



# Offensive Security Course Outline

BackTrack Development Team

Mati Aharoni



## Offensive Security Online Course Description

### Overview

The need to understand the attacker and his methods is **vital** for better defending our networks. “Offensive Security” is designed for System Administrators and security professionals who want to get acquainted with the world of Offensive Security, but do not have the time to spend on a full blown course.

This course will introduce the basic (and not so basic) vectors of attack.

For an additional fee, you can choose to implement and understand these attacks in a safe, secluded Offensive-Security lab environment.

### Prerequisites

- The student must have a solid understanding of Network Administration and TCP/IP, and a reasonable level of familiarity with Linux, in order to complete the course.
- A modern PC, with the capability of displaying full screen video and sound.
- A fast Internet connection to view or download the Videos.
- A fast Internet connection to connect to the Offensive Security Labs over VPN.



## Course Description

“Offensive Security” is not your usual IT security course. The labs are challenging and the exercises are hard, often requiring a certain degree of personal research and self study. This is especially true for the extended version of “Offensive Security” which includes the practical labs and Certification Challenge.

It is vital that you meet the technical prerequisites as stated above, otherwise you might find yourself lost as the course progresses. In many cases, previous knowledge is assumed and theoretical explanations are shortened or referenced, in case the student needs a refresher. Please note, we do not have a refund policy – it is **your** responsibility to make sure you meet the mentioned technical requirements.

However, if you do meet the technical requirements, this course will very quickly expose you to the world of Offensive Security, and teach you the inner workings, tools and methodologies of modern day attackers.



## Course Objectives

### Primary Objectives:

- The student will gain insight into the offensive security field, which will expand awareness for the need of **real world** security solutions.
- The student will learn to implement various reconnaissance techniques.
- The student will learn to implement and identify various attack vectors.
- The student will learn to implement and identify various post exploitation techniques.

### Secondary Objectives:

- The student will be familiarized with BackTrack to a competent level.
- The student will be introduced to Bash Scripting.
- The student will be introduced to Python Scripting.

## Offensive Security Labs

Our labs are accessible over the Internet using a high speed connection. The lab simulates real world scenarios, with a variety of operating systems and network devices. Most of the exercises take place in the labs, and are therefore the ideal solution for students wishing to gain hands on experience.



## Certification

Students who take the extended “Offensive Security” course (including labs) can opt to take a Certification Challenge, in which the students will be presented with an unfamiliar network scenario which they will have to attack. The challenge will be scheduled for a specific date.

Upon successful completion of the challenge, the student will receive an **OSCP** (Offensive Security Certified Professional) certificate, which testifies their competency of attack methods and techniques using BackTrack.

## Course Aids

Our labs provide complete coverage for all the course exercises. However, there are some modules which you might want to exercise locally (topics such as Reverse Engineering and Exploitation techniques come to mind).

In such a case, you will need either an additional low end computer (P III 256 RAM) or virtual machine software, running Windows 2000 Server SP4 (unpatched). Obviously we can not provide you with these images, due to licensing restrictions.



## Registration Process

- The registration process involves sending a no commitment pre-registration mail, using our contact URL, at:  
<http://www.offensive-security.com/contact.html>
- This mail puts you in a waiting list in order of mail arrival.
- You will then be sent a registration form in which we will collect several personal details (Name, Surname, Address , Contact Information and Email). In addition, you will be asked to fill out a very short questionnaire.
- Once we receive the registration form it will be reviewed, and will be subject to our approval. If approved, you will receive a confirmation mail from us.
- Please note that we reserve the right to refuse “Offensive Security” training, at our discretion.
- If you have opted for the “Offensive Security” Lab access or Certification (available at additional cost), we will schedule a connectivity test with you, to verify accessibility to the labs, to your satisfaction.
- Once payment is approved, you will be sent an Email with login information to the Offensive Security Online course, and a link to download the lab videos.



## Offensive Security Course Topics

The following is a course outline describing the main topics discussed. For more details about the course content, please contact us using the [contact](#) link.

<b>1. Module 1 - BackTrack Basics</b>
1.1 Finding your way around the tools
1.1.1 Exercise 1
1.2 Basic Services
1.2.1 DHCP
1.2.2 Static IP assignment
1.2.3 Apache
1.2.4 SSHD
1.2.5 Tftpd
1.2.6 VNC Server
1.2.7 Exercise 2
1.3 Basic Bash Environment
Overview
1.3.1 Simple Bash Scripting
1.3.2 Exercise 3
1.3.3 Possible Solution for Exercise 3
1.3.4 Exercise 4
1.4 Netcat The Almighty
Overview
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



1.4.4.1 Scenario 1 – Bind Shell

1.4.4.2 Scenario 2 – Reverse Shell

1.4.5 Exercise 5

1.5 Using WireShark (Ethereal)

Overview

1.5.1 Peeking at a Sniffer

1.5.2 Capture filters

1.5.3 Following TCP Streams

1.5.4 Exercise 6

## 2. **Module 2- Information Gathering Techniques**

A note from the authors

2.1 Open Web Information Gathering

Overview

2.1.1 Google Hacking

2.1.1.1 Advanced Google Operators

2.1.1.2 Searching within a Domain

2.1.1.3 Nasty Example #1

2.1.1.4 Nasty Example #2

2.1.1.5 Email Harvesting

2.1.1.6 Finding Vulnerable Servers using Google

2.1.1.7 Google API

2.2. Miscellaneous Web Resources

2.2.1 Other search engines

2.2.2 Netcraft

2.2.3 Whois Reconnaissance

2.3 Exercise 7

## 3. **Module 3- Open Services Information Gathering**

A note from the authors

3.1 DNS Reconnaissance



3.1.1 Interacting with a DNS server
3.1.1.1 MX Queries
3.1.1.2 NS Queries
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 8
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 9
3.3 SMTP reconnaissance
3.3.1 Exercise 10
<b>4. Module 4- Port Scanning</b>
A note from the authors
4.1 TCP Port Scanning Basics
4.2 UDP Port Scanning Basics
4.3 Port Scanning Pitfalls
4.4 Nmap
4.5 Scanning across the network
4.5.1 Exercise 11
4.6 Unicornscan
<b>5. Module 5- ARP Spoofing</b>
A note from the authors
5.1 The Theory
5.2 Doing it the hard way



5.2.1 Victim Packet
5.2.2 Gateway Packet
5.3 Ettercap
5.3.1 DNS Spoofing
5.3.2 Fiddling with traffic
5.3.3 Exercise 12
<b>6. Module 6- Buffer overflow Exploitation (Win32)</b>
A note from the authors
Overview
6.1 Looking for the Bugs
6.2 Fuzzing
6.3 Replicating the Crash
6.4 Controlling EIP
6.4.1 Binary Tree analysis
6.4.2 Sending a unique string
6.5 Locating Space for our Shellcode
6.6 Redirecting the execution flow
6.7 Finding a return address
6.7.1 Using OllyDbg
6.8 Getting our shell
6.9 Improving exploit stability
6.9.1 Exercise 13
<b>7. Module 7- Working With Exploits</b>
7.1 Looking for an exploit on BackTrack
7.1.1 RPC DCOM Example
7.1.2 Wingate Example
7.1.3 Exercise 14
7.2 Looking for exploits on the web
7.2.1 Security Focus



7.2.2 Milw0rm.com

## 8. Module 8- Transferring Files

8.1 The non interactive shell

8.2 Uploading Files

8.2.1 Using TFTP

8.2.1.1 TFTP Pros

8.2.1.2 TFTP Cons

8.2.2 Using FTP

8.2.3 Inline Transfer - Using echo and DEBUG.exe

8.3 Exercise 15

## 9. Module 9 - Exploit frameworks

9.1 Metasploit

9.1.1 Metasploit Command Line Interface (MSFCLI)

9.1.2 Metasploit Console (MSFCONSOLE)

9.1.3 Metasploit Web Interface (MSFWEB)

9.1.4 Exercise 16

9.1.5 Interesting Payloads

9.1.5.1 Meterpreter Payload

9.1.5.2 PassiveX Payload

9.1.5.3 Binary Payloads

9.1.6 Exercise 17

9.1.7 Framework v3.0

9.1.7.1 Framework 3 Auxiliary Modules

9.1.8 Framework v3.0 Kung Foo

9.1.8.1 db\_autopwn

9.1.8.2 Kernel Payloads

9.1.9 Exercise 18

9.2 Core Impact

9.2.1 Exercise 19



## 10. **Module 10- Client Side Attacks**

A note from the authors

10.1 Client side attacks

10.2 MS04-028

10.3 MS06-001

10.4 Client side exploits in action

10.5 Exercise 20

## 11. **Module 11- Port Fun**

A note from the authors

11.1 Port Redirection

11.2 SSL Encapsulation - Stunnel

11.2.1 Exercise 21

11.3 HTTP CONNECT Tunneling

11.4 ProxyTunnel

11.4.1 Exercise 22

11.5 SSH Tunneling

11.6 What about content inspection ?

## 12. **Module 12- Password Attacks**

A note from the authors

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 WYD

12.3.2 Exercise 23



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 Exercise 24
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
<b>13. Module 13 - Web Application Attack vectors</b>
13.1 SQL Injection
13.1.1 Identifying SQL Injection Vulnerabilities
13.1.2 Enumerating Table Names
13.1.3 Enumerating the column types
13.1.4 Fiddling with the Database
13.1.5 Microsoft SQL Stored Procedures
13.1.6 Code execution
13.2 Web Proxies
13.3 Command injection Attacks
13.3.1 Exercise 25
<b>END OF VIDEO PRESENTATION</b>
<b>14. Module 14 - Trojan Horses</b>
14.1 Binary Trojan Horses
14.2 Open source Trojan horses
14.2.1 Spybot
14.2.2 Insider
14.3 World domination Trojan horses
14.3.1 Rxbot



## 15. **Module 15 - Windows Oddities**

### 15.1 Alternate NTFS data Streams

#### 15.1.1 Exercise 26

### 15.2 Registry Backdoors

#### 15.2.1 Exercise 27

## 16. **Module 16 - Rootkits**

### 16.1 Aphex Rootkit

### 16.2 HXDEF Rootkit

### 16.3 Exercise R.I.P