Network scanning using Nmap

Name-> Vijay Bhushan Singh
E-mail-> vijay8303blw@gmail.com
College-> Indian Institute of Information Technology, Manipur
Phone_no-> 8303420912

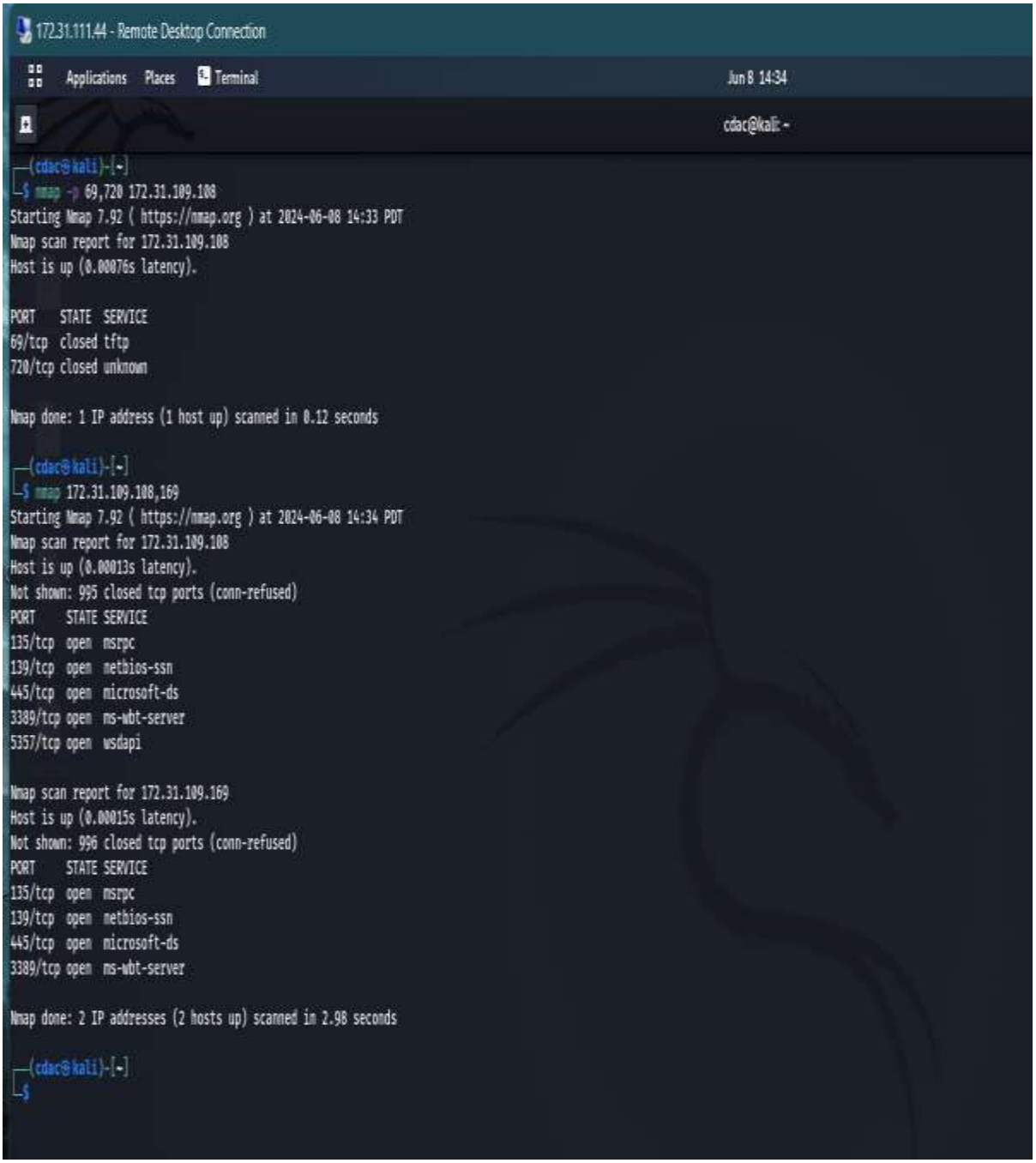
---

1) Basic Nmap Scan against IP or host.

