SANS South Florida 2015

Fort Lauderdale, FL November 9-14

Choose from these popular courses:

Web App Penetration Testing and Ethical Hacking *NEW!*

Security Essentials Bootcamp Style

Hacker Tools, Techniques, Exploits, and Incident Handling

Advanced Digital Forensics and Incident Response

Advanced Network Forensics and Analysis

Advanced Smartphone Forensics

"This is my 6th SANS training event and SANS continues to deliver. They offer relevant, practical, and highly informative courses that are taught by instructors who truly understand the content."

-Tyler Leet, Computer Services, Inc.

GIAC Approved Training

Register at sans.org/event/south-florida-2015

SAVE **$400** by registering & paying early!

See page 13 for more details.

SANS Instructors are real-world practitioners who specialize in the subjects they teach. All instructors undergo rigorous training and testing in order to become SANS Certified Instructors. This guarantees that what you learn in class will be up-to-date and relevant to your job. The SANS South Florida 2015 line-up of instructors includes:

Adrien de Beaupre

Rob Lee

Hal Pomeranz

Kevin Fiscus

Heather Mahalik

Bryan Simon

Evening Bonus Sessions: Don't miss these extra evening events that make SANS a great value for your security training:

Hunting Your Adversary – How to Operate and Leverage an Incident Response Hunt Team
Rob Lee

DLP FAIL!!! Using Encoding, Steganography, and Covert Channels to Evade DLP and Other Critical Controls
Kevin Fiscus

Bueller... Bueller... Smartphone Forensics Moves Fast: Stay Current or Miss Evidence
Heather Mahalik

IR Event Log Analysis
Hal Pomeranz

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

PAGE 8

Be sure to register and pay by Sept. 16th for a $400 tuition discount!

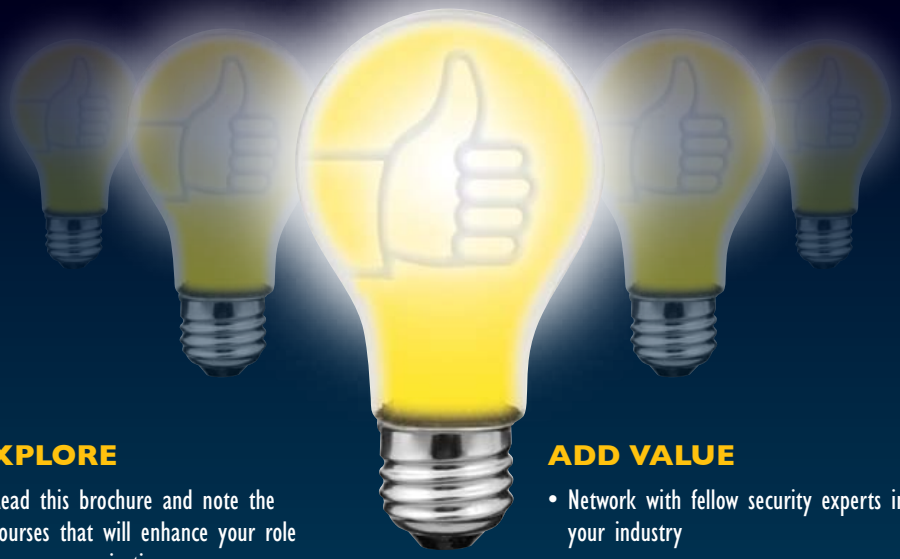
Relax in the heart of downtown Fort Lauderdale, where world-class restaurants, hopping nightclubs and enchanting courtyards frame the city's only hotel on the trendy Las Olas Boulevard – the Riverside Hotel.

PAGE 13

Courses-at-a-Glance

	MON 11/9	TUE 11/10	WED 11/11	THU 11/12	FRI 11/13	SAT 11/14
SEC401 **Security Essentials Bootcamp Style**	Page 2					
SEC504 **Hacker Tools, Techniques, Exploits, and Incident Handling**	Page 3					
SEC542 **Web App Penetration Testing and Ethical Hacking *NEW!***	Page 4					
FOR508 **Advanced Digital Forensics and Incident Response**	Page 5					
FOR572 **Advanced Network Forensics and Analysis**	Page 6					
FOR585 **Advanced Smartphone Forensics**	Page 7					

The Value of SANS Training and *YOU*



EXPLORE

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

RELATE

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

VALIDATE

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

SAVE

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

ADD VALUE

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

ALTERNATIVES

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

ACT

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

Return on Investment

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

REMEMBER

the SANS promise:

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

SECURITY 401

Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Nov 9 - Sat, Nov 14
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Bryan Simon

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

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

Learn to build a security roadmap that can scale today and into the future.

