SANS EMEA

NOVEMBER 16TH TO 21ST 2015 • GRAND CONNAUGHT ROOMS, LONDON, WC2

SANS LONDON

THE WORLD'S LARGEST & MOST TRUSTED PROVIDER OF CYBER SECURITY TRAINING

12 SANS INSTITUTE TRAINING COURSES AT ONE EVENT

Immersive Training ★ World Class Instructors ★ GIAC Certification ★ SANS@Night evening talks and networking ★ Social Functions

SEC542
Web App Penetration Testing and Ethical Hacking

SEC401
Security Essentials Bootcamp Style

SEC501
Advanced Security Essentials - Enterprise Defender

SEC503
Intrusion Detection In-Depth

SEC504
Hacker Tools, Techniques, Exploits and Incident Handling

SEC511
Continuous Monitoring and Security Operations

SEC560
Network Penetration Testing and Ethical Hacking

SEC575
Mobile Device Security and Ethical Hacking

SEC579
Virtualization and Private Cloud Security

SEC660
Advanced Penetration Testing, Exploit Writing, & Ethical Hacking

FOR408
Windows Forensic Analysis

ICS410
ICS/SCADA Security Essentials

Register online and see full course descriptions at **www.sans.org/event/london-2015**

See inside for unique code- register and pay before September the 30th and **save €375**

HM Government
SANS is a Cyber Security Supplier to Government

GIAC

COURSES AT A GLANCE

SANS EMEA

All courses run from the 16th – 21st November
apart from ICS410 which runs from the 16th – 20th November

		MON 16	TUE 17	WED 18	THU 19	FRI 20	SAT 21
SEC 401 SANS Security Essentials Bootcamp Style	Stephen Sims	PG 8 →					
SEC 501 Advanced Security Essentials - Enterprise Defender	Paul A. Henry	PG 9 →					
SEC 503 Intrusion Detection In-Depth	Jess Garcia	PG 10 →					
SEC 504 Hacker Tools, Techniques, Exploits and Incident Handling	Steve Armstrong	PG 11 →					
SEC 511 Continuous Monitoring and Security Operations	Eric Conrad	PG 12 →					
SEC 542 Web App Penetration Testing and Ethical Hacking	Pieter Danhieux	PG 13 →					
SEC 560 Network Penetration Testing and Ethical Hacking	Bryce Galbraith	PG 14 →					
SEC 575 Mobile Device Security and Ethical Hacking	Raul Siles	PG 15 →					
SEC 579 Virtualization and Private Cloud Security	Dave Shackleford	PG 16 →					
SEC 660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	James Lyne	PG 17 →					
FOR 408 Windows Forensic Analysis	Rob Lee	PG 18 →					
ICS 410 ICS/SCADA Security Essentials	Justin Searle	PG 19 →					

Register at www.sans.org/event/london-2015

SANS LONDON 2015
REGISTRATION INFORMATION

REGISTER ONLINE AT: WWW.SANS.ORG/EVENT/LONDON-2015

REGISTER EARLY AND SAVE

Register for #SANSLondon and pay before the 30th of September and save €375 by entering the code EarlyBird15

All course prices are listed at sans.org/event/london-2015

GROUP SAVINGS
(APPLIES TO TUITION ONLY)

5-9 people = 5%

10 or more people = 10%

Early bird rates and/or other discounts cannot be combined with the group discount.

To obtain a group discount please email emea@sans.org.

TO REGISTER

To register, go to **www.sans.org/event/london-2015** Select your course or courses and indicate whether you plan to test for GIAC certification.

How to tell if there is room available in a course: 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.

CONFIRMATION

Look for e-mail confirmation. It will arrive soon after you register. We recommend you register and pay early to ensure you get your first choice of courses.

An immediate e-mail confirmation is sent to you when the registration is submitted properly. If you have not received e-mail confirmation within two business days of registering, please call the SANS Registration office at +1 301-654-7267 9:00am - 8:00pm Eastern Time or email emea@sans.org.

CANCELLATION

You may subsitute another person in your place at any time by sending an e-mail request to emea@sans.org.

Cancellation requests by Oct 21st, 2015, by emailing emea@sans.org

ABOUT SANS

SANS is the most trusted and by far the largest source for information security training and security certification in the world.

The SANS Institute was established in 1989 as a cooperative research and education organisation. Our training programs now reach more than 200,000 security professionals around the world.

SANS provides intensive, immersion training designed to help you and your staff master the practical steps necessary for defending systems and networks against the most dangerous threats - the ones being actively exploited.

SANS courses are full of important and immediately useful techniques that you can put to work as soon as you return to the office. They were developed through a consensus process involving hundreds of administrators, security managers and information security professionals. Courses address security fundamentals and awareness as well as the in-depth technical aspects of the most crucial areas of IT security.

SANS-certified instructors are recognised as the best in the world. To find the best teachers for each topic, SANS runs a continuous competition for instructors. Last year more than 100 people tried out for the SANS faculty, but only five new potential instructors were selected.

SANS provides training through several delivery methods, both live & virtual: classroom-style at a training event, online at your own pace, guided study with a local mentor, or onsite at your workplace. SANS courses are taught in English by our world class SANS instructors, or in French or Spanish if you attend one of our excellent partner training events in France or Spain.

In addition to top-notch training, SANS offers certification through the GIAC security certification program and numerous free security resources such as newsletters, whitepapers, and webcasts.

Why SANS is the best training and educational investment

- Intensive, hands-on immersion training with the highest-quality courseware in the industry.
- Incomparable instructors and authors who are industry experts and practitioners fighting the same cyber battles as you and discovering new ways to thwart attacks.
- Training that strengthens a student's ability to achieve a GIAC certification, which is unique in the field of information security certifications because it not only tests a candidate's knowledge, but also the candidate's ability to put that knowledge into practice in the real world.

Register at www.sans.org/event/london-2015

ABOUT SANS LONDON 2015

SANS London runs from Monday 16th to Saturday 21st November at the Grand Connaught Rooms in London's West End and hosts 12 courses drawn from across the SANS curriculum.

Registration fees include all courseware and training materials plus morning and afternoon break refreshments and lunch served in the restaurant of the Grand Connaught Rooms. Accommodation is not included.

