# NMAP Lab

991451344

Professor: Sebastian Maniak

Timothy Pang

# Introduction

In this lab, we are tasked with using nmap to identify target machines by sweeping through a network range, to specify port ranges in nmap and analyze the nmap-services file to determine more popular ports as well as to conduct TCP port scanning and analyze the difference between the two.

# Initial Scan

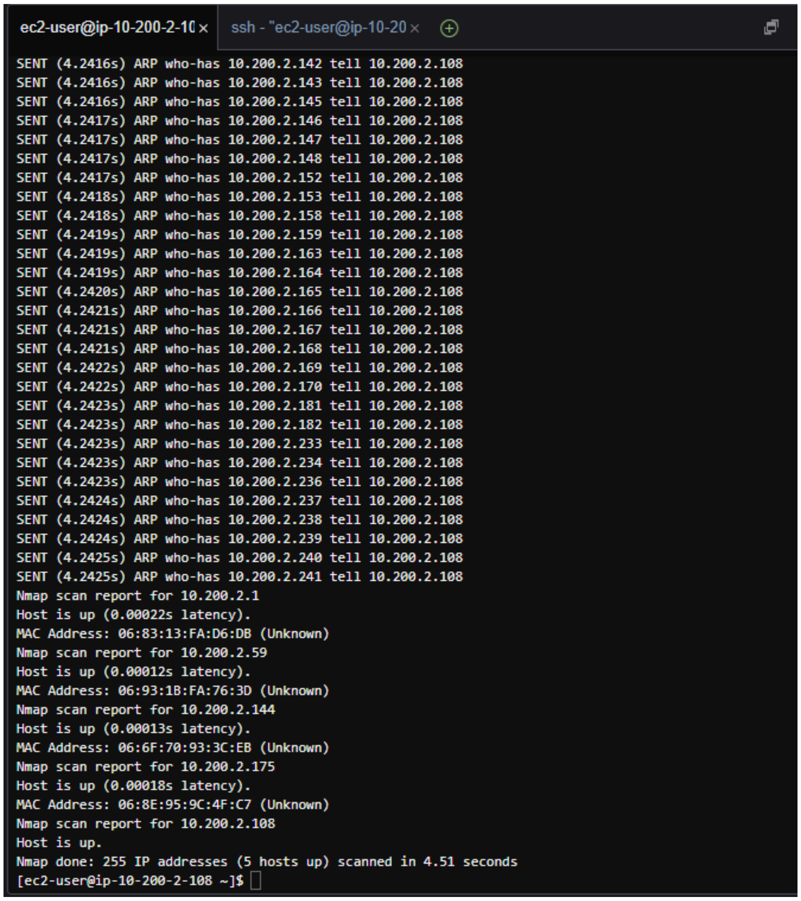
## What does -n do? :

According to the options summary, -n means never do DNS resolution.

## What does -sP do? :

Looking at the output without -sP, -sP is for condensing the packet trace information to each ip from 1 – 255, as well as it shows the host information for the networks that are up.

