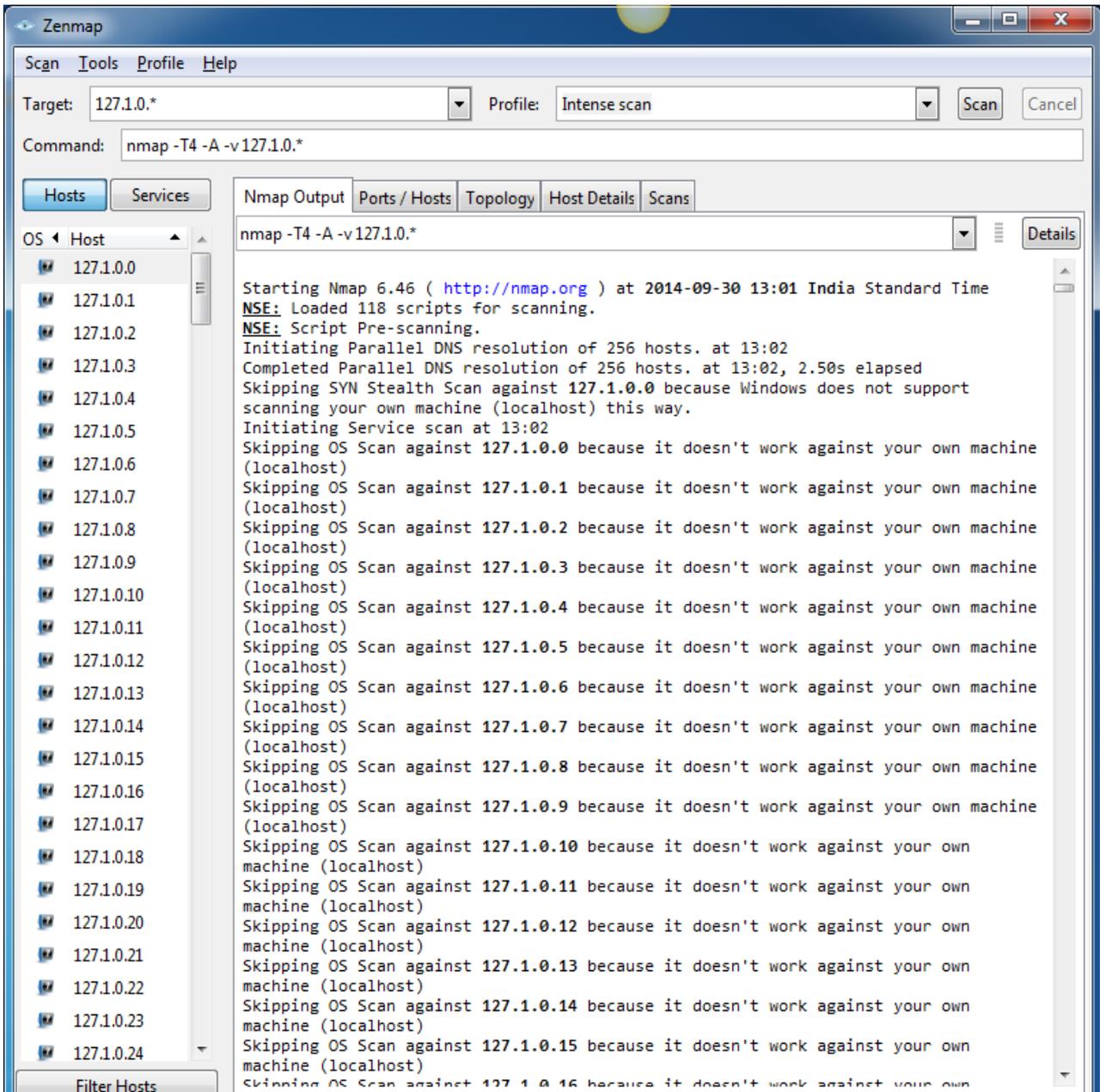


## Using Nmap-Zenmap GUI

Scanning Multiple IPs: Enter the Target IP address range and Select the type of scan

