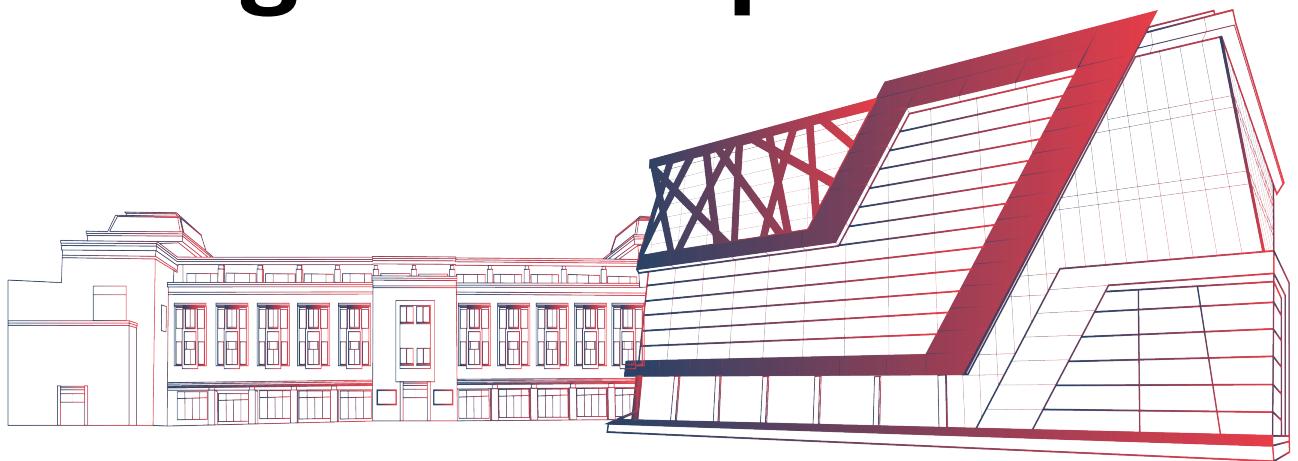


# Scanning- Zenmap



# Zenmap Tool

Zenmap is the **official graphical user interface (GUI)** for the Nmap Security Scanner.

It is a **multi-platform, free and open-source application** designed to make Nmap **easy to use for beginners** while providing **advanced features for experienced Nmap users**.

