SANS

The Most Trusted Name in Information and Software Security Training

Security West 2013

San Diego, CA • May 7-16, 2013

EMERGING TRENDS IN INFORMATION SECURITY

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

Network Penetration Testing and Ethical Hacking

Web App Penetration Testing and Ethical Hacking

Computer Forensic Investigations – Windows In-Depth

Security Leadership Essentials for Managers

Intrusion Detection In-Depth

Auditing Networks, Perimeters, and Systems

And more!

"SANS courses focus on what you really need to know to quickly improve the security in your organization."
-Adan Lopez Sanchez, Jazz Aviation

Register at www.sans.org/security-west-2013

Global Information Assurance Certification GIAC www.giac.org

GIAC Approved Training

Dear Colleague,

I am pleased to invite you to San Diego for "**SANS Security West 2013 – Emerging Trends in Information Security**" from May 7-16. The training event will offer more than 25 outstanding hands-on immersion courses for all security professionals in audit, security management, technical security, penetration testing, and computer forensics. The training team will be led by SANS world-class Faculty Fellows Dr. Eric Cole, David Hoelzer, Hal Pomeranz, Ed Skoudis, Rob Lee, and Jason Fossen, as well as Senior Instructors Paul A. Henry, Mike Poor, Stephen Sims, James Tarala, and many others.

This brochure is designed to provide you with all of the information you need to choose the courses at SANS Security West 2013 that best fit your training needs. The course descriptions are detailed and thorough, so please share the brochure with your colleagues or your boss to help them understand all that you will learn when you attend.

SANS Security West 2013 will focus on emerging trends and feature evening talks and a star-studded panel discussion. One of our *SANS@Night* talks will discuss tools to make Windows more secure from malware. You will also learn what the advanced persistent threat (APT) is really all about, that it is not going away, and how to create an action plan for building a network to defend against it. And you don't want to miss participating in *NetWars – Tournament Play*!

Look for our complete list of special activities, including evening talks, special events, vendor expo, welcome reception, and all of the networking opportunities that provide the ultimate SANS experience to both reinforce and enhance your training. The SANS promise is that you will not only learn how to use your problem-solving and technical skills in a safe environment, you will also be able to apply what you learn the minute you get back to your office.

Please review the complete training list on the *Courses-at-a-Glance* page. Our new cutting-edge courses being offered at SANS Security West 2013 are:

- **SEC505: Securing Windows and Resisting Malware**
- **SEC642: Advanced Web App Penetration Testing and Ethical Hacking**
- **FOR508: Advanced Computer Forensic Analysis and Incident Response**
- **FOR526: Windows Memory Forensics In-Depth**

Be sure to register by March 27, 2013 for a $500 tuition discount! For more savings, our ten short, skills-based courses are steeply discounted with the purchase of a 5-day or 6- day courses. To help you choose which courses would be the most helpful to you or your company. Our detailed format will help you focus on the courses that map to each specialty. And if you want to talk to me about it, feel free to drop me a line at Stephen@sans.edu and I'll get back to you.

Finally, have you been thinking about earning a Master's degree? Information security threats are evolving daily, and the best way to stay ahead of the new threat is continuous training to hone your skills. See this brochure to find out about the degree requirements and which courses will help launch you on your way toward an advanced degree. The brochure also provides information about earning *GIAC Certification* with your training.

SANS Security West 2013 will be held at the fabulous Manchester Grand Hyatt Hotel on the waterfront in San Diego. This destination location offers a retreat for the whole family. Explore Seaport Village, cruise the bay, walk to the Gaslamp Quarter, or visit the San Diego Zoo, Sea World, or the museums in Balboa Park.

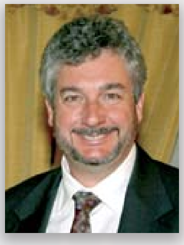
Hone your cyber skills while experiencing the best that southern California has to offer. Make your reservations now! ***A special discount rate of $207 Single/Double will be honored based on space availability, but it is only available through April 16, 2013.*** Government per diem rooms are available with proper ID; simply call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room.

Register today for SANS Security West 2013. We are looking forward to meeting you in San Diego!

Kind regards,

Stephen Northcutt

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



Stephen Northcutt

Here's what SANS Security West 2012 alumni have said about the value of SANS training:

"Since this is my first SANS course, it really opened my eyes in general to what IT security is all about. I've been in ESec for two years and now the dots are finally connecting, seeing the big clear picture."
-Joe Madamba, State Compensation Insurance Fund

"The best security training bar none!"
-John Carlson, Nelnet

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

"The sheer amount of quality professionals present set SANS apart."
-Reuben Johnson, DES, ISS, SvcOps

Courses-at-a-Glance

<table>
<tr><th colspan="2">Please check the website for an up-to-date course list at
www.sans.org/event/security-west-2013</th><th>TUE
5/7</th><th>WED
5/8</th><th>THU
5/9</th><th>FRI
5/10</th><th>SAT
5/11</th><th>SUN
5/12</th><th>MON
5/13</th><th>TUE
5/14</th><th>WED
5/15</th><th>THU
5/16</th></tr>
<tr><td>AUD507</td><td>Auditing Networks, Perimeters, and Systems</td><td></td><td></td><td colspan="6">PAGE 21</td><td></td><td></td></tr>
<tr><td>AUD521</td><td>Meeting the Minimum: PCI/DSS 2.0: Becoming and Staying Compliant</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="2">P 25</td></tr>
<tr><td>DEV522</td><td>Defending Web Applications Security Essentials</td><td></td><td></td><td colspan="6">PAGE 14</td><td></td><td></td></tr>
<tr><td>FOR408</td><td>Computer Forensic Investigations – Windows In-Depth</td><td></td><td></td><td colspan="6">PAGE 15</td><td></td><td></td></tr>
<tr><td>FOR508</td><td>Advanced Computer Forensic Analysis and Incident Response NEW!</td><td></td><td></td><td colspan="6">PAGE 16</td><td></td><td></td></tr>
<tr><td>FOR526</td><td>Windows Memory Forensics In-Depth NEW!</td><td></td><td></td><td colspan="5">PAGE 17</td><td></td><td></td><td></td></tr>
<tr><td>FOR610</td><td>Reverse-Engineering Malware: Malware Analysis Tools and Techniques</td><td></td><td></td><td colspan="5">PAGE 18</td><td></td><td></td><td></td></tr>
<tr><td>MGT305</td><td>Technical Communication and Presentation Skills for Security Professionals</td><td></td><td>P 24</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>MGT414</td><td>SANS® +S™ Training Program for the CISSP® Certification Exam</td><td></td><td></td><td colspan="6">PAGE 19 SIMULCAST</td><td></td><td></td></tr>
<tr><td>MGT415</td><td>A Practical Introduction to Risk Assessment NEW!</td><td></td><td>P 24</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>MGT433</td><td>Securing The Human: Building and Deploying an Effective Security Awareness Program</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="2">P 24</td></tr>
<tr><td>MGT512</td><td>SANS Security Leadership Essentials For Managers with Knowledge Compression™</td><td></td><td></td><td colspan="5">PAGE 20</td><td></td><td></td><td></td></tr>
<tr><td>MGT535</td><td>Incident Response Team Management</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>P 25</td><td></td></tr>
<tr><td>SEC401</td><td>Security Essentials Bootcamp Style</td><td></td><td></td><td colspan="6">PAGE 2 SIMULCAST</td><td></td><td></td></tr>
<tr><td>SEC434</td><td>Log Management In-Depth: Compliance, Security, Forensics, and Troubleshooting</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="2">P 23</td></tr>
<tr><td>SEC501</td><td>Advanced Security Essentials – Enterprise Defender</td><td></td><td></td><td colspan="6">PAGE 3</td><td></td><td></td></tr>
<tr><td>SEC503</td><td>Intrusion Detection In-Depth</td><td></td><td></td><td colspan="6">PAGE 4 SIMULCAST</td><td></td><td></td></tr>
<tr><td>SEC504</td><td>Hacker Techniques, Exploits, and Incident Handling</td><td></td><td></td><td colspan="6">PAGE 5</td><td></td><td></td></tr>
<tr><td>SEC505</td><td>Securing Windows and Resisting Malware NEW!</td><td></td><td></td><td colspan="6">PAGE 6</td><td></td><td></td></tr>
<tr><td>SEC524</td><td>Cloud Security Fundamentals</td><td colspan="2">P 22</td><td colspan="3">SIMULCAST</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>SEC546</td><td>IPv6 Essentials</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="2">P 22</td></tr>
<tr><td>SEC560</td><td>Network Penetration Testing and Ethical Hacking</td><td></td><td></td><td colspan="6">PAGE 7 SIMULCAST</td><td></td><td></td></tr>
<tr><td>SEC566</td><td>Implementing and Auditing the Twenty Critical Security Controls – In-Depth</td><td></td><td></td><td colspan="5">PAGE 8</td><td></td><td></td><td></td></tr>
<tr><td>SEC575</td><td>Mobile Device Security and Ethical Hacking</td><td></td><td></td><td colspan="6">PAGE 9</td><td></td><td></td></tr>
<tr><td>SEC579</td><td>Virtualization and Private Cloud Security</td><td></td><td></td><td colspan="6">PAGE 10</td><td></td><td></td></tr>
<tr><td>SEC580</td><td>Metasploit Kung Fu for Enterprise Pen Testing</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="2">P 23</td></tr>
<tr><td>SEC617</td><td>Wireless Ethical Hacking, Penetration Testing, and Defenses</td><td></td><td></td><td colspan="6">PAGE 11</td><td></td><td></td></tr>
<tr><td>SEC642</td><td>Advanced Web App Penetration Testing and Ethical Hacking NEW!</td><td></td><td></td><td colspan="6">PAGE 12</td><td></td><td></td></tr>
<tr><td>SEC660</td><td>Advanced Penetration Testing, Exploits, and Ethical Hacking</td><td></td><td></td><td colspan="6">PAGE 13</td><td></td><td></td></tr>
<tr><td>SEC710</td><td>Advanced Exploit Development</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="2">P 23</td></tr>
<tr><td></td><td>NetWars – Tournament Play</td><td></td><td></td><td></td><td></td><td></td><td colspan="2">P 28</td><td></td><td></td><td></td></tr>
</table>

