SANS Pen Test Austin 2015

Austin, TX | May 18-23

CYBERSECURITY TRAINING EVENT

This SPECIAL event features:

NETWARS

Three nights of fun NetWars challenges

(more than traditional SANS events!)

CYBERCITY

One night of SANS CyberCity missions

(where you'll engage in a hands-on kinetic cyber range – saving the city from a disaster!)

Coin-a-Palooza

Get a chance to earn up to four SANS Pen Test Challenge Coins for various classes you've taken in the past

All of these exciting evening sessions are available AT NO EXTRA CHARGE for people who sign up for a six-day course at the SANS Pen Test Austin event.

> *"Anyone tasked with the security of their company needs this sort of training and knowledge."*
> -Brendan Flanning, Fandango

6 COURSES OFFERED

SEC401: Security Essentials Bootcamp Style

SEC504: Hacker Tools, Techniques, Exploits & Incident Handling

SEC560: Network Penetration Testing & Ethical Hacking

SEC542: Web App Penetration Testing & Ethical Hacking

SEC660: Advanced Penetration Testing, Exploit Writing & Ethical Hacking

SEC617: Wireless Ethical Hacking, Pen Testing & Defenses

sans.org/event/pentest2015

SAVE $400

by paying early! See page 13 for details.

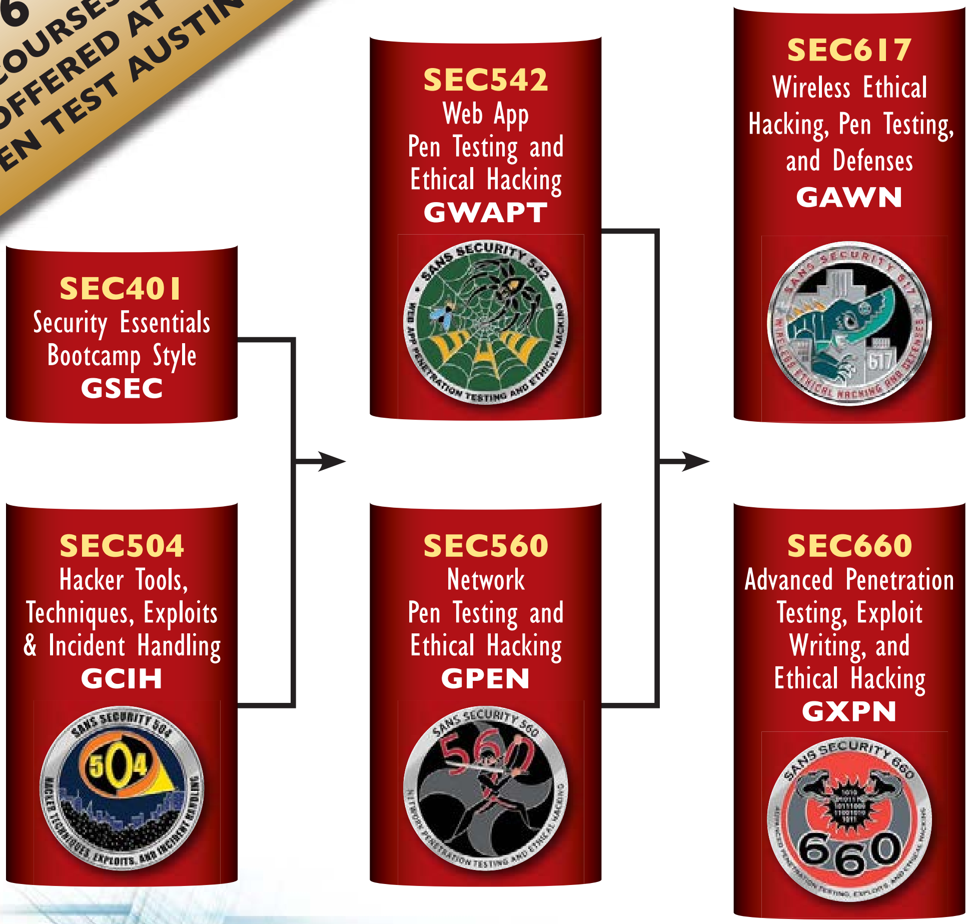
GLOBAL INFORMATION ASSURANCE CERTIFICATION GIAC www.giac.org

