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

SANS San Antonio 2017

August 6-11

PROTECT YOUR COMPANY AND ADVANCE YOUR CAREER
WITH HANDS-ON, IMMERSION-STYLE

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

Seven courses in:

- CYBER DEFENSE
- PENETRATION TESTING
- ETHICAL HACKING
- DETECTION & MONITORING
- CYBER THREAT INTELLIGENCE MANAGEMENT

GIAC CERTIFICATIONS
GIAC-Approved Training

"SANS training is the best, bar none. Instructors are celebrities in their fields. I have completed seven courses and all of them have been top notch."
-Dow Shirley, ZAGG Inc.

SAVE $400
Register and pay by June 14th – Use code **EarlyBird17**

www.sans.org/san-antonio

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 San Antonio 2017 lineup of instructors includes:

Rebekah Brown
Instructor
@PDXBek

Kevin Fiscus
Certified Instructor
@kevinbfiscus

Bryce Galbraith
Principal Instructor
@brycegalbraith

Jonathan Ham
Certified Instructor
@jhamcorp

G. Mark Hardy
Certified Instructor
@g_mark

Keith Palmgren
Senior Instructor
@kpalmgren

Matthew Toussain
Instructor
@0sm0s1z

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 9.

KEYNOTE: ***Everything You've Ever Learned About Passwords Is Wrong***
Keith Palmgren

Anti-Ransomware: How to Turn the Tables
G. Mark Hardy

Shell Is Only The Beginning: Understanding Metasploit Post Exploitation Modules
Kevin Fiscus

Save $400 when you register and pay by June 14th using code EarlyBird17

Courses at a Glance

	SUN 8-6	MON 8-7	TUE 8-8	WED 8-9	THU 8-10	FRI 8-11
SEC301 Intro to Information Security	Page 2					
SEC401 Security Essentials Bootcamp Style	Page 3					
SEC503 Intrusion Detection In-Depth	Page 4					
SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	Page 5					
SEC560 Network Penetration Testing and Ethical Hacking	Page 6					
FOR578 Cyber Threat Intelligence	Page 7					
MGT512 SANS Security Leadership Essentials for Managers with Knowledge Compression™	Page 8					

Securing **Approval** and **Budget** for Training

Packaging matters

Write a formal request

- All organizations are different, but because training requires a significant investment of both time and money, most successful training requests are made via a written document (short memo and/or a few powerpoint slides) that justifies the need and benefit. Most managers will respect and value the effort.
- Provide all the necessary information in one place. In addition to your request, provide all the right context by including the summary pages on Why SANS?, the Training Roadmap, the instructor bio, and additional benefits available at our live events or online.

Clearly state the benefits

Be specific

- How does the course relate to the job you need to be doing? Are you establishing baseline skills? Transitioning to a more focused role? Decision-makers need to understand the plan and context for the decision.
- Highlight specifics of what you will be able to do afterwards. Each SANS course description includes a section titled "You Will Be Able To." Be sure to include this in your request so that you make the benefits clear. The clearer the match between the training and what you need to do at work, the better.

Set the context

Establish longer-term expectations

- Information security is a specialized career path within IT, with practices that evolve as attacks change. Because of this, organizations should expect to spend 6%-10% of salaries to keep professionals current and improve their skills. Training for such a dynamic field is an annual, per-person expense, and not a once-and-done item.
- Take a GIAC Certification exam to prove the training worked. Employers value the validation of skills and knowledge that a GIAC Certification provides. Exams are psychometrically designed to establish competency for related job tasks.
- Consider offering trade-offs for the investment. Many professionals build annual training expense into their employment agreements even before joining a company. Some offer to stay for a year after they complete the training.

