

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)

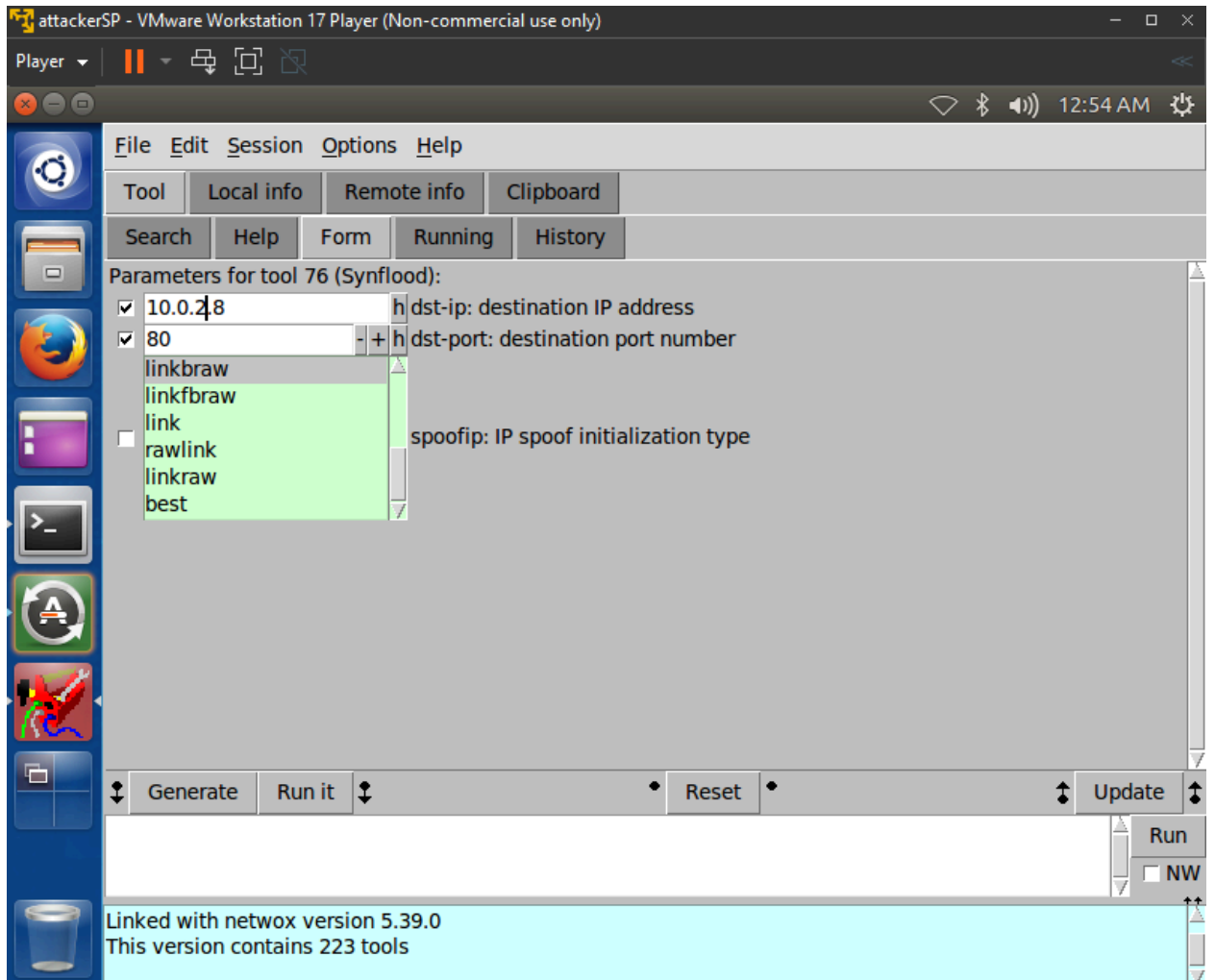
TASK 1: SYN FLOODING ATTACK

- 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_backlog`
- 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)

clientSP - VMware Workstation 17 Player (Non-commercial use only)

Player ▾ [Icons]