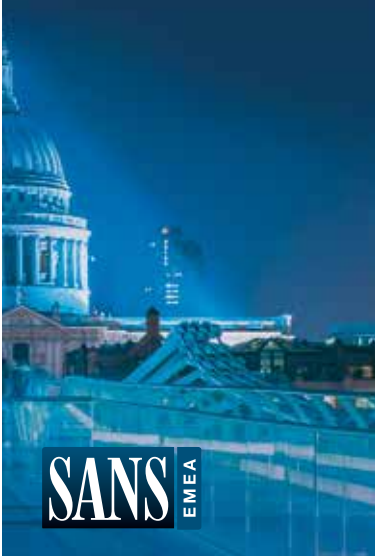
Training runs from 9am-5pm each day except for course SEC401 which finishes at 7pm Monday-Friday and 5pm on Saturday, course SEC504 which finishes at 7.15pm on Monday and then 9am-5pm Saturday and then course SEC660 which finishes at 7pm Monday-Friday and 5pm on Saturday.

Students are able to attend NetWars, free SANS@night talks and evening social functions. The demand for places at SANS London events is always high so please register online as soon as possible to secure a seat at SANS London 2015.

Read on for course descriptions or visit **www.sans.org/event/london-2015**. Over the page you will find the SANS Career Roadmap which provides examples of how SANS courses fit into your career development plan.

CONTENTS

SANS EMEA:
PO Box 124,
Swansea, SA3 9BB, UK



SANS EMEA

SANS IT SECURITY TRAINING AND YOUR

CAREER ROAD MAP

CORE COURSES

FUNCTION:

INFORMATION SECURITY

Information security professionals are responsible for research and analysis of security threats that may effect an organisation's assets, products, or technical specifications.

These security professionals will dig deeper into technical protocols and specifications related to security threats than most of their peers, identifying strategies to defend against attacks by gaining an intimate knowledge of the threats.

SAMPLE JOB TITLES:
Cyber Security Analyst , Cyber Security Engineer, Cyber Security Architect

SEC301
Intro to Information Security
GISF

SEC401
Security Essentials Bootcamp Style
GSEC

SEC501
Advanced Security Essentials Enterprise Defender
GCED

FUNCTION:

NETWORK OPERATIONS CENTRE, SYSTEM ADMIN, SECURITY ARCHITECTURE

A Network Operations Centre (NOC) is where IT professionals supervise, monitor, and maintain the enterprise network. The NOC is the focal point for network troubleshooting, software distribution and updating, router and system management, performance monitoring, and coordination with affiliated networks.

The NOC analysts work hand-in-hand with the Security Operations Centre, which safeguards the enterprise and continuously monitors threats against it.

SAMPLE JOB TITLES:
Security Analyst / Engineer, SOC Analyst, Cyber Threat Analyst, CERT Member, Malware Analyst

CORE COURSES
SEC301 GISF › SEC401 GSEC › SEC501 GCED

SEC505
Securing Windows with PowerShell and the Critical Security Controls
GCWN

SEC506
Securing Linux/Unix
GCUX

SEC566
Implementing and Auditing the Critical Security Controls - In-depth
GCCC

SEC579
Virtualisation and Private Cloud Security

FUNCTION:

INCIDENT RESPONSE

When the security of a system or network has been compromised, the incident responder is the first-line defense during the breach. The responder not only has to be technically astute, he/she must be able to handle stress under fire while navigating people, processes, and technology to help respond and mitigate a security incident.

SAMPLE JOB TITLES:
Security analyst/engineer, SOC analyst, Cyber threat analyst, CERT member, Malware analyst

CORE COURSES
SEC301 GISF › SEC401 GSEC

SEC504
Hacker Tools, Techniques, Exploits and Incident Handling
GCIH

Network Analysis

SEC503
Intrusion Detection In-Depth
GCIA

FOR572
Advanced Network Forensics and Analysis
GNFA

Endpoint Analysis

FOR408
Windows Forensic Analysis
GCFE

FOR508
Advanced Digital Forensics and Incident Response
GCFA

Malware Analysis

FOR610
Reverse Engineering Malware: Malware Analysis Tools & Techniques
GREM

FOR578
Cyber Threat Intelligence

Specialisations

FOR526
Windows Memory Forensics In-Depth

MGT535
Incident Response Team Management

FUNCTION:

PENETRATION TESTING/ VULNERABILITY ASSESSMENT

Because offense must inform defense, these experts provide enormous value to an organisation by applying attack techniques to find security vulnerabilities, analyse their business risk implications, and recommend mitigations before they are exploited by real-world attackers.

SAMPLE JOB TITLES:
Penetration tester, Vulnerability assessor, Ethical hacker, Red/Blue team member, Cyberspace engineer

CORE COURSES
SEC301 GISF › SEC401 GSEC

SEC504
Hacker Tools, Techniques, Exploits and Incident Handling
GCIH

Network & Exploits

SEC560
Network Penetration Testing and Ethical Hacking
GPEN

SEC660
Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
GXPN

SEC760
Advanced Exploit Development for Penetration Testers

Web

SEC542
Web App Penetration Testing and Ethical Hacking
GWAPT

SEC642
Advanced Web App Penetration Testing and Ethical Hacking

Mobile / Wireless

SEC575
Mobile Device Security and Ethical Hacking
GMOB

SEC617
Wireless Ethical Hacking, Penetration Testing, and Defenses
GAWN

Lab Centred

SEC561
Intense Hands-on Pen Testing Skill Development (with SANS NetWars)

SEC562
CyberCity Hands-on Kinetic Cyber Range Exercise

Specialisations

SEC580
Metasploit Kung Fu for Enterprise Pen Testing

SEC573
Python for Penetration Testers

Nov 15

FUNCTION:

SECURITY OPERATIONS CENTRE/ INTRUSION DETECTION

The Security Operations Centre (SOC) is the focal point for safeguarding against cyber-related incidents, monitoring security, and protecting assets of the enterprise network and endpoints. SOC Analysts are responsible for enterprise situational awareness and continuous surveillance, including monitoring traffic, blocking unwanted traffic to and from the Internet, and detecting any type of attack. Point solution security technologies are the starting point for hardening the network against possible intrusion attempts.

CORE COURSES
SEC301 ▸ SEC401

SEC504
Hacker Tools, Techniques, Exploits, & Incident Handling
GCIH

SAMPLE JOB TITLES:
Intrusion Detection Analyst, Security Operations Centre Analyst / Engineer, CERT Member, Cyber Threat Analyst

Endpoint Monitoring

SEC501
Advanced Security Essentials - Enterprise Defender
GCED

FOR508
Advanced Digital Forensics and Incident Response
GCFA

Network Monitoring

SEC502
Perimeter Detection In-Depth
GPPA

SEC503
Intrusion Detection In-Depth
GCIA

FOR572
Advanced Network Forensics and Analysis
GCIA

SEC511
Continuous Monitoring and Security Operations
GMON

SEC550
Active Defense, Offensive Countermeasurers, & Cyber Deception

Threat Intelligence

FOR578
Cyber Threat Intelligence

FUNCTION:

RISK & COMPLIANCE/ AUDITING/ GOVERNANCE

These experts assess and report risks to the organisation by measuring compliance with policies, procedures, and standards. They recommend improvements to make the organisation more efficient and profitable through continuous monitoring of risk management.