SECURITY 401

Security Essentials Bootcamp Style

Six-Day Program • Thu, May 9 - Tue, May 14
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.

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**
- **Anyone new to information security with some background in information systems and networking**

With the APT (advanced persistent threat), organizations are going to be targeted. Whether the attacker is successful penetrating an organization's network depends on the organization's defense. While defending against attacks is an ongoing challenge with new threats emerging all of the time, including the next generation of threats, organizations need to understand what works in cyber security. What has worked and will always work is taking a risk-based approach to cyber defense. Before your organization spends a dollar of its IT budget or allocates any resources or time 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?

SANS SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast. *More info on page 28.*

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

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.

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. He has a master's degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. Dr. Cole is the author of several books, including ***Hackers Beware***, ***Hiding in Plain Site***, ***Network Security Bible***, and ***Insider Threat***. He is the inventor of over 20 patents and is a researcher, writer, and speaker. He is also a member of the Commission on Cyber Security for the 44th President and several executive advisory boards. Dr. Cole is 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.

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

SECURITY 501

Advanced Security Essentials – Enterprise Defender

Six-Day Program • Thu, May 9 - Tue, May 14
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Bryce Galbraith

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**

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

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

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

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

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

"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/security-west-2013.

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**.

GIAC CERTIFIED ENTERPRISE DEFENDER GCED
www.giac.org

"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

SANS TECHNOLOGY INSTITUTE KNOWLEDGE FOR PEACE
www.sans.edu

SECURITY 503

Intrusion Detection In-Depth

Six-Day Program • Thu, May 9 - Tue, May 14
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Mike Poor

If you have an inkling of awareness of security (even my elderly aunt knows about the perils of the Interweb!), you often hear the disconcerting news about another high-profile company getting compromised. The security landscape is continually changing from what was once only perimeter protection to a current exposure of always-connected and often-vulnerable. Along with this is a great demand for security savvy employees who can help to detect and prevent intrusions. That is our goal in the Intrusion Detection In-Depth course – to acquaint you with the core knowledge, tools, and techniques to prepare you to defend your networks.

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.

> ***"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 – the first is a more basic one that assists you by giving hints for answering the questions. Students who feel that they would like more guidance can use this approach. The second approach provides no hints, permitting a student who may already know the material or who has quickly mastered new material a more challenging experience. Additionally, there is an "extra credit" stumper question for each exercise intended to challenge the most advanced student.

By week's end, your head should be overflowing with newly gained knowledge and skills; and your luggage should be swollen with course book material that didn't quite get absorbed into your brain during this intense week of learning. This course will enable you to "hit the ground running" once returning to a live environment.

> ***"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

Mike Poor *SANS Senior Instructor*

Mike is a founder and senior security analyst for the DC firm InGuardians, Inc. In the past he has worked for Sourcefire as a research engineer and for SANS leading 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.

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

Who Should Attend:

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

> ***"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.

SANS SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast. ***More info on page 28.***

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

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

SECURITY 504

Hacker Techniques, Exploits, and Incident Handling

Six-Day Program • Thu, May 9 - Tue, May 14
9:00am - 6:30pm (Day 1) • 9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits • Laptop Required
Instructor: Ed Skoudis

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**

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

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

Ed Skoudis *SANS Faculty Fellow*

Ed Skoudis is the founder of Counter Hack Challenges, an innovative organization that designs, builds, and operates popular infosec challenges and simulations including NetWars, Cyber Quests, and Cyber Foundations. Ed's expertise includes hacker attacks and defenses, the information security industry, and computer privacy issues, with over fifteen years of experience in information security. Ed authored and regularly teaches the SANS courses on network penetration testing (Security 560) and incident response (Security 504), helping over three thousand information security professionals each year improve their skills and abilities to defend their networks. He has performed numerous security assessments; conducted exhaustive anti-virus, anti-spyware, Virtual Machine, and IPS research; and responded to computer attacks for clients in financial, high technology, healthcare, and other industries. Ed conducted a demonstration of hacker techniques against financial institutions for the United States Senate and is a frequent speaker on issues associated with hacker tools and defenses. He has published numerous articles on these topics as well as the Prentice Hall best sellers ***Counter Hack Reloaded*** and ***Malware: Fighting Malicious Code***. Ed was also awarded 2004-2012 Microsoft MVP awards for Windows Server Security and is an alumnus of the Honeynet Project. Previously, Ed served as a security consultant with InGuardians, International Network Services (INS), Global Integrity, Predictive Systems, SAIC, and Bell Communications Research (Bellcore). Ed also blogs about command line tips. **http://blog.commandlinekungfu.com**

> ***"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 INSTITUTE
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

SECURITY 505

Securing Windows and Resisting Malware

Six-Day Program • Thu, May 9 - Tue, May 14
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Jason Fossen

New Course!

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 you can follow along on your laptop. 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).

> *"You will know and be confident on how to enable Windows PK1 after taking this course. I had no practical experience, but plenty of theory. Jason broke down the pros and cons of the whole process. Excellent!!"*
> -Othello Swanston, DTRA-DOD

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.

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**

> *"SEC505 teaches you how to use features in Windows that are free, and do the same as the features we're already paying a lot of attention to."*
> -Magne Smedsrud, NATO

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/security-west-2013.

GIAC CERTIFIED WINDOWS SECURITY ADMINISTRATOR GCWN

www.giac.org

SANS TECHNOLOGY INSTITUTE KNOWLEDGE FOR PEACE SCIENTIA PROFICIT

www.sans.edu

sapere aude

www.sans.org/cyber-guardian

SECURITY 560

Network Penetration Testing and Ethical Hacking

Six-Day Program • Thu, May 9 - Tue, May 14
9:00am - 5:00pm (Course Day 1) • 9:00am - 5:00pm (Course Days 2-6)
37 CPE/CMU Credits • Laptop Required
Instructor: George Bakos

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.

SANS SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast. *More info on page 28.*

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

Attendees will learn how to perform detailed reconnaissance, learning about a target's infrastructure by mining blogs, search engines, and social networking sites. We'll then turn our attention to scanning, experimenting with numerous tools in hands-on exercises. 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/security-west-2013.

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

George Bakos *SANS Certified Instructor*

George Bakos has been interested in computer security since the early 1980s when he discovered the joys of BBSs and corporate databases. These days he is a senior engineer for Northrop Grumman's Cyber Threat Analysis & Intelligence team working to understand what's going on inside the minds and hearts of his adversaries. He was the developer of Tiny Honeypot and the IDABench intrusion analysis system and was one of the researchers behind the Dartmouth Distributed Honeynet System. George developed and taught the U.S. Army National Guard's CERT technical curriculum and ran the NGB's Information Operations Training and Development Center research lab for two years, fielding and supporting Computer Emergency Response Teams nationwide. Outside the lab, George enjoys the beauties of his home state, Vermont, through skiing, ice and rock climbing, and mountain biking.

