Port Scanner

Monday, November 18, 2024 2:34 AM

This project is a Python-based custom implementation of a port scanner that replicates some of the functionality of **nmap** using **Scapy**, a powerful library for network packet manipulation. The scanner allows users to specify an IP address or CIDR block (a range of IPs) and scan specific ports to check if they are open. The tool supports three types of scans:

1. **TCP-Ack Scan**: This scan sends TCP packets with the ACK (Acknowledgment) flag set, typically used to determine whether a port is open or filtered (i.e., behind a firewall).
2. **TCP-Syn Scan**: This scan sends TCP packets with the SYN flag set (part of the TCP handshake process). It's often used in stealthy scans to detect open ports without fully completing the handshake.
3. **UDP Scan**: This scan sends UDP packets to a target port. Unlike TCP, UDP is connectionless, so the response is either a packet or no response at all, helping identify open UDP ports.

The script is designed to take input via command-line arguments using the **argparse** library. Users can specify the target (IP or CIDR block), the ports they want to scan, and the type of scan they wish to perform. The application then outputs whether the specified ports are open or closed based on the scan results.

Additionally, an extra feature is included where the port scanner is also implemented using **Python's socket library**, instead of Scapy. This version is a simpler, more basic implementation, which can be run in the same way as the Scapy-based version but without the need for Scapy. This approach gives users an alternative method for port scanning using the standard Python libraries, and it provides a deeper understanding of how port scanning works under the hood.

The tool is useful for network administrators and security professionals performing penetration testing, vulnerability assessments, or just monitoring the availability of certain services on a network. With a flexible command-line interface, the scanner can be adapted for use in a variety of network environments.