Systems & Network Training

Save on expenses. This course is also available on your premises.

Penetration testing and Ethical Hacking

A 5 day Hands on training course

Description

An advanced, technical, hands on course focusing on ethical hacking and counter hacking. The course revolves around a series of exercises based on "hacking" into a network (pen testing the network) and then defending against the hacks.

Key outcomes

By the end of the course delegates will be able to:

- ✓ Perform penetration tests.
- ✓ Explain the technical workings of various penetration tests.
- ✓ Produce reports on results of penetration tests.
- ✓ Defend against hackers.

Training approach

This structured course uses Instructor Led Training to provide the best possible learning experience. Small class sizes ensure students benefit from our engaging and interactive style of teaching with delegates encouraged to ask questions throughout the course. Quizzes follow each major section allowing checking of learning. Hands on sessions are used throughout to allow delegates to consolidate their new skills.

Details

Who will benefit?
Technical support staff, auditors and security professionals. Staff who are responsible for network infrastructure integrity.

Prerequisites
IP security foundation for engineers.
Definitive IP VPNs for engineers.

Duration: 5 days

Customer rating: ★★★★½

Generic training	Small class sizes	Hands On training	Our courseware	Customise your course
Generic training compliments product specific courses covering the complete picture of all relevant devices including the protocols "on the wire".	We limit our maximum class size to 8 delegates; often we have less than this. This ensures optimal interactivity between delegates and instructor.	The majority of our courses use hands on sessions to reinforce the theory.	We write our own courses; courseware does not just consist of slides and our slides are diagrams not bullet point text.	Please contact us if you would like a course to be customised to meet your specific requirements. Have the course your way.
"Friendly environment with expert teaching that teaches the why before the how." G.C. Fasthosts	*"Excellent course. The small class size was a great benefit..."* M.B. IBM	*"Not many courses have practice added to it. Normally just the theoretical stuff is covered."* J.W. Vodafone	*"Comprehensive materials that made the course easy to follow and will be used as a reference point."* V.B. Rockwell Collins	*"I was very impressed by the combination of practical and theory. Very informative. Friendly approachable environment, lots of hands on."* S.R. Qinetiq

Penetration testing and Ethical Hacking

Course content

Introduction

Hacking concepts, phases, types of attacks, “White hacking”, What is penetration testing? Why use pen testing, black box vs. white box testing, equipment and tools, security lifecycles, counter hacking, pen testing reports, methodologies, legal issues.

Physical security and social engineering

Testing access controls, perimeter reviews, location reviews, alarm response testing. Request testing, guided suggestions, trust testing. Social engineering concepts, techniques, counter measures, Identity theft, Impersonation on social media, Footprints through social engineering

Reconnaissance (discovery)

Footprinting methodologies, concepts, threats and countermeasures, WHOIS footprinting, Gaining contacts and addresses, DNS queries, NIC queries, ICMP ping sweeping, system and server trails from the target network, information leaks, competitive intelligence. Scanning pen testing.

Gaining access

Getting past passwords, password grinding, spoofed tokens, replays, remaining anonymous.

Scanning (enumeration)

Gaining OS info, platform info, open port info, application info. Routes used, proxies, firewalking, Port scanning, stealth port scanning, vulnerability scanning, FIN scanning, Xmas tree scanning, Null scanning, spoofed scanning, Scanning beyond IDS. Enumeration concepts, counter measures and enumeration pen testing.

Hacking

Hacking webservers, web applications, Wireless networks and mobile platforms. Concepts, threats, methodology, hacking tools and countermeasures.

Trojan, Backdoors, Sniffers, Viruses and Worms

Detection, concepts, countermeasures, Pen testing Trojans, backdoors, sniffers and viruses. MAC attacks, DHCP attacks, ARP poisoning, DNS poisoning Anti-Trojan software, Malware analysis Sniffing tools.

Exploiting (testing) vulnerabilities

Buffer overflows,, simple exploits, brute force methods, UNIX based, Windows based, specific application vulnerabilities.

DoS/DDoS

Concepts, techniques, attack tools, Botnet, countermeasures, protection tools, DoS attack pen testing.

SQL Injection

Types and testing, Blind SQL Injection, Injection tools, evasion and countermeasures.

Securing networks

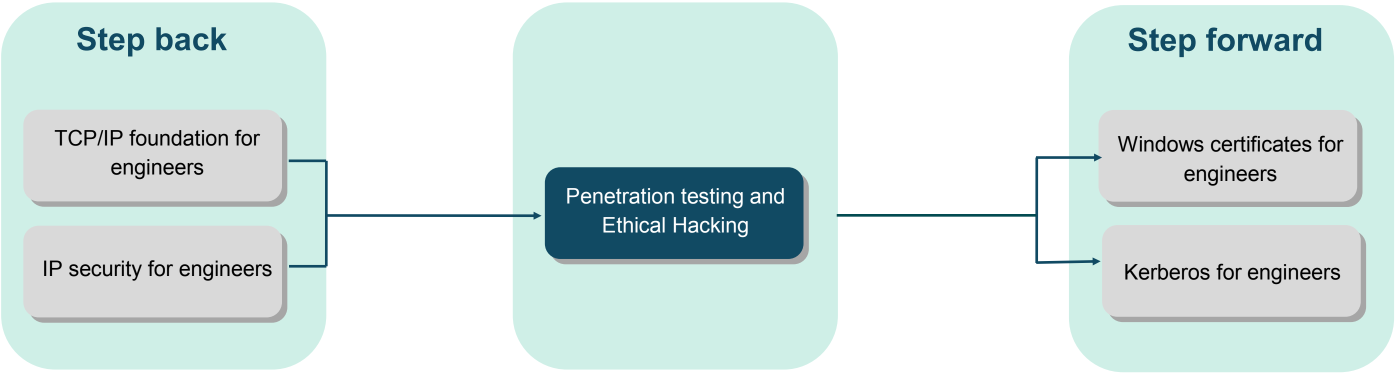
“Hurdles”, firewalls, DMZ, stopping port scans, IDS, Honeypots, Router testing, firewall testing, IDS testing, Buffer Overflow.

Cryptography

PKI, Encryption algorithms, tools, Email and Disk Encryption.

Information security

Document grinding, privacy.



Step back

TCP/IP foundation for engineers

IP security for engineers

Penetration testing and Ethical Hacking

Step forward

Windows certificates for engineers

Kerberos for engineers