Network Scanning and Mapping with Nmap

ATOYEBI BABATUNDE

8/21/2024

TABLE OF CONTENTS

1. Project Overview

1.1 Objective

The objective of this project is to perform a comprehensive network scan using Nmap to identify active hosts, open ports, and services running on the network. This project aims to demonstrate basic network scanning techniques as part of my transition from HR to cybersecurity

1.2 Tools Used

- Nmap Version: 7.94SVN
- Operating System: Kali Linux
- Text Editor for Documentation: Nano

1.3 Scope of Project

- Network Range Scanned: *"192.168.77.0/24"*
- Target: Local Network (Home lab)
- Purpose: To identify devices on the network and gather information on open ports and services

2. Nmap Commands Used

2.1 Explanation of Commands

- ***-sn***: to perform a ping scan on a network so as to list all devices that are up or online on the network range used i.e. 192.168.77.0/24
- ***-sV***: open ports to determine service/version info
- ***-A***: enables OS detection, version detection, script scanning and traceroute
- ***-oN***: saves output in normal format to a file I named "***scan_results_txt***"
- ***192.168.77.128:*** specifies the IP range to scan (home lab)

3. Results

3.1 Summary of Findings

After conducting a preliminary scan on the network (192.168.77.0/24) using ***"nmap –sn"*** the following result was observed:

- IP range scanned is ***192.168.77.0/24***

- A total of 256 host (i.e. 256 IP addresses) on the network was scanned.
- 2 host were detected as "Up" i.e. ***192.168.77.2*** and ***192.168.77.128*** (home lab). **(See Figure 1)**

3.2 Detailed Result

For ethical reason, host ***102.168.77.128 (home lab)*** only was further scanned using ***"nmap (host)"*** for open ports and the following result was observed: **(see Figure 2)**

- Host 192.168.77.128 is reachable, with a very low latency indicating it's likely on a local network or within close proximity.
- All 1000 scanned ports on 192.168.77.128 are in ignored states, this means that Nmap did not find any open ports, and the ports that were scanned are either closed or filtered. In this case, the "conn-refused" indicates that the ports are closed because no services are running on them that would accept connections.
- Nmap scanned 1000 common TCP ports by default. All of these ports were found to be closed, meaning the host is not running any services on these ports, or it is rejecting any connection attempt.

An advanced scan (stealth SYN scan i.e. ***"nmap –sS hostname"*** was carried out to see if certain firewalls can be bypassed to detect open ports and the result received was a lot showing all 1000 ports in ignored state. **(see Figure 3)**

A more rigorous scan using **"nmap –A 192.168.77.0/24"** (which uses a more extensive probing method) displays OS detection, version detection, script scanning and traceroute. A result showed 4 hosts to be "Up" and below are the details: **(see Figure 4)**

I. **Host 192.168.77.1**
- Ports: 902/tcp,912/tcp and 5357/tcp ports are open
- OS detection: detected a possibility of Microsoft Windows XP SP3 (89% certainty)
- Other info: shows MAC address "00:50:56:C0:00:08" (VMware), this suggest it might be a general-purpose device, likely running a Windows XP system within a VMware environment.

II. **Host 192.168.77.2**
- Ports: 53/tcp port "filtered" which means that Nmap was unable to determine whether the port is open or closed because the scan attempts were blocked.
- OS detection: detected as VMware Player virtual NAT device
- Other info: shows MAC Address: 00:50:56:E7:C0:18 (VMware)

III. **Host 192.168.77.254**

- Ports: All 1000 scanned TCP ports were either filtered or ignored.
- OS detection: Too many fingerprints matched, making it difficult to accurately determine the OS.
- Other info: shows MAC Address: 00:50:56:F1:3F:A8 (VMware)

IV. **Host 192.168.77.128**

- Ports: All 1000 scanned TCP ports were closed (connection refused).
- OS detection: Too many fingerprints matched, making OS identification unreliable.
- Other info: Host is up with a latency of 0.00012s

4. Analysis

4.1 Interpretation of Result

- The network scan revealed four active hosts, with varying levels of open ports and services. The presence of VMware services indicates virtualized environments, likely part of a home lab setup.
- Security Implications: The open ports detected, especially those related to VMware, could be potential entry points for attackers if not secured properly. It's important to review the security settings on these devices.

