THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH

SANS Pen Test Austin 2017

Austin, TX | March 27 - April 1

HANDS-ON, IMMERSION-STYLE

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

PENETRATION TESTING
ETHICAL HACKING
VULNERABILITY ASSESSMENT
EXPLOIT DEVELOPMENT
WEB APP PEN TESTING

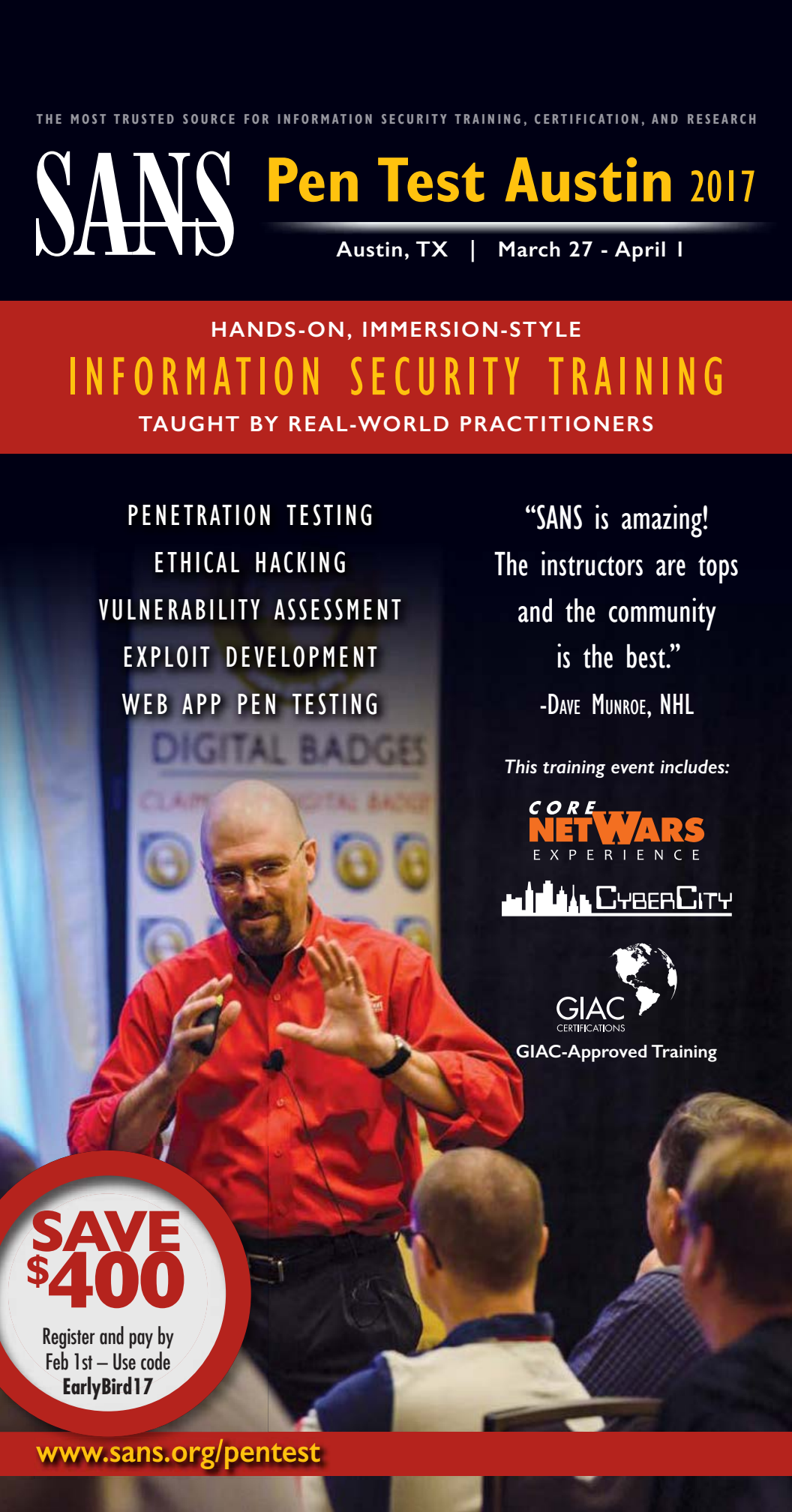
"SANS is amazing! The instructors are tops and the community is the best."
-Dave Munroe, NHL

This training event includes:

CORE NETWARS EXPERIENCE

CYBERCITY

GIAC CERTIFICATIONS
GIAC-Approved Training



SAVE $400

Register and pay by Feb 1st – Use code **EarlyBird17**

www.sans.org/pentest

Hackers

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

Ed Skoudis

If this sounds like you, you can't afford to miss **SANS Pen Test Austin 2017**. There will be six days of nonstop, in-depth, and hands-on ethical hacking, penetration testing, and exploit development training.

