

9. Analysing network packet stream using tcpdump and wireshark. Perform basic network service tests using nc.

Installing tcpdump and analysing network packet stream

Procedure:

Step 1: Update the system

sudo apt-get update

Step 2: Install tcpdump on the system

sudo apt-get install tcpdump

Step 3: Check the version

tcpdump --version

To capture packets from a source ip.

tcpdump -n src host ip-address

OUTPUT

```
ner-VirtualBox:~$ sudo tcpdump -v
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
09:30:20.938746 IP (tos 0x0, ttl 64, id 17814, offset 0, flags [DF], proto UDP (17), length 75)
    ner-VirtualBox.domain.name.56383 > RTK_GW.domain.name.domain: 50943+ A? connectivity-check.ubuntu.com. (47)
09:30:20.946971 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto UDP (17), length 171)
    RTK_GW.domain.name.domain > ner-VirtualBox.domain.name.56383: 50943 2/3/0 connectivity-check.ubuntu.com. A 35.232.111.17, connectivity-check.ubuntu.com. A 35.224.170.84 (143)
09:30:20.948698 IP (tos 0x0, ttl 64, id 43917, offset 0, flags [DF], proto TCP (6), length 60)
    ner-VirtualBox.domain.name.37590 > 84.170.224.35.bc.googleusercontent.com.http: Flags [S], cksum 0xf411 (incorrect -> 0xdb0e), seq 2387821799, win 64240, options [mss 1460,sackOK,TS val 3821024155 ec
r 0,nop,wscale 7], length 0
09:30:20.976316 IP (tos 0x0, ttl 64, id 17815, offset 0, flags [DF], proto UDP (17), length 72)
    ner-VirtualBox.domain.name.44641 > RTK_GW.domain.name.domain: 33465+ PTR? 1.101.168.192.in-addr.arpa. (44)
09:30:20.978261 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto UDP (17), length 104)
    RTK_GW.domain.name.domain > ner-VirtualBox.domain.name.44641: 33465* 1/0/0 1.101.168.192.in-addr.arpa. PTR RTK_GW.domain.name. (76)
09:30:20.979636 IP (tos 0x0, ttl 64, id 17816, offset 0, flags [DF], proto UDP (17), length 72)
    ner-VirtualBox.domain.name.37289 > RTK_GW.domain.name.domain: 16181+ PTR? 6.101.168.192.in-addr.arpa. (44)
09:30:20.981791 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto UDP (17), length 112)
    RTK_GW.domain.name.domain > ner-VirtualBox.domain.name.37289: 16181* 1/0/0 6.101.168.192.in-addr.arpa. PTR ner-VirtualBox.domain.name. (84)
09:30:20.983548 IP (tos 0x0, ttl 64, id 17817, offset 0, flags [DF], proto UDP (17), length 72)
    ner-VirtualBox.domain.name.36180 > RTK_GW.domain.name.domain: 8824+ PTR? 84.170.224.35.in-addr.arpa. (44)
09:30:21.016407 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto UDP (17), length 124)
    RTK_GW.domain.name.domain > ner-VirtualBox.domain.name.36180: 8824 1/0/0 84.170.224.35.in-addr.arpa. PTR 84.170.224.35.bc.googleusercontent.com. (96)
09:30:21.951780 IP (tos 0x0, ttl 64, id 43918, offset 0, flags [DF], proto TCP (6), length 60)
    ner-VirtualBox.domain.name.37590 > 84.170.224.35.bc.googleusercontent.com.http: Flags [S], cksum 0xf411 (incorrect -> 0xd783), seq 2387821799, win 64240, options [mss 1460,sackOK,TS val 3821025158 ec
r 0,nop,wscale 7], length 0
09:30:22.241307 IP (tos 0x0, ttl 60, id 0, offset 0, flags [DF], proto TCP (6), length 60)
    84.170.224.35.bc.googleusercontent.com.http > ner-VirtualBox.domain.name.37590: Flags [S.], cksum 0x1d0d (correct), seq 2347169248, ack 2387821800, win 64768, options [mss 1420,sackOK,TS val 33017328
41 ecr 3821025158,nop,wscale 7], length 0
09:30:22.241416 IP (tos 0x0, ttl 64, id 43919, offset 0, flags [DF], proto TCP (6), length 52)
    ner-VirtualBox.domain.name.37590 > 84.170.224.35.bc.googleusercontent.com.http: Flags [.], cksum 0xf409 (incorrect -> 0x459a), ack 1, win 502, options [nop,nop,TS val 3821025448 ecr 3301732841], leng
th 0
09:30:22.242129 IP (tos 0x0, ttl 64, id 43920, offset 0, flags [DF], proto TCP (6), length 139)
    ner-VirtualBox.domain.name.37590 > 84.170.224.35.bc.googleusercontent.com.http: Flags [P.], cksum 0xf460 (incorrect -> 0x83f2), seq 1:88, ack 1, win 502, options [nop,nop,TS val 3821025449 ecr 330173
2841], length 87: HTTP, length: 87
    GET / HTTP/1.1
    Host: connectivity-check.ubuntu.com
    Accept: */*
    Connection: close
```

