THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS NORTHERN VIRGINIA McLean 2016

McLean, VA February 15-20

Eight courses to choose from:

Security Essentials Bootcamp Style

Hacker Tools, Techniques, Exploits, and Incident Handling

Web App Penetration Testing and Ethical Hacking

Intrusion Detection In-Depth

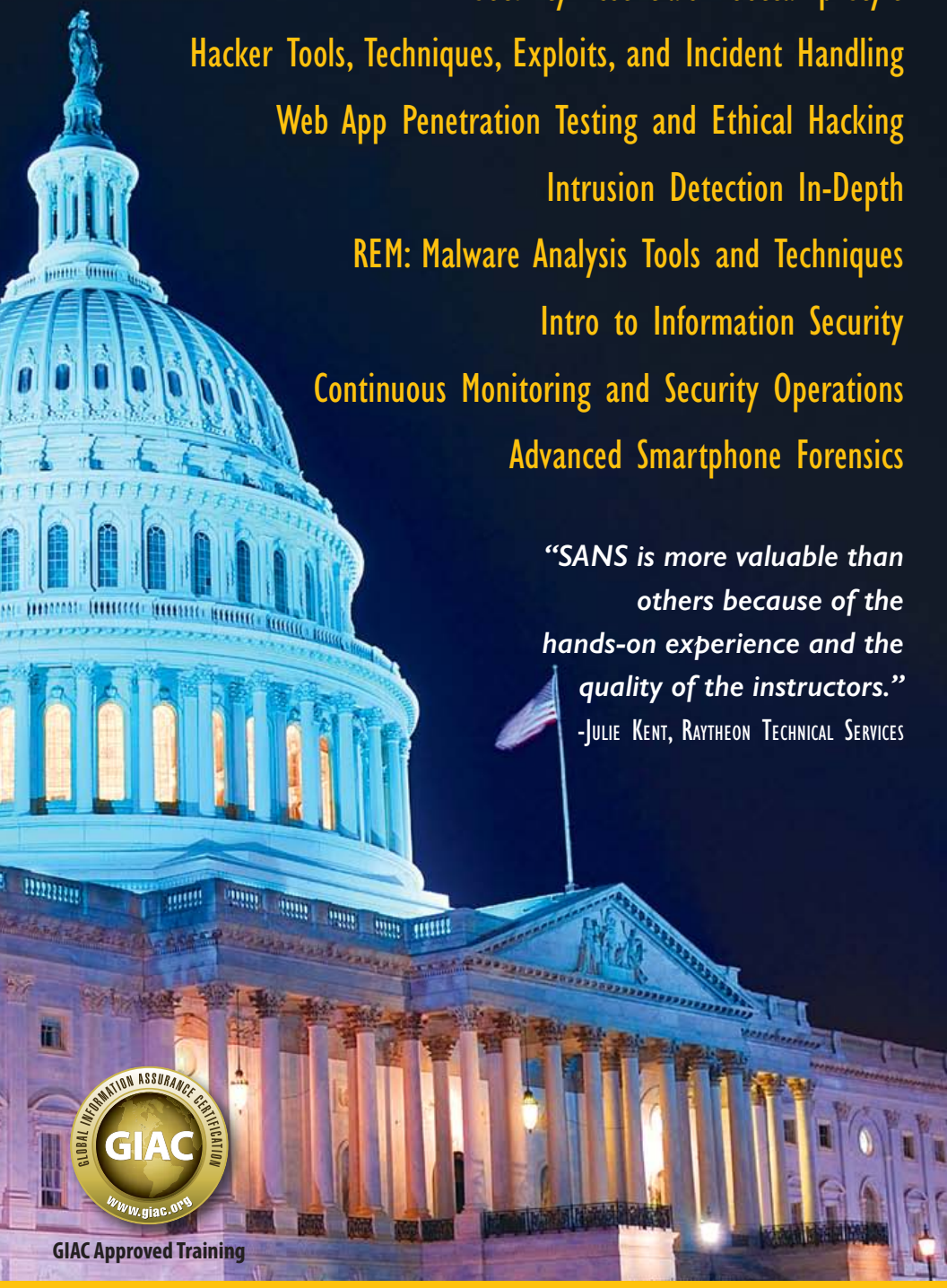
REM: Malware Analysis Tools and Techniques

Intro to Information Security

Continuous Monitoring and Security Operations

Advanced Smartphone Forensics

"SANS is more valuable than others because of the hands-on experience and the quality of the instructors."
-Julie Kent, Raytheon Technical Services



GIAC Approved Training

SAVE $400 on SANS Northern Virginia – McLean courses!

