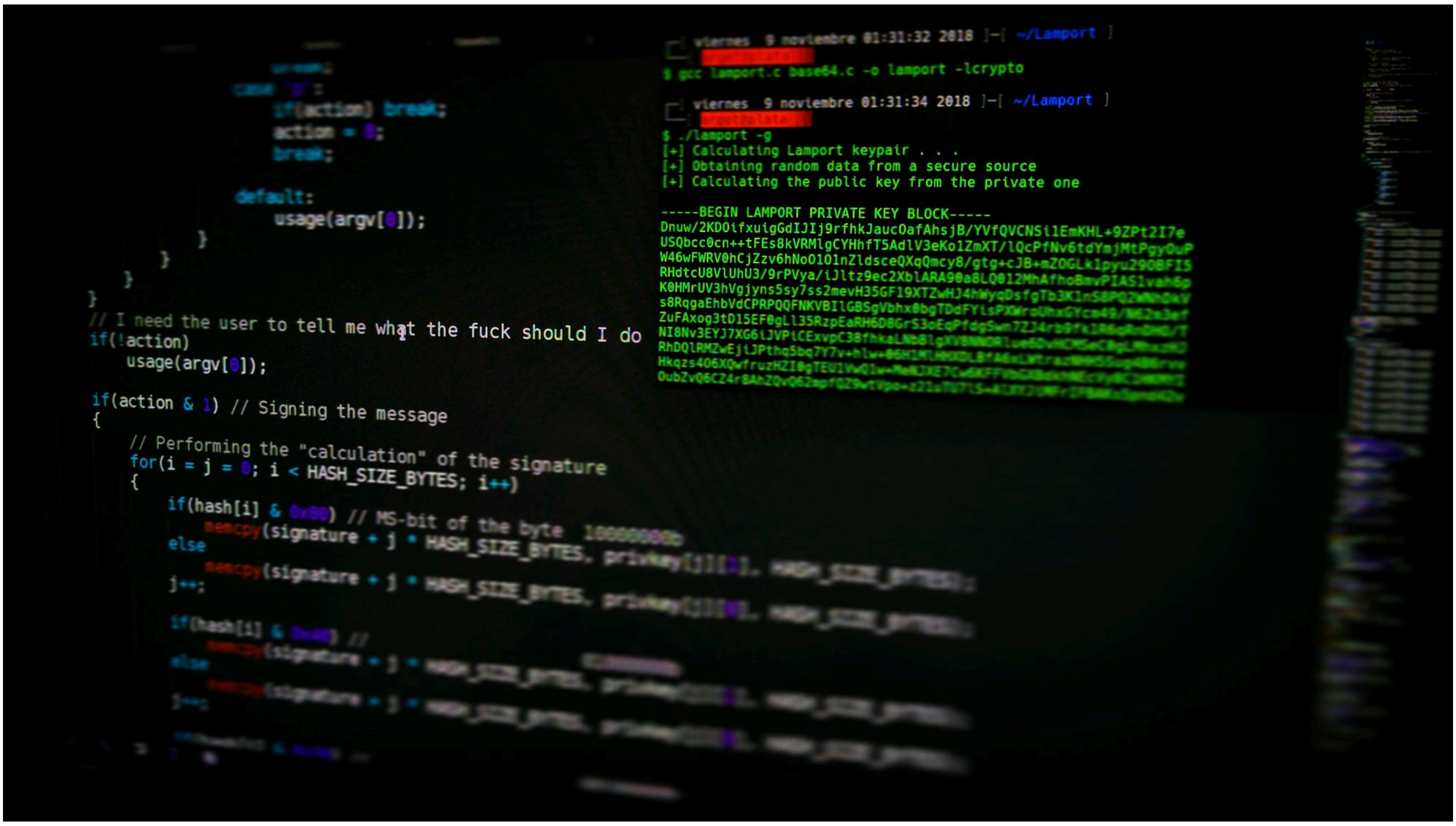
OCTOBER 2, 2020 / #CYBERSECURITY

What is Nmap and How to Use it – A Tutorial for the Greatest Scanning Tool of All Time

Manish Shivanandhan



```
        default:
            usage(argv[0]);
    }
  }
}
// I need the user to tell me what the fuck should I do
if(!action)
    usage(argv[0]);

if(action & 1) // Signing the message
{
    // Performing the "calculation" of the signature
    for(i = j = 0; i < HASH_SIZE_BYTES; i++)
    {
        if(hash[i] & 0x80) // MS-bit of the byte
```

```
viernes 9 noviembre 01:31:32 2018 ]-[ ~/Lamport ]
$ gcc lamport.c base64.c -o lamport -lcrypto

viernes 9 noviembre 01:31:34 2018 ]-[ ~/Lamport ]
$ ./lamport -g
[+] Calculating Lamport keypair . . .
[+] Obtaining random data from a secure source
[+] Calculating the public key from the private one

-----BEGIN LAMPORT PRIVATE KEY BLOCK-----
Dnuw/2KDOifxuigGdIJIj9rfhkJaucOafAhsjB/YVfQVCNSi1EmKHL+9ZPt2I7e
USQbcc0cn++tFEs8kVRMlgCYHhfT5AdlV3eKo1ZmXT/lQcPfNv6tdYmjMtPgyOuP
[illegible]
```

Nmap is the most famous scanning tool used by penetration testers. In this article, we will look at some core features of Nmap along with a few useful commands.

