15 Great Courses – 2 Convenient Locations

Northern Virginia 2013

Reston, VA

April 8-13, 2013

CAPITAL SANS REGION

Cyber Guardian 2013

Baltimore, MD

April 15-20, 2013

Hands-on immersion training:

Reston, VA | April 8-13

SEC401: Security Essentials Bootcamp Style

SEC566: Implementing and Auditing the Twenty Critical Security Controls – In-Depth

SEC575: Mobile Device Security and Ethical Hacking

SEC642: Advanced Web App Penetration Testing and Ethical Hacking ***NEW!***

FOR408: Computer Forensic Investigations - Windows In-Depth

MGT512: Security Leadership Essentials For Managers with Knowledge Compression™

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

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

Baltimore, MD | April 15-20

SEC501: Advanced Security Essentials - Enterprise Defender

SEC502: Perimeter Protection In-Depth

SEC503: Intrusion Detection In-Depth

SEC504: Hacker Techniques, Exploits, and Incident Handling

SEC505: Securing Windows and Resisting Malware ***NEW!***

SEC542: Web App Penetration Testing and Ethical Hacking

SEC560: Network Penetration Testing and Ethical Hacking

FOR508: Advanced Computer Forensic Analysis and Incident Response ***NEW!***

GLOBAL INFORMATION ASSURANCE CERTIFICATION GIAC www.giac.org

GIAC Approved Training

Register at www.sans.org/event/cyber-guardian-2013

Dear Colleague,

Stephen Northcutt

Allow me to invite you to our **SANS Capital Region 2013** event. SANS is presenting two training events over two weeks in two cities near Washington D.C. The two events are **SANS Northern Virginia 2013** in Reston from April 8-13 and **SANS Cyber Guardian 2013** in Baltimore from April 15-20. These events feature top instructors from SANS who can ensure not only that you learn the material, but that you can apply it immediately when you return to the office.

SANS Northern Virginia 2013 which will be held at the **Sheraton Reston** campus with a unique lineup of seven comprehensive hands-on technical training courses from some of the best instructors in the industry. From our popular Security Essentials to our new cutting-edge course SEC642: Advanced Web App Penetration Testing and Ethical Hacking, we have the training you need. This is a chance to enroll in IT security, computer forensics, and security management courses that will improve your security skills.

SANS Cyber Guardian 2013, to be held at the **Hilton Baltimore** campus, is the SANS event that will get you on the path to becoming a *Cyber Guardian*. We are featuring all four baseline courses, plus one course for the Red Team, and two courses for the Blue Team. This doesn't mean that only *Cyber Guardian* candidates may attend. While these offerings support this program, these SANS courses are open to anyone. The event features the *NetWars Tournament* which will be held on April 18-19. *SANS NetWars* is a hands-on, interactive learning environment that enables information security professionals to develop and master the skills they need. Participants learn while working through various challenge levels, all hands-on, with a focus on skills information security professionals can use in their jobs every day.

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

Please take the time to look through the brochure, I think you will find the two events interesting and inviting—and necessary. 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! If I can help you select the course that will best boost your career, please drop me a line at **Stephen@sans.edu**.

Kind Regards,

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

"The depth of this course is amazing; it has given me a list of actual solutions to implement in a security policy, and was worth every penny. I can't wait to sign up for my next course!"
-Julie Skamangas, EWA-IIT

"I'm amazed at how much I learned – opened up a whole new world for me!"
-Erick McCroskey, Institute of Defense Analyses

"Very valuable information that I will be able to use immediately when I return to work."
-Mary Knight, NAVSEA HQ

SANS **Northern Virginia** Courses **(RESTON, VA)**

	MON 4/8	TUE 4/9	WED 4/10	THU 4/11	FRI 4/12	SAT 4/13
FOR408: Computer Forensic Investigations - Windows In-Depth	PAGE 1					
MGT414: SANS® +S™ Training Program for the CISSP® Certification Exam	PAGE 3					
MGT512: Security Leadership Essentials For Managers with Knowledge Compression™	PAGE 4					
SEC401: Security Essentials Bootcamp Style	PAGE 5					
SEC566: Implementing and Auditing the Twenty Critical Security Controls – In-Depth	PAGE 13					
SEC575: Mobile Device Security and Ethical Hacking	PAGE 14					
SEC642: Advanced Web App Penetration Testing and Ethical Hacking ***NEW!***	PAGE 15					

