LOVELY PROFESSIONAL UNIVERSITY

Transforming Education Transforming India

Assignment submitted by

Asifuzzaman Asif

Reg: 11900157

Roll: 38

Section: KE057

Subject: INT301

Assignment submitted to

Navjot Kaur

GitHub Link: https://github.com/Asif734/Open_Source

Question Number Allocated: 7

Question: Suppose you are an ethical hacker and you are asked to perform a scan on your simulated network. Your task is to identify a) live hosts, b) services running on live hosts, c) banner grabbing d) OS fingerprinting d) conducting performance scans based on your current network bandwidth. Use any open-source software to generate a report on the same.

1.Introduction

To perform the assigned task **Network Mapper (NMAP)** is used. Nmap is an open-source software which is available for all the operating system. It is used for network exploration, management, and security auditing. It is very easy to use, support a wide range of features and scanning techniques. Nmap can be used to scan and map networks, identify hosts and services, perform OS detection and version fingerprinting, and detect vulnerabilities and security issues. It supports a wide range of scanning techniques, including ping scanning, port scanning, version detection, and service enumeration.

Nmap can be run from the command line or through a graphical user interface, and supports a variety of output formats, including text, XML, grapable file.

1.1 Objective

The objective of detecting live host, banner grabbing, OS fingerprinting, services running on live host, and performance scan on a network is to gather information about the network and its hosts. This information can be used to assess the security of the network and identify any vulnerabilities that may exist.

1. Detecting live hosts is the first step in understanding the network's topology and identifying potential targets for attacks or vulnerabilities that need to be addressed.
2. Identifying the services running on a live host can help in identifying any vulnerabilities that may be present in those services. This can help in prioritizing patching and other remediation efforts.
3. Banner grabbing involves collecting information about the software and services running on the hosts, which can be used to identify specific vulnerabilities or attack vectors.
4. OS fingerprinting is the process of identifying the operating system running on a particular host. This information can be useful in determining which vulnerabilities may be present on the host, as well as which exploits may be effective against it.
5. Finally, performance scans can be used to identify any performance issues on the network. This can include issues such as slow response times, high latency, or packet loss, which can be indicative of underlying network issues that need to be addressed.

Overall, the objective of these activities is to gather information about the network and its hosts so that any potential vulnerabilities can be identified and addressed before they can be exploited by attackers.

1.2 Description of the project

In this project, we are asked to detect live host, services on host, banner grabbing, os fingerprint and perform performance scan.

Live host detection is the process of determining whether a particular host is active and responding to network traffic. The goal of live host detection is to identify hosts that are currently connected to the network and reachable, as well as to identify any potential issues that may be preventing communication with the host. Common method of live host detection is using ICMP and TCP.Services on a live host refer to the software applications or programs running on that host that provide a specific functionality or service. Examples of services that may run on a live host include web servers, email servers, file transfer protocol (FTP) servers, domain name system (DNS) servers, and database servers, among others.Banner grabbing is a technique used to gather information about the software and services running on a remote host by capturing the response banners sent by those services.OS fingerprinting is a technique used to identify the operating system running on a remote host. It involves analyzing the responses to various probes sent to the host to determine the unique characteristics of the operating system.A performance scan on a network is a type of network scan that is focused on measuring and analyzing the performance characteristics of the network. The goal of a performance scan is to identify bottlenecks, errors, and other issues that may be affecting the performance of the network, and to provide insights that can be used to optimize the network's performance. There is various method of doing performance scan on network.

1.3 Scope of the project

The scope of detecting live host, services, banner grabbing, OS fingerprint, and performance scan on a network can vary depending on the specific goals and requirements of the network administrator or security professional.

- At a high level, the scope of these activities typically involves identifying and analyzing the various components of the network, including the hosts, services, and operating systems that are running on the network. This information can be used to identify potential vulnerabilities, security risks, and performance issues that may be present on the network.