SEC401: Security Essentials Bootcamp Style is focused on teaching you the essential information security skills and techniques you need to protect and secure your organization's critical information assets and business systems. This course will show you how to prevent your organization's security problems from being headline news in the *Wall Street Journal*!

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

With the advanced persistent threat, it is almost inevitable that organizations will be targeted. Whether the attacker is successful in penetrating an organization's network depends on the effectiveness of the organization's defense. Defending against attacks is an ongoing challenge, with new threats emerging all of the time, including the next generation of threats. Organizations need to understand what really works in cybersecurity. What has worked, and will always work, is taking a risk-based approach to cyber defense. Before your organization spends a dollar of its IT budget or allocates any resources or time to anything in the name of cybersecurity, three questions must be answered:

- What is the risk?
- Is it the highest priority risk?
- What is the most cost-effective way to reduce the risk?

Security is all about making sure you focus on the right areas of defense. In SEC401 you will learn the language and underlying theory of computer and information security. You will gain the essential and effective security knowledge you'll need if you are given the responsibility for securing systems and/or organizations. This course meets both of the key promises SANS makes to our students: (1) You will learn up-to-the-minute skills you can put into practice immediately upon returning to work; and (2) You will be taught by the best security instructors in the industry.

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

BUNDLE ONDEMAND WITH THIS COURSE
sans.org/ondemand

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

"Great explanations on crypto! Took a semester-long course and this was much better. The instructor maintains the energy for the entire class and never hesitates to answer questions."
-David Lawrence, Livermore National Laboratory

Bryan Simon *SANS Certified Instructor*

Bryan Simon is an internationally recognized expert in cybersecurity and has been working in the information technology and security field since 1991. Over the course of his career, Bryan has held various technical and managerial positions in the education, environmental, accounting, and financial services sectors. Bryan speaks on a regular basis at international conferences and with the press on matters of cybersecurity. He has taught staff from organizations such as the FBI, NATO, and the UN. Bryan has specialized expertise in defensive and offensive capabilities. He has received recognition for his work in IT Security, and was most recently profiled by McAfee (part of Intel Security) as an IT Hero. Bryan holds 11 GIAC Certifications including GSEC, GCWN, GCIH, GCFA, GPEN, GWAPT, GAWN, GISP, GCIA, GCED, and GCUX. Bryan's scholastic achievements have contributed to his serving as a current member of the Advisory Board for the SANS Institute, and his acceptance into the prestigious SANS Cyber Guardian program. Bryan is a SANS instructor for SEC401, SEC501, SEC505, and SEC511. @BryanOnSecurity

SECURITY 504

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Mon, Nov 9 - Sat, Nov 14
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Kevin Fiscus

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

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection or one or two disgruntled employees (and whose does not!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth. As defenders, it is essential we understand these hacking tools and techniques.

Who Should Attend

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

"This course gave me a better understanding of what a hacker can do and how he does it – which will help me with incident handling."
-Jill Gallagher, HSBC

"This course helped me fill in the finer details and gaps in my knowledge. I understood the higher level concepts. I have worked with a few of the tools but this helped put it all together."
-Jenna Esparza, Los Alamos National Laboratory

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

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

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

Bundle OnDemand
with this course
sans.org/ondemand

Kevin Fiscus *SANS Certified Instructor*

Kevin Fiscus is the founder of and lead consultant for Cyber Defense Advisors, where he performs security and risk assessments, vulnerability and penetration testing, security program design, policy development and security awareness with a focus on serving the needs of small and mid-sized organizations. Kevin has over 20 years of IT experience and has focused exclusively on information security for the past 12. He currently holds the CISA, GPEN, GREM, GCFA-Gold, GCIA-Gold, GCIH, GAWN, 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 the red team and blue team. Kevin has taught many of SANS most popular classes including SEC401, SEC464, SEC504, SEC542, SEC560, SEC575, FOR508, and MGT414. In addition to his security work, he is a proud husband and father of two children. @kevinbfiscus

SECURITY 542

Web App Penetration Testing and Ethical Hacking

NEW

SANS

Six-Day Program
Mon, Nov 9 - Sat, Nov 14
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor:
Adrien de Beaupre

- GIAC Cert: GWAPT
- STI Master's Program
- OnDemand Bundle

Web applications play a vital role in every modern organization. However, if your organization doesn't properly test and secure its web apps, adversaries can compromise these applications, damage business functionality, and steal data. Unfortunately, many organizations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems.

