COMP 4670

Tutorials

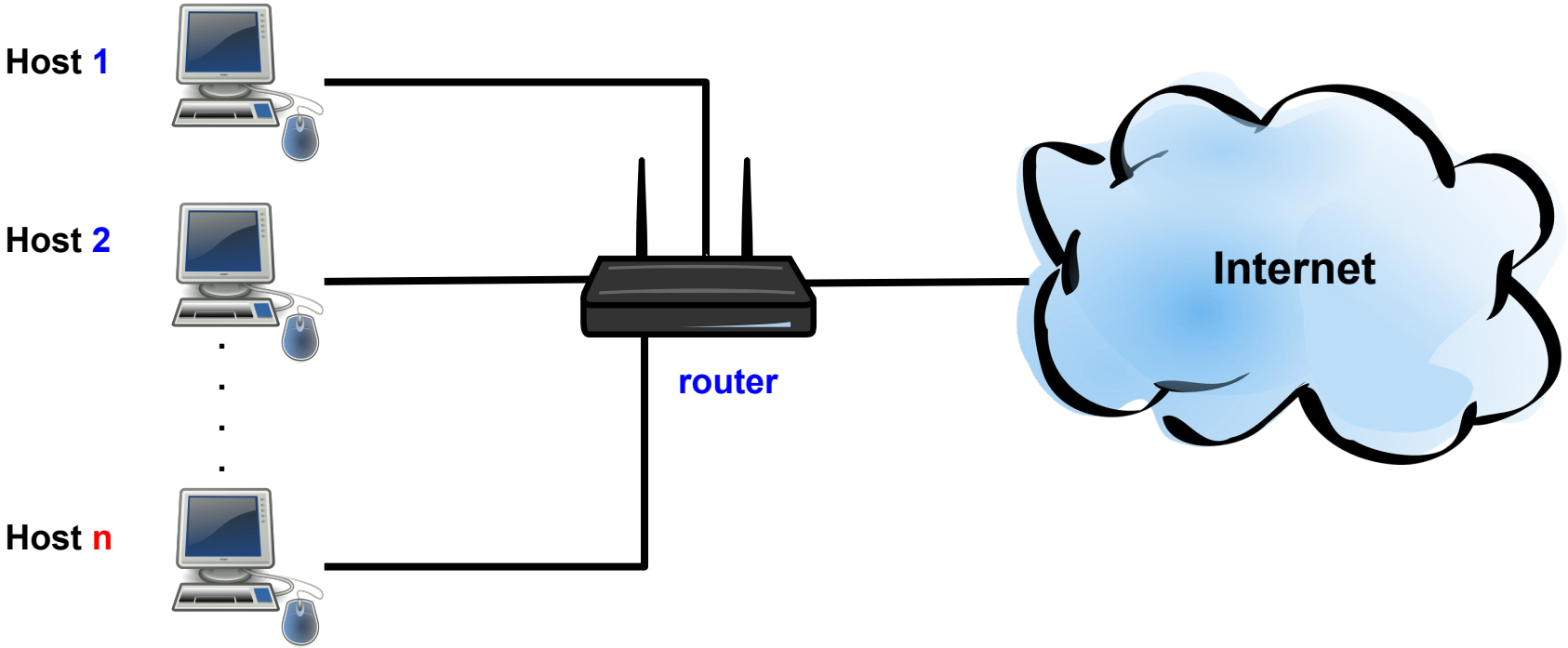
Network Attacks Part 1

Dr. Sherif Saad

Attacks List

1. Network Mapping in IP Layer
2. Spoofing Attacks in Network Layer
3. DOS Attack in Network Layer
4. Network Mapping and Service Discovery

Target Network: Local Area Network



The Attacker

- Someone with malicious intention who is connected to the same network as his targets (victims).
- He is interested in eavesdropping (spying on other hosts in the same network), preventing other hosts from accessing the internet.
- The attacker could connect to the target network over a wired or wireless connection.

ARP Spoofing: Attack Overview

- An ARP spoofing attack takes advantages of the Address Resolution Protocol workflow.
- The attacker spoof the MAC address of one of the hosts (nodes) on the same LAN and link his IP address to the spoofed MAC address.
- The ability to spoof the MAC address of another host enables the attacker to eavesdrop the communication between this host and other hosts on the network, disconnect the host from the network, or limits the ability of the host to connect to specific hosts.

How is the ARP work?

Host Name H1
IP Address 192.168.0.101
MAC 90:CD:B6:40:45:F7

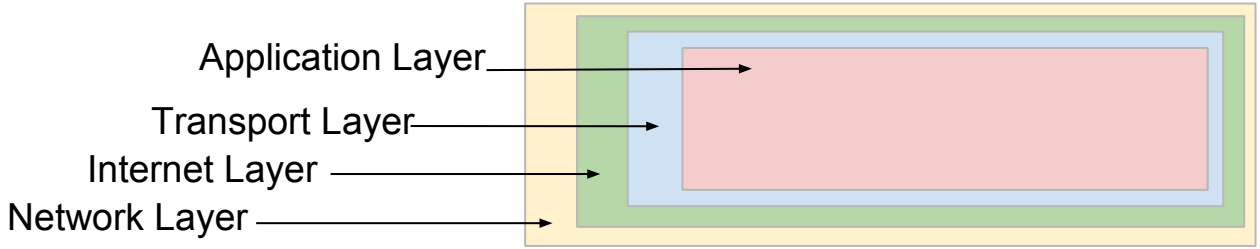
Host Name H2
IP Address 192.168.0.107
MAC 81:AC:F1:51:31:H3

- The two hosts (H1 & H2) are on the same local area network, each host has a unique IP address (logical address) and unique MAC address (physical address)
- Let assume that that H1 wants to send a message to H2. The are connected to a TCP/IP network over ethernet

How is the ARP work?

Host Name H1
IP Address 192.168.0.101
MAC 90:CD:B6:40:45:F7

Host Name H2
IP Address 192.168.0.107
MAC 81:AC:F1:51:31:H3



How is the ARP work?

Host Name H1
IP Address 192.168.0.101
MAC 90:CD:B6:40:45:F7

Host Name H2
IP Address 192.168.0.107
MAC 81:AC:F1:51:31:H3

Source MAC: 90:CD:B6:40:45:F7

Destination MAC:?? ?? ?? ?? ?? ??

Source IP: 192.168.0.101
Destination IP: 192.168.0.107

Network Layer

Internet Layer

How is the ARP work?

Host Name H1
IP Address 192.168.0.101
MAC 90:CD:B6:40:45:F7

Host Name H2
IP Address 192.168.0.107
MAC 81:AC:F1:51:31:H3

- H1 needs to know the MAC address of H2 to add it to the ethernet frame header, otherwise H1 will not be able to send the message to H2.
- H1 will use ARP to discover the MAC address of H2
- Every host has an ARP table this ARP table simply maps IP addresses to MAC addresses.
- When H1 attempts to send a message to H2. H1 will check his ARP table to retrieve H2 MAC address. If H1 did not find H2 MAC address it will create an ARP request

How is the ARP work?

Host Name H1
IP Address 192.168.0.101
MAC 90:CD:B6:40:45:F7

Host Name H2
IP Address 192.168.0.107
MAC 81:AC:F1:51:31:H3

IP Address	MAC
192.168.0.102	F1:95:F2:AC:19:B7

ARP Table of H1

How is the ARP work?

Host Name H1
IP Address 192.168.0.101
MAC 90:CD:B6:40:45:F7

Host Name H2
IP Address 192.168.0.107
MAC 81:AC:F1:51:31:H3

IP Address	MAC
192.168.0.102	F1:95:F2:AC:19:B7

ARP Table of H1

1. H1 did not find the MAC address of H2 in his ARP table.
2. H1 creates an ARP request and broadcast this ARP request to the Network (LAN).
3. Simply asking the host with the 192.168.0.107 to send its MAC address as a reply to his ARP request.

How is the ARP work?

Host Name H1
IP Address 192.168.0.101
MAC 90:CD:B6:40:45:F7

Host Name H2
IP Address 192.168.0.107
MAC 81:AC:F1:51:31:H3

1. When H2 receives the ARP request from H1. It will add H1 MAC address and IP address its ARP Table.
2. Then it will create an ARP response that includes H2 MAC address and sends it to H1.
3. When H1 receives the response it will update its ARP table

IP Address	MAC
192.168.0.102	F1:95:F2:AC:19:B7
192.168.0.105	A1:17:C5:FC:91:D1
192.168.0.101	90:CD:B6:40:45:F7

ARP Table of H2

How is the ARP work?