Register and pay by Dec 23rd – sans.org/mclean-2016

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 become SANS instructors. This guarantees what you learn in class will be up-to-date and relevant to your job. The SANS McLean 2016 line-up of instructors includes:

Dr. Eric Cole
Faculty Fellow

Jonathan Ham
Certified Instructor

Micah Hoffman
Certified Instructor

Cindy Murphy
Certified Instructor

Michael Murr
Principal Instructor

Keith Palmgren
Certified Instructor

Ismael Valenzuela
SANS Instructor

Lenny Zeltser
Senior Instructor

Evening Bonus Sessions

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

- KEYNOTE: ***Malware Analysis for Incident Responders: Getting Started*** – Lenny Zeltser
- ***Running Away from Security: Web App Vulnerabilities and OSINT Collide*** – Micah Hoffman
- ***Debunking the Complex Password Myth*** – Keith Palmgren
- ***The 14 Absolute Truths of Security*** – Keith Palmgren
- ***Hunting for Indicators of Compromise with Free Open-Source Tools (Practical Kung-Fu)*** – Ismael Valenzuela

Be sure to register and pay by Dec 23rd for a $400 tuition discount!

Courses-at-a-Glance

	MON 2-15	TUE 2-16	WED 2-17	THU 2-18	FRI 2-19	SAT 2-20	
SEC301 **Intro to Information Security**							Page 1
SEC401 **Security Essentials Bootcamp Style**							Page 2
SEC503 **Intrusion Detection In-Depth**							Page 3
SEC504 **Hacker Tools, Techniques, Exploits, and Incident Handling**							Page 4
SEC511 **Continuous Monitoring and Security Operations**							Page 5
SEC542 **Web App Penetration Testing and Ethical Hacking**							Page 6
FOR585 **Advanced Smartphone Forensics**							Page 7
FOR610 **Reverse-Engineering Malware: Malware Analysis Tools and Techniques**							Page 8

SEC301:

Intro to Information Security

SANS

Five-Day Program
Mon, Feb 15 - Fri, Feb 19
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Keith Palmgren
- GIAC Cert: GISF
- OnDemand Bundle

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

- Are you 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 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: Introduction 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 no prior knowledge of security and limited knowledge of technology. 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**. 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!***

giac.org

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

"This was my first attendance to a SANS course and I didn't know what to expect, but I was quite impressed and it exceeded my expectations. I loved the books provided for us to add additional notes.
-Erica Johnson, Zebra Technologies

"SEC301 gave me a much broader understanding of security threats, terminology, processes and help resources."
-John Wyatt, Kohler Co.

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

SEC401:
Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Feb 15 - Sat, Feb 20
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Dr. Eric Cole

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

Who Should Attend

- Security professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Operations personnel who do not have security as their primary job function but need an understanding of security to be effective
- IT engineers and supervisors who need to know how to build a defensible network against attacks

"SEC401 was probably one of the most interesting courses I've taken, and it's giving me a different perspective on the topic of security that will help me at my workplace to make better decisions."
-Pablo Delgado, EOG Resources

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

Dr. Eric Cole *SANS Faculty Fellow*

Dr. Cole is an industry-recognized security expert with over 20 years of hands-on experience. He currently performs leading-edge security consulting and works in research and development to advance the state of the art in information systems security. Dr. Cole has experience in information technology with a focus on perimeter defense, secure network design, vulnerability discovery, penetration testing, and intrusion detection systems. He has a master's degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. Dr. Cole is the author of several books, including *Hackers Beware*, *Hiding in Plain Site*, *Network Security Bible*, and *Insider Threat*. He is the inventor of over 20 patents and is a researcher, writer, and speaker. He is also a member of the Commission on Cybersecurity for the 44th President and several executive advisory boards. Dr. Cole is founder of Secure Anchor Consulting, where he provides state-of-the-art security services and expert witness work. He also served as CTO of McAfee and Chief Scientist for Lockheed Martin. Dr. Cole is actively involved with the SANS Technology Institute (STI) and SANS, working with students, teaching, and maintaining and developing courseware. @drericcole

SEC503:
Intrusion Detection In-Depth

SANS

Six-Day Program
Mon, Feb 15 - Sat, Feb 20
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jonathan Ham

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

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?

