Parshvanath Charitable Trust's
A. P. SHAH INSTITUTE OF TECHNOLOGY
(Approved by AICTE New Delhi & Govt. of Maharashtra, Affiliated to University of Mumbai)
(Religious Jain Minority)

# Department of Computer Engineering

## Experiment: 07

## Aim:

Perform network discovery using discovery tools-Nmap

## Description:

Nmap stands for Network Mapper. It is an open source tool that is used widely for network discovery and security auditing. Nmap was originally designed to scan large networks, but it can work equally well for single hosts. Network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets to determine: • what hosts are available on the network, • what services those hosts are offering, • what operating systems they are running on, • what type of firewalls are in use, and other such characteristics. Nmap runs on all major computer operating systems such as Windows, Mac OS X, and Linux.

Basic Steps:

Before attacking a system, it is required that you know what operating system is hosting a website. Once a target OS is known, then it becomes easy to determine which vulnerabilities might be present to exploit the target system. Below is a simple nmap command which can be used to identify the operating system serving a website and all the opened ports associated with the domain name, i.e., the IP address. $nmap -O -v facebook.com It will show you the following sensitive information about the given domain name or IP address: Starting Nmap 5.51 ( http://nmap.org ) at 2015-10-04 09:57 CDT Initiating Parallel DNS resolution of 1 host. at 09:57 Completed Parallel DNS resolution of 1 host. at 09:57, 0.00s elapsed Initiating SYN Stealth Scan at 09:57

Scanning facebook.com (66.135.33.172) [1000 ports] Discovered open port 22/tcp on 66.135.33.172

Discovered open port 3306/tcp on 66.135.33.172

Discovered open port 80/tcp on 66.135.33.172 Discovered open port 443/tcp on 66.135.33.172

Completed SYN Stealth Scan at 09:57, 0.04s elapsed (1000 total ports) Initiating OS detection (try #1) against tutorialspoint.com (66.135.33.172) Retrying OS detection (try #2)

against tutorialspoint.com (66.135.33.172) Retrying OS detection (try #3) against tutorialspoint.com (66.135.33.172) Retrying OS detection (try #4) against tutorialspoint.com (66.135.33.172) Retrying OS detection (try #5) against tutorialspoint.com (66.135.33.172) Nmap scan report for tutorialspoint.com (66.135.33.172) Host is up (0.000038s latency). Not shown: 996 closed ports

**Port Scanning**

We have just seen information given by the nmap command. This command lists down all the open ports on a given server.

```
22/tcpopen

ssh 80/tcpopen http

443/tcp open https

3306/tcpopen mysql
```

You can also check if a particular port is opened or not using the following command:

```
$nmap -sT -p 443 facebook.com
```

It will produce the following result:

Starting Nmap5.51 ( http://nmap.org ) at 2017-08-04 10:19 CDT Nmap scan report for facebook.com (66.135.33.172) [Assume]

Host is up (0.000067s latency).

PORT STATE SERVICE 443/tcpopen https

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds

Once a hacker knows about open ports, then he can plan different attack techniques through the open ports.

**Quick Fix**: It is always recommended to check and close all the unwanted ports to safeguard the system from malicious attacks.

**Ping Sweep**:

A ping sweep is a network scanning technique that you can use to determine which IP address from a range of IP addresses map to live hosts. Ping Sweep is also known as ICMP sweep.

You can use fping command for ping sweep. This command is a ping-like program which uses the Internet Control Message Protocol (ICMP) echo request to determine if a host is up.

fping is different from ping in that you can specify any number of hosts on the command line, or specify a file containing the lists of hosts to ping. If a host does not respond within a certain time limit and/or retry limit, it will be considered unreachable.

