Network Security (4 days)

How to plan and implement secure networks, detect attacks and test security policies

Relevant Platforms:

- **Linux**
- **Unix**
- **FreeBSD**
- **Solaris**
- **Cisco IOS**
- **Windows NT**
- **Windows 2000**
- **Windows XP**
- **Windows .NET**

The course is generic to all networked operating systems, but reference will be made to the above platforms.

You will learn how to

- Determine the risk to your network
- Develop and implement a security policy
- Audit your network's security
- Use modern network security techniques, such as X.509, IPSec, SSL, TLS etc
- Use ethical hacking to identify security weaknesses.
- Harden your network services and applications
- Keep up to date with security issues

Course Benefits

The growth of the Internet and the wide-spread use of computer networks have brought great benefits to businesses. At the same time they have opened up business systems to remote hacking from employees through to anonymous crackers at the other side of the world.

The related growth in network applications has increased the complexity and consequently the vulnerability of networked systems.

Whilst techniques to secure network systems exist they are many and complex. This course gives the attendee a good understanding of network security risks and the appropriate techniques that can be used to reduce and control those risks.

Who Should Attend

This course is ideal technical staff and managers involved in network management. It is helpful if attendees have a basic understanding of networking principles but background information is supplied throughout the course.

Course Contents

Networking Recap

- Review of networking basics
- OSI 7 Layer Model
- TCP/IP – Internet Model
- Network terminology
- Common network protocols

What is Security?

- Confidentiality
- Integrity
- Authentication
- Non-repudiation
- Availability
- Access-Control
- Business Issues

Risks and Vulnerabilities

- Information disclosure
- Information leakage
- Integrity violation
- Masquerading
- Denial of service
- Illegitimate use
- Trojan Horses
- Back Doors
- Password Cracking
- Buffer Overflows
- Scanning and Sniffing
- Spoofing
- TCP/IP protocol attacks
- Session Hijacking
- Denial of Service
- Others…
- Social weaknesses
- Physical weaknesses

Security Policies

- Risk analysis
- Security Policies
- Who are you protecting?
- What are you protecting?
- Cost-benefit
- Recovery
- Ownership
- Standards

Cryptography

- Symmetric key cryptography
- Public key cryptography
- Hash functions and MAC

Digital Certificates and X.509

- Digital certificates
- X.509 certificates
- Certificate authorities
- PGP certificates

Physical Network Security

- Cabling
- IEEE802 networks
- Wireless
- Tempest

Datalink Security

- ARP Poisoning
- MAC addresses
- VLANs
- IEEE802.10 SILS

IP & Routing Security

- IP Fragmentation
- Spoofing & SYN Flooding
- ICMP redirects
- Source routing
- Dynamic routing

Firewalls and NAT

- Operation of TCP and UDP
- Ports and Sockets
- Firewall rules
- Typical firewall settings
- Stateful firewalls
- Proxy Servers
- Application layer firewalls
- NAT

IPSec & VPNs

- Cryptographic techniques
- AH & ESP Headers
- Transport and tunnel modes
- Security associations
- ISAKMP & IKE
- Oakley
- VPN Solutions

TLS and SSL

- Secure Sockets Layer
- Transport Layer Security

Name Service Security

- The Domain Name System - DNS
- TSIG & DNSSEC
- WINS
- LDAP

Securing Network Operating Systems

- UNIX
- Linux
- Windows
- Others

Network Application Security

- Basic services
- Berkley "r" commands
- E-mail (SMTP)
- POP/IMAP servers
- Web-Servers
- Other issues…

Keeping up to date

- CERT

Network Management Security

- SNMP & Security

Ethical Hacking

- Auditing and testing
- Password crackers
- Scanners – nessus, nmap…
- Sniffers – ethereal, supersniff…
- War dialers – beep, ptools…
- Wireless – Airsnort, Netstumbler…
- Miscellaneous – brutus, nmap…

Practicals

Each module has detailed hands-on exercises or demonstrations associated with it. Every delegate has at least one server provided for their own use.

The Trainers

All our trainers are practising network consultants with extensive experience with network security.

The Company

For further information about the training and our company see our web-site at www.erion.co.uk

Erion