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

SANS EMEA

JULY 13TH TO 18TH 2015 • GRAND CONNAUGHT ROOMS, LONDON, WC2

SANS LONDON

IN THE SUMMER 2015

10 VITAL SANS COURSES

WORLD RENOWNED INSTRUCTORS • NETWARS • SANS AT NIGHT TALKS

www.sans.org/event/london-in-the-summer-2015

COURSES AT A GLANCE

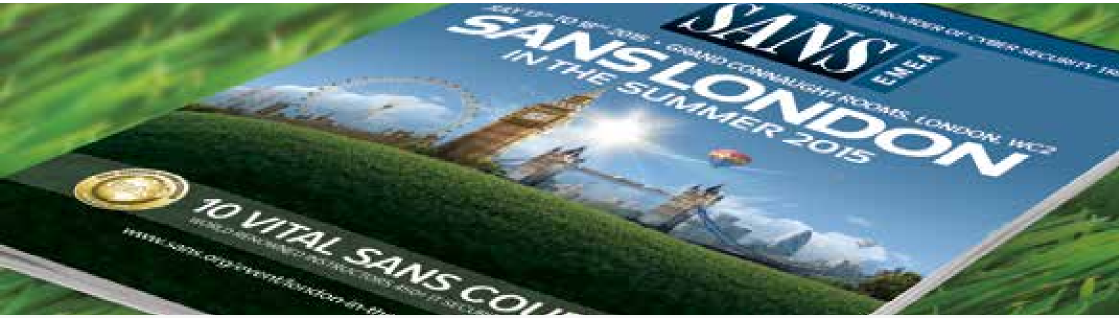
SANS EMEA

			MON 13	TUE 14	WED 15	THU 16	FRI 17	SAT 18
SEC 401	SANS Security Essentials Bootcamp Style	Stephen Sims	PG 8	→	→	→	→	→
SEC 504	Hacker Tools, Techniques, Exploits and Incident Handling	Steve Armstrong	PG 9	→	→	→	→	→
SEC 561	Intense Hands-on Pen Testing Skill Development (with SANS Netwars)	Tim Medin	PG 10	→	→	→	→	→
SEC 575	Mobile Device Security and Ethical Hacking	Raul Siles	PG 11	→	→	→	→	→
DEV 522	Defending Web Applications Security Essentials	Jason Lam	PG 12	→	→	→	→	→
FOR 508	Advanced Digital Forensics and Incident Response	Jess Garcia	PG 13	→	→	→	→	→
FOR 572	Advanced Network Forensics and Analysis	George Bakos	PG 14	→	→	→	→	→
FOR 610	Reverse-Engineering Malware: Malware Analysis Tools and Techniques	Lenny Zeltser	PG 15	→	→	→	→	→
MGT 512	SANS Security Leadership Essentials for Managers with Knowledge Compression™	G. Mark Hardy	PG 16	→	→	→	→	
AUD 507	Auditing and Monitoring Networks, Perimeters & Systems	James Tarala	PG 17	→	→	→	→	→

Register at www.sans.org/event/london-in-the-summer-2015

SANS LONDON IN THE SUMMER 2015 REGISTRATION INFORMATION

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



REGISTER EARLY AND SAVE

Register & pay by May 27th 2015 and save up to €375.00

Discount applies to five and six day courses only.

Save over €500 on any 2-day course when booked with a long course.

All course prices are listed at www.sans.org/event/london-in-the-summer-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-in-the-summer-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 must be received by 17 June, 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 organization. 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 conference 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.

WELCOME TO SANS LONDON IN THE SUMMER

SANS London In The Summer runs from Monday 13th to Saturday 18th July at the Grand Connaught Rooms in London's West End and hosts 10 courses drawn from across the SANS curriculum.

Training takes place in classroom format with all books, cds, etc provided and all courses led by SANS Instructors.

Training fees include lunch at the venue plus morning and afternoon break refreshments. Accommodation is not included.

Training runs from 9am-5pm each day except for course SEC401 that finishes at 7pm Monday-Friday and 5pm on Saturday.

Students are able to attend free SANS@night talks and evening social functions. The demand for places at SANS London events is always high – which is why we've expanded this summer event – so please register online as soon as possible to secure a seat at SANS London In The Summer 2015.

Read on for course descriptions or visit www.sans.org/london-in-the-summer-2015

SANS European Security Awareness Summit

July 8-10, Grand Connaught Rooms, London, WC2

2-day Training and 1-day Summit event. Learn how to build, maintain and measure a high-impact awareness campaign

Speakers confirmed from:

- Lockheed Martin
- Bank Of England
- ENISA
- Diageo

...and more

www.sans.org/european-security-awareness-summit

CONTENTS

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

SANS EMEA

SANS IT SECURITY TRAINING AND YOUR

CAREER ROAD MAP

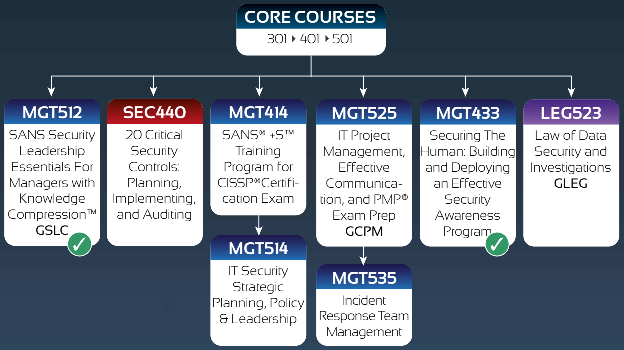
CORE COURSES ↓

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. Leadership must be armed with current knowledge and best practice examples to make timely and effective decisions that benefit the entire enterprise information infrastructure.