Installing wireshark and analysing network packet stream

Wireshark is a free and open-source network protocol analyser widely used around the globe. With Wireshark, you can capture incoming and outgoing packets of a network in real-time and use it for network troubleshooting, packet analysis, software and communication protocol development, and many more.

Procedure:

Step 1: Update the system

sudo apt-get update

Step 2: Install wireshark on the system

sudo apt-get install wireshark

Step 3: Check the version

wireshark --version

OUTPUT

```
hermes-VirtualBox:~$ sudo apt install wireshark
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libc-ares2 libdouble-conversion3 liblua5.2-0 libpcr2-16-0 libqt5core5a libqt5dbus5 libqt5gui5 libqt5multimedia5 libqt5multimedia5-plugins libqt5multimedia5-tools libqt5multimedia5-widgets
  libqt5network5 libqt5opengl5 libqt5sprintsupport5 libqt5svg5 libqt5widgets5 libsnm2ldbl libsnappy1v5 libspandsp2 libssh-gcrypt-4 libwireshark-data libwireshark3 libwireshark3-dev libwireshark3-gtk
  libxcb-xinerama0 libxcb-xinput0 qt5-gtk-platformtheme qttranslations5-l10n wireshark-common wireshark-qt
Suggested packages:
  qt5-image-formats-plugins qtwallands snmp-mibs-downloader geolupdate geolp-database geolp-database-extra libjs-leaflet libjs-leaflet.markercluster wireshark-doc
The following NEW packages will be installed:
  libc-ares2 libdouble-conversion3 liblua5.2-0 libpcr2-16-0 libqt5core5a libqt5dbus5 libqt5gui5 libqt5multimedia5 libqt5multimedia5-plugins libqt5multimedia5-tools libqt5multimedia5-widgets
  libqt5network5 libqt5opengl5 libqt5sprintsupport5 libqt5svg5 libqt5widgets5 libsnm2ldbl libsnappy1v5 libspandsp2 libssh-gcrypt-4 libwireshark-data libwireshark3 libwireshark3-dev libwireshark3-gtk
  libxcb-xinerama0 libxcb-xinput0 qt5-gtk-platformtheme qttranslations5-l10n wireshark-common wireshark-qt
0 upgraded, 31 newly installed, 0 to remove and 0 not upgraded.
Need to get 32.9 MB of archives.
After this operation, 163 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ln.archive.ubuntu.com/ubuntu focal/universe amd64 libdouble-conversion3 amd64 3.1.5-4ubuntu1 [37.9 kB]
Get:2 http://ln.archive.ubuntu.com/ubuntu focal/main amd64 libpcr2-16-0 amd64 10.34-7 [184 kB]
Get:3 http://ln.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5core5a amd64 5.12.8+dfsg-0ubuntu1 [2,005 kB]
Get:4 http://ln.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5dbus5 amd64 5.12.8+dfsg-0ubuntu1 [208 kB]
Get:5 http://ln.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5network5 amd64 5.12.8+dfsg-0ubuntu1 [674 kB]
Get:6 http://ln.archive.ubuntu.com/ubuntu focal/main amd64 libxcb-xinerama0 amd64 1.14-2 [5,268 B]
Get:7 http://ln.archive.ubuntu.com/ubuntu focal/main amd64 libxcb-xinput0 amd64 1.14-2 [29.3 kB]
