IOT & Cyber Security - Week 2 - Scanning Activity

1) How many hops from your machine to your assigned website?

We use the "tracert" command on google.com and we have 13 hops.

```
::\Users\borte>tracert google.com
Tracing route to google.com [
over a maximum of 30 hops:
                                 <1 ms 192.168.2.20
        <1 ms
                     <1 ms
         8 ms
2
3
4
5
6
7
8
9
10
11
12
                     4 ms
                                  3 ms
                                          10.255.255.32
        26 ms
                     41 ms
                                 54 ms
                                          10.10.2.141
        18 ms
                     39 ms
*
                                 31 ms
                                           10.10.2.9
                                          Request timed out.
                                12 ms 01-adana-xrs-t2-1---98-lefkosa-t3-1.statik.turktelekom.com.tr [81.212.30.160]
23 ms 35-izmir-xrs-t2-1---01-adana-xrs-t2-1.statik.turktelekom.com.tr [195.175.166.0]
47 ms 35-ebgp-izmir-sr12e-k---35-izmir-xrs-t2-1.statik.turktelekom.com.tr [81.212.30.5]
        12 ms
                     15 ms
        42 ms
                     44 ms
                                          307-sof-col-2---35-ebgp-izmir-sr12e-k.statik.turktelekom.com.tr [212.156.104.162] 142.250.167.192
        49 ms
                     78 ms
                                 70 ms
                    91 ms
36 ms
        48 ms
                                 50 ms
                                 53 ms
        67 ms
                                          142.250.210.95
142.250.56.111
                                 34 ms
        60 ms
                    208 ms
                                          sof02s49-in-f14.1e100.net [
Trace complete.
```

2) Which step causes the biggest delay in the route? What is the average duration of that delay?

In 5th line because there is a time out and the average duration is 85ms.

```
\Users\borte>tracert google.com
Tracing route to google.com [
over a maximum of 30 hops:
                                  <1 ms 192.168.2.20
3 ms 10.255.255.32
         <1 ms
8 ms
                      <1 ms
                       4 ms
                                            10.10.2.141
10.10.2 9
                      41 ms
                                  * Request timed out.
                                  12 ms 01-adana-xrs-t2-1---98-lefkosa-t3-1.statik.turktelekom.com.tr [81.212.30.160]
23 ms 35-izmir-xrs-t2-1---01-adana-xrs-t2-1.statik.turktelekom.com.tr [195.175.166.0]
47 ms 35-ebgp-izmir-sr12e-k---35-izmir-xrs-t2-1.statik.turktelekom.com.tr [81.212.30.5]
         42 ms
                      44 ms
         49 ms
                      78 ms
                                   70 ms
                                             307-sof-col-2---35-ebgp-izmir-sr12e-k.statik.turktelekom.com.tr [212.156.104.162]
         48 ms
                      91 ms
                                  50 ms
                                            142.250.167.192
 11
12
         67 ms
                     36 ms
                                  53 ms
                                            142.250.210.95
         60 ms
                                   34 ms
                                            142.250.56.111
                    208 ms
                                            sof02s49-in-f14.1e100.net [4
         43 ms
                                  55 ms
                     38 ms
 race complete
```

```
C:\Users\borte>ping google.com

Pinging google.com [ with 32 bytes of data:
Reply from 100 bytes=32 time=65ms TTL=54
Reply from 100 bytes=32 time=37ms TTL=54
Reply from 100 bytes=32 time=180ms TTL=54
Reply from 100 bytes=32 time=60ms TTL=54
Reply from 100 bytes=32 time=180ms TTL=54
Reply f
```

3) What are the main nameservers for the website?

The main nameserver is a google.com

```
C:\Users\borte>nslookup google.com
Server: dns.cypking
Address: Management
Non-authoritative answer:
Name: google.com
Addresses: Management
Addresses: Man
```

4) Who is the registered contact?

We can see this with the "whois" command. I did this in linux terminal because windows cmd doesn't support it.

```
Protakali:~# whois google.com

Domain Name: GOOGLE.COM

Registry Domain ID: 2138514_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.markmonitor.com

Registrar URL: http://www.markmonitor.com

Updated Date: 2019-09-09T15:39:04Z

Creation Date: 1997-09-15T04:00:00Z

Registry Expiry Date: 2028-09-14T04:00:00Z

Registrar: MarkMonitor Inc.

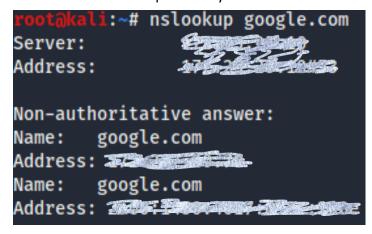
Registrar IANA ID: 292

Registrar Abuse Contact Email: abusecomplaints∂markmonitor.com

Registrar Abuse Contact Phone: +1.2086851750
```

5) What is the MX Record for the website?

MX Record command is nslookup. I show you from linux terminal.



6) Where is the website hosted?

Reflection Part:

- 1) Did you have any issues or challenges with the scans?

 I have only one issue. I couldn't run the mx record command fully.
- 2) How did you overcome them?
 I got over it with what we saw in class and research I did on the internet.
- 3) How will they affect your final report?

 It was a very fun part for me. Learning about windows cmd commands and linux commands showed me how things work in the background. With the Scanning activity, I learned how the threads in the network reach us and how I can examine them.