**I. Nmap Output:** This is the default tab and shows the output of the command.

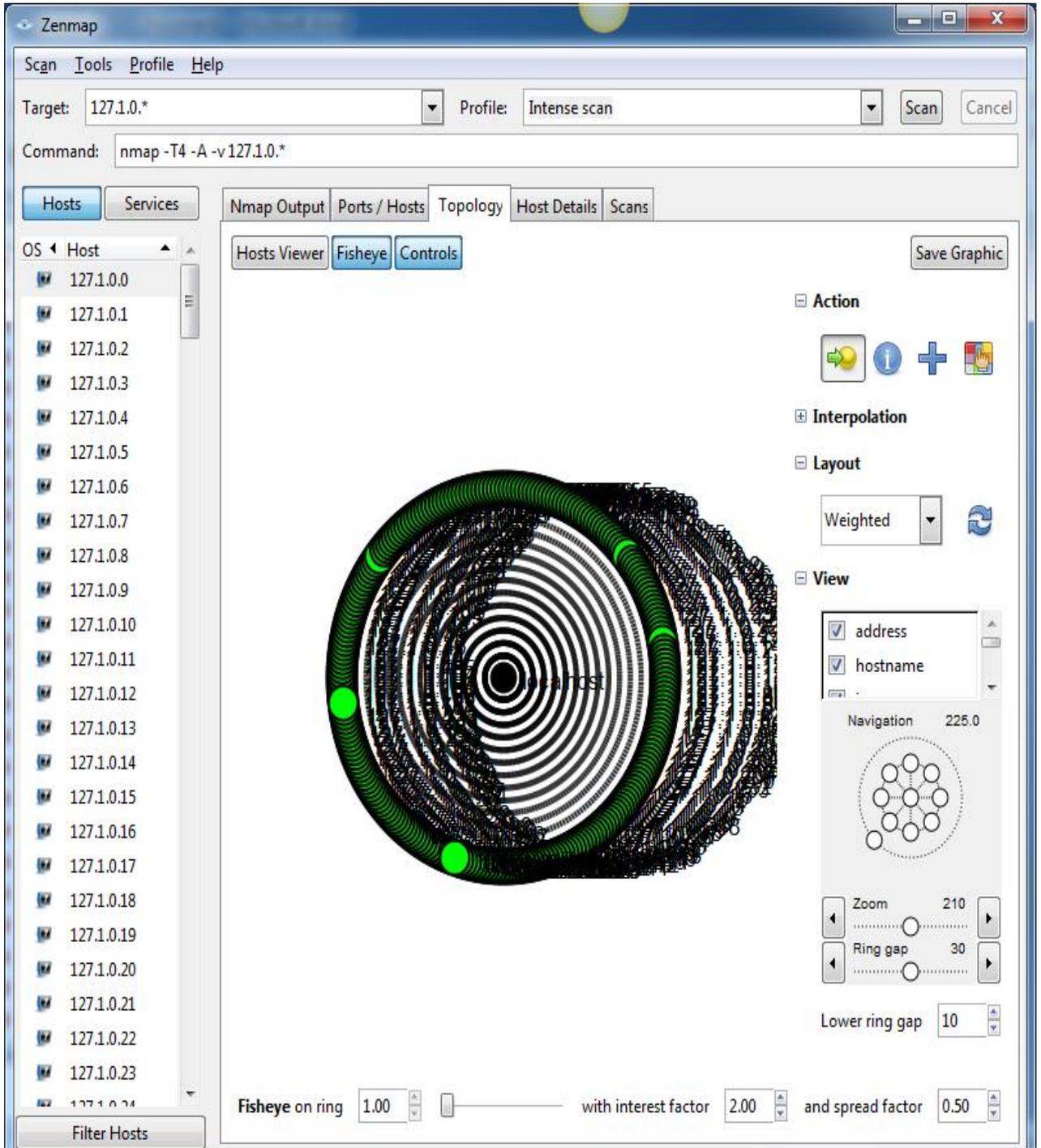


## II. Ports/Hosts: This tab shows you what ports are open on what hosts.

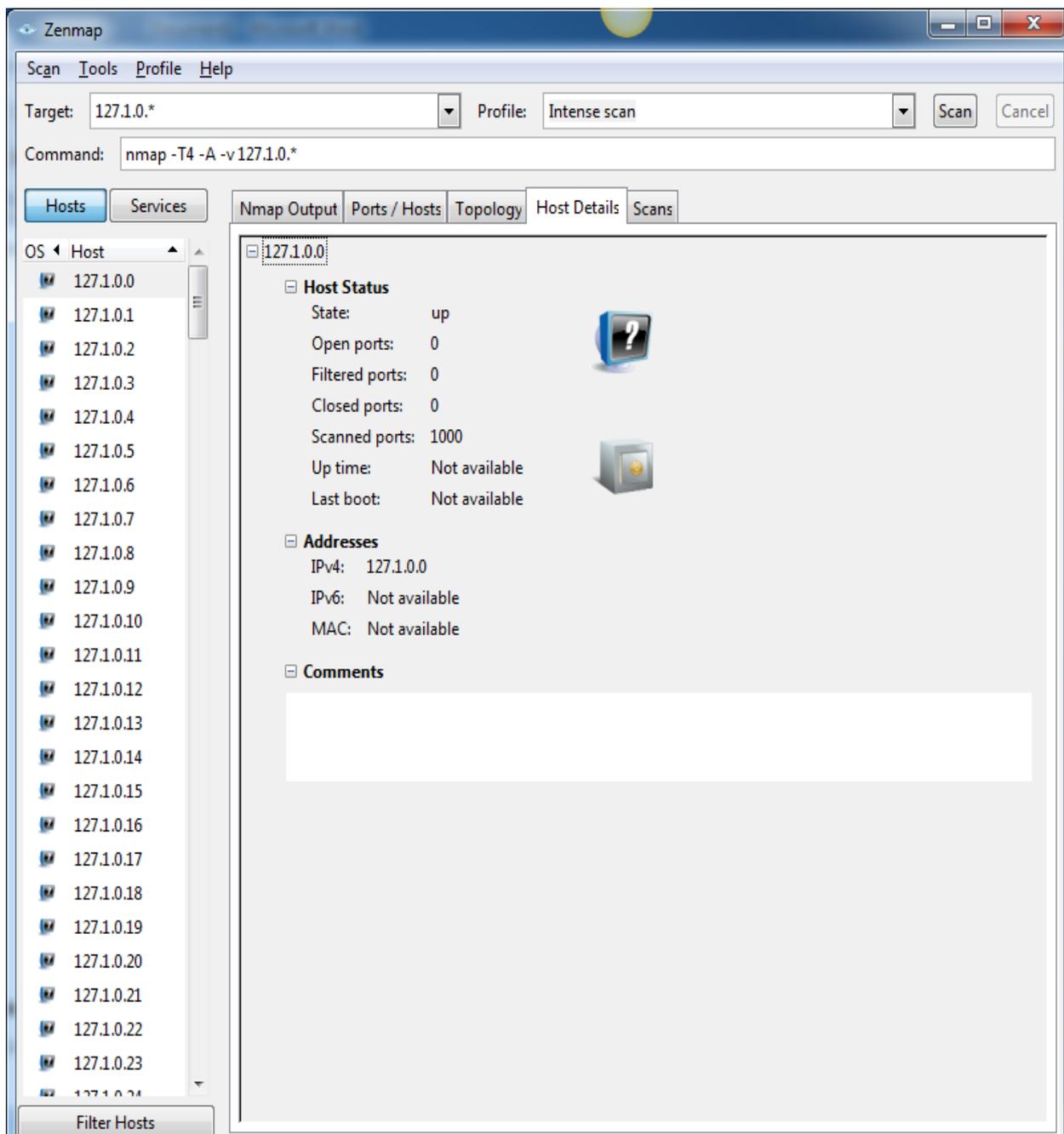
The screenshot shows the Zenmap application window. At the top, there are menu options: Scan, Tools, Profile, and Help. Below the menu, the Target is set to 127.1.0.\* and the Profile is Intense scan. The Command field contains nmap -T4 -A -v 127.1.0.\*. The main interface has several tabs: Hosts, Services, Nmap Output, Ports / Hosts, Topology, Host Details, and Scans. The 'Ports / Hosts' tab is active, showing a list of hosts on the left and a table of open ports on the right.

OS	Host	Port	Protocol	State	Service	Version
	127.1.0.0	1	tcp	open	tcpmux	
