Name : Shruti Gandhi
Class : TEIT - 1
Batch : T12 - 27
Subject : CNS
Date : 12/09/2021

ASSIGNMENT 7

AIM : Study of packet sniffer tools wireshark and TCPDUMP.

LAB OUTCOME : Explore the different network reconnaissance tools to gather information about networks.

THEORY :

Tcpdump is a command line utility that allows to capture and analyze network traffic going through your system. It is often used to help troubleshoot network traffic & issues & security testing.

- Display available interfaces :
  To list number of available interfaces on system, run command :
  `# tcpdump -D`
- Basic command for sniffing :
  To stop tcpdump from resolving ip addresses to hostnames use -n option.
  `# tcpdump -n.`
- Detailed output : To get more details about packet, verbose -v is used.
  `# tcpdump -v -n`

- Capture packets from specific interface.
  Tcpdump command captures from all interfaces, however -i switch only capture from desired interface.
  # tcpdump -i eth0
- Capture only N number of packets.
  The command screen will scroll up until you interrupt, but using -c option, you can capture specified number of packets.
  # tcpdump -c 5 -i eth0
- Print captured packets in ASCII
  The -A option is used to display the packages in ASCII format.
  # tcpdump -A -i eth0
- Capture only TCP packets.
  To capture TCP packets, run commands with tcp option
  # tcpdump -i eth0 tcp
- Capture packets from source IP
  To capture packets with specific source IP address,
  # tcpdump -i eth0 src 192.168.13.128
- Capture and save packets in .pcap format.
  # tcpdump -i eth0 -w capture1.pcap
- Read file of captured packets.
  # tcpdump -r capture1.pcap

CONCLUSION: Hence, we have studied and implemented various tcpdump commands

```
┌──(root㉿kali)-[/home/shruti/Desktop]
└─# tcpdump -c 3 -i eth0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
23:29:00.305900 IP 192.168.195.129.32806 > ec2-35-83-153-254.us-west-2.compute.amazonaws.com.https: Flags [P.], seq 708485006:708485041, ack 2131302463, win 62780, len
gth 35
23:29:00.311632 IP ec2-35-83-153-254.us-west-2.compute.amazonaws.com.https > 192.168.195.129.32806: Flags [.], ack 35, win 64240, length 0
23:29:00.313625 IP 192.168.195.129.52463 > 192.168.195.2.domain: 53670+ PTR? 254.153.83.35.in-addr.arpa. (44)
3 packets captured
14 packets received by filter
0 packets dropped by kernel
```

```
└─# tcpdump -n -i eth0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
23:24:35.710120 IP 192.168.195.1.5353 > 224.0.0.251.5353: 0 A (QM)? wpad.local. (28)
23:24:35.713860 IP6 fe80::3984:4643:fdb1:5e4e.5353 > ff02::fb.5353: 0 A (QM)? wpad.local. (28)
23:24:35.717234 IP 192.168.195.1.137 > 192.168.195.255.137: UDP, length 50
23:24:35.718936 IP 192.168.195.1.5353 > 224.0.0.251.5353: 0 A (QM)? wpad.local. (28)
23:24:35.720781 IP6 fe80::3984:4643:fdb1:5e4e.5353 > ff02::fb.5353: 0 A (QM)? wpad.local. (28)
23:24:35.722759 IP 192.168.195.1.5353 > 224.0.0.251.5353: 0 A (QM)? wpad.local. (28)
23:24:35.723515 IP6 fe80::3984:4643:fdb1:5e4e.54556 > ff02::1:3.5355: UDP, length 22
23:24:35.724121 IP 192.168.195.1.54556 > 224.0.0.252.5355: UDP, length 22
23:24:35.724744 IP6 fe80::3984:4643:fdb1:5e4e.5353 > ff02::fb.5353: 0 A (QM)? wpad.local. (28)
23:24:35.729323 IP 192.168.195.1.137 > 192.168.195.255.137: UDP, length 50
23:24:36.474427 IP 192.168.195.1.137 > 192.168.195.255.137: UDP, length 50
23:24:36.480260 IP 192.168.195.1.137 > 192.168.195.255.137: UDP, length 50
23:24:36.713137 IP 192.168.195.1.5353 > 224.0.0.251.5353: 0 A (QM)? wpad.local. (28)
23:24:36.715842 IP6 fe80::3984:4643:fdb1:5e4e.5353 > ff02::fb.5353: 0 A (QM)? wpad.local. (28)
23:24:36.721003 IP 192.168.195.1.5353 > 224.0.0.251.5353: 0 A (QM)? wpad.local. (28)
23:24:36.722879 IP6 fe80::3984:4643:fdb1:5e4e.5353 > ff02::fb.5353: 0 A (QM)? wpad.local. (28)
23:24:37.225662 IP 192.168.195.1.137 > 192.168.195.255.137: UDP, length 50
23:24:37.231970 IP 192.168.195.1.137 > 192.168.195.255.137: UDP, length 50
^C
18 packets captured
18 packets received by filter
0 packets dropped by kernel
```