What is Nmap?

Nmap is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications.

Gordon Lyon (pseudonym Fyodor) wrote Nmap as a tool to help map an entire network easily and to find its open ports and services.

Nmap has become hugely popular, being featured in movies like The Matrix and the popular series Mr. Robot.

Why use Nmap?

There are a number of reasons why security pros prefer Nmap over other scanning tools.

First, Nmap helps you to quickly map out a network without sophisticated commands or configurations. It also supports simple commands (for example, to check if a host is up) and complex scripting through the Nmap scripting engine.

Other features of Nmap include:

- Ability to quickly recognize all the devices including servers, routers, switches, mobile devices, etc on single or multiple networks.
- Helps identify services running on a system including web servers, DNS servers, and other common applications. Nmap can also detect application versions with reasonable accuracy to help detect existing vulnerabilities.
- Nmap can find information about the operating system running on devices. It can provide detailed information like OS versions, making it easier to plan additional approaches during penetration testing.
- During security auditing and vulnerability scanning, you can use Nmap to attack systems using existing scripts from the Nmap Scripting Engine.
- Nmap has a graphical user interface called Zenmap. It helps you develop visual mappings of a network for better usability and reporting.

Commands

Let's look at some Nmap commands. If you don't have Nmap installed, you can get it from here.

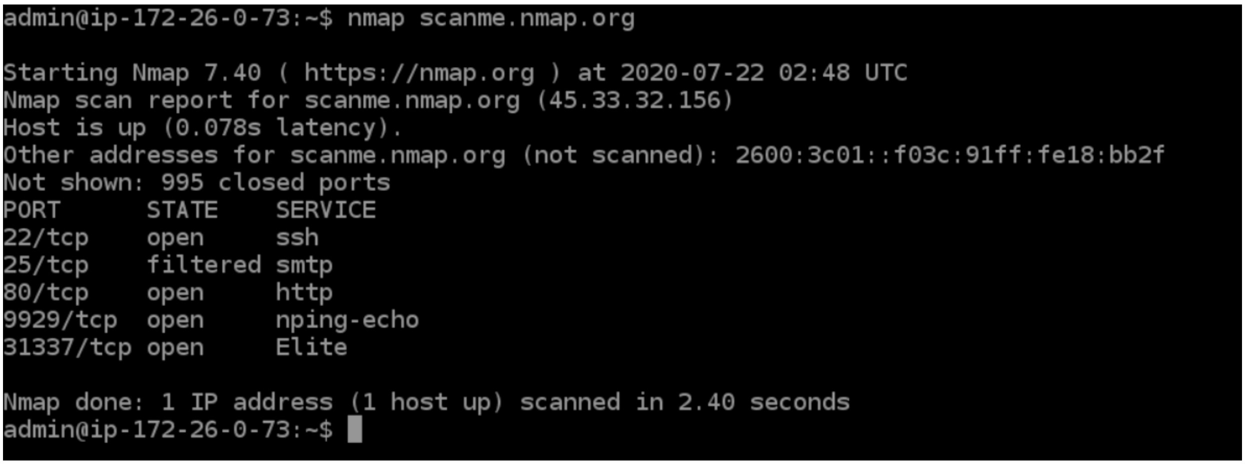
Basic scans

- **Ping scan** — Scans the list of devices up and running on a given subnet.

```
> nmap -sp 192.168.1.1/24
```

- **Scan a single host** — Scans a single host for 1000 well-known ports. These ports are the ones used by popular services like SQL, SNTP, apache, and others.

```
> nmap scanme.nmap.org
```



```
admin@ip-172-26-0-73:~$ nmap scanme.nmap.org

Starting Nmap 7.40 ( https://nmap.org ) at 2020-07-22 02:48 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.078s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 2.40 seconds
admin@ip-172-26-0-73:~$ █
```

Stealth scan

Stealth scanning is performed by sending an SYN packet and analyzing the response. If SYN/ACK is received, it means the port is open, and you can open a TCP connection.

However, a stealth scan never completes the 3-way handshake, which makes it hard for the target to determine the scanning system.

```
> nmap -sS scanme.nmap.org
```

while to get a response.

