

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.

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.

www.giac.org

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.

www.sans.edu

Dr. Eric Cole *SANS Faculty Fellow*

Dr. Cole is an industry-recognized security expert with over 20 years of hands-on experience. Dr. Cole currently performs leading-edge security consulting and works in research and development to advance the state of the art in information systems security. Dr. Cole has experience in information technology with a focus on perimeter defense, secure network design, vulnerability discovery, penetration testing, and intrusion detection systems. He has a master's degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. Dr. Cole is the author of several books, including "Hackers Beware," "Hiding in Plain Site," "Network Security Bible," and "Insider Threat." He is the inventor of over 20 patents and is a researcher, writer, and speaker. He is also a member of the Commission on Cyber Security for the 44th President and several executive advisory boards. Dr. Cole is founder of Secure Anchor Consulting, where he provides state-of-the-art security services and expert witness work. He also served as CTO of McAfee and Chief Scientist for Lockheed Martin. Dr. Cole is actively involved with the SANS Technology Institute (STI) and SANS, working with students, teaching, and maintaining and developing courseware. He is a SANS faculty Fellow and course author.

SECURITY 502

Perimeter Protection In-Depth

OFFERED AT
SANS Northern Virginia

Six-Day Program
Mon, Mar 17 - Sat, Mar 22
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Seth Misenar

- GIAC Cert: GPPA
- Masters Program
- Cyber Guardian

There is no single fix for securing your network. That's why this course is a comprehensive analysis of a wide breadth of technologies. In fact, this is probably the most diverse course in the SANS catalog, as mastery of multiple security techniques is required to defend your network from remote attacks. You cannot just focus on a single OS or security appliance. A proper security posture must be comprised of multiple layers. This course was developed to give you the knowledge and tools necessary at every layer to ensure your network is secure.

Who Should Attend

- Information security officers
- Intrusion analysts
- IT managers
- Network architects
- Network security engineers
- Network and system administrators
- Security managers
- Security analysts
- Security architects
- Security auditors

"The course is very valuable because it shows you the techniques and methods attackers use and how to defend against them."
-Curtis Greer, U.S. Navy

"SEC502 opened my eyes so wide it scared me!"
-George Scarborough, Defense Logistics Agency

"As an analyst, these courses are the most relevant in the industry."
-Louis Robichaud, Atlantic Lottery Corp.

Is there traffic passing by my firewall I didn't expect? How did my system get compromised when no one can connect to it from the Internet? Is there a better solution than anti-virus for controlling malware? We'll dig into these questions and more and answer them.

www.giac.org

The course material has been developed using the following guiding principles:

- **Learn the process, not one specific product.**
- **You learn more by doing, so hands-on problem solving is key.**
- **Always peel back the layers and identify the root cause.**

www.sans.edu

While technical knowledge is important, what really matters are the skills to properly leverage it. This is why the course is heavily focused on problem solving and root cause analysis. While these are usually considered soft skills, they are vital to being effective in the role of security architect. So along with the technical training, you'll learn risk-management capabilities and even a bit of Zen empowerment.

www.sans.org/cyber-guardian

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.

SECURITY 503

Intrusion Detection In-Depth

NEW

OFFERED AT
SANS Cyber Guardian

Six-Day Program
Mon, Mar 3 - Sat, Mar 8
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

"SEC503 added additional skills to my knowledge base. I learned a lot more than I originally expected."
-Robert Strawley, U.S. Army

"Mike has a gift for making a potentially dry subject matter very interesting; excellent teaching and presentation skills."
-Jennifer Torres, BAH

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.

SECURITY 504

Hacker Techniques, Exploits, and Incident Handling

OFFERED AT
SANS Northern Virginia

Six-Day Program
Mon, Mar 17 - Sat, Mar 22
9:00am - 6:30pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits
Laptop Required
Instructor: Michael Murr

- 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

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8570

"SEC504 was a great course in all aspects; content, presentation, and instructor. I would really like more courses and opportunities for this training."
-Tom Patterson, Sage Software

"As someone who works in information security but has never had to do a full incident report, SEC504 taught me all the proper processes and steps."
-Todd Choryan, Motorola Solutions

