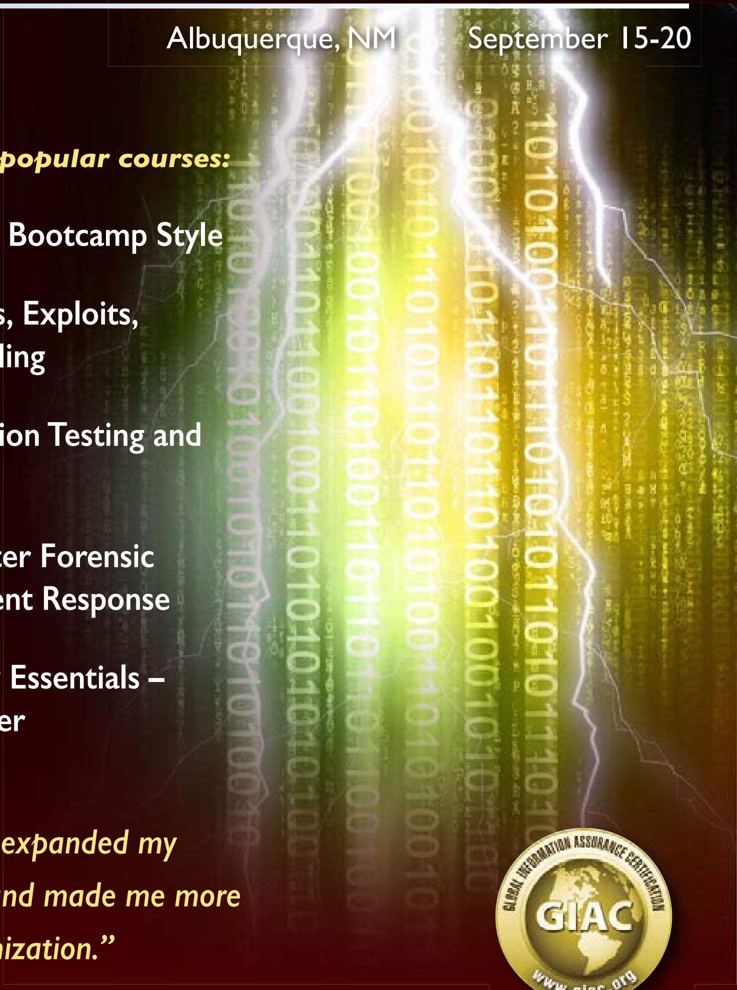
THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS

Albuquerque 2014

Albuquerque, NM September 15-20



Choose from these popular courses:

- Security Essentials Bootcamp Style
- Hacker Techniques, Exploits, and Incident Handling
- Network Penetration Testing and Ethical Hacking
- Advanced Computer Forensic Analysis and Incident Response
- Advanced Security Essentials – Enterprise Defender

"SANS courses have expanded my security knowledge and made me more valuable to my organization."

-Lance Grover, Consolidated Graphic

GLOBAL INFORMATION ASSURANCE CERTIFICATION GIAC www.giac.org

GIAC Approved Training

Register at

www.sans.org/event/albuquerque-2014

Save $400

by registering early!

See page 13 for more details.

SANS is bringing a new event to **Albuquerque in September** with courses in IT security, network pen testing, forensic analysis, and incident handling. This brochure will provide a complete course schedule, course descriptions, instructor bios, and information about earning your master's degree through the **SANS Technology Institute** (STI). Plus, don't miss our relevant evening talks including a keynote presentation and important topics regarding today's security concerns. These bonus sessions are open to all paid attendees at no additional cost.

All five of our courses offered at SANS Albuquerque have associated **GIAC** certifications, and four certifications align with **DoDD 8570**. GIAC tests and validates the ability of practitioners in information security, forensics, and software security. GIAC certification holders are recognized as experts in the IT industry and are sought after globally by government, military and industry to protect the cyber environment. Earn a master's degree or post baccalaureate certificate program at the **SANS Technology Institute**, the only accredited graduate institution focused solely on cybersecurity. For more information, see our STI page and visit the website at **www.sans.edu**.

All of our instructors for SANS Albuquerque 2014 are industry leaders who have proven they understand the challenges you face on a daily basis. Their real-world experience increases the practical value of the course material, and they will ensure that you not only learn the material but that you can use it the day you return to the office.