- The scope of detecting live hosts involves scanning the network to identify the IP addresses and devices that are active and connected to the network. This can include identifying hosts that are online and available for communication, as well as identifying hosts that may be offline or inaccessible.
- The scope of services detection involves identifying the software and applications that are running on each of the live hosts that have been identified. This can include identifying the specific services that are running, as well as identifying the ports and protocols that are being used to communicate with these services.
- Banner grabbing and OS fingerprinting involve identifying specific characteristics of the services and operating systems that are running on the live hosts. Banner grabbing involves analyzing the response banners sent by the services to identify software and version numbers, while OS fingerprinting involves analyzing the responses to various probes to identify unique characteristics of the operating system.
- Finally, the scope of performance scanning involves analyzing the performance characteristics of the network to identify any issues or bottlenecks that may be affecting network performance. This can include measuring metrics such as bandwidth utilization, latency, packet loss, and throughput to identify potential issues and provide insights that can be used to optimize network performance.
- Overall, the scope of detecting live hosts, services, banner grabbing, OS fingerprint, and performance scan on a network is broad and can vary depending on the specific goals and requirements of the network administrator or security professional. These activities are all important components of network security and can help to identify potential vulnerabilities and optimize network performance.

2. System Description

2.1 Target system description

In this project, I have taken my LAN network as my target system. LAN stands for Local Area Network. It’s a network where a group of two or more computer or devices are connected. I have taken Home WIFI network as target system. This router provides high-speed, secure, and convenient wireless network access. It supports 802.11n (2.4 GHz), 802.11b, and 802.11g. It can implement the network access at a high speed by using a powerful external antenna.

It's ip address is: **192.168.18.1**

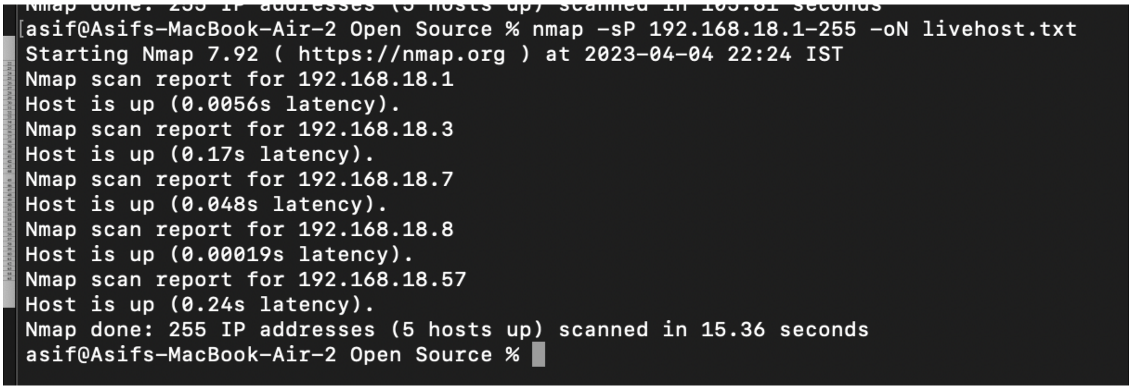
I have performed network scan for the computer or devices connected to this network.

3. Analysis Report

Here, I have asked to perform the following operations to a simulated network such as live host detection, services running on live host, banner grabbing, os fingerprint and performance scan. I have performed those operation to all the devices which is connected to my local area network.

