UNDERSTANDING TCP/IP BASED ATTACKS

OVERVIEW

- TCP/IP vulnerabilities, attacks
- Protocol designs and implementations
- Attacks on TCP/IP protocols use linux operating systems
- Assume that tasks are on the same network as the victims
- Use sniffer tools to determine where the attacks may happen

VMWARE

- All three
- Make sure internet is disconnected from server VM

TOOLS

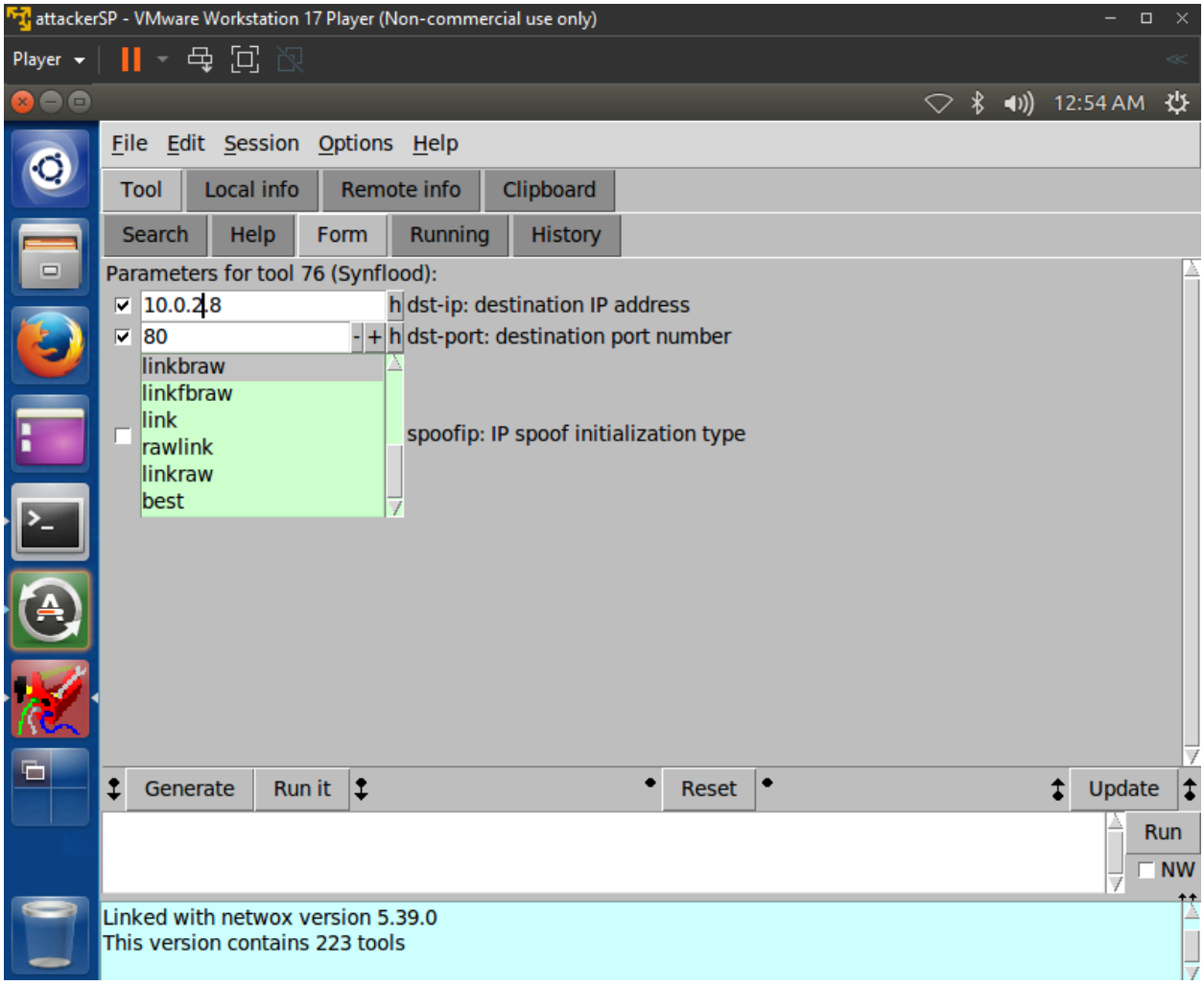
- Netwag (sending network packets of different types w different contents)
- Wireshark
- Tshark (terminal based network packet analyser)