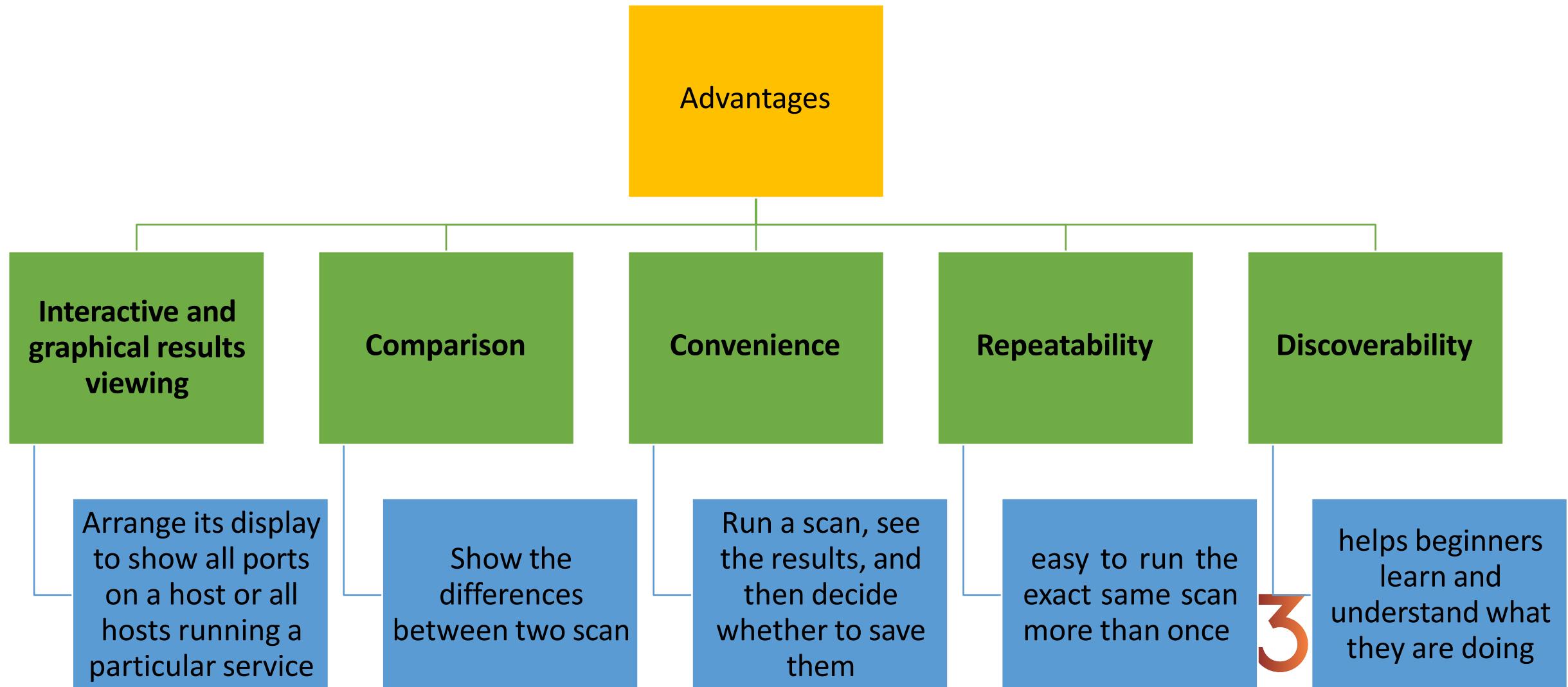
Scan results **can be saved and viewed later**.