SEC301

Intro to Information Security

GISF Certification
Information Security Fundamentals

www.giac.org/gisf

Five-Day Program
Sun, Aug 6 - Thu, Aug 10
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Keith Palmgren

"Labs reinforced the security principles in a real-world scenario."
-Tyler Moore, Rockwell

"This course was the perfect blend of technical and practical information for someone new to the field, and I would recommend it!"
-Steve Mecco, Draper

▶II **Bundle OnDemand**
with this course
www.sans.org/ondemand

To determine if the SANS SEC301 course is right for you, ask yourself five simple questions:

- **Do you have basic computer knowledge, but are new to information security and in need of an introduction to the fundamentals?**
- **Are you bombarded with complex technical security terms that you don't understand?**
- **Are you a non-IT security manager (with some technical knowledge) who lays awake at night worrying that your company will be the next mega-breach headline story on the 6 o'clock news?**
- **Do you need to be conversant in basic security concepts, principles, and terms, even if you don't need "deep in the weeds" detail?**
- **Have you decided to make a career change to take advantage of the job opportunities in information security and need formal training/certification?**

If you answer yes to any of these questions, the **SEC301: Intro to Information Security** training course is for you. Jump-start your security knowledge by receiving insight and instruction from real-world security experts on critical introductory topics that are fundamental to information security. This completely revised five-day, comprehensive course covers everything from core terminology to the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles.

This course is designed for students who have a basic knowledge of computers and technology but no prior knowledge of cybersecurity. The hands-on, step-by-step teaching approach will enable you to grasp all of the information presented even if some of the topics are new to you. You'll learn the fundamentals of information security that will serve as the foundation of your InfoSec skills and knowledge for years to come.

Written by a security professional with over 30 years of experience in both the public and private sectors, SEC301 provides uncompromising real-world insight from start to finish. The course prepares you for the Global Information Security Fundamentals (GISF) certification test, as well as for the next course up the line, **SEC401: Security Essentials Bootcamp Style**. It also delivers on the ***SANS promise: You will be able to use the knowledge and skills you learn in SEC301 as soon as you return to work.***

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 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 17 training courses. Keith currently holds the CISSP, GSEC, CEH, Security+, Network+, A+, and CTT+ certifications. **@kpalmgren**

SEC401

Security Essentials Bootcamp Style

GSEC Certification
Security Essentials

www.giac.org/gsec

Six-Day Program
Sun, Aug 6 - Fri, Aug 11
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Bryce Galbraith

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 specialists, penetration testers, and auditors who need a solid foundation of security principles to be as effective as possible at their jobs
- Anyone new to information security with some background in information systems and networking

"This training answers the 'why' of my work practices, and asks the 'why not' for the practices my company doesn't follow."
-Thomas Petro, Southern California Edison

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

STOP and ask yourself the following questions:

- **Do you fully understand why some organizations get compromised and others do not?**
- **If there were compromised systems on your network, are you confident you would be able to find them?**
- **Do you know the effectiveness of each security device and are you certain they are all configured correctly?**
- **Are proper security metrics set up and communicated to your executives to drive security decisions?**

If you do not know the answers to these questions, SEC401 will provide the information security training you need in a bootcamp-style format that is reinforced with hands-on labs.

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. Our course will show you how to prevent your organization's security problems from being headline news in the *Wall Street Journal*!

Prevention Is Ideal but Detection Is a Must

With the rise in 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 will 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.

SANS Technology Institute
www.sans.edu

www.sans.org/8140

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

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 he 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, holds several security certifications, and speaks at conferences around the world. **@brycegalbraith**

SEC503

Intrusion Detection In-Depth

GCIA Certification
Certified Intrusion Analyst

www.giac.org/gcia

Six-Day Program
Sun, Aug 6 - Fri, Aug 11
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jonathan Ham

Who Should Attend

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

"This training directly correlates to my agency's mission of conducting network forensics/ intrusion investigations."

-Chris G., U.S. Air Force Office of Special Investigations

"I would recommend this to network/ security people who have some experience already but need to sharpen their skills."

-M.S., AOL

Reports of prominent organizations being hacked and suffering irreparable reputational damage have become all too common. How can you prevent your company from becoming the next victim of a major cyber attack?

Preserving the security of your site in today's threat environment is more challenging than ever before. The security landscape is continually changing from what was once only perimeter protection to protecting exposed and mobile systems that are almost always connected and sometimes vulnerable. Security-savvy employees who can help detect and prevent intrusions are therefore in great demand. Our goal in **SEC503: Intrusion Detection In-Depth** is to acquaint you with the core knowledge, tools, and techniques to defend your networks with insight and awareness. The training will prepare you to put your new skills and knowledge to work immediately upon returning to a live environment.

