Pratham U-210905407

Computer Networks Lab 4:Network Data Analysis using tcpdump

1. While tcpdump host your_host is running in one command window, run ping 127.0.0.1 from another command window. From the ping output, is the 127.0.0.1 interface on? Can you see any ICMP message sent from your host in the tcpdump output? Why?

Sol:

> **sudo tcpdump -vv host 172.16.48.71**

Yes, you would be able to see ICMP (Internet Control Message Protocol) messages in the `tcpdump` output. When you are capturing packets using `tcpdump` with the filter `host your_host`, you're only capturing traffic related to communication with `your_host`. Since you're pinging the loopback address (`127.0.0.1`), which is local traffic and doesn't go through the physical network interface, you would indeed see ICMP Echo Request and Echo Reply packets in the `tcpdump` output.

This is because the local network stack treats the loopback interface like any other network interface and processes traffic through it, generating the appropriate ICMP messages.

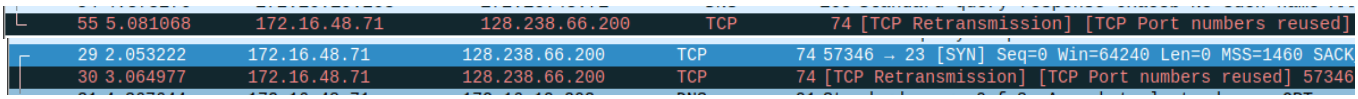
```
student@selab-25:~$ sudo tcpdump -vv host 172.16.48.71
tcpdump: listening on enp2s0, link-type EN10MB (Ethernet), snapshot length 26214
4 bytes
09:42:27.465496 IP (tos 0x0, ttl 64, id 25505, offset 0, flags [DF], proto ICMP
(1), length 84)
    selab-25 > 172.16.48.84: ICMP echo request, id 3, seq 20, length 64
09:42:27.466320 IP (tos 0x0, ttl 64, id 5972, offset 0, flags [none], proto ICMP
 (1), length 84)
    172.16.48.84 > selab-25: ICMP echo reply, id 3, seq 20, length 64
09:42:27.482116 IP (tos 0x0, ttl 64, id 8280, offset 0, flags [none], proto UDP
(17), length 82)
    selab-25.51225 > mpl-dc-adc01.manipal.edu.domain: [bad udp cksum 0x9c82 -> 0
xea50!] 22467+ [1au] PTR? 84.48.16.172.in-addr.arpa. ar: . OPT UDPsize=1472 (54)
09:42:27.510831 IP (tos 0x0, ttl 127, id 25489, offset 0, flags [none], proto UD
P (17), length 141)
    mpl-dc-adc01.manipal.edu.domain > selab-25.51225: [udp sum ok] 22467 NXDomai
n q: PTR? 84.48.16.172.in-addr.arpa. 0/1/1 ns: 16.172.in-addr.arpa. SOA localhos
t. nobody.invalid. 1 600 1200 604800 10800 ar: . OPT UDPsize=4000 (113)
```

2. While tcpdump host your_host is running to capture traffic from your machine, execute telnet 128.238.66.200. Note there is no host with this IP address in the current configuration of the lab network. Save the tcpdump output of the first few packets for the lab report. After getting the necessary output, terminate the telnet session. From the saved tcpdump output, describe how the ARP timeout and retransmission were performed. How many attempts were made to resolve a non-existing IP address?

Sol :

> **sudo tcpdump -vv -w capture.pcap host 172.16.48.71**

- ARP Timeout and Retransmission: In the captured packets, you should see ARP requests sent by your machine to resolve the MAC address of the non-existing IP address (`128.238.66.200`). If no response is received (since the IP address doesn't exist), ARP will retransmit the request after a certain timeout period. You'll notice multiple ARP requests without corresponding responses.
- Number of Attempts: 3



3. Briefly explain the purposes of the following tcpdump expressions.
a. tcpdump udp port 520
b. tcpdump -x -s 120 ip proto 89
c. tcpdump -x -s 70 host ip addr1 and (ip addr2 or ip addr3)
d. tcpdump -x -s 70 host ip addr1 and not ip addr2

a. `tcpdump udp port 520`: This expression captures UDP packets that are sent to or received from port 520. Port 520 is associated with the RIP (Routing Information Protocol) protocol, which is used by routers to exchange routing information in an IP network.
b. `tcpdump -x -s 120 ip proto 89`: This expression captures IP packets with protocol number 89. Protocol number 89 corresponds to OSPF (Open Shortest Path First), which is a routing protocol used in IP networks. The `-x` flag specifies that the packet contents should be displayed in hexadecimal and ASCII format, and the `-s 120` flag sets the snapshot length to 120 bytes.

c. `tcpdump -x -s 70 host ip addr1 and (ip addr2 or ip addr3)`: This expression captures packets involving the host with the IP address `ip addr1` and either `ip addr2` or `ip addr3`. The `-x` flag displays packet contents in hexadecimal and ASCII format, and the `-s 70` flag sets the snapshot length to 70 bytes. This expression can be used to capture communication between specific hosts.