Albuquerque has scenic beauty, abundant cacti, generous sunshine, and a rich history, plus offers plenty of evening activities to give your brain a rest! Make your travel plans to attend SANS Albuquerque, now!

Our host hotel, **Albuquerque Marriott**, has a special discounted room rate of $119.00 S/D and will be honored based on space availability. Government per diem rooms are available with proper ID. This rate includes high-speed Internet in your room and is only available through August 30, see page (13) for details on how to get the best savings. The Albuquerque Marriott is located in the heart of the restaurant and shopping district, and just minutes from the Albuquerque Sunport, Historic Old Town, and the Sandia Peak Tram.

Register and pay for any of the 6-day courses by July 30 to save $400 on tuition fees! Get the training you need while enjoying this great city! Come see for yourself why SANS is the leading organization in computer security training.

SANS

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

"This is my first SANS experience and it has been a positive one. I'm looking forward to more."
-Stephen Ellis, CB&I

"Easily the most beneficial training I've ever attended."
-Josh Howard, City Bank

"Course material was done very well and accommodated all skill levels."
-Ryan Lougheed, Covidien

SC MAGAZINE AWARDS 2014 WINNER
Honored in the U.S.

Courses-at-a-Glance

		MON 9/15	TUE 9/16	WED 9/17	THU 9/18	FRI 9/19	SAT 9/20
SEC401	**Security Essentials Bootcamp Style**	**Page 1**					
SEC501	**Advanced Security Essentials - Enterprise Defender**	**Page 2**					
SEC504	**Hacker Techniques, Exploits, and Incident Handling**	**Page 3**					
SEC560	**Network Penetration Testing and Ethical Hacking**	**Page 4**					
FOR508	**Adv. Computer Forensic Analysis & Incident Response**	**Page 5**					

@SANSInstitute *Join the conversation:* **#SANSABQ**

SECURITY 401

Security Essentials Bootcamp Style

Six-Day Program
Mon, Sept 15 - Sat, Sept 20
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPE/CMU Credits
Instructor: Paul A. Henry

- GIAC Cert: GSEC
- Masters Program
- Cyber Guardian
- DoDD 8570

It seems wherever you turn organizations are being broken into, and the fundamental question that everyone wants answered is: Why? Why is it that some organizations get broken into and others do not? Organizations are spending millions of dollars on security and are still compromised. The problem is they are doing good things but not the right things. Good things will lay a solid foundation, but the right things will stop your organization from being headline news in the *Wall Street Journal*. SEC401's focus is to teach individuals the essential skills, methods, tricks, tools and techniques needed to protect and secure an organization's critical information assets and business systems.

This course teaches you the right things that need to be done to keep an organization secure. The focus is not on theory but practical hands-on tools and methods that can be directly applied when a student goes back to work in order to prevent all levels of attacks, including the APT (advanced persistent threat). In addition to hands-on skills, we will teach you how to put all of the pieces together to build a security roadmap that can scale today and into the future. When you leave our training we promise that you will have the techniques that you can implement today and tomorrow to keep your organization at the cutting edge of cyber security. Most importantly, your organization will be secure because students will have the skill sets to use the tools to implement effective security.

Before your organization spends a dollar of its IT budget or allocates any resources or time to anything in the name of cyber security, three questions must be answered:

1. What is the risk?
2. Is it the highest priority risk?
3. Is it the most cost-effective way of reducing the risk?

Security is all about making sure you are focusing on the right areas of defense. By attending SEC401, you will learn the language and underlying theory of computer security. In addition, you will gain the essential, up-to-the-minute knowledge and skills required for effective security if you are given the responsibility for securing systems and/or organizations.

"SEC401 not only teaches the material and supplements with labs, it provides real-life practical applications and examples to further emphasizing relevance!"
-Sherry Yavetak, Wells Fargo

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8570

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 has helped me to revisit our projects and policies to see where we should enforce a re-evaluation on the policy standards."
-K. Kang, M.O.D.

