Systems & Network Training

Cyber security for engineers

A 5 day Hands on training course

Save on expenses. This course is also available on your premises.

Description

This cyber security course focuses on the network side of security. Technologies rather than specific products are studied focusing around the protection of networks using firewalls and VPNs.

Key outcomes

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

- Describe:
  Basic security attacks, RADIUS, SSL, VPNs
- Deploy firewalls and secure networks.
- Explain how the various technologies involved in an IP VPN work.
- Describe and implement:
  L2TP, IPsec, SSL, MPLS L3 VPNs.

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?
Anyone working in the security field.

Prerequisites
TCP/IP foundation for engineers.

Duration: 5 days

Overall rating: ★★★★★

Generic Training	Small Class Sizes	Hands On Training	Our Courseware	Customise Your Course
Generic training compliments product specific courses covering the complete picture of all relevant devices including the protocols "on the wire".	We limit our maximum class size to 8 delegates; often we have less than this. This ensures optimal interactivity between delegates and instructor.	The majority of our courses use hands on sessions to reinforce the theory.	We write our own courses; courseware does not just consist of slides and our slides are diagrams not bullet point text.	Please contact us if you would like a course to be customised to meet your specific requirements. Have the course your way.
"*Friendly environment with expert teaching that teaches the why before the how.*" G.C. Fasthosts	*"Excellent course. The small class size was a great benefit..."* M.B. IBM	*"Not many courses have practice added to it. Normally just the theoretical stuff is covered."* J.W. Vodafone	*"Comprehensive materials that made the course easy to follow and will be used as a reference point."* V.B. Rockwell Collins	*"I was very impressed by the combination of practical and theory. Very informative. Friendly approachable environment, lots of hands on."* S.R. Qinetiq

Cyber security for engineers

Course Content

Security review
Denial of service, DDOS, data manipulation, data theft, data destruction, security checklists, incident response.
Security exploits
IP spoofing, SYN attacks, hijacking, reflectors and amplification, keeping up to date with new threats. Hands on: port scanning, use a “hacking” tool.
Client and Server security
Windows, Linux, Log files, syslogd, accounts, data security. Hands on: Server hardening.
Firewall introduction
What is a firewall? Firewall benefits, concepts. Hands on: launching various attacks on a target.
Firewall types
Packet filtering, SPI, Proxy, Personal. Software firewalls, hardware firewalls. Firewall products. Hands on: Simple personal firewall configuration.
Packet filtering firewalls
Things to filter in the IP header, stateless vs. stateful filtering. ACLs. Advantages of packet filtering. Hands on: Configuring packet filtering firewalls.
Stateful packet filtering
Stateful algorithms, packet-by-packet inspection, application content filtering, tracks, special handling (fragments, IP options), sessions with TCP and UDP. Firewall hacking detection: SYN attacks, SSL, SSH interception. Hands on: SPI firewalls.
Proxy firewalls
Circuit level, application level, SOCKS. Proxy firewall plusses and minuses. Hands on: Proxy firewalls.
Firewall architectures
Small office, enterprise, service provider, what is a DMZ? DMZ architectures, bastion hosts, multi DMZ. Virtual firewalls, transparent firewalls. Dual firewall design, high availability, load balancing, VRRP. Hands on: Resilient firewall architecture.
Testing firewalls
Configuration checklist, testing procedure, monitoring firewalls, logging, syslog. Hands on: Testing firewalls.
Encryption
Encryption keys, Encryption strengths, Secret key vs Public key, algorithms, systems, SSL, SSH, Public Key Infrastructures. Exercise: Password cracking.
Authentication
Types of authentication, Securid, Biometrics, PGP, Digital certificates, X.509 v3, Certificate authorities, CRLs, RADIUS. Exercise: Using certificates.
VPN overview
What is a VPN? What is an IP VPN? VPNs vs. Private Data Networks, Internet VPNs, Intranet VPNs, Remote access VPNs, Site to site VPNs, VPN benefits and disadvantages.
VPN Tunnelling
VPN components, VPN tunnels, tunnel sources, tunnel end points, tunnelling topologies, tunnelling protocols, which tunnelling protocol? Requirements of tunnels.
L2TP
Overview, components, how it works, security, packet authentication, L2TP/IPsec, L2TP/PPP, L2 vs L3 tunnelling. Hands on: Implementing a L2TP tunnel.
IPsec
AH, HMAC, ESP, transport and tunnel modes, Security Association, encryption and authentication algorithms, manual vs automated key exchange, NAT and other issues. Hands on: Implementing an IPsec VPN.
SSL VPNs
Layer 4 VPNs, advantages, disadvantages. SSL. TLS. TLS negotiation, TLS authentication. TLS and certificates. Hands on: Implementing a SSL VPN.
MPLS VPNs
Introduction to MPLS, why use MPLS, Headers, architecture, label switching, LDP, MPLS VPNs, L2 versus L3 VPNs. Point to point versus multipoint MPLS VPNs. MBGP and VRFs and their use in MPLS VPNs. Hands on: Implementing a MPLS L3 VPN.
Penetration testing
Hacking webservers, web applications, Wireless networks and mobile platforms. Concepts, threats, methodology. Hands on: Hacking tools and countermeasures.