## How many hosts do you see online? :



```
SENT (4.2416s) ARP who-has 10.200.2.142 tell 10.200.2.108
SENT (4.2416s) ARP who-has 10.200.2.143 tell 10.200.2.108
SENT (4.2416s) ARP who-has 10.200.2.145 tell 10.200.2.108
SENT (4.2417s) ARP who-has 10.200.2.146 tell 10.200.2.108
SENT (4.2417s) ARP who-has 10.200.2.147 tell 10.200.2.108
SENT (4.2417s) ARP who-has 10.200.2.148 tell 10.200.2.108
SENT (4.2417s) ARP who-has 10.200.2.152 tell 10.200.2.108
SENT (4.2418s) ARP who-has 10.200.2.153 tell 10.200.2.108
SENT (4.2418s) ARP who-has 10.200.2.158 tell 10.200.2.108
SENT (4.2419s) ARP who-has 10.200.2.159 tell 10.200.2.108
SENT (4.2419s) ARP who-has 10.200.2.163 tell 10.200.2.108
SENT (4.2419s) ARP who-has 10.200.2.164 tell 10.200.2.108
SENT (4.2420s) ARP who-has 10.200.2.165 tell 10.200.2.108
SENT (4.2421s) ARP who-has 10.200.2.166 tell 10.200.2.108
SENT (4.2421s) ARP who-has 10.200.2.167 tell 10.200.2.108
SENT (4.2421s) ARP who-has 10.200.2.168 tell 10.200.2.108
SENT (4.2422s) ARP who-has 10.200.2.169 tell 10.200.2.108
SENT (4.2422s) ARP who-has 10.200.2.170 tell 10.200.2.108
SENT (4.2423s) ARP who-has 10.200.2.181 tell 10.200.2.108
SENT (4.2423s) ARP who-has 10.200.2.182 tell 10.200.2.108
SENT (4.2423s) ARP who-has 10.200.2.233 tell 10.200.2.108
SENT (4.2423s) ARP who-has 10.200.2.234 tell 10.200.2.108
SENT (4.2423s) ARP who-has 10.200.2.236 tell 10.200.2.108
SENT (4.2424s) ARP who-has 10.200.2.237 tell 10.200.2.108
SENT (4.2424s) ARP who-has 10.200.2.238 tell 10.200.2.108
SENT (4.2424s) ARP who-has 10.200.2.239 tell 10.200.2.108
SENT (4.2425s) ARP who-has 10.200.2.240 tell 10.200.2.108
SENT (4.2425s) ARP who-has 10.200.2.241 tell 10.200.2.108
Nmap scan report for 10.200.2.1
Host is up (0.00022s latency).
MAC Address: 06:83:13:FA:D6:DB (Unknown)
Nmap scan report for 10.200.2.59
Host is up (0.00012s latency).
MAC Address: 06:93:1B:FA:76:3D (Unknown)
Nmap scan report for 10.200.2.144
Host is up (0.00013s latency).
MAC Address: 06:6F:70:93:3C:EB (Unknown)
Nmap scan report for 10.200.2.175
Host is up (0.00018s latency).
MAC Address: 06:8E:95:9C:4F:C7 (Unknown)
Nmap scan report for 10.200.2.108
Host is up.
Nmap done: 255 IP addresses (5 hosts up) scanned in 4.51 seconds
[ec2-user@ip-10-200-2-108 ~]$
```

Figure 1.

There are a total of 5 hosts online.

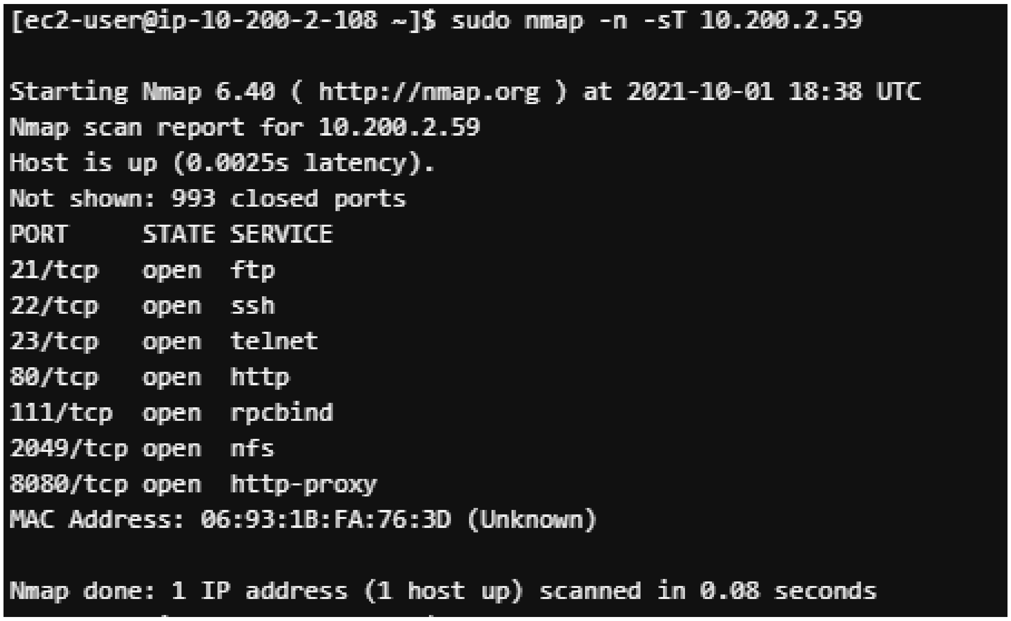
## Scanning Linux (Vulnerable host)

### How long did the scan take? :

The scan took 0.08 seconds.

