SANS

THE MOST TRUSTED NAME IN INFORMATION
AND SOFTWARE SECURITY TRAINING

Austin 2013

Austin, TX • May 19-24, 2013

Hands-on immersion training programs, including:

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

Virtualization and Private Cloud Security

Computer Forensic Investigations – Windows In-Depth

IT Security Strategic Planning, Policy and Leadership

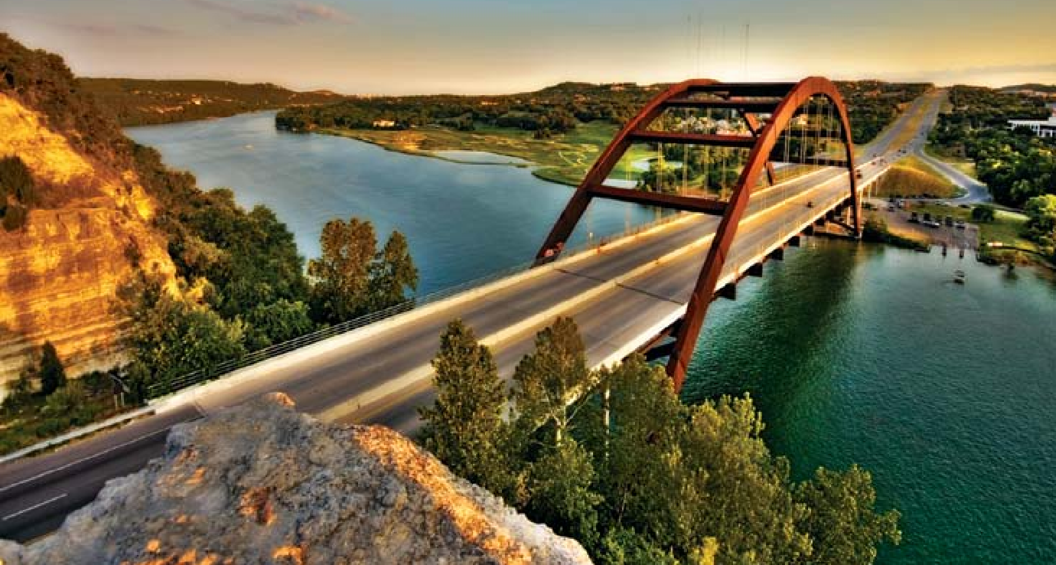
*"I said it back in 2004 and it still holds true today;
SANS offers the best training in the industry."*

-BRIAN HUGHES, USDA

Register at
**www.sans.org/
event/austin-2013**

GLOBAL INFORMATION ASSURANCE CERTIFICATION
GIAC
www.giac.org

GIAC Approved Training



Dear Colleague,

Allow me to invite you to our first **SANS Austin 2013** training event. We will be at the **Omni Hotel Downtown Austin** campus on **May 19-24**. Enhance your skills by taking advantage of this hands-on training, presented by security industry leaders, Dr. Eric Cole, Paul A. Henry, Kevin Fiscus, Mike Pilkington, along with me. We will ensure that you not only learn the material, but that you can also apply it immediately when you return to the office. You'll see why SANS is the most trusted source in computer security training, certification, and research.

Please take the time to look through the brochure, I think you will find this event interesting and inviting. Don't miss information about our evening events and talks that enhance your training. This brochure will walk you through course descriptions and instructor bios. You will find information about the *GIAC Certifications* that you can earn in addition to your training. Three of our courses offered at SANS Austin 2013 are associated with a *GIAC Certification* and SEC401 and SEC504 are aligned with *DoD Directive 8570*. Four of our courses (SEC401, SEC504, FOR408, and SEC514) will help you earn your *Master's Degree at SANS Technology Institute (STI)*. This brochure will provide you with information about why you should apply!

Our campus, Omni Hotel Downtown Austin, is in the city that is known as the "Live Music Capital of the World." With more than 100 locations that feature music, you are sure to find the entertainment that you enjoy. Choose from jazz and rock, or blues, country, reggae, or tejano.

A special discounted rate of $204 Single/Double will be honored at the Omni Austin Hotel Downtown based on space availability, and this rate includes high-speed Internet in your room. Government per diem rooms are available with proper ID; you must call the hotel and specifically ask for this rate. Make your reservations now, as this special rate is only available through April 26, 2013.

