Tcpdump packet capture

Scenario

You're a network analyst who needs to use `tcpdump` to capture and analyze live network traffic from a Linux virtual machine.

The lab starts with your user account, called `analyst`, already logged in to a Linux terminal.

Your Linux user's home directory contains a sample packet capture file that you will use at the end of the lab to answer a few questions about the network traffic that it contains.

Here's how you'll do this: **First**, you'll identify network interfaces to capture network packet data. **Second**, you'll use `tcpdump` to filter live network traffic. **Third**, you'll capture network traffic using `tcpdump`. **Finally**, you'll filter the captured packet data.

```
analyst@43f661657444:~$ sudo ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1460
        inet 172.17.0.2  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:ac:11:00:02  txqueuelen 0  (Ethernet)
        RX packets 903  bytes 13674375 (13.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 586  bytes 47945 (46.8 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
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 57  bytes 8381 (8.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 57  bytes 8381 (8.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

analyst@43f661657444:~$
```

Figure 1 identifying the interfaces that are available

```
analyst@43f661657444:~$ sudo tcpdump -D
1.eth0 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.nflog (Linux netfilter log (NFLOG) interface)
5.nfqueue (Linux netfilter queue (NFQUEUE) interface)
analyst@43f661657444:~$
```

Figure 2 identifying the interface options available for packet capture

```
analyst@43f661657444:~$ sudo tcpdump -D
1.eth0 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.nflog (Linux netfilter log (NFLOG) interface)
5.nfqueue (Linux netfilter queue (NFQUEUE) interface)
analyst@43f661657444:~$ sudo tcpdump -i eth0 -v -c5
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
19:17:51.332367 IP (tos 0x0, ttl 64, id 63182, offset 0, flags [DF], proto TCP (6), length 114)
    43f661657444.5000 > nginx-us-west1-b.c.qwiklabs-terminal-vms-prod-00.internal.49090: Flags [P.], cksum 0x588d
 (incorrect -> 0x105e), seq 2395402421:2395402483, ack 2487137078, win 501, options [nop,nop,TS val 1856672364 ec
r 357366343], length 62
19:17:51.332562 IP (tos 0x0, ttl 63, id 27427, offset 0, flags [DF], proto TCP (6), length 52)
    nginx-us-west1-b.c.qwiklabs-terminal-vms-prod-00.internal.49090 > 43f661657444.5000: Flags [.], cksum 0x70c7
(correct), ack 62, win 507, options [nop,nop,TS val 357366516 ecr 1856672364], length 0
19:17:51.342921 IP (tos 0x0, ttl 64, id 63183, offset 0, flags [DF], proto TCP (6), length 147)
    43f661657444.5000 > nginx-us-west1-b.c.qwiklabs-terminal-vms-prod-00.internal.49090: Flags [P.], cksum 0x58ae
 (incorrect -> 0x219c), seq 62:157, ack 1, win 501, options [nop,nop,TS val 1856672375 ecr 357366516], length 95
19:17:51.343151 IP (tos 0x0, ttl 63, id 27428, offset 0, flags [DF], proto TCP (6), length 52)
    nginx-us-west1-b.c.qwiklabs-terminal-vms-prod-00.internal.49090 > 43f661657444.5000: Flags [.], cksum 0x7052
(correct), ack 157, win 507, options [nop,nop,TS val 357366527 ecr 1856672375], length 0
19:17:51.349642 IP (tos 0x0, ttl 64, id 60478, offset 0, flags [DF], proto UDP (17), length 69)
    43f661657444.41981 > metadata.google.internal.domain: 37506+ PTR? 2.0.19.172.in-addr.arpa. (41)
5 packets captured
12 packets received by filter
0 packets dropped by kernel
analyst@43f661657444:~$
```

Figure 3 Filtering live network packet data from the eth0 interface with tcpdump

```
analyst@43f661657444:~$ sudo tcpdump -i eth0 -nn -c9 port 80 -w capture.pcap &
[1] 12748
analyst@43f661657444:~$ tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Figure 4 Capturing packet data into a file called capture.pcap

```
curl opensource.google.com
<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="https://opensource.google/">here</A>.
</BODY></HTML>
analyst@43f661657444:~$ 9 packets captured
10 packets received by filter
0 packets dropped by kernel
```

Figure 5 Using curl to generate some HTTP (port 80) traffic

```
ls -l capture.pcap
-rw-r--r-- 1 root root 1445 Jul 22 19:18 capture.pcap
[1]+  Done                    sudo tcpdump -i eth0 -nn -c9 port 80 -w capture.pcap
analyst@43f661657444:~$
```

Figure 6 Verifying that packet data has been captured

```
analyst@43f661657444:~$ sudo tcpdump -D
1.eth0 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.nflog (Linux netfilter log (NFLOG) interface)
5.nfqueue (Linux netfilter queue (NFQUEUE) interface)
analyst@43f661657444:~$ sudo tcpdump -i eth0 -v -c5
analyst@43f661657444:~$ sudo tcpdump -nn -r capture.pcap -v
reading from file capture.pcap, link-type EN10MB (Ethernet)
19:18:55.377661 IP (tos 0x0, ttl 64, id 29602, offset 0, flags [DF], proto TCP (6), length 60)
    172.17.0.2.36380 > 74.125.195.102.80: Flags [S], cksum 0xba25 (incorrect -> 0xa222), seq 3189073282, win 6532
0, options [mss 1420,sackOK,TS val 2328211483 ecr 0,nop,wscale 7], length 0
19:18:55.378218 IP (tos 0x60, ttl 126, id 0, offset 0, flags [DF], proto TCP (6), length 60)
    74.125.195.102.80 > 172.17.0.2.36380: Flags [S.], cksum 0x85f5 (correct), seq 2778403737, ack 3189073283, win
 65535, options [mss 1420,sackOK,TS val 2987634683 ecr 2328211483,nop,wscale 8], length 0
19:18:55.378269 IP (tos 0x0, ttl 64, id 29603, offset 0, flags [DF], proto TCP (6), length 52)
    172.17.0.2.36380 > 74.125.195.102.80: Flags [.], cksum 0xba1d (incorrect -> 0xb29a), ack 1, win 511, options
[nop,nop,TS val 2328211484 ecr 2987634683], length 0
19:18:55.378327 IP (tos 0x0, ttl 64, id 29604, offset 0, flags [DF], proto TCP (6), length 137)
    172.17.0.2.36380 > 74.125.195.102.80: Flags [P.], cksum 0xba72 (incorrect -> 0x214e), seq 1:86, ack 1, win 51
1, options [nop,nop,TS val 2328211484 ecr 2987634683], length 85: HTTP, length: 85
        GET / HTTP/1.1
        Host: opensource.google.com
        User-Agent: curl/7.64.0
        Accept: */*