SANS **Cyber Guardian** Courses **(BALTIMORE, MD)**

	MON 4/15	TUE 4/16	WED 4/17	THU 4/18	FRI 4/19	SAT 4/20
FOR508: Advanced Computer Forensic Analysis and Incident Response ***NEW!***	PAGE 2					
SEC501: Advanced Security Essentials - Enterprise Defender	PAGE 6					
SEC502: Perimeter Protection In-Depth	PAGE 7					
SEC503: Intrusion Detection In-Depth	PAGE 8					
SEC504: Hacker Techniques, Exploits, and Incident Handling	PAGE 9					
SEC505: Securing Windows and Resisting Malware ***NEW!***	PAGE 10					
SEC542: Web App Penetration Testing and Ethical Hacking	PAGE 11					
SEC560: Network Penetration Testing and Ethical Hacking	PAGE 12					

FORENSICS 408

Computer Forensic Investigations – Windows In-Depth

Six-Day Program • Mon, Apr 8 - Sat, Apr 13
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Rob Lee

SANS NORTHERN VIRGINIA **RESTON, VA**

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 cybercrime law enforcement agents to piece together what happened.

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 crimes. 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, detectives
- Media exploitation analysts
- Information security managers
- Information technology lawyers and paralegals
- Anyone interested in computer forensic investigations

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

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

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

"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

Rob Lee *SANS Faculty Fellow*

Rob Lee is an entrepreneur and consultant in the Washington D.C. area and currently the Curriculum Lead and author for digital forensic and incident response training at the SANS Institute in addition to owning his own firm. Rob has more than 15 years' experience in computer forensics, vulnerability and exploit development, intrusion detection/prevention, and incident response. Rob graduated from the U.S. Air Force Academy and earned his MBA from Georgetown University. He served in the U.S. Air Force as a member of the 609th Information Warfare Squadron (IWS), the first U.S. military operational unit focused on information warfare. Later, he was a member of the Air Force Office of Special Investigations (AFOSI) where he led a team on computer crime investigations and incident response. Over the next 7 years, he worked directly with a variety of government agencies in the law enforcement, U.S. Department of Defense, and intelligence communities as the technical lead for a vulnerability discovery and exploit development team, a cyber-forensics branch, and 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 and 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**.

"FOR408 is absolutely necessary for any computer forensic type career. Excellent information!"
-Rebecca Passmore, FBI

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

www.giac.org

www.sans.edu

FORENSICS 508

Advanced Computer Forensic Analysis and Incident Response

Six-Day Program • Mon, Apr 15 - Sat, Apr 20
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Alissa Torres

SANS CYBER GUARDIAN **BALTIMORE, MD**

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. Don't miss the NEW FOR508!

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: Advanced Computer Forensic Analysis and Incident Response 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?**

The updated FOR508 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 was 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.

"Everything you need to learn for the basics of forensics in just six days; any more knowledge and your head would explode!"

-Matthew Harvey, U.S. Department of Justice

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**

"Excellent course, invaluable hands-on experience taught by people who not only know the tools and techniques, but know their quirkiness through practical, real-world experience."

-John Alexander, U.S. Army

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

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

www.giac.org

www.sans.edu

Alissa Torres *SANS Instructor*

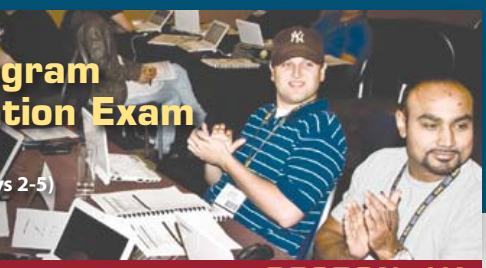
Alissa Torres currently works at Mandiant, finding evil on a daily basis. She has 10 years of technical expertise in the information technology field. Previously, she was a digital forensic investigator on a government contractor security team, performing employee investigations and incident response. She has extensive experience in information security, spanning government, academic and corporate environments, and holds a Bachelors degree from the University of Virginia and a Masters from the University of Maryland in Information Technology. Alissa has taught at the Defense Cyber Investigations Training Academy (DCITA) and various government agencies, specializing in incident response and offensive methodologies. In addition, she frequently presents at various industry conferences and currently holds the following industry certifications: GCFA, GPEN, CISSP, EnCE.

"This course doesn't just train you on tools, it teaches you about the system as a whole where important information is saved then how to extract that information."

-Kevin Lees, USNA

MANAGEMENT 414

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



Six-Day Program • Mon, Apr 8 - Sat, Apr 13
9:00am - 7:00pm (Day 1) • 8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6) • 46 CPE/CMU Credits
Laptop NOT Required • Instructor: Dr. Eric Cole

SANS NORTHERN VIRGINIA **RESTON, VA**

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.

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.
- Security professionals who want to reinforce what they learned in training and prove their skills and knowledge with a GISP certification.