	127.1.0.1	3	tcp	open	compressnet	
	127.1.0.2	4	tcp	open	unknown	unknown
	127.1.0.3	6	tcp	open	unknown	unknown
	127.1.0.4	7	tcp	open	echo	
	127.1.0.5	9	tcp	open	discard	
	127.1.0.6	13	tcp	open	daytime	
	127.1.0.7	17	tcp	open	qotd	
	127.1.0.8	19	tcp	open	chargen	
	127.1.0.9	20	tcp	open	ftp-data	
	127.1.0.10	21	tcp	open	ftp	
	127.1.0.11	22	tcp	open	ssh	
	127.1.0.12	23	tcp	open	telnet	
	127.1.0.13	24	tcp	open	priv-mail	
	127.1.0.14	25	tcp	open	smtp	
	127.1.0.15	26	tcp	open	rsftp	
	127.1.0.16	30	tcp	open	unknown	unknown
	127.1.0.17	32	tcp	open	unknown	unknown
	127.1.0.18	33	tcp	open	dsp	
	127.1.0.19	37	tcp	open	time	
	127.1.0.20	42	tcp	open	nameserver	
	127.1.0.21	43	tcp	open	whois	
	127.1.0.22	49	tcp	open	tacacs	
	127.1.0.23	53	tcp	open	domain	
	127.1.0.23	70	tcp	open	gopher	

