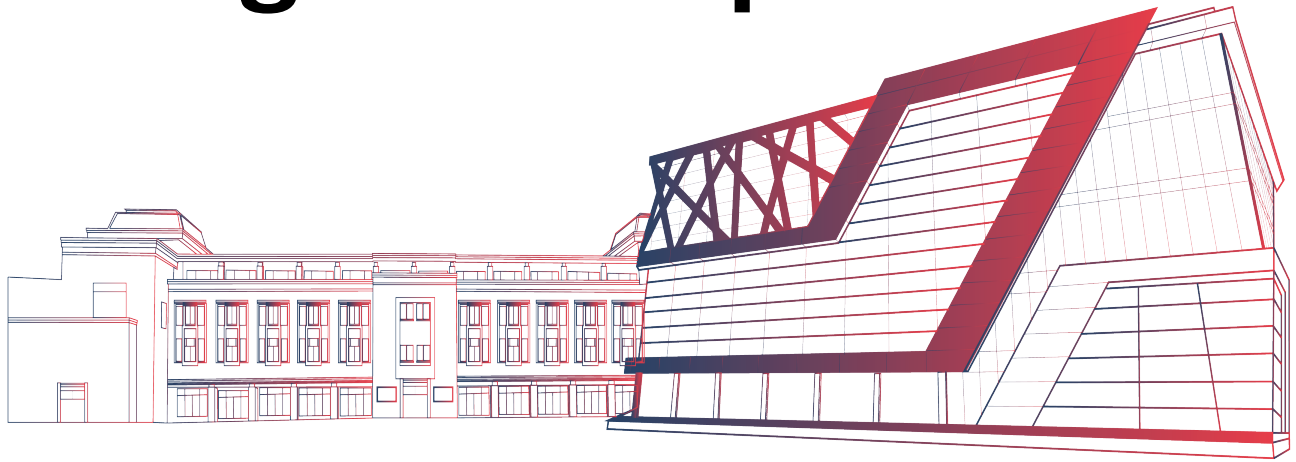
THE NORTHCAP UNIVERSITY

Scanning- Zenmap



30 YEARS OF EXCELLENCE

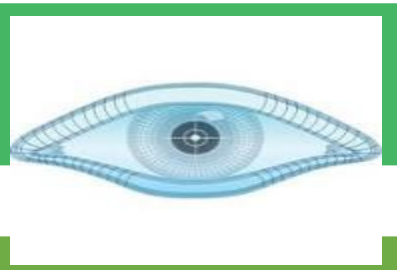
NAAC Accredited

Zenmap Tool

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

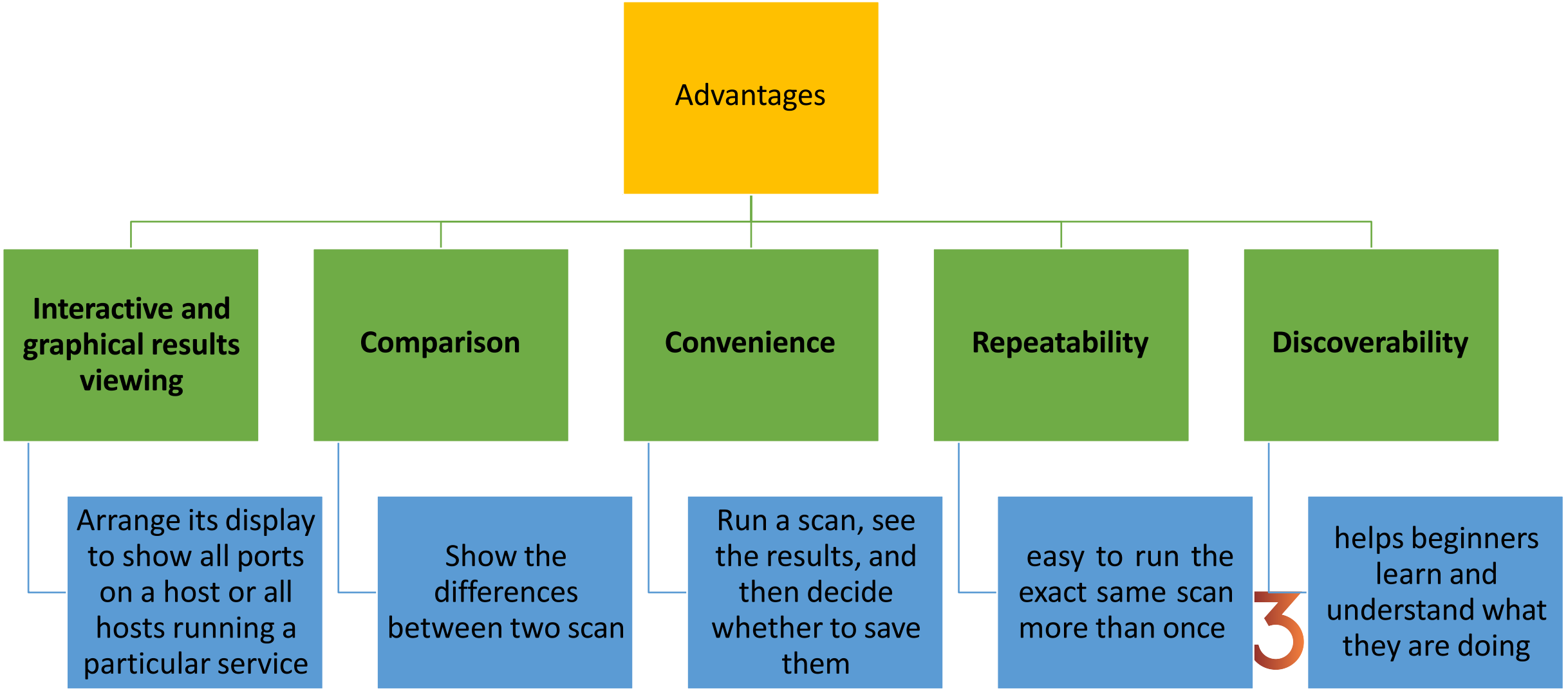
