

IP security foundation for engineers

A 2 day **Hands on** training course



Description

Connection to the Internet is becoming an essential business tool. This course looks at firewalls, digital certificates, encryption and other essential topics for securing networks. A generic course that looks at firewalls and VPNs. Hands on sessions include using hacking tools and configuring firewalls.



Key outcomes

By the end of the course delegates will be able to:

- ✓ Describe:
 - Basic security attacks
 - RADIUS
 - SSL
 - VPNs
- ✓ Implement digital certificates
- ✓ Deploy firewalls.
- ✓ Secure networks.



Training approach

This structured course uses Instructor Led Training to provide the best possible learning experience. Small class sizes ensure students benefit from our engaging and interactive style of teaching with delegates encouraged to ask questions throughout the course. Quizzes follow each major section allowing checking of learning. Hands on sessions are used throughout to allow delegates to consolidate their new skills.



Details

Who will benefit?

Network administrators. Network operators. Security auditors.

Prerequisites

TCP/IP foundation for engineers.

Duration: 2 days

Customer rating: ★★★★★

Generic training



Generic training complements product specific courses covering the complete picture of all relevant devices including the protocols "on the wire".

"Friendly environment with expert teaching that teaches the why before the how."
G.C. Fasthosts

Small class sizes



We limit our maximum class size to 8 delegates; often we have less than this. This ensures optimal interactivity between delegates and instructor.

"Excellent course. The small class size was a great benefit..."
M.B. IBM

Hands On training



The majority of our courses use hands on sessions to reinforce the theory.

"Not many courses have practice added to it. Normally just the theoretical stuff is covered."
J.W. Vodafone

Our courseware



We write our own courses; courseware does not just consist of slides and our slides are diagrams not bullet point text.

"Comprehensive materials that made the course easy to follow and will be used as a reference point."
V.B. Rockwell Collins

Customise your course



Please contact us if you would like a course to be customised to meet your specific requirements. Have the course your way.

"I was very impressed by the combination of practical and theory. Very informative. Friendly approachable environment, lots of hands on."
S.R. Qinetiq

IP security foundation for engineers

Course content

TCP/IP review

Brief overview of the relevant headers. Exercise: Download software for course, use analyser to capture passwords on the wire.

Security review

Policies, Types of security breach, denial of service, data manipulation, data theft, data destruction, security checklists, incident response.

Security exploits

The Internet worm, IP spoofing, SYN attack, hijacking, Ping o' Death... keeping up to date with new threats. Exercise: Use a port scanning tool, use a "hacking" tool.

Firewalls

Products, Packet filtering, DMZ, content filtering, stateful packet inspection, Proxies, firewall architectures, Intrusion Detection Systems, Viruses. Exercise: Set up a firewall and prevent attacks.

NAT

NAT and PAT, Why use NAT, NAT-ALG, RSIP.

Encryption

Encryption keys, Encryption strengths, Secret key vs Public key, algorithms, systems, SSL, SSH, Public Key Infrastructures. Exercise: Run a password-cracking program.

Authentication

Types of authentication, Securid, Biometrics, PGP, Digital certificates, X.509 v3, Certificate authorities, CRLs, PPP authentication, RADIUS. Exercise: Using certificates.

VPNs and IPSec

What is a VPN, tunnelling, L2F, PPTP, L2TP, IPSec, AH, ESP, transport mode, tunnel mode.