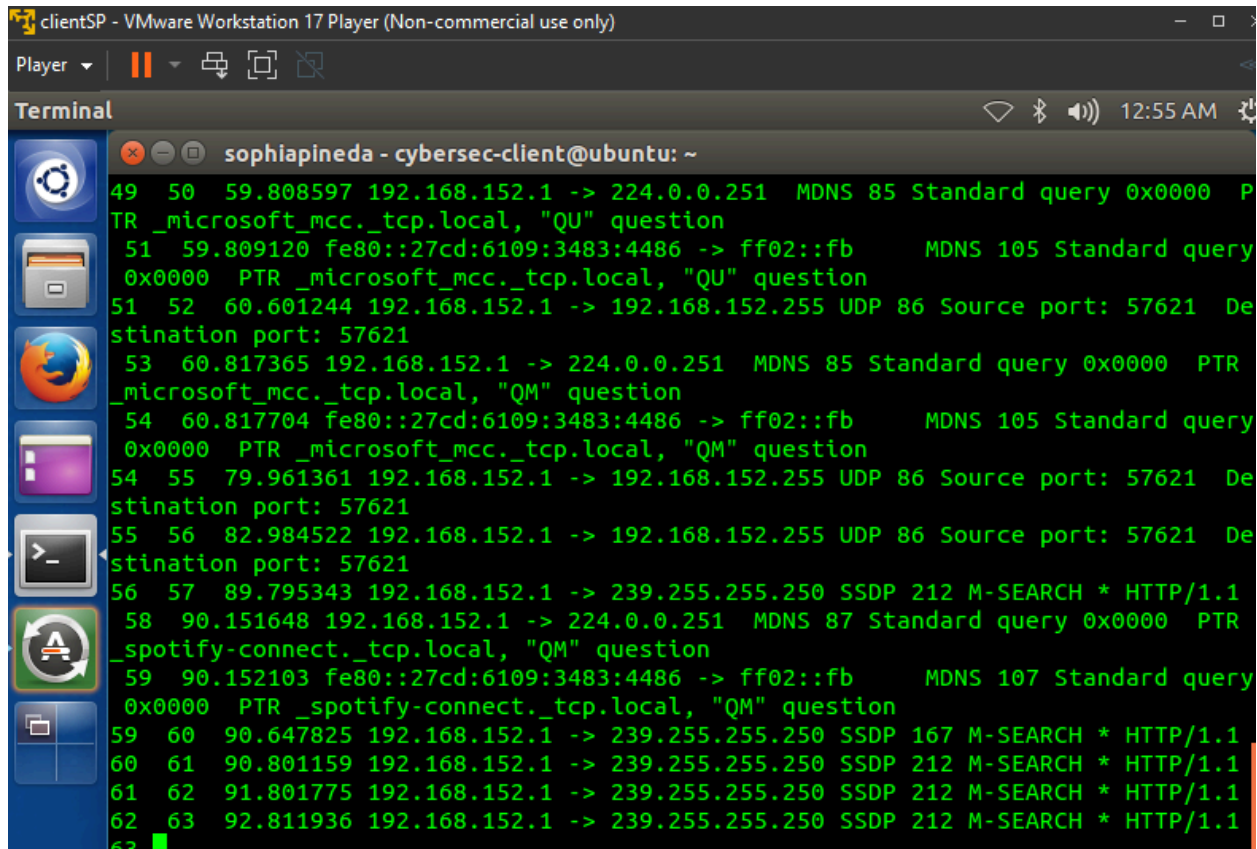
Terminal 12:55 AM [Icons]

sophiapineda - cybersec-client@ubuntu: ~

```
49 50 59.808597 192.168.152.1 -> 224.0.0.251 MDNS 85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
51 59.809120 fe80::27cd:6109:3483:4486 -> ff02::fb MDNS 105 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
51 52 60.601244 192.168.152.1 -> 192.168.152.255 UDP 86 Source port: 57621 Destination port: 57621
53 60.817365 192.168.152.1 -> 224.0.0.251 MDNS 85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" question
54 60.817704 fe80::27cd:6109:3483:4486 -> ff02::fb MDNS 105 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" question
54 55 79.961361 192.168.152.1 -> 192.168.152.255 UDP 86 Source port: 57621 Destination port: 57621
55 56 82.984522 192.168.152.1 -> 192.168.152.255 UDP 86 Source port: 57621 Destination port: 57621
56 57 89.795343 192.168.152.1 -> 239.255.255.250 SSDP 212 M-SEARCH * HTTP/1.1
58 90.151648 192.168.152.1 -> 224.0.0.251 MDNS 87 Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
59 90.152103 fe80::27cd:6109:3483:4486 -> ff02::fb MDNS 107 Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
59 60 90.647825 192.168.152.1 -> 239.255.255.250 SSDP 167 M-SEARCH * HTTP/1.1
60 61 90.801159 192.168.152.1 -> 239.255.255.250 SSDP 212 M-SEARCH * HTTP/1.1
61 62 91.801775 192.168.152.1 -> 239.255.255.250 SSDP 212 M-SEARCH * HTTP/1.1
62 63 92.811936 192.168.152.1 -> 239.255.255.250 SSDP 212 M-SEARCH * HTTP/1.1
63
```

