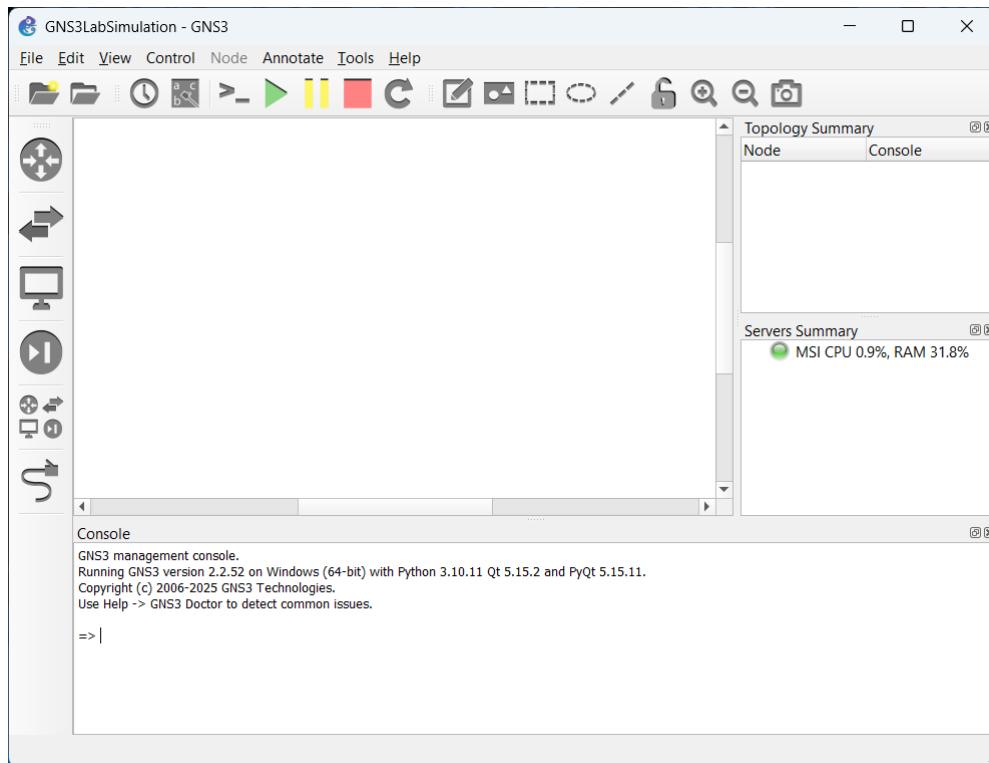


How to analyze the traffic captured in the Wireshark

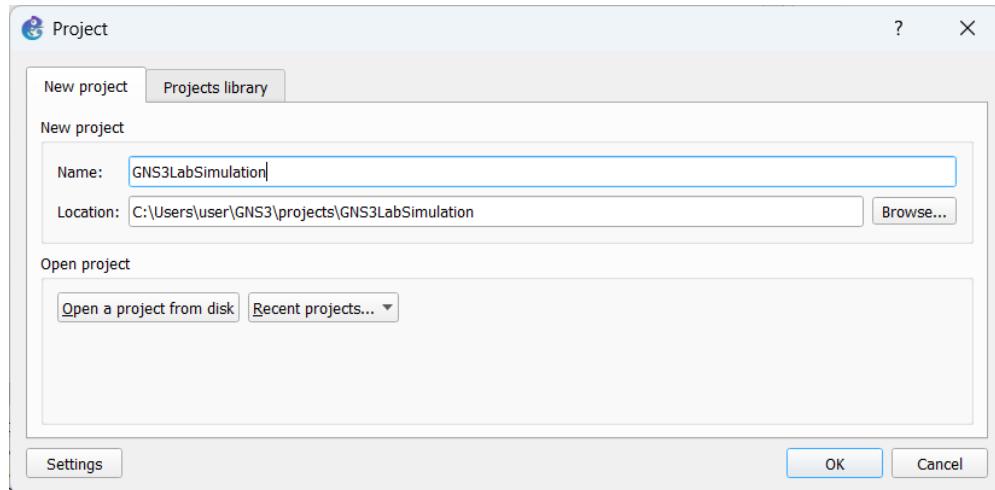
Environment setup (VMware and GNS3 configuration)

GNS3 setup

1. Download GNS3 from <https://www.gns3.com/software/download>
2. Open GNS3 from 'Downloads'
 - a. You'll see this windows

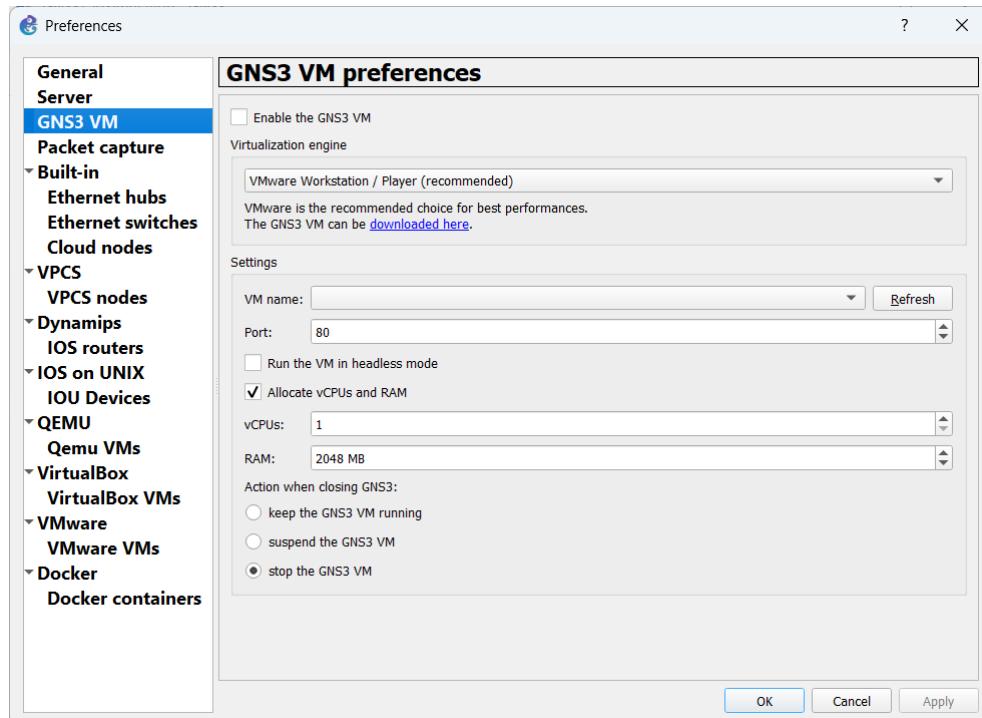


3. Name your project.
 - a. Here it's going to be named 'GNS3LabSimulation'

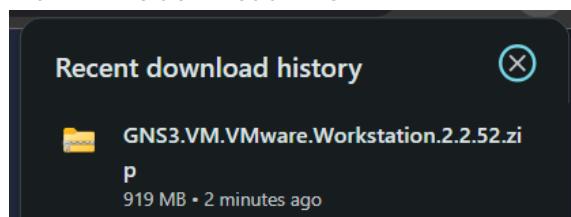


4. Open Edit >> Preferences >> GNS3 VM preferences

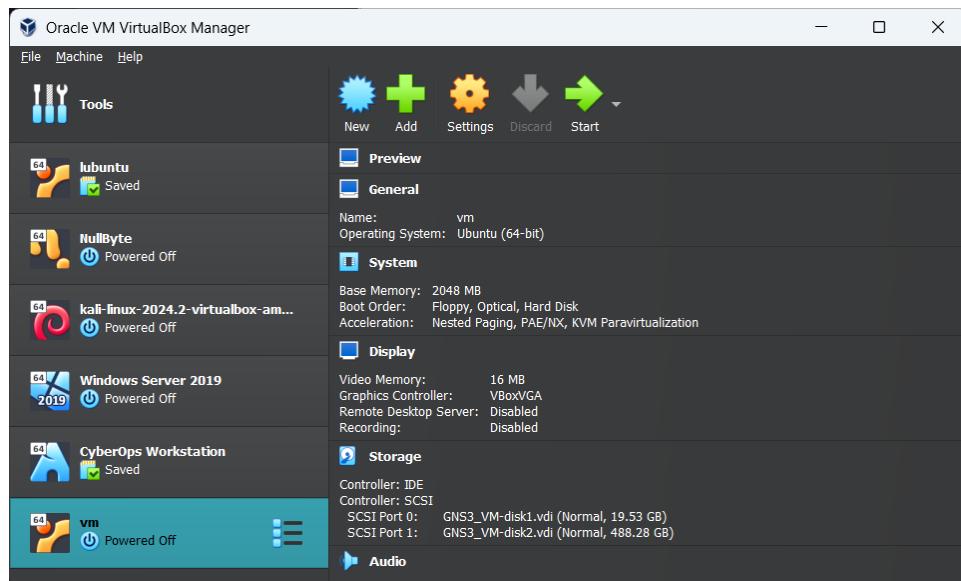
- a. You'll see this windows



- b. Tap 'download here' >> download the file.
c. Wait till the download finish.

