Linux Administration

Nmap

Xavier Belanger

What is Nmap?

- Nmap stands for “Network Mapper”.
- It’s a network scanner that can be used to discover and identify devices and servers on a network.
- It’s been initially created by Gordon “Fyodor” Lyon, at the end of the 90s.

Ethical hacking reminder

- Scanning a computer that you do not manage or that is not your own could have legal consequences depending on the local jurisdiction.
- ***Inappropriate Usage***
  Because of the slight risk of crashes and because a few black hats like to use Nmap for reconnaissance prior to attacking systems, there are administrators who become upset and may complain when their system is scanned. Thus, it is often advisable to request permission before doing even a light scan of a network.

https://nmap.org/book/man-legal.html

Purpose

There is multiple reasons why you may need to use Nmap:

- discover and list all devices connected to a network
- validate firewall rules
- network troubleshooting
- finding vulnerabilities

Installation and usage

- Nmap is usually available as a package for most Linux distributions.
- Installers are also available for MS Windows and Mac OS X.
- Some options may require root or administrator access.

Basic usage

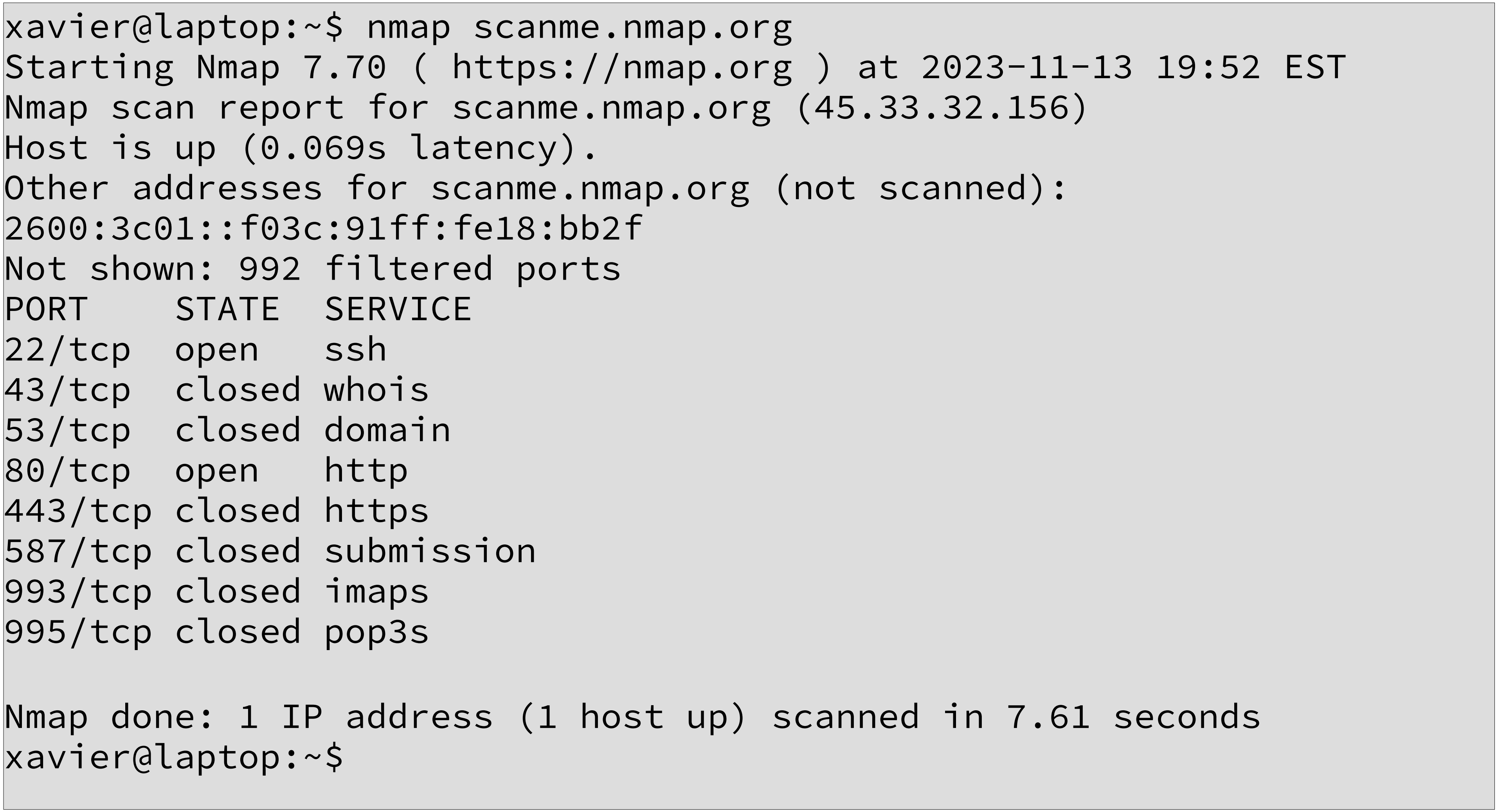
- nmap <*target*>
- <target> could be a hostname, an IP address or an IP network:
  - nmap server.example.net
  - nmap 192.168.25.87
  - nmap 10.5.0.0/16