It is a **multi-platform, free and open-source application** designed to make Nmap **easy to use for beginners** while providing **advanced features for experienced Nmap users.**

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



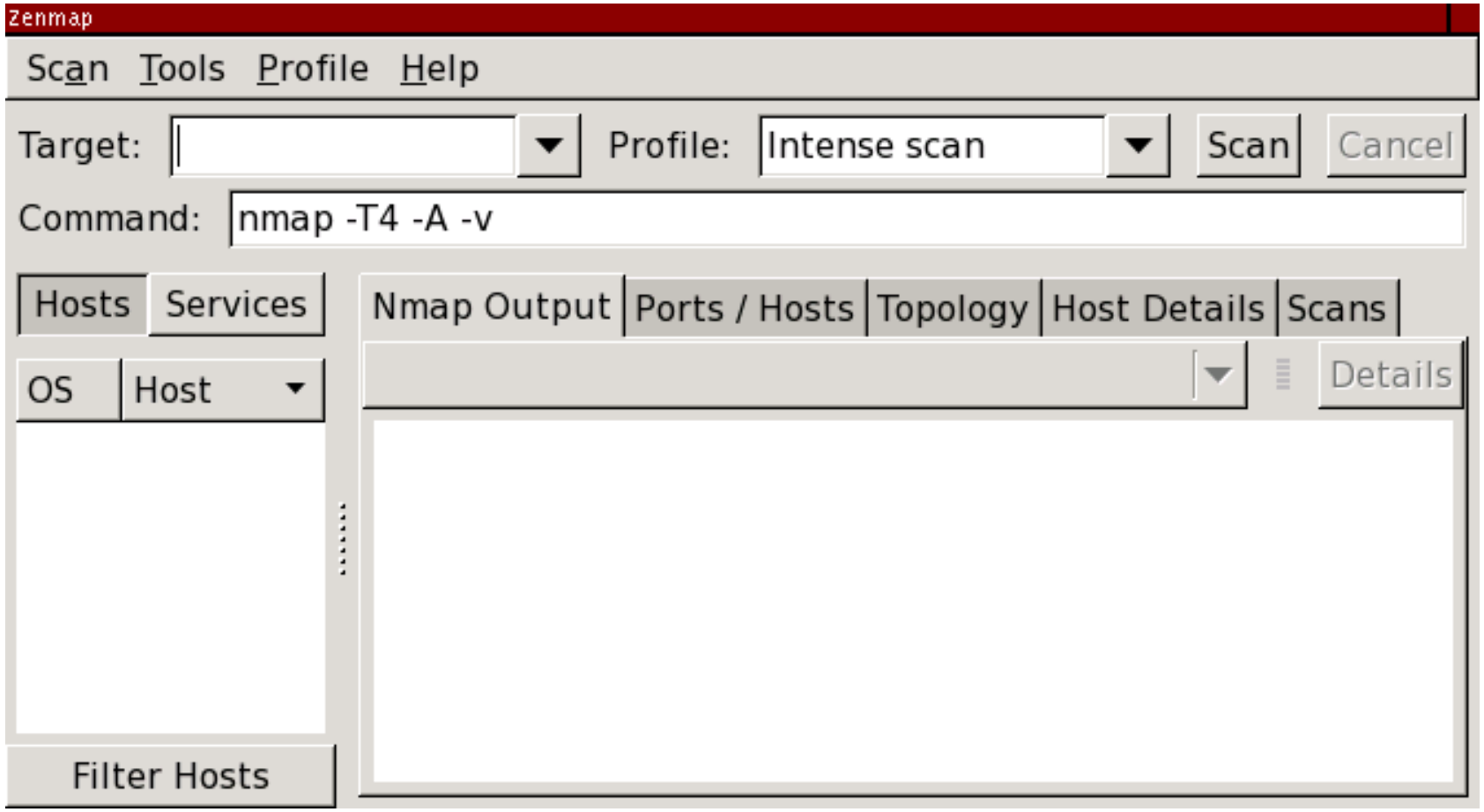
Saved scans **can be compared** with one another to see how they differ

