Peer Response

Jonathan, it is a great post about the scanning techniques and analysis result. Especially highlighted the scanning on opened TCP ports and email security protocol.

Reference to the TCP port findings by Nmap in Appendix 3, there were 8 ports limited in the scan result. By default, Nmap scans the most common 1,000 ports for each protocol with the well-known port list or it can set a port range to scan from 1 through 65535 (Nmap, N.D.). In the past, the well-known port numbers range is between 1 and 1023 (Parziale et al, 2006). After the accumulation of applications over a period of time, there are more than 13000 official ports have been registered in Internet Assigned Numbers Authority (IANA) nowadays. System ports (0-1023), user ports (1024-49151), and dynamic and/or private ports (49152-65535) are the three types of port numbers that are assigned (IANA, 2021). Nevertheless, to avoid using the well-known port, most of the application service ports can customize or by using Network Address Port Translation (NAPT) to redirect a different port number to the internal service (Parziale et al, 2006).

A2hosting servers have provided non-encrypted ports for e-mail service as it is a public hosting company that supports domains without Secure Sockets Layer (SSL) (A2hosting, N.D). Alternatively, it could use the email applications like iRedMail which provide the option to disable plaintext authentication, thereby forcing users to use secure port numbers (iRedMail, N.D). Moreover, the Dig command showed that the www.customersrus.co.uk domain has configured Sender Policy Framework (SPF) with text strings recorded in the Domain Name System (DNS) (Parziale et al, 2006). The SPF record is a list of all the IP addresses that can send email on behalf of the domain to prevent domain spoofing (Wong & Schlitt, 2006).

References:

Nmap (N.D.) Port Specification and Scan Order. *Nmap Reference Guide*. Available from: https://nmap.org/book/man-port-specification.html [Accessed 10 December 2021].

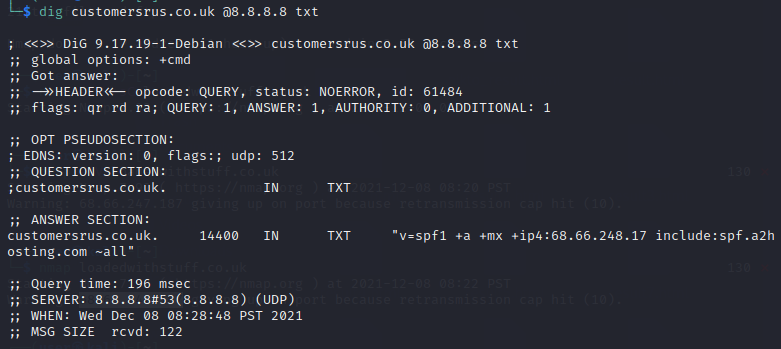
Parziale, L. et al, (2006) *TCP/IP tutorial & technical overview*. IBM Redbooks. Available via the Vitalsource Bookshelf [Accessed 10 December 2021].

IANA (Dec 3, 2021) Service Name and Transport Protocol Port Number Registry. *Assignments*. Available from: https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml [Accessed 10 December 2021].

A2 Hosting, Inc. (N.D.) How to access e-mail accounts with client applications. *Knowledge Base.* Available from: https://www.a2hosting.com/kb/getting-started-guide/setting-up-e-mail/accessing-e-mail-accounts-with-client-applications [Accessed 10 December 2021].

iRedMail (N.D) Allow insecure POP3/IMAP connections. *Document Index*. Available from: htps://docs.iredmail.org/allow.insecure.pop3.imap.smtp.connections.html [Accessed 10 December 2021].

Wong, M. & Schlitt, W. (April 2006) Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail. *Experimental*. Available from: https://datatracker.ietf.org/doc/html/rfc4408 [Accessed 10 December 2021].



<https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=289168>

Jonathan Callaghan