### What ports did you discover? :

Discovered ports 21,22,23,80,111,2049 and 8080.

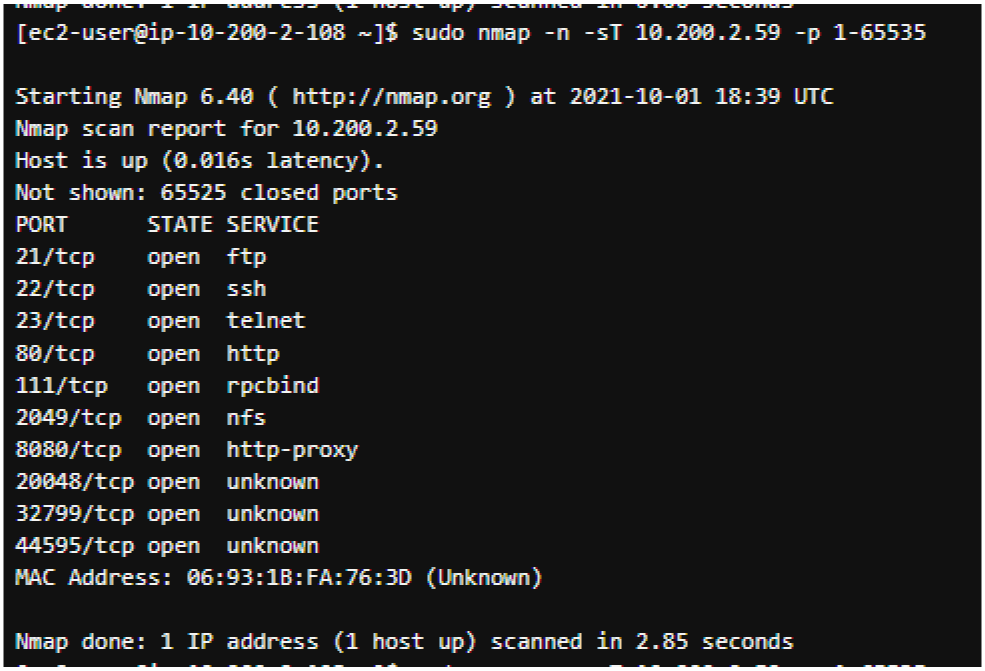


```
[ec2-user@ip-10-200-2-108 ~]$ sudo nmap -n -sT 10.200.2.59

Starting Nmap 6.40 ( http://nmap.org ) at 2021-10-01 18:38 UTC
Nmap scan report for 10.200.2.59
Host is up (0.0025s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
80/tcp   open  http
111/tcp  open  rpcbind
2049/tcp open  nfs
8080/tcp open  http-proxy
MAC Address: 06:93:1B:FA:76:3D (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

Figure 2.

## What ports/services have you discovered? :

Running sudo nmap -n -sT 10.200.2.59 -p 1-65535



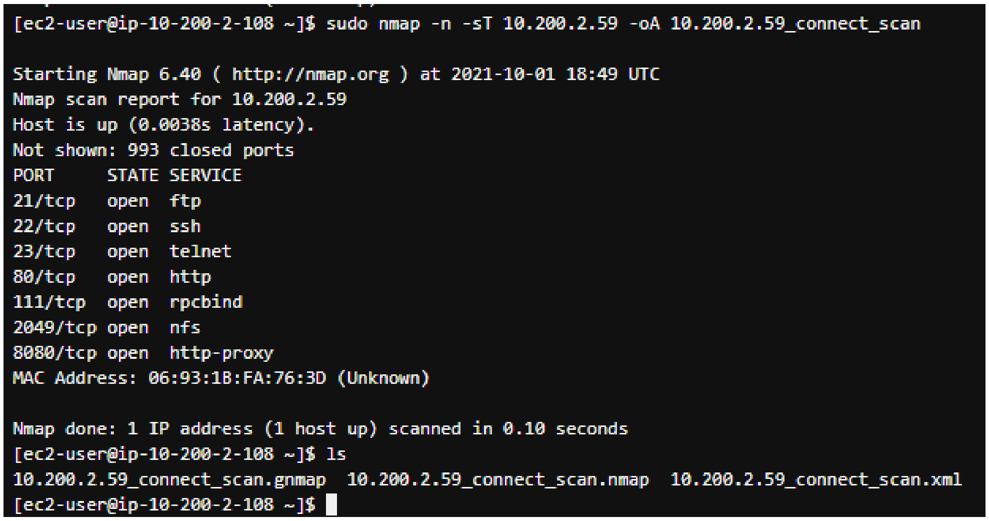
```
[ec2-user@ip-10-200-2-108 ~]$ sudo nmap -n -sT 10.200.2.59 -p 1-65535

