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

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

SANS EMEA

MON 29 FEB - SAT 5 MAR, 2016

SANS LONDON SPRING

#SANSLondon

8 SANS COURSES

SEC401
Security Essentials Bootcamp Style

SEC504
Hacker Tools, Techniques, Exploits and Incident Handling

SEC542
Web App Penetration Testing and Ethical Hacking

SEC560
Network Penetration Testing and Ethical Hacking

SEC760
Advanced Exploit Development for Penetration Testers

FOR508
Advanced Digital Forensics and Incident Response

FOR526
Memory Forensics In-Depth Techniques

AUD507
Auditing & Monitoring Networks, Perimeters & Systems

Register online and see full course descriptions at **www.sans.org/london-in-the-spring-2016**

Save 450 Euro with discount code "EarlyBird16" for any course by 20th Jan, 2016

HM Government

SANS is a Cyber Security Supplier to Government

GIAC

COURSES AT A GLANCE

			MONDAY 29	TUESDAY 01	WEDNESDAY 02	THURSDAY 03	FRIDAY 04	SATURDAY 05
SEC 401	Security Essentials Bootcamp Style	Dr. Eric Cole	PG 8					
SEC 504	Hacker Tools, Techniques, Exploits and Incident Handling	Steve Armstrong	PG 9					
SEC 542	Web App Penetration Testing and Ethical Hacking	Pieter Danhieux	PG 10					
SEC 560	Network Penetration Testing and Ethical Hacking	Erik Van Buggenhout	PG 11					
SEC 760	Advanced Exploit Development for Penetration Testers	Jake Williams	PG 12					
FOR 508	Advanced Digital Forensics and Incident Response	Jess Garcia	PG 13					
FOR 526	Memory Forensics In-Depth	Alissa Torres	PG 14					
AUD 507	Auditing & Monitoring Networks, Perimeters & Systems	David Hoelzer	PG 15					

Register now: www.sans.org/london-in-the-spring-2016

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 programmes 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 1000 people tried out for the SANS faculty, but only a handful of potential instructors were selected.

SANS provides training through several delivery methods, both live and virtual: classroom-style at a training event, online at your own pace, guided study with a local mentor, or private training 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 certification programme and numerous free security resources such as newsletters, whitepapers, and webcasts.

Contact SANS
Tel +44 203 384 3470
Email emea@sans.org

@SANSEMEA ##SANSLondon

CONTENTS

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

WELCOME TO SANS LONDON SPRING 2016

SANS London Spring 2016 runs from Monday 29th February to Saturday 5th March at the Grand Connaught Rooms and hosts 8 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 hotel restaurant. Accommodation is not included.

Training runs from 9am-5pm except for course SEC401 that finishes at 7pm Monday-Friday and 5pm on Saturday and SEC504 and SEC560 that finish at 7:15pm on Monday. SEC760 runs from 9am-5pm and then restarts 5:15pm – 7pm Monday-Friday and finishes at 5pm Saturday.

Students are able to attend free SANS@Night talks and evening social functions. The demand for places at London events is always high so please register online as soon as possible to secure a seat at SANS London Spring 2016.

Read on for course descriptions or visit www.sans.org/london-in-the-spring-2016 . Over the page you will find the SANS Career Roadmap which provides examples of how SANS courses fit into your career development plan.

EVENT LOCATION

Hotel:
Grand Connaught Rooms
61-65 Great Queen Street
London, GB
WC2B 5DA

Telephone:
+44 (0) 20 7405 7811
E-mail:
enquires.gcr@principal-hayley.com
Website:
www.grandconnaughtrooms.com

SANS LONDON SPRING 2016 REGISTRATION INFORMATION

REGISTER ONLINE AT: WWW.SANS.ORG/LONDON-IN-THE-SPRING-2016

REGISTER EARLY AND SAVE

Register for #SANSLondon and pay before the 20th of January and save €450 by entering the code EarlyBird16