Who Should Attend

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

SEC542 helps students move beyond push-button scanning to professional, thorough, high-value web application penetration testing.

Customers expect web applications to provide significant functionality and data access. Even beyond the importance of customer-facing web applications, internal web applications increasingly represent the most commonly used business tools within any organization. Unfortunately, there is no "patch Tuesday" for custom web applications, so major industry studies find that web application flaws play a major role in significant breaches and intrusions. Adversaries increasingly focus on these high-value targets either by directly abusing public-facing applications or by focusing on web apps as targets after an initial break-in.

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

"As with all SANS training I've taken, even when I think I know the subject well I'm learning something new."
-Benjamin Bagby, XE.com

SEC542 enables students to assess a web application's security posture and convincingly demonstrate the impact of inadequate security that plagues most organizations.

Students will come to understand major web application flaws and their exploitation and, most importantly, learn a field-tested and repeatable process to consistently find these flaws and convey what they have learned to their organizations. Even technically gifted security geeks often struggle with helping organizations understand risk in terms relatable to business. Much of the art of penetration testing has less to do with learning how adversaries are breaking in than it does with convincing an organization to take the risk seriously and employ appropriate countermeasures. The goal of SEC542 is to better secure organizations through penetration testing, and not just show off hacking skills. The course will help you demonstrate the true impact of web application flaws through exploitation.

"SANS training is like a catalyst. It not only boosts your knowledge but also inspires you to learn more."
-Tan Koon Yaw

In addition to high-quality course content, SEC542 focuses heavily on in-depth, hands-on labs to ensure that students can immediately apply all they learn.

giac.org

sans.edu

sans.org/cyber-guardian

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

Adrien de Beaupre *SANS Certified Instructor*

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

FORENSICS 508

Advanced Digital Forensics and Incident Response

SANS

Six-Day Program
Mon, Nov 9 - Sat, Nov 14
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Rob Lee

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

digital-forensics.sans.org

"Real-case examples and talking about real-world 'best-practice' is most valuable. Class discussions and questions were the best part of learning the material."
-Davie Yeo, Alvarez & Marsal

"Rob is fantastic and one of the best instructors I've had. I will need a week to rest my brain."
-Lorretta Filiault, Dynamac Corporation

FOR508: Advanced Digital Forensics and Incident Response will help you determine:

- How the breach occured
- How systems were affected and compromised
- What attackers took or changed
- How to contain and mitigate the incident

DAY 0: A 3-letter government agency contacts you to say critical information was stolen through a targeted attack on your organization. They won't tell how they know, but they identify several breached systems within your enterprise. An Advanced Persistent Threat adversary, aka an APT, is likely involved – the most sophisticated threat you are likely to face in your efforts to defend your systems and data.

Over 80% of all breach victims learn of a compromise from third-party notifications, not from internal security teams. In most cases, adversaries have been rummaging through your network undetected for months or even years.

Incident response tactics and procedures have evolved rapidly over the past several years. Data breaches and intrusions are growing more complex. Adversaries are no longer compromising one or two systems in your enterprise; they are compromising hundreds. Your team can no longer afford antiquated incident response techniques that fail to properly identify compromised systems, provide ineffective containment of the breach, and ultimately fail to rapidly remediate the incident.

This in-depth incident response course provides responders with advanced skills to hunt down, counter, and recover from a wide range of threats within enterprise networks, including APT adversaries, organized crime syndicates, and hactivism. Constantly updated, FOR508 addresses today's incidents by providing hands-on incident response tactics and techniques that elite responders are successfully using in real-world breach cases.

GATHER YOUR INCIDENT RESPONSE TEAM – IT'S TIME TO GO HUNTING!

