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.

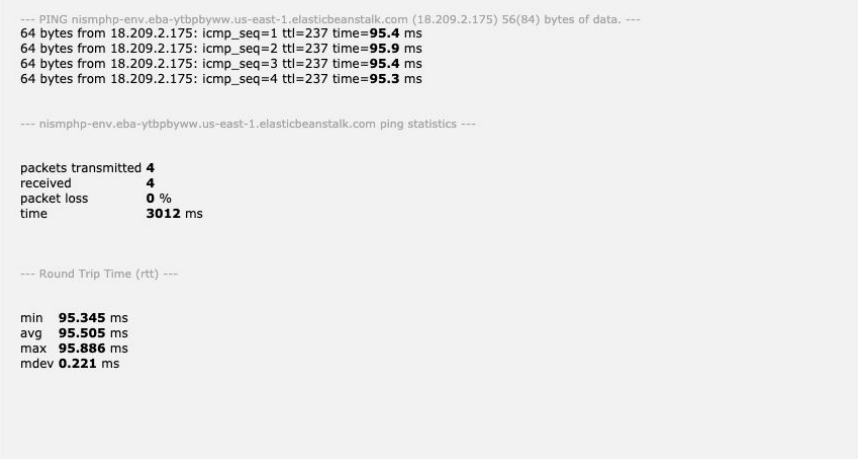
The commands I used were ping, dig, nslookup, traceroute and open ports scan. Additional penetration scans were performed in order to assist with the Unit 6 and Unit 11 assignments.

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).



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

Nslookup:

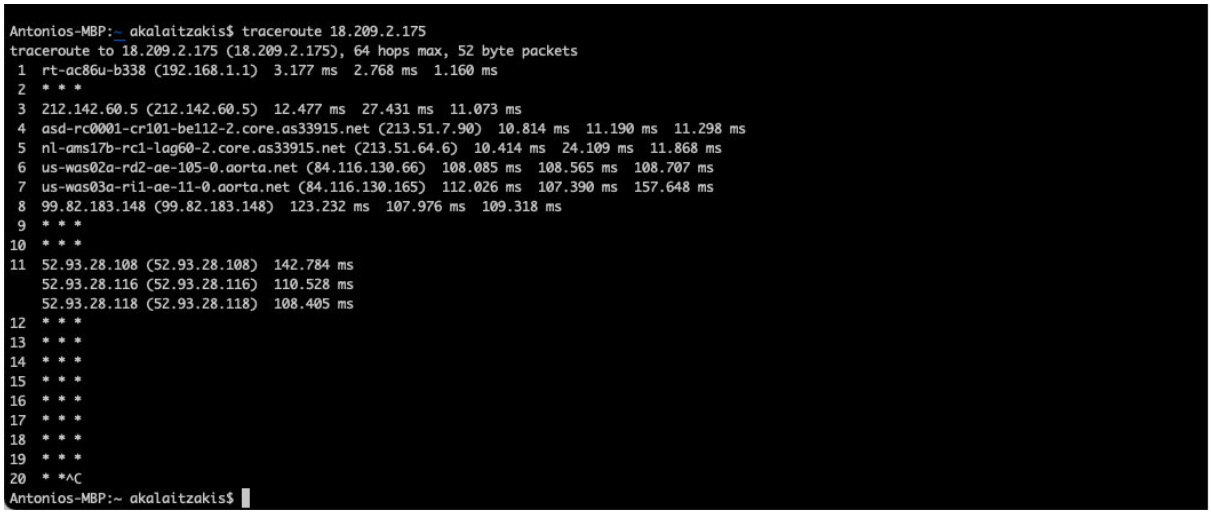
Nslookup can also be used to retrieve the IP address from a URL. I used the nslookup command to perform a DNS Query using the IP address. This returned the server's address.

dig:

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

Traceroute:

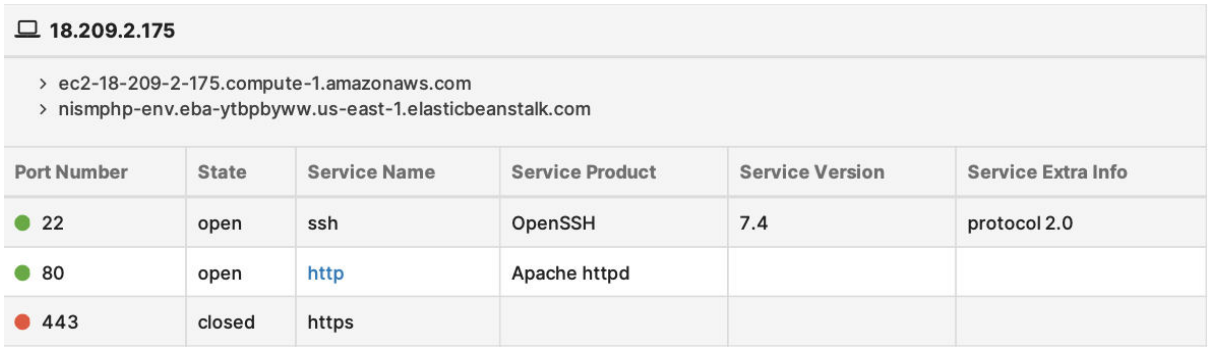
The traceroute command is used to track and "map" the path taken by a packet from our local router to the destination. It reports all the IPs pinged in between (ThousandEyes, n.d).



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

› 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].