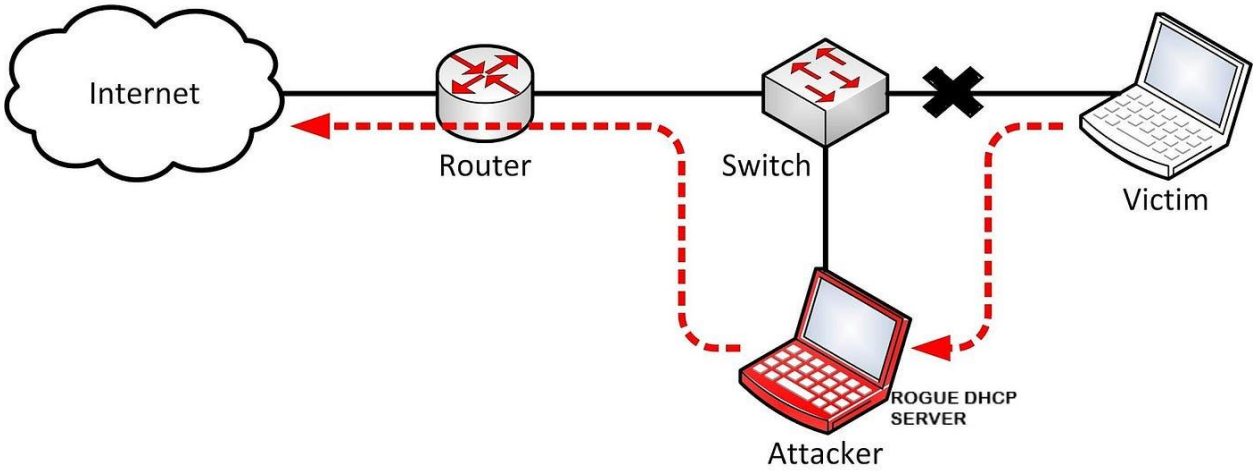
Attack

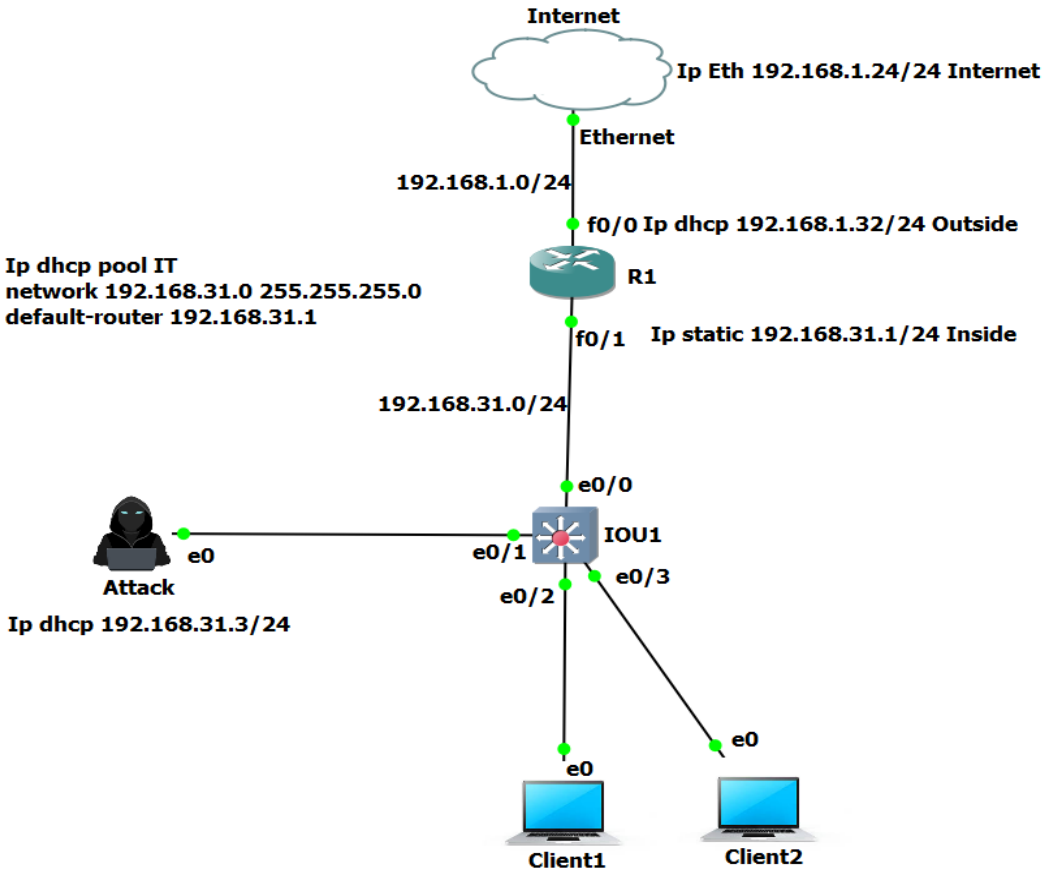
Rouge DHCP Server Attack

Network Security



Made by: - Ahmed Abou_ELmaged Shallan Allam

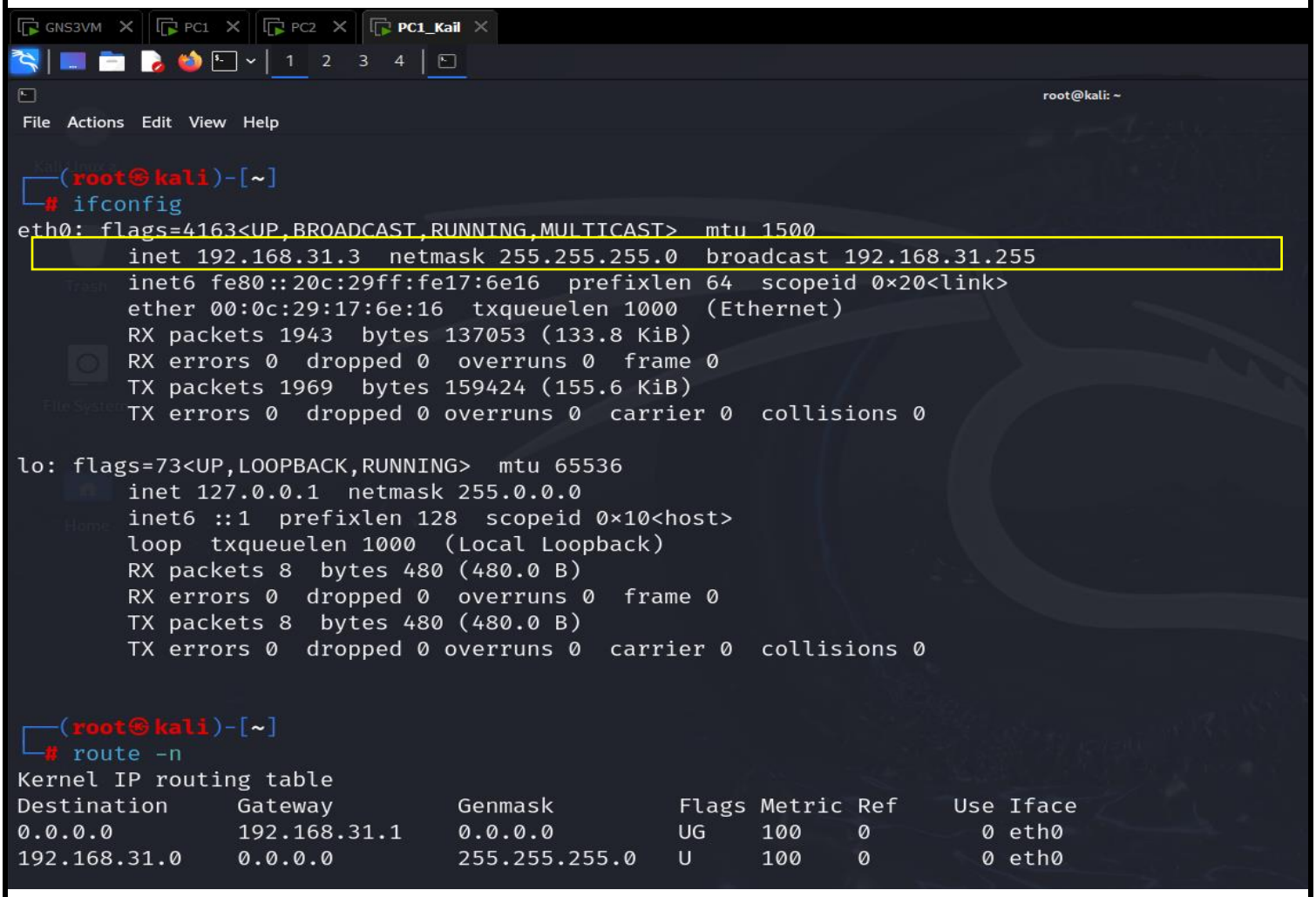
Network Topology: -

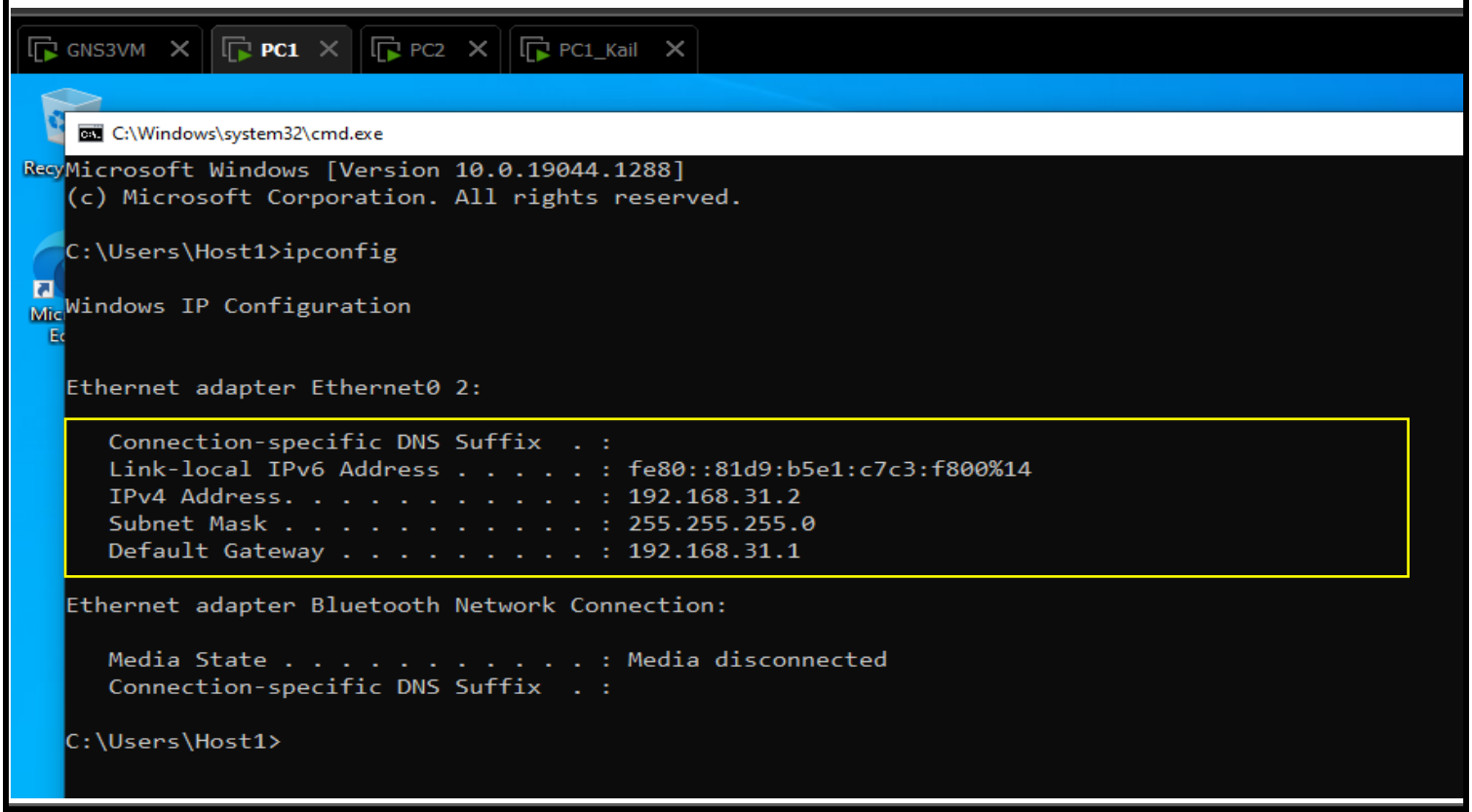


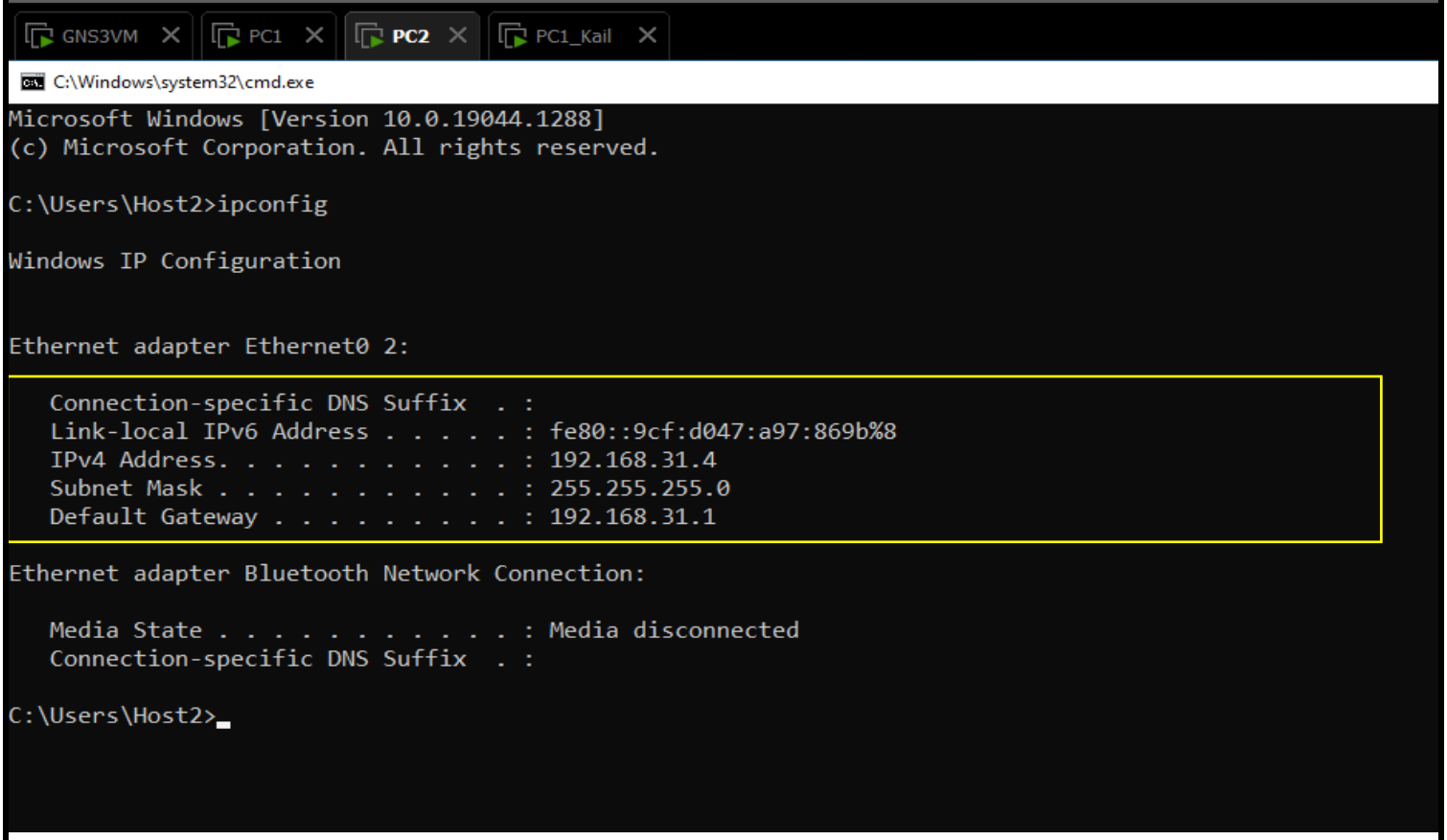
- **Operate DHCP in Router**

```
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/              Lease expiration        Type
                    Hardware address/
                    User name
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#
```




GNS3VM
PC1
PC2
PC1_Kail
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>

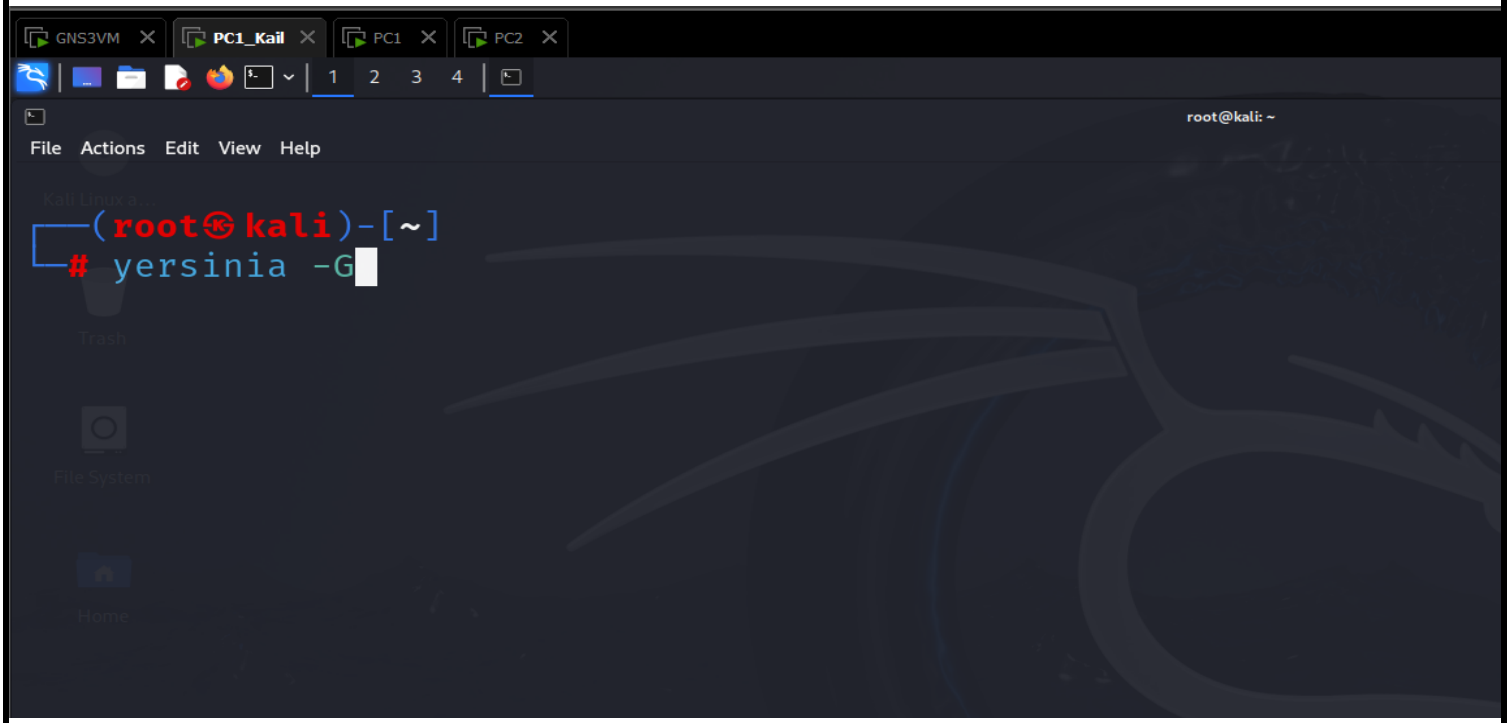

GNS3VM
PC1
PC2
PC1_Kail
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19044.1288]
(c) Microsoft Corporation. All rights reserved.
C:\Users\Host2>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0 2:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::9cf:d047:a97:869b%8
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>

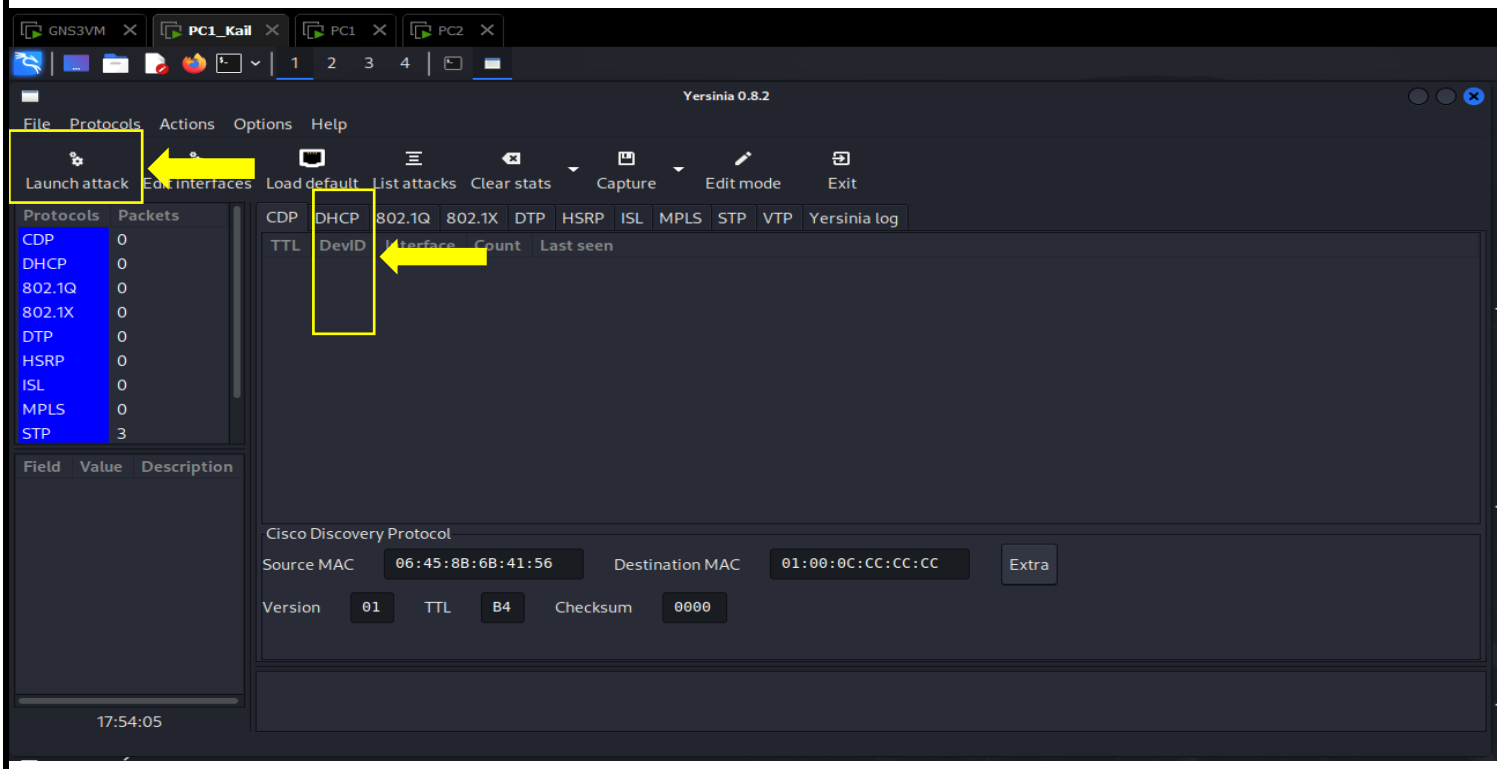
- **Show mac address table in switch**

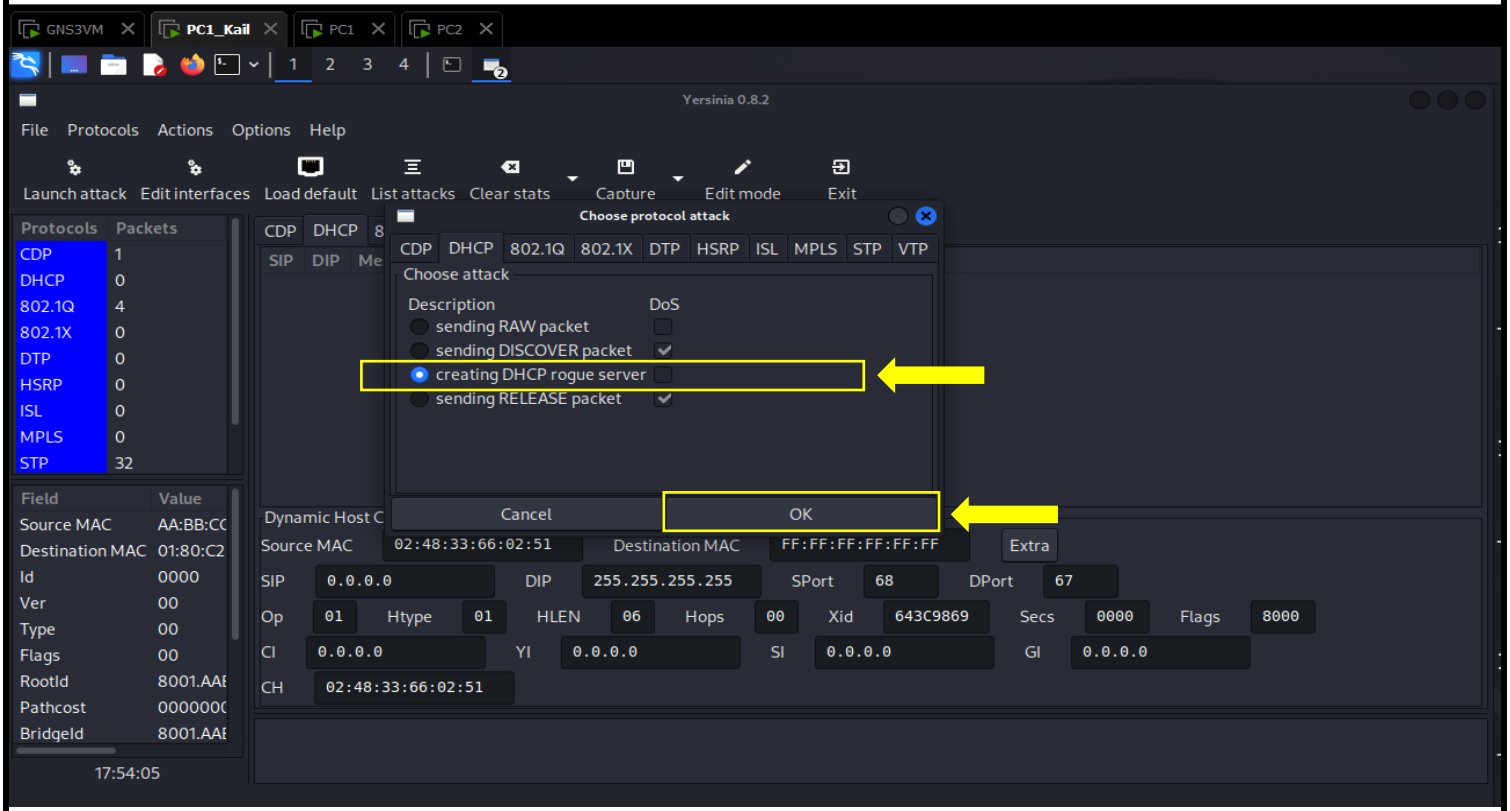
```
IOU1#show mac address-table
          Mac Address Table
-------------------------------------------

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**

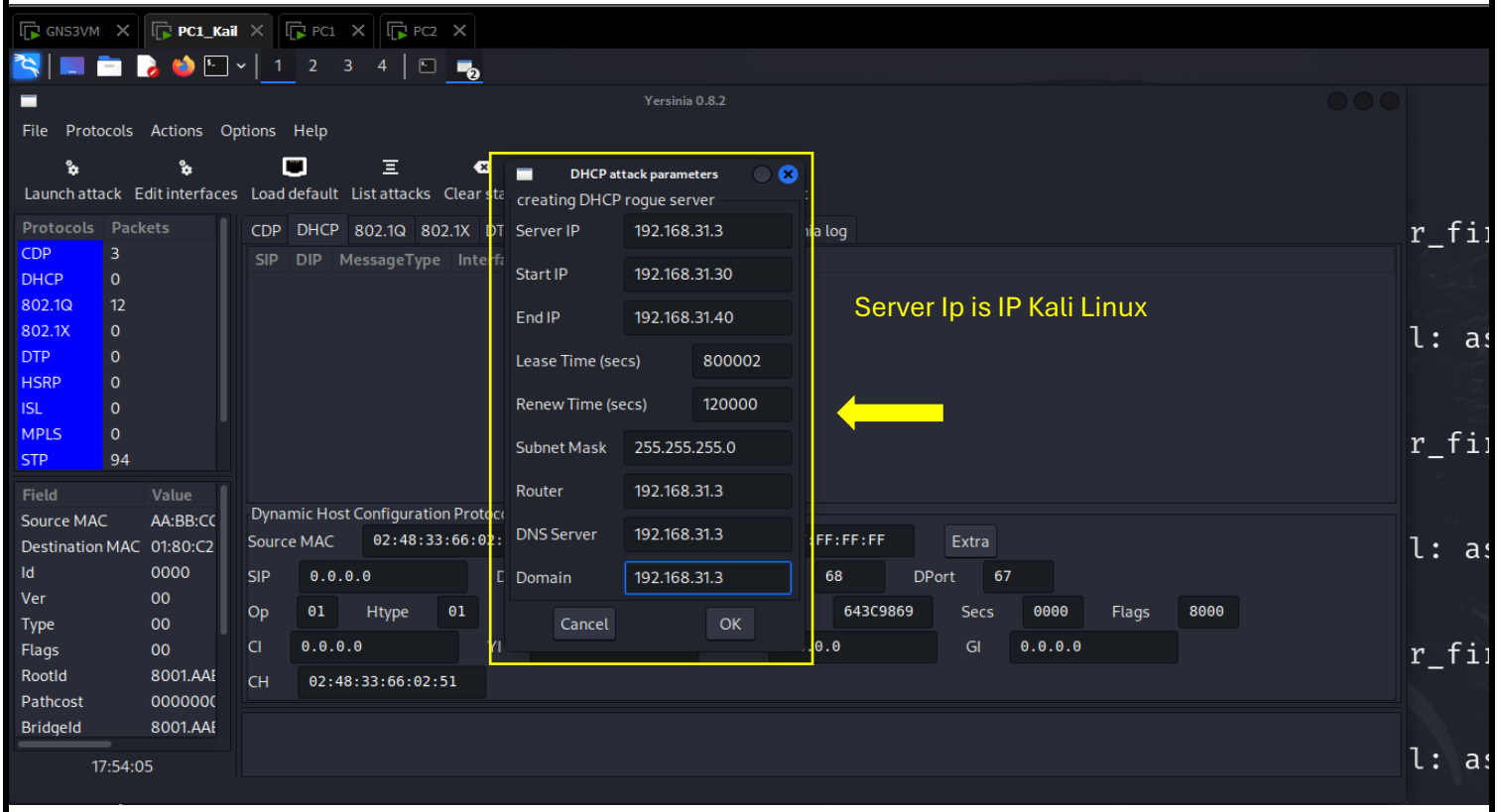
```
┌──(root㉿kali)-[~]
└─# yersinia -G
```

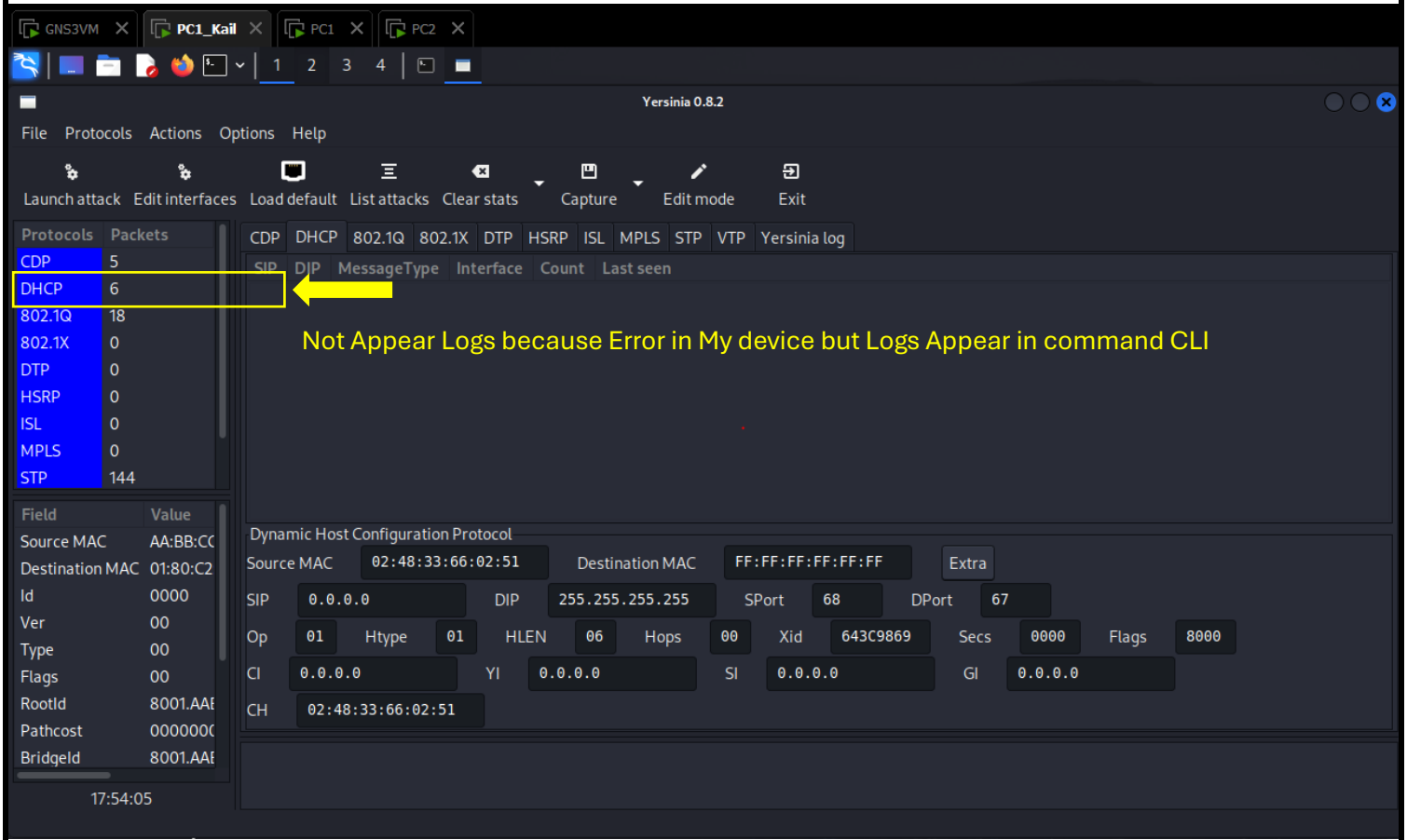




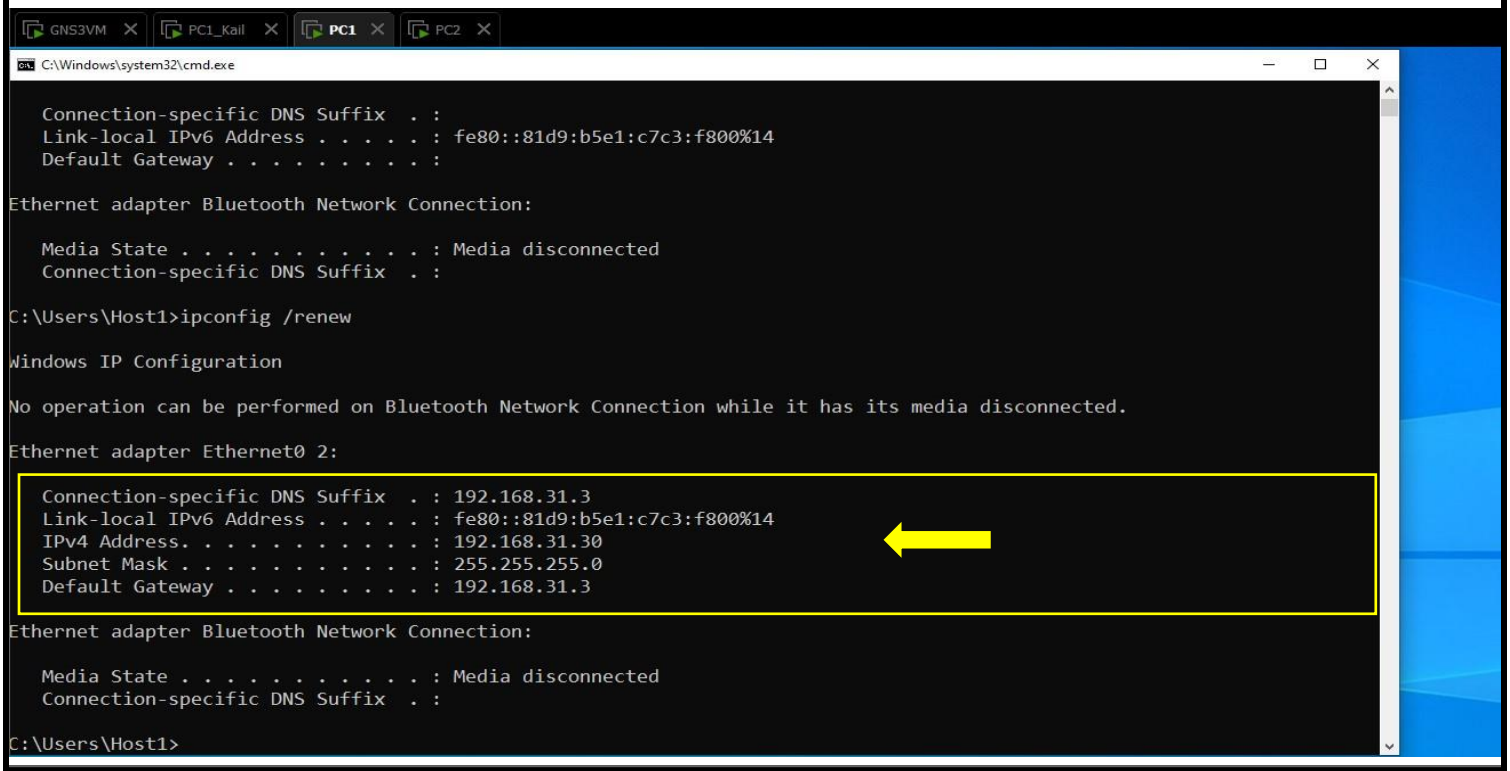


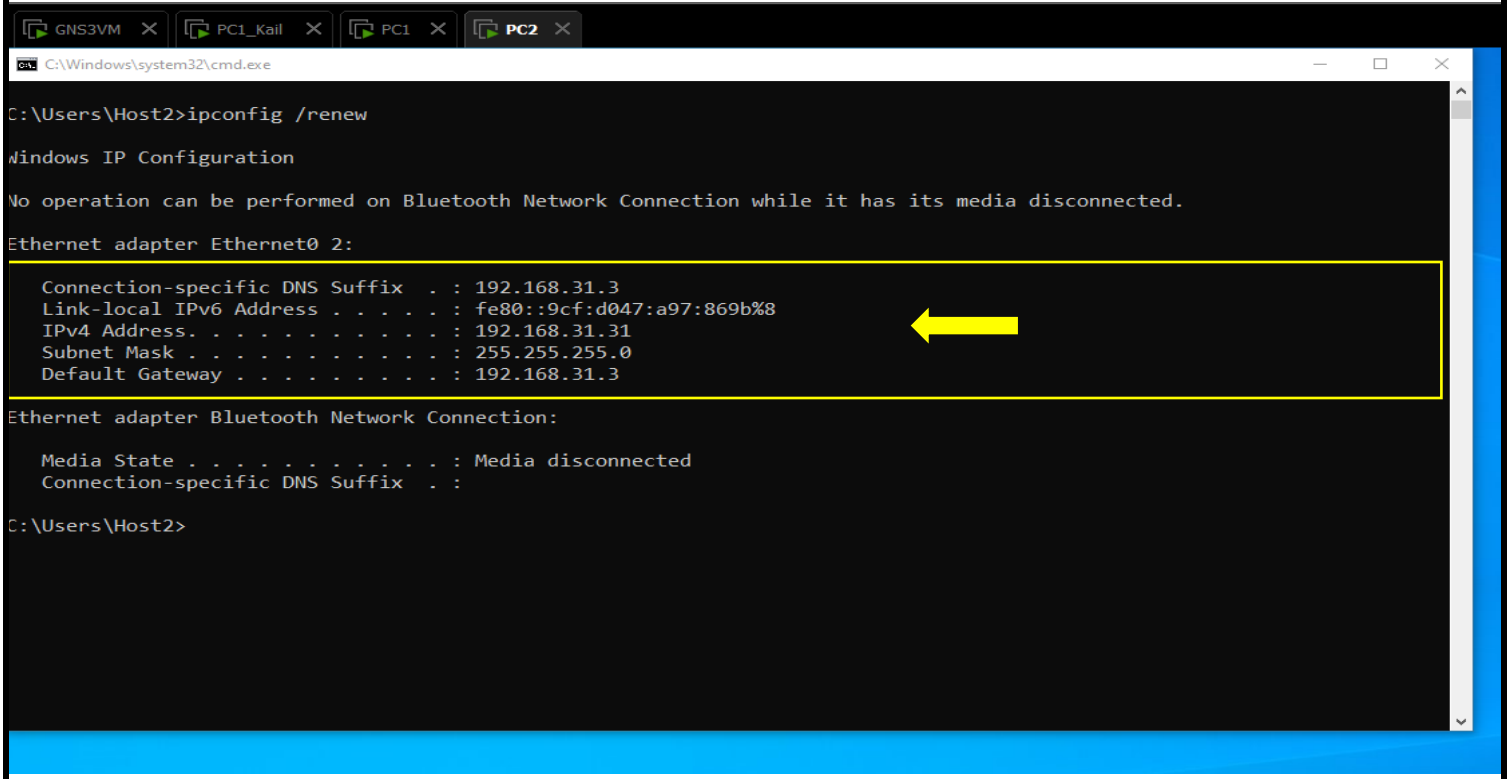
https://www.linkedin.com/in/ahmed-allam-42950622b/ https://github.com/AhmedAllam2003





https://www.linkedin.com/in/ahmed-allam-42950622b/ https://github.com/AhmedAllam2003





Thanks

https://www.linkedin.com/in/ahmed-allam-42950622b/ https://github.com/AhmedAllam2003