Mark Twain said, "It is easier to fool people than to convince them that they've been fooled." Too many IDS/IPS solutions provide a simplistic red/green, good/bad assessment of traffic and too many untrained analysts accept that feedback as the absolute truth. This course emphasizes the theory that a properly trained analyst uses an IDS alert as a starting point for examination of traffic, not as a final assessment. SEC503 imparts the philosophy that the analyst must have access and the ability to examine the alerts to give them meaning and context. You will learn to investigate and reconstruct activity to deem if it is noteworthy or a false indication.

SEC503: Intrusion Detection In-Depth delivers the technical knowledge, insight, and hands-on training you need to defend your network with confidence. You will learn about the underlying theory of TCP/IP and the most used application protocols, such as DNS and HTTP, so that you can intelligently examine network traffic for signs of an intrusion. You will get plenty of practice learning to master different open-source tools like tcpdump, Wireshark, Snort, Bro, tshark, and SiLK. Daily hands-on exercises suitable for all experience levels reinforce the course book material so that you can transfer knowledge to execution. Basic exercises include assistive hints while advanced options provide a more challenging experience for students who may already know the material or who have quickly mastered new material.

SANS Technology Institute
www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

Jonathan Ham *SANS Certified Instructor*

Jonathan is an independent consultant who specializes in large-scale enterprise security issues, from policy and procedure, through staffing and training, to scalable prevention, detection, and response technology and techniques. With a keen understanding of ROI and TCO (and an emphasis on process over products), he has helped his clients achieve greater success for over 20 years, advising in both the public and private sectors, from small upstarts to the Fortune 500. He's been commissioned to teach NCIS investigators how to use Snort, performed packet analysis from a facility more than 2000 feet underground, and chartered and trained the CIRT for one of the largest U.S. civilian federal agencies. He has variously held the CISSP, GSEC, GCIA, and GCIH certifications, and is a member of the GIAC Advisory Board. A former combat medic, Jonathan still spends some of his time practicing a different kind of emergency response, volunteering and teaching for both the National Ski Patrol and the American Red Cross. **@jhamcorp**

SEC504

GCIH Certification
Incident Handler

www.giac.org/gcih

Hacker Tools, Techniques, Exploits, and Incident Handling

Six-Day Program
Sun, Aug 6 - Fri, Aug 11
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
(If your laptop supports only wireless, please bring a USB Ethernet adapter.)
Instructor: Kevin Fiscus

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

"SANS offers very valuable, practical training which makes it possible to return to the workplace and immediately implement improvements and strategies."
-Jill Stuart,
Reserve Bank of Australia

"SEC504 helped me put many pieces of the puzzle together."
-Ian Trimble,
Blue Cross Blue Shield

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.

"[This course is a] good foundation for security incidents. It's a must-have for security incident handlers/managers."-Wu Peihui, Citibank

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 those attacks. Additionally, 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 course 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.

SANS Technology Institute
www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

Kevin Fiscus *SANS Certified Instructor*

Kevin Fiscus is the founder of and lead consultant for Cyber Defense Advisors, where he performs security and risk assessments, vulnerability and penetration testing, security program design, policy development and security awareness with a focus on serving the needs of small and mid-sized organizations. Kevin has over 20 years of IT experience and has focused exclusively on information security for the past 12. He currently holds the CISA, GPEN, GREM, GMOB, GCED, GCFA-Gold, GCIA-Gold, GCIH, GAWN, GPPA, GCWN, GCSC-Gold, GSEC, SCSA, RCSE, and SnortCP certifications and is proud to have earned the top information security certification in the industry, the GIAC Security Expert. Kevin has also achieved the distinctive title of SANS Cyber Guardian for both red team and blue team. Kevin has taught many of SANS' most popular classes including SEC401, SEC464, SEC503, SEC504, SEC542, SEC560, SEC561, SEC575, FOR508, and MGT414. **@kevinbfiscus**

SEC560

Network Penetration Testing and Ethical Hacking

GPEN Certification
Penetration Tester

www.giac.org/gpen

Six-Day Program
Sun, Aug 6 - Fri, Aug 11
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Matthew Toussain

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

"I learned more in one class than in years of self-study!"
-Bradley Milhorn, Compucom Inc.