GIAC Approved Training

SANS Pen Test Austin 2015

Austin, TX | May 18-23

6 COURSES OFFERED AT PEN TEST AUSTIN



SEC401
Security Essentials Bootcamp Style
GSEC

SEC504
Hacker Tools, Techniques, Exploits & Incident Handling
GCIH

SEC542
Web App Pen Testing and Ethical Hacking
GWAPT

SEC560
Network Pen Testing and Ethical Hacking
GPEN

SEC617
Wireless Ethical Hacking, Pen Testing, and Defenses
GAWN

SEC660
Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
GXPN

SANS SECURITY 504
504
HACKER TECHNIQUES, EXPLOITS, AND INCIDENT HANDLING
SANS SECURITY 542
WEB APP PENETRATION TESTING AND ETHICAL HACKING
SANS SECURITY 560
560
NETWORK PENETRATION TESTING AND ETHICAL HACKING
SANS SECURITY 617
617
WIRELESS ETHICAL HACKING AND DEFENSES
SANS SECURITY 660
660
ADVANCED PENETRATION TESTING, EXPLOITS, AND ETHICAL HACKING

SANS Penetration Testing RESOURCES

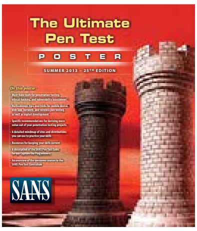
Website
pen-testing.sans.org

Pen Test Blog
pen-testing.sans.org/blog

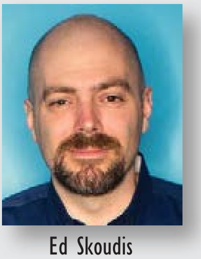
GPWN Mailing List
lists.sans.org/mailman/listinfo/gpwn-list

Webcasts
pen-testing.sans.org/resources/webcasts

Twitter
@pentesttips



Poster & Cheat Sheets
pen-testing.sans.org/resources/downloads


Ed Skoudis

We have a really special event brewing for you at SANS Pen Test Austin 2015, and you've gotta check it out.

Every organization needs skilled people who know how to find vulnerabilities, understand risk, and help prioritize resources based on mitigating potential real-world attacks. That's what SANS Pen Test Austin is all about! If you like to break things, put them back together, find out how they work, and mimic the actions of real-world bad guys, all the while providing real business value to your organization, then this event is exactly what you need.

Every security professional needs to understand how to get the most out of penetration tests and vulnerability assessments. The SANS Pen Test Austin 2015 event is focused on helping you build world-class security assessment and penetration testing skills to do just that. This event is an IDEAL way to take your penetration testing and vulnerability assessment skills to an entirely new level. We're bringing our most popular Pen Test courses, instructors, and bonus sessions together in one place to offer one of SANS most comprehensive Pen Test training experiences ever.

At the SANS Pen Test Austin 2015 event you will not only learn vital and in-demand skills and abilities, but you will network with like-minded security professionals that also see the benefit in taking their Pen Test artistry to the next level.

What's special about SANS Pen Test Austin?

- **SANS' Top Courses Focused on Pen Testing:** Learn hands-on skills that you can directly apply the day you get back to your job.
- **NetWars, NetWars, NetWars:** Enjoy three exciting nights of NetWars challenges, where you can have some fun while building serious infosec skills.
- **Coin-a-Palooza:** Earn up to four additional SANS pen test challenge coins (each with an integrated cipher challenge) based on your performance in SANS NetWars!
- **CyberCity Missions:** Work through an evening of cyber missions that have a direct kinetic impact on the miniature CyberCity environment that SANS built with a real power grid, water reservoir, military base, and more!

I urge you to check out all the great stuff we are offering at SANS Pen Test Austin. It's a truly special SANS event, and I hope to see you there!

