IT PROJECT
DOCUMENTATION

Local Network Audit with NMAP

MORGAN BURERA

Google IT Support
Professional Certificate

JUNE 2025

Ubuntu, Terminal

Table of Contents

This document is part of a personal project portfolio developed during the Google IT Support Certification. All simulations and analyses were performed in a controlled lab environment. These projects serve as a complement to the course and provide an initial hands-on experience applying its concepts to real-world scenarios

I. Project Overview

The goal of this project is to simulate a real-world scenario where a network administrator or IT support technician needs to map an unfamiliar network environment. Using NMAP, i learned to identify live hosts, detect open ports, determine which services are running on each machine, and gather information about the operating systems in use. This project develops foundational skills in network scanning, subnet analysis, and service enumeration.

II. Environment Setup

Component	Details
OS	Ubuntu 22.04 VMs on VirtualBox
Network Type	NAT or Internal Network (ping works between machines)
Test tools	[ip], [nmap], [arp-scan]
Capture Tools	
Server IP	192.168.56.101
Client IP	192.168.56.102

III. Test Setup and Process

- Get the client VM’s IP address:

```
ip a
```

- Check the default route and gateway:

```
ip route
```

- Test connectivity with the gateway:

```
ping [server IP]
```

- Scan the subnet for active hosts:

```
nmap -sn 192.168.122.0/24
```

- Perform a detailed scan on a detected host:

```
nmap -sV -O [server IP]
```

- Use `arp-scan` for live host discovery:

```
sudo apt install arp-scan sudo arp-scan 192.168.122.0/24
```

4. Capture and Analysis

- List of detected IP addresses
- Hostnames (if resolved)
- Open ports and services running
- OS fingerprinting (if successful)

Key Findings:

- The NMAP scan successfully identified all active machines on the local subnet, revealing their assigned IP addresses and open ports.
- Service enumeration (via **-sV**) provided insights into specific services running on target machines, including version numbers — a critical aspect for vulnerability assessment.
- The OS detection feature (**-O**) offered preliminary fingerprinting data, although accuracy varied depending on host configuration and open ports.
- Combining ip, route, and nmap allowed for a full-layer visibility of the network from layer 2 (MAC/IP associations) to layer 7 (services).
- The exercise emphasized how easily accessible service exposure can be detected by anyone with basic tools, highlighting the importance of port security and firewall configuration.
- It also showed the limitations of unauthenticated scanning in a closed/local network, which might not expose all services depending on system hardening.

V/ Resolution / Outcome

VI/ Key Takeaways & Skills Demonstrated

- Network scanning and auditing with NMAP
- Subnet discovery and basic host identification
- CLI proficiency and terminal output interpretation
- Security mindset in identifying exposed services

VIII/ Optional Enhancements, Reflection

- We obtained 256 hosts after the arp scan, it was done on enp0s3 (café). If it was on enp0s8 we would have obtained 2 hosts, no matter the time we wait for as it's an internal network on my machine with two vms.

- The ssh connection was successfull, even though a part was cut you can see that i deleted the user "morgan" in the video before adding him again. I did it that way because in a real world scenario where i will have to manage users on a daily basis, i cannot possibly find every users in the right groups. So i added him again from the scratch.

Video Recording Link

https://youtu.be/-jx9C8sezVY