Starting Nmap 6.40 ( http://nmap.org ) at 2021-10-01 18:39 UTC
Nmap scan report for 10.200.2.59
Host is up (0.016s latency).
Not shown: 65525 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
111/tcp   open  rpcbind
2049/tcp  open  nfs
8080/tcp  open  http-proxy
20048/tcp open  unknown
32799/tcp open  unknown
44595/tcp open  unknown
MAC Address: 06:93:1B:FA:76:3D (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.85 seconds
```

Figure 3.

Ports discovered and their services were:

- Port 21 / ftp
- Port 22 / ssh
- Port 23 / telnet
- Port 80 / http
- Port 111 / rpcbind
- Port 2049 / nfs
- Port 8080 / http-proxy
- Port 20048 / unknown
- Port 32799 / unknown
- Port 44595 / unknown

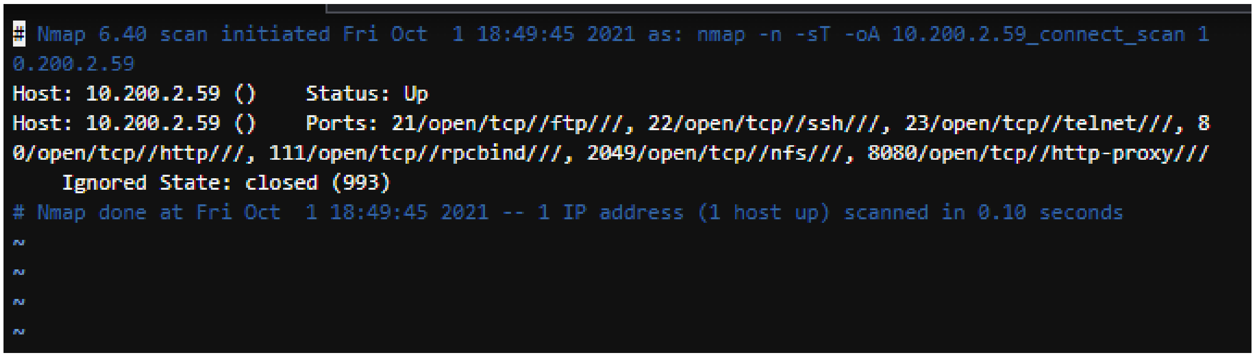
## Output Formats



```
[ec2-user@ip-10-200-2-108 ~]$ sudo nmap -n -sT 10.200.2.59 -oA 10.200.2.59_connect_scan

Starting Nmap 6.40 ( http://nmap.org ) at 2021-10-01 18:49 UTC
Nmap scan report for 10.200.2.59
Host is up (0.0038s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
80/tcp   open  http
111/tcp  open  rpcbind
2049/tcp open  nfs
8080/tcp open  http-proxy
MAC Address: 06:93:1B:FA:76:3D (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
[ec2-user@ip-10-200-2-108 ~]$ ls
10.200.2.59_connect_scan.gnmap  10.200.2.59_connect_scan.nmap  10.200.2.59_connect_scan.xml
[ec2-user@ip-10-200-2-108 ~]$
```

Figure 4.

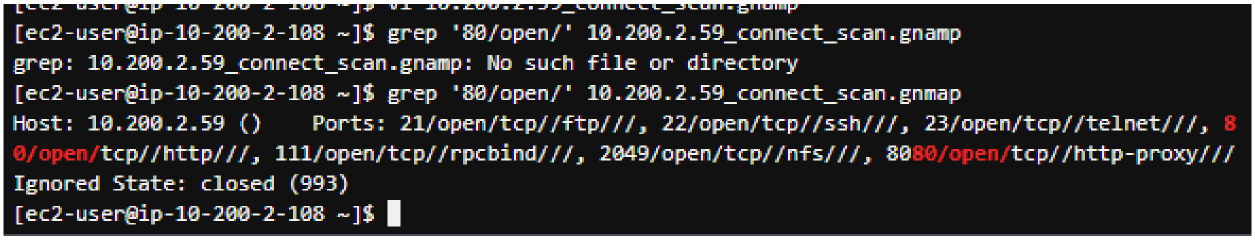
## Using Vi :