Obtaining your CISSP® certification consists of:

- Fulfilling minimum requirements for professional work experience
- Completing the Candidate Agreement
- Review of 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 credentials

"I have taken several CISSP prep courses in the last several years and this by far is the best. Finally I feel that I have the confidence to take the test. Thanks." -Jerry Carse, Sarum, LLC

"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

Dr. Eric Cole *SANS Faculty Fellow*

Dr. Cole is an industry-recognized security expert with over 20 years of hands-on experience. He has experience in information technology with a focus on helping customers focus in 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. 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 the 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. Dr. Cole is an executive leader at Secure Anchor Consulting where he provides leading-edge cyber security consulting services and leads research and development initiatives to advance state-of-the-art information systems security.

"This course 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

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

GIAC INFORMATION SECURITY PROFESSIONAL GISP

www.giac.org

MANAGEMENT 512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program • Mon, Apr 8 - Fri, Apr 12
9:00am - 6:00pm (Course Days 1-4) • 9:00am - 4:00pm (Course Day 5)
33 CPE/CMU Credits • Laptop Required • Instructor: Ted Demopoulos

SANS NORTHERN VIRGINIA **RESTON, VA**

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

Author Statement

When SANS designed the Security Leadership for Managers course, we chose to emulate the format utilized by many executive MBA programs. While core source material is derived from our highly regarded SANS Security Essentials program, we decided to focus this program on the big picture of securing the enterprise: network fundamentals, security technologies, using cryptography, defense-in-depth, policy development, and management practicum. This course includes executive briefings designed to present a distilled summary of vitally important information security topics like operating system security and security threat forecasts. Ultimately, the goal of this program is to ensure that managers charged with the responsibility for information security can make informed choices and decisions that will improve their organization's security.

-Stephen Northcutt

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

Ted Demopoulos *SANS Certified Instructor*

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

www.giac.org

www.sans.edu

SECURITY 401

SANS Security Essentials Bootcamp Style

Six-Day Program • Mon, Apr 8 - Sat, Apr 13
9:00am - 7:00pm (Days 1-5) • 9:00am - 5:00pm (Day 6)
46 CPE/CMU Credits • Laptop Required
Instructor: Eric Conrad

SANS NORTHERN VIRGINIA **RESTON, VA**

It seems wherever you turn organizations are being broken into, and the fundamental question that everyone wants to know is: Why? Why do some organizations get broken into and others not. Organizations are spending millions of dollars on security and are still compromised. The problem is they are doing good things but not the right things. Good things will lay a solid foundation, but the right things will stop your organization from being headline news in the Wall Street Journal. SEC401's focus is to teach individuals the essential skills, methods, tricks, tools and techniques needed to protect and secure an organization's critical information assets and business systems. SEC401 Security Essentials 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 additional 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 be given techniques that you can implement today and tomorrow to keep your organization at the cutting edge of cyber security. Most importantly, your organization will be secure because students will have the skill sets to use the tools to implement effective security.

Who Should Attend:

- **Security professionals who want to fill the gaps in their understanding of technical information security**
- **Managers who want to understand information security beyond simple terminology and concepts**
- **Operations personnel who do not have security as their primary job function but need an understanding of security to be effective**
- **IT engineers and supervisors who need to know how to build a defensible network against attacks**
- **Administrators responsible for building and maintaining systems that are being targeted by attackers**
- **Forensic, penetration testers, auditors who need a solid foundational 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 organizations are going to be targeted. 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. An effective solution uses tools to achieve a key motto of "Prevention is Ideal but Detection is a Must". Before your organization spends a dollar of its IT budget or allocates any resources or time on 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 in on the right areas of defense. By attending SEC401 you will learn the language, tools and methods for effective computer security. The course will help you understand why security is important and how it applies to your job. In addition, you will learn 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. This course meets both of the key promises SANS makes to our students: (1) You will gain up-to-the-minute knowledge you can put into practice immediately upon returning to work; and, (2) You will be taught by the best security instructors in the industry.

"I'm a newbie to security. This course presented a ton of information on this subject in a fast-paced, easy-to-understand manner." -Michael Horkan, Rockwell Automation

Eric Conrad *SANS Certified Instructor*

Certified SANS 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**.

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

GIAC SECURITY ESSENTIALS CERTIFICATION GSEC

www.giac.org

SANS TECHNOLOGY INSTITUTE KNOWLEDGE FOR PEACE

www.sans.edu

sapere aude

www.sans.org/cyber-guardian

SECURITY 501

Advanced Security Essentials – Enterprise Defender

Six-Day Program • Mon, Apr 15 - Sat, Apr 20
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Dr. Eric Cole

SANS CYBER GUARDIAN — BALTIMORE, MD

Cyber security 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. SEC501: Advanced Security Essentials – Enterprise Defender lays a solid foundation for the security practitioner to engage the battle.

