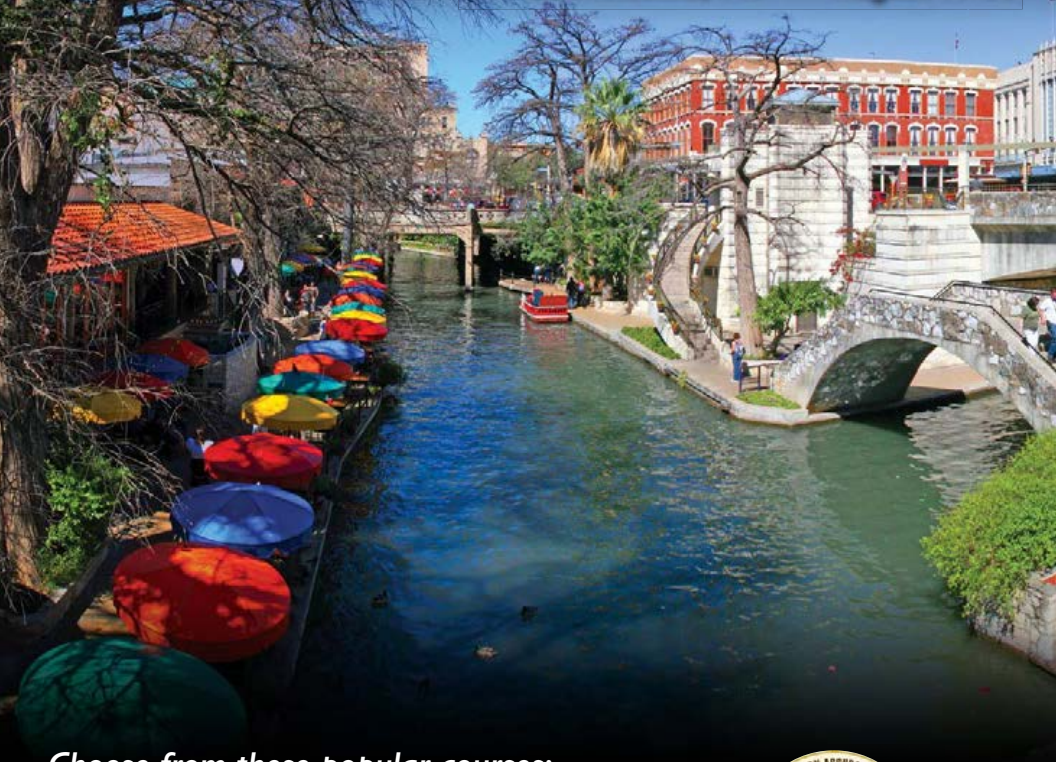
THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

# SANS San Antonio 2014

San Antonio, TX August 11-16



*Choose from these popular courses:*

**Security Essentials Bootcamp Style**

**Hacker Techniques, Exploits, and Incident Handling**

**Intrusion Detection In-Depth**

**SANS Security Leadership Essentials For Managers with Knowledge Compression™**

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

**Memory Forensics In-Depth**

GIAC Approved Training

*"Whether you are new to security or a seasoned professional, you will always learn something at SANS."*

-Gordon Steuart, OPS Consultant

**Register at www.sans.org/event/san-antonio-2014**

**Save $400** by registering early!

See page 13 for more details.

This year **SANS San Antonio 2014** will be held **August 11-16**, at the Westin Riverwalk. We are featuring some of our most popular courses (SEC401, SEC503, SEC504, MGT414, MGT512, and FOR526). Mastery of the skills and techniques taught in the aforementioned courses will advance your security career (SEC401), provide what you need to specialize as an intrusion detection analyst (SEC503), add to your understanding of attackers' tactics and strategies (SEC504), and prepare you for CISSP certification (MGT414). Additionally, we are offering **Security Leadership Essentials for Managers with Knowledge Compression™** (MGT512) and **Memory Forensics** (FOR526).

The hallmark of our success is the comprehensive, intensive hands-on training that we provide, delivered by the most advanced and experienced instructors in the industry. In the classroom, the knowledge, skills, and techniques you will learn will be enhanced by the instructors' real-world experiences and lab exercises. Our instructors will ensure that you not only learn the material but that you can apply it immediately upon returning to your office.