Who Should Attend

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

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 HTTP, so that you can intelligently examine network traffic for signs of an intrusion. You will get plenty of practice learning to configure and master different open-source tools like tcpdump, Wireshark, Snort, Bro, and many more. 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. In addition, most exercises include an "extra credit" stumper question intended to challenge even the most advanced student.

Industry expert Mike Poor has created a VMware distribution, Packetrix, specifically for this course. As the name implies, Packetrix contains many of the tricks of the trade to perform packet and traffic analysis. It is supplemented with demonstration "pcaps," which are files that contain network traffic. This allows students to follow along on their laptops with the class material and demonstrations. The pcaps also provide a good library of network traffic to use when reviewing the material, especially for certification.

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 often 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. The training will prepare you to put your new skills and knowledge to work immediately upon returning to a live environment.

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

"This course was very informative and taught me how to analyze packets and network trafficking at a level I have never been."
-Josh Sutfin, Defense Point Security

"Excellent exposure and training for all skill levels. Thanks for the in-depth analysis combined with real-life scenarios."
-Art Mason, Rackspace ISOC

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 12 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:

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Mon, Feb 15 - Sat, Feb 20
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Michael Murr

- 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 training has raised my awareness on how malicious attackers may attempt to attack systems and how they can be identified, contained, eradicated, and recovered."
-Joseph L., DoD

"The instructor's passion for this topic has influenced me to pursue this area further and to increase my skills. This has been a great experience and the labs were immensely important."
-Stephen M., Army National Guard

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. It 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

Michael Murr *SANS Principal Instructor*

Michael has been a forensic analyst with Code-X Technologies for over five years, has conducted numerous investigations and computer forensic examinations, and has performed specialized research and development. Michael has taught SEC504: Hacker Tools, Techniques, Exploits and Incident Handling; FOR508: Advanced Digital Forensics and Incident Response; and FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques. He has also led SANS@Home courses and is a member of the GIAC Advisory Board. Currently, Michael is working on an open-source framework for developing digital forensics applications. Michael holds the GCIH, GCFA, and GREM certifications and has a degree in computer science from California State University at Channel Islands. Michael also blogs about digital forensics on his forensic computing blog (www.forensicblog.org). @mikemurr

SEC511:
Continuous Monitoring and Security Operations

SANS

Six-Day Program
Mon, Feb 15 - Sat, Feb 20
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Ismael Valenzuela

- GIAC Cert: GMON
- Master's Program
- OnDemand Bundle

We continue to underestimate the tenacity of our adversaries! Organizations are investing a significant amount of time and financial and human resources trying to combat cyber threats and prevent cyber attacks, but despite this tremendous effort organizations are still getting compromised. The traditional perimeter-focused, prevention-dominant approach to security architecture has failed to prevent intrusions. No network is impenetrable, a reality that business executives and security professionals alike have to accept. Prevention is crucial, and we can't lose sight of it as the primary goal. However, a new proactive approach to security is needed to enhance the capabilities of organizations to detect threats that will inevitably slip through their defenses.

Who Should Attend

- Security architects
- Senior security engineers
- Technical security managers
- Security Operations Center (SOC) analysts
- SOC engineers
- SOC managers
- CND analysts
- Individuals working to implement Continuous Diagnostics and Mitigation (CDM), Continuous Security Monitoring (CSM), or Network Security Monitoring (NSM)

"I have so much to bring back to the office from this training, and I am excited to share my findings with my team and manager."
-Stacey Boivin, Alberta Electric System Operator

"SEC511 is a practical approach to continue security monitoring using free and open-source tools either alone or in conjunction with existing tools and devices. This course is a must for anyone responsible for monitoring networks for security."
-Brad Milhorn, CompuCom

The underlying challenge for organizations victimized by an attack is timely incident detection. Industry data suggest that most security breaches typically go undiscovered for an average of seven months. Attackers simply have to find one way into most organizations, because they know that the lack of visibility and internal security controls will then allow them to methodically carry out their mission and achieve their goals.