Saved scans **can be compared** with one another to see how they differ

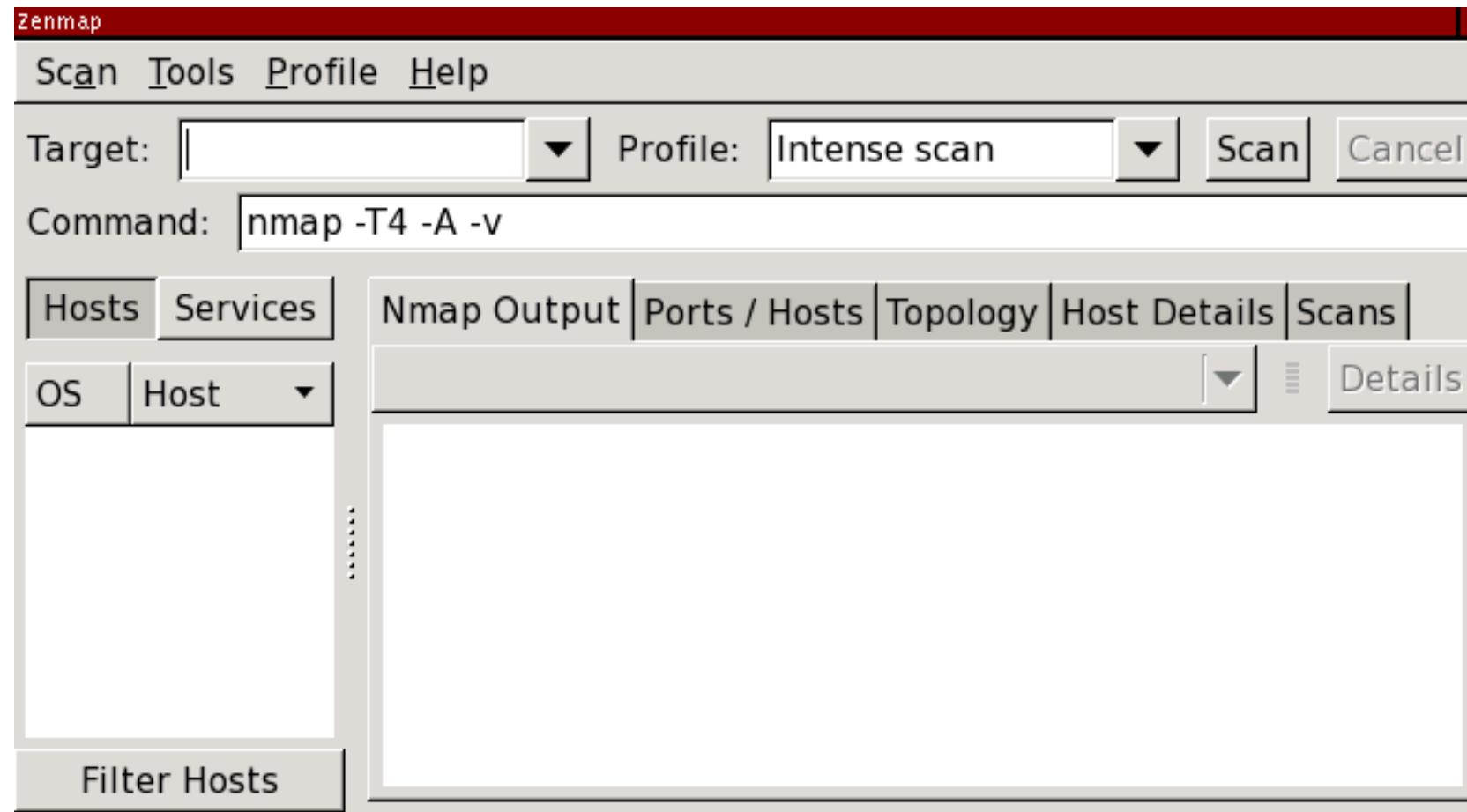


# Zenmap Tool- Advantages



# Zenmap

- Zenmap Main Window



# Zenmap

- **Target and profile selection**

- Target- IP or domain
- Profile- Different scans, as profile changes, commands also changes accordingly

Target:  ▾ Profile:  ▾

Command:



# Zenmap

## Scan Aggregation

Zenmap has the ability to combine the results- a feature known as *scan aggregation*.

When one scan is finished, you may start another in the same window.

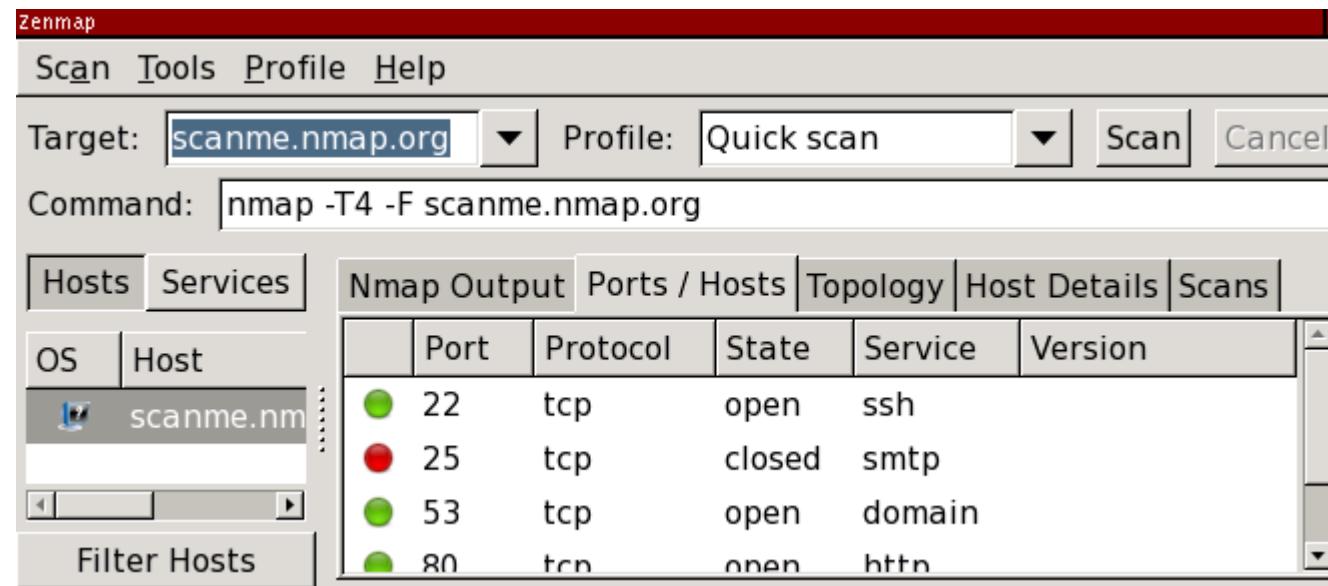
When the second scan is finished, its results are merged with those from the first.

