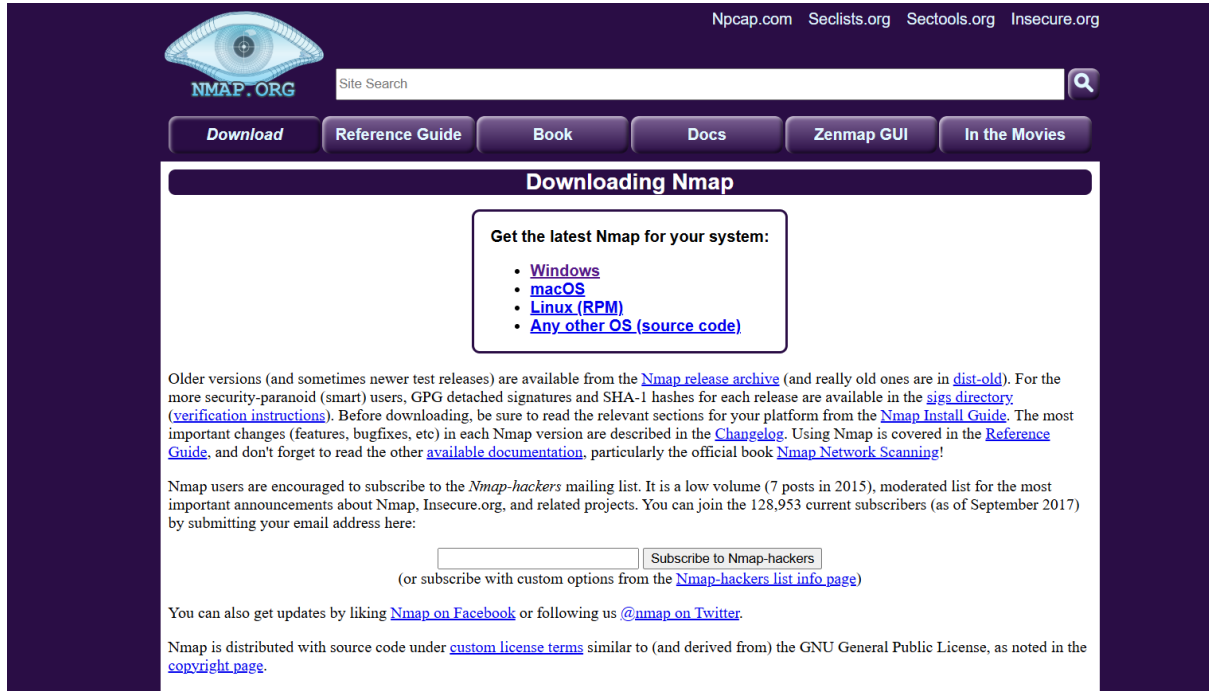


Zenmap

<https://nmap.org/download.html#windows>



The screenshot shows the Nmap.org website with a dark blue header. The header includes the Nmap logo (an eye) and the text 'NMAP.ORG'. To the right of the logo is a search bar labeled 'Site Search'. Further right are links to 'Npcap.com', 'Seclists.org', 'Sectools.org', and 'Insecure.org'. Below the header is a navigation bar with buttons for 'Download', 'Reference Guide', 'Book', 'Docs', 'Zenmap GUI', and 'In the Movies'. The main content area is titled 'Downloading Nmap' and contains a box with the text 'Get the latest Nmap for your system:' followed by a list of links: 'Windows', 'macOS', 'Linux (RPM)', and 'Any other OS (source code)'. Below this box is a paragraph of text about older versions and security features, followed by a paragraph about the Nmap-hackers mailing list and a subscription form. At the bottom, there is a link to 'Nmap on Facebook' and a link to '@nmap on Twitter'. The footer contains a paragraph about the GNU General Public License.

NMAP.ORG

Site Search

Download Reference Guide Book Docs Zenmap GUI In the Movies

Downloading Nmap

Get the latest Nmap for your system:

- [Windows](#)
- [macOS](#)
- [Linux \(RPM\)](#)
- [Any other OS \(source code\)](#)

Older versions (and sometimes newer test releases) are available from the [Nmap release archive](#) (and really old ones are in [dist-old](#)). For the more security-paranoid (smart) users, GPG detached signatures and SHA-1 hashes for each release are available in the [sig directory](#) ([verification instructions](#)). Before downloading, be sure to read the relevant sections for your platform from the [Nmap Install Guide](#). The most important changes (features, bugfixes, etc) in each Nmap version are described in the [Changelog](#). Using Nmap is covered in the [Reference Guide](#), and don't forget to read the other [available documentation](#), particularly the official book [Nmap Network Scanning](#)!

Nmap users are encouraged to subscribe to the *Nmap-hackers* mailing list. It is a low volume (7 posts in 2015), moderated list for the most important announcements about Nmap, Insecure.org, and related projects. You can join the 128,953 current subscribers (as of September 2017) by submitting your email address here:

(or subscribe with custom options from the [Nmap-hackers list info page](#))