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/london-in-the-spring-2016 . Select your course 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 Feb 10th, 2016, by emailing emea@sans.org

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**

Nov 15

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**
      - **FOR508** Advanced Digital Forensics and Incident Response **GCFA**
        - **FOR578** Cyber Threat Intelligence
  - Endpoint Analysis
    - **FOR408** Windows Forensic Analysis **GCFE**
  - Malware Analysis
    - **FOR610** Reverse Engineering Malware: Malware Analysis Tools & Techniques **GREM**

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
    - **SEC542** Web App Penetration Testing and Ethical Hacking **GWAPT**
      - **SEC642** Advanced Web App Penetration Testing and Ethical Hacking
  - Web
    - **SEC575** Mobile Device Security and Ethical Hacking **GMOB**
      - **SEC617** Wireless Ethical Hacking, Penetration Testing, and Defenses **GAWN**
  - Mobile / Wireless
    - **SEC561** Intense Hands-on Pen Testing Skill Development (with SANS NetWars)
      - **SEC562** CyberCity Hands-on Kinetic Cyber Range Exercise
  - Lab Centred

Specialisations
- **SEC580** Metasploit Kung Fu for Enterprise Pen Testing
- **SEC573** Python for Penetration Testers

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.

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

CORE COURSES
SEC301 › SEC401

- **SEC504** Hacker Tools, Techniques, Exploits, & Incident Handling **GCIH**
  - 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:

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**

Specialisations
- **SEC542** Web App Penetration Testing & Ethical Hacking **GWAPT**
- **SEC642** Advanced Web App Penetration Testing & Ethical Hacking

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	Core	Specialisation
MGT512 SANS Security Leadership Essentials For Managers with Knowledge Compression™ **GSLC**	**MGT514** IT Security Strategic Planning, Policy & Leadership	**MGT433** Securing The Human: Building and Deploying an Effective Security Awareness Programme
MGT525 IT Project Management, Effective Communication, and PMP® Exam Prep **GCPM**	**MGT535** Incident Response Team Management	**AUD507** Auditing & Monitoring Networks, Perimeters, and Systems **GSNA**
MGT414 SANS Training Programme for CISSP® Certification **GISP**	**LEG523** Law of Data Security and Investigations **GLEG**	

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:

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**
  - **FOR508** Advanced Digital Forensics and Incident Response **GCFA**
    - **FOR526** Memory Forensics In-Depth
    - **FOR610** Reverse Engineering Malware: Malware Analysis Tools & Techniques **GREM**
  - **FOR585** Advanced Smartphone Forensics
  - **FOR518** MAC Forensic Analysis
- **SEC504** Hacker Tools, Techniques, Exploits and Incident Handling **GCIH**

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.

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

- **ICS410** ICS/SCADA Security Essentials **GICSP**
  - **ICS515** ICS Active Response and Defense & Response

SEC 401

SECURITY ESSENTIALS BOOTCAMP STYLE

INSTRUCTOR: DR ERIC COLE
Six-Day Programme
Mon 29th Feb – Sat 5th Mar, 9am - 7pm (Sat 9am - 5pm)
46 CPE/CMU Credits | GIAC Cert: GSEC
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 analyse 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

SEC401: Security Essentials Bootcamp Style focuses on teaching the essential skills and techniques needed to protect and secure an organisation's critical information assets and business systems. Learn the most effective steps to prevent attacks and detect adversaries with actionable techniques that can be directly applied back in the workplace. SEC401 also includes tips and tricks from the experts that can help you win the battle against the wide range of cyber adversaries that want to harm your environment.

Security is all about making sure you focus on the right areas of defence. In SEC401 you will learn the language and underlying theory of computer and information security. Take this class and gain the essential and effective security knowledge you need if you are responsible for securing systems and/or an organisation.

SEC401 is aligned with the GSEC certification from GIAC and represents the ideal preparation for this exam. Professionals can demonstrate that they are qualified for IT systems hands-on roles with respect to security tasks by studying for and passing the GSEC exam.

