

Internet Security: **Internet Security Fundamentals**

Overview

Good security begins with regular assessment, and that is the premise behind the Internet Security Fundamentals course. Internet Security Fundamentals is an intensive, hands on two day course that places attendees in the shoes of an attacker to get a complete understanding of Internet and Network defence, from both sides of the spectrum.

Participants get hands-on experience with actual assessment tools, and learn the techniques attackers use with gathering information for an attack.

Students also learn invaluable rules on how to immediately improve their own corporate security, and learn where to obtain the latest security information.

In short Internet Security Fundamentals attendees leave with an in-depth understanding of the threats and risks facing their organizations security as well as the basic knowledge in how to counter them.

What You Will Learn

- Basic Internet Overview
- Review security resources available on the internet
- Internet Components and protocols
- Understand Routers, DNS, Firewalls, TCP/IP, UDP, Ports and services (mail, web, FTP etc)

- Network Mapping and Information Gathering
- How IP can be used and abused to gather information and gain access undetected using common IT tools such as -

- Ping, Traceroute, Whois, Host Identification, Port and Service scanning, Telnet, Fingerprinting and OS detection.

- Vulnerability scanning using a range of freeware scanners.
- Stealth Scanner
- NMAP
- Nessus
- SecureScan NX
- How scanners detect vulnerabilities

Suitable for

The course is designed specifically for IT managers, Information security managers, Network or System administrators, Project managers, Team leaders, Software testers and all other professionals directly or indirectly involved with information security.

Course Content

- What makes a Hacker
- How does the Hacker work
- Information discovery
- Legal/Ethical Issues including a look at ISO17799/BS7799
- Trojan Horses
- Technical Fundamentals
- Firewall Technology
- Sniffing the wire
- Patch Management
- Password Attacks
- Bruteforce Hacking
- Cracking Unix
- Wireless Security

Course Instructors

Our instructors are experienced SecureTest Security Engineers, who have thorough knowledge of the security breaches on the Internet through their day-to-day work with testing and supporting organizations and network security.

Pre-Requisites

The courses materials cover all topics within the course.

Duration

2-Days. The course begins at 9.30 on Day 1 and ends at 16.00 on Day 2

Cost

£995+Vat

The course training fees include attendance of the course for one delegate, all course materials and training equipment, as well as lunch and refreshments during the course. The training fee does NOT include travel, accommodation or other expenses incurred.

For further information please contact Customer Services on:
+44 (0)20 7621 9740 or e-mail info@cstl.com