Lab Assignment 3: Exploring the Tools

Course Code:	CYB301
Course Name:	Security, Defense, and Response
Time:	90+ minutes in class
Student name:	Saiprasad Raman
Student ID:	23074624

Materials and Resources

Textbooks:	N/A
Software:	Kali Linux Windows 11 Enterprise VM
Websites:	Wireshark Solar Winds
Videos:	N/A
Other:	N/A

Assignment Description

You will install and use various tools in this lab for accessing and exploring networks for different operating systems (Oss).

Assignment Steps

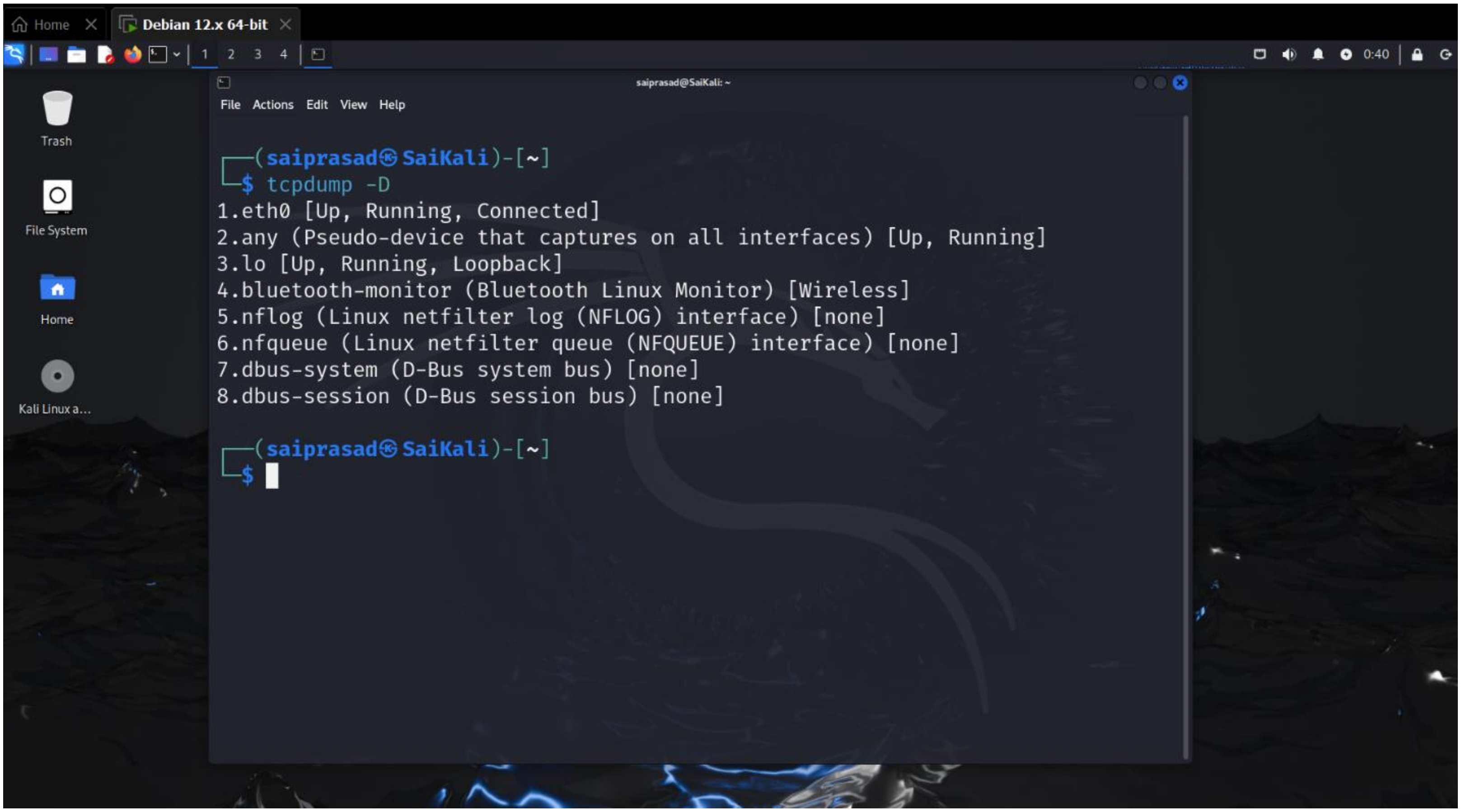
Activity 1: Protocol Analyzer: tcpdump

Log in to Kali Linux as a root user.

tcpdump is a common packet sniffer for Linux. It works from the shell, and it is relatively easy to use. Type the following command:

- tcpdump -D

This command will display all the interfaces on your computer so you can select which one to use.

