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

SANS EMEA

OCTOBER 17TH TO 29TH 2015 • HILTON DUBAI JUMERIAH, DUBAI

GULF REGION 2015

6 VITAL SANS COURSES

World Renowned Instructors ★ NETWARS ★ SANS@Night talks

SEC401
Security Essentials Bootcamp Style
- - - Jonathan Ham - - -

SEC504
Hacker Tools, Techniques, Exploits and Incident Handling
- - - Steve Armstrong - - -

SEC542
Web App Penetration Testing and Ethical Hacking
- - - Adrien de Beaupre - - -

SEC560
Network Penetration Testing and Ethical Hacking
- - - Erik Van Buggenhout - - -

SEC575
Mobile Device Security and Ethical Hacking
- - - Raul Siles - - -

DEV522
Defending Web Applications Security Essentials
- - - Jason Lam - - -

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

See inside for unique code – register and pay before September 16th and **save $500**

GIAC

SANS EMEA COURSES AT A GLANCE

SAT 17TH - THU 29TH OCTOBER, 2015

		SAT 17	SUN 18	MON 19	TUE 20	WED 21	THU 22	FRI 23	SAT 24	SUN 25	MON 26	TUE 27	WED 28	THU 29
SEC 401	SANS Security Essentials Bootcamp Style	Jonathan Ham	PG 8 →											
SEC 504	Hacker Tools, Techniques, Exploits and Incident Handling	Steve Armstrong	PG 9 →											
SEC 542	Web App Penetration Testing and Ethical Hacking	Adrien de Beaupre							PG 10 →					
SEC 560	Network Penetration Testing and Ethical Hacking	Erik Van Buggenhout							PG 11 →					
SEC 575	Mobile Device Security and Ethical Hacking	Raul Siles	PG 12 →											
DEV 522	Defending Web Applications Security Essentials	Jason Lam							PG 13 →					

Register at www.sans.org/event/gulf-region-2015

SANS GULF REGION 2015 REGISTRATION INFORMATION

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

REGISTER EARLY AND SAVE

Register and pay before by September 16th and save $500 by using code EarlyBird15

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/gulf-region-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 **sans.org/event/gulf-region-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 Oct 7th, 2015, by emailing emea@sans.org

ABOUT SANS

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

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

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

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

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

SANS provides training through several delivery methods, both live & virtual: classroom-style at a 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.

Register at www.sans.org/event/gulf-region-2015

WELCOME TO SANS GULF REGION 2015

SANS Gulf Region runs from Saturday 17th to Thursday 29th October at the Hilton Dubai Jumeriah in Dubai and hosts 6 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 Saturday-Wednesday and 5pm on Thursday and course SEC560 that finishes at 7.15pm on the Saturday.

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

Read on for course descriptions or visit www.sans.org/event/gulf-region-2015

CONTENTS

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

SANS EMEA

SANS EMEA

SANS IT SECURITY TRAINING AND YOUR

CAREER ROAD MAP

CORE COURSES

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
  - **SEC504** Hacker Techniques, Exploits, and Incident Handling GCIH

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:

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
    - **FOR578** Cyber Threat Intelligence
  - **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 organisation 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 Hack
  - **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** — Virtualisation 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 organisation by measuring compliance with policies, procedures, and standards. These experts make recommendations for improvements to make the organisation 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 attacher.

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
  - **SEC503** — Intrusion Detection In-Depth — GCIA
    - **FOR572** — Advanced Network Forensics & Analysis
      - **FOR578** — Cyber Threat Intelligence
- 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
      - **FOR610** — Reverse Engineering Malware: Malware Analysis Tools & Techniques — GREM
  - **FOR585** — Advanced Smartphone and Mobile Device Forensics
  - **FOR518** — MAC Foremsic Analysis

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

SANS ICS410: ICS/SCADA Security Essentials
Provides a set of standardised 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

Specialisations

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

SEC 401

SECURITY ESSENTIALS BOOTCAMP STYLE

Instructor: Jonathan Ham
Six-Day Program: Sat 17th – Thu 22nd October, 9:00am - 7:00pm (5pm on Thu)
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 analyse 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 organisation and prepare a checklist to validate security, creating metrics to tie into training and awareness
- Identify visible weaknesses of a system utilising 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 utilising CIS Scoring Tools and create a system baseline across the organisation

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 organisation's critical information assets and business systems. Our course will show you how to prevent your organisation'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 organisations will be targeted. Whether the attacker is successful in penetrating an organisation's network depends on the effectiveness of the organisation's defence. Defending against attacks is an on going challenge, with new threats emerging all of the time, including the next generation of threats. Organisations need to understand what really works in cybersecurity. What has worked, and will always work, is taking a risk-based approach to cyber defence. Before your organisation 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 defence. 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 organisations.