```
# Nmap 6.40 scan initiated Fri Oct  1 18:49:45 2021 as: nmap -n -sT -oA 10.200.2.59_connect_scan 1
0.200.2.59
Host: 10.200.2.59 ()    Status: Up
Host: 10.200.2.59 ()    Ports: 21/open/tcp//ftp///, 22/open/tcp//ssh///, 23/open/tcp//telnet///, 8
0/open/tcp//http///, 111/open/tcp//rpcbind///, 2049/open/tcp//nfs///, 8080/open/tcp//http-proxy///
    Ignored State: closed (993)
# Nmap done at Fri Oct  1 18:49:45 2021 -- 1 IP address (1 host up) scanned in 0.10 seconds
~
~
~
~
```

Figure 5.

## Execute grep :

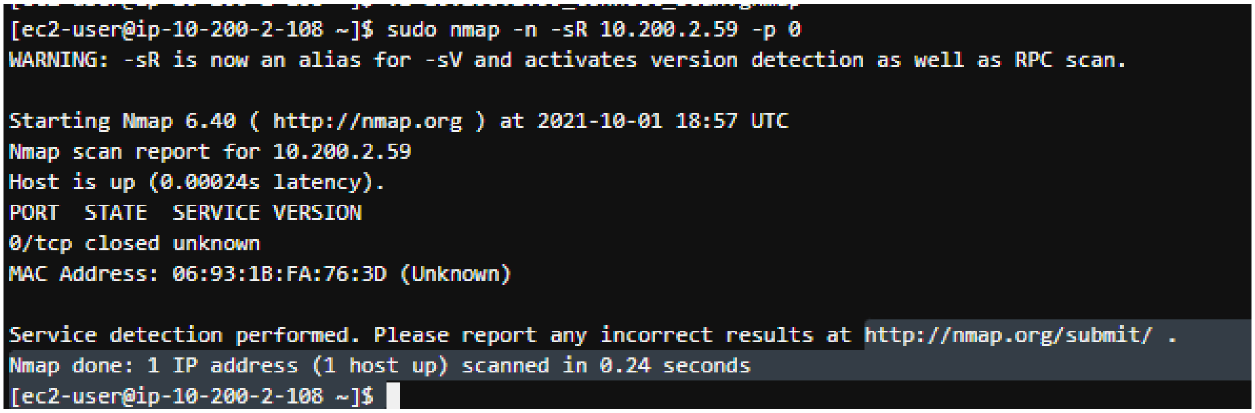


```
[ec2-user@ip-10-200-2-108 ~]$ grep '80/open/' 10.200.2.59_connect_scan.gnamp
grep: 10.200.2.59_connect_scan.gnamp: No such file or directory
[ec2-user@ip-10-200-2-108 ~]$ grep '80/open/' 10.200.2.59_connect_scan.gnmap
Host: 10.200.2.59 ()    Ports: 21/open/tcp//ftp///, 22/open/tcp//ssh///, 23/open/tcp//telnet///, 8
0/open/tcp//http///, 111/open/tcp//rpcbind///, 2049/open/tcp//nfs///, 8080/open/tcp//http-proxy///
Ignored State: closed (993)
[ec2-user@ip-10-200-2-108 ~]$
```

Figure 6.

# Port Scans

## Port Zero tcpdump and the packets :

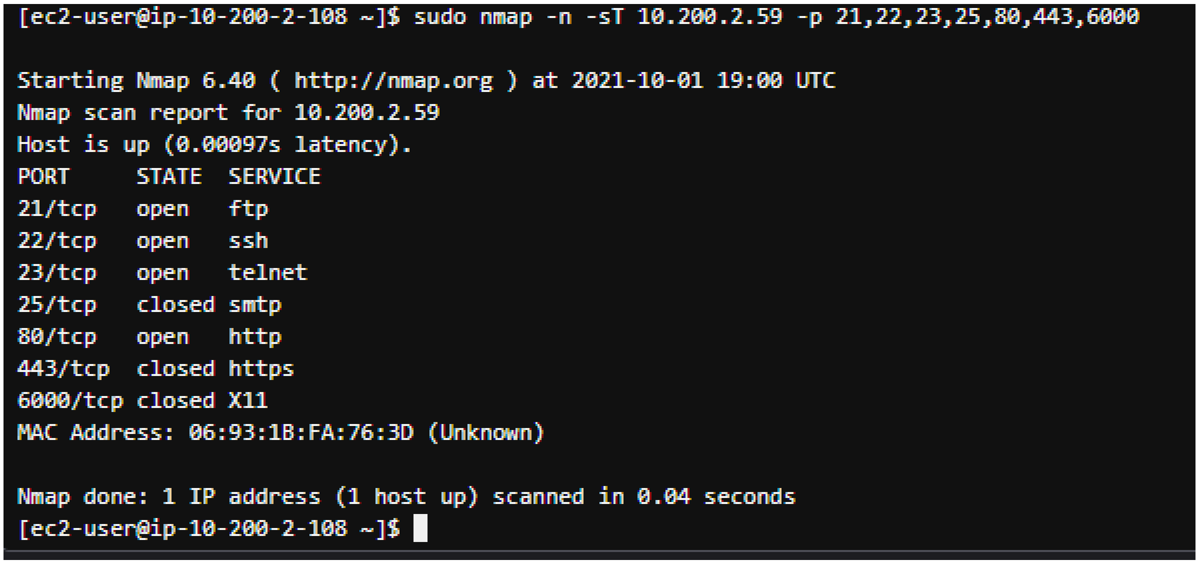