Every organization needs skilled people 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.

This SANS training event isn't just for penetration testers and red team members, it is for any information security professional who wants to understand the mindset, tools, and techniques used by adversaries who intrude where they don't belong.

What's special about **SANS Pen Test Austin**?

- **SANS Training:** Learn hands-on skills that you can directly apply the day you get back to your job. Courses are for every level of information security practitioner, from SEC401 (Introductory) to SEC660 (Advanced Pen Test).
- **The NetWars Experience (version 4.0):** Enjoy three exciting nights of the SANS NetWars Experience, 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 the SANS NetWars Experience!
- **SANS CyberCity Missions:** Hone your skills as you protect the fictional citizens of CyberCity from the threat of nefarious cyber-attackers inside this real physical model city. You'll see what it looks like to hack a modern city.
- **And much more...**

I urge you to check out all the great stuff we are offering at this event. It's truly a special SANS training experience, 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 (www.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

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!

SANS Instructors

SANS instructors are real-world practitioners who specialize in the subjects they teach. All instructors undergo rigorous training and testing in order to teach SANS courses. This guarantees that what you learn in class will be up to date and relevant to your job. The SANS Pen Test Austin 2017 lineup of instructors includes:

Eric Conrad
Senior Instructor
@eric_conrad

Adrien de Beaupre
Certified Instructor
@adriendb

James Leyte-Vidal
Instructor
@jamesleytevidal

Tim Medin
Certified Instructor
@timmedin

Keith Palmgren
Senior Instructor
@kpalmgren

Chris Pizor
Certified Instructor
@chris_pizor

Stephen Sims
Senior Instructor
@Steph3nSims

Ed Skoudis
Faculty Fellow
@edskoudis

Donald Williams
Certified Instructor
@donaldjwilliam5

CORE NETWARS EXPERIENCE

CYBERCITY

Special Events

Two NetWars Experiences are FREE for all SANS Pen Test Austin 2017 students, but registration is limited! Register for either CORE NetWars or NetWars CyberCity with your course to guarantee your seat.

Non-student entrance fees are $1,520 for Core NetWars and $659 for NetWars CyberCity

Save $400 when you register and pay by Feb 1st using code EarlyBird17

Courses at a Glance

		MON 3-27	TUE 3-28	WED 3-29	THU 3-30	FRI 3-31	SAT 4-1
SEC401	Security Essentials Bootcamp Style	Page 3 SIMULCAST					
SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling	Page 4 SIMULCAST					
SEC542	Web App Penetration Testing and Ethical Hacking	Page 5					
SEC550	Active Defense, Offensive Countermeasures and Cyber Deception	Page 6					
SEC560	Network Penetration Testing and Ethical Hacking	Page 7 SIMULCAST					
SEC562	CyberCity Hands-on Kinetic Cyber Range Exercise	Page 8					
SEC617	Wireless Ethical Hacking, Penetration Testing & Defenses	Page 9					
SEC642	Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques *NEW!*	Page 10					
SEC660	Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	Page 11					
Core NetWars Experience							
NetWars – CyberCity							

SEC401:
Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Mar 27 - Sat, Apr 1
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Keith Palmgren

See page 17 for details.

www.giac.org/gsec

www.sans.edu

www.sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"This course has been the most comprehensive security training in my 21 years of IT professional experience."
-Marcus M., U.S. Air Force

This course will teach you the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. You'll 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*!

Who Should Attend

- Security professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Operations personnel who do not have security as their primary job function but need an understanding of security to be effective
- IT engineers and supervisors who need to know how to build a defensible network against attacks
- Administrators responsible for building and maintaining systems that are being targeted by attackers
- Forensic analysts, penetration testers, and auditors who need a solid foundation of security principles so they can be as effective as possible at their jobs
- Anyone new to information security with some background in information systems and networking

With the rise of advanced persistent threats, 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.

