Network Scanning Report

Network scanning is a crucial step in assessing the security posture of a network. By systematically scanning for open ports and active services, vulnerabilities can be identified and mitigated, thus enhancing the overall security of the network. In this report, we will analyze the results of different scanning techniques performed on the Metasploitable machine using Nmap, with a focus on TCP and SYN scans on well-known ports, as well as a scan with the "-A" switch.

1. TCP Scan on Well-Known Ports:

- Scan Details:
  - Source: [Your Machine IP]
  - Target: [Metasploitable Machine IP]
  - Type: TCP Scan with `-sS` flag
- Observations from Wireshark Capture:
  - The captured packets indicate that the TCP handshake is not completed.
  - Ports responding with [RST, ACK] packets confirm closed ports with no active services.
- Conclusion:
  - TCP SYN scan efficiently identifies closed ports without completing the full handshake.

2. SYN Scan on Well-Known Ports:

- Scan Details:
  - Source: [Your Machine IP]
  - Target: [Metasploitable Machine IP]
  - Type: SYN Scan with `-sS` flag
- Observations from Wireshark Capture:
  - Similar to the TCP SYN scan, closed ports respond with [RST, ACK] packets.
  - Additional packets following the SYN packet are observed, characteristic of the `-sT` switch.
- Conclusion:
  - The SYN scan provides similar results to the TCP SYN scan but includes additional packets.

3. Scan with "-A" Switch on Well-Known Ports:

- Scan Details:
    - Source: [Your Machine IP]
    - Target: [Metasploitable Machine IP]
    - Type: Scan with `-A` switch
- Observations from Wireshark Capture:
    - More invasive scanning is observed with the `-A` switch.
    - Valuable information such as the target's operating system version and available services on open ports is retrieved.
- Conclusion:
    - Despite being more invasive, the `-A` switch provides valuable insights into the target's system and services.

Overall Conclusion:

- Network scanning plays a critical role in identifying potential security risks and vulnerabilities within a network.
- Understanding the behavior of different scanning techniques helps in effectively assessing and securing the network.
- The results obtained from the scans highlight the importance of thorough network reconnaissance in strengthening network defenses.