"One of the things I love to hear from students after teaching Security 401 is 'I have worked in security for many years and after taking this course I realised how much I did not know.' With the latest version of Security Essentials and the Bootcamp, we have really captured the critical aspects of security and enhanced those topics with examples to drive home the key points. After you have attended Security 401, I am confident you will walk away with solutions to problems you have had for a while, plus solutions to problems you did not even know you had."

Eric Cole
Course Author

"It is making me question my own beliefs. I will be challenging colleagues and strategies when I return to work. The course is full of logical, workable solutions."
ANTHONY USHER, HMRC

SEC 504

HACKER TOOLS, TECHNIQUES, EXPLOITS AND INCIDENT HANDLING

INSTRUCTOR: STEVE ARMSTRONG
Six-Day Programme:
Mon 29th Feb – Sat 5th Mar, 9am - 7:15pm (Sat 9am - 5pm)
37 CPE/CMU Credits | GIAC Cert: GCIH
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 defences 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 defences for Windows, Unix, switches, routers, and other systems
- Application-level vulnerabilities, attacks, and defences
- How to develop an incident handling process and prepare a team for battle
- Legal issues in incident handling

"Very structured and well prepared course. Interesting and engaging for people new to the field as well as experienced professionals."
EWE KONKOLSKA, PRUDENTIAL

SEC 542

WEB APP PENETRATION TESTING AND ETHICAL HACKING

INSTRUCTOR: PIETER DANHIEUX
Six-Day Programme
Mon 29th Feb – Sat 5th Mar, 9am - 5pm
36 CPE/CMU Credits | GIAC Cert: GWAPT
Laptop Required

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

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.

"SEC542 provides rapid exposure to a variety of tools and techniques invaluable to recon on target site."
GARETH GRINDLE, QA LTD

SEC 560

NETWORK PENETRATION TESTING AND ETHICAL HACKING

INSTRUCTOR: ERIK VAN BUGGENHOUT
Six-Day Programme:
Mon 29th Feb – Sat 5th Mar, 9am - 7:15pm (Tue - Sat 9am - 5pm)
37 CPE/CMU Credits | GIAC Cert: GPEN
Laptop Required

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.

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 utilise built-in operating system tools on Windows and Linux in a weaponised 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

" I had a great time. SEC560 has tons of useful material and techniques. As with all SANS training, I leave knowing that I can apply this as soon as I am back at work."
BENJAMIN BAGBY, XE.COM

SEC 760

ADVANCED EXPLOIT DEVELOPMENT FOR PENETRATION TESTERS

INSTRUCTOR: JAKE WILLIAMS
Six-Day Programme
Mon 29th Feb – Sat 5th Mar, 9am - 5pm
46 CPE/CMU Credits
Laptop Required

YOU WILL LEARN...

- To discover zero-day vulnerabilities in programs running on fully-patched modern operating systems
- To create exploits to take advantage of vulnerabilities through a detailed penetration testing process
- To use the advanced features of IDA Pro and write your own IDC and IDA Python scripts
- To perform remote debugging of Linux and Windows applications
- To understand and exploit Linux heap overflows
- To write Return Oriented Shellcode
- To perform patch diffing against programs, libraries, and drivers to find patched vulnerabilities
- To perform Windows heap overflows and use-after-free attacks
- To use precision heap sprays to improve exploitability
- To perform Windows Kernel debugging up through Windows 8 64-bit
- To jump into Windows kernel exploitation

COURSE DETAILS

Vulnerabilities in modern operating systems such as the latest Linux distributions are often very complex and subtle. Yet, they could expose organisations to significant attacks, undermining their defences when wielded by very skilled attackers. Few security professionals have the skillset to discover let alone even understand at a fundamental level why the vulnerability exists and how to write an exploit to compromise it. Conversely, attackers must maintain this skillset regardless of the increased complexity.

