

Forum:[Hack Forums](#)

Thread: [{Tutorial} ZenMap - A GUI of Nmap - An Intermediate Guide](#)

Pr0m3th3us - March 19, 2025, 8:10 pm

In this Intermediate thread we will go over more in-depth uses of Zenmap. Which includes Intense Scans, Ports/Hosts, TCP vs UDP, and Topo maps. As mentioned this is a very powerful tool for hackers of all types and is highly underestimated by many beginners. After all when and if you gain access to a network you want to know as much as possible about it before you proceed, correct?

Intense Scans

An intense scan on Zenmap uses aggressive scanning techniques, which gives us a lot more info about the machine or network we are scanning. This will take longer, but its worth it.

What Info An Intense Scan Shows

1. Host Discovery (Ping Scan)

Identifies if the target is online.

Uses ICMP Echo Requests, TCP SYN, and ACK packets to detect live hosts.

2. Port Scanning (Service Detection)

Scans for open, closed, and filtered ports.

Uses SYN Scan (-sS) for stealthy port probing.

Identifies the state of ports:

Open: Actively accepting connections.

Closed: No service running but reachable.

Filtered: Firewalled or blocked by security measures.

3. Service and Version Detection

Identifies services running on open ports (e.g., HTTP, SSH, FTP).

Detects the software version and potential vulnerabilities.

Example output:

Code 22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (protocol 2.0)

80/tcp open http Apache httpd 2.4.29 ((Ubuntu))

4. OS Detection

Tries to determine the operating system running on the target.

Uses TCP/IP fingerprinting to analyze response behaviors.

Example:

Code Running: Linux 4.X

OS CPE: cpe:/o:linux:linux_kernel:4

5. Traceroute

Shows the path (hops) packets take to reach the target.

Helps detect firewalls, proxies, or routing anomalies.

6. Script Scanning (NSE - Nmap Scripting Engine)

Runs various scripts to detect vulnerabilities and extract additional info.

Examples: Detects default credentials, Identifies outdated services, Enumerates SMB shares on Windows machines.

7. Reverse DNS Resolution

Attempts to find the domain name associated with the IP.

In part 3 we will be using a lot of this info to find vulnerabilities on a specific machine in the network. But for now just scan your networks/devices and read through the lines of code and look at all the info under different tabs to get a better understanding of what is entailed. Compare 2 machines and see where they differ, you may spot something useful!

What Is a Port, and What Do They Mean?

Ports are logical connections that are used by programs and services to exchange information. they range from 0-65535. They are broken down into 3 categories.

1. Well-Known Ports (0 – 1023)
2. Registered Ports (1024 – 49,151)
3. Dynamic / Private / Ephemeral Ports (49,152 – 65,535)

A port specifically determines a program or service on a computer that is going to be used. Ports are opened by some programs, operating systems, or you can manually open them in your router. In Zenmap you can see what ports are open, using the Ports/Hosts tab. As you can see i have 2 ports open on this PC. Ports 22 and 8080.

If you go to <https://google.com> in your browser your machine will convert the domain name to googles IP address and add port 443 after the IP like this "215.114.85.17:443". Once the IP has been found its all up to the port after that, googles server will see "443" and forward it to googles web service so you can retrieve the page. Here are some common ports.

Port 20 & 21 (FTP - File Transfer Protocol)

- 20: Data transfer
- 21: Command/control

Port 22 (SSH - Secure Shell)

Used for secure remote login and file transfers (SCP/SFTP).

Port 25 (SMTP - Simple Mail Transfer Protocol)

Used for sending emails (commonly replaced by ports 587/465 for secure mail).

Port 53 (DNS - Domain Name System)

Resolves domain names to IP addresses (also uses UDP).

Port 80 (HTTP - Hypertext Transfer Protocol)

Standard web traffic (insecure).

Port 110 (POP3 - Post Office Protocol v3)

Used for retrieving emails from a server.

Port 143 (IMAP - Internet Message Access Protocol)

Used for email retrieval and synchronization across multiple devices.

Port 443 (HTTPS - Secure HTTP)

Secure web browsing using SSL/TLS encryption.

Port 3389 (RDP - Remote Desktop Protocol)

Used for remote desktop connections to Windows PCs.

Port 3306 (MySQL Database)

Used for database management and connections.

Knowing what ports are being used on what machine is very useful. For instance if you are in your neighbors network and you see port 443 is open that means the machine may be hosting a service that uses HTTPS. Zenmap has a line under the Ports/Hosts tab called "Service", this will usually list what service that port is using so you don't have to google it.

TCP And UDP

Whenever a computer wants to communicate with another computer it needs to be reliable so it can guarantee the data is received correctly, this is where TCP (Transmission Control Protocol) comes in. TCP is a connection oriented protocol, which means it must first acknowledge a session between the 2 machines. It does this by using a "3 way handshake". The first step is your machine will send a message called a "syn", next the receiving machine will send back an acknowledgment called a "syn ack", finally your machine will send another message called "ack received" back to the target machine.

UDP (User Datagram Protocol) on the other hand is like the red headed stepchild of the two, it is also for sending and receiving data but it is connection-less. It does not establish a connection and does not guarantee data delivery. Think of it as "fire and forget".

After you have run your intense scan, click on a machine under your Hosts tab on the left side. You will see under your Ports/Hosts tab there is a line named "protocol". This is where you can see what protocol each port on that machine is using. You may see "filtered" under the "state" line. This means a firewall, filter, or other network obstacle is blocking the port, preventing the scanner from

determining if the port is actually open or closed.

Topology Map

This is by far one of the best parts of Zenmap in my opinion. Zenmap's "Topology" tab provides an interactive, animated visualization of the connections between hosts on a network. Hosts are shown as nodes on a graph that extends radially from the center. Click on a host and it becomes the new center and see what the network looks like from its point of view. The graph rearranges itself in a smooth animation to reflect the new view of the network. Run a new scan and every new host and network path will be added to the topology automatically.

Each regular host in the network is represented by a little circle. The color and size of the circle is determined by the number of open ports on the host. The more open ports, the larger the circle. A white circle represents an intermediate host in a network path that was not port scanned. If a host has fewer than three open ports, it will be green; between three and six open ports, yellow; more than six open ports, red.

If a host is a router, switch, or wireless access point, it is drawn with a square rather than a circle.

Network distance is shown as concentric gray rings. Each additional ring signifies one more network hop from the center host.

Connections between hosts are shown with colored lines. Primary traceroute connections are shown with blue lines. Alternate paths (paths between two hosts where a different path already exists) are drawn in orange. Which path is primary and which paths are alternates is arbitrary and controlled by the order in which paths were recorded. The thickness of a line is proportional to its round-trip time; hosts with a higher RTT have a thicker line. Hosts with no traceroute information are clustered around localhost, connected with a dashed black line.

If there is no RTT for a hop (a missing traceroute entry), the connection is shown with a blue dashed line and the unknown host that makes the connection is shown with a blue outline.

In part 3 we will go over how to find vulnerabilities, what they mean, 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

Pr0m3th3us - March 19, 2025, 8:20 pm

(Mar 19, 2025 08:16 PM)vrs Wrote: [\[CITE\]](#) Handsome looking guide you've got here Rustmaster, great work!

Good to see your virtual lans are now shimmering in and out of the ether.
Thanks!

What virtual lans? I don't even own a computer....allegedly...?

JoseMar - March 20, 2025, 2:36 am

I appreciate this thread [Pr0m3th3us](#) It's packed with valuable insights into Zenmap's advanced features. The breakdown of intense scans, port states, and service detection is beneficial, and the explanation of the topology map provides a great visual understanding of network structures. It's an excellent resource for anyone looking to improve their network reconnaissance skills!
Keep up your great work! +10 Popularity
?

Pr0m3th3us - March 20, 2025, 3:13 am

(Mar 20, 2025 02:36 AM)JoseMar Wrote: [\[CITE\]](#) I appreciate this thread [Pr0m3th3us](#) It's packed with valuable insights into Zenmap's advanced features. The breakdown of intense scans, port states, and service detection is beneficial, and the explanation of the topology map provides a great visual understanding of network structures. It's an excellent resource for anyone looking to improve their network reconnaissance skills!
Keep up your great work! +10 Popularity
?

Thanks, I need to add a couple of things to the legend for the topology which I will do tomorrow!

Bastille - March 20, 2025, 5:12 am

Really nice thread !

The first part of it about Zenmap is similar to nmap but with a GUI, however I wasn't even aware that the Graph feature existed on Zenmap, I'm not familiar with this version of Nmap. That was nice to go beyond the tool and approach aspect such as ports, TCP/UDP protocols, and so on, so at least people beginning understand what thet ACTUALLY do, which is almost never the case when they start (we all have been SK back in the days tho ..)

That can be really useful for reports or to understand the composition of a network.