This is known as **aggregated view (*network inventory*)**.



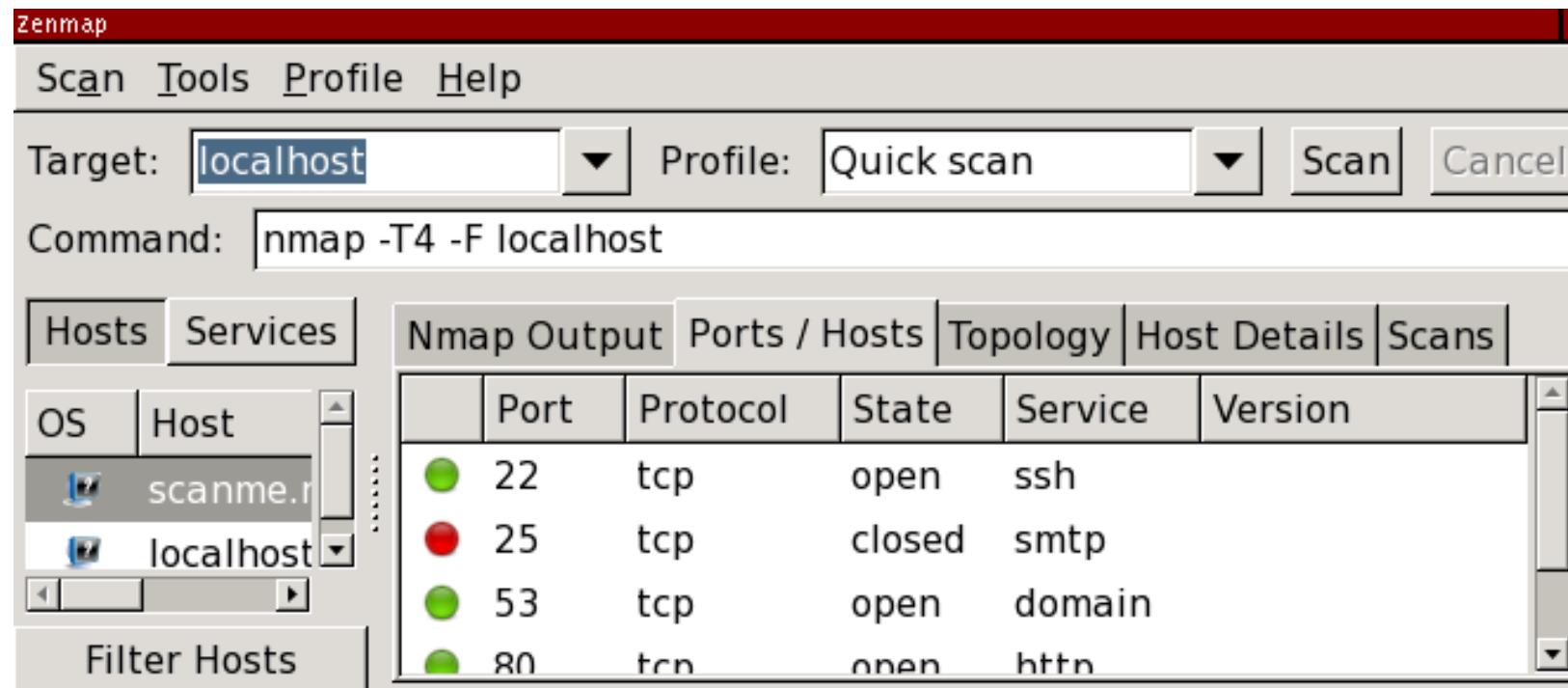
# Zenmap-2 scans

1<sup>st</sup> Step: Run a quick scan against scanme.nmap.org



# Zenmap- 2 scans

2<sup>nd</sup> step: quick scan against localhost



Zenmap

Scan Tools Profile Help

Target: localhost Profile: Quick scan Scan Cancel

