SOC Analyst Project

SOChecker

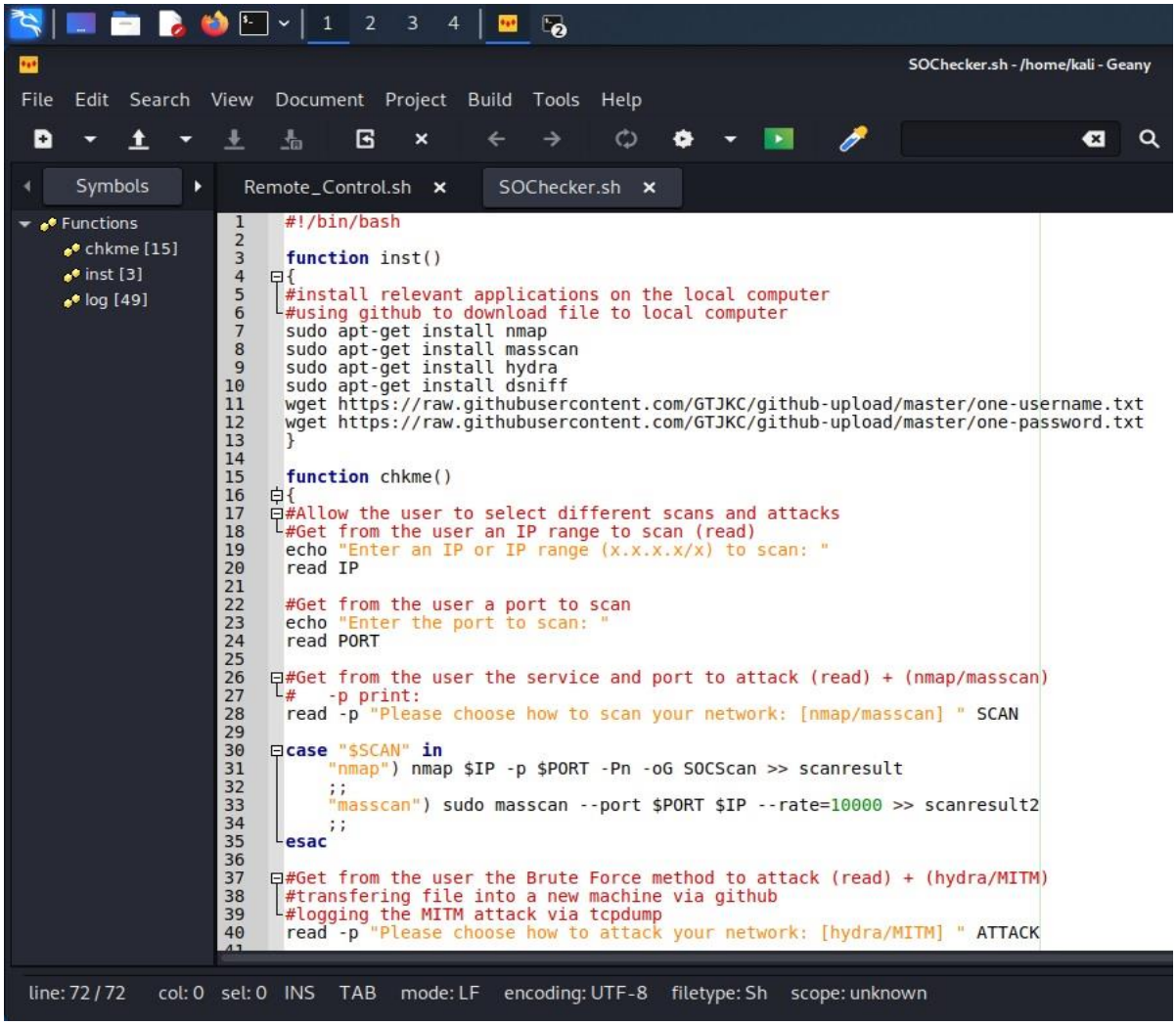
Objective:

