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

# SANS Tysons Corner Spring 2017

McLean, VA | March 20-25

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

## INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

**Eight courses on**

Cyber Defense
Penetration Testing
Detection & Monitoring
Incident Response
Ethical Hacking
Management

"The SANS instructors are the best in the game. Their technical knowledge combined with presentation skills and real-world examples make for an unparalleled training experience."

-Chris Gergen, Bank of North Dakota

GIAC
GIAC-Approved Training

**SAVE $400**

Register and pay by Jan 25th – Use code **EarlyBird17**

www.sans.org/tysons-corner-spring

# SANS Tysons Corner Spring 2017 MARCH 20-25

## 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 Tysons Corner Spring 2017 lineup of instructors includes:

**Jonathan Ham**
*Certified Instructor*
@jhamcorp

**G. Mark Hardy**
*Certified Instructor*
@g_mark

**Randy Marchany**
*Certified Instructor*
@randymarchany

**Michael Murr**
*Principal Instructor*
@mikemurr

**Keith Palmgren**
*Senior Instructor*
@kpalmgren

**Anuj Soni**
*Certified Instructor*
@asoni

**John Strand**
*Senior Instructor*
@strandjs

**Eric Zimmerman**
*Instructor*
@EricRZimmerman

## Evening Bonus Sessions

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

KEYNOTE: ***If I Wake Evil!!!*** – John Strand

***The End of Banking as We Know It*** – G. Mark Hardy

***Malware Analysis: House Rules*** – Anuj Soni

***(Am)Cache Rules Everything Around Me*** – Eric Zimmerman

***Save $400 when you register and pay by Jan 25th using code EarlyBird17***

## Courses at a Glance

| | | MON 3-20 | TUE 3-21 | WED 3-22 | THU 3-23 | FRI 3-24 | SAT 3-25 |
|---|---|---|---|---|---|---|---|
| SEC401 | Security Essentials Bootcamp Style | Page 1 | | | | | |
| SEC503 | Intrusion Detection In-Depth | Page 2 | | | | | |
| SEC504 | Hacker Tools, Techniques, Exploits, and Incident Handling | Page 3 | | | | | |
| SEC560 | Network Penetration Testing and Ethical Hacking | Page 4 | | | | | |
| SEC566 | Implementing and Auditing the Critical Security Controls – In-Depth | Page 5 | | | | | |
| FOR508 | Advanced Digital Forensics, Incident Response, and Threat Hunting | Page 6 | | | | | |
| FOR610 | Reverse-Engineering Malware: Malware Analysis Tools and Techniques | Page 7 | | | | | |
| MGT512 | SANS Security Leadership Essentials for Managers with Knowledge Compression™ | Page 8 | | | | | |

***Register today for SANS Tysons Corner Spring 2017!***
***www.sans.org/tysons-corner-spring***

@SANSInstitute
Join the conversation:
#SANSTysons

SEC401:
# Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Mar 20 - Sat, Mar 25
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Keith Palmgren

www.giac.org/gsec

www.sans.edu


www.sans.org/8140

www.sans.org/cyber-guardian

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

"This week has definitely changed my perspective on IT security. It has made me more paranoid. Thanks SANS!"
-CHARLES LEE, BASIN ELECTRIC POWER COOPERATIVE

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.**

## 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

**Keith Palmgren** *SANS Senior Instructor*

Keith Palmgren is an IT security professional with 26 years of experience in the field. He began his career with the U.S. Air Force working with cryptographic keys and codes management. He also worked in what was at the time the newly-formed computer security department. Following the Air Force, Keith worked as an MIS director for a small company before joining AT&T/Lucent as a senior security architect working on engagements with the DoD and the National Security Agency. As security practice manager for both Sprint and Netigy, Keith built and ran the security consulting practice, responsible for all security consulting world-wide and for leading dozens of security professionals on many consulting engagements across all business spectrums. For the last several years, Keith has run his own company, NetIP, Inc. He divides his time between consulting, training, and freelance writing projects. As a trainer, Keith has satisfied the needs of nearly 5,000 IT professionals and authored 17 training courses. Keith currently holds the CISSP, GSEC, CEH, Security+, Network+, A+, and CTT+ certifications. @kpalmgren

SEC503:
# Intrusion Detection In-Depth

SANS

Six-Day Program
Mon, Mar 20 - Sat, Mar 25
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jonathan Ham

*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.