QUESTIONS

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



```
clientSP - VMware Workstation 17 Player (Non-commercial use only)
Player
Terminal
sophiapineda - cybersec-client@ubuntu: ~
49 50 59.808597 192.168.152.1 -> 224.0.0.251 MDNS 85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
51 59.809120 fe80::27cd:6109:3483:4486 -> ff02::fb MDNS 105 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
51 52 60.601244 192.168.152.1 -> 192.168.152.255 UDP 86 Source port: 57621 Destination port: 57621
53 60.817365 192.168.152.1 -> 224.0.0.251 MDNS 85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" question
54 60.817704 fe80::27cd:6109:3483:4486 -> ff02::fb MDNS 105 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" question
54 55 79.961361 192.168.152.1 -> 192.168.152.255 UDP 86 Source port: 57621 Destination port: 57621
55 56 82.984522 192.168.152.1 -> 192.168.152.255 UDP 86 Source port: 57621 Destination port: 57621
56 57 89.795343 192.168.152.1 -> 239.255.255.250 SSDP 212 M-SEARCH * HTTP/1.1
58 90.151648 192.168.152.1 -> 224.0.0.251 MDNS 87 Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
59 90.152103 fe80::27cd:6109:3483:4486 -> ff02::fb MDNS 107 Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
59 60 90.647825 192.168.152.1 -> 239.255.255.250 SSDP 167 M-SEARCH * HTTP/1.1
60 61 90.801159 192.168.152.1 -> 239.255.255.250 SSDP 212 M-SEARCH * HTTP/1.1
61 62 91.801775 192.168.152.1 -> 239.255.255.250 SSDP 212 M-SEARCH * HTTP/1.1
62 63 92.811936 192.168.152.1 -> 239.255.255.250 SSDP 212 M-SEARCH * HTTP/1.1
63
```

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

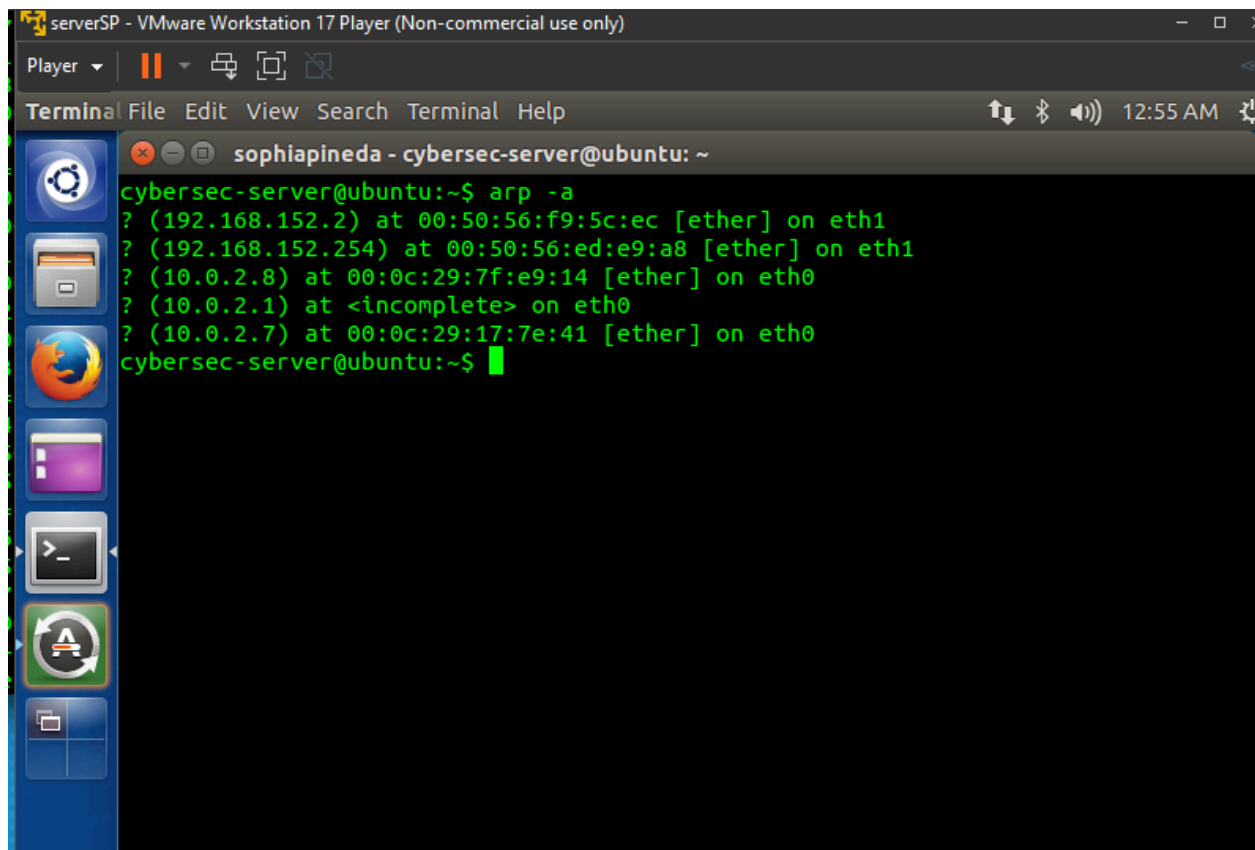
- High severity, linked to Denial of Service attack since high number of syn requests overwhelms the syn ports
- prevents the user from being able to respond to high traffic and leaves itself vulnerable

