Security Testing for the Enterprise and the Web (3 Days)

This is a practical computer-based interactive workshop designed to provide a foundation for security testing. You will learn the terminology, the unique issues, and the process for testing security in web and enterprise applications. As a result of attending this seminar, you should be able to understand security issues and have an increased comfort level in testing the security of web-based and enterprise applications.

Security Testing for the Enterprise and the Web will help you become more comfortable and confident in dealing with security testing issues. You will emerge from this three-day session knowing how to develop a security testing strategy and security test plan. You will learn the details of how attackers break into system and how to design tests to validate that security is adequate to prevent such attacks. You will also have an understanding of how hackers and crackers think.

The information that your company obtains and stores is perhaps its most valuable corporate asset. Learn how to protect it and make sure protection measures are working in this course.

Return on Investment

- Protect your most valuable corporate asset - your data
- Understand how the attackers think
- Become familiar with networking and application technology so that you can define effective security tests
- Understand which risks are associated with security issues and how they can affect your test planning and execution.
- Learn which tools can be used in security testing
- Advance your career by broadening your testing expertise.

Who Will Benefit

- QA Managers
- Test managers
- Test analysts
- Testers
- End users
- Web developers
- General managers who are responsible for making IT security decisions in their organizations
- IT auditors and internal auditors

The program requires basic IT and testing knowledge or experience

Course Topics

Module SECA - Introduction to Computer Security

Introduces the student to basic concepts of information security in a variety of environments, including web-based and internal corporate systems. Security will be examined in the light of risks, benefits and threats.

- What is Security Testing?
- Is Security Testing Possible?
- The Risks
- The Benefits
- The Threats
- Who is at Risk?

Module SECB - Understanding the Attackers

By understanding how computer crooks think, security professionals and testers can leverage that information to effective audit and test systems.

- Who are the Hackers and Crackers?
- How do the Hackers and Crackers Think?
- What tools do they Use?
- Where do they Meet?
- How do they Work?
- The Five Phases of a Security Attack

Module SECC - Understanding the Technology

Before we can make sense of testing techniques and cracker exploits, we must understand the underlying technologies that allow access to systems. This module is somewhat technical, but is aimed at people with little or no technical expertise in networking and systems administration.

- Networking Basics
- Firewalls
- Data Layers and Physical Layers
- Ethernet
- ARP Query and Response
- Hubs and Switches
- How Sniffers Intercept Packets
- Network Security Solutions
- Operating Systems: UNIX, Windows NT and 2000
- Where to Check for Security Updates

Module SECD - Security Protocols and Techniques

There are a variety of security protocols and techniques that are commonly in use. This module examines those techniques and how they work.

- Transaction Security Essentials
- Encryption Basics
    - How Public Key Encryption Works
    - Data Encryption System (DES) File Encryption
- VPNs
- Digital Certificates
- Certification Authorities
- Digital Signatures

- SSL
- Cookies

Module SECE - Internet Privacy and Information Privacy

There is considerable debate as to whether there is such a thing as privacy in the digital age. Even with an assumed level of lack of privacy, there are still significant privacy concerns that individuals and organizations need to be aware of. Lack of attention to privacy concerns can hurt a company's online business or can cause an individual personal losses.

- Is There Such a Thing as "Internet Privacy?"
- Privacy Threats
- Privacy Remedies
- Information Privacy Concerns - How Crooks Steal and Exploit Sensitive Corporate Information
- Corporate Espionage
- Protecting Private Information in Internal Systems
- Verifying and Validating the Protection of Sensitive Information

Module SECF - A Process for Security Testing

This module presents a process for planning, conducting and evaluating security testing.

- Determine Test Strategy and Tools
- Perform Security Assessment
- Develop Security Policy
- Identify Security Risks: Functional & Structural
- Script Functions To Be Security Tested
- Design Automated Security Tests
- Perform Test And Report Results

Module SECG - How to Develop a Security Testing Strategy

Like other forms of testing, the test strategy is an effective way to define the test objectives, the scope of testing, and the attributes that make testing a particular system or web site unique.

- How Testing Fits into an Enterprise Security Process
- Questions for Determining a Security Test Strategy
- Exercise - Case Study

Module SECH - How to Perform a Security Assessment

One of the basic activities in computer security in the security assessment. This is a verification of an organization's security efforts and helps to identify strengths and weaknesses. This module walks you through the process of performing a security assessment, analyzing the findings, and reporting the results.

- Defining the Scope of the Assessment
- Identifying the Risks
- Assessing and Prioritizing the Risks
- Reporting the Findings
- Mitigating the Risks

Module SECI - Writing a Security Test Plan

This module describes how to customize your own security test plan standard and how to use that standard in developing security test plans.