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

"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 becomes 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 indications 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. By understanding how the attacker broke in, this can be fed back into more effective and robust preventive and detective measures, completing the security lifecycle.

"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

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

Dr. Eric Cole *SANS Faculty Fellow*

Dr. Cole is an industry-recognized security expert with over 20 years of hands-on experience. He has experience in information technology with a focus on helping customers focus in 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. 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 the 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. Dr. Cole is an executive leader at Secure Anchor Consulting where he provides leading-edge cyber security consulting services and leads research and development initiatives to advance state-of-the-art information systems security.

"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

GIAC CERTIFIED ENTERPRISE DEFENDER GCED
www.giac.org

SANS TECHNOLOGY INSTITUTE KNOWLEDGE FOR PEACE
www.sans.edu

SECURITY 502

Perimeter Protection In-Depth

Six-Day Program • Mon, Apr 15 - Sat, Apr 20
9:00am - 7:00pm (Days 1-5) • 9:00am - 5:00pm (Day 6)
46 CPE/CMU Credits • Laptop Required
Instructor: Tanya Baccam

SANS CYBER GUARDIAN **BALTIMORE, MD**

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 operating system 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.

The course starts by looking at common problems. 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. We spend quite a bit of time learning about IP. To secure your network you really need to understand the idiosyncrasies of the protocol. Once you have an understanding of the complexities of IP, we'll learn how to control it on the wire. We'll learn how to deploy traffic control while avoiding some of the most common mistakes.

A proper layered defense needs to include each individual host - not just the hosts exposed to access from the Internet, but hosts that have any kind of direct or indirect Internet communication capability. We'll start with OS lockdown techniques and move on to third-party tools that can permit you to do anything from sandbox insecure applications to full-blown application policy enforcement.

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.**

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 strengthen your risk management capabilities and even gain a bit of Zen empowerment.

"Tanya is well prepared and knows her topics. Great job."
-Brent Day, Cabela's

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

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

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

Tanya Baccam *SANS Senior Instructor*

Tanya is a SANS senior instructor, as well as a SANS courseware author. With more than 10 years of information security experience, Tanya has consulted with a variety of clients about their security architecture in areas such as perimeter security, network infrastructure design, system audits, Web server security, and database security. Currently, Tanya provides a variety of security consulting services for clients, including system audits, vulnerability and risk assessments, database assessments, Web application assessments, and penetration testing. She has previously worked as the director of assurance services for a security services consulting firm and served as the manager of infrastructure security for a healthcare organization. She also served as a manager at Deloitte & Touche in the Security Services practice. Tanya has played an integral role in developing multiple business applications and currently holds the CPA, GIAC GCFW, GIAC GCIH, CISSP, CISM, CISA, CCNA, and OCP DBA certifications. Tanya completed a bachelor of arts degree with majors in accounting, business administration and management information systems.

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

SECURITY 503

Intrusion Detection In-Depth

Six-Day Program • Mon, Apr 15 - Sat, Apr 20
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Mike Poor

SANS CYBER GUARDIAN — BALTIMORE, MD

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.

"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.

Who Should Attend:

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

"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.

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.

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

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, Apr 15 - Sat, Apr 20
9:00am - 6:30pm (Course Day 1) • 9:00am - 5:00pm (Course Days 2-6)
37 CPE/CMU Credits • Laptop Required
Instructor: John Strand

SANS CYBER GUARDIAN **BALTIMORE, MD**

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.

"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

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

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.

"The SANS 504 class, in my opinion, is the benchmark for learning; gaining a better understanding, and applying the necessary skills for defending one's network."
-William Price, The Kenjya Group

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.

"This online conference for the course is awesome. Instructors are excellent. Being able to do it from anywhere is sweet."
-Giovanni Navarrette, TDS Telecom

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

www.giac.org

John Strand *SANS Senior Instructor*

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

www.sans.edu

"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

www.sans.org/cyber-guardian

SECURITY 505

Securing Windows and Resisting Malware

Six-Day Program • Mon, Apr 15 - Sat, Apr 20
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Jason Fossen

SANS CYBER GUARDIAN **BALTIMORE, MD**

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 is the best training so far that I have received. Jason Fossen is the best and most knowledgeable Microsoft geek I have met."
-Ceferino Aratea, Jr. NAVAIR

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.

This course will also prepare you for the GIAC Certified Windows Security Administrator (GCWN) certification exam to help prove your security skills and Windows expertise.