TASK 1: SYN FLOODING ATTACK

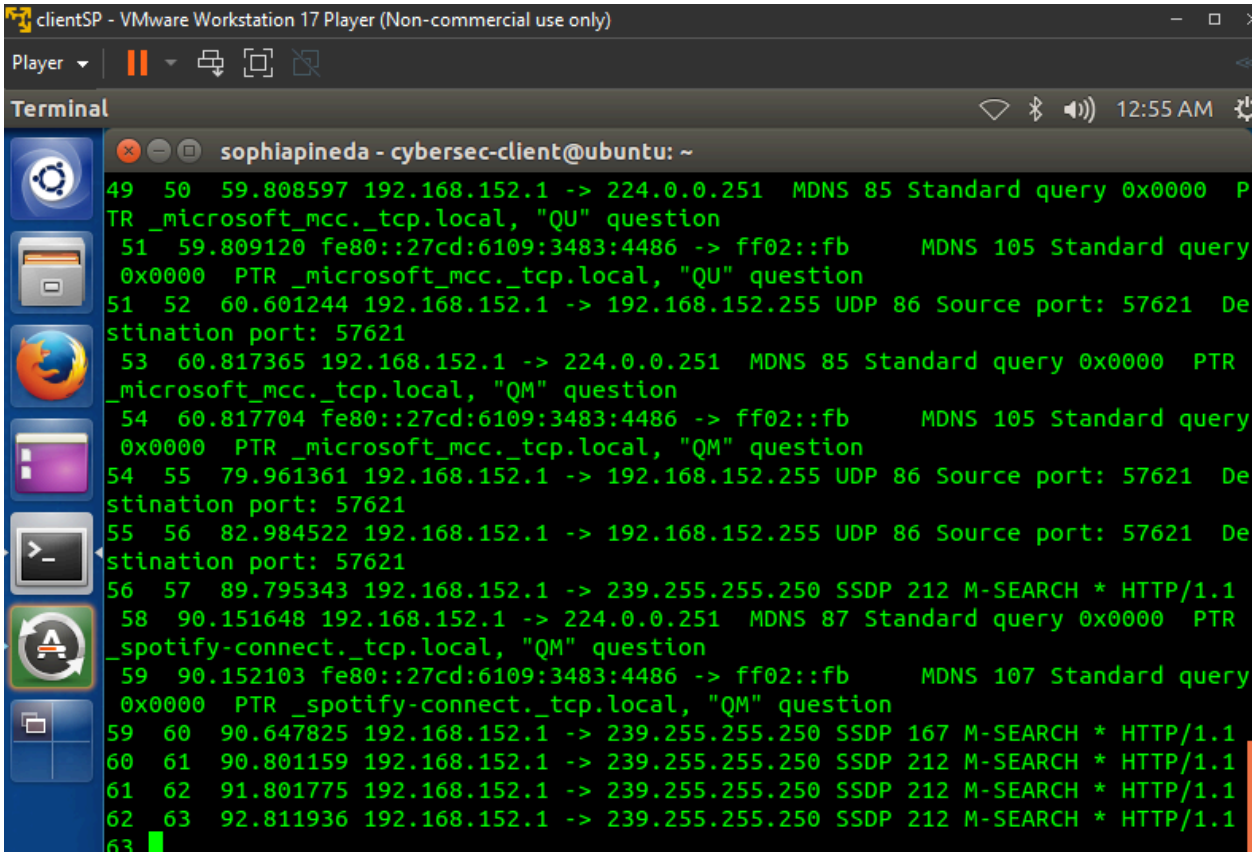
- SYN flood- DoS attack where many SYN requests are sent to a victim's TCP port, but attackers don't finish the 3 way handshake procedure
    - They use spoofed IP address
- Floods victim's queue that's for half-opened connections: victim can't open anymore connections

STEPS

- Check system queue size setting: sysctl –q net.ipv4.tcp_max_syn_backlkog
- Check number in queue: netstat –na
- Enter sudo tshark on client VM
- Enter sudo netwag on attacker VM, select 76 Synflood and enter details (SCREENSHOT)