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)



serverSP - VMware Workstation 17 Player (Non-commercial use only)

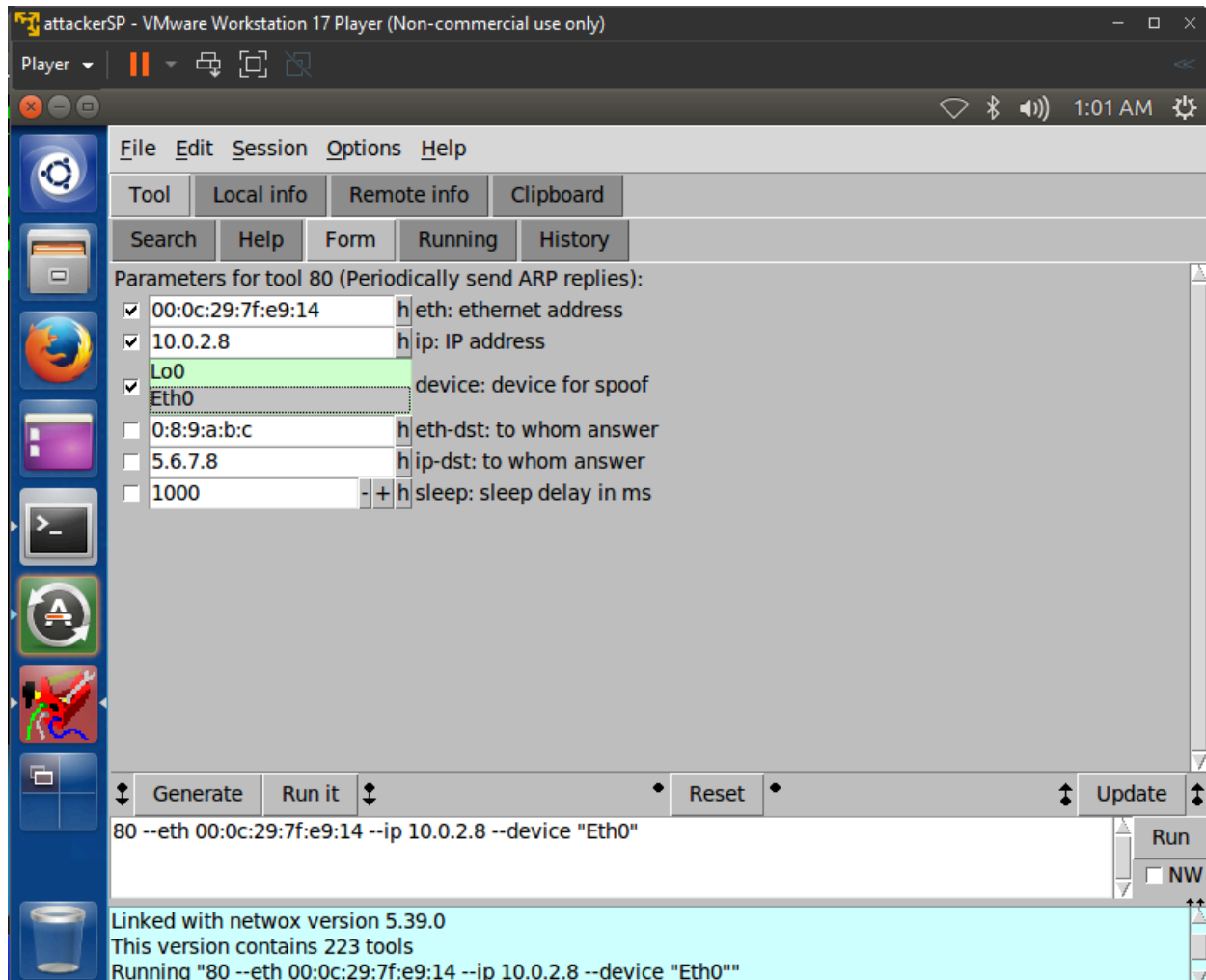
Player | [Pause] [Full Screen] [Detach]

