Network Security Scanner Nmap

This is a comprehensive activity to test your knowledge about the learning outcomes of this course and to use the knowledge that you have learned to administrate a large network. Specifically, we will use port-scanning techniques to probe devices on the network and to locate services these devices offer. In order to do a simple port scan to determine whether a port is open or closed, we will use numerous Nmap scan types to determine the OS and service fingerprinting of the remote devices. Please follow the steps below.


2. William John Holden’s Pamn IP Scanner app is an unofficial port of Nmap to Android OS. Open the app and use it to scan active IP addresses in your local area network and build an “Internal IP address set.”


4. For each of the IP addresses in your “internal IP address set” and “external IP address set,” use different commands provided by the app to determine the potential OS versions and fingerprints run on that IP address.

5. For each of those same IP addresses, use different commands provided by the app to identify services run on that IP address.

6. Based on the findings in steps 4 and 5, determine which device in your LAN or the external IP address is the most secure and which one is the least secure.

7. Explore all the commands available in the app, and try to draw a topology map of all the devices corresponding to IP addresses in both of your “internet IP address set” and “external IP address set.” In order to compete this part of the assignment, you may need to use the ping and traceroute commands/tools in subunit 6.5.