"It introduces the whole process of pen testing from start of engagement to end."
-Barry Tsang, Deloitte

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

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

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

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

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

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

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.

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

Matthew Toussain *SANS Instructor*

Matthew Toussain is an active-duty U.S. Air Force officer and the founder of Spectrum Information Security, a firm focused on maximizing the value proposition of information security programs. As an avid information security researcher, Matthew regularly hunts for vulnerabilities in computer systems and releases tools to demonstrate the effectiveness of attacks and countermeasures. He has been a guest speaker at many conference venues, including DEFCON, the largest security conference in the world. After graduating from the U.S. Air Force Academy, where he architected and instructed the summer cyber course that now trains over 400 cadets per year, Matthew served as the Senior Cyber Tactics Development Lead for the Air Force. He directed the teams responsible for developing innovative tactics, techniques, and procedures for offensive operations as well as for cyber protection teams (CPT). Later, as a member of the 688th Cyber Warfare Wing he managed the Air Force's transition of all 18 CPTs to fully operational capability. As a founding member of Spectrum, Matthew regularly performs a wide variety of information security services. He earned his master's degree in information security engineering as one of the first graduates of the SANS Technology Institute and supports many national and international cyber competitions including the CCDC, SANS Netwars, and the National Security Agency's Cyber Defense Exercise as a red team member and instructor. @0sm0s1z

FOR578

Cyber Threat Intelligence

GIAC Certification Available Late 2017

Five-Day Program
Sun, Aug 6 - Thu, Aug 10
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Rebekah Brown

Who Should Attend

- Incident response team members
- Threat hunters
- Experienced digital forensic analysts
- Security Operations Center personnel and information security practitioners
- Federal agents and law enforcement officials
- SANS FOR408, FOR572, FOR508, or FOR610 graduates looking to take their skills to the next level

"Outstanding course material and instructor presentation! FOR578 truly drills into the analytic process, while remaining technical. I highly recommend this course to anyone performing any level of intelligence support to defensive cyber operations."

-Thomas L., U.S. Air Force

▶II **Bundle OnDemand**
WITH THIS COURSE
www.sans.org/ondemand

Make no mistake: current network defense, threat hunting, and incident response practices contain a strong element of intelligence and counterintelligence that cyber analysts must understand and leverage in order to defend their networks, proprietary data, and organizations.

FOR578: Cyber Threat Intelligence will help network defenders, threat hunting teams, and incident responders to:

- **Understand and develop skills in tactical, operational, and strategic-level threat intelligence**
- **Generate threat intelligence to detect, respond to, and defeat advanced persistent threats (APTs)**
- **Validate information received from other organizations to minimize resource expenditures on bad intelligence**
- **Leverage open-source intelligence to complement a security team of any size**
- **Create Indicators of Compromise (IOCs) in formats such as YARA, OpenIOC, and STIX**

The collection, classification, and exploitation of knowledge about adversaries – collectively known as cyber threat intelligence – gives network defenders information superiority that is used to reduce the adversary's likelihood of success with each subsequent intrusion attempt. Responders need accurate, timely, and detailed information to monitor new and evolving attacks, as well as methods to exploit this information to put in place an improved defensive posture.

Cyber threat intelligence thus represents a force multiplier for organizations looking to update their response and detection programs to deal with increasingly sophisticated advanced persistent threats. Malware is an adversary's tool but the real threat is the human one, and cyber threat intelligence focuses on countering those flexible and persistent human threats with empowered and trained human defenders.

During a targeted attack, an organization needs a top-notch and cutting-edge threat hunting or incident response team armed with the threat intelligence necessary to understand how adversaries operate and to counter the threat. **FOR578: Cyber Threat Intelligence** will train you and your team in the tactical, operational, and strategic-level cyber threat intelligence skills and tradecraft required to make security teams better, threat hunting more accurate, incident response more effective, and organizations more aware of the evolving threat landscape.