4.2 Recommendations

- **Secure Open Ports:** Close unnecessary open ports, especially those related to VMware.
- **Implement Firewalls:** Ensure that firewall rules are properly configured to limit exposure.

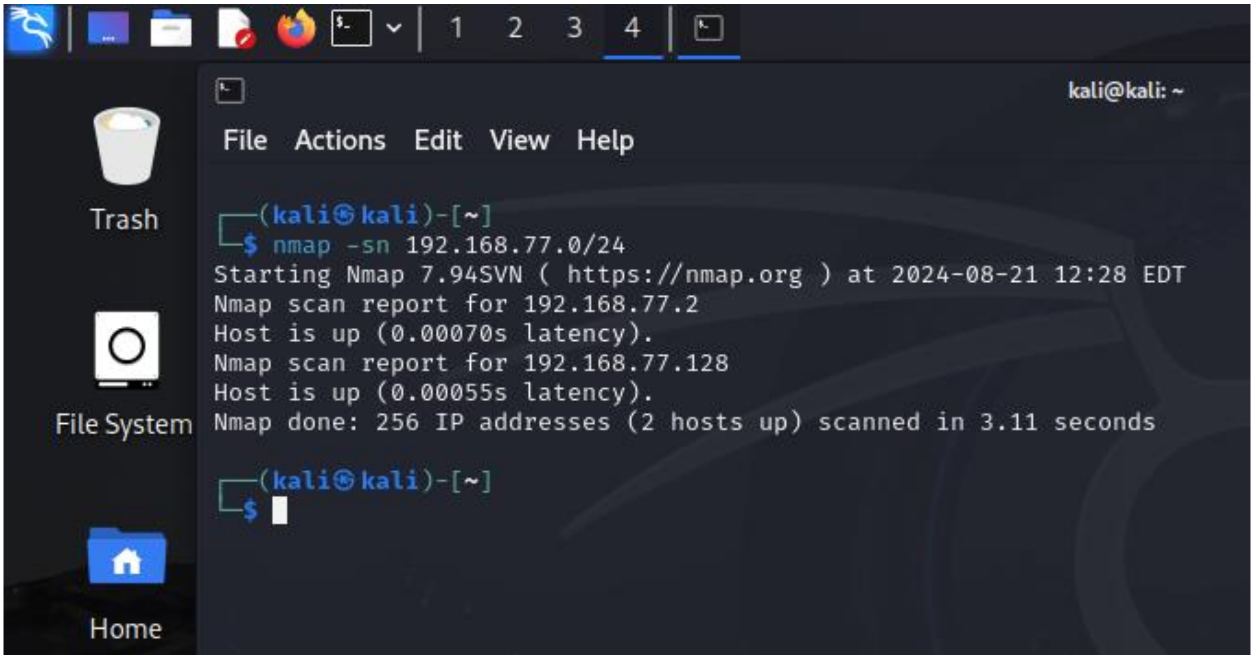
5. Conclusion

This project successfully demonstrated the use of Nmap for network scanning and mapping. The results provided valuable insights into the network's structure, identifying active hosts and the services they offer. This project serves as a foundational step in my cybersecurity learning journey.