```
[ec2-user@ip-10-200-2-108 ~]$ sudo nmap -n -sR 10.200.2.59 -p 0
WARNING: -sR is now an alias for -sV and activates version detection as well as RPC scan.

Starting Nmap 6.40 ( http://nmap.org ) at 2021-10-01 18:57 UTC
Nmap scan report for 10.200.2.59
Host is up (0.00024s latency).
PORT  STATE  SERVICE VERSION
0/tcp closed unknown
MAC Address: 06:93:1B:FA:76:3D (Unknown)

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
[ec2-user@ip-10-200-2-108 ~]$
```

Figure 7.

On the tcpdump there are no changes however because port 0 is closed and you can’t connect to it, it is considered invalid.

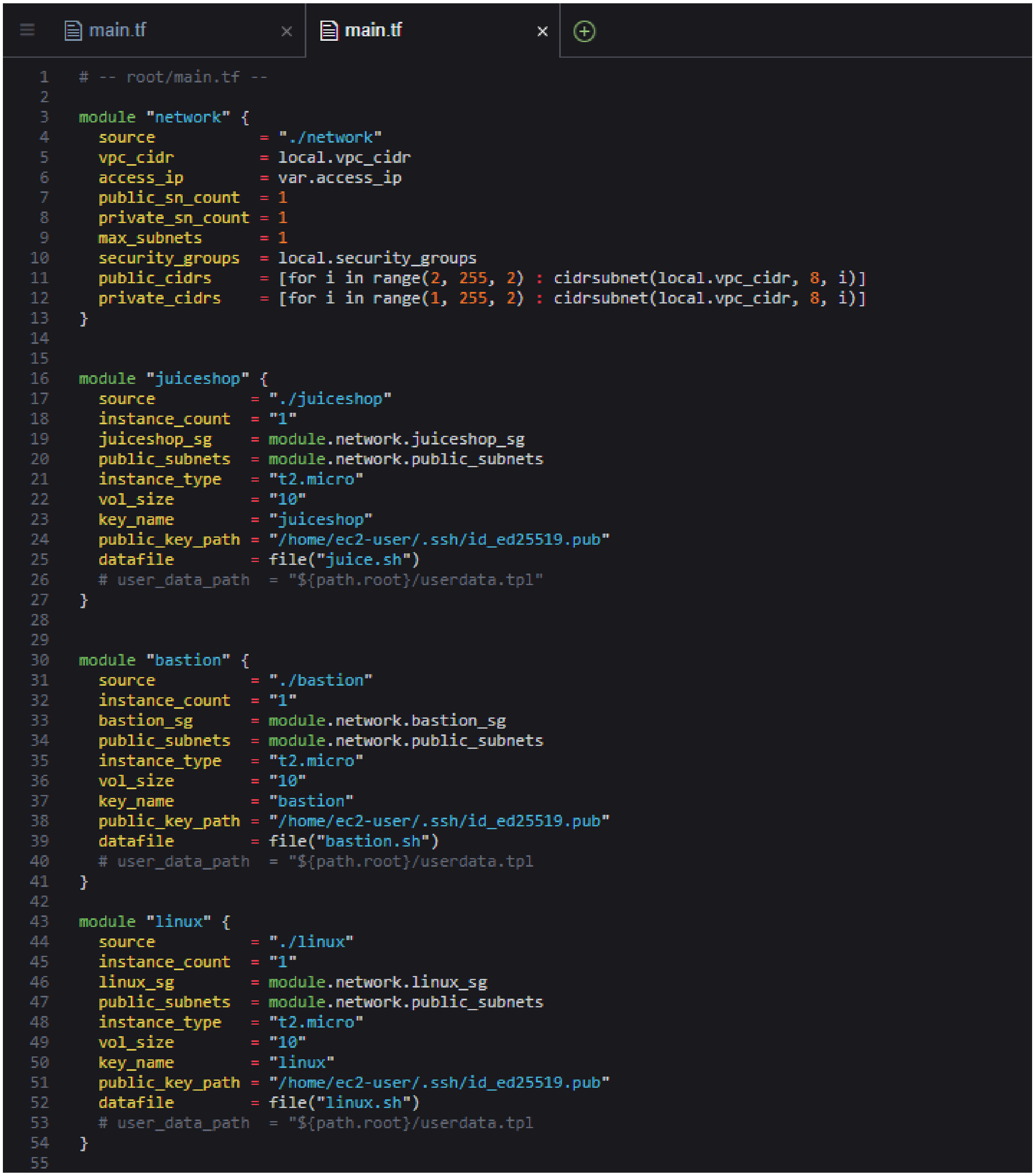
## Command that scans ports :