Five of our courses at San Antonio 2014 are aligned with the **DoD Directive 8570**. We encourage you to visit the **GIAC** page and register for your certification attempt today. Are you interested in a Master's Degree? You can also take courses towards a master's degree at **SANS Technology Institute (STI)** – Information Security Management (MSISM) or Engineering (MSISE). SANS Technology Institute is the only accredited graduate institution focused solely on cybersecurity. For more information see our STI page and apply today!

SANS San Antonio 2014 is at the **Westin Riverwalk**, and a special discounted rate of $189.00 S/D will be honored based on space availability through July 9th. The hotel is located on the Paseo del Rio, better known as the Riverwalk, which means it is within walking distance of many attractions such as the Alamo mission, La Villita historic arts village, and Market Square, a three-block outdoor plaza lined with restaurants, shops, and produce stands that is one of America's top-ten outdoor markets according to Frommer's.

**Register and pay by June 18 to save $400 on tuition fees.** Start making your training and travel plans now; let your colleagues and friends know about SANS San Antonio 2014. We look forward to seeing you there.

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

**"Excellent presentation- Taking a difficult subject and summing it up quite nicely."**
-Jason Khoury, Marriott

**"Tons of information presented, but the instructor steps through the information in a methodical logical manner."**
-Daniel Byrnside, SC Army National Guard

**"Great use of "real-world" examples to explain course content."**
-Ottis Nelson, U.S. Navy

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

## Courses-at-a-Glance

| | | MON 8/11 | TUE 8/12 | WED 8/13 | THU 8/14 | FRI 8/15 | SAT 8/16 |
|---|---|---|---|---|---|---|---|
| SEC401 | Security Essentials Bootcamp Style | Page 1 | | | | | |
| SEC503 | Intrusion Detection In-Depth | Page 2 | | | | | |
| SEC504 | Hacker Techniques, Exploits, and Incident Handling | Page 3 | | | | | |
| MGT414 | SANS® +S™ Training Program for the CISSP® Cert Exam | Page 4 | | | | | |
| MGT512 | SANS Security Leadership Essentials For Managers with Knowledge Compression™ | Page 5 | | | | | |
| FOR526 | Memory Forensics In-Depth | Page 6 | | | | | |

@SANSInstitute *Join the conversation:* #SANSSanAntonio

SECURITY 401

# Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Aug 11 - Sat, Aug 16
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPE/CMU Credits
Instructor: Keith Palmgren

- 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.

## 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

**"Extremely useful material and I am now fired up to take follow-up courses."**
-Rehan Mahmoud, Google

**"Having fun while learning infosec, it doesn't get much better than that!"**
-Todd Lundit, Samaritan Health

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.

www.giac.org

www.sans.edu

www.sans.org/
cyber-guardian


www.sans.org/8570

*"SEC401 is a great place to start for a wide range of topics. It IS in-depth, and leaves you wanting more."*
-Todd Condit, Samaritan Health

## 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.

SECURITY 503

# Intrusion Detection In-Depth

SANS

Six-Day Program
Mon, Aug 11 - Sat, Aug 16
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor:
Dr. Johannes Ullrich

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

## Who Should Attend

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

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

This course spans a wide variety of topics from foundational material such as TCP/IP to detecting an intrusion, building in breadth and depth along the way. It's kind of like the "soup to nuts" or bits to bytes to packets to flow of traffic analysis.

Hands-on exercises supplement the course book material, allowing you to transfer the knowledge in your head to your keyboard using the Packetrix VMware distribution created by industry practitioner and SANS instructor Mike Poor. As the Packetrix name implies, the distribution contains many of the tricks of the trade to perform packet and traffic analysis. All exercises have two different approaches. A more basic one that assists you by giving hints for answering the questions. Students who feel that they would like more guidance can use this approach. The second approach provides no hints, permitting a student who may already know the material or who has quickly mastered new material a more challenging experience. Additionally, there is an "extra credit" stumper question for each exercise intended to challenge the most advanced student.