Paul A. Henry *SANS Senior Instructor*

Paul Henry is a Senior Instructor with the SANS Institute and 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 (USA), and both government as well as telecommunications projects throughout Southeast Asia. @phenrycissp

SECURITY 501

Advanced Security Essentials – Enterprise Defender

Six-Day Program
Mon, Sept 15 - Sat, Sept 20
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Keith Palmgren

- GIAC Cert: GCED
- Masters Program
- DoDD 8570

SANS
sans.org

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

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

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

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

Who Should Attend

- Students who have taken Security Essentials and want a more advanced 500-level course similar to SEC401
- People who have foundational knowledge covered in SEC401, do not want to take a specialized 500-level course, and still want broad, advanced coverage of the core areas to protect their systems
- Anyone looking for detailed technical knowledge on how to protect against, detect, and react to the new threats that will continue to cause harm to an organization

GCED
www.giac.org

SANS Technology Institute — Knowledge for Peace
www.sans.edu

www.sans.org/8570

"Even for a network novice, it is extremely beneficial in understanding fundamentals of malware. SEC501 is an outstanding course for all levels."
-Dana Rucinski,
U.S. Cyber Command

"SEC501 has "refreshed" my hands-on experience, and familiarization with new software for router/switches emerging technologies."
-Deneen Farrell,
U.S. Cyber Command

Keith Palmgren *SANS Certified 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 & 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 MIS 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 a total of 17 training courses. Keith currently holds the CISSP, GSEC, CEH, Security+, Network+, A+, and CTT+ certifications. @kplamgren

SECURITY 504

Hacker Techniques, Exploits, and Incident Handling

Six-Day Program
Mon, Sept 15 - Sat, Sept 20
9:00am - 6:30pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits
Laptop Required
Instructor: Bryce Galbraith

- GIAC Cert: GCIH
- Masters Program
- Cyber Guardian
- DoDD 8570

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

If your organization has an Internet connection or one or two disgruntled employees (and whose doesn't!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth.

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

This challenging course is particularly well suited to individuals who lead or are a part of an incident handling team. Furthermore, general security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, detect, and respond to attacks.

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8570

"I learned a lot about policy I would never have thought to learn before."
-Zane Markel,
U.S. Naval Academy

"Bryce is an excellent instructor. His knowledge and delivery is exceptional."
-Chris Shipp, DM Petroleum Operations Company

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 provides 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

SANS
sans.org

SECURITY 560

Network Penetration Testing and Ethical Hacking

Six-Day Program
Mon, Sept 15 - Sat, Sept 20
9:00am - 6:30pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits
Laptop Required
Instructor: Adrien de Beaupre

- GIAC Cert: GPEN
- Masters Program
- Cyber Guardian

Pen Test Brochure Challenge

aHR0cDovL2JpdC5se
S8xbHA5MEx6Cg==

> **"SEC560 helped to take the stew of ideas and techniques in my head and organize them in a 'professionally' usable way."**
>
> -Richard Tafoya,
> Redflex Traffic Systems

> **"Learning all these tools is super valuable for security professionals or even system admins, they help understand how things work."**
>
> -Igor Guarisma

As a cyber security 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 duty head-on.

Who Should Attend

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

THE MUST-HAVE COURSE FOR EVERY WELL-ROUNDED SECURITY PROFESSIONAL

The whole course 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 awesome 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, learning about a target's infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures.You'll be equipped to scan target networks using best-of-breed tools from experience in our hands-on labs. 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, wireless, 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.

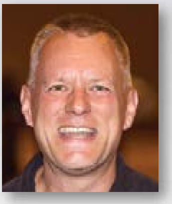
LEARN THE BEST WAYS TO TEST YOUR OWN SYSTEMS BEFORE THE BAD GUYS ATTACK

With comprehensive coverage of tools, techniques, and methodologies for network, web app, and wireless testing, SEC560 truly prepares you to conduct high-value penetration testing projects end-to-end, step-by-step. Every organization needs skilled infosec personnel who can find vulnerabilities and mitigate their impacts, and this whole course is specially designed to get you ready for that role. With over 30 detailed hands-on labs through- out, 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 masterfully, safely, and efficiently.