SECURITY 566

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

Five-Day Program • Thu, May 9 - Mon, May 13
9:00am - 5:00pm • 30 CPE/CMU Credits
Laptop Required • Instructor: James Tarala

Who Should Attend:

- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense personnel or contractors
- Federal agencies or clients
- Private sector organizations looking to improve information assurance processes and secure their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance

SPECIAL NOTE: This in-depth course has been updated to incorporate new attack vectors published in version 4.2 of 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.

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

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 organization in order to improve its cyber defense."

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.

> ***"The course provides a good framework for how to implement the Top 20 controls in a systematic way."***
>
> -Mike Schaub,
> Constellation Energy
> Nuclear Group

The course shows security professionals how to implement the controls in an existing network though 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 • Thu, May 9 - Tue, May 14
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • 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 enterprise resource planning 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.

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/security-west-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, which is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities.

SECURITY 579

Virtualization and Private Cloud Security

Six-Day Program • Thu, May 9 - Tue, May 14
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/security-west-2013.

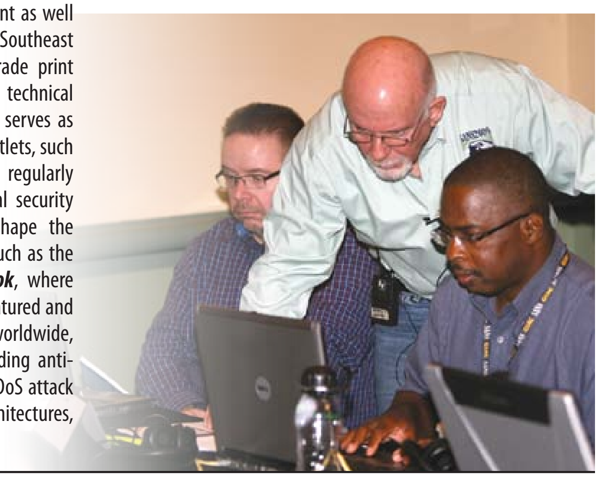
In addition, many organizations are evolving virtualized infrastructure into private clouds - internal shared services running on virtualized infrastructure. Security architecture, policies, and processes will need to adapt to work within a cloud infrastructure, and there are many changes that security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



SECURITY 617

Wireless Ethical Hacking, Penetration Testing, and Defenses

Six-Day Program • Thu, May 9 - Tue, May 14
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Larry Pesce

Despite the security concerns many of us share regarding wireless technology, it is here to stay. In fact, not only is wireless here to stay, but it is growing in deployment and utilization with wireless LAN technology and WiFi as well as with other applications, including cordless telephones, smart homes, embedded devices, and more. Technologies like ZigBee and WiMAX offer new methods of connectivity to devices, while other wireless technology, including WiFi, Bluetooth and DECT, continue their massive growth rate, each introducing its own set of security challenges and attacker opportunities.

Who Should Attend:

- Ethical hackers and penetration testers
- Network security staff
- Network and system administrators
- Incident response teams
- Information security policy decision makers
- Technical auditors
- Information security consultants
- Wireless system engineers
- Embedded wireless system developers

"The course offers an in-depth look at the how and why of wireless exploits. It gets you thinking again."
-Todd Hick, BIMA

To be a wireless security expert, you need to have a comprehensive understanding of the technology, threats, exploits, and defense techniques along with hands-on experience in evaluating and attacking wireless technology. Not limiting your skill-set to WiFi, you'll need to evaluate the threat from other standards-based and proprietary wireless technologies as well. This course takes an in-depth look at the security challenges of many different wireless technologies, exposing you to wireless security threats through the eyes of an attacker. Using readily available and custom-developed tools, you'll navigate your way through the techniques attackers use to exploit WiFi networks, including attacks against WEP, WPA/WPA2, PEAP, TTLS, and other systems, You'll also develop attack techniques leveraging Windows 7 and Mac OS X. We'll also examine the commonly overlooked threats associated with Bluetooth, ZigBee, DECT, and proprietary wireless systems. As part of the course, you'll receive the SWAT Toolkit, which will be used in hands-on labs to back up the course content and reinforce wireless ethical hacking techniques.

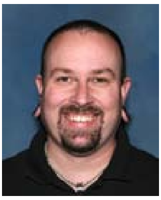
"In-depth information you need to know if you're responsible for securing wireless networks."
-Ryan Grennier, COCC

Using assessment and analysis techniques, this course will show you how to identify the threats that expose wireless technology and build on this knowledge to implement defensive techniques that can be used to protect wireless systems.

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

"This was a great in-depth look at every facet down to the protocol layer… great experience!"
-Keith Wilson, Department of Defense

www.giac.org



Larry Pesce *SANS Certified Instructor*

Larry is a Senior Security Consultant with NWN Corporation in Waltham, MA. He worked for many years in Security and Disaster Recovery in healthcare, performing penetration testing, wireless assessments, and hardware hacking. He also diverts a significant portion of his attention co-hosting the PaulDotCom Security Weekly podcast and likes to tinker with all things electronic and wireless, much to the disappointment of his family, friends, and warranties. Larry also co-authored ***Linksys WRT54G Ultimate Hacking*** and ***Using Wireshark and Ethereal*** from Syngress. Larry is an Extra Class Amateur Radio operator (KB1TNF) and enjoys developing hardware and real-world challenges for the Mid-Atlantic Collegiate Cyber Defense Challenge.

www.sans.edu

"I have taken other wireless classes in the past - none of them went as in depth as this course did, the materials/books provided will be an excellent reference."
-Chris Connolly, NYPD

www.sans.org/cyber-guardian

SECURITY 642

Advanced Web App Penetration Testing and Ethical Hacking

Six-Day Program • Thu, May 9 - Tue, May 14
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Justin Searle

This course is designed to teach you the advanced skills and techniques required to test web applications today. This advanced pen 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 (CtF) event, which tests the knowledge you will have acquired the previous five days.

> ***"Subject material is current. Instructor is a pro. Great stuff. I'll be back. "***
> -Brian Houlihan, National Credit Union Administration

Who Should Attend:

- Web penetration testers
- Security consultants
- Developers
- QA testers
- System administrators
- IT managers
- System architects

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.

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.

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

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.

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.

> ***"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

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.

> ***"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

Justin Searle *SANS Certified Instructor*

Justin is a Managing Partner of UtiliSec, specializing in Smart Grid security architecture design and penetration testing. He 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. He 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).

SECURITY 660

Advanced Penetration Testing, Exploits, and Ethical Hacking

Six-Day Program • Thu, May 9 - Tue, May 14
9:00am - 7:00pm (Days 1-5) • 9:00am - 5:00pm (Day 6)
46 CPE/CMU Credits • Laptop Required
Instructor: Stephen Sims

Who Should Attend:

- **Network and systems penetration testers**
- **Incident handlers**
- **Application developers**
- **IDS engineers**

SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking is designed as a logical progression point for those who have completed SANS SEC560: Network Penetration Testing and Ethical Hacking, or for those with existing penetration testing experience. Students with the prerequisite knowledge to take this course will walk through dozens of real-world attacks used by the most seasoned penetration testers. The methodology of a given attack is discussed, followed by exercises in a real-world lab environment to solidify advanced concepts and allow for the immediate application of techniques in the workplace. Each day includes a two-hour evening bootcamp to allow for additional mastery of the techniques discussed and even more hands-on exercises. A sample of topics covered include weaponizing Python for penetration testers, attacks against network access control (NAC) and VLAN manipulation, network device exploitation, breaking out of Linux and Windows restricted environments, IPv6, Linux privilege escalation and exploit-writing, testing cryptographic implementations, fuzzing, defeating modern OS controls such as ASLR and DEP, Return Oriented Programming (ROP), Windows exploit-writing, and much more!

> *"Most comprehensive coverage of fuzzing. I would have signed up for the course for that alone."*
>
> -Adam Kliarsky,
> Cedars-Sinai Medical Center

Attackers are becoming more clever and their attacks more complex. In order to keep up with the latest attack methods, one must have a strong desire to learn, the support of others, and the opportunity to practice and build experience. SANS SEC660 engages attendees with in-depth knowledge of the most prominent and powerful attack vectors and an environment to perform these attacks in numerous hands-on scenarios. This course goes far beyond simple scanning for low-hanging fruit, and shows penetration testers how to model the abilities of an advanced attacker to find significant flaws in a target environment and demonstrate the business risk associated with these flaws.

