

Forum:[Hack Forums](#)

Thread: [{Tutorial} Zenmap - A GUI of Nmap - A Beginners Guide](#)

Pr0m3th3us - March 17, 2025, 9:49 pm

This TUT is for beginners who want a GUI version of Nmap and may be intimidated by command lines. If you like me you get lost sometimes looking at endless lines of text in the terminal. I tend to read text on a monitor by scanning for bullet points instead of going word for word (bad habit). Alas! with Kali Linux we have a lot more GUI programs to help slightly autistic people like us! This is part 1 of a 3 part series.

Quick Overview Nmap as most know, is the main tool used for network security professionals and hackers of all colored hats. Used mainly for network discovery and security auditing, the tool is very powerful and extends the usefulness of Nmap by having the ability to compare scans, allows admins to easily track new hosts or services appearing on the networks, and you can save profiles to make it easy to run scans to streamline your work.

Getting started Zenmap comes standard with Kali Linux but I will include the code for Debian/Ubuntu if you need to install it.

Code `sudo apt update`

`sudo apt upgrade`

`sudo apt install zenmap`

It is located under 02 - Vulnerability Analysis, find it and open it.

Performing a Quick Scan

First we will enter your machine's IP "192.168.1.237" in the Target field, if you do not know your local IP then open your terminal and type "ifconfig" so see it. You can also put in multiple targets separated by a space.

In the "profile" field we are going to select the type of scan we are wanting. This is where your custom profile scans will be saved, there are many types pre-saved such as ping, regular, intense, and quick scans. We are going for quick scan this time.

In the "command" field it will show you the Nmap command you basically built from selecting the other fields.

On the left side we see the host/s, the icon next to the host indicates the OS of the machine if Zenmap can obtain it. Once you select a host you can click the "ports/hosts" tab and see the specific ports of that host. You can also click on "host details" tab and get a more detailed list of info on each host depending on the scan type.

If you click on the "services" tab you can see which host/s (will show multiple hosts later) is running a specific service.

Once you have run a scan and want to save it you can just click the "scan" menu in the top left and

select save scan, or use CTRL S. You can save in XML format or in TXT format.

What Info a Quick Scan Shows

- Open Ports: Identifies which ports are open on the target system.
- Basic Service Detection: Provides basic information about the services running on those open ports, but usually without detailed version numbers.
- Host Discovery: Determines whether the target is active and reachable on the network.
- Limited OS Detection: May provide some basic information about the operating system but not as detailed as an intense scan.
- Reduced Scan Time: The quick scan is optimized for speed, so it completes much faster than more comprehensive scans.

This info is very useful when working in the Networking field, such as network security, cybersecurity network engineer, or even working at a help desk position and trying to diagnose network issues.

Scanning Your Network for All Devices

Next we will enter into the "target" field, "192.168.1.0/24". This specifies a target IP address range to scan, which is the subnet from 192.168.1.0 to 192.168.1.255. So for instance if you live in an apartment complex and you want to see if someone is stealing your Wifi.

Then for the profile we will use "ping scan" and press scan. This will ping all devices connected to the network. As you can see i have 3 computers, 1 tv, 1 phone, and my router.

What Info A Ping Scan Shows

- Host Availability: Identifies which IP addresses are active (i.e., responding to ICMP echo requests).
- Network Reachability: Confirms if the target network is reachable from the scanning machine.
- Response Times: Provides information on the latency or response times from the active hosts.
- Basic Host Information: May include the MAC address of the responding devices if available.

Comparing Multiple Scans One of the most useful features of Zenmap is comparing scans from different instances or times. So for instance you can run the same scan daily and compare results to see if there are any changes to your network.

To view comparisons go to the "tools" menu, and click compare results. You will then select an "A" scan and "B" scan. Once you load them it will open the comparison and show the output in color coded format for easy identification of differences.

In my next tutorial i will go over the Topo maps, intense scans and more!

Disclaimer:

The information provided on this tutorial is for general informational purposes only and does not constitute advice of any kind. While we strive to ensure the accuracy and reliability of the information presented, we make no warranties or representations, express or implied, regarding its completeness, accuracy, timeliness, or suitability for any particular purpose. Hackforums shall not be liable for any loss or damage of any kind arising from the use of or reliance on the information provided. We encourage you to consult with qualified professionals before making any decisions

based on this information

<https://hackforums.net/showthread.php?tid=6294576>

Hungry4Knowledge - March 18, 2025, 2:44 am

Just what I needed, as I am at the nmap section on THM. Thanks.

Bastille - March 18, 2025, 3:29 am

Very nice tutorial man, a good way for beginners to learn how port scanning works

JoseMar - March 18, 2025, 7:25 am

I used it in the past when I was starting to hack, but now I exclusively use Nmap. By the way, this is HQ content, mate; keep it up! Cheers!?

Pr0m3th3us - March 18, 2025, 4:24 pm

(Mar 17, 2025 09:50 PM)php Wrote: [\[CITE\]](#) Very HQ tutorial thank you!

I'm curious in your experience, what custom scan profiles have you found most useful for everyday security monitoring that might not be obvious to newcomers? The comparison feature seems particularly valuable for tracking network changes over time.

I honestly have only used the pre loaded profiles ?

(Mar 17, 2025 11:21 PM)vrs Wrote: [\[CITE\]](#) Interesting tutorial, thanks for writing this up. I often consider myself a GUI wizard as I do not know any commands even inside windows such as ping & trace etc. Looking forward to seeing the topography demonstrations in a real world network like you've simulated in your lab here.

Thanks, my whole life is a simulation.

(Mar 18, 2025 02:44 AM)Hungry4Knowledge Wrote: [\[CITE\]](#) Just what I needed, as I am at the nmap section on THM. Thanks.

That's awesome bro!

(Mar 18, 2025 03:29 AM)Bastille Wrote: [\[CITE\]](#) Very nice tutorial man, a good way for beginners to learn how port scanning works

Thanks, i will go over common ports and what they mean in the next TUT.

(Mar 18, 2025 07:25 AM)JoseMar Wrote: [\[CITE\]](#) I used it in the past when I was starting to hack, but now I exclusively use Nmap. By the way, this is HQ content, mate; keep it up! Cheers!?

Thanks, Care to explain why that is? and the pros/cons.

JoseMar - March 18, 2025, 4:37 pm

(Mar 18, 2025 04:24 PM)Rustoleum Wrote: [\[CITE\]](#) Thanks, Care to explain why that is? and the pros/cons.

Nmap

Pros:

Faster execution

More control with advanced scripting (NSE)

Lightweight, no GUI overhead

Preferred for automation and scripting

Cons:

The steeper learning curve for beginners

Requires memorizing commands and flags

Zenmap (GUI for Nmap)

Pros:

User-friendly, great for beginners

Visual representation of scan results

Easier to manage and compare scans

Cons:

Slightly slower due to GUI overhead

Lacks full flexibility of command-line options

Not ideal for automation

Pr0m3th3us - March 18, 2025, 4:41 pm

(Mar 18, 2025 04:37 PM)JoseMar Wrote: [\[CITE\]](#) Nmap

Pros:

Faster execution

More control with advanced scripting (NSE)

Lightweight, no GUI overhead

Preferred for automation and scripting

Cons:

The steeper learning curve for beginners

Requires memorizing commands and flags

Zenmap (GUI for Nmap)

Pros:

User-friendly, great for beginners

Visual representation of scan results

Easier to manage and compare scans

Cons:

Slightly slower due to GUI overhead

Lacks full flexibility of command-line options

Not ideal for automation

Nice thanks, hopefully beginners see this post! Appreciate it!