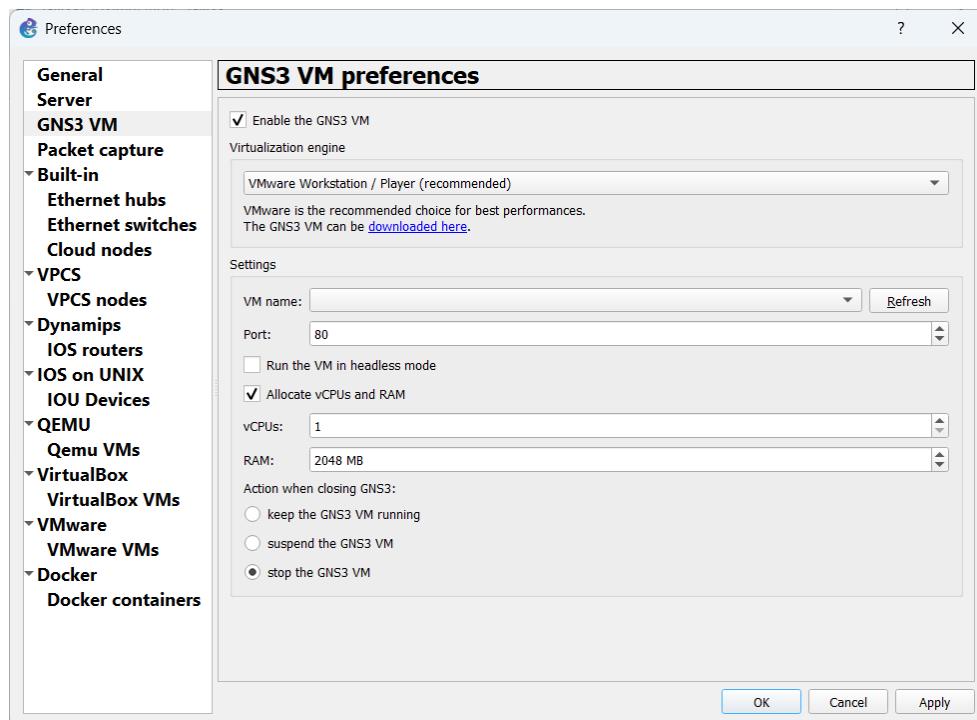


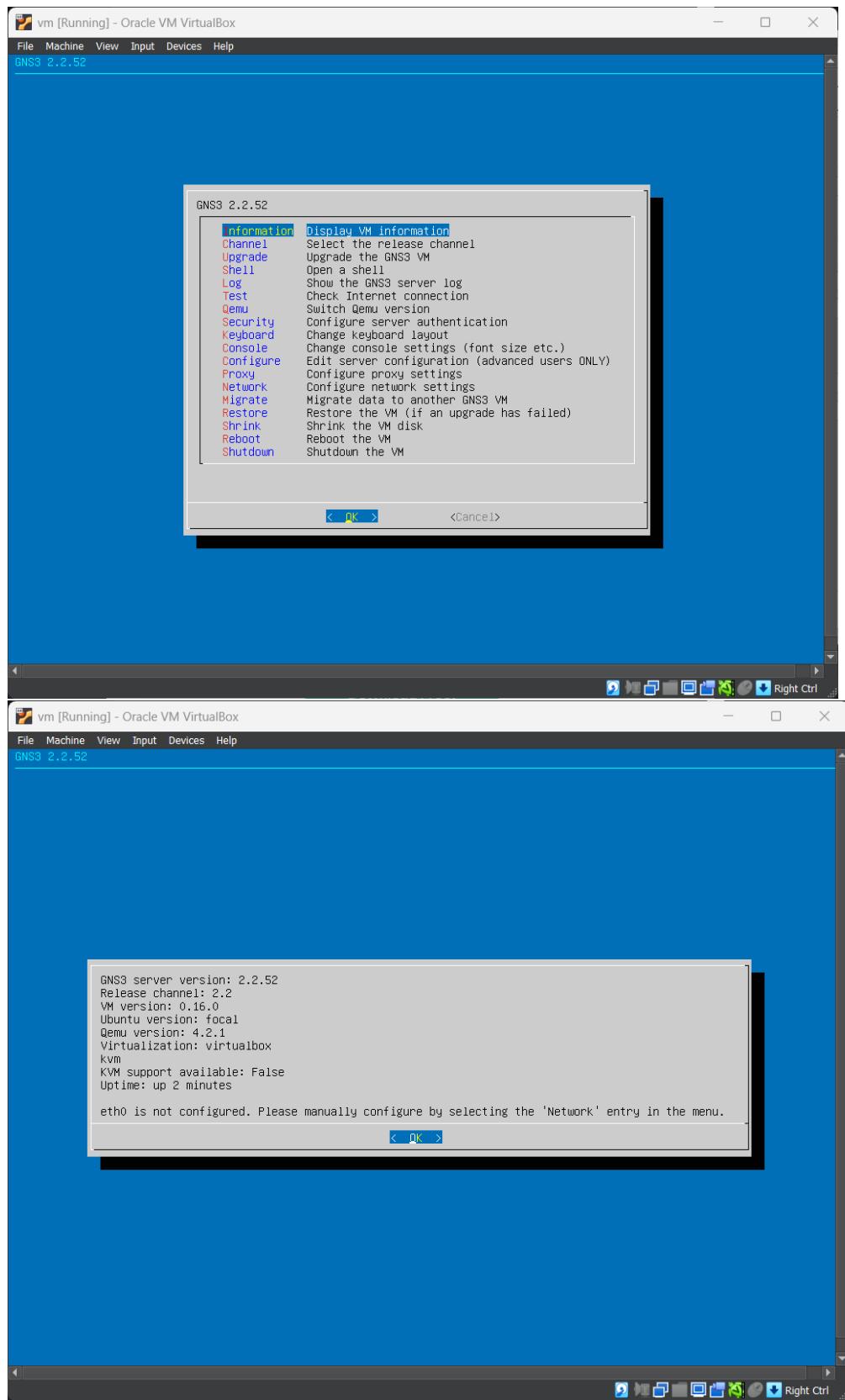
5. Open the file and it will be opened in your Oracle VM.



6. Go to your 'GNS3 VM preferences' >> Tap 'Enable the GNS3 VM' >> 'Apply'

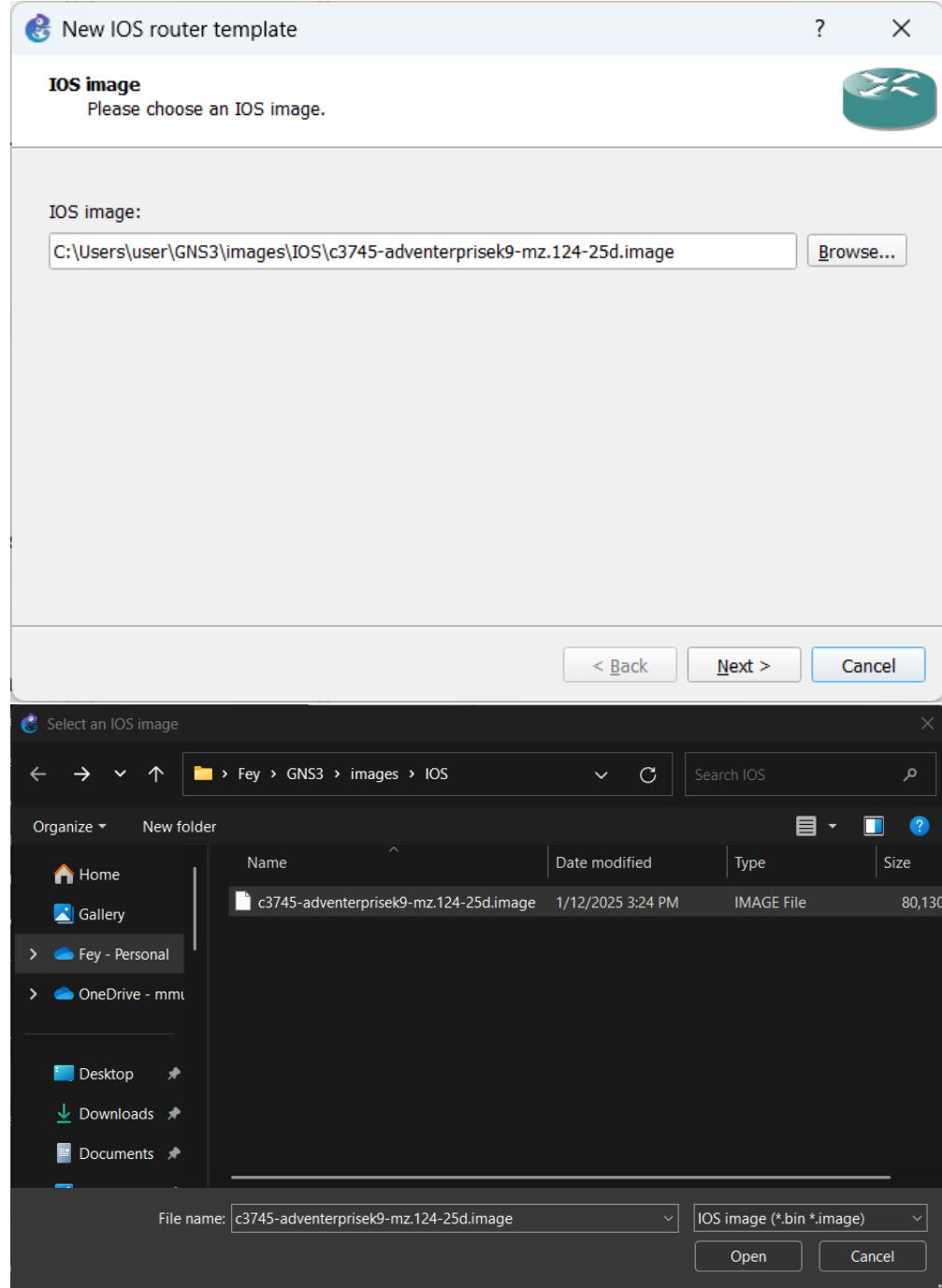
a. You'll be met with below windows :





7. In 'GNS3 VM preferences', go to 'IOS routers' >> 'New' >> 'Browse' >> choose your router IOS image that you have

- a. You can download from here too <https://github.com/hegdepavankumar/Cisco-Images-for-GNS3-and-EVE-NG?tab=readme-ov-file>
- b. Choose your IOS image



- c. Rename your router >> Next

New IOS router - c3745-adventerprisek9-mz.124-25d.image ? X

Name and platform
Please choose a descriptive name for this new IOS router and verify the platform and chassis.

Name: CiscoRouter-c3745

Platform: c3745

Chassis:

This is an EtherSwitch router

< Back Next > Cancel

d. Specify your ports

New IOS router - c3745-adventerprisek9-mz.124-25d.image ? X

Network adapters
Please choose the default network adapters that should be inserted into every new instance of this router.

slot 0: GT96100-FE

slot 1: NM-1FE-TX

slot 2: NM-1FE-TX

slot 3: NM-1FE-TX

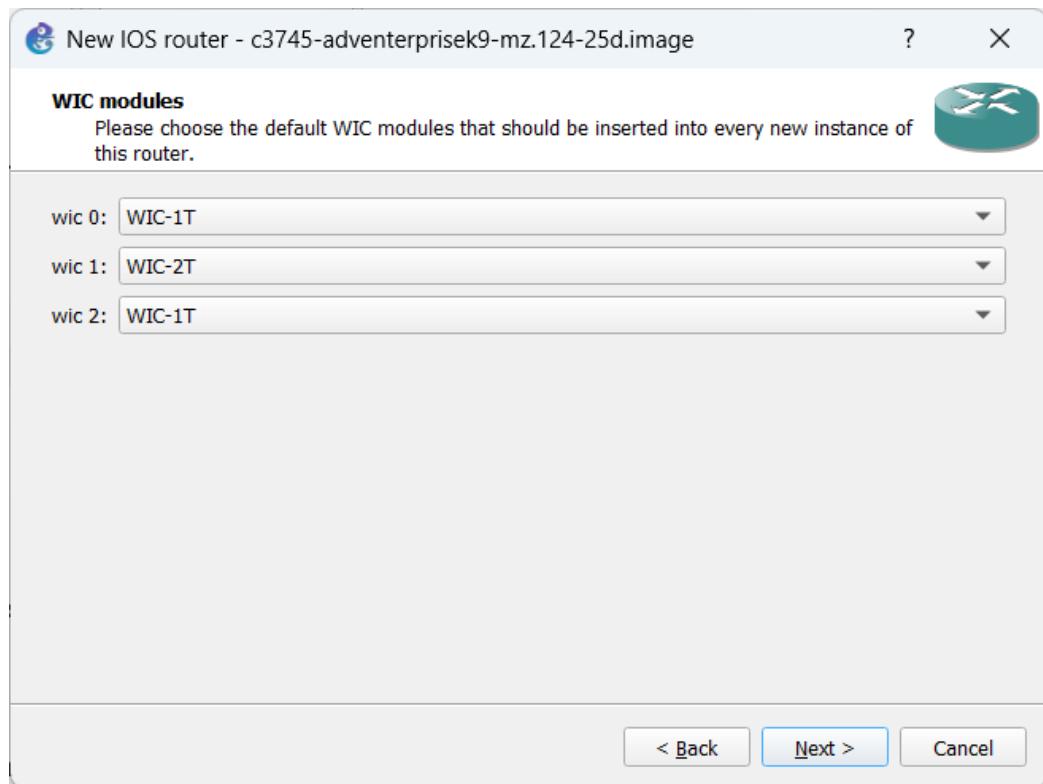
slot 4: NM-1FE-TX

slot 5:

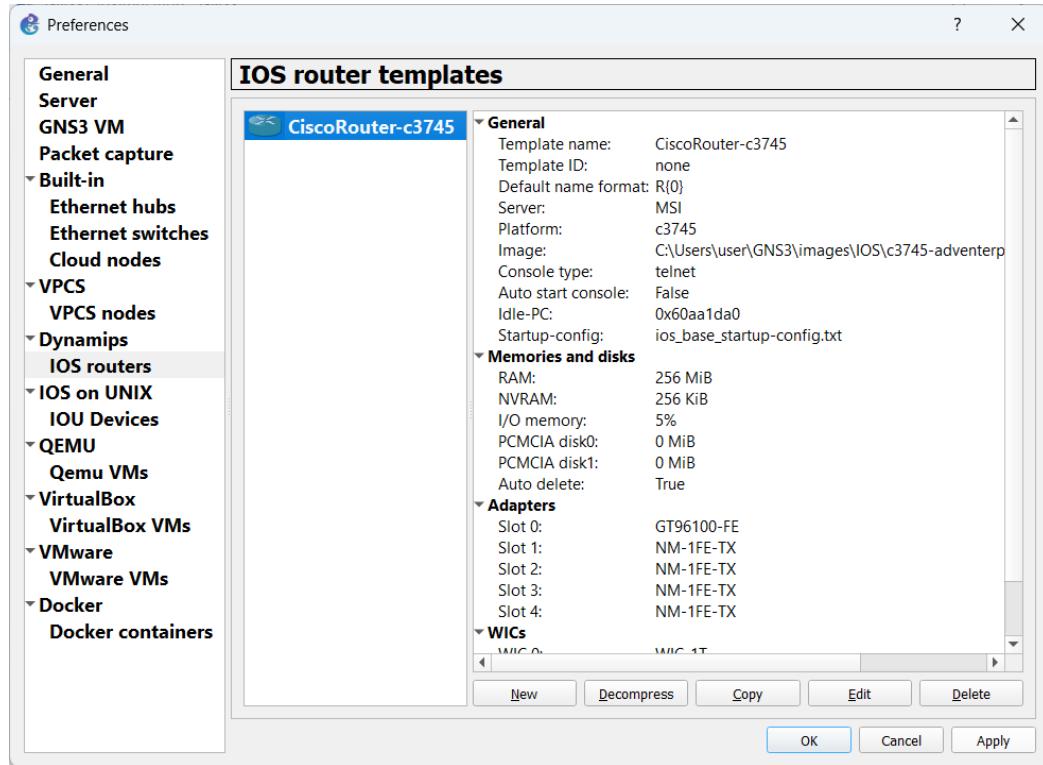
slot 6:

< Back Next > Cancel

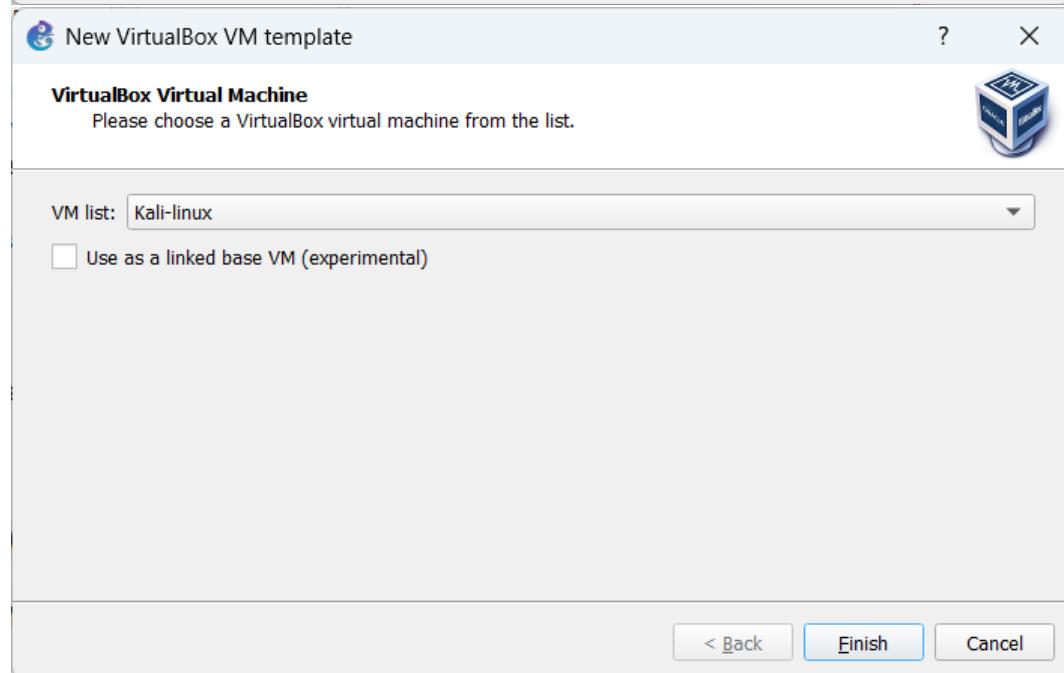
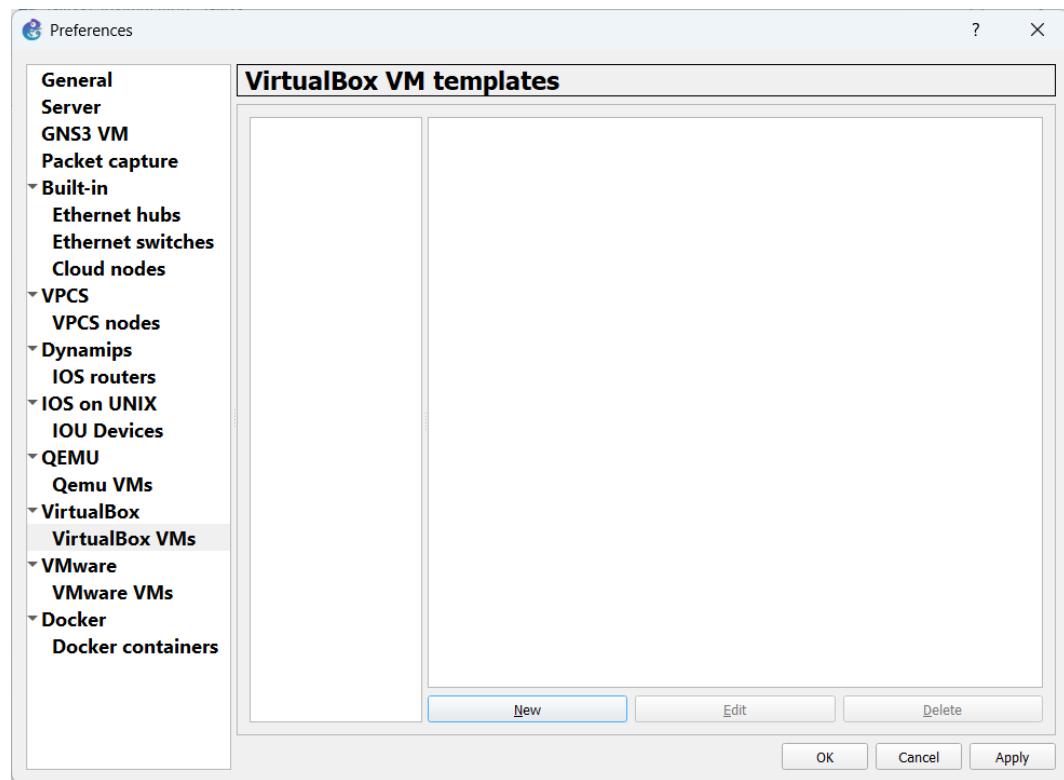
e. Specify your wireless ports



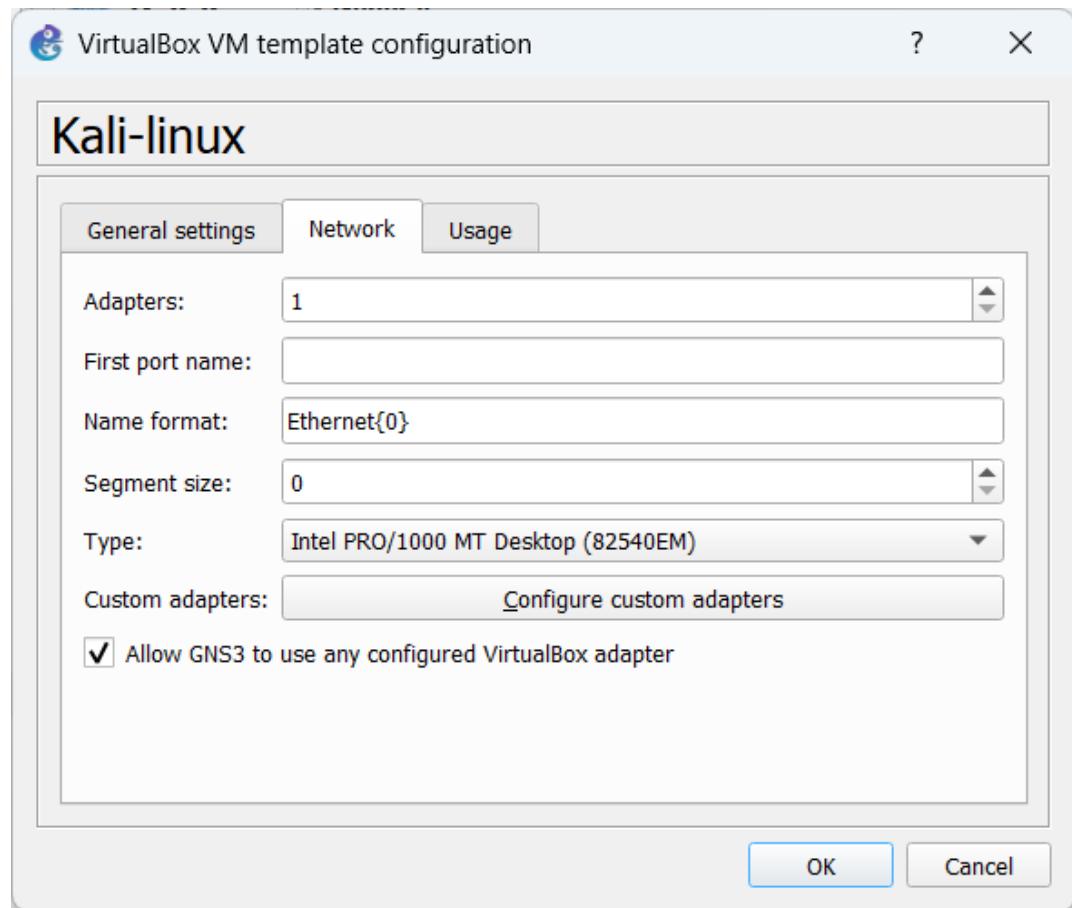
f. Next >> Finish >> Apply



8. In 'GNS3 VM preferences', go to 'VirtualBox VMs' >> New

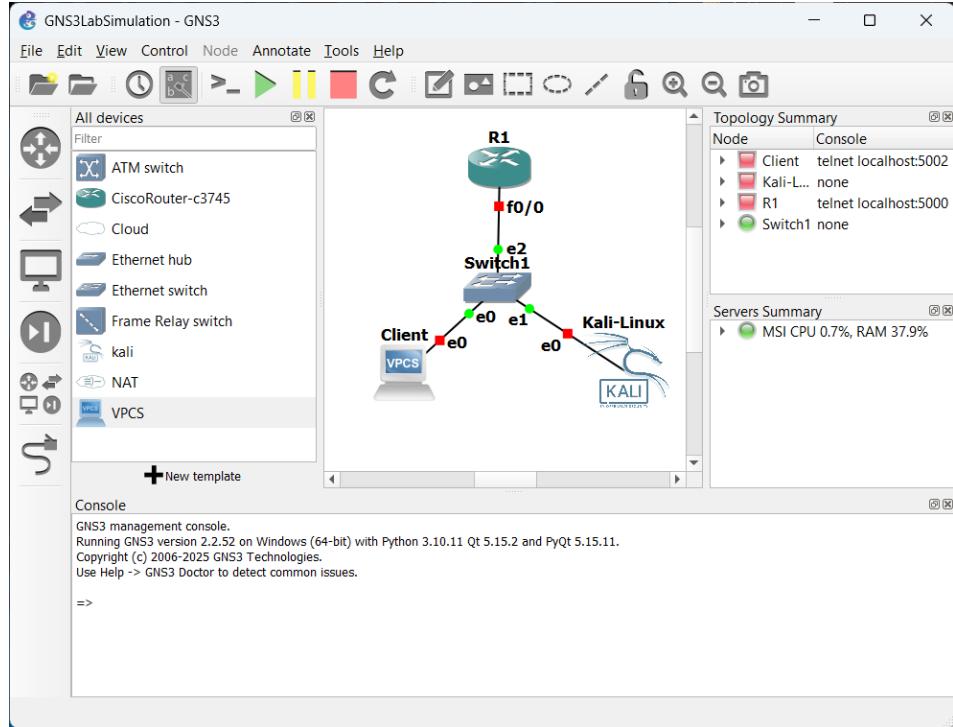


- a. Tap on 'Allow GNS3 to use any configured VirtualBox adapter' >> OK >> Apply >> OK



Network topology creation in GNS3

1. Setup a simple topology between cisco router, switch, vpcs and kali



2. On R1, choose 'Start' >> Console

a. You'll see this windows

```
*Mar 1 00:00:03.803: %LINK-5-CHANGED: Interface Serial0/0, changed state to administratively down
*Mar 1 00:00:03.803: %LINK-5-CHANGED: Interface Serial0/1, changed state to administratively down
*Mar 1 00:00:03.803: %LINK-5-CHANGED: Interface Serial0/2, changed state to administratively down
*Mar 1 00:00:03.807: %LINK-5-CHANGED: Interface Serial0/3, changed state to administratively down
*Mar 1 00:00:03.807: %LINK-5-CHANGED: Interface FastEthernet1/0, changed state to administratively down
*Mar 1 00:00:03.819: %LINK-5-CHANGED: Interface FastEthernet2/0, changed state to administratively down
*Mar 1 00:00:03.823: %LINK-5-CHANGED: Interface FastEthernet3/0, changed state to administratively down
*Mar 1 00:00:04.675: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down
*Mar 1 00:00:04.771: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state to down
*Mar 1 00:00:04.803: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to down
*Mar 1 00:00:04.803: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state to down
*Mar 1 00:00:04.803: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2, changed state to down
*Mar 1 00:00:04.807: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3, changed state to down
*Mar 1 00:00:04.807: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to down
*Mar 1 00:00:04.819: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/0, changed state to down
*Mar 1 00:00:04.819: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet3/0, changed state to down
*Mar 1 00:00:04.819: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to down
```

b. Show ip address

```
R1#sh ip int brief
Interface          IP-Address      OK? Method Status           Protocol
FastEthernet0/0    unassigned      YES unset administratively down down
Serial0/0          unassigned      YES unset administratively down down
FastEthernet0/1    unassigned      YES unset administratively down down
Serial0/1          unassigned      YES unset administratively down down
Serial0/2          unassigned      YES unset administratively down down
Serial0/3          unassigned      YES unset administratively down down
FastEthernet1/0    unassigned      YES unset administratively down down
FastEthernet2/0    unassigned      YES unset administratively down down
FastEthernet3/0    unassigned      YES unset administratively down down
FastEthernet4/0    unassigned      YES unset administratively down down
R1#
```

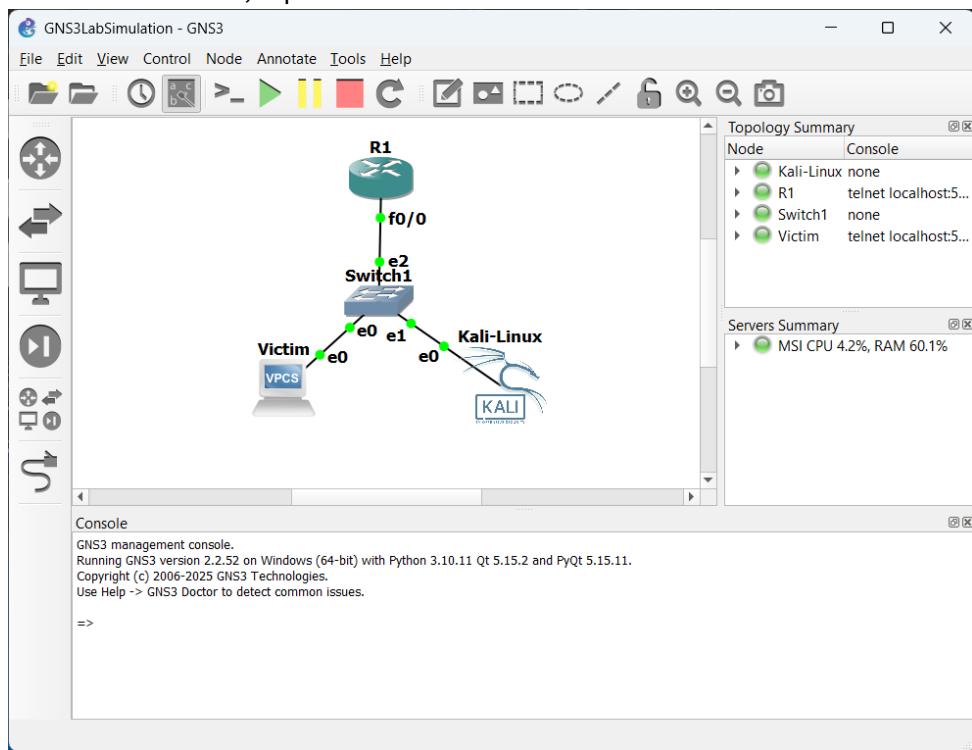
solarwinds | Solar-PuTTY free tool © 2019-2024 SolarWinds Worldwide, LLC. All rights reserved.

c. Set ip address for f0/0

```
R1#en
R1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int f0/0
R1(config-if)#ip add 192.168.0.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#
*Mar 1 00:03:44.847: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 00:03:45.847: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config-if)#exit
R1(config)#
R1#
```

solarwinds | Solar-PuTTY free tool © 2019-2024 SolarWinds Worldwide, LLC. All rights reserved.

3. On ‘Victim’ and ‘Kali-Linux’, tap ‘Start’



4. On ‘Victim’

a. Set ip address for VPCS

```

Victim> ip 192.168.0.77/24 192.168.0.1
Checking for duplicate address...
PC1 : 192.168.0.77 255.255.255.0 gateway 192.168.0.1

Victim> show ip

NAME      : Victim[1]
IP/MASK   : 192.168.0.77/24
GATEWAY   : 192.168.0.1
DNS       :
MAC       : 00:50:79:66:68:00
LPORT     : 10010
RHOST:PORT: 127.0.0.1:10011
MTU:      : 1500

```

- b. Test connectivity with router

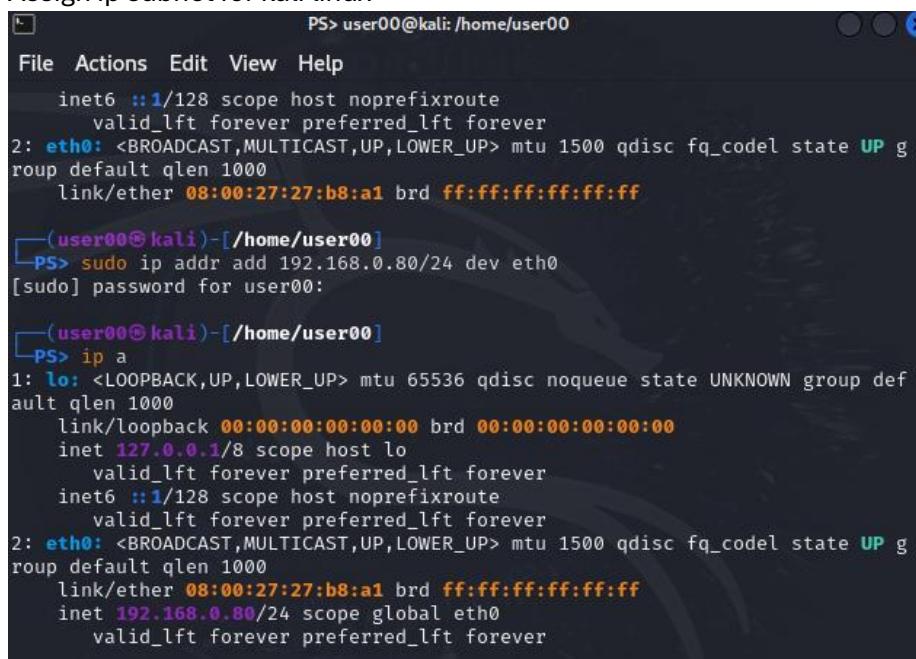
```

Victim> ping 192.168.0.1
84 bytes from 192.168.0.1 icmp_seq=1 ttl=255 time=8.731 ms
84 bytes from 192.168.0.1 icmp_seq=2 ttl=255 time=9.611 ms
84 bytes from 192.168.0.1 icmp_seq=3 ttl=255 time=1.983 ms
84 bytes from 192.168.0.1 icmp_seq=4 ttl=255 time=1.840 ms
84 bytes from 192.168.0.1 icmp_seq=5 ttl=255 time=2.918 ms

```

5. On ‘Kali-Linux’

- a. Assign ip subnet for kali linux



The screenshot shows a terminal window with the following content:

```

PS> user00@kali: /home/user00
File Actions Edit View Help
inet6 ::1/128 scope host noprefixroute
    valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b8:a1 brd ff:ff:ff:ff:ff:ff
    (user00㉿kali)-[~/home/user00]
    PS> sudo ip addr add 192.168.0.80/24 dev eth0
[sudo] password for user00:

    (user00㉿kali)-[~/home/user00]
    PS> ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b8:a1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.80/24 scope global eth0
        valid_lft forever preferred_lft forever

```

- b. Assign default gateway

```
(user00㉿kali)-[~/home/user00]
└─$ sudo ip link set eth0 up
[sudo] password for user00:

(user00㉿kali)-[~/home/user00]
└─$ sudo ip routr add default via 192.168.0.1
Object "rour" is unknown, try "ip help".

(user00㉿kali)-[~/home/user00]
└─$ sudo ip route add default via 192.168.0.1

(user00㉿kali)-[~/home/user00]
└─$ ss
```

Generating traffic

1. Ping test in kali

```
(user00㉿kali)-[~/home/user00]
└─$ ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=255 time=22.2 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=255 time=4.52 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=255 time=10.7 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=255 time=8.55 ms
64 bytes from 192.168.0.1: icmp_seq=5 ttl=255 time=4.19 ms
64 bytes from 192.168.0.1: icmp_seq=6 ttl=255 time=5.96 ms
64 bytes from 192.168.0.1: icmp_seq=7 ttl=255 time=10.4 ms
64 bytes from 192.168.0.1: icmp_seq=8 ttl=255 time=8.48 ms
```

2. End ping test with Ctrl+C

```
PS> user00@kali:/home/user00
File Actions Edit View Help
64 bytes from 192.168.0.1: icmp_seq=86 ttl=255 time=4.19 ms
64 bytes from 192.168.0.1: icmp_seq=87 ttl=255 time=1.57 ms
64 bytes from 192.168.0.1: icmp_seq=88 ttl=255 time=9.42 ms
64 bytes from 192.168.0.1: icmp_seq=89 ttl=255 time=7.19 ms
64 bytes from 192.168.0.1: icmp_seq=90 ttl=255 time=5.39 ms
64 bytes from 192.168.0.1: icmp_seq=91 ttl=255 time=10.1 ms
64 bytes from 192.168.0.1: icmp_seq=92 ttl=255 time=6.99 ms
64 bytes from 192.168.0.1: icmp_seq=93 ttl=255 time=12.5 ms
64 bytes from 192.168.0.1: icmp_seq=94 ttl=255 time=7.63 ms
64 bytes from 192.168.0.1: icmp_seq=95 ttl=255 time=8.17 ms
64 bytes from 192.168.0.1: icmp_seq=96 ttl=255 time=8.74 ms
64 bytes from 192.168.0.1: icmp_seq=97 ttl=255 time=4.86 ms
64 bytes from 192.168.0.1: icmp_seq=98 ttl=255 time=6.82 ms
64 bytes from 192.168.0.1: icmp_seq=99 ttl=255 time=2.94 ms
64 bytes from 192.168.0.1: icmp_seq=100 ttl=255 time=8.30 ms
64 bytes from 192.168.0.1: icmp_seq=101 ttl=255 time=2.99 ms
64 bytes from 192.168.0.1: icmp_seq=102 ttl=255 time=7.46 ms
64 bytes from 192.168.0.1: icmp_seq=103 ttl=255 time=2.14 ms
64 bytes from 192.168.0.1: icmp_seq=104 ttl=255 time=12.0 ms
64 bytes from 192.168.0.1: icmp_seq=105 ttl=255 time=8.12 ms
^C
— 192.168.0.1 ping statistics —
105 packets transmitted, 105 received, 0% packet loss, time 104186ms
rtt min/avg/max/mdev = 1.570/7.834/22.229/3.384 ms
```

3. Modify network configuration file to ensure configurations persist after reboot

```
PS> user00@kali: /home/user00
File Actions Edit View Help
64 bytes from 192.168.0.1: icmp_seq=89 ttl=255 time=7.19 ms
64 bytes from 192.168.0.1: icmp_seq=90 ttl=255 time=5.39 ms
64 bytes from 192.168.0.1: icmp_seq=91 ttl=255 time=10.1 ms
64 bytes from 192.168.0.1: icmp_seq=92 ttl=255 time=6.99 ms
64 bytes from 192.168.0.1: icmp_seq=93 ttl=255 time=12.5 ms
64 bytes from 192.168.0.1: icmp_seq=94 ttl=255 time=7.63 ms
64 bytes from 192.168.0.1: icmp_seq=95 ttl=255 time=8.17 ms
64 bytes from 192.168.0.1: icmp_seq=96 ttl=255 time=8.74 ms
64 bytes from 192.168.0.1: icmp_seq=97 ttl=255 time=4.86 ms
64 bytes from 192.168.0.1: icmp_seq=98 ttl=255 time=6.82 ms
64 bytes from 192.168.0.1: icmp_seq=99 ttl=255 time=2.94 ms
64 bytes from 192.168.0.1: icmp_seq=100 ttl=255 time=8.30 ms
64 bytes from 192.168.0.1: icmp_seq=101 ttl=255 time=2.99 ms
64 bytes from 192.168.0.1: icmp_seq=102 ttl=255 time=7.46 ms
64 bytes from 192.168.0.1: icmp_seq=103 ttl=255 time=2.14 ms
64 bytes from 192.168.0.1: icmp_seq=104 ttl=255 time=12.0 ms
64 bytes from 192.168.0.1: icmp_seq=105 ttl=255 time=8.12 ms
^C
— 192.168.0.1 ping statistics —
105 packets transmitted, 105 received, 0% packet loss, time 104186ms
rtt min/avg/max/mdev = 1.570/7.834/22.229/3.384 ms

└─(user00㉿kali)-[~/home/user00]
└─$ PS> sudo nano /etc/network/interface
└─(user00㉿kali)-[~/home/user00]
└─$ PS> ┌

PS> user00@kali: /home/user00
File Actions Edit View Help
GNU nano 8.2          /etc/network/interface *
auto eth0
iface eth0 inet static
    address 192.168.0.80
    netmask 255.255.255.0
    gateway 192.168.0.1

^G Help      ^O Write Out   ^F Where Is   ^K Cut       ^T Execute
^X Exit      ^R Read File   ^\ Replace    ^U Paste     ^J Justify
```

```
PS> user00@kali: /home/user00
File Actions Edit View Help
GNU nano 8.2          /etc/network/interface *
auto eth0
iface eth0 inet static
    address 192.168.0.80
    netmask 255.255.255.0
    gateway 192.168.0.1

Command to execute: sudo systemctl restart networking
^G Help      ^P Older      M-F New Buffer ^S Spell Check ^J Full Justify
^C Cancel    ^N Newer       M-\ Pipe Text  ^Y Linter   ^O Formatter
```

4. Sending icmp ping request over to victim to test connectivity

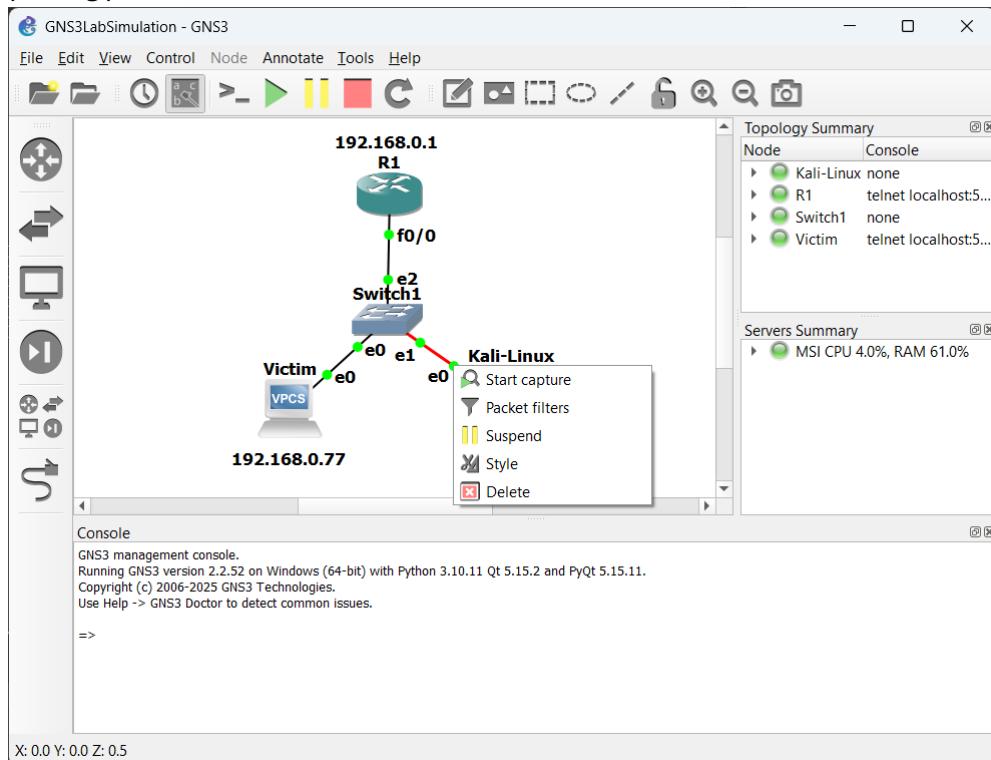
```
(user00㉿kali)-[~/home/user00]
PS> ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=255 time=6.42 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=255 time=13.4 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=255 time=1.89 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=255 time=4.89 ms
^C
--- 192.168.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3010ms
rtt min/avg/max/mdev = 1.885/6.644/13.385/4.219 ms

(user00㉿kali)-[~/home/user00]
PS> ping 192.168.0.77
PING 192.168.0.77 (192.168.0.77) 56(84) bytes of data.
64 bytes from 192.168.0.77: icmp_seq=1 ttl=64 time=2.19 ms
64 bytes from 192.168.0.77: icmp_seq=2 ttl=64 time=1.64 ms
64 bytes from 192.168.0.77: icmp_seq=3 ttl=64 time=1.27 ms
64 bytes from 192.168.0.77: icmp_seq=4 ttl=64 time=3.89 ms
^C
--- 192.168.0.77 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 1.265/2.243/3.886/1.003 ms

(user00㉿kali)-[~/home/user00]
PS>
```

Capturing and filtering packets in Wireshark

1. Start capturing packets



2. Ethernet type 0x0806 (ARP)

a. Filter: eth.type == 0x0806

No.	Time	Source	Destination	Protocol	Length Info
1511..	2485.209372	PCSSystemtec_27:b8:...	Private_66:68:00	ARP	60 Who has 192.168.0.77? Tell 192.168.0.80
1511..	2485.209372	Private_66:68:00	PCSSystemtec_27:b8:...	ARP	60 192.168.0.77 is at 00:50:79:66:68:00
1514..	2506.702483	PCSSystemtec_27:b8:...	Private_66:68:00	ARP	60 Who has 192.168.0.77? Tell 192.168.0.80
1514..	2506.703460	Private_66:68:00	PCSSystemtec_27:b8:...	ARP	60 192.168.0.77 is at 00:50:79:66:68:00
1517..	2527.940402	PCSSystemtec_27:b8:...	Private_66:68:00	ARP	60 Who has 192.168.0.77? Tell 192.168.0.80
1517..	2527.941306	Private_66:68:00	PCSSystemtec_27:b8:...	ARP	60 192.168.0.77 is at 00:50:79:66:68:00
1519..	2549.177213	PCSSystemtec_27:b8:...	Private_66:68:00	ARP	60 Who has 192.168.0.77? Tell 192.168.0.80
1519..	2549.177213	Private_66:68:00	PCSSystemtec_27:b8:...	ARP	60 192.168.0.77 is at 00:50:79:66:68:00
1522..	2570.670336	PCSSystemtec_27:b8:...	Private_66:68:00	ARP	60 Who has 192.168.0.77? Tell 192.168.0.80
1522..	2570.671313	Private_66:68:00	PCSSystemtec_27:b8:...	ARP	60 192.168.0.77 is at 00:50:79:66:68:00
1525..	2591.909851	PCSSystemtec_27:b8:...	Private_66:68:00	ARP	60 Who has 192.168.0.77? Tell 192.168.0.80
1525..	2591.909851	Private_66:68:00	PCSSystemtec_27:b8:...	ARP	60 192.168.0.77 is at 00:50:79:66:68:00