SEC660 starts off by introducing advanced penetration concepts, and an overview to help prepare students for what lies ahead. The focus of day one is on network attacks, an area often left untouched by testers. Topics include accessing, manipulating, and exploiting the network. Attacks are performed against NAC, VLANs, OSPF, 802.1X, CDP, IPv6, VOIP, SSL, ARP, SNMP, and others. Day two starts off with a technical module on performing penetration testing against various cryptographic implementations. The rest of the day is spent on network booting attacks, escaping Linux restricted environments such as chroot, and escaping Windows restricted desktop environments. Day three jumps into an introduction of Python for penetration testing, Scapy for packet crafting, product security testing, network and application fuzzing, and code coverage techniques. Days four and five are spent exploiting programs on the Linux and Windows operating systems. You will learn to identify privileged programs, redirect the execution of code, reverse-engineer programs to locate vulnerable code, obtain code execution for administrative shell access, and defeat modern operating system controls such as ASLR, canaries, and DEP using Return Oriented Programming (ROP) and other techniques. Local and remote exploits, as well as client-side exploitation techniques are covered. The final course day is dedicated to numerous penetration testing challenges requiring you to solve complex problems and capture flags.

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

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

Stephen Sims *SANS Senior Instructor*

Stephen Sims is an industry expert with over 15 years of experience in information technology and security. Stephen currently works out of San Francisco as a consultant. He has spent many years performing security architecture, exploit development, reverse engineering, and penetration testing. Stephen has an MS in information assurance from Norwich University and is a course author and senior instructor for the SANS Institute. He is the author of SANS' only 700-level course, SEC710: Advanced Exploit Development, which concentrates on complex heap overflows, patch diffing, and client-side exploits. Stephen is also the lead author on SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking. He holds the GIAC Security Expert (GSE) certification as well as the CISSP, CISA, Immunity NOP, and many other certifications. In his spare time Stephen enjoys snowboarding and writing music.

DEVELOPER 522

Defending Web Applications Security Essentials

Six-Day Program • Thu, May 9 - Tue, May 14
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Jason Lam

This is the course to take if you have to defend web applications!

Traditional network defenses, such as firewalls, fail to secure web applications. The quantity and importance of data entrusted to web applications is growing, and defenders need to learn how to secure it. DEV522 covers the OWASP Top 10 and will help you to better understand web application vulnerabilities, thus enabling you to properly defend your organization's web assets.

> *"Advanced option for exercises was nice – haven't seen that before. Jason was very good about Q & A! Very open to comments and questions."*
> -Renee McDonald, Department of Defense

Mitigation strategies from an infrastructure, architecture, and coding perspective will be discussed alongside real-world implementations that really work. The testing aspect of vulnerabilities will also be covered so you can ensure your application is tested for the vulnerabilities discussed in class.

To maximize the benefit for a wider range of audiences, the discussions in this course will be programming language agnostic. Focus will be maintained on security strategies rather than coding level implementation.

DEV522: Defending Web Applications Security Essentials is intended for anyone tasked with implementing, managing, or protecting Web applications. It is particularly well suited to application security analysts, developers, application architects, pen testers, and auditors who are interested in recommending proper mitigations to web security issues and infrastructure security professionals who have an interest in better defending their web applications.

Who Should Attend:

- Application developers
- Application security analysts or managers
- Application architects
- Penetration testers who are interested in learning about defensive strategies
- Security professionals who are interested in learning about web application security
- Auditors who need to understand defensive mechanisms in web applications
- Employees of PCI compliant organizations who need to be trained to comply with PCI requirements

> *"This course really proved to me that ignorance is bliss. I learned a lot that I could immediately take back to the office."*
> -Shawn Shirley, Ferrum College

The course will cover the topics outlined by OWASP's Top 10 risks document as well as additional issues the authors found of importance in their day-to-day web application development practice. The topics that will be covered include:

- **Infrastructure Security**
- **Server Configuration**
- **Authentication mechanisms**
- **Application language configuration**
- **Application coding errors like SQL Injection and Cross-Site Scripting**
- **Cross-Site Request Forgery**
- **Authentication Bypass**
- **Web services and related flaws**
- **Web 2.0 and its use of web services**
- **XPATH and XQUERY languages and injection**
- **Business logic flaws**
- **Protective HTTP Headers**

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

> *"What you don't know about web app defense is most likely killing you and you wouldn't know it."*
> -Michael Malarkey, Bank of America

GIAC CERTIFIED WEB APPLICATION DEFENDER GWEB

www.giac.org

Jason Lam *SANS Certified Instructor*

Jason is a senior security analyst at a major financial institution in Canada. His recent SANS Institute courseware development includes Defending Web Application Security Essentials and Web Application Pen Testing Hands-On Immersion. Jason started his career as a programmer before moving on to ISP network administration, where he handled network security incidents, which sparked his interest in information security. Jason specializes in Web application security, penetration testing, and intrusion detection. He currently holds a BA in computer science from York University in Toronto, Ontario, as well as the CISSP, GCIA, GCFW, GCUX, GCWN, and GCIH certifications.

www.sans.edu

FORENSICS 408

Computer Forensic Investigations – Windows In-Depth

Six-Day Program • Thu, May 9 - Tue, May 14
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Rob Lee

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

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 crime investigations and an incident response team. Over the next 7 years, he worked directly with a variety of government agencies in the law enforcement, U.S. Department of Defense, and intelligence communities as the technical lead for a vulnerability discovery and an exploit development team, lead for a cyber-forensics branch, and lead for a computer forensic and security software development team. Most recently, Rob was a Director for MANDIANT, a commercial firm focusing on responding to advanced adversaries such as the APT. Rob co-authored the book ***Know Your Enemy***, 2nd Edition. Rob is also co-author of the MANDIANT threat intelligence report ***M-Trends: The Advanced Persistent Threat***. Rob frequently contributes articles at the SANS Blog **http://computer-forensics.sans.org**.

"FOR408 is absolutely necessary for any computer forensic type career. Excellent information!"

-Rebecca Passmore, FBI

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

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 • Thu, May 9 - Tue, May 14
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Chad Tilbury

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, US Army

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

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

www.giac.org

www.sans.edu

Chad Tilbury *SANS Certified Instructor*

Chad Tilbury has spent over twelve years responding to computer intrusions and conducting forensic investigations. His extensive law enforcement and international experience stems from working with a broad cross-section of Fortune 500 corporations and government agencies around the world. During his service as a Special Agent with the Air Force Office of Special Investigations, he investigated and conducted computer forensics for a variety of crimes, including hacking, abduction, espionage, identity theft, and multi-million dollar fraud cases. He has led international forensic teams and was selected to provide computer forensic support to the United Nations Weapons Inspection Team. Chad has worked as a computer security engineer and forensic lead for a major defense contractor and as the Vice President of Worldwide Internet Enforcement for the Motion Picture Association of America. In that role, he managed Internet anti-piracy operations for the seven major Hollywood studios in over sixty countries. Chad is a graduate of the U.S. Air Force Academy and holds a B.S. and M.S. in Computer Science as well as GCFA, GCIH, GREM, and ENCE certifications. He is currently a consultant specializing in incident response, corporate espionage, and computer forensics.

FORENSICS 526

Windows Memory Forensics In-Depth

Five-Day Program • Thu, May 9 - Mon, May 13
9:00am - 5:00pm • 30 CPE/CMU Credits
Laptop Required • Instructor: Jesse Kornblum

New Course!

FOR526 - Memory Analysis In-Depth is a critical course for any serious investigator who wishes to tackle advanced forensic and incident response cases. Memory analysis is now a crucial skill for any investigator who is analyzing intrusions.

Malware can hide, but it must run – the malware paradox is key to understanding that while intruders are becoming more advanced with anti-forensic tactics and techniques, it is impossible to hide their footprints completely from a skilled incident responder performing memory analysis. Learn how memory analysis works by learning about memory structures and context, memory analysis methods, and the current tools used to parse system ram.

> *"The presentation, exercises, labs, and data provided are the best in the computer forensics industry."*
> -Rebecca Passmore FBI

> *"Totally awesome, relevant and eye opening. I want to learn more every day."*
> -Matthew Britton, Blue Cross Blue Shield of Louisiana

Who Should Attend:

- Incident response team members
- Law enforcement officers
- Forensic examiners
- Malware analysts
- Information technology professionals
- System administrators
- And anybody who plays a part in the acquisition, preservation, forensics, or analysis of Microsoft Windows computers.