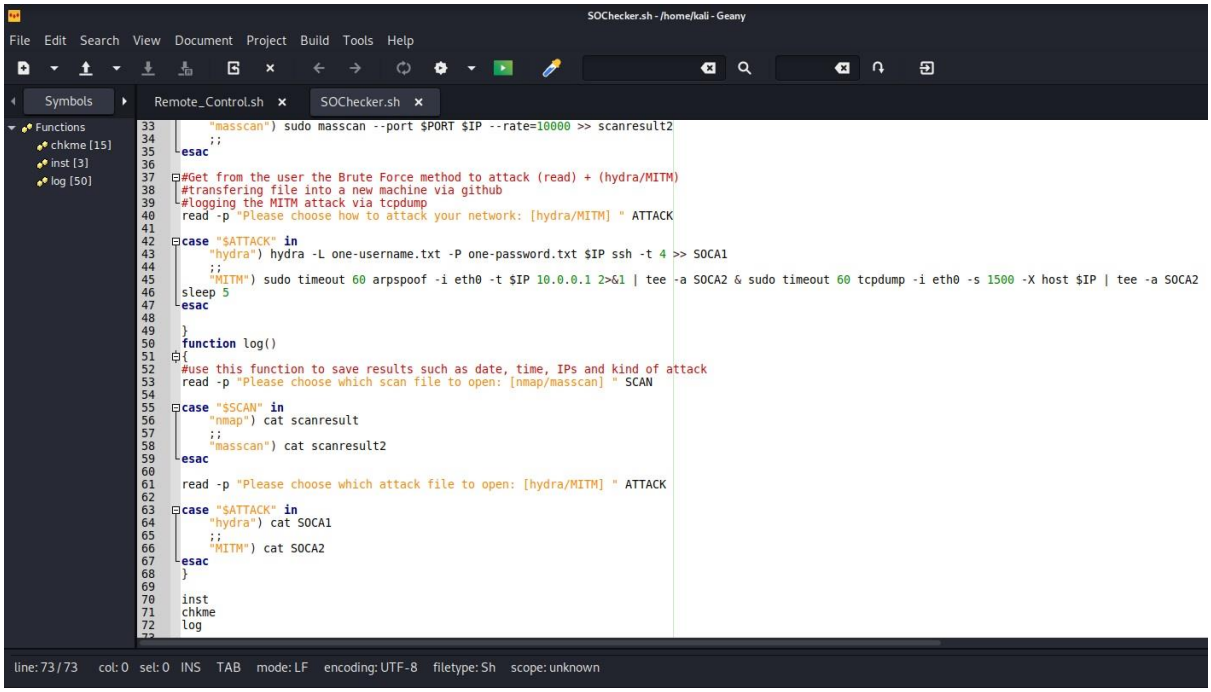
Create a script that runs different cyber attacks in a given network to check if monitoring alerts appear.

Using geany to write a script to assist with the scanning and attack process.