SAMPLE JOB TITLES:
Auditor, Compliance Officer

SEC566
Implementing & Auditing the Critical Security Controls - In-Depth
GCCC

AUD507
Auditing & Monitoring Networks, Perimeters, and Systems
GSNA

FUNCTION:

SECURE DEVELOPMENT

The security-savvy software developer leads all developers in the creation of secure software, implementing secure programming techniques that are free from logical design and technical implementation flaws.

This expert is ultimately responsible for ensuring customer software is free from vulnerabilities that can be exploited by an attacker.

SAMPLE JOB TITLES:
Developer, Software Architect, QA Tester, Development Manager

Securing the Human for Developers STH.Developer
Application Security Awareness Modules

DEV522
Defending Web Applications Security Essentials
GWEB

DEV541
Secure Coding in Java/JEE: Developing Defensible Applications
GSSP-JAVA

DEV544
Secure Coding in .NET: Developing Defensible Applications
GSSP-.NET

FUNCTION:

CYBER OR IT SECURITY MANAGEMENT

Management of people, processes, and technologies is critical for maintaining proactive enterprise situational awareness and for the ongoing success of continuous monitoring efforts. These managers must have the leadership skills, current knowledge, and best practice examples to make timely and effective decisions that benefit the entire enterprise information infrastructure.

SAMPLE JOB TITLES:
CISO, Cyber Security Manager / Officer, Security Director

Foundational

MGT512
SANS Security Leadership Essentials For Managers with Knowledge Compression™
GSLC

MGT525
IT Project Management, Effective Communication, and PMP® Exam Prep
GCPM

MGT414
SANS Training Programme for CISSP® Certification
GISP

Core

MGT514
IT Security Strategic Planning, Policy & Leadership

MGT535
Incident Response Team Management

LEG523
Law of Data Security and Investigations
GLEG

Specialisation

MGT433
Securing The Human: Building and Deploying an Effective Security Awareness Programme

AUD507
Auditing & Monitoring Networks, Perimeters, and Systems
GSNA

FUNCTION:

DIGITAL FORENSIC INVESTIGATIONS & MEDIA EXPLOITATION

With today's ever-changing technologies and environments, it is inevitable that every organisation will deal with cybercrime, including fraud, insider threats, industrial espionage, and phishing. To help solve these challenges, organisations are hiring digital forensic professionals and relying on cybercrime law enforcement agents to piece together a comprehensive account of what happened.

SAMPLE JOB TITLES:
Computer Crime Investigator, Law Enforcement, Digital Investigations Analyst, Media Exploitation Analyst, Information Technology Litigation Support & Consultant, Insider Threat Analyst

FOR408
Windows Forensic Analysis
GCFE

SEC504
Hacker Tools, Techniques, Exploits and Incident Handling
GCIH

FOR508
Advanced Digital Forensics and Incident Response
GCFA

FOR585
Advanced Smartphone Forensics

FOR518
MAC Forensic Analysis

FOR526
Memory Forensics In-Depth

FOR610
Reverse Engineering Malware: Malware Analysis Tools & Techniques
GREM

FUNCTION:

INDUSTRIAL CONTROL SYSTEMS / SCADA

ICS-focused courses are designed to equip both security professionals and control system engineers with the knowledge & skills they need to safeguard critical infrastructure.

ICS410
ICS/SCADA Security Essentials
GICSP

ICS515
ICS Active Response and Defense & Response

SAMPLE JOB TITLES:
IT & OT Support, IT & OT Cyber Security, ICS Engineer

Specialisations

SEC542
Web App Penetration Testing & Ethical Hacking
GWAPT

SEC642
Advanced Web App Penetration Testing & Ethical Hacking

SEC 401

SECURITY ESSENTIALS BOOTCAMP STYLE

Instructor: Stephen Sims
Six-Day Program: Mon 16th – Sat 21st November, 9:00am - 7:00pm (5pm on Sat)
46 CPE/CMU Credits
Laptop Required

You will learn...

- To develop effective security metrics that provide a focused playbook that IT can implement, auditors can validate, and executives can understand
- To analyze and assess the risk to your environment in order to drive the creation of a security roadmap that focuses on the right areas of security
- Practical tips and tricks to focus in on high-priority security problems within your organisation and on doing the right things that will lead to security solutions that work
- Why some organisations are winning and some are losing when it comes to security and, most importantly, how to be on the winning side
- The core areas of security and how to create a security program that is anchored on PREVENT-DETECT-RESPOND.

Course details

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

Is SEC401: Security Essentials Bootcamp Style the right course for you?

STOP and ask yourself the following questions:

1. Do you fully understand why some organisations get compromised and others do not?
2. If there were compromised systems on your network, are you confident that you would be able to find them?
3. Do you know the effectiveness of each security device and are you certain that they are all configured correctly?
4. Are proper security metrics set up and communicated to your executives to drive security decisions?

If you do not know the answers to these questions, SEC401 course will provide the information security training you need in a bootcamp-style format that is reinforced with hands-on labs.

"Security Essentials 401 has relit my passion and excitement for Information Security."
Emma Baker, Capgemini

SEC 501

ADVANCED SECURITY ESSENTIALS - ENTERPRISE DEFENDER

Instructor: Paul A. Henry
Six-Day Program: Mon 16th – Sat 21st November, 9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required

Course details

Effective cybersecurity is more important than ever as attacks become stealthier, have a greater financial impact, and cause broad reputational damage. SEC501: Advanced Security Essentials - Enterprise Defender builds on a solid foundation of core policies and practices to enable security teams to defend their enterprise.

It has been said of security that "prevention is ideal, but detection is a must." However, detection without response has little value. Network security needs to be constantly improved to prevent as many attacks as possible and to swiftly detect and respond appropriately to any breach that does occur. This PREVENT - DETECT - RESPONSE strategy must be in place both externally and internally. As data become more portable and networks continue to be porous, there needs to be an increased focus on data protection. Critical information must be secured regardless of whether it resides on a server, in a robust network architecture, or on a portable device.

Of course, despite an organisation's best efforts to prevent network attacks and protect its critical data, some attacks will still be successful. Therefore, organisations need to be able to detect attacks in a timely fashion. This is accomplished by understanding the traffic that is flowing on your networks, looking for indications of an attack, and performing penetration testing and vulnerability analysis against your organisation to identify problems and issues before a compromise occurs.

Finally, once an attack is detected we must react quickly and effectively and perform the forensics required. Knowledge gained by understanding how the attacker broke in can be fed back into more effective and robust preventive and detective measures, completing the security lifecycle.

