Experiment 11

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

Roll No.	19
Name	Manav Jawrani
Class	D15-A
Subject	Security Lab
LO Mapped	LO4: Use tools like sniffers, port scanners and other related tools for analyzing packets in a network.

Aim: Download, install nmap and use it with different options to scan open ports, perform OS fingerprinting, ping scan, tcp port scan,udp port scan, etc.

Introduction:

Nmap: 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:

- **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 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 or IP>

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

Implementation Steps\Installation Steps:
Step 0: Installing Nmap from the link.
$sudo apt-get install nmap

Obtaining Your IP addresses.
Use the ifconfig command in Linux.
Performing a Scan of the Local Network.
Step 1: For the following steps, please use the nmap command line tool installed on Ubuntu

Step 2: Scan your subnet to determine how many hosts can be found. For example, if you are on the192.168.1.0 subnet, you would enter the following command:
$nmap –sP 192.168.1.*

Step 3: Next perform a stealth scan (Please use the IP for your subnet):
$nmap –sS –P0 –p 192.169.1.*

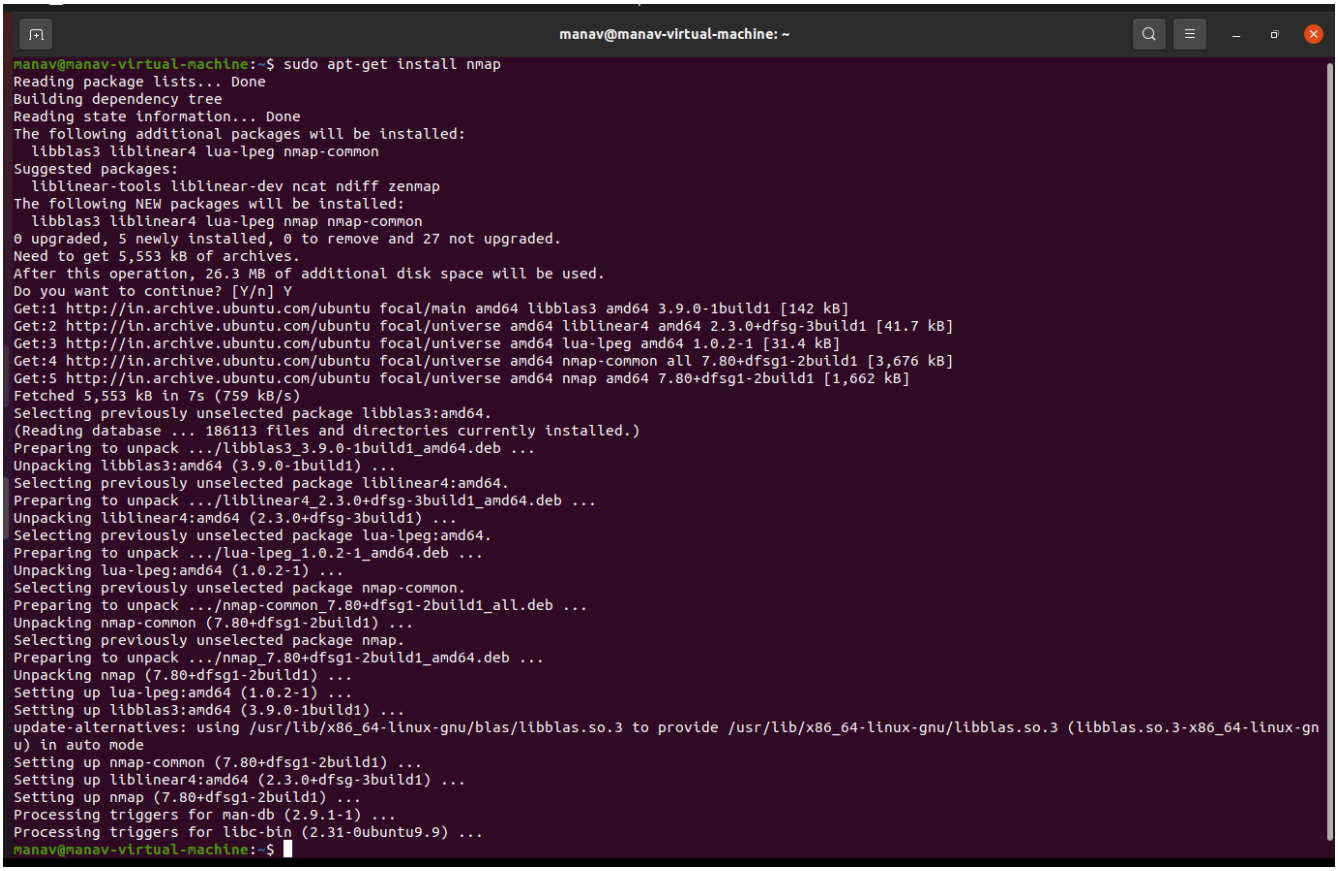
Step 4: Now, you'll perform an OS identification. Use the Linux O/S to scan your Windows machine:
i. nmap –O Windows_IP_ADDRESS
ii. OS Type
iii. Now we want to use the Windows machine to scan the Linux O/S. Go to a Windows DOS prompt and enter the following command:
iv. nmap –O Linux_IP_ADDRESS
v. Now we will perform a service selection scan. Let's scan for all computers with FTP running. We would do that as follows:
$nmap –p21 192.168.1.*