Attackers will use anti-forensic techniques to hide their tracks. They use rootkits, file wiping, timestamp adjustments, privacy cleaners, and complex malware to hide in plain sight avoiding detection by standard host-based security measures. Every action that adversaries make will leave a trace; you merely need to know where to look. Memory analysis will give you the edge that you need in order to discover advanced adversaries in your network.

FOR526 - Memory Analysis In-Depth is one of the most advanced courses in the SANS Digital Forensics and Incident Response Curriculum. This cutting-edge course covers everything you need to step through memory analysis like a pro.

> *"This is the best SANS course I have taken so far and Jesse was by far the best instructor. I hope to take more classes with him in the future."*
> -Jonathan Hinson, Duke Energy

You Will Be Able To:

- **Utilize stream-based data parsing tools to extract AES-encryption keys from a physical memory image to aid in the decryption of encryption files & volumes such as TrueCrypt & BitLocker**
- **Gain insight into the current network activity of the host system by retrieving network packets from a physical memory image and examining them with a network packet analyzer**
- **Inspect a Windows crash dump to discern processes, process objects and current system state at the time of crash through use of various debugging tools such as kd,WinDBG, and livekd**
- **Conduct Live System Memory Analysis with the powerful SysInternal's tool, Process Explorer, to collect real-time data on running processes allowing for rapid triage**
- **Use the SIFT workstation and in-depth knowledge of PE File modules in physical memory, extract and analyze packed and non-packed PE binaries from memory and compare them to their known disk-bound files.**
- **Discover key features from memory such as the BIOS keyboard buffer, Kernel Debugging Data Block (KDBG), Executive Process (EPROCESS) structures, and handles based on signature and offset searching, gaining a deeper understanding of the inner workings of popular memory analysis tools**
- **Analyze memory structures using high-level and low-level techniques to reveal hidden and terminated processes and extract processes, drivers, and memory sections for further analysis**
- **Use a variety of means to capture memory images in the field, explaining the advantages and limitations of each method**

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

Jesse Kornblum *SANS Instructor*

Jesse Kornblum is a Security Engineer for Facebook. Based in the San Francisco Bay area, his research focuses on computer forensics and computer security. He has helped pioneer the field of memory analysis and authored a number of computer forensics tools. These tools include the Hashdeep suite of programs and the ssdeep system for fuzzy hashing similar files. A graduate of the Massachusetts Institute of Technology, Mr. Kornblum previously served as a computer crime investigator for the Air Force and with the Department of Justice.

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

FORENSICS 610

Reverse-Engineering Malware: Malware Analysis Tools and Techniques

Five-Day Program • Thu, May 9 - Mon, May 13
9:00am - 5:00pm • 30 CPE/CMU Credits
Laptop Required • Instructor: Hal Pomeranz

This popular malware analysis course has helped forensic investigators, malware specialists, incident responders, and IT administrators assess malware threats. The course teaches a practical approach to examining malicious programs—spyware, bots, trojans, etc.—that target or run on Microsoft Windows. This training also looks at reversing web-based malware, such as JavaScript and Flash files, as well as malicious document files. By the end of the course, you'll learn how to reverse-engineer malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and other tools for turning malware inside-out!

The malware analysis process taught in this class helps incident responders assess the severity and repercussions of a situation that involves malicious software. It also assists in determining how to contain the incident and plan recovery steps. Forensics investigators also learn how to understand key characteristics of malware present on compromised systems, including how to establish indicators of compromise (IOCs) for scoping and containing the intrusion.

Who Should Attend:

- **People with responsibilities in the areas of incident response, forensic investigation, Windows security, and system administration.**
- **Those who deal with incidents involving malware and would like to learn how to understand key aspects of malicious programs.**
- **People who have a strong understanding of core systems and networking concepts but have had a limited exposure to programming and assembly concepts.**
- **People who have experimented with aspects of malware analysis prior to the course and are looking to formalize and expand their malware forensics expertise.**

A Methodical Approach to Reverse-Engineering

The course begins by covering fundamental aspects of malware analysis. The course continues by discussing essential x86 assembly language concepts. Towards the end of the course, you'll learn to analyze malicious document files that take the form of Microsoft Office and Adobe PDF documents.

Hands-On Training for Malware Analysis and Reversing

Hands-on workshop exercises are a critical aspect of this course and allow you to apply reverse-engineering techniques by examining malware in a controlled environment. When performing the exercises, you'll study the supplied specimen's behavioral patterns and examine key portions of its code. You'll examine malware on a Windows virtual machine that you'll infect during the course and will use the supplied Linux virtual machine (REMnux) that includes tools for examining and interacting with malware.

Complexity of the Course: Formalizing and Expanding Your Malware Analysis Skills

While the field of reverse-engineering malware is in itself advanced, the course begins by covering this topic from an introductory level and quickly progresses to discuss malware analysis tools and techniques of intermediate complexity. Neither programming experience nor the knowledge of assembly is required to benefit from the course. However, you should have a general idea about core programming concepts, such as variables, loops, and functions. The course spends some time discussing essential aspects of x86 assembly to allow malware analysts to navigate through malicious executables using a debugger and a disassembler.

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

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

www.giac.org

www.sans.edu

Hal Pomeranz *SANS Faculty Fellow*

Hal Pomeranz is the founder and technical lead for Deer Run Associates, a consulting company focusing on Digital Forensics and Information Security. He is the creator of the SANS/GIAC Linux/Unix Security Track (GCUX), as well as being an instructor in the SANS Forensics curriculum. An expert in the analysis of Linux and Unix systems, Hal provides forensic analysis services through his own consulting firm and by special arrangement with MANDIANT. He has consulted on several major cases for both law enforcement and commercial clients. Hal is a regular contributor to the SANS Computer Forensics blog (**http://computer-forensics.sans.org/blog**), and co-author of the weekly Command-Line Kung Fu blog (**http://blog.commandlinekungfu.com**). Listen to Hal discuss "Memory Forensics for Incident Response" in this SANS webcast that every DFIR professional should listen to. **https://www.sans.org/webcasts/memory-forensics-incident-response-95647**

MANAGEMENT 414

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

Six-Day Program • Thu, May 9 - Tue, May 14
9:00am - 7:00pm (Day 1) • 8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6) • 46 CPE/CMU Credits
Laptop NOT Required • Instructor: Seth Misenar

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

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

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

Obtaining your CISSP® certification consists of:

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

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

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**

> *"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

SANS SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast. *More info on page 28.*

Seth Misenar *SANS Certified Instructor*

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

> *"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/security-west-2013.

GIAC INFORMATION SECURITY PROFESSIONAL GISP

www.giac.org

MANAGEMENT 512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program • Thu, May 9 - Mon, May 13
9:00am - 6:00pm (Course Days 1-4) • 9:00am - 4:00pm (Course Day 5)
33 CPE/CMU Credits • Laptop Required • Instructor: Stephen Northcutt

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

Who Should Attend:

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

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

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

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

Stephen Northcutt *SANS Faculty Fellow*

Stephen Northcutt founded the GIAC certification and 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**

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

GIAC SECURITY LEADERSHIP CERTIFICATION GSLC

www.giac.org

SANS TECHNOLOGY INSTITUTE KNOWLEDGE FOR PEACE

www.sans.edu

AUDIT 507

Auditing Networks, Perimeters, and Systems

Six-Day Program • Thu, May 9 - Tue, May 14
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: David Hoelzer

One of the most significant obstacles facing many auditors today is how exactly to go about auditing the security of an enterprise. What systems really matter? How should the firewall and routers be configured? What settings should be checked on the various systems under scrutiny? Is there a set of processes that can be put into place to allow an auditor to focus on the business processes rather than the security settings? All of these questions and more will be answered by the material covered in this course.

This course is organized specifically to provide a risk-driven method for tackling the enormous task of designing an enterprise security validation program. After covering a variety of high-level audit issues and general audit best practices, the students will have the opportunity to dive deep into the technical how-to for determining the key controls that can be used to provide a level of assurance to an organization. Tips on how to repeatedly verify these controls and techniques for automatic compliance validation will be given from real-world examples.

One of the struggles that IT auditors face today is assisting management to understand the relationship between the technical controls and the risks to the business that these affect. In this course these threats and vulnerabilities are explained based on validated information from real-world situations. The instructor will take the time to explain how this can be used to raise the awareness of management and others within the organization to build an understanding of why these controls specifically and auditing in general are important. From these threats and vulnerabilities, we will explain how to build the ongoing compliance monitoring systems and how to automatically validate defenses through instrumentation and automation of audit checklists.