Michael Murr *SANS Certified Instructor*

Michael has been a forensic analyst with Code-X Technologies for over five years, has conducted numerous investigations and computer forensic examinations, and has performed specialized research and development. Michael has taught SANS SEC504 (Hacker Techniques, Exploits, and Incident Handling), SANS FOR508 (Computer Forensics, Investigation, and Response), and SANS FOR610 (Reverse-Engineering Malware); has led SANS@Home courses; and is a member of the GIAC Advisory Board. Currently, Michael is working on an open-source framework for developing digital forensics applications. Michael holds the GCIH, GCFA, and GREM certifications and has a degree in computer science from California State University at Channel Islands. Michael also blogs about Digital forensics on his Forensic Computing blog. www.forensicblog.org

SECURITY 505

Securing Windows and Resisting Malware

Six-Day Program
Mon, Mar 17 - Sat, Mar 22
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Jason Fossen

- GIAC Cert: GCWN
- Masters Program
- Cyber Guardian

In April of 2014, Microsoft will stop releasing any new security patches for Windows XP. Like it or not, migrating off Windows XP is no longer optional, the clock is counting down. The **Securing Windows and Resisting Malware** course is fully updated for Windows Server 2012, Windows 8, Server 2008-R2, and Windows 7.

This course is about the most important things to do to secure Windows and how to minimize the impact on users of these changes. You'll see the instructor demo the important steps live, and, if you bring a laptop, you can follow along too. The manuals are filled with screenshots and step-by-step exercises, so you can do the steps alongside the instructor in seminar or later on your own time if you prefer.

We've all got anti-virus scanners, but what else needs to be done to combat malware and intruders using Advanced Persistent Threat (APT) techniques? Today's weapon of choice for hackers is stealthy malware with remote control channels, preferably with autonomous worm capabilities, installed through client-side exploits. While other courses focus on detection or remediation, the goal of this course is to prevent the infection in the first place (after all, first things first).

Especially in Server 2012 and beyond, PowerShell dominates Windows scripting and automation. It seems everything can be managed through PowerShell now. And if there's a needed skill that will most benefit the career of a Windows specialist, it's being able to write PowerShell scripts, because most of your competition will lack scripting skills, so it's a great way to make your resume stand out. This course devotes an entire day to PowerShell scripting, but you don't need any prior scripting experience.

Who Should Attend

- Windows security engineers and system administrators
- Anyone who wants to learn PowerShell
- Anyone who wants to implement the 20 Critical Security Controls
- Those who must enforce security policies on Windows hosts
- Anyone who needs a whole drive encryption solution
- Those deploying or managing a PKI or smart cards
- Anyone who needs to prevent malware infections

"Windows is everywhere and security is paramount. No matter whether you hate Windows or not, SEC505 is a must."
-David Ellis,
MS Army National Guard

"I would never be able to figure all this out on my own! Jason does an excellent job clarifying concepts I'm not familiar with. Love the tools and scripts he provided and the manual is much more helpful than Microsoft books."
-Kristen Fettig, Florida Power and Light/NextEra Energy

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

Jason Fossen *SANS Faculty Fellow*

Jason Fossen is a principal security consultant at Enclave Consulting LLC, a published author, and a frequent public speaker on Microsoft security issues. He is the sole author of the SANS' week-long Securing Windows course (SEC505), maintains the Windows day of Security Essentials (SEC401.5), and has been involved in numerous other SANS' projects since 1998. He graduated from the University of Virginia, received his master's degree from the University of Texas at Austin, and holds a number of professional certifications. He currently lives in Dallas, Texas. Jason blogs about Windows Security Issues on the SANS Windows Security Blog. http://blogs.sans.org/windows-security

SECURITY 542

Web App Penetration Testing and Ethical Hacking

OFFERED AT
SANS Northern Virginia

Six-Day Program
Mon, Mar 17 - Sat, Mar 22
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Timothy Tomes

- GIAC Cert: GWAPT
- Masters Program
- Cyber Guardian

"SEC542 is an essential course for application security professionals."
-John Yamich, Exact Target

"Web apps assessment is currently what I do. SEC542 really fills in the gaps in on-the-job training."
-James Kelly, Blue Canopy LLP

"With the infinite tools used for web application penetration, SEC542 helps you understand and use the best tools for your environment."
-Linh Sithihao, UT South Western Medical Center

Assess Your Web Apps in Depth

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

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

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

Who Should Attend

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

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

Timothy Tomes *SANS Instructor*

Tim Tomes is a Senior Security Consultant and Researcher for Black Hills Information Security with experience in information technology and application development. A veteran, Tim spent nine years as an Officer in the United States Army conducting various information security related activities. Tim manages multiple open source projects such as the Recon-ng Framework, the HoneyBadger Geolocation Framework, and PushPin, is a SANS Instructor for SEC542 Web Application Penetration Testing, writes technical articles for PaulDotCom, and frequently presents at information security conferences such as ShmooCon and DerbyCon.