Command: nmap -T4 -F localhost

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS	Host	Port	Protocol	State	Service	Version
	scanme.r	22	tcp	open	ssh	
	localhost	25	tcp	closed	smtp	
		53	tcp	open	domain	
		80	tcp	open	http	

Filter Hosts

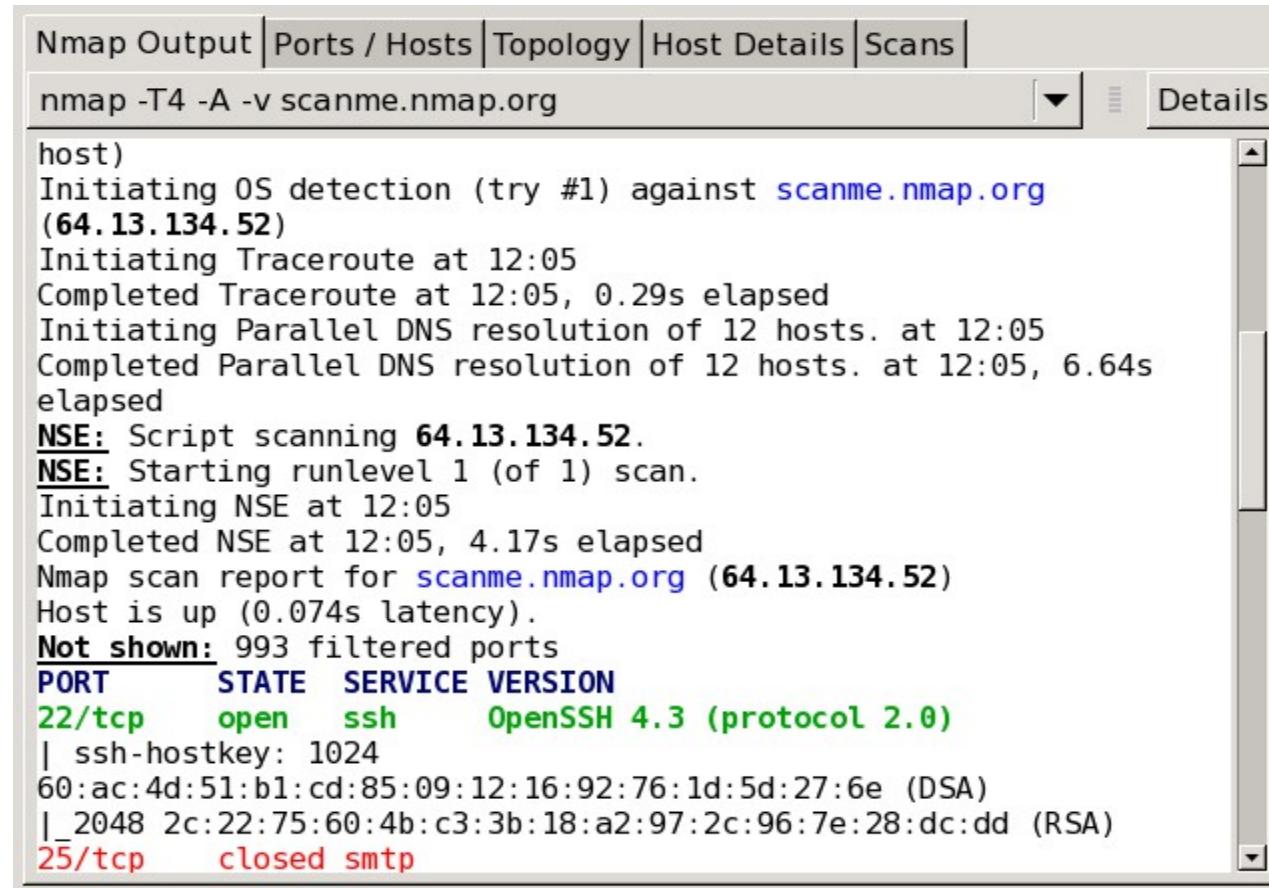
Now results for both scanme and localhost are shown.