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

Zenmap

Scan Aggregation

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

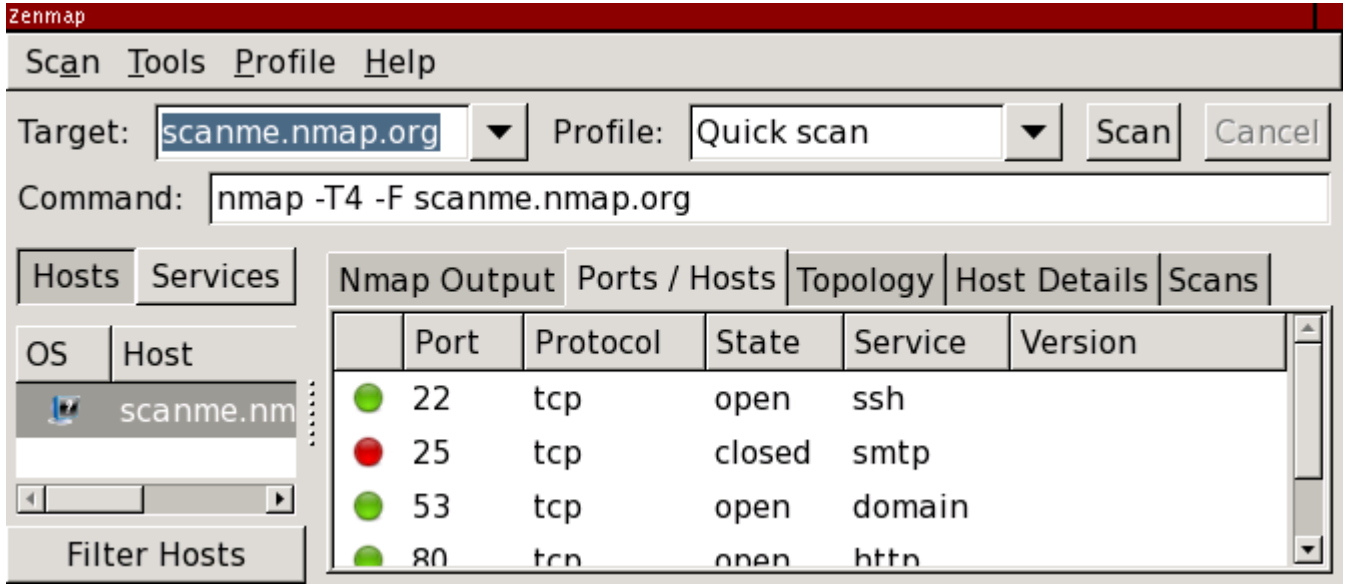
When one scan is finished, you may start another in the same window.