OFFERED AT
SANS Cyber Guardian

SECURITY 560
Network Penetration Testing and Ethical Hacking

Six-Day Program
Mon, Mar 3 - Sat, Mar 8
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

"Ed does a fantastic job teaching this course and the material is laid out better than most!"
- Jeffrey Blasnitz, FBI

"After only one day, I already feel I have a more structured approach and understanding of pen testing. Having instructors like Skoudis who are working in the real world, successfully, and also writing the course is critical to the quality of SANS courses."
-Lawrence Wolfenden, FBI

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.

SECURITY 573

Python for Penetration Testers

NEW

Five-Day Program
Mon, Mar 17 - Fri, Mar 21
9:00am - 5:00pm
30 CPE/CMU Credits
Laptop Required
Instructor: Mark Baggett

Your target has been well hardened. So far, your every attempt to compromise their network has failed. But, you did find evidence of a vulnerability, a lucky break in their defensive posture. Sadly, all of your tools have failed to successfully exploit it. Your employers demand results. What do you do when off-the-shelf tools fall short? You write your own tool.

The best penetration testers can customize existing open source tools or develop their own tools. The ability to read, write, and customize software is what distinguishes the good penetration tester from the great penetration tester. This course is designed to give you the skills you need for tweaking, customizing, or outright developing your own tools to put you on the path of becoming a great penetration tester. Again and again, organizations serious about security emphasize their need for skilled tool builders. There is a huge demand for people who can understand a problem and then rapidly develop prototype code to attack or defend against it. Join us and learn Python in-depth and fully weaponized.

Unfortunately, many penetration testers do not have these skills today. The time and effort required to develop programming skills may seem overwhelming. But it is not beyond your reach. This course is designed to meet you at your current skill level, appealing to a wide variety of backgrounds ranging from people without a drop of coding experience all the way up to skilled Python developers looking to increase their expertise and map their capabilities to penetration testing. Because you can't become a world-class tool builder by merely listening to lectures, the course is chock full of hours of hands-on labs every day that will teach you the skills required to develop serious Python programs and how to apply those skills in penetration testing engagements.

The course begins with an introduction to SANS pyWars. pyWars is a 4-day Capture the Flag competition that runs parallel to the course material. It will challenge your existing programming skills and help you develop new skills at your own individualized pace. This allows experienced programmers to quickly progress to more advanced concepts while novice programmers spend time building a strong foundation. This individualized approach allows everyone to hone their current skills making them the most lethal weapon they can be.

Who Should Attend

- Security professionals who want to learn how to develop Python applications.
- Penetration testers who want to move from being a consumer of security tools to the creator security tools
- Technolgists that need custom tools to test their infrastructure and desire to create those tools themselves

What You Will Receive With This Course

- A virtual machine with sample code and working examples
- A copy of "Violent Python"

Mark Baggett *SANS Certified Instructor*

Mark Baggett is the owner of Indepth Defense, an independent consulting firm that offers incident response and penetration testing services. He has served in a variety of roles from software developer to Chief Information Security Officer. Mark is the author of SANS Python for Penetration testers course (SEC573) and the pyWars gaming environment. Mark teaches several classes in SANS Penetration Testing curriculum including SEC504 (Incident Handing), SEC560 (Penetration Testing) and his Python course. Mark is very active in the information security community. Mark is the founding president of The Greater Augusta ISSA (Information Systems Security Association) chapter which has been extremely successful in bringing networking and educational opportunities to Augusta Information Technology workers. As part of the Pauldotcom Team, Mark generates blog content for the "pauldotcom.com" podcast . In January 2011, Mark assumed a new role as the Technical Advisor to the DoD for SANS. Today he assists various government branches in the development of information security training programs.

