

### Unit 3- Network Scanning Exercise

How many hops from your machine to your assigned website?

The traceroute command “traceroute + “IP address” allows a maximum of 64 hops. With my local router being the first hop, the scan started losing packets and looping in the same IP address on the eleventh hop. Following this, I stopped running the command.

```
Antonios-MBP:~ akalaitzakias$ traceroute 18.209.2.175
traceroute to 18.209.2.175 (18.209.2.175), 64 hops max, 52 byte packets
 1  rt-ac86u-b338 (192.168.1.1)  3.177 ms  2.768 ms  1.160 ms
 2  * * *
 3  212.142.60.5 (212.142.60.5)  12.477 ms  27.431 ms  11.073 ms
 4  asd-rc0001-cr101-be112-2.core.as33915.net (213.51.7.90)  10.814 ms  11.190 ms  11.298 ms
 5  nl-ams17b-rc1-lag60-2.core.as33915.net (213.51.64.6)  10.414 ms  24.109 ms  11.868 ms
 6  us-was02a-rd2-ae-105-0.aorta.net (84.116.130.66)  108.085 ms  108.565 ms  108.707 ms
 7  us-was03a-r11-ae-11-0.aorta.net (84.116.130.165)  112.026 ms  107.390 ms  157.648 ms
 8  99.82.183.148 (99.82.183.148)  123.232 ms  107.976 ms  109.318 ms
 9  * * *
10  * * *
11  52.93.28.108 (52.93.28.108)  142.784 ms
    52.93.28.116 (52.93.28.116)  110.528 ms
    52.93.28.118 (52.93.28.118)  108.405 ms
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * ^C
Antonios-MBP:~ akalaitzakias$
```

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

The biggest latency was recorded to the final target. This could be a result of an active firewall blocking requests or a slow internet connection at the target. The average delay was 120 ms.

What are the main nameservers for the website?

**175.2.209.18.in-addr.arpa and ec2-18-209-2-175.compute-1.amazonaws.com**

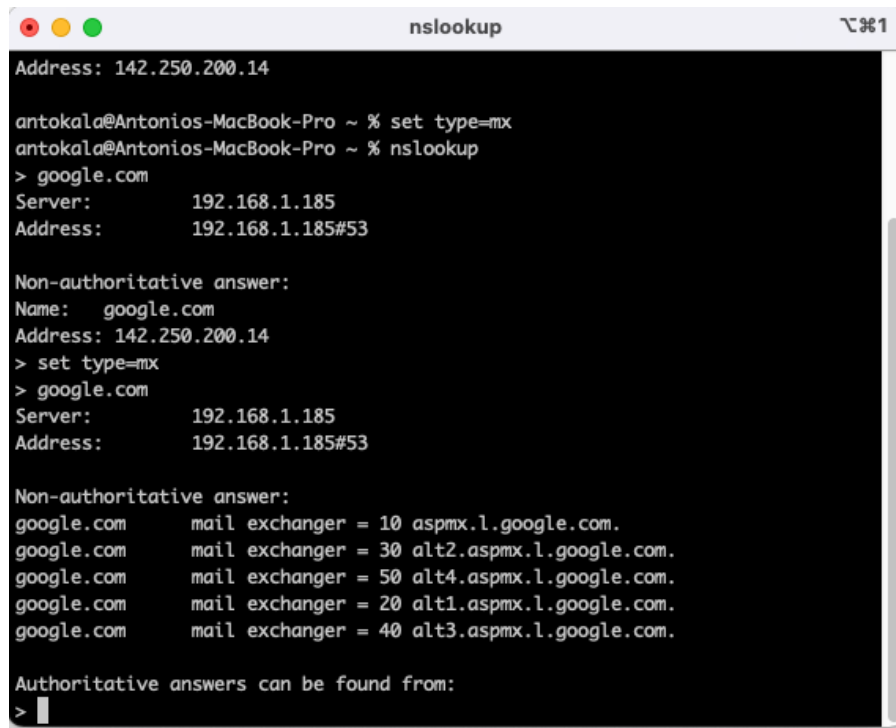
```
Antonios-MBP:~ akalaitzakias$ nslookup 18.209.2.175
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
175.2.209.18.in-addr.arpa      name = ec2-18-209-2-175.compute-1.amazonaws.com.

Authoritative answers can be found from:
Antonios-MBP:~ akalaitzakias$
```

What is the MX record for the website?