You will learn...

- How to build a comprehensive security program focused on preventing, detecting, and responding to attacks
- Core components of building a defensible network infrastructure and how to properly secure routers, switches, and network infrastructure
- Methods to detect advanced attacks of systems that are currently compromised
- Formal methods for performing a penetration test to find weaknesses in an organisation's security apparatus
- Ways to respond to an incident and how to execute the six-step process of incident response: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned
- Approaches to remediating malware and how to clean up a compromised system

"SEC501 offers a great explanation of Net Defense best practices that often get overlooked."
Kirk G, U.S. Navy

SEC 503

INTRUSION DETECTION IN-DEPTH

Instructor: Jess Garcia

Six-Day Program: Mon 16th – Sat 21st November, 9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required

You will learn...

- How to analyze traffic traversing your site to avoid becoming another "Hacked!" headline
- How to place, customize, and tune your IDS/IPS for maximum detection
- Hands-on detection, analysis, and network forensic investigation with a variety of open-source tools
- TCP/IP and common application protocols to gain insight about your network traffic, enabling you to distinguish normal from abnormal traffic
- The benefits of using signature-based, flow, and hybrid traffic analysis frameworks to augment detection

Course details

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.

SEC503 is most appropriate for students who are or will become intrusion detection/prevention or security analysts, although others may benefit from the course as well. Students range all the way from seasoned analysts to novices with some TCP/IP background, but to keep pace with the class students are expected to have at least a basic working knowledge of TCP/IP (see www.sans.org//media/security-training/tcpip_quiz.php). Please note that the Packetrix VMware used in class is a Linux distribution, so we strongly recommend that you spend some time getting familiar with a Linux environment that uses the command line for entry, along with learning some of the core Unix commands, before coming to class.

"Course was designed around real-world intrusions and is highly needed for network security administrators and/or analysts."

Hector Araiza, U.S. Air Force

SEC 504

HACKER TOOLS, TECHNIQUES, EXPLOITS & INCIDENT HANDLING

Instructor: Steve Armstrong

Six-Day Program: Mon 16th – Sat 21st November, 9:00am - 7:15pm
37 CPE/CMU Credits
Laptop Required

Course details

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organisation has an Internet connection or one or two disgruntled employees (and whose doesn't!), 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.

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

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

You will learn...

- How best to prepare for an eventual breach
- The step-by-step approach used by many computer attackers
- Proactive and reactive defenses for each stage of a computer attack
- How to identify active attacks and compromises
- The latest computer attack vectors and how you can stop them
- How to properly contain attacks
- How to ensure that attackers do not return
- How to recover from computer attacks and restore systems for business
- How to understand and use hacking tools and techniques
- Strategies and tools for detecting each type of attack
- Attacks and defenses for Windows, Unix, switches, routers, and other systems
- Application-level vulnerabilities, attacks, and defenses
- How to develop an incident handling process and prepare a team for battle
- Legal issues in incident handling

"As someone who works in information security but has never had to do a full incident report, SEC504 is teaching me all the proper processes and steps."

Todd Choryan, Motorola Solutions

SEC 511

CONTINUOUS MONITORING AND SECURITY OPERATIONS

Instructor: Eric Conrad

Six-Day Program: Mon 16th – Sat 21st November, 9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required

You will learn...

- Analyze a security architecture for deficiencies
- Apply the principles learned in the course to design a defensible security architecture
- Understand the importance of a detection-dominant security architecture and security operations centers (SOC)
- Identify the key components of Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/ Continuous Monitoring (CM)
- Determine appropriate security monitoring needs for organisations of all sizes
- Implement a robust Network Security Monitoring/Continuous Security Monitoring (NSM/CSM)
- Determine requisite monitoring capabilities for a SOC environment
- Determine capabilities required to support continuous monitoring of key Critical Security Controls
- Utilize tools to support implementation of Continuous Monitoring (CM) per NIST guidelines SP 800-137

Course details

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

The Defensible Security Architecture, Network Security Monitoring (NSM)/ Continuous Diagnostics and Mitigation (CDM)/ Continuous Security Monitoring (CSM), taught in this course will best position your organisation or Security Operations Centre (SOC) to analyse threats and detect anomalies that could indicate cybercriminal behaviour. The payoff for this new proactive approach would be early detection of an intrusion, or successfully thwarting the efforts of attackers altogether. The National Institute of Standards and Technology (NIST) developed guidelines described in NIST SP 800-137 for Continuous Monitoring (CM), and Your SEC511 journey will conclude with one last hill to climb!

The final day (Day 6) features a capture-the-flag competition that challenges you to apply the skills and techniques learned in the course to detect and defend the modern security architecture that has been designed. Course authors Eric Conrad and Seth Misenar have designed the capture-the-flag competition to be fun, engaging, comprehensive, and challenging. You will not be disappointed!

SEC 542

WEB APP PENETRATION TESTING AND ETHICAL HACKING

Instructor: Pieter Danhieux

Six-Day Program: Mon 16th – Sat 21st November, 9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required

Course details

Web applications play a vital role in every modern organisation. This becomes apparent when adversaries compromise these applications, damage business functionality and steal data.

Unfortunately, many organisations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems. SEC542 helps students move beyond push-button penetration testing to professional web application penetration testing that finds flaws before the adversaries discover and abuse them.

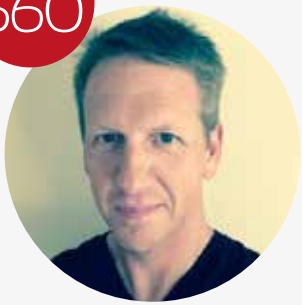
Modern cyber defence requires a realistic and thorough understanding of web application security issues. Anyone can learn to sling a few web hacks, but web application penetration testing requires something deeper. SEC542 will enable students to capably assess a web application's security posture and convincingly demonstrate the impact of inadequate security that plagues most organisations. Students will come to understand major web application flaws and their exploitation and, most importantly, learn a field-tested and repeatable process to consistently find these flaws and convey what they have learned to their organisations.

You will learn...

- To apply a repeatable methodology to deliver high-value penetration tests.
- How to discover and exploit key web application flaws.
- How to explain the potential impact of web application vulnerabilities.
- The importance of web application security to an overall security posture.
- How to wield key web application attack tools more efficiently.

"Every class gives you invaluable information from real-world testing you cannot find in a book."
David Fava, The Boeing Company

SEC 560



NETWORK PENETRATION TESTING AND ETHICAL HACKING

Instructor: Bryce Galbraith

Six-Day Program: Mon 16th – Sat 21st November, 9:00am - 5:00pm
37 CPE/CMU Credits
Laptop Required

You will learn...

