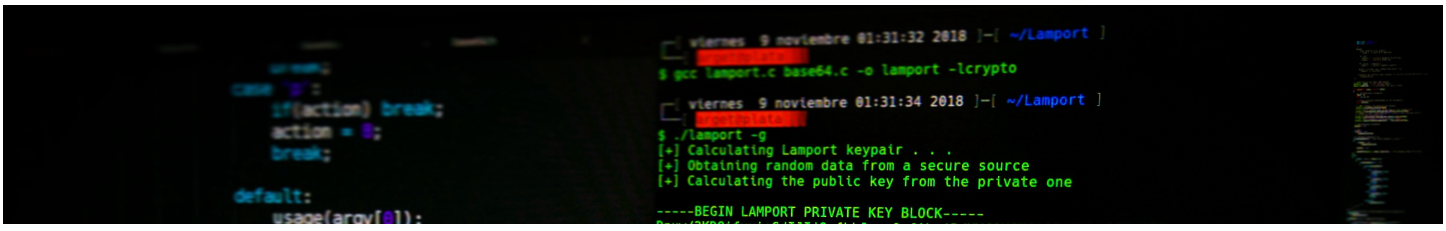
CYBERSECURITY

Nmap — A Guide To The Greatest Scanning Tool Of All Time

Network-Mapper (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.

Manish Shivanandhan Follow

Jul 22 · 8 min read ★



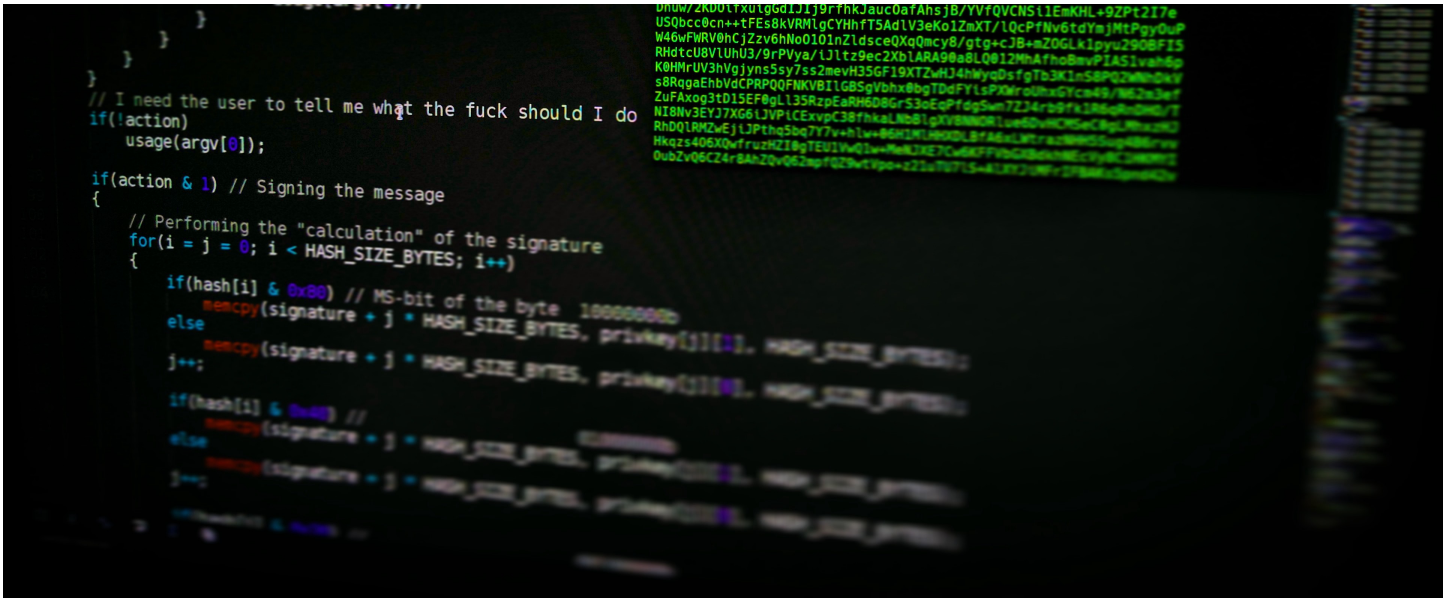


Photo by Arget on Unsplash

What is Nmap?

Nmap is the short form 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. Nmap allows network admins to find out the devices running on their network, discover open ports and services, and detect vulnerabilities.

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 is also hugely popular, being featured in movies like The Matrix and the popular series Mr. Robot.

Why Nmap?

There are a number of reasons why Nmap is preferred over other scanning tools. Nmap helps you to quickly map out a network without sophisticated commands or configurations. Nmap supports simple commands (eg. 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.
- 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 to 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

Scanning the list of active devices in a network is the first step in network mapping. There are two types of scans you can use for that:

- **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, etc.

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

Nmap Basic Scan

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, hence it's hard for the target to determine the scanning system.

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

You can use the **'-sS'** command to perform a stealth scan. Remember, stealth scanning is slower and not as aggressive as the other types of scanning, so you might have to wait a

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.

Nmap Version Scanning

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
```

You can use the additional flags like — osscan-limit to limit the search to a few expected targets. Nmap will display the confidence percentage for each OS guess. Again, OS detection is not always accurate, but it goes a long way in helping a pen tester get closer to his / her target.

Nmap OS Scanning

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.

Nmap Aggressive Scan

Scanning Multiple Hosts

Nmap has the capability of scanning multiple hosts simultaneously. This feature comes in 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

```
> nmap -p 973 192.164.0.1
```

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

Verbose Output

```
> 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.

Nmap Verbose Output

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.

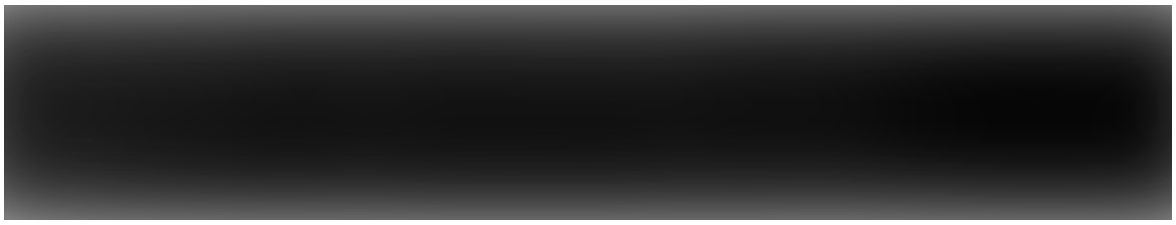
```
> nmap -oN output.txt scanme.nmap.org
```

Nmap File output

XML output

Nmap scans can also be exported to XML. It is also the preferred file format of most pen-testing tools, making it easily parsable when importing scan results.

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



Nmap XML Output

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
```

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.

Nmap Scripts

NSE also has attack scripts that are used in attacking the network and various networking protocols. 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.

Zenmap UI

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 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 lets you quickly scan and discover essential information about your network, hosts, ports, firewalls, and operating systems. Nmap has numerous settings, flags, and preferences that help system administrators analyze a network in detail.

If you are interested 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.*

Cybersecurity Cybercrime Penetration Testing Network Security Computer Security

Learn more.

Medium is an open platform where 170 million readers come to find insightful and dynamic thinking. Here, expert and undiscovered voices alike dive into the heart of any topic and bring new ideas to the surface. Learn more

Make Medium yours.

Follow the writers, publications, and topics that matter to you, and you'll see them on your homepage and in your inbox. Explore

Share your thinking.

If you have a story to tell, knowledge to share, or a perspective to offer — welcome home. It's easy and free to post your thinking on any topic. Write on Medium

---