Professional Documentation: Packet Capture with tcpdump

Date: July 18, 2025
Analyst: Aarush Nepali
Lab Duration: 1 Hour
Lab Level: Beginner

Lab Overview

Objective

The objective of this lab was to gain hands-on experience using **tcpdump**, a command-line packet analyzer, to capture, filter, and analyze live network traffic in a Linux environment. Tasks included identifying network interfaces, capturing packets, saving them to a `.pcap` file, and analyzing the data.

Key Skills Demonstrated

- Identifying available network interfaces using `ifconfig` and `tcpdump -D`.
- Capturing live traffic with **tcpdump** using port-based filters (e.g., port `80`).
- Saving captured packets to a `.pcap` file for offline analysis.
- Analyzing packet details, including headers and payloads, using **verbose (`-v`)** and **hex/ASCII (`-x`)** output formats.

Detailed Task Breakdown

Task 1: Identify Network Interfaces

Actions Performed:

1. Ran `sudo ifconfig` to list active interfaces.
2. Used `sudo tcpdump -D` to verify capture-capable interfaces.

Findings:

- **Primary Interface:** `eth0` (Ethernet) with IP `172.17.0.2`.

- **Loopback Interface:** `lo` (localhost `127.0.0.1`).

Commands:

```
sudo ifconfig      # List network interfaces
sudo tcpdump -D    # Show capture-capable interfaces
```

```
analyst@b916af7ac7b5:~$ sudo ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1460
        inet 172.18.0.2  netmask 255.255.0.0  broadcast 172.18.255.255
        ether 02:42:ac:12:00:02  txqueuelen 0  (Ethernet)
        RX packets 848  bytes 13998453 (13.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 444  bytes 40248 (39.3 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
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 208  bytes 22972 (22.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 208  bytes 22972 (22.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
analyst@b916af7ac7b5:~$ sudo 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]
```

Task 2: Inspect Live Traffic with tcpdump

Action:
Captured **5 packets** from `eth0` using verbose output:

```
sudo tcpdump -i eth0 -v -c5
```

Packet Analysis Highlights:

- **Timestamps and Protocols:** Example - `10:57:33.427749 IP`
- **IP Header Details:**
    - `tos 0x0`, `ttl 64`, `proto TCP (6)`

- **TCP Communication:**
  - Source → Destination: `7acb26dc1f44.5000 > nginx-us-east1...59788`
  - Flags: `[P.]` (PUSH + ACK), with `seq`, `ack`, and `win` fields

Key Takeaway:

- Verbose output (`-v`) reveals detailed IP/TCP header information useful for connectivity troubleshooting.

```
analyst@b916af7ac7b5:~$ sudo tcpdump -i eth0 -v -c5
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length
262144 bytes
20:39:30.361283 IP (tos 0x0, ttl 64, id 25944, offset 0, flags [DF], prot
o TCP (6), length 128)
    b916af7ac7b5.5000 > nginx-us-central1-b.c.qwiklabs-terminal-vms-prod-
00.internal.59816: Flags [P.], cksum 0x589a (incorrect -> 0x8893), seq 42
91515416:4291515492, ack 3511762226, win 998, options [nop,nop,TS val 429
3441487 ecr 1483810351], length 76
20:39:30.361537 IP (tos 0x0, ttl 63, id 37840, offset 0, flags [DF], prot
o TCP (6), length 52)
    nginx-us-central1-b.c.qwiklabs-terminal-vms-prod-00.internal.59816 >
b916af7ac7b5.5000: Flags [.], cksum 0x8629 (correct), ack 76, win 507, op
tions [nop,nop,TS val 1483810402 ecr 4293441487], length 0
20:39:30.426510 IP (tos 0x0, ttl 64, id 39362, offset 0, flags [DF], prot
o UDP (17), length 69)
    b916af7ac7b5.54072 > metadata.google.internal.domain: 51306+ PTR? 2.0
.17.172.in-addr.arpa. (41)
20:39:30.432302 IP (tos 0x0, ttl 63, id 0, offset 0, flags [none], proto
UDP (17), length 143)
    metadata.google.internal.domain > b916af7ac7b5.54072: 51306 1/0/0 2.0
.17.172.in-addr.arpa. PTR nginx-us-central1-b.c.qwiklabs-terminal-vms-pro
d-00.internal. (115)
20:39:30.433076 IP (tos 0x0, ttl 64, id 25945, offset 0, flags [DF], prot
o TCP (6), length 141)
    b916af7ac7b5.5000 > nginx-us-central1-b.c.qwiklabs-terminal-vms-prod-
```

```
analyst@b916af7ac7b5:~$ sudo tcpdump -i eth0 -v -c5
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length
262144 bytes
20:39:30.361283 IP (tos 0x0, ttl 64, id 25944, offset 0, flags [DF], prot
o TCP (6), length 128)
    b916af7ac7b5.5000 > nginx-us-central1-b.c.qwiklabs-terminal-vms-prod-
00.internal.59816: Flags [P.], cksum 0x589a (incorrect -> 0x8893), seq 42
91515416:4291515492, ack 3511762226, win 998, options [nop,nop,TS val 429
3441487 ecr 1483810351], length 76
20:39:30.361537 IP (tos 0x0, ttl 63, id 37840, offset 0, flags [DF], prot
o TCP (6), length 52)
    nginx-us-central1-b.c.qwiklabs-terminal-vms-prod-00.internal.59816 >
b916af7ac7b5.5000: Flags [.], cksum 0x8629 (correct), ack 76, win 507, op
tions [nop,nop,TS val 1483810402 ecr 4293441487], length 0
20:39:30.426510 IP (tos 0x0, ttl 64, id 39362, offset 0, flags [DF], prot
o UDP (17), length 69)
    b916af7ac7b5.54072 > metadata.google.internal.domain: 51306+ PTR? 2.0
.17.172.in-addr.arpa. (41)
20:39:30.432302 IP (tos 0x0, ttl 63, id 0, offset 0, flags [none], proto
UDP (17), length 143)
    metadata.google.internal.domain > b916af7ac7b5.54072: 51306 1/0/0 2.0
.17.172.in-addr.arpa. PTR nginx-us-central1-b.c.qwiklabs-terminal-vms-pro
d-00.internal. (115)
20:39:30.433076 IP (tos 0x0, ttl 64, id 25945, offset 0, flags [DF], prot
o TCP (6), length 141)
    b916af7ac7b5.5000 > nginx-us-central1-b.c.qwiklabs-terminal-vms-prod-
00.internal.59816: Flags [P.], cksum 0x58a7 (incorrect -> 0x962b), seq 76
:165, ack 1, win 998, options [nop,nop,TS val 4293441559 ecr 1483810402],
 length 89
5 packets captured
10 packets received by filter
0 packets dropped by kernel
```

Task 3: Capture Traffic to a File

Actions Performed:

1. Captured **9 HTTP packets** using port filter and saved them to a file:
2. `sudo tcpdump -i eth0 -nn -c9 port 80 -w capture.pcap &`
3. Generated traffic with:
4. `curl opensource.google.com`
5. Verified the capture file:
6. `ls -l capture.pcap`

Explanation of Flags Used:

- `-nn`: Disables DNS and port name resolution.
- `port 80`: Filters for HTTP traffic.
- `-w`: Writes captured packets to file.

Output:

- `.pcap` file size: ~2–3 KB (9 packets).

```
0 packets dropped by kernel
analyst@b916af7ac7b5:~$ sudo tcpdump -i eth0 -nn -c9 port 80 -w capture.p
cap &
[1] 13515
analyst@b916af7ac7b5:~$ tcpdump: listening on eth0, link-type EN10MB (Eth
ernet), snapshot length 262144 bytes

analyst@b916af7ac7b5:~$ sudo tcpdump -i eth0 -nn -c9 port 80 -w capture.p
cap &
[2] 13524
analyst@b916af7ac7b5:~$ tcpdump: listening on eth0, link-type EN10MB (Eth
ernet), snapshot length 262144 bytes
```

```
analyst@b916af7ac7b5:~$ curl opensource.google.com
<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=ut
f-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@b916af7ac7b5:~$ 9 packets captured
10 packets received by filter
0 packets dropped by kernel
9 packets captured
10 packets received by filter
0 packets dropped by kernel

[1]-  Done                    sudo tcpdump -i eth0 -nn -c9 port 80 -w cap
ture.pcap
[2]+  Done                    sudo tcpdump -i eth0 -nn -c9 port 80 -w cap
ture.pcap
analyst@b916af7ac7b5:~$ ls -l capture.pcap
-rw-r--r-- 1 tcpdump tcpdump 1445 Jul 18 20:48 capture.pcap
```

Task 4: Analyze Captured Packets

Actions Performed:

1. Analyzed `.pcap` file with verbose flag:
2. `sudo tcpdump -nn -r capture.pcap -v`
    - Observed TCP handshake (SYN, SYN-ACK) between `172.17.0.2` and `146.75.38.132`.
3. Inspected raw payload using hex and ASCII:
4. `sudo tcpdump -nn -r capture.pcap -X`

- Revealed HTTP headers like: `GET / HTTP/1.1`

Key Findings:

- **Source IP:** `172.17.0.2` (local VM)
- **Destination IP:** `146.75.38.132` (Google server)
- **TCP Flags:** `[S]` (SYN), `[S.]` (SYN-ACK), `[P.]` (PUSH + ACK)

```
analyst@b916af7ac7b5:~$ sudo tcpdump -nn -r capture.pcap -v
reading from file capture.pcap, link-type EN10MB (Ethernet), snapshot len
gth 262144
20:48:28.727111 IP (tos 0x0, ttl 64, id 30217, offset 0, flags [DF], prot
o TCP (6), length 60)
    172.18.0.2.56788 > 64.233.181.139.80: Flags [S], cksum 0xa2b7 (incorr
ect -> 0xfac7), seq 190862029, win 65320, options [mss 1420,sackOK,TS val
 401168244 ecr 0,nop,wscale 6], length 0
20:48:28.729192 IP (tos 0x0, ttl 126, id 0, offset 0, flags [DF], proto T
CP (6), length 60)
    64.233.181.139.80 > 172.18.0.2.56788: Flags [S.], cksum 0xfe39 (corre
ct), seq 2806953869, ack 190862030, win 65535, options [mss 1420,sackOK,T
S val 31169260 ecr 401168244,nop,wscale 8], length 0
20:48:28.729242 IP (tos 0x0, ttl 64, id 30218, offset 0, flags [DF], prot
o TCP (6), length 52)
    172.18.0.2.56788 > 64.233.181.139.80: Flags [.], cksum 0xa2af (incorr
ect -> 0x28e0), ack 1, win 1021, options [nop,nop,TS val 401168246 ecr 31
169260], length 0
20:48:28.729313 IP (tos 0x0, ttl 64, id 30219, offset 0, flags [DF], prot
o TCP (6), length 137)
    172.18.0.2.56788 > 64.233.181.139.80: Flags [P.], cksum 0xa304 (incor
rect -> 0x9693), seq 1:86, ack 1, win 1021, options [nop,nop,TS val 40116
8246 ecr 31169260], length 85: HTTP, length: 85
        GET / HTTP/1.1
        Host: opensource.google.com
        User-Agent: curl/7.74.0
        Accept: */*

20:48:28.729487 IP (tos 0x0, ttl 126, id 0, offset 0, flags [DF], proto T
CP (6), length 52)
    64.233.181.139.80 > 172.18.0.2.56788: Flags [.], cksum 0x286d (correc
t), ack 86, win 1051, options [nop,nop,TS val 31169260 ecr 401168246], le
ngth 0
20:48:28.734525 IP (tos 0x0, ttl 126, id 0, offset 0, flags [DF], proto T
CP (6), length 634)
    64.233.181.139.80 > 172.18.0.2.56788: Flags [P.], cksum 0x0410 (corre
ct), seq 1:583, ack 86, win 1051, options [nop,nop,TS val 31169265 ecr 40
1168246], length 582: HTTP, length: 582
```

```
analyst@b916af7ac7b5:~$ sudo tcpdump -nn -r capture.pcap -X
reading from file capture.pcap, link-type EN10MB (Ethernet), snapshot len
gth 262144
20:48:28.727111 IP 172.18.0.2.56788 > 64.233.181.139.80: Flags [S], seq 1
90862029, win 65320, options [mss 1420,sackOK,TS val 401168244 ecr 0,nop,
wscale 6], length 0
        0x0000:  4500 003c 7609 4000 4006 222a ac12 0002  E..<v.@.@."*...
.
        0x0010:  40e9 b58b ddd4 0050 0b60 52cd 0000 0000  @......P.`R....
.
        0x0020:  a002 ff28 a2b7 0000 0204 058c 0402 080a  ...(............
.
        0x0030:  17e9 5774 0000 0000 0103 0306            ..Wt........
20:48:28.729192 IP 64.233.181.139.80 > 172.18.0.2.56788: Flags [S.], seq
2806953869, ack 190862030, win 65535, options [mss 1420,sackOK,TS val 311
69260 ecr 401168244,nop,wscale 8], length 0
        0x0000:  4500 003c 0000 4000 7e06 5a33 40e9 b58b  E..<..@.~.Z3@...
.
        0x0010:  ac12 0002 0050 ddd4 a74e b78d 0b60 52ce  .....P...N...`R
.
        0x0020:  a012 ffff fe39 0000 0204 058c 0402 080a  .....9..........
.
        0x0030:  01db 9aec 17e9 5774 0103 0308            ......Wt....
20:48:28.729242 IP 172.18.0.2.56788 > 64.233.181.139.80: Flags [.], ack 1
, win 1021, options [nop,nop,TS val 401168246 ecr 31169260], length 0
        0x0000:  4500 0034 760a 4000 4006 2231 ac12 0002  E..4v.@.@."1....
.
        0x0010:  40e9 b58b ddd4 0050 0b60 52ce a74e b78e  @......P.`R..N..
.
        0x0020:  8010 03fd a2af 0000 0101 080a 17e9 5776  ..............W
v
        0x0030:  01db 9aec                                ....
20:48:28.729313 IP 172.18.0.2.56788 > 64.233.181.139.80: Flags [P.], seq
1:86, ack 1, win 1021, options [nop,nop,TS val 401168246 ecr 31169260], l
ength 85: HTTP: GET / HTTP/1.1
        0x0000:  4500 0089 760b 4000 4006 21db ac12 0002  E...v.@.@.!.....
.
```

Conclusion & Takeaways

- Successfully **captured, saved, and analyzed** real-time HTTP traffic using `tcpdump`.
- Applied **essential filtering techniques** for focused analysis.
- Verified end-to-end connection via TCP handshake and HTTP headers.
- Strengthened foundational skills in **command-line packet inspection**.

Next Steps

- Explore **advanced filters** using BPF (e.g., `host`, `net`, `not`).

- Investigate packet payloads for **malware indicators** or anomalies.
- Create **automated tcpdump scripts** for regular traffic auditing.

Lab Artifacts

Commands Executed

```
# Task 1: Interface Identification
sudo ifconfig
sudo tcpdump -D

# Task 2: Live Capture
sudo tcpdump -i eth0 -v -c5

# Task 3: Save to File
sudo tcpdump -i eth0 -nn -c9 port 80 -w capture.pcap &
curl opensource.google.com
ls -l capture.pcap

# Task 4: Analyze .pcap
sudo tcpdump -nn -r capture.pcap -v
sudo tcpdump -nn -r capture.pcap -X
```

Key Observations

Metric	Value
Captured Interface	`eth0`
HTTP Server IP	`146.75.38.132`
TCP Flags Observed	SYN, SYN-ACK, PSH-ACK
Packet Storage	`capture.pcap` (9 PKTs)

Final Notes

This lab strengthened skills in **network traffic analysis and capture using tcpdump**, a critical skill for SOC analysts and network defenders. Future labs will build upon this foundation by incorporating **Wireshark**, **malware forensics**, and **real-world threat detection** scenarios.

Appendix: tcpdump Flags Cheat Sheet

Flag	Purpose
`-i`	Specify capture interface
`-nn`	Disable DNS and port resolution
`-v`	Enable verbose output (headers)
`-X`	View packet contents in hex/ASCII
`-w`	Write packets to file
`-c`	Capture specified number of packets