Host Name H1
IP Address 192.168.0.101
MAC 90:CD:B6:40:45:F7

Host Name H2
IP Address 192.168.0.107
MAC 81:AC:F1:51:31:H3

IP Address	MAC
192.168.0.102	F1:95:F2:AC:19:B7
192.168.0.107	81:AC:F1:51:31:H3

ARP Table of H1

IP Address	MAC
192.168.0.102	F1:95:F2:AC:19:B7
192.168.0.105	A1:17:C5:FC:91:D1
192.168.0.101	90:CD:B6:40:45:F7

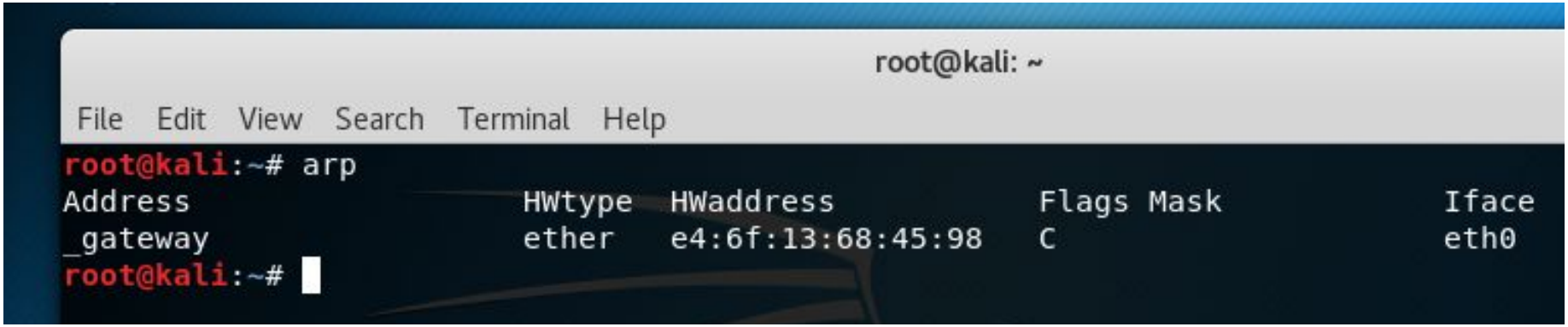
ARP Table of H2

ARP Spoofing: How-To ??

1. The attacker is connected to the network.
2. The attacker is using a Linux box (e.g. Kali Linux).
3. The attacker needs to probe the network and discover live hosts (currently connect hosts) and select his target.

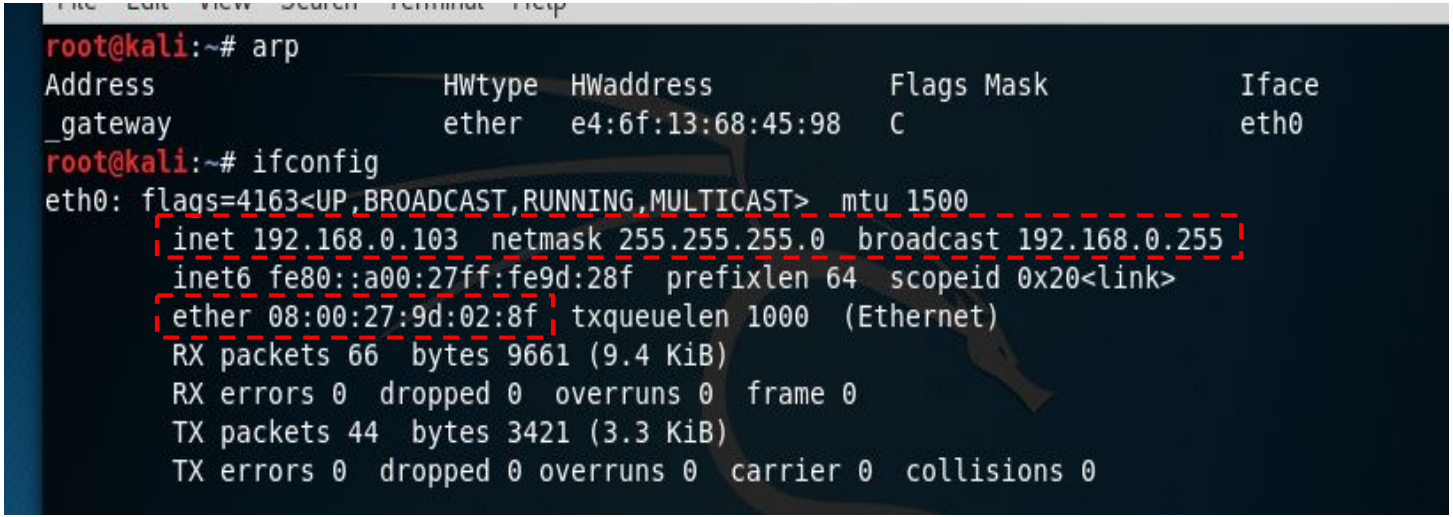
STEP-01: Probing the Network

The attacker uses the command **arp** to display his machine arp table. At this point the table only contains the MAC address of the network gateway



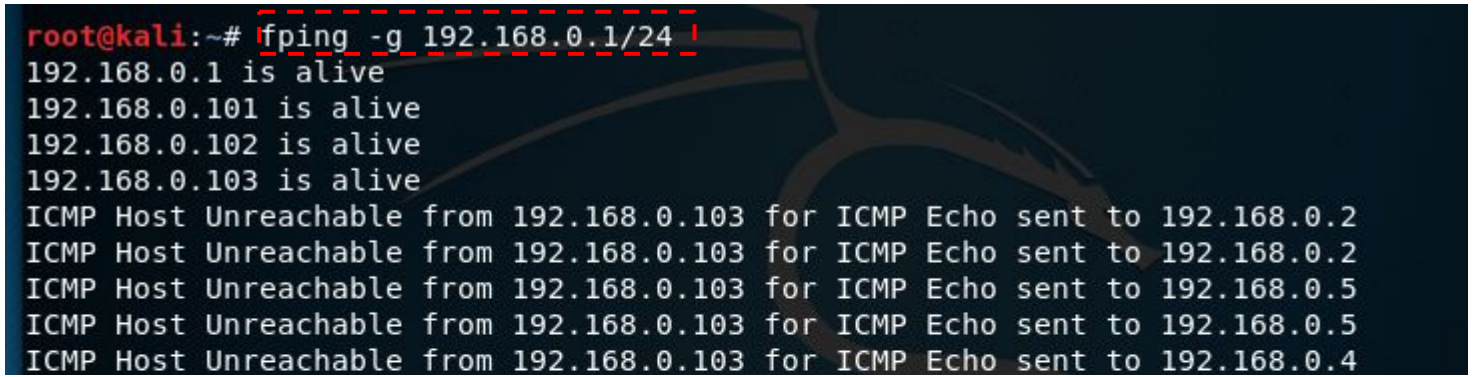
STEP-01: Probing the Network

The attacker uses the command **ifconfig** to display his machine IP address, the network broadcast address, network mahis MAC address and other information



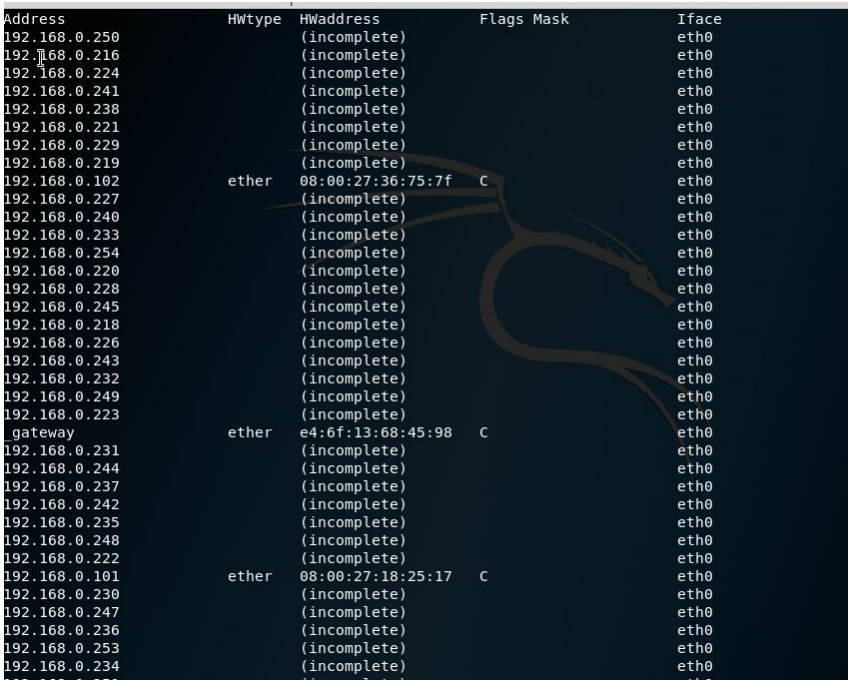
STEP-01: Probing the Network

The attacker uses fping -g 192.168.0.1/24 to send an ICMP ECHO Request to every potential host on the network. (This known as ICMP Sweep or Ping Sweep). Any live Host will return an ICMP ECHO Reply.