SECURITY 575

Mobile Device Security and Ethical Hacking

OFFERED AT
SANS Northern Virginia

Six-Day Program
Mon, Mar 17 - Sat, Mar 22
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Joshua Wright
- GIAC Cert: GMOB
- Masters Program

Who Should Attend

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

Mobile phones and tablets have become essential to enterprise and government networks, from small organizations to Fortune 500 companies and large-scale agencies. Often, mobile phone deployments grow organically, adopted by multitudes of end-users for convenient email access as well as managers and executives who need access to sensitive organizational resources from their favored personal mobile devices. In other cases, mobile phones and tablets have become critical systems for a wide variety of production applications from ERP to project management. With increased reliance on these devices, organizations are quickly recognizing that mobile phones and tablets need greater security implementations than a simple screen protector and clever password.

Whether the device is an Apple iPhone or iPad, a Windows Phone, an Android or BlackBerry phone or tablet, the ubiquitous mobile device has become a hugely attractive and vulnerable target for nefarious attackers. The use of mobile devices introduces a vast array of new risks to organizations, including:

- **Distributed sensitive data storage and access mechanisms**
- **Lack of consistent patch management and firmware updates**
- **The high probability of device loss or theft, and more.**

Mobile code and apps are also introducing new avenues for malware and data leakage, exposing critical enterprise secrets, intellectual property, and personally identifiable information assets to attackers. To further complicate matters, today there simply are not enough people with the security skills needed to manage mobile phone and tablet deployments.

This course was designed to help organizations struggling with mobile device security by equipping personnel with the skills needed to design, deploy, operate, and assess a well-managed secure mobile environment. From practical policy development to network architecture design and deployment, and mobile code analysis to penetration testing and ethical hacking, this course will help you build the critical skills necessary to support the secure deployment and use of mobile phones and tablets in your organization.

You will gain hands-on experience in designing a secure mobile phone network for local and remote users and learn how to make critical decisions to support devices effectively and securely. You will also be able to analyze and evaluate mobile software threats, and learn how attackers exploit mobile phone weaknesses so you can test the security of your own deployment. With these skills, you will be a valued mobile device security analyst, fully able to guide your organization through the challenges of securely deploying mobile devices.

"Joshua is excellent; great energy and knowledge. He also uses a great pace."
-David Crisafi - FBI

"In the fast paced world of BYOD and mobile device management, SEC575 is a must-have course for info sec managers."
-Jude Meche, DSCC

www.giac.org

www.sans.edu

Joshua Wright *SANS Senior Instructor*

Joshua Wright is a senior technical analyst with Counter Hack, a company devoted to the development of information security challenges for education, evaluation, and competition. Through his experiences as a penetration tester, Josh has worked with hundreds of organizations on attacking and defending mobile devices and wireless systems, ethically disclosing significant product and protocol security weaknesses to well-known organizations. As an open-source software advocate, Josh has conducted cutting-edge research resulting in several software tools that are commonly used to evaluate the security of widely deployed technology targeting WiFi, Bluetooth, and ZigBee wireless systems, smart grid deployments, and the Android and Apple iOS mobile device platforms. As the technical lead of the innovative CyberCity, Josh also oversees and manages the development of critical training and educational missions cyber warriors in the US military, government agencies, and critical infrastructure providers.

OFFERED AT
SANS Northern Virginia

SECURITY 579
Virtualization and Private Cloud Security

Six-Day Program
Mon, Mar 17 - Sat, Mar 22
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructors: Dave Shackleford and Chris Farrow

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.

"In one week, I am learning practical information that normally would take months to learn. Best of all, I can apply the knowledge immediately."
-Barry Lyons, Northrop Grumman

"Virtualization security can be taken for granted, but taking SEC579 will open your eyes. It's the future and not enough people understand it."
-Gordon Steuart, Wells Fargo

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.

SECURITY 760

Advanced Exploit Development for Penetration Testers

BETA

OFFERED AT
SANS Northern Virginia

Six-Day Program
Mon, Mar 17 - Sat, Mar 22
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructors: Jake Williams

Vulnerabilities in modern operating systems such as Microsoft Windows 7/8, Server 2012, and the latest Linux distributions are often very complex and subtle. Yet, they could expose organizations to significant attacks, undermining their defenses when wielded by very skilled attackers. Few security professionals have the skillset to discover let alone even understand at a fundamental level why the vulnerability exists and how to write an exploit to compromise it. Conversely, attackers must maintain this skillset regardless of the increased complexity. SANS SEC760: Advanced Exploit Development for Penetration Testers teaches the skills required to reverse engineer 32-bit and 64-bit applications, perform remote user application and kernel debugging, analyze patches for 1-day exploits, and write complex exploits, such as use-after-free attacks, against modern software and operating systems.

