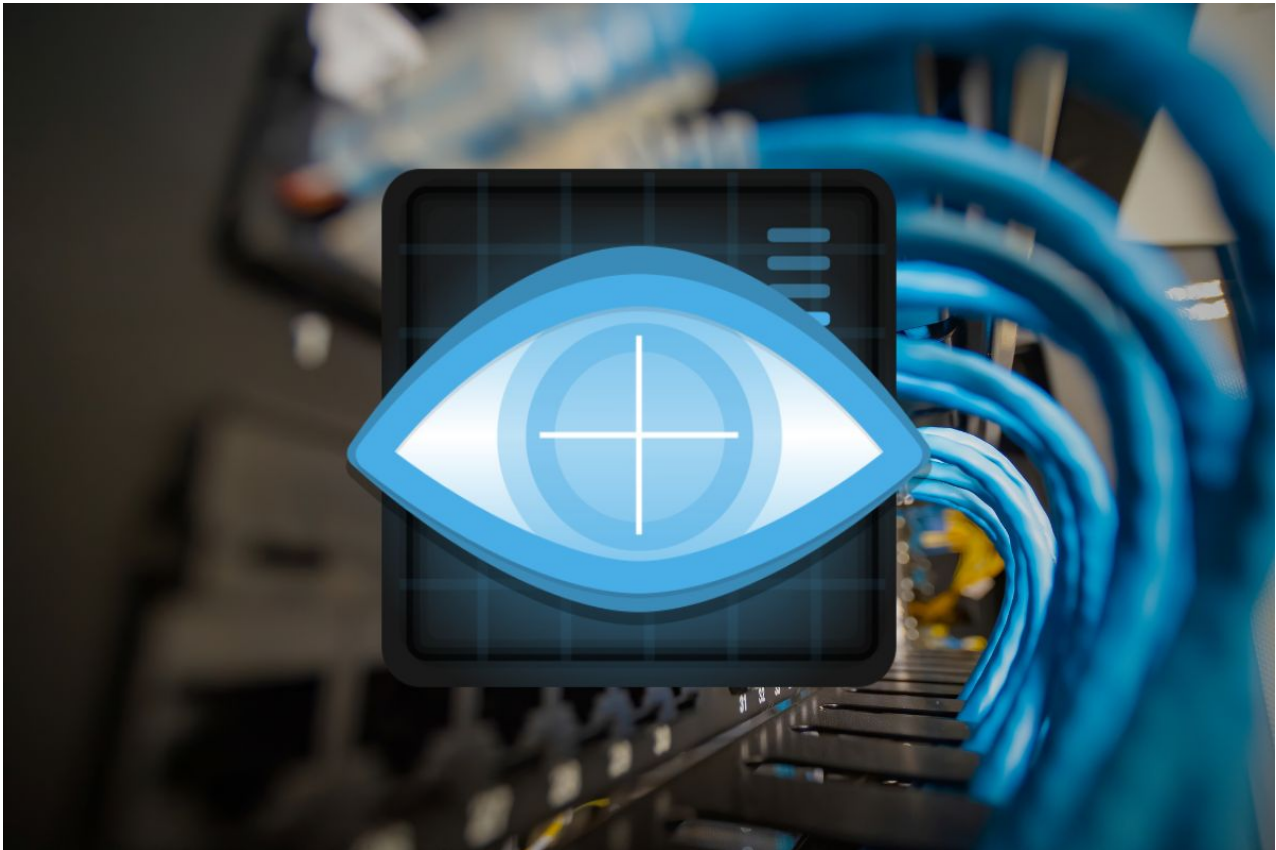


Getting Started with Zenmap on Kali Linux (Nmap GUI)

 infosecscout.com/install-zenmap-kali-linux

Patrick Fromaget



If you're using Kali Linux, you probably know about Nmap, the most popular security scanner tool. Nmap is great, but using it is not that intuitive, that's why Zenmap comes to life, to provide us with access to a GUI, that will simplify using Nmap when a desktop environment is available (like on Kali Linux). It's not preinstalled on Kali, but here is how to get it.

While Zenmap is no longer actively maintained, it's still available in the Kali Linux default repository. So, it can be installed with the system package manager (APT). It's also possible to download the sources from the website to get the latest version.

I tried it on my system, and will show you how to install it and get started with this tool on your own.

