For the scan of the opposite team’s website, multiple scans and tools were used such as: Nmap, Traceroute, Nslookup, Whois, MTR, Ping and Dig. As a team, we collated our results together to provide the following information. The exercise seems to emulate reconnaissance which is the first step of the network security assessment methodology. The purpose of reconnaissance is to map the network, hosts and sometimes users to provide a foundation for further assessment activities, such as vulnerability scanning (McNab, C., 2016).

Using Traceroute (Linux) or tracert (Windows), we were able to see the distance between our machines to the target website. We found collectively that we had a few timeouts / no TTL expiry replies from some servers along the route while the command was running; however, on average we saw between 13 - 30 plus hops. These scans used ICMP packets, which have low priority and are sometimes simply blocked by some firewalls.

Utilizing MTR and Nmap we were able to send TCP packets for tracerouting, which assemble a more realistic route for traffic, since standard http requests to load a website are typically sent via TCP. Nmap additionally gave some more features to e.g. fragment packets, to circumvent web application firewalls (WAF), which Amazon Web Services (AWS) likely does have in place. Our results for this were varied, some showing only two hops which is unrealistically short. This however could be explained by the fact that the router from our home networks handled the majority of TCP traffic, which led to skipping of hops in the result of the scan. Using mobile phone WiFi spots, or cloud hosted Kali installations, we were able to circumvent the issue and managed to see 5 to 11 hops.

We were also able to identify the hosting locations and multiple nameservers through our scans. We also were able to find the MX records of the website using Nslookup; however, some of our team did experience issues with finding this information, initial scans not showing any MX record available.

A number of us did encounter issues with network diagnostic tools utilising ICMP, such as Traceroute. This may be due to security controls encountered on the route the packets take, for example firewalls (Parziale, L., et al, 2006). That being said, we were able to overcome challenges and collectively find useful information using basic scans against the opposite website.

REFERENCES

McNab, C. (2016) *Network Security Assessment: Know Your Network*. 3rd ed. O’Reilly Media.

Parziale, L., Britt, D., Davis, C., Forrester, J., Lui, W., Matthews, C. & Rosselot, N. (2006) *TCP/IP Tutorial And Technical Overview*. 8th ed. New York: IBM.