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

Keith Palmgren *SANS Senior Instructor*

Keith Palmgren is an IT security professional with 26 years of experience in the field. He began his career with the U.S. Air Force working with cryptographic keys and codes management. He also worked in what was at the time the newly-formed computer security department. Following the Air Force, Keith worked as an Management Information Systems director for a small company before joining AT&T/Lucent as a senior security architect working on engagements with the DoD and the National Security Agency. As security practice manager for both Sprint and Netigy, Keith built and ran the security consulting practice, responsible for all security consulting world-wide and for leading dozens of security professionals on many consulting engagements across all business spectrums. For the last several years, Keith has run his own company, NetIP, Inc. He divides his time between consulting, training, and freelance writing projects. As a trainer, Keith has satisfied the needs of nearly 5,000 IT professionals and authored 17 training courses. Keith currently holds the CISSP, GSEC, CEH, Security+, Network+, A+, and CTT+ certifications. @kpalmgren

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Mon, Mar 27 - Sat, Apr 1
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Donald Williams

See page 17 for details.

www.giac.org/gcih

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

▶II
BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

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
- 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

"Higher education is often a hacker's playground/training camp. Courses like SEC504 are important to learn what to watch for." -Michael Barton, Princeton University

This course enables you to turn the tables on computer attackers by helping you understand their 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. 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 attacks. 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, exploiting, and defending systems. This 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.**

"Excellent course! I've learned about the techniques and tools used by the bad guys and I have a greater understanding of how to protect our network."
-Howard Duck, Schools Financial Credit Union

Donald Williams *SANS Certified Instructor*

Donald retired from active duty in 2014 after over 20 years of service in the U.S. Army. He has extensive experience in incident handling, intrusion analysis, and network auditing. During his career in the Army, he served as the Defensive Cyber Operations Chief for the Army's Regional Computer Emergency Response Team in South West Asia (RCERT-SWA), directly overseeing the intrusion analysis and incident response teams for one of the Army's largest networks spanning over 10 countries. Donald holds several GIAC certifications, including the GIAC Security Expert (GSE), GCIH, GCIA, and GSNA certifications, as well as numerous other industry certifications. @donaldjwilliam5

SEC542:

Web App Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Mon, Mar 27 - Sat, Apr 1
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Eric Conrad

www.giac.org/gwapt

SANS Technology Institute
www.sans.edu

www.sans.org/cyber-guardian

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"This course shows a hands-on way of doing web app testing and not just how to use this tool or that." -Christopher J. Stover, Infogressive Inc.

Web applications play a vital role in every modern organization. But if your organization does not properly **test** and **secure** its web apps, adversaries can 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.

Who Should Attend

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

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 business tools within any organization. **Unfortunately, there is no "patch Tuesday" for custom web applications, and major industry studies find 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.

"This training boosted my thoughts and perspective on IT and has taught me how to think outside of the box." -Ephraim P., U.S. Air Force

Modern cyber defense requires a realistic and thorough understanding of web application security issues. Anyone can learn to sling a few web hacks, but effective web application penetration testing requires something deeper.

In this course, students will come to understand major web application flaws and their exploitation. Most importantly, they'll 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. This course will help you demonstrate the true impact of web application flaws through exploitation.

In addition to having more than 30 formal hands-on labs, the course culminates in a web application pen test tournament, powered by the SANS NetWars Cyber Range. **This Capture-the-Flag event on the final day brings students into teams to apply their newly acquired command of web application penetration testing techniques in a fun way that hammers home lessons learned.**

Eric Conrad *SANS Senior Instructor*

Eric Conrad is lead author of the book *The CISSP Study Guide*. Eric's career began in 1991 as a UNIX systems administrator for a small oceanographic communications company. He gained information security experience in a variety of industries, including research, education, power, Internet, and healthcare. He is now president of Backshore Communications, a company focusing on intrusion detection, incident handling, information warfare, and penetration testing. He is a graduate of the SANS Technology Institute with a master of science degree in information security engineering. In addition to the CISSP, he holds the prestigious GIAC Security Expert (GSE) certification as well as the GIAC GPEN, GCIH, GCIA, GCFA, GAWN, and GSEC certifications. Eric also blogs about information security at ericconrad.com. @eric_conrad

SEC550:
Active Defense, Offensive Countermeasures & Cyber Deception

SANS

Five-Day Program
Mon, Mar 27 - Fri, Mar 31
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Chris Pizor

The current threat landscape is shifting. Traditional defenses are failing us. **We need to develop new strategies to defend ourselves.** Even more importantly, we need to better understand who is attacking us and why. You may be able to immediately implement some of the measures we discuss in this course, while others may take a while. Either way, consider what we discuss as a collection of tools at your disposal when you need them to annoy attackers, determine who is attacking you, and, finally, attack the attackers.

