SANS Pen Test Austin 2016

Austin, TX | April 18-23

CYBERSECURITY TRAINING EVENT

This SPECIAL event features:

NETWARS

Three nights of fun NetWars challenges

(more than traditional SANS events!)

Internet of Things

We will have a collection of "things" in which you can try to find vulnerabilities. We will walk through an introduction that covers how to extract and analyze firmware, as well as the types of bugs that are most commonly found.

Coin-a-Palooza

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

NetWars is available AT NO EXTRA CHARGE for those who sign up for a course at the SANS Pen Test Austin event.

"Hands down, one of the best SANS courses I have taken! I learned cutting-edge pen testing techniques in a hands-on environment that challenged my abilities and increased my overall knowledge."

-Dave Odom, Bechtel

6 COURSES OFFERED

- SEC401: Security Essentials Bootcamp Style
- SEC504: Hacker Tools, Techniques, Exploits & Incident Handling
- *NEW!* SEC560: Network Penetration Testing & Ethical Hacking
- SEC642: Advanced Web App Penetration Testing and Ethical Hacking
- SEC660: Advanced Penetration Testing, Exploit Writing & Ethical Hacking
- *NEW!* HOSTED: Physical Security Specialist - Facilities Edition

sans.org/pentest2016

SAVE $400

by paying early! See page 13 for details.

GIAC Approved Training

"Hackers"

- individuals who enjoy the intellectual challenge of creatively overcoming and circumventing limitations of systems to achieve novel and clever outcomes.

Ed Skoudis

Does this sound like you? If so, we've got a really special event brewing for you at SANS Pen Test Austin 2016, and you've gotta check it out. Every organization needs people with real-world skills who know how to find vulnerabilities, understand risk, and help prioritize resources based on mitigating potential 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. SANS Pen Test Austin 2016 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 penetration test training experiences ever.

At SANS Pen Test Austin 2016, you will not only learn vital and in-demand skills and abilities, you'll also network with like-minded security professionals who also see the benefit in taking their pen testing artistry to the next level.

What's special about SANS Pen Test Austin 2016?

- **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 five additional SANS Pen Test Challenge Coins (each with an integrated cipher challenge) based on your performance in SANS NetWars!
- **Internet of Things.** We will have a collection of "things" in which you can try to find vulnerabilities. We will walk through an introduction of how to extract and analyze firmware, and the types of bugs that are most commonly found.

I urge you to check out all of our great offerings at this event. It's truly a special SANS training event, and I hope to see you there!

Ed Skoudis
SANS Pen Test Curriculum Lead

The Value of SANS Training & YOU

EXPLORE

- Read this brochure and note the courses that will enhance your role in your organization
- Use the Career Roadmap (sans.org/media/security-training/roadmap.pdf) to plan your growth in your chosen career path

RELATE

- Consider how security needs in your workplace will be met with the knowledge you'll gain in a SANS course
- Know the education you receive will make you an expert resource for your team

VALIDATE

- Pursue a GIAC Certification after your training to validate your new expertise
- Add a NetWars challenge to your SANS experience to prove your hands-on skills

SAVE

- Register early to pay less using early-bird specials
- Consider group discounts or bundled course packages to make the most of your training budget

ADD VALUE

- Network with fellow security experts in your industry
- Prepare thoughts and questions before arriving to share with the group
- Attend SANS@Night talks and activities to gain even more knowledge and experience from instructors and peers alike

ALTERNATIVES

- If you cannot attend a live training event in person, attend the courses virtually via SANS Simulcast
- Use SANS OnDemand or vLive to complete the same training online from anywhere in the world, at any time

ACT

- Bring the value of SANS training to your career and organization by registering for a course today, or contact us at 301-654-SANS with further questions

Return on Investment

SANS live training is recognized as the best resource in the world for information security education. With SANS, you gain significant returns on your InfoSec investment. Through our intensive immersion classes, our training is designed to help your staff master the practical steps necessary for defending systems and networks against the most dangerous threats – the ones being actively exploited.

REMEMBER

the SANS promise:

You will be able to apply our information security training the day you get back to the office!