Receive a discount of up to $500 for any full course paid for by Wednesday, April 3, 2013!

Kind Regards,

Stephen Northcutt

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

Stephen Northcutt

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

"Awesome course, why look elsewhere for training."
-Vincent Bartsch, Cubic Transportation

"This is where technology is going. Cutting edge stuff. I'm never disappointed with SAN'S courses and instructors."
-Brian Houlihan, National Credit Union Administration

"The course 'dug deep' using tools (FTK imager) I've used for years and showed me features I was never aware of."
-Shawn Dorsey, U.S. Naval Criminal Investigative Service

Courses-at-a-Glance

		FRI 5/19	SAT 5/20	SUN 5/21	MON 5/22	TUE 5/23	WED 5/24
SEC401	Security Essentials Bootcamp Style	PAGE 1					
SEC504	Hacker Techniques, Exploits, and Incident Handling	PAGE 2					
SEC579	Virtualization and Private Cloud Security	PAGE 3					
FOR408	Computer Forensic Investigations – Windows In-Depth	PAGE 4					
MGT514	IT Security Strategic Planning, Policy, and Leadership	PAGE 5					

SECURITY 401

Security Essentials Bootcamp Style

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

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

With the APT (advanced persistent threat), organizations are going to be targeted. Whether the attacker is successful penetrating an organization's network depends on the organization's defense. While defending against attacks is an ongoing challenge with new threats emerging all of the time, including the next generation of threats, organizations need to understand what works in cyber security. What has worked and will always work is taking a risk-based approach to cyber defense. Before your organization spends a dollar of its IT budget or allocates any resources or time 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 on the right areas of defense. By attending SEC401 you will learn the language and underlying theory of computer security. Since all jobs today require an understanding of security, this course will help you understand why security is important and how it applies to your job. In addition, you will gain the essential, up-to-the-minute knowledge and skills required for effective security if you are given the responsibility for securing systems and/or organizations. This course meets both of the key promises SANS makes to our students: (1) You will gain cutting-edge knowledge you can put into practice immediately upon returning to work; and, (2) You will be taught by the best security instructors in the industry.

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

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

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

Dr. Eric Cole *SANS Faculty Fellow*

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

SECURITY 504

Hacker Techniques, Exploits, and Incident Handling

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

If your organization has an Internet connection or one or two disgruntled employees (and whose doesn't!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth.

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

By helping you understand attackers' tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan, the in-depth information in this course helps you turn the tables on computer attackers. This course addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still so prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course includes a time-tested, step-by-step process for responding to computer incidents; a detailed description of how attackers undermine systems so you can prepare, detect, and respond to them; and a hands-on workshop for discovering holes before the bad guys do. Additionally, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence.

This challenging course is particularly well-suited to individuals who lead or are a part of an incident handling team. Furthermore, general security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, detect, and respond to attacks.

Who Should Attend:

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

> *"The 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

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

Kevin Fiscus *SANS Faculty Fellow*

Kevin Fiscus is the Director of NWN Corporation's NProtect national security practice with experience in the performance of security and risk assessments, vulnerability and penetration testing, security program design, policy development, security awareness and the implementation of a wide range of security technologies. Kevin currently holds the GCFA, GCFW, GCIA, GCIH, GCWN, GSEC, GAWN, CISSP, CISA, RCSE, SCSA and SnortCP certifications and has taught a variety of SANS events including multiple Stay Sharp classes, SEC504, FOR508 and MGT414.

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

GIAC Certified Incident Handler GCIH
www.giac.org

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

SECURITY 579

Virtualization and Private Cloud Security

Six-Day Program • Sun, May 19 - Fri, May 24
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop provided during class • Instructor: Paul A. Henry

Who Should Attend:

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

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

Server virtualization vulnerabilities

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

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

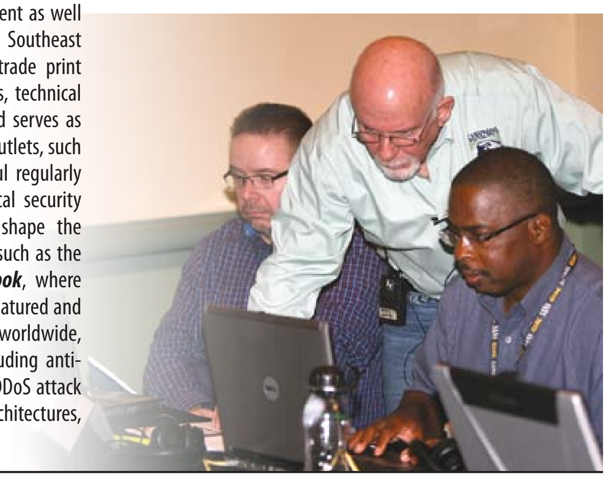
In addition, many organizations are evolving virtualized infrastructure into private clouds - internal shared services running on virtualized infrastructure. Security architecture, policies, and processes will need to adapt to work within a cloud infrastructure, and there are many changes that security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

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

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

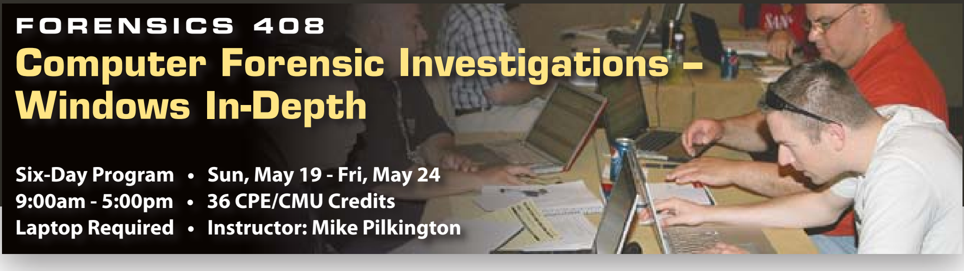
Paul A. Henry *SANS Senior Instructor*

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



FORENSICS 408

Computer Forensic Investigations – Windows In-Depth



Six-Day Program • Sun, May 19 - Fri, May 24
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Mike Pilkington

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 in these cases.

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

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

Who Should Attend:

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

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

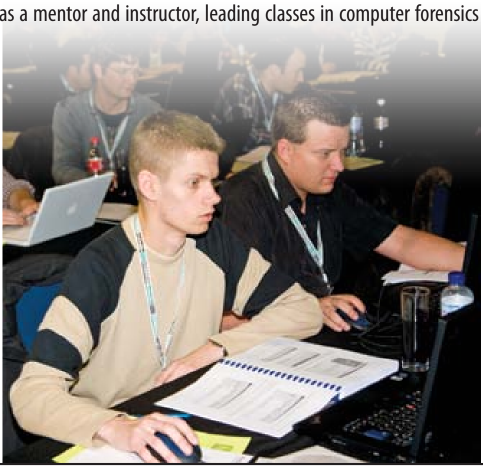
Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/austin-2013.

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

Mike Pilkington *SANS Instructor*

Mike Pilkington is a Senior Security Consultant for a Fortune 500 company in the oil & gas industry. He has been an IT professional since graduating in 1996 from the University of Texas with a B.S. in Mechanical Engineering. Since joining his company in 1997, he has been involved in software quality assurance, systems administration, network administration, and information security. Mike currently serves as a lead responder on the company's intrusion detection and incident response team. Outside the office, Mike has been involved with the SANS Institute as a mentor and instructor, leading classes in computer forensics and wireless security. He has also held over a dozen IT certifications, including those from Microsoft (MSCE), Cisco (CCNP, CCDP), Check Point (CCSA), Guidance (EnCE), SANS (GCFA, GCFE, GREM, GCIA, GCIH, GAWN, GSNA), and ISC² (CISSP).



> *"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

MANAGEMENT 514

IT Security Strategic Planning, Policy, and Leadership

Five-Day Program • Sun, May 19 - Fri, May 24
9:00am - 5:00pm • 30 CPE/CMU Credits
Laptop Recommended • Instructor: Stephen Northcutt

Strategic planning is hard for people in IT and IT Security because we spend so much time responding and reacting. Some of us have been exposed to a SWOT or something similar in an MBA course, but we almost never get to practice until we get promoted to a senior position, and then we are not equipped with the skills we need to run with the pack.