SAMPLE JOB TITLES:
Developer, Software architect, QA tester, Dev manager



CORE COURSES
301 ▸ 401 ▸ 501

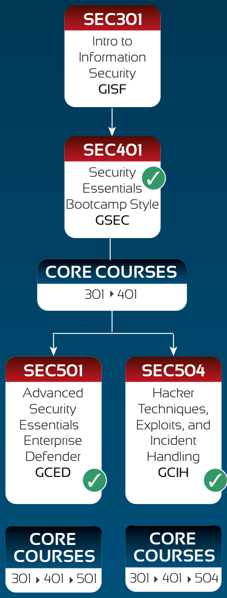
- **MGT512** SANS Security Leadership Essentials For Managers with Knowledge Compression™ GSLC ✓
- **SEC440** 20 Critical Security Controls: Planning, Implementing, and Auditing
- **MGT414** SANS® +S™ Training Program for CISSP® Certification Exam
  - **MGT514** IT Security Strategic Planning, Policy & Leadership
- **MGT525** IT Project Management, Effective Communication, and PMP® Exam Prep GCPM
  - **MGT535** Incident Response Team Management
- **MGT433** Securing The Human: Building and Deploying an Effective Security Awareness Program ✓
- **LEG523** Law of Data Security and Investigations GLEG

FUNCTION:

INFORMATION SECURITY

Responsible for research and analysis of security threats that may affect a company's assets, products or technical specifications. This analyst will dig into technical protocols and specifications for a greater understanding of security threats than most of his/her peers, identifying strategies to defend against attacks through intimate knowledge of the threats.

SAMPLE JOB TITLES:
IT security analyst , IT security engineer, IT security architect



- **SEC301** Intro to Information Security GISF
- **SEC401** Security Essentials Bootcamp Style GSEC ✓

CORE COURSES
301 ▸ 401

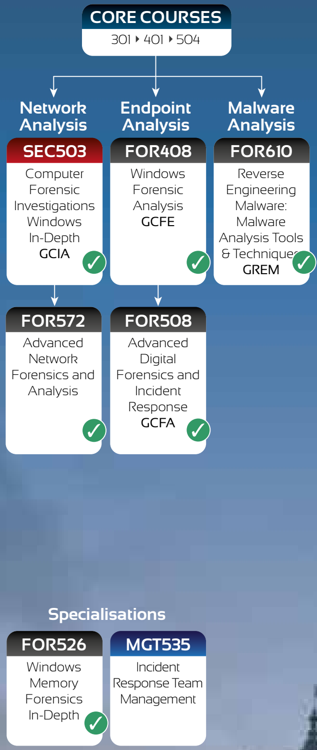
- **SEC501** Advanced Security Essentials Enterprise Defender GCED ✓
  CORE COURSES 301 ▸ 401 ▸ 501
- **SEC504** Hacker Techniques, Exploits, and Incident Handling GCIH ✓
  CORE COURSES 301 ▸ 401 ▸ 504

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
301 ▸ 401 ▸ 504

Network Analysis
- **SEC503** Computer Forensic Investigations Windows In-Depth GCIA ✓
- **FOR572** Advanced Network Forensics and Analysis ✓

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 ✓

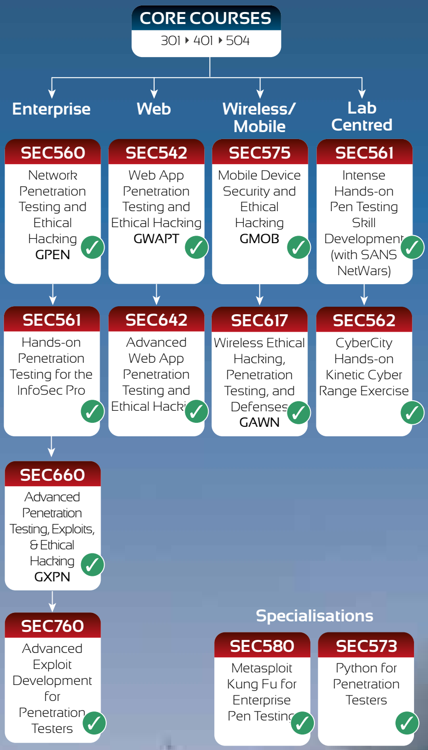
Specialisations
- **FOR526** Windows Memory Forensics In-Depth ✓
- **MGT535** Incident Response Team Management

FUNCTION:

PENETRATION TESTING/ VULNERABILITY ASSESSMENT

Because offense must inform defense, these experts provide enormous value to an organization by applying attack techniques to find security vulnerabilities, analyze 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



CORE COURSES
301 ▸ 401 ▸ 504

Enterprise
- **SEC560** Network Penetration Testing and Ethical Hacking GPEN ✓
- **SEC561** Hands-on Penetration Testing for the InfoSec Pro ✓
- **SEC660** Advanced Penetration Testing, Exploits, & 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 ✓

Wireless/ Mobile
- **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 ✓

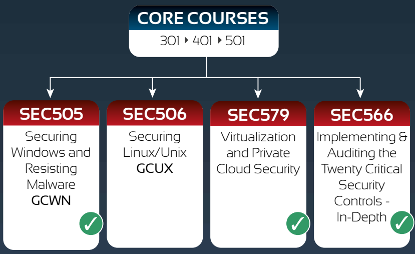
✓ = Live training available in EMEA

FUNCTION:

NETWORK OPS CENTER, SYSTEM ADMIN, SECURITY ARCHITECTURE

A network operations center (NOC) is a place from which IT professionals supervise, monitor and maintain the enterprise network. The network operations center is the focal point for network troubleshooting, software distribution and updating, router and system management, performance monitoring, and coordination with affiliated networks. The NOC works hand-in-hand with the SOC, which safeguards the enterprise and continuously monitors for threats against it.

