Unit 4

Collaborative Discussion

Our group investigated how to obtain as much network information as possible for the assigned website, **www.staffmatters.co.uk**. The activity recommended several command-line tools to begin the investigation, such as NSLOOKUP (name server lookup), ping, tracert (traceroute) and WHOIS.

Establishing the footprint of a network consists of several steps used in gathering information about network owners of a domain under interest. The first three steps were undertaken in the scanning activity, namely (1) identifying the domain name; (2) locating the network range using NSLOOKUP and WHOIS; (3) confirming the machine is still active using PING (Sheikh, 2021). For Step 2, NSLOOKUP was used to query the default DNS server for the domain name, IP address mapping details, and DNS records of the target website; including the mail exchange ("mx") server. I specified additional options to the command-line tool via the “-type” switch, namely “ns” to show domain name server information and “soa” (“Start of Authority”) to show a domain’s primary DNS server.

The WHOIS registry database provides public information about registrants of a domain, including their telephone number, email address, first and last name, as well as the registered company address of the domain owner. Using an available WHOIS service (https://dnschecker.org/ip-whois-lookup.php), information for six registrants was obtained. Since this information is open to public viewing, it is essential to question the role of GDPR on this data. Lu et al. (2021) note that WHOIS might not provide complete public information in future requests due to ICANN's Temporary Specification that proposes registrars and registries enable a tiered-access framework that allows usage of WHOIS data for legitimate purposes (e.g., law enforcement and commercial litigation) (ICANN, ND). Based on the public information provided by WHOIS, the scan identified the hosting server is in Michigan, USA and an IP address range between `68.66.212.0` and `68.66.255.255`.

TRACERT was another tool used to discover the footprint of the network between the scanning computer and the target domain. TRACERT focuses on the number of hops and milliseconds a data packet takes to reach a target server using Internet Control Message Protocol (ICMP). If a data packet is rejected or dropped by a router, the output will be either an asterisk (*) or “Request Timed Out”. This is because some routers may consider ICMP traffic non-essential. Interesting to note is that the distance between servers impacts the hop

time of ICMP data packets and, therefore, may be leveraged to determine the general geolocation of a given server (Wang et al., 2017).

References

ICANN (ND). Temporary Specification for gTLD Registration Data. Available from https://www.icann.org/resources/pages/gtld-registration-data-specs-en. [Accessed 10 Dec. 2021]

Lu, C., Liu, B., Zhang, Y., Li, Z., Zhang, F., Duan, H., Liu, Y., Chen, J.Q., Liang, J., Zhang, Z. & Hao, S. (2021). From WHOIS to WHOWAS: A Large-Scale Measurement Study of Domain Registration Privacy under the GDPR.

RFC3912 (2004). WHOIS Protocol Specification. Available from https://datatracker.ietf.org/doc/rfc3912/ [Accessed 10 Dec. 2021]

Sheikh, A. (2021). Footprinting and Reconnaissance/Scanning Networks. *Certified Ethical Hacker (CEH) Preparation Guide*: 11-25. Apress, Berkeley, CA.

Wang, Z., Chen, Y., Wen, H., Zhao, L. & Sun, L. (2017). Discovering routers as secondary landmarks for accurate IP geolocation. *IEEE 86th Vehicular Technology Conference (VTC-Fall)*: pp. 1-5.