

# Penetration Testing With BackTrack



## PWB Online Syllabus ver. 3.0

## Table of Content

### Before we Begin

- i. Legal Stuff
- ii. Important Notes
- iii. Lab IP Address Spaces
- iv. How to approach this course
- v. Reporting
  - i. Reporting for PWB
  - ii. Interim Documentation
- vi. Penetration Testing Methodology

### 1. Module 1 - BackTrack Basics

- 1.1 Finding your way around BackTrack
  - 1.1.1 Exercise
- 1.2 BackTrack Services
  - 1.2.1 DHCP
  - 1.2.2 Static IP assignment
  - 1.2.3 SSHD
  - 1.2.4 Apache
  - 1.2.5 FTP
  - 1.2.6 TFTP
  - 1.2.7 VNC Server
  - 1.2.8 Additional Resources
  - 1.2.9 Exercise
- 1.3 The Bash Environment
  - 1.3.1 Simple Bash Scripting
  - 1.3.2 Sample Exercise
  - 1.3.3 Sample Solution
  - 1.3.4 Additional Resources
  - 1.3.5 Exercise
- 1.4 Netcat the Almighty
  - 1.4.1 Connecting to a TCP/UDP port with Netcat
  - 1.4.2 Listening on a TCP/UDP port with Netcat
  - 1.4.3 Transferring files with Netcat
  - 1.4.4 Remote Administration with Netcat
  - 1.4.5 Exercise
- 1.5 Using Wireshark
  - 1.5.1 Peeking at a Sniffer
  - 1.5.2 Capture and Display filters
  - 1.5.3 Following TCP Streams
  - 1.5.4 Additional Resources

## 1.5.5 Exercise

## 2. Module 2- Information Gathering Techniques

### 2.1 Open Web Information Gathering

#### 2.1.1 Google Hacking

### 2.2. Miscellaneous Web Resources

#### 2.2.1 Other search engines

#### 2.2.2 Netcraft

#### 2.2.3 Whois Reconnaissance

### 2.3 Exercise

## 3. Module 3- Open Services Information Gathering

### 3.1 DNS Reconnaissance

#### 3.1.1 Interacting with a DNS server

#### 3.1.2 Automating lookups

#### 3.1.3 Forward lookup bruteforce

#### 3.1.4 Reverse lookup bruteforce

#### 3.1.5 DNS Zone Transfers

#### 3.1.6 Exercise

### 3.2 SNMP reconnaissance

#### 3.2.1 Enumerating Windows Users

#### 3.2.2 Enumerating Running Services

#### 3.2.3 Enumerating open TCP ports

#### 3.2.4 Enumerating installed software

#### 3.2.5 Exercise

### 3.3 SMTP reconnaissance

### 3.4 Microsoft Netbios Information Gathering

#### 3.4.1 Null sessions

#### 3.4.2 Scanning for the Netbios Service

#### 3.4.3 Enumerating Usernames/ Password policies

#### 3.4.4 Exercise

### 3.5 Maltego

#### 3.5.1 Network Infrastructure

#### 3.5.2 Social Infrastructure

## 4. Module 4- Port Scanning

### 4.1 TCP Port Scanning Basics

### 4.2 UDP Port Scanning Basics

### 4.3 Port Scanning Pitfalls

### 4.4 Nmap

#### 4.4.1 Network Sweeping

#### 4.4.2 OS fingerprinting

#### 4.4.3 Banner Grabbing / Service Enumeration

### 4.4.4 Nmap Scripting Engine

- 4.5 PBNJ
- 4.6 Unicornscan
- 4.7 Exercise

## 5. Module 5- ARP Spoofing

- 5.1 The Theory
- 5.2 Doing it the hard way
- 5.3 Ettercap

## 6. Module 6- Buffer Overflow Exploitation

- 6.1 Looking for Bugs
- 6.2 Fuzzing
- 6.3 Exploiting Windows Buffer Overflows
  - 6.3.1 Replicating the Crash
  - 6.3.2 Controlling EIP
  - 6.3.3 Locating Space for our Shellcode
  - 6.3.4 Redirecting the execution flow
  - 6.3.5 Finding a return address
  - 6.3.6 Basic shellcode creation
  - 6.3.7 Getting our shell
  - 6.3.8 Exercise