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

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8570

**"SEC503 is probably one of the most interesting training courses I have ever taken."**
-David Mirch, HP

**"Johannes has an excellent teaching approach and did a great job of fighting the brain overload later in the day."**
-Brad Meyers, Molina Healthcare

**Johannes Ullrich, Ph.D.** *SANS Senior Instructor*

Dr. Johannes Ullrich is the Dean of Research and a faculty member of the SANS Technology Institute. In November of 2000, Johannes started the DShield.org project, which he later integrated into the Internet Storm Center. His work with the Internet Storm Center has been widely recognized. In 2004, Network World named him one of the 50 most powerful people in the networking industry. Secure Computing Magazine named him in 2005 one of the Top 5 influential IT security thinkers. His research interests include IPv6, Network Traffic Analysis and Secure Software Development. Johannes is regularly invited to speak at conferences and has been interviewed by major publications, radio as well as TV stations. He is a member of the SANS Technology Institute's Faculty and Administration as well as Curriculum and Long Range Planning Committee. As chief research officer for the SANS Institute, Johannes is currently responsible for the GIAC Gold program. Prior to working for SANS, Johannes worked as a lead support engineer for a web development company and as a research physicist. Johannes holds a PhD in Physics from SUNY Albany and is located in Jacksonville, Florida. He also maintains a daily security news summary podcast and enjoys blogging about application security.

SECURITY 504

# Hacker Techniques, Exploits, and Incident Handling

SANS
sans.org

Six-Day Program
Mon, Aug 11 - Sat, Aug 16
9:00am - 6:30pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits
Laptop Required
Instructor: Dave Shackleford

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

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.

## 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

**"As a director of IT, SEC504 showed me what my security team should be doing."**
-Brian Bounds, Texas Biomedical Research Institute

**"SEC504 was a fantastic learning experience. So much information presented in a manner that was understandable."**
-Scotlyn Monk, Ingalls Information Security

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8570

**Dave Shackleford** *SANS Senior Instructor*

Dave Shackleford is the owner and principal consultant of Voodoo Security and a SANS analyst, senior instructor, and course author. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering, and is a VMware vExpert with extensive experience designing and configuring secure virtualized infrastructures. He has previously worked as CSO for Configuresoft, CTO for the Center for Internet Security, and as a security architect, analyst, and manager for several Fortune 500 companies. Dave is the author of the Sybex book Virtualization Security: Protecting Virtualized Environments, as well as the coauthor of Hands-On Information Security from Course Technology. Recently Dave coauthored the first published course on virtualization security for the SANS Institute. Dave currently serves on the board of directors at the SANS Technology Institute and helps lead the Atlanta chapter of the Cloud Security Alliance.

MANAGEMENT 414

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

SANS sans.org

Six-Day Program
Mon, Aug 11 - Sat, Aug 16
9:00am - 7:00pm (Day 1)
8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6)
46 CPE/CMU Credits
Laptop NOT Needed
Instructor: Ted Demopoulos
- GIAC Cert: GISP
- DoDD 8570

**Take advantage of SANS CISSP® Get Certified Program currently being offered.**

www.sans.org/special/cissp-get-certified-program

**"Ted is awesome! He made the material easy to understand and had great real-world examples."**
-Jane Veal, Manulife

**"Ted was an excellent instructor. He was able to clearly explain all topics covered. His presentation skills were superb and was consistent over the entire day."**
-Mike Acheson, DN

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

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

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

## Who Should Attend

- Security professionals who are interested in understanding the concepts covered in the CISSP® exam as determined by (ISC)²
- Managers who want to understand the critical areas of network security
- System, security, and network administrators who want to understand the pragmatic applications of the CISSP® 10 Domains
- Security professionals and managers looking for practical ways the 10 domains of knowledge can be applied to the current job
- In short, if you desire a CISSP® or your job requires it, MGT414 is the training for you to get GISP certified