Ed Skoudis
SANS Pen Test Curriculum Lead

SEC401

Security Essentials Bootcamp Style

Six-Day Program | May 18-23 | 46 CPEs | Laptop Required
Instructor: Bryce Galbraith

Major Update!
Newly Released in 2015

Learn the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. Learn tips and tricks from the experts so that you can win the battle against the wide range of cyber adversaries that want to harm your environment.

Learn to build a security roadmap that can scale today and into the future.

SEC401: Security Essentials Bootcamp Style is focused on teaching you the essential information security skills and techniques you need to protect and secure your organization's critical information assets and business systems. This course will show you how to prevent your organization's security problems from being headline news in the *Wall Street Journal*!

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

With the advanced persistent threat, it is almost inevitable that organizations will be targeted. Whether the attacker is successful in penetrating an organization's network depends on the effectiveness of the organization's defense. 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 really works in cybersecurity. What has worked, and will always work, is taking a risk-based approach to cyber defense. Before your organization spends a dollar of its IT budget or allocates any resources or time to anything in the name of cybersecurity, three questions must be answered:

- **What is the risk?**
- **Is it the highest priority risk?**
- **What is the most cost-effective way to reduce the risk?**

Security is all about making sure you focus on the right areas of defense. In SEC401 you will learn the language and underlying theory of computer and information security. You will gain the essential and effective security knowledge you'll need 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 learn up-to-the-minute skills you can put into practice immediately upon returning to work; and (2) You will be taught by the best security instructors in the industry.

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

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

ATTEND REMOTELY
If you are unable to attend this event, this course is also available via SANS Simulcast.
sans.org/event/pentest2015/attend-remotely

WHO SHOULD ATTEND:

- Security professionals
- Managers
- Operations personnel
- IT engineers and supervisors
- Administrators
- Forensic specialists, penetration testers, and auditors

SANS
SEC401

giac.org

sans.org/cyber-guardian

sans.edu

sans.org/ondemand

MEETS DoDD 8570 REQUIREMENTS

sans.org/8570

SEC504
Hacker Tools, Techniques, Exploits, and Incident Handling

Six-Day Program | May 18-23 | 37 CPEs | Laptop Required
Instructor: Michael Murr

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection or one or two disgruntled employees (and whose does not!), 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. As defenders, it is essential we understand these hacking tools and techniques.

"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

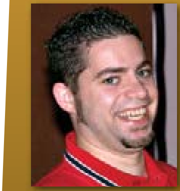
By helping you understand attackers' tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan, this course helps you turn the tables on computer attackers. It addresses the latest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

"This class teaches you all of the hacking techniques that you need as an incident handler."
-Demonique Lewis, TerpSys

The course is particularly well-suited to individuals who lead or are a part of an incident handling team. 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.

"SEC504 opens your eyes to the real cyberworld. It encourages thinking about security of data and network access."
-Frank Munson, Virginia International Terminal

ATTEND REMOTELY
If you are unable to attend this event, this course is also available via SANS Simulcast.
sans.org/event/pentest2015/attend-remotely



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

SANS
SEC504

GCIH
giac.org

sapere aude
sans.org/cyber-guardian

sans.edu

sans.org/ondemand

MEETS DoDD 8570 REQUIREMENTS
sans.org/8570

SEC542
Web App Penetration Testing and Ethical Hacking

Six-Day Program | May 18-23 | 36 CPEs | Laptop Required
Instructor: Seth Misenar

Web applications play a vital role in every modern organization. This becomes apparent when adversaries compromise these applications, damage business functionality and steal data. Unfortunately, many organizations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems. SEC542 helps students move beyond push-button penetration testing to professional web application penetration testing that finds flaws before the adversaries discover and abuse them.

Customers expect web applications to provide significant functionality and data access. Even beyond the importance of customer-facing web applications, internal web applications increasingly represent the most commonly used tools within any organization. Unfortunately, there is no "patch Tuesday" for custom web applications, so, not surprisingly, every major industry study finds that web application flaws play a major role in significant breaches and intrusions. Adversaries increasingly focus on these high-value targets either by directly abusing public-facing applications or by focusing on web apps as targets after an initial break-in.

