

Forum:[Hack Forums](#)

Thread: [scanning for open ports](#)

unhappyhacker - August 24, 2024, 4:47 pm

I have read about people scanning the internet looking for open ports. What scanner program does this. The only scanner i have seen you have to know the IP to scan it. But just generally scanning for open ports? What software? Please note I have no intention of trying to exploit any open ports. i want to learn how they scan the internet without knowing the IP

Mercury - August 24, 2024, 5:20 pm

You need NMAP. There is loads of information and tutorials out there. I'd start with this article:

<https://nmap.org/book/man-target-specification.html>

DramaKing - August 24, 2024, 6:44 pm

(Aug 24, 2024 04:47 PM)unhappyhacker Wrote: [\[CITE\]](#) I have read about people scanning the internet looking for open ports. What scanner program does this. The only scanner i have seen you have to know the IP to scan it. But just generally scanning for open ports? What software? Please note I have no intention of trying to exploit any open ports. i want to learn how they scan the internet without knowing the IP

IP addresses are required to communicate with any device on a network. You can perform host detection to find alive hosts prior to port scanning. Just don't try scanning IPv6 addresses.

ScrubspooF - August 24, 2024, 7:34 pm

(Aug 24, 2024 06:44 PM)DramaKing Wrote: [\[CITE\]](#) IP addresses are required to communicate with any device on a network. You can perform host detection to find alive hosts prior to port scanning. Just don't try scanning IPv6 addresses.

Nmap has supported IPv6 since 2002.

DramaKing - August 24, 2024, 7:49 pm

(Aug 24, 2024 07:34 PM)ScrubspooF Wrote: [\[CITE\]](#) Nmap has supported IPv6 since 2002.

Of course Nmap supports IPv6, it would just be foolhardy to try to detect live hosts using IPv6.

Bastille - August 24, 2024, 10:18 pm

As said above nmap is a great tool however it requires additional knowledge related to networking :

- IP versions (IPv4 and IPv6)
- Ports (number, role, services)
- Firewalling
- Control flags (SYN, ACK, RST, ...)
- Stealth scan
- Script scans

I highly recommend you the following :

- Don't try on networks you don't own, try on your own machines / network
- Read the manual to understand what to do
- There are some exercises on websites such as tryhackme.com

Be aware that there is also a graphic version called Zenmap, because nmap is a command line tool

BlackSoulZN5006 - August 25, 2024, 6:28 pm

NMAP and as well as Nikto.

SuNgO - August 26, 2024, 2:12 pm

Definitely NMAP, that's what you need!

unhappyhacker - August 27, 2024, 3:52 am

I can't get NMAP to work. First it says KB4474419 is missing but it is not. I then go on and it says it's installed but it won't work. When I try to open it I get

pythonw.exe - System Error

The program can't start because api-ms-win-core-path-l1-1-0.dll is missing from your computer. Try reinstalling the program to fix this problem.

I have reinstalled it three times

DramaKing - August 27, 2024, 5:51 am

(Aug 27, 2024 03:52 AM)unhappyhacker Wrote: [\[CITE\]](#) I can't get NMAP to work. First it says KB4474419 is missing but it is not. I then go on and it says it's installed but it won't work. When I try to open it I get

pythonw.exe - System Error

The program can't start because api-ms-win-core-path-l1-1-0.dll is missing from your computer. Try reinstalling the program to fix this problem.

I have reinstalled it three times

What version of Windows? If it's v. 10 or 11, you should have no problem.

unhappyhacker - August 27, 2024, 6:14 am

(Aug 27, 2024 05:51 AM)DramaKing Wrote: [\[CITE\]](#) What version of Windows? If it's v. 10 or 11, you should have no problem.

Win 7 64 bit

DramaKing - August 27, 2024, 6:32 am

(Aug 27, 2024 06:14 AM)unhappyhacker Wrote: [\[CITE\]](#) Win 7 64 bit

I won't rag on you for not upgrading, presumably you have reasons, even though the system requirements for 10 aren't any beefier than 7. It is terrible for your OpSec and general security, though. Software compatibility is becoming increasingly bad.