Who Should Attend

- Senior network and system penetration testers
- Secure application developers (C & C++)
- Reverse engineering professionals
- Senior incident handlers
- Senior threat analysts
- Vulnerability researchers
- Security researchers

"Once again, blown away by the in-depth content, just when I thought I got it, there was more info to dissect."
-Matthew Britton, BCBSLA

"SANS courses cover everything about a topic, from technical details, management considerations, to practical advice."
- Lachlon Walsh, Defence

You Will Learn

- How to write modern exploits against the Windows 7 and 8 operating systems
- How to perform complex attacks such as use-after-free, Kernel exploit techniques, one-day exploitation through patch analysis, and other advanced topics
- The importance of utilizing a Security Development Lifecycle (SDL) or Secure SDLC, along with Threat Modeling
- How to effectively utilize various debuggers and plug-ins to improve vulnerability research and speed
- How to deal with modern exploit mitigation controls aimed at thwarting success and defeating determination

Jake Williams *SANS Certified 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.

FORENSICS 408

Computer Forensic Investigations – Windows In-Depth

OFFERED AT
SANS Northern Virginia

Six-Day Program
Mon, Mar 17 - Sat, Mar 22
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Rob Lee
- GIAC Cert: GCFE
- Masters Program

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 an calling cybercrime law enforcement agents to piece together what happened in these cases.

Who Should Attend

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

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

"Hands down the BEST forensics class EVER!! Blew my mind at least once a day for 6 days!"
-Jason Jones, USAF

"The windows artifact analysis, and browser history analysis is much more inclusive in FOR408 than the training offered by other software vendors."
-Jason De Mont, Bank of America

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 8 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.

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

www.giac.org

www.sans.edu

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. Rob frequently contributes articles at the SANS Blog http://computer-forensics.sans.org.

FORENSICS 508

Advanced Computer Forensic Analysis and Incident Response

OFFERED AT
SANS Cyber Guardian

Six-Day Program
Mon, Mar 3 - Sat, Mar 8
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Jake Williams

- 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

"FOR508 is fantastic; a roller coaster barrage of forensic tools and nuances backed by real-world scenarios."
-Razi Asaduddin, ExxonMobil

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

Jake Williams *SANS Certified 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.

MANAGEMENT 414

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

OFFERED AT
SANS Northern Virginia

Six-Day Program
Mon, Mar 17 - Sat, Mar 22
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 Needed
Instructor: Eric Conrad
- GIAC Cert: GISP
- DoDD 8570

Who Should Attend

- Security professionals who are interested in understanding the concepts covered in the CISSP® exam as determined by (ISC)²
- Managers who want to understand the critical areas of network security
- System, security, and network administrators who want to understand the pragmatic applications of the CISSP® 10 Domains
- Security professionals and managers looking for practical ways the 10 domains of knowledge can be applied to the current job
- In short, if you desire a CISSP® or your job requires it, MGT414 is the training for you to get GISP certified

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

www.giac.org

www.sans.org/8570

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
- Periodic Audit of CPEs to maintain the credential

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

"This course really helped me with all 10 domain areas, and focusing on the important details. Without MGT414, there is too much information to digest."
-Michael Nowatkowski, USMA

"Eric Conrad gave great details on what the students need to focus on while taking the test. I have tested before and Eric is right on!"
-Joshuajuan Brown, DOD

"MGT414 was worth the money. I'm self-employed so I made the decision to pay and attend, definitely worth it."
-Anna Cannington, Cannon IT Services, LLC

Eric Conrad *SANS Certified Instructor*

Eric Conrad is lead author of the book "The CISSP Study Guide." Eric's career began in 1991 as a UNIX systems administrator for a small oceanographic communications company. He gained information security experience in a variety of industries, including research, education, power, Internet, and health care. He is now president of Backshore Communications, a company focusing on intrusion detection, incident handling, information warfare, and penetration testing. He is a graduate of the SANS Technology Institute with a master of science degree in information security engineering. In addition to the CISSP, he holds the prestigious GIAC Security Expert (GSE) certification as well as the GIAC GPEN, GCIH, GCIA, GCFA, GAWN, and GSEC certifications. Eric also blogs about information security at www.ericconrad.com.

