Network Scan Report

Scanned Target:Metasploitable (192.168.1.101)

1. OS Fingerprint:
Based on the scan results, the operating system running on the target appears to be Linux (kernel version 2.6.x).

2. SYN Scan:
The SYN scan revealed 977 closed ports on the target system.

3. TCP Connect Scan:
The TCP Connect scan also identified 977 closed ports on the target system.

4. Differences between TCP Connect and SYN Scans:
The SYN scan and TCP Connect scan both aim to identify open ports on the target system, but they use different methods to achieve this:

- SYN Scan: This scan uses the SYN flag in TCP packets to determine if a port is open, closed, or filtered. It sends SYN packets to each port and analyzes the response. If the port is open, it will receive a SYN-ACK response. If the port is closed, it will receive a RST response. If the port is filtered, it may receive no response or an ICMP unreachable message. The SYN scan is faster than the TCP Connect scan because it does not complete the full TCP handshake.

- TCP Connect Scan:This scan completes the full TCP handshake with each port to determine its status. It sends a SYN packet and waits for a SYN-ACK response. If it receives a SYN-ACK, it sends an ACK packet to establish the connection. If it receives a RST packet, it knows the port is closed. The TCP Connect scan is slower than the SYN scan because it completes the full TCP handshake for each port.

In summary, the main difference between the two scans is the method used to determine if a port is open. The SYN scan is faster but less reliable, while the TCP Connect scan is slower but more accurate.

5. Version Detection:

Version detection was performed on the open ports, revealing the following services (refer to previous report for details).

Conclusion:

Overall, the scan results indicate that the target system (Metasploitable) is running Linux with a kernel version of 2.6.x. There are 23 open ports, with various services running including FTP, SSH, Telnet, SMTP, DNS, HTTP, RPC, NetBIOS, SMB, Rexec, Rlogin, RSH, RMI, Shell, NFS, MySQL, PostgreSQL, IRC, AJP, and Apache Tomcat.

The SYN scan and TCP Connect scan were both effective in identifying the open ports on the target system, with no significant differences in the results. However, the SYN scan is generally preferred for its speed and efficiency in scanning large networks.