Terminal File Edit View Search Terminal Help | [Speaker] 12:55 AM

sophiapineda - cybersec-server@ubuntu: ~

```
cybersec-server@ubuntu:~$ arp -a
? (192.168.152.2) at 00:50:56:f9:5c:ec [ether] on eth1
? (192.168.152.254) at 00:50:56:ed:e9:a8 [ether] on eth1
? (10.0.2.8) at 00:0c:29:7f:e9:14 [ether] on eth0
? (10.0.2.1) at <incomplete> on eth0
? (10.0.2.7) at 00:0c:29:17:7e:41 [ether] on eth0
cybersec-server@ubuntu:~$
```

- 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

```
serverSP - VMware Workstation 17 Player (Non-commercial use only)
Player
Terminal
sophiapineda - cybersec-server@ubuntu: ~
64 bytes from 10.0.2.8: icmp_seq=13 ttl=64 time=0.276 ms
64 bytes from 10.0.2.8: icmp_seq=14 ttl=64 time=0.238 ms
64 bytes from 10.0.2.8: icmp_seq=15 ttl=64 time=0.257 ms
64 bytes from 10.0.2.8: icmp_seq=16 ttl=64 time=0.298 ms
64 bytes from 10.0.2.8: icmp_seq=17 ttl=64 time=0.465 ms
64 bytes from 10.0.2.8: icmp_seq=18 ttl=64 time=0.344 ms
64 bytes from 10.0.2.8: icmp_seq=19 ttl=64 time=0.271 ms
^C
--- 10.0.2.8 ping statistics ---
19 packets transmitted, 19 received, 0% packet loss, time 17998ms
rtt min/avg/max/mdev = 0.238/0.288/0.465/0.052 ms
cybersec-server@ubuntu:~$ arp -a
? (192.168.152.2) at 00:50:56:f9:5c:ec [ether] on eth1
? (192.168.152.254) at 00:50:56:ed:e9:a8 [ether] on eth1
? (10.0.2.8) at 00:0c:29:7f:e9:14 [ether] on eth0
? (10.0.2.1) at <incomplete> on eth0
? (10.0.2.7) at 00:0c:29:17:7e:41 [ether] on eth0
cybersec-server@ubuntu:~$ arp -a
? (192.168.152.2) at 00:50:56:f9:5c:ec [ether] on eth1
? (192.168.152.254) at 00:50:56:ed:e9:a8 [ether] on eth1
? (10.0.2.8) at 00:0c:29:7f:e9:14 [ether] on eth0
? (10.0.2.1) at <incomplete> on eth0
? (10.0.2.7) at 00:0c:29:17:7e:41 [ether] on eth0
cybersec-server@ubuntu:~$
```