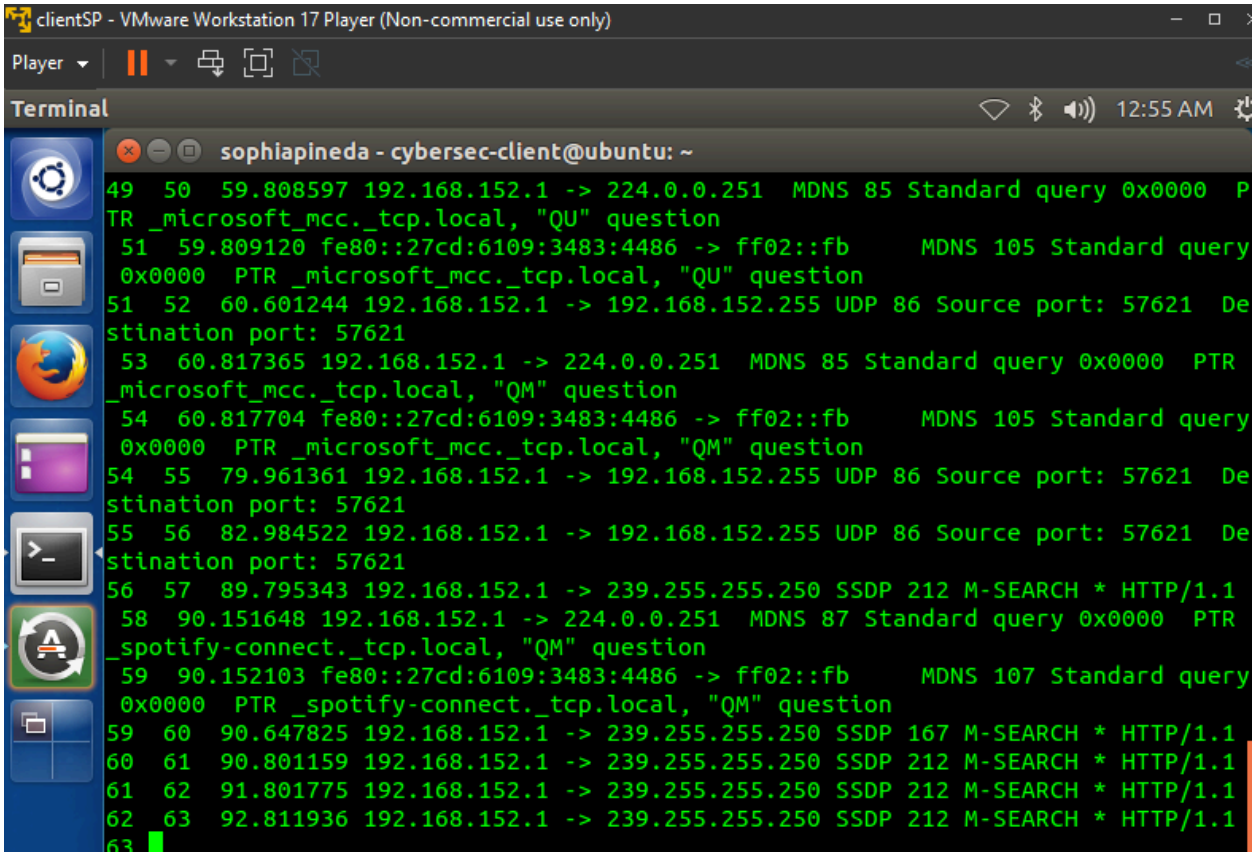


- Observer captured packets on client VM (SCREENSHOT)



QUESTIONS

1. Observe the attack and take screenshots of the attack scenario



2. Comment on your observation.

- Different source IP reaching out each time
- Methodical
- Fast paced

3. Categorize this attack in terms of severity and how it is linked to the DoS attack

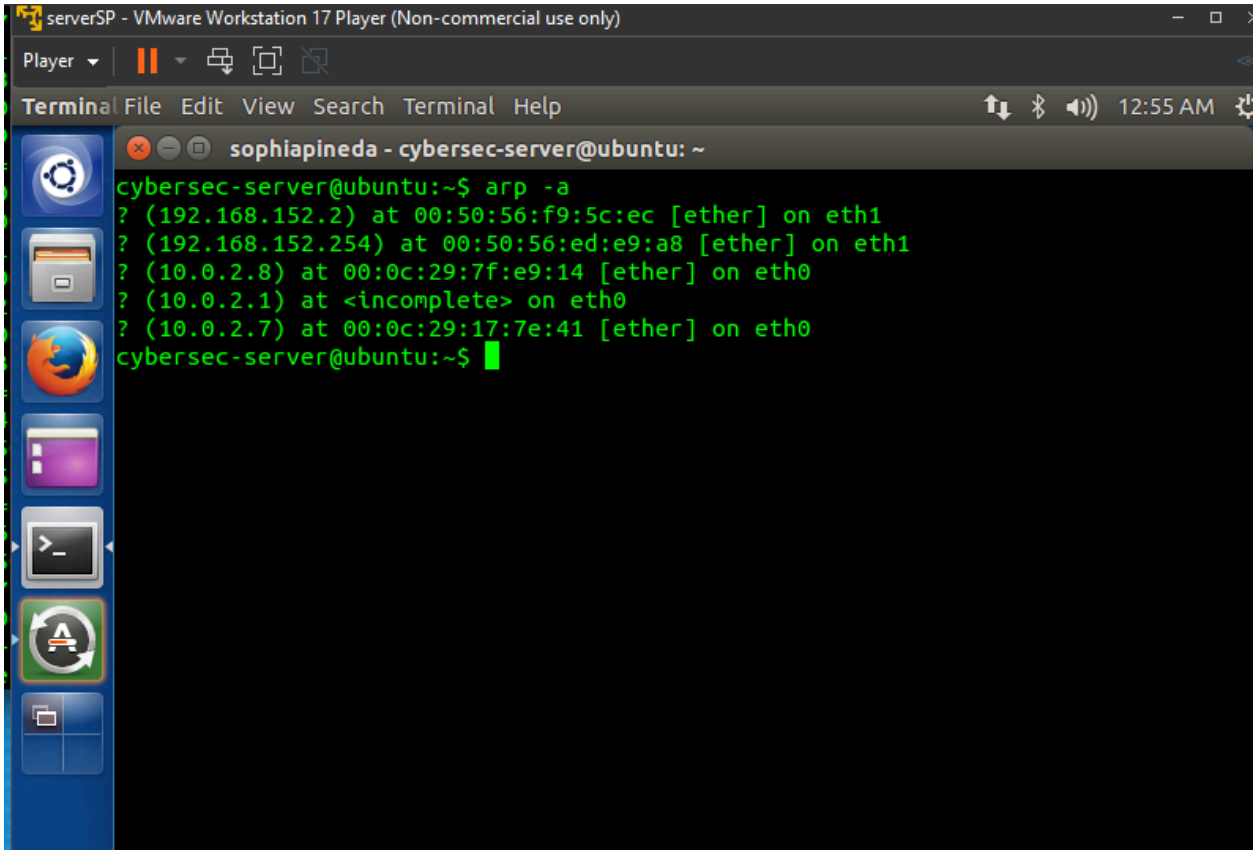
- High severity, linked to Denial of Service attack since high number of syn requests overwhelms the syn ports
- prevents the user from being able to respond to high traffic and leaves itself vulnerable