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian



Adrien de Beaupre *SANS Certified Instructor*

Adrien de Beaupre is a senior Information Security Consultant with Intru-Shun.ca Inc., experienced in penetration testing and incident response. Mr. de Beaupre holds the ISC2 CISSP, GXPN (GIAC Exploit Researcher and Advanced Penetration Tester), GWAPT (GIAC Web Application Penetration Tester), GPEN (GIAC Penetration Tester), GCIH (GIAC Certified Incident Handler), GSEC (GIAC Security Essentials), OPST (OSSTMM Professional Security Tester), and OPSA (OSSTMM Professional Security Analyst) certifications. As a volunteer member of the SANS Internet Storm Center (isc.sans.edu) he performs incident handling and threat analysis duties. When not geeking out he can be found with his family, or at the dojo. @adriendb

FORENSICS 508

Advanced Computer Forensic Analysis and Incident Response

SANS
sans.org

Six-Day Program
Mon, Sept 15 - Sat, Sept 20
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Alissa Torres

- GIAC Cert: GCFA
- Masters Program
- Cyber Guardian
- DoDD 8570

This course focuses on providing incident responders with the necessary skills to hunt down and counter a wide range of threats within enterprise networks, including economic espionage, hactivism, and financial crime syndicates. The completely updated FOR508 addresses today's incidents by providing real-life, hands-on response tactics.

DAY 0: A 3-letter government agency contacts you to say that critical information was stolen from a targeted attack on your organization. Don't ask how they know, but they tell you that there are several breached systems within your enterprise. You are compromised by an Advanced Persistent Threat, aka an APT – the most sophisticated threat you are likely to face in your efforts to defend your systems and data.

Over 90% of all breach victims learn of a compromise from third party notification, not from internal security teams. In most cases, adversaries have been rummaging through your network undetected for months or even years. Gather your team—it's time to go hunting.

FOR508 will help you determine:

- **How did the breach occur?**
- **What systems were compromised?**
- **What did they take? What did they change?**
- **How do we remediate the incident?**

This course trains digital forensic analysts and incident response teams to identify, contain, and remediate sophisticated threats—including APT groups and financial crime syndicates. A hands-on lab—developed from a real-world targeted attack on an enterprise network—leads you through the challenges and solutions. You will identify where the initial targeted attack occurred and which systems an APT group compromised. The course will prepare you to find out which data were stolen and by whom, contain the threat, and provide your organization the capabilities to manage and counter the attack.

During a targeted attack, an organization needs the best incident responders and forensic analysts in the field. FOR508 will train you and your team to be ready to do this work.

> **"I've taken other network intrusion classes but nothing this in depth. FOR508 is outstanding!"**
>
> -Craig Goldsmith, OCRCFL

Who Should Attend

- Information security professionals
- Incident response team members
- Experienced digital forensic analysts
- Federal agents and law enforcement
- Red team members, penetration testers, and exploit developers
- SANS FOR408 and SEC504 graduates

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

What you will receive with this course

- SIFT Workstation Virtual Machine
- F-Response TACTICAL Edition with a 2 year license
- Best-selling book "File System Forensic Analysis" by Brian Carrier
- Course DVD loaded with case examples, additional tools, and documentation

> **"FOR508 is definitely a deep dive into forensics. You'll come away with a lot of knowledge and a lot of topics to continue to study."**
>
> -Jeff Stiles, Aeris Secure

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8570

Alissa Torres *SANS Certified Instructor*

Alissa Torres is a certified SANS instructor, specializing in advanced computer forensics and incident response. Her industry experience includes serving in the trenches as part of the Mandiant Computer Incident Response Team (MCIRT) as an incident handler and working on an internal security team as a digital forensic investigator. She has extensive experience in information security, spanning government, academic and corporate environments and holds a Bachelors degree from the University of Virginia and a Masters from the University of Maryland in Information Technology. Alissa has taught at the Defense Cyber Investigations Training Academy (DCITA), delivering incident response and network basics to security professionals entering the forensics community. She has presented at various industry conferences and B-Sides events. In addition to being a GIAC Certified Forensic Analyst (GCFA), she holds the GCFE, GPEN, CISSP, EnCE, CFCE, MCT, and CTT+ certifications. @sibertor

ALBUQUERQUE BONUS SESSIONS

SANS@Night Evening Talks

Enrich your SANS training experience! Evening talks given by our instructors and selected subject matter experts help you broaden your knowledge, hear from the voices that matter in computer security, and get the most for your training dollar.

