Assignment: 11

Explain and Write a script for the same and attach a screenshot:

1. What is the purpose of the "-sS" flag in Nmap?
2. How does Nmap determine if a port is open, closed, or filtered?
3. What is the difference between TCP SYN scan (-sS) and TCP connect scan (-sT)?
4. How can you specify a range of ports to scan using Nmap?
5. What is the significance of the "-p-" option in Nmap?
6. How does Nmap perform version detection on services running on open ports?
7. What are the common output formats supported by Nmap?
8. How can you use Nmap to perform a ping scan without port scanning?
9. Explain the difference between "Aggressive scan" and "Intense scan" in Nmap.
10. How does Nmap determine the operating system of a target host?
11. How can you specify a list of target hosts in Nmap?
12. Explain the purpose of the "-A" option in Nmap.
13. What is the role of NSE (Nmap Scripting Engine) in Nmap scans?
14. How does Nmap handle scanning IPv6 hosts?
15. What are the differences between TCP, UDP, and SCTP scans in Nmap? Write script also.