Who Should Attend

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

SEC550: Active Defense, Offensive Countermeasures, and Cyber Deception is based on the Active Defense Harbinger Distribution live Linux environment funded by the Defense Advanced Research Projects Agency (DARPA). This virtual machine is built from the ground up for defenders to quickly implement Active Defenses in their environments. The course is very heavy with hands-on activities – we won't just talk about **Active Defenses**, we will work through **labs** that will enable you to quickly and easily implement what you learn in your own working environment.

"Invaluable course for learning how to identify hackers and their methods and how to boot them from your company."
-Da-Wyone Haynes, TransAmerica

"The value of SEC550 is less of the exact materials and more of the mindset and a way of thinking it instills. This is the value of all SANS classes I have taken."
-Kevin Holleran, Four Winds Casino

You Will Be Able To

- Track bad guys with callback Word documents
- Use Honeybadger to track web attackers
- Block attackers from successfully attacking servers with honeyports
- Block web attackers from automatically discovering pages and input fields
- Understand the legal limits and restrictions of Active Defense
- Obfuscate DNS entries
- Create non-attributable Active Defense Servers
- Combine geolocation with existing Java applications
- Create online social media profiles for cyber deception
- Easily create and deploy honeypots

What You Will Receive

- A fully functioning Active Defense Harbinger Distribution ready to deploy
- Class books and a DVD with the necessary tools and the OCM virtual machine, which is a fully functional Linux system with the OCM tools installed and ready to go for the class and for the students' work environments

Chris Pizor *SANS Certified Instructor*

Chris Pizor is a civilian employee working for the U.S. Air Force as the lead curriculum designer for cyber warfare operations training. Chris served on active duty in the USAF as a Network Intelligence Analyst before retiring in 2010. He was part of the initial cadre of the NSA Threat Operations Center and helped develop tactics to discover and eradicate intrusions into U.S. government systems. Chris has worked in the intelligence community for more than 20 years, including 12 years focused on cybersecurity. Over the course of his active duty career, Chris received multiple individual and team awards. Chris is passionate about security and helping others advance their security knowledge, and is continuously researching and refining his own skills so he can prepare U.S. airmen and women and other professionals to defend their vital networks and critical infrastructure. Chris earned a bachelor's degree in intelligence studies and information operations from the American Military University and a master's of science in cybersecurity from University of Maryland University College. He holds the GSEC, GCIA, GCIH, GPEN, GXPN, GCFA, GISP, and CISSP certifications. When Chris isn't working, he enjoys spending time with his wife and two young children, woodworking, and spending time outdoors. @chris_pizor

SEC560:

Network Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Mon, Mar 27 - Sat, Apr 1
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Ed Skoudis

See page 17 for details.

www.giac.org/gpen

www.sans.edu

www.sans.org/cyber-guardian

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"SEC560 works for everyone! It starts from the ground up and runs from there – tremendous value and exceptional experience."
-Scott Trest, University FCU

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.

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.

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.

You will learn 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.**

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

Ed Skoudis *SANS Faculty Fellow*

Ed Skoudis has taught cyber incident response and advanced penetration testing techniques to more than 12,000 cybersecurity professionals. He is the lead for the SANS Penetration Testing Curriculum. His courses distill the essence of real-world, front-line case studies because he is consistently one of the first experts brought in to provide after-attack analysis of major breaches where credit card and other sensitive financial data is lost. Ed led the team that built NetWars, the low-cost, widely used cyber training and skills assessment ranges relied upon by military units and corporations with major assets at risk. His team also built CyberCity, the fully authentic urban cyber warfare simulator that was featured on the front page of the *Washington Post*. He was the expert called in by the White House to test the security viability of the Trusted Internet Connection (TIC) that now protects U.S. government networks and to lead the team that first publicly demonstrated significant security flaws in virtual machine technology. He has a rare capability to translate advanced technical knowledge into easy-to-master guidance, as evidenced by the popularity of his step-by-step *Counter Hack* books. @edskoudis