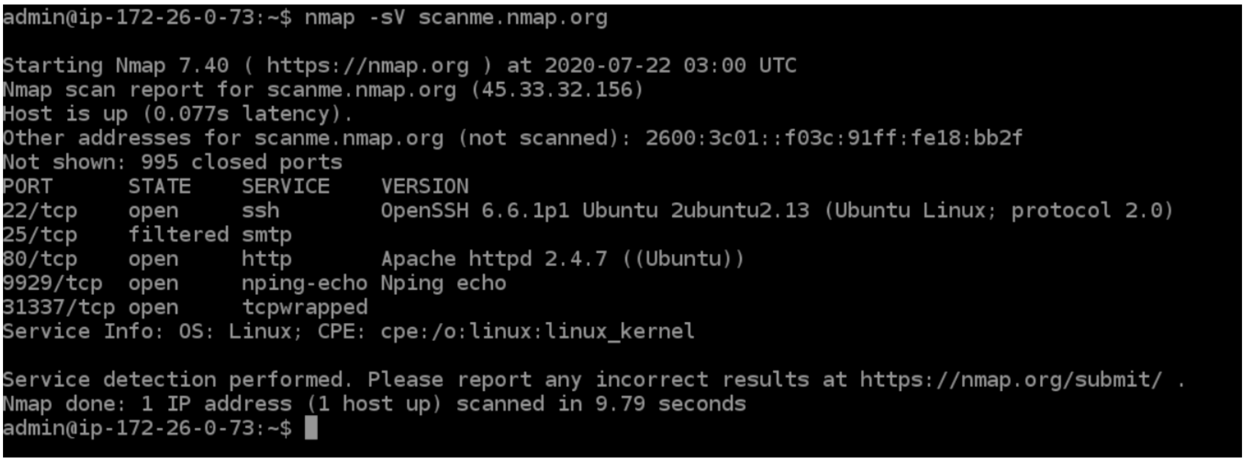
Version scanning

Finding application versions is a crucial part in penetration testing.

It makes your life easier since you can find an existing vulnerability from the Common Vulnerabilities and Exploits (CVE) database for a particular version of the service. You can then use it to attack a machine using an exploitation tool like Metasploit.

```
> nmap -sV scanme.nmap.org
```

To do a version scan, use the '-sV' command. Nmap will provide a list of services with its versions. Do keep in mind that version scans are not always 100% accurate, but it does take you one step closer to successfully getting into a system.



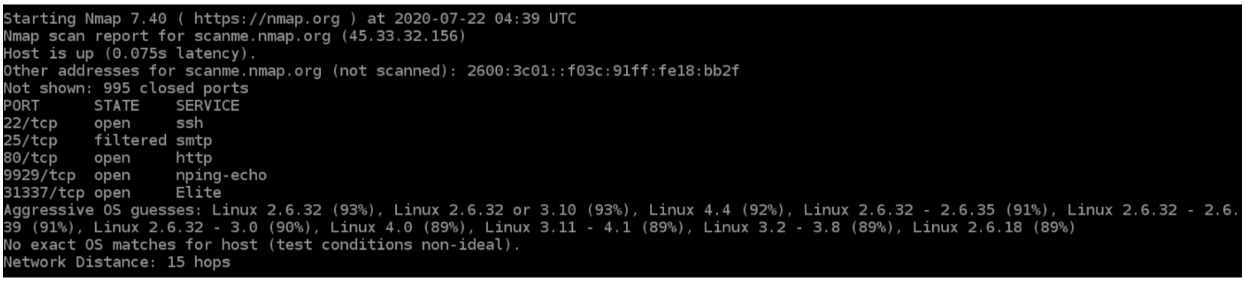
```
admin@ip-172-26-0-73:~$ nmap -sV scanme.nmap.org

Starting Nmap 7.40 ( https://nmap.org ) at 2020-07-22 03:00 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.077s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE    VERSION
22/tcp    open     ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open     http       Apache httpd 2.4.7 ((Ubuntu))
9929/tcp  open     nping-echo Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.79 seconds
admin@ip-172-26-0-73:~$ █
```

OS Scanning

In addition to the services and their versions, Nmap can provide information about the underlying operating system using TCP/IP fingerprinting. Nmap will also try to find the system uptime during an OS scan.

```
> nmap -sV scanme.nmap.org
```

Again, OS detection is not always accurate, but it goes a long way towards helping a pen tester get closer to their target.



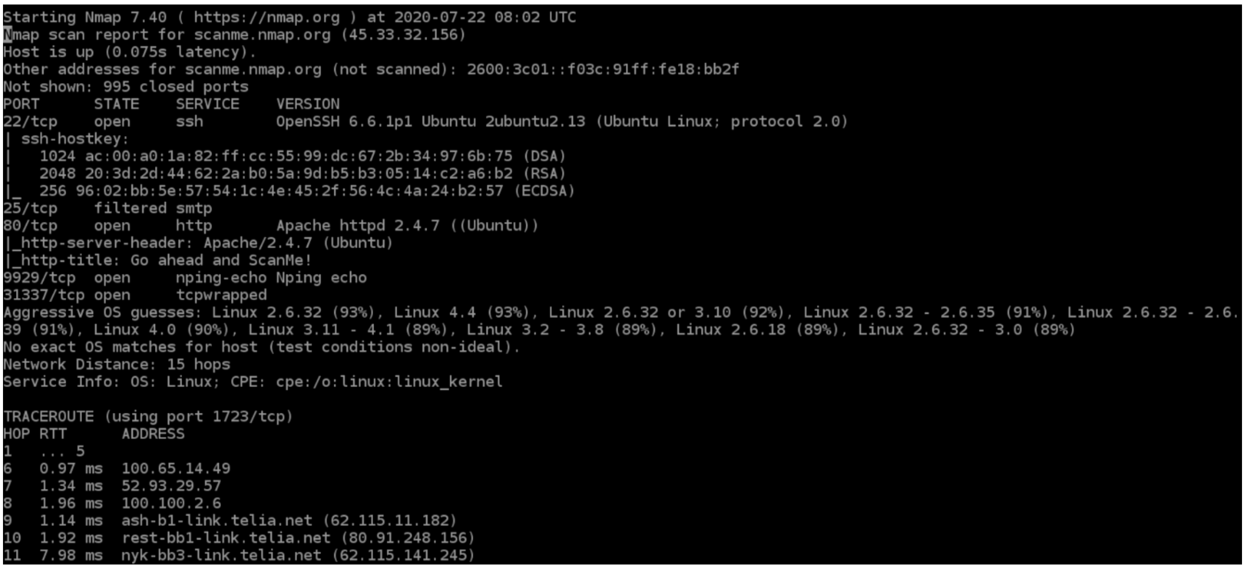
```
Starting Nmap 7.40 ( https://nmap.org ) at 2020-07-22 04:39 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.075s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
9929/tcp  open     nping-echo
31337/tcp open     Elite
Aggressive OS guesses: Linux 2.6.32 (93%), Linux 2.6.32 or 3.10 (93%), Linux 4.4 (92%), Linux 2.6.32 - 2.6.35 (91%), Linux 2.6.32 - 2.6.
39 (91%), Linux 2.6.32 - 3.0 (90%), Linux 4.0 (89%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 2.6.18 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 15 hops
```