The Defensible Security Architecture, Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Security Monitoring (CSM) taught in this course will best position your organization or Security Operations Center to analyze threats and detect anomalies that could indicate cybercriminal behavior. The payoff for this new proactive approach is early detection of an intrusion, or successfully thwarting the efforts of attackers altogether. The National Institute of Standards and Technology (NIST) developed guidelines described in NIST SP 800-137 for Continuous Monitoring (CM), and this course will greatly increase your understanding and enhance your skills in implementing CM utilizing the NIST framework.

GIAC CERTIFIED MONITORING CERTIFICATION
GMON
giac.org

SANS Technology Institute
sans.edu

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

Ismael Valenzuela *SANS Instructor*

Since he founded one of the first IT Security consultancies in Spain, Ismael Valenzuela has participated as a security professional in numerous projects across the globe in the last 15 years. He currently works as IR/Forensics Technical Practice Manager at Intel Security in North America. Prior to joining Intel, Ismael worked as Global IT Security Manager for iSOFT Group Ltd, one of the world's largest providers of healthcare IT solutions. The author of security articles for Hakin9, INSECURE Magazine and the SANS Forensics Blog, Ismael also has experience teaching at BlackHat, serves on the GIAC Advisory Board and is a Community SANS Instructor for the Computer Forensics, Intrusion Detection and Continuous Monitoring tracks. He holds a bachelor's degree in computer science from the University of Malaga (Spain), is certified in Business Administration, and holds numerous professional certifications including GREM, GCFA, GCIA, GCIH, GPEN, GCUX, GCWN, GWAPT, GSNA, CISSP, ITIL, CISM, and IRCA 27001. He is the lead auditor for Bureau Veritas. Some of his articles are freely available at http://blog.ismaelvalenzuela.com. @aboutsecurity

SEC542:
Web App Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Mon, Feb 15 - Sat, Feb 20
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Micah Hoffman

- 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, and 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.

"Excellent resources for defense! The attackers' perspectives are realistic and the real-world scenarios are relevant." -Nathan P., USAF

"The instructor's knowledge gave me a better perspective on the development process, and helped peel back the onion on infrastructure and environments. This has taught me how to think outside of the box." -Ephraim P., USAF

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.

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.

GWAPT
giac.org

SANS Technology Institute
sans.edu

sans.org/cyber-guardian

Bundle OnDemand
with this course
sans.org/ondemand

Micah Hoffman *SANS Certified Instructor*

Micah Hoffman has been working in the information technology field since 1998, supporting federal government, commercial, and internal customers in their efforts to discover and quantify information security weaknesses within their organizations. He leverages years of hands-on, real-world penetration testing and incident response experience to provide excellent solutions to his customers. Micah holds the GAWN, GWAPT, and GPEN certifications as well as the CISSP Micah is an active member of the NoVAHackers community, writes Recon-ng modules and enjoys tackling issues with the Python scripting language. When not working, teaching, or learning, Micah can be found hiking or backpacking on the Appalachian Trail or the many park trails in Maryland. @WebBreacher

FOR585:
Advanced Smartphone Forensics

SANS

Six-Day Program
Mon, Feb 15 - Sat, Feb 20
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Cindy Murphy
- OnDemand Bundle

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.

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

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.

DFIR
digital-forensics.sans.org

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

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!

Cindy Murphy *SANS Certified Instructor*

Cindy Murphy is a detective with the City of Madison, WI Police Department and has been a law enforcement officer since 1985. She is a certified forensic examiner and has been involved in computer forensics since 1999. Det. Murphy has directly participated in the examination of hundreds of hard drives, cell phones, and other items of digital evidence pursuant to criminal investigations, including financial crimes, homicides, missing persons, computer intrusions, sexual assaults, child pornography, and various other crimes. She has testified as a computer forensics expert in state and federal courts on numerous occasions, using her knowledge and skills to assist in the successful investigation and prosecution of criminal cases involving digital evidence. She also helped to develop the digital forensics certificate program at Madison Area Technical College. She has presented internationally on various digital forensics topics and frequently writes articles and whitepapers on various forensics-related topics. Det. Murphy earned her MSc in Forensic Computing and Cyber Crime Investigation at University College, Dublin, where she completed her dissertation on victim age estimation from child exploitation images. She is also involved with the Wisconsin Association of Computer Crimes Investigators (WACCI) where served as past president of the WACCI West Chapter, and she has also been involved with Chicago Electronic Crimes Task Force, High Tech Crime Consortium (HTCC), High Tech Crime Network (HTCN), and the International Guild of Knot Tyers (IGKT). @cindymurph