SEC562:

CyberCity Hands-on Kinetic Cyber Range Exercise

SANS

Six-Day Program
Mon, Mar 27 - Sat, Apr 1
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Tim Medin

Computers, networks, and programmable logic controllers operate most of the physical infrastructure of our modern world, ranging from electrical power grids, water systems, and traffic systems all the way down to HVAC systems and industrial automation. Increasingly, security professionals need the skills to assess and defend this important infrastructure. **In this innovative and cutting-edge course based on the SANS CyberCity kinetic range, you will learn how to analyze and assess the security of control systems and related infrastructure, finding vulnerabilities that could result in significant kinetic impact.**

Who Should Attend

- Red and blue team members
- Cyber warriors
- Incident handlers
- Penetration testers
- Ethical hackers
- Other security personnel who are first responders when systems come under attack

"The benefit from this course is the experience in tinkering with industry standard hardware control systems such as PLCs and software SCADA systems. No other class seems to target this up-and-coming subject area."

-Phillip A. Smith

NetWars CyberCity

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 physical world. As computer technology, networks, and industrial control systems permeate nearly every aspect of modern life, military, government, and commercial organizations have an increasing need for skilled defenders to protect critical infrastructure. We engineered and built CyberCity to help organizations grow these capabilities in their teams.

CyberCity is a 1:87 scale miniaturized physical city that features SCADA-controlled electrical power distribution, as well as water, transit, hospital, bank, retail, and residential infrastructure. CyberCity engages participants to defend the city's components from terrorist cyber attacks, as well as to utilize offensive tactics to retake or maintain control of critical assets.

Participants engage in **missions**, with specific operation orders describing the **defensive** or **offensive** goal they need to achieve. On some missions, participants prevent attackers from undermining the CyberCity infrastructure and wreaking havoc, with all the kinetic action captured through streaming video cameras mounted around the physical city. On **offensive missions**, participants must seize control of CyberCity assets, retaking them from adversaries and using them to achieve a kinetic impact specified in their operation orders. Each mission includes not only a list of goals to be achieved, but also specific sensitive city assets that are out of bounds for the engagement, requiring additional tactical planning to adhere to the rules of engagement.

To achieve mission objectives, **participants work as a team**, engaging in effective mission planning, devising overall strategies and particular tactics, and exercising detailed technical skills. Furthermore, some participants will be charged as leaders of their teams, helping to build and assess leadership skills, decision-making capabilities, and the ability to brief senior leadership. **Multiple realistic defensive and offensive missions test the cyberspace engineer's ability to thwart the best efforts of a well-funded terrorist organization or other cyber attacker trying to control city assets.**

Tim Medin *SANS Certified Instructor*

Tim Medin is a senior technical analyst at Counter Hack, a company devoted to the development of information security challenges for education, evaluation, and competition. Through the course of his career, Tim has performed penetration tests on a wide range of organizations and technologies. Prior to Counter Hack, Tim was a senior security consultant for FishNet Security, where most of his focus was on penetration testing. He gained information security experience in a variety of industries including previous positions in control systems, higher education, financial services, and manufacturing. Tim regularly contributes to the SANS Penetration Testing Blog (pen-testing.sans.org/blog) and the Command Line Kung Fu Blog (blog.commandlinekungfu.com). He is also project lead for the Laudanum Project, a collection of injectable scripts designed to be used in penetration testing. @timmedin

SEC617:

Wireless Ethical Hacking, Penetration Testing, and Defenses

SANS

Six-Day Program
Mon, Mar 27 - Sat, Apr 1
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: James Leyte-Vidal

www.giac.org/gawn

www.sans.edu

www.sans.org/cyber-guardian

"The detailed cryptographic explanations made it easier to understand how various encryption algorithms work."
-Jonathan Wilhoit, Fluor

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 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.

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 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 their 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 defensive 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.**

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**.

