

Zenmap is a tool that allows users of it to see what ports are open, what operating system is being used, see the topology of the network, and more. Zenmap is the GUI version of the very popular Nmap tool. Nmap uses a command line making it less attractive and slightly more difficult to understand then Zenmap. Using this tool can allow network administrators to analyze their entire network to find vulnerabilities and device information.

To begin with Zenmap needs a target to scan. For example, the loopback address (127.0.0.1) scans the user’s current machine. To scan a specific network, the user could put something like 192.168.100.\*. Once a target network has been chosen, a type of scan has to be selected. There are a few pre-configured profiles that have pre-set scan types such as a simple ping command. These profiles can be altered by the user using the profile dropdown menu or by changing the command line input. There are a number of scanning options that can be used by the user available for this tool. After a network target is selected and a profile is selected, the user can scan the network. Hosts show up in the left column and information fills up the larger middle section of the GUI.

After the scan there are some different tabs available to be selected and analyzed. The first is Nmap Output which is the default tab. It shows the output of the command. The output is general text information such as network hosts, ports open, and other helpful information. The second tab is Posts/Hosts. This tab shows what ports are open, what protocol is used, it’s state, and it’s version on each hosts. The next tab is the Topology tab. This tab is especially useful for network audits. It shows the entire topology of the network in a graphical format. Using the loopback address only shows one address since there is only one host. The next tab is Host Details. This tab gives users specific information on a given host. The host can be selected on the left pane of the GUI. The Host Details tab shows information like its status, its address hostname, and its operating system. The final tab is Scans. Scans shows a list of all of the scans launched with Zenmap.

Zenmap finds out this information using various techniques. To find out a systems operating system, Zenmap uses TCP/IP fingerprinting. By sending various TCP and UDP packets Zenmap compares all of the bits it receives back to a large database of more than 2600 operating systems and sees if the bits match any of the known operating systems fingerprints. To find out the network hosts, it depends on the options selected. It generally finds hosts by sending ICMP echo requests, TCP SYN packet to port 443, a TCP ACK packet to port 80, and an ICMP timestamp request. There are many ways to discover ports that Zenmap uses. The different techniques can make it easier to locate open and vulnerable ports. The most basic technique is a TCP SYN scan. It is most used since it is very fast making it easy to scan a large network while being unobtrusive. A TCP SYN scan essentially sends a SYN packet to ports and if a port replies with an ACK then it is open.

Zenmap can be used to perform many basic network administrative tasks. It can allow the users to perform a network audit on their networks by identifying the sources that are connecting to it. It is also used for identifying open ports for weaknesses and vulnerabilities or to prepare for an audit. Another use is to map a network and find out its efficiency.

Just like many network analysis tools, it is possible that Zenmap could be used for malicious practices. Due to the fact that it scans open ports, it is possible for malicious users to find weaknesses and vulnerabilities in networks. Users could also find out what operating systems are being used on the network. The operating system information can be used for attacks if there are any known vulnerabilities in the operating system version. To combat it however, network administrators can use Zenmap to find out if there are any unauthorized users on the network.

Zenmap is a powerful tool that makes it easy for network administrators to monitor their networks. It is simple to use and easy to comprehend. It also gives a large amount of data so that network administrators can maximize their networks security. However, like most network analysis tools, it can be used for malicious practices. It can easily allow hackers to find out users system information and what ports are open. This allows them to better prepare for an attack on any given computer in the network. While it may be a harmful tool, the good outweighs the bad and Zenmap has become one of the most popular network analysis tools available.

Wallen, Jack. *Zenmap Tutorial: Audit your Networks using NMap GUI.* Linux.com <https://www.linux.com/learn/zenmap-tutorial-audit-your-networks-using-nmap-gui>

*NMap Network Scanning.* NMap.org.<https://nmap.org/book/zenmap-results.html#zenmap-tab-topology>

Wallen, Jack. *Map your Network with Zenmap.* Ghacks.net <http://www.ghacks.net/2009/08/09/map-your-network-with-zenmap/>