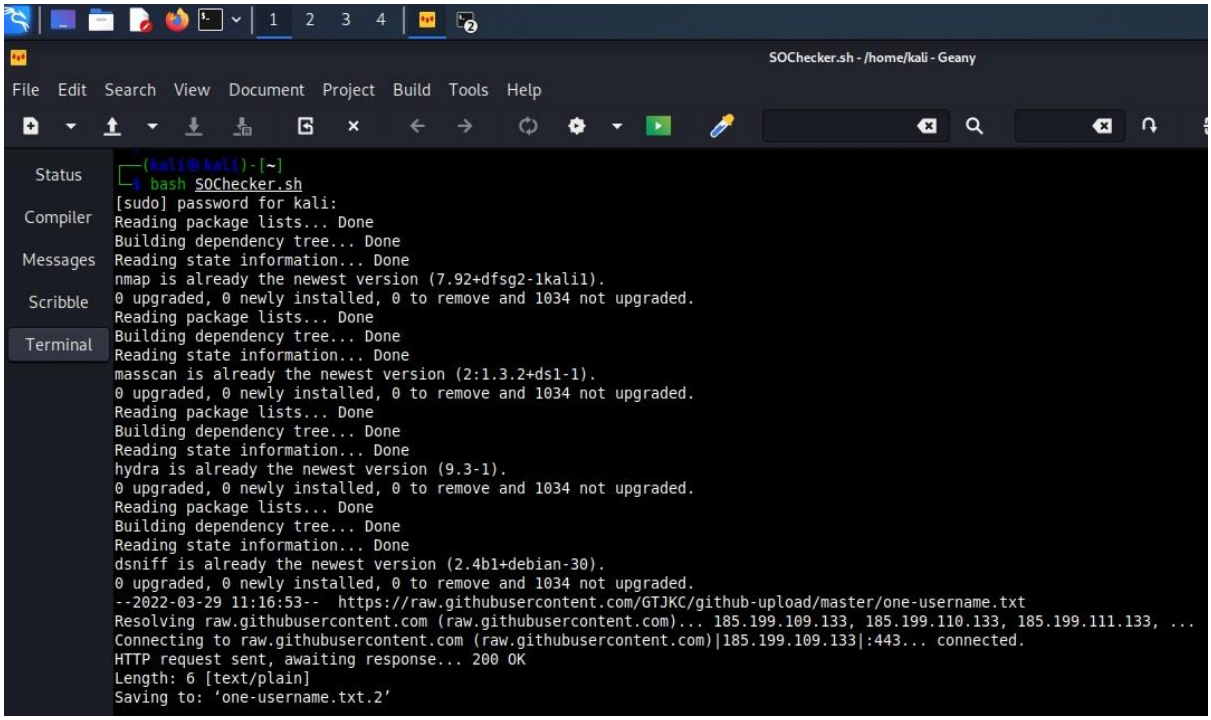
1) Function inst() to install all relevant applications on the local computer..
2) Function chkme() to execute scans and attacks.
   *allow users to choose two method of scanning and two different network attacks to run.
   *scans: nmap/ masscan attacks: hydra/MITM
3) Function LOG() to log executed attacks
   * Every scan or attack should be logged and saved with the date and used arguments.

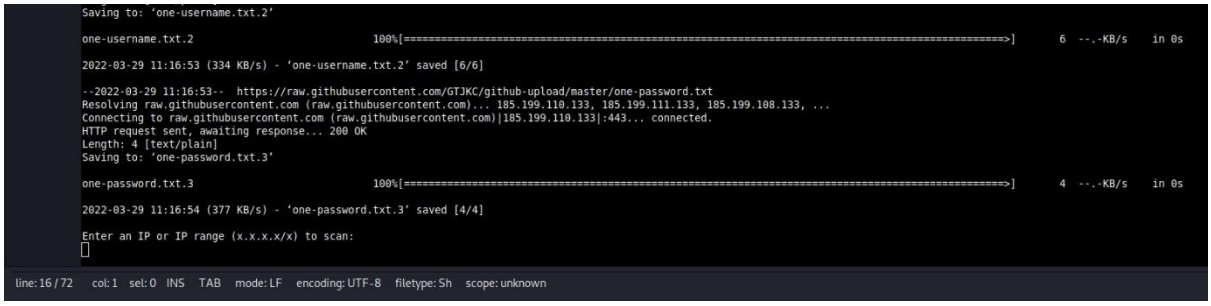
[Figure 1] Geany





[Figure 2] inst





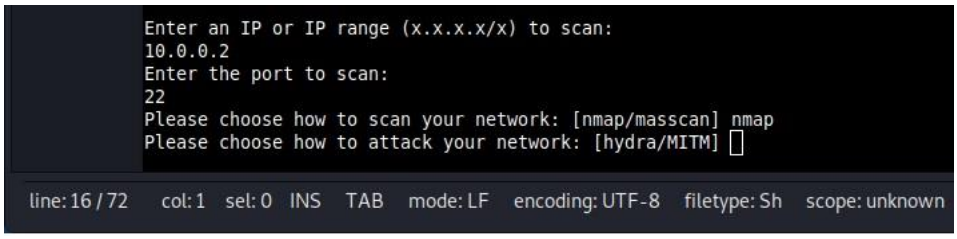
*Proves that installation script works.

The system will detect for any un-install/ un-updated apps, and install it.

Using wget to retrieve the store files from github.

Once all the apps are downloaded, the script will run the next command to scan for location of ip.

[Figure 3] nmap



*Proves that chkme script works.

First, the script would prompt user to key in an IP address to scan, once the user key in, the script will prompt user to key in port to scan.

*Prove that nmap scan script work.