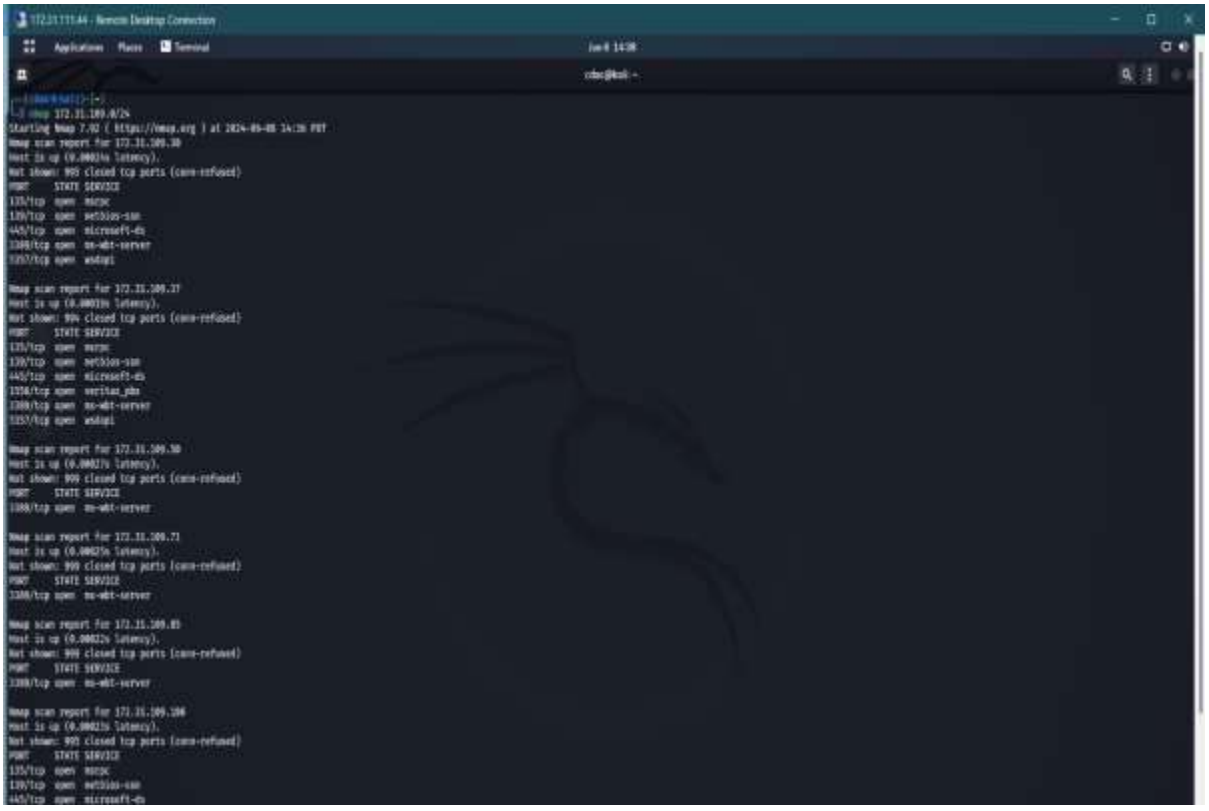
2) Scan specific ports or scan entire port ranges on a local or remote server.