2. Comment

- Address changed, modified by attacker

3. Describe mitigation techniques

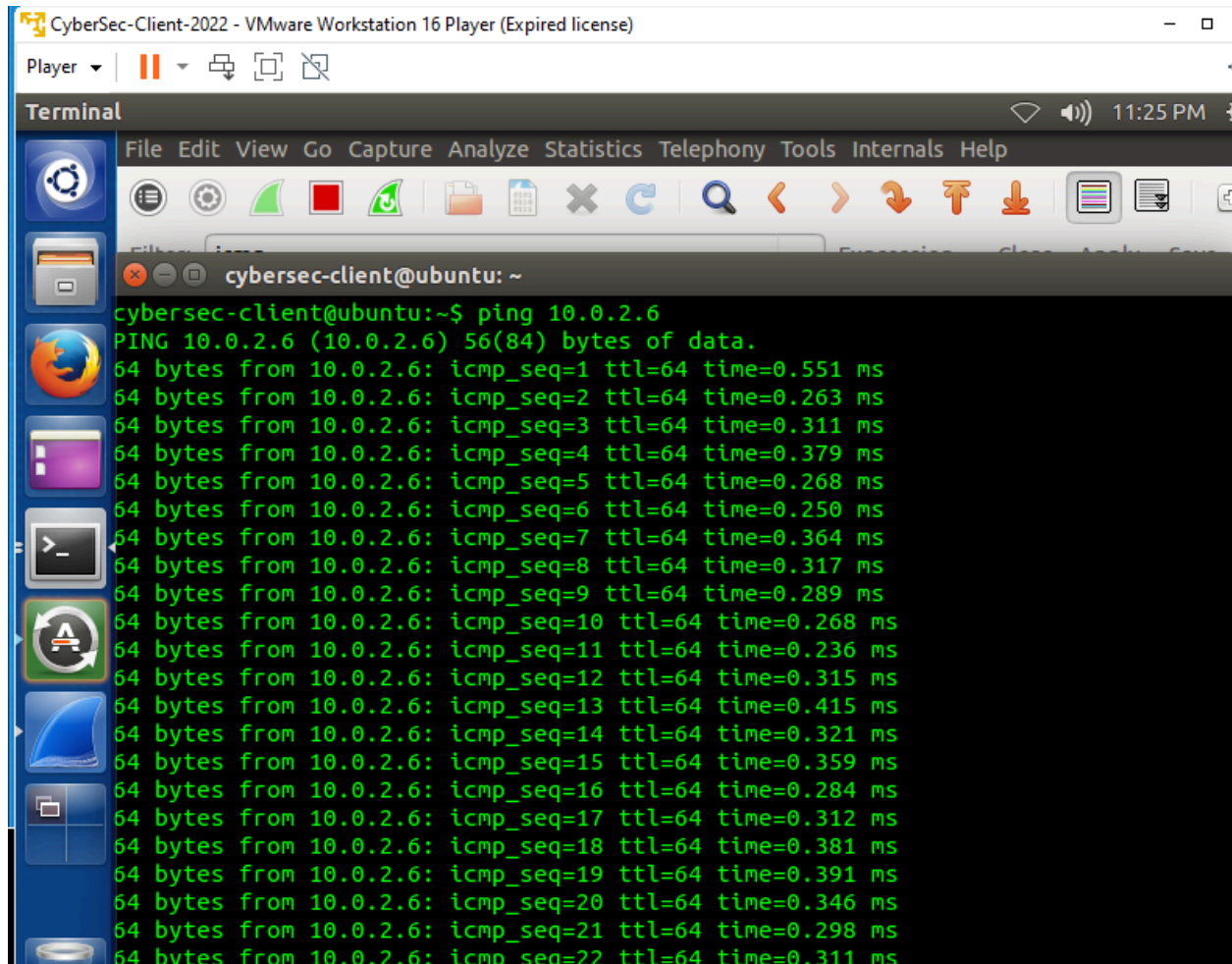
- Static ARP Tables - map all MAC addresses to designated IP address
- Switch Security
- Network Isolation
- Encryption - MAC addresses hidden