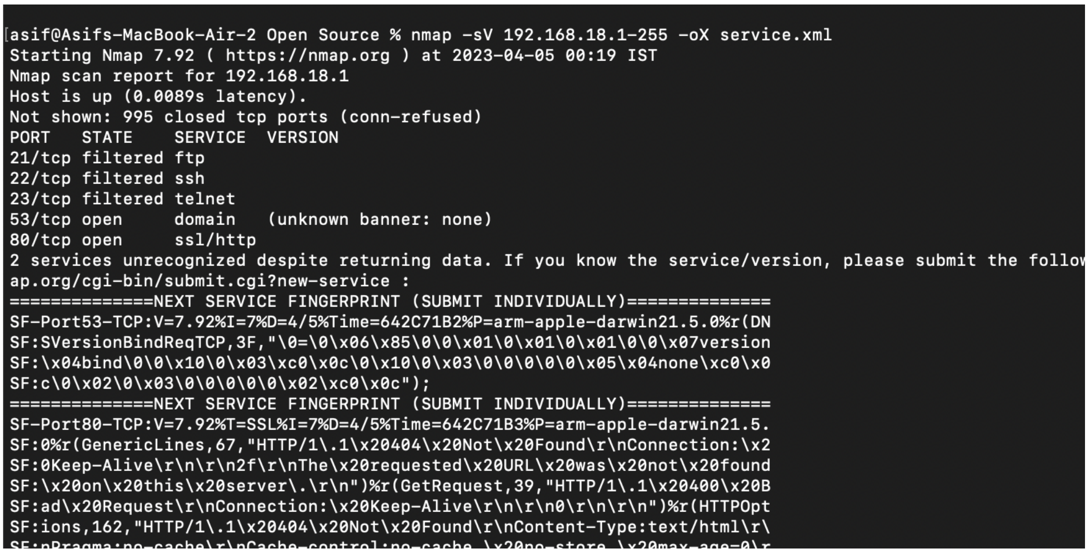
To do all the operations I have taken NMAP which is open source and easy to use and it is capable of generating report for the same. For generating report, nmap is capable of txt, xml and grepable format. Though we can read xml file, we can use other open source software to make xml file to html file which is xsltproc.

a. **Live host:** To detect live host we can use "**nmap -sP <ip address>**" where -sP will ping the network which is up and for generating report we need to add "-oN file.txt" for text file. It is human readable file. Here I have scanned all the ip address that are connected to my network.



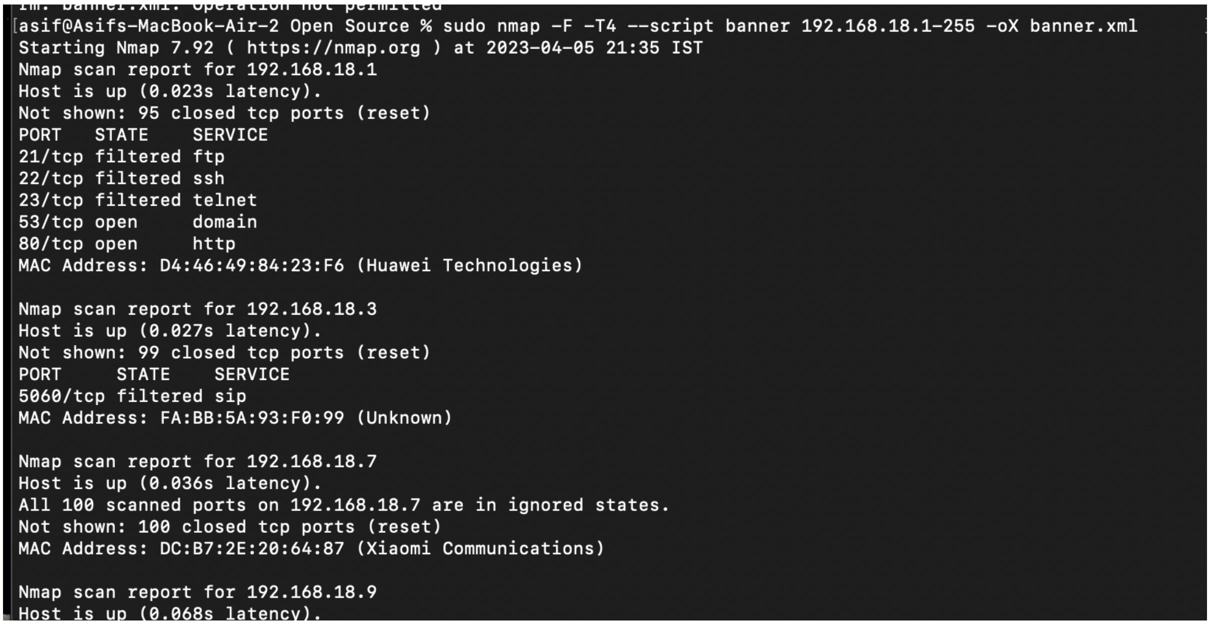
```
Nmap done: 255 IP addresses (5 hosts up) scanned in 105.81 seconds
[asif@Asifs-MacBook-Air-2 Open Source % nmap -sP 192.168.18.1-255 -oN livehost.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-04 22:24 IST
Nmap scan report for 192.168.18.1
Host is up (0.0056s latency).
Nmap scan report for 192.168.18.3
Host is up (0.17s latency).
Nmap scan report for 192.168.18.7
Host is up (0.048s latency).
Nmap scan report for 192.168.18.8
Host is up (0.00019s latency).
Nmap scan report for 192.168.18.57
Host is up (0.24s latency).
Nmap done: 255 IP addresses (5 hosts up) scanned in 15.36 seconds
asif@Asifs-MacBook-Air-2 Open Source %
```