- How to perform a detailed, end-to-end professional penetration test using the best methodologies in the industry
- Hands-on skills to use the most powerful ethical hacking tools, including Nmap, Nessus, Metasploit, John the Ripper, Rainbow Tables, web application attack tools and more
- How to utilize built-in operating system tools on Windows and Linux in a weaponized fashion so that you can pen test while living off the land, avoiding the risk of installing third-party tools
- How to provide true business value through in-depth technical excellence in network penetration testing and ethical hacking
- How to structure and conduct a network penetration testing project with maximum efficiency and appropriate safety

Course details

This course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks and wireless and web apps, with over 30 detailed hands-on labs throughout.

Learn the best ways to test your own systems before the bad guys attack.

Chock full of practical, real-world tips from some of the world's best penetration testers, SEC560 prepares you to perform detailed reconnaissance by examining a target's infrastructure and mining blogs, search engines, social networking sites and other Internet and intranet infrastructure. You will be equipped to scan target networks using best-of-breed tools. We will not just cover run-of-the-mill options and configurations, we will also go over the less-known but highly useful capabilities of the best pen test toolsets available today. After scanning, you will learn dozens of methods for exploiting target systems to gain access and measure real business risk, then examine post-exploitation, password attacks, wireless and web apps, pivoting through the target environment to model the attacks of real-world bad guys.

You will bring comprehensive penetration testing and ethical hacking know-how back to your organisation.

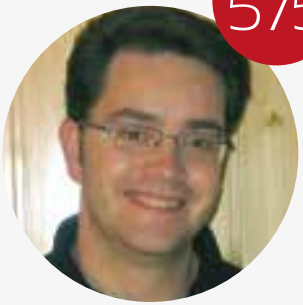
After building your skills in challenging labs over five days, the course culminates with a full-day, real-world network penetration test scenario. You will conduct an end-to-end penetration test, applying the knowledge, tools and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organisation.

"SANS is really the only information security training available and is therefore valuable on its own. The wide subject areas, relating to penetration testing, are what makes SEC560 particularly valuable."

Nicholas Capalbo, Federal Reserve of New York

SEC 575

MOBILE DEVICE SECURITY AND ETHICAL HACKING



Instructor: Raul Siles

Six-Day Program: Mon 16th – Sat 21st November, 9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required

Course details

Mobile phones and tablets have become essential to enterprise and government networks ranging from small organisations to Fortune 500 companies and large agencies. Often, mobile phone deployments grow organically, adopted by multitudes of end-users for convenient email access, as well as by managers and executives who need access to sensitive organisational resources from their favored personal mobile devices. In other cases, mobile phones and tablets have become critical systems for a wide variety of production applications from enterprise resource planning (ERP) to project management.

For all of its convenience, however, the ubiquitous use of mobile devices in the work place and beyond has brought new security risks. As reliance on these devices has grown exponentially, organisations have quickly recognized that mobile phones and tablets need greater security implementations than a simple screen protector and clever password. Whether an Apple iPhone or iPad, a Windows Phone, or an Android or BlackBerry phone or tablet, these devices have become hugely attractive and vulnerable targets for nefarious attackers. The use of such devices poses an array of new risks to organisations, including:

- Distributed sensitive data storage and access mechanisms
- Lack of consistent patch management and firmware updates
- High probability of the device being hacked, lost or stolen

Mobile code and apps are also introducing new avenues for malware and data leakage, exposing critical enterprise secrets, intellectual property, and personally identifiable information assets to attackers. To further complicate matters, today there simply are not enough people with the security skills needed to manage mobile phone and tablet deployments.

You will learn...

- How to capture and evaluate mobile application network activity
- How to decrypt and manipulate Apple iOS application behavior
- How to identify the steps taken by Android malware
- How to reverse-engineer and change Android applications in the Google Play Store
- How to conduct mobile device and mobile application penetration tests

"In the fast paced world of Bring Your Own Device (BYOD) and mobile device management, SEC575 is a must course for infosec managers."

Jude Meche, DSCC

SEC 579

VIRTUALIZATION AND PRIVATE CLOUD SECURITY

Instructor: Dave Shackleford

Six-Day Program: Mon 16th – Sat 21st November, 9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required

You will learn...

- Best practices for configuring and designing virtual security controls and infrastructure
- Vulnerabilities and threats related to virtual infrastructure and cloud environments
- How the network security landscape (products and architecture) is changing with virtualization and private clouds
- New vulnerability assessment and forensic techniques to use within a virtual environment
- How scripting and automation can assist with audits in a virtual environment

Course details

One of today's most rapidly-evolving and widely-deployed technologies is server virtualization. Many organisations are already realizing the cost savings from implementing virtualized servers, and systems administrators love the ease of deployment and management for virtualized systems. More and more organisations are deploying desktop, application and network virtualization, as well. There are even security benefits of virtualization - easier business continuity and disaster recovery, single points of control over multiple systems, role-based access, and additional auditing and logging capabilities for large infrastructures.

With these benefits comes a dark side, however. Virtualization technology is the focus of many new potential threats and exploits and presents new vulnerabilities that must be managed. In addition, there are a vast number of configuration options that security and system administrators need to understand, with an added layer of complexity that has to be managed by operations teams. Virtualization technologies also connect to network infrastructure and storage networks and require careful planning with regard to access controls, user permissions, and traditional security controls.

In addition, many organisations are evolving virtualized infrastructure into private clouds internal shared services running on virtualized infrastructure. Security architecture, policies, and processes will need to adapt to work within a cloud infrastructure, and there are many changes that security and operations teams will need to accommodate to ensure assets are protected.course concludes with a one-day Capture the Flag event that will test both your ability to apply your new tools and coding skills in a penetration testing challenge

"The rush for virtualization is difficult for security sensitive environments. SEC579 helps demonstrate which risks are valid."

Paul Mayers, Lloyds Banking Group

SEC 660

ADVANCED PENETRATION TESTING, EXPLOIT WRITING, & ETHICAL HACKING

Instructor: James Lyne

Six-Day Program: Mon 16th – Sat 21st November, 9:00am - 7:00pm
46 CPE/CMU Credits
Laptop Required

Course details

SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking is designed as a logical progression point for those who have completed SANS SEC560: Network Penetration Testing and Ethical Hacking, or for those with existing penetration testing experience. Students with the prerequisite knowledge to take this course will walk through dozens of real-world attacks used by the most seasoned penetration testers. The methodology of a given attack is discussed, followed by exercises in a hands-on lab to consolidate advanced concepts and facilitate the immediate application of techniques in the workplace.