6. Appendices

6.1 Screenshots

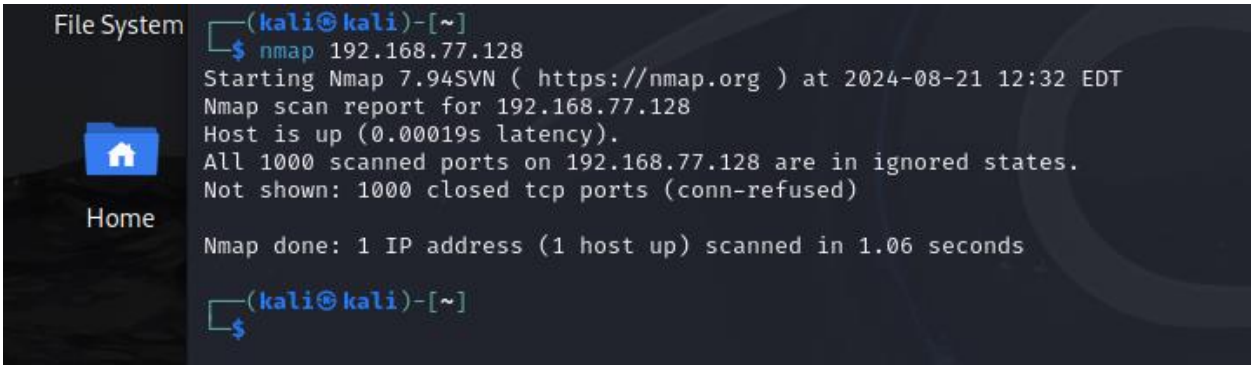
Figure 1 – “Nmap –sn” command output to scan network



```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.77.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-21 12:28 EDT
Nmap scan report for 192.168.77.2
Host is up (0.00070s latency).
Nmap scan report for 192.168.77.128
Host is up (0.00055s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 3.11 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Figure 2 – “Nmap” command to scan for open ports.

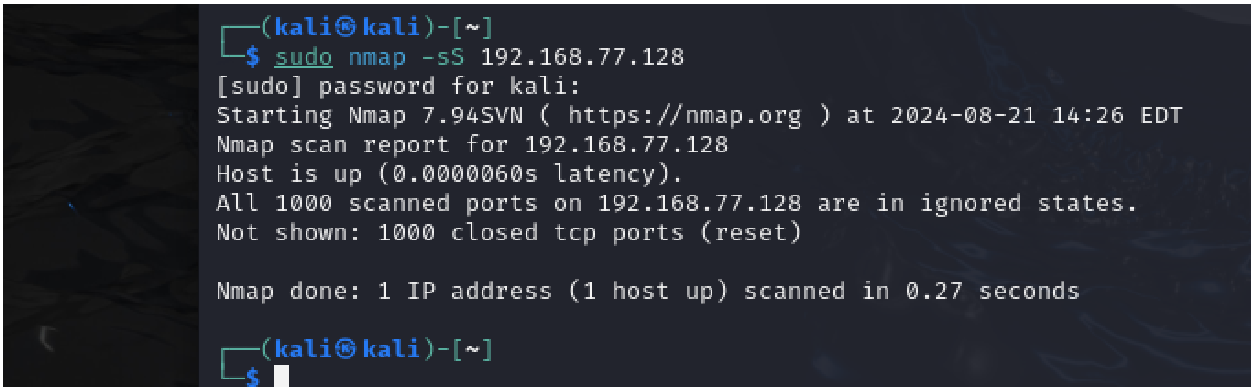


```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.77.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-21 12:32 EDT
Nmap scan report for 192.168.77.128
Host is up (0.00019s latency).
All 1000 scanned ports on 192.168.77.128 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 1.06 seconds