As shown in the script in figure 1, nmap was saved into scanresult file using append (>>). This is to prevent over riding of previous logs after every new scan.

Thus, the result of the scan is not shown and is saved directly into the file, which will be shown in log function.

Once nmap is done, the script will run to the next command, to choose an attack method.

[Figure 4] masscan

```
Enter an IP or IP range (x.x.x.x/x) to scan:
10.0.0.2
Enter the port to scan:
22
Please choose how to scan your network: [nmap/masscan] masscan
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-03-29 16:11:42 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [1 port/host]
Please choose how to attack your network: [hydra/MITM]
line: 16 / 72   col: 1   sel: 0   INS   TAB   mode: LF   encoding: UTF-8   filetype: Sh   scope: unknown
```

*Prove that masscan scan script work.

As shown in the script in figure 1, masscan was saved into scanresult2.

Once masscan is done, the script will run to the next command, to choose an attack method.

[Figure 5] hydra

```
Enter an IP or IP range (x.x.x.x/x) to scan:
10.0.0.2
Enter the port to scan:
22
Please choose how to scan your network: [nmap/masscan] nmap
Please choose how to attack your network: [hydra/MITM] hydra
Please choose which scan file to open: [nmap/masscan]
line: 16 / 72   col: 1   sel: 0   INS   TAB   mode: LF   encoding: UTF-8   filetype: Sh   scope: unknown
```

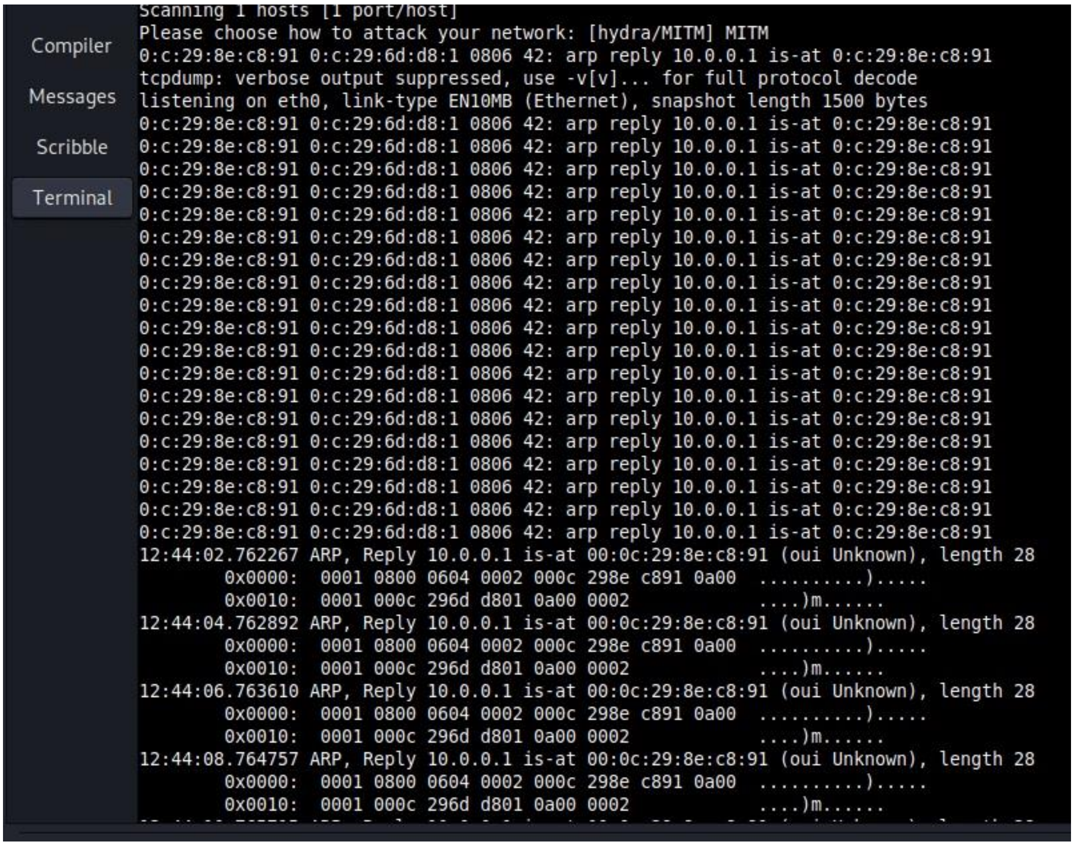
*Proves that hydra attack script work.