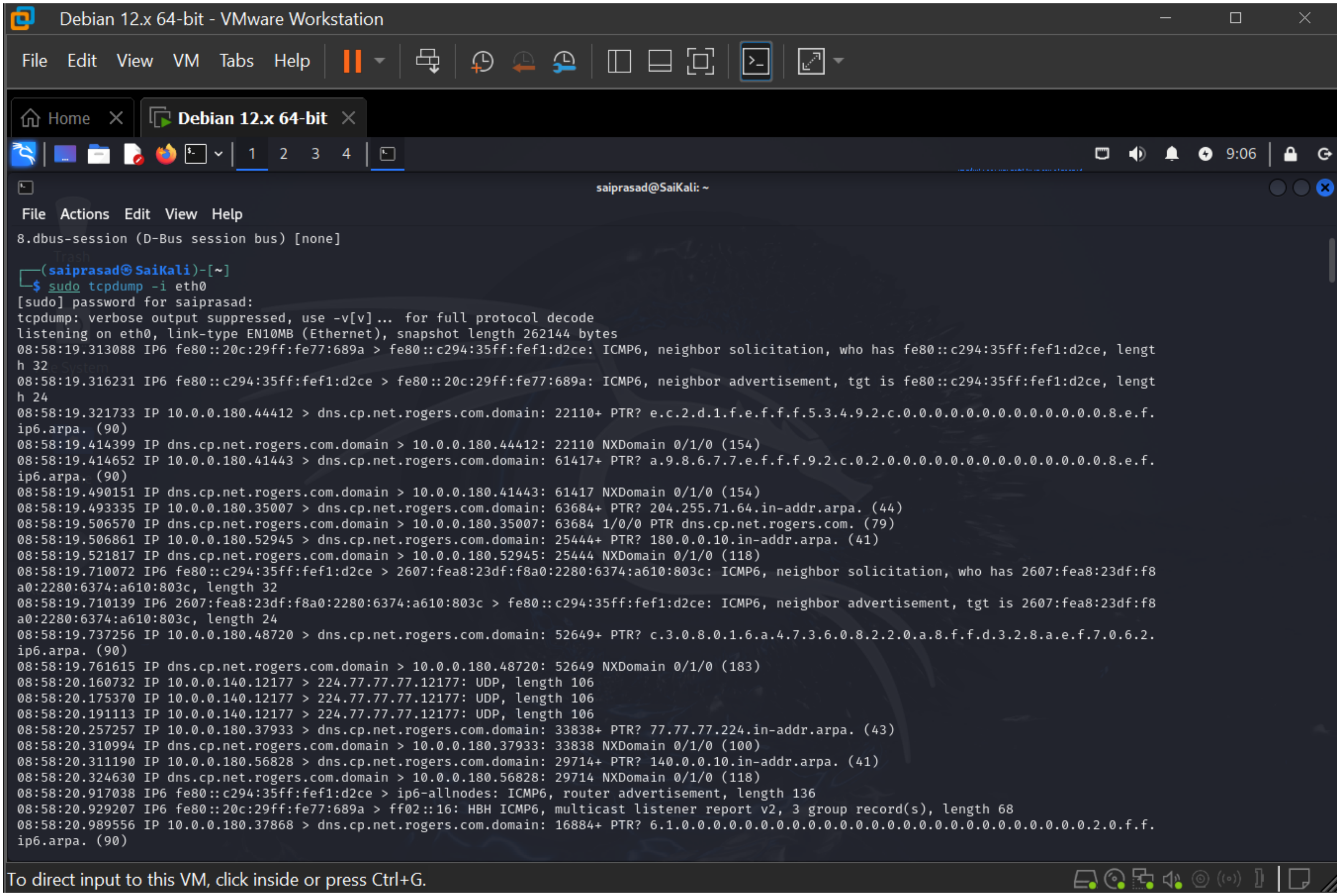


```
┌──(saiprasad㉿SaiKali)-[~]
└─$ tcpdump -D
1.eth0 [Up, Running, Connected]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.bluetooth-monitor (Bluetooth Linux Monitor) [Wireless]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
7.dbus-system (D-Bus system bus) [none]
8.dbus-session (D-Bus session bus) [none]

┌──(saiprasad㉿SaiKali)-[~]
└─$ 
```

- tcpdump -i eth0

This causes tcpdump to capture the network traffic for the network card, eth0.


Debian 12.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Home
Debian 12.x 64-bit
1 2 3 4
9:06
saiprasad@SaiKali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.