"SEC617 is an excellent course to prepare you for wireless lecturing space."
-Gary P., Department of National Defense

James Leyte-Vidal *Instructor*

James Leyte-Vidal is a team lead in a Fortune 100 company, currently focused on remediation efforts and control monitoring. In his 12 years in information security, James has performed various infosec functions including penetration testing, security assessments, remediation, vulnerability management, security program development and management, and incident response. Prior to his work in security, James worked several years as a Windows sysadmin and in a application support role. James has spoken publicly and taught for over 20 years, in college classrooms as well as functions within his own company and elsewhere. James holds the GCIH, GPEN, GWAPT, GAWN, GXPN, GCIA, GCFA, GMOB, GSEC, CISSP, MCSE, and CISA certifications as well as degrees in IT and Psychology. When not teaching or helping to secure his own company, James can usually be found running or taking something apart. @jamesleytevidal

SEC642:

Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques

NEW

Six-Day Program
Mon, Mar 27 - Sat, Apr 1
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
36 CPEs
Laptop Required
Instructor:
Adrien de Beaupre

"This course is outstanding! I would highly recommend it to pen testers who already have a good grasp on SEC542's content."
-Mark Geeslin, Citrix

"It's the perfect course for someone who has a background in web app pen test but wants to really gain advanced skills."
-Matthew Sullivan, Webfilings

Can Your Web Apps Withstand the Onslaught of Modern Advanced Attack Techniques?

Modern web applications are growing more sophisticated and complex as they utilize exciting new technologies and support ever-more critical operations. **Long gone are the days of basic HTML requests and responses.** Even in the age of Web 2.0 and AJAX, the complexity of HTTP and modern web applications is progressing at breathtaking speed. With the demands of highly available web clusters and cloud deployments, web applications are looking to deliver more functionality in smaller packets, with a decreased strain on backend infrastructure. Welcome to an era that includes tricked-out cryptography, **WebSockets**, **HTTP/2**, and a whole lot more. Are your web application assessment and penetration testing skills ready to evaluate these impressive new technologies and make them more secure?

Who Should Attend

- Web penetration testers
- Red team members
- Vulnerability assessment personnel
- Network penetration testers
- Security consultants
- Developers
- QA testers
- System administrators
- IT managers
- System architects

Are You Ready to Put Your Web Apps to the Test with Cutting-Edge Skills?

This pen testing course is designed to teach you the **advanced skills and techniques** required to test modern web applications and next-generation technologies. The course uses a combination of lecture, real-world experiences, and **hands-on exercises** to teach you the techniques to test the security of tried-and-true internal enterprise web technologies, as well as cutting-edge Internet-facing applications. The final course day culminates in a Capture-the-Flag competition where you will apply the knowledge you acquired during the previous five days in a fun environment based on real-world technologies.

Hands-on Learning of Advanced Web App Exploitation Skills

We begin by exploring advanced techniques and attacks to which all modern-day complex applications may be vulnerable. We'll learn about new web frameworks and web backends, then explore encryption as it relates to web applications, digging deep into practical **cryptography** used by the web, including techniques to identify the type of **encryption** in use within the application and methods for **exploiting** or abusing it. We'll look at alternative front ends to web applications and web services such as mobile applications, and examine new protocols such as HTTP/2 and WebSockets. **The final portion of class will focus on how to identify and bypass web application firewalls, filtering, and other protection techniques.**

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, Mar 27 - Sat, Apr 1
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Stephen Sims

www.giac.org/gxpn

SANS Technology Institute

www.sans.edu

www.sans.org/cyber-guardian

Bundle OnDemand
with this course
www.sans.org/ondemand

"SEC660 is a great course, although very challenging and I feel completely out of my depth, and I loved it."
-Daniel Stewart, Dell SecureWorks

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!

"SEC660 has been nothing less than excellent. Both the instructor and assistant are subject-matter experts who have extensive knowledge covering all aspects of the topics covered and then some." -Brian Anderson, Northrop Grumman Corporation

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 provides 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.

"No frills and goes right to the point. The first day alone is what other classes spend a full week on." -Michael Isbitski, Verizon Wireless

Who Should Attend

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

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 a master's of science degree in information assurance from Norwich University. 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

Earn up to 6 CPEs for certification renewal upon completion of Core NetWars

CORE NETWARS

Three Nights of Core NetWars

MAR 27, 28 & 30 | 6:30-9:30 PM | HOSTED BY TIM MEDIN

with Coin-A-Palooza,
your chance to earn up to five SANS Pen Test Challenge Coins

AND

CYBERCITY

One Night of NetWars CyberCity

MAR 31 | 6:30-9:30 PM | HOSTED BY TIM MEDIN

AT

SANS Pen Test Austin 2017!