In this course you will learn the entire strategic planning process: what it is and how to do it; what lends itself to virtual teams; and what needs to be done face to face. We will practice building those skills in class. Topics covered in depth include how to plan the plan, horizon analysis, visioning, environmental scans (SWOT, PEST, Porter's etc.), historical analysis, mission, vision, and value statements. We will also discuss the planning process core, candidate initiatives, the prioritization process, resource and IT change management in planning, how to build the roadmap, setting up assessments, and revising the plan.

Who Should Attend:

This course is designed and taught for existing, recently appointed, and aspiring IT and IT Security managers and supervisors who desire to enhance their leadership and governance skills to develop their staff into a more productive and cohesive team.

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

Policy is a manager's opportunity to express expectations for the workforce, to set the boundaries of acceptable behavior and empower people to do what they ought to be doing. It is easy to get wrong. Have you ever seen a policy and your response was, "No way, I am not going to do that?" Policy must be aligned with an organization's culture. We will break down the steps to policy development so that you have the ability to develop and assess policy successfully.

The third focus of the course is on management and leadership competencies. Leadership is a capability that must be learned, exercised and developed to better ensure organizational success. Strong leadership is brought about primarily through selfless devotion to the organization and staff, tireless effort in setting the example, and the vision to see and effectively use available resources toward the end goal. However, leaders and followers influence each other toward the goal; it is a two-way street where all parties perform their functions to reach a common objective.

www.sans.edu

Effective leadership entails persuading team members to accomplish their objectives while removing obstacles and maintaining the well-being of the team in support of the organization's mission. Grooming effective leaders is critical to all types of organizations, as the most effective teams are cohesive units that work together toward common goals with camaraderie and a can-do spirit!

Leadership tends to be a bit "squishy" and courses covering the topic are often based upon the opinions of people who were successful in the marketplace. However, success can be as much a factor of luck as skill, so we base this part of the course on five decades of the research of social scientists and their experiments going as far back as Maslow and on research as current as Sunstein and Thaler. We discuss leadership skills that apply to commercial business, non-profit, for-profit, or other organizations. This course is designed to develop existing and new supervisors and managers who aspire to go beyond being the boss. It will help you build leadership skills to enhance the organization's climate and team-building skills to support the organization's mission, its growth in productivity, workplace attitude/satisfaction, and staff and customer relationships.

Stephen Northcutt *SANS Faculty Fellow*

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

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 in matter in computer security, and get the most for your training dollar.

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 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.

Everything I know is wrong! How to lead a security team in a time of unprecedented change and challenge. *Stephen Northcutt*

Strong cryptography done correctly can't be defeated! Wrong: a practical attack was published in 2009 against 10 round AES 256, and a theoretical attack against 14 round was published in 2010; quantum key distribution first proved to be flawed in May 2010; and, new attacks continue to be developed. You have to have anti-virus! Well, fine, but it no longer works in a world that generates 30k new variations of malware some days. You should never have more than one service on a server. What about blades and virtualization? Data centers must have raised floors; funny, ours uses risers instead. Hmmm, we read about organizations switching to the iPhone/iPad all the time, Apple must have done something right.

Evolving Threats *Paul A. Henry*

For nearly two decades defenders have fallen into the "Crowd Mentality Trap" and have simply settled on doing the same thing everyone else was doing. While at the same time attackers have clearly evolved both in terms of malware delivery vectors and attack methodology. Today our defenses focus primarily on the gateway and upon attempting to outwit attackers delivery methods. This leaves us woefully exposed and according to a recent Data Breach Report has resulted in 3,765 incidents, 806 million records exposed, and $157 billion (USD) in data breach costs in only the past 6 years.

Privileged Domain Account Protection: How to Limit Credentials Exposure *Mike Pilkington*

In most enterprise networks, there are a number of privileged accounts that are used for maintaining the Windows domain, including accounts for domain administration, configuration management, patch management, vulnerability analysis, and of course incident response. In all of these cases, the accounts have the ability to logon to most, if not all, Windows hosts in the environment. These accounts therefore become high-value targets for attackers. In order to protect these privileged domain accounts, it is important to have a solid understanding of the various circumstances that can expose domain account credentials. In this presentation, I will discuss what you can and cannot do safely with domain accounts. In particular, I will cover attacks against password hashes, security support providers, access tokens, and network authentication protocols. I will then provide a set of recommendations that you can follow to mitigate the risks and protect those privileged domain account credentials in your environment.