b. **Service detection:** To detect the services running on my network, "**nmap -sV <ip address> -oX filename.xml**" command is used. Here -sV is for searching the services that are using by the devices connected to the network.



```
[asif@Asifs-MacBook-Air-2 Open Source % nmap -sV 192.168.18.1-255 -oX service.xml
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-05 00:19 IST
Nmap scan report for 192.168.18.1
Host is up (0.0089s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT   STATE    SERVICE  VERSION
21/tcp filtered ftp
22/tcp filtered ssh
23/tcp filtered telnet
53/tcp open     domain   (unknown banner: none)
80/tcp open     ssl/http
2 services unrecognized despite returning data. If you know the service/version, please submit the follow
ap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port53-TCP:V=7.92%I=7%D=4/5%Time=642C71B2%P=arm-apple-darwin21.5.0%r(DN
SF:SVersionBindReqTCP,3F,"\0=\0\x06\x85\0\0\x01\0\x01\0\x01\0\0\x07version
SF:\x04bind\0\0\x10\0\x03\xc0\x0c\0\x10\0\x03\0\0\0\0\0\x05\x04none\xc0\x0
SF:c\0\x02\0\x03\0\0\0\0\0\x02\xc0\x0c");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.92%T=SSL%I=7%D=4/5%Time=642C71B3%P=arm-apple-darwin21.5.
SF:0%r(GenericLines,67,"HTTP/1\.1\x20404\x20Not\x20Found\r\nConnection:\x2
SF:0Keep-Alive\r\n\r\n2f\r\nThe\x20requested\x20URL\x20was\x20not\x20found
SF:\x20on\x20this\x20server\.\r\n")%r(GetRequest,39,"HTTP/1\.1\x20400\x20B
SF:ad\x20Request\r\nConnection:\x20Keep-Alive\r\n\r\n0\r\n\r\n")%r(HTTPOpt
SF:ions,162,"HTTP/1\.1\x20404\x20Not\x20Found\r\nContent-Type:text/html\r\
SF:nPragma:no-cache\r\nCache-control:no-cache,\x20no-store,\x20max-age=0\r
```

c. **Banner grabbing:** To retrieve information about a network banner grabbing is used. "**nmap -F -T4 –script banner <ip address> -oX file.xml**". Here we can also perform the port scanning by adding "-p22,80" like this. where -F is for fast scanning –T4 is for defining the speed.



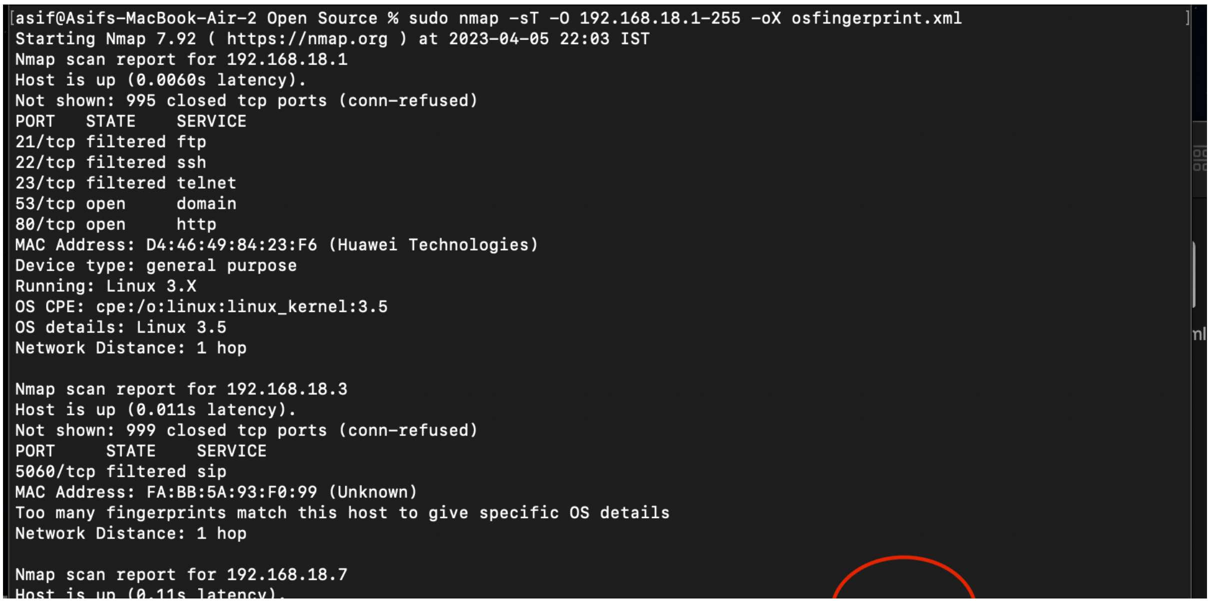
```
rm: banner.xml: Operation not permitted
[asif@Asifs-MacBook-Air-2 Open Source % sudo nmap -F -T4 --script banner 192.168.18.1-255 -oX banner.xml
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-05 21:35 IST
Nmap scan report for 192.168.18.1
Host is up (0.023s latency).
Not shown: 95 closed tcp ports (reset)
PORT   STATE    SERVICE
21/tcp filtered ftp
22/tcp filtered ssh
23/tcp filtered telnet
53/tcp open     domain
80/tcp open     http
MAC Address: D4:46:49:84:23:F6 (Huawei Technologies)

Nmap scan report for 192.168.18.3
Host is up (0.027s latency).
Not shown: 99 closed tcp ports (reset)
PORT     STATE    SERVICE
5060/tcp filtered sip
MAC Address: FA:BB:5A:93:F0:99 (Unknown)

Nmap scan report for 192.168.18.7
Host is up (0.036s latency).
All 100 scanned ports on 192.168.18.7 are in ignored states.
Not shown: 100 closed tcp ports (reset)
MAC Address: DC:B7:2E:20:64:87 (Xiaomi Communications)

Nmap scan report for 192.168.18.9
Host is up (0.068s latency).
```

d. **OS Fingerprint:** "**nmap -O <ip address> -oX file.xml**" where -O for detecting the operating system that are using my network.



