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. **DoS (SYN Flood) – Sends a large number of TCP SYN packets to overwhelm a specific port and exhaust server resources.**

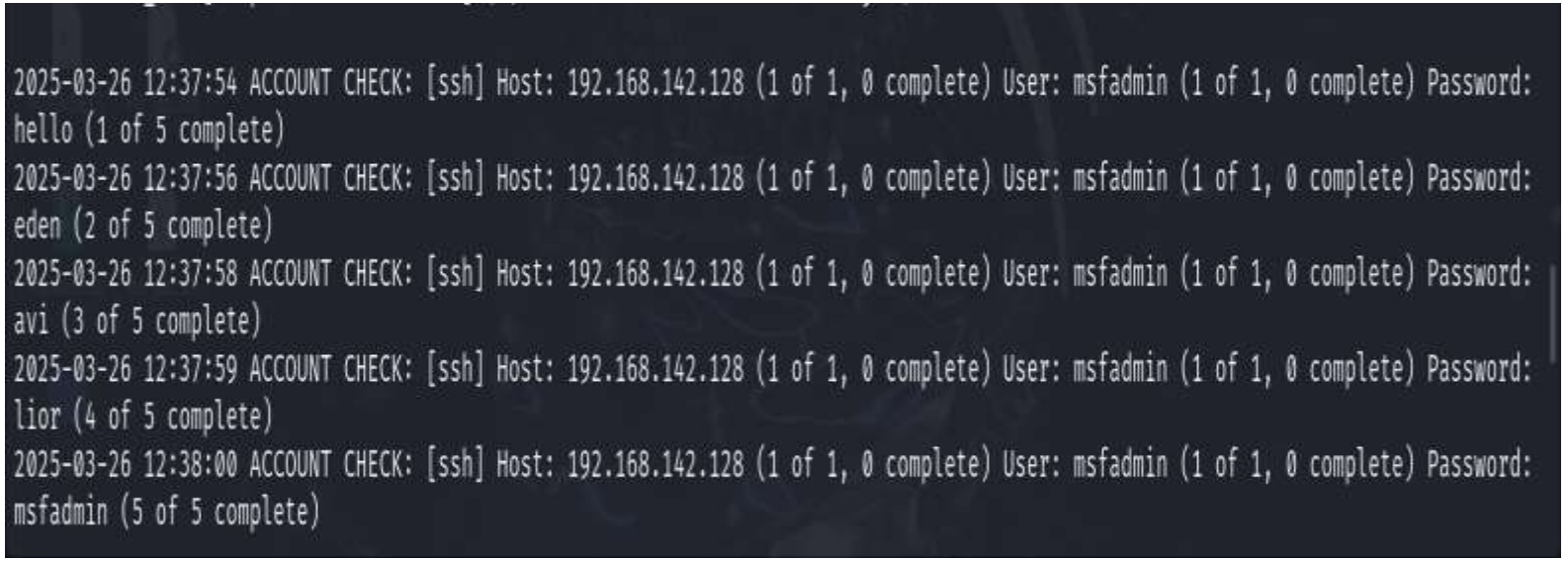
This screenshot shows the attacker sending forged ARP replies to the victim, tricking it into thinking that the attacker's MAC address belongs to the default gateway. This enables Man-in-the-Middle attacks.

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.

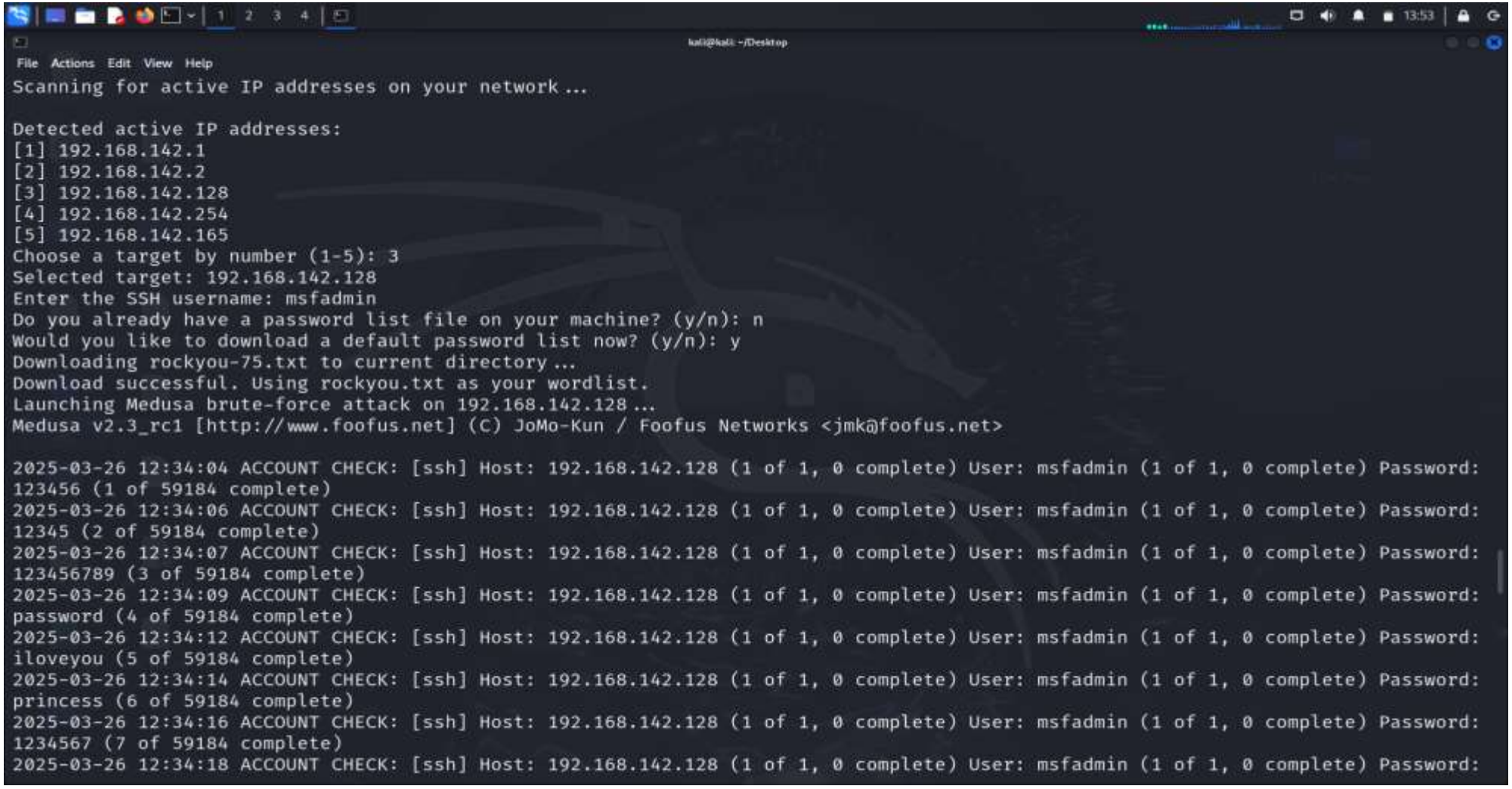
```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:c1:27:42
          inet addr:192.168.142.128  Bcast:192.168.142.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fec1:2742/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          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

lo        Link encap:Local Loopback
          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.

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



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.