TASK 2: ARP (Address resolution protocol) CACHE POISONING

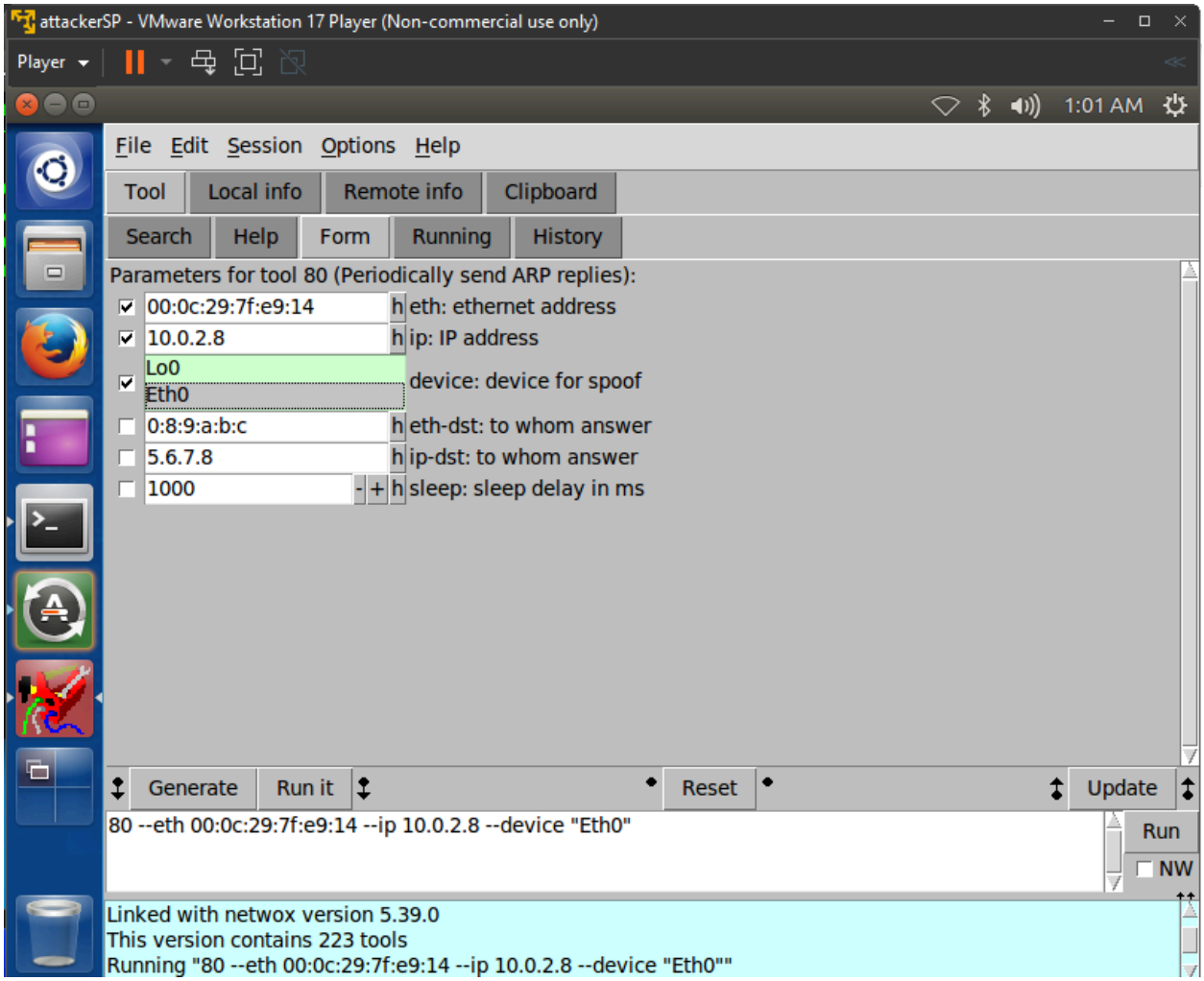
- Mapping between a MAC address and an IP address is resolved through executing the ARP protocol, which will cache the mapping
- Cache can easily be poisoned by malicious ARP messages
- Tricks victim to accept an invalid MAC-to IP mapping and store it in their cache

STEPS

- Enter arp-a on server VM, gets ARP information MAC table (SCREENSHOT)



