Offensive Security

Penetration Testing With BackTrack

PWB Online Syllabus

v.3.0

Table of Contents

Penetration Testing with BackTrack

1. Module 1 - BackTrack Basics

Overview

This module prepares the student for the modules to come, which heavily rely on proficiency with the basic usage of Linux and tools such as the Bash Shell, Netcat and Wireshark.

Module Objectives:

1. At the end of this module, the student should be able to comfortably use the BackTrack Linux Distribution, including Service management, tool location, IP address Management.
2. Basic proficiency of the Linux Bash Shell, Text manipulation and Bash Shell scripting.
3. A practical understanding of the various uses of Netcat.
4. Basic proficiency in the use of the Wireshark network sniffer.

2. Module 2 - Information Gathering Techniques

Overview

This module introduces the topic of general information gathering techniques .

Module Objectives:

1. At the end of this module, the student should be able to gather public information using various resources such as Google, Netcraft and Whois for a specific organization.
2. Students should be able to come up with new and useful “Google hacks” on their own.
3. Building a basic company / organizational profile using publicly available information.

3. Module 3 - Open Services Information Gathering

Overview

This module introduces the student to the topic of “Service Information Gathering”, and to an extent, “Vulnerability Identification”.

Module Objectives:

1. At the end of this module, the student should be able to use tools present in BackTrack to enumerate the basic external network infrastructure, as well as various services such as DNS, SNMP, SMTP and SMB.
2. Students should be able to write their own basic tools in Bash and Python.
3. Students should be able to automate and script various enumeration tools.
4. Basic proficiency in the use of Maltego.

4. Module 4 - Port Scanning

Overview

This module introduces the student to the topic of TCP and UDP port scanning.

Module Objectives:

1. At the end of this module, the student should be able run intelligent TCP and UDP port scans using tools available in BackTrack.
2. The student should be able to identify and avoid common port scanning pitfalls.
3. The student should be able to use Nmap wrappers to log scanned data to MySQL.
4. Basic use of the Nmap NSE scripting engine.

5. Module 5 - ARP Spoofing

Overview

This module introduces ARP Man in the Middle attacks in a switched network, and various passive and active derivatives of these attacks.

Module Objectives:

1. At the end of this module, the student should be able to understand and recreate ARP spoofing attacks by manually editing ARP packets with a HEX editor.
2. Proficiency in the use of Ettercap, and various modules such as DNS and SSL Spoofing.
3. Basic proficiency in writing custom Ettercap filters.

6. Module 6 - Buffer Overflow Exploitation

Overview

This module introduces the students to the world of software exploitation in both Windows and Linux environments.

Module Objectives:

1. At the end of this module, the student should be able to comfortably use the BackTrack Linux Distribution to find, analyse and Exploit simple Buffer Overflow vulnerabilities.
2. Practical use of Windows and Linux debuggers (Immunity Debugger, GDB, EDB) for purposes of exploitation.
3. Understand the mechanisms behind shellcode operation.

7. Module 7 - Working With Exploits

Overview

This module deals with debugging and fixing public exploits to suit our needs. Cross compilation of exploits is also introduced.

Module Objectives:

1. At the end of this module, the student should be able to locate and fix exploits for both Windows and Linux compilation environments.
2. The student should be able to use the MinGW cross compiler on BackTrack to generate PE executables.
3. The student should be able to intelligently replace shellcode in an existing exploit.

8. Module 8 - Transferring Files

Overview

This module introduces several file transfer methods between attacking and victim machines.

Module Objectives:

1. At the end of this module, the student should be able use several file transfer methods, such as FTP, TFTP, DEBUG, and VBS scripting in order to initiate file transfers to a victim machine.
2. The student should understand the dangers of a non interactive shell.
3. The student should understand the practical limitations of each transfer method, as well as pros and cons for each.

9. Module 9 - Exploit Frameworks

Overview

This module introduces the Metasploit and Core Impact Exploit Frameworks, as well as their various functionalities and uses.

Module Objectives:

1. At the end of this module, the student should be able to port simple exploits to MSF format for use in a real environment.
2. The student should be able to use and execute exploits, auxiliary modules client side attacks, etc, using the MSF, as well as create binary payloads and handle them appropriately.
3. Proficiency with the Meterpreter payload and its various rich features, such as file transfers, keylogging, process migration, etc.

10. Module 10 - Client Side Attacks

Overview

This module introduces the concepts and mechanisms behind client side attacks.

Module Objectives:

1. Understand the concepts behind client side attacks, and how they relate to the network infrastructure.
2. Recreate the MS07-017 vulnerability and end up with a working exploit on Windows XP.
3. Use existing client side exploits in order to compromise lab victim machines, as well as execute client side attacks via the Metasploit Framework.

4. Advanced cross compiling of Windows DLL's on BackTrack.

11. Module 11 - Port Fun

Overview

This module introduces several techniques for TCP traffic forwarding and tunneling. These techniques are then implemented in a complex attack scenario.

Module Objectives:

1. The student should understand the differences between "port redirection" and "port tunneling", and be able to implement both using various tools present in BackTrack.
2. The student should be able to encapsulate traffic using SSL and HTTP.
3. The student shold be able to use SSH tunneling techniques to access otherwise non routable machines and networks.

12. Module 12 - Password Attacks

Overview

This module introduces the concepts behind various forms of password attacks, such as online attacks, and offline hash cracking.