Quick Fix To disable ping sweeps on a network, you can block ICMP ECHO requests from outside sources. This can be done using the following command which will create a firewall rule in iptable.

```
$iptables -A OUTPUT -p icmp --icmp-type echo-request -j DROP
```

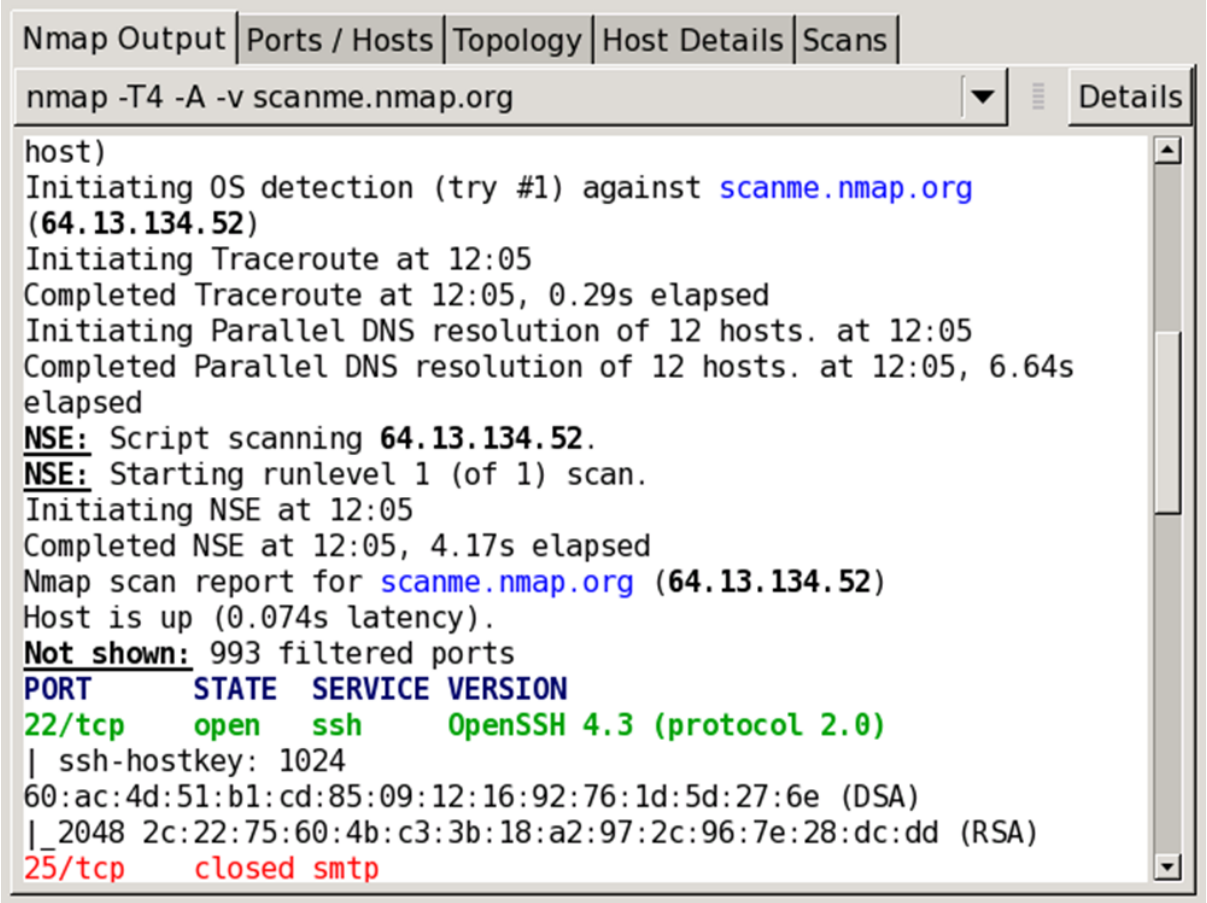
**Interpreting Scan Results**

Nmap's output is displayed during and after a scan. This output will be familiar to Nmap users. Except for Zenmap's color highlighting, this doesn't offer any visualization advantages over running Nmap in a terminal. However, other parts of Zenmap's interface interpret and aggregate the terminal output in a way that makes scan results easier to understand and use.

**Scan Results Tabs**

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”. Each of these are discussed in this section.

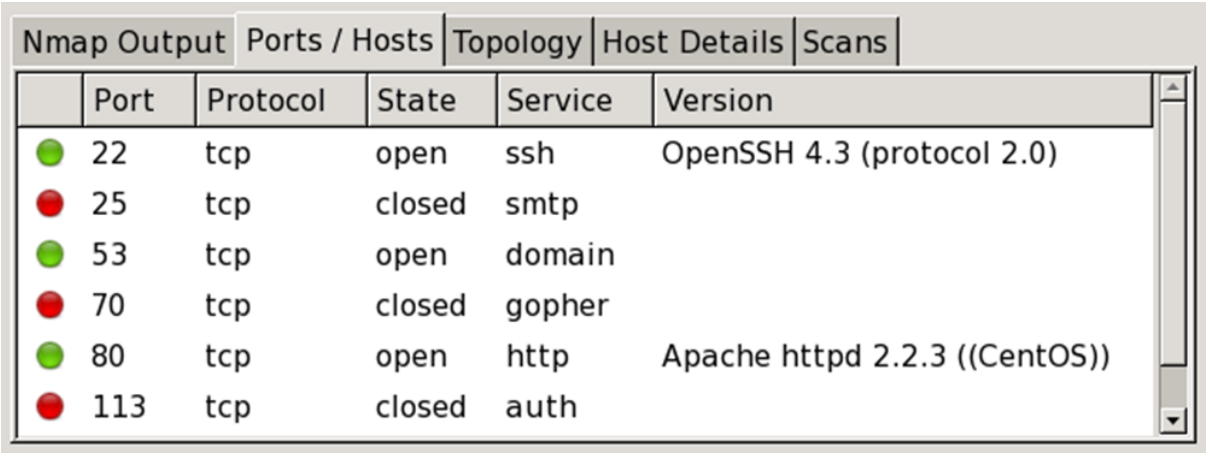
The “Nmap Output” tab



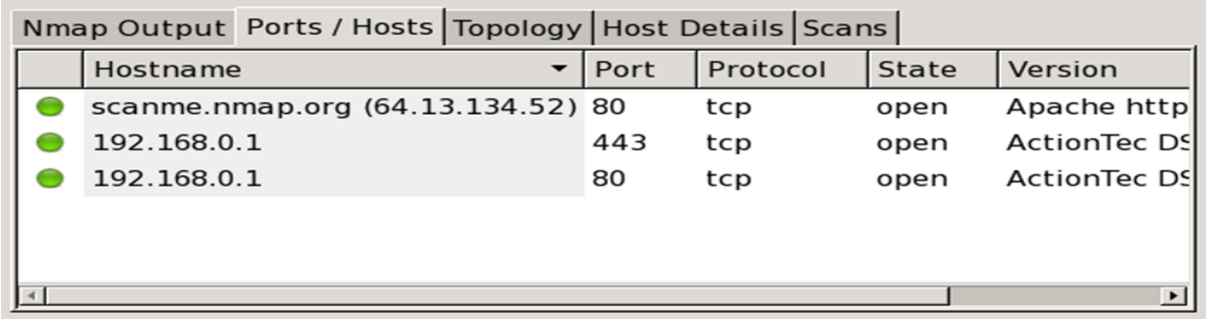

The “Nmap Output” tab is displayed by default when a scan is run. It shows the familiar Nmap terminal output. The display highlights parts of the output according to their meaning; for example, open and closed ports are displayed in different colors. Custom highlights can be configured in zenmap.conf.

Recall that the results of more than one scan may be shown in a window. The drop-down combo box at the top of the tab allows you to select the scan to display. The “Details” button brings up a window showing miscellaneous information about the scan, such as timestamps, command-line options, and the Nmap version number used.

The “Ports / Hosts” tab

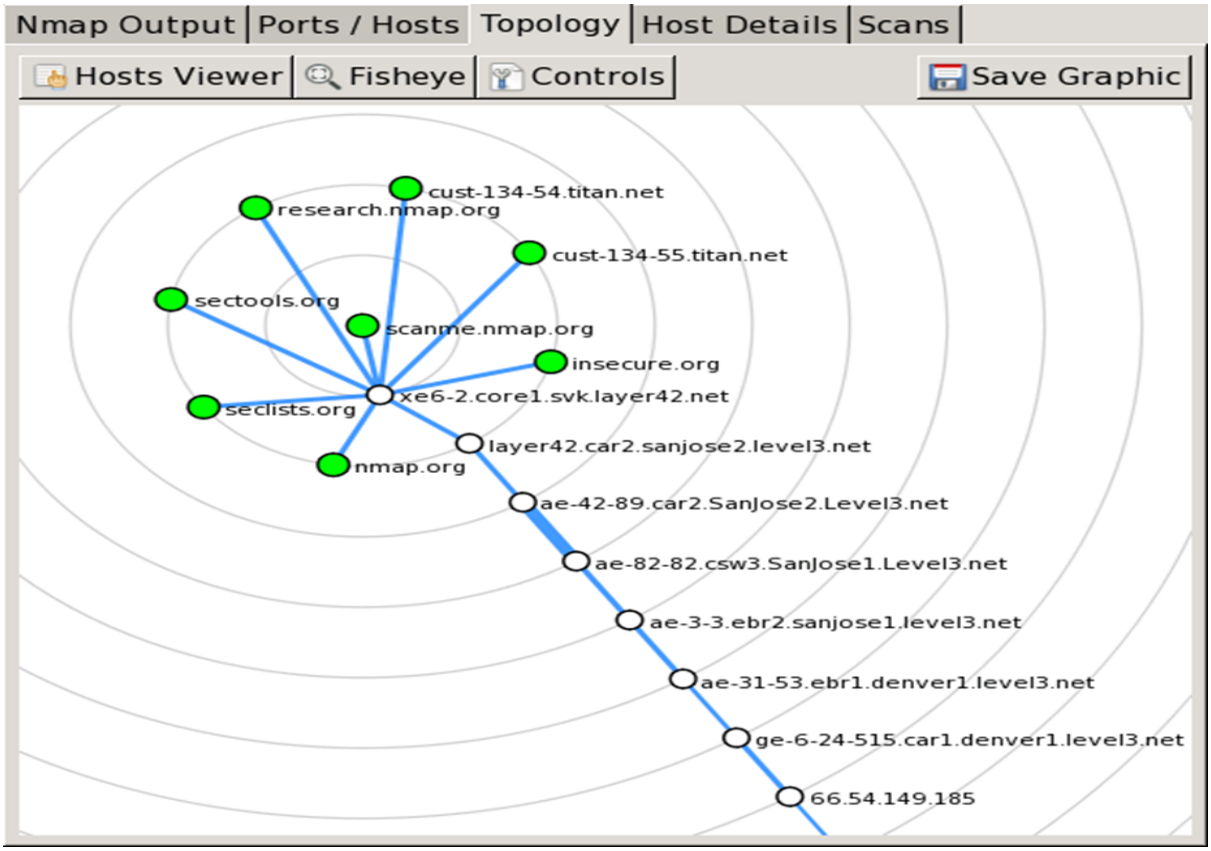


The “Ports / Hosts” tab's display differs depending on whether a host or a service is currently selected. When a host is selected, it shows all the interesting ports on that host, along with version information when available. Host selection is further described in the section called “Sorting by Host”.




When a service is selected, the “Ports / Hosts” tab shows all the hosts which have that port open or filtered. This is a good way to quickly answer the question “What computers are running HTTP?” Service selection is further described in the section called “Sorting by Service”.

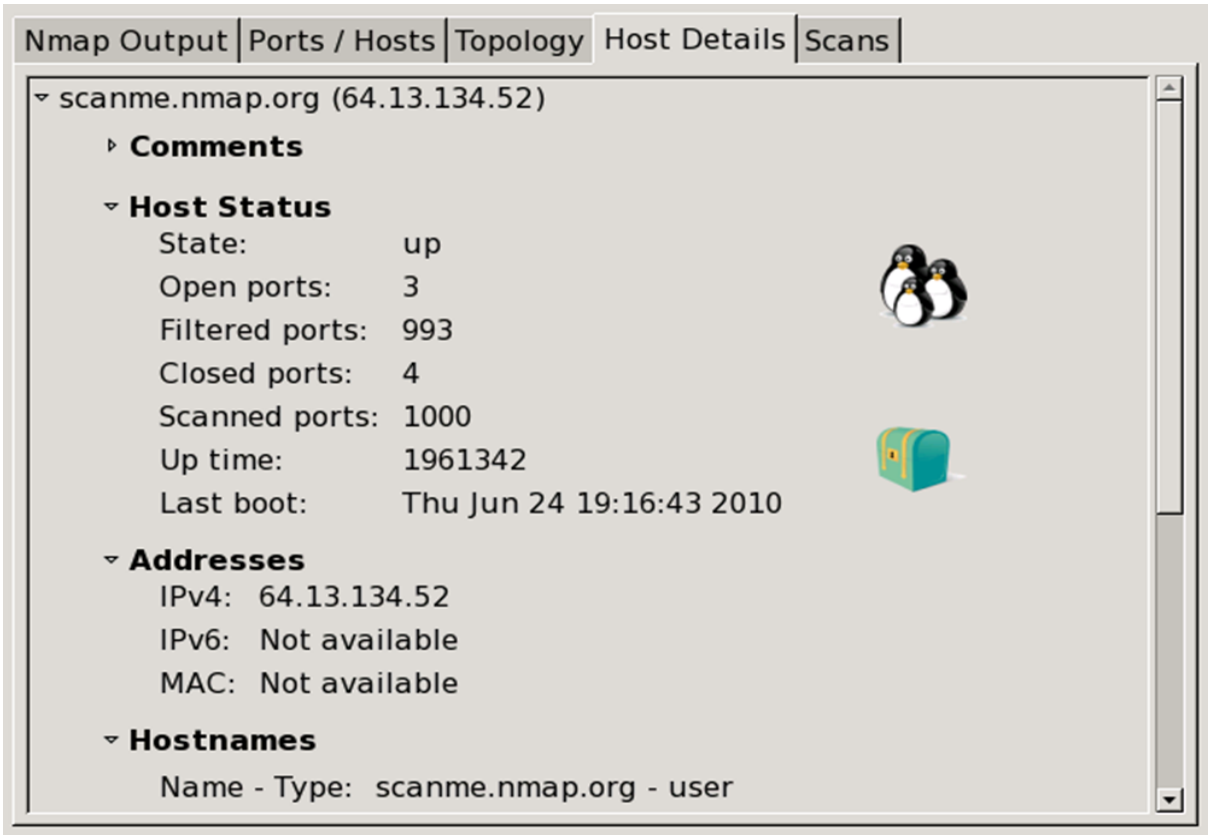
The “Topology” tab




The “Topology” tab is an 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. Because it shows a representation of the network paths between hosts, the “Topology” tab benefits from the use of the --traceroute option. Topology view is discussed in more detail in the section called “Surfing

the Network Topology”.

The “Host Details” tab




The “Host Details” tab breaks all the information about a single host into a hierarchical display. Shown are the host's names and addresses, its state (up or down), and the number and status of scanned ports. The host's uptime, operating system, OS, and other associated details are shown when available. When no exact OS match is found, the closest matches are displayed. There is also a collapsible text field for storing a comment about the host which will be saved when the scan is saved to a file. Each host has an icon that provides a very rough “vulnerability” estimate, which is based solely on the number of open ports. The icons and the numbers of open ports they correspond to are