19:18:55.378451 IP (tos 0x60, ttl 126, id 0, offset 0, flags [DF], proto TCP (6), length 52)
    74.125.195.102.80 > 172.17.0.2.36380: Flags [.], cksum 0xb344 (correct), ack 86, win 256, options [nop,nop,TS
 val 2987634683 ecr 2328211484], length 0
19:18:55.382291 IP (tos 0x80, ttl 126, id 0, offset 0, flags [DF], proto TCP (6), length 634)
    74.125.195.102.80 > 172.17.0.2.36380: Flags [P.], cksum 0x69fe (correct), seq 1:583, ack 86, win 256, options
 [nop,nop,TS val 2987634687 ecr 2328211484], length 582: HTTP, length: 582
        HTTP/1.1 301 Moved Permanently
        Location: https://opensource.google/
        Cross-Origin-Resource-Policy: cross-origin
        Content-Type: text/html; charset=UTF-8
        X-Content-Type-Options: nosniff
```

Figure 7 Using the tcpdump command to filter the packet header data from the capture.pcap capture file

```
analyst@43f661657444:~$ sudo tcpdump -D
1.eth0 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.nflog (Linux netfilter log (NFLOG) interface)
5.nfqueue (Linux netfilter queue (NFQUEUE) interface)
analyst@43f661657444:~$ sudo tcpdump -i eth0 -v -c5
analyst@43f661657444:~$ sudo tcpdump -nn -r capture.pcap -v
reading from file capture.pcap, link-type EN10MB (Ethernet)
19:18:55.377661 IP (tos 0x0, ttl 64, id 29602, offset 0, flags [DF], proto TCP (6), length 60)
    172.17.0.2.36380 > 74.125.195.102.80: Flags [S], cksum 0xba25 (incorrect -> 0xa222), seq 3189073282, win 6532
0, options [mss 1420,sackOK,TS val 2328211483 ecr 0,nop,wscale 7], length 0
19:18:55.378218 IP (tos 0x60, ttl 126, id 0, offset 0, flags [DF], proto TCP (6), length 60)
    74.125.195.102.80 > 172.17.0.2.36380: Flags [S.], cksum 0x85f5 (correct), seq 2778403737, ack 3189073283, win
 65535, options [mss 1420,sackOK,TS val 2987634683 ecr 2328211483,nop,wscale 8], length 0
19:18:55.378269 IP (tos 0x0, ttl 64, id 29603, offset 0, flags [DF], proto TCP (6), length 52)
    172.17.0.2.36380 > 74.125.195.102.80: Flags [.], cksum 0xba1d (incorrect -> 0xb29a), ack 1, win 511, options
[nop,nop,TS val 2328211484 ecr 2987634683], length 0
19:18:55.378327 IP (tos 0x0, ttl 64, id 29604, offset 0, flags [DF], proto TCP (6), length 137)
    172.17.0.2.36380 > 74.125.195.102.80: Flags [P.], cksum 0xba72 (incorrect -> 0x214e), seq 1:86, ack 1, win 51
1, options [nop,nop,TS val 2328211484 ecr 2987634683], length 85: HTTP, length: 85
        GET / HTTP/1.1
        Host: opensource.google.com
        User-Agent: curl/7.64.0
analyst@43f661657444:~$ sudo tcpdump -nn -r capture.pcap -X
reading from file capture.pcap, link-type EN10MB (Ethernet)
19:18:55.377661 IP 172.17.0.2.36380 > 74.125.195.102.80: Flags [S], seq 3189073282, win 65320, options [mss 1420,
sackOK,TS val 2328211483 ecr 0,nop,wscale 7], length 0
        0x0000:  4500 003c 73a2 4000 4006 0d23 ac11 0002  E..<s.@.@..#....
        0x0010:  4a7d c366 8e1c 0050 be15 6582 0000 0000  J}.f...P..e.....
        0x0020:  a002 ff28 ba25 0000 0204 058c 0402 080a  ...(.%..........
        0x0030:  8ac5 b01b 0000 0000 0103 0307            ............
19:18:55.378218 IP 74.125.195.102.80 > 172.17.0.2.36380: Flags [S.], seq 2778403737, ack 3189073283, win 65535, o
ptions [mss 1420,sackOK,TS val 2987634683 ecr 2328211483,nop,wscale 8], length 0
        0x0000:  4560 003c 0000 4000 7e06 4265 4a7d c366  E`.<..@.~.BeJ}.f
        0x0010:  ac11 0002 0050 8e1c a59b 1399 be15 6583  .....P........e.
        0x0020:  a012 ffff 85f5 0000 0204 058c 0402 080a  ................
```

Figure 8 Using the tcpdump command to filter the extended packet data from the capture.pcap capture file