```
[ec2-user@ip-10-200-2-108 ~]$ sudo nmap -n -sT 10.200.2.59 -p 21,22,23,25,80,443,6000

Starting Nmap 6.40 ( http://nmap.org ) at 2021-10-01 19:00 UTC
Nmap scan report for 10.200.2.59
Host is up (0.00097s latency).
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
23/tcp   open   telnet
25/tcp   closed smtp
80/tcp   open   http
443/tcp  closed https
6000/tcp closed X11
MAC Address: 06:93:1B:FA:76:3D (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
[ec2-user@ip-10-200-2-108 ~]$
```

Figure 8.

# AWS Environment



```
# -- root/main.tf --

module "network" {
  source           = "./network"
  vpc_cidr         = local.vpc_cidr
  access_ip        = var.access_ip
  public_sn_count  = 1
  private_sn_count = 1
  max_subnets      = 1
  security_groups  = local.security_groups
  public_cidrs     = [for i in range(2, 255, 2) : cidrsubnet(local.vpc_cidr, 8, i)]
  private_cidrs    = [for i in range(1, 255, 2) : cidrsubnet(local.vpc_cidr, 8, i)]
}


module "juiceshop" {
  source          = "./juiceshop"
  instance_count  = "1"
  juiceshop_sg    = module.network.juiceshop_sg
  public_subnets  = module.network.public_subnets
  instance_type   = "t2.micro"
  vol_size        = "10"
  key_name        = "juiceshop"
  public_key_path = "/home/ec2-user/.ssh/id_ed25519.pub"
  datafile        = file("juice.sh")
  # user_data_path  = "${path.root}/userdata.tpl"
}


module "bastion" {
  source          = "./bastion"
  instance_count  = "1"
  bastion_sg      = module.network.bastion_sg
  public_subnets  = module.network.public_subnets
  instance_type   = "t2.micro"
  vol_size        = "10"
  key_name        = "bastion"
  public_key_path = "/home/ec2-user/.ssh/id_ed25519.pub"
  datafile        = file("bastion.sh")
  # user_data_path  = "${path.root}/userdata.tpl
}

module "linux" {
  source          = "./linux"
  instance_count  = "1"
  linux_sg        = module.network.linux_sg
  public_subnets  = module.network.public_subnets
  instance_type   = "t2.micro"
  vol_size        = "10"
  key_name        = "linux"
  public_key_path = "/home/ec2-user/.ssh/id_ed25519.pub"
  datafile        = file("linux.sh")
  # user_data_path  = "${path.root}/userdata.tpl
}

```

Figure 9.