COURSE DESCRIPTION

Beginning Assessment and Penetration Testing

Foundstone® Services Training Course

The Beginning Assessment and Penetration Testing training provides attendees with the skills to better attack and/or defend networks, hosts, and applications using the same techniques seen in the wild. In our hands-on classroom environment, you will learn step-by-step methods for target reconnaissance, host and service enumeration, vulnerability identification and exploitation, and how attackers use access to expand their influence and control. By learning how to leverage these security techniques and methodologies, you can actively defend your critical internal and external assets against malevolent threats.

Audience

This course is intended for the security engineer, security architect, system administrator, network administrator, domain administrator, penetration tester, red team, blue team, and SOC analyst.

Course Goals

- Targeted information reconnaissance
- Host/network discover
- Manual vulnerability identification
- Windows and Linux host exploitation
- Password cracking
- Expanding influence on a compromised network
- Common web application threats

Agenda at a Glance

- Footprinting
- Scanning
- Enumeration
- System Hacking (Windows)
- System Hacking (UNIX)
- Web Hacking

Course Outline

Module 1—Footprinting

- Overview
- Determine the Scope
- Get Proper Authorization
- Open Source Intelligence Gathering
- WHOIS and DNS Enumeration
- DNS Interrogation
- Network Reconnaissance

Module 2—Scanning

- Host Discovery
- Service Discovery
- Operating System—Detection

Module 3—Enumeration

- Banner Grabbing
- Vulnerability Scanning
- Introduction to Exploitation

Module 4—System Hacking (Windows)

- Network Enumeration
- Host Enumeration
- Enumeration Countermeasures
- Penetration
- Expanding Influence
- Penetration Countermeasures
- Privilege Escalation Attacks
- Privilege Escalation
- Countermeasures
- Pillaging
- Pillaging Countermeasures
- Expanding Influence
- Countermeasures
- Cleanup (Covering Tracks)

Module 5—System Hacking (UNIX)

- Overview of UNIX/Linux
- Enumeration
- Enumeration Countermeasures
- Penetration Countermeasures
- Privilege Escalation Attacks
- Privilege Escalation
- Countermeasures
- Pillaging
- Pillaging Countermeasures
- Expanding Influence
- Countermeasures
- Cleanup (Covering Tracks)

Recommended Pre-Work

Basic understanding of Linux and Microsoft Windows operating systems and TCP/IP networking is required for the course to be fully beneficial.

Module 6—Web Hacking

- Overview of eCommerce
- Architectures
- Discovery
- Configuration Management
- Authentication
- Authorization
- Session Handling
- Data Validation

Learn More

To order, or for further information, please call 1 888 847 8766 or email **SecurityEducation@mcafee.com**.

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com