SAMPLE JOB TITLES:
System/IT administrator, Security administrator , Security architect/engineer



CORE COURSES
301 ▸ 401 ▸ 501

SEC505 Securing Windows and Resisting Malware GCWN ✓

SEC506 Securing Linux/Unix GCUX

SEC579 Virtualization and Private Cloud Security ✓

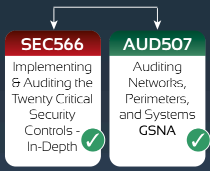
SEC566 Implementing & Auditing the Twenty Critical Security Controls - In-Depth ✓

FUNCTION:

RISK & COMPLIANCE/AUDITING/ GOVERNANCE TITLES

This expert assesses and reports risk to the organization by measuring compliance with policies, procedures, and standards. These experts make recommendations for improvements to make the organization more efficient and profitable through continuous monitoring risk management.

SAMPLE JOB TITLES:
Auditor, Compliance officer



SEC566 Implementing & Auditing the Twenty Critical Security Controls - In-Depth ✓

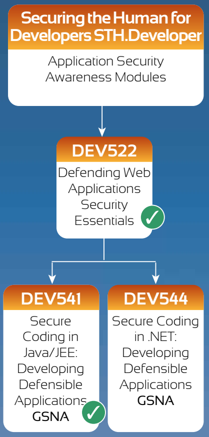
AUD507 Auditing Networks, Perimeters, and Systems GSNA ✓

FUNCTION:

DEVELOPMENT 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 ✓

DEV541 Secure Coding in Java/JEE: Developing Defensible Applications GSNA ✓

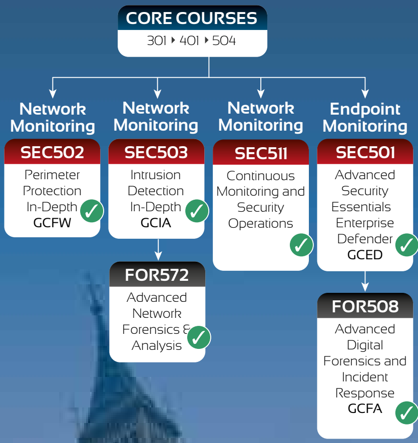
DEV544 Secure Coding in .NET: Developing Defensible Applications GSNA

FUNCTION:

SECURITY OPERATIONS CENTER/INTRUSION DETECTION

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 Center analyst/engineer, CERT member, Cyber threat analyst



CORE COURSES
301 ▸ 401 ▸ 504

Network Monitoring
SEC502 Perimeter Protection In-Depth GCFW ✓

Network Monitoring
SEC503 Intrusion Detection In-Depth GCIA ✓

FOR572 Advanced Network Forensics & Analysis ✓

Network Monitoring
SEC511 Continuous Monitoring and Security Operations ✓

Endpoint Monitoring
SEC501 Advanced Security Essentials Enterprise Defender GCED ✓

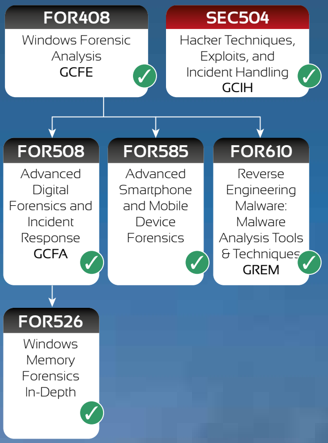
FOR508 Advanced Digital Forensics and Incident Response GCFA ✓

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, Media exploitation analyst Information technology litigation support and consultant analyst



FOR408 Windows Forensic Analysis GCFE ✓

SEC504 Hacker Techniques, Exploits, and Incident Handling GCIH ✓

FOR508 Advanced Digital Forensics and Incident Response GCFA ✓

FOR526 Windows Memory Forensics In-Depth ✓

FOR585 Advanced Smartphone and Mobile Device Forensics ✓

FOR610 Reverse Engineering Malware: Malware Analysis Tools & Techniques GREM ✓

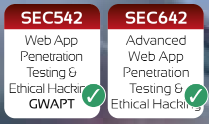
FUNCTION:

INDUSTRIAL CONTROL SYSTEMS / SCADA

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

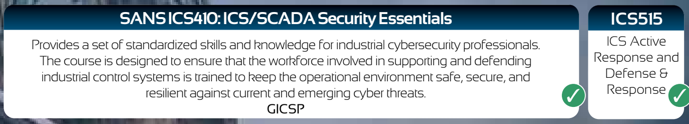
SAMPLE JOB TITLES:
IT & OT Support, IT & OT Cybersecurity, ICS Engineer

Specialisations



SEC542 Web App Penetration Testing & Ethical Hacking GWAPT ✓

SEC642 Advanced Web App Penetration Testing & Ethical Hacking ✓



SANS ICS410: ICS/SCADA Security Essentials

Provides a 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.
GICSP ✓

ICS515 ICS Active Response and Defense & Response ✓

SEC 401

SECURITY ESSENTIALS BOOTCAMP STYLE

Instructor: Stephen Sims

Six-Day Program: Mon 13th – Sat 18th July, 9:00am - 7:00pm (5pm on Sat)
46 CPE/CMU Credits
Laptop Required

You will learn to...