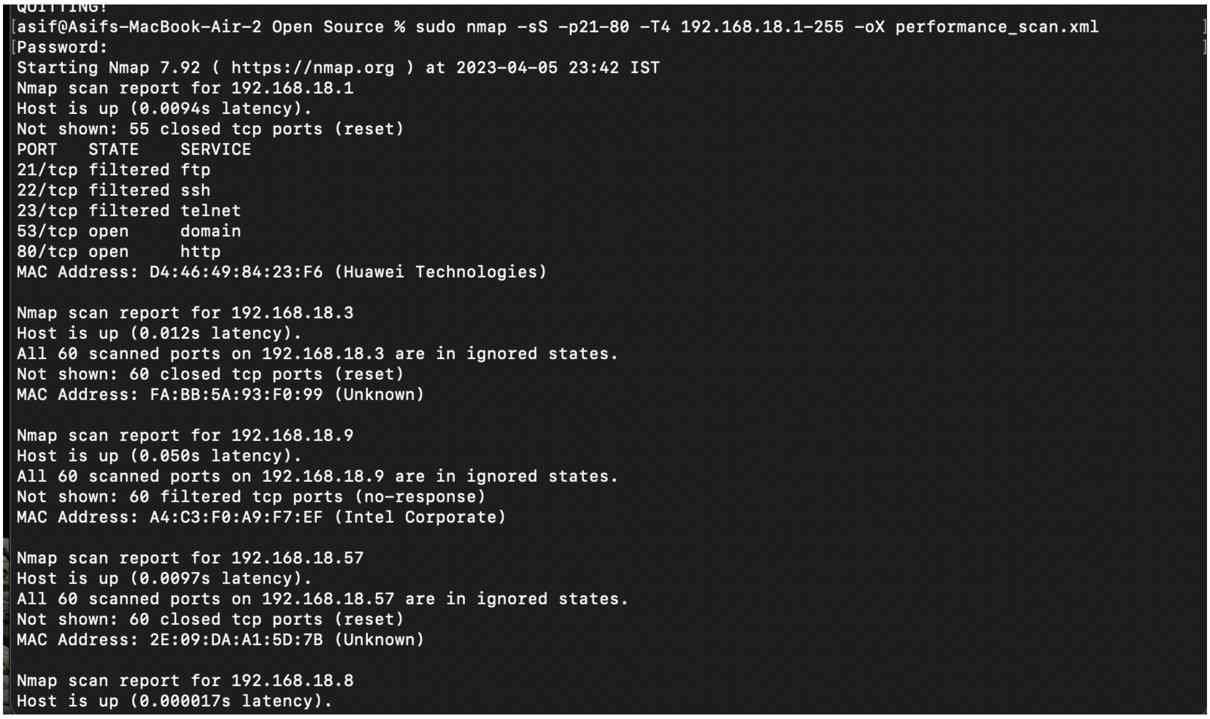
```
[asif@Asifs-MacBook-Air-2 Open Source % sudo nmap -sT -O 192.168.18.1-255 -oX osfingerprint.xml
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-05 22:03 IST
Nmap scan report for 192.168.18.1
Host is up (0.0060s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT   STATE    SERVICE
21/tcp filtered ftp
22/tcp filtered ssh
23/tcp filtered telnet
53/tcp open     domain
80/tcp open     http
MAC Address: D4:46:49:84:23:F6 (Huawei Technologies)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3.5
OS details: Linux 3.5
Network Distance: 1 hop

Nmap scan report for 192.168.18.3
Host is up (0.011s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT     STATE    SERVICE
5060/tcp filtered sip
MAC Address: FA:BB:5A:93:F0:99 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.18.7
Host is up (0.11s latency).
```

e. **Performance scan:** Various method is used for performance scanning in the network. In this project I have used 2 techniques, one is port scanning with timing templates and other one is sending packet rate to the target network.

- **"nmap -sS -p21-80 -T4 <ip address>"**
- **"nmap -sT –min-rate/max-rate 2/….20/.. <ip address"**



