Web Security – Network Based – Beginner Course

The exploding use of Web technologies for corporate intranets and Internet sites has escalated security risks to corporate data and information systems. It is imperative that Web professionals are trained in techniques to effectively protect their sites from internal and external threats.
In this course, you gain extensive hands-on experience securing Web communications and Web sites. You learn the common vulnerabilities of Web sites, as well as how to carry out secure communications across unsecured networks.

The goal of this course is to learn how to:
- Secure Web servers, communications and browsers
- Protect your Web client to minimize risks from applets, scripts and viruses
- Exploit the features of your Web server and operating system to tighten security
- Use Secure Sockets Layer (SSL) to encrypt Web traffic Issue and manage certificates for browser and server authentication Deploy proxy servers as part of a firewall to protect your Web servers and users

---

Part I: Introduction to Web Security

- Web technologies
- The Web client/server architecture
- What does the Web server do?
- Transferring hypertext documents with HTTP
- Dynamic content technologies

- Basic security issues
- Availability
- Authentication
- Privacy
- Integrity

Part II: Securing the Web Client

- Threats and vulnerabilities
- Client information leakage
- How cookies work
- Assessing the threats from Java, JavaScript, VBScript and ActiveX
- Hostile applets and viruses
- Protecting your Web browser

- Disabling Java applets
- Turning off cookies
- Using an online virus checker
- Obtaining browser certificates
- Enabling and disabling signing authorities

Part III: Configuring Network Security

- Operating system security features
- Authenticating users
- File permissions and document roots
- Operating privileges for the server
- Audit tools

- Network security
- Preventing IP address spoofing
- Securing DNS servers
- Minimizing denial-of-service threats

Part IV: Enhancing Web Server Security

- Controlling access

- Configuring user authentication on IIS and Apache

- Restricting access based on hostname/IP address
- Enabling and configuring logging
- Dynamic configuration files
- Extended site functionality
- Securing CGI script invocations
- Guidelines for secure Web programming
- Securing Web communications with SSL
- Public key and private key encryption
- Storing and distributing keys
- Ensuring data integrity with message digests
- Digitally signing data and documents
- Enabling the Secure Sockets Layer (SSL)
- Obtaining and installing server certificates

Part V: Issuing and Managing Certificates

- Why certificates are used
- Preventing eavesdropping with public key encryption
- Authenticating clients and servers
- Utilizing the X.509 v3 Certificate format
- Certificate authorities (CAs)
- Using a public certificate authority
- Non-authoritative certificates
- Chaining certificate authorities
- Classes of certificates
- Trusting CAs in servers and browsers
- Importing CA certificates
- Running your own certificate server
- Choosing which CAs to trust
- Client certificate mapping
- Checking certificate revocation lists

Part VI: Protecting Servers and Clients With Firewalls

- Firewall technologies
- Components of a firewall
- What firewalls can and cannot do
- Comparing firewall types
- Using application proxies
- Selecting firewall topology
- Providing "defense in depth"
- Building a screened subnet
- Securing the Web server

Part VII: Security Management

- Responding to security violations
- Real-time monitoring
- Limiting damage
- Keeping up to date on new threats

Audience:
This course is valuable for those involved in securing Web sites, including Web developers, Webmasters, and systems, network and security administrators. Some experience with Web servers and technologies, plus familiarity with either UNIX or Windows system management is helpful.

Prerequisites:
Some knowledge of networking fundamentals is required.