

Internet and Intranet Security Fundamentals

Course No. WBISF • 3 Days

► COURSE OVERVIEW

One of the main concerns of companies connecting to the Internet is the protection of company data, either on Intranet systems within the company or whilst in transit over the Internet. Due to the public nature of the Internet, companies require the ability to protect their systems from unauthorized access, but at the same time allow full use by authorized personnel. When sending confidential information across the network, companies want to be sure that the data cannot be read by third parties, but also that the recipient can recover the information correctly. In many cases, these concerns apply equally to company intranets and extranets.

This comprehensive course addresses Internet and Intranets security concerns by giving delegates a clear insight into many issues involved and how best to address them.

► AUDIENCE

Project and technical managers with responsibility to investigate, plan and implement security policies with regard to corporate Internet access and intranets. Systems analysts and designers will also benefit. This course discusses security concepts and technologies rather than going into the technical detail of individual products.

► OBJECTIVES

Upon successful completion of this course, students will be able to:

- Understand and plan security policy
- Understand common vulnerabilities and security holes.
- Build defenses against common attacks on networks
- Use encryption and authentication to protect data
- Verify transactions using Public Key Certificates and Digital Signatures
- Secure web and e-mail traffic
- Detect security breaches
- Design a security architecture

- Appreciate the evolving nature of attacks and defenses

► PREREQUISITES

Students should be familiar with the concepts of networking, possibly obtained by attending our Network Primer course. A working knowledge of TCP/IP and standard Internet services (such as web, email and FTP) is essential. Previous knowledge and use of the Internet, possibly gained through attending QA's Internet Technology Fundamentals course is recommended. Familiarity with Windows NT is an advantage, UNIX experience would also be sufficient.

► COURSE OUTLINE

MODULE 1: INTRODUCTION TO NETWORK SECURITY

Topics:

- Security Issues
- Protecting your organization
- Protecting your data
- Measuring security
- Systems vulnerabilities (UNIX, NT, OS/2 and Windows)

MODULE 2: SECURITY IN THE REAL WORLD

Topics:

- Crackers and hackers
- Security scares and the media
- Security and vendors
- Security and you

MODULE 3: SYSTEM-BASED ATTACKS

Topics:

- System security risks
- Impersonation
- Backdoors
- Password stealing



105 West Broad Street
Falls Church, Virginia 22046
Ph: 703.532.1000
Fax: 703.532.1001
Web: www.Knowledge.com

Internet and Intranet Security Fundamentals

Course No. WBISF • 3 Days

Programmatic attacks-Trojan Horses
Viruses and worms

MODULE 4: NETWORK DATA ATTACKS

Topics:

Network security risks
Network snooping and eavesdropping
Network traffic analysis
Replay attacks
Denial of service attacks

MODULE 5: SECURITY THROUGH POLICY

Topics:

Implementing an organizational security policy
User policies
Principles of least privilege
Logging and auditing
Intrusion detection
Reading to attacks
Security audit tools

MODULE 6: PROTECTION THROUGH ENCRYPTION

Topics:

Protection information via encryption
Network encryption
Encryption algorithms
Symmetric key encryption systems
Public key encryption
Challenge-response systems
SSH service
Kerberos
Attacks on encryption systems-cryptanalysis and brute force attacks

MODULE 7: PROTECTION THROUGH AUTHENTICATION

Topics:

Authenticating clients and servers
Authenticating data
Public/private key authentication
Digital signatures
X.509 digital certificates
Trusted third parties
Certificate authorities
Public key infrastructures
Certification infrastructure and services

MODULE 8: TRANSACTIONAL SECURITY

Topics:

Network level security
Point-to-Point Tunneling Protocol (PPTP)
Secure Wide Area Networks (S/WAN)
Application specific security
Pretty Good Privacy (PGP)
Secure MIME (S/MIME)
Network application security
Secure Sockets Layer (SSL)
Private Communications Technology (PCT)
Financial security
Secure Electronic Transactions (SET)
Internet Protocol Security (IPSec)

MODULE 9: SERVER SECURITY

Topics:

Servers and security
Securing servers
Web server security
Mail server security
Internet service security
Servers users and security
Application development and security (CGI, ISAPI, NSAPI and database connectivity)



105 West Broad Street
Falls Church, Virginia 22046
Ph: 703.532.1000
Fax: 703.532.1001
Web: www.Knowledge.com

Internet and Intranet Security Fundamentals

Course No. WBISF • 3 Days

MODULE 10: PROTOCOL SECURITY

Topics:

- TCP/IP and security
- IP issues
- ICMP issues
- TCP issues
- IP attacks
- ICMP attacks
- TCP attacks
- DNS attacks
- UDP issues
- Proprietary protocols
- HTTP tunneling

- Knowledge based vs. behavior based intrusion detection
- Honeypots
- Identifying damage
- Repairing the damage
- Incident response

MODULE 14: EVOLVING RISKS

Topics:

- Evolution of risk
- Evolution of defenses
- Where to go next

MODULE 11: FIREWALLS

Topics:

- Building a secure architecture
- Internet firewalls
- Firewall philosophies
- Classic firewall implementations
- Firewall products and solutions

MODULE 12: PROXY SERVERS

Topics:

- Proxy Services
- Circuit level proxies
- Application proxies
- Web/FTP proxies
- Proxies and SSL

MODULE 13: INTRUSION DETECTION

Topics:

- Anatomy of an incident
- Detection methods
- Host and network based intrusion detection



105 West Broad Street
Falls Church, Virginia 22046
Ph: 703.532.1000
Fax: 703.532.1001
Web: www.Knowlogy.com