Come and join us for these exciting events 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 2017.

External participants are welcome to join for an entry fee of $1,520 (Core NetWars) or $695 (CyberCity).

www.sans.org/pentest

COIN-A-PALOOZA

Earn Up To

5

SANS Pen Test Challenge Coins!

Each SANS pen test course offers a challenge coin for winners of the Day 6 Capture-the-Flag event. There are 11 unique coins available, each with a special cipher on the coin itself. For those who have taken a given SANS course, but have not won the Capture-the-Flag challenge coin, Coin-a-palooza offers the ability to catch up by participating in the three nights of NetWars challenges. You'll have an opportunity to earn up to five challenge coins for your collection and extra bragging rights. Good luck!

Enhance Your Training Experience

Add an

OnDemand Bundle & GIAC Certification Attempt*

to your course within seven days of this event for just $689 each.

SPECIAL PRICING

Extend Your Training Experience with an 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.

Get Certified with GIAC Certifications

GIAC CERTIFICATIONS

- Distinguish yourself as an information security leader
- 30+ GIAC cybersecurity certifications available
- 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 www.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 www.sans.org/community
Live Training in Your Local Region with Smaller Class Sizes

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

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

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

ONLINE TRAINING

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

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

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

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

FUTURE SANS TRAINING EVENTS

Las Vegas 2017
Las Vegas, NV | Jan 23-30

Cyber Threat Intelligence
SUMMIT & TRAINING 2017
Arlington, VA | Jan 25 - Feb 1

SOUTHERN CALIFORNIA
Anaheim 2017
Anaheim, CA | Feb 6-11

Scottsdale 2017
Scottsdale, AZ | Feb 20-25

Dallas 2017
Dallas, TX | Feb 27 - Mar 4

San Jose 2017
San Jose, CA | Mar 6-11

Tysons Corner Spring 2017
McLean, VA | Mar 20-25

ICS Security
SUMMIT & TRAINING 2017
Orlando, FL | Mar 20-27

SANS 2017
Orlando, FL | Apr 7-14

Threat Hunting and IR
SUMMIT & TRAINING 2017
Orlando, FL | Apr 18-25

Baltimore Spring 2017
Baltimore, MD | Apr 24-29

Automotive Cybersecurity
SUMMIT & TRAINING 2017
Detroit, MI | May 1-8

Security West 2017
San Diego, CA | May 9-18

NORTHERN VIRGINIA **Reston** 2017
Reston, VA | May 21-26

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

SANS PEN TEST AUSTIN 2017

Hotel Information

Training Campus
Sheraton Austin Hotel at the Capitol

701 East 11th Street
Austin, TX 78701 | 512-478-1111
www.sans.org/event/pentest2017/location

This Austin hotel is situated within easy walking distance of the state capitol, Erwin Center, 6th Street, and the University of Texas campus, offering musical, cultural, and entertainment experiences.

Special Hotel Rates Available

A special discounted rate of $217.00 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. This rate is only available through March 3, 2017.

Top 5 reasons to stay at the Sheraton Austin Hotel at the Capitol

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 Sheraton Austin Hotel at the Capitol 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 Sheraton Austin Hotel at the Capitol that you won't want to miss!
5. Everything is in one convenient location!

SANS PEN TEST AUSTIN 2017

Registration Information

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

Register online at www.sans.org/pentest

Select your course 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 **EarlyBird17** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**2-1-17**	**$400.00**	**2-22-17**	**$200.00**

Some restrictions apply.

SANS SIMULCAST

To register for a SANS Pen Test Austin 2017 Simulcast course, please visit www.sans.org/event/pentest2017/attend-remotely

SANS Voucher Program

Expand your training budget!

Extend your fiscal year. The SANS Voucher Program provides flexibility and may earn you bonus funds for training.

www.sans.org/vouchers

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 8, 2017 – processing fees may apply.

Open a **SANS 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 FAQs
- Tip of the Day
- Security Posters
- Thought Leaders
- 20 Coolest Careers
- Security Glossary
- SCORE (Security Consensus Operational Readiness Evaluation)

www.sans.org/account