MANAGEMENT 512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program
Mon, Mar 3 - Fri, Mar 7
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPE/CMU Credits
Laptop NOT Needed
Instructor: G. Mark Hardy
& Richard Porter

- 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.

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

"MGT512 gives a good understanding of what knowledge our employees need to have to be successful."
-Teddie Steele,
State Department of FCU

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!

www.giac.org

www.sans.edu

www.sans.org/8570

G. Mark Hardy *SANS Certified Instructor*

G. Mark Hardy is founder and President of National Security Corporation. He has been providing cyber security expertise to government, military, and commercial clients for over 30 years, and is an internationally recognized expert who has spoken at over 250 events world-wide. G. Mark serves on the Advisory Board of CyberWATCH, an Information Assurance/Information Security Advanced Technology Education Center of the National Science Foundation. A retired U.S. Navy Captain, he was privileged to serve in command nine times, including responsibility for leadership training for 70,000 Sailors. He also served as wartime Director, Joint Operations Center for US Pacific Command, and Assistant Director of Technology and Information Management for Naval Logistics in the Pentagon, with responsibility for INFOSEC, Public Key Infrastructure, and Internet security. Captain Hardy was awarded the Defense Superior Service Medal, the Legion of Merit, five Meritorious Service Medals, and 24 other medals and decorations. A graduate of Northwestern University, he holds a BS in Computer Science, a BA in Mathematics, a Masters in Business Administration, a Masters in Strategic Studies, and holds the GSLC, CISSP, CISM and CISA certifications.

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.

SANS CYBER GUARDIAN

Keynote: 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.

SANS CYBER GUARDIAN & SANS NORTHERN VIRGINIA

Code Injection *Jake Williams*

The technological prowess of attackers has increased dramatically over the last several years. Gone are the days when you could hope to discover malware.exe running in the process list. Attackers are migrating to code injection as a method to remain hidden from prying eyes examining process list entries.

Sure, we've all heard the term code injection or DLL injection, but what does it really mean? How does it really work? Hint: it isn't magic. However, many explanations are bereft with hand waving and pressing the "I believe" button. In this webcast, 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.

SANS CYBER GUARDIAN

How the West was Pwned *G. Mark Hardy*

Can you hear it? The giant sucking sound to the East? With it are going more than just manufacturing jobs – it's our manufacturing know-how, intellectual property, military secrets, and just about anything you can think of. If we're so technologically advanced, how are the People's Republic of China (PRC) and others able to continue to pull this off? Why do we keep getting pwned at our own game?

There has been much talk about "cyberwar," but there may not be a war. If a victor can extract tribute from the vanquished, war isn't necessary. Today, intellectual capital is a proxy for tribute. We'll look at some specifics, including documents that outline the plan of attack, details about what operations have been run against us, and progress in efforts to create an international legal framework for when the bits start flying.

SANS CYBER GUARDIAN

Continuous Ownage: Why You Need Continuous Monitoring

Eric Conrad

Repeat after me, I will be breached. Most organizations realize this fact too late, usually after a third party informs them months after the initial compromise. Treating security monitoring as a quarterly auditing process means most compromises will go undetected for weeks or months. The attacks are continuous, and the monitoring must match.

This talk will help you face this problem and describe how to move your organization to a more defensible security architecture that enables continuous security monitoring. The talk will also give you a hint at the value you and your organization will gain from attending Seth Misenar and Eric Conrad's upcoming new course: Continuous Monitoring and Security Operations.

SANS CYBER GUARDIAN & SANS NORTHERN VIRGINIA

GIAC Program Overview

GIAC certification provides assurance that a certified individual meets a minimum level of ability and possesses the skills necessary to do the job. Find out why this is important to your career.