Who Should Attend

- Incident response team leaders and members
- Security Operations Center (SOC) personnel and Information security practitioners
- Experienced digital forensic analysts
- System administrators
- Federal agents and law enforcement
- Red team members, penetration testers, and exploit developers
- SANS FOR408 and SEC504 graduates

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

Bundle OnDemand
WITH THIS COURSE
sans.org/ondemand

Rob Lee *SANS Faculty Fellow*

Rob Lee is an entrepreneur and consultant in the Boston, MA area and currently the Curriculum Lead and author for digital forensic and incident response training at the SANS Institute in addition to owning his own firm. Rob has more than 15 years' experience in computer forensics, vulnerability and exploit development, intrusion detection/prevention, and incident response. Rob graduated from the U.S. Air Force Academy and earned his MBA from Georgetown University. He served in the U.S. Air Force as a member of the 609th Information Warfare Squadron (IWS), the first U.S. military operational unit focused on information warfare. Later, he was a member of the Air Force Office of Special Investigations (AFOSI) where he led crime investigations and an incident response team. Over the next seven years, he worked directly with a variety of government agencies in the law enforcement, U.S. Department of Defense, and intelligence communities as the technical lead for vulnerability discovery and exploit development teams, lead for a cyber-forensics branch, and lead for a computer forensic and security software development team. Most recently, Rob was a Director for MANDIANT, a commercial firm focusing on responding to advanced adversaries such as the APT. Rob co-authored the book *Know Your Enemy, 2nd Edition.* Rob is also co-author of the MANDIANT threat intelligence report "M-Trends: The Advanced Persistent Threat." @robtlee & @sansforensics

FORENSICS 572

Advanced Network Forensics and Analysis

SANS

Six-Day Program
Mon, Nov 9 - Sat, Nov 14
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Hal Pomeranz

- GIAC Cert: GNFA
- STI Master's Program
- OnDemand Bundle

DFIR
digital-forensics.sans.org

"This course is the next step in developing top-notch incident response and network analysis professionals. The material is highly useful and is directly relevant to what our analysts are doing daily."
-Tom L., U.S. Air Force

"FOR572 is an excellent in-depth course on network-level forensics and it provides a deeper understanding into other forensic methods as well."
-Christina Camilleri, BAE Systems

Forensic casework that does not include a network component is a rarity in today's environment. Performing disk forensics will always be a critical and foundational skill for this career, but overlooking the network component of today's computing architecture is akin to ignoring security camera footage of a crime as it was committed. Whether you handle an intrusion incident, data theft case, or employee misuse scenario, the network often has an unparalleled view of the incident. Its evidence can provide the proof necessary to show intent, or even definitively prove that a crime actually occurred.

Who Should Attend

- Incident response team members and forensicators
- Law enforcement officers, federal agents, and detectives
- Information security managers
- Network defenders
- IT professionals
- Network engineers
- Anyone interested in computer network intrusions and investigations
- Security Operations Center personnel and information security practitioners

FOR572: Advanced Network Forensics and Analysis was built from the ground up to cover the most critical skills needed to mount efficient and effective post-incident response investigations. We focus on the knowledge necessary to expand the forensic mindset from residual data on the storage media from a system or device to the transient communications that occurred in the past or continue to occur. Even if the most skilled remote attacker compromised a system with an undetectable exploit, the system still has to communicate over the network. Without command-and-control and data extraction channels, the value of a compromised computer system drops to almost zero. Put another way: ***Bad guys are talking – we'll teach you to listen.***

This course covers the tools, technology, and processes required to integrate network evidence sources into your investigations, with a focus on efficiency and effectiveness. You will leave this week with a well-stocked toolbox and the knowledge to use it on your first day back on the job. We will cover the full spectrum of network evidence, including high-level NetFlow analysis, low-level pcap exploration, ancillary network log examination, and more. We cover how to leverage existing infrastructure devices that may contain months or years of valuable evidence, as well as how to place new collection platforms while an incident is already under way.

The hands-on exercises in this class cover a wide range of tools, including the venerable tcpdump and Wireshark for packet capture and analysis; commercial tools from Splunk, NetworkMiner, and SolarWinds; and open-source tools including nfdump, tcpxtract, ELSA, and more. Through all of these exercises, your shell scripting abilities will come in handy to make easy work of ripping through hundreds and thousands of data records.

GNFA
giac.org

SANS Technology Institute
sans.edu

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

Hal Pomeranz *SANS Faculty Fellow*

Hal Pomeranz is an independent digital forensic investigator who has consulted on cases ranging from intellectual property theft to employee sabotage, organized cybercrime and malicious software infrastructures. He has worked with law enforcement agencies in the U.S. and Europe and global corporations. While equally at home in the Windows or Mac environment, Hal is recognized as an expert in the analysis of Linux and Unix systems. His research on EXT4 file system forensics provided a basis for the development of open-source forensic support for this file system. His EXT3 file recovery tools are used by investigators worldwide. Hal is the creator of the SANS Linux/Unix Security course (GCUX). He holds the GCFA and GREM certifications and teaches the related courses in the SANS Forensics curriculum. He is a respected author and speaker at industry gatherings worldwide. Hal is a regular contributor to the SANS Computer Forensics blog and co-author of the Command Line Kung Fu blog. @hal_pomeranz

FORENSICS 585

Advanced Smartphone Forensics

SANS

Six-Day Program
Mon, Nov 9 - Sat, Nov 14
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Heather Mahalik
▸ OnDemand Bundle

DFIR
digital-forensics.sans.org

"Each day I am impressed with the amount of effort and research put in to provide the class with the most information possible on a subject that changes so frequently."
-Stephanie Kurtz, Deloitte

"Incredibly valuable week of training and would recommend it to anyone looking to expand their mobile forensic skills."
-Manny Ortiz, AT&T

It is almost impossible today to conduct a digital forensic investigation that does not include a smartphone or mobile device. Smartphones are replacing the need for a personal computer, and almost everyone owns at least one. The smartphone may be the only source of digital evidence tracing an individual's movements and motives, and thus can provide the who, what, when, where, why, and how behind a case. **FOR585: Advanced Smartphone Forensics** teaches real-life, hands-on skills that help digital forensic examiners, law enforcement officers, and information security professionals handle investigations involving even the most complex smartphones currently available.

Who Should Attend

- Experienced digital forensic analysts
- Media exploitation analysts
- Information security professionals
- Incident response teams
- Law enforcement officers, federal agents, and detectives
- IT auditors
- SANS SEC575, FOR408, FOR518, and FOR508 graduates looking to take their skills to the next level

The course focuses on smartphones as sources of evidence, providing students with the skills needed to handle mobile devices in a forensically sound manner, manipulate locked devices, understand the different technologies, discover malware, and analyze the results for use in digital investigations by diving deeper into the file systems of each smartphone. Students will be able to obtain actionable intelligence and recover and analyze data that commercial tools often miss for use in internal investigations, criminal and civil litigation, and security breach cases. Students will walk away with knowledge they can immediately put to use on their next smartphone investigation.

YOUR TEXTS AND APPS CAN AND WILL BE USED AGAINST YOU!

The hands-on exercises in this course cover the best commercial and open-source tools available to conduct smartphone and mobile device forensics, and provide detailed instructions on how to manually decode data that tools sometimes overlook. The course will prepare you to recover and reconstruct events relating to illegal or unauthorized activities, determine if a smartphone has been compromised with malware or spyware, and provide your organization with the capability to use evidence from smartphones.

This intensive six-day course will take your mobile device forensics knowledge and abilities to the next level. Smartphone technologies are constantly changing, and most forensics professionals are unfamiliar with the data formats. It is time for the good guys to get smarter and for the bad guys to know that their texts and apps can and will be used against them!

Heather Mahalik *SANS Certified Instructor*

Heather Mahalik is a project manager for Ocean's Edge, where she uses her experience to manage projects focused on wireless cybersecurity and mobile application development. Heather has over 12 years of experience in digital forensics, vulnerability discovery of mobile devices, application reverse engineering and manual decoding. She is currently the course lead for FOR585, Advanced Smartphone Forensics. Previously, Heather headed the mobile device team for Basis Technology, where she led the mobile device exploitation efforts in support of the U.S. government. She also worked as a forensic examiner at Stroz Friedberg and the U.S. State Department Computer Investigations and Forensics Lab, where she focused on high-profile cases. Heather co-authored Practical Mobile Forensics and various white papers, and has presented at leading conferences and instructed classes focused on Mac forensics, mobile device forensics, and computer forensics to practitioners in the field. Heather blogs and hosts work from the digital forensics community at www.smarterforensics.com. @HeatherMahalik

SANS@NIGHT EVENING TALKS

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.