As shown in the script in figure 1, hydra was saved into SOCA1 file using append (>>).

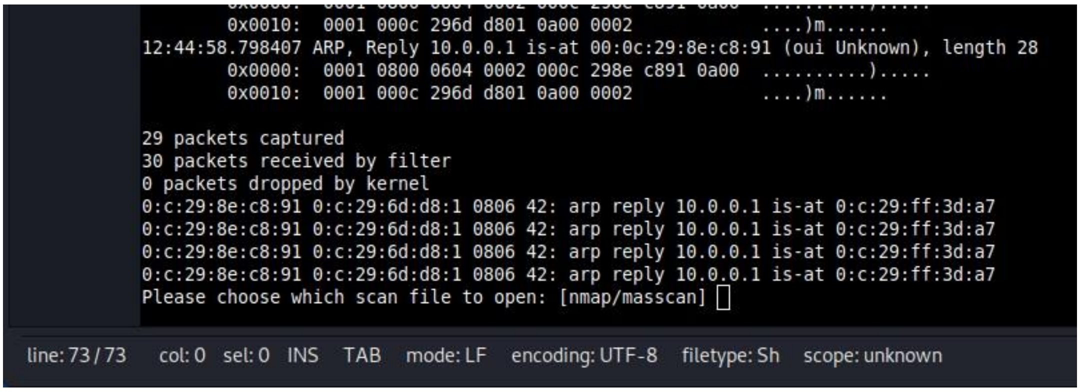
This is to prevent over riding of previous logs after every new attack.

Once hydra is done, the script will run to the next command to choose which log scan file to open.

[Figure 6] MITM



```
Scanning 1 hosts [1 port/host]
Please choose how to attack your network: [hydra/MITM] MITM
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:8e:c8:91
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 1500 bytes
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:8e:c8:91
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:8e:c8:91
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:8e:c8:91
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:8e:c8:91
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:8e:c8:91
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:8e:c8:91
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:8e:c8:91
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:8e:c8:91
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:8e:c8:91
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:8e:c8:91
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:8e:c8:91
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:8e:c8:91
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:8e:c8:91
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:8e:c8:91
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:8e:c8:91
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:8e:c8:91
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:8e:c8:91
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:8e:c8:91
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:8e:c8:91
12:44:02.762267 ARP, Reply 10.0.0.1 is-at 00:0c:29:8e:c8:91 (oui Unknown), length 28
        0x0000:  0001 0800 0604 0002 000c 298e c891 0a00  ..........).....
        0x0010:  0001 000c 296d d801 0a00 0002            ....)m......
12:44:04.762892 ARP, Reply 10.0.0.1 is-at 00:0c:29:8e:c8:91 (oui Unknown), length 28
        0x0000:  0001 0800 0604 0002 000c 298e c891 0a00  ..........).....
        0x0010:  0001 000c 296d d801 0a00 0002            ....)m......
12:44:06.763610 ARP, Reply 10.0.0.1 is-at 00:0c:29:8e:c8:91 (oui Unknown), length 28
        0x0000:  0001 0800 0604 0002 000c 298e c891 0a00  ..........).....
        0x0010:  0001 000c 296d d801 0a00 0002            ....)m......
12:44:08.764757 ARP, Reply 10.0.0.1 is-at 00:0c:29:8e:c8:91 (oui Unknown), length 28
        0x0000:  0001 0800 0604 0002 000c 298e c891 0a00  ..........).....
        0x0010:  0001 000c 296d d801 0a00 0002            ....)m......
```



```
        0x0010:  0001 000c 296d d801 0a00 0002            ....)m......
12:44:58.798407 ARP, Reply 10.0.0.1 is-at 00:0c:29:8e:c8:91 (oui Unknown), length 28
        0x0000:  0001 0800 0604 0002 000c 298e c891 0a00  ..........).....
        0x0010:  0001 000c 296d d801 0a00 0002            ....)m......

29 packets captured
30 packets received by filter
0 packets dropped by kernel
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:ff:3d:a7
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:ff:3d:a7
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:ff:3d:a7
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:ff:3d:a7
Please choose which scan file to open: [nmap/masscan] 
```

*Proves that MITM attack script work.