SEC660 starts off by introducing advanced penetration concepts and providing an overview to prepare students for what lies ahead. The focus of day one is on network attacks, an area often left untouched by testers. Topics include accessing, manipulating, and exploiting the network. Attacks are performed against NAC, VLANs, OSPF, 802.1X, CDP, IPv6, VOIP, SSL, ARP, SNMP, and others. Day two starts with a technical module on performing penetration testing against various cryptographic implementations, then turns to network booting attacks, escaping Linux restricted environments such as chroot, and escaping Windows restricted desktop environments. Day three jumps into an introduction of Python for penetration testing, Scapy for packet crafting, product security testing, network and application fuzzing, and code coverage techniques. Days four and five are spent exploiting programs on the Linux and Windows operating systems. You will learn to identify privileged programs, redirect the execution of code, reverse-engineer programs to locate vulnerable code, obtain code execution for administrative shell access, and defeat modern operating system controls such as ASLR, canaries, and DEP using ROP and other techniques. Local and remote exploits as well as client-side exploitation techniques are covered. The final course day is devoted to numerous penetration testing challenges that require students to solve complex problems and capture flags.
Among the biggest benefits of SEC660 is the expert-level hands-on guidance provided through the labs and the additional time allotted each evening to reinforce daytime material and master the exercises.

You will learn...

- How to perform penetration testing safely against network devices such as routers, switches, and NAC implementations.
- How to test cryptographic implementations.
- How to exploit environments using virtualization and network booting technology such as PXE.
- How to fuzz network and stand-alone applications.
- How to write exploits against applications running on Linux and Windows systems.
- How to bypass exploit mitigations such as ASLR, DEP, and stack canaries.

"No frills and goes right to the point. The first day alone is what other classes spend a full week on."
Michael Isbitski, Verizon Wireless

FOR 408

WINDOWS FORENSIC ANALYSIS

Instructor: Rob Lee
Six-Day Program: Mon 13th – Sat 18th November, 9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required

You will learn...

- How to conduct in-depth forensic analysis of Windows operating systems and media exploitation focusing on Windows 7, Windows 8/8.1, XP, and Windows Server 2008/2012
- How to identify artifact and evidence locations to answer critical questions, including application execution, file access, data theft, external device usage, cloud services, geo-location, file download, anti-forensics, and detailed system usage
- How to focus your capabilities on analysis instead of how to use a specific tool
- How to extract key answers and build an in-house forensic capability via a variety of free, open-source, and commercial tools provided within the SANS Windows SIFT Workstation

Course details

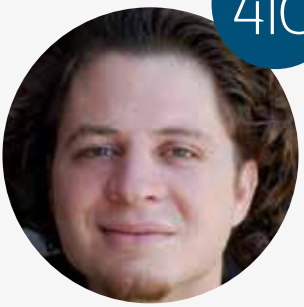
FOR408: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of the Microsoft Windows operating systems. You can't protect what you don't know about, and understanding forensic capabilities and artifacts is a core component of information security. Learn to recover, analyse, 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, Windows 8/8.1, Office and Office365, cloud storage, Sharepoint, Exchange, Outlook,). Students leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Nothing is left out - attendees learn to analyse everything from legacy Windows XP systems to just discovered Windows 8.1 artifacts.

"Best forensics course I have taken to date. Vast amounts of information."
Ellen Clark, FBI

ICS 410

ICS/SCADA SECURITY ESSENTIALS



Instructor: Justin Searle
Five-Day Program: Mon 16th – Fri 20th November, 9:00am - 5:00pm
30 CPE/CMU Credits
Laptop Required

Course details

SANS has joined forces with industry leaders to equip security professionals and control system engineers with the cybersecurity skills they need to defend national critical infrastructure. ICS410: ICS/SCADA Security Essentials provides a foundational set of standardized skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

The course will provide you with:

- An understanding of industrial control system components, purposes, deployments, significant drivers, and constraints.
- Hands-on lab learning experiences to control system attack surfaces, methods, and tools
- Control system approaches to system and network defense architectures and techniques
- Incident-response skills in a control system environment
- Governance models and resources for industrial cybersecurity professionals.

You will learn...

- How to run Windows command line tools to analyse the system looking for high-risk items
- How to run Linux command line tools (ps, ls, netstat, ect) and basic scripting to automate the running of programs to perform continuous monitoring of various tools
- How to install VMWare and create virtual machines to create a virtual lab to test and evaluate tools/ security of systems
- How to better understand various industrial control systems and their purpose, application, function, and dependencies on network IP and industrial communications
- How to work with operating systems (system administration concepts for Unix/Linux and/or Windows operating systems)
- How to work with network infrastructure design (network architecture concepts, including topology, protocols, and components)
- How to better understand the systems' security lifecycle
- How to better understand information assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)

"Great introduction into ICS landscape and associated security concerns. The ICS material presented will provide immediate value relative to helping secure my company."
Mike Poulos, Coca-Cola Enterprises

SANS LONDON 2015

INSTRUCTORS

SANS instructors are considered the best in the world. Not only do they meet SANS' stringent requirements for excellence, they are also all real-world practitioners. The instructors ensure that what you learn in class will be up to date and relevant to your job.

We have an outstanding line up of European and US-based instructors at SANS London 2015. Read on for profiles of this elite group.

STEVE ARMSTRONG

Certified Instructor

Steve started working in the security arena in 1994 whilst serving in the UK Royal Air Force. He specialized in the technical aspects of IT security from 1997 onward, and before retiring from active duty, he lead the RAF's penetration and TEMPEST testing teams. He founded Logically Secure in 2006 to provide specialist security advice to government departments, defense contractors, the online video gaming industry, and both music and film labels worldwide.

In addition to contributing to the OSSTMM and authoring the SME targeted Certified Digital Security (CDS) standard and the music and film industry's digital security standards (CDSA), Steve provides wireless penetration testing and incident response services for some of the biggest household names in media.

ERIC CONRAD

Senior Instructor

SANS Senior Instructor Eric Conrad is the lead author of SANS MGT414: SANS Training Program for CISSP® Certification, and coauthor of both SANS SEC511: Continuous Monitoring and Security Operations and SANS SEC542: Web App Penetration Testing and Ethical Hacking. He is also the lead author of the books the CISSP Study Guide, and the Eleventh Hour 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 health care. He is now CTO of Backshore Communications, a company focusing on hunt teaming, intrusion detection, incident handling, 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.

PIETER DANHIEUX

Certified Instructor

Pieter Danhieux is a certified instructor for the SANS Institute, teaching military, government, and private organisations offensive techniques on how to target and assess organisations, systems, and individuals for security weaknesses. He is also one of the founders of the security and hacking conference BRUCON in Belgium.