SEC760: Advanced Exploit Development for Penetration Testers teaches the skills required to reverse engineer 32-bit and 64-bit applications, perform remote user application and kernel debugging, analyse patches for one-day exploits, and write complex exploits, such as use-after-free attacks, against modern software and operating systems. Some of the skills you will learn in SEC760 include:

- How to write modern exploits against the Windows 7 and 8 operating systems
- How to perform complex attacks such as use-after-free, Kernel exploit
- techniques, one-day exploitation through patch analysis, and other advanced topics
- The importance of utilising a Security Development Lifecycle (SDL) or Secure SDLC, along with Threat Modeling
- How to effectively utilise various debuggers and plug-ins to improve vulnerability research and speed
- How to deal with modern exploit mitigation controls aimed at thwarting success and defeating determination

"SEC760 is a kind of training we could not get anywhere else. It is not a theory, we got to implement and to exploit everything we learned."
JENNY KITAICHIT, INTEL

FOR 508

ADVANCED DIGITAL FORENSICS AND INCIDENT RESPONSE

INSTRUCTOR: JESS GARCIA
Six-Day Programme:
Mon 29th Feb – Sat 5th Mar, 9am - 5pm
36 CPE/CMU Credits | GIAC Cert: GCFA
Laptop Required

COURSE DETAILS

Over 80% of all breach victims learn of a compromise from third-party notifications, not from internal security teams. In most cases, adversaries have been rummaging through your network undetected for months or even years.

Incident response tactics and procedures have evolved rapidly over the past several years. Data breaches and intrusions are growing more complex. Adversaries are no longer compromising one or two systems in your enterprise; they are compromising hundreds. Your team can no longer afford antiquated incident response techniques that fail to properly identify compromised systems, provide ineffective containment of the breach, and ultimately fail to rapidly remediate the incident.

This in-depth incident response course provides responders with advanced skills to hunt down, counter, and recover from a wide range of threats within enterprise networks, including APT adversaries, organised crime syndicates, and hactivism. Constantly updated, the incident response course (FOR508) addresses today's incidents by providing hands-on incident response tactics and techniques that elite responders are successfully using in real-world breach cases.

FOR508: Advanced Digital Forensics and Incident Response will help you determine:

1. How the breach occurred
2. Compromised and affected systems
3. What attackers took or changed
4. Incident containment and remediation

YOU WILL LEARN...

- To apply incident response processes, threat intelligence, and digital forensics to investigate breached enterprise environments
- To discover every system compromised in your enterprise utilising incident response tools such as F-Response and digital forensic analysis capabilities in the SIFT Workstation to identify APT beach head and spear phishing attack mechanisms, lateral movement, and data exfiltration techniques
- The SIFT Workstation's capabilities, and perform forensic analysis and incident response on any remote enterprise hard drive or system memory without having to image the system first
- How to use system memory and the Volatility toolset to discover active malware on a system, determine how the malware was placed there, and recover it to help develop key threat intelligence
- How to detect advanced capabilities such as Stuxnet, TDSS, or APT command and control malware immediately through memory analysis using Redline's Malware Rating Index (MRI)

"Excellent course and delivery. I have learned a great deal and look forward to using skills in my job."
HELEN BARNARD, ROYAL NAVY

FOR 526

MEMORY FORENSICS IN-DEPTH

INSTRUCTOR: ALISSA TORRES
Six-Day Programme
Mon 29th Feb – Sat 5th Mar, 9am - 5pm
36 CPE/CMU Credits
Laptop Required

YOU WILL LEARN...