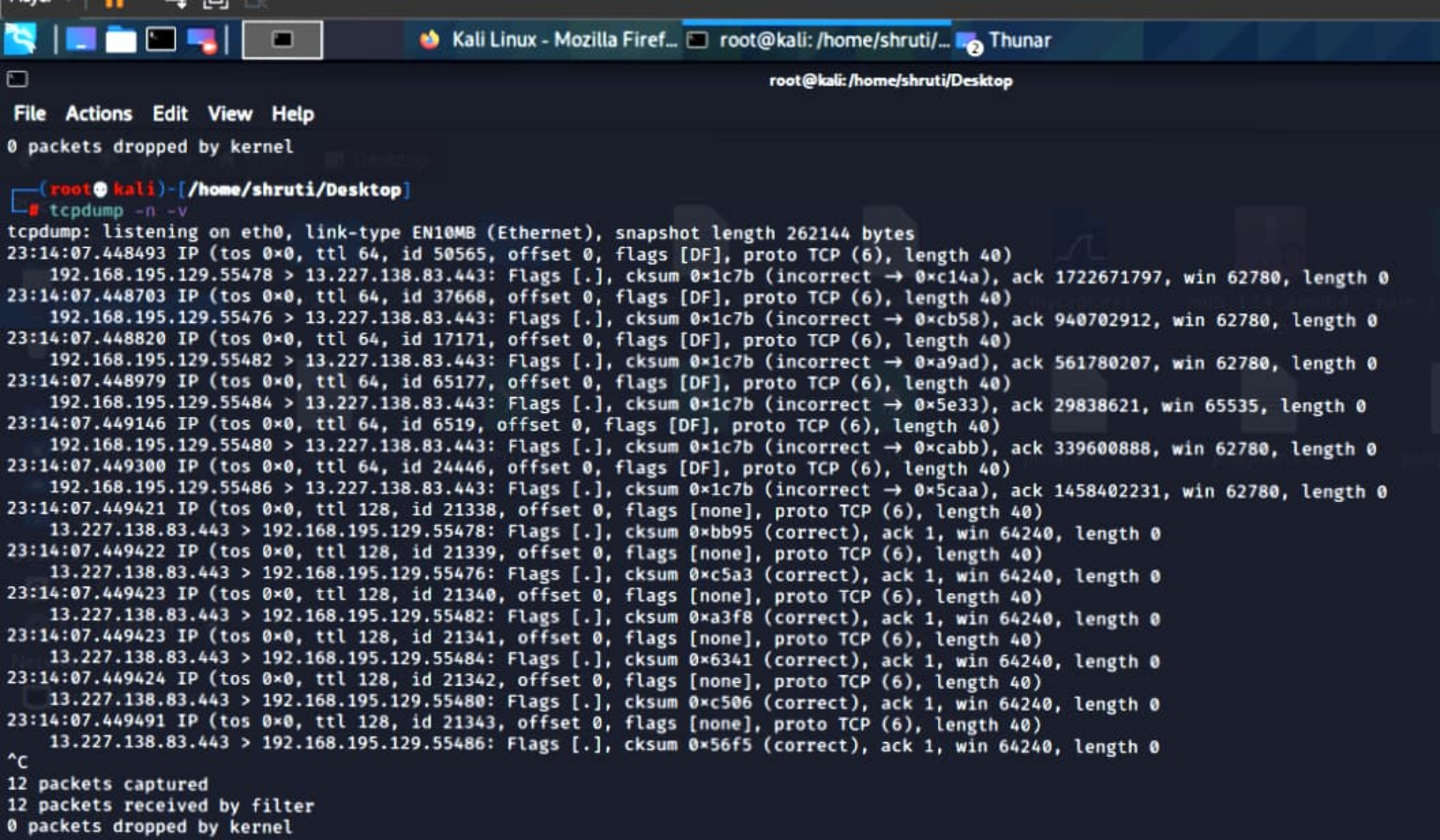
```
┌──(root💀kali)-[/home/shruti/Desktop]
└─# tcpdump -n -v icmp
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
```

```
┌──(root㉿kali)-[/home/shruti/Desktop]
└─# tcpdump -n -v tcp
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
```

```
┌──(root💀kali)-[/home/shruti/Desktop]
└─# ping 192.168.44.2
PING 192.168.44.2 (192.168.44.2) 56(84) bytes of data.

^C
--- 192.168.44.2 ping statistics ---
36 packets transmitted, 0 received, 100% packet loss, time 35846ms
```

```
┌──(root㉿kali)-[/home/shruti/Desktop]
└─# tcpdump -n -e -c 10
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
23:15:49.848528 00:0c:29:72:20:fc > 00:50:56:f2:28:fc, ethertype IPv4 (0x0800), length 54: 192.168.195.129.42696 > 34.218.7.136.443: Flags [.], ack 540828273, win 6278
0, length 0
23:15:49.849199 00:50:56:f2:28:fc > 00:0c:29:72:20:fc, ethertype IPv4 (0x0800), length 60: 34.218.7.136.443 > 192.168.195.129.42696: Flags [.], ack 1, win 64240, lengt
h 0
^C
2 packets captured
2 packets received by filter
0 packets dropped by kernel
```