THERE IS NO TEACHER BUT THE ENEMY!

Rebekah Brown *SANS Instructor*

Rebekah Brown is the threat intelligence lead for Rapid7, supporting incident response, analytic response, global services and product support. She is a former NSA network warfare analyst, U.S. Cyber Command training and exercise lead, and Marine Corps crypto-linguist who has helped develop threat intelligence programs at the federal, state, and local levels as well as in the private sector at a Fortune 500 company. She has an associate's degree in Chinese Mandarin, a B.A. in international relations, and is wrapping up a M.A. in homeland security with a cybersecurity focus and a graduate certificate in intelligence analysis. **@PDXBek**

MGT512

GSLC Certification
Security Leadership

www.giac.org/gslc

SANS Security Leadership Essentials for Managers with Knowledge Compression™

Five-Day Program
Sun, Aug 6 - Thu, Aug 10
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop Recommended
Instructor: G. Mark Hardy

Who Should Attend

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

"MGT512 is one of the most valuable courses I've taken with SANS. It really did help bridge the gap from security practitioner to security orchestrator. Truly a gift!"
-John Madick, Epiq Systems, Inc.

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 the 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 U.S. government managers and supporting contractors.

Essential security topics covered in this management track 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, and 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.

Knowledge Compression™

Maximize your learning potential!
Knowledge Compression™ is an optional add-on feature to a SANS class that 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!

SANS Technology Institute
www.sans.edu

www.sans.org/8140

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

G. Mark Hardy *SANS Certified Instructor*

G. Mark Hardy is founder and president of the National Security Corporation. He has been providing cybersecurity expertise to government, military, and commercial clients for over 30 years, and is an internationally recognized expert who has spoken at over 250 events worldwide. He 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 U.S. 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 B.S. in computer science, a B.A. in mathematics, a master's degree in business administration, and a master's degree in strategic studies, and holds the GSLC, CISSP, CISM, and CISA certifications. @g_mark

Bonus Sessions

Enrich your SANS training experience! Evening talks 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: Everything You've Ever Learned About Passwords Is Wrong

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 will learn how to create significantly stronger passwords that are easier to remember—for their users, for themselves, and even for their children.

Anti-Ransomware: How to Turn the Tables

G. Mark Hardy

"OMG! We just got hit with ransomware!" What you don't usually hear next is "LOL!" You can build defenses that prevent ransomware from paralyzing your organization – we'll show you how. Ransomware is a billion dollar industry, and it's growing tremendously. Lost productivity costs far more than the average ransom, so executives just say, "Pay the darn thing." But what if you could stop ransomware in its tracks? We'll demonstrate tools and methodologies that are battle-proven and ACTUALLY WORK as evidenced by fully contained ransomware "explosions" that went nowhere. We'll offer insights into the future of this attack vector and venture predictions on how this industry will evolve and what to expect next.

Shell Is Only The Beginning: Understanding Metasploit Post-Exploitation Modules

Kevin Fiscus

Metasploit is a fantastic hacking tool. Having a huge range or exploits and a collection of different payloads that are easy to use makes compromising vulnerable system almost trivial. Many a penetration tester have been given the opportunity to do their "happy dance" by compromising a system and getting shell on the target system. Getting shell, however, is only the beginning of the penetration test. When taking martial arts, it is common to hear that becoming a blackbelt is only the beginning of the training. Penetration testing is similar. The test really begins when you get shell. Once you have access to the compromised system, what do you do? This talk will discuss the often overlooked post-exploitation modules in Metasploit. These are the components in Metasploit that allow you to capture keystrokes, identify new targets, grab credentials, identify users, determine what applications are installed, and even identify if you have compromised a physical or virtual host. During this talk, we will describe and demonstrate many of these modules, adding to your arsenal of penetration testing techniques.

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

- 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

Whether you choose to attend a training class live or online, the entire SANS team is dedicated to ensuring your training experience exceeds expectations.