Aggressive Scanning

Nmap has an aggressive mode that enables OS detection, version detection, script scanning, and traceroute. You can use the -A argument to perform an aggressive scan.

```
> nmap -A scanme.nmap.org
```

Aggressive scans provide far better information than regular scans. However, an aggressive scan also sends out more probes, and it is more likely to be detected during security audits.



```
Starting Nmap 7.40 ( https://nmap.org ) at 2020-07-22 08:02 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.075s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE    VERSION
22/tcp    open     ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|_  256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
25/tcp    filtered smtp
80/tcp    open     http       Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
9929/tcp  open     nping-echo Nping echo
31337/tcp open     tcpwrapped
Aggressive OS guesses: Linux 2.6.32 (93%), Linux 4.4 (93%), Linux 2.6.32 or 3.10 (92%), Linux 2.6.32 - 2.6.35 (91%), Linux 2.6.32 - 2.6.
39 (91%), Linux 4.0 (90%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 2.6.18 (89%), Linux 2.6.32 - 3.0 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 15 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 1723/tcp)
HOP RTT      ADDRESS
1   ... 5
6   0.97 ms  100.65.14.49
7   1.34 ms  52.93.29.57
8   1.96 ms  100.100.2.6
9   1.14 ms  ash-b1-link.telia.net (62.115.11.182)
10  1.92 ms  rest-bb1-link.telia.net (80.91.248.156)
11  7.98 ms  nyk-bb3-link.telia.net (62.115.141.245)
```

real handy when you are managing vast network infrastructure.

You can scan multiple hosts through numerous approaches:

- Write all the IP addresses in a single row to scan all of the hosts at the same time.

```
> nmap 192.164.1.1 192.164.0.2 192.164.0.2
```

- Use the asterisk (*) to scan all of the subnets at once.

```
> nmap 192.164.1.*
```

- Add commas to separate the addresses endings instead of typing the entire domains.

```
> nmap 192.164.0.1,2,3,4
```

- Use a hyphen to specify a range of IP addresses

```
> nmap 192.164.0.0-255
```

Port Scanning

Port scanning is one of the most fundamental features of Nmap. You can scan for ports in several ways.

- Using the -p param to scan for a single port

- If you specify the type of port, you can scan for information about a particular type of connection, for example for a TCP connection.

```
> nmap -p T:7777, 973 192.164.0.1
```

- A range of ports can be scanned by separating them with a hyphen.

```
> nmap -p 76–973 192.164.0.1
```

- You can also use the **-top-ports** flag to specify the top n ports to scan.

```
> nmap --top-ports 10 scanme.nmap.org
```

Scanning from a File

If you want to scan a large list of IP addresses, you can do it by importing a file with the list of IP addresses.

```
> nmap -iL /input_ips.txt
```

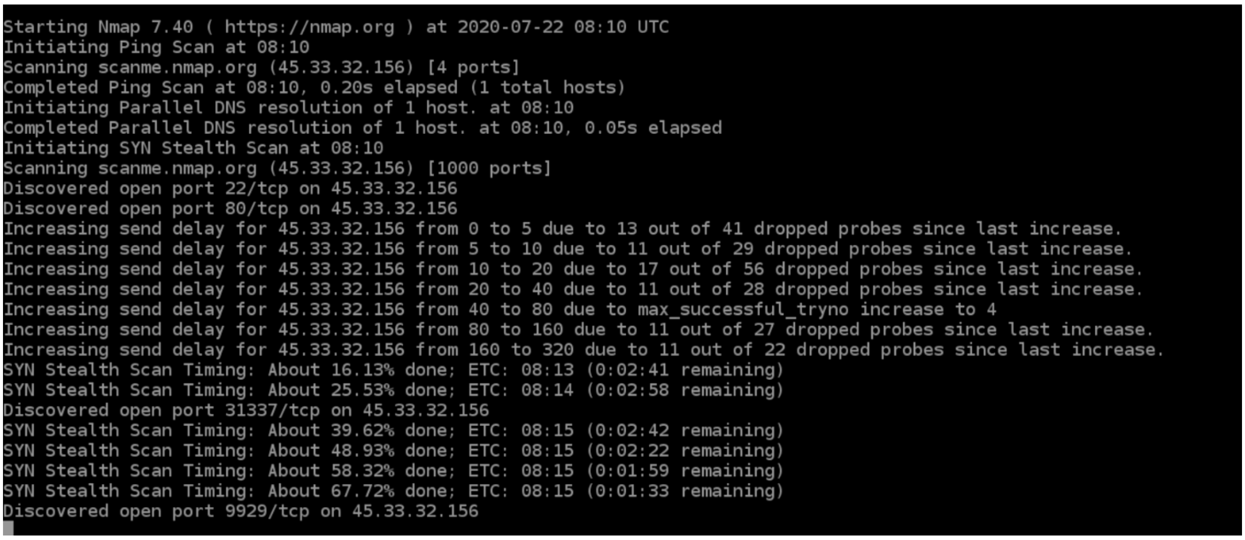
The above command will produce the scan results of all the given domains in the “input_ips.txt” file. Other than simply scanning the IP addresses, you can use additional options and flags as well.