Pieter has worked in the cyber security space since 2002. He was one of the youngest persons ever in Belgium to obtain the Certified Information Systems Security Professional (CISSP) certification. He then obtained the Certified Information Systems Auditor (CISA) and the GIAC Certified Forensics Analyst program (GCFA) and is currently one of the select few people worldwide to hold the GIAC Security Expert (GSE) certification.

Pieter currently runs a software engineering and cyber security company with a bunch of intelligent geeks in Australia. Until January 2015, he was an executive at BAE Systems in his role as Head of Delivery of the Applied Intelligence business unit. Before that, Pieter worked for seven years at Ernst & Young in Europe as one of their information security experts running a team of attack and penetration resources operating in the financial industry and telecommunication space.

BRYCE GALBRAITH

Principal Instructor

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

JESS GARCIA

Principle Instructor

Jess Garcia, founder of One eSecurity, is a Senior Security Engineer with over 15 years of experience in Information Security.

During the last 5 years Jess has worked in highly sensitive projects in Europe, USA, Latin America and the Middle East with top global customers in sectors such as financial & insurance, corporate, media, health, communications, law firms or government, in areas such as Incident Response & Computer Forensics, Malware Analysis, Security Architecture Design and Review, etc.

Previously, Jess worked for 10 years as a systems, network and security engineer in the Spanish Space Agency, where he collaborated as a security advisor with the European Space Agency, NASA, and other international organisations.

Jess is a frequent speaker at security events, having been invited to dozens of them around the world during the last few years. Jess has also contributed to several books, articles, SANS courseware, the GIAC program, etc. Jess is an active security researcher in areas such as Incident Response and Computer Forensics or Honeynets.

Jess holds a Masters of Science in Telecommunications Engineering from the Univ. Politecnica de Madrid.

PAUL A. HENRY

Senior Instructor

Paul Henry is a Senior Instructor with the SANS Institute and one of the world's foremost global information security and computer forensic experts with more than 30 years of experience covering all 10 domains of network security. Paul began his career in critical infrastructure / process control supporting power generation and currently manages security initiatives and incident response for Global 2000 enterprises and government organisations worldwide.

Paul is a principal at vNet Security, LLC and is keeping a finger on the pulse of network security as the security and forensic analyst at Lumension Security and as a retained security expert for multiple financial and healthcare firms.

ROB LEE

Fellow

Rob Lee is an entrepreneur and consultant in the Washington, DC area, specializing in information security, incident response, and digital forensics. Rob is currently the curriculum lead and author for digital forensic and incident response training at the SANS Institute in addition to owning his own firm. Rob has more than 15 years of experience in computer forensics, vulnerability and exploit discovery, intrusion detection/prevention, and incident response.

Rob graduated from the U.S. Air Force Academy and served in the U.S. Air Force as a founding member of the 609th Information Warfare Squadron, the first U.S. military operational unit focused on information warfare. Rob co-authored the book Know Your Enemy, 2nd Edition. Rob earned his MBA from Georgetown University in Washington DC. He was awarded the Digital Forensic Examiner of the Year from the Forensic 4Cast Awards. Rob is an ardent blogger about computer forensics and incident response topics at the SANS Computer Forensic Blog. Rob is also a co-author of the MANDIANT threat intelligence report M-Trends: The Advanced Persistent Threat.

JAMES LYNE

Certified Instructor

Director, EMEA at SANS and Director of Technology Strategy at security firm Sophos. James comes from a background in cryptography but over the years has worked in a wide variety of security problem domains including anti-malware and hacking. James spent many years as a hands-on analyst dealing with deep technical issues and is a self-professed "massive geek". Eventually James escaped dark rooms and learned some social skills, and today is a keen presenter at conferences and industry events. With a wide range of experience working in a technical and a strategic capacity from incident response to forensics with some of the world's largest and most paranoid organisations James participates in industry panels, policy groups, and is a frequently-called-upon expert advisor all over the world. James is a frequent guest lecturer and often appears in the media including national TV. As a young spokesperson for the industry James is extremely passionate about talent development and participates in initiatives to identify new talent for the industry and to develop it. Ask James to show you his best geek party trick.

JUSTIN SEARLE

Certified Instructor

Justin Searle is a Managing Partner of UtiliSec, specializing in Smart Grid security architecture design and penetration testing. Justin led the Smart Grid Security Architecture group in the creation of NIST Interagency Report 7628 and played key roles in the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG). He currently leads the testing group at the National Electric Sector Cybersecurity Organisation Resources (NESCOR). Justin has taught courses in hacking techniques, forensics, networking, and intrusion detection for multiple universities, corporations, and security conferences. Mr. Searle is currently a certified instructor for the SANS Institute. In addition to electric power industry conferences, Justin frequently presents at top international security conferences such as Black Hat, DEFCON, OWASP, Nullcon, and AusCERT. Justin co-leads prominent open source projects including the Samurai Web Testing Framework (SamuraiWTF), the Samurai Security Testing Framework for Utilities (SamuraiSTFU), Middler, Yokoso!, and Laudanum. Justin has an MBA in International Technology and is a CISSP and SANS GIAC certified Incident Handler (GCIH), Intrusion Analyst (GCIA), and Web Application Penetration Tester (GWAPT).

RAUL SILES

Certified Instructor

Raul Siles is a founder and senior security analyst with Taddong. His more than 10 years of expertise performing advanced security services and solutions in various worldwide industries include security architecture design and reviews, penetration tests, incident handling, forensic analysis, security assessments, and information security research in new technologies, such as Web applications, wireless, honeynets, virtualization, mobile devices, and VoIP. Raul is one of the few individuals who have earned the GIAC Security Expert (GSE) designation. He is a SANS Institute author and instructor of penetration testing courses, a regular speaker at security conferences, author of security books and articles, and contributes to research and open-source projects. He loves security challenges, is a member of international organisations, such as the Honeynet Project, and is a handler for the Internet Storm Center (ISC). Raul holds a master's degree in computer science from UPM (Spain) and a postgraduate in security and e-commerce.

STEPHEN SIMS

Senior Instructor

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

DAVE SHACKLEFORD

Senior Instructor

Dave Shackleford is the owner and principal consultant of Voodoo Security and a SANS analyst, senior instructor, and course author. He has consulted with hundreds of organisations in the areas of security, regulatory compliance, and network architecture and engineering, and is a VMware vExpert with extensive experience designing and configuring secure virtualized infrastructures. He has previously worked as CSO for Configuresoft, CTO for the Center for Internet Security, and as a security architect, analyst, and manager for several Fortune 500 companies. Dave is the author of the Sybex book Virtualization Security:

Protecting Virtualized Environments, as well as the coauthor of Hands-On Information Security from Course Technology. Recently Dave coauthored the first published course on virtualization security for the SANS Institute. Dave currently serves on the board of directors at the SANS Technology Institute and helps lead the Atlanta chapter of the Cloud Security Alliance.

