As group 4 we used a lot of tools during our scanning sessions which include MTR, Nmap, Ping, Whois, DNS, OWASP and traceroute. However, for my personal scans, I decided to use Nmap and Traceroute.

# **Traceroute**

Traceroute is a network testing term that is used to examine the hops that communication will follow across an IP network (HackerTarget, N.D). Packets are sent across the network and a Time to Live (TTL) is measured. It is always a good thing to see the path which the network is taking as it travels across the globe

# Result

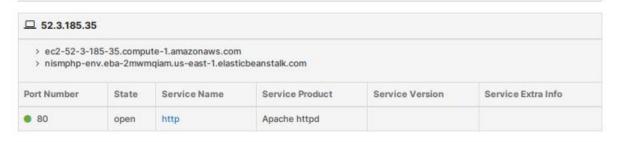
HOST: 0e3280ddb536	.oss%	Snt	Last	Avg	Best	Wrst S	tDev
1.  172.17.0.1	0.0%	2	0.1	0.1	0.1	0.1	0.0
2.  gw-li777.linode.com	0.0%	2	0.4	0.4	0.4	0.4	0.0
3.  10.206.64.14	0.0%	2	1.6	1.0	0.4	1.6	0.0
4.  10.206.32.68	0.0%	2	0.9	1.0	0.9	1.0	0.0
5.  10.206.32.53	0.0%	2	0.7	0.6	0.5	0.7	0.0
6.  de-cix1.nyc.amazon.com	0.0%	2	1.4	1.5	1.4	1.6	0.0
7.  52.93.247.165	0.0%	2	15.3	17.4	15.3	19.6	3.0
8.  52.93.59.61	0.0%	2	1.0	1.9	1.0	2.7	1.0
9.  ???	100.0	2	0.0	0.0	0.0	0.0	0.0
10.  ???	100.0	2	0.0	0.0	0.0	0.0	0.0
11.  ???	100.0	2	0.0	0.0	0.0	0.0	0.0
12.  ???	100.0	2	0.0	0.0	0.0	0.0	0.0
13.  ???	100.0	2	0.0	0.0	0.0	0.0	0.0
14.  150.222.251.33	0.0%	2	11.2	9.7	8.1	11.2	2.0
15.  ???	100.0	2	0.0	0.0	0.0	0.0	0.0

# **NMAP**

Port scanning is part of the first phase of a penetration test and allows you to find all network entry points available on a target system (Pentest-tools, N.D). Cyberpedia (N.D) also explains that running a port scan on a network or server reveals which ports are open and listening (receiving information), as well as revealing the presence of security devices such as firewalls that are present between the sender and the target.

# **RESULT**

## Found 1 open port (1 host)



riost: nismphp-env.eba-2mwmqiam.us-east-1.elasticbeanstalk.com
Ports: Top 100 ports
Ping host: True
Detect OS: False
Detect ov: Detect svc version: True Traceroute: False

#### Scan information

2021-07-25 16:54:50 UTC+03 2021-07-25 16:55:01 UTC+03 Start time: Finish time:

Scan duration: 11 sec Scan status: Finished

## References

Cyberpedia (N.D) What is a port scan Available from: https://www.paloaltonetworks.com/cyberpedia/what-is-a-port-scan

HackerTarget (N.D) Online Traceroute using MTR Available from: https://hackertarget.com/online-traceroute/

Pentest-tools.com (N.D) About this online port scanner Available from: https://pentest-tools.com/network-vulnerability-scanning/tcp-port-scanner-onlinenmap