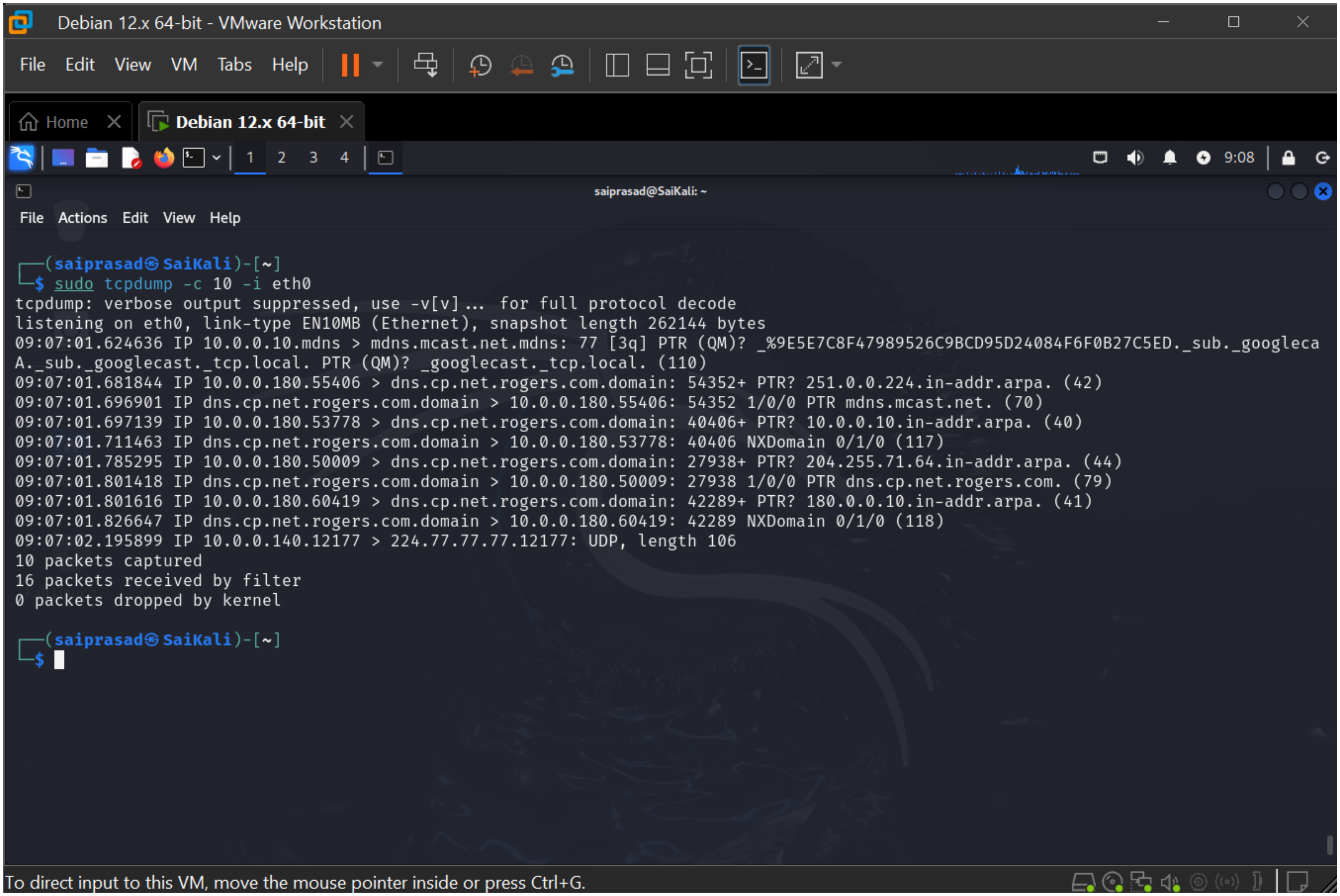
```
8.dbus-session (D-Bus session bus) [none]

┌──(saiprasad㉿SaiKali)-[~]
└─$ sudo tcpdump -i eth0
[sudo] password for saiprasad:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
08:58:19.313088 IP6 fe80::20c:29ff:fe77:689a > fe80::c294:35ff:fef1:d2ce: ICMP6, neighbor solicitation, who has fe80::c294:35ff:fef1:d2ce, lengt
h 32
08:58:19.316231 IP6 fe80::c294:35ff:fef1:d2ce > fe80::20c:29ff:fe77:689a: ICMP6, neighbor advertisement, tgt is fe80::c294:35ff:fef1:d2ce, lengt
h 24
08:58:19.321733 IP 10.0.0.180.44412 > dns.cp.net.rogers.com.domain: 22110+ PTR? e.c.2.d.1.f.e.f.f.f.5.3.4.9.2.c.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.
ip6.arpa. (90)
08:58:19.414399 IP dns.cp.net.rogers.com.domain > 10.0.0.180.44412: 22110 NXDomain 0/1/0 (154)
08:58:19.414652 IP 10.0.0.180.41443 > dns.cp.net.rogers.com.domain: 61417+ PTR? a.9.8.6.7.7.e.f.f.f.9.2.c.0.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.
ip6.arpa. (90)
08:58:19.490151 IP dns.cp.net.rogers.com.domain > 10.0.0.180.41443: 61417 NXDomain 0/1/0 (154)
08:58:19.493335 IP 10.0.0.180.35007 > dns.cp.net.rogers.com.domain: 63684+ PTR? 204.255.71.64.in-addr.arpa. (44)
08:58:19.506570 IP dns.cp.net.rogers.com.domain > 10.0.0.180.35007: 63684 1/0/0 PTR dns.cp.net.rogers.com. (79)
08:58:19.506861 IP 10.0.0.180.52945 > dns.cp.net.rogers.com.domain: 25444+ PTR? 180.0.0.10.in-addr.arpa. (41)
08:58:19.521817 IP dns.cp.net.rogers.com.domain > 10.0.0.180.52945: 25444 NXDomain 0/1/0 (118)
08:58:19.710072 IP6 fe80::c294:35ff:fef1:d2ce > 2607:fea8:23df:f8a0:2280:6374:a610:803c: ICMP6, neighbor solicitation, who has 2607:fea8:23df:f8
a0:2280:6374:a610:803c, length 32
08:58:19.710139 IP6 2607:fea8:23df:f8a0:2280:6374:a610:803c > fe80::c294:35ff:fef1:d2ce: ICMP6, neighbor advertisement, tgt is 2607:fea8:23df:f8
a0:2280:6374:a610:803c, length 24
08:58:19.737256 IP 10.0.0.180.48720 > dns.cp.net.rogers.com.domain: 52649+ PTR? c.3.0.8.0.1.6.a.4.7.3.6.0.8.2.2.0.a.8.f.f.d.3.2.8.a.e.f.7.0.6.2.
ip6.arpa. (90)
08:58:19.761615 IP dns.cp.net.rogers.com.domain > 10.0.0.180.48720: 52649 NXDomain 0/1/0 (183)
08:58:20.160732 IP 10.0.0.140.12177 > 224.77.77.77.12177: UDP, length 106
08:58:20.175370 IP 10.0.0.140.12177 > 224.77.77.77.12177: UDP, length 106
08:58:20.191113 IP 10.0.0.140.12177 > 224.77.77.77.12177: UDP, length 106
08:58:20.257257 IP 10.0.0.180.37933 > dns.cp.net.rogers.com.domain: 33838+ PTR? 77.77.77.224.in-addr.arpa. (43)
08:58:20.310994 IP dns.cp.net.rogers.com.domain > 10.0.0.180.37933: 33838 NXDomain 0/1/0 (100)
08:58:20.311190 IP 10.0.0.180.56828 > dns.cp.net.rogers.com.domain: 29714+ PTR? 140.0.0.10.in-addr.arpa. (41)
08:58:20.324630 IP dns.cp.net.rogers.com.domain > 10.0.0.180.56828: 29714 NXDomain 0/1/0 (118)
08:58:20.917038 IP6 fe80::c294:35ff:fef1:d2ce > ip6-allnodes: ICMP6, router advertisement, length 136
08:58:20.929207 IP6 fe80::20c:29ff:fe77:689a > ff02::16: HBH ICMP6, multicast listener report v2, 3 group record(s), length 68
08:58:20.989556 IP 10.0.0.180.37868 > dns.cp.net.rogers.com.domain: 16884+ PTR? 6.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.
ip6.arpa. (90)
```

You can also alter tcpdump's behaviour with a variety of command flags such as the following:

- tcpdump -c 10 -i eth0

This tells tcpdump to capture only the first 100 packets on interface eth0 and then stop.

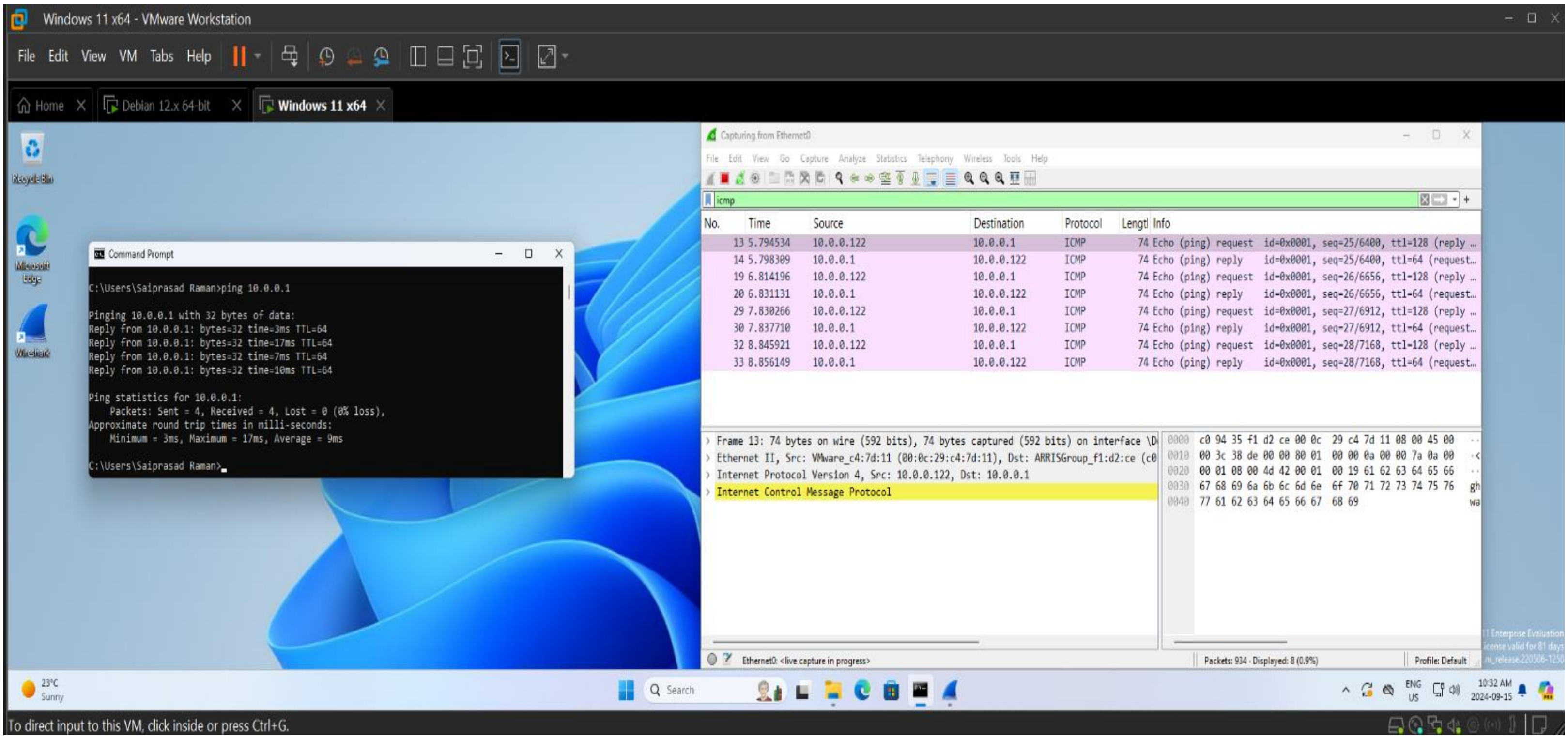

Debian 12.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Home
Debian 12.x 64-bit
1 2 3 4
9:08
saiprasad@SaiKali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
┌──(saiprasad㉿SaiKali)-[~]
└─$ sudo tcpdump -c 10 -i eth0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
09:07:01.624636 IP 10.0.0.10.mdns > mdns.mcast.net.mdns: 77 [3q] PTR (QM)? _%9E5E7C8F47989526C9BCD95D24084F6F0B27C5ED._sub._googleca
A._sub._googlecast._tcp.local. PTR (QM)? _googlecast._tcp.local. (110)
09:07:01.681844 IP 10.0.0.180.55406 > dns.cp.net.rogers.com.domain: 54352+ PTR? 251.0.0.224.in-addr.arpa. (42)
09:07:01.696901 IP dns.cp.net.rogers.com.domain > 10.0.0.180.55406: 54352 1/0/0 PTR mdns.mcast.net. (70)
09:07:01.697139 IP 10.0.0.180.53778 > dns.cp.net.rogers.com.domain: 40406+ PTR? 10.0.0.10.in-addr.arpa. (40)
09:07:01.711463 IP dns.cp.net.rogers.com.domain > 10.0.0.180.53778: 40406 NXDomain 0/1/0 (117)
09:07:01.785295 IP 10.0.0.180.50009 > dns.cp.net.rogers.com.domain: 27938+ PTR? 204.255.71.64.in-addr.arpa. (44)
09:07:01.801418 IP dns.cp.net.rogers.com.domain > 10.0.0.180.50009: 27938 1/0/0 PTR dns.cp.net.rogers.com. (79)
09:07:01.801616 IP 10.0.0.180.60419 > dns.cp.net.rogers.com.domain: 42289+ PTR? 180.0.0.10.in-addr.arpa. (41)
09:07:01.826647 IP dns.cp.net.rogers.com.domain > 10.0.0.180.60419: 42289 NXDomain 0/1/0 (118)
09:07:02.195899 IP 10.0.0.140.12177 > 224.77.77.77.12177: UDP, length 106
10 packets captured
16 packets received by filter
0 packets dropped by kernel

┌──(saiprasad㉿SaiKali)-[~]
└─$ 
```

Activity 2: Protocol Analyzer: Wireshark

Log in to Windows 11 Enterprise VM and then download and install Wireshark.


Windows 11 x64 - VMware Workstation
File Edit View VM Tabs Help
Home
Debian 12.x 64-bit
Windows 11 x64
Recycle Bin
Microsoft Edge
Wireshark
Command Prompt
Capturing from Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Ethernet0: <live capture in progress>
Packets: 934 · Displayed: 8 (0.9%)
Profile: Default
23°C
Sunny
Search
To direct input to this VM, click inside or press Ctrl+G.

```
C:\Users\Saiprasad Raman>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:
Reply from 10.0.0.1: bytes=32 time=3ms TTL=64
Reply from 10.0.0.1: bytes=32 time=17ms TTL=64
Reply from 10.0.0.1: bytes=32 time=7ms TTL=64
Reply from 10.0.0.1: bytes=32 time=10ms TTL=64

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 17ms, Average = 9ms

C:\Users\Saiprasad Raman>
```

icmp

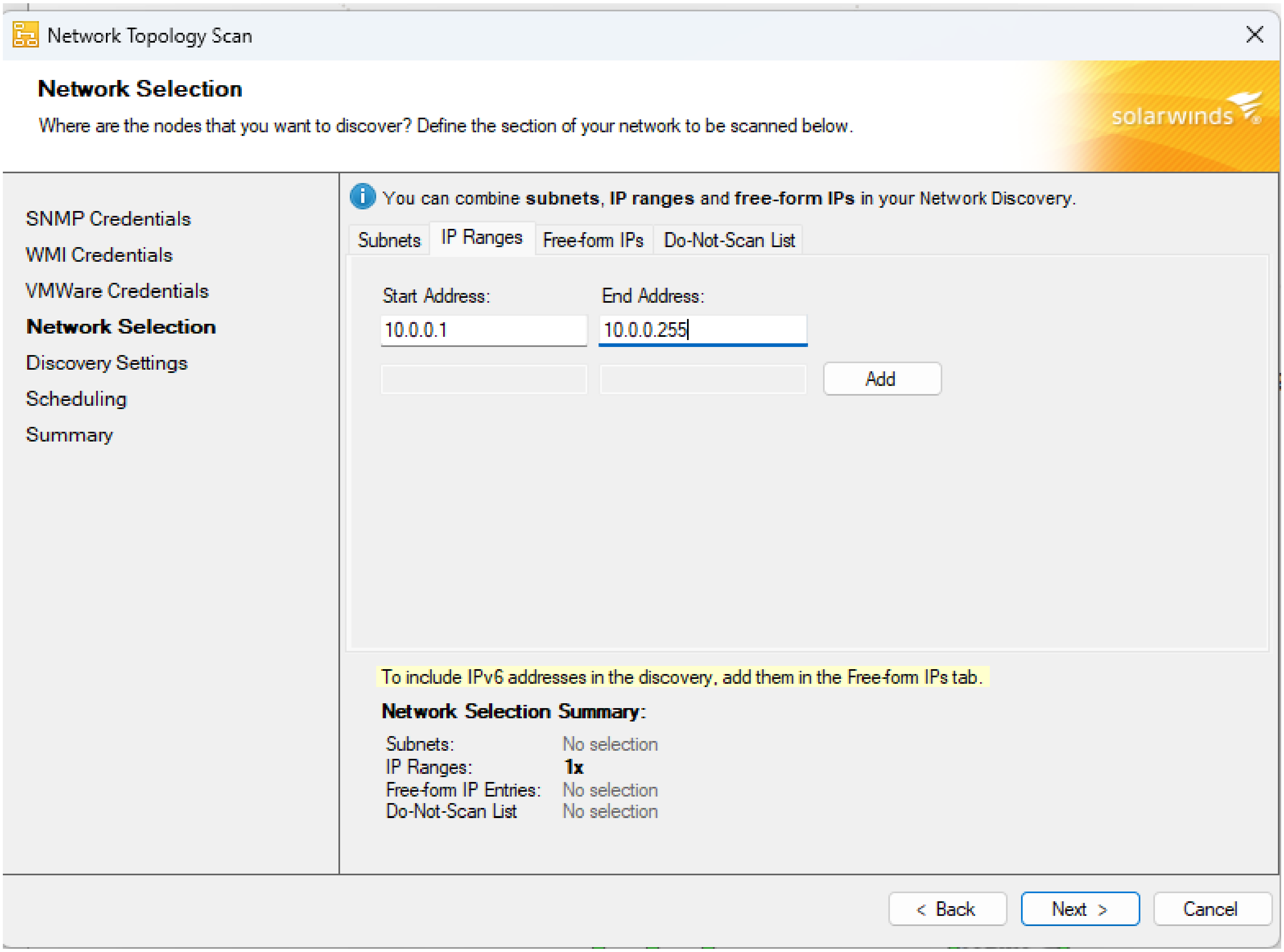
```
No.  Time      Source       Destination  Protocol  Lengt Info
  13 5.794534  10.0.0.122   10.0.0.1     ICMP      74 Echo (ping) request  id=0x0001, seq=25/6400, ttl=128 (reply …
  14 5.798309  10.0.0.1     10.0.0.122   ICMP      74 Echo (ping) reply    id=0x0001, seq=25/6400, ttl=64 (request…
  19 6.814196  10.0.0.122   10.0.0.1     ICMP      74 Echo (ping) request  id=0x0001, seq=26/6656, ttl=128 (reply …
  20 6.831131  10.0.0.1     10.0.0.122   ICMP      74 Echo (ping) reply    id=0x0001, seq=26/6656, ttl=64 (request…
  29 7.830266  10.0.0.122   10.0.0.1     ICMP      74 Echo (ping) request  id=0x0001, seq=27/6912, ttl=128 (reply …
  30 7.837710  10.0.0.1     10.0.0.122   ICMP      74 Echo (ping) reply    id=0x0001, seq=27/6912, ttl=64 (request…
  32 8.845921  10.0.0.122   10.0.0.1     ICMP      74 Echo (ping) request  id=0x0001, seq=28/7168, ttl=128 (reply …
  33 8.856149  10.0.0.1     10.0.0.122   ICMP      74 Echo (ping) reply    id=0x0001, seq=28/7168, ttl=64 (request…
```

```
> Frame 13: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \D
> Ethernet II, Src: VMware_c4:7d:11 (00:0c:29:c4:7d:11), Dst: ARRISGroup_f1:d2:ce (c0
> Internet Protocol Version 4, Src: 10.0.0.122, Dst: 10.0.0.1
> Internet Control Message Protocol
```

```
0000  c0 94 35 f1 d2 ce 00 0c  29 c4 7d 11 08 00 45 00
0010  00 3c 38 de 00 00 80 01  00 00 0a 00 00 7a 0a 00
0020  00 01 08 00 4d 42 00 01  00 19 61 62 63 64 65 66
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76
0040  77 61 62 63 64 65 66 67  68 69
```

Wireshark lets you determine the time difference in the packets which is helpful to determine why the packets are being interrupted and which domain is affecting it. It also shows the expected packet while the missing packets gets highlighted in 'Red' TCP protocol. The [Request/Response in frame] section gives us the details of the connected segments further determining the delay in packets and the interruptions between these segments. If we go through each packet and trace its flow, we would be able to trace the websites and for http connections it is possible look at the images from the website via the info section. We can also retrieve usernames and passwords for Telnet and FTP connections via right clicking on the segment and selecting 'follow TCP stream'.

Activity 3: Network Scanner: Solar Winds



Network Selection

Where are the nodes that you want to discover? Define the section of your network to be scanned below.

You can combine **subnets**, **IP ranges** and **free-form IPs** in your Network Discovery.

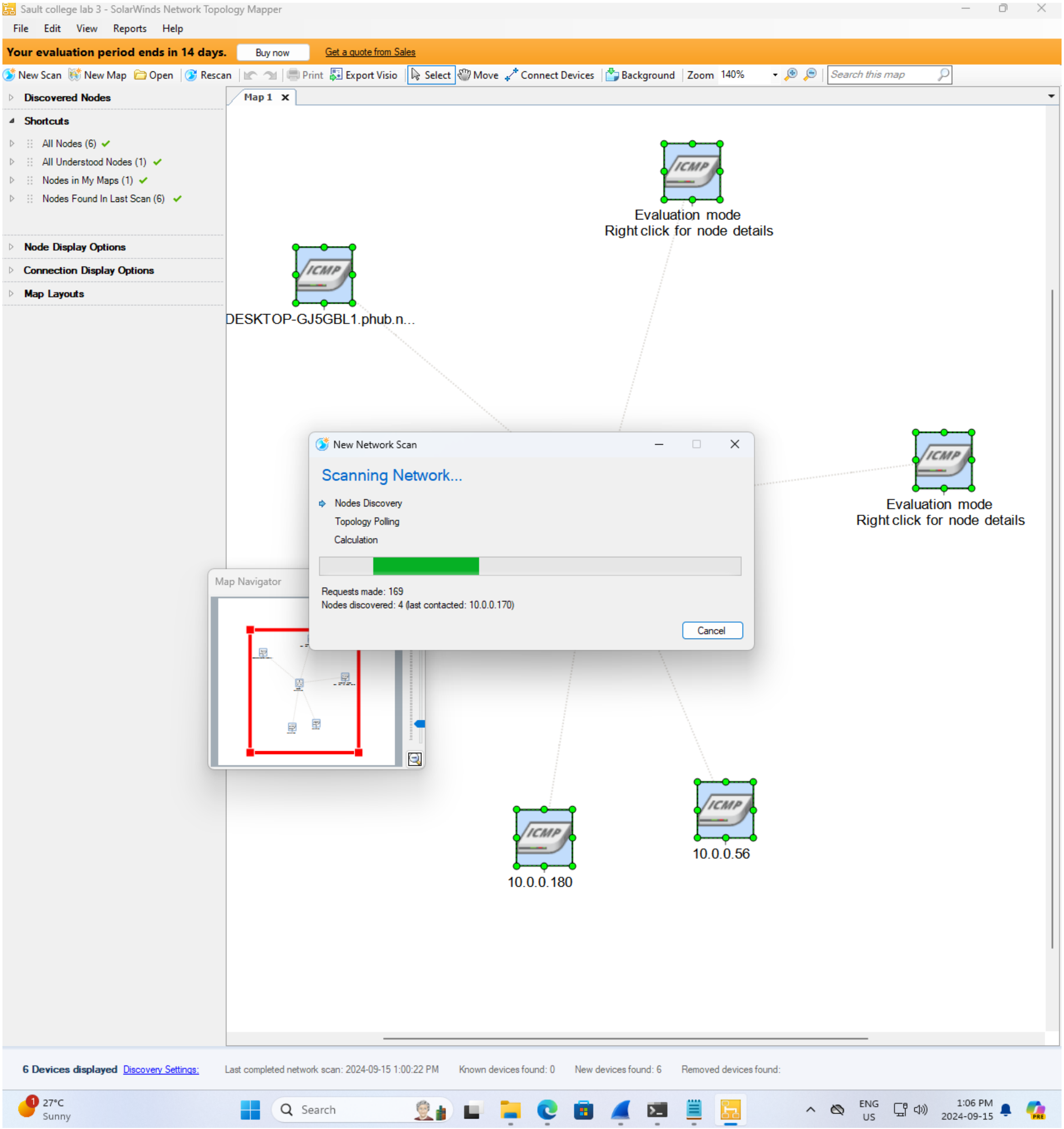
Start Address: 10.0.0.1

End Address: 10.0.0.255

To include IPv6 addresses in the discovery, add them in the Free-form IPs tab.

Network Selection Summary:

Subnets:	No selection
IP Ranges:	**1x**
Free-form IP Entries:	No selection
Do-Not-Scan List	No selection



New Network Scan

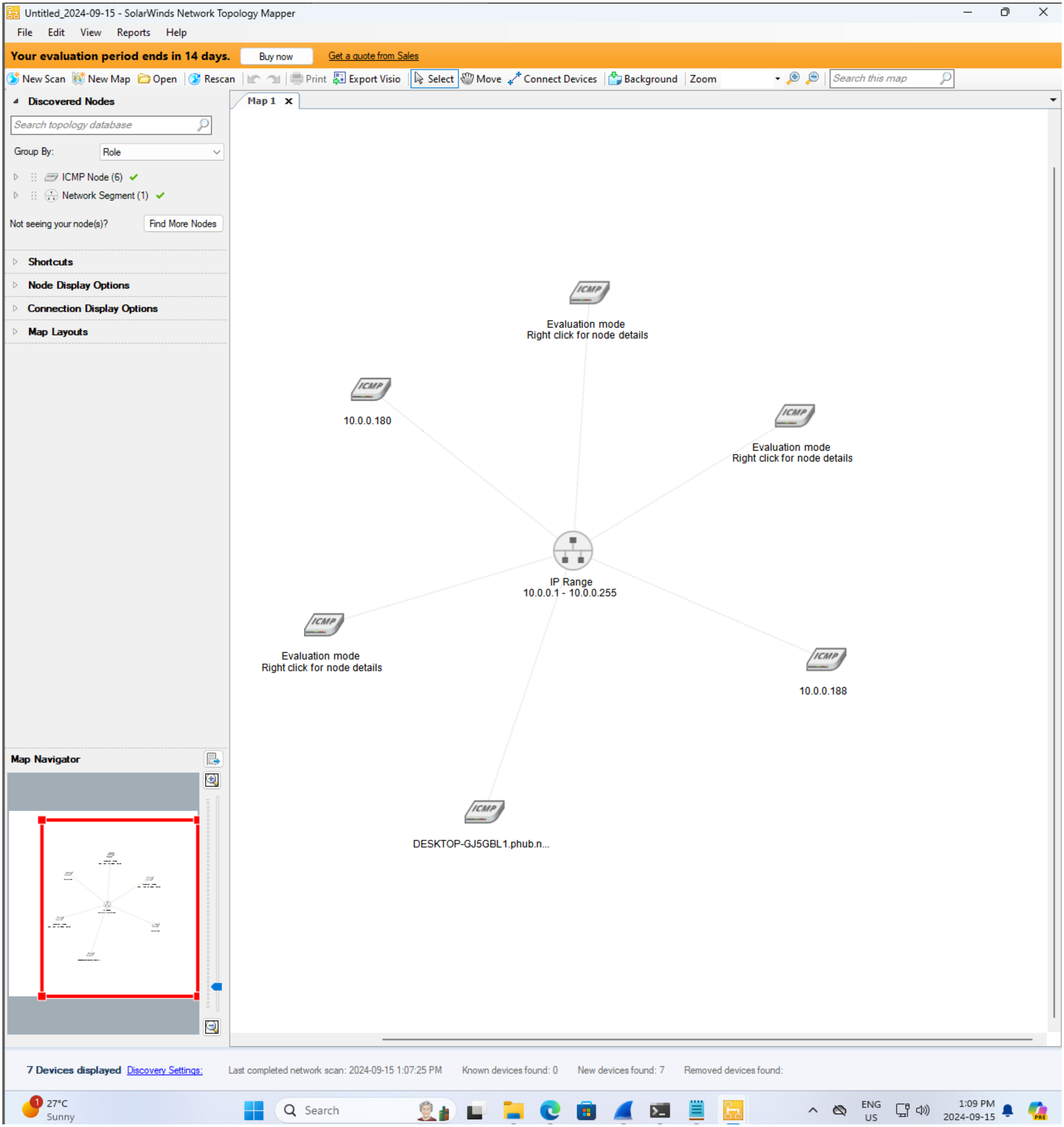
Scanning Network...

- Nodes Discovery
- Topology Polling
- Calculation

Requests made: 169
Nodes discovered: 4 (last contacted: 10.0.0.170)

Cancel

6 Devices displayed Discovery Settings: Last completed network scan: 2024-09-15 1:00:22 PM Known devices found: 0 New devices found: 6 Removed devices found:



Your evaluation period ends in 14 days.

Not seeing your node(s)?

7 Devices displayed Discovery Settings: Last completed network scan: 2024-09-15 1:07:25 PM Known devices found: 0 New devices found: 7 Removed devices found: