



**The hackers' methods
in theory and practice**



Hacking Techniques Training





Hacker: Hack'er, *n.*
A **skilled** operator who infiltrates computer systems.

One of the biggest problems facing many organisations today is a lack of in-house security knowledge. Gaining an insight into the hackers' methods of penetrating networks is certainly not easy. Whilst product-specific courses are available, few vendors like to discuss their products' limitations and the whole process can be long and difficult, not to mention expensive.

The right strategy

To defend against hacking, one must think like a hacker and study their methods. Sec-Tec offers a unique training course which provides an exciting insight into the techniques employed by hackers to gain access to systems. Built on years of experience in testing the security of financial institutions and Government departments, the course examines the tools hackers use and demonstrates how to defend against them.

What is included?

The course is regularly updated to keep up with the ever-changing and fast-moving world of IT security. The topics currently covered include:

- Hackers, hacking and the underground
- TCP/IP security
- DNS security
- Web security
- FTP security
- E-Mail security
- Windows® security
- UNIX® security
- Vulnerability assessment using freely available tools

Our pedigree

Sec-Tec's policy has always been to stay product-independent in order to be able to offer the best possible advice and service. The course is taught by our principal Penetration Tester who has experience of hundreds of penetration-testing assignments.

Location

Usually, the course is held at our training facility in London: our purpose-built hacking network provides the experience of real-life attack scenarios in a hands-on environment.

Duration

The course lasts for two days, after which delegates leave with presentation materials, a Certificate of Attendance, and a CD-ROM containing a fully-functional suite of hacking tools in order to test their own network security.



Introduction	Thinking like a Hacker, Developer Assumption, Vulnerabilities and Exploits, What is Security?
TCP/IP Background	TCP/IP History, TCP/IP Architecture.
TCP/IP and Security	ARP Poisoning, Network Sniffing, IP Fragmentation, Spoofing and SYN Flooding.
Domain Name Server(DNS)	Why Hack DNS?, the Human Factor, Record Changing, Secure DNS Servers.
E-Mail Security	SMTP, POP3, IMAP, SPAM, Content, Server Implementations, Dangerous Commands.
Web Security	CGI, ASP and JSP Technologies, Tampering with Variables, Default Scripts, Directory-Traversal Attacks, Buffer Overflows, Cross-Site Scripting Attacks, SQL Injection Attacks, Weak Session Credentials, Hidden Form Fields, JSP Weaknesses.
Firewalls	Packet Filters, Application Layer Firewalls, Stateful Inspection Firewalls, Network Address Translation (NAT), NAT Limitations, Hardened Operating Systems and Firewall Limitations. What Firewalls Can't Protect.
Windows 2000/2003	Active Directory, Group Policy, Popular GPO Settings, Account Lockout, Null Sessions, Network Authentication Mechanisms including LM, NTLM and NTLMv2, Active Directory Restore Account, EFS, Hardening Windows.
Unix Security	UNIX History, the UNIX Universe, UNIX Architecture, Users and Groups, Password Basics, the Password File, Sun's Network Information Service (NIS), File Systems and Permissions, Changing File Permissions, SETUID and SETGID, Extra Services and Logging.
Hacking Tools and Methodologies	DNS, RIPE, Port Scanners, Banner Enumeration, Vulnerability Databases, CGI Scanners, DumpSec, Nessus and Commercial Tools.

On-site training

For training requirements involving four or more delegates, the entire two-day course can be delivered on-site, using specially-configured laptops in a peer-to-peer networking environment. This option is available at no extra charge and can therefore represent a considerable saving over the normal costs of sending a number of delegates to a publicly-held course.

For more information, including training dates, visit www.sec-tec.co.uk, or call us on 020 8317 7962.





www.sec-tec.co.uk



Tel: +44 (0) 20 8317 7962
Fax: +44 (0) 20 8317 8051
Email: info@sec-tec.co.uk
Web: www.sec-tec.co.uk