Get:8 http://ln.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5gui5 amd64 5.12.8+dfsg-0ubuntu1 [2,971 kB]
Get:9 http://ln.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5widgets5 amd64 5.12.8+dfsg-0ubuntu1 [2,293 kB]
Get:10 http://ln.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5svg5 amd64 5.12.8-0ubuntu1 [131 kB]
Get:11 http://ln.archive.ubuntu.com/ubuntu focal/main amd64 liblua5.2-0 amd64 5.2.4-1-bud1ds [186 kB]
Get:12 http://ln.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5multimedia5 amd64 5.12.8-0ubuntu1 [283 kB]
Get:13 http://ln.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5opengl5 amd64 5.12.8+dfsg-0ubuntu1 [136 kB]
Get:14 http://ln.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5multimedia5-widgets5 amd64 5.12.8-0ubuntu1 [36.8 kB]
Get:15 http://ln.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5multimedia5-tools5 amd64 5.12.8-0ubuntu1 [164 kB]
Get:16 http://ln.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5multimedia5-plugins amd64 5.12.8-0ubuntu1 [197 kB]
Get:17 http://ln.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5sprintsupport5 amd64 5.12.8+dfsg-0ubuntu1 [193 kB]
Get:18 http://ln.archive.ubuntu.com/ubuntu focal/universe amd64 libsnm2ldbl amd64 0.4.8-4+dfsg-16 [108 kB]
Get:19 http://ln.archive.ubuntu.com/ubuntu focal/universe amd64 libspandsp2 amd64 0.8.6+dfsg-2 [272 kB]
Get:20 http://ln.archive.ubuntu.com/ubuntu focal-updates/main amd64 libssh-gcrypt-4 amd64 0.9.3-2ubuntu2.2 [202 kB]
Get:21 http://ln.archive.ubuntu.com/ubuntu focal/universe amd64 libwireshark-data all 3.2.3-1 [1,456 kB]
Get:22 http://ln.archive.ubuntu.com/ubuntu focal-updates/main amd64 libc-ares2 amd64 1.15.0-1ubuntu0.1 [38.2 kB]
Get:23 http://ln.archive.ubuntu.com/ubuntu focal/main amd64 libsnappy1v5 amd64 1.1.8-1build1 [16.7 kB]
Get:24 http://ln.archive.ubuntu.com/ubuntu focal/universe amd64 libwireshark3 amd64 3.2.3-1 [61.1 kB]
Get:25 http://ln.archive.ubuntu.com/ubuntu focal/universe amd64 libwireshark3-dev amd64 3.2.3-1 [199 kB]
Get:26 http://ln.archive.ubuntu.com/ubuntu focal/universe amd64 libwireshark3-gtk amd64 3.2.3-1 [15.2 MB]
Get:27 http://ln.archive.ubuntu.com/ubuntu focal/universe amd64 qt5-gtk-platformtheme amd64 5.12.8+dfsg-0ubuntu1 [124 kB]
Get:28 http://ln.archive.ubuntu.com/ubuntu focal/universe amd64 qttranslations5-l10n all 5.12.8-0ubuntu1 [1,486 kB]
Get:29 http://ln.archive.ubuntu.com/ubuntu focal/universe amd64 wireshark-common amd64 3.2.3-1 [441 kB]
Get:30 http://ln.archive.ubuntu.com/ubuntu focal/universe amd64 wireshark-qt amd64 3.2.3-1 [3,774 kB]
Get:31 http://ln.archive.ubuntu.com/ubuntu focal/universe amd64 wireshark amd64 3.2.3-1 [5,088 B]
Fetched 32.9 MB in 5s (6,613 kB/s)
Extracting templates from packages: 100%
```

