Collaborative Discussion 2 – Initial Post (Team A)

How many hops from your machine to your assigned website?

For this we used the traceroute tool, which is available on MacOS, Windows, and Linux machines. This tool reports information about each hop taken by a packet between a computer and remote host. We initially struggled to get a result using traceroute on the provided AWS URL, however increasing the maximum number of hops from 30 to 64 allowed a full traceroute to be completed without timing out. It took 37 hops from our machine to the assigned website (*How to troubleshoot network connectivity using ping and traceroute*, no date; Tetz, 2011; Broad and Bindner, 2014; Edwards and Bramante, 2015).

What are the main nameservers for the website?

To find the information on the main nameservers we used both dig and nslookup. Both tools can be used to retrieve various DNS information for a given website. Setting the record type to NS returns the appropriate information. Windows machines use nslookup, Linux machines use sig, and MacOS machines can use both (*How to troubleshoot DNS with dig and nslookup*, no date).

Who is the registered contact?

Similarly to the nameservers above, the registered contact can be found by using the nslookup or dig tools and setting the DNS record type to RP. These tools did not reveal any useful information relating to the registered contact. We therefore used the whois command(Bruen, 2015) to determine the registered contact- Amazon

What is the MX record for the website?

Similarly to the nameservers above, the registered contact can be found by using the nslookup or dig tools and setting the DNS record type to MX. We did not identify any information using this command, and therefore used the whois command (Bruen, 2015).

Where is the website hosted?

Similarly to the nameservers above, the registered contact can be found by using the nslookup or dig tools and setting the DNS record type to LOC. This command was not able to determine the location, therefore a whois command was performed to determine the location- Reno, Nevada, USA

References

Broad, J. and Bindner, A. (2014) ‘Chapter 8 - Scanning’, in Broad, J. and Bindner, A. (eds) *Hacking with Kali*. Boston: Syngress, pp. 103–130. doi: https://doi.org/10.1016/B978-0-12-407749-2.00008-2.

Bruen, G. O. (2015) *WHOIS Running the Internet: Protocol, Policy, and Privacy*. Wiley. Available at: https://books.google.co.za/books?id=mgmeCAAAQBAJ.

Edwards, J. and Bramante, R. (2015) *Networking Self-Teaching Guide: OSI, TCP/IP, LANs, MANs, WANs, Implementation, Management, and Maintenance*. Wiley. Available at: https://books.google.co.za/books?id=YSPPBwAAQBAJ.

How to troubleshoot DNS with dig and nslookup (no date). Available at: https://www.a2hosting.co.uk/kb/getting-started-guide/internet-and-networking/troubleshooting-dns-with-dig-and-nslookup#Using-dig-on-Apple-Mac-OS-X-and-Linux (Accessed: 10 September 2021).

How to troubleshoot network connectivity using ping and traceroute (no date). Available at: https://www.a2hosting.com/kb/getting-started-guide/internet-and-networking/troubleshooting-network-connectivity-with-ping-and-traceroute#Testing-the-path-to-a-remote-host-with-traceroute (Accessed: 11 September 2021).

Tetz, E. (2011) *Cisco Networking All-in-One For Dummies*. Wiley (--For dummies). Available at: https://books.google.co.za/books?id=7DVtgcZVOYIC.