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

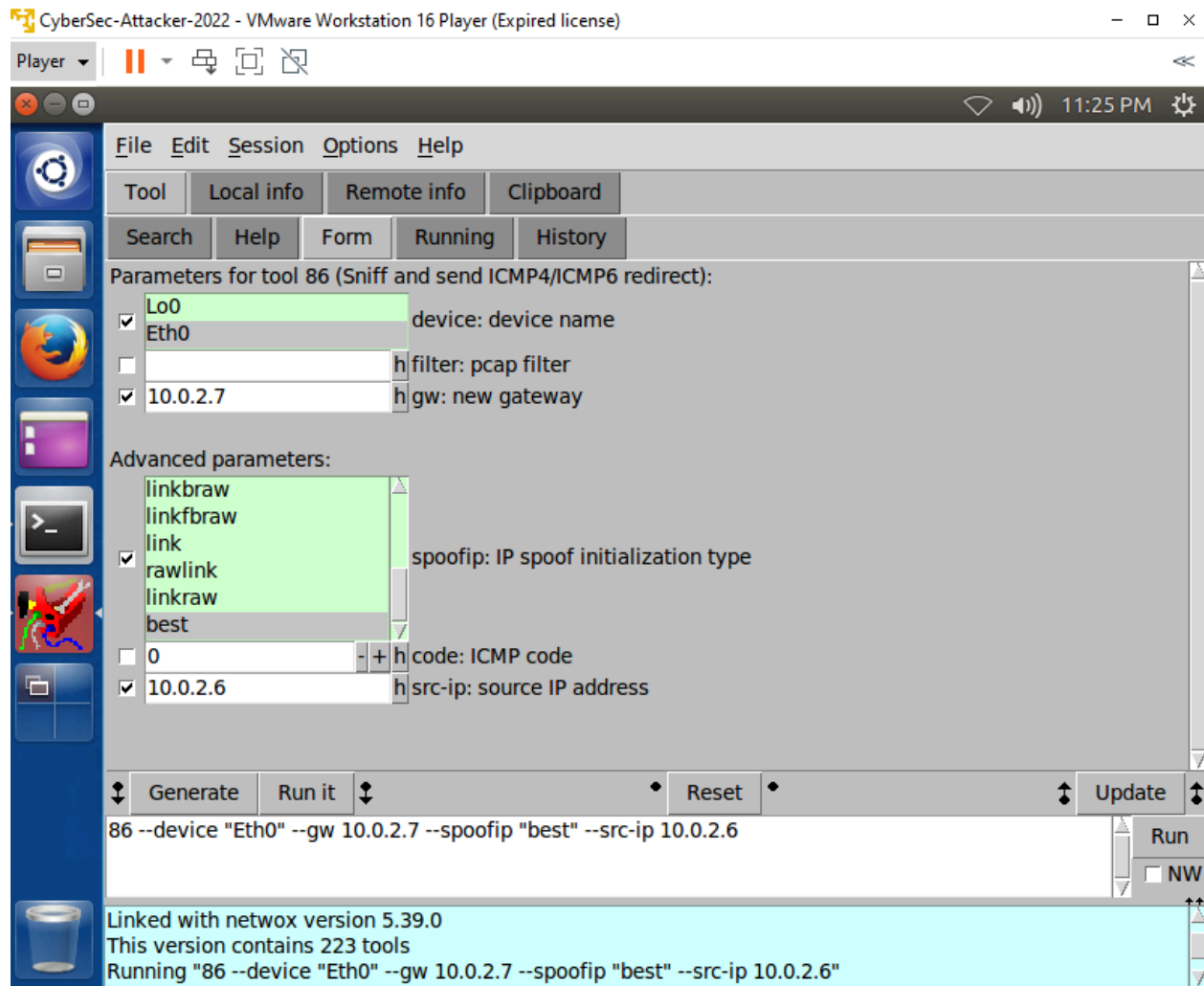
STEPS

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



```
cybersec-client@ubuntu:~$ ping 10.0.2.6
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data.
64 bytes from 10.0.2.6: icmp_seq=1 ttl=64 time=0.551 ms
64 bytes from 10.0.2.6: icmp_seq=2 ttl=64 time=0.263 ms
64 bytes from 10.0.2.6: icmp_seq=3 ttl=64 time=0.311 ms
64 bytes from 10.0.2.6: icmp_seq=4 ttl=64 time=0.379 ms
64 bytes from 10.0.2.6: icmp_seq=5 ttl=64 time=0.268 ms
64 bytes from 10.0.2.6: icmp_seq=6 ttl=64 time=0.250 ms
64 bytes from 10.0.2.6: icmp_seq=7 ttl=64 time=0.364 ms
64 bytes from 10.0.2.6: icmp_seq=8 ttl=64 time=0.317 ms
64 bytes from 10.0.2.6: icmp_seq=9 ttl=64 time=0.289 ms
64 bytes from 10.0.2.6: icmp_seq=10 ttl=64 time=0.268 ms
64 bytes from 10.0.2.6: icmp_seq=11 ttl=64 time=0.236 ms
64 bytes from 10.0.2.6: icmp_seq=12 ttl=64 time=0.315 ms
64 bytes from 10.0.2.6: icmp_seq=13 ttl=64 time=0.415 ms
64 bytes from 10.0.2.6: icmp_seq=14 ttl=64 time=0.321 ms
64 bytes from 10.0.2.6: icmp_seq=15 ttl=64 time=0.359 ms
64 bytes from 10.0.2.6: icmp_seq=16 ttl=64 time=0.284 ms
64 bytes from 10.0.2.6: icmp_seq=17 ttl=64 time=0.312 ms
64 bytes from 10.0.2.6: icmp_seq=18 ttl=64 time=0.381 ms
64 bytes from 10.0.2.6: icmp_seq=19 ttl=64 time=0.391 ms
64 bytes from 10.0.2.6: icmp_seq=20 ttl=64 time=0.346 ms
64 bytes from 10.0.2.6: icmp_seq=21 ttl=64 time=0.298 ms
64 bytes from 10.0.2.6: icmp_seq=22 ttl=64 time=0.311 ms
```