MITM is running both arpspoof and tcpdump concurrently with a timeout set at 60s.

Arpspoof is the MITM attack while tcpdump is to log the attacks.

Time out is to stop the attack after 60s.

Sleep 5 waits for 5 second for arpspoof spillover to be over, before running the next command.

[Figure 7] log- nmap

```
Please choose how to attack your network: [hydra/MITM] hydra
Please choose which scan file to open: [nmap/masscan] nmap
# Nmap 7.92 scan initiated Tue Mar 29 11:36:45 2022 as: nmap -p 22 -Pn -oG SOCScan 10.0.0.2
Host: 10.0.0.2 ()       Status: Up
Host: 10.0.0.2 ()       Ports: 22/open/tcp//ssh///
# Nmap done at Tue Mar 29 11:36:53 2022 -- 1 IP address (1 host up) scanned in 8.08 seconds
Please choose which attack file to open: [hydra/MITM]
line: 16 / 72   col: 1   sel: 0   INS   TAB   mode: LF   encoding: UTF-8   filetype: Sh   scope: unknown
```

*Proves that log script works.

*Proves that nmap log script works.

When asked which scan file to open, the user key nmap, it would cat scanresult file and show the result of the scan.

[Figure 8] log- masscan

```
Compiler
Messages
Scribble
Terminal
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:ff:3d:a7
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:ff:3d:a7
Please choose which scan file to open: [nmap/masscan] masscan
SOCScan2Discovered open port 22/tcp on 10.0.0.2
Discovered open port 49676/tcp on 10.0.0.1
Discovered open port 49667/tcp on 10.0.0.1
Discovered open port 636/tcp on 10.0.0.1
Discovered open port 49701/tcp on 10.0.0.1
Discovered open port 49762/tcp on 10.0.0.1
Discovered open port 464/tcp on 10.0.0.1
Discovered open port 49678/tcp on 10.0.0.1
Discovered open port 445/tcp on 10.0.0.1
Discovered open port 49675/tcp on 10.0.0.1
Discovered open port 49666/tcp on 10.0.0.1
Discovered open port 3269/tcp on 10.0.0.1
Discovered open port 135/tcp on 10.0.0.1
Discovered open port 88/tcp on 10.0.0.1
Discovered open port 49713/tcp on 10.0.0.1
Discovered open port 3268/tcp on 10.0.0.1
Discovered open port 53/tcp on 10.0.0.1
Discovered open port 49700/tcp on 10.0.0.1
Discovered open port 593/tcp on 10.0.0.1
Discovered open port 9389/tcp on 10.0.0.1
Discovered open port 139/tcp on 10.0.0.1
Discovered open port 5985/tcp on 10.0.0.1
Discovered open port 389/tcp on 10.0.0.1
Discovered open port 22/tcp on 10.0.0.2
Discovered open port 22/tcp on 10.0.0.2
Discovered open port 22/tcp on 10.0.0.2
Discovered open port 22/tcp on 10.0.0.2
Discovered open port 22/tcp on 10.0.0.2
Discovered open port 22/tcp on 10.0.0.2
Discovered open port 22/tcp on 10.0.0.2
Discovered open port 22/tcp on 10.0.0.2
Discovered open port 22/tcp on 10.0.0.2
Please choose which attack file to open: [hydra/MITM]
line: 60 / 73   col: 0   sel: 0   INS   TAB   mode: LF   encoding: UTF-8   filetype: Sh   scope: log
```

*Proves that masscan log script works.

When asked which scan file to open, when the user key nmap, it would cat scanresult2 file and show the result of the scan.