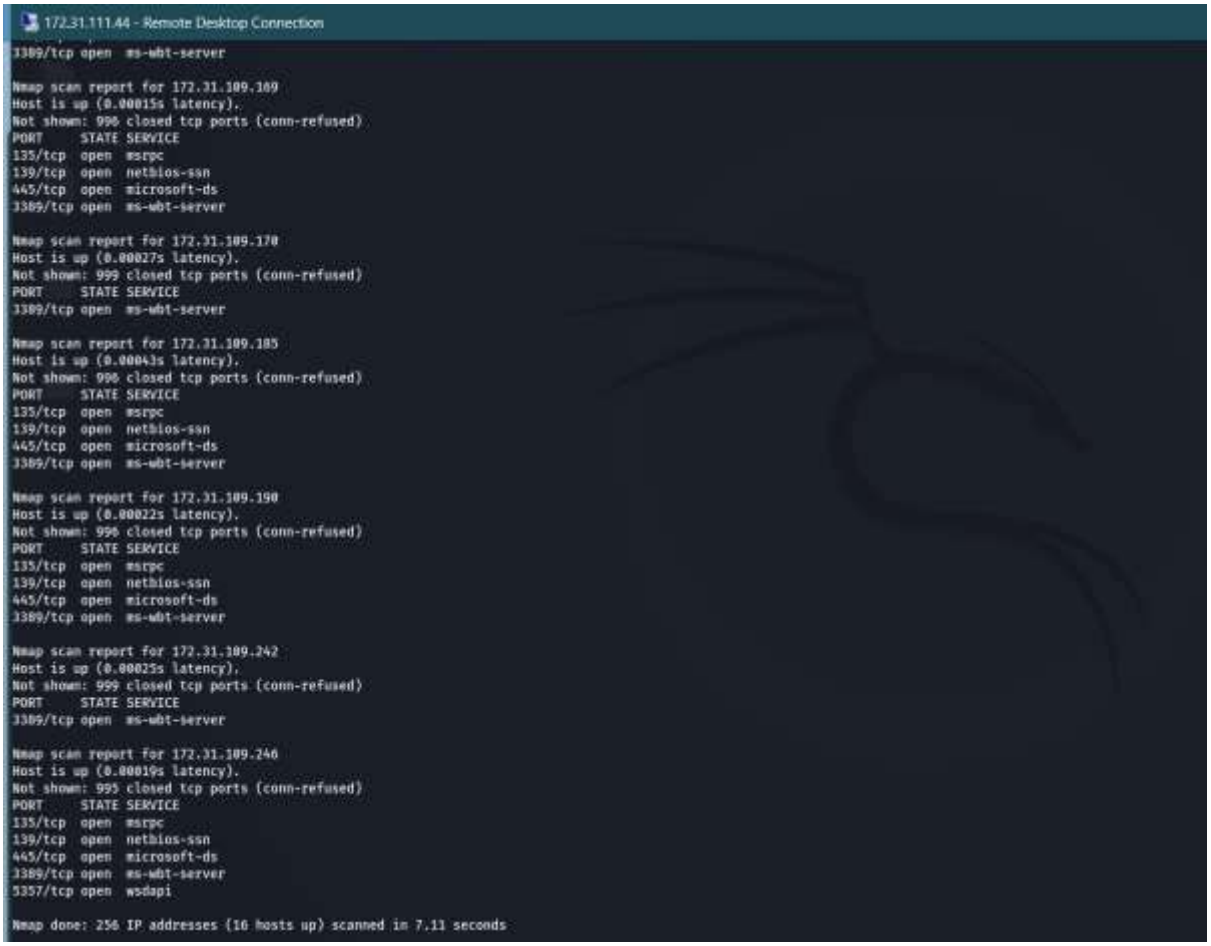
3) Nmap is able to scan all possible ports, but it can also scan specific ports.

4) Scan multiple IP addresses.

