CYB 552 – TCP PORT SCANNER

1.) A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

a.) Open Ports: Port scanning assists in locating open ports on a computer of interest. Open ports may indicate services that are open to the network and might serve as entry points for attackers. Vulnerability Assessment: Knowing which services operate on open ports allows security professionals to analyze their security and discover potential flaws. Network Mapping: It helps map the network architecture so that managers may comprehend the services that are operating and how they are configured.

b.) The distinction between open and closed ports:   
An open port means that a service is actively listening for connections on that port.   
For example, suppose Port 80 (HTTP) on a web server is open, allowing people to visit the website.   
A closed port means that no service is using it to listen. The server may provide an error message or deny the connection attempt. For instance, the FTP service is unavailable when port 21 (FTP) is closed.

c.) A given IP address and port are attempted to be connected through the socket.connect\_ex() function.   
Return Values: 0 indicates that the port is open if the connection was successful.   
An error code (non-zero) is returned in the event of a failure, signifying that the port is closed or inaccessible.

d.) The sock.A one-second timeout is established for the connection attempt via the settimeout(1) function.   
Relevance:   
Effectiveness: Setting a timeout prevents the application from being idle forever if a port does not respond. As a result, the scanner swiftly go to the next port.