Summary Post – Unit 6

As the world moves into a digital era, online technologies continue to grow at a rapid pace. These include desktop and web applications as well as the adoption of cloud computing. While online technologies make our lives easier, it is becoming a challenge for cybersecurity professionals to keep up with security threats and vulnerabilities that arise (Jamil et al., 2018).

One of the ways that cybersecurity professionals attempt to secure websites and servers is by performing regular scans and penetration testing using scanning tools. The purpose of a scanning tool is to acquire more information about a specific host or target (I.T Governance Ltd, 2021). A scanning task was performed on a website called “https://loadedwithstuff.co.uk” with basic scanning tools such as *traceroute, mtr, dig*, *nslookup, whois, nmap* and *telnet* to extract useful information.

Information such as hops to destination, round trip times (RTT), name servers (NS), open ports amongst others were revealed. This task proved the simplicity involved to obtain sensitive information regarding a website. A scan tool of note is *nmap* (Network Mapper)which determines open ports to a server (Kaur & Kaur, 2017). While *nmap* is often used by attackers it is also used by network administrators and security professionals to perform security audits on networks (Hoque et at., 2014).

In addition, Chan (2021) mentions that *nmap* could enable version detection during the scan with the “sV” option (Nmap, N.D). Version detection will try to elicit responses and gather information, a view that the writer agrees with. Callaghan (2021) highlights the usage and importance of the *dig* command for querying information, a view the writer appreciates. Furthermore, *dig* can also trace the path taken by appending the *+trace* option to the *dig* command as seen in the image attached.

In conclusion, scanning tools provide the opportunity to discover sensitive information on servers/websites which could result in potential hacking. Server and website administrators should make use of these tools and strive to ensure that their systems remain secure.

Graphical user interface, text

Description automatically generated

List of References

Callaghan, J. (2021) ’Collaborative Learning Discussion 2’. Peer response submitted to University of Essex Online for [NISM\_PCOM7E November 2021] Initial Post by Zihaad Khan. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=289200 [Accessed 17 December 2021].

Chan, Y. (2021) ’Collaborative Learning Discussion 2’. Peer response submitted to University of Essex Online for [NISM\_PCOM7E November 2021] Initial Post by Zihaad Khan. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=289200 [Accessed 17 December 2021].

Hoque, N., Monowar, B.H., Baishya, R.C., Bhattacharyya, D.K., Kalita, J.K. (2014) Network attacks: Taxonomy, tools and systems. *Journal of Network and Computer Applications*, 40(1): 307-324. Available from: https://www.sciencedirect.com/science/article/pii/S1084804513001756 [Accessed 17 December 2021].

I.T Governance Ltd (2021) Vulnerability scanning: what it is and how it works. Available from: <https://www.itgovernance.co.uk/vulnerability-scanning> [Accessed 18 December 2021].

Jamil, A., Asif, K., Ashraf, R., Mehmood, S., Mustafa, G. (2018) ‘A comprehensive study of cyber attacks &amp; counter measures for web systems’, *2nd International Conference on Future Networks and Distributed Systems* *(ICFNDS)*. New York, 26 June 2018, Association for Computing Machinery. Article 50, 1–7.

Kaur, G., Kaur, N. (2017) Penetration Testing - Reconnaissance with NMAP Tool. *International Journal of Advanced Research in Computer Science.* 8(3): 844-846. Available from: <http://www.ijarcs.info/index.php/Ijarcs/article/view/3111/3094> [Accessed 18 December 2021]

Nmap (N.D.) Service and Version Detection. *Nmap Reference Guide*. Available from: https://nmap.org/book/man-version-detection.html [Accessed 17 December 2021].