

Collaborative Learning Discussion 2: Scanning Exercise and Results

The scanning exercise was performed against the AWS server set up by the university, as multiple teams had admin problems running their own servers.

The commands I used were ping, dig, nslookup, traceroute and open ports scan. Additional penetration scans were performed in order to assist with the Unit 6 and Unit 11 assignments.

The server's link used for the scan was the <http://nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com>.

Ping:

First, I run the ping command in order to obtain the server's IP address.

Ping allows us to send data packages to specific URL or IP address and check if the server responds and how long it took to transmit the package (How-to geek, 2018).

```
--- PING nismphp-env.eba-ytbpbyww.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-ytbpbyww.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
```

The server's IP address is 18.209.2.175 and the average latency was 95 ms.

Nslookup:

Nslookup can also be used to retrieve the IP address from a URL. I used the nslookup command to perform a DNS Query using the IP address. This returned the server's address.

```
Antonios-MBP:~ akalaitzakis$ 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:~ akalaitzakis$
```

dig:

The dig command is used to retrieve information about the DNS name servers (GeeksforGeeks, 2020).

```
Antonios-MBP:~ akalaizakis$ dig 18.209.2.175

; <<> DiG 9.10.6 <<> 18.209.2.175
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 39434
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;18.209.2.175.                IN      A

;; AUTHORITY SECTION:
.                600     IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2021060700 1800 900 604800 86400

;; Query time: 13 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Mon Jun 07 18:43:52 CEST 2021
;; MSG SIZE rcvd: 116

Antonios-MBP:~ akalaizakis$
```

Traceroute:

The traceroute command is used to track and “map” the path taken by a packet from our local router to the destination. It reports all the IPs pinged in between (ThousandEyes, n.d).

```
Antonios-MBP:~ akalaizakis$ 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:~ akalaizakis$
```

As my test showed, the packet performed eleven hops until it started losing packages. The first hop started from my local router, it passed through six IP addresses, until it finally reached the destination.

Port scan:

Finally, I performed an open port scan. Open ports are ports operating using the TCP or UDP protocol and are configured to accept external packages (Tunggal, 2021).

📄 18.209.2.175					
<ul style="list-style-type: none">> ec2-18-209-2-175.compute-1.amazonaws.com> nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com					
Port Number	State	Service Name	Service Product	Service Version	Service Extra Info
● 22	open	ssh	OpenSSH	7.4	protocol 2.0
● 80	open	http	Apache httpd		
● 443	closed	https			

References:

GeeksforGeeks (2020) How to Use the Ping Command to Test Your Network Available from: <https://www.geeksforgeeks.org/dig-command-in-linux-with-examples/> [Accessed 3 June 2021].

How-to Geek (2018) How to Use the Ping Command to Test Your Network Available from: <https://www.howtogeek.com/355664/how-to-use-ping-to-test-your-network/> [Accessed 3 June 2021].

ThousandEyes (n.d) What is Traceroute & What is it For? Available from: <https://www.thousandeyes.com/learning/glossary/traceroute> [Accessed 3 June 2021].

UpGuard (2021) What is an Open Port and are they Dangerous? Available from: <https://www.upguard.com/blog/open-port> [Accessed 3 June 2021].