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: Sat 17th – Thu 22nd October, 9:00am - 5:00pm
37 CPE/CMU Credits
Laptop Required

Course details

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.

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.

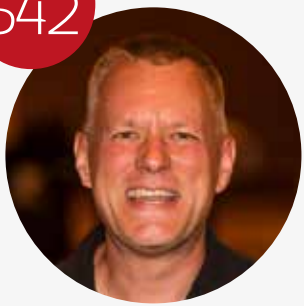
This challenging course is particularly well suited to individuals who lead or are a part of an incident handling team. Furthermore, general security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, 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 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

"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 542



WEB APP PENETRATION TESTING AND ETHICAL HACKING

Instructor: Adrien de Beaupre

Six-Day Program: Sat 24th – Thu 29th October, 9:00am - 5:00pm
36 CPE/CMU Credits
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. But, if your organisation does not properly test and secure its web apps, adversaries can 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 scanning to professional, thorough, high-value web application penetration testing.

Customers expect web applications to provide significant functionality and data access. Even beyond the importance of customer-facing web applications, internal web applications increasingly represent the most commonly used business tools within any organisation. Unfortunately, there is no "patch Tuesday" for custom web applications, so major industry studies find that web application flaws play a major role in significant breaches and intrusions. Adversaries increasingly focus on these high-value targets either by directly abusing public-facing applications or by focusing on web apps as targets after an initial break-in.

Modern cyber defence requires a realistic and thorough understanding of web application security issues. Anyone can learn to sling a few web hacks, but effective web application penetration testing requires something deeper.

SEC542 enables students to 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. Even technically gifted security geeks often struggle with helping organisations understand risk in terms relatable to business. Much of the art of penetration testing has less to do with learning how adversaries are breaking in than it does with convincing an organisation to take the risk seriously and employ appropriate countermeasures.

"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 Program: Sat 24th – Thu 29th October, 9:00am - 5:00pm (7:15pm on Sat)
37 CPE/CMU Credits
Laptop Required

Course details

As a cyber security professional, you have a unique responsibility to find and understand your organisation's vulnerabilities, and to work diligently to mitigate them before the bad guys pounce. Are you ready? SANS SEC560, our flagship course for penetration testing, fully arms you to address this duty head-on.

SEC560 is the must-have course for every well-rounded security professional.

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.

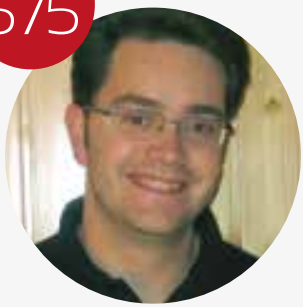
After building your skills in challenging labs over five days, the course culminates with a full-day, real-world network penetration test scenario. You will conduct an end-to-end penetration test, applying the knowledge, tools and principles from throughout the course as you discover and exploit vulnerabilities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

You will learn to...

- 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

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

SEC 575



MOBILE DEVICE SECURITY AND ETHICAL HACKING

Instructor: Raul Siles

Six-Day Program: Sat 17th – Thu 22nd October, 9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required

You will learn to...

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

Course details

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

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

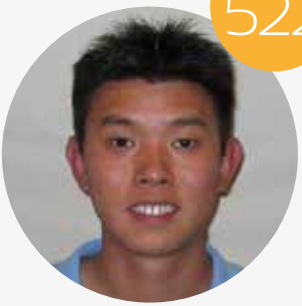
SEC575: Mobile Device Security and Ethical Hacking is designed to help organisations secure their mobile devices by equipping personnel with the knowledge to design, deploy, operate, and assess a well-managed and safe mobile environment. The course will help you build the critical skills to support your organisation's secure deployment and use of mobile phones and tablets. You will learn how to capture and evaluate mobile device network activity, disassemble and analyse mobile code, recognise weaknesses in common mobile applications, and conduct full-scale mobile penetration tests.

You will gain hands-on experience in designing a secure mobile phone network for local and remote users and learn how to make critical decisions to support devices effectively and securely. You will also learn to analyse and evaluate mobile software threats, as well as understand how attackers exploit mobile phone weaknesses, so that you can test the security of your own deployment. With these skills, you will be a valued mobile device security analyst, fully able to guide your organisation through the challenges of securely deploying mobile devices.