GCIA
www.giac.org/gcia

SANS Technology Institute
www.sans.edu

sapere aude
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

## 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

SEC504:

# Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Mon, Mar 20 - Sat, Mar 25
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: John Strand

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
- 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

"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

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

**John Strand** *SANS Senior Instructor*

Along with SEC504, John Strand also teaches SEC560: Network Penetration Testing and Ethical Hacking and SEC464: Hacker Detection for System Administrators. John is also the course author for SEC464. When not teaching for SANS, John co-hosts PaulDotCom Security Weekly, the world's largest computer security podcast. He also is the owner of Black Hills Information Security, specializing in penetration testing and security architecture services. He has presented for the FBI, NASA, the NSA, and at DefCon. In his spare time he writes loud rock music and makes various futile attempts at fly fishing. @strandjs

SEC560:

# Network Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Mon, Mar 20 - Sat, Mar 25
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Michael Murr

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.

## Who Should Attend

- Security personnel whose job involves assessing networks and systems to find and remediate vulnerabilities
- Penetration testers
- Ethical hackers
- Defenders who want to better understand offensive methodologies, tools, and techniques
- Auditors who need to build deeper technical skills
- Red and blue team members
- Forensics specialists who want to better understand offensive tactics

"I recommend this course to all incident responders as it offers a clear view of red team TTPs and concepts." -Lesley Carhart, Motorola Solutions

**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.**

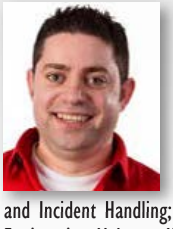
GPEN
www.giac.org/gpen

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

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

"This course pulls together all of the tools needed for pen testing in a very clear and logical manner. SEC560 is excellent and highly valuable training!"
-Bill Hinds,
Project Management Institute



**Michael Murr** *SANS Principal Instructor*

Michael has been a forensic analyst with Code-X Technologies for over five years. He has conducted numerous investigations and computer forensic examinations, and performed specialized research and development. Michael has taught SEC504:Hacker Techniques, Exploits, and Incident Handling; FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting; and FOR610: Reverse-Engineering Malware. He has also led SANS Online Training courses, and is a member of the GIAC Advisory Board. Currently, Michael is working on an open-source framework for developing digital forensics applications. He 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

SEC566:

# Implementing and Auditing the Critical Security Controls – In-Depth

SANS

Five-Day Program
Mon, Mar 20 - Fri, Mar 24
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Randy Marchany

www.giac.org/gccc

www.sans.edu

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

## Who Should Attend

- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense personnel or contractors
- Staff and clients of federal agencies
- Private sector organizations looking to improve information assurance processes and secure their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance

Cybersecurity attacks are increasing and evolving so rapidly that it is more difficult than ever to prevent and defend against them. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches? This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS).

As threats evolve, an organization's security should too. To enable your organization to stay on top of this ever-changing threat scenario, SANS has designed a comprehensive course on how to implement the Critical Security Controls, a prioritized, risk-based approach to security. Designed by private and public sector experts from around the world, the Controls are the best way to block known attacks and mitigate damage from successful attacks. They have been adopted by the U.S. Department of Homeland Security, state governments, universities, and numerous private firms.

The Controls are specific guidelines that CISOs, CIOs, IGs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defenses. They are designed to complement existing standards, frameworks, and compliance schemes by prioritizing the most critical threat and highest payoff defenses, while providing a common baseline for action against risks that we all face.

The Controls are an effective security framework because they are based on actual attacks launched regularly against networks. Priority is given to Controls that (1) mitigate known attacks, (2) address a wide variety of attacks, and (3) identify and stop attackers early in the compromise cycle. The British government's Center for the Protection of National Infrastructure describes the Controls as the "baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence."

"Excellent use of cases and very applicable, and I will be able to directly apply the lessons to my organization." -Dominic N., Bechtel Marine

SANS' in-depth, hands-on training will teach you how to master the specific techniques and tools needed to implement and audit the Critical Controls. It will help security practitioners understand not only how to stop a threat, but why the threat exists, and how to ensure that security measures deployed today will be effective against the next generation of threats.

The course shows security professionals how to implement the Controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the Controls are effectively implemented.