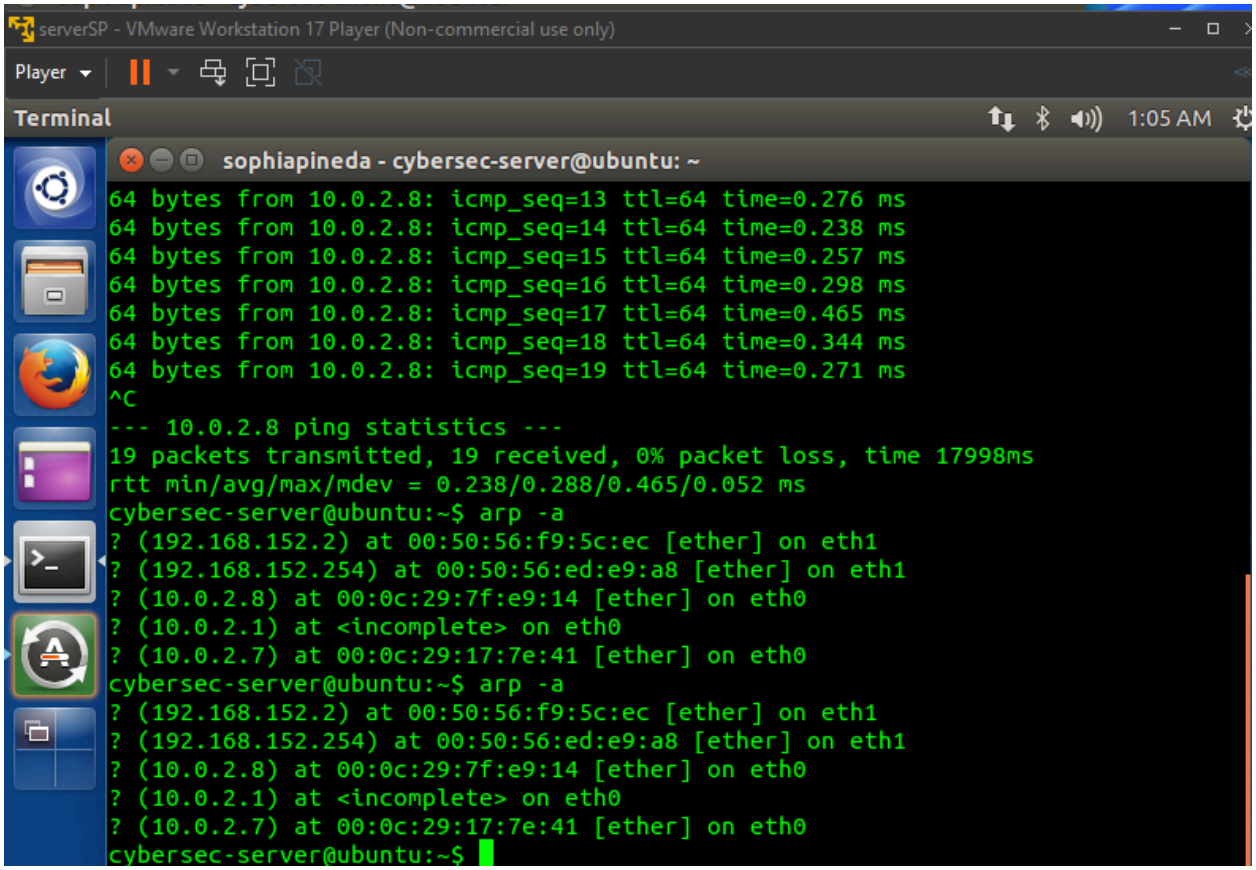
- Enter sudo netwag on attacker VM, select tool 80 and add fake MAC address and IP address, and select interface (SCREENSHOT)



- Check MAC table on server VM and observer change (SCREENSHOT)
- PING SERVER?

