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

SANS Las Vegas 2017

January 23-30

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

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

Nine courses on

Cyber Defense
Penetration Testing
Incident Response
Digital Forensics
Ethical Hacking
Management

"SANS course materials are excellent! I have so much to bring back to the office, and I am excited to share my findings with my team and manager."
-Stacey Boivin, AESO

GIAC
GIAC-Approved Training

SAVE $400
when you register and pay by Nov 30th using code **EarlyBird17**

www.sans.org/las-vegas

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 Las Vegas 2017 lineup of instructors includes:

Carlos Cajigas
SANS Instructor
@Carlos_Cajigas

Eric Conrad
Senior Instructor
@eric_conrad

Ted Demopoulos
Principal Instructor
@TedDemop

Kevin Fiscus
Certified Instructor
@kevinbfiscus

Philip Hagen
Certified Instructor
@PhilHagen

G. Mark Hardy
Certified Instructor
@g_mark

David R. Miller
Certified Instructor
@DRM_CyberDude

The training campus for SANS Las Vegas 2017 is in Planet Hollywood Resort and Casino featuring Las Vegas hotel accommodations fit for the celebrity A-List, and perfect for Hollywood buffs.
PAGE 13

Evening Bonus Sessions

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

KEYNOTE: ***Quality Not Quantity: Continuous Monitoring's Deadliest Events*** Eric Conrad

Infosec Rock Star: Geek Will Only Get You So Far – Ted Demopoulos

CISSP®: How to Get the Certification That Matters the Most – David R. Miller

The Tap House – Philip Hagen

Virtualizing Forensic Images Using Free Tools in Linux – Carlos Cajigas

Save $400 when you register and pay by Nov 30th using code EarlyBird17

Courses-at-a-Glance

		MON 1-23	TUE 1-24	WED 1-25	THU 1-26	FRI 1-27	SAT 1-28	SUN 1-29	MON 1-30
SEC401	Security Essentials Bootcamp Style	Page 1 SIMULCAST							
SEC504	Hacker Tools, Techniques, Exploits & Incident Handling	Page 2 SIMULCAST							
SEC542	Web App Penetration Testing and Ethical Hacking	Page 3							
FOR408	Windows Forensic Analysis	Page 4							
FOR572	Advanced Network Forensics and Analysis	Page 5 SIMULCAST							
MGT414	SANS Training Program for CISSP® Certification	Page 6							
MGT512	SANS Security Leadership Essentials For Managers with Knowledge Compression™	Page 7							
SEC580	Metasploit Kung Fu for Enterprise Pen Testing							Pg 8	
MGT415	A Practical Introduction to Cybersecurity Risk Management							Pg 8	

SEC401:

Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Jan 23- Sat, Jan 28
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Ted Demopoulos

ALSO AVAILABLE VIA SIMULCAST
www.sans.org/simulcast

GSEC
www.giac.org/gsec

SANS Technology Institute
www.sans.edu

www.sans.org/8140

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

"Ted is an excellent instructor, and the course content covers a wide range of essential security topics."
-Nikhil Keshwala, Huawei Technologies

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

Ted Demopoulos *SANS Principal Instructor*

Ted Demopoulos' first significant exposure to computers was in 1977 when he had unlimited access to his high school's PDP-11 and hacked at it incessantly. He consequently almost flunked out but learned he liked playing with computers. His business pursuits began in college and have been ongoing ever since. His background includes over 25 years in information security and business, including 20+ years as an independent consultant. Ted helped start a successful information security company, was the CTO at a "textbook failure" of a software startup, and has advised many businesses. Ted is a frequent speaker at conferences and other events, quoted often by the press. He also has written two books on social media, has an ongoing software concern in Austin, Texas in the virtualization space, and is the recipient of a Department of Defense Award of Excellence. In his spare time, he is a food and wine geek, enjoys flyfishing, and plays with his children. @TedDemop

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Mon, Jan 23- Sat, Jan 28
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Kevin Fiscus

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 for, exploiting, and defending systems. This will enable you to discover the holes in your system before the bad guys do!

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

"Kevin keeps the topic interesting and I am able to pick up key points by the way he keys in on the topic."
-Christian Campbell, nGuard, Inc.