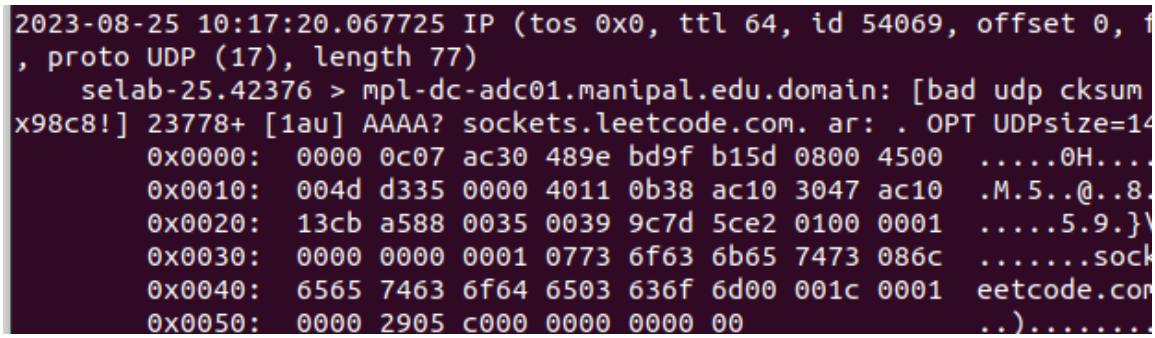
d. `tcpdump -x -s 70 host ip addr1 and not ip addr2`: This expression captures packets involving the host with the IP address `ip addr1` but excludes packets involving the host with the IP address `ip addr2`. The `-x` flag displays packet contents in hexadecimal and ASCII format, and the `-s 70` flag sets the snapshot length to 70 bytes. This expression can be used to capture traffic between specific hosts while excluding traffic involving another specific host.

4. Basic packet decoding
1) Write a tcpdump command to dump network traffic from an Ethernet connection to the screen in human readable output format. Perform the following operation and write down the observations.
a) Capture all the traffic of maximum snap length of 65,535 bytes and provide the hexadecimal and ASCII decodes of all the traffic in each packet.

> sudo tcpdump -c 2 -tttt -XXv -s 65535 -v

```
    selab-25.43046 > mpl-dc-adc01.manipal.edu.domain: [bad udp cksum 0x9c7d -> 0
xf802!] 64292+ [1au] A? sockets.leetcode.com. ar: . OPT UDPsize=1472 (49)
        0x0000:  0000 0c07 ac30 489e bd9f b15d 0800 4500  .....0H....]..E.
        0x0010:  004d bc20 0000 4011 224d ac10 3047 ac10  .M....@."M..0G..
        0x0020:  13cb a826 0035 0039 9c7d fb24 0100 0001  ...&.5.9.}.$....
        0x0030:  0000 0000 0001 0773 6f63 6b65 7473 086c  .......sockets.l
        0x0040:  6565 7463 6f64 6503 636f 6d00 0001 0001  eetcode.com.....
        0x0050:  0000 2905 c000 0000 0000 00              ..).........
```

b) Find the IP addresses, IP packet length, TCP port numbers, TCP flags, etc. by using the reference chart to locate those fields on the hexadecimal dump.
> sudo tcpdump -c 2 -tttt -XXv -s 65535 -v


2023-08-25 10:17:20.067725 IP (tos 0x0, ttl 64, id 54069, offset 0, f
, proto UDP (17), length 77)
selab-25.42376 > mpl-dc-adc01.manipal.edu.domain: [bad udp cksum
x98c8!] 23778+ [1au] AAAA? sockets.leetcode.com. ar: . OPT UDPsize=14
0x0000: 0000 0c07 ac30 489e bd9f b15d 0800 4500 .....0H....
0x0010: 004d d335 0000 4011 0b38 ac10 3047 ac10 .M.5..@..8.
0x0020: 13cb a588 0035 0039 9c7d 5ce2 0100 0001 .....5.9.}\
0x0030: 0000 0000 0001 0773 6f63 6b65 7473 086c .....sock
0x0040: 6565 7463 6f64 6503 636f 6d00 001c 0001 eetcode.com
0x0050: 0000 2905 c000 0000 0000 00 ..).....