# Zenmap-Result

- Each scan window contains five tabs which each display different aspects of the scan results.
- They are:
  - “Nmap Output”,
  - “Ports / Hosts”,
  - “Topology”,
  - “Host Details”, and
  - “Scans”.

# Zenmap-Result

- “Nmap Output” tab
  - open and closed ports are displayed in different colors



Nmap Output | Ports / Hosts | Topology | Host Details | Scans

nmap -T4 -A -v scanme.nmap.org

```
host)
Initiating OS detection (try #1) against scanme.nmap.org
(64.13.134.52)
Initiating Traceroute at 12:05
Completed Traceroute at 12:05, 0.29s elapsed
Initiating Parallel DNS resolution of 12 hosts. at 12:05
Completed Parallel DNS resolution of 12 hosts. at 12:05, 6.64s
elapsed
NSE: Script scanning 64.13.134.52.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 12:05
Completed NSE at 12:05, 4.17s elapsed
Nmap scan report for scanme.nmap.org (64.13.134.52)
Host is up (0.074s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey: 1024
| 60:ac:4d:51:b1:cd:85:09:12:16:92:76:1d:5d:27:6e (DSA)
| 2048 2c:22:75:60:4b:c3:3b:18:a2:97:2c:96:7e:28:dc:dd (RSA)
25/tcp    closed  smtp
```

# Zenmap-Result

## The “Ports / Hosts” tab

- It shows all the interesting ports on that host along with version information when available

	Port	Protocol	State	Service	Version
●	22	tcp	open	ssh	OpenSSH 4.3 (protocol 2.0)
●	25	tcp	closed	smtp	
●	53	tcp	open	domain	
●	70	tcp	closed	gopher	
●	80	tcp	open	http	Apache httpd 2.2.3 ((CentOS))
●	113	tcp	closed	auth	