"Real eye-opener, not only suitable for pen-testers, but also for technical security roles."
Pascal Buyl, YARA

DEV 522

DEFENDING WEB APPLICATIONS SECURITY ESSENTIALS



Instructor: Jason Lam

Six-Day Program: Sat 24th – Thu 29th October, 9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required

Course details

Traditional network defences, 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 organisation'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 maximise 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.

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

"Not only does DEV522 teach the defences for securing web apps, it also shows how common and easy the attacks are thus the need to secure the apps"

Brandon Hardin, ITC

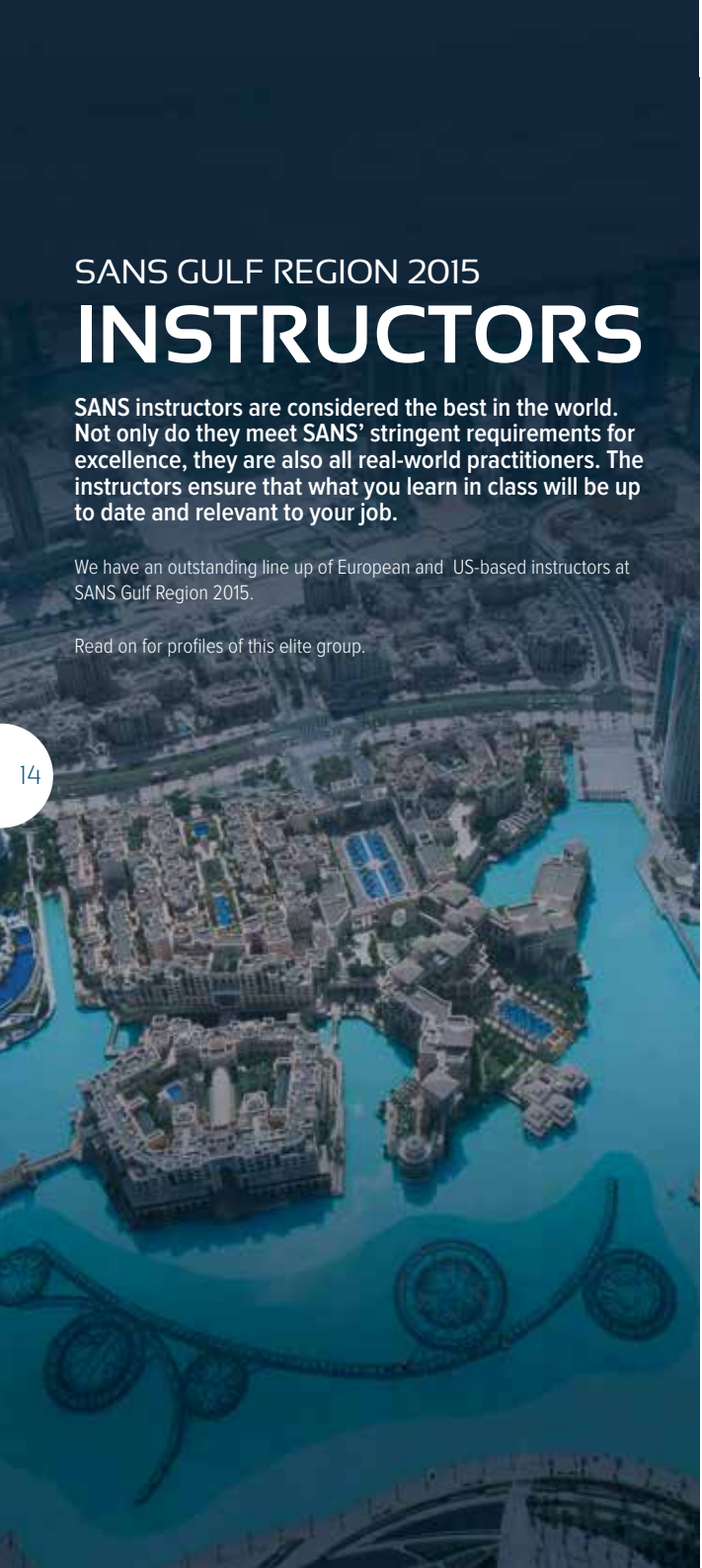
SANS GULF REGION 2015

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 Gulf Region 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, defence 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.

ADRIEN DE BEAUPRE

Certified Instructor

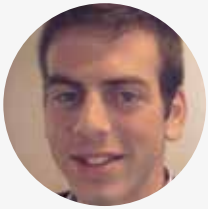
Adrien de Beaupre is a certified SANS instructor and works as an independent consultant in Ottawa, Ontario. His work experience includes technical instruction, vulnerability assessment, penetration testing, intrusion detection, incident response and forensic analysis.