FOR610:

Reverse-Engineering Malware: Malware Analysis Tools and Techniques

SANS

Six-Day Program
Mon, Feb 15 - Sat, Feb 20
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Lenny Zeltser

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

DFIR
digital-forensics.sans.org

Who Should Attend

- Individuals who have dealt with incidents involving malware and want to learn how to understand key aspects of malicious programs
- Technologists who have informally experimented with aspects of malware analysis prior to the course and are looking to formalize and expand their expertise in this area
- Forensic investigators and IT practitioners looking to expand their skillsets and learn how to play a pivotal role in the incident response process

"FOR610 is the best course in the the industry for performing malware analysis. The instructors are the top experts in their field."
-David Bernal, Alstom

This popular course explores malware analysis tools and techniques in depth. FOR610 training has helped forensic investigators, incident responders, security engineers, and IT administrators acquire the practical skills to examine malicious programs that target and infect Windows systems. Understanding the capabilities of malware is critical to an organization's ability to derive threat intelligence, respond to information security incidents, and fortify defenses. This course builds a strong foundation for reverse-engineering malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and other tools useful for turning malware inside-out.

The course begins by covering fundamental aspects of malware analysis. You will learn how to set up an inexpensive and flexible laboratory to examine the inner workings of malicious software, and how to use the lab to uncover characteristics of real-world malware samples. Then you will learn to examine the specimens' behavioral patterns and code. The course continues by discussing essential x86 assembly language concepts. You will examine malicious code to understand its key components and execution flow. In addition, you will learn to identify common malware characteristics by looking at suspicious Windows API patterns employed by bots, rootkits, keyloggers, downloaders, and other types of malware.

You will also learn how to handle self-defending malware, bypassing the protection offered by packers, and other anti-analysis methods. In addition, given the frequent use of browser malware for targeting systems, you will learn practical approaches to analyzing malicious browser scripts, de-obfuscating JavaScript and VBScript to understand the nature of the attack.

You will learn how to analyze malicious documents that take the form of Microsoft Office and Adobe PDF files. Such documents act as a common infection vector and may need to be examined when dealing with large-scale infections as well as targeted attacks. The course also explores memory forensics approaches to examining malicious software, especially useful if the software exhibits rootkit characteristics.

The course culminates with a series of capture-the-flag-style challenges designed to reinforce the techniques learned in class and provide additional opportunities to learn practical, hands-on malware analysis skills in a fun setting.

Hands-on workshop exercises are a critical aspect of this course and allow you to apply malware analysis techniques by examining malware in a lab that you control. When performing the exercises, you will study the supplied specimens' behavioral patterns and examine key portions of their code. To support these activities, you will receive pre-built Windows and Linux virtual machines that include tools for examining and interacting with malware.

GIAC REVERSE ENGINEERING MALWARE
GREM
giac.org

SANS Technology Institute
sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

Lenny Zeltser *SANS Senior Instructor*

Lenny Zeltser is a seasoned business and tech leader with extensive experience in information technology and security. As a product management director at NCR Corp, he heads the software and services group that address customers' data protection needs. Before NCR, Lenny led the enterprise security consulting practice at a major cloud services provider. He also trains professionals in digital forensics and malware combat at SANS Institute. In addition, Lenny is a Board of Directors member at SANS Technology Institute. Lenny's expertise is strongest at the intersection of business, technology, and information security and includes incident response, cloud services, and product management. He frequently speaks at conferences, writes articles, and has co-authored books on network security and malicious software. Lenny has an MBA degree from MIT Sloan, a Computer Science degree from the University of Pennsylvania and has earned the prestigious GIAC Security Expert designation from SANS Institute. Visit www.zeltser.com to learn about his projects and interests. @lennyzeltser

BONUS SESSIONS – 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.