Who Should Attend:

- Windows security engineers and system administrators
- Anyone who wants to learn PowerShell
- Anyone who wants to implement the SANS 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
- IIS administrators and webmasters with servers at risk

"All Windows administrators responsible for securing IIS should attend this course."
-Billy Taylor,
Naval Sea Logistics Center

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

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

Instructor Statement

I've happily been with SANS for over a decade, and the courses I write are always guided by two questions: 1) What do administrators need to know to secure their networks? and 2) What should administrators learn to advance their careers as IT professionals? My concern is with the health of your network and your career. As a security consultant I've seen it all (good, bad, and ugly), and my experience goes into the manuals I write for SANS and the stories I tell in seminars. The Securing Windows course is packed with interesting and useful advice that is hard or impossible to find on the Internet. We always have a good time, so I hope to meet you at the next training event! -Jason Fossen

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 Institute's 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. **www.sans.org/windows-security**

SECURITY 542

Web App Penetration Testing and Ethical Hacking

Six-Day Program • Mon, Apr 15 - Sat, Apr 20
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Kevin Johnson

SANS CYBER GUARDIAN — BALTIMORE, MD

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:

- 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

"Fun while you learn! Just don't tell your manager. Every class gives you invaluable information from real world testing you cannot find in a book."
-David Fava, The Boeing Company

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

"Kevin Johnson is one of the best instructors ever! He is so cutting-edge, he made me bleed!"
-Aamir Lakhani, World Wide Technology

Kevin Johnson *SANS Senior Instructor*

Kevin Johnson is a Senior Security Consultant with Secure Ideas. Kevin has a long history in the IT field including system administration, network architecture, and application development. He has been involved in building incident response and forensic teams, architecting security solutions for large enterprises, and penetration testing everything from government agencies to Fortune 100 companies. Kevin is an instructor and author for the SANS Institute and a contributing blogger at TheMobilityHub.

Kevin has performed a large number of trainings, briefings, and presentations for both public events and internal trainings. Kevin teaches for the SANS Institute on a number of subjects. He is the author of three classes: SEC542: Web Application Penetration Testing and Ethical Hacking; SEC642: Advanced Web Application Penetration Testing; and SEC571: Mobile Device Security. Kevin has presented at a large number of conventions, meetings, and industry events. Some examples of these are: DerbyCon, ShmooCon, DEFCON, Blackhat, ISACA, Infragard, and ISSA.

In addition, Kevin is very involved in the open source community and runs a number of open source projects. These include SamuraiWTF, a web pen-testing environment; Laudanum, a collection of injectable web payloads; Yokoso!, an infrastructure fingerprinting project; and a number of others. Kevin is also involved in MobiSec and SH5ARK. Kevin was the founder and lead of the BASE project for Snort before transitioning that to another developer.

"SEC542 is a step-by-step introduction to testing and penetrating web applications, a must for anyone who builds, maintains, or audits web systems."
-Brad Milhorn, i2P LLC

GIAC WEB APP PEN TESTER GWAPT
www.giac.org

SANS TECHNOLOGY INSTITUTE KNOWLEDGE FOR PEACE
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

SECURITY 560

Network Penetration Testing and Ethical Hacking

Six-Day Program • Mon, Apr 15 - Sat, Apr 20
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Bryce Galbraith

SANS CYBER GUARDIAN BALTIMORE, MD

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

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.

"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

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, examining 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/cyber-guardian-2013.

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

Bryce Galbraith *SANS Certified Instructor*

As a contributing author of the internationally best-selling book ***Hacking Exposed: Network Security Secrets & Solutions***, Bryce helped bring the secret world of hacking out of the darkness and into the public eye. Bryce has held security positions at global ISPs and Fortune 500 companies, he was a member of Foundstone's renowned penetration testing team and served as a senior instructor and co-author of Foundstone's ***Ultimate Hacking: Hands-On*** course series. Bryce is currently the owner of Layered Security where he and his team provide specialized vulnerability assessment and penetration testing services for clients. He teaches several of The SANS Institute's most popular courses and develops curriculum around current topics. He has taught the art of ethical hacking and countermeasures to thousands of IT professionals from a who's who of top companies, financial institutions, and government agencies around the globe. Bryce is an active member of several security-related organizations, he speaks at numerous conferences, and holds several security certifications and blogs about security issues at **http://blog.layeredsec.com**.

SECURITY 566

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

Five-Day Program • Mon, Apr 8 - Fri, Apr 12
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: James Tarala

SANS NORTHERN VIRGINIA **RESTON, VA**

SPECIAL NOTE: This in-depth course has been updated to incorporate new attack vectors published in version 4.0 of the Critical Controls released November 5, 2012. **www.sans.org/critical-security-controls**

Cybersecurity attacks are increasing and evolving so rapidly that is more difficult than ever to prevent and defend against them. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches?