> *"SEC542 provides rapid exposure to a variety of tools and techniques invaluable to recon on target site."* -Gareth Grindle, QA Ltd.

Modern cyber defense requires a realistic and thorough understanding of web application security issues. Anyone can learn to sling a few web hacks, but web application penetration testing requires something deeper. SEC542 will enable students to capably assess a web application's security posture and convincingly demonstrate the impact of inadequate security that plagues most organizations. Students will come to understand major web application flaws and their exploitation and, most importantly, learn a field-tested and repeatable process to consistently find these flaws and convey what they have learned to their organizations.

Even technically gifted security geeks often struggle with helping organizations understand risk in terms relatable to business. Much of the art of penetration testing has less to do with learning how adversaries are breaking in than it does with convincing an organization to take the risk seriously and employ appropriate countermeasures. The goal of SEC542 is to better secure organizations through penetration testing, and not just show off hacking skills. The course will help you demonstrate the true impact of web application flaws through exploitation.

Beyond high-quality course content, SEC542 focuses heavily on hands-on exercises to ensure that students can immediately apply all they learn. The world-class team of seasoned security professionals who serve as SEC542 instructors ensures that you will be taught by someone who is both a gifted instructor and a skilled practitioner. In addition to more than 30 formal hands-on labs throughout the course, there is also a Capture the Flag event on the final day during which students work in teams to perform a web application penetration test from start to finish.

ATTEND REMOTELY
If you are unable to attend this event, this course is also available via SANS Simulcast.
sans.org/event/pentest2015/attend-remotely

WHO SHOULD ATTEND:

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

SANS
SEC542

GWAPT
giac.org

sans.edu

sans.org/ondemand

sans.org/cyber-guardian

SEC560
Network Penetration Testing and Ethical Hacking

Six-Day Program | May 18-23 | 37 CPEs | Laptop Required

Instructor: Ed Skoudis

As a cybersecurity professional, you have a unique responsibility to find and understand your organization's vulnerabilities, and to work diligently to mitigate them before the bad guys pounce. Are you ready? SANS SEC560, our flagship course for penetration testing, fully arms you to address this task head-on.

"This type of training is fantastic, all new penetration testers and personnel who interact with testers or set up assessments should take SEC560." -Christopher Duffy, Knowledge Consulting Group

SEC560 is the must-have course for every well-rounded security professional.

This course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks and wireless and web apps, with over 30 detailed hands-on labs throughout.

"I think if you genuinely want to learn how exploitation techniques work and how to properly think like a hacker, it would be silly not to attend." -Mark Hamilton, McAfee

Learn the best ways to test your own systems before the bad guys attack.

Chock full of practical, real-world tips from some of the world's best penetration testers, SEC560 prepares you to perform detailed reconnaissance by examining a target's infrastructure and mining blogs, search engines, social networking sites and other Internet and intranet infrastructure. You will be equipped to scan target networks using best-of-breed tools. We will not just cover run-of-the-mill options and configurations, we will also go over the less-known but highly useful capabilities of the best pen test toolsets available today. After scanning, you will learn dozens of methods for exploiting target systems to gain access and measure real business risk, then examine post-exploitation, password attacks, wireless and web apps, pivoting through the target environment to model the attacks of real-world bad guys.

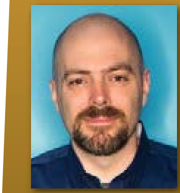
"I really enjoyed having real-world stories, not just technical 'how-to,' but also the logistical items such as cleaning up after the pen test." -Matt Armstrong, Stroz Friedberg, LLC

You will bring comprehensive penetration testing and ethical hacking know-how back to your organization.

After building your skills in challenging labs over five days, the course culminates with a full-day, real-world network penetration test scenario. You will conduct an end-to-end penetration test, applying the knowledge, tools and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization.

