# Layer 1 - Finding Rogue Devices on a Network using Nmap

## Abstract:

This project dives into the practical use of Nmap, a tool known for its prowess in network scanning, to hunt down unauthorized devices lurking within a network. With Nmap's array of features, including host discovery, service detection, and vulnerability scanning, we demonstrate its critical role in ensuring network security. The research methodically explores how Nmap identifies devices that aren't supposed to be on the network, flags open ports, and spots potential security loopholes. It emphasizes Nmap's flexibility through scripting, enabling tailored scans for more nuanced threats like rogue DHCP servers or devices exploiting UPnP vulnerabilities. The findings underscore Nmap's invaluable contribution to maintaining a secure, intruder-free network environment, spotlighting its efficacy in the continual battle against network intrusions and vulnerabilities. This project not only showcases Nmap's capabilities but also solidifies its position as an indispensable asset in the toolkit of network administrators and cybersecurity professionals.