- Design and build a network architecture using VLAN's, NAC and 802.1x based on an APT indicator of compromise
- Run Windows command line tools to analyze the system looking for high-risk items
- Run Linux command line tools (ps, ls, netstat, etc.) and basic scripting to automate the running of programs to perform continuous monitoring of various tools
- Install VMWare and create virtual machines to create a virtual lab to test and evaluate tools/ security of systems
- Create an effective policy that can be enforced within an organization and prepare a checklist to validate security, creating metrics to tie into training and awareness
- Identify visible weaknesses of a system utilizing various tools to include dumpsec and OpenVAS, and once vulnerabilities are discovered, cover ways to configure the system to be more secure
- Determine overall scores for systems utilizing CIS Scoring Tools and create a system baseline across the organization

Course details

SEC401: Security Essentials Bootcamp Style is focused on teaching you the essential information security skills and techniques you need to protect and secure your organization's critical information assets and business systems. Our course will show you how to prevent your organization's security problems from being headline news in the Wall Street Journal!

"Prevention is Ideal but Detection is a Must."

With the advanced persistent threat, it is almost inevitable that organizations will be targeted. Whether the attacker is successful in penetrating an organization's network depends on the effectiveness of the organization's defense. Defending against attacks is an on going challenge, with new threats emerging all of the time, including the next generation of threats. Organizations need to understand what really works in cybersecurity. What has worked, and will always work, is taking a risk-based approach to cyber defense. Before your organization spends a dollar of its IT budget or allocates any resources or time to anything in the name of cybersecurity, three questions must be answered:

1. What is the risk?
2. Is it the highest priority risk?
3. What is the most cost-effective way to reduce the risk?

Security is all about making sure you focus on the right areas of defense. In SEC401 you will learn the language and underlying theory of computer and information security. You will gain the essential and effective security knowledge you will need if you are given the responsibility for securing systems and/or organizations.

This course meets both of the key promises SANS makes to our students:

1. You will learn up-to-the-minute skills you can put into practice immediately upon returning to work; and
2. You will be taught by the best security instructors in the industry.

"Security Essentials 401 has relit my passion and excitement for Information Security."

Emma Baker, Capgemini

SEC 504

HACKER TOOLS, TECHNIQUES, EXPLOITS AND INCIDENT HANDLING

Instructor: Steve Armstrong

Six-Day Program: Mon 13th – Sat 18th July, 9:00am - 5:00pm
37 CPE/CMU Credits
Laptop Required

Course details

If your organization 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.

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, the in-depth information in this course helps you turn the tables on computer attackers. This course addresses the latest cutting-edge insidious attack vectors and the "oldie-but-goodie" attacks that are still so prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course includes a time-tested, step-by- step process for responding to computer incidents; a detailed description of how attackers undermine systems so you can prepare, detect, and respond to them; and a hands-on workshop for discovering holes before the bad guys do. Additionally, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence.

This challenging course is particularly well suited to individuals who lead or are a part of an incident handling team. Furthermore, 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 to...

- 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

> **"This course excels not only on giving a modern framework in incident handling, but also on providing lots and lots of hands on examples."**
> Michael Moerz

SEC 561

INTENSE HANDS-ON PEN TESTING SKILL DEVELOPMENT (WITH SANS NETWARS)

Instructor: Tim Medin

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

You will learn to...

- Use network scanning and vulnerability assessment tools to effectively map out networks and prioritize discovered vulnerabilities for effective remediation
- Use password analysis tools to identify weak authentication controls leading to unauthorized server access
- Evaluate web applications for common developer flaws leading to significant data loss conditions
- Manipulate common network protocols to maliciously reconfigure internal network traffic patterns
- Identify weaknesses in modern anti-virus signature and heuristic analysis systems
- Inspect the configuration deficiencies and information disclosure threats present on Windows and Linux servers
- Bypass authentication systems for common web application implementations
- Exploit deficiencies in common cryptographic systems
- Bypass monitoring systems by leveraging IPv6 scanning and exploitation tools

Course details

To be a top pen test professional, you need fantastic hands-on skills for finding, exploiting, and resolving vulnerabilities. SANS top instructors engineered SEC561: Intense Hands-on Pen Testing Skill Development from the ground up to help you get good fast. The course teaches in-depth security capabilities through 80%+ hands-on exercises and labs, maximizing keyboard time on in-class labs and making this SANS' most hands-on course ever. With over 30 hours of intense labs, students experience a leap in their capabilities, as they come out equipped with the practical hands-on skills needed to address today's pen test and vulnerability assessment projects in enterprise environments.

To get the most out of this course, students should have at least some prior hands-on vulnerability assessment or penetration testing experience (at least 6 months) or have taken at least one other penetration testing course (such as SANS SEC504, SEC560, or SEC542). The course will build on that background, helping participants ramp up their skills even further across a broad range of penetration testing disciplines.

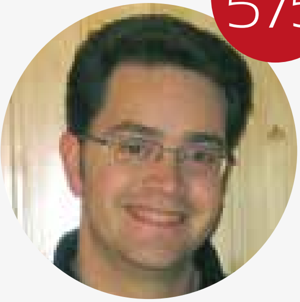
Throughout the course, an expert instructor coaches students as they work their way through solving increasingly demanding real-world information security scenarios that they can apply the day that they get back to their jobs.

A lot of people can talk about these concepts, but this course teaches you how to actually apply them hands-on and in-depth. SEC561 shows security personnel, including penetration testers, vulnerability assessment personnel, auditors, and operations personnel, how to leverage in-depth techniques to get powerful results in every one of their projects. The course is overflowing with practical lessons and innovative tips, all with direct hands-on application.

Throughout the course, students interact with brand new, custom-developed scenarios built just for this course on the innovative NetWars challenge infrastructure, which guides them through the numerous hands-on labs providing questions, hints, and lessons learned as they build their skills.

SEC 575

MOBILE DEVICE SECURITY AND ETHICAL HACKING



Instructor: Raul Siles

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

Course details

Now covering BlackBerry 10, Apple iOS 7, and Android 4.3 devices
Mobile phones and tablets have become essential to enterprise and government networks, from small organizations to Fortune 500 companies and largescale 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 organizational 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 to project management. With increased reliance on these devices, organizations are quickly recognizing that mobile phones and tablets need greater security implementations than a simple screen protector and clever password.