Verbosity and Exporting Scan Results

Penetration testing can last days or even weeks. Exporting Nmap results can be useful to avoid redundant work and to help with creating final reports. Let’s look at some ways to export Nmap scan results.

```
> nmap -v scanme.nmap.org
```

The verbose output provides additional information about the scan being performed. It is useful to monitor step by step actions Nmap performs on a network, especially if you are an outsider scanning a client's network.

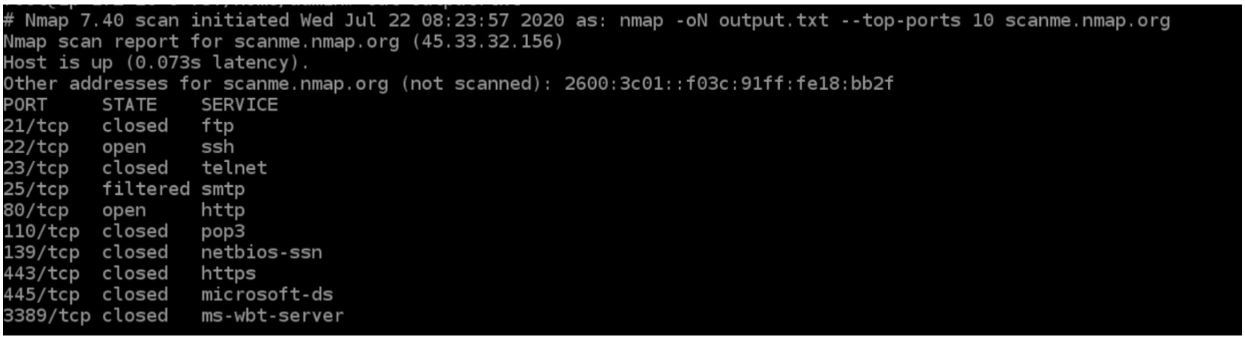


```
Starting Nmap 7.40 ( https://nmap.org ) at 2020-07-22 08:10 UTC
Initiating Ping Scan at 08:10
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 08:10, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:10
Completed Parallel DNS resolution of 1 host. at 08:10, 0.05s elapsed
Initiating SYN Stealth Scan at 08:10
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Increasing send delay for 45.33.32.156 from 0 to 5 due to 13 out of 41 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 5 to 10 due to 11 out of 29 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 10 to 20 due to 17 out of 56 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 20 to 40 due to 11 out of 28 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 40 to 80 due to max_successful_tryno increase to 4
Increasing send delay for 45.33.32.156 from 80 to 160 due to 11 out of 27 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 160 to 320 due to 11 out of 22 dropped probes since last increase.
SYN Stealth Scan Timing: About 16.13% done; ETC: 08:13 (0:02:41 remaining)
SYN Stealth Scan Timing: About 25.53% done; ETC: 08:14 (0:02:58 remaining)
Discovered open port 31337/tcp on 45.33.32.156
SYN Stealth Scan Timing: About 39.62% done; ETC: 08:15 (0:02:42 remaining)
SYN Stealth Scan Timing: About 48.93% done; ETC: 08:15 (0:02:22 remaining)
SYN Stealth Scan Timing: About 58.32% done; ETC: 08:15 (0:01:59 remaining)
SYN Stealth Scan Timing: About 67.72% done; ETC: 08:15 (0:01:33 remaining)
Discovered open port 9929/tcp on 45.33.32.156
```

Normal output

Nmap scans can also be exported to a text file. It will be slightly different from the original command line output, but it will capture all the essential scan results.

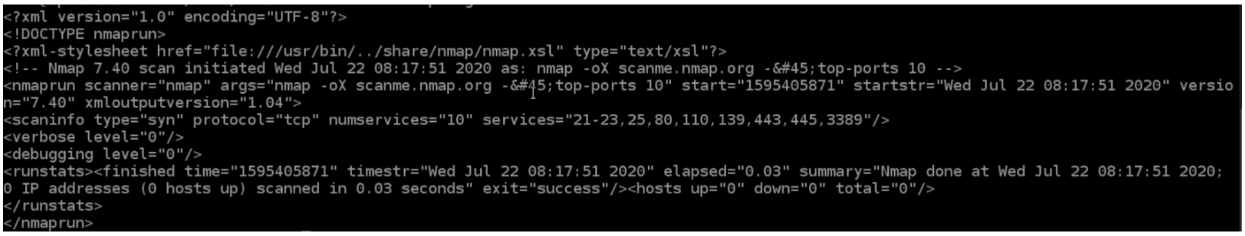
```
> nmap -oN output.txt scanme.nmap.org
```



```
# Nmap 7.40 scan initiated Wed Jul 22 08:23:57 2020 as: nmap -oN output.txt --top-ports 10 scanme.nmap.org
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.073s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
PORT     STATE    SERVICE
21/tcp   closed   ftp
22/tcp   open     ssh
23/tcp   closed   telnet
25/tcp   filtered smtp
80/tcp   open     http
110/tcp  closed   pop3
139/tcp  closed   netbios-ssn
443/tcp  closed   https
445/tcp  closed   microsoft-ds
3389/tcp closed   ms-wbt-server
```

testing tools, making it easily parsable when importing scan results.

```
> nmap -oX output.xml scanme.nmap.org
```