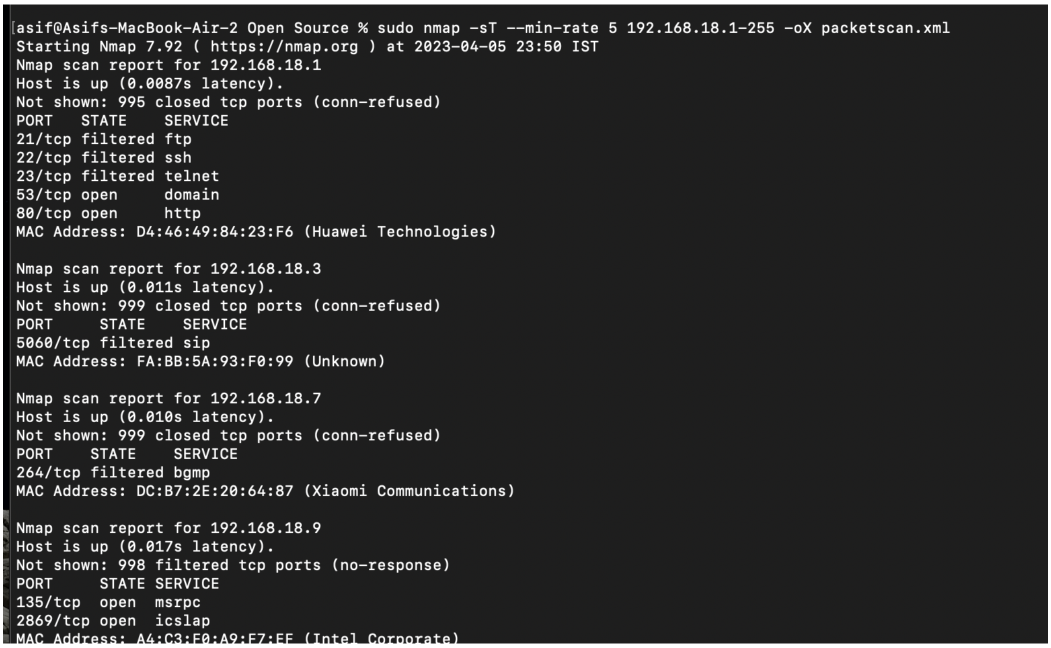
```
QUITTING!
[asif@Asifs-MacBook-Air-2 Open Source % sudo nmap -sS -p21-80 -T4 192.168.18.1-255 -oX performance_scan.xml
[Password:
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-05 23:42 IST
Nmap scan report for 192.168.18.1
Host is up (0.0094s latency).
Not shown: 55 closed tcp ports (reset)
PORT   STATE    SERVICE
21/tcp filtered ftp
22/tcp filtered ssh
23/tcp filtered telnet
53/tcp open     domain
80/tcp open     http
MAC Address: D4:46:49:84:23:F6 (Huawei Technologies)

Nmap scan report for 192.168.18.3
Host is up (0.012s latency).
All 60 scanned ports on 192.168.18.3 are in ignored states.
Not shown: 60 closed tcp ports (reset)
MAC Address: FA:BB:5A:93:F0:99 (Unknown)

Nmap scan report for 192.168.18.9
Host is up (0.050s latency).
All 60 scanned ports on 192.168.18.9 are in ignored states.
Not shown: 60 filtered tcp ports (no-response)
MAC Address: A4:C3:F0:A9:F7:EF (Intel Corporate)

Nmap scan report for 192.168.18.57
Host is up (0.0097s latency).
All 60 scanned ports on 192.168.18.57 are in ignored states.
Not shown: 60 closed tcp ports (reset)
MAC Address: 2E:09:DA:A1:5D:7B (Unknown)

Nmap scan report for 192.168.18.8
Host is up (0.000017s latency).
```