www.giac.org


www.sans.org/8570

## Obtaining your CISSP® certification consists of:

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

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

## Ted Demopoulos *SANS Certified Instructor*

Ted Demopoulos' first significant exposure to computers was in 1977 when he had unlimited access to his high school's PDP-11 and hacked at it incessantly. He consequently almost flunked out but learned he liked playing with computers a lot. His business pursuits began in college and have been continuous ever since. His background includes over 25 years of experience in information security and business, including 20+ years as an independent consultant. Ted helped start a successful information security company, was the CTO at a "textbook failure" of a software startup, and has advised several other businesses. Ted is a frequent speaker at conferences and other events, quoted often by the press, and maintains Security Certs, a Web site on Security Certifications. He also has written two books on Social Media, has an ongoing software concern in Austin, Texas in the virtualization space, and is the recipient of a Department of Defense Award of Excellence. Ted lives in New Hampshire and more about him is available at Demopoulos Associates. In his spare time, he is also a food and wine geek, enjoys flyfishing, and playing with his children.

MANAGEMENT 512

# SANS Security Leadership Essentials For Managers with Knowledge Compression™

SANS
sans.org

Five-Day Program
Mon, Aug 11 - Fri, Aug 15
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPE/CMU Credits
Laptop NOT Needed
Instructor: G. Mark Hardy
- GIAC Cert: GSLC
- Masters Program
- DoDD 8570

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

## Who Should Attend

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

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

**"MGT512 encompasses topics in all security areas. This was my first SANS experience and I greatly enjoyed it. I will certainly advocate to my superiors the value I have received."**
-Mark McCready,
Modern Woodmen of America

**"MGT512 course material and the instructor were top notch. SANS delivers a quality product every time."**
-Charles Brown III,
MCSF-Blount Island

## Knowledge Compression™

Knowledge Compression™ is an optional add-on feature to a SANS class which aims to maximize the absorption and long-term retention of large amounts of data over a relatively short period of time. Through the use of specialized training materials, in-class reviews, examinations and test-taking instruction, Knowledge Compression™ ensures students have a solid understanding of the information presented to them. By attending classes that feature this advanced training product, you will experience some of the most intense and rewarding training programs SANS has to offer, in ways that you never thought possible!

www.giac.org

www.sans.edu

www.sans.org/8570

## G. Mark Hardy *SANS Certified Instructor*

G. Mark Hardy is founder and President of National Security Corporation. He has been providing cyber security expertise to government, military, and commercial clients for over 30 years, and is an internationally recognized expert who has spoken at over 250 events world-wide. G. Mark serves on the Advisory Board of CyberWATCH, an Information Assurance/Information Security Advanced Technology Education Center of the National Science Foundation. A retired U.S. Navy Captain, he was privileged to serve in command nine times, including responsibility for leadership training for 70,000 Sailors. He also served as wartime Director, Joint Operations Center for US Pacific Command, and Assistant Director of Technology and Information Management for Naval Logistics in the Pentagon, with responsibility for INFOSEC, Public Key Infrastructure, and Internet security. Captain Hardy was awarded the Defense Superior Service Medal, the Legion of Merit, five Meritorious Service Medals, and 24 other medals and decorations. A graduate of Northwestern University, he holds a BS in Computer Science, a BA in Mathematics, a Masters in Business Administration, a Masters in Strategic Studies, and holds the GSLC, CISSP, CISM and CISA certifications.

FORENSICS 526

# Memory Forensics In-Depth

SANS

Six-Day Program
Mon, Aug 11 - Sat, Aug 16
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Jake Williams

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

**"All manuals should be written like those used in FOR526. Not only do you see the answers, but also know how you got there."**
-Barry Friedman, NY Police

**"FOR526 is a great deep dive into memory and an excellent tutorial to creating plugins for volatility."**
-Karel Nykles, CESNET

**"FOR526 helped me to expand my knowledge of host forensics."**
-Christopher Courchesne, ManTech Intl.

## *Malware Can Hide, But It Must Run*

Acquiring and analyzing physical memory is seen by Digital Forensics and Incident Response (DFIR) professionals as critical to the success of an investigation, whether it be a criminal case, employee policy violation, or enterprise intrusion. Investigators who are not looking at volatile memory are leaving evidence on the table. The valuable contents of RAM hold evidence of user actions as well as evil processes and furtive behaviors implemented by malicious code. It is this evidence that often proves to be the "smoking gun" that unravels the story of what happened on a system.