- To utilise stream-based data parsing tools to extract AES-encryption keys
- To capture, examine and analyse physical memory image and structures
- Windows, Mac, and Linux Memory Analysis Covered
- To conduct Live System Memory Analysis
- How to extract and analyse packed and non-packed PE binaries from memory
- To gain insight into the latest anti-memory analysis techniques and how to overcome them

COURSE DETAILS

FOR526: Memory Forensics In-Depth provides the critical skills necessary for digital forensics examiners and incident responders to successfully perform live system memory triage and analyse captured memory images. The course uses the most effective freeware and open-source tools in the industry today and provides an in-depth understanding of how these tools work. FOR526 is a critical course for any serious DFIR investigator who wants to tackle advanced forensics, trusted insider, and incident response cases.

In today's forensics cases, it is just as critical to understand memory structures, as it is to understand disk and registry structures. Having in-depth knowledge of Windows memory internals allows the examiner to access target data specific to the needs of the case at hand. For those investigating platforms other than Windows, this course also introduces OSX and Linux memory forensics acquisition and analysis using hands-on lab exercises.

There is an arms race between analysts and attackers. Modern malware and post-exploitation modules increasingly employ self-defence techniques that include more sophisticated rootkit and anti-memory analysis mechanisms that destroy or subvert volatile data. Examiners must have a deeper understanding of memory internals in order to discern the intentions of attackers or rogue trusted insiders. FOR526 draws on best practices and recommendations from experts in the field to guide DFIR professionals through acquisition, validation, and memory analysis with real-world and malware-laden memory images.

"This training opened my eyes for the need to collect memory images, as well as physical images for single computer analysis, such as theft of IP or other employee investigations."
GREG CAOUETTE, KROLL

AUD 507

AUDITING & MONITORING NETWORKS, PERIMETERS & SYSTEMS

INSTRUCTOR: DAVID HOELZER
Six-Day Programme:
Mon 29th Feb – Sat 5th Mar, 9am - 5pm
36 CPE/CMU Credits | GIAC Cert: GSNA
Laptop Required

COURSE DETAILS

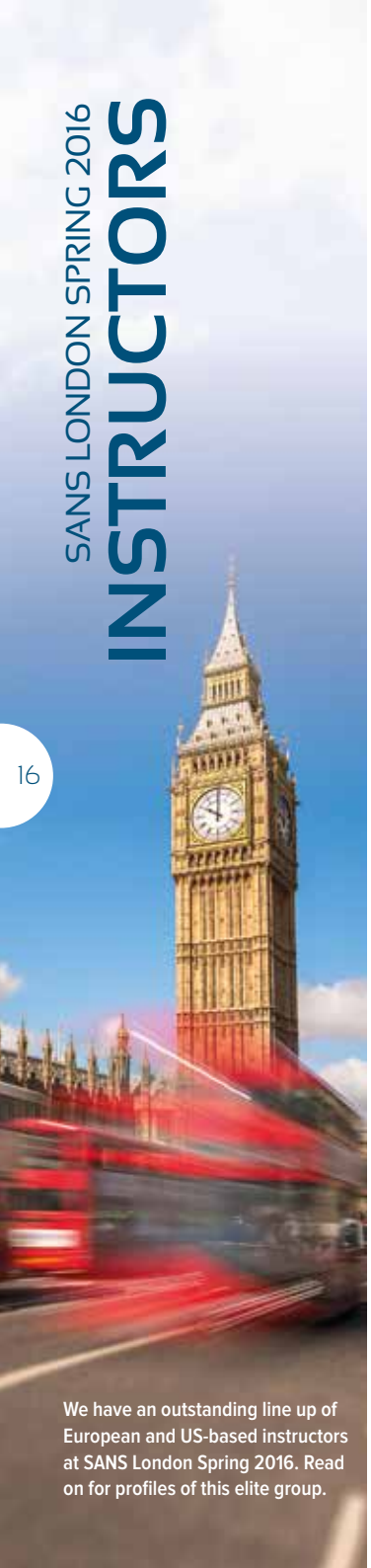
This track specifically helps to provide a risk driven method for tackling the enormous task of designing an enterprise security validation programme. After covering a variety of high-level audit issues and general audit best practice, the students have the opportunity to dive deep into the technical how-to for determining the key controls that can be used to provide a level of assurance to an organisation. Tips on how to repeatedly verify these controls and techniques for continuous monitoring and automatic compliance validation are given from real world examples.