Nmap does currently support Windows 7, hmm.

EDIT: I'm going to say that the current Nmap uses Python 3, which I can certainly tell you fails to run on Win7. The Nmap team probably needs to update the compatibility list. I found a hacky workaround here: <https://github.com/nalexandru/api-ms-win-core-path-HACK>. Your other options are to run an older version of Nmap or use masscan, Angry IP Scanner, or MegaPing.

unhappyhacker - August 27, 2024, 7:08 am

(Aug 27, 2024 06:32 AM)DramaKing Wrote: [\[CITE\]](#) I won't rag on you for not upgrading, presumably you have reasons, even though the system requirements for 10 aren't any beefier than 7. It is terrible for your OpSec and general security, though. Software compatibility is becoming increasingly bad.

Nmap does currently support Windows 7, hmm.

EDIT: I'm going to say that the current Nmap uses Python 3, which I can certainly tell you fails to run on Win7. The Nmap team probably needs to update the compatibility list. I found a hacky workaround here: <https://github.com/nalexandru/api-ms-win-core-path-HACK>. Your other options are to run an older version of Nmap or use masscan, Angry IP Scanner, or MegaPing.

OK thanks. I don't like the windows 10, tiles etc. Can masscan, Angry IP Scanner, or MegaPing scan the internet looking for open ports. Or do you have to pick an ip, scan that and then another. I do not intend to do anything to any open ports. I just want to learn about scanning

DramaKing - August 27, 2024, 7:17 am

(Aug 27, 2024 07:08 AM)unhappyhacker Wrote: [\[CITE\]](#) OK thanks. I don't like the windows 10, tiles etc. Can masscan, Angry IP Scanner, or MegaPing scan the internet looking for open ports. Or do you have to pick an ip, scan that and then another. I do not intend to do anything to any open ports. I just want to learn about scanning

You're asking someone who hadn't used any of these tools apart from lab assignments. I looked up MegaPing, and you can specify the From address as 0.0.0.0 and the To address as 223.255.255.255. That should give you around 3.5 billion addresses. Don't get caught.

shadowcrow - August 27, 2024, 8:58 am

(Aug 24, 2024 04:47 PM)unhappyhacker Wrote: [\[CITE\]](#) I have read about people scanning the internet looking for open ports. What scanner program does this. The only scanner i have seen you have to know the IP to scan it. But just generally scanning for open ports? What software? Please note I have no intention of trying to exploit any open ports. i want to learn how they scan the internet without knowing the IP

If you want to scan the internet then nmap is of course one of the best you can use but for widescanning I recommend [ZGRAB](#)

But if you don't know what you are doing...don't do it or learn how these scanners work - some are good for mass scanning and others better for scanning of specific hosts for information.

While portscanning is legal in most parts of the world, active vulnerability scanning could get you in jail...

unhappyhacker - August 28, 2024, 2:16 am

(Aug 27, 2024 07:17 AM)DramaKing Wrote: [\[CITE\]](#) You're asking someone who hadn't used any of these tools apart from lab assignments. I looked up MegaPing, and you can specify the From address as 0.0.0.0 and the To address as 223.255.255.255. That should give you around 3.5 billion addresses. Don't get caught. How would I get caught? Do people know they are scanned? Angry Ip needs Jave/OpenJDK which I found at <https://adoptium.net/temurin/releases/>. Is this OK?

DramaKing - August 28, 2024, 3:59 am

(Aug 28, 2024 02:16 AM)unhappyhacker Wrote: [\[CITE\]](#) How would I get caught? Do people know they are scanned? Angry Ip needs Jave/OpenJDK which I found at <https://adoptium.net/temurin/releases/>. Is this OK?

Don't know that site. Always downloaded Java from Oracle.

SIM-5320087 - October 9, 2024, 12:28 pm

Many thanks for sharing, much appreciated!

