CSE3502 INFORMATION SYSTEM MANAGEMENT

TCPdump

Priyal Bhardwaj 18BIT0272

CONTENTS

Overview

Features

- Installation
- Packet Capturing Options (Cheat Sheet)
- Analysing Traffic

Demo

Overview

- **tcpdump** is a packet sniffing and packet analyzing tool.
- popular network debugging tool.
- used to capture, filter, and analyse network traffic.
- used to intercept and display packets transmitted/received on a network.
- filters used to restrict analysis to packets of interest.
- used as a security tool as well.
- saves the captured information in a pcap file.

Features

01 Installation

- **Debian & Ubuntu**
  sudo apt-get install tcpdump
- **Windows**
  download & install winpcap
  Download and execute windump.exe
- **Linux**
  already installed

Features

02 Packet Capturing Options (Click here for Cheat Sheet)

Switch	**Syntax**
-D	tcpdump -D
-i any	tcpdump -i any
-i eth0	tcpdump -i eth0
-c	tcpdump -c
-A	tcpdump -i eth0 -A

Features

02 Packet Capturing Options (Click here for Cheat Sheet)

Switch	Syntax
-w	tcpdump -i eth0 -w tcpdump.txt
-r	tcpdump -r tcpdump.txt
-n	tcpdump -n -i eth0
-nn	tcpdump -n -i eth0
dst	tcpdump dst 10.1.1.100

Features

03 Analysing Traffic

```
20:58:26.765637 IP 10.0.0.50.80 > 10.0.0.1.53181: Flags [F.],
seq 1, ack 2, win 453, options [nop,nop,TS val 3822939 ecr
249100129], length 0
```

- Unix timestamp (20:58:26.765637)
- protocol (IP)
- the source hostname or IP, and port number (10.0.0.50.80)
- destination hostname or IP, and port number (10.0.0.1.53181)

Features

03 Analysing Traffic

```
20:58:26.765637 IP 10.0.0.50.80 > 10.0.0.1.53181: Flags [F.], seq 1, ack
2, win 453, options [nop,nop,TS val 3822939 ecr 249100129], length 0
```

- TCP Flags (`Flags [F.]`)
- S – SYN
- F – FIN
- . – ACK
- P – PUSH
- R – RST.

Features

03 Analysing Traffic

```
20:58:26.765637 IP 10.0.0.50.80 > 10.0.0.1.53181: Flags [F.], seq 1, ack
2, win 453, options [nop,nop,TS val 3822939 ecr 249100129], length 0
```

- Sequence number of the data in the packet. (seq 1)
- Acknowledgement number (ack 2)
- Window size (win 453).
- TCP options.
- Length of the data payload. (length 0)

Demo

```
priyalb@priyalb-VirtualBox:~$ sudo tcpdump -h
tcpdump version 4.9.3
libpcap version 1.9.1 (with TPACKET_V3)
OpenSSL 1.1.1f  31 Mar 2020
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqStuUvxX#] [ -B size ] [ -c count ]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -i interface ] [ -j tstamptype ] [ -M secret ] [ --number ]
                [ -Q in|out|inout ]
                [ -r file ] [ -s snaplen ] [ --time-stamp-precision precision ]
                [ --immediate-mode ] [ -T type ] [ --version ] [ -V file ]
                [ -w file ] [ -W filecount ] [ -y datalinktype ] [ -z postrotat
e-command ]
                [ -Z user ] [ expression ]
priyalb@priyalb-VirtualBox:~$ sudo tcpdump -D
1.enp0s3 [Up, Running]
2.lo [Up, Running, Loopback]
3.any (Pseudo-device that captures on all interfaces) [Up, Running]
4.bluetooth-monitor (Bluetooth Linux Monitor) [none]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
```

Demo

```
priyalb@priyalb-VirtualBox:~$ sudo tcpdump -i any -c 5
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 by
tes
22:33:15.227814 ARP, Request who-has 192.168.1.12 tell dsldevice.lan, length 46
22:33:15.231021 IP localhost.53242 > localhost.domain: 32428+ [1au] PTR? 12.1.1
68.192.in-addr.arpa. (54)
22:33:15.231735 IP priyalb-VirtualBox.56832 > dsldevice.lan.domain: 10156+ PTR?
 12.1.168.192.in-addr.arpa. (43)
22:33:15.284061 IP dsldevice.lan.domain > priyalb-VirtualBox.56832: 10156 NXDom
ain 0/1/0 (120)
22:33:15.284519 IP localhost.domain > localhost.53242: 32428 NXDomain 0/0/1 (54
)
5 packets captured
23 packets received by filter
12 packets dropped by kernel
```