# Zenmap-Result

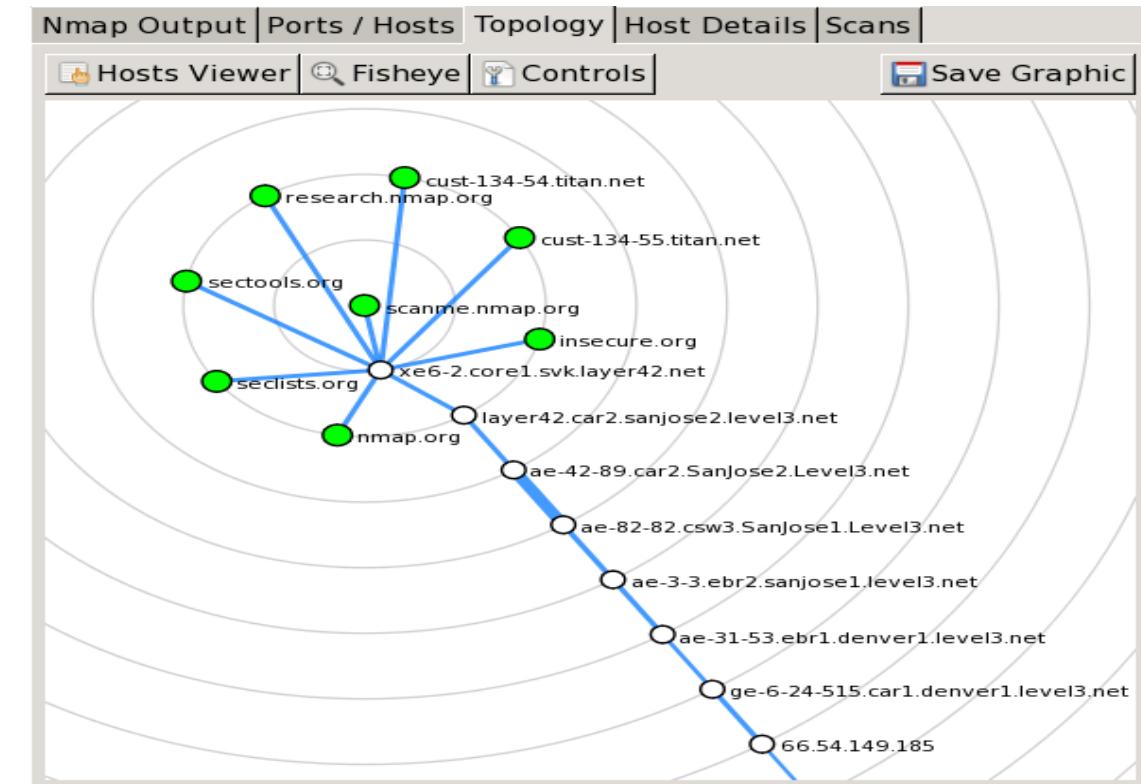
## “Topology” tab

interactive view of the **connections between hosts in a network.**

Hosts are arranged in **concentric rings**.

Each ring represents an **additional network hop** from the center node.

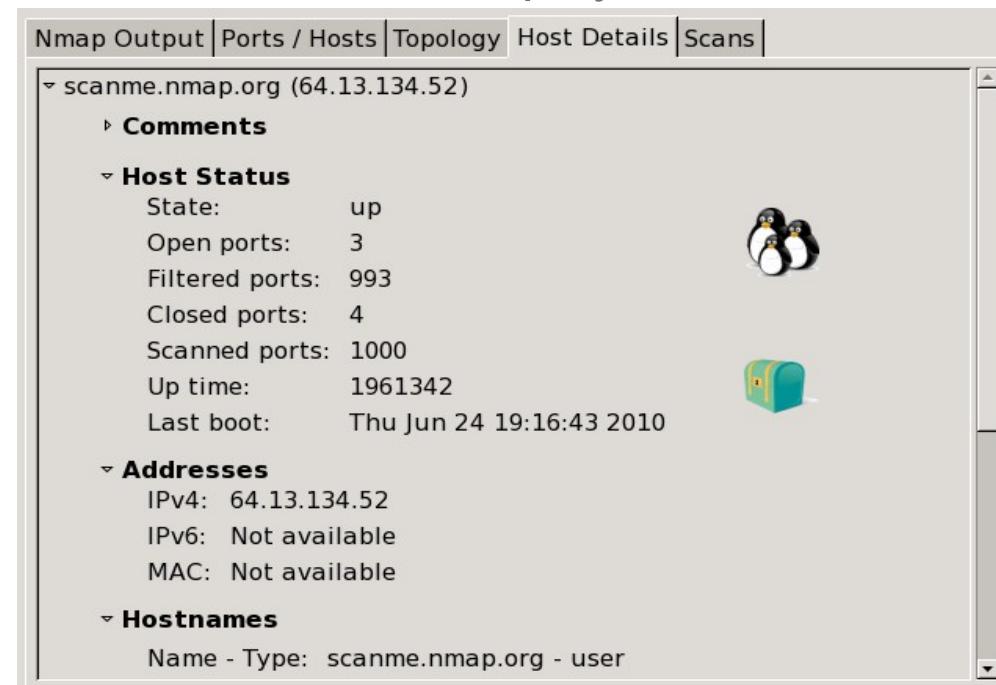
Clicking on a node brings it to the center.