Who Should Attend:

- Auditors seeking to identify key controls in IT systems
- Audit professionals looking for technical details on auditing
- Managers responsible for overseeing the work of an audit or security team
- Security professionals newly tasked with audit responsibilities
- System and network administrators looking to better understand what an auditor is trying to achieve, how auditors think, and how to better prepare for an audit
- System and network administrators seeking to create strong change control management and detection systems for the enterprise

You'll be able to use what you learn immediately. Five of the six days in the course will either produce or provide you directly with a general checklist that can be customized for your audit practice. Each of these days includes hands-on exercises with a variety of tools discussed during the lecture sections so that you will leave knowing how to verify each and every control described in the class. Each of the five hands-on days gives you the chance to perform a thorough technical audit of the technology being considered by applying the checklists provided in class to sample audit problems in a virtualized environment. Each student is invited to bring a Windows XP Professional or higher laptop for use during class. Macintosh computers running OS X may also be used with VMWare Fusion.

A great audit is more than marks on a checklist; it is the understanding of what the underlying controls are, what the best practices are, and why. Sign up for this course and experience the mix of theoretical, hands-on, and practical knowledge.

David Hoelzer *SANS Faculty Fellow*

David Hoelzer is a high-scoring SANS Fellow instructor and author of more than twenty sections of SANS courseware. He is an expert in a variety of information security fields, having served in most major roles in the IT and security industries over the past twenty-five years. Recently, David was called upon to serve as an expert witness for the Federal Trade Commission for ground-breaking GLBA Privacy Rule litigation. David has been highly involved in governance at the SANS Technology Institute, serving as a member of the Curriculum Committee as well as Audit Curriculum Lead. As a SANS instructor, David has trained security professionals from organizations including NSA, DHHS, Fortune 500 security engineers and managers, various Department of Defense sites, national laboratories, and many colleges and universities. David is a research fellow in the Center for Cybermedia Research and also a research fellow for the Identity Theft and Financial Fraud Research Operations Center (ITFF/ROC). He also is an adjunct research associate of the UNLV Cybermedia Research Lab and a research fellow with the Internet Forensics Lab. David has written and contributed to more than 15 peer reviewed books, publications, and journal articles. Currently, David serves as the principal examiner and director of research for Enclave Forensics, a New York/Las Vegas based incident response and forensics company. He also serves as the chief information security officer for Cyber-Defense, an open source security software solution provider. In the past, David served as the director of the GIAC Certification program, bringing the GIAC Security Expert certification to life. David holds a BS in IT, Summa Cum Laude, having spent time either attending or consulting for Stony Brook University, Binghamton University, and American Intercontinental University.

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

GIAC SYSTEMS AND NETWORK AUDITOR GSNA

www.giac.org

SANS TECHNOLOGY INSTITUTE KNOWLEDGE FOR PEACE

www.sans.edu

Security 524
Cloud Security Fundamentals

Two-Day Course • Tue, May 7 - Wed, May 8 • 9:00am - 5:00pm • 12 CPE/CMU Credits
Laptop Required • Instructor: Paul A. Henry

Many organizations today are feeling pressure to reduce IT costs and optimize IT operations. Cloud computing is rapidly emerging as a viable means to create dynamic, rapidly provisioned resources for operating platforms, applications, development environments, storage and backup capabilities, and many more IT functions. A staggering number of security considerations exist that information security professionals need to consider when evaluating the risks of cloud computing.

The first fundamental issue is the loss of hands-on control of system, application, and data security. Many of the existing best practice security controls that infosec professionals have come to rely on are not available in cloud environments, stripped down in many ways, or not able to be controlled by security teams. Security professionals must become heavily involved in the development of contract language and Service Level Agreements (SLAs) when doing business with Cloud Service Providers (CSPs). Compliance and auditing concerns are compounded. Control verification and audit reporting within CSP environments may be less in-depth and frequent as audit and security teams require.

The SANS Cloud Security Fundamentals course starts out with a detailed introduction to the various delivery models of cloud computing ranging from Software as a Service (SaaS) to Infrastructure as a Service (IaaS) and everything in between. Attendees will start off the second day with coverage of audits and assessments for cloud environments. The day will include hands-on exercises for students to learn about new models and approaches for performing assessments, as well as evaluating audit and monitoring controls. Next the class will turn to protecting the data itself! New approaches for data encryption, network encryption, key management, and data lifecycle concerns will be covered in-depth.

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

SANS SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast. *More info on page 28.*

Security 546
IPv6 Essentials

Two-Day Course • Wed, May 15 - Thu, May 16 • 9:00am - 5:00pm • 12 CPE/CMU Credits
Laptop Required • Instructor: SANS Staff

We are out of IPv4 addresses. ISPs worldwide will have to rapidly adopt IPv6 over the coming years to grow, in particular as mobile devices require more and more address space. Already, modern operating systems implement IPv6 by default. Windows 7, for example, ships with Teredo enabled by default. This course is designed not just for implementers of IPv6, but also for those who just need to learn how to detect IPv6 and defend against threats unintentional IPv6 use may bring.

IPv6 is currently being implemented at a rapid pace in Asia in response to the exhaustion of IPv4 address space, which is most urgently felt in rapidly growing networks in China and India. Even if you do not feel the same urgency of IP address exhaustion, you may have to connect to these IPv6 resources as they become more and more important to global commerce.

Implementing IPv6 should not happen without carefully considering the security impact of the new protocol. Even if you haven't implemented it yet, the ubiquitous IPv6 support in modern operating systems easily leads to unintentional IPv6 implementation, which may put your network at risk. In this course, we will start out by introducing the IPv6 protocol, explaining in detail many of its features like the IPv6 header, extension headers and auto configuration. Only by understanding the design of the protocols in depth will it be possible to appreciate the various attacks and mitigation techniques. The course will address how to take advantage of IPv6 to re-think how to assign addresses in your network and how to cope with what some suggest is the biggest security problem in IPv6: no more NAT! IPv6 doesn't stop at the network layer. Many application layer protocols change in order to support IPv6, and we will take a close look at protocols like DNS, DHCPv6 and more.

The course covers various security technologies like firewalls and Intrusion Detection and Prevention Systems (IDS/IPS). It also addresses the challenges in adequately configuring these systems and makes suggestions as to how apply to existing best practices to IPv6. Upcoming IPv6 attacks are discussed using tools like the THC IPv6 attack suite and others as an example.

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

> *"The course has crammed all the IPv6 information possible to fit into two days."*
>
> -Craig Lindsey, Blue Cross Blue Shield of Alabama

> *"The IPv4 to IPv6 transition planning is something everyone needs to see."*
>
> -Eric Gallagher, NCCAM

Security 434
Log Management In-Depth: Compliance, Security, Forensics, and Troubleshooting

Two-Day Course • Wed, May 15 - Thu, May 16 • 9:00am - 5:00pm • 12 CPE/CMU Credits
Laptop Required • Instructor: Dr. Eric Cole

This first-ever dedicated log management class teaches system, network, and security logs, and their analysis and management. It covers the complete lifecycle of dealing with logs: the whys, hows and whats. You will learn how to enable logging and then how to deal with the resulting data deluge by managing data retention, analyzing data using search, filtering and correlation as well as how to apply what you learned to key business and security problems. The class also teaches applications of logging to forensics, incident response and regulatory compliance.

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

The class author, Dr. Anton Chuvakin, probably has more experience in the application of logs to IT and IT security than anyone else in the industry. This means he and the other instructors chosen to teach this course have made a lot of mistakes through trial and error along the way. You can save yourself a lot of pain and your organization a lot of money by learning about the common mistakes people make working with logs.

Security 580
Metasploit Kung Fu for Enterprise Pen Testing

Two-Day Course • Wed, May 15 - Thu, May 16 • 9:00am - 5:00pm • 12 CPE/CMU Credits
Laptop Required • Instructor: SANS Staff

Many enterprises today face regulatory or compliance requirements that mandate regular penetration testing and vulnerability assessments. Commercial tools and services for performing such tests can be expensive. While really solid free tools such as Metasploit are available, many testers do not understand the comprehensive feature sets of such tools and how to apply them in a professional-grade testing methodology. Metasploit was designed to help testers with confirming vulnerabilities using an Open Source and easy-to-use framework. This course will help students get the most out of this free tool.