Demo

```
priyalb@priyalb-VirtualBox:~$ sudo tcpdump -i any -c 5 -A
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 by
tes
22:35:51.344956 ARP, Request who-has 192.168.1.5 tell dsldevice.lan, length 46
........\..c................................
22:35:51.345599 IP localhost.45213 > localhost.domain: 64143+ [1au] PTR? 5.1.16
8.192.in-addr.arpa. (53)
E..Q*8@.@.........5...5.=..... .........5.1.168.192.in-addr.arpa.......).......
..
22:35:51.345787 IP priyalb-VirtualBox.52677 > dsldevice.lan.domain: 13571+ PTR?
 5.1.168.192.in-addr.arpa. (42)
E..F1.@.@..|...........5.2..5...........5.1.168.192.in-addr.arpa.....
22:35:51.396465 IP dsldevice.lan.domain > priyalb-VirtualBox.52677: 13571 NXDom
ain 0/1/0 (119)
E.....@.@...........5......5...........5.1.168.192.in-addr.arpa.............
..A.prisoner.iana.org.
hostmaster.root-servers.D.....  :....<. :..     :.
22:35:51.397063 IP localhost.domain > localhost.45213: 64143 NXDomain 0/0/1 (53
)
E..Q.E@.@.. ...5.....5...=..............5.1.168.192.in-addr.arpa.......).......
..
5 packets captured
23 packets received by filter
12 packets dropped by kernel
```

Demo

```
priyalb@priyalb-VirtualBox:~$ sudo tcpdump -i any -c 5 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 by
tes
22:37:48.109731 IP 192.168.1.18.39863 > 192.168.1.255.15600: UDP, length 35
22:37:48.377308 IP 192.168.1.2.34940 > 192.168.1.1.53: 49087+ A? connectivity-c
heck.ubuntu.com. (47)
22:37:48.406211 IP 192.168.1.1.53 > 192.168.1.2.34940: 49087 3/3/0 A 35.232.111
.17, A 34.122.121.32, A 35.224.170.84 (159)
22:37:48.407797 IP 192.168.1.2.48582 > 35.224.170.84.80: Flags [S], seq 1703532
440, win 64240, options [mss 1460,sackOK,TS val 2567344273 ecr 0,nop,wscale 7],
 length 0
22:37:48.696691 IP 35.224.170.84.80 > 192.168.1.2.48582: Flags [S.], seq 311278
2637, ack 1703532441, win 64768, options [mss 1412,sackOK,TS val 558406227 ecr
2567344273,nop,wscale 7], length 0
5 packets captured
6 packets received by filter
0 packets dropped by kernel
```