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

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

How Are You Protecting Your

Data?

Network?

Systems?

Critical Infrastructure?

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

GIAC offers over 20 specialized certifications in security, forensics, penetration testing, web application security, 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

Learn more about GIAC and how to *Get Certified* at **www.giac.org**

GLOBAL INFORMATION ASSURANCE CERTIFICATION GIAC www.giac.org

What's Your Next Career Move?

The information security field is growing and maturing rapidly; are you positioned to win? A Master's Degree in Information Security from the SANS Technology Institute will help you build knowledge and skills in management or technical engineering.

STI offers two unique master's degree programs:

Master of Science in Information Security Engineering

Master of Science in Information Security Management

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

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.
www.sans.edu

SANS TECHNOLOGY INSTITUTE
KNOWLEDGE FOR PEACE
SCIENTIA PRO PACE

www.sans.edu
info@sans.edu
720.941.4932

Four of the courses being offered at SANS Austin 2013 may be applied towards an STI master's degree.

Department of Defense Directive 8570 *(DoD 8570)*

www.sans.org/8570

DoD 8570 is changing to 8140 in 2013

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 8570/8140 requirements.

DoD Approved Baseline Certifications

IAT Level I	IAT Level II	IAT Level III
A+-CE Network+CE SSCP	**GSEC** Security+CE SSCP	**GCIH** **GSE** CISA CISSP (or Associate)

IAM Level I	IAM Level II	IAM Level III
GSLC CAP Security+CE	**GSLC** CAP CISM CISSP (or Associate)	**GSLC** CISM CISSP (or Associate)

IASAE I	IASAE II	IASAE III
CISSP (or Associate)	CISSP (or Associate)	CISSP - ISSEP CISSP - ISSAP

CNDSP Analyst	CNDSP Infrastructure Support
GCIA **GCIH** CEH	SSCP CEH

CNDSP Incident Responder	CNDSP Infrastructure Support
GCIH CSIH CEH	**GSNA** CSIA CEH

CNDSP Incident Responder
CISSP - ISSMP CISM

SANS Training Courses for DoD Approved Certifications

SANS TRAINING COURSE	DoD APPROVED CERT	SANS TRAINING COURSE	DoD APPROVED CERT
SEC401: SANS Security Essentials Bootcamp Style	GSEC	**AUD507:** Auditing Networks, Perimeters and Systems	GSNA
SEC503: Intrusion Detection In-Depth	GCIA	**MGT414:** SANS® +S™ Training Program for the CISSP® Certification Exam	CISSP
SEC504: Hacker Techniques, Exploits & Incident Handling	GCIH	**MGT512:** SANS Security Essentials for Managers with Knowledge Compression™	GSLC

*DoD 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

SANS CYBER GUARDIAN PROGRAM

www.sans.org/cyber-guardian

Stay ahead of cyber threats!

Join the SANS Cyber Guardian program today.

How the Program Works

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.

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

Program Prerequisites

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

Core Courses

SEC503	Intrusion Detection In-Depth (GCIA)
SEC504	Hacker Techniques, Exploits, and Incident Handling (GCIH)
SEC560	Network Penetration Testing and Ethical Hacking (GPEN)
FOR508	Advanced Computer Forensic Analysis & Incident Response (GCFA)

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

Blue Team Courses

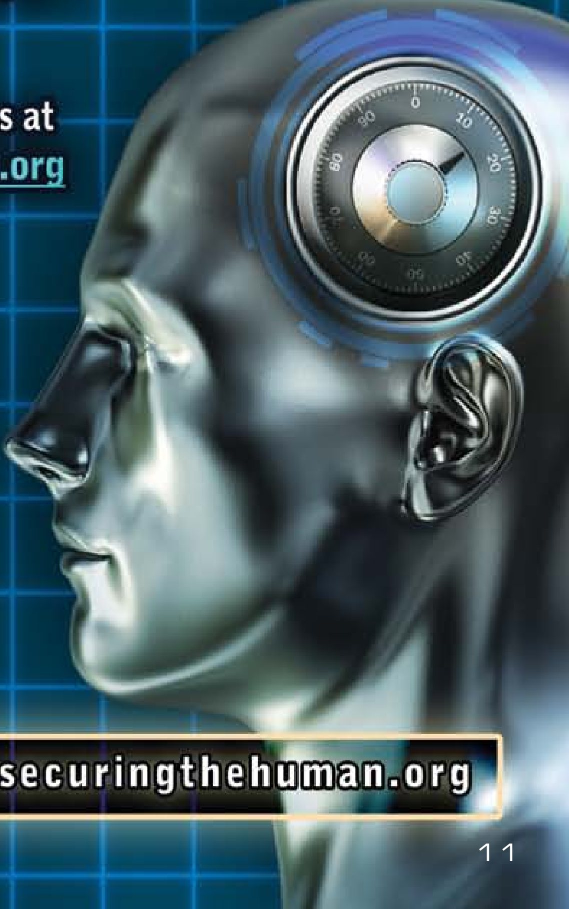
SEC502	Perimeter Protection In-Depth (GCFW)
SEC505	Securing Windows & Resisting Malware (GCWN)
SEC506	Securing Linux/Unix (GCUX)