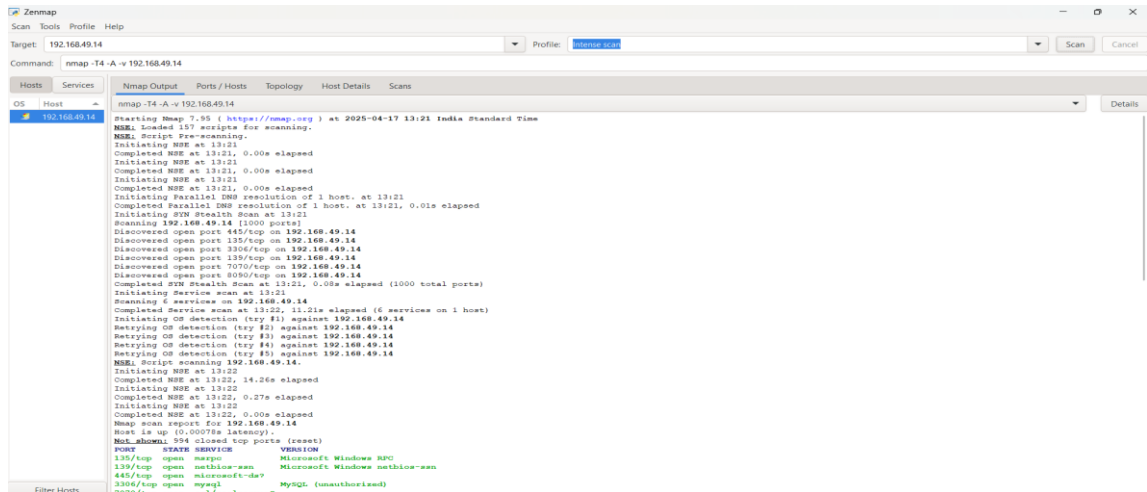
You can also get updates by liking [Nmap on Facebook](#) or following us [@nmap on Twitter](#).

Nmap is distributed with source code under [custom license terms](#) similar to (and derived from) the GNU General Public License, as noted in the [copyright page](#).

CMD :-

- C:\Users\Acer>nmap solvetic.com
- C:\Users\Acer>nmap -sV solvetic.com
- C:\Users\Acer>nmap -O solvetic.com
- :\Users\Acer>ipconfig


Put IP



```
zenmap
Scan Tools Profile Help
Target: 192.168.49.14
Command: nmap -T4 -A -v 192.168.49.14
Hosts: 192.168.49.14
Nmap Output:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-17 13:21 India Standard Time
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:21
Completed NSE at 13:21, 0.00s elapsed
Initiating NSE at 13:21
Completed NSE at 13:21, 0.00s elapsed
Initiating NSE at 13:21
Completed NSE at 13:21, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 13:21
Completed Parallel DNS resolution of 1 host. at 13:21, 0.01s elapsed
Initiating SYN Stealth Scan at 13:21
Scanning 192.168.49.14 [1000 ports]
Discovered open port 445/tcp on 192.168.49.14
Discovered open port 135/tcp on 192.168.49.14
Discovered open port 1360/tcp on 192.168.49.14
Discovered open port 139/tcp on 192.168.49.14
Discovered open port 10700/tcp on 192.168.49.14
Discovered open port 8080/tcp on 192.168.49.14
Completed SYN Stealth Scan at 13:21, 0.00s elapsed (1000 total ports)
Initiating Service scan at 13:21
Scanning 6 services on 192.168.49.14
Completed Service scan at 13:22, 11.21s elapsed (6 services on 1 host)
Initiating OS detection (try #1) against 192.168.49.14
Retrying OS detection (try #2) against 192.168.49.14
Retrying OS detection (try #3) against 192.168.49.14
Retrying OS detection (try #4) against 192.168.49.14
Retrying OS detection (try #5) against 192.168.49.14
NSE: Script scanning 192.168.49.14.
Initiating NSE at 13:22
Completed NSE at 13:22, 14.26s elapsed
Initiating NSE at 13:22
Completed NSE at 13:22, 0.27s elapsed
Initiating NSE at 13:22
Completed NSE at 13:22, 0.00s elapsed
Nmap scan report for 192.168.49.14
Host is up (0.0007s latency).
Not shown: 954 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  rdp          Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  smb          Microsoft smb
8080/tcp   open  mysql        MySQL (unauthenticated)
10700/tcp  open  http         Apache/2.4.18 (Ubuntu)
```

Steps :-

1. Download the Installer

- Go to the official Nmap website:
 <https://nmap.org/download.html>
- Under **Microsoft Windows binaries**, click on the link to download the **Latest stable** release self-installer: [nmap-7.95-setup.exe](#)

2. Run the Installer

- Locate the downloaded .exe file (usually in your **Downloads** folder).
- Double-click to launch the installer.
- If prompted by **User Account Control (UAC)**, click **Yes** to allow changes.

3. Installation Wizard

Follow the steps:

1. **Welcome Screen** – Click **Next**.
2. **License Agreement** – Accept and click **Next**.
3. **Select Components** – Make sure the following are checked:
 - Nmap
 - Ncat
 - Zenmap (GUI frontend, optional but useful)
 - Ndiff (for comparing scan results)
 - Npcap (required for packet sniffing/scanning)
4. **Choose Installation Location** – Leave it default or select a path, then click **Next**.
5. **Install Npcap** – A separate installer for **Npcap** will launch:
 - Choose **“Install Npcap in WinPcap API-compatible Mode”**
 - Leave other defaults checked
 - Click **Install**
6. After Npcap installs, Nmap installation continues and completes.

4. Finish and Launch

- Click **Finish** once installation is complete.
 - You can now use:
 - **Zenmap GUI** (shortcut will be on desktop/start menu)
 - **Command-line Nmap** via Command Prompt
-

5. Verify Installation

Open **Command Prompt** (cmd) and type:

nmap -v

You should see version information and confirmation that Nmap is installed properly.

6. Test Scan

Try scanning a test host:

nmap scanme.nmap.org