KEYNOTE: Evolving Threats *Paul A. Henry*

For nearly two decades defenders have fallen into the "Crowd Mentality Trap" and have simply settled on doing the same thing everyone else was doing. While at the same time attackers have clearly evolved both in terms of malware delivery vectors and attack methodology. Today our defenses focus primarily on the gateway and upon attempting to outwit attacker's delivery methods. This leaves us woefully exposed and according to a recent Data Breach Report has resulted in 3,765 incidents, 806 million records exposed, and $157 billion (USD) in data breach costs in only the past 6 years.

The 13 Absolute Truths of Security *Keith Palmgren*

Keith Palmgren has identified thirteen "Absolute Truths" of security - things that remain true regardless of circumstance, network topology, organizational type, or any other variable. Recognizing these thirteen absolute truths and how they affect a security program can lead to the success of that program. Failing to recognize these truths will spell almost certain doom. Here we will take a non-technical look at each of the thirteen absolute truths in turn, examine what they mean to the security manager, what they mean to the security posture, and how understanding them will lead to a successful security program.

Extracting User Credentials using Memory Forensics *Alissa Torres*

Though Windows credential extraction and password cracking are often categorized as offensive skills, used by pentesters and sophisticated attackers, digital forensic examiners and incident responders can also put these techniques to use to further their investigations. Just by parsing a physical memory image of a Windows system, local and domain user account password hashes can be pulled from the registry hives and plaintext credentials can be extracted from the wdigest in the lsass process for logged on users. For employee or criminal investigations, cracking a user's logon password can allow the examiner access to encrypted files or accounts due to frequent password re-use by users. Likewise, in intrusion cases, being able to dump credentials from a compromised system allows the IR team to assess what accesses the attacker was able to acquire, providing for better scoping of the intrusion. This webcast walks through several practical forensics use cases for Windows credential extraction from memory and includes excerpts from the SANS FOR526: Memory Forensics In-Depth class.

Debunking the Complex Password Myth *Keith Palmgren*

Perhaps the worst advice you can give a user is "choose a complex password". The result is the impossible-to-remember password requiring the infamous sticky note on the monitor. In addition, that password gets used at a dozen sites at home, AND the very same password gets used at work. The final result ends up being the devastating password compromise. In this one-hour talk, we will look at the technical and non-technical (human nature) issues behind passwords. Attendees will gain a more complete understanding of passwords and receive solid advice on creating more easily remembered AND significantly stronger passwords at work and at home, for their users, for themselves and even for their children.

Bust a Cap in a Web App with ZAP *Adrien de Beaupre*

The Zed Attack Proxy (ZAP) is the Open Web Application Security Project's (OWASP) flagship testing tool. This presentation will describe the why and how of attacking your own web-based applications with ZAP. The presentation will include a walk-through of the web application testing methodology where ZAP is used as the attack tool.

MAKE YOUR NEXT MOVE COUNT

Earn a Respected Graduate Degree

"It's great to learn from an organization at the forefront of both academics, and in the field."

-Joseph Faust,
MSISE Program

Master's Degree Programs:

▸ M.S. in Information Security Engineering

▸ M.S. in Information Security Management

Specialized Graduate Certificates:

▸ Penetration Testing & Ethical Hacking

▸ Incident Response

▸ Cybersecurity Engineering (Core)

Top Reasons Students Choose SANS Graduate Programs:

- World-class, cutting-edge technical courses that refine and specialize your skills
- Teaching faculty with an unparalleled reputation for industry leadership and who bring the material to life
- Simulation and group projects that teach students to write, present, and persuade effectively
- Validation from multiple GIAC certifications even before you earn your degree
- Flexibility to attend courses when and where you need them, either live in classrooms or online from home or work
- A reputation that helps accelerate career growth—employers will recognize and respect a master's degree from SANS