Hunting Your Adversary – How to Operate and Leverage an Incident Response Hunt Team

Rob Lee

Over 80% of all breach victims learn of a compromise from third-party notifications, not from internal security teams. In most cases, adversaries have been rummaging through your network undetected for months or even years. Incident response tactics and procedures have evolved rapidly over the past several years. Data breaches and intrusions are growing more complex. Adversaries are no longer compromising one or two systems in your enterprise; they are compromising hundreds. To counter this, many incident response teams are either responding to incidents or hunting for the next ones. As a result, Incident Response Hunt teams have become a dedicated component to most modern SOCs. Incident response techniques that collect, classify, and exploit knowledge about these adversaries - collectively known as cyber threat intelligence – enable network defenders to establish a state of information superiority that decreases the adversary's likelihood of success with each subsequent intrusion attempt. Learn how IR/Hunt teams are formed, operate, best practices, and how they engage their targets across the enterprise. Learn how to hunt your adversaries or simply become another victim.

DLP FAIL!!! Using Encoding, Steganography, and Covert Channels to Evade DLP and Other Critical Controls

Kevin Fiscus

It's all about the information! Two decades after the movie Sneakers, the quote remains as relevant as ever. The fact that someone hacks into an environment is interesting but not that relevant. What is important is what happens after the compromise. If the data are destroyed or modified, organizations are negatively impacted but the benefits to an attacker for destruction or alteration are somewhat limited. Stealing information however, is highly profitable. Identity theft, espionage, and financial attacks involve the exfiltration of sensitive data. As a result, organizations deploy tools to detect and/or stop that data exfiltration. While these tools can be extremely valuable, many have serious weaknesses; attackers can encode, hide, or obfuscate the data, or can use secret communication channels. This session will talk about and demonstrate a range of these methods.

Bueller... Bueller... Smartphone Forensics Moves Fast: Stay Current or Miss Evidence

Heather Mahalik

How have smartphone OS upgrades to iOS 8 and Lollipop changed the game of forensics? The goal of this talk will be to cover new locations for data storage, how the tools stand up to the changes and how to manually recover data that the tools miss. We will look at residual data from older OSs on Android and iOS (because an upgrade doesn't delete the old data) and determine how the data can be parsed and decoded while staying within a limited budget.

IR Event Log Analysis

Hal Pomeranz

Windows event logs contain a bewildering variety of messages. But honing in on a few key events can quickly profile attacker activity. From administrator logins to scheduled tasks to entries related to system services, and more, the event logs are a one-stop shop. Learn to "crack the code" and enhance your investigations by adding event log analysis to your toolset.

Bust a Cap in a Web App with ZAP

Adrien de Beaupre

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

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

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

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

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

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

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

ONLINE TRAINING

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

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

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

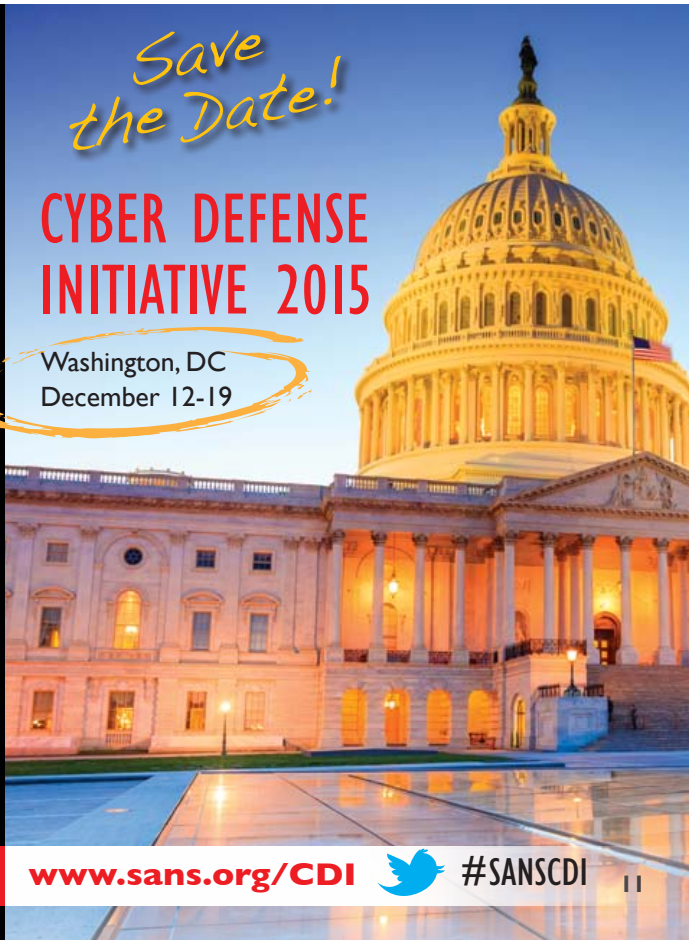
OnDemand Bundles sans.org/ondemand/bundles
Extend Your Training with an OnDemand Bundle Including Four Months of E-learning

