Assignment 1

Gohil Dwijesh
2017CS50407

Prafful
2017CS10369

August 2019

1 Local network analysis

Day-1			Day-2			Day-3		
Afternoon	Evening	Night	Afternoon	Evening	Night	Afternoon	Evening	Night
10.243.144.0: 10.243.144.1, 10.243.144.164	-1	-1	-1	-1	-1	-1	-1	-1
10.254.243.0: 10.254.243.1, 10.254.243.2, 10.254.243.5, 10.254.243.6	-1	-1	-1	-1	-1	-1	-1	-1
10.254.239.0: 10.254.239.1, 10.254.239.2, 10.254.239.5, 10.254.239.6	-1	-1	-1	-1	-1	-1	-1	-1
10.254.236.0: 10.254.236.9, 10.254.236.10, 10.254.236.13, 10.254.236.14, 10.254.236.17, 10.254.236.18, 10.254.236.21, 10.254.236.22	-1	-1	-1	-1	-1	-1	-1	-1

Table 1: Analysis over Ethernet

Day-1			Day-2			Day-3		
Afternoon	Evening	Night	Afternoon	Evening	Night	Afternoon	Evening	Night
-1	-1	-1	-1	-1	-1	-1	-1	-1
-1	-1	-1	-1	-1	-1	-1	-1	-1
-1	-1	-1	-1	-1	-1	-1	-1	-1
-1	-1	-1	-1	-1	-1	-1	-1	-1

Table 2: Analysis over wife

2 Internet Architecture

3 Packet Analysis

a) Grabbing and analysing packats while visiting www.iitd.ac.in website

i) DNS filter

- My laptop(10.184.52.92) sends DNS query to IIT Delhi DNS server(10.10.2.2)
- Asking for IP addresses for the requested domain name (iitd.ac.in) and all the domain names which are linked with that web page(i.e., library.iitd.ac.in)
- IIT Delhi DNS server replies with IP address of the queried domain name. For example, reply for iitd.ac.in domain name is 10.7.174.111
- Time taken for the both query and reply for iitd.ac.in domain name is 0.008394231 seconds
- Different time taken for different queries

ii) HTTP filter

- 150 HTTP requests found
- My laptop(10.184.52.92) sends an HTTP request to iitd.ac.in(10.7.174.111) website host, asking for the html(or similar) code of the web-page
- Host(10.7.174.111) sends an HTTP respond to me(10.184.52.92), sending the web-page code
- Complex web-pages consist of references to many other files(.css, .js, etc.), photos, gifs, etc. in its HTML code
- My browser starts rendering the received code. As soon as it finds references to any file that is located in the server, it sends a new HTTP request, asking for the content of that file
- As the browser encounters file references while rendering, it keeps asking for the content via HTTP requests

iii) TCP filter

- Optimization done by the browser:
  - There are multiple TCP connections made from source port to destination port(80). Each TCP connection defers in source port(43001-43187). By default each connection is persistent unless client explicitly signals the closing of TCP connection
  - Multiple HTTP requests-responses can be made on the same TCP connection. In general these requests are pipe-lined
  - Such HTTP requests-responses can be made on all the TCP connections between the source and the destination host
  - This configuration makes TCP protocols to work more efficiently, and reduces the network traffic
- Yes, there are some content objects that are fetched on the same TCP port because of multiple HTTP requests can be made on the same TCP connection
- After any TCP connection is established, client sends an HTTP request to server and as soon as the server receives the request it sends back a TCP ack packet to the client and vice versa

iv) Time taken to download the complete web-page

- Time at the first DNS query: 2.311199694 sec
- Time at the last HTTP response: 5.853938462 sec
- Total time taken to download the complete web-page is: 3.54273877 sec

v) HTTP vs HTTPS protocols

- Observations:
  - After tracing for http://www.indianexpress.com website and analyzing the packets we could find exactly one HTTP packet and instead we found TLSv1.2 packets
- HTTP vs HTTPS:
  - HTTP response packet contains:

```
HTTP/1.1 301 Moved Permanently
Location: https://indianexpress.com
```

  - HTTPS is more secure than HTTP. It consists of SSL certificate that encrypts the data being transferred on the network for the security purposes. It also uses TLS(Transport Layer Security) protocol to prevent the data being modified or corrupted
  - That is why we see TLSv1.2 packets instead of HTTP packets
- Take home message:
  - Sensitive websites that involve routing of sensitive user data, prefer secure connection. Indianexpress also uses the secure connection, so we can not see the data being transffered(in this case: the webpage content), because it is encrypted using SSL certificate.

4 Tinkering with the network setting

4.1 Where to configure IP address and DNS server

- Linux: add the following to /etc/network/interfaces file.

```
auto eth0
iface eth0 inet static
    address 10.0.0.41
    netmask 255.255.255.0
```

```
network 10.0.0.0
broadcast 10.0.0.255
gateway 10.0.0.1
dns-nameservers 10.0.0.1 8.8.8.8
dns-domain acme.com
dns-search acme.com
```

4.2 Configure static IP address on android

- wifi settings -> networks details -> IP setting(change it from DHCP to Static) -> (fill the details)

4.3 Static IP Assignment vs Dynamic IP Assignment

- Static IP addresses are the fixed IP addresses given to any device on internet and Dynamic IP addresses change over time(dynamically assigned).
- Static IP addresses are more vulnerable compared to Dynamic ones. So mail servers, gaming servers which are not worried about their locations, generally use static IP addressing, while business, offices, etc. uses dynamic IP addressing.