Whether the device is an Apple iPhone or iPad, a Windows Phone, an Android or BlackBerry phone or tablet, the ubiquitous mobile device has become a hugely attractive and vulnerable target for nefarious attackers. The use of mobile devices introduces a vast array of new risks to organizations, including:

- Distributed sensitive data storage and access mechanisms
- Lack of consistent patch management and firmware updates
- The high probability of device loss or theft, and more

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.

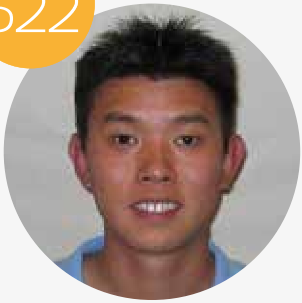
This course was designed to help organizations struggling with mobile device security by equipping personnel with the skills needed to design, deploy, operate, and assess a well-managed secure mobile environment. From practical policy development to network architecture design and deployment, and from mobile code analysis to penetration testing and ethical hacking, this course will help you build the critical skills necessary to support the secure deployment and use of mobile phones and tablets in your organization.

You will learn to...

- Develop effective policies to control employeeowned (Bring Your Own Device, BYOD) and enterprise-owned mobile devices including the enforcement of effective passcode policies and permitted application
- Utilize jailbreak tools for Apple iOS and Android systems such as redsn0w, Absinthe
- Conduct an analysis of iOS and Android filesystem data using SqliteSpy, Plist Editor, and AXMLPrinter to plunder compromised devices and extract sensitive mobile device use information such as the SMS history, browser history, GPS history, and user dictionary keywords
- Analyze Apple iOS and Android applications with reverse engineering tools including class-dump, JD-GUI, dextranslator, and apktool to identify malware and information leakage threats in mobile applications
- Conduct an automated security assessment of mobile applications using iAuditor, Cycript, MobileSubstrate, TaintDroid, and DroidBox to identify security flaws in mobile applications

"Cutting edge security material, well taught."
Donald Farrell, Kingsisle Entertainment Inc.

DEV
522



DEFENDING WEB APPLICATIONS SECURITY ESSENTIALS

Instructor: Jason Lam

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

Topics include...

- Infrastructure Security
- Server Configuration
- Authentication mechanisms
- Application language configuration
- Application coding errors like SQL Injection and Cross-Site Scripting
- Cross-Site Request Forging
- Authentication Bypass
- Web services and related flaws
- Web 2.0 and its use of web services
- XPATH and XQUERY languages and injection
- Business logic flaws
- Protective HTTP Headers

Course details

Traditional network defenses, such as firewalls, fail to secure web applications. The quantity and importance of data entrusted to web applications is growing, and defenders need to learn how to secure it. DEV522 covers the OWASP Top 10 and will help you to better understand web application vulnerabilities, thus enabling you to properly defend your organization's web assets.

Mitigation strategies from an infrastructure, architecture, and coding perspective will be discussed alongside real-world implementations that really work. The testing aspect of vulnerabilities will also be covered so you can ensure your application is tested for the vulnerabilities discussed in class.

To maximize the benefit for a wider range of audiences, the discussions in this course will be programming language agnostic. Focus will be maintained on security strategies rather than coding level implementation.

DEV522: Defending Web Applications Security Essentials is intended for anyone tasked with implementing, managing, or protecting Web applications. It is particularly well suited to application security analysts, developers, application architects, pen testers, and auditors who are interested in recommending proper mitigations to web security issues and infrastructure security professionals who have an interest in better defending their web applications.

The course will cover the topics outlined by OWASP's Top 10 risks document as well as additional issues the authors found of importance in their day-to-day web application development practice.

The course will make heavy use of hands-on exercises. It will conclude with a large defensive exercise, reinforcing the lessons learned throughout the week.

> **"Not only does DEV522 teach the defenses for securing web apps, it also shows how common and easy the attacks are thus the need to secure the apps"**
> Brandon Hardin, ITC

FOR 508

ADVANCED DIGITAL FORENSICS AND INCIDENT RESPONSE

Instructor: Jess Garcia

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

Course details

This course focuses on providing incident responders with the necessary skills to hunt down and counter a wide range of threats within enterprise networks, including economic espionage, hactivism, and financial crime syndicates. The completely updated FOR508 addresses today's incidents by providing real-life, hands-on response tactics.

Over 90% of all breach victims learn of a compromise from third-party notification, not from internal security teams. In most cases, adversaries have been rummaging through your network undetected for months or even years. Gather your team – it's time to go hunting.

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

- How did the breach occur?
- What systems were compromised?
- What did they take?
- What did they change?
- How do we remediate the incident?

FOR508 trains digital forensic analysts and incident response teams to identify, contain, and remediate sophisticated threats including APT groups and financial crime syndicates. A hands-on lab – developed from a real-world targeted attack on an enterprise network leads you through the challenges and solutions. You will identify where the initial targeted attack occurred and which systems an APT group compromised.

The course will prepare you to find out which data was stolen and by whom, contain the threat, and provide your organization the capabilities to manage and counter the attack. During a targeted attack, an organization needs the best incident responders and forensic analysts in the field. FOR508 will train you and your team to be ready to do this work.

Course topics...

- Advanced use of a wide range of best-of-breed open-source tools in the SANS SIFT Workstation to perform incident response and digital forensics.
- Responding to advanced adversaries such as nation-state actors, organized crime, and hacktivists.
- Rapid incident response analysis and breach assessment.
- Incident response and intrusion forensics methodology.
- Remote and enterprise incident response system analysis.
- Windows live incident response.
- Memory analysis during incident response.
- Timeline analysis.
- System restore points and volume shadow copy exploitation.
- In-depth windows NTFS file system examination to detect APT groups and advanced insider threats.
- Detection of anti-forensics and adversary hiding techniques.
- Discovery of unknown malware on a system.
- Adversary threat intelligence development, indicators of compromise, and usage.