Red Team Courses

SEC542	Web App Penetration Testing & Ethical Hacking (GWAPT)
SEC617	Wireless Ethical Hacking, Penetration Testing, and Defenses (GAWN)
SEC660	Advanced Penetration Testing, Exploits, and Ethical Hacking (GXPN)

The SANS Cyber Guardian program is a unique opportunity for information security individuals or organizational teams to develop specialized skills in incident handling, perimeter protection, forensics, and penetration testing.

For detailed information about the Cyber Guardian program, visit www.sans.org/cyber-guardian



0
10
20
30
40
50
60
70
80
90

Future SANS Training Events

SANS **Monterey** 2013

Monterey, CA
March 22-27, 2013
www.sans.org/event/monterey-2013

SANS **Northern Virginia** 2013

Reston, VA
April 8-13, 2013
www.sans.org/event/northern-virginia-2013

SANS **Cyber Guardian** 2013

Baltimore, MD
April 15-20, 2013
www.sans.org/event/cyber-guardian-2013

SANS **AppSec** 2013

Austin, TX
April 22-27, 2013
www.sans.org/event/appsec-2013

SANS CyberCon 2013
Online Training Event
Intense courses. Top instructors. No travel.

SANS **CyberCon** 2013

Online Conference
April 22-27, 2013
www.sans.org/event/cybercon-2013

SANS **Security West** 2013

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

Virtualization & Cloud Summit

Mobile Device Security Summit

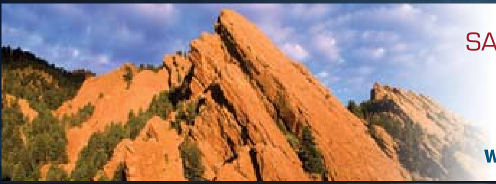
Anaheim, CA | May 30 - June 6, 2013
www.sans.org/event/mobile-device-security-summit-2013
www.sans.org/event/virtualization-cloud-summit-2013

SANSFIRE 2013

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

SANS **DFIR** SUMMIT & TRAINING 2013

Austin, TX
July 9-16, 2013
www.sans.org/event/dfir-summit-2013



SANS **Rocky Mountain** 2013

Denver, CO
July 15-20, 2013
www.sans.org/event/rocky-mountain-2013

Dates may change. Get the complete list of events at www.sans.org

SANS Austin 2013

Hotel Information

Conference Location
Omni Austin Hotel Downtown

700 San Jacinto @ 8th Street | Austin, TX 78701
Phone: 512-476-3700
www.omnihotels.com/Home/FindAHotel/AustinDowntown.aspx

Special Hotel Rates Available

A special discounted rate of $204.00 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 April 26, 2013. To make reservations please call (800) THE-OMNI (800-843-6664) 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 Omni Austin Hotel Downtown

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 Omni Austin Hotel Downtown, 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 Omni Austin Hotel Downtown that you won't want to miss!

5 Everything is in one convenient location!

SANS Austin 2013

Registration Information

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

Register online at www.sans.org/event/austin-2013

SANS
The Most Trusted Source for Information and Software Security Training

To register, go to www.sans.org/event/austin-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 April 24, 2013. There is a $300 cancellation fee per registration.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	**4/3/13**	**$500.00**	**4/17/13**	**$250.00**

Some restrictions apply.

Group Savings (Applies to tuition only)

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

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

SANS Voucher Credit Program

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