Ethical Hacker 4 – Network scanning and enumeration

A screenshot of a computer

Description automatically generated

* **Read, show, and explain about the different type of portscanning techniques.**

The terminal has found 37 out of the 256 possible hosts in the 192.168.167/24 network running by using the -sP scanning. It also works for finding my own hosts:

Graphical user interface, text

Description automatically generated

Example of a TCP SYN scan:

Text

Description automatically generated

example of a TCP connect scan:

Text

Description automatically generated

The -sT scan type is for the TCP connection scanning. The server receives SYN from the client to find out if the server is there. After that, the server sends a response containing SYN/ACK to notify the client of its presence. Finally, the client sends ACK to notify that they are ready to establish a communication. Nmap can find out if a port is open or closed by using this 3-way handshake. In the given example, the ports 80 and 443 have been chosen because they are used to deliver http services.

example of a UDP scan:

Text

Description automatically generated

The -sU scan type is for the UDP connection scanning. It sends UDP packet for the targeted port. The port is close if an ICMP (Internet Control Message Protocol) “port unreachable” is returned. Otherwise, the service responds with a UDP packet.

* **Read, show, and explain about** **service scans for enumeration**.

Example of a version detection scan:

Graphical user interface, text

Description automatically generated

The detection command searches through open ports to find useful information about what is currently running and how. This example shows the service and version run on port 80.

* **Read, show, and explain how you can detect the operating system of a system**

**Example of an operating system detection scan:**

Text

Description automatically generated

The OS detection scan is run using the -O flag. Nmap sends multiple TCP and UDP packets to the remote host and examines the responses thoroughly. After multiple tests have been performed, nmap searches through the contents of its database to look for a match.