NETWORK SECURITY
(Assignment 2)

./mydump -h (Help Command)

Usage:
mydump [-i interface] [-r file] [-s string] expression [-h]
-i Capture packets from the network device <interface> (e.g., eth0). If not specified, mydump should automatically select a default interface to listen on
-r Read packets from <file> in tcpdump format
-s Display packets that contain <string> in their payload
<expression> BPF filter that specifies which packets will be dumped. If no filter is given, all packets seen on the interface (or contained in the trace) should be dumped. Otherwise, only packets matching <expression> should be dumped
-h Displays the help message

Parse command line arguments

- Parse command line options using getopt function
- Program supports following arguments: -i (Capture live packets from the specified interface), -r (Read packets from the file given in tcpdump format), -s (display packets that contains string in their payload), -h (help message), <exp> (BFP filter)
- If -i and -r are given at the same time, preference is given to -r
- If none of the options are given, then program will get the default interface using pcap_lookupdev and create handle using pcap_open_live
- If -r is given, then it will create pcap handler using pcap_open_offline
- Apply the BFP filter if specified by the user to filter the packets

Capture Packet

- Capture the packet one by one in a loop
- For each packet, read the structure ethernet header details which includes ether type, source MAC address, destination MAC address and length of the packet
- If the packet is not IP, then print the packet length and ethernet header details, return and read next packet
- If the packet is IP, read the IP header and calculate the IP header length (first byte of IP header & 0x0F)*4. Fetch the protocol type, source IP address, destination IP from the IP header

(Protocol type : TCP)

- If the protocol type is TCP, then read the TCP header from the packet
- Calculate the source port and destination port from the TCP header. Compute the payload size by subtracting size of (ethernet header + IP header + TCP header) from the packet length and get the payload from the packet

(Protocol type : UDP)

- If the protocol type is UDP, then read the UDP header from the packet. UDP header size is fixed (8 bytes)

- Calculate the source port and destination port from the UDP header. Compute the payload size by subtracting size of(ethernet header + IP header + UDP header) from the packet length and get the payload from the packet

(Protocol type : ICMP)

- If the protocol type is ICMP, then read the ICMP header from the packet. ICMP header size is fixed (8 bytes)
- Compute the payload size by subtracting size of(ethernet header + IP header + ICMP header) from the packet length and get the payload from the packet

Print packet

- While printing the packet, check if the string pattern was given by the user. If string is given by the user, check the string in the payload. If payload doesn't contains the string, ignore the packet. Else, print the packet details including packet length, source MAC address, destination MAC address, ether type, source IP address, destination IP address, protocol type, source port, destination port, payload depending on the ether type and protocol type.

Sample outputs

1. Command: ./mydump (no arguments)

```
root@ubuntu:/home/ssingla94/Desktop/Solution/Sniffer/New# ./mydump

2017-10-14 14:55:06.481105 00:50:56:c0:00:08 -> 01:00:5e:7f:ff:fa IP 0x800 len 2
16 192.168.233.1:49945 -> 239.255.255.250:1900 UDP
4d 2d 53 45 41 52 43 48 20 2a 20 48 54 54 50 2f    M-SEARCH * HTTP/
31 2e 31 0d 0a 48 4f 53 54 3a 20 32 33 39 2e 32    1.1..HOST: 239.2
35 35 2e 32 35 35 2e 32 35 30 3a 31 39 30 30 0d    55.255.250:1900.
0a 4d 41 4e 3a 20 22 73 73 64 70 3a 64 69 73 63    .MAN: "ssdp:disc
6f 76 65 72 22 0d 0a 4d 58 3a 20 31 0d 0a 53 54    over"..MX: 1..ST
3a 20 75 72 6e 3a 64 69 61 6c 2d 6d 75 6c 74 69    : urn:dial-multi
73 63 72 65 65 6e 2d 6f 72 67 3a 73 65 72 76 69    screen-org:servi
63 65 3a 64 69 61 6c 3a 31 0d 0a 55 53 45 52 2d    ce:dial:1..USER-
41 47 45 4e 54 3a 20 47 6f 6f 67 6c 65 20 43 68    AGENT: Google Ch
72 6f 6d 65 2f 36 31 2e 30 2e 33 31 36 33 2e 31    rome/61.0.3163.1
30 30 20 57 69 6e 64 6f 77 73 0d 0a 0d 0a          00 Windows....

2017-10-14 14:55:07.479879 00:50:56:c0:00:08 -> 01:00:5e:7f:ff:fa IP 0x800 len 2
16 192.168.233.1:49945 -> 239.255.255.250:1900 UDP
4d 2d 53 45 41 52 43 48 20 2a 20 48 54 54 50 2f    M-SEARCH * HTTP/
31 2e 31 0d 0a 48 4f 53 54 3a 20 32 33 39 2e 32    1.1..HOST: 239.2
35 35 2e 32 35 35 2e 32 35 30 3a 31 39 30 30 0d    55.255.250:1900.
0a 4d 41 4e 3a 20 22 73 73 64 70 3a 64 69 73 63    .MAN: "ssdp:disc
```