One of the struggles that IT auditors face today is assisting management to understand the relationship between the technical controls and the risks to the business that these affect. In this course these threats and vulnerabilities are explained based on validated information from real world situations. The instructor will take the time to explain how this can be used to raise the awareness of management and others within the organisation to build an understanding of why these controls specifically are important and why auditing in general is important. From these threats and vulnerabilities, we explain how to build ongoing compliance monitoring systems and how to automatically validate defences through instrumentation and automation of audit checklists.

YOU WILL LEARN...

- To understand the different types of controls (e.g., technical vs. non-technical) essential to performing a successful audit
- To conduct a proper network risk assessment to identify vulnerabilities and prioritise what will be audited
- To establish a well-secured baseline for computers and networks - a standard to conduct an audit against
- To perform a network and perimeter audit using a seven-step process
- To audit firewalls to validate that rules/settings are working as designed, blocking traffic as required
- To utilise vulnerability assessment tools effectively to provide management with the continuous remediation information necessary to make informed decisions about risk and resources.
- To audit web applications' configuration, authentication, and session management to identify vulnerabilities attackers can exploit
- To utilise scripting to build a system to baseline and automatically audit Active Directory and all systems in a Windows domain.

"Comprehensive coverage on web application auditing and introduced new concepts and tools that will be very useful."
SRINATH KANNAN, ACCENTURE



We have an outstanding line up of European and US-based instructors at SANS London Spring 2016. Read on for profiles of this elite group.

STEVE ARMSTRONG

CERTIFIED INSTRUCTOR

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

When not teaching for SANS, Steve provides penetration testing and incident response services for some of the biggest household names in gaming and music media. To relax Steve enjoys playing Battlefield to loud music and developing collaborative DFIR tools.

ERIK VAN BUGGENHOUT

INSTRUCTOR

Erik is an instructor for the SANS SEC542 "Web Application Penetration Testing & Ethical Hacking" and SANS SEC560 "Network Penetration Testing & Ethical Hacking" courses. Next to his teaching activities for SANS, Erik is the head of technical security services at nViso. NViso is a Brussels-based IT security firm founded in early 2013. At nViso, Erik mainly focuses on security assessments (both on a network and application level). Next to security assessments, he also advises clients on how they can improve their IT security posture. Before co-founding nViso, Erik was a manager at Ernst & Young, where he led a team of technical security experts in the Diegem (Brussels) office. Together with his team, he delivered technical security advisory services to major clients in the EMEIA financial services industry.

DR ERIC COLE

FELLOW

Dr. Cole is an industry-recognised security expert with over 20 years of hands-on experience. Dr. Cole has experience in information technology with a focus on helping customers focus on the right areas of security by building out a dynamic defence. Dr. Cole has a master's degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. He served as CTO of McAfee and Chief Scientist for Lockheed Martin.

Dr. Cole is the author of several books, including Advanced Persistent Threat, Hackers Beware, Hiding in Plain Sight, Network Security Bible 2nd Edition, and Insider Threat.

He is the inventor of over 20 patents and is a researcher, writer, and speaker. He is also a member of the Commission on Cyber Security for the 44th President and several executive advisory boards.

Dr. Cole is the founder and an executive leader at Secure Anchor Consulting where he provides leading-edge cyber security consulting services, expert witness work, and leads research and development initiatives to advance the state-of-the-art in information systems security.

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 is Co-founder and Chief Architect of the Secure Code Warrior platform (http://www.securecodewarrior.com), a gamified environment where developers and security testers can learn how to properly identify and fix security weaknesses in software. Until January 2015, he was part of the leadership at BAE Systems APAC in his role as Head of Delivery of the Applied Intelligence business unit.