To capture network packet streams type,
wireshark
then copy the ip address

Capturing from enp0s3

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1726	72.421892981	192.168.101.6	142.251.42.77	TCP	66	47134 → 443 [FIN, ACK] Seq=103 Ack=40 Win=501 Len=0
1727	72.452264158	142.251.42.77	192.168.101.6	TCP	66	443 → 47134 [ACK] Seq=40 Ack=103 Win=265 Len=0 TSval=
1728	72.452264592	142.251.42.77	192.168.101.6	TCP	66	443 → 47134 [FIN, ACK] Seq=40 Ack=103 Win=205 Len=0
1729	72.452352053	192.168.101.6	142.251.42.77	TCP	66	47134 → 443 [ACK] Seq=104 Ack=41 Win=501 Len=0 TSval=
1730	72.452264670	142.251.42.77	192.168.101.6	TCP	66	443 → 47134 [ACK] Seq=41 Ack=104 Win=265 Len=0 TSval=
1731	73.706586758	192.168.101.3	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
1732	74.382536651	192.168.101.6	142.250.183.130	TLSv1.2	105	Application Data
1733	74.420563249	142.250.183.130	192.168.101.6	TCP	66	443 → 52836 [ACK] Seq=40 Ack=79 Win=265 Len=0 TSval=
1734	74.463899998	192.168.101.6	142.250.183.130	TLSv1.2	90	Application Data
1735	74.463899957	192.168.101.6	142.250.183.130	TCP	66	52836 → 443 [FIN, ACK] Seq=103 Ack=40 Win=501 Len=0
1736	74.494896490	142.250.183.130	192.168.101.6	TCP	66	443 → 52836 [ACK] Seq=40 Ack=103 Win=265 Len=0 TSval=
1737	74.494896756	142.250.183.130	192.168.101.6	TCP	66	443 → 52836 [FIN, ACK] Seq=40 Ack=103 Win=265 Len=0
1738	74.494960334	192.168.101.6	142.250.183.130	TCP	66	52836 → 443 [ACK] Seq=104 Ack=41 Win=501 Len=0 TSval=
1739	74.494896855	142.250.183.130	192.168.101.6	TCP	66	443 → 52836 [ACK] Seq=41 Ack=104 Win=265 Len=0 TSval=
1740	74.707068919	192.168.101.3	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
1741	75.707762084	192.168.101.3	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
1742	75.776305161	192.168.101.6	54.182.1.170	TCP	66	[TCP Dup ACK 39#7] 55934 → 80 [ACK] Seq=1 Ack=1 Win=
1743	75.897863280	54.182.1.170	192.168.101.6	TCP	66	[TCP Dup ACK 40#7] [TCP ACKed unseen segment] 80 → 5

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface enp0s3, id 0

Ethernet II, Src: PcsCompu 71:fd:a1 (08:00:27:71:fd:a1), Dst: Syrotech_ab:a3:6e (38:94:e0:ab:a3:6e)

Internet Protocol Version 4, Src: 192.168.101.6, Dst: 117.18.237.29

Transmission Control Protocol, Src Port: 53158, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

0000 38 94 e0 ab a3 6e 08 00 27 71 fd a1 08 00 45 00 8 . . . n . . ' q . . . E .

0010 00 34 48 a0 40 00 40 06 6a 45 c0 a8 65 06 75 12 . 4 H 0 0 . j E . e u .

0020 ed 1d cf a6 00 50 98 f7 5f d6 c5 dc 19 cc 80 10 P

0030 01 f5 88 05 00 00 01 01 08 0a 51 8d 57 bb a7 3c Q W . < .

0040 1b 73 . s

enp0s3: <live capture in progress>

Packets: 1744 · Displayed: 1744 (100.0%)

Profile: Default