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

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

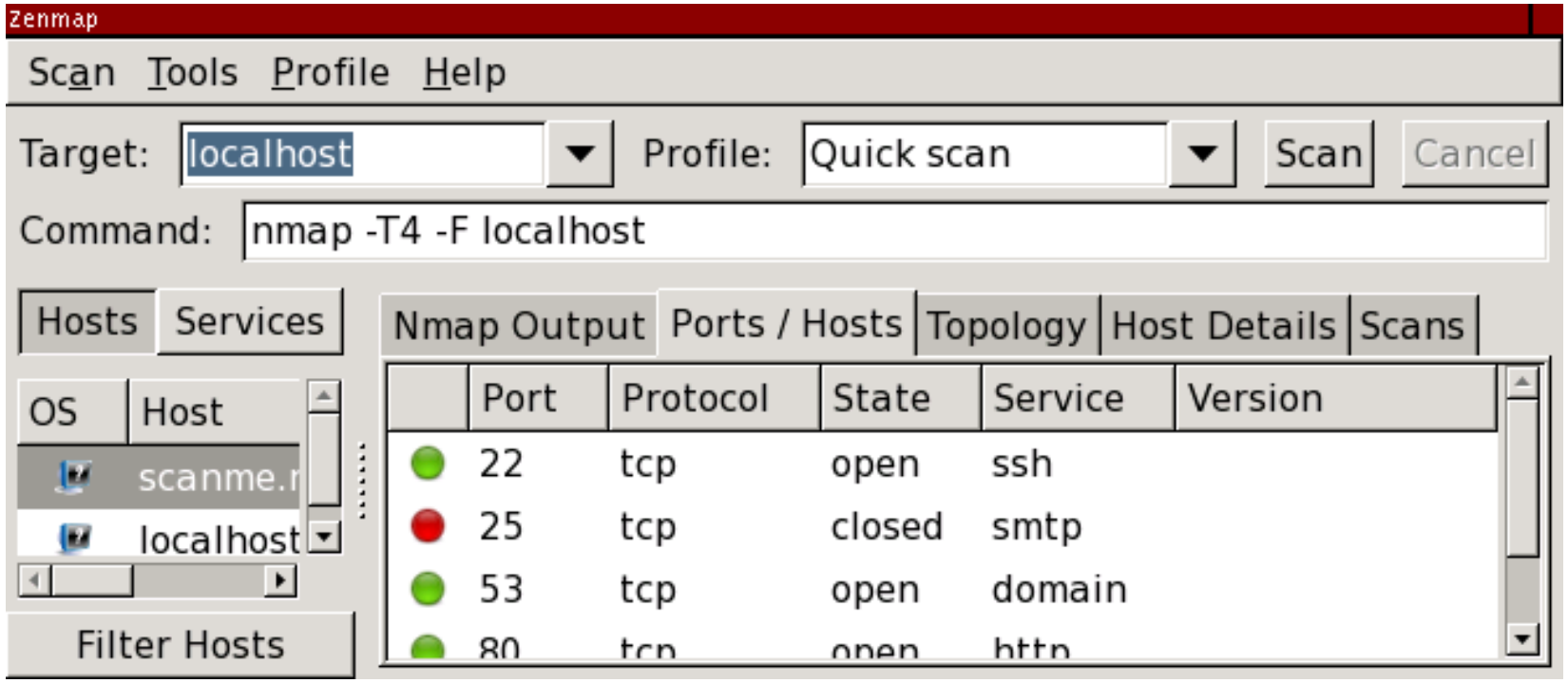
Zenmap-2 scans

1st Step: Run a quick scan against scanme.nmap.org



Zenmap- 2 scans

2nd step: quick scan against localhost



Now results for both scanme and localhost are shown.