SEC401:
Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Apr 18 - Sat, Apr 23
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Paul A. Henry

- GIAC Cert: GSEC
- STI Master's Program
- Cyber Guardian
- DoDD 8570
- OnDemand Bundle

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*!

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

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.

AVAILABLE VIA SIMULCAST
sans.org/simulcast

Who Should Attend

- Security professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Operations personnel who do not have security as their primary job function but need an understanding of security to be effective
- IT engineers and supervisors who need to know how to build a defensible network against attacks

"SEC401 was an excellent introduction to networking security fundamentals that every IT person should attend."
-Fawad Sami, Vermilian

GSEC
giac.org

SANS Technology Institute
sans.edu

sapere aude
sans.org/cyber-guardian

sans.org/8570

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

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 principal 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 (United States), and both government as well as telecommunications projects throughout Southeast Asia. @phenrycissp

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Mon, Apr 18 - Sat, Apr 23
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
Laptop Required
37 CPEs
Instructor: Kevin Fiscus

- GIAC Cert: GCIH
- STI Master's Program
- Cyber Guardian
- DoDD 8570
- OnDemand Bundle

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.

Who Should Attend

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

By helping you understand attackers' tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan, 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 for, 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!

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.

AVAILABLE VIA SIMULCAST
sans.org/simulcast

"SEC504 walks through the entire incident handling process in full depth with practical scenarios and labs."
-Christopher Holden, Protivity

"This is the real deal. This is real-world stuff that we can implement in our environments tomorrow."
-Garrett Bemis, Pacific Northwest National Laboratory

GCIH
giac.org

SANS Technology Institute
sans.edu

sapere aude
sans.org/cyber-guardian

sans.org/8570

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

Kevin Fiscus *SANS Certified Instructor*

Kevin Fiscus is the founder of and lead consultant for Cyber Defense Advisors, where he performs security and risk assessments, vulnerability and penetration testing, security program design, policy development and security awareness with a focus on serving the needs of small and mid-sized organizations. Kevin has over 20 years of IT experience and has focused exclusively for the past 12 years on information security. Kevin currently holds the CISA, GPEN, GREM, GMOB, GCED, GCFA-Gold, GCIA-Gold, GCIH, GAWN, GPPA, GCWN, GCSC-Gold, GSEC, SCSA, RCSE, and SnortCP certifications and is proud to have earned the top information security certification in the industry, the GIAC Security Expert. Kevin has also achieved the distinctive title of SANS Cyber Guardian for both red team and blue team. @kevinbfiscus

SEC560:

Network Penetration Testing and Ethical Hacking

NEW

SANS

Six-Day Program
Mon, Apr 18 - Sat, Apr 23
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
Laptop Required
37 CPEs
Instructor: Ed Skoudis

- GIAC Cert: GPEN
- Cyber Guardian
- STI Master's Program
- OnDemand Bundle

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.

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

With comprehensive coverage of tools, techniques, and methodologies for network penetration testing, SEC560 truly prepares you to conduct high-value penetration testing projects step-by-step and end-to-end. Every organization needs skilled information security personnel who can find vulnerabilities and mitigate their effects, and this entire course is specially designed to get you ready for that role. The course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks, and web app manipulation, with over 30 detailed hands-on labs throughout. The course is chock full of practical, real-world tips from some of the world's best penetration testers to help you do your job safely, efficiently…and masterfully.

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

SEC560 is designed to get you ready to conduct a full-scale, high-value penetration test – and on the last day of the course you'll do just that. After building your skills in comprehensive and challenging labs over five days, the course culminates with a final full-day, real-world penetration test scenario. You'll conduct an end-to-end pen test, applying knowledge, tools, and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization, demonstrating the knowledge you've mastered in this course.

This course will teach you how to perform detailed reconnaissance, studying a target's infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. Our hands-on labs will equip you to scan target networks using best-of-breed tools. We won't just cover run-of-the-mill options and configurations, we'll also go over the lesser-known but super-useful capabilities of the best pen test toolsets available today. After scanning, you'll learn dozens of methods for exploiting target systems to gain access and measure real business risk. You'll dive deep into post-exploitation, password attacks, and web apps, pivoting through the target environment to model the attacks of real-world bad guys to emphasize the importance of defense in depth.