ALSO AVAILABLE VIA SIMULCAST
www.sans.org/simulcast

GCIH
www.giac.org/gcih

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

www.sans.org/8140

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

Kevin Fiscus *SANS Certified Instructor*

Kevin Fiscus is the founder of and lead consultant for Cyber Defense Advisors, where he performs security and risk assessments, vulnerability and penetration testing, security program design, policy development and security awareness with a focus on serving the needs of small and mid-sized organizations. Kevin has over 20 years of IT experience and has focused exclusively 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

SEC542:

Web App Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Mon, Jan 23- Sat, Jan 28
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Eric Conrad

www.giac.org/gwapt

www.sans.edu

www.sans.org/cyber-guardian

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

"The content of SEC542 is very relevant as it features recently discovered vulnerabilities. It also effectively, from my view, caters to various experience levels."
-Malcolm King, Morgan Stanley

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.

Who Should Attend

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

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 course has been well worth it! I can't wait to take the advanced pen testing course." -Ben Johnson, Time Inc.

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.**

Eric Conrad *SANS Senior Instructor*

Eric Conrad is lead author of the book *The CISSP Study Guide*. Eric's career began in 1991 as a UNIX systems administrator for a small oceanographic communications company. He gained information security experience in a variety of industries, including research, education, power, Internet, and healthcare. He is now president of Backshore Communications, a company focusing on intrusion detection, incident handling, information warfare, and penetration testing. He is a graduate of the SANS Technology Institute with a master of science degree in information security engineering. In addition to the CISSP, he holds the prestigious GIAC Security Expert (GSE) certification as well as the GIAC GPEN, GCIH, GCIA, GCFA, GAWN, and GSEC certifications. Eric also blogs about information security at ericconrad.com. @eric_conrad

FOR408:
Windows Forensic Analysis

SANS

Six-Day Program
Mon, Jan 23- Sat, Jan 28
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Carlos Cajigas

Master Windows Forensics – You can't protect what you don't know about.

Every organization must prepare for cyber crime occurring on its computer systems and within its networks. Demand has never been greater for analysts who can investigate crimes like fraud, insider threats, industrial espionage, employee misuse, and computer intrusions. Government agencies increasingly require trained media exploitation specialists to recover key intelligence from Windows systems. To help solve these cases, SANS is training a new cadre of the world's best digital forensic professionals, incident responders, and media exploitation masters capable of piecing together what happened on computer systems second by second.

Who Should Attend

- Information security professionals
- Incident response team members
- Law enforcement officers, federal agents, and detectives
- Media exploitation analysts
- Anyone interested in a deep understanding of Windows forensics

"The Windows registry forensic section blew my mind! I didn't think it stored that much information." -Tung Nguyen, Denver Water

FOR408: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of the Microsoft Windows operating systems. You can't protect what you don't know about, and understanding forensic capabilities and artifacts is a core component of information security. Learn to recover, analyze, and authenticate forensic data on Windows systems. Understand how to track detailed user activity on your network and how to organize findings for use in incident response, internal investigations, and civil/criminal litigation. Use your new skills for validating security tools, enhancing vulnerability assessments, identifying insider threats, tracking hackers, and improving security policies. Whether you know it or not, Windows is silently recording an unimaginable amount of data about you and your users. FOR408 teaches you how to mine this mountain of data.

Proper analysis requires real data for students to examine. The completely updated FOR408 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7/8/10, Office and Office365, cloud storage, Sharepoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques to investigate even the most complicated systems they might encounter. Nothing is left out – attendees learn to analyze everything from legacy Windows XP systems to just-discovered Windows 10 artifacts.

FIGHT CRIME. UNRAVEL INCIDENTS...ONE BYTE AT A TIME

www.giac.org/gcfe

SANS Technology Institute
www.sans.edu

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

"The methods taught and the tools introduced will be very beneficial to me as an analyst performing examinations."
-Joseph Selph, IBM

Carlos Cajigas *SANS Instructor*

As an incident responder, cybercrimes investigator, digital forensics trainer, retired detective, Carlos has amassed a wealth of experience in high-technology crime investigations. As a detective with the West Palm Beach Police Department, he specialized in computer crime investigations. He has conducted examinations on hundreds of digital devices to go along with hundreds of hours of digital forensics training. His training includes courses by Guidance Software (EnCase), National White Collar Crime Center (NW3C), Access Data (FTK), United States Secret Service (USSS), IACIS, and SANS. Carlos holds bachelor's and master's degrees from Palm Beach Atlantic University (FL). In addition, he holds various certifications in the digital forensics field, including EnCase Certified Examiner (EnCE), Certified Forensic Computer Examiner (CFCE) from IACIS, and the GIAC Certifications GCFE and GCFA. He is currently an incident responder for a Fortune 500 company, where he is responsible for responding to computer and network security threats for clients in North and South America. @Carlos_Cajigas