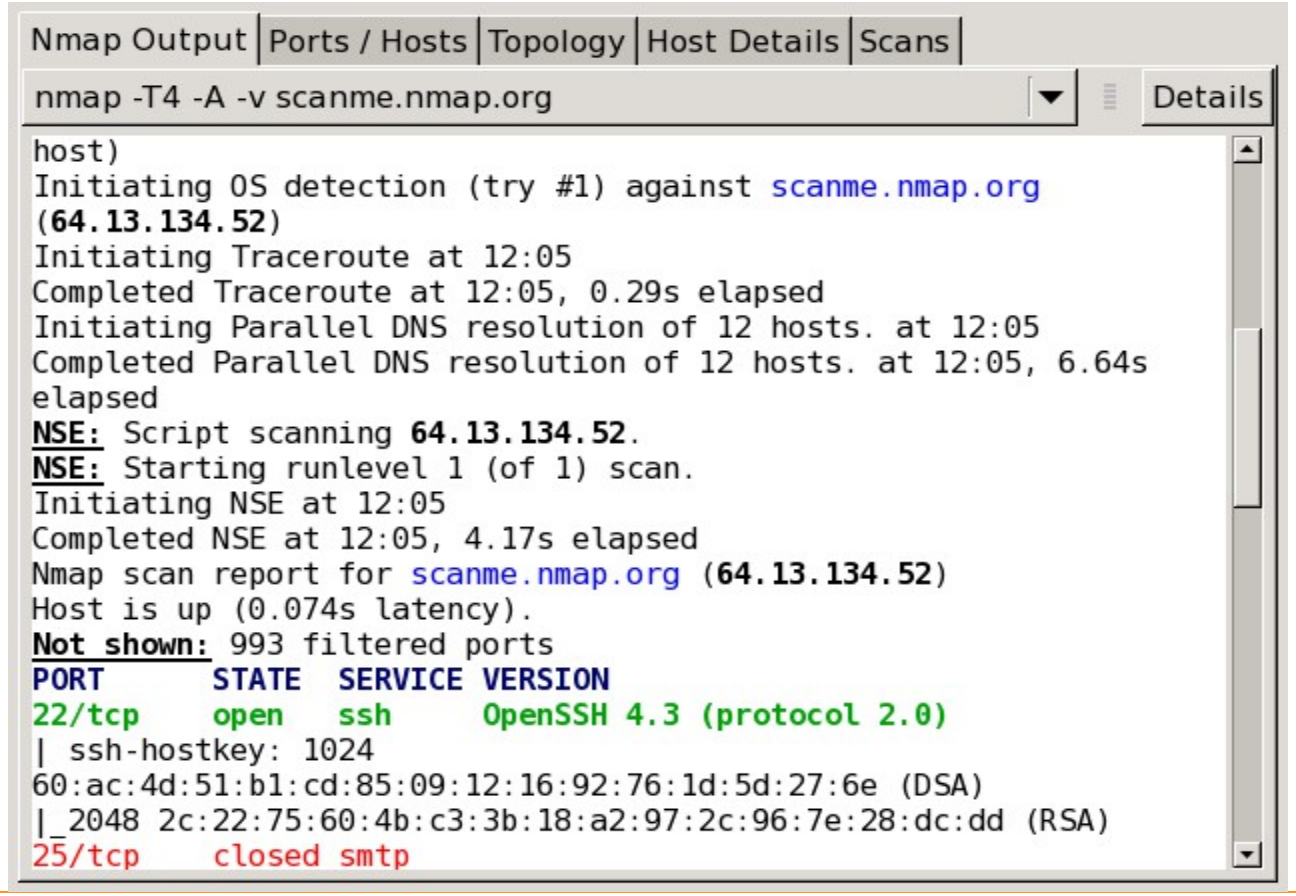
Zenmap-Result

- 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

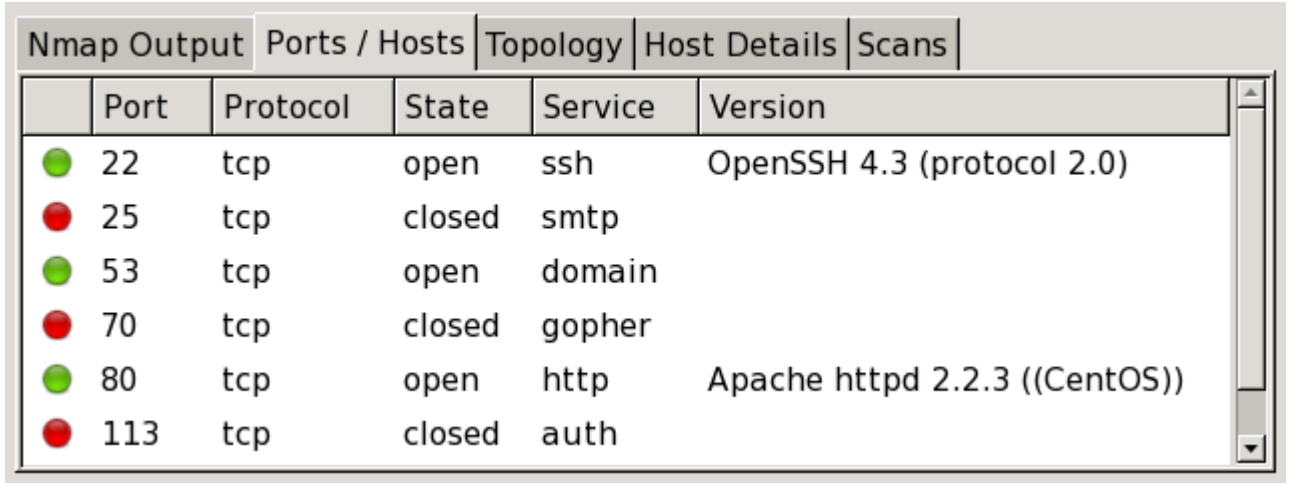


Zenmap-Result

THE NORTHCAP UNIVERSITY