SANS CYBER GUARDIAN & SANS NORTHERN VIRGINIA

SANS Technology Institute Open House

BONUS SESSIONS

SANS NORTHERN VIRGINIA

Keynote: **Windows Exploratory Surgery with Process Hacker** *Jason Fossen*

In this talk we'll rummage around inside the guts of Windows while on the lookout for malware, using a free tool named Process Hacker (similar to Process Explorer). Understanding processes, threads, drivers, handles, and other OS internals is important for analyzing malware, doing forensics, troubleshooting, and hardening the OS. If you have a laptop, get Process Hacker from SourceForge.net and together we'll take a peek under the GUI to learn about Windows internals and how to use Process Hacker for combating malware. http://processhacker.sourceforge.net

SANS NORTHERN VIRGINIA

Real-World Risk – What Incident Responders Can Leverage from IT Operations *Eric Conrad*

Incident Response teams can develop an early warning system to detect breaches and breach activity before an incident becomes persistent by working with system administrators. SANS Instructor Eric Conrad will show how to break the cycle of the left hand not knowing what the right hand is doing, using the framework of the 20 Critical Security Controls.

SANS NORTHERN VIRGINIA

Continuous Ownage: Why you Need Continuous Monitoring *Seth Misenar*

Repeat after me, I will be breached. Most organizations realize this fact too late, usually after a third party informs them months after the initial compromise. Treating security monitoring as a quarterly auditing process means most compromises will go undetected for weeks or months. The attacks are continuous, and the monitoring must match.

This talk will help you face this problem and describe how to move your organization to a more defensible security architecture that enables continuous security monitoring. The talk will also give you a hint at the value you and your organization will gain from attending Seth Misenar and Eric Conrad's upcoming new course: Continuous Monitoring and Security Operations.

SANS NORTHERN VIRGINIA

Detecting Deception: If Someone Was Lying To You, Would You Know It? *Michael Murr*

Most people are no better than a coin toss at detecting deception. In fact, research has shown that many of the common beliefs about lying, such as the direction you look, are flat-out wrong. This talk examines the tools and techniques that have been demonstrated to be effective, both in the lab and in the field, at assessing a person's deceptive behavior. If you want to learn how to figure out if someone is lying to you, don't miss this talk.

SANS NORTHERN VIRGINIA

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.

Vendor Showcase

10:30am-10:50am | 12:30pm-1:15pm | 3:00pm-3:20pm

Our events incorporate external vendor partners showcasing some of the best security solutions available. Take advantage of the opportunity to interact with the people behind the products and learn what they have to offer you and your organization.

SANS CYBER GUARDIAN
Tuesday, March 4

SANS NORTHERN VIRGINIA
Tuesday, March 18

SANS CYBER GUARDIAN PROGRAM

Real Threats

Real Skills

Real Success

Join Today!

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

www.sans.org/cyber-guardian

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

Prerequisites

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

Core Courses

SEC503 (GCIA) | SEC504 (GCIH) | SEC560 (GPEN) | FOR508 (GCFA)

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

Blue Team Courses

SEC502 (GPPA) | SEC505 (GCWN) | SEC506 (GCUX)

Red Team Courses

SEC542 (GWAPT) | SEC617 (GAWN) | SEC660 (GXPN)

Department of Defense Directive 8570 *(DoDD 8570)*

www.sans.org/8570

Department of Defense Directive 8570 (DoDD 8570) provides guidance and procedures for the training, certification, and management of all government employees who conduct information assurance functions in assigned duty positions. These individuals are required to carry an approved certification for their particular job classification. GIAC provides the most options in the industry for meeting 8570 requirements.

SANS Training Courses for DoDD Approved Certifications

SANS TRAINING COURSE		DoDD APPROVED CERT
SEC401	Security Essentials Bootcamp Style	GSEC
SEC501	Advanced Security Essentials – Enterprise Defender	GCED
SEC503	Intrusion Detection In-Depth	GCIA
SEC504	Hacker Techniques, Exploits, and Incident Handling	GCIH
AUD507	Auditing Networks, Perimeters, and Systems	GSNA
FOR508	Advanced Computer Forensic Analysis and Incident Response	GCFA
MGT414	SANS® +S™ Training Program for the CISSP® Certification Exam	CISSP
MGT512	SANS Security Essentials for Managers with Knowledge Compression™	GSLC

Compliance/Recertification:

To stay compliant with DoDD 8570 requirements, you must maintain your certifications. GIAC certifications are renewable every four years. Go to www.giac.org to learn more about certification renewal.