Decoding Nmap output - 1

```
xavier@laptop:~$ nmap server.home.arpa
Starting Nmap 7.70 ( https://nmap.org ) at 2023-11-13 19:52 EST
Nmap scan report for server.home.arpa (192.168.1.50)
Host is up (0.028s latency).
Not shown: 992 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
443/tcp   open  https
2049/tcp  open  nfs
32768/tcp open  filenet-tms
32769/tcp open  filenet-rpc

Nmap done: 1 IP address (1 host up) scanned in 4.78 seconds
xavier@laptop:~$
```

Decoding Nmap output - 2



```
xavier@laptop:~$ nmap scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2023-11-13 19:52 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.069s latency).
Other addresses for scanme.nmap.org (not scanned):
2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 filtered ports
PORT    STATE  SERVICE
22/tcp  open   ssh
43/tcp  closed whois
53/tcp  closed domain
80/tcp  open   http
443/tcp closed https
587/tcp closed submission
993/tcp closed imaps
995/tcp closed pop3s

Nmap done: 1 IP address (1 host up) scanned in 7.61 seconds
xavier@laptop:~$
```

Scanning a specific port

- By default Nmap scans only the 1,000 most common ports. If you are looking for a specific port, you will need to use additional options.
- For a TCP port:
  - nmap -p T:<port> <target>
- For a UDP port:
  - nmap -sU -p U:<port> <target>
- You can also specify a port list or a port range:
  - nmap -p 80,443 server.example.net
  - nmap -p 1-1024 server.example.net

Using Nmap scripts

- A large collection of scripts is provided with Nmap to get more details about an available service.
- Documentation is accessible online: https://nmap.org/nsedoc/scripts/

Nmap script example - 1

```
xavier@laptop:~$ nmap -p T:22 scanme.nmap.org --script=ssh-auth-methods
Starting Nmap 7.70 ( https://nmap.org ) at 2023-11-13 20:18 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.070s latency).
Other addresses for scanme.nmap.org (not scanned):
2600:3c01::f03c:91ff:fe18:bb2f

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password

Nmap done: 1 IP address (1 host up) scanned in 1.26 seconds
xavier@laptop:~$
```

Nmap script example - 2

```
xavier@laptop:~$ nmap -p T:443 server.home.arpa --script=ssl-cert
Starting Nmap 7.70 ( https://nmap.org ) at 2023-11-13 20:22 EST
Nmap scan report for server.home.arpa (192.168.1.50)
Host is up (0.014s latency).

PORT    STATE SERVICE
443/tcp open  https
| ssl-cert: Subject: commonName=server.home.arpa/stateOrProvinceName=NORTH
CAROLINA/countryName=US
| Issuer: commonName=server.home.arpa/stateOrProvinceName=NORTH
CAROLINA/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-06-29T01:24:32
| Not valid after:  2023-12-26T01:24:32
| MD5:   f415 1e66 78de 5f67 c0c5 40aa e56b cdf7
|_SHA-1: 00ec da12 4b65 8611 7a58 654c 2eab 0a01 6cdb 0c69

Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
xavier@laptop:~$
```