AVAILABLE VIA SIMULCAST
sans.org/simulcast

Who Should Attend

- Security personnel whose job involves assessing networks and systems to find and remediate vulnerabilities
- Penetration testers
- Ethical hackers
- Defenders who want to better understand offensive methodologies, tools, and techniques
- Auditors who need to build deeper technical skills
- Red and blue team members
- Forensics specialists who want to better understand offensive tactics

GPEN
giac.org

SANS Technology Institute
sans.edu

sapere aude
sans.org/cyber-guardian

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

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 that help train cyber warriors 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 15 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 3,000 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

SEC642:

Advanced Web App Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Mon, Apr 18 - Sat, Apr 23
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor:
Adrien de Beaupre

sans.org/simulcast

"SEC642 is the perfect course for someone who has a background in web app pen testing, but wants to really gain advanced skills."
-Matthew Sullivan, Webfilings

"I like this training because it is very hands on and not just focused on slides – very helpful for the real world."
-Zach Moreno, Chico Security

This course is designed to teach you the advanced skills and techniques required to test today's web applications. 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.

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.

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.

This information-packed, advanced pen testing course will wrap up with a full-day Capture-the-Flag event that will target an imaginary organization's web applications and 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.

Adrien de Beaupre *SANS Certified Instructor*

Adrien de Beaupre works as an independent consultant in beautiful Ottawa, Ontario. His work experience includes technical instruction, vulnerability assessment, penetration testing, intrusion detection, incident response and forensic analysis. He is a member of the SANS Internet Storm Center (isc.sans.edu). He is actively involved with the information security community, and has been working with SANS since 2000. Adrien holds a variety of certifications including the GXPN, GPEN, GWAPT, GCIH, GCIA, GSEC, CISSP, OPST, and OPSA. When not geeking out he can be found with his family, or at the dojo. @adriendb

SEC660:

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

SANS

Six-Day Program
Mon, Apr 18 - Sat, Apr 23
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Stephen Sims

- GIAC Cert: GXPN
- Cyber Guardian
- STI Master's Program
- OnDemand Bundle

Who Should Attend

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

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, Windows exploit-writing, and much more!

"This course gave me the background and tools I'll need to go deeper!"
-Kristine A., DoD

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

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.

giac.org

sans.edu

sans.org/cyber-guardian

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

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 of 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. @Steph3nSims

HOSTED:

Physical Security Specialist – Facilities Edition

NEW

Five-Day Program | Mon, Apr 18 - Fri, Apr 22 | 9:00am - 5:00pm | Laptop NOT Needed | 30 CPEs

Instructor: The CORE Group

Physical security is an oft-overlooked component of data and system security in the technology world. While frequently forgotten, it is no less critical than timely patches, appropriate password policies, and proper user permissions. You can have the most hardened servers and network, but that doesn't make the slightest difference if someone can gain direct access to a keyboard or, worse yet, march your hardware right out the door.

Who Should Attend

This training is ideal for anyone who is tasked with making physical security decisions regarding existing or new facilities.

The **CORE Group** is a firm with divisions that focus on penetration testing, physical defense, personal protection details, and law enforcement training. Those who attend this course will leave with a full awareness of how to best protect buildings and grounds from unauthorized access, as well as how to compromise most existing physical security in order to gain access themselves. Our subject-matter experts will immerse you in all the necessary components of a well-layered physical defense system and then teach you how to conduct a thorough site analysis of a facility.

During the first two days of this course, attendees will not only learn how to distinguish good locks and access control from poor ones, but will also become well-versed in picking and bypassing many of the most common locks in order to assess their own company's security posture or to augment their career as a penetration tester.

On the third and fourth days, students will learn to evaluate physical barriers, defensive lighting, doors, external and internal physical intrusion detection systems, camera placement, access controls, and standard operating procedures. They will also be exposed to best-practice standards and a robust variety of adversarial methodologies used to compromise weak targets such as social engineering and the exploitation of a weak employee culture. Numerous in-depth case studies and practical hands-on demonstrations will be utilized to solidify the acquisition of knowledge.