As threats evolve, an organization's security should too. To enable your organization to stay on top of this ever-changing threat scenario, SANS has designed a comprehensive course on how to implement the Twenty Critical Security Controls, a prioritized, risk-based approach to security. Designed by private and public sector experts from around the world, the Controls are the best way to block known attacks and mitigate damage from successful attacks. They have been adopted by the U.S. Department of Homeland Security, state governments, universities, and numerous private firms.

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

"James does an outstanding job of providing an overview of each control as well as offering his perspective and experience, which adds a lot of value."
-Danny Tomlinson, Kapstone Paper

The Controls are specific guidelines that CISOs, CIOs, IGs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defenses. They are designed to complement existing standards, frameworks, and compliance schemes by prioritizing the most critical threat and highest payoff defenses, while providing a common baseline for action against risks that we all face.

The Controls are an effective security framework because they are based on actual attacks launched regularly against networks. Priority is given to Controls that (1) mitigate known attacks (2) address a wide variety of attacks, and (3) identify and stop attackers early in the compromise cycle.

The British government's Center for the Protection of National Infrastructure describes the Controls as the "baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence."

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

The Course: Implementing and Auditing the Twenty Critical Security Controls

SANS' in-depth, hands-on training will teach you how to master the specific techniques and tools needed to implement and audit the Critical Controls. It will help security practitioners understand not only how to stop a threat, but why the threat exists, and how to ensure that security measures deployed today will be effective against the next generation of threats. Specifically, by the end of the course students will know how to:

- **Create a strategy to successfully defend their data**
- **Implement controls to prevent data from being compromised**
- **Audit systems to ensure compliance with Critical Control standards.**

"This class is extremely valuable for any organization wanting to know where they stand on security."
-David Obrien, Costco

The course shows security professionals how to implement the controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the Controls are effectively implemented.

James Tarala *SANS Senior Instructor*

James Tarala is a principal consultant with Enclave Security and is based out of Venice, Florida. He is a regular speaker and senior instructor with the SANS Institute as well as a courseware author and editor for many SANS auditing and security courses. As a consultant, he has spent the past few years architecting large enterprise IT security and infrastructure architectures, specifically working with many Microsoft-based directory services, e-mail, terminal services, and wireless technologies. He has also spent a large amount of time consulting with organizations to assist them in their security management, operational practices, and regulatory compliance issues, and he often performs independent security audits and assists internal audit groups to develop their internal audit programs. James completed his undergraduate studies at Philadelphia Biblical University and his graduate work at the University of Maryland. He holds numerous professional certifications.

SECURITY 575

Mobile Device Security and Ethical Hacking

Six-Day Program • Mon, Apr 8 - Sat, Apr 13
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Joshua Wright

SANS NORTHERN VIRGINIA RESTON, VA

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.

Who Should Attend:

- Security personnel whose job involves assessing, deploying, or securing mobile phones and tablets
- Network and system administrators supporting mobile phones and tablets
- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills

The security risks of mobile phone and tablet device use in the workplace

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

- **distributed sensitive data storage and access mechanisms**
- **lack of consistent patch management and firmware updates**
- **the high probability of device loss or theft, and more.**

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

"With the mad rush towards mobile device adoption at the point of sale and industry regulations and laws struggling to keep up, thank goodness SANS helps companies maintain secure operations."
-Dean Altman, Discount Tire

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

From mobile device security policy development, to design and deployment, and more

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

"Sec575 offers invaluable material, Josh Wright's energy and enthusiasm are incomparable!"
-Randy Pauli, Chelan County PUD

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

Joshua Wright *SANS Senior Instructor*

Joshua Wright is an independent information security analyst and senior instructor with the SANS Institute. A widely recognized expert in the wireless security field, Josh has worked with private and government organizations to evaluate the threat surrounding wireless technology and evolving threats. As an open-source enthusiast, Josh has developed a variety of tools that can be leveraged for penetration testing and security analysis. Josh publishes his tools, papers and techniques for effective security analysis on his website at **www.willhackforsushi.com**.

"Wow. This course is everything you need to know about mobile device deployment, risks and more. Don't deploy your mobile devices without taking this course first!"
-Bryan Simon, INTEGRIS Credit Union

SECURITY 642

Advanced Web App Penetration Testing and Ethical Hacking

Six-Day Program • Mon, Apr 8 - Sat, Apr 13
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Justin Searle

SANS NORTHERN VIRGINIA **RESTON, VA**

This course is designed to teach you the advanced skills and techniques required to test web applications today. This advanced penetration testing course uses a combination of lecture, real-world experiences, and hands-on exercises to educate you in the techniques used to test the security of enterprise applications. The final day of the course culminates in a Capture the Flag event, which tests the knowledge you will have acquired the previous five days.

