April 22-27, 2013

SANS CyberCon 2013

Online Training Event

Intense courses. Top instructors. No travel.

Choose from seven popular courses:

SEC401
Security Essentials Bootcamp Style

SEC504
Hacker Techniques, Exploits, and Incident Handling

SEC575
Mobile Device Security and Ethical Hacking

FOR408
Computer Forensic Investigations – Windows In-Depth

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

AUD444
Auditing Security & Controls of Active Directory & Windows

AUD445
Auditing Security and Controls of Oracle Databases

"I was surprised how much I liked this format (live virtual delivery). Because I have attended other SANS classes in person, I was skeptical, but I loved it."

-Jon Truan, Oak Ridge National Laboratory

SANS

Symantec

Platinum Sponsor

Register at www.sans.org/event/cybercon-2013

What is SANS CyberCon?

SANS CyberCon is a live online training event that meets in virtual classrooms, allowing students to interact directly with their classmates and instructors. SANS CyberCon students attend popular courses that are taught online by SANS' top instructors. Students also have the opportunity to attend daily bonus sessions that discuss current topics in information security. In short, SANS CyberCon is perfect for professionals who wish to keep their skills current but cannot travel due to personal or professional commitments!

Why Choose SANS CyberCon?

Key Reasons to Attend from SANS CyberCon Alumni:

Flexible – get the training you need without neglecting your family and work obligations

Zero travel costs – easier to get approved and ideal for individuals with no travel budget

Archive access – all class sessions are recorded and can be replayed for four months

CyberCon is a great way to spend voucher dollars

Courses-at-a-Glance

		MON 4/22	TUE 4/23	WED 4/24	THU 4/25	FRI 4/26	SAT 4/27
MGT414	SANS® +S™ Training Program for the CISSP® Cert Exam	PAGE 2					
SEC401	Security Essentials Bootcamp Style	PAGE 3					
SEC504	Hacker Techniques, Exploits, and Incident Handling	PAGE 4					
SEC575	Mobile Device Security and Ethical Hacking	PAGE 5					
AUD444	Auditing Security and Controls of Active Directory and Windows	PAGE 6					
AUD445	Auditing Security and Controls of Oracle Databases				PAGE 7		
FOR408	Computer Forensic Investigations – Windows In-Depth	PAGE 8					

Testimonials from SANS CyberCon Alumni

"When I was offered the opportunity to lead a new business area at my company I needed some in-depth training fast, but I was still breastfeeding my 12 week old daughter and travel was out of the question."

Robin Norris, EMC

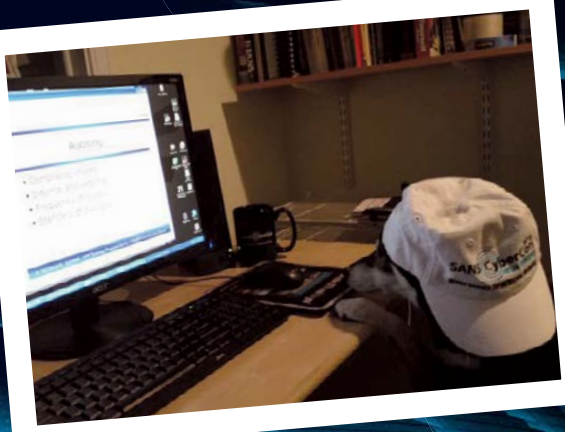


Photo Contest Winner – Pet, Figure, Toy Category

"The conference was a success and will be a great example that we at CoVantage Credit Union can use to show the feasibility of online learning."

Aaron Hurt, CoVantage Credit Union

"CyberCon was the perfect solution for me. Because it was virtual, I was able to attend class on the first day without having to cancel a weekend getaway. Also, since I was paying for this myself not having to cover travel was huge."

Mark Dirks, Steptoe & Johnson LLP

Photo Contest Runner Up – Pet, Figure, Toy Category

Photo Contest Runner Up – People Category

"I was surprised and excited to hear about SANS CyberCon which I could attend from home. I found the format to be equally beneficial to in person training and so much more fun and convenient that I am now recommending it to everyone!"

