SOC_Checker is an automatic attack system.

Might be used to check SOC teams vigilance. Available attacks - Men in the Midlle, SMB Brute-Force, DHCP starvation. The script checks if necessary tools are installed and if not installs them.

Men in the Middle Attack (ARP poisoning tactic) – enable routing, launch attack with arpspoofing and urlsnarf. User can press S at any time to stop the attack. Once the attack is completed disable routing to restore default settings. Log the attack.

On the target side before MITM attack:

(attacker IP – 192.168.49.142; default gateway – 192.168.49.2, different MAC addresses)

```
C:\Users\test>arp -a

Interface: 192.168.49.145 --- 0x4
  Internet Address      Physical Address      Type
  192.168.49.2          00-50-56-e6-12-25     dynamic
  192.168.49.142        00-0c-29-f5-6c-b3     dynamic
  192.168.49.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

After:

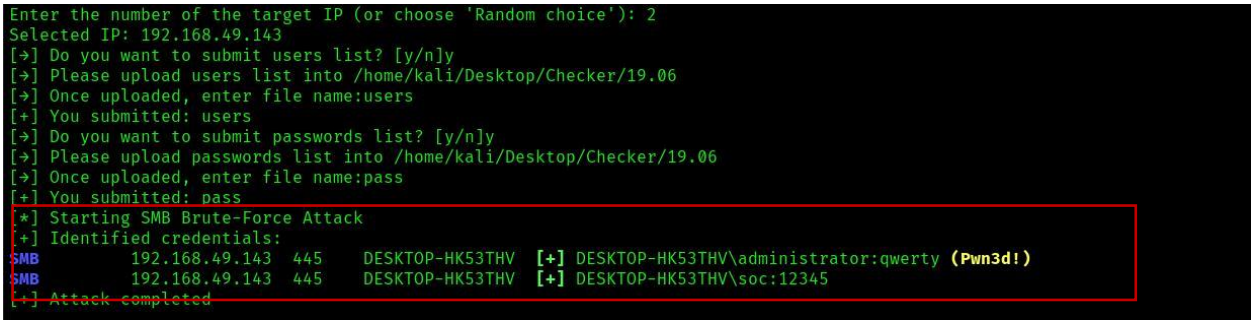
(MAC address duplication)

```
C:\Users\test>arp -a

Interface: 192.168.49.145 --- 0x4
  Internet Address      Physical Address      Type
  192.168.49.2          00-0c-29-f5-6c-b3     dynamic
  192.168.49.142        00-0c-29-f5-6c-b3     dynamic
  192.168.49.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

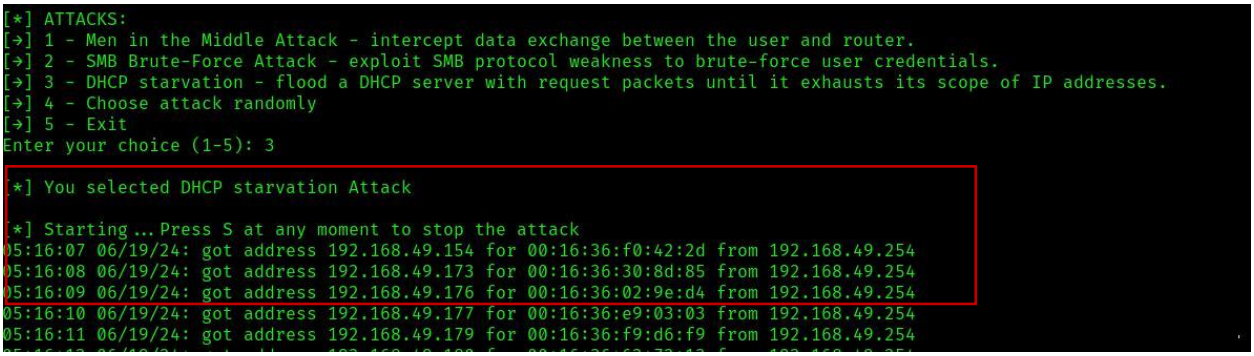
SMB Brute-Force attack: crackmapexec against hosts with 445 (SMB) port open. User can submit users and password list. If no list is submitted – download and use lists from GitHub.

```
Attack stopped
0
[+] Routing disabled to restore default settings

[*] ATTACKS:
[→] 1 - Men in the Middle Attack - intercept data exchange between the user and router.
[→] 2 - SMB Brute-Force Attack - exploit SMB protocol weakness to brute-force user credentials.
[→] 3 - DHCP starvation - flood a DHCP server with request packets until it exhausts its scope of IP addresses.
[→] 4 - Choose attack randomly
[→] 5 - Exit
Enter your choice (1-5): 2

[*] You selected SMB Brute-Force Attack

[*] Scanning for hosts running SMB service
Found the following hosts:
1. 192.168.49.1
2. 192.168.49.143
3. 192.168.49.145
4. Random choice
Enter the number of the target IP (or choose 'Random choice'): 2
```