I do not have the MX records of the target website, and since the server is down, I performed an MX scan against google.com in order to show the way we can obtain the MX records.



```
Address: 142.250.200.14

antokala@Antonios-MacBook-Pro ~ % set type=mx
antokala@Antonios-MacBook-Pro ~ % nslookup
> google.com
Server:      192.168.1.185
Address:     192.168.1.185#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.200.14
> set type=mx
> google.com
Server:      192.168.1.185
Address:     192.168.1.185#53

Non-authoritative answer:
google.com    mail exchanger = 10 aspmx.l.google.com.
google.com    mail exchanger = 30 alt2.aspmx.l.google.com.
google.com    mail exchanger = 50 alt4.aspmx.l.google.com.
google.com    mail exchanger = 20 alt1.aspmx.l.google.com.
google.com    mail exchanger = 40 alt3.aspmx.l.google.com.

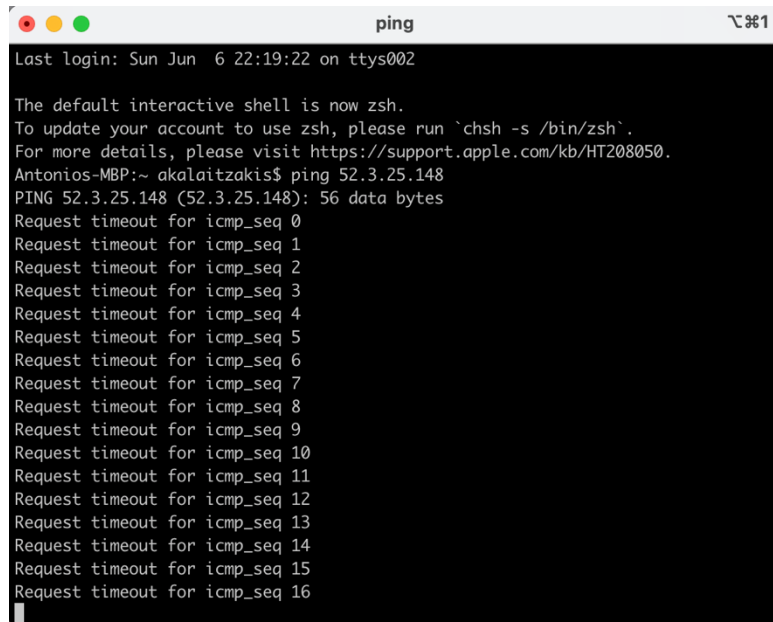
Authoritative answers can be found from:
> 
```

Where is the website hosted?

The website is hosted in Northern Virginia, US.

## Issues with the scans:

When we first received the target server, the IP address provided was wrong. I was running the ping command, but it was resulting in timeout errors.

A terminal window titled 'ping' with a macOS-style title bar (red, yellow, green buttons). The window shows the output of a ping command. It starts with a login message: 'Last login: Sun Jun 6 22:19:22 on ttys002'. Then it says 'The default interactive shell is now zsh. To update your account to use zsh, please run `chsh -s /bin/zsh`. For more details, please visit https://support.apple.com/kb/HT208050.' The user then runs 'ping 52.3.25.148'. The output shows 'PING 52.3.25.148 (52.3.25.148): 56 data bytes' followed by 17 lines of 'Request timeout for icmp\_seq 0' through 'icmp\_seq 16'.

```
ping
Last login: Sun Jun 6 22:19:22 on ttys002

The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
Antonios-MBP:~ akalaizakis$ ping 52.3.25.148
PING 52.3.25.148 (52.3.25.148): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
Request timeout for icmp_seq 5
Request timeout for icmp_seq 6
Request timeout for icmp_seq 7
Request timeout for icmp_seq 8
Request timeout for icmp_seq 9
Request timeout for icmp_seq 10
Request timeout for icmp_seq 11
Request timeout for icmp_seq 12
Request timeout for icmp_seq 13
Request timeout for icmp_seq 14
Request timeout for icmp_seq 15
Request timeout for icmp_seq 16
```

In order to overcome the error, I run the “ping” command again, but I used the domain name rather than its IP. As a result, the domain replied with its correct IP address.

```
--- PING nismphp-env.eba-ytbpyww.us-east-1.elasticbeanstalk.com (18.209.2.175) 56(84) bytes of data. ---
64 bytes from 18.209.2.175: icmp_seq=1 ttl=237 time=95.4 ms
64 bytes from 18.209.2.175: icmp_seq=2 ttl=237 time=95.9 ms
64 bytes from 18.209.2.175: icmp_seq=3 ttl=237 time=95.4 ms
64 bytes from 18.209.2.175: icmp_seq=4 ttl=237 time=95.3 ms

--- nismphp-env.eba-ytbpyww.us-east-1.elasticbeanstalk.com ping statistics ---

packets transmitted 4
received 4
packet loss 0 %
time 3012 ms

--- Round Trip Time (rtt) ---

min 95.345 ms
avg 95.505 ms
max 95.886 ms
mdev 0.221 ms
```