Live Classroom Instruction

Premier Training Events

Our most recommended format, live SANS training events feature SANS' top instructors teaching multiple courses at a single time and location. This allows for:

- Focused, immersive learning without the distractions of your office environment
- Direct access to SANS Certified Instructors
- Interacting with and learning from other professionals
- Attending SANS@Night events, NetWars tournaments, vendor presentations, industry receptions, and many other activities

Our premier live training events in North America, serving thousands of students, are held in Orlando, Washington DC, Las Vegas, New Orleans, and San Diego. Regional events with hundreds of students are held in most major metropolitan areas during the year. See page 16 for upcoming training events in North America.

Summits

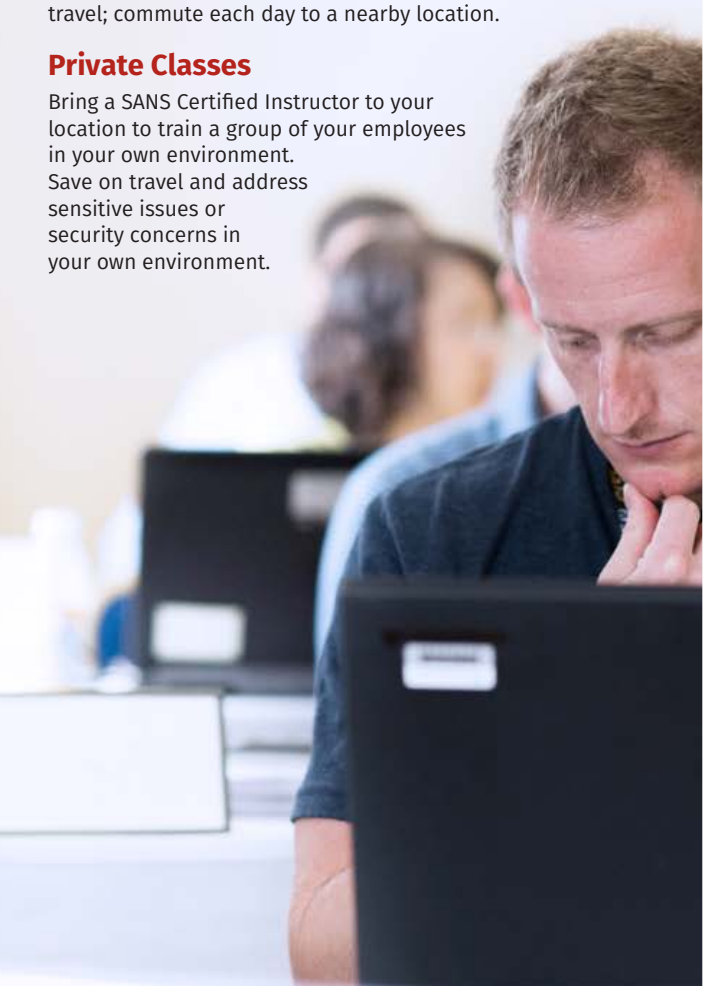
SANS Summits focus one or two days on a single topic of particular interest to the community. Speakers and talks are curated to ensure the greatest applicability to participants.

Community SANS Courses

Same SANS courses, courseware, and labs, are taught by up-and-coming instructors in a regional area. Smaller classes allow for more extensive instructor interaction. No need to travel; commute each day to a nearby location.

Private Classes

Bring a SANS Certified Instructor to your location to train a group of your employees in your own environment. Save on travel and address sensitive issues or security concerns in your own environment.



Online Training

SANS Online successfully delivers the same measured learning outcomes to students at a distance that we deliver live in classrooms. More than 30 courses are available for you to take whenever or wherever you want. Thousands of students take our courses online and achieve certifications each year.

Top reasons to take SANS courses online:

- Learn at your own pace, over four months
- Spend extra time on complex topics
- Repeat labs to ensure proficiency with skills
- Save on travel costs
- Study at home or in your office

Our SANS OnDemand, vLive, Simulcast, and SelfStudy formats are backed by nearly 100 professionals who ensure we deliver the same quality instruction online (including support) as we do at live training events.