- 6.4 Exploiting Linux Buffer Overflows
  - 6.4.1 Setting things up
  - 6.4.2 Controlling EIP
  - 6.4.3 Landing the Shell
  - 6.4.4 Avoiding ASLR

## 7. Module 7- Working With Exploits

- 7.1 Looking for an exploit on BackTrack
- 7.2 Looking for exploits on the web

## 8. Module 8- Transferring Files

- 8.1 The non interactive shell
- 8.2 Uploading Files
  - 8.2.1 Using TFTP
  - 8.2.2 Using FTP
  - 8.2.3 Inline Transfers
- 8.3 Exercise

## 9. Module 9 – Exploit frameworks

- 9.1 Metasploit
- 9.2 Interesting Payloads
  - 9.2.1 Meterpreter Payload
  - 9.2.3 Binary Payloads
  - 9.2.4 Other Framework v3.x features

## 9.3 Core Impact

## 10. Module 10- Client Side Attacks

- 10.1 Client side attacks
- 10.2 CVE-2009-0927
- 10.3 MS07-017 – From PoC to Shell
- 10.4 MS06-001
- 10.5 Client side exploits in action
- 10.6 Exercise

## 11. Module 11- Port Fun

- 11.1 Port Redirection
- 11.2 SSL Encapsulation - Stunnel
- 11.3 HTTP CONNECT Tunneling
- 11.4 ProxyTunnel
- 11.5 SSH Tunneling
- 11.6 What about content inspection?

## 12. Module 12- Password Attacks

- 12.1 Online Password Attacks
- 12.2 Hydra
  - 12.2.1 FTP Bruteforce
  - 12.2.2 POP3 Bruteforce
  - 12.2.3 SNMP Bruteforce
  - 12.2.4 Microsoft VPN Bruteforce
  - 12.2.5 Hydra GTK
- 12.3 Password profiling
  - 12.3.1 CeWL
- 12.4 Offline Password Attacks
  - 12.4.1 Windows SAM
  - 12.4.2 Windows Hash Dumping – PWDump / FGDump
  - 12.4.3 John the Ripper
  - 12.4.4 Rainbow Tables
  - 12.4.5 “Windows does WHAT????”
  - 12.4.6 Exercise
- 12.5 Physical Access Attacks
  - 12.5.1. Resetting Microsoft Windows
  - 12.5.2 Resetting a password on a Domain Controller
  - 12.5.3 Resetting Linux Systems
  - 12.5.4 Resetting a Cisco Device

## 13. Module 13 - Web Application Attack vectors

- 13.1 Cross Site Scripting
  - 13.1.1 Browser redirection / iframe injection
  - 13.1.2 Stealing Cookies / Abusing Sessions
- 13.2 Local and Remote File Inclusion
- 13.3 SQL Injection in PHP / MySQL

- 13.3.1 Authentication Bypass
- 13.3.2 Enumerating the Database
- 13.3.3 Code Execution

#### 13.4 SQL Injection in ASP / MSSQL

- 13.4.1 Identifying SQL Injection Vulnerabilities
- 13.4.2 Enumerating Table Names
- 13.4.3 Enumerating the column types
- 13.4.4 Fiddling with the Database
- 13.4.5 Microsoft SQL Stored Procedures
- 13.4.6 Code execution

- 13.5 Web Proxies

- 13.6 Exercise

#### 14. Module 14 - Trojan Horses

- 14.1 Binary Trojan Horses
- 14.2 Open source Trojan horses
- 14.3 World domination Trojan horses

#### 15. Module 15 - Windows Oddities

- 15.1 Alternate NTFS data Streams
- 15.2 Registry Backdoors

#### 16. Module 16 - Rootkits

- 16.1 Aphex Rootkit
- 16.2 HXDEF Rootkit
- 16.3 Exercise R.I.P

Final Challenges