┌──(kali㉿kali)-[~]
└─$
```

Figure 3 – “Nmap –sS “ command to perform stealth SYN scan to further check for open ports which might be protected with firewalls



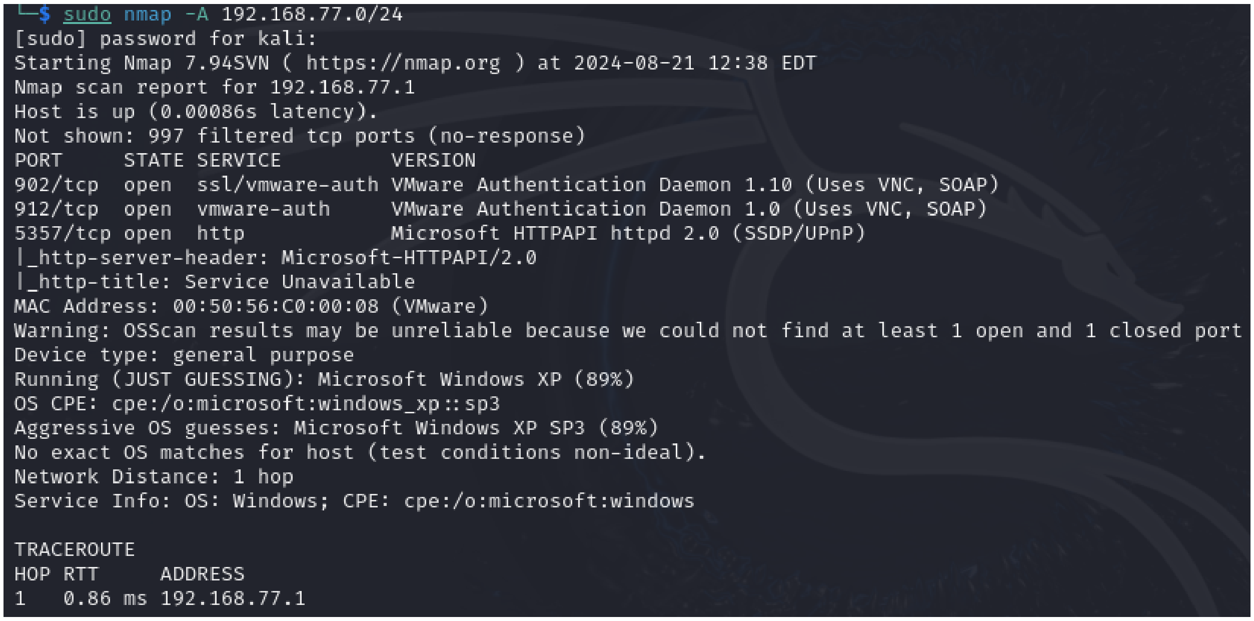
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.77.128
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-21 14:26 EDT
Nmap scan report for 192.168.77.128
Host is up (0.0000060s latency).
All 1000 scanned ports on 192.168.77.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Figure 4 (a – d)

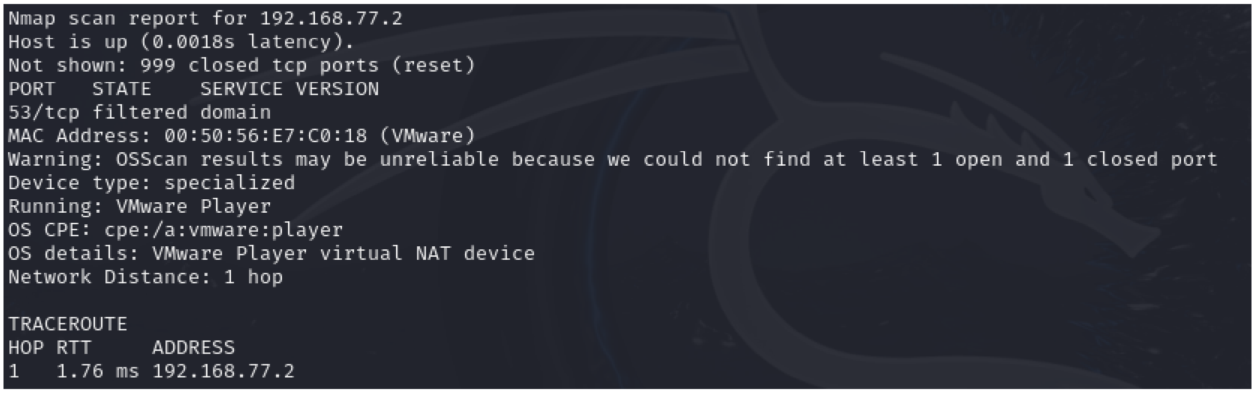
a) “nmap –A” command output for host 192.168.77.1