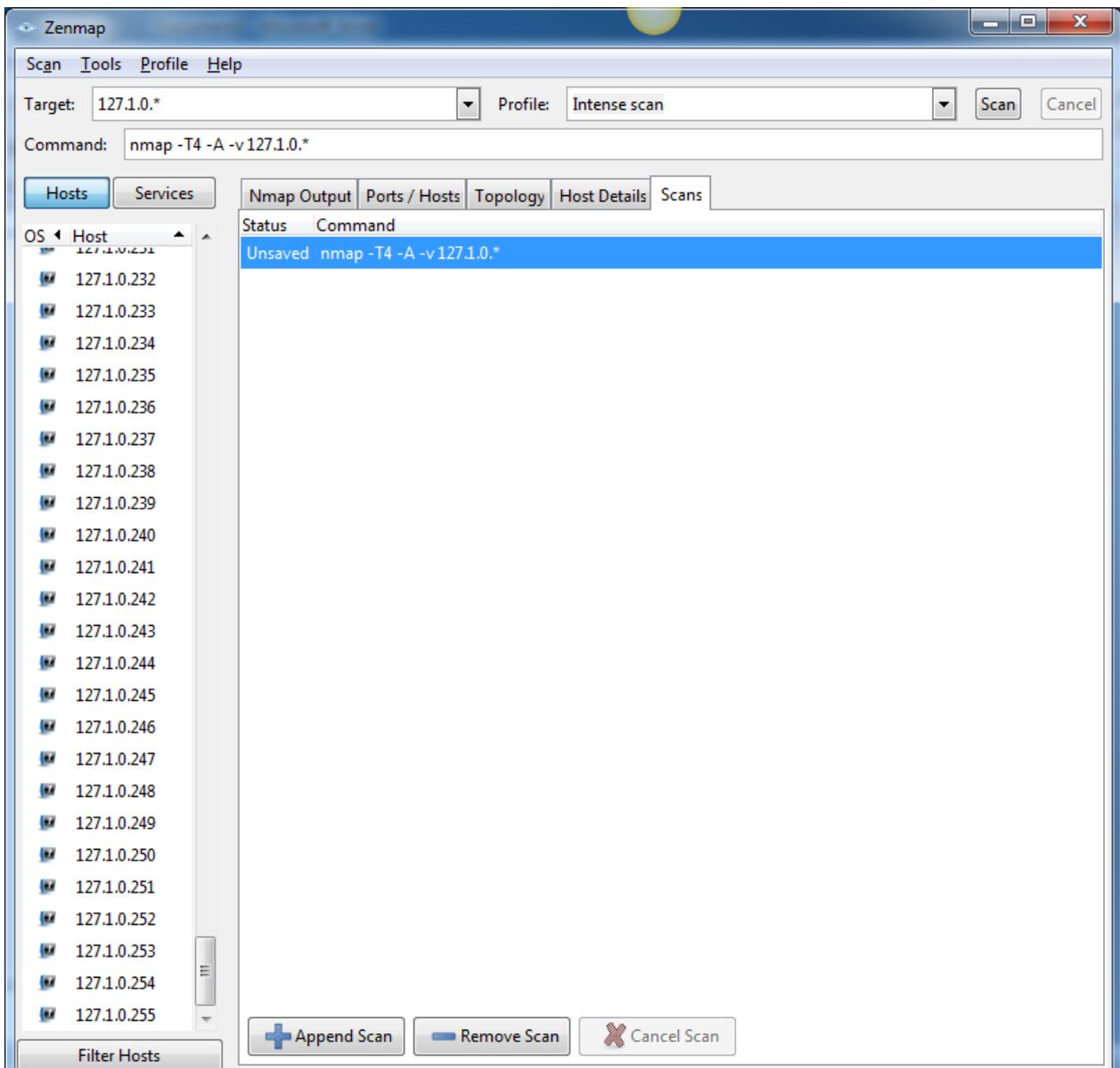
**III. Topology:** This tab is a must-use for audits as it shows the actual topology of your n/w.



**IV. Host details:** This tab will give you specific information about a selected host. To select a host you simply select the desired target from the left pane where all of the IP addresses or host names are listed.



**V. Scans:** This tab lists all of the scans you have executed. Most of these will be unsaved scans. You can, of course, select one of your past scans and re-run it by selecting said scan and clicking the Scan button.



The Zenmap tool is actually a graphical front end for the very popular Nmap command line tool. Nmap is an open source tool for network security and auditing. Although Nmap is incredibly powerful, when working with larger networks most administrators do not want to work with command line only tools. And besides, as they say "A picture is worth a thousand words". In this case that is very much true because Zenmap will give you an interactive graphical map of your network.