

Security Vulnerabilities Assessment (Ethical Hacking): Understanding the Threats - Hands-on Practical



A unique, authoritative, high-value, hands-on practical course which provides an essential understanding of the tools, methodologies and vulnerabilities that hackers could employ to exploit the IT systems of your organisation



[Schedule](#)



[Email](#)



Call +44 (0)113 398 335

Course benefits

Most organisations now realise that in order to defend themselves against the threat of attack by hackers, crackers, and indeed any individual intent on causing disruption to their IT systems, IT staff must have an informed and current understanding of the present-day methodologies, tools, and vulnerabilities which allow these exploits to happen.

This course is designed to educate IT support staff to allow them to defend their systems against hacking attacks. During this course, delegates learn about the hacker mindset and become familiar with the tools and methodologies that are used to attack systems.

Objectives

This course fulfills two vital objectives for anyone working in IT systems administration, IT security or IT support roles:

1. The course builds a strong awareness of the wide range of risks and threats now faced even by organisations which believe they have strong security solutions in place.
2. The course provides delegates with a solid understanding of the control measures that need to be put in place in order to limit an organisation's vulnerabilities and risk of attack.

During the course, delegates learn:

- The tools, techniques and methodologies employed by hackers in a dedicated lab environment.
- How hackers can collect and assimilate information about an organisation's infrastructure whilst avoiding detection.
- How information may be used to assess your IT systems' weaknesses and subsequently launch an attack against target systems.
- The techniques that are typically used to gain access into a system.
- The types of tools that are used to elevate access on a system.
- The techniques used by hackers to conceal their tracks and the methods via which access to a target system may be maintained.
- The limitations of security firewall systems and the tools used to bypass them.
- How hackers bypass Intrusion Detection Systems (IDS).
- Measures that you can employ to secure and protect information against hacker attacks.

Hands-on practical labs

Using state-of-the-art classroom setups, delegates work with

Course 335: Content

An Introduction to Hacking

A background into hacking
Understanding hacker genres
Review of high profile attacks

Risks to your Business

Impacts on your organisation and its reputation
Operational and financial risks

TCP/IP Essentials

A review of TCP/IP protocols and ports
IP, TCP, UDP, ICMP
Protocol numbers
TCP and UDP ports
Spoofing and session hijacking
Denial of Service attacks (DoS)

Attack Methodology

The anatomy of a typical attack

Hacker Tools and Techniques

The categories of tools and techniques employed by hackers

Information

Discovery

How information about a target can be acquired

Target Scanning System Detection

Examining the target landscape
Sophisticated scanning methods
Fingerprinting
Operating system detection

Vulnerability Assessment

How attackers probe for weaknesses
The use of 'Firewalking' to map out access controls

Exploitation and Privilege Escalation

How easily can access be gained to a system?
How privilege is escalated to achieve full control of Windows and UNIX systems

Trojans, Back-Doors and Root Kits

Practical hands-on use of 'Trojan horses' and 'back doors'
Working with root kits to hide the presence of a hacker at the application and kernel level

Firewall and IDS Evasion

How attacks can traverse a firewall
The role of intrusion detection systems (IDS)
How IDS can be evaded

Hacking Prevention

Security policy
System integrity
Hardening
Monitoring
Security tools
Vulnerability assessment
Penetration testing

their own Microsoft Windows and UNIX systems, and associated server software. A wide range of hacking tools are featured and used during the course.

Who should attend?

This course is a must-have for all people responsible for the security or support of IT systems within an organisation, including Systems Administrators, Network Administrators, Systems Auditors, Security Officers, and IT Security Professionals.

With the rapid increase in the numbers of hackers and hacker tools, the increasing complexity of IT systems and networks, and with the continuous announcement of security vulnerabilities in operating systems, applications software, and network infrastructure devices, all IT support professionals must now become knowledgeable in the essentials of network security and vulnerability assessment.

Pre-requisites

Delegates must have a basic understanding of TCP/IP protocols, and a technical background in Microsoft Windows 2000, Microsoft Windows XP or UNIX operating systems.



Copyright © 1996-2003 LEVER Technology Group plc, Ebor Court, Westgate, Leeds, LS1 4ND, UK
Tel: +44 (0) 113 398 335 Fax: +44 (0) 113 398 3301
[Important Notices](#) and [Privacy Statement](#) Maintained by www.lever.co.uk