Student: Kingsley

The practical activity in unit 3 involves me using a trace route which is a command line utility to identify the exact path a data packet takes in terms of route connected to as it travels across the internet. (from the sender to its destination in this case a hosted server www.allmytpe.co.uk). This concept helps to identify bottlenecks in the process like where and why server are timing outs or lagging

Performing this activity on Microsoft windows 10 OS, 13 hoops were discovered with highest hoop in terms of delay at step 7. Round trip time was completed at 76Ms duration on average suggesting the route might just be too most far away from the next route. (long distance between route 6 and 7 and 8) and not necessarily a lag. Had it been there was a consistent rise in the round trip time from hoop 7 towards the ends hoops then this might be a cause for concern

Using WINMTR for further analysis, after running for 12 minutes it was discovered that there were package lost with average of 2.23% but hoop 10 has the highest package loss of 22. This did not suggest much of a problem since it is one off and not a continuation and the latency result did not suggest any upward trend either

Using nslookup via command line of a window machine the main nameserver and the MX record was determined

A network search of WHOIS lookup returned information on the registered contact and where the website was hosted

Thank you, Kingsley, for the summary of your scanning findings.

There are consistent findings with the traceroute results and the latency is quite similar, suggesting the packets are following the route from different country destinations. Your conclusions in the WINMTR further support these results as there is no constant increase in latency, and there were no issues with packets dropping off. We can safely assume the discrepancy is due to the user's location.

Introducing numerous scanning tools further supports a rounded conclusion of results. Using the nslookup and whois commands are helpful to gain knowledge of the nameserver, MX record and registered contact (Parziale, 2006). Additionally, the use of the dig command would have been of benefit too. The dig tool has greater flexibility than nslookup as it will provide name servers, IP addresses, and mail servers. The ease of this method means it can be conducted all in one command quickly.

With regard to configuration, dig offered options to send queries to specified ports and particular TCP based queries (O'Reilly & Associates, 2002). Furthermore, insights can be gained from Nmap (Nmap Online, N.D.), which can support scanning open ports for further analysis (Internet Assigned Numbers Authority, N.D.) and email security protocols. This is helpful to avoid using well-known ports for a customised security design. Therefore providing a wide range of resources are useful to understand the methodology or process of how threat actors may be staging an attack and allowing administrators knowledge to implement an improved security policy.

Internet Assigned Numbers Authority. (N.D.). IANA. Available: https://www.iana.org/ [Accessed 5 December 2021].

Nmap Online. (N.D.). Scan. Available: https://nmap.online/ [Accessed 5 December 2021].

O'reilly & Associates. (2002). DNS and BIND. Available: https://docstore.mik.ua/orelly/networking_2ndEd/dns/ch12_09.htm [Accessed 13 December 2021].

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.