> **"I've taken other network intrusion classes but nothing this in-depth. The class is outstanding!"**
> Craig Goldsmith, FBI

FOR
572

ADVANCED NETWORK FORENSICS AND ANALYSIS

Instructor: George Bakos

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

You will learn to...

- Extract files from network packet captures and proxy cache files, allowing follow-on malware analysis or definitive data loss determinations
- Use historical NetFlow data to identify relevant past network occurrences, allowing accurate incident scoping
- Reverse engineer custom network protocols to identify an attacker's command-and-control abilities and actions
- Decrypt captured SSL traffic to identify an attackers' actions and what data they extracted from the victim
- Use data from typical network protocols to increase the fidelity of the investigation's findings
- Examine traffic using common network protocols to identify patterns of activity or specific actions that warrant further investigation
- Incorporate log data into a comprehensive analytic process
- Learn how attackers leverage man-in-the-middle tools to intercept seemingly secure communications

Course details

Forensic casework that does not include a network component is a rarity in today's environment. Performing disk forensics will always be a critical and foundational skill for this career, but overlooking the network component of today's computing architecture is akin to ignoring security camera footage of a crime as it was committed. Whether you handle an intrusion incident, data theft case, or employee misuse scenario, the network often has an unparaleled view of the incident. Its evidence can provide the proof necessary to show intent, or even definitively prove that a crime actually occurred.

FOR572 was built from the ground up to cover the most critical skills needed to mount efficient and effective post-incident response investigations. We focus on the knowledge necessary to expand the forensic mindset from residual data on the storage media from a system or device to the transient communications that occurred in the past or continue to occur. Even if the most skilled remote attacker compromised a system with an undetectable exploit, the system still has to communicate over the network. Bad guys are talking – we'll teach you to listen.

This course covers the tools, technology, and processes required to integrate network evidence sources into your investigations. You will leave this week with a well-stocked toolbox and the knowledge to use it on your first day back on the job. We will cover the full spectrum of network evidence, including high-level NetFlow analysis, low-level pcap exploration, ancillary network log examination, and more. We cover how to leverage existing infrastructure devices that may contain months or years of valuable evidence, as well as how to place new collection platforms while an incident is already under way.

FOR572 is truly an advanced course - we hit the ground running on day one. Bring your entire bag of skills: forensic techniques and methodologies, networking (from the wire all the way up to user-facing services), Linux shell utilities, and everything in between.

"This is an incredible curriculum. This class NEEDED to happen and I am glad it did."
Peter Steinmann

FOR 610

REVERSE-ENGINEERING MALWARE: MALWARE ANALYSIS TOOLS AND TECHNIQUES

Instructor: Lenny Zeltser

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

Course details

This popular malware analysis course has helped forensic investigators, malware specialists, incident responders, and IT administrators assess malware threats. The course teaches a practical approach to examining malicious programs spyware, bots, trojans, etc. that target or run on Microsoft Windows. This training also looks at reversing web-based malware, such as JavaScript and Flash files, as well as malicious document files. By the end of the course, you'll know how to reverse- engineer malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and other tools for turning malware inside-out!

The course begins by covering fundamental aspects of malware analysis and continues by discussing essential x86 assembly language concepts. Towards the end of the course, you'll learn to analyze malicious document files that take the form of Microsoft Office and Adobe PDF documents.

The malware analysis process taught in this class helps incident responders assess the severity and repercussions of a situation that involves malicious software. It also assists in determining how to contain the incident and plan recovery steps. Forensics investigators also learn how to understand key characteristics of malware present on compromised systems, including how to establish indicators of compromise (IOCs) for scoping and containing the intrusion.

Hands-on workshop exercises are a critical aspect of this course and allow you to apply reverse-engineering techniques by examining malware in a controlled environment. When performing the exercises, you'll study the supplied specimen's behavioral patterns and examine key portions of its code. You'll examine malware on a Windows virtual machine that you'll infect during the course and will use the supplied Linux virtual machine (REMnux) that includes tools for examining and interacting with malware

You will learn to...

- Build an isolated laboratory environment for analyzing code and behavior of malicious programs
- Employ network and system-monitoring tools to examine how malware interacts with the file system, the registry, the network and other processes on Microsoft Windows
- Uncover and analyze malicious JavaScript,VB Script and ActionScript components of web pages, which are often used as part of drive-by attacks
- Control some aspect of the malicious program's behavior through network traffic interception and code patching
- Use a disassembler and a debugger to examine inner-workings of malicious Windows executables
- Bypass a variety of defensive mechanisms designed by malware authors to misdirect, confuse and otherwise slow down the analyst
- Recognize and understand common assembly-level patterns in malicious code, such as DLL injection

"SANS London has really been enlightening. In four words 'Serious About Network Security'. Top notch!"

Patricio Correia, Tribunal Constitucional

MGT 512

SANS SECURITY LEADERSHIP ESSENTIALS FOR MANAGERS WITH KNOWLEDGE COMPRESSION™

Instructor: G. Mark Hardy

Five-Day Program: Mon 13th – Fri 17th July, 9:00am - 5:00pm
33 CPE/CMU Credits

You will learn to...