0–2 open ports,

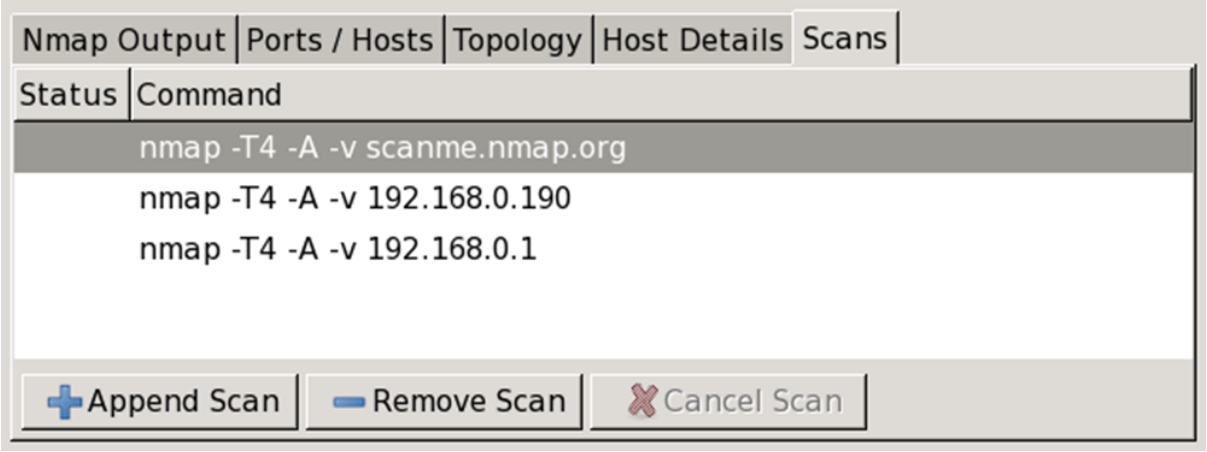
3–4 open ports,

5–6 open ports,

7–8 open ports, and

9 or more open ports.

The “Scans” tab

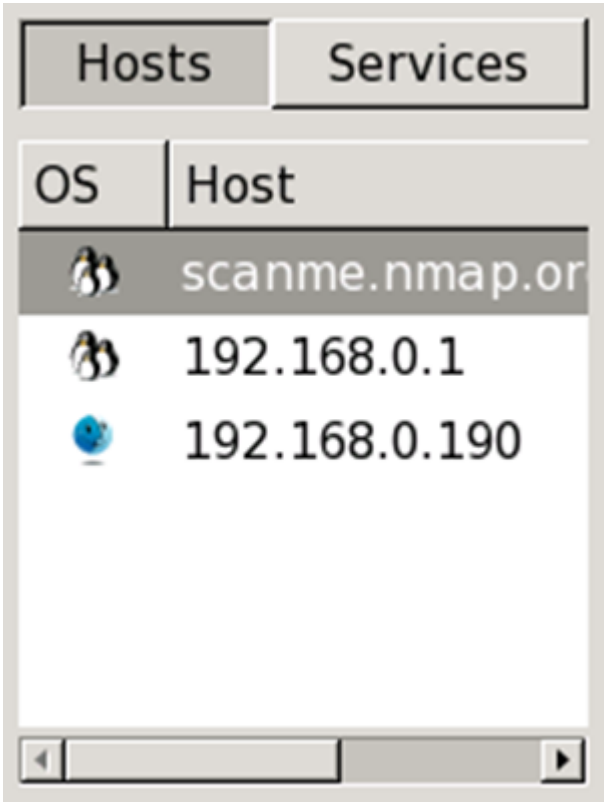



The “Scans” tab shows all the scans that are aggregated to make up the network inventory. From this tab you can add scans (from a file or directory) and remove scans.

While a scan is executing and not yet complete, its status is “Running”. You may cancel a running scan by clicking the “Cancel Scan” button.

Sorting by Host

Figure Host selection




On the left side of Zenmap's main window is a column headed by two buttons labeled “Hosts” and “Services”. Clicking the “Hosts” button will bring up a list of all hosts that were scanned, as in Figure. Commonly this contains just a single host, but it can contain thousands

in a large scan. The host list can be sorted by OS or host name/IP address by clicking the headers at the top of the list. Selecting a host will cause the “Ports / Hosts” tab to display the interesting ports on that host.

Each host is labeled with its host name or IP address and has an icon indicating the operating system that was detected for that host. The icon is meaningful only if OS detection (-O) was performed. Otherwise, the icon will be a default one indicating that the OS is unknown. Figure shows all possible icons. Note that Nmap's OS detection cannot always provide the level of specificity implied by the icons; for example a Red Hat Linux host will often be displayed with the generic Linux icon.

**Conclusion:**

Network scanning provides a wealth of information about the target network, which is valuable regardless of whether you're trying to attack the network or protect it from attack. While performing a basic scan is a simple matter, the network scanners covered in this experiment provide a wide array of options to tweak your scan to achieve the best results. Nmap is used to detect IP spoofing and port scanning.