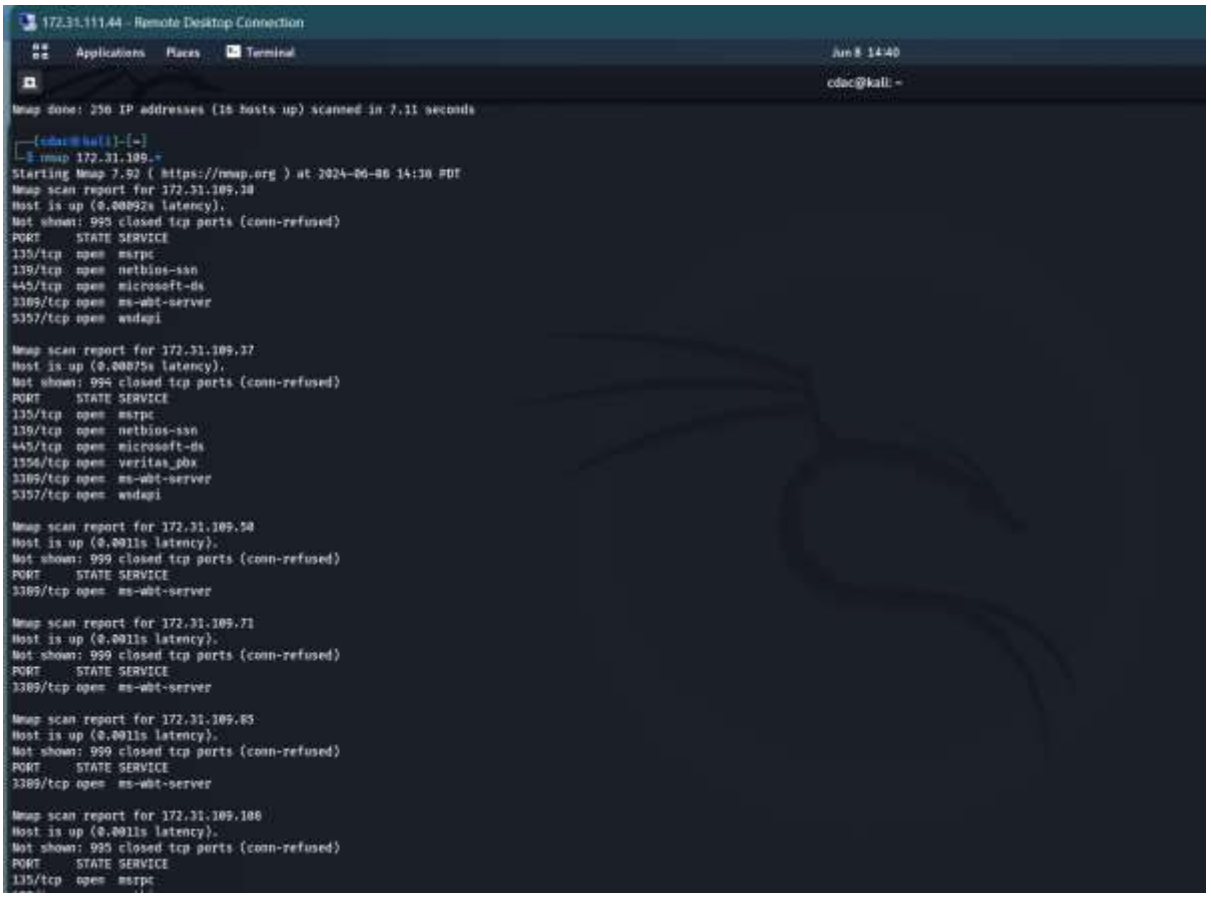


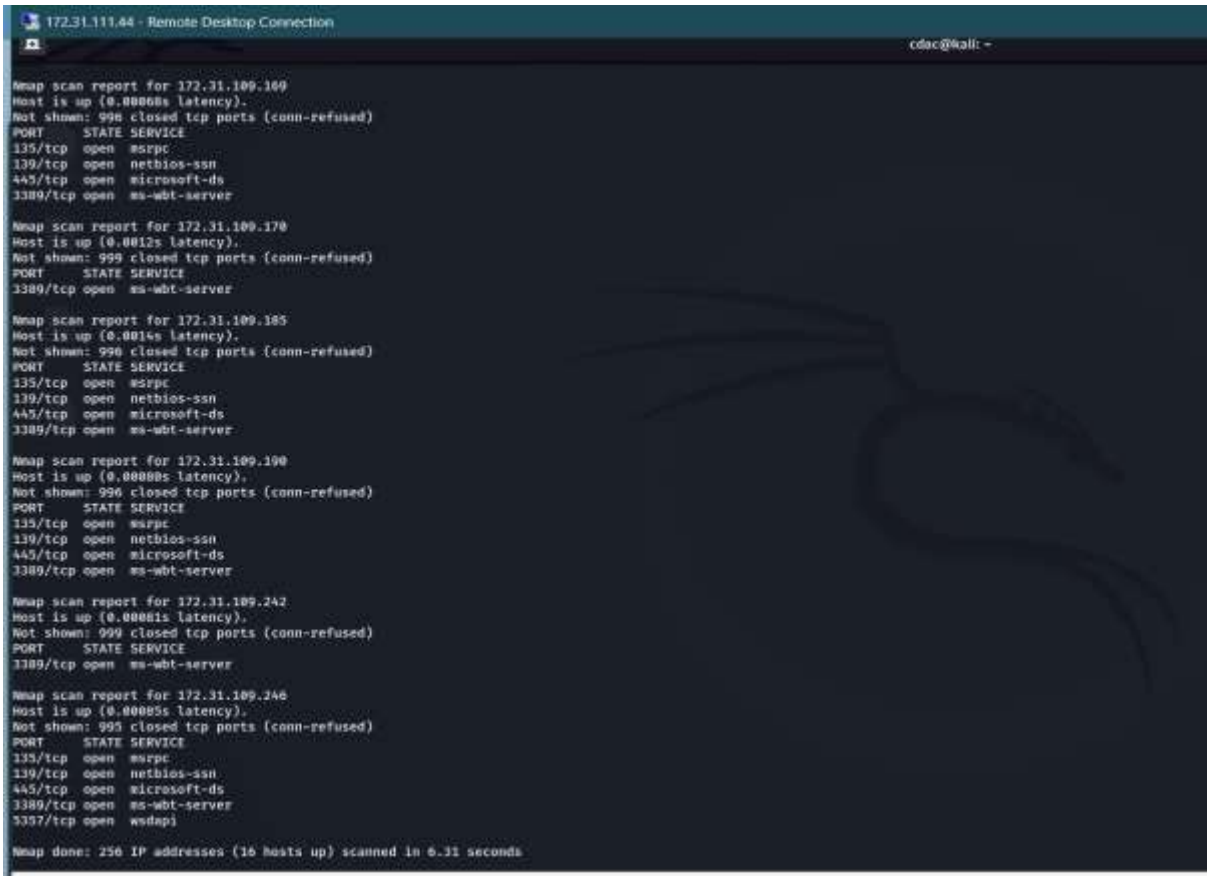
5) Scan IP ranges.