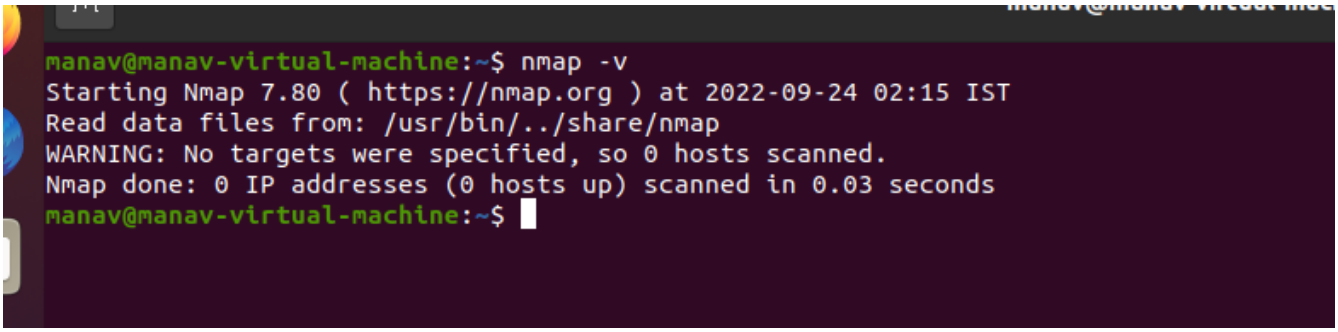
Step 5: List the IP addresses with that has the FTP open:

Input and Output:

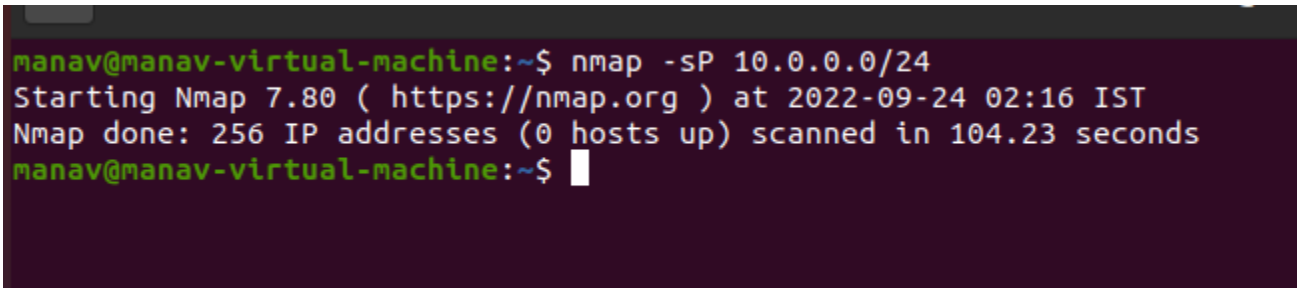
A. Installation of nmap:

$sudo apt-get install nmap

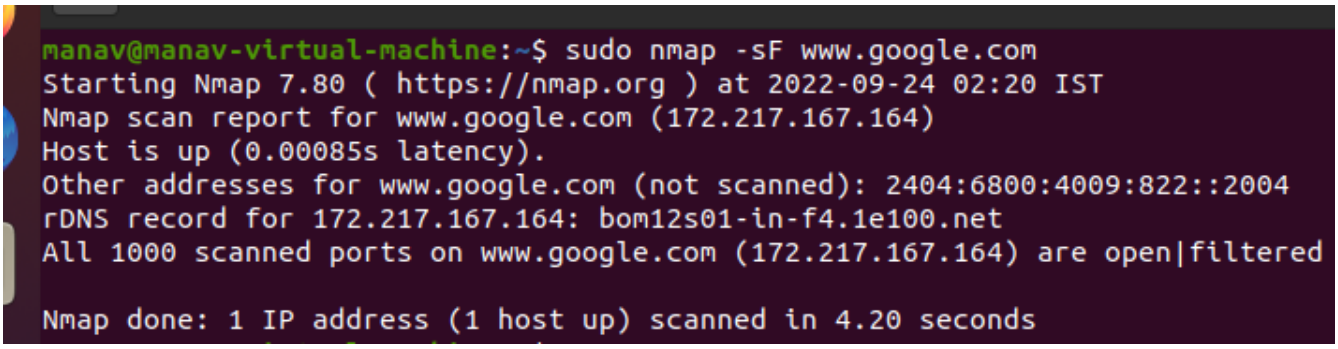




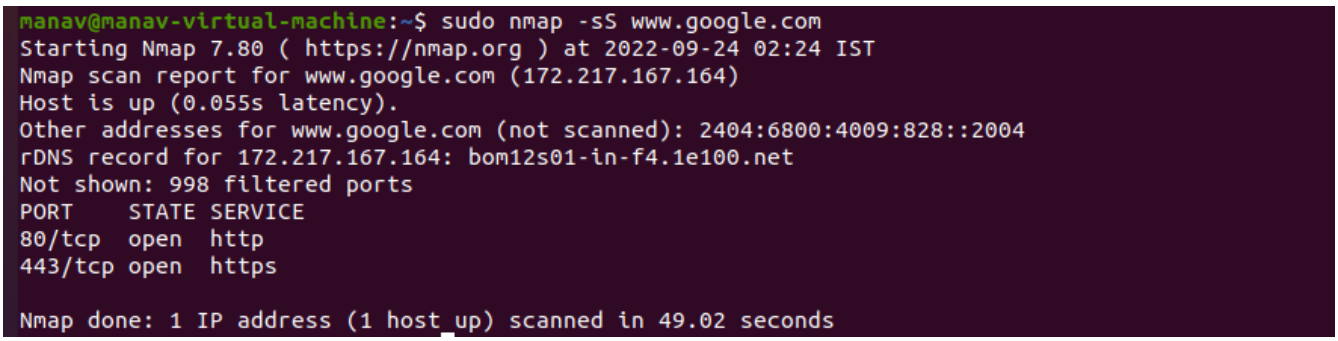
B. $nmap -sP 10.0.0.0/24
Ping scans the network, listing machines that respond to ping.



C. FIN scan (-sF). Sets just the TCP FIN bit.
$sudo nmap -sF www.google.com



D. Scan IP addresses and ports of a website or server
$sudo nmap -sS www.google.com



E. -sV (Version detection):
Enables version detection, as discussed above. Alternatively, can use -A, which enables version detection among other things.
$sudo nmap -A -sV www.google.com

```
manav@manav-virtual-machine:~$ sudo nmap -A -sV www.google.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-24 02:28 IST
Nmap scan report for www.google.com (172.217.174.228)
Host is up (0.0079s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:81d::2004
rDNS record for 172.217.174.228: bom12s03-in-f4.1e100.net
Not shown: 998 filtered ports
PORT    STATE SERVICE   VERSION
80/tcp  open  http      gws
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.0 200 OK
|     Date: Fri, 23 Sep 2022 20:59:57 GMT
|     Expires: -1
|     Cache-Control: private, max-age=0
|     Content-Type: text/html; charset=ISO-8859-1
|     P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
|     Server: gws
|     X-XSS-Protection: 0
|     X-Frame-Options: SAMEORIGIN
|     Set-Cookie: 1P_JAR=2022-09-23-20; expires=Sun, 23-Oct-2022 20:59:57 GMT; path=/; domain=.google.com; Secure
|     Set-Cookie: AEC=AakniGOdsqgQxDoWLbZlb8n_z_8oya5OOp7fB9n2x9DZ7U2foPCakOUEGw; expires=Wed, 22-Mar-2023 20:59:57 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax
|     Set-Cookie: NID=511=u76iR-uR6V25yrJjJXb9Z_S0cq2lz03oTRbkyyOa4GrqbnGYhDi1GabZ5TNS3Thik7R_lJY6ky49QXhLDvOXKknBwIMjPrtBE1dxHLxOIRYrnZGqK8F4UEvxzOeisExhQie8oP1LavvnmFEryIEP2wf5ZfXPevtmWEtPFuJyly4; expi
res=Sat, 25-Mar-2023 20:59:57 GMT; path=/; domain=.google.com; HttpOnly
|     Accept-Ranges: none
|     Vary: Accept-Encoding
|     <!doctype html><html
|   HTTPOptions:
|     HTTP/1.0 405 Method Not Allowed
|     Allow: GET, HEAD
|     Date: Fri, 23 Sep 2022 20:59:57 GMT
|     Content-Type: text/html; charset=UTF-8
|     Server: gws
|     Content-Length: 1592
|     X-XSS-Protection: 0
|     X-Frame-Options: SAMEORIGIN
|     <!DOCTYPE html>
|     <html lang=en>
|     <meta charset=utf-8>
|     <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width">
|     <title>Error 405 (Method Not Allowed)!!1</title>
|     <style>
|_    *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{backg
round:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-w
idth:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#l
|_http-favicon: Google
| http-robots.txt: 226 disallowed entries (15 shown)
| /search /sdch /groups /index.html? /? /?hl=*&
```

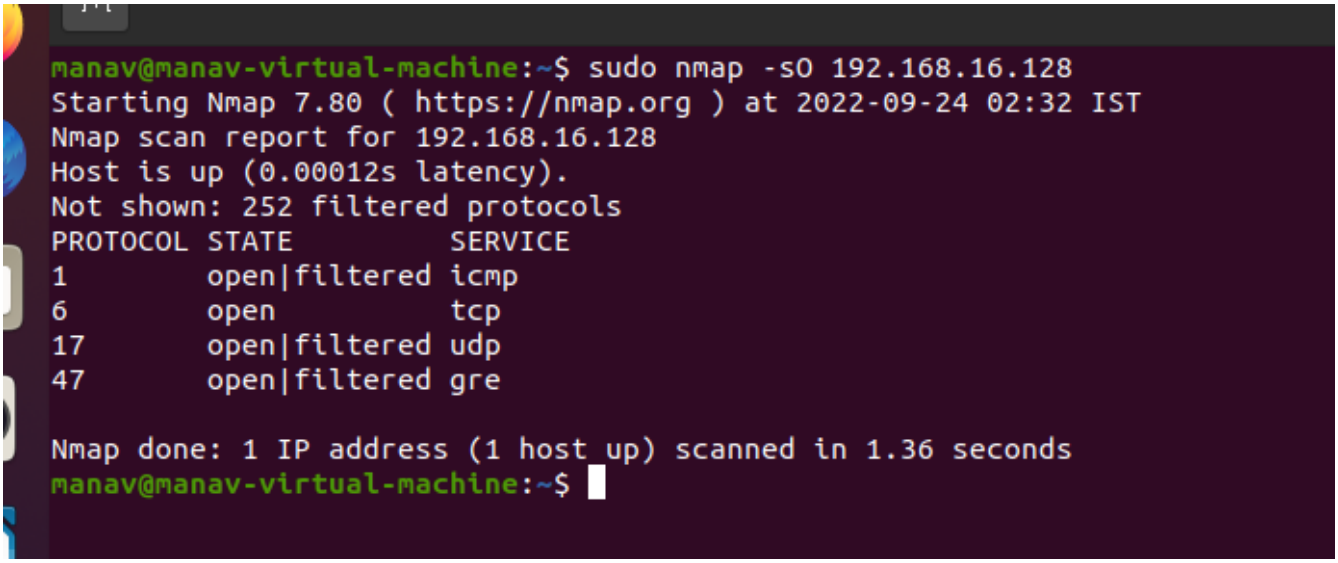
```
SF:%r(GetRequest,2602,"HTTP/1\.0\x20200\x20OK\r\nDate:\x20Fri,\x2023\x20Se
SF:p\x202022\x2021:00:03\x20GMT\r\nExpires:\x20-1\r\nCache-Control:\x20pri
SF:vate,\x20max-age=0\r\nContent-Type:\x20text/html;\x20charset=ISO-8859-1
SF:\r\nP3P:\x20CP=\"This\x20is\x20not\x20a\x20P3P\x20policy!\x20See\x20g\.
SF:co/p3phelp\x20for\x20more\x20info\.\"\r\nServer:\x20gws\r\nX-XSS-Protec
SF:tion:\x200\r\nX-Frame-Options:\x20SAMEORIGIN\r\nSet-Cookie:\x201P_JAR=2
SF:022-09-23-21;\x20expires=Sun,\x2023-Oct-2022\x2021:00:03\x20GMT;\x20pat
SF:h=/;\x20domain=\.google\.com;\x20Secure\r\nSet-Cookie:\x20AEC=AakniGMfA
SF:0imUfVGwBAj9t6ooRj5rKYQQ9nkPUr3bLFuzC1Q90K5XuGqNMc;\x20expires=Wed,\x20
SF:22-Mar-2023\x2021:00:03\x20GMT;\x20path=/;\x20domain=\.google\.com;\x20
SF:Secure;\x20HttpOnly;\x20SameSite=lax\r\nSet-Cookie:\x20NID=511=vVvXywwF
SF:hwfNRQcBVWBWmDHKgFMwaokrEgPkcapwdPqrYV831CifmGAy_j3O4G1Fpa5fYegJWCf9ZxI
SF:5ZnX2Lak_3Xts9oROkU9G1UPsRWH5JIZdevzvUbuKnI5nPZm1q-BgAxwta3SdAgHj1u1c9T
SF:aXmR8WHJgFSLlCA8vsvpU;\x20expires=Sat,\x2025-Mar-2023\x2021:00:03\x20GM
SF:T;\x20path=/;\x20domain=\.google\.com;\x20HttpOnly\r\nAlt-Svc:\x20h3=\"
SF::443\";\x20ma=2592000,h3-29=\":443\";\x20ma=2592000,h3-Q050=\":")%r(HTT
SF:POptions,7BC,"HTTP/1\.0\x20405\x20Method\x20Not\x20Allowed\r\nAllow:\x2
SF:0GET,\x20HEAD\r\nDate:\x20Fri,\x2023\x20Sep\x202022\x2021:00:04\x20GMT\
SF:r\nContent-Type:\x20text/html;\x20charset=UTF-8\r\nServer:\x20gws\r\nCo
SF:ntent-Length:\x201592\r\nX-XSS-Protection:\x200\r\nX-Frame-Options:\x20
SF:SAMEORIGIN\r\nAlt-Svc:\x20h3=\":443\";\x20ma=2592000,h3-29=\":443\";\x2
SF:0ma=2592000,h3-Q050=\":443\";\x20ma=2592000,h3-Q046=\":443\";\x20ma=259
SF:2000,h3-Q043=\":443\";\x20ma=2592000,quic=\":443\";\x20ma=2592000;\x20v
SF:=\"46,43\"\r\n\r\n<!DOCTYPE\x20html>\n<html\x20lang=en>\n\x20\x20<meta\
SF:x20charset=utf-8>\n\x20\x20<meta\x20name=viewport\x20content=\"initial-
SF:scale=1,\x20minimum-scale=1,\x20width=device-width\">\n\x20\x20<title>E
SF:rror\x20405\x20\(Method\x20Not\x20Allowed\)!!1</title>\n\x20\x20<style>
SF:\n\x20\x20\x20\x20\*{margin:0;padding:0}html,code{font:15px/22px\x20ari
SF:al,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:
SF:7%\x20auto\x200;max-width:390px;min-height:180px;padding:30px\x200\x201
SF:5px}\*\x20>\x20body{background:url\(//www\.google\.com/images/errors/ro
SF:bot\.png\)\x20100%\x205px\x20no-repeat;padding-right:205px}p{margin:11p
SF:x\x200\x2022p");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized
Running: Microsoft Windows XP|7|2012, VMware Player
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:player
OS details: Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, VMware Player virtual NAT device
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.08 ms _gateway (192.168.189.2)
2   0.06 ms bom12s03-in-f4.1e100.net (172.217.174.228)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 124.10 seconds
manav@manav-virtual-machine:~$
```