[Figure 9] log- hydra

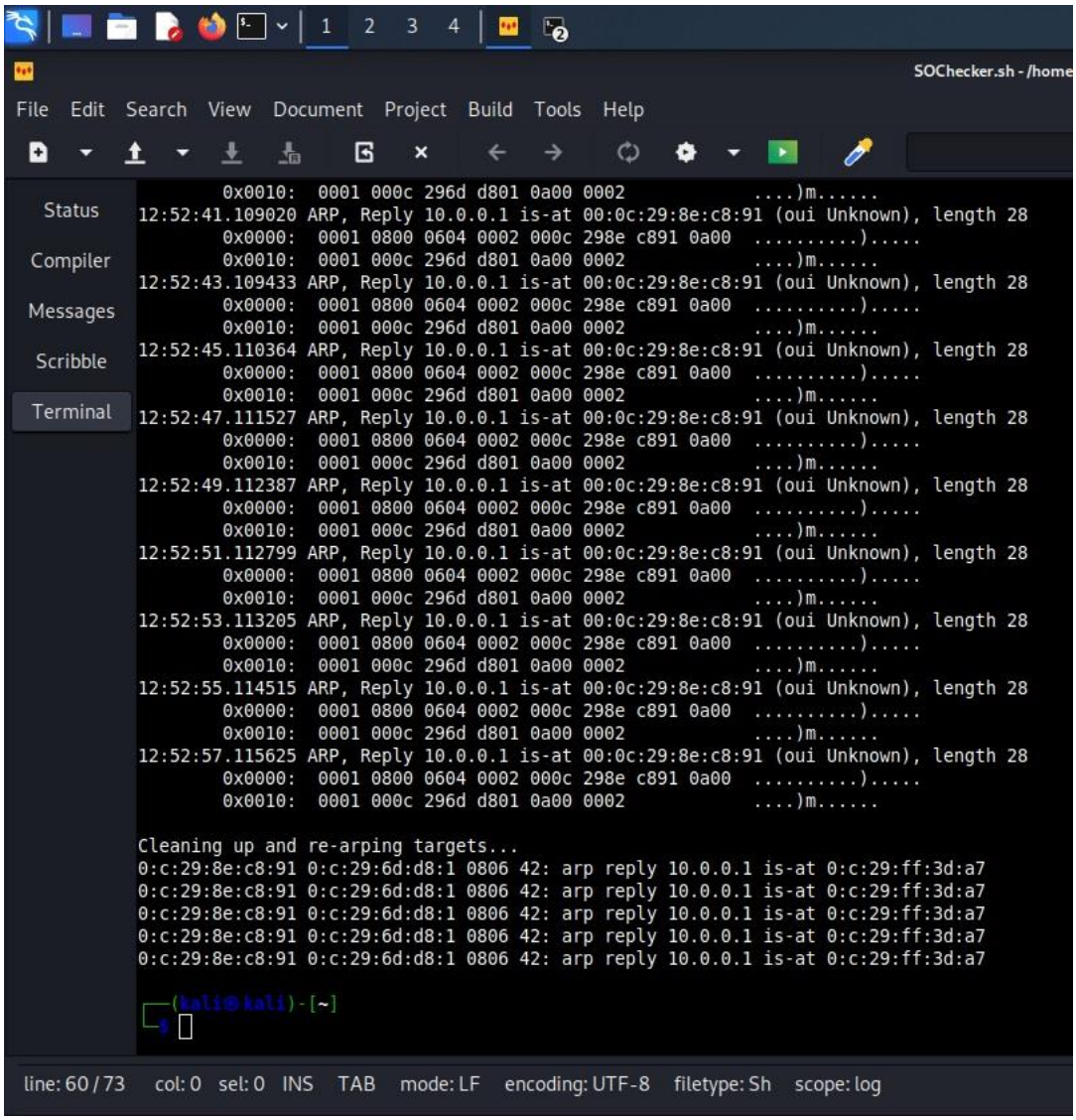
```
Compiler   Please choose how to attack your network: [hydra/MITM] hydra
           Please choose which scan file to open: [nmap/masscan] nmap
Messages   # Nmap 7.92 scan initiated Tue Mar 29 11:36:45 2022 as: nmap -p 22 -Pn -oG SOCScan 10.0.0.2
           Host: 10.0.0.2 ()       Status: Up
Scribble   Host: 10.0.0.2 ()       Ports: 22/open/tcp//ssh///
           # Nmap done at Tue Mar 29 11:36:53 2022 -- 1 IP address (1 host up) scanned in 8.08 seconds
Terminal   Please choose which attack file to open: [hydra/MITM] hydra
           Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore la
           ws and ethics anyway).

           Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-24 03:35:59
           [DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
           [DATA] attacking ssh://10.0.0.2:22/
           1 of 1 target completed, 0 valid password found
           Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-03-24 03:36:32
           Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore la
           ws and ethics anyway).

           Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-27 11:44:44
           [DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
           [DATA] attacking ssh://10.0.0.2:22/
           1 of 1 target completed, 0 valid password found
           Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-03-27 11:45:16
           Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore la
           ws and ethics anyway).

           Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-29 11:39:48
           [DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
           [DATA] attacking ssh://10.0.0.2:22/
           1 of 1 target completed, 0 valid password found
           Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-03-29 11:40:20

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

*Proves that hydra log script works.

When asked which scan file to open, when the user key hydra, it would cat SOCA1 file and show the result of the attack.

And the scripts end.

[Figure 10] log- MITM



```
        0x0010:  0001 000c 296d d801 0a00 0002            ....)m......
12:52:41.109020 ARP, Reply 10.0.0.1 is-at 00:0c:29:8e:c8:91 (oui Unknown), length 28
        0x0000:  0001 0800 0604 0002 000c 298e c891 0a00  ..........).....
        0x0010:  0001 000c 296d d801 0a00 0002            ....)m......
12:52:43.109433 ARP, Reply 10.0.0.1 is-at 00:0c:29:8e:c8:91 (oui Unknown), length 28
        0x0000:  0001 0800 0604 0002 000c 298e c891 0a00  ..........).....
        0x0010:  0001 000c 296d d801 0a00 0002            ....)m......
12:52:45.110364 ARP, Reply 10.0.0.1 is-at 00:0c:29:8e:c8:91 (oui Unknown), length 28
        0x0000:  0001 0800 0604 0002 000c 298e c891 0a00  ..........).....
        0x0010:  0001 000c 296d d801 0a00 0002            ....)m......
12:52:47.111527 ARP, Reply 10.0.0.1 is-at 00:0c:29:8e:c8:91 (oui Unknown), length 28
        0x0000:  0001 0800 0604 0002 000c 298e c891 0a00  ..........).....
        0x0010:  0001 000c 296d d801 0a00 0002            ....)m......
12:52:49.112387 ARP, Reply 10.0.0.1 is-at 00:0c:29:8e:c8:91 (oui Unknown), length 28
        0x0000:  0001 0800 0604 0002 000c 298e c891 0a00  ..........).....
        0x0010:  0001 000c 296d d801 0a00 0002            ....)m......
12:52:51.112799 ARP, Reply 10.0.0.1 is-at 00:0c:29:8e:c8:91 (oui Unknown), length 28
        0x0000:  0001 0800 0604 0002 000c 298e c891 0a00  ..........).....
        0x0010:  0001 000c 296d d801 0a00 0002            ....)m......
12:52:53.113205 ARP, Reply 10.0.0.1 is-at 00:0c:29:8e:c8:91 (oui Unknown), length 28
        0x0000:  0001 0800 0604 0002 000c 298e c891 0a00  ..........).....
        0x0010:  0001 000c 296d d801 0a00 0002            ....)m......
12:52:55.114515 ARP, Reply 10.0.0.1 is-at 00:0c:29:8e:c8:91 (oui Unknown), length 28
        0x0000:  0001 0800 0604 0002 000c 298e c891 0a00  ..........).....
        0x0010:  0001 000c 296d d801 0a00 0002            ....)m......
12:52:57.115625 ARP, Reply 10.0.0.1 is-at 00:0c:29:8e:c8:91 (oui Unknown), length 28
        0x0000:  0001 0800 0604 0002 000c 298e c891 0a00  ..........).....
        0x0010:  0001 000c 296d d801 0a00 0002            ....)m......

Cleaning up and re-arping targets...
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:ff:3d:a7
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:ff:3d:a7
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:ff:3d:a7
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:ff:3d:a7
0:c:29:8e:c8:91 0:c:29:6d:d8:1 0806 42: arp reply 10.0.0.1 is-at 0:c:29:ff:3d:a7

┌──(kali㉿kali)-[~]
└─$ 
```

*Proves that MITM log script works.

When asked which scan file to open, when the user key MITM, it would cat SOCA2 file and show the result of the attack.

And the scripts end.