ATTEND REMOTELY
If you are unable to attend this event, this course is also available via SANS Simulcast.
sans.org/event/pentest2015/attend-remotely

Course updates, prerequisites, special notes, or laptop requirements: **sans.org/event/pentest2015/courses**



WHO SHOULD ATTEND:

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

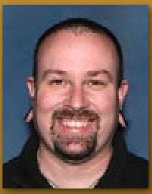
SANS SEC560

giac.org

sans.edu

sans.org/ondemand

sans.org/cyber-guardian



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

SANS
SEC617

giac.org

sans.edu

sans.org/ondemand

sans.org/cyber-guardian

SEC617
Wireless Ethical Hacking, Penetration Testing, and Defenses

Six-Day Program | May 18-23 | 36 CPEs | 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, 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 Z-Wave offer new methods of connectivity to devices, while other wireless technology, including WiFi, Bluetooth, Bluetooth Low Energy, and DECT, continue their massive growth rate, each introducing its own set of security challenges and attacker opportunities.

"The labs were great and provided a good means to practice the material. An excellent course for all levels of professionals who are dealing with wireless in the organization."
-John Fruge, B&W Technical Services

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 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.

"SEC617 helps bridge the gap of knowledge between the specialized attackers and corporate administrators."
-Robert Luettjohann, Overstock.com

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.

SEC660

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Six-Day Program | May 18-23 | 46 CPEs | Laptop Required

Instructor: Stephen Sims

This course is designed as a logical progression point for those who have completed **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 includes 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!

"The CTF with teams was awesome!!! I learned a lot more when working through some of the issues with my peers."
-Mike Evans, Alaska Airlines

Attackers are becoming more clever and their attacks more complex. In order to keep up with the latest attack methods, you need a strong desire to learn, the support of others, and the opportunity to practice and build experience. 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 is actually a technical class and not 'fad' info security garbage everyone else is teaching."
-Kyle Hanslovan, ManTech

Among the biggest benefits of SEC660 is the expert-level hands-on guidance provided through the labs and the additional time allotted each evening to reinforce daytime material and master the exercises.

"The SEC660 course was hands-on, packed with content, and current to today's technology!"
-Michael Horken, Rockwell Automation

WHO SHOULD ATTEND:

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

SANS

SEC660

giac.org

sans.edu

sans.org/ondemand

sans.org/cyber-guardian

Course updates, prerequisites, special notes, or laptop requirements: **sans.org/event/pentest2015/courses**

AUSTIN BONUS SESSIONS

The Effectiveness of Microsoft's EMET *Stephen Sims*

In this talk we will take a look at Microsoft's Enhanced Mitigation Experience Toolkit (EMET) and how it stops exploits from working. This free tool has a low adoption rate inside of companies, but has the ability to stop 0-day attacks from being successful. We will cover the effectiveness of the various controls, how they work, as well as techniques used to bypass the tool in targeted attacks.

Why Our Defenses Are Failing Us. One Click Is All It Takes.

Bryce Galbraith

Organizations are spending unprecedented amounts of money in an attempt to defend their assets...yet all too often, one click is all it takes for everything to come toppling down around them. Every day we read in the news about national secrets, intellectual property, financial records, and personal details being exfiltrated from the largest organizations on earth. How is this being done? How are adversaries bypassing our defenses (e.g. strong passwords, non-privileged accounts, anti-virus, firewalls/proxies, IDS/IPS, logging, etc.)? And most importantly, what can we do about it? A keen understanding of the true risks we face in today's threatscape is paramount to keeping your ones and zeros where they belong.

Continuous Ownage: Why you Need Continuous Monitoring

Seth Misenar

Repeat after me, "I will be breached." Most organizations realize this fact too late, usually after a third party informs them months after the initial compromise. Treating security monitoring as a quarterly auditing process means most compromises will go undetected for weeks or months. The attacks are continuous, and the monitoring must match. This talk will help you face this problem and describe how to move your organization to a more defensible security architecture that enables continuous security monitoring.

NetWars CORE Tournament Three Full Nights!