QUESTIONS

1. Observer attack and take screenshots of attack scenario



2. Comment

- Address changed, modified by attacker

3. Describe mitigation techniques

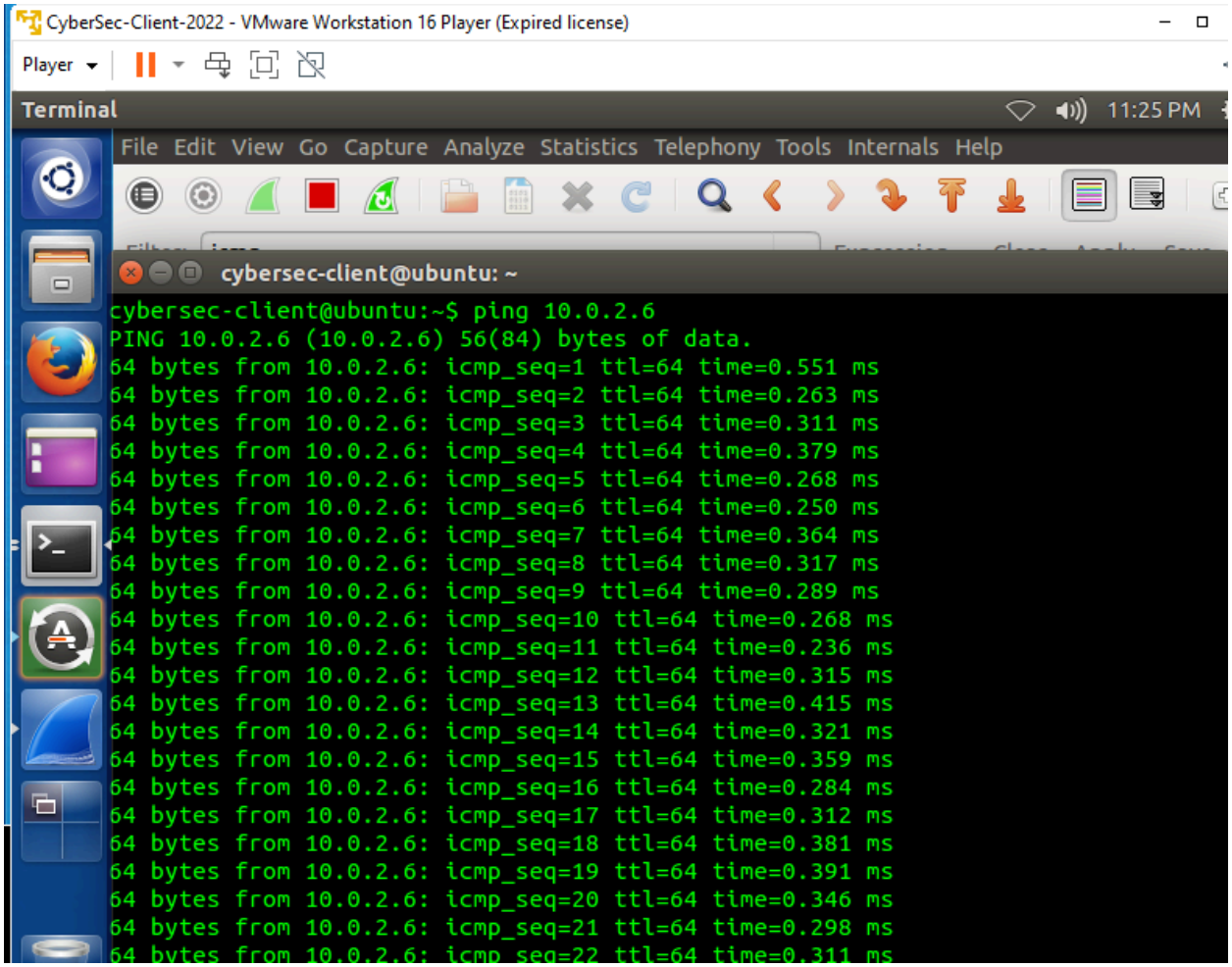
- Static ARP Tables - map all MAC addresses to designated IP address
- Switch Security
- Network Isolation
- Encryption - MAC addresses hidden

TASK 3: ICMP REDIRECT ATTACK

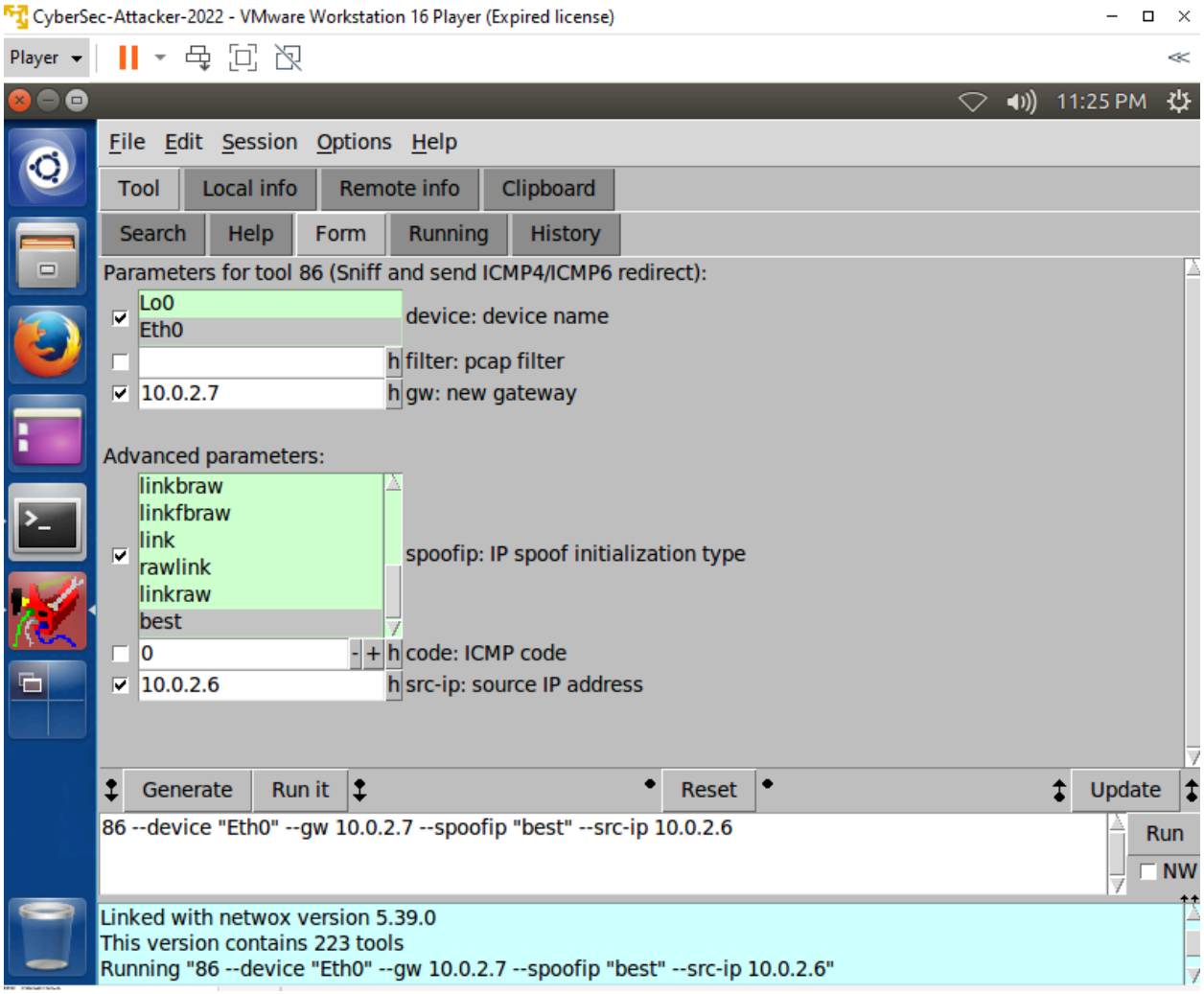
- ICMP redirect message used by routers, provides routing info to hosts
- When host receives this info, it will modify its routing table
- Attackers can spoof ICMP redirect messages, tricking victim to incorrectly modify table