- Establish a minimum standard for IT security knowledge, skills, and abilities. In a nutshell, this course covers all of the non-operating system topics that are in SANS Security Essentials, though not to the same depth. The goal is to enable managers and auditors to speak the same language as system, security, and network administrators.
- Establish a minimum standard for IT management knowledge, skills and abilities. I keep running into managers that do not know TCP/IP, and that is okay; but then they do not know how to calculate total cost of ownership (TCO), leaving me quietly wondering what they do know.
- Save the up-and-coming generation of senior and rapidly advancing managers a world of pain by sharing the things we wish someone had shared with us. As the saying goes, it is okay to make mistakes, just make new ones.

Course details

This completely updated course is designed to empower advancing managers who want to get up to speed quickly on information security issues and terminology. You won't just learn about security, you will learn how to manage security. Lecture sections are intense; the most common student comment is that it's like drinking from a fire hose. The diligent manager will gain vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. Additionally, the course has been engineered to incorporate the NIST Special Publication 800 (series) guidance so that it can be particularly useful to US government managers and supporting contractors.

Essential security topics covered in this management track include: network fundamentals and applications, power, cooling and safety, architectural approaches to defense in depth, cyber attacks, vulnerability assessment and management, security policies, contingency and continuity planning, awareness management, risk management analysis, incident handling, Web application security, offensive and defensive information warfare, culminating with our management practicum. The material uses Knowledge Compression™, special charts, and other proprietary SANS techniques to help convey the key points of critical slides and keep the information flow rate at a pace senior executives demand every teaching hour of the course. The course has been evaluated and approved by CompTIA's CAQC program for Security + 2008 to ensure that managers and their direct reports have a common baseline for security terminology and concepts. You will be able to put what you learn into practice the day you get back into the office.

AUD 507

AUDITING AND MONITORING NETWORKS, PERIMETERS & SYSTEMS

Instructor: James Tarala

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

Course details

One of the most significant obstacles facing many auditors today is how exactly to go about auditing the security of an enterprise. What systems really matter? How should the firewall and routers be configured? What settings should be checked on the various systems under scrutiny? Is there a set of processes that can be put into place to allow an auditor to focus on the business processes rather than the security settings? How do we turn this into a continuous monitoring process? All of these questions and more will be answered by the material covered in this course.

This track specifically helps to provide a risk driven method for tackling the enormous task of designing an enterprise security validation program. 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 repeatably 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
- Conduct a proper network risk assessment to identify vulnerabilities and prioritize what will be audited
- Establish a well-secured baseline for computers and networks—a standard to conduct an audit against
- Perform a network and perimeter audit using a seven-step process
- Audit firewalls to validate that rules/settings are working as designed, blocking traffic as required
- Utilize vulnerability assessment tools effectively to provide management with the continuous remediation information necessary to make informed decisions about risk and resources.
- Audit web application’s configuration, authentication, and session management to identify vulnerabilities attackers can exploit
- Utilize scripting to build a system to baseline and automatically audit Active Directory and all systems in a Windows domain.

> **“By far, this is the most hands-on, technical tool-oriented auditing class I have ever seen. I cannot imagine another class that forces you to use real tools in real situations. It is just like gaining real world experience“**
>
> Jay Russell, u.s. Navy

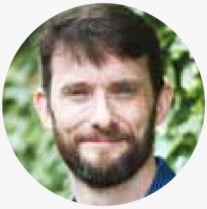
SANS LONDON IN THE SUMMER 2015
INSTRUCTORS

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 in the Summer 2015.

Read on for profiles of this elite group.

STEVE ARMSTRONG

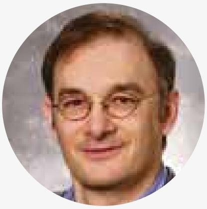


Certified Instructor

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.

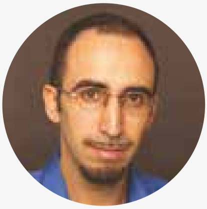
GEORGE BAKOS



Certified Instructor

George Bakos is a SANS Instructor and Technical Fellow & Manager of Cyber Threat Assessment & Awareness at Northrop Grumman. While at the Institute for Security Technology Studies, George was the developer of Tiny Honeypot and the IDABench intrusion analysis system and led the Dartmouth Distributed Honeynet System, fielding deception systems and studying the actions of attackers worldwide. He developed and taught the U.S. Army National Guard's CERT technical curriculum and ran the NGB's Information Operations Training and Development Center research lab for two years, fielding and supporting Computer Emergency Response Teams throughout the United States. A recognized authority in computer security, he has contributed to numerous books and open source software projects; has been interviewed on radio, television, and online publications; briefed the highest levels of government; and has been a member of the SANS Institute teaching faculty since 2001

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 organizations.

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.

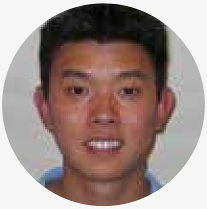
Jess holds a Masters of Science in Telecommunications Engineering from the Univ. Politecnica de Madrid.

G. MARK HARDY

Certified Instructor

G. Mark Hardy is founder and President of National Security Corporation. He has been providing cyber security expertise to government, military, and commercial clients for over 30 years. G. Mark serves on the Advisory Board of CyberWATCH, an Information Assurance/Information Security Advanced Technology Education Center of the National Science Foundation. A retired U.S. Navy Captain, he also served as wartime Director, Joint Operations Center for US Pacific Command, and Assistant Director of Technology and Information Management for Naval Logistics in the Pentagon. Captain Hardy was awarded the Defense Superior Service Medal, the Legion of Merit, five Meritorious Service Medals, and 24 other medals and decorations. A graduate of Northwestern University, he holds a BS in Computer Science, a BA in Mathematics, a Masters in Business Administration, a Masters in Strategic Studies, and holds the GSLC, CISSP, CISM and CISA certifications.