```
└─$ sudo nmap -A 192.168.77.0/24
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-21 12:38 EDT
Nmap scan report for 192.168.77.1
Host is up (0.00086s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE         VERSION
902/tcp  open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp  open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
5357/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
MAC Address: 00:50:56:C0:00:08 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows XP SP3 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT     ADDRESS
1   0.86 ms 192.168.77.1
```

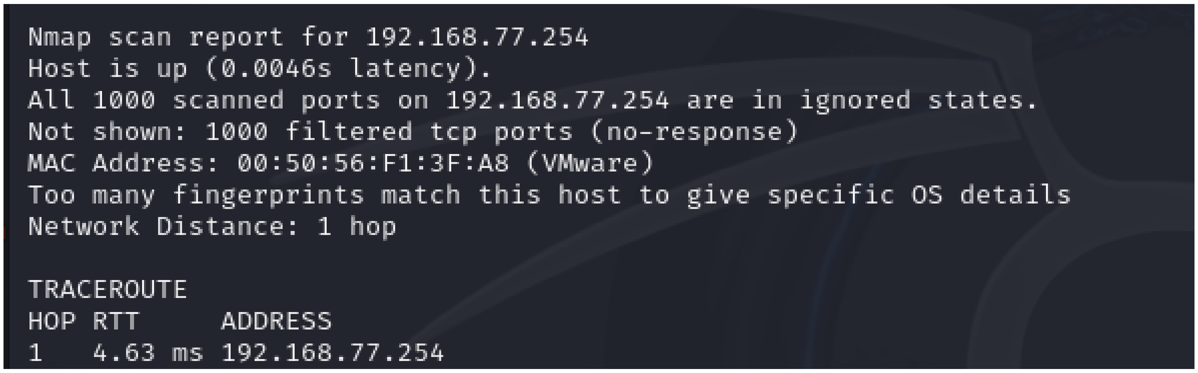
b) “nmap –A” command output for host 192.168.77.2



```
Nmap scan report for 192.168.77.2
Host is up (0.0018s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE    SERVICE VERSION
53/tcp filtered domain
MAC Address: 00:50:56:E7:C0:18 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized
Running: VMware Player
OS CPE: cpe:/a:vmware:player
OS details: VMware Player virtual NAT device
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   1.76 ms 192.168.77.2
```

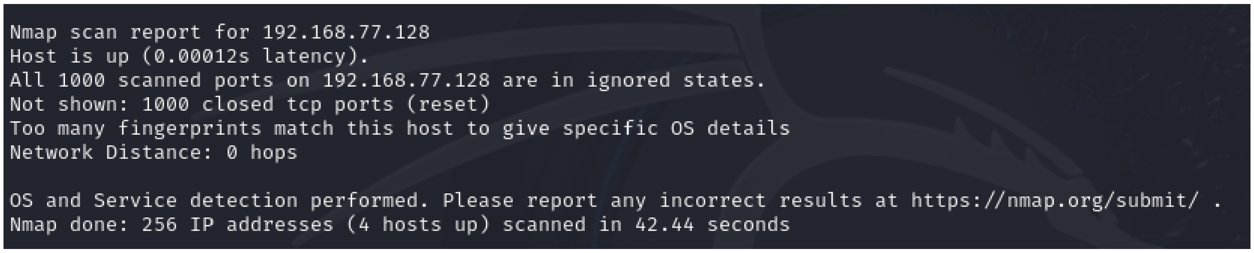
c) “nmap –A” command output for host 192.168.77.254



```
Nmap scan report for 192.168.77.254
Host is up (0.0046s latency).
All 1000 scanned ports on 192.168.77.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F1:3F:A8 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   4.63 ms 192.168.77.254
```

d) “nmap –A” command output for host 192.168.77.128



```
Nmap scan report for 192.168.77.128
Host is up (0.00012s latency).
All 1000 scanned ports on 192.168.77.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 42.44 seconds
```