- 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)

CyberSec-Client-2022 - VMware Workstation 16 Player (Expired license)

Player

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: icmp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
942	133.69174900	Vmware_61:67:82	Broadcast	ARP	60	Who has
943	133.99401400	Vmware_61:67:82	Broadcast	ARP	60	Who has
944	134.00604500	10.0.2.8	10.0.2.6	ICMP	98	Echo (pi
945	134.00633200	10.0.2.6	10.0.2.8	ICMP	98	Echo (pi
946	134.29517200	10.0.2.6	10.0.2.8	ICMP	70	Redirect
947	134.29519400	10.0.2.6	10.0.2.6	ICMP	70	Redirect
948	134.58033500	192.112.36.4	192.168.30.144	TCP	60	domain >
949	134.58050400	192.168.30.144	192.112.36.4	TCP	60	58307 >
950	134.60824900	Vmware_61:67:82	Broadcast	ARP	60	Who has
951	134.68654600	Vmware_61:67:82	Broadcast	ARP	60	Who has
952	134.87657400	192.168.30.144	128.63.2.53	DNS	60	Standard
953	134.90943200	Vmware_61:67:82	Broadcast	ARP	60	Who has
954	135.00703000	10.0.2.8	10.0.2.6	ICMP	98	Echo (pi
955	135.00737300	10.0.2.6	10.0.2.8	ICMP	98	Echo (pi
956	135.21190900	Vmware_61:67:82	Broadcast	ARP	60	Who has
957	135.51306100	Vmware_61:67:82	Broadcast	ARP	60	Who has
958	135.68794400	Vmware_61:67:82	Broadcast	ARP	60	Who has
959	135.82199900	10.0.2.6	10.0.2.8	ICMP	70	Redirect
960	135.82205500	10.0.2.6	10.0.2.6	ICMP	70	Redirect
961	136.00674200	10.0.2.8	10.0.2.6	ICMP	98	Echo (pi
962	136.00714000	10.0.2.6	10.0.2.8	ICMP	98	Echo (pi

QUESTIONS

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

CyberSec-Client-2022 - VMware Workstation 16 Player (Expired license)

Player

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: icmp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
942	133.69174900	Vmware_61:67:82	Broadcast	ARP	60	Who has
943	133.99401400	Vmware_61:67:82	Broadcast	ARP	60	Who has
944	134.00604500	10.0.2.8	10.0.2.6	ICMP	98	Echo (pi
945	134.00633200	10.0.2.6	10.0.2.8	ICMP	98	Echo (pi
946	134.29517200	10.0.2.6	10.0.2.8	ICMP	70	Redirect
947	134.29519400	10.0.2.6	10.0.2.6	ICMP	70	Redirect
948	134.58033500	192.112.36.4	192.168.30.144	TCP	60	domain >
949	134.58050400	192.168.30.144	192.112.36.4	TCP	60	58307 >
950	134.60824900	Vmware_61:67:82	Broadcast	ARP	60	Who has
951	134.68654600	Vmware_61:67:82	Broadcast	ARP	60	Who has
952	134.87657400	192.168.30.144	128.63.2.53	DNS	60	Standard
953	134.90943200	Vmware_61:67:82	Broadcast	ARP	60	Who has
954	135.00703000	10.0.2.8	10.0.2.6	ICMP	98	Echo (pi
955	135.00737300	10.0.2.6	10.0.2.8	ICMP	98	Echo (pi
956	135.21190900	Vmware_61:67:82	Broadcast	ARP	60	Who has
957	135.51306100	Vmware_61:67:82	Broadcast	ARP	60	Who has
958	135.68794400	Vmware_61:67:82	Broadcast	ARP	60	Who has
959	135.82199900	10.0.2.6	10.0.2.8	ICMP	70	Redirect
960	135.82205500	10.0.2.6	10.0.2.6	ICMP	70	Redirect
961	136.00674200	10.0.2.8	10.0.2.6	ICMP	98	Echo (pi
962	136.00714000	10.0.2.6	10.0.2.8	ICMP	98	Echo (pi

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