Within the original post, basic scans were conducted on https://allmytype.co.uk. First, the routes to the website were mapped using the traceroute command in windows (a2hosting, 2021). It was determined that there were fifteen hops to the location. The latency of the pings increased during the latter half around hop nine. Overall, the route was stable and there were no dropped packets. Using the Linux command Dig, the name servers were able to be queried. Dig showed four different name servers, with them being Ns1.a2hosting, Ns2.a2hosting, Ns3.a2hosting, and Ns4.a2hosting. Similarly, another Linux command whois shows the registered contact for the website(DomainTools, 2021). The command showed that the contact was a company that sold domains named ENOM. Through the same dig command, a mail server was also discovered. Lastly, the website was determined to be hosted through A2 hosting, which is based in the Netherlands (Hostingchecker, 2021).

The contributions contributed by others also brought up great points. Nslookup is definitely a powerful tool. It is a native command to windows, which for one makes it very accessible. As well it provides a lot of customizability. The commands can be catered to the specific needs of the user, to find information. It is also rather easy to read and interpret the results. The combination of nslookup with other web tools or Dig can be used to provide more overall functionality.

As well the scans do show a critical opening for where cyberattacks could occur. The dig commands were able to show the IP addresses for both the name servers and the mail server with minimal effort. The four name servers do provide redundancy, in case there is a DDoS attack (cisa, 2019). However, at the same time, the addresses are exposed and can be easily attacked. The use of external security technologies such as the use of proxy to hide the IP addresses. As well, an NGFW with network address translation(NAT) could also be used to hide the IP’s.

References:

A2hosting. (2021) How to troubleshoot network connectivity using ping and traceroute. Available from:<https://www.a2hosting.com/kb/getting-started-guide/internet-and-networking/troubleshooting-network-connectivity-with-ping-and-traceroute> [Accessed 1 December 2021].

CISA.(2010) Understanding Denial-of-Service Attacks. Available from:<https://www.cisa.gov/uscert/ncas/tips/ST04-015> [Accessed 11 December 2021].

DomainTools. (2021) Whois Lookup. Available from:<https://whois.domaintools.com/allmytype.co.uk> [Accessed 1 December 2021].

Hostingchecker. (2021) Finding out who is hosting any website. Available from:

<https://hostingchecker.com/> [Accessed 1 December 2021].