01_Assignment tcpdump — soln

1. Write a tcpdump command that captures all packets coming from the IP address `192.168.1.100`.

```
tcpdump src host 192.168.1.100
```

2. You want to capture traffic only on port 443 (HTTPS). Write the appropriate tcpdump capture filter to achieve this.

```
tcpdump port 443
```

3. You need to capture all HTTP traffic (port 80) and all ICMP traffic. Write a single tcpdump filter to achieve this.

```
tcpdump 'port 80 or icmp'
```

4. In Wireshark, how would you write a display filter to show only the HTTP GET requests from a capture file?

- In Wireshark, use the following **display filter** :

```
http.request.method == "GET"
```

5. In Wireshark, write a capture filter using Berkeley Packet Filter (BPF) syntax to capture traffic from the IP address `192.168.1.1` to the IP address `192.168.1.2`.

```
host 192.168.1.1 and host 192.168.1.2
```

6. You are tasked with analyzing only UDP traffic on port 53. Write a tcpdump command using the appropriate filter to capture this traffic.

```
tcpdump udp port 53
```

7. Write a tcpdump filter to capture only the SYN packets during the TCP handshake.

```
tcpdump 'tcp[tcpflags] & (tcp-syn) != 0 and tcp[tcpflags] & (tcp-ack) == 0'
```

8. How would you modify a BPF capture filter to exclude all traffic on port 22 (SSH) while still capturing HTTP traffic on port 80?

```
tcpdump 'port 80 and not port 22'
```

9. Write a Wireshark display filter to show DNS query packets for the domain name `example.com`.

- In Wireshark, use the following **display filter** :

```
dns.qry.name == "example.com"
```

10. You are analyzing network performance and want to capture only packets larger than 1000 bytes. Write the tcpdump filter to achieve this.

```
tcpdump 'greater 1000'
```

11. Write a tcpdump command that captures only the traffic between two specific IP addresses, `192.168.1.10` and `192.168.1.20`.

```
tcpdump host 192.168.1.10 and host 192.168.1.20
```

12. How would you use a BPF filter in Wireshark to capture only ARP traffic?

- In Wireshark, use the following **capture filter** :

```
arp
```

13. Write a tcpdump command that captures packets where the source IP is `192.168.2.5` and the destination port is 80.

```
tcpdump src host 192.168.2.5 and dst port 80
```

14. You need to capture all traffic related to a specific TCP stream (stream number 3). Write the appropriate tcpdump command to achieve this.

- To capture a specific TCP stream, first identify the unique combination of source/destination IPs and ports for the stream. Then use:

```
tcpdump 'host <src_ip> and host <dst_ip> and port <src_port> and port <dst_port>'
```

- Alternatively, if you're working with Wireshark, you can use the **display filter** :

```
tcp.stream == 3
```

15. Write a tcpdump command that captures only traffic with the UDP protocol and a payload size greater than 512 bytes.

```
tcpdump 'udp and greater 512'
```