STEPS

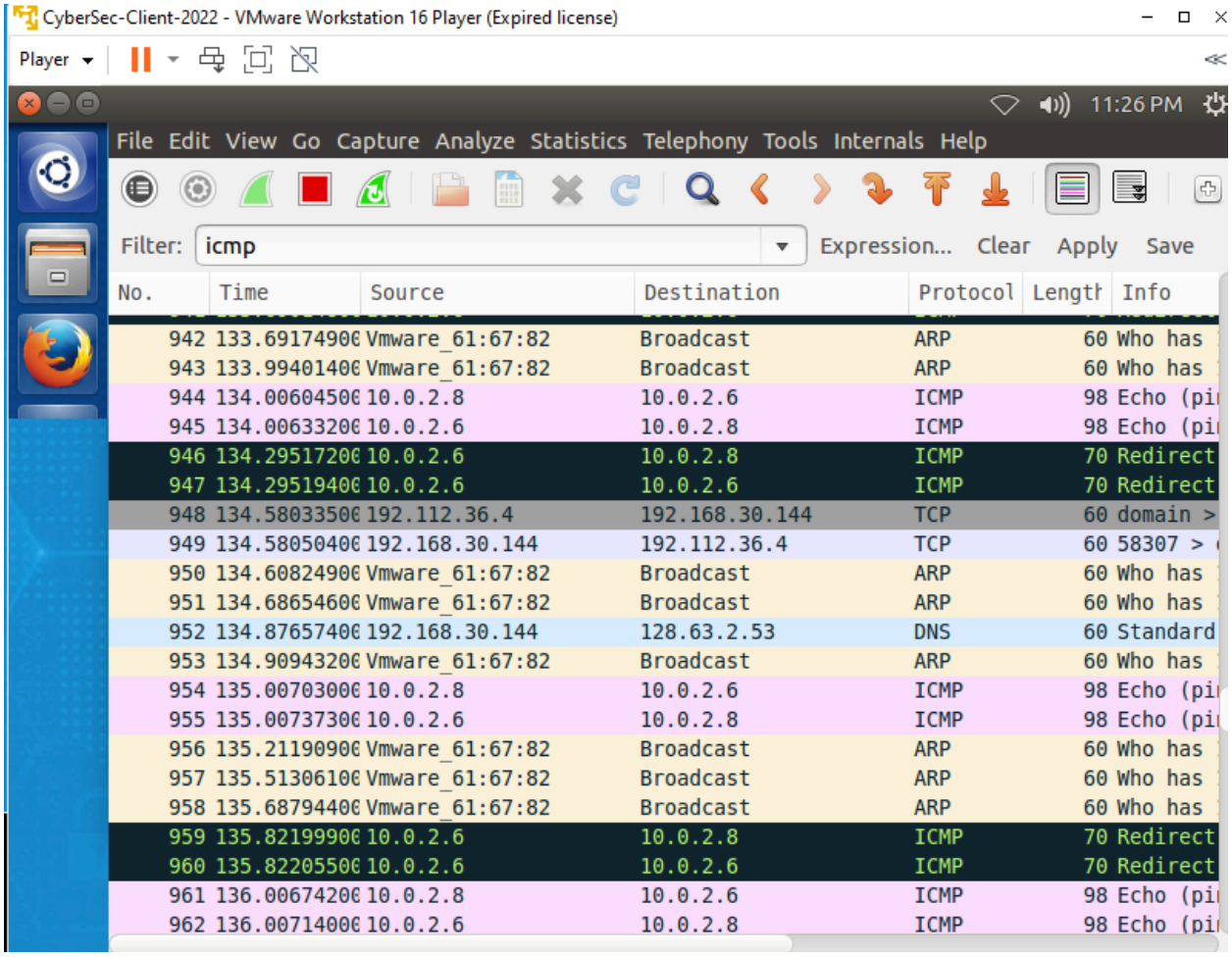
- Enter sudo wireshark on client VM, filter to ICMP
- Ping server on client VM (SCREENSHOT)