The training concludes on day five with an intense specialization focus: **safe-cracking**. Students will all be issued a mounted safe dial and will learn the fundamentals of safe manipulation and attack. While many commercially-available safes offer high security, the most document safes and gun safes currently in the field do not. Most individuals can learn how to manipulate and open a conventional safe dial with one day of instruction. Today is that day.

By the end of this course, students will be very prepared to make educated and fiscally-responsible security decisions not only for their respective organizations but also for themselves. Participants will be able to approach any target, site-unseen, and then either conduct a walk-through assessment highlighting attack vectors, or proceed directly with an attack and thus gain physical access to critical areas and infrastructure. Additionally, these newly minted professionals from our training will also be able to provide sound documentation while making recommendations to management or to their insurance providers, saving money for their companies.

The CORE Group *Instructor*

The CORE Group provides specialized consulting that focuses on physical security solutions, including training, blended penetration testing, and innovative tools for clients who seek security on all surfaces. Its senior team's combined experience in the physical security sector represents decades of hard knowledge and applied work.

The CORE Group finds innovative ways to augment typical security auditing, assessment, and training by approaching topics that others often fail to consider: mechanical locks, electronic locks, safes, alarm systems, elevator systems, and much more.

NETWARS

Are you one of the top Information Security Professionals in Texas?

Prove your knowledge and skills at

3 Nights of NetWars at SANS Pen Test Austin 2016!

TUE, APR 19 WED, APR 20 FRI, APR 22

Come and join us for this exciting event to test your skills in a challenging and fun learning environment. Registration for NetWars is **FREE OF CHARGE TO ALL STUDENTS AT SANS PEN TEST AUSTIN 2016.** External participants are welcome to join for an entry fee of $1,450.

SANS NetWars is a dynamic cyber range that allows participants to build, practice, and measure their skills in a real-world environment using defensive, analytic, and offensive tactics. We designed NetWars to appeal to a wide range of participant skill sets by using a system with different levels.

All players start at Level 1, which measures foundational cybersecurity skills. More skilled players can rise rapidly through the ranks to a level suitable for their skill set – top players can make it to Level 4, and only the best of the best can reach level 5.

sans.org/pentest2016

AUSTIN
BONUS SESSION

Internet of things

Hosted by Stephen Sims

Monday, April 18 | 7:15-9:15pm

Somewhere along the line, product developers thought it would be a good idea to connect things like pet food dispensers and automated plant-watering devices to the Internet and smartphone apps.

What could go wrong?

We will have a collection of "things" in which you can try to find vulnerabilities. We will walk through an introduction that covers how to extract and analyze firmware, as well as the types of bugs that are most commonly found.

Build Your Best Career

WITH

SANS

Add an

OnDemand Bundle & **GIAC Certification Attempt**

to your course within seven days of this event for just $659 each.

SPECIAL PRICING

OnDemand Bundle

- Four months of supplemental online review
- 24/7 online access to your course lectures, materials, quizzes, and labs
- Subject-matter expert support to help you increase your retention of course material

"The course content and OnDemand delivery method have both exceeded my expectations."

-Robert Jones, Team Jones, Inc.

GIAC Certification

- Distinguish yourself as an information security leader
- 30+ GIAC certifications to choose from
- Two practice exams included
- Four months of access to complete the attempt

"GIAC is the only certification that proves you have hands-on technical skills."

-Christina Ford, Department of Commerce

MORE INFORMATION

www.sans.org/ondemand/bundles www.giac.org

*GIAC and OnDemand Bundles are only available for certain courses.

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

Multi-Course Training Events sans.org/security-training/by-location/all
Live Instruction from SANS' Top Faculty, Vendor Showcase, Bonus Evening Sessions, and Networking with Your Peers

Community SANS sans.org/community
Live Training in Your Local Region with Smaller Class Sizes

Private Training sans.org/private-training
Live Onsite Training at Your Office Location. Both In-person and Online Options Available

Mentor sans.org/mentor
Live Multi-Week Training with a Mentor

Summit sans.org/summit
Live IT Security Summits and Training

ONLINE TRAINING

OnDemand sans.org/ondemand
E-learning Available Anytime, Anywhere, at Your Own Pace

vLive sans.org/vlive
Online Evening Courses with SANS' Top Instructors

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

OnDemand Bundles sans.org/ondemand/bundles
Extend Your Training with an OnDemand Bundle Including Four Months of E-learning