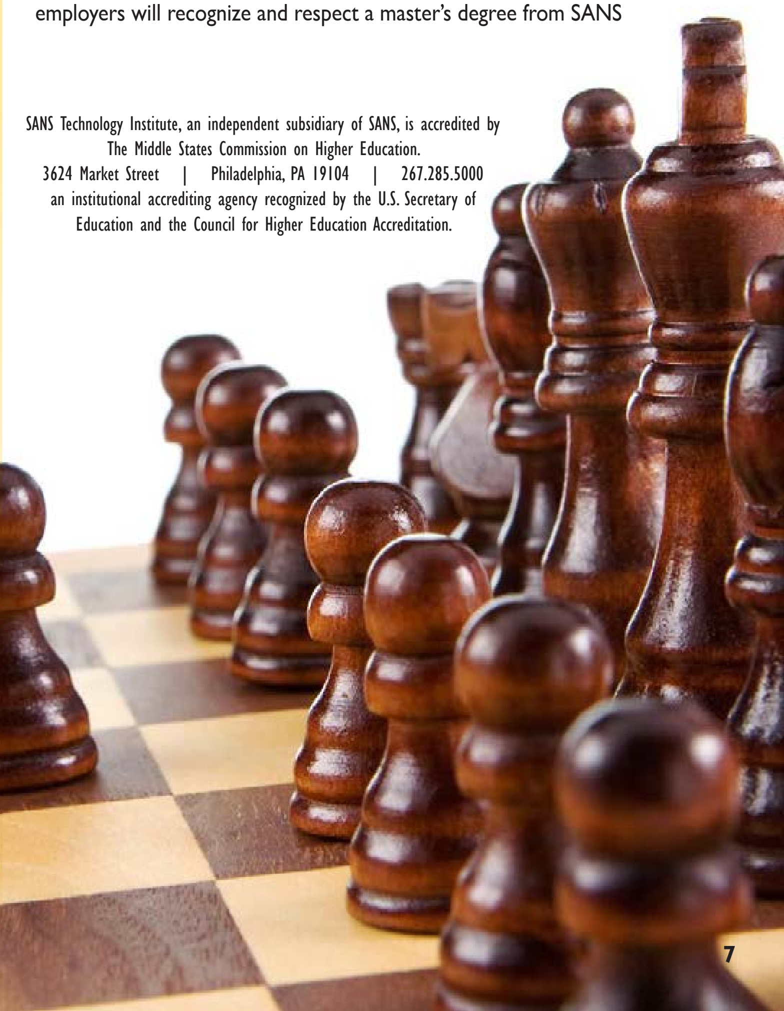
SANS Technology Institute, an independent subsidiary of SANS, is accredited by The Middle States Commission on Higher Education.
3624 Market Street | Philadelphia, PA 19104 | 267.285.5000
an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

SANS TECHNOLOGY INSTITUTE
KNOWLEDGE FOR PEACE
SCIENTIA PRO PACE

Learn more at

www.sans.edu

info@sans.edu



How Are You Protecting Your

- Data?
- Network?
- Systems?
- Critical Infrastructure?

Risk management is a top priority. The security of these assets depends on the skills and knowledge of your security team. Don't take chances with a one-size fits all security certification. **Get GIAC certified!**

GIAC offers over 27 specialized certifications in security, forensics, penetration testing, web application security, IT audit, management, and IT security law.

"GIAC is the only certification that proves you have hands-on technical skills."
-Christina Ford, Department of Commerce

"GIAC Certification demonstrates an applied knowledge versus studying a book."
-Alan C, USMC

Learn more
about GIAC
and how to
Get Certified at
www.giac.org

GLOBAL INFORMATION ASSURANCE CERTIFICATION
GIAC
www.giac.org

Department of Defense Directive 8570

(DoDD 8570)

www.sans.org/8570

Department of Defense Directive 8570 (DoDD 8570) provides guidance and procedures for the training, certification, and management of all government employees who conduct information assurance functions in assigned duty positions. These individuals are required to carry an approved certification for their particular job classification. GIAC provides the most options in the industry for meeting 8570 requirements.

DoD Baseline IA Certifications

IAT Level I	IAT Level II	IAT Level III	IAM Level I	IAM Level II	IAM Level III
A+CE	**GSEC**	**GCED**	**GSLC**	**GSLC**	**GSLC**
Network+CE	Security+CE	**GCIH**	CAP	**CISSP**	**CISSP**
SSCP	SSCP	**CISSP**	Security+CE	(or Associate)	(or Associate)
		(or Associate)		CAP, CASP	CISM
		CISA		CISM	

Computer Network Defense (CND) Certifications

CND Analyst	CND Infrastructure Support	CND Incident Responder	CND Auditor	CND Service Provider Manager
GCIA	SSCP	**GCIH**	**GSNA**	CISSP - ISSMP
GCIH	CEH	**GCFA**	CISA	CISM
CEH		CSIH, CEH	CEH	

Information Assurance System Architecture & Engineering (IASAE) Certifications

IASAE I	IASAE II	IASAE III
CISSP	**CISSP**	CISSP - ISSEP
(or Associate)	(or Associate)	CISSP - ISSAP
	CASP	

Computer Environment (CE) Certifications

GCWN	**GCUX**

Compliance/Recertification:

To stay compliant with DoDD 8570 requirements, you must maintain your certifications. GIAC certifications are renewable every four years.

