Homework 5

Objective:
Answer the following research-based questions with explanations.

1. Explain what port scanning is and why security testers must scan all ports instead of only well-known ports.

2. Choose two different types of port scans (e.g., SYN, Connect, NULL, XMAS, ACK, FIN, UDP). Explain how each scan works and what type of response indicates whether a port is open or closed.

3. Describe one port-scanning/vulnerability scanning tool (such as Nmap, Nessus, OpenVAS, Fping, or Hping3). What is its purpose, and how can scripting be used to make scanning more efficient?