KEYNOTE: Malware Analysis for Incident Responders: Getting Started *Lenny Zeltser*

Knowing how to analyze malware has become a critical skill for incident responders and forensic investigators. A good way to get started with such efforts involves examining how malicious software behaves in a controlled laboratory environment. In this two-hour briefing, Lenny Zeltser demonstrates key aspects of this process, walking you through behavioral analysis of a malware specimen by using several free tools and even peeking into the world of code analysis. You will see practical techniques in action and understand how malware analysis will help you to triage the incident to assess key capabilities of the malicious software. You will also learn how to determine ways of identifying this malware on systems in your environment by establishing indicators of compromise. This seminar will help you start learning how to turn malware inside out.

Running Away from Security: Web App Vulnerabilities and OSINT Collide *Micah Hoffman*

Lately it seems like more and more of our lives are being sucked into the computer world. There are wrist-sensors for tracking our steps, phone apps that plot our workouts on maps, and sites to share our healthy-eating and weight-loss progress. When people sign up for these sites, they usually use pseudonyms or the sites give them a unique numbered ID to keep their information "private." How hard would it be to connect a person's step-counting, diet history, and other info on these health sites to their real lives? Are businesses using these sites for non-fitness purposes? This talk will show weaknesses in several web applications used for health and exercise tracking and reveal [spoiler alert] how trivial it is to find the real people behind the "private" accounts.

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.

The 14 Absolute Truths of Security *Keith Palmgren*

Keith Palmgren has identified 14 "Absolute Truths" of security – things that remain true regardless of circumstance, network topology, organizational type, or any other variable. Recognizing these 14 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 14 absolute truths in turn and examine what they mean to the security manager and the security posture, and how understanding them will lead to a successful security program.

Hunting for Indicators of Compromise with Free Open-Source Tools (Practical Kung-Fu) *Ismael Valenzuela*

In this talk, Ismael Valenzuela will explain the methods and techniques used by world-class incident response teams to leverage the power of open-source tools like Yara and Bro to do IOC hunting during continuous monitoring or when reacting to emergency incidents.

Build Your Best Career

WITH

SANS

Add an

OnDemand Bundle & GIAC Certification Attempt*

to your course within seven days of this event for just $659 each.

SPECIAL PRICING

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.

GIAC Certification

- Distinguish yourself as an information security leader
- 30+ GIAC certifications to choose from
- 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

**OnDemand Bundles and GIAC certifications are not available for all courses*

OTHER SANS TRAINING EVENTS

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

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

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

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

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

SANS Cyber Threat Intelligence SUMMIT & TRAINING
Alexandria, VA | February 3-10

SANS Scottsdale 2016
Scottsdale, AZ | February 8-13

ICS Security SUMMIT & TRAINING
Orlando, FL | February 16-23

SANS Anaheim 2016
Anaheim, CA | February 22-27

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 McLEAN 2016

Hotel Information

Training Campus

Hilton McLean Tysons Corner

7920 Jones Branch Drive
McLean, VA 22102
703-847-5000
sans.org/event/mclean-2016/location

Experience impeccable service at the Hilton McLean Tysons Corner hotel near Washington, DC. This contemporary hotel is located in the center of Tysons Corner's technology corridor, between Ronald Reagan National Airport and Washington Dulles International Airport. It is also just minutes from world-class shopping at Tysons Corner Center and the Galleria Mall. Take the Silver Line Metro from the McLean Station into downtown Washington, DC. A complimentary shuttle servicing a one-mile radius of the hotel is also provided.

Special Hotel Rates Available

A special discounted rate of $184.00 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 Jan. 25, 2016.

Top 5 reasons to stay at the Hilton McLean Tysons Corner

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 Hilton McLean Tysons Corner, 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 Hilton McLean Tysons Corner that you won't want to miss!
5. Everything is in one convenient location!

SANS McLEAN 2016

Registration Information

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

Register online at sans.org/event/mclean-2016/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 **EarlyBird16** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**12-23-15**	**$400.00**	**1-13-16**	**$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 January 27, 2016 – 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** 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 FAQ
- Tip of the Day
- Security Posters
- Thought Leaders
- 20 Coolest Careers
- Security Glossary
- SCORE (Security Consensus Operational Readiness Evaluation)

sans.org/security-resources