Tue, May 19; Wed, May 20; and Fri, May 22
6:30pm - 9:30pm

CyberCity

Thursday, May 21
6:30pm - 9:30pm

Coin-a-palooza

For participants who have taken a given SANS course, but have not won the capture the flag challenge coin, this event will offer the ability to catch up on the coins by participating in the three nights of NetWars challenges. If you've taken 504 in the past (but didn't win the coin), and make it from NetWars Level 1 into 2, you'll earn the 504 coin! If you make it into Level 3, you'll get your choice of a 542, 560, 561, 573 or 575 coin, provided you've taken the associated course sometime in the past. Make it into Level 4, and you'll get your choice of a 617, 642, 660 or 760 coin if you've had those classes! And, if you win NetWars, you'll get the NetWars coin. With Coin-a-palooza, you'll have an opportunity to win up to 4 challenge coins for your collection.

NetWars Comes in Four Forms

TOURNAMENT | CONTINUOUS | CYBERCITY | COURSE

Core NetWars is designed to help participants develop skills in several critical areas:

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

NetWars Tournament runs over an intense two- to three-day period, at a training event or hosted onsite. Many enterprises, government agencies, and military organizations rely on NetWars Tournament OnSite training to help identify skilled personnel and as part of extensive hands-on skill development.

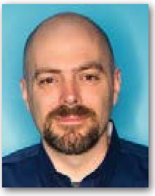
Take NetWars Continuous online and get up to 12 CPEs

NetWars Continuous allows participants to build their skills on their own time over a four-month period working from their office or home across the Internet. With a whole set of new challenges beyond those included in NetWars Tournament, participants can build their skills and experiment with new techniques in this Internet-accessible cyber range. Also, NetWars Continuous supports a unique Automated Hint System that turns dead ends into learning opportunities.

NetWars CyberCity, our most in-depth and ambitious offering, is designed to teach warriors and infosec pros that cyber action can have significant kinetic impact in the real world. With its 1:87 scale miniaturized physical city that features SCADA-controlled electrical power, water, transit, hospital, bank, retail, and residential infrastructures, CyberCity engages cyber defenders to protect the city's components.

The NetWars Courses: SEC561 & SEC562 are each 6 days of hands-on intensive learning, featuring 80% lab and exercise time and 20% debriefings to keep the lessons focused on practical keyboard technical skills. SANS 'top-gun' instructors provide a guided mission through SANS NetWars, working with participants to make sure the lessons of NetWars are hammered home. These offerings are truly designed to quickly enhance an individual's skills across a wide variety of different information security disciplines.

PEN TEST AUSTIN INSTRUCTORS



Ed Skoudis *SANS Faculty Fellow*

Ed Skoudis is the founder of Counter Hack, an innovative organization that designs, builds, and operates popular infosec challenges and simulations including CyberCity, NetWars, Cyber Quests, and Cyber Foundations. As director of the CyberCity project, Ed oversees the development of missions which help train cyber warriors in how to defend the kinetic assets of a physical, miniaturized city. Ed's expertise includes hacker attacks and defenses, incident response, and malware analysis, with over fifteen years of experience in information security. Ed authored and regularly teaches the SANS courses on network penetration testing (SEC560) and incident response (SEC504), helping over three thousand information security professionals each year improve their skills and abilities to defend their networks. He has performed numerous security assessments; conducted exhaustive anti-virus, anti-spyware, Virtual Machine, and IPS research; and responded to computer attacks for clients in government, military, financial, high technology, healthcare, and other industries. Previously, Ed served as a security consultant with InGuardians, International Network Services (INS), Global Integrity, Predictive Systems, SAIC, and Bell Communications Research (Bellcore). Ed also blogs about command line tips and penetration testing. @edskoudis

Bryce Galbraith *SANS Principal Instructor*

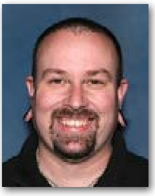
As a contributing author of the internationally bestselling book *Hacking Exposed: Network Security Secrets & Solutions*, Bryce helped bring the secret world of hacking out of the darkness and into the public eye. Bryce has held security positions at global ISPs and Fortune 500 companies, he was a member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

