CYB 552 – UDP PORT SCAN

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

a.) It doesn't use a three-way handshake as TCP does. There is no assurance that the target system will react when a UDP packet is transmitted.  
In contrast, TCP port scanning requires a three-way handshake in which the scanner sends a SYN packet and waits for a SYN-ACK response if the port is open. If the port is closed, the target system will send a RST packet, indicating that it is closed.  
The lack of a response in UDP scanning might indicate that the port is either open and the target system opted not to answer, or that the port is being filtered by a firewall. UDP ports are frequently listed as "Open or filtered" when scanned because of this.

b.) When a UDP scan shows "Open or filtered," it indicates that no answer was received. This might indicate that the port is open but silent, or that it has been blocked by a firewall. UDP scans, in contrast to TCP, require specific answers to verify closed ports.

c.) If `sock.settimeout(1)` is set, the UDP scanner will wait for a response in just one second. This avoids waiting endlessly and enables the scanner to quickly forward to the next port in the case that no answer is received.

d.) The scanner waits endlessly for replies in the absence of a timeout, which results in considerable delays on unresponsive ports. Setting a timeout allows the scanner to bypass ports with no responses, resulting in a quicker and more efficient scanning procedure.