

Forum:[Hack Forums](#)

Thread: [Nmap for newbs](#)

Perfect - May 18, 2024, 3:08 pm

Exploring Nmap

Nmap is like the Sherlock Holmes of cybersecurity tools. It helps you uncover hidden treasures and vulnerabilities in your network. Let's dive into this Swiss Army knife of network scanning and see how it can level up your cybersecurity game!

Why Nmap?

Nmap is the go-to tool for network discovery and security auditing. It's like having x-ray vision for your network, letting you see what's lurking in the shadows.

Key Features:

Port Scanning:

Nmap can scan thousands of ports on a target system to find open ports and services. It's like knocking on doors to see who's home.

OS Detection:

With OS detection capabilities, Nmap can guess the operating system of a target device based on how it responds to network probes. It's like figuring out someone's identity from their handwriting.

Service Version Detection:

Nmap can identify the version numbers of services running on open ports, helping you pinpoint potential vulnerabilities. It's like knowing exactly what tools your opponent has in their arsenal.

Scripting Engine:

Nmap's scripting engine allows you to automate tasks and customize your scans with scripts tailored to your needs. It's like having a personal assistant who can do all the heavy lifting for you.

Flexible Output Options:

Nmap offers various output formats, including plain text, XML, and interactive mode, making it easy to analyze scan results. It's like presenting your findings in a format that everyone can understand.

Getting Started:

Here's a quick guide to start using Nmap:

1. Install Nmap:

You can download Nmap for free from the official website. It's available for Windows, Linux, and macOS.

2. Run a Simple Scan:

Open a terminal or command prompt and type `nmap [target]` to scan a specific target. Replace `[target]` with the IP address or hostname of the target device.

3. Explore Advanced Options:

Once you're comfortable with the basics, explore Nmap's advanced options, such as OS detection `-O` or version detection `-sV`, to gather more information about your targets.

Helpful Resources:

Here are some resources to help you master Nmap:

[Nmap Reference Guide](#): The official Nmap reference guide covers everything from basic usage to advanced scanning techniques.

[Nmap Documentation](#): Dive deeper into Nmap's features and functionalities with the official documentation.

[Nmap Screenshots](#): Browse through screenshots of Nmap in action to get a visual understanding of its capabilities.

[Nmap Mailing List](#): Join the Nmap mailing list to connect with other users, ask questions, and share tips.

[Nmap Downloads](#): Download the latest version of Nmap and additional data files from the official website.

Start Scanning Today!

With Nmap in your toolkit, you'll be able to uncover hidden vulnerabilities and secure your network like a pro. So don your detective hat, fire up Nmap, and start scanning!

Nel son - May 18, 2024, 6:03 pm

yeah is good to know

Aarshdeep - May 19, 2024, 1:14 am

can u give more brief explanation if possible.

7 - May 19, 2024, 1:15 am

(May 19, 2024 01:14 AM)Aarshdeep Wrote: [\[CITE\]](#) can u give more brief explanation if possible.

Lol, you won't succeed in this industry if this guide is too long for you.

I suggest taking the time and learning in more depth , not less.

klantutan2042 - June 22, 2024, 2:40 am

can you give more sample how to use nmap?

TheBreadman - August 4, 2024, 1:36 pm

Alright, I'll be sure to use these resources in the future

Had3s03 - August 6, 2024, 12:37 pm

(May 19, 2024 01:15 AM)NulldB Wrote: [\[CITE\]](#) Lol, you won't succeed in this industry if this guide is

too long for you.

I suggest taking the time and learning in more depth , not less.

(Aug 4, 2024 01:36 PM)TheBreadman Wrote: [\[CITE\]](#) Alright, I'll be sure to use these resources in the future

Zenmap (made my nmap) is also pretty good for learning some of the advanced options/simplifies some things, plus a GUI makes it feel good imo. it may have been downloaded with nmap when/if you downloaded it

<https://nmap.org/zenmap/>

7 - August 7, 2024, 1:56 am

(Aug 6, 2024 12:37 PM)Had3s03 Wrote: [\[CITE\]](#) Zenmap (made my nmap) is also pretty good for learning some of the advanced options/simplifies some things, plus a GUI makes it feel good imo. it may have been downloaded with nmap when/if you downloaed it

<https://nmap.org/zenmap/>

yeah if you prefer using gui zenmap is a good option.

Im sure there are a few actually.

masquerosurfer - August 15, 2024, 8:57 am

can someone explain me how do i get the ip of someone? im trying to make a bully pay for what he did on me and i wanted to learn how to hack

nice tool this is really good keep going

Hosting Farmer - August 25, 2024, 9:25 am

Good guide, how about nmap scan for page title string grep or other? Example results list.txt "Ajenti" from ip most password are default.