# Zenmap-Result

## The “Host Details” tab

- breaks all the information about a single host into a hierarchical display.
- Show addresses,
- its state (up/down)
- the number and status of scanned ports.
- operating system,
- OS icon
- etc



The screenshot shows the 'Host Details' tab in Zenmap. The main content area displays the following information for the host `scanme.nmap.org (64.13.134.52)`:

- Comments:** None listed.
- Host Status:**
  - State: up
  - Open ports: 3
  - Filtered ports: 993
  - Closed ports: 4
  - Scanned ports: 1000
  - Up time: 1961342
  - Last boot: Thu Jun 24 19:16:43 2010
- Addresses:**
  - IPv4: 64.13.134.52
  - IPv6: Not available
  - MAC: Not available
- Hostnames:**
  - Name - Type: scanme.nmap.org - user

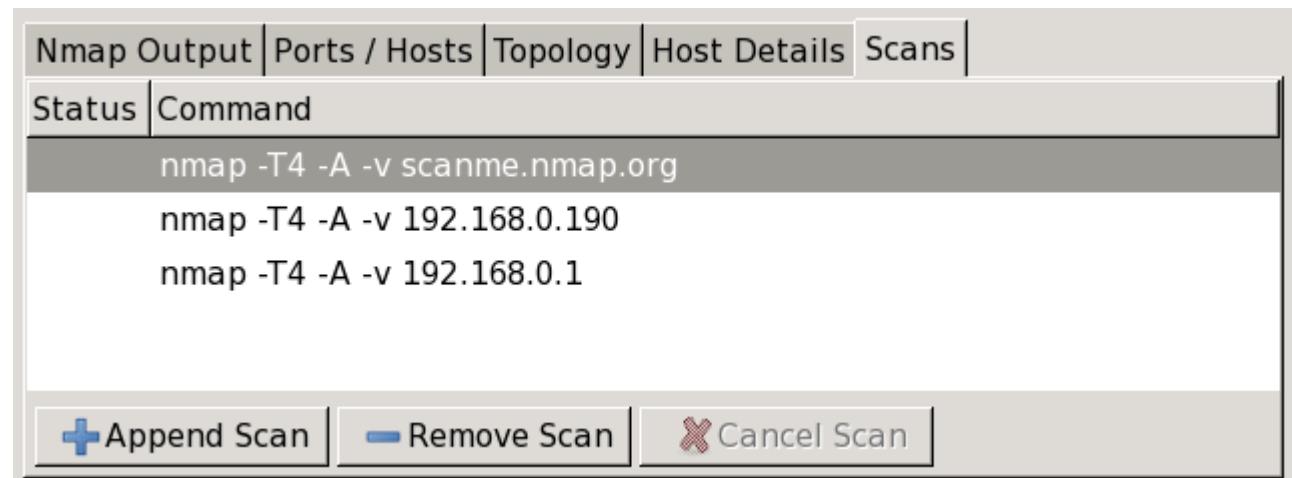
On the right side of the interface, there are two small icons: a group of penguins and a green backpack.



# Zenmap-Result

## The “Scans” tab

- shows all the scans that are aggregated to make up the network inventory



The screenshot shows the 'Scans' tab of the Zenmap interface. At the top, there are tabs for 'Nmap Output', 'Ports / Hosts', 'Topology', 'Host Details', and 'Scans'. The 'Scans' tab is active. Below the tabs, there are two sections: 'Status' and 'Command'. The 'Status' section shows the status of three scans: 'nmap -T4 -A -v scanme.nmap.org' (running), 'nmap -T4 -A -v 192.168.0.190' (idle), and 'nmap -T4 -A -v 192.168.0.1' (idle). At the bottom, there are three buttons: '+ Append Scan', 'Remove Scan' (with a minus sign icon), and 'Cancel Scan' (with a red X icon).



# Zenmap GUI-Task 20 mins

- Download the zenmap tool and try its basic commands
- Create a word file and write command and paste the screenshots.
- Task
  - Enter IP/domain
  - Find the difference between 2 hosts information
  - Merge two scans
  - Intense scan
  - Quick scan

# Assignment

- How to run scripts in Zenmap
- How to find the is firewall enabled or disabled in Zenmap
- Can we perform IP or MAC spoofing in Zenmap

# Zenmap- 2 scans



Can we scan two hosts in Nmap??

