

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

SANS **Baltimore Spring 2017**

April 24-29

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

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

Nine courses in:

CYBER DEFENSE
DETECTION & MONITORING
PENETRATION TESTING
INCIDENT RESPONSE

DIGITAL FORENSICS
ETHICAL HACKING
MANAGEMENT



GIAC-Approved Training

“SANS training is the most comprehensive
information security training I’ve taken
in my 21 years of IT professional experience.”

-MARCUS M., U.S. AIR FORCE

**SAVE
\$400**

Register and pay by
March 1st — Use code
EarlyBird17

www.sans.org/baltimore-spring

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 Baltimore Spring 2017 lineup of instructors includes:



Kevin Fiscus
Certified Instructor
@kevinbfiscus



Bryce Galbraith
Principal Instructor
@brycegalbraith



Jonathan Ham
Certified Instructor
@jhamcorp



Moses Hernandez
Instructor
@mosesrenegade



David Hoelzer
Faculty Fellow
@it_audit



Bryan Simon
Certified Instructor
@BryanOnSecurity



Stephen Sims
Senior Instructor
@Steph3nSims



Ismael Valenzuela
Instructor
@aboutsecurity



Eric Zimmerman
Instructor
@EricZimmerman

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 10.

KEYNOTE: *Exploitation 101: Stacks, NX/DEP, ASLR, and ROP!* – David Hoelzer

Steganography: The Hidden Threat – Kevin Fiscus

(Am)Cache Rules Everything Around Me – Eric Zimmerman

The Node Situation – Moses Hernandez

Save \$400 when you register and pay by March 1st using code *EarlyBird17*

Courses at a Glance

	MON 4-24	TUE 4-25	WED 4-26	THU 4-27	FRI 4-28	SAT 4-29
SEC401 Security Essentials Bootcamp Style	Page 1					
SEC503 Intrusion Detection In-Depth	Page 2					
SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	Page 3					
SEC511 Continuous Monitoring and Security Operations	Page 4					
SEC542 Web App Penetration Testing and Ethical Hacking	Page 5					
SEC560 Network Penetration Testing and Ethical Hacking	Page 6					
SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	Page 7					
FOR508 Advanced Digital Forensics, Incident Response, and Threat Hunting	Page 8					
MGT512 SANS Security Leadership Essentials for Managers with Knowledge Compression™	Page 9					

Register today for SANS Baltimore Spring 2017!
www.sans.org/baltimore-spring



@SANSInstitute
Join the conversation:
#SANSBaltimore

SEC401:

Security Essentials Bootcamp Style

Six-Day Program

Mon, Apr 24 - Sat, Apr 29

9:00am - 7:00pm (Days 1-5)

9:00am - 5:00pm (Day 6)

46 CPEs

Laptop Required

Instructor: Bryan Simon


www.giac.org/gsec

www.sans.edu

www.sans.org/8140

**BUNDLE
ONDEMAND**

WITH THIS COURSE

www.sans.org/ondemand

“I have been armed with so much knowledge that I can now go back and have the right conversations to move towards a more secure environment.”

-JASON BLAY,

BECKMAN COULTER, INC.

This course will teach you the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. You'll 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*!

With the rise of 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'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.

PREVENTION IS IDEAL BUT DETECTION IS A MUST.



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 instructed individuals from organizations such as the FBI, NATO, and the UN in matters of cybersecurity, on two continents. 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 12 GIAC certifications including GSEC, GCWN, GCIH, GCEA, GPEN, GWAPT, GAWN, GISP, GCIA, GCED, GCUX, and GISF. Bryan's scholastic achievements have resulted in the honor of sitting 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

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

SEC503:

Intrusion Detection In-Depth

Six-Day Program

Mon, Apr 24 - Sat, Apr 29

9:00am - 5:00pm

36 CPEs

Laptop Required

Instructor: Jonathan Ham



www.giac.org/gcia



www.sans.edu



www.sans.org/cyber-guardian



www.sans.org/8140



**BUNDLE
ONDEMAND**

WITH THIS COURSE

www.sans.org/ondemand

"This course allows analysts to not only understand what to look for in packets, but why they are doing so."

-KATIE KELLEY,
GREAT RIVER ENERGY

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 (all levels), system, and security analysts
- ▶ Network engineers/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.

"It is invaluable to get real-world examples from professionals currently working in this field as well as teaching it." -MIKE HEYMANN, EOG RESOURCES

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.