STEP-01: Probing the Network

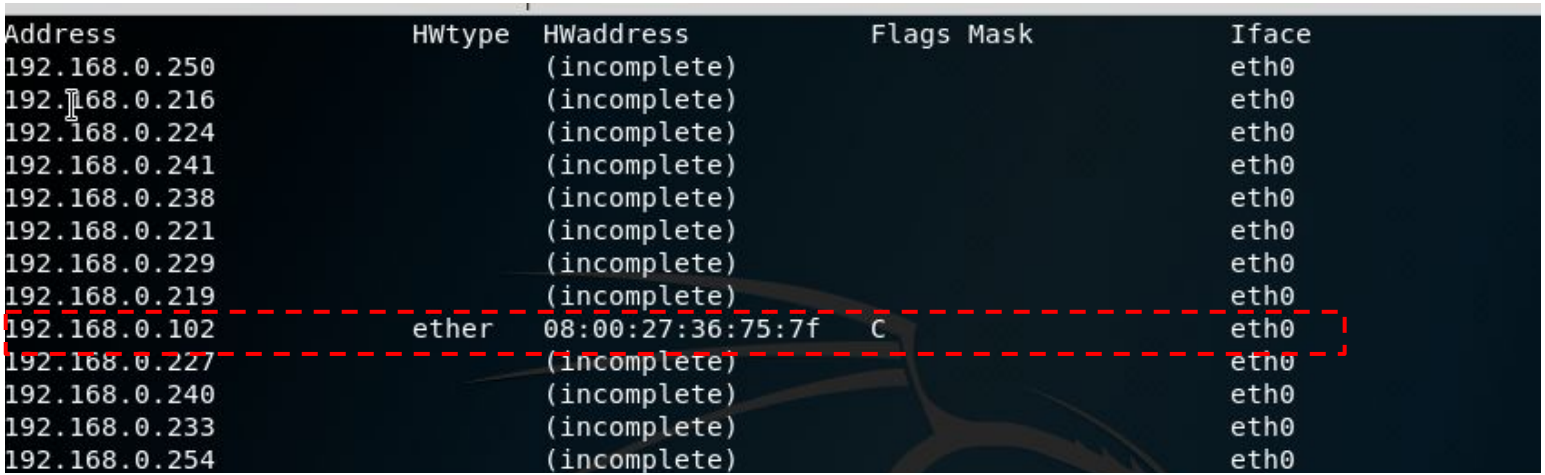
Again, the attacker uses the command **arp** to display his machine arp table.



Address	HWtype	HWaddress	Flags Mask	Iface
192.168.0.250		(incomplete)		eth0
192.168.0.216		(incomplete)		eth0
192.168.0.224		(incomplete)		eth0
192.168.0.241		(incomplete)		eth0
192.168.0.238		(incomplete)		eth0
192.168.0.221		(incomplete)		eth0
192.168.0.229		(incomplete)		eth0
192.168.0.219		(incomplete)		eth0
192.168.0.102	ether	08:00:27:36:75:7f	C	eth0
192.168.0.227		(incomplete)		eth0
192.168.0.240		(incomplete)		eth0
192.168.0.233		(incomplete)		eth0
192.168.0.254		(incomplete)		eth0
192.168.0.220		(incomplete)		eth0
192.168.0.228		(incomplete)		eth0
192.168.0.245		(incomplete)		eth0
192.168.0.218		(incomplete)		eth0
192.168.0.226		(incomplete)		eth0
192.168.0.243		(incomplete)		eth0
192.168.0.232		(incomplete)		eth0
192.168.0.249		(incomplete)		eth0
192.168.0.223		(incomplete)		eth0
_gateway	ether	e4:6f:13:68:45:98	C	eth0
192.168.0.231		(incomplete)		eth0
192.168.0.244		(incomplete)		eth0
192.168.0.237		(incomplete)		eth0
192.168.0.242		(incomplete)		eth0
192.168.0.235		(incomplete)		eth0
192.168.0.248		(incomplete)		eth0
192.168.0.222		(incomplete)		eth0
192.168.0.101	ether	08:00:27:18:25:17	C	eth0
192.168.0.230		(incomplete)		eth0
192.168.0.247		(incomplete)		eth0
192.168.0.236		(incomplete)		eth0
192.168.0.253		(incomplete)		eth0
192.168.0.234		(incomplete)		eth0

STEP-01: Probing the Network

Again, the attacker uses the command **arp** to display his machine arp table.



```
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.0.250                    (incomplete)                              eth0
192.168.0.216                    (incomplete)                              eth0
192.168.0.224                    (incomplete)                              eth0
192.168.0.241                    (incomplete)                              eth0
192.168.0.238                    (incomplete)                              eth0
192.168.0.221                    (incomplete)                              eth0
192.168.0.229                    (incomplete)                              eth0
192.168.0.219                    (incomplete)                              eth0
192.168.0.102            ether   08:00:27:36:75:7f   C                     eth0
192.168.0.227                    (incomplete)                              eth0
192.168.0.240                    (incomplete)                              eth0
192.168.0.233                    (incomplete)                              eth0
192.168.0.254                    (incomplete)                              eth0
```

STEP-01: Probing the Network

What did the attacker learn so far?

```
root@kali:~# fping -g 192.168.0.1/24
192.168.0.1 is alive
192.168.0.101 is alive
192.168.0.102 is alive
192.168.0.103 is alive
ICMP Host Unreachable from 192.168.0.
ICMP Host Unreachable from 192.168.0.
```

```
192.168.0.229                    (incomplete)
192.168.0.219                    (incomplete)
192.168.0.102            ether   08:00:27:36:75:7f   C
192.168.0.227                    (incomplete)
192.168.0.240                    (incomplete)
192.168.0.233                    (incomplete)
```

```
_gateway                 ether   e4:6f:13:68:45:98   C                     et
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.103  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe9d:28f  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:9d:02:8f  txqueuelen 1000  (Ethernet)
```

STEP-01: Probing the Network

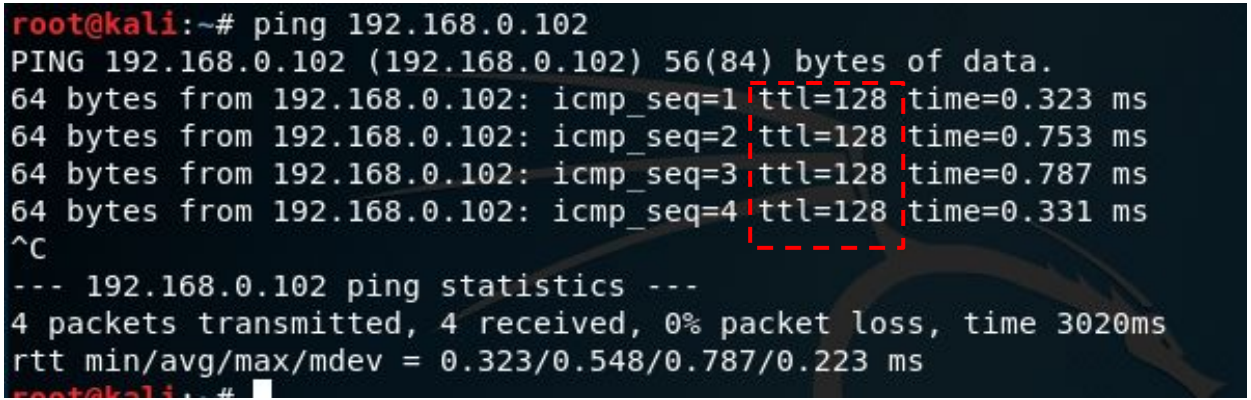
What did the attacker learn so far?

1. There are only 4 live hosts on the network (the attacker machine is one of them).
2. The attacker knows the IP addresses of the other hosts and the MAC address associated with each IP address.

STEP-01: Probing the Network

The attacker use ping command (send ICMP ECHO request to single host) to pings the other host on the network.

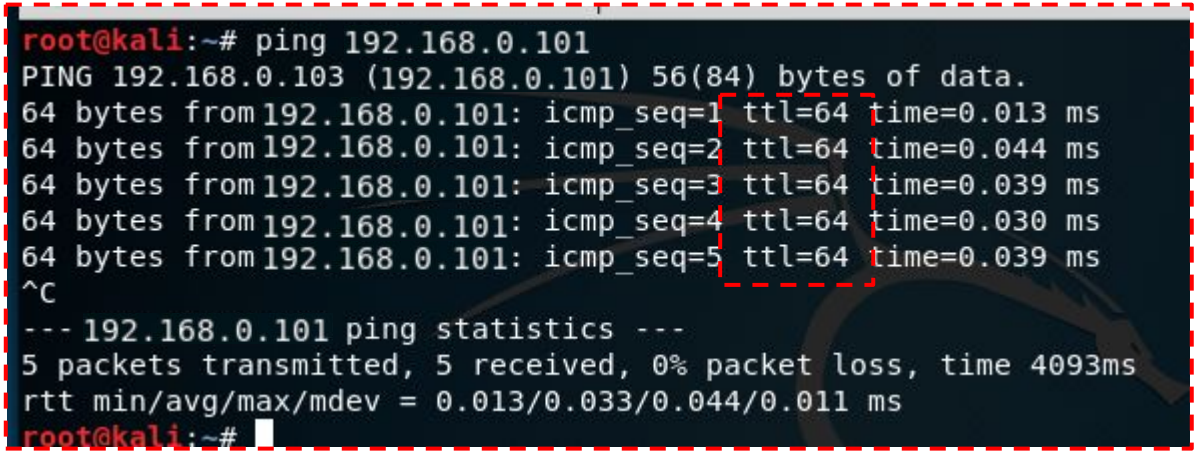
Ping 192.168.0.102



STEP-01: Probing the Network

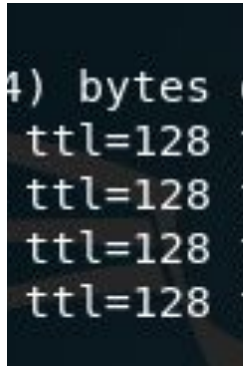
The attacker use ping command (send ICMP ECHO request to single host) to pings the other host on the network.