Seth Misenar *SANS Principal 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. Beyond his security consulting practice, Seth is a regular instructor for SANS. He teaches numerous SANS classes, including SEC401, SEC504, and SEC542. Seth has also served as both virtual mentor and technical director for SANS OnDemand, the online course delivery arm of the SANS Institute. @sethmisenar

Michael Murr *SANS Certified Instructor*

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



Larry Pesce *SANS Certified Instructor*

Larry is a senior security analyst with InGuardians after a long stint 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, warranties and his second Leatherman Multi-tool. 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. @haxorthematrix Blog: www.haxorthematrix.com

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 performing reverse engineering, exploit development, threat modeling, 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, SEC760: Advanced Exploit Development for Penetration Testers, which concentrates on complex heap overflows, patch diffing, and client-side exploits. Stephen is also the lead author on SEC660. 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. @Steph3nSims

FUTURE SANS TRAINING EVENTS

10TH ANNUAL ICS Security SUMMIT – ORLANDO 2015
Orlando, FL | February 22 - March 2 | #SANSICS

SANS DFIR Monterey 2015
Monterey, CA | February 23-28 | #DFIRMonterey

SANS Cyber Guardian 2015
Baltimore, MD | March 2-7 | #CyberGuardian

SANS Northern Virginia 2015
Reston, VA | March 9-14 | #SANSNoVA

SANS Houston 2015
Houston, TX | March 23-28 | #SANSHouston

SANS 2015
Orlando, FL | April 11-18 | #SANS2015

SANS Security West 2015
San Diego, CA | May 4-12 | #SecurityWest

SANSFIRE 2015
Baltimore, MD | June 13-20 | #SANSFIRE

SANS Rocky Mountain 2015
Denver, CO | June 22-27 | #SANSRockyMtn

Visit sans.org for a complete schedule.

SANS OnDemand Bundle

Add an OnDemand Bundle to your course to get an additional four months of intense training! OnDemand Bundles are just $629 when added to your live course, and include:

- Four months of OnDemand access to our custom e-learning platform
- Quizzes
- Labs
- MP3s and Videos of lectures
- Subject-Matter Expert support

Visit sans.org/ondemand/bundles
for more information about OnDemand Bundles now.

SANS Simulcast

Can't travel to Pen Test Austin 2015?

The following courses will be Simulcast live from the event:

SEC401 | SEC504 | SEC542 | SEC560

sans.org/simulcast

SANS PEN TEST AUSTIN 2015

Hotel Information

Training Campus

Omni Austin Hotel Downtown

700 San Jacinto @ 8th Street
Austin, TX 78701
sans.org/pentest2015/location

For magnificent luxury in the heart of the Texas state capital, Omni Austin Hotel Downtown offers an unparalleled experience. Enjoy spectacular views, well-appointed accommodations and easy access to the Austin Convention Center, the Texas State Capitol, and the 6th Street Entertainment District.

Special Hotel Rates Available

A special discounted rate of $213.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through April 24, 2015. To make reservations, please call (800) THE-OMNI (800-843-6664) and ask for the SANS group rate.

Top 5 reasons to stay at the Omni Austin Hotel Downtown

1 All SANS attendees receive complimentary high-speed Internet when booking in the SANS block.

2 No need to factor in daily cab fees and the time associated with travel to alternate hotels.

3 By staying at the Omni Austin Hotel Downtown, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.

4 SANS schedules morning and evening events at the Omni Austin Hotel Downtown that you won't want to miss!

5 Everything is in one convenient location!

SANS PEN TEST AUSTIN 2015

Registration Information

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

Register online at sans.org/pentest2015/courses

Select your course or courses and indicate whether you plan to test for GIAC certification.

If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with Internet access must complete the online registration form. We do not take registrations by phone.

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	4/1/15	$400.00	4/22/15	$200.00

Some restrictions apply.

Group Savings (Applies to tuition only)*

10% discount if 10 or more people from the same organization register at the same time

5% discount if 5-9 people from the same organization register at the same time

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

**Early-bird rates and/or other discounts cannot be combined with the group discount.*

Cancellation

You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by April 29, 2015 – processing fees may apply.

SANS Voucher Credit Program

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