2. Command: ./mydump -i ens33

```
root@ubuntu:/home/ssingla94/Desktop/Solution/Sniffer/New# ./mydump -i ens33

2017-10-14 14:56:25.791321 00:0c:29:f4:c9:86 -> 00:50:56:ec:7e:dc ARP 0x806 len
42

2017-10-14 14:56:25.791863 00:50:56:ec:7e:dc -> 00:0c:29:f4:c9:86 ARP 0x806 len
60

2017-10-14 14:57:06.491335 00:50:56:c0:00:08 -> 01:00:5e:7f:ff:fa IP 0x800 len 2
16 192.168.233.1:52122 -> 239.255.255.250:1900 UDP
4d 2d 53 45 41 52 43 48 20 2a 20 48 54 54 50 2f    M-SEARCH * HTTP/
31 2e 31 0d 0a 48 4f 53 54 3a 20 32 33 39 2e 32    1.1..HOST: 239.2
35 35 2e 32 35 35 2e 32 35 30 3a 31 39 30 30 0d    55.255.250:1900.
0a 4d 41 4e 3a 20 22 73 73 64 70 3a 64 69 73 63    .MAN: "ssdp:disc
6f 76 65 72 22 0d 0a 4d 58 3a 20 31 0d 0a 53 54    over"..MX: 1..ST
3a 20 75 72 6e 3a 64 69 61 6c 2d 6d 75 6c 74 69    : urn:dial-multi
73 63 72 65 65 6e 2d 6f 72 67 3a 73 65 72 76 69    screen-org:servi
63 65 3a 64 69 61 6c 3a 31 0d 0a 55 53 45 52 2d    ce:dial:1..USER-
41 47 45 4e 54 3a 20 47 6f 6f 67 6c 65 20 43 68    AGENT: Google Ch
72 6f 6d 65 2f 36 31 2e 30 2e 33 31 36 33 2e 31    rome/61.0.3163.1
30 30 20 57 69 6e 64 6f 77 73 0d 0a 0d 0a          00 Windows....
```

3. Command: ./mydump -r dump.pcap -s amazon

```
root@ubuntu:/home/ssingla94/Desktop/Solution/Sniffer/New# ./mydump -r dump.pcap
 -s amazon

2013-01-12 19:31:19.154432 c4:3d:c7:17:6f:9b -> 00:0c:29:e9:94:8e IP 0x800 len
207 92.240.68.152:17260 -> 192.168.0.200:80 TCP
2e 2e 5c 2e 2e 2e 2e 33 47 45 54 20 68 74 74 70    ..\....3GET http
3a 2f 2f 65 63 78 2e 69 6d 61 67 65 73 2d 61 6d    ://ecx.images-am
61 7a 6f 6e 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f    azon.com/images/
49 2f 34 31 6f 5a 31 58 73 69 4f 41 4c 2e 5f 53    I/41oZ1XsiOAL._S
4c 35 30 30 5f 41 41 33 30 30 5f 2e 6a 70 67 20    L500_AA300_.jpg
48 54 54 50 2f 31 2e 31 2e 55 73 65 72 2d 41 67    HTTP/1.1.User-Ag
65 6e 74 3a 20 77 65 62 63 6f 6c 6c 61 67 65 2f    ent: webcollage/
31 2e 31 33 35 61 2e 48 6f 73 74 3a 20 65 63 78    1.135a.Host: ecx
2e 69 6d 61 67 65 73 2d 61 6d 61 7a 6f 6e 2e 63    .images-amazon.c
6f 6d 2e 2e 2e                                     om...

2013-01-12 19:31:19.154453 00:0c:29:e9:94:8e -> c4:3d:c7:17:6f:9b IP 0x800 len
66 192.168.0.200:80 -> 92.240.68.152:17260 TCP
2e 2e 2e 42 2e 2e 5c 2e                            ...B..\.

2013-01-12 19:31:19.163445 00:0c:29:e9:94:8e -> c4:3d:c7:17:6f:9b IP 0x800 len
81 192.168.0.200:37605 -> 194.168.4.100:53 UDP
```