Network Security Protection using Network Profile

Abstract:

today's digital age, securing networks against potential cyber threats has become a top priority for organizations. One effective approach to enhancing network security is through the use of network profiling. A proposed network profile is a set of information that contains details about each user, such as their IP address, MAC address, device vendor, open ports and network latency, etc.

By analyzing this information, security professionals can identify potential security threats and implement preventive measures if an attacker breaches the network. This project examines the concept of network profiles and their use in network security protection.

It also explores the benefits of using a network profile in network security and examines the challenges associated with developing a network profile, such as the need for accurate and comprehensive data collection. In addition, this project emphasizes the importance of regularly maintaining and updating network profiles to accommodate changes in network behavior. Finally, the project presents a case study of a real-world implementation of network profiles in network security protection.

The program works by taking an IP address or network address to scan it and a protocol (ICMP, ARP, TCP, or UDP) and performs a network scan based on the specified protocol. I performed the practical side using Python programing language. The main work is done using Scapy to send packets to the specified IP address and capture the response. then compares the list of detected hosts with a list of known devices, identified by their IP and MAC addresses. Then block any intrusion that is detected.