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	

30 YEARS OF EXCELLENCE

NAAC Accredited

Zenmap-Result

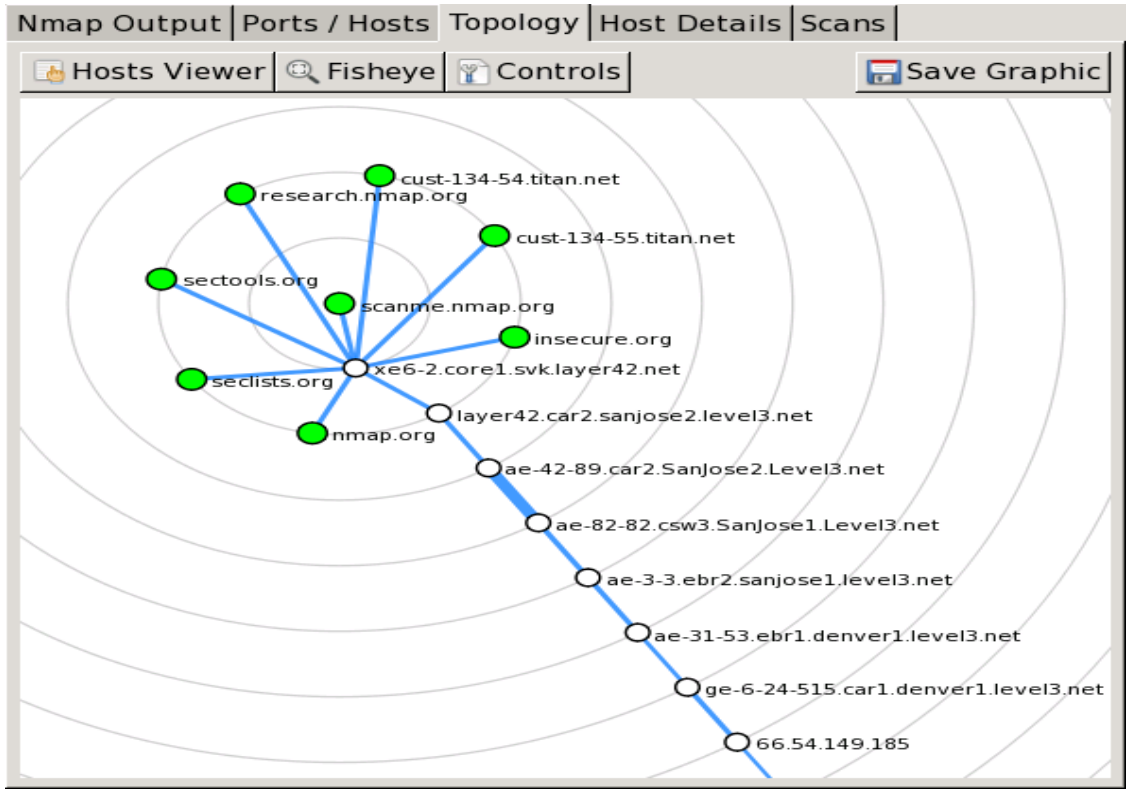
“Topology” tab

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.