EVENT LOCATION & TRAVEL INFORMATION SANS LONDON 2015

Event Location:
Grand Connaught Rooms 61-65 Great Queen Street, London, WC2B 5DA
Telephone: +44 (0)20 7405 7811
E-mail: enquires.gcr@principal-hayley.com
Website: www.grandconnaughtrooms.com

Arriving by London Underground

- Nearest Underground stations: Covent Garden and Holborn
- Covent Garden Underground station (Piccadilly line) is a short walk from the venue
- Holborn Underground station (Piccadilly and Central Line) is also a short walk

Arriving by Mainline Train

- Nearest station: Kings Cross
- London Euston, Kings Cross and St Pancras International stations are under a thirty minute walk from the venue or a short taxi ride
- Kings Cross station is just three stop away on the London Underground's Piccadilly line
- All of London's remaining main-line stations, including London Victoria, Paddington and Waterloo are easily reached by the Underground network

Arriving by Air

- Nearest airport: London Heathrow International airport
- London Heathrow International airport is 18 miles away
- All of London's international and domestic airports have excellent links into central London

By Car

Satellite navigation coordinates:
51.515567, - 0.120687
(post code WC2B 5DA)

Hotels

There are many hotels in the area. SANS partner hotel is Hotel Russell, 1 - 8 Russell Square, London, WC1B 5BE

SANS London attendees can receive a special rate of £165 exc. VAT including breakfast at the Hotel Russell near to the Grand Connaught Rooms during SANS London 2015.

Simply quote booking code SANS141114 when booking through their reservations department on +44 (0)207 520 1827 or russell.reservations@principal-hayley.com to receive the rate.
www.hotelrussellllondon.co.uk

CHALLENGE YOURSELF BEFORE THE ENEMY DOES

NETWARS

NetWars is a series of hands-on, in-depth computer and network security challenges designed to test a participant's experience and skills. NetWars Tournament comes in two forms Core and DFIR.

Core NetWars Tournament

SANS Core NetWars is a suite of hands-on, interactive learning scenarios that enable information security professionals to develop and master the real-world, in-depth skills they need to excel in their field. In SANS' award-winning courses, attendees consistently rate our hands-on exercises as the most valuable part of the course. With Core NetWars, we have really raised the ante, as participants learn in a cyber range while working through various challenge levels, all hands-on, with a focus on mastering the skills information security professionals can use in their jobs every day.

Who should attend?

- Security professionals
- System administrators
- Network administrators
- Ethical hackers
- Penetration testers
- Incident handlers
- Security auditors
- Vulnerability assessment personnel
- Security Operations Center (SOC) staff members

DFIR NetWars Tournament

SANS DFIR NetWars Tournament is an incident simulator packed with a vast amount of forensic and incident response challenges. DFIR NetWars Tournament is packed with challenges covering host forensics, network forensics, and malware and memory analysis. It is developed by incident responders and analysts who use these skills daily to stop data breaches and solve crimes. Sharpen your team's skills prior to being involved in a real incident.

Who should attend?

- Digital forensic analysts
- Reverse engineering and malware analysts
- Incident responders
- Law enforcement officers, federal agents, or detectives
- Forensic examiners
- Security erations Center (SOC) analysts
- Cyber crime inves tigators
- Media exploitation analysts

sans.org/netwars

Students who register and pay for any long course (5 or 6 days) at a SANS event that includes a NetWars Tournament may participate in the tournament at that event free of charge.

SANS SECURING THE HUMAN SECURITY AWARENESS TRAINING

SANS Securing The Human was created to provide computer-based security awareness training for end users. The product line has since expanded to serve end users, developers, ICS engineers, utilities, and the healthcare market.

Securing The Human Key Benefits:

- Computer based training enables employees to take training at a time and place that is convenient for them
- Short modular videos allow employees to complete the training in multiple short sessions
- A choice of 43 modules allows training to be tailored to address specific audiences
- Module quiz questions test learner comprehension
- Track training completion for compliance reporting purposes
- 29 language options offer consistent training across your entire organisation regardless of location
- Goes beyond compliance and focuses on changing behavior

How can we help?
www.securingthehuman.org/resources/getting-support

For more information about Securing The Human, to request a demo or if you want advice on how to plan your awareness program contact our expert team:

Phone: +44 203 3384 3470
Email: mtudge@sans.org

www.securingthehuman.org

FUTURE SANS EMEA TRAINING EVENTS 2015/16

For a full list of training events, please visit www.sans.org

		IT AUDIT	DEVELOPER	MANAGE	FORENSICS								ICS/SCADA		SECURITY														
		6 DAYS	6 DAYS	5 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	5 DAYS	6 DAYS	6 DAYS	5 DAYS	5 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	5 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS
LOCATION	DATE	AUD507	DEV522	MGT512	FOR408	FOR508	FOR518	FOR526	FOR572	FOR578	FOR585	FOR610	ICS410	ICS515	SEC401	SEC501	SEC503	SEC504	SEC505	SEC511	SEC542	SEC560	SEC566	SEC573	SEC575	SEC579	SEC660	SEC760
LONDON	NOV 14TH - 23RD			●	●								●		●	●	●	●		●	●	●			●	●	●	●
CAPE TOWN	NOV 30TH - DEC 5TH					●									●			●										
DUBAI, 2016	JAN 9TH - 14TH													●			●					●						
BRUSSELS WINTER, 2016	JAN 18TH - 23RD				●				●						●			●			●							
COPENHAGEN, 2016	FEB 1ST - 6TH																											
MUNICH WINTER, 2016	FEB 15TH - 20TH										●	●			●				●	●								
LONDON SPRING, 2016	FEB 29TH - MAR 5TH	●				●		●							●			●			●	●			●			●
ABU DHABI, 2016	MAR 12TH - 17TH			●										●														
SECURE EUROPE, 2016	APR 4TH - 15TH				●				●						●	●	●	●					●				●	
ICS AMSTERDAM, 2016	APR 18TH - 23RD												●	●														
PRAGUE, 2016	MAY 9TH - 14TH														●			●		●		●						
PEN TEST BERLIN, 2016	JUN 20TH - 25TH																	●			●	●		●				●
LONDON SUMMER, 2016	JUL 11TH - 16TH																											
ICS LONDON, 2016	SEP 19TH - 25TH																											

Most courses are also available online, via SANS OnDemand. Contact emea@sans.org for information.

Dates, locations and courses offered subject to change