JESS GARCIA

PRINCIPAL INSTRUCTOR

Jess Garcia is the founder and technical lead of One eSecurity, a global Information Security company specialised in Incident Response and Digital Forensics.

With near 20 years in the field, and an active researcher in the area of innovation for Digital Forensics, Incident Response and Malware Analysis, Jess is today an internationally recognised Digital Forensics and Cybersecurity expert, having led the response and forensic investigation of some of the world's biggest incidents in recent times.

In his career Jess has worked in a myriad of highly sensitive projects with top global customers in sectors such as financial & insurance, corporate, media, health, communications, law firms or government, in other Cybersecurity areas as well such as Security Architecture Design and Review, Penetration Tests, Vulnerability Assessments, etc.

A Principal SANS Instructor with almost 15 years of SANS instructing experience, Jess is also a regular invited speaker at Security and DFIR conferences worldwide.

DAVID HOELZER

FELLOW

David Hoelzer is a SANS Fellow instructor and author of more than twenty sections of SANS courseware. He is an expert in a variety of information security fields, having served in most major roles in the IT and security industries over the past twenty-five years. Recently, David was called upon to serve as an expert witness for the Federal Trade Commission for ground breaking GLBA Privacy Rule litigation. David has been highly involved in governance at SANS Technology Institute, serving as a member of the Curriculum Committee as well as Audit Curriculum Lead. As a SANS instructor, David has trained security professionals from organisations including NSA, DHHS, Fortune 500 security engineers and managers, various Department of Defence sites, national laboratories, and many colleges and universities. David has written and contributed to more than 15 peer reviewed books, publications, and journal articles. Currently David serves as the chief information security officer for Cyber-Defence, an open source security software solution provider. In the past, David served as the director of the GIAC Certification program, bringing the GIAC Security Expert certification to life.

ALISSA TORRES

CERTIFIED INSTRUCTOR

Alissa Torres is a certified SANS instructor, specialising in advanced computer forensics and incident response. Her industry experience includes serving in the trenches as part of the Mandiant Computer Incident Response Team (MCIRT) as an incident handler and working on an internal security team as a digital forensic investigator. She has extensive experience in information security, spanning government, and academic, and corporate environments and holds a Bachelors degree from University of Virginia and a Masters from University of Maryland in Information Technology. Alissa has taught as an instructor at the Defence Cyber Investigations Training Academy (DCITA), delivering incident response and network basics to security professionals entering the forensics community. She has presented at various industry conferences and numerous B-Sides events. In addition to being a GIAC Certified Forensic Analyst (GCFA), she holds the GCFE, GPEN, CISSP, EnCE, CFCE, MCT and CTT+.

JAKE WILLIAMS

CERTIFIED INSTRUCTOR

Jake Williams is a Principal Consultant at Rendition Infosec. He has more than a decade of experience in secure network design; penetration testing, incident response, forensics, and malware reverse engineering. Jake is the co-author of the SANS FOR610 course (Malware Reverse Engineering) and the FOR526 course (Memory Forensics). He is also a contributing author for the SEC760 course (Advanced Exploit Development). In addition to teaching these courses, Jake also teaches a number of other forensics and security courses.

Jake regularly responds to cyber intrusions performed by state-sponsored actors in financial, defence, aerospace, and healthcare sectors using cutting edge forensics and incident response techniques. He often develops custom tools to deal with specific incidents and malware reversing challenges.

Jake has spoken at Blackhat, Shmoocon, CEIC, B-Sides, DC3, as well as numerous SANS Summits and government conferences. He is also a two-time victor at the annual DC3 Digital Forensics Challenge. Jake used this experience with, and love of, CTF events to design the critically acclaimed NetWars challenges for the SANS malware reversing and memory forensics courses.