Kali Linux - Mozilla Firef...
root@kali: /home/shruti/...
Thunar
root@kali: /home/shruti/Desktop
File Actions Edit View Help
0 packets dropped by kernel
┌──(root㉿kali)-[/home/shruti/Desktop]
└─# tcpdump -n -v
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
23:14:07.448493 IP (tos 0×0, ttl 64, id 50565, offset 0, flags [DF], proto TCP (6), length 40)
192.168.195.129.55478 > 13.227.138.83.443: Flags [.], cksum 0×1c7b (incorrect → 0×c14a), ack 1722671797, win 62780, length 0
23:14:07.448703 IP (tos 0×0, ttl 64, id 37668, offset 0, flags [DF], proto TCP (6), length 40)
192.168.195.129.55476 > 13.227.138.83.443: Flags [.], cksum 0×1c7b (incorrect → 0×cb58), ack 940702912, win 62780, length 0
23:14:07.448820 IP (tos 0×0, ttl 64, id 17171, offset 0, flags [DF], proto TCP (6), length 40)
192.168.195.129.55482 > 13.227.138.83.443: Flags [.], cksum 0×1c7b (incorrect → 0×a9ad), ack 561780207, win 62780, length 0
23:14:07.448979 IP (tos 0×0, ttl 64, id 65177, offset 0, flags [DF], proto TCP (6), length 40)
192.168.195.129.55484 > 13.227.138.83.443: Flags [.], cksum 0×1c7b (incorrect → 0×5e33), ack 29838621, win 65535, length 0
23:14:07.449146 IP (tos 0×0, ttl 64, id 6519, offset 0, flags [DF], proto TCP (6), length 40)
192.168.195.129.55480 > 13.227.138.83.443: Flags [.], cksum 0×1c7b (incorrect → 0×cabb), ack 339600888, win 62780, length 0
23:14:07.449300 IP (tos 0×0, ttl 64, id 24446, offset 0, flags [DF], proto TCP (6), length 40)
192.168.195.129.55486 > 13.227.138.83.443: Flags [.], cksum 0×1c7b (incorrect → 0×5caa), ack 1458402231, win 62780, length 0
23:14:07.449421 IP (tos 0×0, ttl 128, id 21338, offset 0, flags [none], proto TCP (6), length 40)
13.227.138.83.443 > 192.168.195.129.55478: Flags [.], cksum 0×bb95 (correct), ack 1, win 64240, length 0
23:14:07.449422 IP (tos 0×0, ttl 128, id 21339, offset 0, flags [none], proto TCP (6), length 40)
13.227.138.83.443 > 192.168.195.129.55476: Flags [.], cksum 0×c5a3 (correct), ack 1, win 64240, length 0
23:14:07.449423 IP (tos 0×0, ttl 128, id 21340, offset 0, flags [none], proto TCP (6), length 40)
13.227.138.83.443 > 192.168.195.129.55482: Flags [.], cksum 0×a3f8 (correct), ack 1, win 64240, length 0
23:14:07.449423 IP (tos 0×0, ttl 128, id 21341, offset 0, flags [none], proto TCP (6), length 40)