## Who Should Attend

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

Just as it is crucial to understand disk and registry structures in order to substantiate findings in traditional system forensics, it is equally critical to understand memory structures. Having in-depth knowledge of Windows memory internals allows the examiner to access target data specific to the needs of the current case. There is an arms race between analysts and attackers. Modern malware and post-exploitation modules increasingly employ self-defense techniques that include more sophisticated rootkit and anti-memory analysis mechanisms that destroy or subvert volatile data. Examiners must have a deeper understanding of memory internals in order to discern the intentions of attackers or rogue trusted insiders. This course takes the DFIR professional through acquisition, validation, and memory analysis with hands-on, real-world, and malware-laden memory images. The course draws on best practices and recommendations from top experts in the DFIR field. The final section provides students with a direct memory forensics challenge that makes use of the SANS NetWars Tournament platform. These challenges strengthen the student's ability to respond to typical and atypical memory forensics challenges from all types of cases, from investigating the user to isolating the malware.

FOR526 provides the critical skills necessary for digital forensics examiners and incident responders to deftly analyze captured memory images and live response audits. By using the most effective freeware and open-source tools in the industry today and delivering a deeper understanding of how these tools work, this course shows DFIR professionals how to unravel the real story of what happened on a system. It is a critical course for any serious investigator who wants to tackle advanced forensics, trusted insider, and incident response cases.

**Remember:** "Malware can hide, but it must run." It is this malware paradox that is the key to understanding that while intruders are becoming more advanced with anti-forensic tactics and techniques, it is impossible for them to hide their footprints completely from a skilled incident responder performing memory analysis. FOR526 will ensure that you and your team are ready to respond to the challenges inherent in DFIR by using cutting-edge memory forensics tools and techniques.

## Jake Williams *SANS Certified Instructor*

Jake Williams is the chief scientist at CSRgroup computer security consultants and has more than a decade of experience in secure network design, penetration testing, incident response, forensics and malware reverse engineering. Before joining CSRgroup, he worked with various government agencies in information security roles. Jake is a two-time victor at the annual DC3 Digital Forensics Challenge.

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/san-antonio-2014/courses

# SAN ANTONIO 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: The Bot Inside the Machine *Dr. Johannes Ullrich*

Embedded systems are the new target. As our networks grow uncontrolled and unsupervised, forgotten machines will take over and rule us all soon. Analyzing the embedded malware that comes with this presents a number of challenges. Current debuggers and virtualization techniques that mimic these systems are incomplete and will not allow us to completely analyze malware the way we are used to in good old desktop malware environments. These malware blackboxes need different instrumentations and techniques. We will present some ideas on how to analyze these malware samples, and introduce you to embedded system analysis (unless your bot is removing this event from your smart watch's reminder list).

### Weaponizing Cybercurrencies *G. Mark Hardy*

Bitcoin is dead. Long live Bitcoin. Satoshi Nakamoto was no dummy. In the early days, he (they) mined over 1,000,000 Bitcoins when nobody really cared. If Bitcoin (or any other cybercurrency) were to increase in value at the rate it did last year, someone will be holding a massive currency weapon. George Soros destabilized the British Pound in 1992 and made over 1,000,000,000 profit. In the largest counterfeiting operation in history, Nazi Germany devised Operation Bernhard to destabilize the British economy by dropping millions of pound notes from Luftwaffe aircraft. If the holder of a giga-cybercurrency has a currency digital weapon that works frictionlessly in milliseconds, against whom will he target it? Can it destabilize an entire government? Can it be continuously reused for blackmail? What should governments be doing now to plan for this contingency and fight back? We'll discuss an entirely new class of information weapon – digital cryptocurrency – and how it might either change the course of history, or be relegated to the ash heap of failure.

### Infosec Rock Star: How to be a More Effective Security Professional *Ted Demopoulos*

Why are some of us much more effective than others? A very few of us are so effective, and well known, that we might even be called the rock stars of our industry. Now we personally may never be swamped by groupies, but we can learn the skills, be more effective, well respected, and well paid. Obviously it's not just about technology; in fact most of us are very good at the technology part. The myth of the geek with zero social skills is just that, a myth. However, the fact is that increasing our skills more on the social and business sides will make most of us more effective at what we do than learning how to read hex better while standing on our heads, becoming 'One with Metasploit' or understanding the latest hot technologies will.