EVENT LOCATION & TRAVEL INFORMATION SANS LONDON SPRING

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

Arriving by London Underground

Nearest Underground stations:

- 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 stops away on the London Underground's Piccadilly line
- All of London's remaining mainline stations including London Victoria, Paddington and Waterloo are easily reached by the Underground network

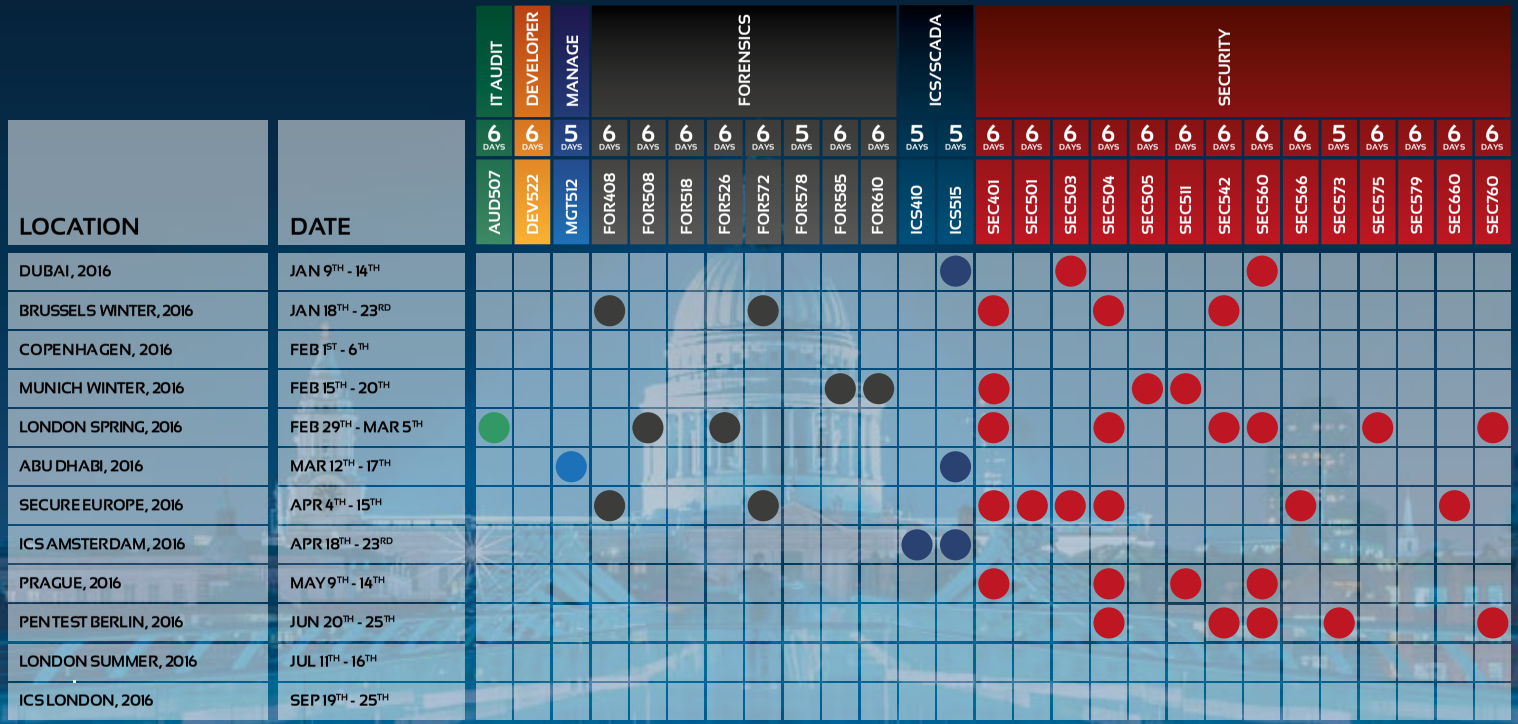
Arriving by Air

- 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

Contact SANS: Tel +44 203 384 3470 | Email emea@sans.org

FUTURE SANS EMEA TRAINING EVENTS 2016

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



V15 - A5

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

Dates, Locations and Courses offered subject to change