Hi Jonathan

Great summary on the use of scanning tools provided.

In addition, “nmap” is a very useful tool to detect loopholes in networks and servers. As you have pointed out this reveals open ports on servers, with this information hackers can easily launch attacks. The most common and simplest of attacks being TCP SYN flooding, ICMP flooding and UDP flooding (Hoque et at., 2014). These attacks are considered to be a form of DOS (Denial of Service) attacks causing servers to become unresponsive and unavailable. 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).

Furthermore from the “nmap” results posted, we can see that FTP (File Transfer Protocol) is open on port 21. FTP is used to transfer files between systems in clear text, when specific commands are used such as “get” and “put”; a data connection is established between the client and the server (Parziale et al., 2006). Since data is sent in clear text, attackers can use various network tools and packet traces such a Wireshark to sniff and gain access to the data (Parziale et al., 2006). FTP is therefore considered to be unsecure and is currently being replaced by SFTP (Secure File Transfer Protocol). In the industry today many companies are making this move mandatory for file transfers between systems. SFTP makes use of TLS (Transport Layer Security) which defines a standard for data encryption between two systems (Parziale et al., 2006).

List of references

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 12 December 2021].

Parziale, L., Britt, D., Davis, C., Forrester, J., Lui, W., Matthews, C. & Rosselot, N. (2006). *TCP/IP Tutorial And Technical Overview.*8th ed. New York, IBM.