### 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.

### 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.

### How to Spy on your Employees with Memory Forensics *Jake Williams*

Many companies can't afford employee endpoint monitoring software such as SpectorPro, and yet still have the need to figure out how a rogue employee is spending his time on the job. Consider a cheaper solution for employee spying – one that makes use of native Windows services and an investigator's ninja memory analysis skills. Whether it be creating a scheduled task to send a machine to hibernate or instantiating an unsuspected memory dump, targeted-employee spying can be done on the cheap. Through process enumeration, browsing history reconstruction and memory-mapped file extraction, watch as your presenters piece together what our trusted insider was doing on their company computer, unbeknownst to his boss. Even if you don't have the need to covertly investigate a rogue employee (yet), this talk will arm you the knowledge to know what is within the realm of the possible.

# How Are You Protecting Your


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

GIAC offers over 20 specialized certifications in security, forensics, penetration testing, web application security, IT audit, management, and IT security law.

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

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

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

# 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 |
|---|---|---|
| A+CE<br>Network+CE<br>SSCP | **GSEC**<br>Security+CE<br>SSCP | **GCED**<br>**GCIH**<br>**CISSP**<br>(or Associate)<br>CISA |

| IAM Level I | IAM Level II | IAM Level III |
|---|---|---|
| **GSLC**<br>CAP<br>Security+CE | **GSLC**<br>**CISSP**<br>(or Associate)<br>CAP, CASP<br>CISM | **GSLC**<br>**CISSP**<br>(or Associate)<br>CISM |

## Computer Network Defense (CND) Certifications

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

## Information Assurance System Architecture & Engineering (IASAE) Certifications

| IASAE I | IASAE II | IASAE III |
|---|---|---|
| **CISSP**<br>(or Associate) | **CISSP**<br>(or Associate)<br>CASP | CISSP - ISSEP<br>CISSP - ISSAP |

## 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.

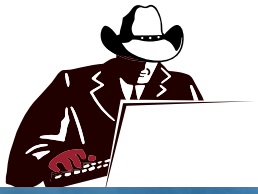
| SANS TRAINING COURSE | DoDD APPROVED CERT |
|---|---|
| SEC401 | GSEC |
| SEC501 | GCED |
| SEC503 | GCIA |
| SEC504 | GCIH |
| AUD507 | GSNA |
| FOR508 | GCFA |
| MGT414 | CISSP |
| MGT512 | GSLC |

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

# FUTURE SANS TRAINING EVENTS

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



## Digital Forensics & Incident Response SUMMIT

Austin, TX | June 3-10

## SANS Rocky Mountain 2014

Denver, CO | June 9-14

## 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 ICS Industrial Control Systems

## ICS Security TRAINING 2014 - HOUSTON

Houston, TX | July 21-25

## SANS Boston 2014

Boston, MA | July 28 - August 2

## SANS Cyber Defense SUMMIT

Nashville, TN | August 13-20

## SANS Virginia Beach 2014

Virginia Beach, VA | August 18-29

# 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 SAN ANTONIO 2014

# Hotel Information

*Training Campus*
**Westin Riverwalk**

**420 West Market Street**
**San Antonio , TX**
**www.sans.org/event/san-antonio-2014/location**

## Special Hotel Rates Available

**A special discounted rate of $189.00 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 July 9, 2014. To make reservations please call Central Reservations at (888) 627-8396 and ask for the SANS group rate.**

Located on the world famous Riverwalk in San Antonio, the Westin Riverwalk is the perfect location to relax and recharge. Expect a warm welcome when you visit. Enjoy delicious dark chocolates imported from Venezuela when you check in. The Westin's accommodations offer amenities that will leave you feeling refreshed and rejuvenated.

## Top 5 reasons to stay at the Westin Riverwalk

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 Westin Riverwalk, 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 Westin Riverwalk that you won't want to miss!
5. Everything is in one convenient location!

SANS SAN ANTONIO 2014

# Registration Information

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


**Register online at www.sans.org/event/san-antonio-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** | **6/18/14** | **$400.00** | **7/9/14** | **$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 July 23, 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**