Master Linux Commands

Your essential Linux handbook

Want to level up your Linux skills? Here is the perfect solution to become efficient on Linux. **20% off today!**

[Download now](#)

How to install Zenmap on Kali Linux

Zenmap is available in the APT repository on Kali Linux, and can be installed in one single command line. It'll then be available with the other tools in the main menu.

Update your system

Master your cyber security skills:

Secure your spot in the Accelerator Program, with early access to exclusive resources.

Get 1000+ classes, unlimited mentorship, and more.

Before doing anything else, make sure your system is up-to-date, and the package manager sources is updated too, so we avoid any conflict in the next step.

You can do this by opening a terminal and typing:

```
sudo apt update
```

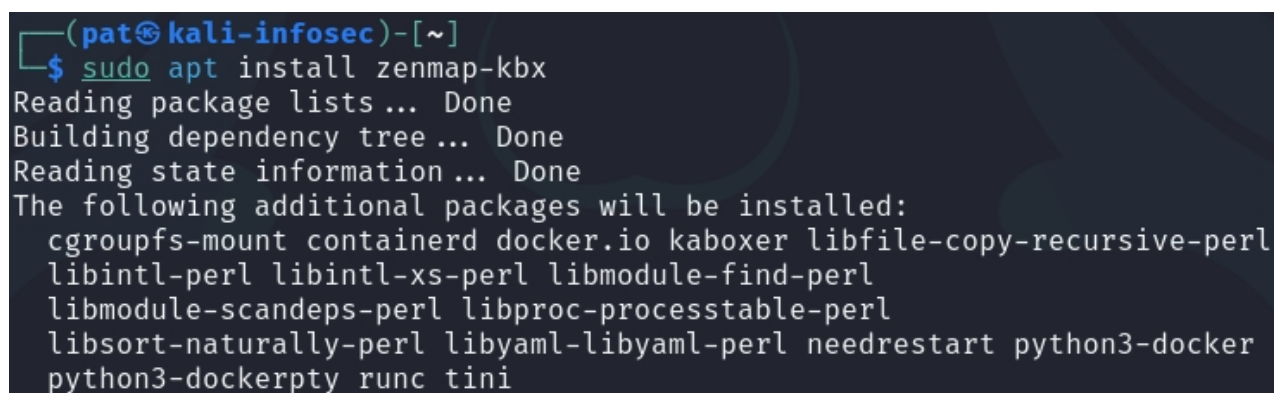
```
sudo apt upgrade
```

This will synchronize the package versions with the Kali Linux servers and download the new versions of the packages already installed on your system.

Install the main package

Once done, Zenmap can be installed with APT, using this command line:

```
sudo apt install zenmap-kbx
```

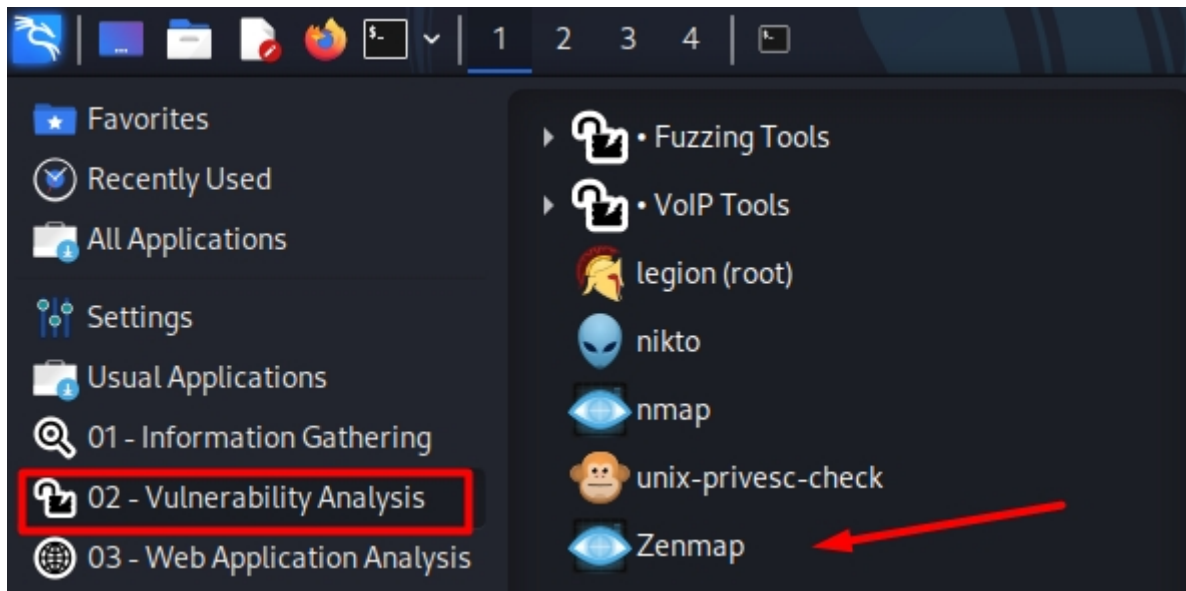


```
(pat@kali-infosec)-[~]  
$ sudo apt install zenmap-kbx  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  cgroupfs-mount containerd docker.io kboxer libfile-copy-recursive-perl  
  libintl-perl libintl-xs-perl libmodule-find-perl  
  libmodule-scandeps-perl libproc-processtable-perl  
  libsort-naturally-perl libyaml-libyaml-perl needrestart python3-docker  
  python3-dockerpty runc tini
```

