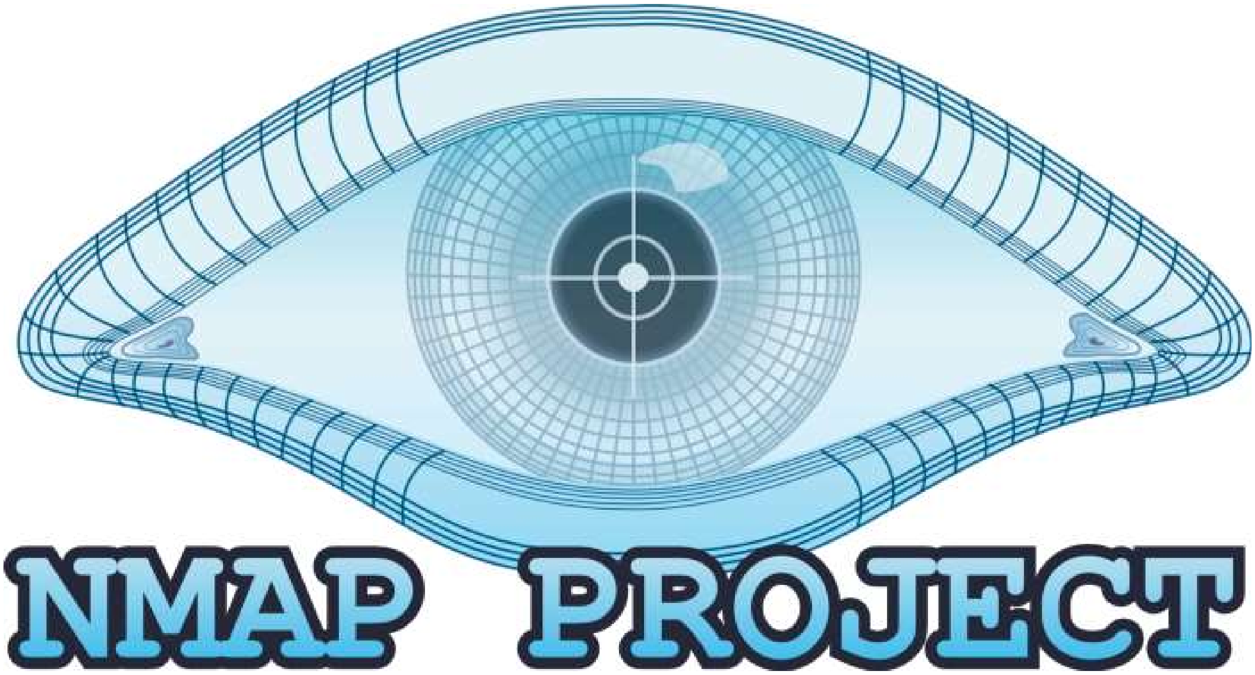
Luke Stephens (@hakluke)
3.7K Followers · About Follow

Hakluke’s Guide to Nmap — Port Scanning is Just The Beginning

Luke Stephens (@hakluke) Aug 26 · 5 min read ★



A while back, I posted a Twitter thread that described the Nmap features that I actually use. It really blew up! Nearly 80,000 people saw that thread, so I thought it would be good to put it into a blog post that can be searched and referred to over the long term. The original tweet is here: https://twitter.com/hakluke/status/1263821957163741185

The thing is, Nmap is one of those *OG* hacking tools that has been around since forever, and it's incredible, but similar to amass, Nmap is one of those tools that is synonymous with hacking, and extremely well known, but most people don't know how to use it to full advantage. Many people rarely do more than this:

```
$ nmap host
```

If you're doing this, you're not even scanning all the ports, and you're definitely not exfiltrating all of the information that Nmap is capable of finding! Nmap is a port scanner at heart, but it does so much more than just tell you which ports are open. You can use Nmap for service/OS detection and even vuln scanning. In this blog post, I'm going to outline how I use Nmap. I hope that by reading this, you will be able to use Nmap more effectively, and find more bugs!

The Basic Scan

By default Nmap does a standard TCP SYN scan on the top 1000 ports of host. I never really use this by itself.

```
$ nmap host
```

At an absolute minimum, I will get more verbosity using -v or -vv.

```
$ nmap -vv host
```

Target Specification

Nmap accepts target specification in loads of different formats including plain IP addresses, CIDR ranges and dash notation.

```
$ nmap hostname
$ nmap 123.123.123.123
$ nmap 123.123.123.1/24
$ nmap 123.123.123.1-255
```

Ping Sweeping

If you just want to find which hosts are alive, you can perform a ping scan with -sn

```
$ nmap -sn 123.123.123.1/24
```

Sometimes, hosts don’t respond to ping. To skip ping checks and just scan the host ports anyway, use -Pn:

```
$ nmap -Pn host
```

Scan Targets in a File

To scan a list of hosts from a file, use -iL:

```
$ nmap -iL ./hosts.txt
```

Scan Types

There are 9 scan types. The main 2 that you will use are:

```
TCP SYN (-sS)
UDP (-sU)
```

The default scan type is TCP SYN. To scan UDP ports use `-sU` . Other scan types can be useful for stealth or probing firewalls but may sacrifice accuracy or speed. You can find more information about the different nmap scan types here: https://nmap.org/book/man-port-scanning-techniques.html

Specifying Ports

You can specify which ports to scan with -p. **By default, only 1000 ports are scanned**. To scan all ports:

```
$ nmap -p 1-65535 host
```

Protip: To scan all ports you can also use `nmap -p- host` , which is shorthand for `nmap -p 1-65535 host` .

You can also specify a comma separated list with single ports, ranges and specific UDP ports:

```
$ nmap -p 23,23,25,110,80-90,U:53,1000-2000
```

Version and OS Enumeration

When Nmap finds an open port it can probe further to discover what service it is running if you specify `-sV` . You can set how intense you want the probes to be from 0 (light probe, fast but not accurate) to 9 (try all probes, slow but accurate)

```
$ nmap -sV — version-intensity 9
```

Nmap can guess which operating system a host is running based the scan results. Enable this feature with `-O` :

```
$ nmap -O host
```

Firewall Evasion

It also has extensive firewall evasion functionality. I've honestly never used these features but they allow you to do some cool things including spoofing the source address.

Output Formats

Nmap offers many output formats. Some are better for humans to read, others are better for parsing into other tools. I tend to output scans into all formats using:

```
$ nmap -oA outputfile host
```

Specific options include:

```
-oN Normal
-oX XML
-oS scr1pt k1dd13
-oG greppable
```

Scan Speed

You can also adjust the speed that nmap scans at. using -T<0–5>. A higher number means a higher speed.

Higher speed means less accuracy, and vice versa.

```
$ nmap -T3 host
```

Nmap Scripting Engine

This is where Nmap gets ***really*** interesting! It can also run Lua scripts. These can do pretty much anything. Nmap comes with about 600 of them that perform various vuln scanning and enumeration tasks, but you can also code your own.

The location of Lua scripts is:

```
<nmap directory>/share/nmap/scripts/*
```

Depending on your setup, you might also find them by running:

```
$ locate *.nse
```

As an example of using Nmap scripts, to check if a host is vulnerable to Eternal Blue, you could run:

```
$ nmap --script=smb-vuln-cve-2017–7494 host
```

Some scripts require arguments, you can specify them with `--script-args=n1=v1,n2=v2` etc.

To get help on which arguments may be accepted by a script:

```
$ nmap --script-help=scriptname
```

To upgrade your scripts to the latest and greatest, just run:

```
$ nmap --script-updatedb
```

A Nice Alias -A

A helpful alias is -A, which will enable OS detection, service version detection, script scanning, and traceroute.

```
nmap -A host
```

My Go-To Command

For a thorough scan of a single host, a decent go-to command is:

```
$ nmap -A -p1-65535 -v host
```

A Few Hot Tips

These are just random tips from the comments of my original tweet that didn't totally fit into the other categories but were too useful to leave out.

If your scan is taking a long time and you want more verbosity, hit 'v' while the scan is running. You can increase it multiple steps during the scan. No need to stop the scan to add '-v'!

Convert Nmap XML output to report friendly HTML using xsltproc.

```
xsltproc <nmap-output.xml> -o <nmap-output.html>
```

If you output to a file with -oN, -oG or -oX, you can interrupt a scan in progress and pick up exactly where you left off later by using `resume <file>`.

Conclusion

I haven’t even covered all of the awesome features that Nmap has here, but I’ve covered all of the features that I have ever found to be useful.

If you like this blog post, follow me on Twitter and subscribe to my YouTube channel.

Hacking Bug Bounty Nmap Recon Cybersecurity