Network Scanner: A Python-Based Tool for Network Exploration and Security Assessment

In this age and time when network security is critical, tools…efficiency tools which will aid network exploration and analysis are critical. This project describes a Network Scanner written in Python, which is able to find all the active devices on a network, enumerate the open ports and examine computer configurations on the network. With the extensive library ecosystem of Python, which includes Scapy and threading, the program becomes lightweight while still significant in network exploration. The primary problem addressed by this program is that of network intrusion for the purpose of penetration testing, or alternative, network mapping together with finding out what could be the major ligatures in the network. Usually the tools for analysis of devices, communication systems, networks, and their integrated functions, have a relatively steep learning curve or require a lot of time and resources to grasp. This scanner however, is attractive because it is simple to use and the users are easily guided making it the ideal tool for educational purposes and small portions of security assessments. Some elements of the scanner include the use of ARP in device discovery, Open Port detection via multi-threaded scanning and the introduction of network ranges and ports as parameters of the scan. Python serves as the foundation due to its ease of writing and understanding and other good libraries that facilitate the process of creating programs. Future expansions involve adding a part that uses AI and ML algorithms that will improve the accuracy of analysis, vulnerability prediction and self suggestive mechanisms respectively.