**Randy Marchany** *SANS Certified Instructor*

Randy is the Chief Information Security Officer at Virginia Tech University and the Director of the university's IT Security Laboratory. He is a co-author of the original SANS Top 10 Internet Threats, the SANS Top 20 Internet Threats, the SANS Consensus Roadmap for Defeating DDoS Attacks, and the SANS Incident Response: Step-by-Step guides. Randy is a member of the Center for Internet Security development team that produced and tested the CIS Solaris, HPUX, AIX, Linux and Windows2000/XP security benchmarks and scoring tools. He was a member of the White House Partnership for Critical Infrastructure Security working group that developed a Consensus Roadmap for responding to the DDOS attacks in 2000. @randymarchany

FOR508:

# Advanced Digital Forensics, Incident Response, and Threat Hunting

SANS

Six-Day Program
Mon, Mar 20 - Sat, Mar 25
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

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

## 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

*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."

"This was a great course. I learned some great techniques and this will lead to some changes in our incident response process." -Rick, Syngenta

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!

## 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. @EricRZimmerman

FOR610:

# Reverse-Engineering Malware: Malware Analysis Tools and Techniques

SANS

Six-Day Program
Mon, Mar 20 - Sat, Mar 25
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Anuj Soni


www.giac.org/grem


www.sans.edu

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

## 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

This popular malware analysis course helps forensic investigators, incident responders, security engineers and IT administrators acquire practical skills for examining malicious programs that target and infect Windows systems. Understanding the capabilities of malware is critical to an organization's ability to derive the threat intelligence it needs to respond to information security incidents and fortify defenses. The course builds a strong foundation for analyzing 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 understand the inner workings of malicious software and 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. Additionally, 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.

This course will teach you how to handle self-defending malware. You'll learn how to bypass 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 and deobfuscating JavaScript and VBScript to understand the nature of the attack.

"I conduct incident response activities and learning how to reverse engineer malware is critical." -Eric Moss, Booz Allen Hamilton

You will also 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 it exhibits rootkit characteristics.

The course culminates with a series of Capture-the-Flag challenges designed to reinforce the techniques learned in class and provide additional opportunities to learn practical 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.

## Anuj Soni *SANS Certified Instructor*

Anuj feeds his passion for technical analysis through his role as a Senior Threat Researcher at Cylance, where he performs malware research and reverse engineering. Anuj also brings his problem-solving abilities to his teaching at SANS, which gives him the opportunity to impart his deep technical knowledge and practical skills to students. Since entering the information security field in 2005, Anuj has performed numerous intrusion investigations to help government and commercial clients mitigate attacks against the enterprise. His malware hunting and technical analysis skills have resulted in the successful identification, containment, and remediation of multiple threat actor groups. Anuj has analyzed hundreds of malware samples to assess function, purpose, and impact, and his recommendations have improved the security posture of numerous organizations. Highly sought after as a technical thought leader and adviser, Anuj excels not only in delivering rigorous forensic analysis, but also in process development, knowledge management, and team leadership to accelerate incident response efforts. @asoni

MGT512:

# SANS Security Leadership Essentials for Managers with Knowledge Compression™

SANS

Five-Day Program
Mon, Mar 20 - Fri, Mar 24
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop Recommended
Instructor: G. Mark Hardy

www.giac.org/gslc

www.sans.edu

www.sans.org/8140

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

"This course is very comprehensive and provides excellent awareness of how web servers and interaction work. Worth your time!"
-Steve McGee, Curaspan Health Group

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.

## 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

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!

## G. Mark Hardy *SANS Certified Instructor*

G. Mark Hardy is founder and president of National Security Corporation. He has been providing cybersecurity expertise to government, military, and commercial clients for over 30 years, and is an internationally recognized expert who has spoken at over 250 events world-wide. He serves on the Advisory Board of CyberWATCH, an Information Assurance/Information Security Advanced Technology Education Center of the National Science Foundation. A retired U.S. Navy Captain, he was privileged to serve in command nine times, including responsibility for leadership training for 70,000 sailors. He also served as wartime Director, Joint Operations Center for U.S. Pacific Command, and Assistant Director of Technology and Information Management for Naval Logistics in the Pentagon, with responsibility for InfoSec, public key infrastructure, and Internet security. Captain Hardy was awarded the Defense Superior Service Medal, the Legion of Merit, five Meritorious Service Medals, and 24 other medals and decorations. A graduate of Northwestern University, he has bachelor's degrees in computer science and mathematics, and master's degrees in business administration and strategic studies, along with the GSLC, CISSP, CISM, and CISA certifications. @g_mark

# 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:

## If I Wake Evil!!!

***John Strand***

Let's say I went to the dark side to get their sweet, sweet cookies. Let's say that all goodness had left me. How would I attack you? This talk will answer that question. It will also show you how to stop me.