FUTURE SANS TRAINING EVENTS

Security East 2016
New Orleans, LA | Jan 25-30

Cyber Threat Intelligence
SUMMIT & TRAINING 2016
Alexandria, VA | Feb 3-10

Scottsdale 2016
Scottsdale, AZ | Feb 8-13

NORTHERN VIRGINIA **McLean** 2016
McLean, VA | Feb 15-20

ICS Security
SUMMIT & TRAINING 2016
Orlando, FL | Feb 16-23

Anaheim 2016
Anaheim, CA | Feb 22-27

Philadelphia 2016
Philadelphia, PA | Feb 29 - Mar 5

SANS 2016
Orlando, FL | Mar 12-21

NORTHERN VIRGINIA **Reston** 2016
Reston, VA | Apr 4-9

Atlanta 2016
Atlanta, GA | Apr 4-9

Threat Hunting and Incident Response
SUMMIT & TRAINING 2016
New Orleans, LA | Apr 12-19

Security West 2016
San Diego, CA | Apr 29 - May 6

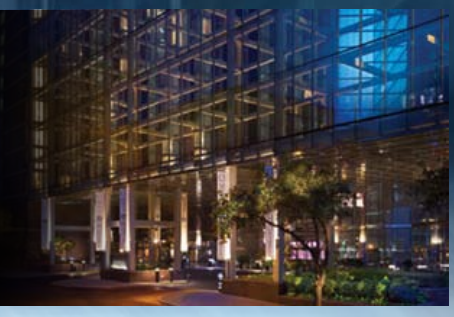
Baltimore Spring 2016
Baltimore, MD | May 9-14

Houston 2016
Houston, TX | May 9-14

Information on all events can be found at
sans.org/security-training/by-location/all

SANS PEN TEST AUSTIN 2016

Hotel Information



Training Campus

Omni Austin Hotel Downtown

700 San Jacinto At 8th Street
Austin, TX 78701
512-476-3700
sans.org/event/pentest2016/location

For magnificent luxury in the heart of the Texas state capital, Omni Austin Hotel Downtown offers an unparalleled experience for business and vacation travelers alike. Enjoy spectacular views, well-appointed accommodations, and easy access to the Texas State Capitol, and the 6th Street Entertainment District. Whether you're looking for high culture, live music or an unforgettable event, Omni Austin Hotel Downtown can make it happen for you.

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 March 25, 2016.

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 2016

Registration Information

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

Register online at sans.org/pentest2016/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.

Use code **EarlyBird16** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**2-24-16**	**$400.00**	**3-16-16**	**$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.

Cancellation

You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by March 30, 2016 – 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

Open a **SANS Portal Account** today to enjoy these FREE resources:

WEBCASTS

Ask The Expert Webcasts – SANS experts bring current and timely information on relevant topics in IT Security.

Analyst Webcasts – A follow-on to the SANS Analyst Program, Analyst Webcasts provide key information from our whitepapers and surveys.

WhatWorks Webcasts – The SANS WhatWorks webcasts bring powerful customer experiences showing how end users resolved specific IT Security issues.

Tool Talks – Tool Talks are designed to give you a solid understanding of a problem, and to show how a vendor's commercial tool can be used to solve or mitigate that problem.

NEWSLETTERS

NewsBites – Twice-weekly high-level executive summary of the most important news relevant to cybersecurity professionals

OUCH! – The world's leading monthly free security-awareness newsletter designed for the common computer user

@RISK: The Consensus Security Alert – A reliable weekly summary of (1) newly discovered attack vectors, (2) vulnerabilities with active new exploits, (3) how recent attacks worked, and (4) other valuable data

OTHER FREE RESOURCES

- InfoSec Reading Room
- Top 25 Software Errors
- 20 Critical Controls
- Security Policies
- Intrusion Detection FAQ
- Tip of the Day
- Security Posters
- Thought Leaders
- 20 Coolest Careers
- Security Glossary
- SCORE (Security Consensus Operational Readiness Evaluation)

sans.org/security-resources