Go to www.giac.org to learn more about certification renewal.

SANS TRAINING COURSE	DoDD APPROVED CERT
SEC401	GSEC
SEC501	GCED
SEC503	GCIA
SEC504	GCIH
AUD507	GSNA
FOR508	GCFA
MGT414	CISSP
MGT512	GSLC

DoDD 8570 certification requirements are subject to change, please visit http://iase.disa.mil/eta/iawip for the most updated version.

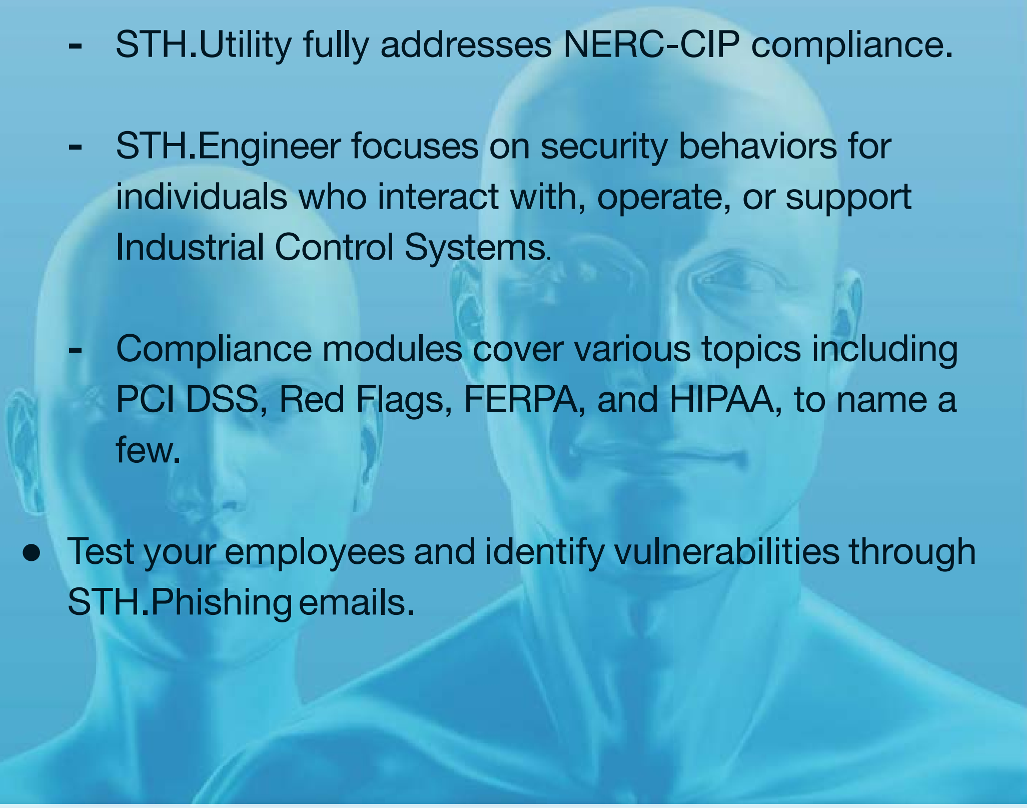
For more information, contact us at 8570@sans.org or visit www.sans.org/8570

SECURING THE HUMAN

SECURITY AWARENESS FOR THE 21ST CENTURY

End User - Utility - Engineer - Developer - Phishing

- Go beyond compliance and focus on changing behaviors.
- Create your own training program by choosing from a variety of modules:
  - STH.End User is mapped against the Critical Security Controls.
  - STH.Developer uses the OWASP Top 10 web vulnerabilities as a framework.
  - STH.Utility fully addresses NERC-CIP compliance.
  - STH.Engineer focuses on security behaviors for individuals who interact with, operate, or support Industrial Control Systems.
  - Compliance modules cover various topics including PCI DSS, Red Flags, FERPA, and HIPAA, to name a few.
- Test your employees and identify vulnerabilities through STH.Phishing emails.