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 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](https://twitter.com/jhamcorp)

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

Six-Day Program

Mon, Apr 24 - Sat, Apr 29

9:00am - 7:15pm (Day 1)

9:00am - 5:00pm (Days 2-6)

37 CPEs

Laptop Required

Instructor: Kevin Fiscus


www.giac.org/gcih

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

**BUNDLE
ONDEMAND**

WITH THIS COURSE

www.sans.org/ondemand

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.**

“Great instruction! SEC504 covered topics very thoroughly and gave great examples.”

-KEVIN H., U.S. DEPARTMENT OF HOMELAND SECURITY

This course enables you to turn the tables on computer attackers by helping you to 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 attacks. 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, 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.**

“This was a valuable course and will benefit me in the aspect of explaining the pieces attackers follow to gain access to system networks and the practices to mitigate these attacks.” - DEREK S., U.S. AIR FORCE



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 for the past 12 years on information security. Kevin 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. @kevinbfiscus

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

SEC511:

Continuous Monitoring and Security Operations

New Extended Bootcamp Hours to Enhance Your Skills

SANS

Six-Day Program
Mon, Apr 24 - Sat, Apr 29
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Laptop Required
Instructor: Ismael Valenzuela



www.giac.org/gmon



www.sans.edu

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

“This course had great lessons that will be actionable to what I do day to day, and it will help me fill in the gaps at my current work environment.”
-KEVIN SOUTH,
NAVIENT CORPORATION

We continue to underestimate the tenacity of our adversaries! Organizations are investing a significant amount of time and financial and human resources trying to prevent and combat 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.

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.

“Outstanding content and instructor.”

-AL FOSTER, U.S. DEPARTMENT OF THE INTERIOR

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 (SOC) 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.

Who Should Attend

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



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 over the past 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. He holds a bachelor's degree in computer science from the University of Malaga (Spain), is certified in business administration, and holds many professional certifications. These include the highly regarded GIAC Security Expert (GSE #132) in addition to GREM, GCFA, GCIA, GCIH, GPEN, GCUX, GCWN, GWAPT, GSNA, CISSP, ITIL, CISM, and IRCA 27001 Lead Auditor from Bureau Veritas UK. Some of his articles are freely available at <http://blog.ismaelvalenzuela.com>. @aboutsecurity

SEC 542:

Web App Penetration Testing and Ethical Hacking

Six-Day Program

Mon, Apr 24 - Sat, Apr 29

9:00am - 5:00pm

36 CPEs

Laptop Required

Instructor: Moses Hernandez


www.giac.org/gwapt

www.sans.edu

www.sans.org/cyber-guardian

**BUNDLE
ONDEMAND**

WITH THIS COURSE

www.sans.org/ondemand

"This course shows a hands-on way of doing web app testing and not just how to use this tool or that."

-CHRISTOPHER J. STOVER,
INFOGRESSIVE INC.



Moses Hernandez SANS Instructor

Moses Hernandez is a seasoned security professional with over 15 years in the IT industry. He has held positions as a network engineer, network architect, security architect, platform engineer, site reliability engineer, and consulting sales engineer. He has a background in complex network systems, systems administration, forensics, penetration testing, and development. He has worked with some of the largest companies in the nation as well as fast-growing, bootstrap startups. Moses has developed information security regimens safeguarding some of the most sensitive personal data in the nation. He creates custom security software to find and mitigate unknown threats, and works on continually evolving his penetration testing skills. He enjoys building software, networks, systems, and working with business-minded individuals. Moses's current passions include offensive forensics, building secure systems, finance, economics, history, and music. [@mosesrengade](https://twitter.com/mosesrengade)

Web applications play a vital role in every modern organization. But if your organization does not 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.

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, and 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.

"This training boosted my thoughts and perspective on IT and has taught me how to think outside of the box." -EPHRAIM P., U.S. AIR FORCE

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.

In this course, students will come to understand major web application flaws and their exploitation. Most importantly, they'll 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. This course will help you demonstrate the true impact of web application flaws through exploitation.

In addition to having more than 30 formal hands-on labs, the course culminates in a web application pen test tournament, powered by the SANS NetWars Cyber Range. **This Capture-the-Flag event on the final day brings students into teams to apply their newly acquired command of web application penetration testing techniques in a fun way that hammers home lessons learned.**

Who Should Attend

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

SEC560:

Network Penetration Testing and Ethical Hacking

Six-Day Program

Mon, Apr 24 - Sat, Apr 29

9:00am - 7:15pm (Day 1)

9:00am - 5:00pm (Days 2-6)

37 CPEs

Laptop Required

Instructor: Bryce Galbraith


www.giac.org/gpen

www.sans.edu

www.sans.org/cyber-guardian

**BUNDLE
ONDEMAND**

WITH THIS COURSE

www.sans.org/ondemand

"My continuing education in cyber offensive/defensive techniques is essential and this has been the most valuable training I've had in a while. The instructor was excellent and explained all the concepts so even a cave man could understand."

