

Forum:[Hack Forums](#)

Thread: [A Beginners Guide to Scanning with nmap](#)

VKNS - July 24, 2023, 1:15 pm

Polite Notice

Please do not try this on targets without the owner's permission. Even though you're technically not attacking anything, this can still get you dismissed from employment, sued or in hot water with your ISP.

Hey HF! ?

Today, I want to share with you a beginner-friendly guide on how to use nmap - a powerful and versatile network scanning tool. Whether you're a cybersecurity enthusiast, a system administrator, or just someone curious about network security, nmap can be an invaluable asset in your toolkit.

What is nmap?

NMAP stands for Network Mapper. It is a free, open-source tool that lets you explore networks and do security audits. It figures out what hosts and services are running on a computer network, kind of like drawing a map of the network's layout.

Before we delve into nmap's features, let's get it up and running on your system. Here's how to install nmap on different platforms:

Download the installer from the official nmap website and run it like any other Windows application.

Fairly self-explanatory, but if you need to be guided through the installer, I have included screenshots here: [\(Click to View\)](#)

You can use Homebrew or MacPorts package managers to install nmap easily. Open your Terminal and type:

Code brew install nmap

Alternatively, you can follow the guide here: [\(Click to View\)](#)

Most Linux distributions have nmap in their default package repositories. Simply use your package manager (apt, yum, dnf, etc.) to install it:

Code `sudo apt install nmap`

If you're running a distribution that doesn't have a package manager, you'll need to figure out how to install this yourself. This is an nmap tutorial, not a linux tutorial.

Once you have nmap installed, using it is quite straightforward. Open your terminal or command prompt and type:

Code `nmap <target>`

Replace `<target>` with the IP address or hostname of the device or network you want to scan. Nmap will start scanning and provide you with valuable information:

Breaking down the screenshot above: **PORT** (`<port>/<protocol>`): This column shows the port and protocol that nmap has discovered.

STATE: This column shows (you guessed it!) the state of the port. **open** - An application on your target is listening for/accepting TCP/UDP/SCTP connections on this port. This is what you're looking for.

closed - A closed port is accessible, which means it receives and responds to packets; but there is no application or service running on this port.

SERVICE - Shows the service or application accepting connections on this port.

Note: There are other states for ports, which you can read about [here](#).

Common ways to scan

Nmap offers several scanning techniques to gather specific information about hosts and services. Some of the most commonly used options include:

Basic TCP Scan: This is the default scan and checks the top 1000 TCP ports on the target.
`nmap target`

UDP Scan: Use this if you suspect there are open UDP ports on the target system.
`nmap -sU target`

Operating System Detection: Nmap can try to determine the operating system of the target.
`nmap -O target`

Version Detection: This option allows nmap to attempt to determine the version of services running on open ports.
`nmap -sV target`

Saving Output

Nmap can generate extensive output, so it's often helpful to save it for later analysis. To save the results to a file, use the following:
`nmap -oN scan_results.txt target`

Lucky for us, nmap now comes with the Nmap Scripting Engine (NSE), which lets us run LUA scripts alongside a regular nmap scan.

We're given a ton of scripts to play with, but the most popular one for finding vulnerabilities in services is ported with nmap and usually requires no extra installation steps:

vulners.nse

Once you've had a quick look at your target and verified that there are open ports to scan for vulns, run the following command, replacing <target> with your target hostname or IP Address:

```
Code nmap -sV --script vulners <target>
```

If you're lucky, you'll get something back that looks like this:

This is showing us that Port 80 is running a service called lighttpd, version 1.4.59. Under that, it shows a small list of CVEs with links to the vulners database; explaining the vulnerabilities in detail. The numbers you see (5.0, 4.3, 0.0) are the severity of the vulnerability; with a higher number meaning more severe.

Make note of the CVEs listed in this search. In my example, We have the following:

CVE-2022-41556

CVE-2022-22707

CVE-2022-41556

These CVEs are used across several vulnerability databases. Just googling the CVE will return thousands of results on most vulnerabilities. Using CVE-2022-41556 as an example, I searched google and found the following page on the Vulnerability:

The page shares various information on the vulnerability, including the following:

An Overview of the vulnerability.

Attack complexity.

Attack Vector.

Privileges Required.

How to fix/patch the vulnerability.

Thanks for reading. I hope you've learned something; I certainly learned a few things writing this post.

All the best.

HunT3R09 - July 24, 2023, 1:49 pm

This will get the feet wet , Thanks for the great share keep the good work up.

Bastille - July 25, 2023, 12:29 am

Nice thread buddy, really easy to read with all images that separates the different parts, thanks for the share !

Ezocain - July 25, 2023, 1:28 am

Great introduction to nmap, an essential tool for any hacker and researcher.

It's incredible what you'll learn just from writing a beginners guide on something you already knew. At least when it's as well written and properly done like this one.

Inspired me to do the same, but what intrigued me most is the NSE, a part of nmap I haven't really taken a good look at.

Good work!

shifumaster - July 25, 2023, 4:17 am

thanks dude appreciate it

Rezcal - July 27, 2023, 1:58 pm

Thanks my man, really appreciate this

TheMiddleMan - August 8, 2023, 5:24 am

This was a very helpful guide to using nmap thank you so much for posting this thread and taking the time to do so it's helped me get a better understanding on how to use nmap at first it looked daunting and I didn't really know why one uses it specifically but it's definitely got me considering nmap as my main mapping tool for potential security assistance jobs

plextrax123 - August 25, 2023, 2:15 pm

thank you so much I've been looking for nmap guide ?

lolipop32 - August 26, 2023, 3:01 am

Pretty straight forward.

zadig767 - August 26, 2023, 4:13 am

thank you for this guide

JamesChoe - August 27, 2023, 3:15 am

Nice thread very detailed thanks buddy

Alien8ed - December 14, 2024, 12:44 pm

Excellent thread my friend.

It is a very good summary of the first steps with this tool.

member13415 - December 18, 2024, 6:11 pm

thanks so much very helpful

man_its_a_hot_one - December 20, 2024, 11:54 pm

This is excellent for beginners, great job dude. For anyone interested in learning more you could always buy the nmap network scanning book from Amazon which I'm pretty sure is actually written by the person who invented/coded the nmap port scanner.

sadmin - January 9, 2025, 11:37 pm

thanks man, i'm new to nmap so this helped alot

everynight - February 19, 2025, 1:26 am

Thank you very much for your sharing.