Module Objectives:

1. The student should understand programmatically the mechanisms behind online and offline password crackers by writing relevant python scripts.
2. The student should be able to create custom and organization specific profiles password lists.

3. Proficiency in the use of John the ripper to crack various hash formats.
4. A practical understanding of the use of Rainbowtables and GPU accelerated hash cracking techniques.

13. Module 13 - Web Application Attack vectors

Overview

This module introduces common web application attacks, such as XSS, Cookie stealing, LFI/RFI attacks, and SQL injection attacks across various platforms.

Module Objectives:

1. The student should programmatically understand the underlying concepts behind each vulnerability class.
2. The student should be able to identify and exploit each vulnerability class accordingly.
3. The student should be familiar with basic SQL queries, and database structure.
4. The student should be able to use advanced database functions such as MySQL advanced functions and MSSQL stored procedures.
5. Understand and use an attacking Web Proxy as part of a web application attack.

14. Module 14 - Trojan Horses

Overview

This module various classes of Windows based Trojan horses.

Module Objectives:

1. The student should understand the difference between Trojan horse fucntionalities.
2. Experience with various Trojans in the lab environment.

15. Module 15 - Windows Oddities

Overview

This module introduces various Windows oddities, and otherwise strange OS behaviour.

Module Objectives:

1. The student should understand ADS and experience the notorious Windows registrty bug.

16. Module 16 - Rootkits

Overview

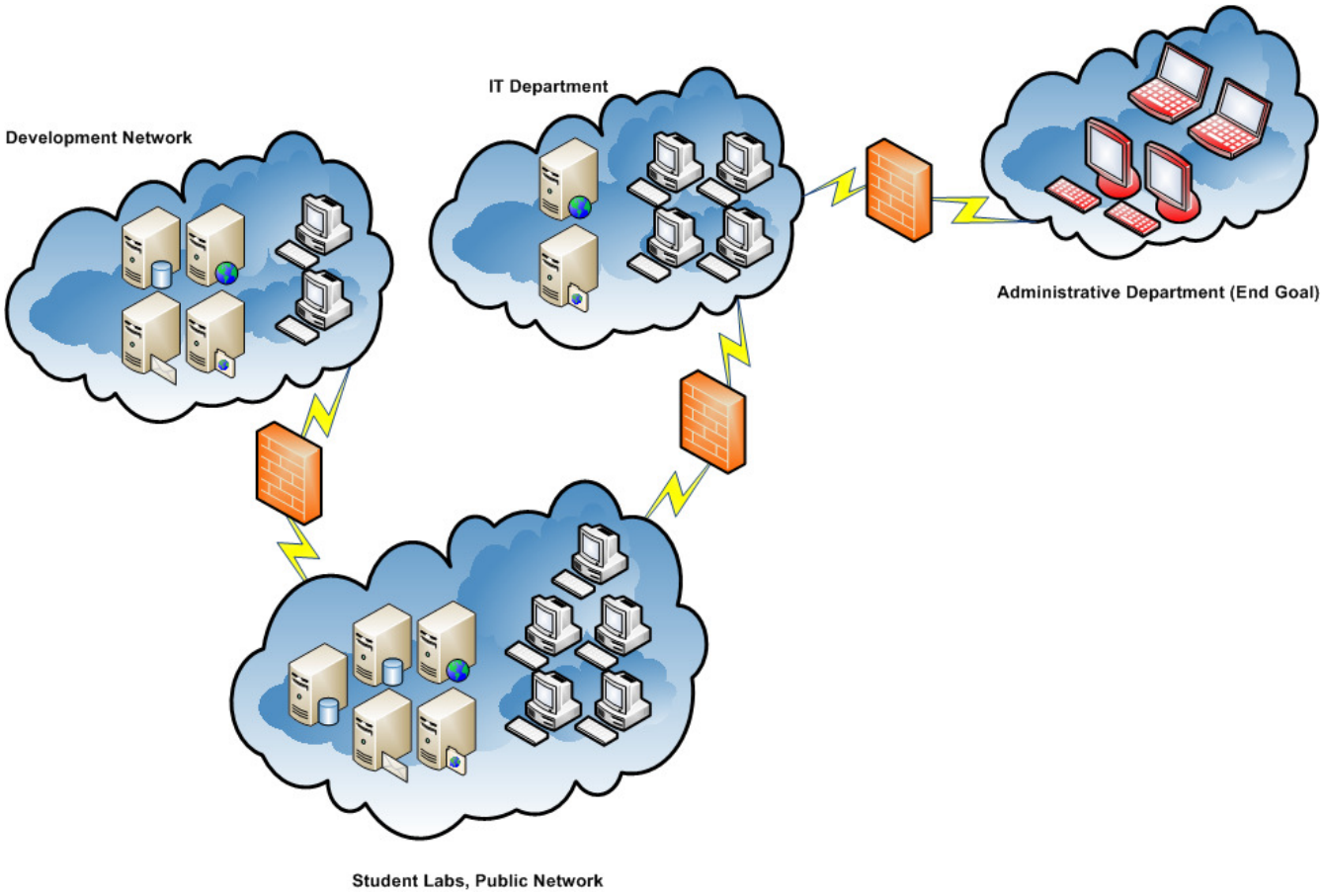
This module various classes of Windows based rootkits and their possible effects on a compromised machine.

Module Objectives:

1. The student should understand the underlying concepts of rootkits.
2. Experience with various rootkits in the lab environment.

Final Challenges:

THINC.LOCAL Network Layout



PAGE INTENTIONALLY LEFT BLANK