-DONALD A. U.S. AIR FORCE



Bryce Galbraith SANS Principal Instructor

As a contributing author of the international bestseller *Hacking Exposed: Network Security Secrets & Solutions*, Bryce helped bring the secret world of hacking out of the darkness and into the public eye. He has held security positions at global ISPs and Fortune 500 companies, was a member of Foundstone's renowned penetration testing team, and served as a senior instructor and co-author of Foundstone's Ultimate Hacking: Hands-On course series. Bryce is currently the owner of Layered Security, where he provides specialized vulnerability assessment and penetration testing services for clients. He teaches several of the SANS Institute's most popular courses and develops curriculum around current topics. He has taught the art of ethical hacking and countermeasures to thousands of IT professionals from a who's who of top companies, financial institutions, and government agencies around the globe. Bryce is an active member of several security-related organizations, holds several security certifications, and speaks at conferences worldwide. @brycegalbraith

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.

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 **over 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.

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 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.

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

SEC660:

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Six-Day Program

Mon, Apr 24 - Sat, Apr 29

9:00am - 7:00pm (Days 1-5)

9:00am - 5:00pm (Day 6)

46 CPEs

Laptop Required

Instructor: Stephen Sims



www.giac.org/gxpn



www.sans.edu



www.sans.org/cyber-guardian



**BUNDLE
ONDEMAND**

WITH THIS COURSE

www.sans.org/ondemand

"SEC660 gave me the background and tools that I'll need to go deeper!"

-KRISTINE A.,

U.S. DEPARTMENT OF DEFENSE



Stephen Sims SANS Senior Instructor

Stephen Sims is an industry expert with over 15 years of experience in information technology and security. Stephen currently works out of San Francisco as a consultant performing reverse engineering, exploit development, threat modeling, and penetration testing. Stephen has a master's of science degree in information assurance from Norwich University. He is the author of SANS' only 700-level course, SEC760: Advanced Exploit Development for Penetration Testers, which concentrates on complex heap overflows, patch diffing, and client-side exploits. Stephen is also the lead author of SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking. He holds the GIAC Security Expert (GSE) certification as well as the CISSP, CISA, Immunity NOP, and many other certifications. In his spare time, Stephen enjoys snowboarding and writing music. @Steph3nSims

SANS

This course is designed as a logical progression point for those who have completed **SEC560: Network Penetration Testing and Ethical Hacking**, or for those with existing penetration testing experience.

Students with the prerequisite knowledge to take this course will walk through dozens of real-world attacks used by the most seasoned penetration testers. The methodology of a given attack is discussed, followed by exercises in a real-world lab environment to solidify advanced concepts and allow for the immediate application of techniques in the workplace. **Each day includes a two-hour evening bootcamp to allow for additional mastery of the techniques discussed and even more hands-on exercises.**

A sample of topics covered includes weaponizing Python for penetration testers, attacks against network access control (NAC) and VLAN manipulation, network device exploitation, breaking out of Linux and Windows restricted environments, IPv6, Linux privilege escalation and exploit-writing, testing cryptographic implementations, fuzzing, defeating modern OS controls such as ASLR and DEP, return-oriented programming (ROP), Windows exploit-writing, and much more!

"SEC660 has been nothing less than excellent. Both the instructor and assistant are subject-matter experts who have extensive knowledge covering all aspects of the topics covered and then some." -BRIAN ANDERSON, NORTHROP GRUMMAN CORPORATION

Attackers are becoming more clever and their attacks more complex. In order to keep up with the latest attack methods, you need a strong desire to learn, the support of others, and the opportunity to practice and build experience. **SEC660 provides attendees with in-depth knowledge of the most prominent and powerful attack vectors and an environment to perform these attacks in numerous hands-on scenarios.** This course goes far beyond simple scanning for low-hanging fruit, and shows penetration testers how to model the abilities of an advanced attacker to find significant flaws in a target environment and demonstrate the business risk associated with these flaws.