Debbie Nuttall, Praemittias Group

MANAGEMENT 414

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

Six-Day Program • Mon, Apr 22 - Sat, Apr 27
Day 1: 9:00am - 7:00pm (US Central Time Zone)
Days 2-5: 8:00am - 7:00pm (US Central Time Zone)
Day 6: 8:00am - 5:00pm (US Central Time Zone)
46 CPE/CMU Credits • Instructor: Eric Conrad

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 Resume**
- **Passing the CISSP® 250 multiple-choice question exam with a scaled score of 700 points or greater**
- **Submitting a properly completed and executed Endorsement Form**
- **Period Audit of CPEs to maintain the credential**

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

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

-Jeff Jones, Constellation Energy Group

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**.

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

-Carl Williams, Harris Corporation

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

www.giac.org

SECURITY 401

Security Essentials Bootcamp Style

Six-Day Program • Mon, Apr 22 - Sat, Apr 27
Days 1-5: 9:00am - 7:00pm (US Central Time Zone)
Day 6: 9:00am - 5:00pm (US Central Time Zone)
46 CPE/CMU Credits • Instructor: Dr. Eric Cole

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 experts, penetration testers, and 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 cutting-edge knowledge you can put into practice immediately upon returning to work; and, (2) You will be taught by the best security instructors in the industry.

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

www.giac.org

www.sans.edu

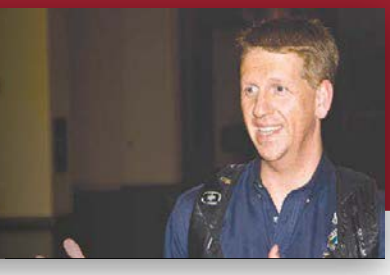
www.sans.org/cyber-guardian

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 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 in which 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 the state-of-the-art in information systems security.

SECURITY 504

Hacker Techniques, Exploits, and Incident Handling



Six-Day Program • Mon, Apr 22 - Sat, Apr 27
Day 1: 9:00am - 6:30pm (US Central Time Zone)
Days 2-6: 9:00am - 5:00pm (US Central Time Zone)
37 CPE/CMU Credits • Instructor: Bryce Galbraith

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 "old-ie-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/cybercon-2013.

www.giac.org

Bryce Galbraith *SANS Certified Instructor*

As a contributing author of the internationally bestselling 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**.

www.sans.edu

www.sans.org/cyber-guardian

"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

SECURITY 575

Mobile Device Security and Ethical Hacking

Six-Day Program • Mon, Apr 22 - Sat, Apr 27
9:00am - 5:00pm (US Central Time Zone)
36 CPE/CMU Credits • Instructor: Christopher Crowley

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.

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.

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**

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

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.

"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

Christopher Crowley *SANS Certified Instructor*

Mr. Crowley has 10 years of industry experience managing and securing networks. He has GSEC, GCIA, GCIH (gold), GCFA, and CISSP certifications. His teaching experience includes GSEC, GCIA, and GCIH Mentor; Apache web server administration and configuration; and shell programming.

He was awarded the SANS 2009 Local Mentor of the year award, "The Mentor of the Year Award is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities."

AUD444

Auditing Security and Controls of Active Directory and Windows

NEW 3-DAY COURSE!

Three-Day Program • Mon, Apr 22 - Wed, Apr 24
9:00am - 5:00pm (US Central Time Zone)
18 CPE/CMU Credits • Instructor: Tanya Baccam

Auditors need to be able to understand how Active Directory operates and the key business risks that are present. This course was written to teach auditors how to identify and assess those business risks. Active Directory and Windows systems are typically well known and utilized within organizational infrastructures. However, they can be difficult to audit since there are a large number of settings on the end system. This course provides the tools and techniques to effectively conduct an Active Directory and Windows audit, and while doing so identify key business process controls that may be missing. Students have the opportunity to look at the business process controls and then how those can be verified by looking at Active Directory and the Windows systems that exist. Plus, students are given the knowledge to be able to add additional value as part of their audits by being able to identify the technology risks that may have been overlooked. The hands-on exercises reinforce the topics discussed in order to give students the opportunity to conduct an audit on their own Windows systems, as well as understand the different security options that Windows provides.

Who Should Attend:

- Internal auditors
- IT Specialist auditors
- IT Auditors
- IT Audit managers
- Information system auditors
- Information technology auditors
- Information security officers

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

444.1 Hands On: Day One

In order to properly audit Active Directory, auditors have to have an understanding of the Active Directory architecture and the role AD plays for an organization. These foundations are more are covered in provide a solid foundation to build from throughout the course.