Ping 192.168.0.101

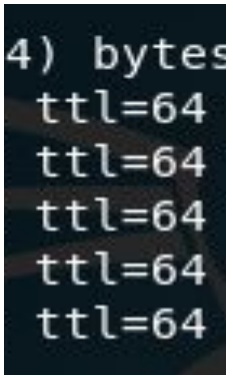


STEP-01: Probing the Network

- Time-to-live (TTL) is a value in an Internet Protocol (IP) packet that tells a network router whether or not the packet has been in the network too long and should be discarded.
- An IP TTL is set initially by the system sending the packet. It can be set to any value between 1 and 255
- Different operating systems set different defaults.



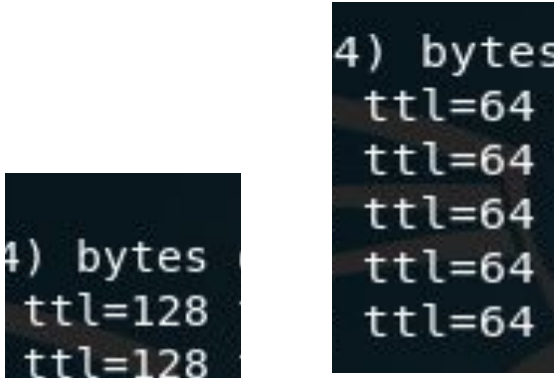
192.168.0.102



192.168.0.101

STEP-01: Probing the Network

- Each router that receives the packet subtracts at least 1 from the count; if the count remains greater than 0, the router forwards the packet, otherwise it discards it and sends an Internet Control Message Protocol (ICMP) message back to the originating host.



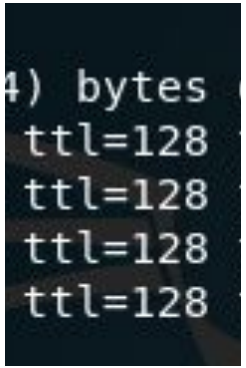
192.168.0.101

192.168.0.102

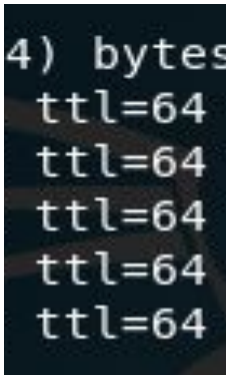
STEP-01: Probing the Network

- TTL could be used to guess the host operating system (OS Fingerprint).

OS	TTL	Window size (bytes)
Linux 2.4 and 2.6	64	5,840
Google customized Linux	64	5,720
Linux kernel 2.2	64	32,120
FreeBSD	64	65,535
OpenBSD, AIX 4.3	64	16,384
Windows 2000	128	16,384
Windows XP	128	65,535
Windows 7, Vista, and Server 8	128	8,192
Cisco Router IOS 12.4	255	4,128
Solaris 7	255	8,760
MAC	64	65,535



192.168.0.10
Window Host



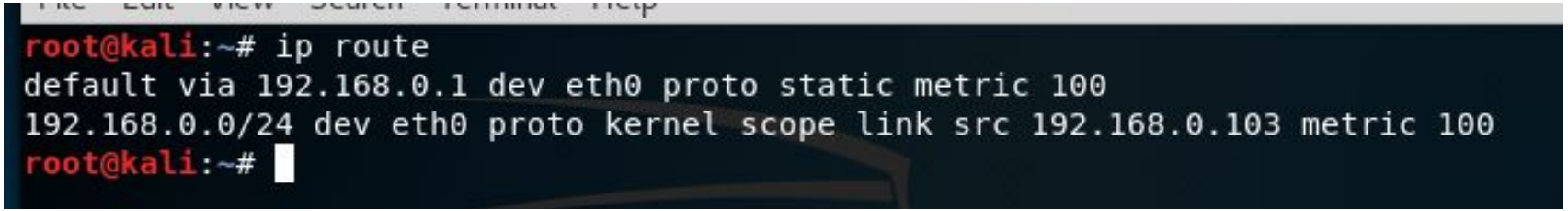
192.168.0.101
Linux Host

STEP-02: ARP Spoofing

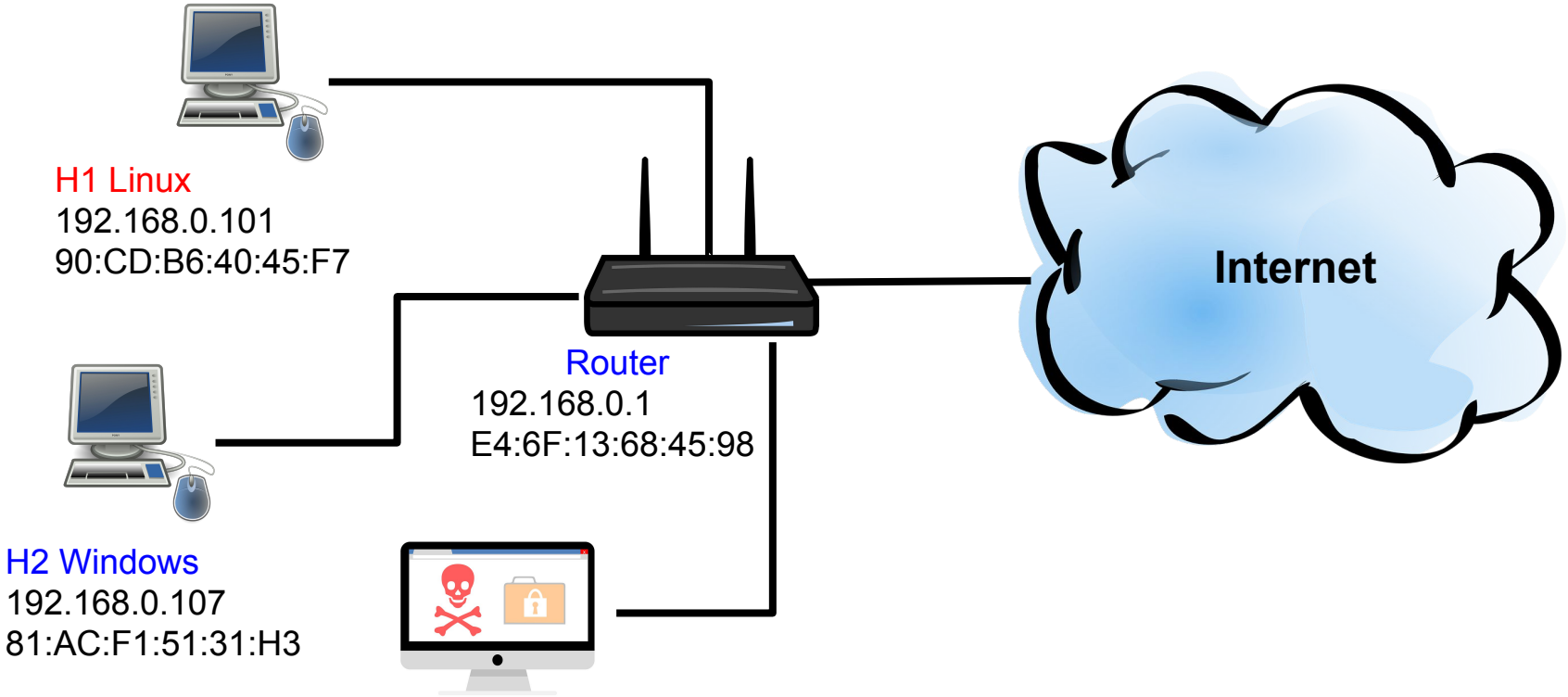
1. The attacker decided to attacks the Windows machine
2. Since there are only 2 hosts in the network in addition to the attacker the attacker will use ARP spoofing to trick the Windsor machine to believes that the attacker machine is the network router.
3. The attacker will like his IP to the MAC address of the network router. Only the victim machine will see this link.
4. The attacker will send an ARP message (announcement) only to the Victim machine that links attacker MAC address to the Router IP address.

STEP-02: ARP Spoofing

The attacker needs to confirm that he/she knows the router IP address. The attacker use the command **ip route**

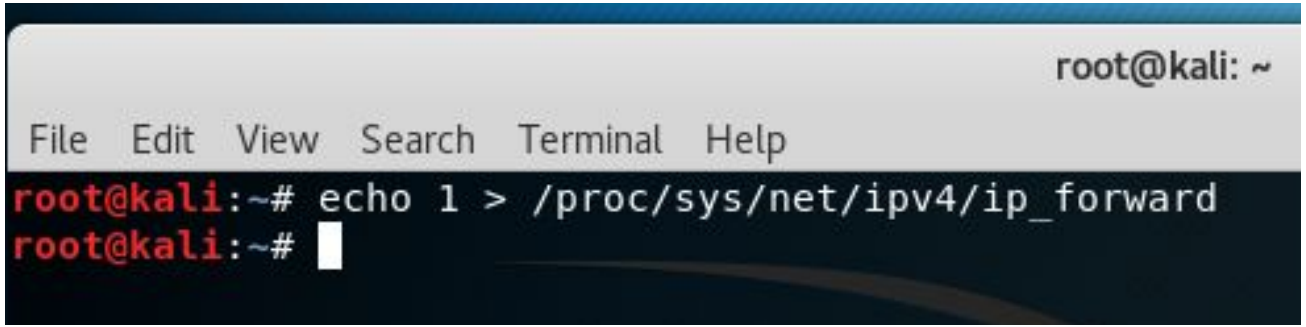


Target Network: Local Area Network



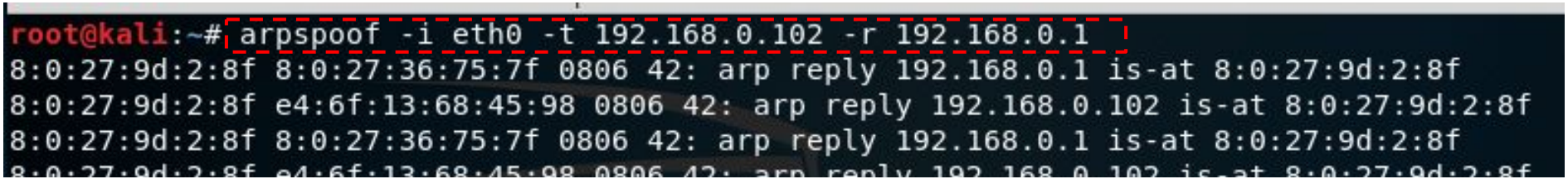
STEP-02: ARP Spoofing

- The attacker will enable IP Forwarding on his machine.
- IP forwarding also known as Internet routing is a process used to determine which path a packet or datagram can be sent.
- The attacker will use the following command to enable his machine to forward IP packets.



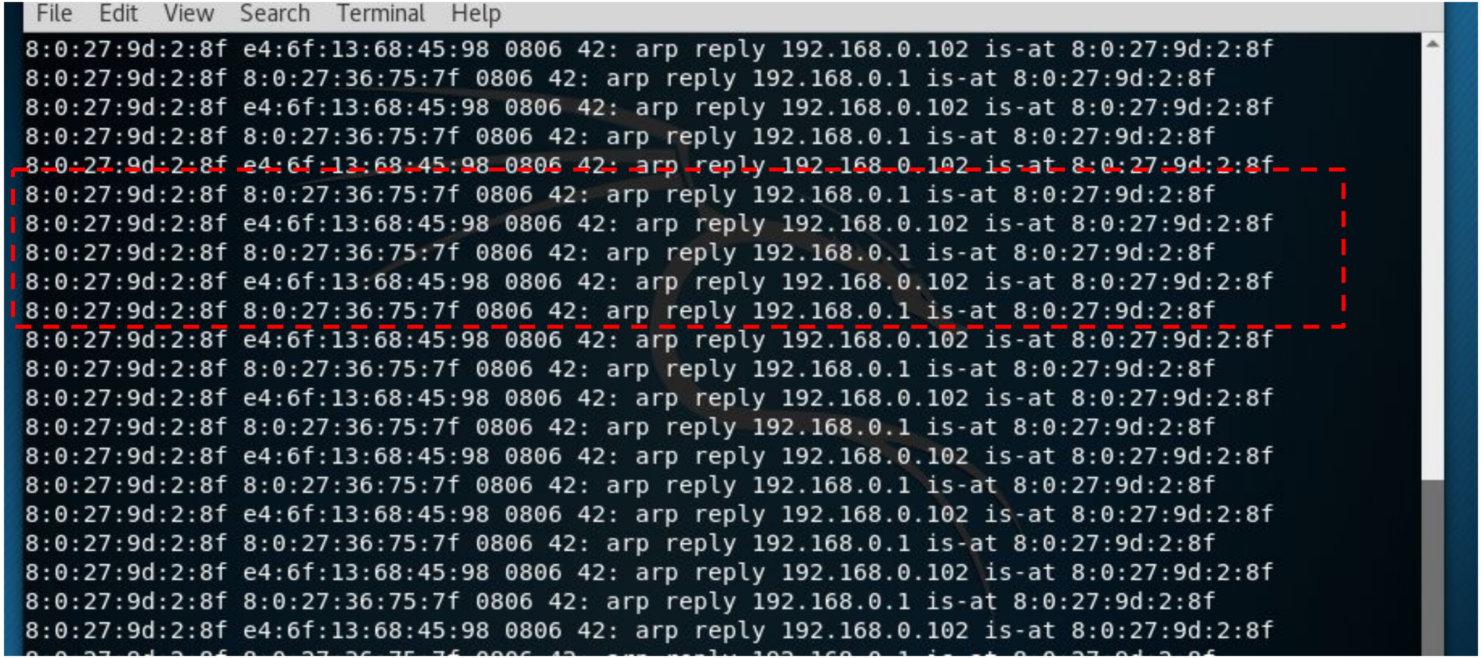
STEP-02: ARP Spoofing

- After enabling IP Forwarding, the attacker will use a malicious tool to send crafted ARP malicious messages to the target claiming that the attacker MAC address is the MAC address of the network router
- The attacker use ARPSPOOF tool (available on Kali Linux)



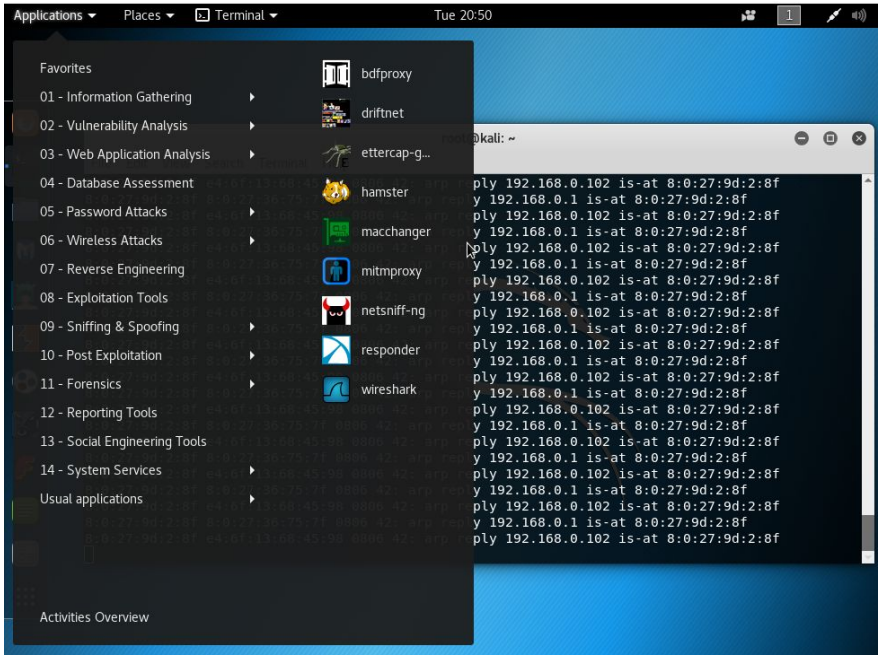
STEP-02: ARP Spoofing

- The tool will continue sending the crafted ARP reply over and over



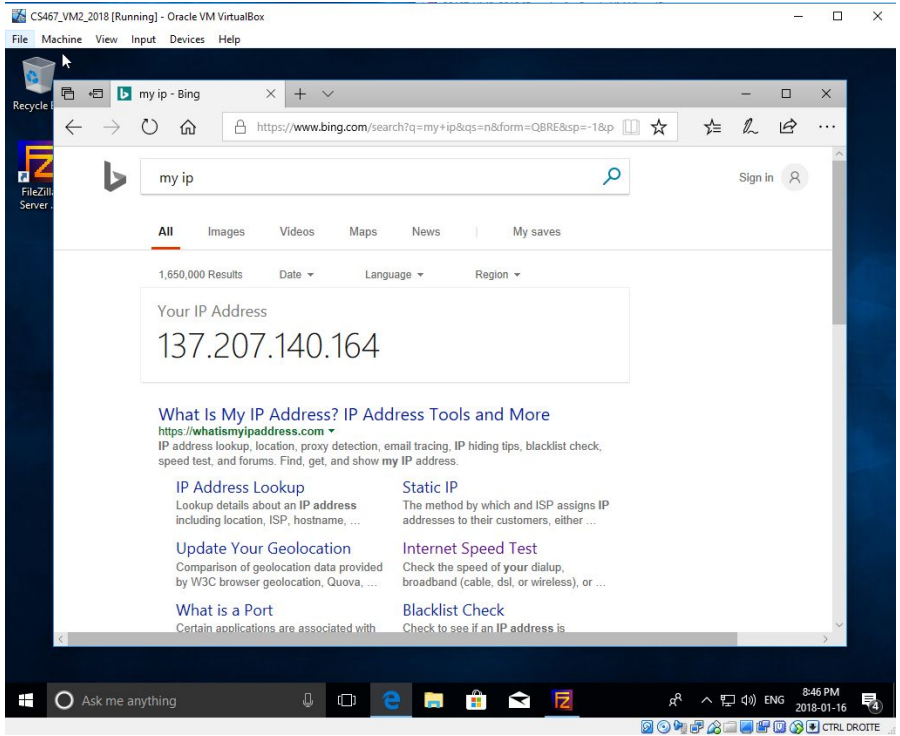
STEP-03: Man-in-the-Middle (eavesdropping)

- Now all the network traffic sent from the victim to the internet goes to the attacker machine.
- The attacker could use a network sniffer to capture and record all the network traffic.

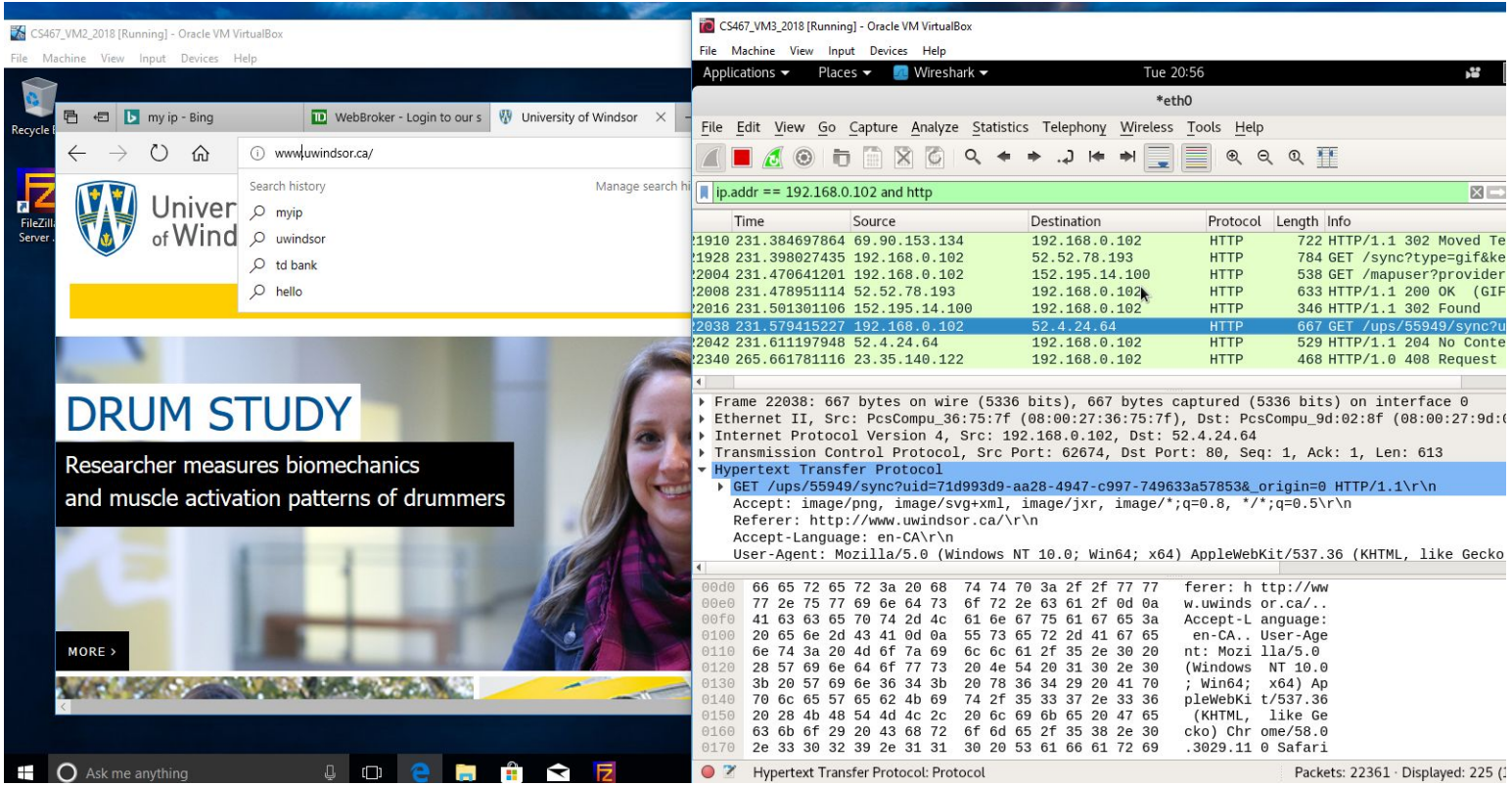


STEP-03: Man-in-the-Middle (eavesdropping)

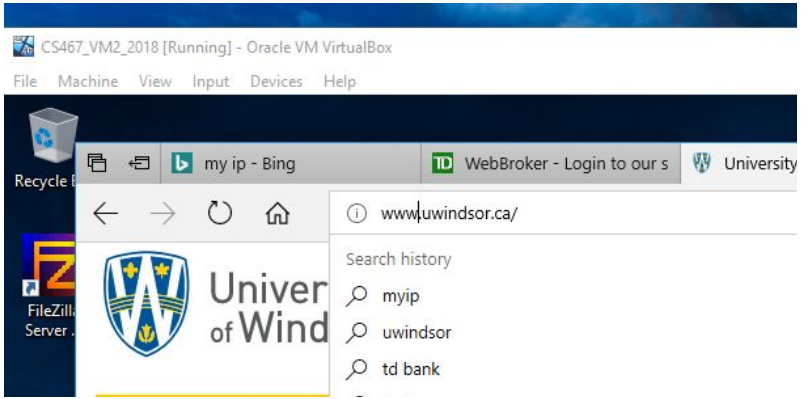
- The victim machine could access the internet.
- Nothing from the victim point of view change.



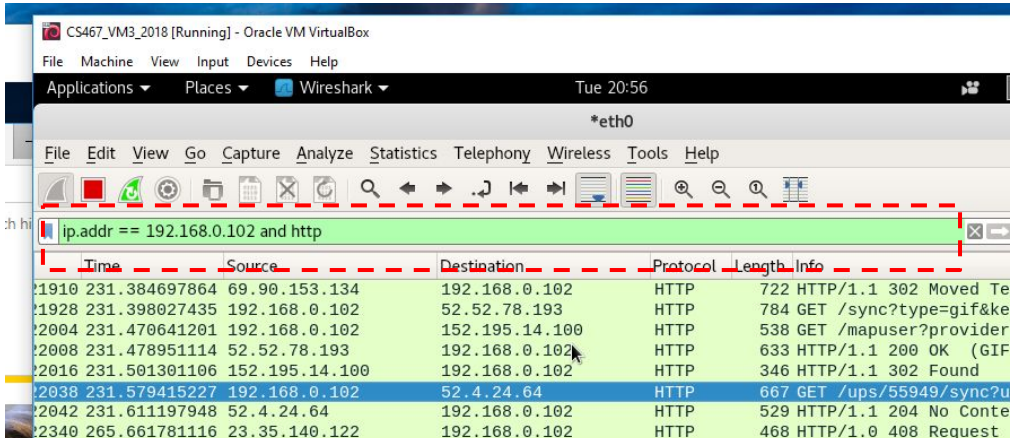
STEP-03: Man-in-the-Middle (eavesdropping)



STEP-03: Man-in-the-Middle (eavesdropping)

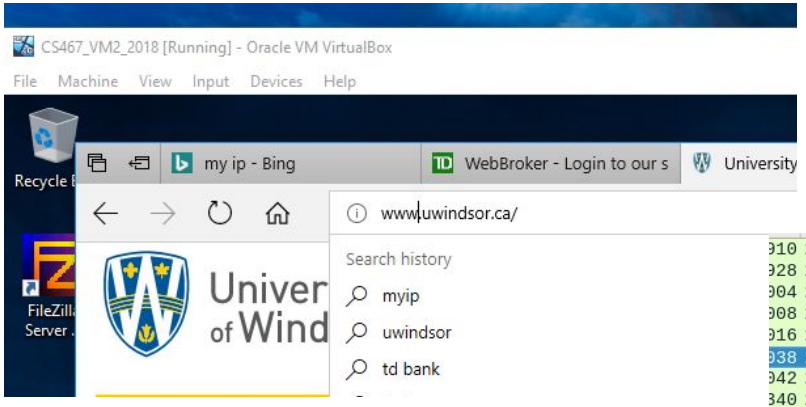


The victim is browsing the web

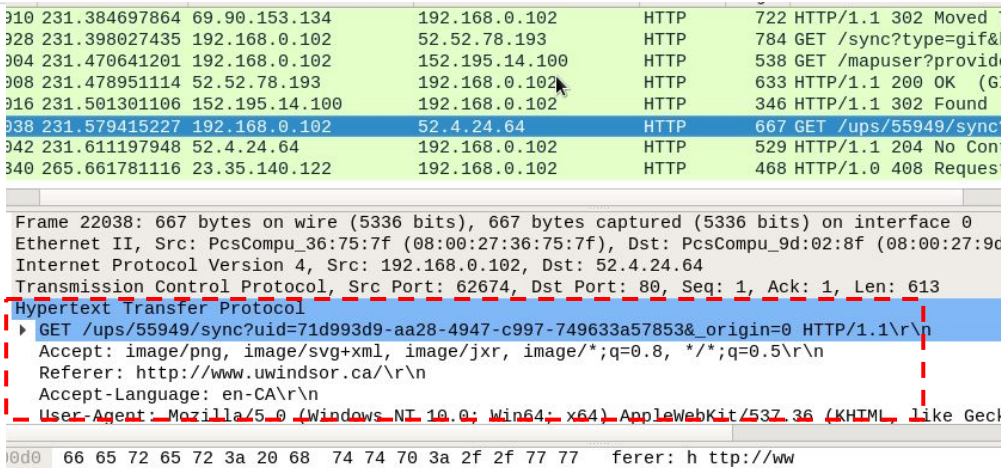


Attacker Machine Sniffing the victim traffic

STEP-03: Man-in-the-Middle (eavesdropping)



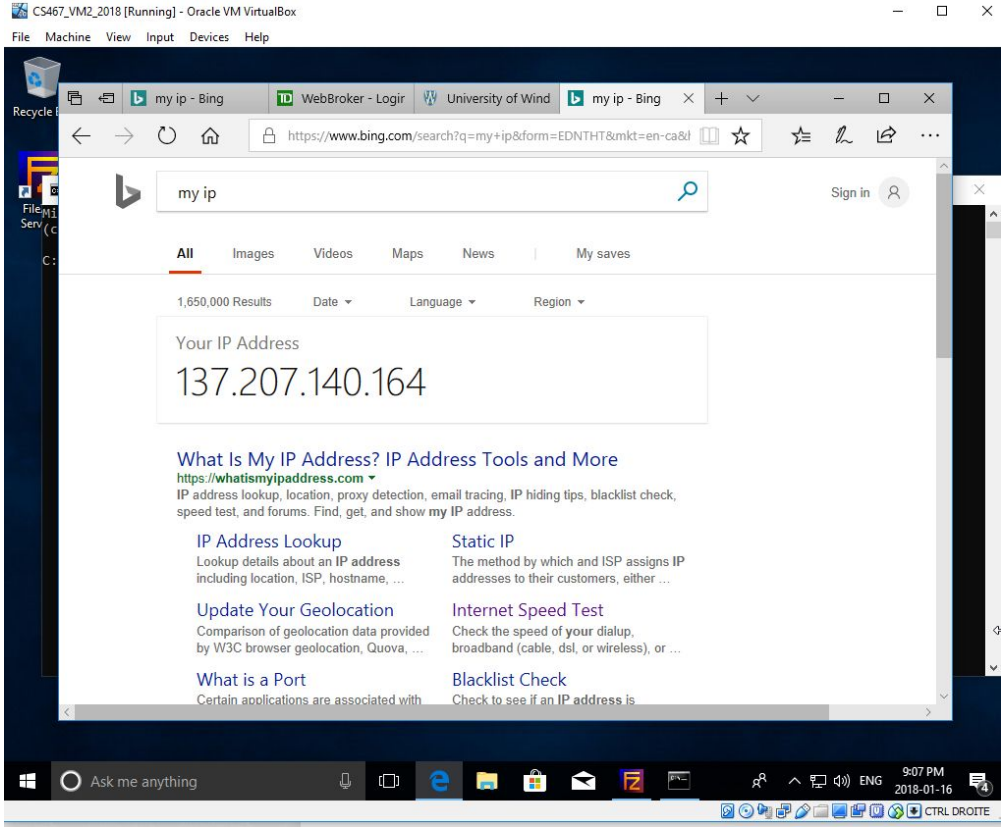
The victim is browsing the web



Attacker Machine Sniffing the victim traffic

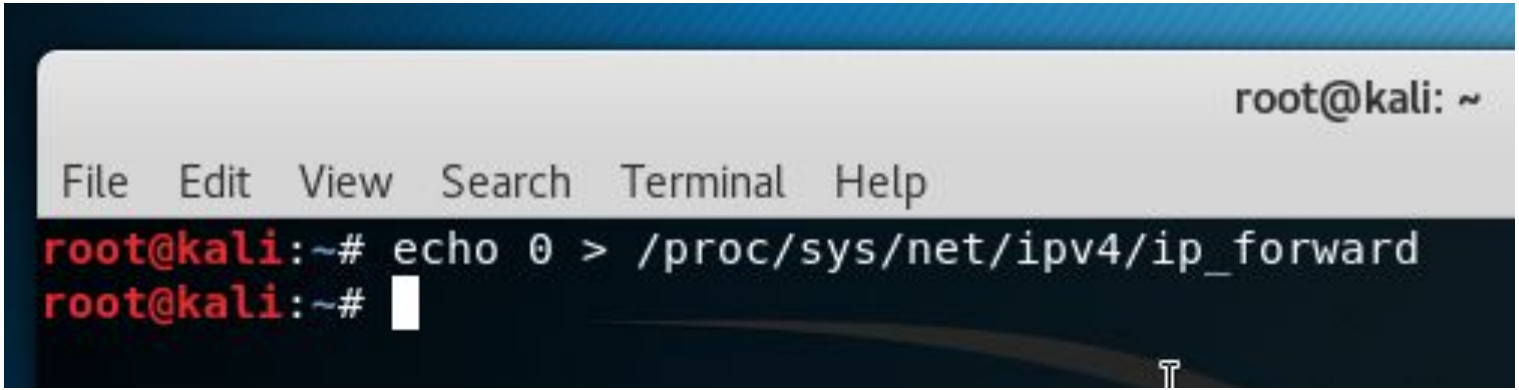
STEP-04: Denial of Service

How could the attacker execute a DoS attack against the victim?



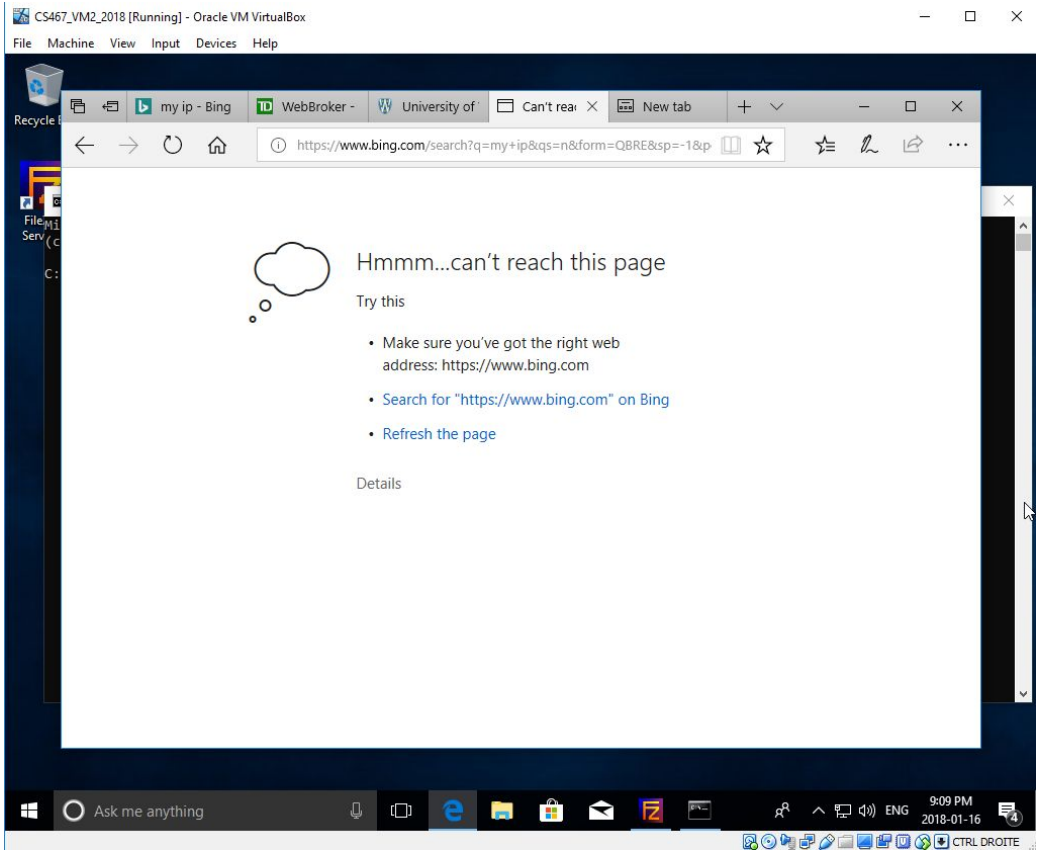
STEP-04: Denial of Service

What will happen if the attacker disable the IP forward on his machine and continue sending the malicious ARP messages?