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

This class will show students how to apply the incredible capabilities of the Metasploit Framework in a comprehensive penetration testing and vulnerability assessment regimen, according to a thorough methodology for performing effective tests. Students who complete the course will have a firm understanding of how Metasploit can fit into their penetration testing and day-to-day assessment activities. The course will provide an in-depth understanding of the Metasploit Framework far beyond simply showing attendees how to exploit a remote system. The class will cover exploitation, post-exploitation reconnaissance, token manipulation, spear-phishing attacks, and the rich feature set of the Meterpreter, a customized shell environment specially created for exploiting and analyzing security flaws.

The course will also cover many of the pitfalls that a tester may encounter when using the Metasploit Framework and how to avoid or work around them, making tests more efficient and safe.

Security 710
Advanced Exploit Development

Two-Day Course • Wed, May 15 - Thu, May 16 • 9:00am - 5:00pm • 14 CPE/CMU Credits
Laptop Required • Instructor: Stephen Sims

SANS SEC710 is an advanced two-day course on exploit development. Students attending this course should know their way around a debugger and have prior experience exploiting basic stack overflows on both Windows and Linux. Terms such as "jmp esp" and "pop/pop/ret" should be nothing new to you. We will move beyond these attack techniques to explore more advanced topics on heap exploitation, format string attacks, and Microsoft patch reversal and exploitation. We will be taking a real Microsoft security patch, reversing it to model the discovery of an undisclosed vulnerability, and developing a client-side exploit that defeats controls such as Address Space Layout Randomization (ASLR).

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

Attendees can apply the skills developed in this class to create and customize exploits for penetration tests of home-grown software applications and newly discovered flaws in widespread commercial software. Understanding the process of exploit development can help enterprises analyze their actual business risks better than the ambiguous hypotheticals we often contend with in most traditional vulnerability assessments.

Management 305
Technical Communication and Presentation Skills for Security Professionals

One-Day Course • Wed, May 8 • 9:00am - 5:00pm • 6 CPE/CMU Credits
Laptop Required • Instructor: David Hoelzer

This course is designed for every IT professional in your organization. In this course we cover the top techniques that will show any attendee how to research and write professional quality reports, how to create outstanding presentation materials, and as an added bonus, how to write expert witness reports. Attendees will also get a crash course on advanced public speaking skills.

Writing reports is a task that many IT professionals struggle with, sometimes from the perspective of writing the report and other times from the perspective of having to read someone else's report! In the morning material, we cover step by step how to work through the process of identifying critical ideas, how to properly research them, how to develop a strong argument in written form, and how to put it all down on paper. We also discuss some of the most common mistakes that can negatively impact the reception of your work and show how to avoid them. Attendees can expect to see the overall quality of their reports improve significantly as a result of this material.

After writing a meaningful report, it is not uncommon to find that we must present the key findings from that report before an audience, whether that audience is our department, upper management, or perhaps even the entire organization. How do you transform an excellent report into a powerful presentation? We will work through a process that works to either condense a report into a presentation or can even be used to write a presentation from scratch that communicates your important thoughts in a meaningful and interesting way.

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

www.sans.edu

Management 415

New Course!

A Practical Introduction to Risk Assessment

One-Day Course • Wed, May 8 • 9:00am - 5:00pm • 6 CPE/CMU Credits
Laptop Required • Instructor: James Tarala

In this course, students will learn the practical skills necessary to perform regular risk assessments for their organizations. The ability to perform a risk assessment is crucial for organizations hoping to defend their systems. There are simply too many threats, too many potential vulnerabilities that could exist, and not enough resources to create an impregnable security infrastructure. Therefore every organization, whether they do so in an organized manner or not, will make priority decisions on how best to defend their valuable data assets. Risk assessment should be the foundational tool used to facilitate thoughtful and purposeful defense strategies.

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

Management 433
Securing The Human: Building and Deploying an Effective Security Awareness Program

Two-Day Course • Wed, May 15 - Thu, May 16 • 9:00am - 5:00pm • 12 CPE/CMU Credits
Laptop Required • Instructor: Lance Spitzner

Organizations have invested in information security for years now. Unfortunately, almost all of this effort has been focused on technology with little, if any, effort on the human factor. As a result, the human is now the weakest link. From RSA and Epsilon to Oak Ridge National Labs and Google, the simplest way for cyber attackers to bypass security is to target your employees. One of the most effective ways to secure the human is an active awareness and education program that goes beyond compliance and that results in changes to behaviors. In this challenging course, you will learn the key concepts and skills to plan, implement, and maintain an effective security awareness program that makes your organization both more secure and compliant. In addition, you will develop metrics to measure the impact of your program and demonstrate value. Finally, through a series of labs and exercises, you will develop your own project and execution plan, so you can immediately implement your customized awareness program upon returning to your organization.

"Great class, diverse group brings good perspective. Instructor interesting, energetic, engaging." -Nancy Kreidler, U.S. Army

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

www.sans.edu

Management 535

Incident Response Team Management

One-Day Course • Wed, May 15 • 9:00am - 5:00pm • 6 CPE/CMU Credits
Laptop Recommended • Instructor: SANS Staff

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

This course will take you to the next level of managing an incident response team. Given the frequency and complexity of today's attacks, incident response has become a critical function for organizations. Detecting and efficiently responding to incidents, especially those where critical resources are exposed to elevated risks, has become paramount, and to be effective, incident response efforts must have strong management processes to facilitate and guide them. Managing an incident response team requires special skills and knowledge. A background in information security management or security engineering is not sufficient for managing incidents. Furthermore, incident responders with strong technical skills do not necessarily become effective incident response managers. Special training is necessary.

"Very useful information for existing or new IR teams."
-Dave Stock, The Mosaic Company

This course was developed by Eugene Schultz, Ph.D, an information security professional with over 26 years of experience, much of it in incident response. He was the founder of the first U.S. government incident response team. Students will learn by applying course content through hands-on skill-building exercises. These exercises range from writing and evaluating incident response procedures, to the table-top validation of procedures, incident response management role playing in hypothetical scenarios, and hands-on experience in tracking incident status in hypothetical scenarios.

AUDIT SKILL-BASED COURSES

Audit 521

Meeting the Minimum: PCI/DSS 2.0: Becoming and Staying Compliant

Two-Day Course • Wed, May 15 - Thu, May 16 • 9:00am - 5:00pm • 12 CPE/CMU Credits
Laptop Required • Instructor: David Hoelzer

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

The payment card industry has been working over the past several years to formalize a standard for security practices that are required for organizations that process or handle payment card transactions. The fruit of this labor is the Payment Card Industry Data Security Standard (currently at version 2.0).

"AUD521 was amazing. Very informative and the instructor made the material interesting. Looking forward to my next SANS course!"
-Nancy Johnsen, Fortis Properties

This standard, which started life as the Visa Digital Dozen, is a set of focused comprehensive controls for managing the risks surrounding payment card transactions, particularly over the Internet. Of course, compliance validation is one of the requirements. This course was created to allow organizations to exercise due care by performing internal validations through a repeatable, objective process. While the course will cover all of the requirements of the standard, the primary focus is on the technical controls and how they can be measured. Every student will leave the class with a toolkit that can be used to validate any PCI/DSS environment technically and the knowledge of how to use it.

"Real-world experience coupled with in-depth knowledge of standards, presented by a first class instructor."
-Grant Dwyer, Fortis Properties

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.

SPECIAL:
ISC² Member Reception sponsored by SANS
Check website for date and time.

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. 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.

Information Assurance Metrics: Practical Steps to Measurement *James Tarala*

Show up to a security presentation, walk away with a specific action plan. In this presentation, James Tarala, a senior instructor with the SANS Institute, will be presenting on making specific plans for information assurance metrics in an organization. Clearly this is an industry buzzword at the moment (when you listen to presentations on the 20 Critical Controls, NIST guidance, or industry banter). Security professionals have to know that their executives are discussing the idea. So how do you integrate information assurance metrics in an organization and achieve value from the effort? Learn what efforts are currently underway in the industry to create consensus metrics guides and what initial steps an organization can take to start measuring the effectiveness of their security program. Small steps are better than no steps, and by the end of this presentation, students will have a start integrating metrics into their information assurance program.

Securing The Kids *Lance Spitzner*

Technology is an amazing tool. It allows our kids to access a tremendous amount of information, meet new people, and communicate with friends around the world. In addition, for them to be successful in the 21st century they have to know and understand how to leverage these new tools. However, with all these capabilities come a variety of new risks, risks that as parents you may not understand or even be aware of. In this one hour presentation we cover the top three risks to kids online and the top five steps you can take to protect them. This course is based on the experiences and lessons learned from a variety of SANS top instructors who not only specialize in security, but are parents just like you. This talk is sponsored and delivered by the SANS Securing The Human program.