DramaKing - August 25, 2024, 12:31 pm

(Aug 25, 2024 09:25 AM)Hosting Farmer Wrote: [\[CITE\]](#) Good guide, how about nmap scan for page title string grep or other? Example results list.txt "Ajenti" from ip most password are default.

Whatever you're saying in your spam, nmap is not a webcrawler.

Hosting Farmer - August 25, 2024, 12:33 pm

(Aug 25, 2024 12:31 PM)DramaKing Wrote: [\[CITE\]](#) Whatever you're saying in your spam, nmap is not a webcrawler.

Toxic and -rep me, I don't care you your problem tiggered. noob...

<https://nmap.org/nsedoc/scripts/http-title.html>

Learn it.

DramaKing - August 25, 2024, 12:34 pm

(Aug 25, 2024 12:33 PM)Hosting Farmer Wrote: [\[CITE\]](#) Toxic and -rep me, I don't care you your problem tiggered.

<https://nmap.org/nsedoc/scripts/http-title.html>

Learn it.

Okay, fine. Still can't understand you.

M?tt - August 25, 2024, 12:48 pm

(Aug 25, 2024 12:31 PM)DramaKing Wrote: [\[CITE\]](#) Whatever you're saying in your spam, nmap is

not a webcrawler.

I think all DramaKing was trying to say is that there's a difference from running scripts against an IP address with a web server compared to a website crawler. I understand what you were saying, but your terminology was just a bit off.

DramaKing - August 25, 2024, 1:07 pm

I misunderstood and don't know every Nmap script. Didn't think I was being 'toxic.' I wonder if this hosting company promoter has heard of Google dorks. The script can only be run on a single URL and grepable Nmap output has issues.

Money- - August 26, 2024, 7:33 am

(Aug 25, 2024 09:25 AM)Hosting Farmer Wrote: [\[CITE\]](#) Good guide, how about nmap scan for page title string grep or other? Example results list.txt "Ajenti" from ip most password are default.

(Aug 25, 2024 01:07 PM)DramaKing Wrote: [\[CITE\]](#) I misunderstood and don't know every Nmap script. Didn't think I was being 'toxic.' I wonder if this hosting company promoter has heard of Google dorks. The script can only be run on a single URL and grepable Nmap output has issues.

You can run the nmap script on multiple urls like this " nmap --script http-title.nse -iL targets.txt "

Where targets.txt can be your IP or domain names without the HTTP protocol like

google.com
hackforums.net

...

..

172.33.21.2

10.10.10.2

..

..

etc....

I guess that's what promoter want probably.

I don't know if nmap checks for Ajenti exploits , you can just look it up on github and look for the RCE exploits you looking for.

Nmap -sC flag uses all scripts but that's too slow and noisy , might as well just use the ones from github or exploit-db <https://www.exploit-db.com/exploits/47497>

or code urself.

Hosting Farmer - August 26, 2024, 8:31 am

(Aug 26, 2024 07:33 AM)Money- Wrote: [\[CITE\]](#) You can run the nmap script on multiple urls like this " nmap --script http-title.nse -iL targets.txt "

Where targets.txt can be your IP or domain names without the HTTP protocol like

google.com
hackforums.net

...

..

172.33.21.2

10.10.10.2

..

..
etc....

I guess that's what promoter want probably.

I don't know if nmap checks for Ajenti exploits , you can just look it up on github and look for the RCE exploits you looking for.

Nmap -sC flag uses all scripts but that's too slow and noisy , might as well just use the ones from github or exploit-db <https://www.exploit-db.com/exploits/47497>

or code urself.

Excellent questions, I will try build code it language C/C++ multi thread faster scan target find if has title page "Ajenti" to save logs.txt ip:port, Most install Ajenti for web panel linux login default username: root and passowrd: admin ?

Money- - August 26, 2024, 8:35 am

(Aug 26, 2024 08:31 AM)Hosting Farmer Wrote: [\[CITE\]](#) Excellent questions, I will try build code it language C/C++ multi thread faster scan target find if has title page "Ajenti" to save logs.txt ip:port, Most install Ajenti for web panel linux login default username: root and passowrd: admin ?

You can use this tool called " httpx " to directly grep the title " ajenti " ask chatgpt to give u a linux command with httpx that will accept list of URLs/IPs to output into logs.txt if its "ajenti" oneliner code that's it, Don't really need C/C++ but yea up to you bro if u want speed.

Zellow - August 26, 2024, 9:55 am

Thanks for the info, very useful

Soeren - September 4, 2024, 7:29 pm

Thanks for the info, I'm currently learning the use of nmap, and this to the point document showed me its potential... Appreciate it !

pompiszon - September 18, 2024, 5:35 am

can u send me for free? no bytes ? [warn]