13.227.138.83.443 > 192.168.195.129.55484: Flags [.], cksum 0×6341 (correct), ack 1, win 64240, length 0
23:14:07.449424 IP (tos 0×0, ttl 128, id 21342, offset 0, flags [none], proto TCP (6), length 40)
13.227.138.83.443 > 192.168.195.129.55480: Flags [.], cksum 0×c506 (correct), ack 1, win 64240, length 0
23:14:07.449491 IP (tos 0×0, ttl 128, id 21343, offset 0, flags [none], proto TCP (6), length 40)
13.227.138.83.443 > 192.168.195.129.55486: Flags [.], cksum 0×56f5 (correct), ack 1, win 64240, length 0
^C
12 packets captured
12 packets received by filter
0 packets dropped by kernel

```
└─# tcpdump -n -i eth0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
23:24:35.710120 IP 192.168.195.1.5353 > 224.0.0.251.5353: 0 A (QM)? wpad.local. (28)
23:24:35.713860 IP6 fe80::3984:4643:fdb1:5e4e.5353 > ff02::fb.5353: 0 A (QM)? wpad.local. (28)
23:24:35.717234 IP 192.168.195.1.137 > 192.168.195.255.137: UDP, length 50
23:24:35.718936 IP 192.168.195.1.5353 > 224.0.0.251.5353: 0 A (QM)? wpad.local. (28)
23:24:35.720781 IP6 fe80::3984:4643:fdb1:5e4e.5353 > ff02::fb.5353: 0 A (QM)? wpad.local. (28)
23:24:35.722759 IP 192.168.195.1.5353 > 224.0.0.251.5353: 0 A (QM)? wpad.local. (28)
23:24:35.723515 IP6 fe80::3984:4643:fdb1:5e4e.54556 > ff02::1:3.5355: UDP, length 22
23:24:35.724121 IP 192.168.195.1.54556 > 224.0.0.252.5355: UDP, length 22
23:24:35.724744 IP6 fe80::3984:4643:fdb1:5e4e.5353 > ff02::fb.5353: 0 A (QM)? wpad.local. (28)
23:24:35.729323 IP 192.168.195.1.137 > 192.168.195.255.137: UDP, length 50
23:24:36.474427 IP 192.168.195.1.137 > 192.168.195.255.137: UDP, length 50
23:24:36.480260 IP 192.168.195.1.137 > 192.168.195.255.137: UDP, length 50
23:24:36.713137 IP 192.168.195.1.5353 > 224.0.0.251.5353: 0 A (QM)? wpad.local. (28)
23:24:36.715842 IP6 fe80::3984:4643:fdb1:5e4e.5353 > ff02::fb.5353: 0 A (QM)? wpad.local. (28)
23:24:36.721003 IP 192.168.195.1.5353 > 224.0.0.251.5353: 0 A (QM)? wpad.local. (28)
23:24:36.722879 IP6 fe80::3984:4643:fdb1:5e4e.5353 > ff02::fb.5353: 0 A (QM)? wpad.local. (28)
23:24:37.225662 IP 192.168.195.1.137 > 192.168.195.255.137: UDP, length 50
23:24:37.231970 IP 192.168.195.1.137 > 192.168.195.255.137: UDP, length 50
^C
18 packets captured
18 packets received by filter
0 packets dropped by kernel
```