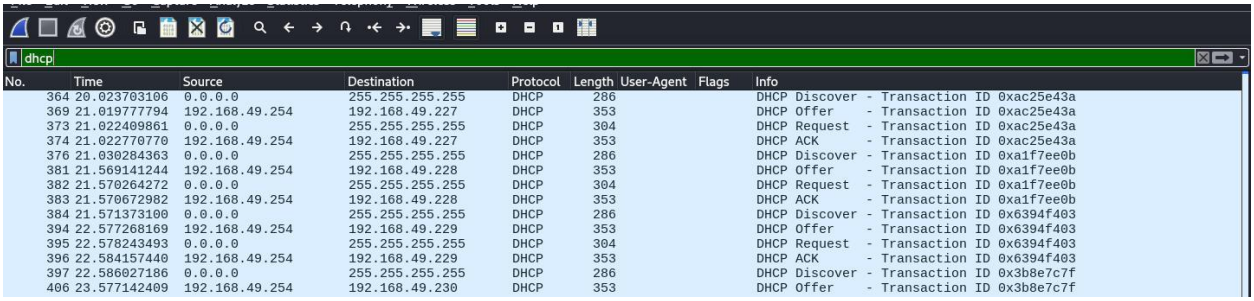
Weak credentials found:



DHCP starvation attack:



DHCP starvation attack monitored in Wireshark:



```
05:17:07 06/19/24: got address 192.168.49.237 for 00:16:36:9a:69:33 from 192.168.49.254
05:17:08 06/19/24: got address 192.168.49.238 for 00:16:36:78:70:be from 192.168.49.254
Attack stopped

[*] ATTACKS:
[→] 1 - Men in the Middle Attack - intercept data exchange between the user and router.
[→] 2 - SMB Brute-Force Attack - exploit SMB protocol weakness to brute-force user credentials.
[→] 3 - DHCP starvation - flood a DHCP server with request packets until it exhausts its scope of IP addresses.
[→] 4 - Choose attack randomly
[→] 5 - Exit
Enter your choice (1-5): 5

[*] Log is saved in /home/kali/Desktop/Checker/19.06. Exiting...
```

Attacks Log:

```
└─$ cat log.txt
Men in the Middle
Start: Wed Jun 19 05:11:35 AM EDT 2024
Target: 192.168.49.145
End: Wed Jun 19 05:14:11 AM EDT 2024
SMB Brute-Force
Start: Wed Jun 19 05:15:36 AM EDT 2024
Target:
Identified credentials:
SMB         192.168.49.143  445    DESKTOP-HK53THV  [+] DESKTOP-HK53THV\administrator:qwerty (Pwn3d!)
SMB         192.168.49.143  445    DESKTOP-HK53THV  [+] DESKTOP-HK53THV\soc:12345
End: Wed Jun 19 05:15:53 AM EDT 2024
DHCP starvation Attack
Start: Wed Jun 19 05:16:06 AM EDT 2024
Target:
End: Wed Jun 19 05:17:08 AM EDT 2024
```