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

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

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 27 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

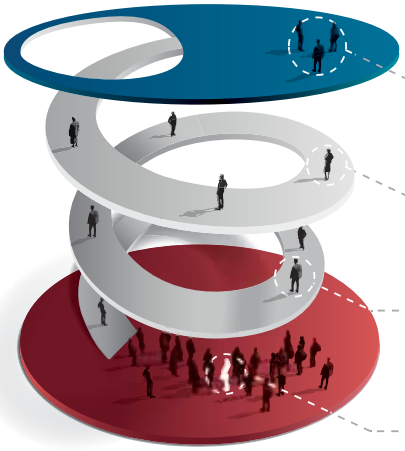
Get Certified at **www.giac.org**

SANS CyberTalent
Powered by GIAC

Contact Us to Learn More
www.sans.org/cybertalent

A Web-Based Recruitment and Talent Management Tool

Introducing SANS CyberTalent Assessments, a new web-based recruitment and talent management tool that helps validate the skills of information security professionals. This unique tool may be used during the recruitment process of new information security employees and to assess the skills of your current staff to create a professional development plan. This tool will save you money and time, as well as provide you with the information required to ensure you have the right skills on your information security team.



Benefits of SANS CyberTalent Assessments

For Recruiting
- Provides a candidate ranking table to compare the skills of each applicant
- Identifies knowledge gaps
- Saves time and money by identifying candidates with the proper skillset

For Talent Management
- Determines baseline knowledge levels
- Identifies knowledge gaps
- Helps develop a professional development plan

US and Canada 301.654.SANS (7267)
EMEA and APAC inquiries: + 44 (0) 20 3598 2363

FUTURE SANS TRAINING EVENTS

Security East 2014
New Orleans, LA
January 20-25

AppSec 2014
Austin, TX
February 3-8

CyberCon Spring 2014
Online
February 10-15

Scottsdale 2014
Scottsdale, AZ
February 17-22

dē-'fər-'kän

DFIRCON 2014
Monterey, CA
March 5-10

ICS Security
SUMMIT 2014 - ORLANDO
Lake Buena Vista, FL | March 12-18

SANS 2014
Orlando, FL
April 5-14

Austin 2014
Austin, TX
April 28 - May 3

Security West 2014
San Diego, CA
May 10-15

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

Multi-Course Training Events
Live instruction from SANS' top faculty, vendor showcase, bonus evening sessions, and networking with your peers
www.sans.org/security-training/by-location/all

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

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

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

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

ONLINE TRAINING

OnDemand
E-learning available anytime, anywhere, at your own pace
www.sans.org/ondemand

vLive
Convenient online instruction from SANS' top instructors
www.sans.org/vlive

Simulcast
Attend a SANS training event without leaving home
www.sans.org/simulcast

CyberCon
Live online training event
www.sans.org/cybercon

SelfStudy
Self-paced online training for the motivated and disciplined infosec student www.sans.org/selfstudy

HOTEL INFORMATION

SANS CYBER GUARDIAN

Training Campus
Sheraton Inner Harbor

300 South Charles Street
Baltimore, MD 21201
www.sans.org/event/cyber-guardian-2014/location

Special Hotel Rates Available

A special discounted rate of $179.00 S/D will be honored based on space availability. These rates available through February 14, 2014.

You can call the hotel directly at (410) 962-8300 or the Toll Free Starwood Reservation Hot Line at (800) 325-3535 and ask for the SANS group rate.

SANS NORTHERN VIRGINIA

Training Campus
Sheraton Reston

11810 Sunrise Valley Drive
Reston, VA 20191
www.sans.org/event/northern-virginia-2014/location

Special Hotel Rates Available

A special discounted rate of $145.00 S/D will be honored based on space availability. These rates available through March 2, 2014.

To make reservations please call (703) 620-9000 and ask for the SANS group rate.

Top 5 reasons to stay at the SANS host hotel

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

REGISTRATION INFORMATION

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

SANS CYBER GUARDIAN

REGISTER AT
www.sans.org/event/cyber-guardian-2014/courses

SANS NORTHERN VIRGINIA

REGISTER AT
www.sans.org/event/northern-virginia-2014/courses

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.

Register Early and Save

SANS CYBER GUARDIAN

Register & Pay By

DATE	DISCOUNT
January 8, 2014	**$400.00**
January 22, 2014	**$250.00**

Cancellation date: February 12, 2014

SANS NORTHERN VIRGINIA

Register & Pay By

DATE	DISCOUNT
January 22, 2014	**$400.00**
February 5, 2014	**$250.00**

Cancellation date: February 26, 2014

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 the event's cancellation date – processing fees may apply.