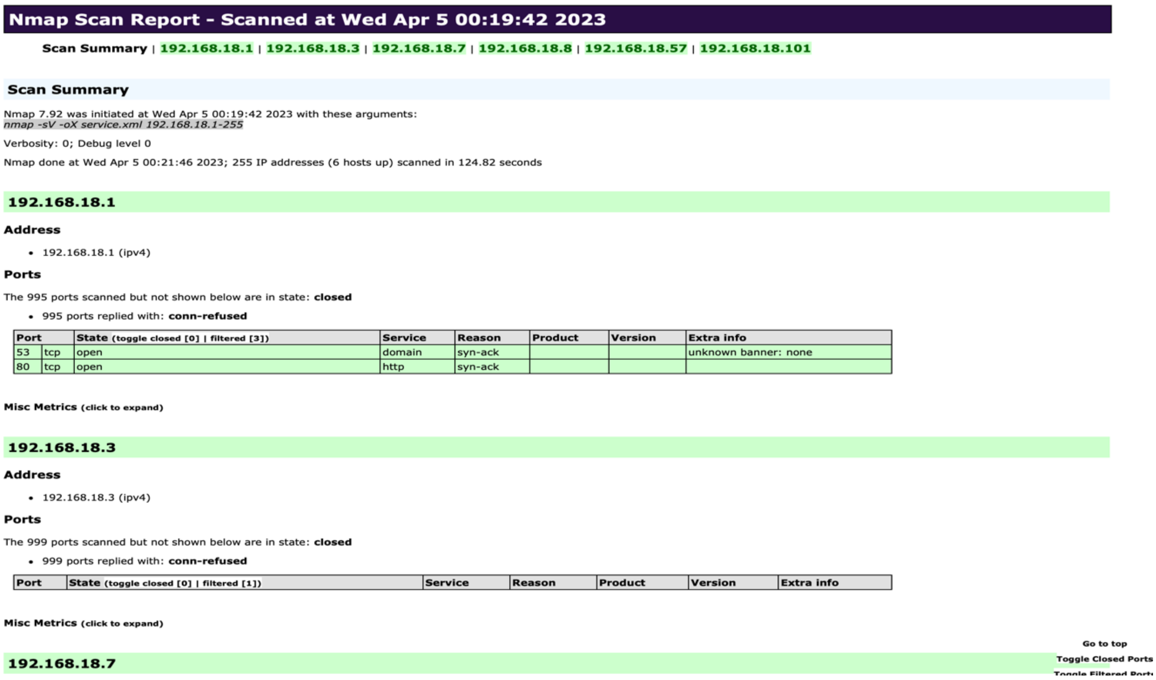
```
asif@Asifs-MacBook-Air-2 Open Source % sudo nmap -sT --min-rate 5 192.168.18.1-255 -oX packetscan.xml
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-05 23:50 IST
Nmap scan report for 192.168.18.1
Host is up (0.0087s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT   STATE    SERVICE
21/tcp filtered ftp
22/tcp filtered ssh
23/tcp filtered telnet
53/tcp open     domain
80/tcp open     http
MAC Address: D4:46:49:84:23:F6 (Huawei Technologies)

Nmap scan report for 192.168.18.3
Host is up (0.011s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT     STATE    SERVICE
5060/tcp filtered sip
MAC Address: FA:BB:5A:93:F0:99 (Unknown)

Nmap scan report for 192.168.18.7
Host is up (0.010s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT    STATE    SERVICE
264/tcp filtered bgmp
MAC Address: DC:B7:2E:20:64:87 (Xiaomi Communications)

Nmap scan report for 192.168.18.9
Host is up (0.017s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
2869/tcp open  icslap
MAC Address: A4:C3:F0:A9:F7:EE (Intel Corporate)
```

- To convert xml file to hmtl format is: “**xsltproc file.xml -o file.html**”



Nmap Scan Report - Scanned at Wed Apr 5 00:19:42 2023

Scan Summary | 192.168.18.1 | 192.168.18.3 | 192.168.18.7 | 192.168.18.8 | 192.168.18.57 | 192.168.18.101

Scan Summary

Nmap 7.92 was initiated at Wed Apr 5 00:19:42 2023 with these arguments:
nmap -sV -oX service.xml 192.168.18.1-255

Verbosity: 0; Debug level 0

Nmap done at Wed Apr 5 00:21:46 2023; 255 IP addresses (6 hosts up) scanned in 124.82 seconds

192.168.18.1

Address

- 192.168.18.1 (ipv4)

Ports

The 995 ports scanned but not shown below are in state: **closed**

- 995 ports replied with: **conn-refused**

Port		State (toggle closed [0] | filtered [3])	Service	Reason	Product	Version	Extra info
53	tcp	open	domain	syn-ack			unknown banner: none
80	tcp	open	http	syn-ack			

Misc Metrics (click to expand)

192.168.18.3

Address

- 192.168.18.3 (ipv4)

Ports

The 999 ports scanned but not shown below are in state: **closed**

- 999 ports replied with: **conn-refused**

Port	State (toggle closed [0] | filtered [1])	Service	Reason	Product	Version	Extra info

Misc Metrics (click to expand)

192.168.18.7

4. References

- Nmap documentation “https://nmap.org/”
- Nmap help “nmap –help”