He is a member of the SANS Internet Storm Center (isc.sans.edu). He is actively involved with the information security community, and has been working with SANS since 2000.

Adrien holds a variety of certifications including the GXPN, GPEN, GWAPT, GCIH, GCIA, GSEC, CISSP, OPST, and OPSA.

When not geeking out he can be found with his family, or at the dojo.

ERIK VAN BUGGENHOUT



Certified 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.

JONATHAN HAM

Certified Instructor

Jonathan is an independent consultant who specialises in large-scale enterprise security issues, from policy and procedure, through staffing and training, to scalable prevention, detection, and response technology and techniques.

With a keen understanding of ROI and TCO (and an emphasis on process over products), he has helped his clients achieve greater success for over 20 years, advising in both the public and private sectors, from small upstarts to the Fortune 500.

He's been commissioned to teach NCIS investigators how to use Snort, performed packet analysis from a facility more than 2000 feet underground, and chartered and trained the CIRT for one of the largest U.S. civilian Federal agencies.

He has variously held the CISSP, GSEC, GCIA, and GCIH certifications, and is a member of the GIAC Advisory Board.

A former combat medic, Jonathan still spends some of his time practicing a different kind of emergency response, volunteering and teaching for both the National Ski Patrol and the American Red Cross.

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.

RAUL SILES

Certified Instructor

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

The FREE SANS Portal account

Sign up for a SANS Portal account

and receive free Webcasts,

Newsletters, latest security news

and updates, including:

SANS **News**Bites

SANS NewsBites is a semi-weekly, high-level executive summary of the most important news articles that have been published on computer security during the previous week. Each news item is briefly summarised and includes a reference on the web for more information, when available.

Sign up and stay updated with the high-level perspective of all the latest security news. New issues are delivered free every Tuesday and Friday.

@**RISK:** The Consensus Security Alert

@RISK provides a reliable weekly summary of:

1. Newly discovered attack vectors
2. Vulnerabilities with active new exploits
3. Insightful explanations of how recent attacks worked and other valuable data

A key purpose of the @RISK is to provide data that will ensure that the 20 Critical Controls (the US and UK benchmark for effective protection of networked systems) continue to be the most effective defences for all known attack vectors.

Ouch!

OUCH! is the first consensus monthly security awareness report for end users. It shows what to look for and how to avoid phishing and other scams, plus viruses and other malware -- using the latest attacks as examples. It also provides pointers to great resources like the amazing Phishing Self-Test. 460 organisations, large and small, helped make it a useful service. More than 100 security officers check each issue for accuracy and readability before it is distributed to the community.
If you want to distribute OUCH to all your users you may either forward it or subscribe a single address that is a mailing list.

Webcasts

SANS Information Security Webcasts are live web broadcasts combining knowledgeable speakers with presentation slides. SANS offers several types of webcasts designed to provide valuable information and enhance your security knowledge.

Ask The Expert Webcasts: SANS Experts bring current and timely information on relevant topics in IT Security. ATE webcasts are the go-to online format to obtain actionable information to help you in your security goals.

- Analyst Webcasts: A follow-on to the SANS Analyst Program, Analyst webcasts provide key information from our whitepapers and surveys.
- WhatWorks Webcasts: The SANS WhatWorks webcasts bring powerful customer experiences showing how end users resolved specific IT Security issues.
- Tool Talks: Tool Talks are designed to give you a solid understanding of a problem, and how a vendor's commercial tool can be used to solve or mitigate that problem.

Register FREE at www.sans.org

To register for your **free** SANS Portal Account go to **www.sans.org**

SANS SECURING THE HUMAN SECURITY AWARENESS TRAINING

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

Securing The Human Key Benefits:

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

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

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

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

www.securingthehuman.org

EVENT LOCATION & TRAVEL INFORMATION SANS GULF REGION 2015

Event Location:
Hilton Dubai Jumeirah Resort, The Walk, Dubai Marina P.O.Box 2431, Dubai, U.A.E
Telephone: +971 4 399 1111
E-mail: info.jumeirah@hilton.com
Website: www.hilton.com

Directions from the Airport:

Dubai International Airport:
Exit Dubai International Airport via Al Quds St/D 91 and take the ramp on the left to E 11. Continue onto Sheikh Zayed Road taking exit 35. Follow the signs to Jumeirah Beach Road. As you turn left, the destination will be on your right.