Demo

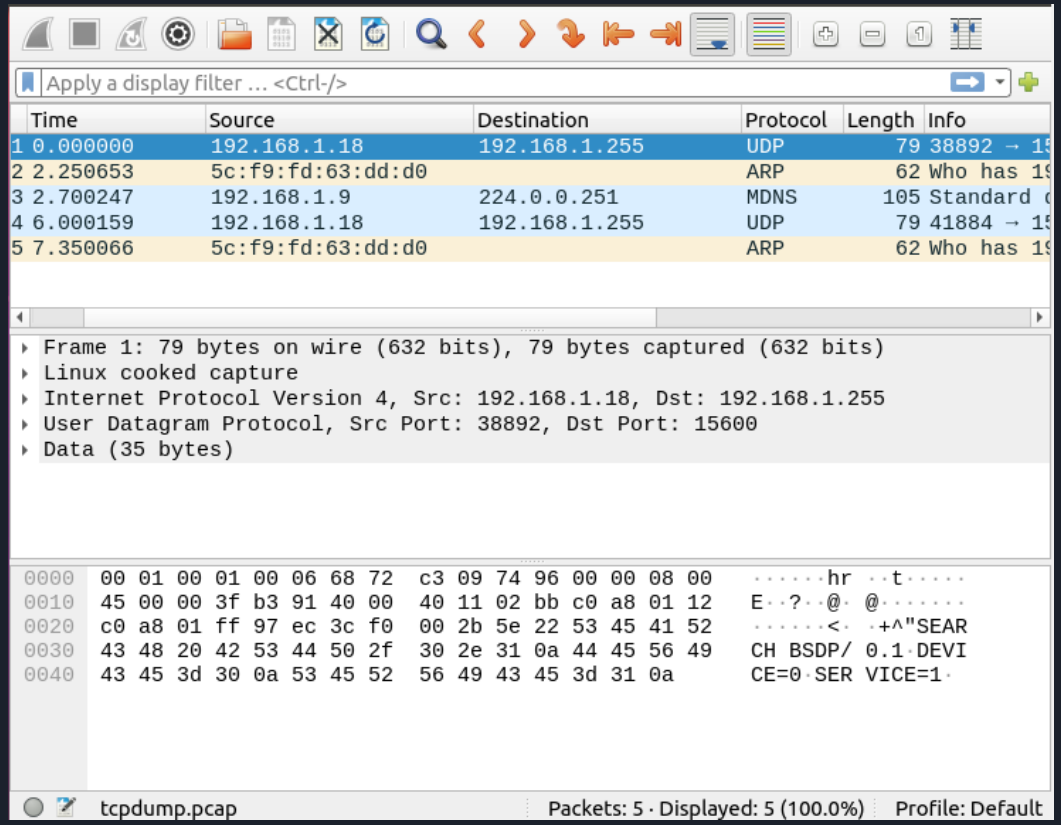
```
priyalb@priyalb-VirtualBox:~$ sudo tcpdump -i any -c 5 -nn
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 by
tes
22:38:44.869075 IP 192.168.1.9.5353 > 224.0.0.251.5353: 148 [2q] PTR (QM)? _233
637DE._sub._googlecast._tcp.local. PTR (QM)? _googlecast._tcp.local. (61)
22:38:45.836446 ARP, Request who-has 192.168.1.12 tell 192.168.1.1, length 46
22:38:48.177746 IP 192.168.1.18.36909 > 192.168.1.255.15600: UDP, length 35
22:38:50.932999 ARP, Request who-has 192.168.1.12 tell 192.168.1.1, length 46
22:38:51.809293 IP 192.168.1.8.5353 > 224.0.0.251.5353: 0 [3q] [1au] PTR (QM)?
_homekit._tcp.local. PTR (QM)? _companion-link._tcp.local. PTR (QM)? _sleep-pro
xy._udp.local. (112)
5 packets captured
5 packets received by filter
0 packets dropped by kernel
```

Demo

```
priyalb@priyalb-VirtualBox:~$ sudo tcpdump -i any -c5 -w tcpdump.pcap
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 2
62144 bytes
5 packets captured
5 packets received by filter
0 packets dropped by kernel
```

tcpdump.pcap file can be viewed in wireshark

Demo


Apply a display filter … <Ctrl-/>
Time Source Destination Protocol Length Info
1 0.000000 192.168.1.18 192.168.1.255 UDP 79 38892 → 15
2 2.250653 5c:f9:fd:63:dd:d0 ARP 62 Who has 19
3 2.700247 192.168.1.9 224.0.0.251 MDNS 105 Standard
4 6.000159 192.168.1.18 192.168.1.255 UDP 79 41884 → 15
5 7.350066 5c:f9:fd:63:dd:d0 ARP 62 Who has 19
Frame 1: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)
Linux cooked capture
Internet Protocol Version 4, Src: 192.168.1.18, Dst: 192.168.1.255
User Datagram Protocol, Src Port: 38892, Dst Port: 15600
Data (35 bytes)
0000 00 01 00 01 00 06 68 72 c3 09 74 96 00 00 08 00 ·····hr ··t·····
0010 45 00 00 3f b3 91 40 00 40 11 02 bb c0 a8 01 12 E··?··@· @·····
0020 c0 a8 01 ff 97 ec 3c f0 00 2b 5e 22 53 45 41 52 ·····<· ·+^"SEAR
0030 43 48 20 42 53 44 50 2f 30 2e 31 0a 44 45 56 49 CH BSDP/ 0.1·DEVI
0040 43 45 3d 30 0a 53 45 52 56 49 43 45 3d 31 0a CE=0·SER VICE=1·
tcpdump.pcap
Packets: 5 · Displayed: 5 (100.0%)
Profile: Default

Thank you!