Cycle 7

Download and install nmap. Use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan.

**1. Aim:** Download and install nmap. Use it with different options to scan open

ports,perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, etc.

**2. Objectives:** objective of this module to learn nmap installation & use this to scan

different ports.

**3. Outcomes:** students will be able to:-

 Scan the network using scanning techniques available in NMAP.

 Use current techniques, skills, and tools necessary for computing practice

4. **Hardware / Software Required :** NMAP Tool

**5. Theory:**

Nmap (Network Mapper) is a security scanner originally written by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich) used to discover hosts and services on a computer network, thus creating a "map" of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host and then analyzes the responses. Unlike many simple port scanners that just send packets at some predefined constant rate, Nmap accounts for the network conditions (latency fluctuations, network congestion, the target interference with the scan) during the run. Also, owing to the large and active user community providing feedback and contributing to its features, Nmap has been able to extend its discovery capabilities beyond simply figuring out whether a host is up or down and which ports are open and closed; it can determine the operating system of the target, names and versions of the listening services,estimated uptime,type of device, and presence of a firewall.

**Nmap features include:**

**Host Discovery** – Identifying hosts on a network. For example, listing the hosts which

respond to pings or have a particular port open.

**Port Scanning** – Enumerating the open ports on one or more target hosts.

Version Detection – Interrogating listening network services listening on remote devices

to determine the application name and version number.

**OS Detection** – Remotely determining the operating system and some hardware

characteristics of network devices.

Basic commands working in Nmap

**For target specifications:**

nmap <target‘s URL or IP with spaces between them>

**For OS detection:**

nmap -O <target-host's URL or IP>

**For version detection:**

nmap -sV <target-host's URL orIP>

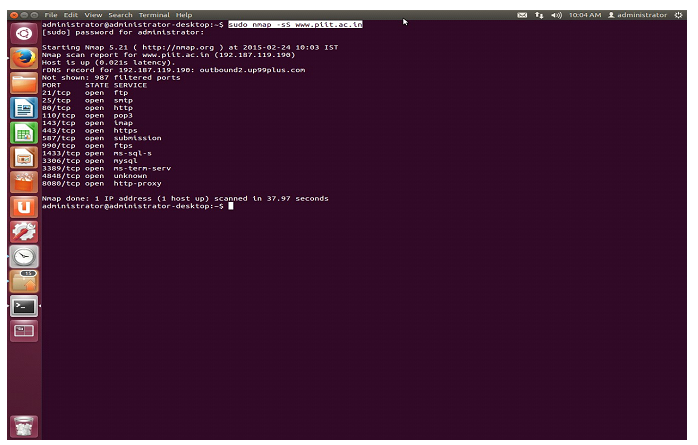
After the installation of nmap:> sudo apt-get install nmap

SYN scan is the default and most popular scan option for good reasons. It can be

performed quickly, scanning thousands of ports per second on a fast network not

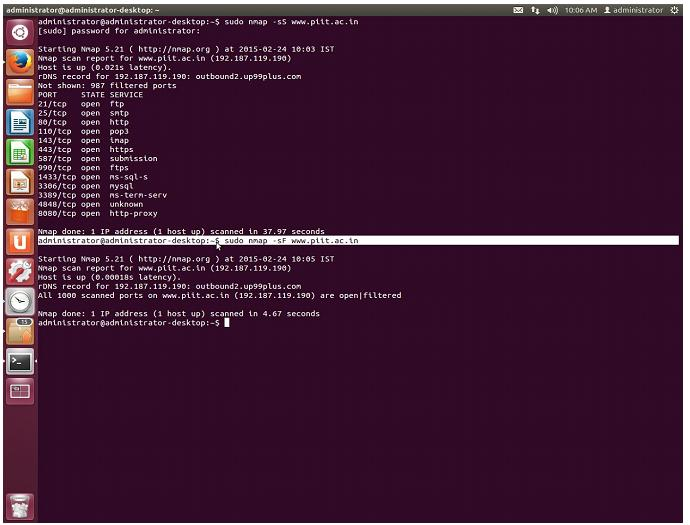
hampered by restrictive firewalls. It is also relatively unobtrusive and stealthy since it never

completes TCP connections.



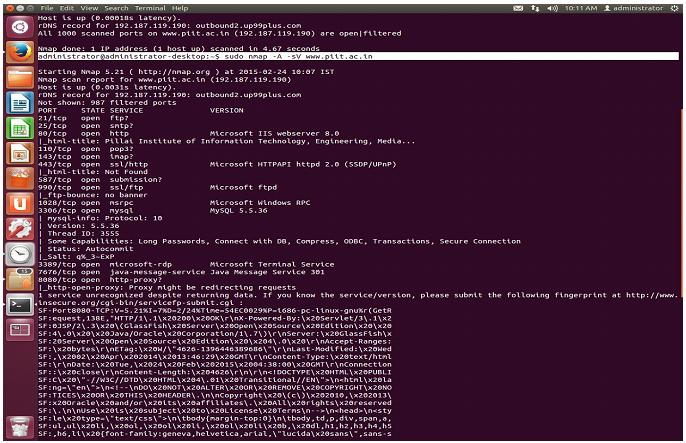
FIN scan (-sF)

Sets just the TCP FIN bit.



-sV (Version detection) :Enables version detection, as discussed above. Alternatively, we can

use -A, which enables version detection among other things.

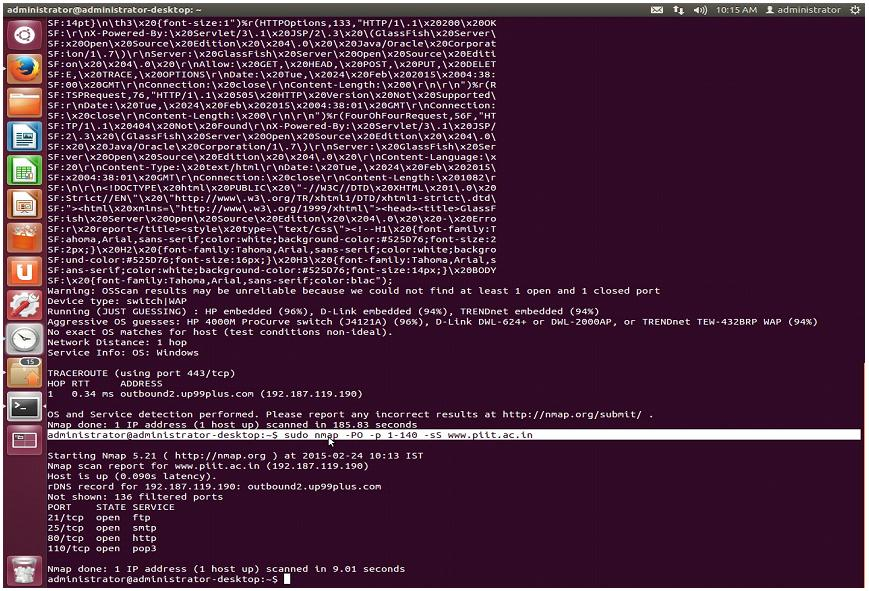


-PO protocol list (IP Protocol Ping) :

The newest host discovery option is the IP protocol ping, which sends IP packets with the

specified protocol number set in their IP header. The protocol list takes the same format as do

port lists in the previously discussed TCP, UDP and SCTP host discovery options.

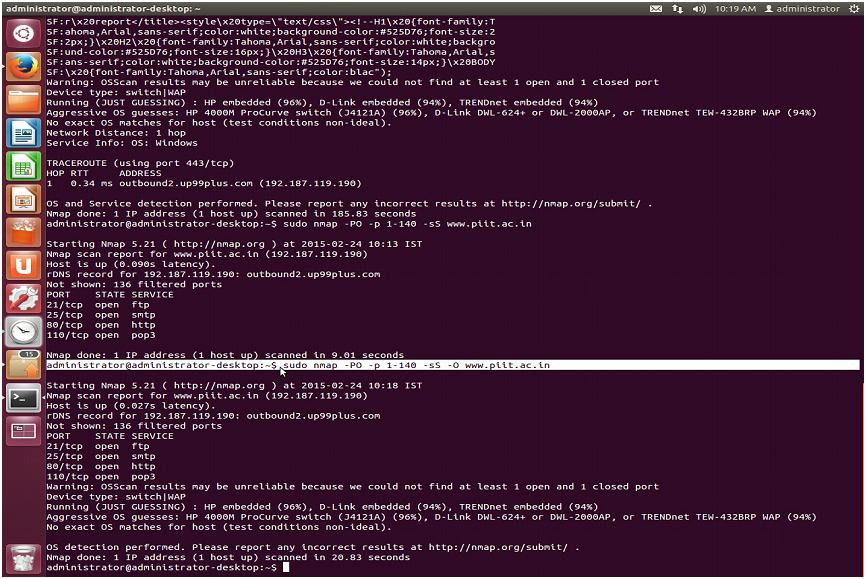


-p port ranges (Only scan specified ports) .

This option specifies which ports you want to scan and overrides the default. Individual port

numbers are OK, as are ranges separated by a hyphen (e.g. 1-1023). The beginning and/or

end values of a range may be omitted, causing Nmap to use 1 and 65535, respectively

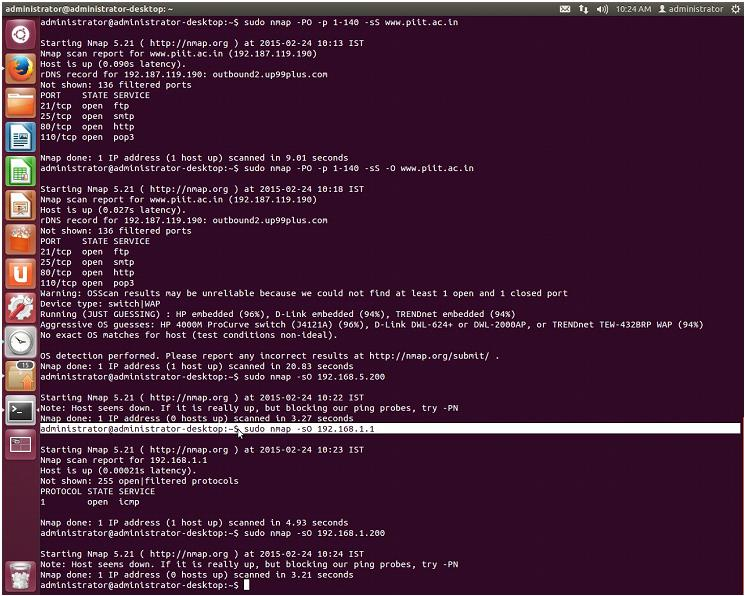


-sO (IP protocol scan) .

IP protocol scan allows you to determine which IP protocols (TCP, ICMP, IGMP, etc.) are

supported by target machines. This isn´t technically a port scan, since it cycles through IP

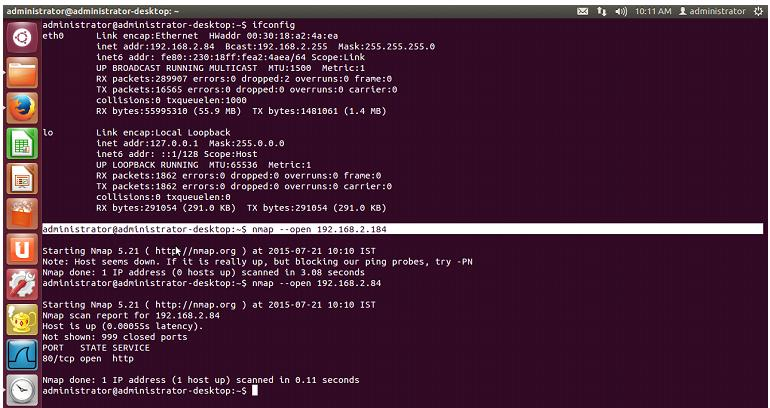
protocol numbers rather than TCP or UDP port numbers.



--open (Show only open (or possibly open) ports) .

Sometimes you only care about ports you can actually connect to (open ones), and don´t want

results cluttered with closed, filtered, and closed filtered ports.

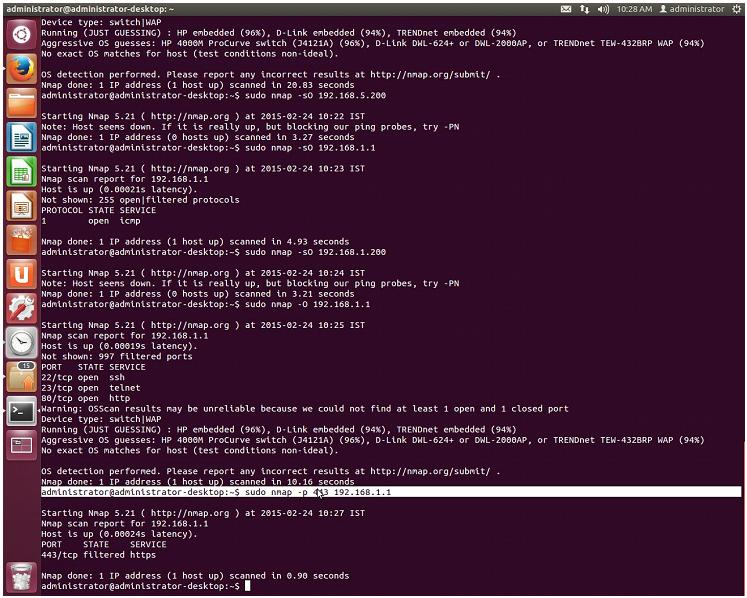


-p port ranges (Only scan specified ports) .

This option specifies which ports you want to scan and overrides the default. Individual port

numbers are OK, as are ranges separated by a hyphen (e.g. 1-1023). The beginning and/or

end values of a range may be omitted, causing Nmap to use 1 and 65535, respectively.



-sT (TCP connect scan) .

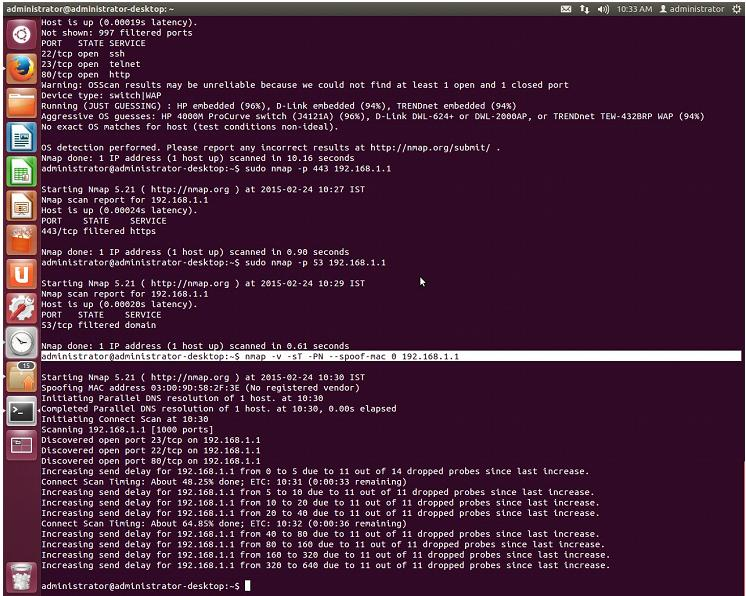
TCP connect scan is the default TCP scan type when SYN scan is not an option. This is the

case when a user does not have raw packet privileges or is scanning IPv6 networks. Instead

of writing raw packets as most other scan types do, Nmap asks the underlying operating

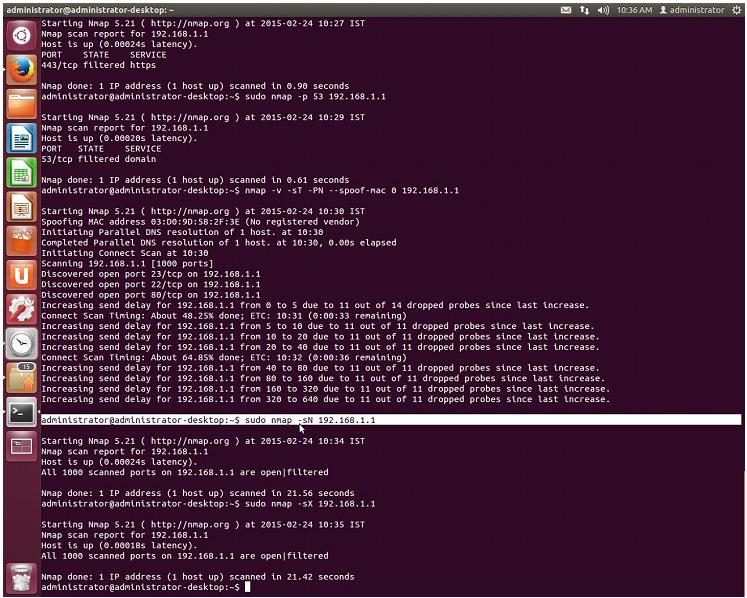
system to establish a connection with the target machine and port by issuing the connect

system call. Along with spoofing.



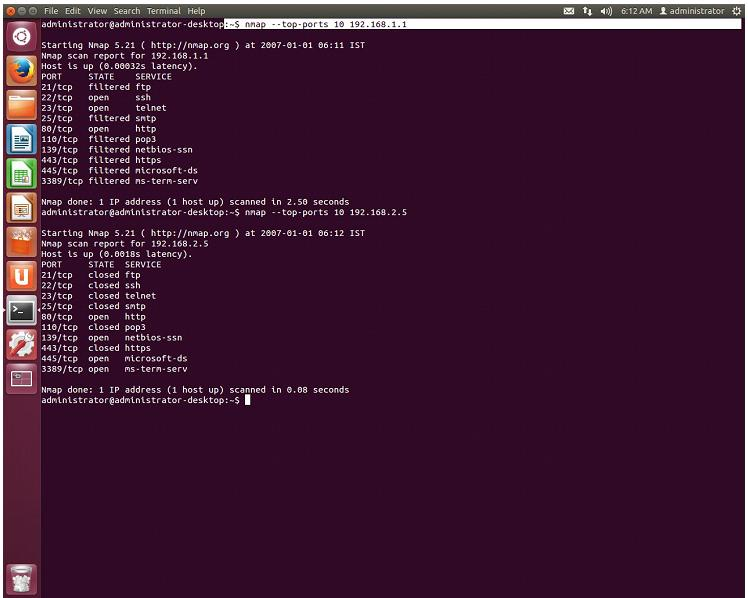
Null scan (-sN):

Does not set any bits (TCP flag header is 0)



--top-ports <integer of 1 or greater>

Scans the N highest-ratio ports found in nmap-services file.



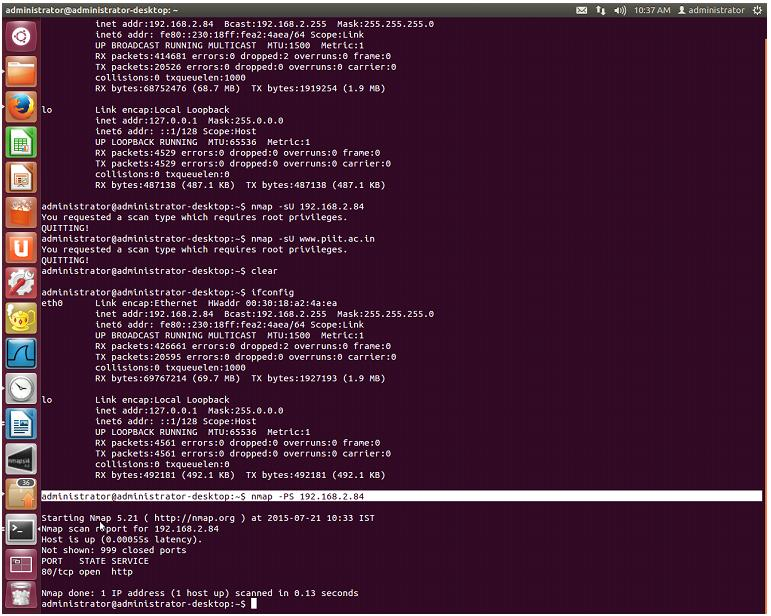
-PS port list (TCP SYN Ping) .

This option sends an empty TCP packet with the SYN flag set. The default destination port is

80 (configurable at compile time by changing DEFAULT\_TCP\_PROBE\_PORT\_SPEC

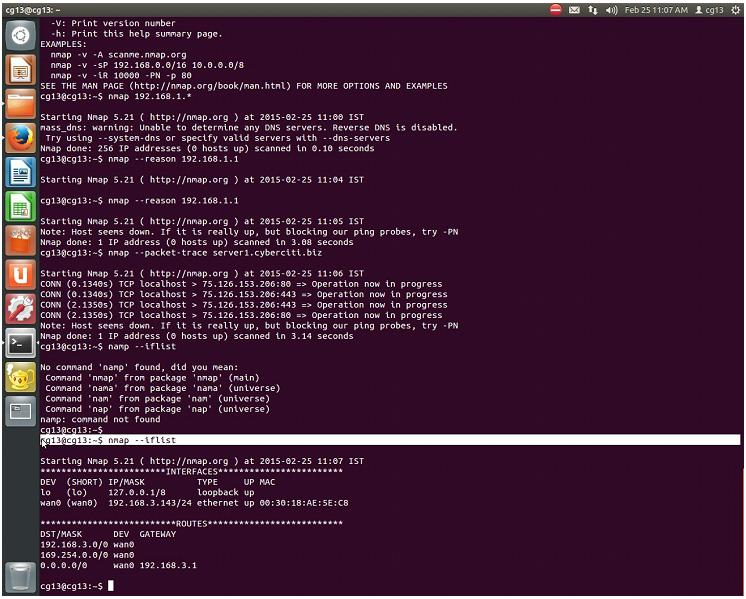
innmap.h). Alternate ports can be specified as a parameter. The syntax is the same as for the

-p except that port type specifiers like T: are not allowed.



nmap –iflist

host interface and route information with nmap by using ―–iflist‖ option.



**6. 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.