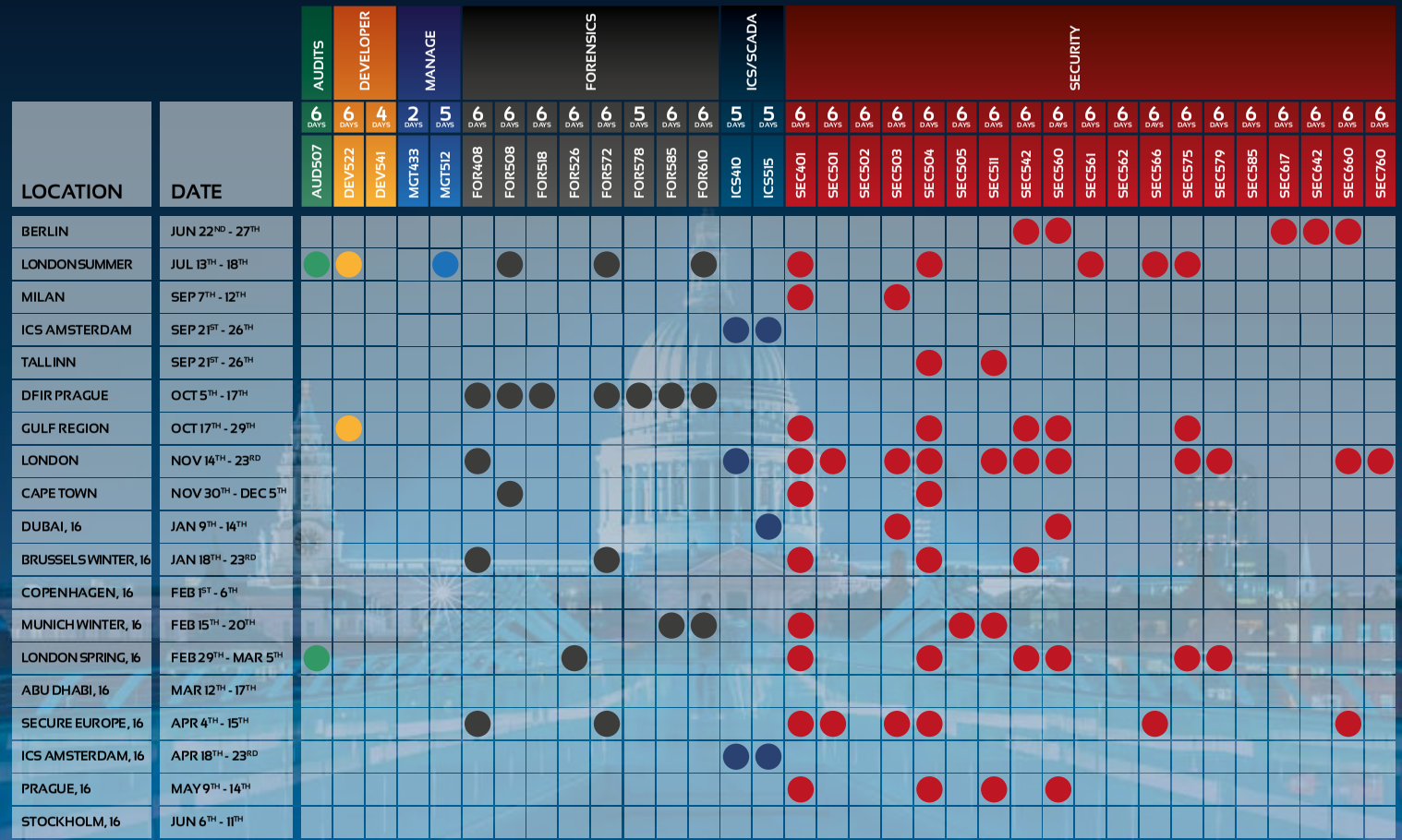
Distance from Hotel: 22 mi.
Drive Time: 45 min.
Taxi: Typical minimum charge 100.0 AED

Abu Dhabi International Airport:
Follow signs to Dubai. When entering Dubai on Sheik Zayed Road, take exit 29 and follow signs for Dubai Marina. Enter Jumeirah Beach Road and as you turn left, the destination will be on your right.

Distance from Hotel: 62 mi.
Drive Time: 70 min.
Taxi: Typical minimum charge 220.0 AED

FUTURE SANS EMEA TRAINING EVENTS 2015/16

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



V10- A5

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

Dates, Locations and Courses offered subject to change