Key points include: Why securing kids online is harder then securing kids in the physical world; Top three risks they face – strangers, friends, and themselves; Use of education to inform and secure them; Use of a dedicated computer just for kids; Kids Acceptable Use Policy; Filtering and monitoring tools; Additional lessons learned and resources to learn more.

Securing The Human *Lance Spitzner*

Organizations have traditionally invested most of their security in technology, with little effort in protecting their employees. As a result, many attackers today target the weakest link, the human. Awareness, not just technology, has become key to reducing risk and remaining compliant. This high-level talk designed for management explains why humans are so vulnerable, how they are being actively exploited, and what organizations can do about it.

Key points include: How humans are nothing more than another type of operating system, albeit a highly vulnerable one; Why humans are so bad at judging risk and how attackers exploit these vulnerabilities; How an effective awareness program patches these vulnerabilities and reduces risk; How to develop a modular and flexible program that reaches multi-cultures; How to create and effectively use metrics.

2013 Bonus Sessions

Certifiably Certifiable *Seth Misenar*

An alphabet soup of required certifications seems to follow every job posting; and yet for all these letters, are our organizations becoming more secure? Are our security certifications failing us? Are we failing our security certifications? This talk will be a discussion on the past and current state of security certifications. Additionally, the future of security certifications and what modifications are needed will be discussed. Talk by Seth Misenar, GSE, CASP, CISSP, GSEC, GCIA, GCIH, GPEN, GWAPT, GCFA, GCWN, GCFW, MCSE, MCDBA, Cyber Guardian Red/Blue Team, etc.

Windows Exploratory Surgery with Process Hacker *Jason Fossen*

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

Gone In 60 Minutes *David Hoelzer*

60 minutes from discovery through exploitation - how fast is your patching process?

In this fast paced talk, David Hoelzer will walk you through the process a hacker might go through to discover a flaw, engineer a working proof of concept, and then convert that into a working Metasploit exploit module... All in 60 minutes. If you're not a technical person, don't worry. There's still plenty to take away from this talk. If you are a technical person come along and see if there's a trick or two that you can use!

The Ancient Art of Falconry *Justin Searle*

Come and experience a taste of the ancient art of falconry. Explore the world of raptors, take in their lethal beauty, and hear of the partnership that can be formed between man and beast. Learn the process of identification, trapping, training, trusting, and hunting with one of nature's most efficient predators. Understand what is needed to become a licensed falconer in your state and how you can begin your own unforgettable journey in this time-honored tradition. After all, every security professional needs his technology-free hobbies.

Evolving Threats *Paul A. Henry*

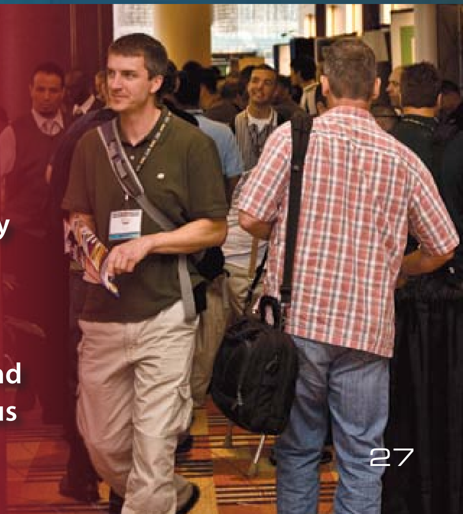
For nearly two decades defenders have fallen into the "Crowd Mentality Trap" and have simply settled on doing the same thing everyone else was doing. While at the same time attackers have clearly evolved both in terms of malware delivery vectors and attack methodology. Today our defenses focus primarily on the gateway and upon attempting to outwit the delivery methods of the attackers. 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.

For dates, times, and complete information, please visit
www.sans.org/event/security-west-2013/bonus-sessions

Vendor Expo

Friday, May 10, 2013
12:00pm - 1:30pm and 5:00pm - 7:00pm

Given that (virtually) everything in security is accomplished with a tool, exposure to those tools is a very important part of the SANS Training Event learning experience. Leading solutions providers will be on-hand for a one-day vendor expo, an added bonus to registered training event attendees.



NETWARS

A True Hands-On Interactive Security Challenge!

NetWars is a computer and network security challenge designed to test participants' experience and skills in a safe, controlled environment while having a little fun with your fellow IT security professionals. NetWars is designed to help participants develop skills in several critical arenas:

- Vulnerability Assessments
- System Hardening
- Malware Analysis
- Digital Forensics
- Incident Response
- Packet Analysis
- Penetration Testing
- Intrusion Detection

The NetWars competition will be played over two evenings:
Sunday, May 12 - Monday, May 13.

Prizes will be awarded at the conclusion of the games.

REGISTRATION IS LIMITED AND IS FREE to students attending any long course at SANS Security West 2013 *(NON-STUDENT ENTRANCE FEE IS $999)*.

In-Depth, Hands-On, InfoSec Skills – *Embrace the Challenge*
www.sans.org/netwars

SANS Simulcast

You don't have to miss out on SANS' top-rated training. Attend select SANS Security West 2013 courses remotely via SANS Simulcast!

How SANS Simulcast Works

Cutting-edge webcast technology and live instruction combine to deliver a fun and engaging remote learning experience. Remote students will also receive four months of access to an archived copy of the class to use as a reference tool or to catch up on a missed session. The platform is web-based so students simply need a solid Internet connection to participate.

SANS Event Simulcast classes are:

COST-EFFECTIVE - You can save thousands of dollars on travel costs, making Event Simulcast an ideal solution for students working with limited training budgets or travel bans.

ENGAGING - Event Simulcast classes are live and interactive, allowing you to ask questions and share experiences with your instructor and classmates.

CONDENSED - Complete your course quickly; all SANS Event Simulcast classes take no longer than six days to complete.

REPEATABLE - Event Simulcast classes are recorded and placed in an online archive in case you have to miss part of the class or just wish to view the material again at a later date.

COMPLETE - You will receive the same books, discs, and MP3 audio files that conference students receive, and you will see and hear the same information as it is presented at the live event.

The following Security West 2013 courses will be available via SANS Simulcast:

Short Course:
SEC524

Long Courses:
MGT414 SEC401
SEC503 SEC560

To register for a Security West 2013 Simulcast course, please visit **www.sans.org/simulcasts**

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

Real Threats

Real Skills

Real Success

Join Today!

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

**www.sans.org/
cyber-guardian**

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.

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)

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

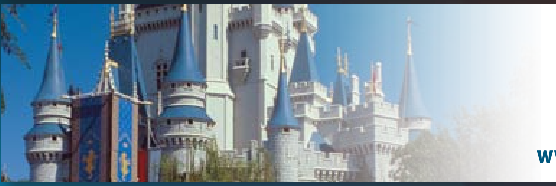
SANS TECHNOLOGY INSTITUTE
SCIENTIA PRO PACE
KNOWLEDGE FOR PEACE

16 of the courses being offered at Security West 2013 may be applied towards an STI Master's Degree.

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 **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

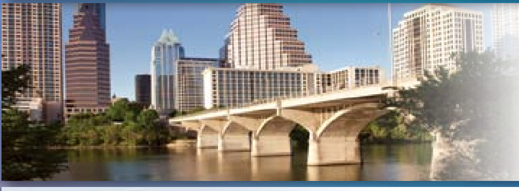
SANS **AppSec** 2013

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

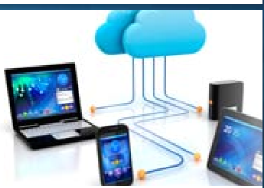


SANS **Austin** 2013

Austin, TX
May 19-24, 2013
www.sans.org/event/austin-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 15-23, 2013
www.sans.org/event/sansfire-2013

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

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

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 Security West 2013

Hotel Information

Conference Location
Manchester Grand Hyatt

One Market Place | San Diego, CA 92101
Phone: 619-233-6464
http://manchestergrand.hyatt.com

Special Hotel Rates Available

A special discounted rate of $207.00 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 April 16, 2013. To make reservations please call (800) 233-1234 or (619) 232-1234 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 Manchester Grand Hyatt

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 Manchester Grand Hyatt, 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 Manchester Grand Hyatt that you won't want to miss!

5 Everything is in one convenient location!

SANS Security West 2013

Registration Information

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

SANS
The Most Trusted Source for Information and Software Security Training

To register, go to www.sans.org/event/security-west-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 17, 2013. There is a $300 cancellation fee per registration.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	**3/27/13**	**$500.00**	**4/10/13**	**$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