FOR572:
Advanced Network Forensics and Analysis

SANS

Six-Day Program
Mon, Jan 23- Sat, Jan 28
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Philip Hagen

ALSO AVAILABLE VIA SIMULCAST
www.sans.org/simulcast

GNFA
www.giac.org/gnfa

SANS Technology Institute
www.sans.edu

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

"This course has well-organized professional material, and the instructors, like Phil, have real-world experiences that are extremely valued and my main reason for attending."
-Dennis Allen,
SEI Investments Company

The network IS the new investigative baseline.

There is simply no incident response action that doesn't include a communications component any more. Whether you conduct threat hunting operations, traditional casework, or post-mortem incident response, understanding the nature of how systems have communicated is critical to success. Even in disk- and memory-based incident response work, artifacts that clarify a subject's network actions can be keystone findings you can't afford to miss. Whether you are handling a data breach, intrusion scenario, or employee misuse case, or you are threat hunting (proactively trawling your organization's data stores for evidence of an undiscovered compromise), you need to effectively examine and interpret network artifacts.

Who Should Attend

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

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

Whether you are a consultant responding to a client's site, a law enforcement professional assisting victims of cyber crime and seeking prosecution of those responsible, or an on-staff forensic practitioner, this course offers hands-on experience with real-world scenarios that will help take your work to the next level. Previous SANS security curriculum students and other network defenders will benefit from the FOR572 perspective on security operations as they take on more incident response and investigative responsibilities. SANS forensics alumni from FOR408 and FOR508 can take their existing knowledge and apply it directly to the network-based attacks that occur daily. In FOR572, we solve the same caliber of real-world problems without any convenient hard drive or memory images.

Philip Hagen *SANS Certified Instructor*

Philip Hagen has been working in the information security field since 1998, covering the full spectrum including deep technical tasks, management of an entire computer forensic services portfolio, and executive responsibilities. Currently, Phil is an Evangelist at Red Canary, where he engages with current and future customers of Red Canary's managed threat detection service to ensure their use of the service is best aligned for success in the face of existing and future threats. Phil started his security career while attending the U.S. Air Force Academy, with research covering both the academic and practical sides of security. He served in the Air Force as a communications officer at Beale AFB and the Pentagon. In 2003, Phil became a government contractor, providing technical services for various IT and information security projects. These included systems that demanded 24x7x365 functionality. He later managed a team of 85 computer forensic professionals in the national security sector. He provided forensic consulting services for law enforcement, government, and commercial clients prior to joining the Red Canary team. Phil is the course lead and co-author of FOR572: Advanced Network Forensics and Analysis. @PhilHagen

MGT414:

SANS Training Program for CISSP® Certification

SANS

Six-Day Program
Mon, Jan 23- Sat, Jan 28
9:00am - 7:00pm (Day 1)
8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6)
46 CPEs
Laptop NOT Needed
Instructor: David R. Miller

SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that is specifically designed to prepare students to successfully pass the CISSP® exam.

MGT414 focuses solely on the eight domains of knowledge as determined by (ISC)^2 that form a critical part of CISSP® exam. Each domain of knowledge is dissected into its critical components, and those components are then discussed in terms of their relationship with one another and with other areas of information security.

Who Should Attend

- Security professionals who want to understand the concepts covered in the CISSP® exam as determined by (ISC)^2
- Managers who want to understand the critical areas of information security
- System, security, and network administrators who want to understand the pragmatic applications of the CISSP® eight domains
- Security professionals and managers looking for practical ways to apply the eight domains of knowledge to their current activities

You Will Be Able To:

- Understand the eight domains of knowledge that are covered on the CISSP® exam
- Analyze questions on the exam and be able to select the correct answer
- Apply the knowledge and testing skills learned in class to pass the CISSP® exam
- Understand and explain all of the concepts covered in the eight domains of knowledge
- Apply the skills learned across the eight domains to solve security problems when you return to work

Note:
The CISSP® exam itself is not hosted by SANS. You will need to make separate arrangements to take the CISSP® exam. Please note as well that the GISP exam offered by GIAC is NOT the same as the CISSP® exam offered by (ISC)^2.