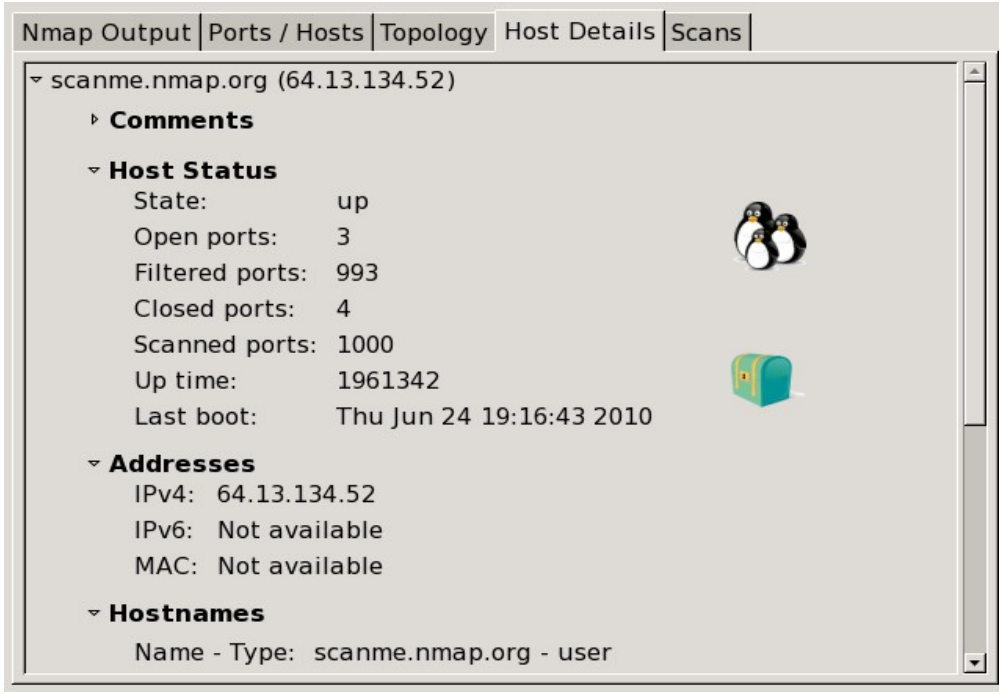
Clicking on a node brings it to the center.



Zenmap-Result

The “Host Details” tab

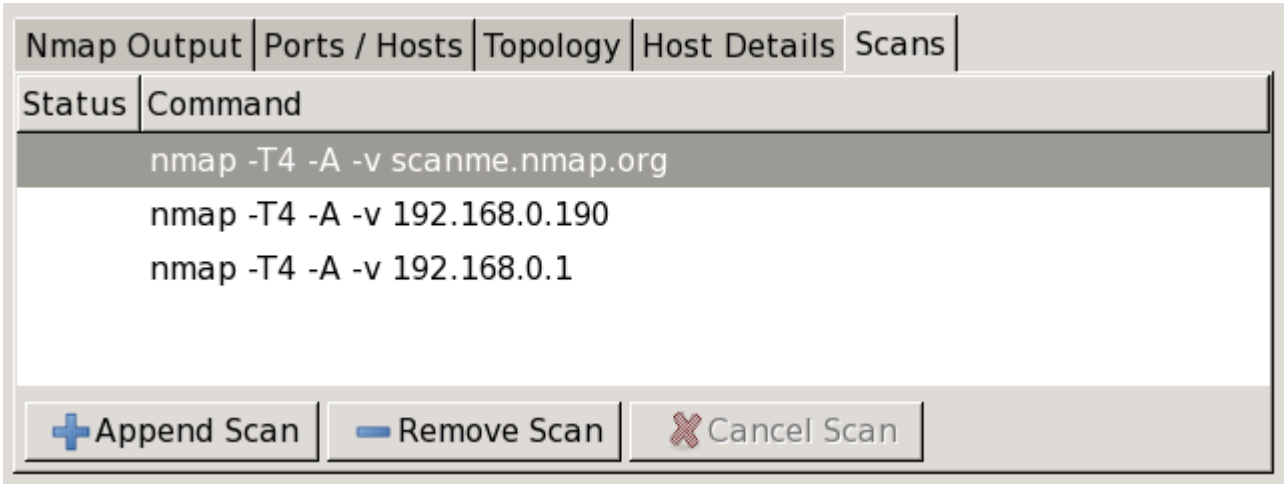
- breaks all the information about a single host into a hierarchical display.
- Show addresses,
- its state (up/down)
- the number and status of scanned ports.
- operating system,
- OS icon
- **etc**



Zenmap-Result

The “Scans” tab

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



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??