We will begin by exploring specific techniques and attacks to which applications are vulnerable. These techniques and attacks use advanced ideas and skills to exploit the system through various controls and protections. This learning will be accomplished through lectures and exercises using real world applications.

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

We will then explore encryption as it relates to web applications. You will learn how encryption works as well as techniques to identify the type of encryption in use within the application. Additionally, you will learn methods for exploiting or abusing this encryption, again through lecture and labs.

The next day of class will focus on how to identify web application firewalls, filtering, and other protection techniques. You will then learn methods to bypass these controls in order to exploit the system. You'll also gain skills in exploiting the control itself to further the evaluation of the security within the application.

"Thank you for offering this class. It has been a tremendous assistance to me in strengthening my web app pen testing skills."

-Mark Geeslin, Citrix

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

Following these general exploits, you will learn techniques that target specific enterprise applications. You will attack systems such as content management and ticketing systems. We will explore the risks and flaws found within these systems and how to better exploit them. This part of the course will also include web services and mobile applications due to their prevalence within modern organizations.

This information-packed advanced pen testing course will wrap up with a full day Capture the Flag (CtF) event. This CtF will target an imaginary organization's web applications and will include both Internet and intranet applications of various technologies. This event is designed to allow you to put the pieces together from the previous five days reinforcing the information and learning you will have gained.

The SANS promise is that you will be able to use these ideas immediately upon returning to the office in order to better perform penetration tests of your web applications and related infrastructure. This course will enhance your exploitation and defense skill sets as well as fulfill a need to teach more advanced techniques than can be covered in the foundational course, SEC542: Web Application Penetration Testing and Ethical Hacking.

"Outstanding course!! It is great to have an opportunity to learn the material from someone who is extremely relevant in the field and is able to impart the value of his experiences."

-Bobby Bryant, DoD

Justin Searle *SANS Certified Instructor*

Justin is a Managing Partner of UtiliSec, specializing in Smart Grid security architecture design and penetration testing. Justin led the Smart Grid Security Architecture group in the creation of NIST Interagency Report 7628 and currently plays key roles in the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG), National Electric Sector Cybersecurity Organization Resources (NESCOR), and Smart Grid Interoperability Panel (SGIP). Justin has taught courses in hacking techniques, forensics, networking, and intrusion detection for multiple universities, corporations, and security conferences, and is currently an instructor for the SANS Institute. In addition to electric power industry conferences, Justin frequently presents at top security conferences such as Black Hat, DEFCON, OWASP, and AusCERT. Justin co-leads prominent open source projects including the Samurai Web Testing Framework, Middler, Yokoso!, and Laudanum. Justin has an MBA in International Technology and is a CISSP and SANS GIAC certified Incident Handler (GCIH), Intrusion Analyst (GCIA), and Web Application Penetration Tester (GWAPT).

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.

RESTON & BALTIMORE

APT: It is Not Time to Pray, It is Time to Act *Dr. Eric Cole*

Albert Einstein said "We cannot solve our problems with the same thinking we used when we created them." With the new advanced and emerging threat vectors that are breaking into networks with relative ease, a new approach to security is required. The myth that these attacks are so stealthy they cannot be stopped is just not true. There is no such thing as an unstoppable adversary. It is not time to pray, it is time to act. In this engaging talk one of the experts on the advanced persistent threat (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.

RESTON

Infosec Rock Star: How to be a More Effective Security Professional *Ted Demopoulos*

Why are some of us much more effective than others? A very few of us are so effective, and well known, that we might even be called the rock stars of our industry. Now we personally may never be swamped by groupies, but we can learn the skills be more effective, well respected, and well paid. Obviously it's not just about technology; in fact most of us are very good at the technology part. And although the myth of the Geek with zero social skills is just that, a myth, the fact is that increasing our skills more on social and business side will make most of us more effective at what we do than learning how to read hex better while standing on our heads, becoming 'One with Metasploit' or understanding the latest hot technologies.

RESTON

Pentesting Web Apps with Python *Justin Searle*

Interested in expanding your scripting skills to further customize your penetration testing approach? The goal of this talk is to teach you basic python skills you can use every day. Join one of the SamuraiWTF project leads and learn how to interact with websites using python scripts and python shells. Understand the differences between the major HTTP libraries like httplib and urllib2. Walk through sample code that performs username harvesting and dictionary attacks. Learn how to use Python's multithreaded features to speed up your scripts. And most importantly, discover PyCIT, a new opensource project that provides simple, documented, and functional python templates to accelerate your python scripting efforts.