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE nmaprun>
<?xml-stylesheet href="file:///usr/bin/../share/nmap/nmap.xsl" type="text/xsl"?>
<!-- Nmap 7.40 scan initiated Wed Jul 22 08:17:51 2020 as: nmap -oX scanme.nmap.org -&#45;top-ports 10 -->
<nmaprun scanner="nmap" args="nmap -oX scanme.nmap.org -&#45;top-ports 10" start="1595405871" startstr="Wed Jul 22 08:17:51 2020" versio
n="7.40" xmloutputversion="1.04">
<scaninfo type="syn" protocol="tcp" numservices="10" services="21-23,25,80,110,139,443,445,3389"/>
<verbose level="0"/>
<debugging level="0"/>
<runstats><finished time="1595405871" timestr="Wed Jul 22 08:17:51 2020" elapsed="0.03" summary="Nmap done at Wed Jul 22 08:17:51 2020;
0 IP addresses (0 hosts up) scanned in 0.03 seconds" exit="success"/><hosts up="0" down="0" total="0"/>
</runstats>
</nmaprun>
```

Multiple Formats

You can also export the scan results in all the available formats at once using the -oA command.

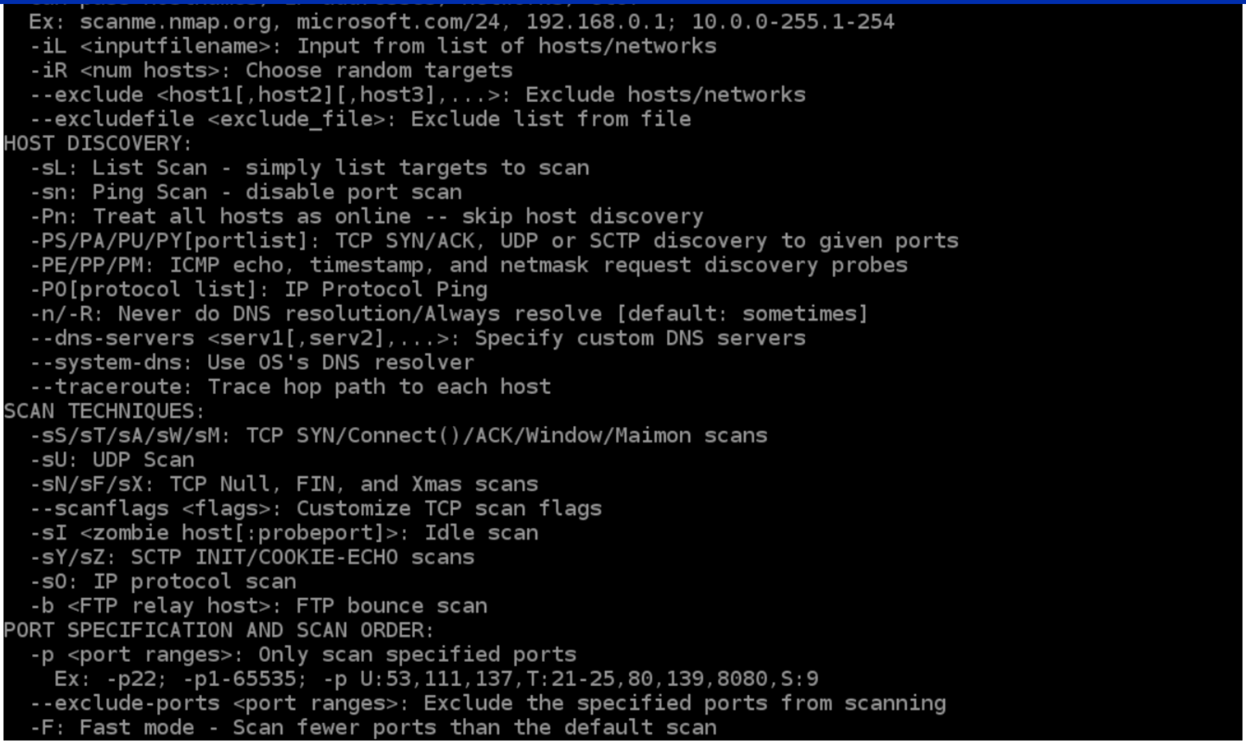
```
> nmap -oA output scanme.nmap.org
```

The above command will export the scan result in three files — output.xml, output. Nmap and output.gnmap.

Nmap Help

Nmap has a built-in help command that lists all the flags and options you can use. It is often handy given the number of command-line arguments Nmap comes with.