"No frills and goes right to the point. The first day alone is what other classes spend a full week on." -MICHAEL ISBITSKI, VERIZON WIRELESS

Who Should Attend

- ▶ Network and systems penetration testers
- ▶ Incident handlers
- ▶ Application developers
- ▶ IDS engineers

FOR508:

Advanced Digital Forensics, Incident Response, and Threat Hunting

Six-Day Program

Mon, Apr 24 - Sat, Apr 29

9:00am - 5:00pm

36 CPEs

Laptop Required

Instructor: Eric Zimmerman



www.giac.org/gcfa



www.sans.edu



www.sans.org/cyber-guardian



www.sans.org/8140



**BUNDLE
ONDEMAND**

WITH THIS COURSE

www.sans.org/ondemand



Eric Zimmerman SANS Instructor

As a former Special Agent with the FBI, one of Eric's responsibilities was managing on-scene triage. He identified several gaps in an existing process and started creating solutions to address them. What began as building and expanding a few live response tools took Eric down a path that eventually led to him writing more than 50 programs that are now used by nearly 8,800 law enforcement officers in over 80 countries. Much of Eric's work involved designing and building software related to investigations of sexual abuse of children. In a single year, Eric's programs led to the rescue of hundreds of these children. As a result, in May 2012, Eric's was given a National Center for Missing and Exploited Children's Award, which honors outstanding law enforcement professionals who have performed above and beyond the call of duty. Eric was also presented with the U.S. Attorney Award for Excellence in Law Enforcement in 2013. Today, Eric serves as a Senior Director at Kroll in the company's cybersecurity and investigations practice. Eric's teaching philosophy focuses on the long-term gains achieved by not only understanding the nuts and bolts of how to run a tool and consume output, but also getting a deeper understanding of how tools work "under the hood." His focus on understating the big picture of digital forensics prepares students to perform better analysis, do new research of their own, and identify the best tools or techniques to perform successful investigations — all skills that will have a lifelong impact. [@EricZimmerman](#)

FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting will help you:

- > Detect how and when a breach occurred
- > Identify compromised and affected systems
- > Determine what attackers took or changed
- > Contain and remediate incidents
- > Develop key sources of threat intelligence
- > Hunt down additional breaches using knowledge of the adversary

DAY 0: A 3-letter government agency contacts you to say an advanced threat group is targeting organizations like yours, and that your organization is likely a target. They won't tell how they know, but they suspect that there are already several breached systems within your enterprise. An advanced persistent threat, aka an APT, is likely involved. This is the most sophisticated threat that you are likely to face in your efforts to defend your systems and data, and these adversaries may have been actively rummaging through your network undetected for months or even years.

This is a hypothetical situation, but the chances are very high that hidden threats already exist inside your organization's networks. Organizations can't afford to believe that their security measures are perfect and impenetrable, no matter how thorough their security precautions might be. Prevention systems alone are insufficient to counter focused human adversaries who know how to get around most security and monitoring tools. The key is to catch intrusions in progress, rather than after attackers have completed their objectives and done worse damage to the organization. For the incident responder, this process is known as "threat hunting."

"For me, the best information for take-aways is the tactics and information behind the analysis." -DEREK B., U.S. AIR FORCE

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

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

Who Should Attend

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

MGT512:

SANS Security Leadership Essentials for Managers with Knowledge Compression™

Five-Day Program

Mon, Apr 24 - Fri, Apr 28

9:00am - 6:00pm (Days 1-4)

9:00am - 4:00pm (Day 5)

33 CPEs

Laptop Recommended

Instructor: David Hoelzer


www.giac.org/gslc

www.sans.edu

www.sans.org/8140

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

“MGT512 was a great course that ties all of the principles of security, and the instructor was knowledgeable and enthusiastic.”

-ERIC A., U.S. ARMY



David Hoelzer SANS Faculty Fellow

David Hoelzer is a high-scoring SANS Fellow instructor and author of more than 20 sections of SANS courseware. He is an expert in a variety of information security fields, having served in most major roles in the IT and security industries over the past 25 years. Recently, David was called upon to serve as an expert witness for the Federal Trade Commission for ground-breaking GLBA Privacy Rule litigation. David has been highly involved in governance at SANS Technology Institute, serving as a member of the Curriculum Committee as well as Audit Curriculum Lead. As a SANS instructor, David has trained security professionals from organizations including NSA, DHHS, Fortune 500 companies, various Department of Defense sites, national laboratories, and many colleges and universities. David is a research fellow at the Center for Cybermedia Research and at the Identity Theft and Financial Fraud Research Operations Center (ITFF/ROC). He also is an adjunct research associate of the UNLV Cybermedia Research Lab and a research fellow with the Internet Forensics Lab. David has written and contributed to more than 15 peer-reviewed books, publications, and journal articles. Currently, David serves as the principal examiner and director of research for Enclave Forensics, a New York/Las Vegas-based incident response and forensics company. He also serves as the chief information security officer for Cyber-Defense, an open-source security software solution provider. In the past, David served as the director of the GIAC Certification program, bringing the GIAC Security Expert certification to life. David holds a BS in IT, Summa Cum Laude, having spent time either attending or consulting for Stony Brook University, Binghamton University, and American Intercontinental University. @it_audit

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 learn vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. In addition, 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!

