

## Course 754

# Web Security Foundations

### (4 days)

#### **Who should attend...**

In this advanced hands-on course, students will learn to enhance security on Web Servers. Students will experience different types of vulnerabilities and the technologies necessary to minimize Web Server exposure. Topics such as Cryptography, Digital Certificates, Public Key Infrastructure (PKI), Service and Application Security, Spyware/Malware, Network Monitoring, and basic Firewall/Proxy Server configuration will be discussed and practiced. This will benefit Security Administrators, System Administrators, Network Administrators, Web Developers, and Managers who need to understand how security affects the Web Server platforms on corporate networks.

#### **Suggested Prerequisites...**

- Experience with Windows, Unix or Linux Operating System Management
- Experience with Internet Information Server or Apache
- Ability to read/write basic HTML

#### **Course Outline...**

##### **Chapter 1: Security Fundamentals**

Areas of Security: OS, Services, Local & Network Applications, Networking Protocols

**Workshop: How good is security out-of-the-box? Testing with Nessus & NMAP**

Cryptography Primer: Symmetric, ASymmetric, & Hashing Algorithms

Digital Certificates & Public Key Infrastructure

**Workshop: Digital Signing & Encryption Workshop**

##### **Chapter 2: Installing a Web Server**

Internet Information Server

Apache Web Server

**Workshop: Installing Internet Information Server or Apache**

Testing Web Server Security

Configure Access Logging

**Workshop: How good is security out-of-the-box? Testing with Nessus & NMAP**



### **Chapter 3: Operating System Security**

System Services: Mapping to Executables/Processes/Port Usage

*Workshop: Removing non-essential services*

Authentication between the Web Server and Operating System

Web Server to File System Security

*Workshop: Establishing Web Server to Operating System Security*

### **Chapter 4: Network Security**

Monitoring your network

Common Port Usage & Application identification

*Workshop: Network Monitoring with Ethereal*

Defending a Web Server with a Firewall

*Demonstration: Configuration of a Firewall to Defend a Web Server*

Defending a Web Server with a Proxy Server

*Workshop: Configure a Software Proxy Server for defense*

### **Chapter 5: Understanding Browser to Web Server Communication**

Monitoring Application Access

*Workshop: Viewing all files used by applications*

Web Browser (Internet Explorer, Netscape & Firefox) Security

Active Components presented through Web Browsers

*Workshop: Defining and Controlling Web Browser configuration*

Malware/Spyware

*Workshop: Detecting and Removing Malware/Spyware*

### **Chapter 6: Securing Web Servers with Cryptography**

Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

Certificate Authorities (CA) and Public Key Infrastructure (PKI)

Using SSL/TLS on a Web Server

*Workshop: Requesting a Digital Certificate from a CA and enable SSL/TLS*

Distributing Trust in an Enterprise

Installing a Certificate Authority

*Workshop: Install a Root Certificate Authority and issue certificates*

### **Chapter 7: Processing Data on a Web Server**

Understanding technologies for Server-Side processing

Examining risks of CGI, ASP, Server Side Includes, and other server-side scripting

*Workshop: Implement server side scripts*

Techniques for Secure Web Coding

Running Active Components on Web Servers

Connecting Databases to Web Servers

*Workshop: Establish a connection from a web server to a back-end database*



## **Chapter 8: Putting it all together**

Review of key concepts

### ***Workshop: Audit and Secure a Web Server***

*\*\*Attendees will be presented with a Windows Server running IIS or a Linux Server running Apache with multiple security issues. Students must successfully repair the problems and minimize security vulnerabilities.*

***Additional/Custom Topics are available - please contact your ROI representative to discuss course tailoring!!!***