## The End of Banking as We Know It

### How Crypto Currencies and e-Payments are Breaking Up a Centuries-Old Monopoly

***G. Mark Hardy***

Are we finally ready to go mainstream with alt-currency? Bitcoin got off to a slow start but has attracted millions of VC dollars in the last two years. We'll look at this brave new world of electronic money to understand what it is, how it works, what it can (and cannot) do, and probabilities of success or failure. We'll examine spin-off technologies such as blockchains, and look into the mechanics behind electronic payment systems such as Apple Pay, CurrentC, and Softcard. We'll even talk about why crooks love Bitcoin for ransomware extortion, and dig into the mechanics of how credit card fraud works, and whether that might be going away as well.

## Malware Analysis: House Rules

***Anuj Soni***

Welcome to malware analysis. You're invited to explore, examine, and enjoy. However, we strongly encourage you to review and respect the house rules to make the most of your experience. Whether this is your first time or you're a frequent visitor, we hope this discussion of process and technical suggestions will be a helpful guide to the adventures ahead.

## (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.

# Enhance Your Training Experience

Add an

**OnDemand Bundle & GIAC Certification Attempt***

to your course within seven days of this event for just $689 each.

SPECIAL PRICING

## Extend Your Training Experience with an OnDemand Bundle

- Four months of supplemental online review
- 24/7 online access to your course lectures, materials, quizzes, and labs
- Subject-matter-expert support to help you increase your retention of course material

*"The course content and OnDemand delivery method have both exceeded my expectations."*

-Robert Jones, Team Jones, Inc.

## Get Certified with GIAC Certifications

- Distinguish yourself as an information security leader
- 30+ GIAC cybersecurity certifications available
- Two practice exams included
- Four months of access to complete the attempt

*"GIAC is the only certification that proves you have hands-on technical skills."*

-Christina Ford, Department of Commerce

## MORE INFORMATION

www.sans.org/ondemand/bundles www.giac.org



*GIAC and OnDemand Bundles are only available for certain courses.

# SANS TRAINING FORMATS

## 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

**Security East** 2017
New Orleans, LA | Jan 9-14

**Cloud Security** SUMMIT 2017
San Francisco, CA | Jan 17-19

**Las Vegas** 2017
Las Vegas, NV | Jan 23-30

**Cyber Threat Intelligence**
SUMMIT & TRAINING 2017
Arlington, VA | Jan 25 - Feb 1

SOUTHERN CALIFORNIA
**Anaheim** 2017
Anaheim, CA | Feb 6-11

**Scottsdale** 2017
Scottsdale, AZ | Feb 20-25

**Dallas** 2017
Dallas, TX | Feb 27 - Mar 4

**San Jose** 2017
San Jose, CA | Mar 6-11

**ICS Security**
SUMMIT & TRAINING 2017
Orlando, FL | Mar 20-27

**Pen Test Austin** 2017
Austin, TX | Mar 27 - Apr 1

**SANS 2017**
Orlando, FL | Apr 7-14

**Threat Hunting and IR**
SUMMIT & TRAINING 2017
Orlando, FL | Apr 18-25

**Baltimore Spring** 2017
Baltimore, MD | Apr 24-29

**Automotive Cybersecurity**
SUMMIT & TRAINING 2017
Detroit, MI | May 1-8

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

SANS TYSONS CORNER SPRING 2017

# Hotel Information

*Training Campus*
**Hilton McLean Tysons Corner**

**7920 Jones Branch Drive**
**McLean, VA 22102 | 703-847-5000**
**www.sans.org/event/tysons-corner-spring-2017/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. This rate is only available through February 27, 2017.
To make reservations, please call (703) 847-5000 and ask for the SANS group or SANS government rate.

## 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 TYSONS CORNER SPRING 2017

# Registration Information


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

## Register online at www.sans.org/tysons-corner-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.

Use code **EarlyBird17** when registering early

## Pay Early and Save

| | DATE | DISCOUNT | DATE | DISCOUNT |
|---|---|---|---|---|
| **Pay & enter code before** | **1-25-17** | **$400.00** | **2-8-17** | **$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 March 1, 2017 – processing fees may apply.