Obtaining Your CISSP® Certification Consists of:

- Fulfilling minimum requirements for professional work experience
- Completing the Candidate Agreement
- Review of your résumé
- Passing the CISSP® 250 multiple-choice question exam with a scaled score of 700 points or greater
- Submitting a properly completed and executed Endorsement Form
- Periodic audit of CPEs to maintain the credential

Take advantage of the SANS CISSP® Get Certified Program currently being offered.
www.sans.org/cissp

www.giac.org/gisp

www.sans.org/8140

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

"The instructor was excellent and truly an expert! I'm getting depth in my understanding and David explained some topics better than several books I've read."
-Freda Lurdy, Raytheon

David R. Miller *SANS Certified Instructor*

David has been a technical instructor since the early 1980s and has specialized in consulting, auditing, and lecturing on information system security, legal and regulatory compliance, and network engineering. David has helped many enterprises develop their overall compliance and security program, including through policy writing, network architecture design to include security zones, development of incident response teams and programs, design and implementation of public key infrastructures, security awareness training programs, specific security solution designs like secure remote access and strong authentication architectures, disaster recovery planning and business continuity planning, and pre-audit compliance gap analysis and remediation. He serves as a security lead and forensic investigator on numerous enterprise-wide IT design and implementation projects for Fortune 500 companies, providing compliance, security, technology, and architectural recommendations and guidance. Projects include Microsoft Windows Active Directory enterprise designs, security information and event management systems, intrusion detection and protection systems, endpoint protection systems, patch management systems, configuration monitoring systems, and enterprise data encryption for data at rest, in transit, in use, and within email systems. David is an author, lecturer and technical editor of books, curriculum, certification exams, and computer-based training videos. @DRM_CyberDude

MGT512:

SANS Security Leadership Essentials for Managers with Knowledge Compression™

SANS

Five-Day Program
Mon, Jan 23- Fri, Jan 27
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

SANS Technology Institute
www.sans.edu

www.sans.org/8140

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

"Mark Hardy has excellent teaching skills, and keeps all material interesting using real-life examples. His talk on crypto was awesome!"
-Brett Tode', Zoetis

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

SEC580

Metasploit Kung Fu for Enterprise Pen Testing

Two-Day Course | Sun, Jan 29 - Mon, Jan 30 | 9:00am - 5:00pm | 12 CPEs | Laptop Required
Instructor: Eric Conrad

Many enterprises today face regulatory or compliance requirements that mandate regular penetration testing and vulnerability assessments. Commercial tools and services for performing such tests can be expensive. While really solid free tools such as Metasploit are available, many testers do not understand the comprehensive feature sets of such tools and how to apply them in a professional-grade testing methodology. Metasploit was designed to help testers with confirming vulnerabilities using an open-source and easy-to-use framework. This course will help students get the most out of this free tool.

This class will show students how to apply the incredible capabilities of the Metasploit Framework in a comprehensive penetration testing and vulnerability assessment regimen according to a thorough methodology for performing effective tests. Students who complete the course will have a firm understanding of how Metasploit can fit into their penetration testing and day-to-day assessment activities. The course will provide an in-depth understanding of the Metasploit Framework far beyond simply showing attendees how to exploit a remote system. **The class will cover exploitation, post-exploitation reconnaissance, token manipulation, spear-phishing attacks, and the rich feature set of the Meterpreter, a customized shell environment specially created for exploiting and analyzing security flaws.**

MGT415

A Practical Introduction to Cybersecurity Risk Management

Two-Day Course | Sun, Jan 29 - Mon, Jan 30 | 9:00am - 5:00pm | 12 CPEs | Laptop Required
Instructor: G. Mark Hardy

In this course students will learn the practical skills necessary to perform regular risk assessments for their organizations. The ability to perform a risk assessment is crucial for organizations hoping to defend their systems. There are simply too many threats, too many potential vulnerabilities, and not enough resources to create an impregnable security infrastructure. Therefore every organization, whether it does so in an organized manner or not, will make priority decisions on how best to defend its valuable data assets. Risk assessment should be the foundational tool used to facilitate thoughtful and purposeful defense strategies.

You Will Learn:

- How to perform a risk assessment step by step
- How to map an organization's business requirements to implemented security controls
- The elements of risk assessment and the data necessary for performing an effective risk assessment
- What in-depth risk management models exist for implementing a deeper risk management program in your organization

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:

Quality Not Quantity: Continuous Monitoring's Deadliest Events

Eric Conrad

Most Security Operations Centers (SOCs) are built for compliance, not security. One well-known retail firm suffered the theft of over a million credit cards. Some 60,000 true positive events were reported to the firm's SOC during that missed breach, but they were lost in the noise of millions. If you are bragging about how many events your SOC handles each day, you are doing it wrong. During this talk, we will show you how to focus on quality instead of quantity, and provide an actionable list of the deadliest events that occur during virtually every successful breach.

