

Internet Security: **Guided Penetration Test**

Test your own public servers from our secure environment, under the guidance of our CESG CHECK Team Leaders

Leave the course with a detailed report of your public servers' security

Overview

Penetration testing is an integral part of all good security policies and practices. Only by testing can you validate and ensure that systems have been correctly secured and locked down against hacking threats.

Ideally, one would have a specialist testing company carry out a penetration test regularly. However, employing the services of a third party tester every time you make a policy change to the firewall or update a service pack on the network could start to get expensive, not least impractical.

The Guided Penetration test is designed to show you the methodologies, tools and techniques used to perform a manual test. Delegates will test **their own companies' public network**, supported by two CESG Check 'Green' testing consultants who will guide them through the whole process from the initial information gathering to the production and presentation of the final report.

Course Content

System set-up - Setting a system up for testing, where to place it in the firewall infrastructure.

Operating system choice - protecting the test machine

Documentation - log and data files & how to store them safely

Information gathering - Whois, DNS records

Enumeration - ICMP, port scanners, common pitfalls

Vulnerability assessment tools - what is available, what are the various strengths and weaknesses of each

CGI Scanners

Manual Penetration Testing – where scanners fail, and only human knowledge & intuition can go

Application level testing – application level vulnerabilities account for over 50% of issues found when testing web servers!

Verify results – how to discover false positive results.

Deliverables

Report writing – how to write a report suitable for your target audience; the Management Board will be interested in your test, but may not understand the technicalities.

Simple risk assessment – how to categorise a vulnerabilities' impact in your environment.

High risk

- Vulnerability is ranked High risk, when with one single vulnerability; one could gain unauthorised privileged access to the system under test.

Medium risk

- In the following cases vulnerability is ranked Medium risk: If vulnerability can be combined with one or more other vulnerabilities to gain unauthorised privileged access.

Low risk

- Low risk vulnerabilities are mostly services that shouldn't be open, offering too much information about the system

Suitable for

The course is designed specifically for Information security managers, Security Administrators, Network or System administrators, Software testers and all other professionals directly involved with the technical aspects of information security.

Course Instructors

Our instructors are CESG CHECK 'Green' Team leaders, who have thorough knowledge of the security breaches on the Internet through their day-to-day work with testing and supporting organisations and network security.

Pre-Requisites

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

Duration

One Day.

Cost

£1,495+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