Topics: Windows Foundational Concepts; Active Directory Concepts; Physical, Environment and Availability Controls

444.2 Hands On: Day Two

During this day we will add to the foundational concepts we covered in the first day and get into a number of the technical details for auditing, including access controls, change and patch management, encryption and vulnerability management. We also discuss key services such as DNS, IIS, SQL Server and RDS.

Topics: Network Controls; Application Controls; Change Control, Patching, and Vulnerabilities; Access Controls

444.3 Hands On: Day Three

The final day of the course covers the last steps to include in an Active Directory and Windows effective audit program. Topics such as enabling successful auditing on the system, reviewing privileges, availability considerations, application control and service auditing are discussed.

Topics: Access Controls; Privileges; Logging and Monitoring, System Configuration, Continuous Auditing and Tools

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

You Will Be Able To:

- Query Active Directory using tools such as dsquery, csvde and more to extract audit information such as users, groups, objects, and more
- Understand the role of trusts, forests, operations masters and group policy within an Active Directory environment
- Conduct a vulnerability scan of Windows systems and identify potential audit exceptions
- Determine the current password policy and be able to verify the password policy against corporate policy
- Identify the shares being used by a system being audited and whether the shares are appropriate
- Extract the rights and privileges that are set for a host, and compare them to best practice recommendations
- Determine the audit policy in place and whether the policy is appropriate
- Use built-in tools such as WMIC, SCA and more to quickly audit a Windows system

AUD445

Auditing Security and Controls of Oracle Databases

NEW 3-DAY COURSE!

Three-Day Program • Thu, Apr 25 - Sat, Apr 27
9:00am - 5:00pm (US Central Time Zone)
18 CPE/CMU Credits • Instructor: Tanya Baccam

Over the past few years we have seen attackers target data, since there is a financial incentive to being able to compromise valuable data. The media seem to be reporting new data compromises constantly. That means auditors need to be effectively auditing the controls that should exist to protect this valuable organizational asset.

Oracle Databases often store the data that's being targeted. Oracle Databases are very complex and challenging to audit! Auditors need to be able to effectively audit the processes and controls in place around the database to ensure the asset is being properly protected and the risks properly managed.

This course provides all of the details, including the IT process, and procedural and technical controls that you as an auditor should look for when conducting an Oracle Database audit. Even better, you have the opportunity to get firsthand experience extracting and interpreting data from a live Oracle Database, which allows you to be able to return and immediately conduct an Oracle Database audit. By getting hands-on experience, you get a better understanding of exactly how an Oracle Database operates and what data is available for audit purposes. The course is also put together in such a way that you can add additional value to the business and provide further security recommendations and benefits for the database being audited.

Who Should Attend:

- Internal auditors
- IT Specialist auditors
- IT Auditors
- IT Audit managers
- Information system auditors
- Information technology auditors
- Information security officers

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

You Will Be Able To:

- Utilize SQL to write and/or run scripts as part of an Oracle database audit
- Identify the common data dictionary tables that should be queried to extract valuable audit information and evidence
- Explore Oracle database views to obtain information available
- Identify the key files on the operating system that need to be protected to properly secure an Oracle database, including the permissions that should exist for the files
- Determine which parameters have a security impact and what the parameters should be set to, and why they should be set from a security perspective
- Understand how to query the state of the listener and whether it has been properly secured
- Review whether database links are in use, and if so, whether the proper controls are in place to manage the links
- Identify whether proper password policies are being enforced within the database
- Determine the different methods for auditing and whether proper auditing has been implemented in the database

445.1 Hands On: Day One

In order to properly audit Oracle Databases, auditors have to have an understanding of what is involved in an Oracle Database and how the database operates. These foundations are more will be covered to provide a solid foundation to build from throughout the course.

Topics: Foundations; Oracle Database Concepts; Physical and Environmental Controls; Architectural and Inventory Controls; Change Control, Patch Management and Vulnerabilities; OS, Network and Application Controls

445.2 Hands On: Day Two

There are many authentication and access control options available for Oracle Databases. Auditors must understand what the options are and how they can be implemented so they are properly audited. This day begins by looking at the risks related to the listener, and then moves into the controls around authentication and access control.