Infosec Rock Star: Geek Will Only Get You So Far

Ted Demopoulos

Some of us are so effective, and well known, that the term "Rock Star" is entirely accurate. What kind of skills do Rock Stars have and wannabe Rock Stars need to develop? Although we personally may never be swamped by groupies, we can learn the skills to be more effective, well respected, and well paid. Obviously it's not just about technology; in fact most of us are very good at the technology part. And although the myth of the Geek with zero social skills is just that, a myth, the fact is that increasing our skills more on the social and business side will make most of us more effective at what we do than learning how to read hex better while standing on our heads, becoming "One with Metasploit," or understanding the latest hot technologies.

CISSP®: How to Get the Certification that Matters the Most

David R. Miller

This presentation will show you why the CISSP® certification is so important to your IT career. Companies are in great need of qualified security professionals. The positions and the budget are there. Yet many IT security positions remain unfilled because there are too few certified IT security professionals. This means you can choose which position you want from many companies. It also means that companies are willing to pay higher salaries to get you. This presentation by one of the most experienced CISSP® instructors on the planet will help guide you through the world of certifications and determine which ones are best for you.

The Tap House

Philip Hagen

Packets move pretty fast. The field of Network Forensics needs to move fast, too. Whether you are investigating a known incident, hunting unidentified adversaries in your environment, or enriching forensic findings from disk- and memory-based examinations, it's critical to stay abreast of the latest developments in the discipline. This talk will discuss some of the latest technologies, techniques, and tools that you'll want to know in pursuit of forensication nirvana. Phil is also an avid craft beer fan, so there's a good chance you'll learn something about a new or notable local or national beer in the process. This presentation will be helpful for those who wish to keep up-to-date on the most cutting-edge facets of network forensics.

Virtualizing Forensic Images Using Free Tools in Linux

Carlos Cajigas

Have you ever needed to boot a forensic image to preview the system in a live manner? Would you like to do it without changing a single bit? It is possible! In this session we will discuss the tools and steps required for converting the Donald Blake forensic image into a Virtual Machine (VM). This process is useful, because it gives you the ability to boot an image of an OS drive into a VM, all while preserving the integrity of the image. All changes made by the OS are saved and stored to a cache file. Come see how you accomplish this using free tools under Linux Ubuntu. The presentation will include a live demo.

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 Certification

- 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

Miami 2016
Miami, FL | Nov 7-12

Healthcare Cybersecurity
SUMMIT & TRAINING 2016
Houston, TX | Nov 14-21

San Francisco 2016
San Francisco, CA | Nov 27 - Dec 2

Cyber Defense Initiative 2016
Washington, DC | Dec 10-17

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

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

Tysons Corner Spring 2017
McLean, VA | Mar 20-25

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

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

SANS LAS VEGAS 2017

Hotel Information

Training Campus
Planet Hollywood

3667 Las Vegas Boulevard South
Las Vegas, NV 89109
866-919-7472
www.sans.org/event/las-vegas-2017/location

Planet Hollywood Resort and Casino features Las Vegas hotel accommodations fit for the celebrity A-List, and perfect for Hollywood buffs. Every one of its rooms and suites features one-of-a-kind movie memorabilia set against a backdrop of stylish, modern luxury. When you stay in a Planet Hollywood hotel room, the celebrity lifestyle is yours for the living, and fame lies around every corner.

Special Hotel Rates Available

A special discounted rate of $89.00 S/D will be honored Sunday through Thursday and a rate of $129.00 S/D will be honored on Friday and Saturday based on space availability.

The per diem rate will be honored for Friday and Saturday with proper ID. The Sunday through Thursday group rate is currently lower than the prevailing per diem rate. A resort fee of $32.00 per night plus tax will be added to all room rates. This includes high-speed Internet access (two device connections per room per day), complimentary fitness center access, and local phone calls. These rates are only available through December 30, 2016.

Top 5 reasons to stay at Planet Hollywood

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

SANS LAS VEGAS 2017

Registration Information

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

Register online at www.sans.org/las-vegas

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	**11-30-16**	**$400.00**	**12-21-16**	**$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 December 28, 2016 – processing fees may apply.