F. -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 ́t technically a port scan, since it cycles through

IP protocol numbers rather than TCP or UDP port numbers.

$sudo nmap -sO 192.168.16.128



G. -O (Enable OS detection) .

Enables OS detection, as discussed above. Alternatively, you can use -A to enable OS detection along with other things.

$sudo nmap -A 192.168.16.128

H. -p port ranges (Only scan specific 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.

$sudo nmap -p 413 192.168.16.128

```
manav@manav-virtual-machine:~$ sudo nmap -p 413 192.168.16.128
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-24 02:36 IST
Nmap scan report for 192.168.16.128
Host is up (0.0011s latency).

PORT    STATE    SERVICE
413/tcp filtered smsp

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
manav@manav-virtual-machine:~$
```

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

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

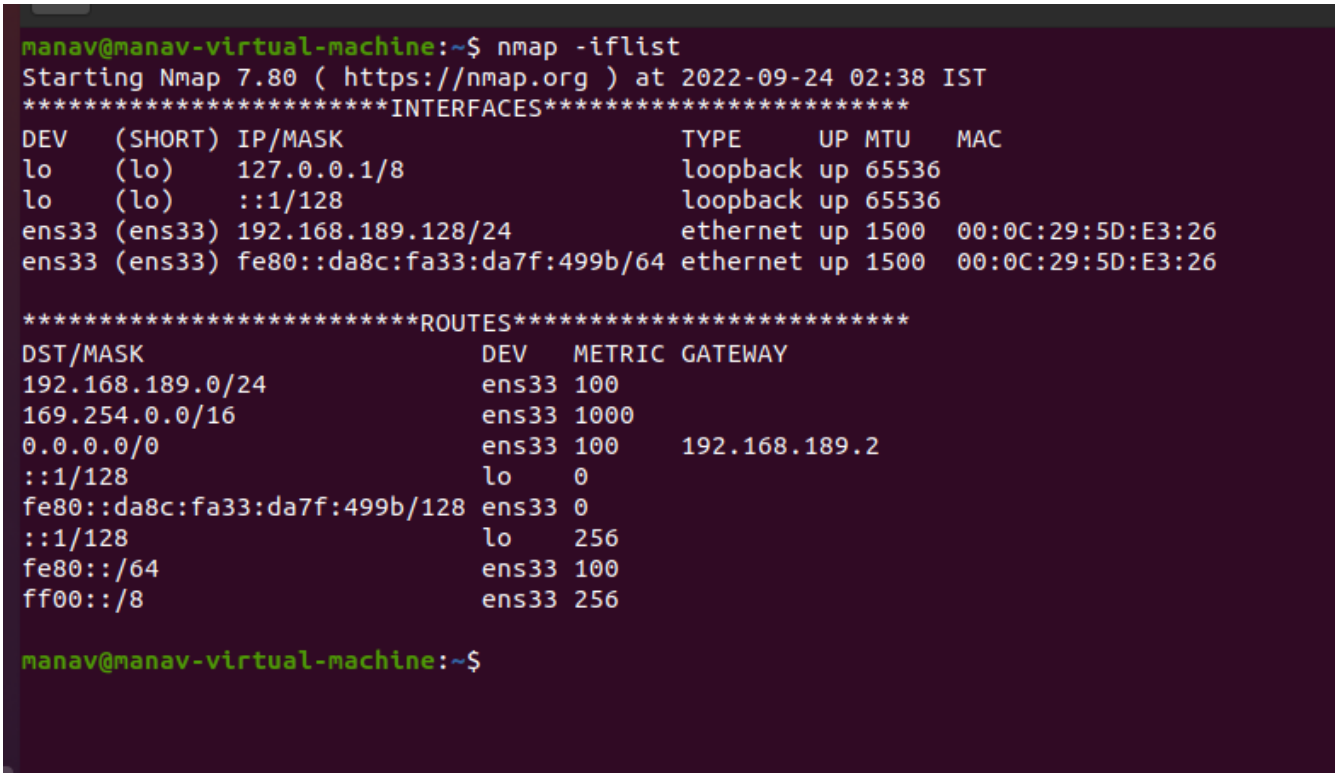
$sudo nmap --top-ports 10 192.168.16.128

```
manav@manav-virtual-machine:~$ sudo nmap --top-ports 10 192.168.16.128
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-24 02:37 IST
Nmap scan report for 192.168.16.128
Host is up (0.0010s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
80/tcp   filtered http
110/tcp  filtered pop3
139/tcp  filtered netbios-ssn
443/tcp  filtered https
445/tcp  filtered microsoft-ds
3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 1.39 seconds
manav@manav-virtual-machine:~$
```

J. nmap –iflist

Host interface and route information with nmap by using –iflist option.

$nmap -iflist



Conclusion:

Thus, we have Downloaded, installed nmap and used it with different options to scan open ports, perform OS fingerprinting, ping scan, tcp port scan,udp port scan, etc.