- Defining a Security Test Plan Standard
- Defining the Scope of Test Planning
- Defining Who Will Perform Testing
- Assemble Test Planning Information as Defined in the Standard
- Reviewing the Plan
- Approving the Plan
- A Sample Security Test Plan
- A Security Test Plan Checklist
- Exercise and Discussion - Reviewing the Sample Security Test Plan

Module SECJ - Testing External Network Attacks

It's difficult to test anything until you understand it. This module is an extensive coverage of some of the most popular and destructive network-based attacks, how they are performed, how they can be prevented and how you can test to assure that the prevention measures have been adequately applied. Topics include:

- Dial-up attacks
    - War-Dialing
    - Password Cracking Techniques
- Network attacks
    - Network Mapping
    - Network Scanning
    - Intrusion Detection System Evasion
    - Data Packet Fragmentation
- Web-based Application Attacks
    - Application Scanning Tools

Module SECK - Testing for Language-based Vulnerabilities

This module covers some of the most popular and destructive language-based attacks, how they are performed, how they can be prevented and how you can test to see if your applications are vulnerable to these kinds of attacks.

- Script Kiddies and Pros
- Application-based attacks
    - Stack-based Buffer Overflow Attacks
    - NOP Sleds
- Developer Defenses
- Tests Against Application Vulnerabilities

Module SECL - Testing for Backdoors and Trojan Horses

This module covers sneak attack techniques such as backdoors and Trojan horses, how they are placed into a system, how they can be prevented and how you can test to assure that the prevention measures have been adequately applied.

- Backdoors and Trojan Horses Defined
- How Backdoors and Trojan Horses are Placed on Systems
- Traditional Rootkits
- Kernel-level Rootkits

Module SECM - Testing Denial-of-Service Attacks

This module covers one of the most difficult attacks to prevent, the denial-of-service attack. You will learn how denial-of-service attacks are performed, how they can be prevented and how you can test to assure that the prevention measures have been adequately applied.

- Locally Stopping Services
- Defenses for Local Stopping of Service
- Tests for Local Stopping of Service
- Remotely Stopping Services
- Defenses for Remotely Stopping Services
- Tests for Remotely Stopping Services
- Remotely Exhausting Services
    - SYN Flood Attacks
    - Smurf Attacks
- Distributed Denial of Service Attacks (DDoS)
- DDoS Defenses
- DDos Tests

Module SECN - Testing Virus and Password Attacks

This module covers virus and password attacks, how they are performed, how they can be prevented and how you can test to assure that the prevention measures have been adequately applied.

- The Nature of Virus Attacks
- Virus Facts
- A Case in Point - The "I Love You" Virus
- The Virus Life Cycle
- Virus Types
- Virus Defenses
- Sources of Virus Information
- Tests for Virus Protection
- Password Attacks
- Password Cracking Tools
- Password Defenses
- Password Protection
- Virus Checklist

Module SECO - Testing Web Application Attacks

An attacker can cause a lot of damage by exploiting techniques used in many web applications to gain access to data and other assets. In this module, we will learn about these kinds of attacks and how to see if your applications are vulnerable.

- Account Harvesting
- Session Hijacking
- Cookie Cracks
- Session Tracking
- SQL Piggybacking
- URL Redirection

Module SECP - Performing Security Tests

Performing security testing can be a difficult and risky effort. This module discusses things to consider in establishing the test environment, communicating the performance of the test, how to view the test results and how to stay out of trouble in performing the test.

- Establishing the Test Environment
- Penetration Testing

- Encryption
- Authorization
- Language-based Tests (C++ vs. Java)
- Testing COTS-based Applications
- Regression Testing
- Reviewing Logs and Alerts
- Exercise - Performing Security Tests

Module SECQ - Reporting the Results of Security Testing

This module presents a standard for security test reporting and a sample security test report.

- Developing a Security Test Report Standard
- A Sample Security Test Report
- Exercise - Writing a Security Test Report

Module SECR - Security Testing Tools

There are a variety of tools that can be used to detect network vulnerabilities, excessive load levels and other cracker exploits.

- Scanners
- Packet Building
- Load and Stress Testing
- Sniffers
- Password Crackers
- Virus Scanners
- Information Querying
- Intrusion Detection
- Network Monitoring

Module SECS - How to Write a Security Response and Recovery Plan

You've done all you can to prevent an attack, but how will your organization respond to a new type of attack? This module presents a standard for a security response and recovery plan. A sample security response and recovery plan will be reviewed and it's applicability determined in light of a case study.

- Developing a Security Response and Recovery Plan Standard
- A Sample Security Response and Recovery Plan
- Exercise - Review the Sample Security Response and Recovery Plan
- Exercise - Case study

Module SECT - Protecting Intellectual Property in the Digital Age

In a digital world, it becomes easy to take someone else's proprietary content and use them as your own without regard for copyright laws. This applies to all sorts of content - software, intellectual property (IP) , music, just to name a few. This module discusses some of the issue surrounding this topic and some things that are being done to protect IP rights.

- The Problem
- The Issues
- Means of IP Protection
- The Threat
- The Outlook

Module SECU - Developing an Action Plan for Security

In this module, you will develop an action plan for yourself and your organization to address security testing.

- Identifying Your Greatest Needs
- Developing an Action Plan