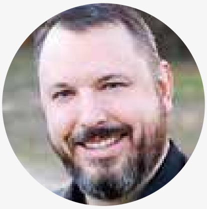
JASON LAM



Certified Instructor

Jason Lam is a senior security analyst at a major financial institution in Canada. His recent SANS Institute courseware development includes Defending Web Application Security Essentials and Web Application Pen Testing Hands-On Immersion. He is currently a SANS certified instructor. Jason started his career as a programmer before moving on to ISP network administration, where he handled network security incidents, which sparked his interest in information security. Jason specializes in Web application security, penetration testing, and intrusion detection. He holds a BA in computer science from York University in Toronto, Ontario, as well as the CISSP, GCIA, GCFW, GCUX, GCWN, and GCIH certifications.

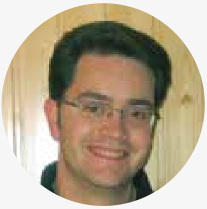
TIM MEDIN



Certified Instructor

Tim Medin is a SANS Instrcutor and senior technical analyst at Counter Hack, a company devoted to the development of information security challenges for education, evaluation, and competition. Prior to Counter Hack, Tim was a Senior Security Consultant for FishNet Security with a focus on penetration testing. He information security experience in a variety of industries including previous positions in control systems, higher education, financial services, and manufacturing. Tim regularly contributes to the SANS Penetration Testing Blog (pen-testing.sans.org/blog/) and the Command Line Kung Fu Blog (blog.commandlinekungfu.com). He is also project lead for the Laudanum Project, a collection of injectable scripts designed to be used in penetration testing.

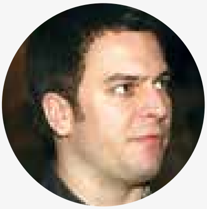
RAUL SILES



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 organizations, 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.

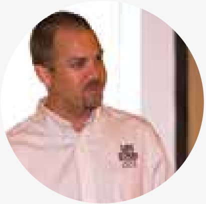
STEPHEN SIMS



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.

JAMES TARALA



Senior Instructor

James Tarala is a principal consultant with Enclave Security and is based out of Venice, Florida. He is a regular speaker and senior instructor with the SANS Institute as well as a courseware author and editor for many SANS auditing and security courses. As a consultant, he has spent the past few years architecting large enterprise IT security and infrastructure architectures, specifically working with many Microsoft-based directory services, e-mail, terminal services, and wireless technologies. He has also spent a large amount of time consulting with organizations to assist them in their security management, operational practices, and regulatory compliance issues, and he often performs independent security audits and assists internal audit groups in developing their internal audit programs. James completed his undergraduate studies at Philadelphia Biblical University and his graduate work at the University of Maryland. He holds numerous professional certifications.

LENNY ZELTSER

Senior Instructor

Lenny Zeltser is product management director at NCR Corp, leading the software and services group that address customers' data protection needs. Before NCR, Lenny led the enterprise security consulting practice at a major cloud services provider. Lenny's expertise is strongest at the intersection of business, technology, and information security and includes incident response, cloud services, and product management. He frequently speaks at conferences, writes articles, and has co-authored books on network security and malicious software. Lenny has an MBA degree fromMIT Sloan, a Computer Science degree from the University of Pennsylvania and has earned the prestigiousGIAC Security Expert designation from SANS Institute. He is also a board director of Sans Technology Institute.

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 organization 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

EVENT LOCATION & TRAVEL INFORMATION SANS LONDON IN THE SUMMER 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 Undergroundstation (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 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

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 in the Summer 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.hotelrusselllondon.co.uk

SANS EMEA

FUTURE SANS EMEA TRAINING EVENTS 2015/16

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

		AUDITS	DEVELOPER		MANAGE		FORENSICS						ICS/SCADA		SECURITY																		
		6 DAYS	6 DAYS	4 DAYS	2 DAYS	5 DAYS	6 DAYS	6 DAYS	6 DAYS	6 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	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS
LOCATION	DATE	AUD507	DEV522	DEV541	MGT433	MGT512	FOR408	FOR508	FOR518	FOR572	FOR585	FOR610	ICS410	ICS515	SEC401	SEC501	SEC502	SEC503	SEC504	SEC505	SEC511	SEC542	SEC560	SEC561	SEC562	SEC566	SEC575	SEC579	SEC585	SEC617	SEC642	SEC660	SEC760
ICS LONDON	APR 27TH - MAY 2ND												●												●								
SEC401 LONDON	APR 27TH - MAY 2ND														●																		
BAHRAIN	MAY 2ND - 7TH												●		●																		
SECURE EUROPE	MAY 5TH - 23RD			●	●			●			●				●			●	●		●						●	●					
ICS VIENNA	JUN 6TH - 10TH												●																				
DUBLIN	JUN 8TH - 13TH						●								●																		
BERLIN	JUN 22ND - 27TH																					●	●							●	●	●	
LONDON IN THE SUMMER	JUL 13TH - 18TH	●	●			●		●		●		●			●				●					●		●	●						
MILAN	SEP 7TH - 12TH														●			●															
ICS AMSTERDAM	SEP 21ST - 26TH												●																				
TALLINN	SEP 21ST - 26TH														●				●		●												
DFIR PRAGUE	OCT 5TH - 17TH						●	●	●	●	●	●																					
GULF REGION	OCT 17TH - 29TH		●												●				●			●	●				●						
LONDON	NOV 14TH - 23RD						●						●		●	●		●	●		●	●	●				●	●				●	●
CAPE TOWN	NOV 30TH - DEC 5TH							●							●				●														
BRUSSELS	JAN 2016						●			●					●				●			●											
DUBAI	JAN 2016													●				●					●										
MUNICH	FEB 2016											●			●				●		●								●				
OSLO	FEB 2016							●					●																		●		

Dates, Locations and Courses offered subject to change