> "I am thoroughly pleased with the OnDemand modality. From a learning standpoint, I lose nothing. In fact, the advantage of setting my own pace with respect to balancing work, family, and training is significant, not to mention the ability to review anything that I might have missed the first time."
>
> -Kevin E., U.S. Army

> "The decision to take five days away from the office is never easy, but so rarely have I come to the end of a course and had no regret whatsoever. This was one of the most useful weeks of my professional life."
>
> -Dan Trueman, Novae PLC

Future Training Events

Northern Virginia – Reston	Reston, VA	May 21-26
Atlanta	Atlanta, GA	May 30 - June 4
Houston	Houston, TX	June 5-10
San Francisco Summer	San Francisco, CA	June 5-10
Rocky Mountain	Denver, CO	June 12-17
Charlotte	Charlotte, NC	June 12-17
Minneapolis	Minneapolis, MN	June 19-24
Columbia, MD	Columbia, MD	June 26 - July 1
ICS & Energy	Houston, TX	July 10-15
Los Angeles – Long Beach	Long Beach, CA	July 10-15

SANSFIRE Washington, DC July 22-29

San Antonio	San Antonio, TX	Aug 6-11
Boston	Boston, MA	Aug 7-12
New York City	New York, NY	Aug 14-19
Salt Lake City	Salt Lake City, UT	Aug 14-19
Chicago	Chicago, IL	Aug 21-26
Virginia Beach	Virginia Beach, VA	Aug 21 - Sep 1
Tampa – Clearwater	Clearwater, FL	Sep 5-10
San Francisco Fall	San Francisco, CA	Sep 5-10

Network Security Las Vegas, NV Sep 10-17

Baltimore	Baltimore, MD	Sep 25-30
Rocky Mountain Fall	Denver, CO	Sep 25-30
Phoenix-Mesa	Mesa, AZ	Oct 9-14
Tysons Corner Fall	Washington, DC	Oct 16-21
San Diego Fall	San Diego, CA	Oct 30 - Nov 4
Seattle	Seattle, WA	Oct 30 - Nov 4

Future Summit Events

Security Operations Center	Washington, DC	June 5-12
Digital Forensics	Austin, TX	June 22-29
Security Awareness	Nashville, TN	July 31 - Aug 9
Data Breach	Chicago, IL	Sep 25 - Oct 2
Secure DevOps	Denver, CO	Oct 10-17

Future Community SANS Events

Local, single-course events are also offered throughout the year via SANS Community. Visit **www.sans.org/community** for up-to-date Community course information.

Hotel Information

Grand Hyatt San Antonio
600 E. Market Street
San Antonio, TX 78205
Phone: 210-224-1234
www.sans.org/event/san-antonio-2017/location

Discover the distinctly diverse personality of San Antonio in grand style. Set along the spectacular River Walk, Grand Hyatt San Antonio places you near trendy downtown bars, hot clubs, Zagat-rated restaurants and all the attractions that make this one of the most culturally rich cities in the country.

Special Hotel Rates Available

A special discounted rate of $175.00 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 14, 2017**. To make reservations, please call **210-224-1234** and ask for the SANS group rate.

Top 5 reasons to stay at the Grand Hyatt San Antonio

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 Grand Hyatt San Antonio 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 Grand Hyatt San Antonio that you won't want to miss!
5. Everything is in one convenient location!

Registration Information

Register online at **www.sans.org/san-antonio**

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

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.

Pay Early and Save*

Use code **EarlyBird17** when registering early

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code by	**6-14-17**	**$400.00**	**7-5-17**	**$200.00**

*Some restrictions apply. Early bird discounts do not apply to Hosted courses.

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 & Access Policy

If an attendee must cancel, a substitute may attend instead. Substitution requests can be made at any time prior to the event start date. Processing fees will apply. All substitution requests must be submitted by email to registration@sans.org. If an attendee must cancel and no substitute is available, a refund can be issued for any received payments by **July 12, 2017**. A credit memo can be requested up to the event start date. All cancellation requests must be submitted in writing by mail or fax and received by the stated deadlines. Payments will be refunded by the method that they were submitted. Processing fees will 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