SANS

CDI

Cyber Defense and Security Training

Over 25 hands-on immersion courses along with NetWars Tournaments



REGISTER AT www.sans.org/CDI #SANSCDI

FUTURE SANS TRAINING EVENTS

SANS Virginia Beach 2015
Virginia Beach, VA | August 24 - September 4 | #SANSVaBeach

SANS Chicago 2015
Chicago, IL | August 30 - September 4 | #SANSChicago

SANS Crystal City 2015
Crystal City, VA | September 8-13 | #SANSCrystalCity

SANS Network Security 2015
Las Vegas, NV | September 12-21 | #SANSNetworkSecurity

SANS Baltimore 2015
Baltimore, MD | September 21-26 | #SANSBaltimore

SANS Cyber Security Enforcement SUMMIT & TRAINING
Dallas, TX | September 21-26

SANS Seattle 2015
Seattle, WA | October 5-10 | #SANSSeattle

SANS Tysons Corner 2015
Tysons Corner, VA | October 12-17 | #SANSTysonsCorner

SANS Cyber Defense San Diego 2015
San Diego, CA | October 19-24 | #CyberDefSD

SANS Pen Test Hackfest SUMMIT & TRAINING
Alexandria, VA | November 16-23

SANS San Francisco 2015
San Francisco, CA | November 30 - December 5 | #SANS-SanFran

SANS Security Leadership SUMMIT & TRAINING
Dallas, TX | December 3-10

SANS Cyber Defense Initiative 2015
Washington, DC | December 12-19 | #SANSCDI

SANS Las Vegas 2016
Las Vegas, NV | January 9-14

SANS Security East 2016
New Orleans, LA | January 25-30

SANS 2016
Orlando, FL | March 12-21

SANS SOUTH FLORIDA 2015

Hotel Information

Training Campus
Riverside Hotel

620 East Las Olas Boulevard
Fort Lauderdale, FL 33301
954-467-0671
sans.org/event/south-florida-2015/location

Relax in the heart of downtown Fort Lauderdale, where world-class restaurants, hopping nightclubs and enchanting courtyards frame the city's only hotel on the trendy Las Olas Boulevard – the Riverside Hotel.

Special Hotel Rates Available

A special discounted rate of $159.00 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 October 16, 2015.

Top 5 reasons to stay at the Riverside Hotel

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

SANS SOUTH FLORIDA 2015

Registration Information

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

Register online at sans.org/event/south-florida-2015/courses

Select your course or courses and indicate whether you plan to test for GIAC certification.

If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with Internet access must complete the online registration form. We do not take registrations by phone.

Use code **EarlyBird15** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**9/16/15**	**$400.00**	**10/14/15**	**$200.00**

Some restrictions apply.

Group Savings (Applies to tuition only)

10% discount if 10 or more people from the same organization register at the same time
5% discount if 5-9 people from the same organization register at the same time

To obtain a group discount, complete the discount code request form at sans.org/security-training/discounts prior to registering.

Cancellation

You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by October 21, 2015 – processing fees may apply.

SANS Voucher Credit Program

Expand your training budget! Extend your Fiscal Year. The SANS Voucher Discount Program pays you credits and delivers flexibility. **sans.org/vouchers**


Open a
SANS Portal
Account
Sign up for a
SANS Portal
Account
and receive free
webcasts, newsletters,
the latest news and
updates, and many other
free resources.
sans.org/account