SANS SECURING THE HUMAN

For a free trial visit us at:
www.securingthehuman.org

FUTURE SANS TRAINING EVENTS

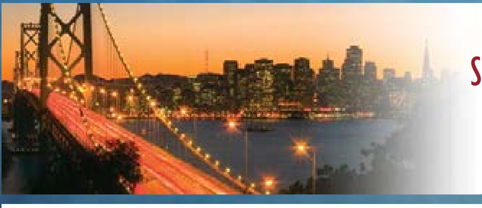
Information on all events can be found at www.sans.org/security-training/by-location/all

SANSFIRE 2014

Baltimore, MD | June 21-30

SANS Capital City 2014

Washington, DC | July 7-12



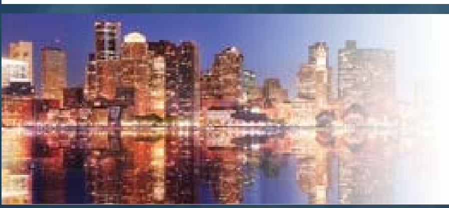
SANS San Francisco 2014

San Francisco, CA | July 14-19

SANS Industrial Control Systems

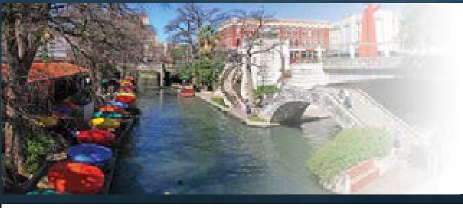
ICS Security TRAINING 2014 - HOUSTON

Houston, TX | July 21-25



SANS Boston 2014

Boston, MA | July 28 - August 2



SANS San Antonio 2014

San Antonio, TX | August 11-16

SANS Cyber Defense SUMMIT

Nashville, TN | August 13-20

SANS Virginia Beach 2014

Virginia Beach, VA | August 18-29

SANS Crystal City 2014

Crystal City, VA | September 8-13

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

Multi-Course Training Events

Live Instruction from SANS' Top Faculty, Vendor Showcase, Bonus Evening Sessions, and Networking with Your Peers

www.sans.org/security-training/by-location/all

Community SANS

Live Training in Your Local Region with Smaller Class Sizes

www.sans.org/community

OnSite

Live Training at Your Office Location

www.sans.org/onsite

Mentor

Live Multi-Week Training with a Mentor

www.sans.org/mentor

Summit

Live IT Security Summits and Training

www.sans.org/summit

ONLINE TRAINING

OnDemand

E-learning Available Anytime, Anywhere, at Your Own Pace

www.sans.org/ondemand

vLive

Online, Evening Courses with SANS' Top Instructors

www.sans.org/vlive

Simulcast

Attend a SANS Training Event without Leaving Home

www.sans.org/simulcast

OnDemand Bundles

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

SANS ALBUQUERQUE 2014

Hotel Information

Training Campus
Albuquerque Marriott

2101 Louisiana Boulevard NE
Albuquerque, NM 87110
www.sans.org/event/albuquerque-2014/location

The Albuquerque Marriott is conveniently located in the heart of the restaurant and shopping district, overlooking the Sandia Mountains. Enjoy spectacular views of the city and our beautiful desert from the comfort of your room. You're only steps away from shopping, movie theatres, restaurants and minutes from the Albuquerque Sunport, Historic Old Town and the Sandia Peak Tram.

Special Hotel Rates Available

A special discounted rate of $119.00 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 August 30, 2014.

Top 5 reasons to stay at the Albuquerque Marriott

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 Albuquerque Marriott, 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 Albuquerque Marriott that you won't want to miss!

5 Everything is in one convenient location!

SANS ALBUQUERQUE 2014

Registration Information

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

Register online at www.sans.org/event/albuquerque-2014/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.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	**7/30/14**	**$400.00**	**8/13/14**	**$250.00**

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 www.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 August 27, 2014 – 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. **www.sans.org/vouchers**