Topics: Listener Security; Authentication Process and Methods; Oracle Advanced Security; Access Controls including User Accounts, Roles and Passwords

445.3 Hands On: Day Three

Continuing to build the audit program, Oracle specific risks such as links, parameters, data integrity controls and auditing will be discussed. Links provide database-to-database communication and therefore can be a risk to the database. Students understand the important privileges and parameters to look at, as well as controls that should be in place related to backups and auditing.

Topics: Links; Privileges; Triggers; Parameters; Backups, DRP, and BCP; Restricting Tools and Data Integrity Controls; Auditing

FORENSICS 408

Computer Forensic Investigations – Windows In-Depth

Six-Day Program • Mon, Apr 22 - Sat, Apr 27
9:00am - 5:00pm (US Central Time Zone)
36 CPE/CMU Credits • Instructor: Paul A. Henry

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

"Everyone in forensics who wants to learn analysis needs FOR408."
-Denisse Paz, FBI

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

Who Should Attend:

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

This 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.

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

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

www.giac.org

www.sans.edu

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

Paul A. Henry *SANS Senior Instructor*

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

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**

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 (STI) will help you build knowledge and skills in management or technical engineering.

STI offers two master's degree programs:

Master of Science in Information Security Engineering

Master of Science in Information Security Management

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

www.sans.edu

info@sans.edu

720.941.4932

Three of the courses being offered at SANS CyberCon 2013 may be applied towards an STI Master's Degree.

SANS
CYBER GUARDIAN
PROGRAM

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.

Real Threats
Real Skills
Real Success

Prerequisites

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

Core Courses

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

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

Blue Team Courses

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

Red Team Courses

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

Join Today!

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

www.sans.org/cyber-guardian

SECURITY AWARENESS
FOR THE 21st CENTURY

- Go beyond compliance and focus on changing behaviors.
- Includes videos, newsletters, posters and screen savers .
- Create your own program by choosing from 30 different training modules.
- Training meets mandated compliance requirements including PCI DSS, HIPAA, FERPA, FISMA, SOX and ISO 27001.
- Offered in over 20 languages.
- Host on SANS VLE or on your own LMS.
- For a free trial, visit us at www.securingthehuman.org or contact info@securingthehuman.org for more information.

SANS SECURING THE HUMAN

www.securingthehuman.org

SANS Training Formats

LIVE CLASSROOM TRAINING

Multi-Course Training Events
Live instruction from SANS' top faculty, vendor showcase, bonus evening sessions, and networking with your peers
www.sans.org/security-training/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
E-Learning available anytime, anywhere, at your pace
www.sans.org/ondemand

vLive
Live, Online Instruction from SANS' Top Instructors
www.sans.org/vlive

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

CyberCon
Live Online Training Event
www.sans.org/event/cybercon-2013

SelfStudy
Books and MP3 Files for Independent Learners
www.sans.org/selfstudy

SANS CyberCon 2013

Registration Information

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

How to Register

1. To register, go to www.sans.org/event/cybercon-2013.

Select your course or courses and indicate whether you plan to test for GIAC certification. If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. We do not take registrations by phone.

2. Provide payment information.

Even if you do not want to submit your payment information online, still complete the online form! There is an option to submit credit card information for payment by fax or phone once the online form is completed and you have your invoice number.

SANS ACCEPTS ONLY US and CANADIAN FEDERAL GOVERNMENT PURCHASE ORDERS

If you normally use a PO and are not part of the federal government, please see our additional PO information on the tuition information page: **www.sans.org/network-security-2012/tuition.php**

3. Print your invoice.

If you need one, you must print YOUR OWN INVOICE at the end of the online registration process. The invoice will pop up automatically when the registration is successfully submitted. You may also access your invoice at **https://portal.sans.org/history**.

4. E-mail confirmation will arrive soon after you register.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	3/6/13	$500.00	3/20/13	$250.00

Discount applies to six-day courses only.

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.

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 27, 2013. There is a $300 cancellation fee per registration.

SANS Voucher Credit Program

Expand your Training Budget!

Extend your Fiscal Year.

The SANS Discount Program that pays you credits and delivers flexibility.

www.sans.org/vouchers