```
> nmap -h
```

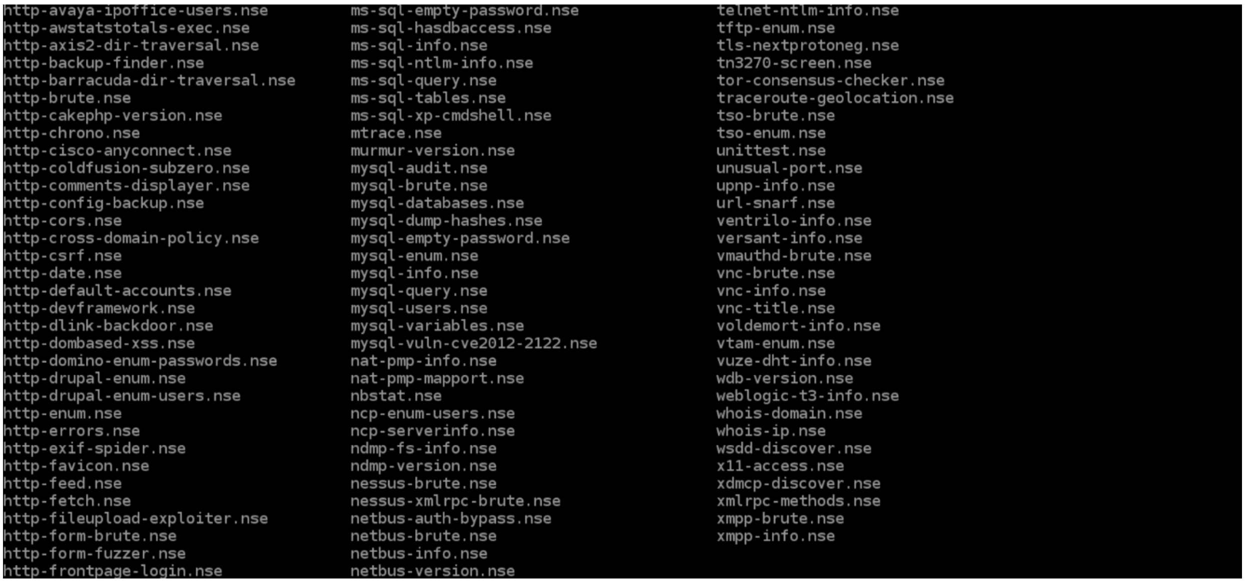


```
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
```

Nmap Scripting Engine

Nmap Scripting Engine (NSE) is an incredibly powerful tool that you can use to write scripts and automate numerous networking features.

You can find plenty of scripts distributed across Nmap, or write your own script based on your requirements. You can even modify existing scripts using the Lua programming language.

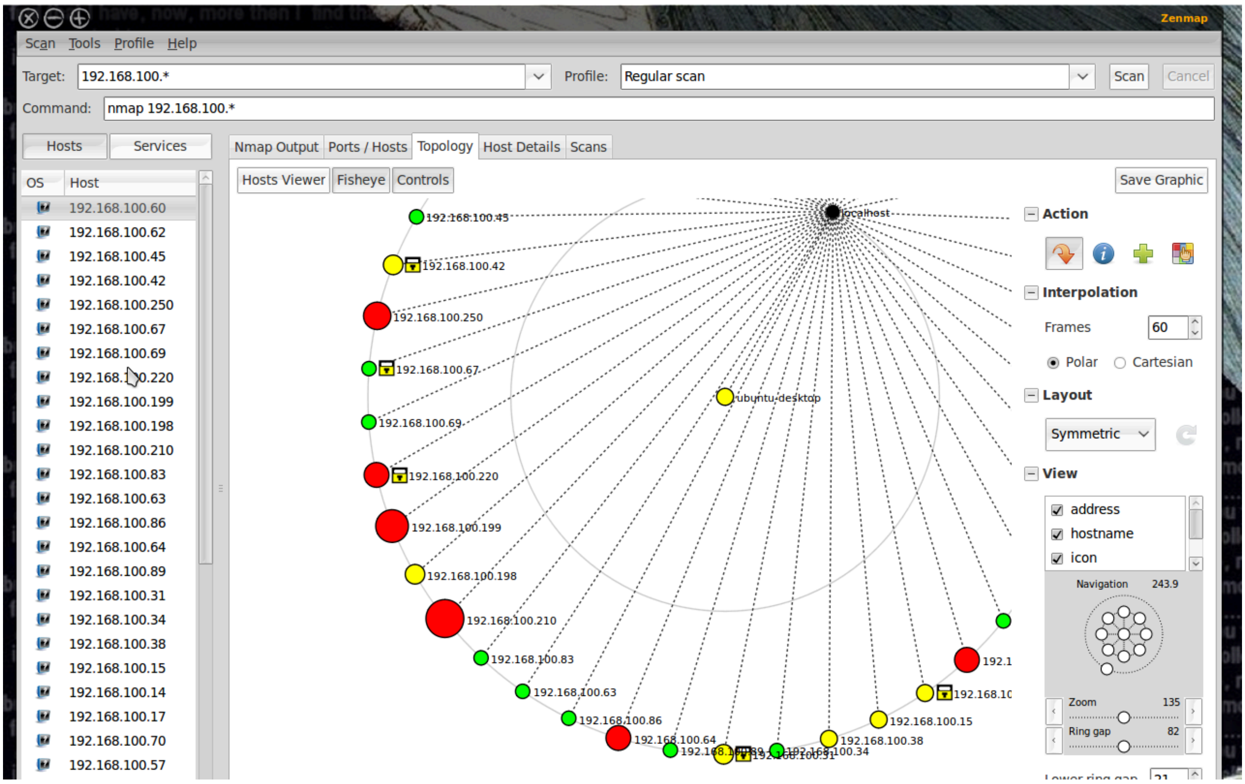


```
http-avaya-ipoffice-users.nse         ms-sql-empty-password.nse               telnet-ntlm-info.nse
http-awstatstotals-exec.nse           ms-sql-hasdbaccess.nse                  tftp-enum.nse
http-axis2-dir-traversal.nse          ms-sql-info.nse                         tls-nextprotoneg.nse
http-backup-finder.nse                ms-sql-ntlm-info.nse                    tn3270-screen.nse
http-barracuda-dir-traversal.nse      ms-sql-query.nse                        tor-consensus-checker.nse
http-brute.nse                        ms-sql-tables.nse                       traceroute-geolocation.nse
http-cakephp-version.nse              ms-sql-xp-cmdshell.nse                  tso-brute.nse
http-chrono.nse                       mtrace.nse                              tso-enum.nse
http-cisco-anyconnect.nse             murmur-version.nse                      unittest.nse
http-coldfusion-subzero.nse           mysql-audit.nse                         unusual-port.nse
http-comments-displayer.nse           mysql-brute.nse                         upnp-info.nse
http-config-backup.nse                mysql-databases.nse                     url-snarf.nse
http-cors.nse                         mysql-dump-hashes.nse                   ventrilo-info.nse
http-cross-domain-policy.nse          mysql-empty-password.nse                versant-info.nse
http-csrf.nse                         mysql-enum.nse                          vmauthd-brute.nse
http-date.nse                         mysql-info.nse                          vnc-brute.nse
http-default-accounts.nse             mysql-query.nse                         vnc-info.nse
http-devframework.nse                 mysql-users.nse                         vnc-title.nse
http-dlink-backdoor.nse               mysql-variables.nse                     voldemort-info.nse
http-dombased-xss.nse                 mysql-vuln-cve2012-2122.nse             vtam-enum.nse
http-domino-enum-passwords.nse        nat-pmp-info.nse                        vuze-dht-info.nse
http-drupal-enum.nse                  nat-pmp-mapport.nse                     wdb-version.nse
http-drupal-enum-users.nse            nbstat.nse                              weblogic-t3-info.nse
http-enum.nse                         ncp-enum-users.nse                      whois-domain.nse
http-errors.nse                       ncp-serverinfo.nse                      whois-ip.nse
http-exif-spider.nse                  ndmp-fs-info.nse                        wsdd-discover.nse
http-favicon.nse                      ndmp-version.nse                        x11-access.nse
http-feed.nse                         nessus-brute.nse                        xdmcp-discover.nse
http-fetch.nse                        nessus-xmlrpc-brute.nse                 xmlrpc-methods.nse
http-fileupload-exploiter.nse         netbus-auth-bypass.nse                  xmpp-brute.nse
http-form-brute.nse                   netbus-brute.nse                        xmpp-info.nse
http-form-fuzzer.nse                  netbus-info.nse
http-frontpage-login.nse              netbus-version.nse
```

Going through the scripting engine in-depth would be out-of-scope for this article, so here is more information about the Nmap scripting engine.

Zenmap

Zenmap is a graphical user interface for Nmap. It is a free and open-source software that helps you get up and running with Nmap.



Target: 192.168.100.*
Profile: Regular scan
Command: nmap 192.168.100.*

OS	Host
	192.168.100.60
	192.168.100.62
	192.168.100.45
	192.168.100.42
	192.168.100.250
	192.168.100.67
	192.168.100.69
	192.168.100.220
	192.168.100.199
	192.168.100.198
	192.168.100.210
	192.168.100.83
	192.168.100.63
	192.168.100.86
	192.168.100.64
	192.168.100.89
	192.168.100.31
	192.168.100.34
	192.168.100.38
	192.168.100.15
	192.168.100.14
	192.168.100.17
	192.168.100.70
	192.168.100.57

Frames 60
● Polar ○ Cartesian
Symmetric
☑ address
☑ hostname
☑ icon
Navigation 243.9
Zoom 135
Ring gap 82

In addition to providing visual network mappings, Zenmap also allows you to save and search your scans for future use.

Zenmap is great for beginners who want to test the capabilities of Nmap without going through a command-line interface.

Conclusion

Nmap is clearly the “Swiss Army Knife” of networking, thanks to its inventory of versatile commands.

Nmap has numerous settings, flags, and preferences that help system administrators analyze a network in detail.

If you want to learn Nmap in-depth, here is a great resource for you.

Loved this article? ***Join my Newsletter*** *and get a summary of my articles and videos every Monday.*

Manish Shivanandhan

Read more posts.

If this article was helpful, share it .

Learn to code for free. freeCodeCamp's open source curriculum has helped more than 40,000 people get jobs as developers. Get started

Trending Books and Handbooks

Learn CSS Transform
What is Programming?
HTTP Networking in JS
How to Write Clean Code
Learn Swift

Build a Static Blog
Python Code Examples
Write React Unit Tests
Learn PHP
Learn Golang

Build an AI Chatbot
Open Source for Devs
Learn Algorithms in JS
Learn Java
Learn Node.js