# Advanced Hacker Methodologies for Security Professionals

## Course Summary

### Description

Elite Penetration Testing Tactics, Techniques, and Skills.

The Advanced Hacker Methodologies for Security Professionals course demonstrates how to defend large scale network infrastructure by learning how attackers leverage weaknesses in networks and systems to gain unauthorized access, cause damage, and steal information. From performing in-depth Open Source INTelligence (OSINT) to using advanced features of exploitation frameworks, students will experience first-hand the excitement of deciphering some of the most closely held secrets of expert penetration testers.

The Student Practical Exercise on day five is a team based Capture The Flag (CTF) event. Students will work in teams to perform a thorough penetration test of a simulated corporation. Specific informational objectives are defined for each step of the process. These objectives are in the form of "flags". Teams will gather all flags with as few hints as possible within the time allotted. Multiple hints will be given for each flag to the point of walking the student through the process required for success. The scoreboard will be displayed throughout to help motivate students to attempt to obtain flags with the least number of hints.

### Objectives

After taking this course, students will be able to understand:

- Advanced Network Reconnaissance Techniques
- How to Interrogate Hosts, Operating Systems and Services
- Web Based Attacks Vectors
- Exploitation Frameworks
- Database Server Compromise Tactics

### Topics

- The Need for Penetration Testing
- Current Threat Environment
- Network Monitoring
- Advanced Usage of Network Monitoring Tools
- Analyzing Full-Content and Statistical Data
- Network Monitoring Exercise
- Intrusion Detection
- Implementing an Intrusion Detection System (IDS)
- Snort Review and Demonstration
- Advanced Features and Analysis of Snort Output
- Output Plugins
- Intrusion Detection Exercise
- Illicit Monitoring
- Intercepting and Monitoring Popular Protocols
- Sniffing in a Switched Environment
- Man-in-the-Middle Methods
- Responder Utility Demonstration
- Illicit Monitoring Exercise
- Network Reconnaissance
- OSINT Introduction
- Traditional Techniques
- Browser Techniques
- Automated Tools
- OSINT demonstration
- OSINT Exercise - Hack Yourself
- Host and Port Scanning Methodology
- Advanced OS and Service Identification

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

# Advanced Hacker Methodologies for Security Professionals

## **Course Summary** (cont’d)

- Scanning Exercise
- Network Reconnaissance (continued)
- Vulnerability Scanning
- Nmap Scripting Engine
- OpenVAS
- Nessus
- Nikto
- Vulnerability Scanning Exercise
- Penetration Testing with Metasploit
- Introduction / Overview
- Auxiliary Modules
- Brute Force Attacks
- Auxiliary Module Exercise
- Client Side Attacks
- Exploitation Modules
- Payloads
- Post Exploitation Scripts
- Meterpreter
- Screen Capture
- Sniffing
- Privilege Escalation
- Avoiding Detection
- Expanding Influence
- Pivoting
- Collaborative Penetration Testing
- Advanced Web Hacking
- SQL Injection
- Advanced Topics in SQL Injection
- Blind SQL Injection
- Cross-Site Scripting (XSS)
- Advanced XSS
- XSS Frameworks
- Cross-Site Request Forgery (CRSF)
- Database Hacking
- Database Discovery and Service Enumeration
- Common Misconfigurations
- Database Content Enumeration
- MySQL exercise
- Analysis of MSSQL Stored / Extended Stored Procedures
- OS Interaction Through the Database
- MSSQL XP CMDSHELL exercise
- Windows Rootkits and Memory Analysis
- Creating and Using Rootkits
- Windows Memory Analysis
- Code-Based Vulnerabilities
- Foundational Study of Computer Architecture, Memory, and Data Structures
- Types of Code-Based Vulnerabilities

### Audience

This course is designed for:

- Incident Responders who need to understand and react to IDS alerts
- Network Defenders seeking to understand Common Access Methods
- Security Managers who desire to improve their Defensive Model
- Security Operations Center Staff seeking to identify signs of compromise
- New members of Penetration Testing and Vulnerability Assessment Teams

### Prerequisites

Students should attend the first course, Hacker Methodologies for Security Professionals, prior to taking this advanced course. Attending students are encouraged to have a good understanding of both the Windows and Unix operating system environments as well as a basic knowledge of TCP/IP networking.

### Duration

Five days

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically