

Internet Security: **Internet Security Advanced**

Overview

As reactive solutions continue to prove ineffective to fast moving attacks, corporations need to turn to proactive assessment to increase security resilience of their networks.

New system vulnerabilities are being uncovered daily and automated hacking has become the newest everyday threat for all sizes of organizations, albeit the proliferation of firewalls and anti-virus programs. Central to the understanding of this development is insight in the methodology being used by these attacks and the vulnerabilities permitting them.

This is the background for Internet Security Advanced, which is a natural follow-up to the popular Internet Security Fundamentals.

The course is an intensive and hands-on 2-day course giving the participant in-depth experience with testing a number of systems, thereby being able to manually verify vulnerabilities found by an automated scan.

Course Content

- **Vulnerabilities**
What are they and where do they come from
False Positives and False Negatives
Verification of test results
- **Operating Systems**
Windows Operating systems – Including NetBios enumeration and attack
Unix Operating systems – Enumeration NFS, RPC, Finger, r commands etc.
- **Network Tools**
Enumeration and attack
Network tools – Netcat, fpipe, nmap, snmpwalk etc.
- **Firewalls**
Weaknesses in firewall rule-sets and exploitation
- **Hacking Exercises**
Exploit existing vulnerabilities to attain administrator rights
- **Databases**
Overview of database security
SQL Injection
- **Man-in-the-middle attacks**
ARP spoofing, ARP flooding
Sniffing switched networks
- **Wireless Hacking techniques**
Overview of wireless technologies
Wireless Scanning and enumeration – Netstumbler, Kismet, ethereal etc
Cracking wireless encryption

What You Will Learn

Through a number of practical hacking exercises, the participant will attain a high level of confidence in evaluating the security level of a given system as well as the insight to define the best path to hardening it.

The participant will reproduce the actual attack that a hacker would make in order to achieve privileged access and will become accustomed with the various types of testing tools through practical usage.

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 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 course objectives focus on technical aspects of IT security and require a relatively high level of technical competence. It is recommended to have participated in the Internet Security Fundamentals 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

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