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

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.

KEYNOTE:

Exploitation 101: Stacks, NX/DEP, ASLR, and ROP!

David Hoelzer

In this two-hour talk, we will begin with basic stack overflows and then introduce the various protections one at a time and demonstrate how they are defeated! The talk will cover stack overflows, bypassing DEP/NX (non-executable stacks), defeating ASLR, and defeating code signing with ROP. While the talk covers technical topics, even those with less of a technical background will walk away with an appreciation of just how easy exploit development actually is!

Steganography: The Hidden Threat

Kevin Fiscus

Steganography is the practice of concealing messages or information such that the existence of the message is hidden. This differs significantly from cryptography, where the fact that a message exists is obvious but its meaning is hidden. With steganography, the fact that the message exists is kept secret from adversaries. This presentation will provide an overview of steganography, including a brief history, different methods used to hide data, methods used to detect the use of steganography in an environment, and methods that can be used to defeat steganography without detection.

(Am)Cache Rules Everything Around Me

Eric Zimmerman

Amcache is a valuable artifact for forensic examiners because it contains a wealth of information related to evidence of execution of programs, including installed applications and other executables that have been run on a computer, the SHA-1 value of the program, and several time stamps of interest that include the last modified time as well as the first time a program was run. By understanding the data available in the Amcache hive, examiners will be able to build better timelines, create whitelists and blacklists of programs to exclude or look for on other systems, and quickly find outliers in the vast amount of data contained in Amcache hives. People attending this session will come away with an understanding of how data are structured and interrelated in the different parts of an Amcache. Attendees will receive free open-source tools that can process these hives quickly and efficiently.

The Node Situation

Moses Hernandez

You cannot begin to understand the situation we now face with Node until you understand the gravity of the situation. In this talk, we will get into where NodeJS as a Web technology is being used on both servers and clients. Start to understand the approach to testing the framework, and all the places you may find JavaScript in use in the environment.

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

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING



Multi-Course Training Events www.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 www.sans.org/community
Live Training in Your Local Region with Smaller Class Sizes



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



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



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

ONLINE TRAINING



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



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



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



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

FUTURE SANS TRAINING EVENTS

SOUTHERN CALIFORNIA

Anaheim 2017

Anaheim, CA | February 6-11

Scottsdale 2017

Scottsdale, AZ | February 20-25

Dallas 2017

Dallas, TX | February 27 - Mar 4

San Jose 2017

San Jose, CA | March 6-11

Tysons Corner Spring 2017

McLean, VA | March 20-25

ICS Security

SUMMIT & TRAINING 2017

Orlando, FL | March 20-27

Pen Test Austin 2017

Austin, TX | March 27 - April 1

SANS 2017

Orlando, FL | April 7-14

Threat Hunting and IR

SUMMIT & TRAINING 2017

Orlando, FL | April 18-25

Automotive Cybersecurity

SUMMIT & TRAINING 2017

Detroit, MI | May 1-8

Security West 2017

San Diego, CA | May 9-18

NORTHERN VIRGINIA

Reston 2017

Reston, VA | May 21-26

Atlanta 2017

Atlanta, GA | May 30 - June 4

Houston 2017

Houston, TX | June 5-10

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

Hotel Information

Training Campus
Sheraton Inner Harbor

300 South Charles Street
Baltimore, MD 21201
410-962-8300

www.sans.org/event/baltimore-spring-2017/location



The Sheraton Inner Harbor Hotel surrounds you with the best of Baltimore. It is steps away from the magnificent Inner Harbor and Oriole Park at Camden Yards. The hotel has everything you need for a comfortable and relaxing stay.

Special Hotel Rates Available

A special discounted rate of \$205.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID. If you are a government attendee, you must call the hotel directly at 410-962-8300 to book your room and mention you are a SANS government attendee. These rates include high-speed Internet in your room and are only available through March 22, 2017.

Top 5 reasons to stay at the Sheraton Inner Harbor

- 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 Sheraton Inner Harbor 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 Sheraton Inner Harbor that you won't want to miss!
- 5 Everything is in one convenient location!

Registration Information

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



Register online at www.sans.org/baltimore-spring

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 before	3-1-17	\$400.00	3-22-17	\$200.00

Some restrictions apply.

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

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 April 5, 2017 – processing fees may 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