- Enter sudo netwag on attacker VM, tool 86, select interface and spoofip: IP spoof initialisation type, input IP address into gw: new gateway and src-ip: source IP address (SCREENSHOT)

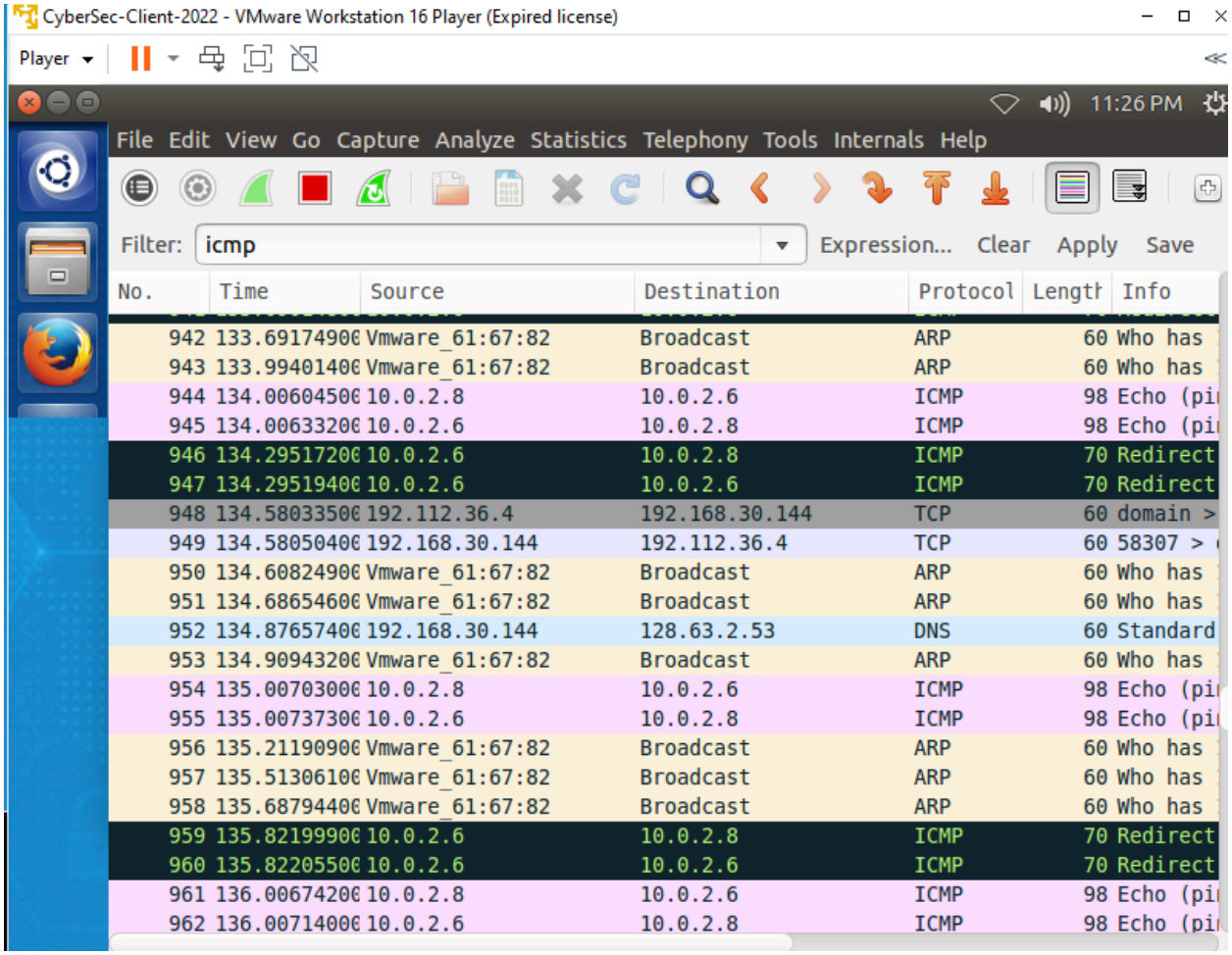


- Observe wireshark packets in client VM (SCREENSHOT)



QUESTIONS

1. Observe the attack and take screenshots of the attack scenario.



2. Comment on your observation.

- Ping redirects different
- Modifies routing table, takes victim outside of LAN network

3. Briefly describe how you can mitigate this attack

- Disable redirects
- Increase network router security
- Only accept packets from the same network