Course Description

Ultimate Hacking: Expert

Foundstone® Services Training Course

This advanced course offers seasoned security veterans an opportunity to test and develop their skills like never before. During this class, students are provided with the latest knowledge and weapons to defend against sophisticated attacks while showcasing how to safeguard their organization's critical information assets. Taught by a select group of our industry-leading consultants, this course is simply the most advanced course oriented toward penetration testing that's currently available.

Course Goals

- Identify and respond to attacks.
- Create custom vulnerability detection.
- Conduct advanced penetration testing.
- Manual web application assessment techniques.
- Understand and craft exploits.

Agenda At A Glance

- Network Monitoring
- Illicit Monitoring
- Network Reconnaissance
- Pen Testing with Metasploit Exploitation
- Advanced Web Hacking
- Database Hacking
- Windows Rootkits and Memory Analysis
- Code-Based Vulnerabilities

Audience

- System and network administrators, corporate security personnel, auditors, law enforcement officers, and consultants responsible for investigating malware outbreaks or network investigations.

intel Security

Recommended Pre-Work

Advanced understanding of UNIX, Windows OS, computer forensics, and TCP/IP networking is required. Students should also have previously taken one or more of our Ultimate Hacking courses.

Course Outline

Module 1—Network Monitoring

- The Case for Monitoring and Detection
- Advanced Usage of Network Monitoring Tools
- Analyzing Full-Content and Session Data
- Implementing an Intrusion Detection System (IDS)
- Advanced Features and Analysis of Snort

Module 2—Illicit Monitoring

- Understanding ARP
- Sniffing in a Switched Environment
- Man-In-The-Middle Methods
- Common Tools and Techniques
- Intercepting and Modifying Popular Protocols
- Creating Custom Man-In-The-Middle Attacks
- Countermeasures

Module 3—Network Reconnaissance

- Exploration and Understanding the Most Popular Tools
- Scanning Methodology
- Advanced OS and Service Identification
- Advanced Port-Scanning Techniques
- Creating Custom Reconnaissance Scripts
- Scanning Efficiently
- Countermeasures

Module 4—Pen Testing with Metasploit Exploitation

- Avoiding Detection
- Tracking Progress
- Enumeration
- Brute Force Attacks
- Payloads and Post-Exploitation
- Advanced Features of Metasploit
- Extending Metasploit
- Countermeasures

Module 5—Advanced Web Hacking

- SQL Injection Overview
- Advanced Topics in SQL Injection
- Cross-Site Scripting (XSS) Overview
- Advanced Topics in XSS
- XSS Frameworks
- Cross-Site Request Forgery (CSRF)
- Countermeasures

Course Description

Module 6—Database Hacking

- Database Discovery and Service Enumeration
- Common Misconfigurations
- Database Content Enumeration
- Analysis of MSSQL-Stored (and Extended-Stored) Procedures
- OS Interaction Through the Database (Shovel the Shell)
- Countermeasures

Module 7—Windows Rootkits and Memory Analysis

- Overview of Rootkits
- Using Windows Rootkits
- Windows Memory Analysis
- Detecting and Removing Windows Rootkits
- Countermeasures

Module 8—Code-based Vulnerabilities

- Foundational Study of Computer Architecture, Memory, and Data Structures
- Static Code Analysis
- Using Debuggers to Discover Potential Vulnerabilities
- Creating Buffer Overflow Exploits
- Understanding Other Types of Code-Based Vulnerabilities
- Countermeasures

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

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com