



Advanced Penetration Testing:: Tactics and Operations

Grayscale Research 2008

Course Index::

Day 1, Developing a Plan	3
Part 1: Creating an Attack Plan.....	3
» Optimal Step by Step Attack Plan	3
» Open Source Security Testing Methodology	3
Part 2: Focus on Documentation.....	3
» Test data collection	3
» Report Formatting.....	3
Day 1: Summary:.....	3
Day 2, Social Engineering and Network Enumeration	4
Part 1: Human Psychology Overview	4
Part 2: Impersonation	4
Part 3: Network Reconnaissance.....	4
Day 2: Summary:.....	4
Day - 3, Resource Attack Methodologies.....	5
Part 1: Understanding and Attempting Session Hijacking.....	5
Part 2: Performing Web Server Attacks.....	5
Part 3: Database Attack.....	5
Day 3: Summary:	5
Day 4 - Understanding and Using Network Attack Methodologies.....	6
Part 1: Attacking the Network	6
Part 2 :Attacking Running Services	6
Part 3: Scanning and Penetrating Wireless Networks.....	6
Part 4: Password Cracking	6
Day 4: Summary:	6
Final Course Activity:.....	7
Storm the Castle: Custom Network Assessment	7

Day 1, Developing a Plan

Part 1: Creating an Attack Plan

» Optimal Step by Step Attack Plan

- Reconnaissance
- Enumeration
- Gaining Access
- Maintaining Access
- Covering Tracks

» Open Source Security Testing Methodology

- Information security
- Process security
- Internet technology security
- Communications security
- Wireless security
- Physical security

Part 2: Focus on Documentation

» Test data collection

» Report Formatting

- Executive Summary
- Project Scope
- Results Analysis
- Summary
- Appendixes

Day 1: Summary:

Penetration testing is not about jumping into a security assessment project by running several tools at random. Penetration testing is about creating a methodical, step-by-step plan that details exactly what you are going to do, when you are going to do it, and how.

Day 1 outlines the steps needed to create a methodical plan, from narrowing the scope of the project, to using the Open-Source Security Testing Methodology Manual (OSSTMM), and finally to writing up the testing report.

Day 2, Social Engineering and Network Enumeration

Part 1: Human Psychology Overview

- » Patience
- » Confidence
- » Trust
- » Inside knowledge

Part 2: Impersonation

- » Tech Support Impersonation
- » Third-Party Impersonation
- » Mail Impersonation
- » End User Impersonation
- » Customer Impersonation
- » Induced Reactions

Part 3: Network Reconnaissance

- » Passive Host Reconnaissance vs. Active Host Reconnaissance
- » Network Scanning

Day 2: Summary:

At the end of the day, it will be evident that no matter how much encryption and security technology you have implemented, a network is never completely secure. You can never get rid of the weakest link the human factor. It does not matter how many firewalls, virtual private networks (VPNs), or encryption devices you have if your employees are willing to give out access to the systems to anyone who asks for it. The easiest way to gain access to a corporation network is to come right out and ask for it.

In order to evaluate this layer of security the student will be learning the common methods of social engineering found in the marketplace. Additionally the student will begin to evaluate and map network devices for reconnaissance.

Day - 3, Resource Attack Methodologies

Part 1: Understanding and Attempting Session Hijacking

- » Defining Session Hijacking
- » Tools

Part 2: Performing Web Server Attacks

- » Understanding Web Language
- » XSS / Cookie Theft
- » E-Commerce Architecture
- » Web Page Spoofing
- » Cookie Guessing
- » Brute Force Attacks

Part 3: Database Attack

- » Database Vulnerabilities
- » Exploiting Databases Remotely
- » SQL Injection Tips and Tricks

Day 3: Summary:

As the student explores network technology, some more advanced penetration testing methodologies will be demonstrated. In the first portion of this curriculum the student will be exposed to Session Hijacking.

Session hijacking is the attempt to overtake an already active session between two hosts. With session hijacking, you take over an already-authenticated host as it communicates with the target yielding access where otherwise there would be none.

Web attacks and SQL injections will also be covered in depth, as well as how to extract data from custom SQL injection points within a hands on example.

Day 4 – Understanding and Using Network Attack Methodologies

Part 1: Attacking the Network

- » Bypassing Firewalls
- » Evading Intruder Detection Systems
- » Router Vulnerabilities
- » Switch Vulnerabilities

Part 2 :Attacking Running Services

- » Service Flaw Enumeration using available tools
- » Exploitation Technology
 - Available Resources
 - Commercial Solutions

Part 3: Scanning and Penetrating Wireless Networks

- » Planning War Driving
- » Tools and Execution

Part 4: Password Cracking

- » Password-Cracking Tools

Day 4: Summary:

By the end of day 5 the student will know how to conduct most of the fundamental tasks of a penetration test. An extra focus is paid to organizing result data for report generation.

The student will audit a local wireless network as well, exploring different methods of attack that can be use to compromise wireless networks.

Final Course Activity:

Storm the Castle: Custom Network Assessment

Activity Scenario:

- Students will be work as a penetration testing team and will attempt to compromise a custom network running multiple services. Students will work hand and hand in a live attack simulation and will by the end of the day, compromise the network.

Goal:

Full network compromise.