3. Ethernet broadcast

a. Filter: eth.addr == ff:ff:ff:ff:ff:ff

No.	Time	Source	Destination	Protocol	Length Info
1457..	2053.993933	PCSSystemtec_27:b8:..	Broadcast	ARP	60 Who has 192.168.0.162? Tell 192.168.0.80
1457..	2054.004256	PCSSystemtec_27:b8:..	Broadcast	ARP	60 Who has 192.168.0.155? Tell 192.168.0.80
1457..	2054.014571	PCSSystemtec_27:b8:..	Broadcast	ARP	60 Who has 192.168.0.138? Tell 192.168.0.80
1457..	2054.025850	PCSSystemtec_27:b8:..	Broadcast	ARP	60 Who has 192.168.0.99? Tell 192.168.0.80
1457..	2054.036162	PCSSystemtec_27:b8:..	Broadcast	ARP	60 Who has 192.168.0.249? Tell 192.168.0.80
1457..	2054.046476	PCSSystemtec_27:b8:..	Broadcast	ARP	60 Who has 192.168.0.125? Tell 192.168.0.80
1457..	2054.055808	PCSSystemtec_27:b8:..	Broadcast	ARP	60 Who has 192.168.0.78? Tell 192.168.0.80
1457..	2054.067101	PCSSystemtec_27:b8:..	Broadcast	ARP	60 Who has 192.168.0.14? Tell 192.168.0.80
1457..	2054.077408	PCSSystemtec_27:b8:..	Broadcast	ARP	60 Who has 192.168.0.42? Tell 192.168.0.80
1457..	2054.087753	PCSSystemtec_27:b8:..	Broadcast	ARP	60 Who has 192.168.0.2? Tell 192.168.0.80
1457..	2054.098050	PCSSystemtec_27:b8:..	Broadcast	ARP	60 Who has 192.168.0.150? Tell 192.168.0.80
1457..	2054.108359	PCSSystemtec_27:b8:..	Broadcast	ARP	60 Who has 192.168.0.77? Tell 192.168.0.80

```

Frame 38: 330 bytes on wire (2640 bits), 330 bytes captured (2640 bits)
Ethernet II, Src: PCSSystemtec_27:b8:a1 (08:00:27:b8:a1), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Discover)

```

4. No ARP

a. Filter: not arp

No.	Time	Source	Destination	Protocol	Length Info
1526..	2606.137182	192.168.0.77	192.168.0.80	TCP	54 36063 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
1526..	2606.297449	192.168.0.80	192.168.0.77	TCP	60 33590 → 32609 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1526..	2606.298527	192.168.0.77	192.168.0.80	TCP	54 32609 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
1526..	2606.462928	192.168.0.80	192.168.0.77	TCP	60 33590 → 61407 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1526..	2606.462928	192.168.0.77	192.168.0.80	TCP	54 61407 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
1526..	2623.147220	c4:01:41:48:00:00	CDP/VT/PaGP/UD...	CDP	350 Device ID: R1 Port ID: FastEthernet0/0
1526..	2686.082831	c4:01:41:48:00:00	CDP/VT/DP/PaGP/UD...	CDP	350 Device ID: R1 Port ID: FastEthernet0/0
1526..	2750.278624	c4:01:41:48:00:00	CDP/VT/DP/PaGP/UD...	CDP	350 Device ID: R1 Port ID: FastEthernet0/0
1526..	2815.514512	c4:01:41:48:00:00	CDP/VT/DP/PaGP/UD...	CDP	350 Device ID: R1 Port ID: FastEthernet0/0
1527..	2882.446523	c4:01:41:48:00:00	CDP/VT/DP/PaGP/UD...	CDP	350 Device ID: R1 Port ID: FastEthernet0/0
1527..	2948.284781	c4:01:41:48:00:00	CDP/VT/DP/PaGP/UD...	CDP	350 Device ID: R1 Port ID: FastEthernet0/0
1527..	3013.632681	c4:01:41:48:00:00	CDP/VT/DP/PaGP/UD...	CDP	350 Device ID: R1 Port ID: FastEthernet0/0

```

Frame 152702: 350 bytes on wire (2800 bits), 350 bytes captured (2800 bits)
IEEE 802.3 Ethernet
Logical-Link Control
Cisco Discovery Protocol

```

5. IPv4 only

a. Filter: ip

No.	Time	Source	Destination	Protocol	Length Info
1526..	2605.648884	192.168.0.80	192.168.0.77	TCP	60 33590 → 23387 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1526..	2605.648884	192.168.0.77	192.168.0.80	TCP	54 23387 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
1526..	2605.810259	192.168.0.80	192.168.0.77	TCP	60 33590 → 37206 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1526..	2605.811279	192.168.0.77	192.168.0.80	TCP	54 37206 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
1526..	2605.971267	192.168.0.80	192.168.0.77	TCP	60 33590 → 22457 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1526..	2605.971267	192.168.0.77	192.168.0.80	TCP	54 22457 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
1526..	2606.136201	192.168.0.80	192.168.0.77	TCP	60 33590 → 36063 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1526..	2606.137182	192.168.0.77	192.168.0.80	TCP	54 36063 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
1526..	2606.297449	192.168.0.80	192.168.0.77	TCP	60 33590 → 32609 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1526..	2606.298527	192.168.0.77	192.168.0.80	TCP	54 32609 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
1526..	2606.462928	192.168.0.80	192.168.0.77	TCP	60 33590 → 61407 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1526..	2606.462928	192.168.0.77	192.168.0.80	TCP	54 61407 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0

```

Frame 152695: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: PCSSyste
Internet Protocol Version 4, Src: 192.168.0.77, Dst: 192.168.0.80
Transmission Control Protocol, Src Port: 61407, Dst Port: 33590, Seq:

```

6. IPv4 address isn't 192.0.2.1

a. Filter: ip.addr != 192.0.2.1

No.	Time	Source	Destination	Protocol	Length Info
1526...	2605.648884	192.168.0.80	192.168.0.77	TCP	60 33590 → 23387 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1526...	2605.648884	192.168.0.77	192.168.0.80	TCP	54 23387 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
1526...	2605.810259	192.168.0.80	192.168.0.77	TCP	60 33590 → 37206 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1526...	2605.811279	192.168.0.77	192.168.0.80	TCP	54 37206 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
1526...	2605.971267	192.168.0.80	192.168.0.77	TCP	60 33590 → 22457 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1526...	2605.971267	192.168.0.77	192.168.0.80	TCP	54 22457 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
1526...	2606.136201	192.168.0.80	192.168.0.77	TCP	60 33590 → 36063 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1526...	2606.137182	192.168.0.77	192.168.0.80	TCP	54 36063 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
1526...	2606.297449	192.168.0.80	192.168.0.77	TCP	60 33590 → 32609 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1526...	2606.298527	192.168.0.77	192.168.0.80	TCP	54 32609 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
1526...	2606.462928	192.168.0.80	192.168.0.77	TCP	60 33590 → 61407 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1526...	2606.462928	192.168.0.77	192.168.0.80	TCP	54 61407 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
Frame 152695: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, link-layer type Ethernet II (Ethernet), source Private_66:68:00 (00:50:79:66:68:00), destination PC55ystem (00:0c:29:4d:0f:00)					
Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: PC55ystem (00:0c:29:4d:0f:00) [eth0]					
Internet Protocol Version 4, Src: 192.168.0.77, Dst: 192.168.0.80 [inet]					
Transmission Control Protocol, Src Port: 61407, Dst Port: 33590, Seq: 0, Ack: 1, Win: 1024, Len: 54					

7. IPv6 only

a. Filter: ipv6

No.	Time	Source	Destination	Protocol	Length Info
23	47.197723	fe80::a00:27ff:fe27... ff02::16		ICMPv6	90 Multicast Listener Report Message v2
25	50.884342	fe80::a00:27ff:fe27... ff02::2		ICMPv6	62 Router Solicitation
27	59.051154	fe80::a00:27ff:fe27... ff02::2		ICMPv6	62 Router Solicitation
30	75.937402	fe80::a00:27ff:fe27... ff02::2		ICMPv6	62 Router Solicitation
33	89.987165	:: ff02::16		ICMPv6	90 Multicast Listener Report Message v2
34	90.140308	:: ff02::1:27ff:b8a1		ICMPv6	86 Neighbor Solicitation for fe80::a00:27ff:fe27:b8a1
35	90.534793	:: ff02::16		ICMPv6	90 Multicast Listener Report Message v2
36	91.144522	fe80::a00:27ff:fe27... ff02::16		ICMPv6	90 Multicast Listener Report Message v2
37	91.224732	fe80::a00:27ff:fe27... ff02::2		ICMPv6	62 Router Solicitation
39	92.006632	fe80::a00:27ff:fe27... ff02::16		ICMPv6	90 Multicast Listener Report Message v2
41	95.460022	fe80::a00:27ff:fe27... ff02::2		ICMPv6	62 Router Solicitation
43	103.944504	fe80::a00:27ff:fe27... ff02::2		ICMPv6	62 Router Solicitation
45	121.206868	fe80::a00:27ff:fe27... ff02::2		ICMPv6	62 Router Solicitation

8. TCP only

a. Filter: tcp

No.	Time	Source	Destination	Protocol	Length Info
89	658.962992	192.168.0.80	192.168.0.77	TCP	60 33590 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
90	658.962992	192.168.0.77	192.168.0.80	TCP	54 587 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
91	658.965004	192.168.0.80	192.168.0.77	TCP	60 33590 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
92	658.965004	192.168.0.80	192.168.0.77	TCP	60 33590 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
93	658.965004	192.168.0.77	192.168.0.80	TCP	54 3306 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
94	658.965004	192.168.0.80	192.168.0.77	TCP	60 33590 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
95	658.965004	192.168.0.77	192.168.0.80	TCP	54 139 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
96	658.965004	192.168.0.80	192.168.0.77	TCP	60 33590 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
97	658.965004	192.168.0.77	192.168.0.80	TCP	54 445 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
98	658.965974	192.168.0.77	192.168.0.80	TCP	54 110 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
99	658.965974	192.168.0.80	192.168.0.77	TCP	60 33590 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
100	658.965974	192.168.0.77	192.168.0.80	TCP	54 143 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
101	658.965974	192.168.0.80	192.168.0.77	TCP	60 33590 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

9 UDP only

a Filter: udp

No.	Time	Source	Destination	Protocol	Length Info
78	645.952600	192.168.0.1	192.168.0.80	ICMP	70 Destination unreachable (Host unreachable)
79	648.442515	192.168.0.80	10.0.236.42	DNS	85 Standard query 0x28b3 PTR 77.0.168.192.in-addr.arpa
80	648.445123	192.168.0.1	192.168.0.80	ICMP	70 Destination unreachable (Host unreachable)
83	652.441681	192.168.0.80	10.0.237.43	DNS	85 Standard query 0x28b4 PTR 77.0.168.192.in-addr.arpa
84	652.451251	192.168.0.1	192.168.0.80	ICMP	70 Destination unreachable (Host unreachable)
85	654.942002	192.168.0.80	10.0.237.43	DNS	85 Standard query 0x28b5 PTR 77.0.168.192.in-addr.arpa
86	654.945459	192.168.0.1	192.168.0.80	ICMP	70 Destination unreachable (Host unreachable)
4471	768.674195	192.168.0.80	10.0.237.43	DNS	89 Standard query 0x84cb A location.services.mozilla.com
4472	768.676691	192.168.0.1	192.168.0.80	ICMP	70 Destination unreachable (Host unreachable)
4473	768.677664	192.168.0.80	10.0.236.42	DNS	89 Standard query 0x84cb A location.services.mozilla.com
4474	768.686984	192.168.0.1	192.168.0.80	ICMP	70 Destination unreachable (Host unreachable)
4475	768.687961	192.168.0.80	10.0.237.43	DNS	89 Standard query 0x84cb A location.services.mozilla.com
4478	768.697289	192.168.0.1	192.168.0.80	ICMP	70 Destination unreachable (Host unreachable)

10. Non-DNS port

- a. Filter: !(udp.port == 53 || tcp.port == 53)

No.	Time	Source	Destination	Protocol	Length Info
72	566.925529	c4:01:41:48:00:00	CDP/VT/PDP/PAgP/UD..	CDP	350 Device ID: R1 Port ID: FastEthernet0/0
73	619.344239	c4:01:41:48:00:00	DEC-MOP-Remote-Cons..	0x6002	77 DEC DNA Remote Console
74	629.715720	c4:01:41:48:00:00	CDP/VT/PDP/PAgP/UD..	CDP	350 Device ID: R1 Port ID: FastEthernet0/0
75	645.885110	PCSSystemtec_27:b8:..	Broadcast	ARP	60 Who has 192.168.0.77? Tell 192.168.0.80
76	645.886076	Private_66:68:00	PCSSystemtec_27:b8:..	ARP	60 192.168.0.77 is at 00:50:79:66:68:00
81	651.118451	PCSSystemtec_27:b8:..	c4:01:41:48:00:00	ARP	60 Who has 192.168.0.1? Tell 192.168.0.80
82	651.122295	c4:01:41:48:00:00	PCSSystemtec_27:b8:..	ARP	60 192.168.0.1 is at c4:01:41:48:00:00
87	658.961039	PCSSystemtec_27:b8:..	Broadcast	ARP	60 Who has 192.168.0.77? Tell 192.168.0.80
88	658.961039	Private_66:68:00	PCSSystemtec_27:b8:..	ARP	60 192.168.0.77 is at 00:50:79:66:68:00
89	658.962992	192.168.0.80	192.168.0.77	TCP	60 33590 > 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
90	658.962992	192.168.0.77	192.168.0.80	TCP	54 587 > 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
91	658.965004	192.168.0.80	192.168.0.77	TCP	60 33590 > 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
92	658.965004	192.168.0.80	192.168.0.77	TCP	60 33590 > 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

11. TCP or UDP port is 80 (HTTP)

- a. Filter: `tcp.port == 80 || udp.port == 80`

No.	Time	Source	Destination	Protocol	Length Info
112	658.967963	192.168.0.80	192.168.0.77	TCP	60 33590 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
114	658.967963	192.168.0.77	192.168.0.80	TCP	54 80 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
8252	1041.799498	192.168.0.80	192.168.0.77	TCP	74 46023 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3...
8255	1041.800477	192.168.0.77	192.168.0.80	TCP	54 80 → 46023 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
1022...	1927.690505	192.168.0.80	192.169.0.1	TCP	60 80 → 0 [SYN] Seq=0 Win=512 Len=0

Frame 112: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) (0% loss).
 ▶ Ethernet II, Src: PCSystmtec_27:b8:a1 (08:00:27:27:b8:a1), Dst: Private (08:00:27:00:00:00)
 ▶ Internet Protocol Version 4, Src: 192.168.0.80, Dst: 192.168.0.77
 ▶ Transmission Control Protocol, Src Port: 33590, Dst Port: 80, Seq: 0,

12. No ARP and no DNS

- a. Filter: not arp and not dns

No.	Time	Source	Destination	Protocol	Length Info
106	658.966893	192.168.0.80	192.168.0.77	TCP	60 33590 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
107	658.966893	192.168.0.77	192.168.0.80	TCP	54 111 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
108	658.966893	192.168.0.77	192.168.0.80	TCP	54 1720 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
109	658.967963	192.168.0.80	192.168.0.77	TCP	60 33590 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
110	658.967963	192.168.0.80	192.168.0.77	TCP	60 33590 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
111	658.967963	192.168.0.77	192.168.0.80	TCP	54 113 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
112	658.967963	192.168.0.80	192.168.0.77	TCP	60 33590 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
113	658.967963	192.168.0.77	192.168.0.80	TCP	54 80 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
114	658.967963	192.168.0.77	192.168.0.80	TCP	54 80 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
115	658.967963	192.168.0.80	192.168.0.77	TCP	60 33590 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
116	658.967963	192.168.0.77	192.168.0.80	TCP	54 199 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
117	658.969468	192.168.0.80	192.168.0.77	TCP	60 33590 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
118	658.970535	192.168.0.77	192.168.0.80	TCP	54 443 → 33590 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0

```

Frame 112: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) 
Ethernet II, Src: PCSSystemtec_27:b8:a1 (08:00:27:b8:a1), Dst: Priv (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 192.168.0.80, Dst: 192.168.0.77
Transmission Control Protocol, Src Port: 33590, Dst Port: 80, Seq: 0, 

```

13. ICMP

a. Filter: icmp

No.	Time	Source	Destination	Protocol	Length Info
→ 4	111.386645	192.168.0.80	192.168.0.77	ICMP	98 Echo (ping) request
← 5	111.388149	192.168.0.77	192.168.0.80	ICMP	98 Echo (ping) reply
6	112.390044	192.168.0.80	192.168.0.77	ICMP	98 Echo (ping) request
7	112.391022	192.168.0.77	192.168.0.80	ICMP	98 Echo (ping) reply
8	113.393407	192.168.0.80	192.168.0.77	ICMP	98 Echo (ping) request
9	113.394385	192.168.0.77	192.168.0.80	ICMP	98 Echo (ping) reply
10	114.395661	192.168.0.80	192.168.0.77	ICMP	98 Echo (ping) request
11	114.396642	192.168.0.77	192.168.0.80	ICMP	98 Echo (ping) reply
15	128.298964	192.168.0.80	192.168.0.1	ICMP	98 Echo (ping) request
16	128.305601	192.168.0.1	192.168.0.80	ICMP	98 Echo (ping) reply
17	129.302428	192.168.0.80	192.168.0.1	ICMP	98 Echo (ping) request
18	129.305904	192.168.0.1	192.168.0.80	ICMP	98 Echo (ping) reply
19	130.305213	192.168.0.80	192.168.0.1	ICMP	98 Echo (ping) request

```

Frame 4: 98 bytes on wire (784 bits), 98 bytes cap 
Ethernet II, Src: PCSSystemtec_27:b8:a1 (08:00:27:b8:a1), Dst: 00:00:00:00:00:00
Internet Protocol Version 4, Src: 192.168.0.80, Dst: 192.168.0.1
Internet Control Message Protocol

```

GNS3LabSimulationCapturedPackets.pcapng

Packets: 793 · Displayed: 17 (2.1%) Profile: Default

Analyzing the captured packets for security threats

1. Ethernet type 0x0806 (ARP)
 - a. Filter: eth.type == 0x0806
 - b. Excessive Arp traffic could indicate Arp spoofing or floods
 - c. Can disrupt communication or redirect traffic malicious actors
2. Ethernet broadcast
 - a. Filter: eth.addr == ff:ff:ff:ff:ff:ff
 - b. Broadcast storms or flood can be indication of DoS attacks
 - c. Can reveal network misconfiguration
3. No ARP
 - a. Filter: not arp
 - b. ARP traffic exclusion can overlook ARP-related attacks
4. IPv4 only
 - a. Filter: ip
 - b. Potentially missing ipv6 adverse threats
5. IPv4 address isn't 192.0.2.1
 - a. Filter: ip.addr != 192.0.2.1
 - b. Good to isolate other traffic
6. IPv6 only
 - a. Filter: ipv6
 - b. Can reveal ipv6 specific attacks
7. TCP only
 - a. Filter: tcp
 - b. Focus on attacks like SYN flood
8. UDP only
 - a. Filter: udp
 - b. Detecting DNS amplification, UDP flood or other UDP-based attacks
9. Non-DNS port
 - a. Filter: !(udp.port == 53 || tcp.port == 53)
 - b. Identify non DNS traffic but risk overlooking DNS tunnelling attacks
10. TCP or UDP port is 80 (HTTP)
 - a. Filter: tcp.port == 80 || udp.port == 80
 - b. Identify http-based attacks like http flood or malicious payload
11. No ARP and no DNS
 - a. Filter: not arp and not dns
 - b. Missing ARP spoofing or DNS tunneling attack
12. ICMP
 - a. Filter: icmp
 - b. Detect icmp -based attacks like ping flood or reconnaissance