RESTON

Practical, Efficient Unix Auditing: With Scripts *James Tarala*

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

For dates, times, and complete information, please visit www.sans.org/event/northern-virginia-2013/bonus-sessions or www.sans.org/event/cyber-guardian-2013/bonus-sessions

A True Hands-On Interactive Security Challenge!

NetWars is a computer and network security challenge designed to test a participant's experience and skills in a safe, controlled environment while having a little fun with your fellow IT security professionals.

The NetWars competition will be played over two evenings: Thursday, April 18 - Friday, April 19.

Prizes will be awarded at the conclusion of the games.

REGISTRATION IS LIMITED AND IS FREE for students attending any long course at SANS Northern Virginia 2013 or SANS Cyber Guardian 2013 *(NON-STUDENT ENTRANCE FEE IS $999).*

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

Financial aid is available; please contact us at www.sans.edu, info@sans.edu, or (720) 941-4932 to learn more.

If you are interested in an STI master's degree but have not completed your bachelor's degree, STI now offers degree completion with our partner Excelsior College.

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

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

Future SANS Training Events

SANS **Scottsdale** 2013
Scottsdale, AZ
February 17-23, 2013
www.sans.org/event/scottsdale-2013

SANS 2013
Orlando, FL
March 8-15, 2013
www.sans.org/event/sans-2013

SANS **AppSec** Summit 2013
Austin, TX
April 22-27, 2013
www.sans.org/event/appsec-2013

SANS **Security West** 2013
San Diego, CA
May 7-16, 2013
www.sans.org/event/security-west-2013

SANS **Austin** 2013
Austin, TX
May 19-24 , 2013
www.sans.org/event/austin-2013

SANSFIRE 2013
Washington, DC
June 15-22, 2013
www.sans.org/event/sansfire-2013

SANS Training Formats

LIVE CLASSROM

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

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
All the Course Content at Your Own Pace
www.sans.org/ondemand

vLive
Virtual Live Training from Your Home or Office
www.sans.org/vlive

Simulcast
Attend Event Training From Your Location
www.sans.org/simulcast

CyberCon
Virtual Conference
www.sans.org/event/cybercon-2013

SelfStudy
Independent Study with Books and MP3s
www.sans.org/selfstudy

SANS Northern Virginia 2013

Hotel Information

Conference Location

Sheraton Reston

11810 Sunrise Valley Drive • Reston, VA 20191
Phone: 703-620-9000 • Fax: 703-620-0024

Special Hotel Rates Available

A special discounted rate of $142.00 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 March 24, 2013. To make reservations please call (703) 620-9000 and ask for the SANS group rate.

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

The hotel will require a major credit card to guarantee your reservation. To cancel your reservation, you must notify the hotel at least 72 hours before your planned arrival date.

Top 5 reasons to stay at the Sheraton Reston 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 Sheraton Reston 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 Sheraton Reston Hotel that you won't want to miss!
5. Everything is in one convenient location!

SANS Northern Virginia 2013

Registration Information

We recommend you register early to ensure you get your first choice of courses.
Register online at www.sans.org/event/northern-virginia-2013

To register, go to www.sans.org/event/northern-virginia-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 March 13, 2013. There is a $300 cancellation fee per registration.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	**2/20/13**	**$500.00**	**3/6/13**	**$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

SANS Cyber Guardian 2013

Hotel Information

Conference Location

Hilton Baltimore

401 W. Pratt Street • Baltimore, MD 21201
Phone: 1-443-573-8700

Special Hotel Rates Available

A special discounted rate of $215.00 S/D will be honored based on space availability. Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through March 21, 2013. To make reservations please call (800) HILTONS (800-445-8667) and ask for the SANS group rate.

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

The hotel will require a major credit card to guarantee your reservation. To cancel your reservation, you must notify the hotel at least 72 hours before your planned arrival date.

Top 5 reasons to stay at the Hilton Baltimore

1. All SANS attendees receive complimentary high-speed Internet when booking in the SANS block.
2. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
3. By staying at the Hilton Baltimore, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.
4. SANS schedules morning and evening events at the Hilton Baltimore that you won't want to miss!
5. Everything is in one convenient location!

SANS Cyber Guardian 2013

Registration Information

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

Register online at www.sans.org/event/cyber-guardian-2013

To register, go to www.sans.org/event/cyber-guardian-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 March 20, 2013. There is a $300 cancellation fee per registration.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	**2/27/13**	**$500.00**	**3/13/13**	**$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