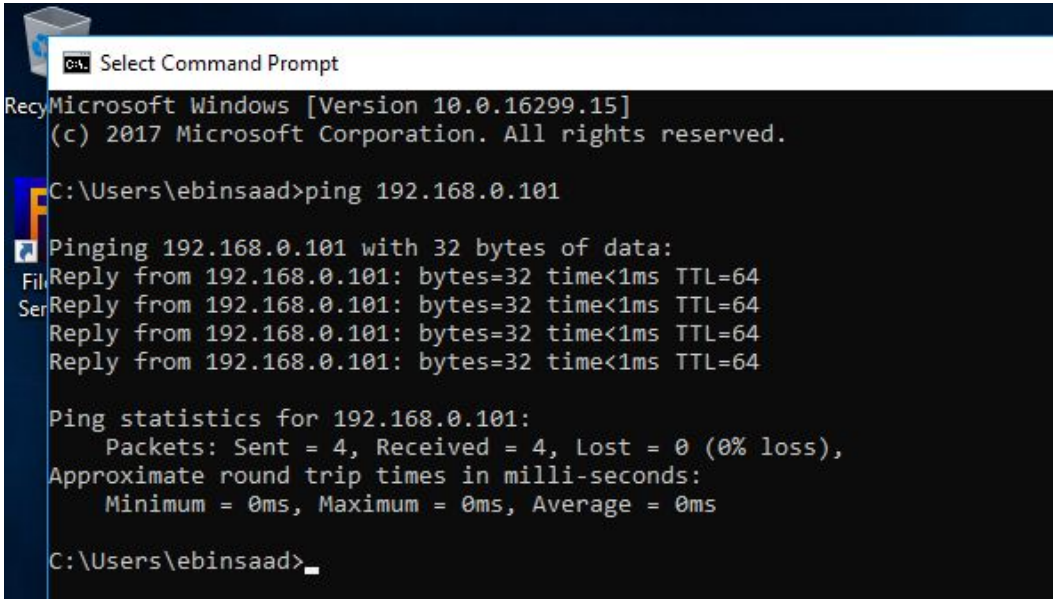
STEP-04: Denial of Service

The victim will not have access to the internet anymore



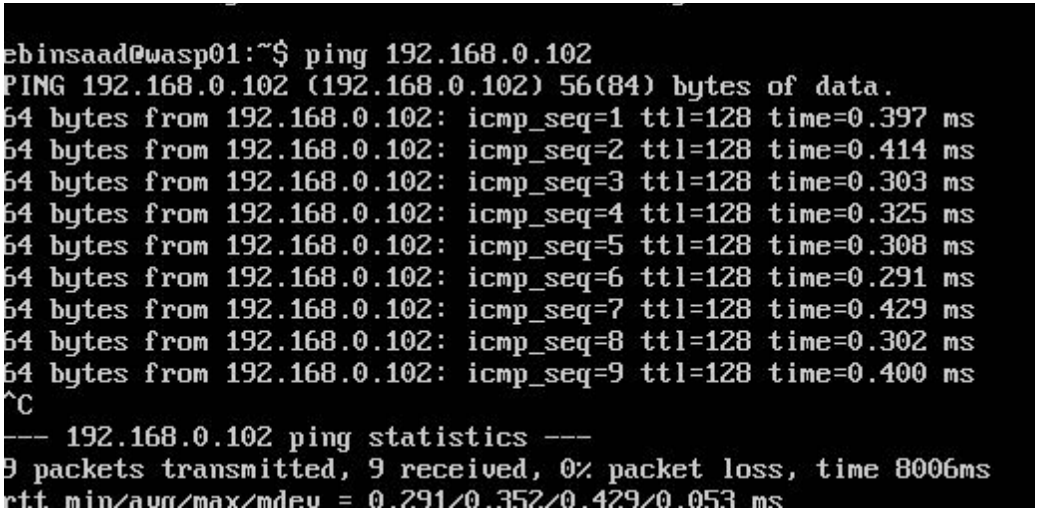
The Scope of the Attack

Let us say that the victim ping other hosts on the network like 192.168.0.101 (the other linux machine)



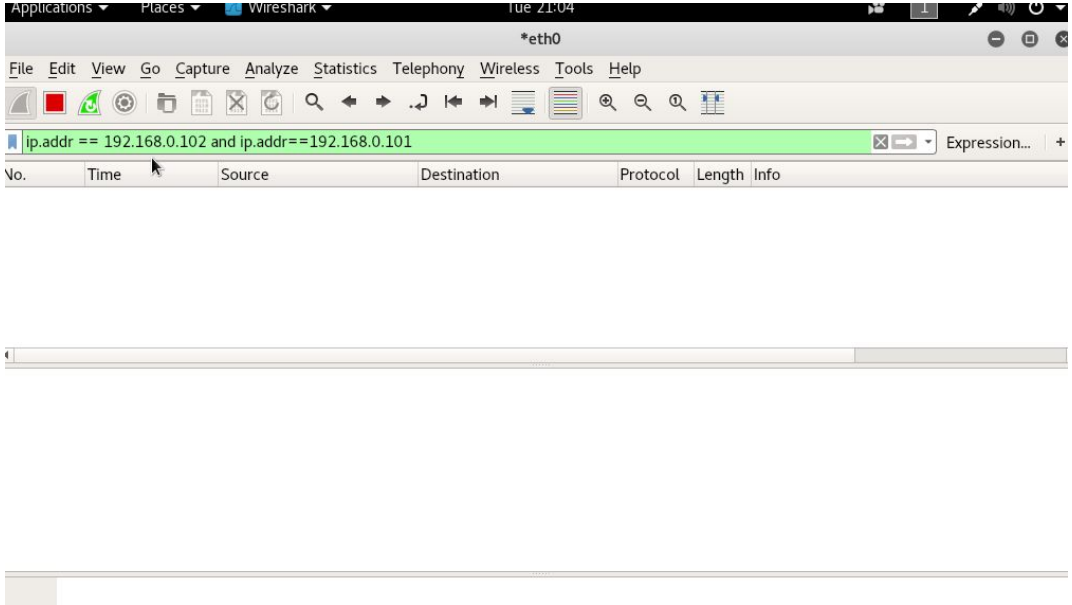
The Scope of the Attack

Also, the 192.168.0.101 (the other linux machine) ping the victim machine 192.168.0.102



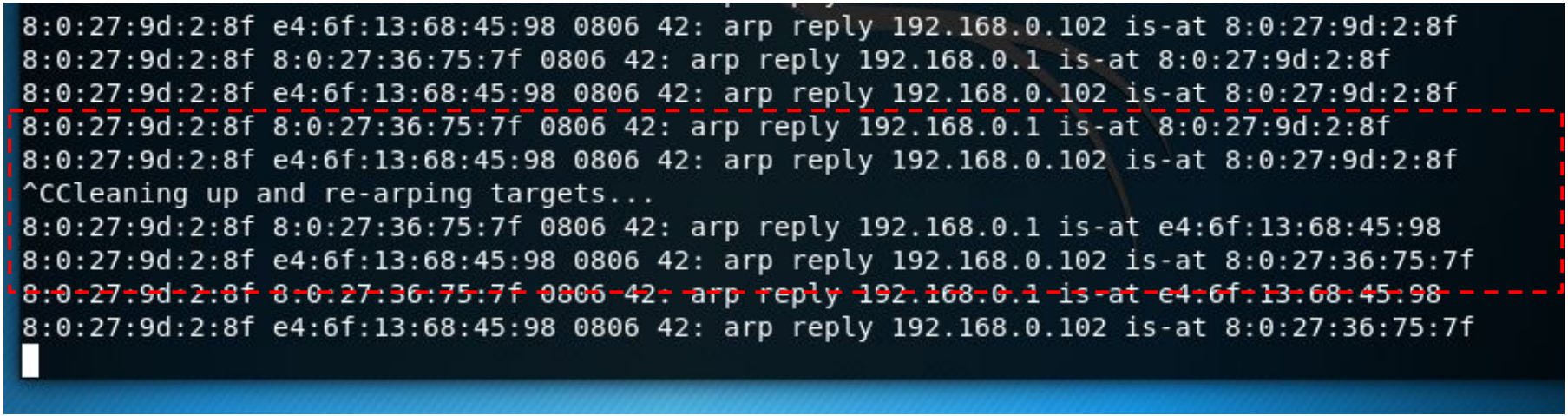
The Scope of the Attack

Do you think the attacker will be able to capture and record these ping messages between the victim machine and the other hosts in the network?



ARP Attack Teardown

Finally, the attacker will end the attack by stopping the arpspoof tool



Questions