As you can see in my screenshot, all dependencies are automatically installed at the same time, so you don't have to worry about anything else.

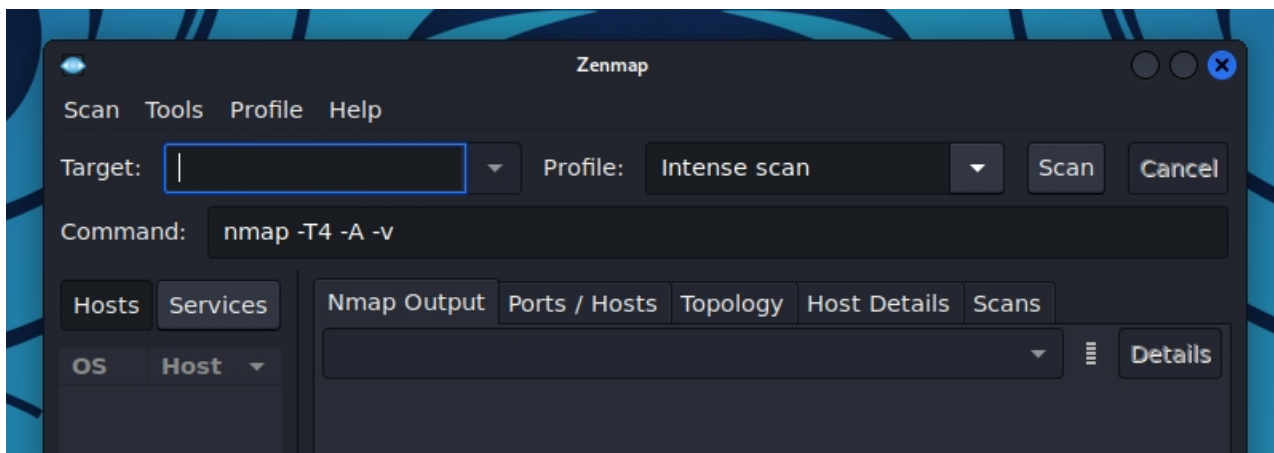
Start the application

Once the package installed, Zenmap will appear in the main menu, under "Vulnerability Analysis":



You can also use the search engine to find it quickly.

When you start it, the interface shows up, looking like that:



The installation wasn't complicated, right? I'll now give you a quick overview of what you can do once Zenmap is installed on Kali.

First steps with Zenmap on Kali Linux

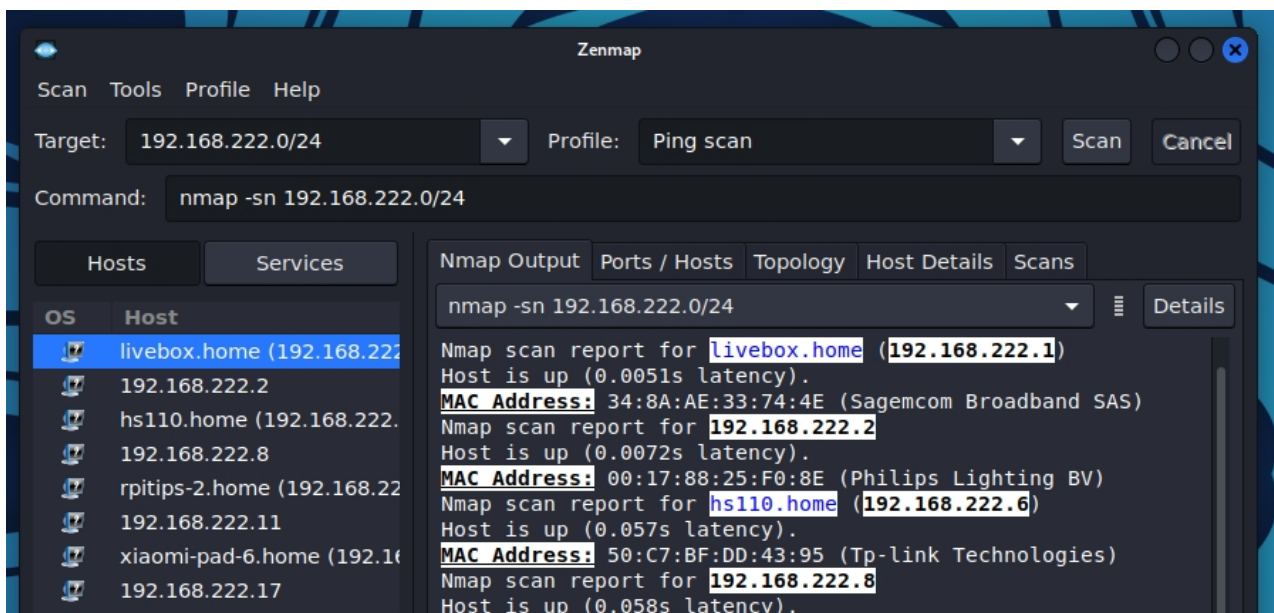
Overall, Zenmap offers the same functionality as its command-line counterpart (nmap), it's just easier to run commands, easier to analyze the results, and better looking (especially for topology and advanced audits).

Network scan

The first thing you can try is to run a network scan on your local network, for example.

To do this, enter a network range in the "Target" field (e.g. 192.168.1.0/24), select the scan type in the profile list (e.g. "Ping scan") and click "Scan" to start the process.

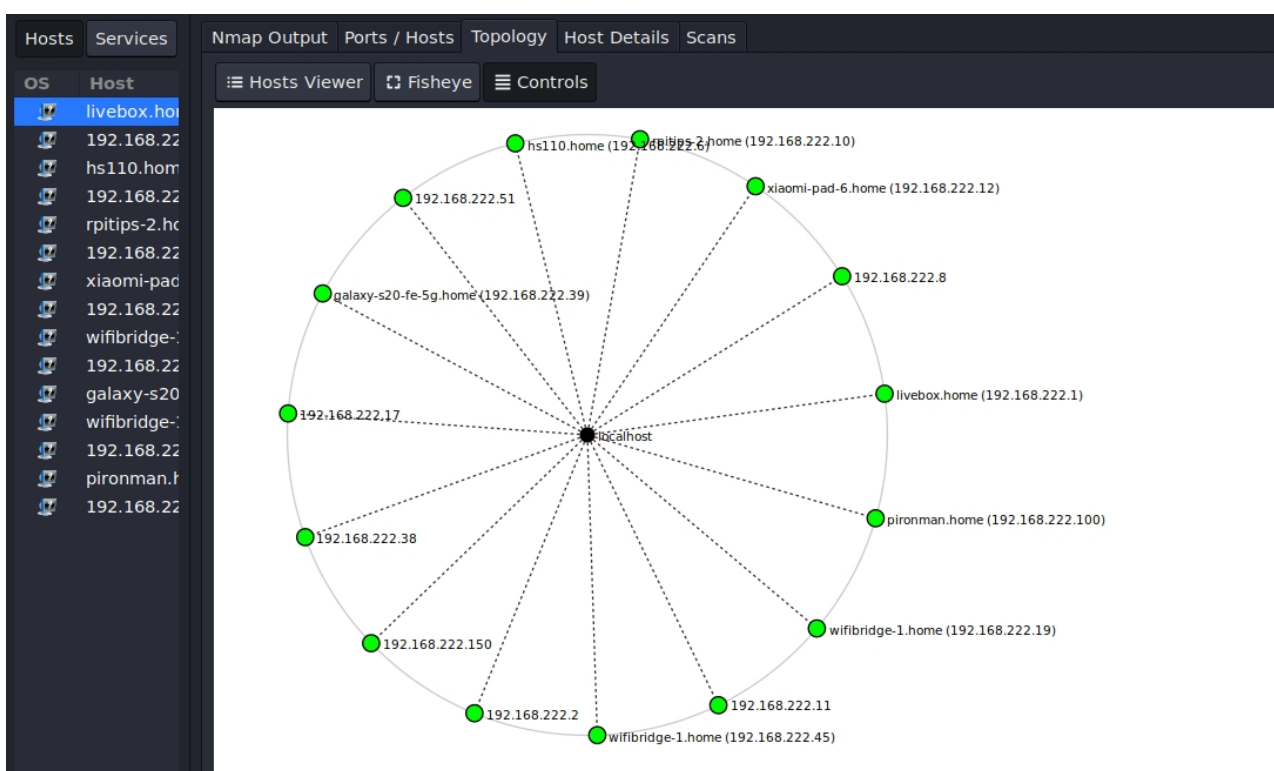
You'll see the corresponding nmap command filled in real-time below the form (if you want to use it in a terminal later), and the scan will start. After a few seconds, you should get a detailed report, looking like that:



On the right, I have the traditional Nmap output for this network scan, but it's also populating the other tabs that are exclusive to Zenmap. For example, on the left, I have a list of all hosts that I can now use for more in-depth scans.

Network topology

Having a GUI for Nmap adds some interesting features, like this network topology tab, where you can see your network scan in a chart:



I just did this on my local network, which is pretty basic (a router with dozens of devices), so it's not that useful, but you get the idea. It's great for getting a quick overview of a particular network.

Target scan

Once you have a better understanding of the network and hosts connected to it, you can do an advanced scan for each IP address, and view the summary under "Host details".

Hide your IP address and location with a free VPN:

[Try it for free now](#), with advanced security features.

2900+ servers in 65 countries. It's free. Forever.

I did it for a Raspberry Pi I have at home, here is what I got:

Host Status

- State: up
- Open ports: 2
- Filtered ports: 0
- Closed ports: 998
- Scanned ports: 1000
- Up time: 3043662
- Last boot: Thu Jan 4 21:12:10 2024

Addresses

- IPv4: 192.168.222.10
- IPv6: Not available
- MAC: B8:27:EB:CC:9E:FE

Hostnames

- Name - Type: rpitips-2.home - PTR

Operating System

- Name: Linux 5.0 - 5.3
- Accuracy: 99%

Ports used

- Port-Protocol-State: 22 - tcp - open
- Port-Protocol-State: 1 - tcp - closed
- Port-Protocol-State: 38824 - udp - closed

OS Classes

Type	Vendor	OS Family	OS Generation	Accuracy
general purpose	Linux	Linux	5.X	99%

At a glance, I can see the device state, IP address, uptime, operating system, etc.

I can even see a list of the opened ports by clicking on the "Ports / Hosts" tab:

Nmap Output	Ports / Hosts		Topology	Host Details	Scans
	Port	Protocol	State	Service	Version
✓	22	tcp	open	ssh	OpenSSH 8.4p1 Raspbian 5+deb11u1 (protocol 2.0)
✓	80	tcp	open	http	Apache httpd 2.4.54 ((Raspbian))

All this without typing any command line, great, right?

Alternatives to Zenmap

As mentioned earlier, Zenmap is no longer actively maintained, and it might be a good idea to look at alternatives, just in case it disappears from the repository one day.

Here are some of the ones you can try that I have already tested on this site:

- [Mastering Netcat on Kali Linux: A beginner's guide](#)
- [How to Install Nessus on Kali Linux: A quick & easy guide](#)
- [How To Install & Use Wireshark On Kali Linux](#)

Whenever you're ready for more security, here are things you should think about:

- **Break free from Gmail**: You should be able to choose what happens to your data. With Proton, only you can read your emails. [Get private email](#).

- **Protect yourself online**: Use a high-speed Swiss VPN that safeguards your privacy. Open-source, no activity logs. [Get Proton VPN risk-free](#).

- **Master Linux commands**: A sure method to learn (and remember) Linux commands. Useful ones only, one at a time, with clear explanations. [Download the e-book](#).