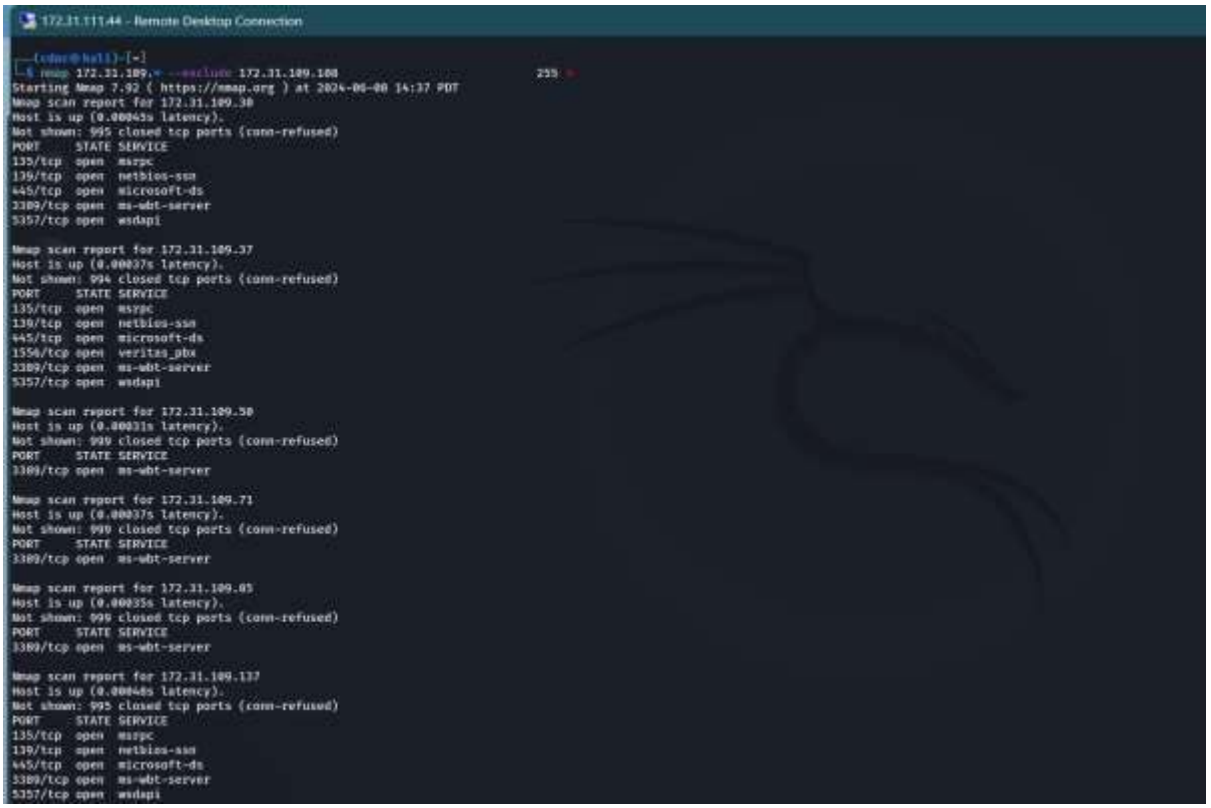


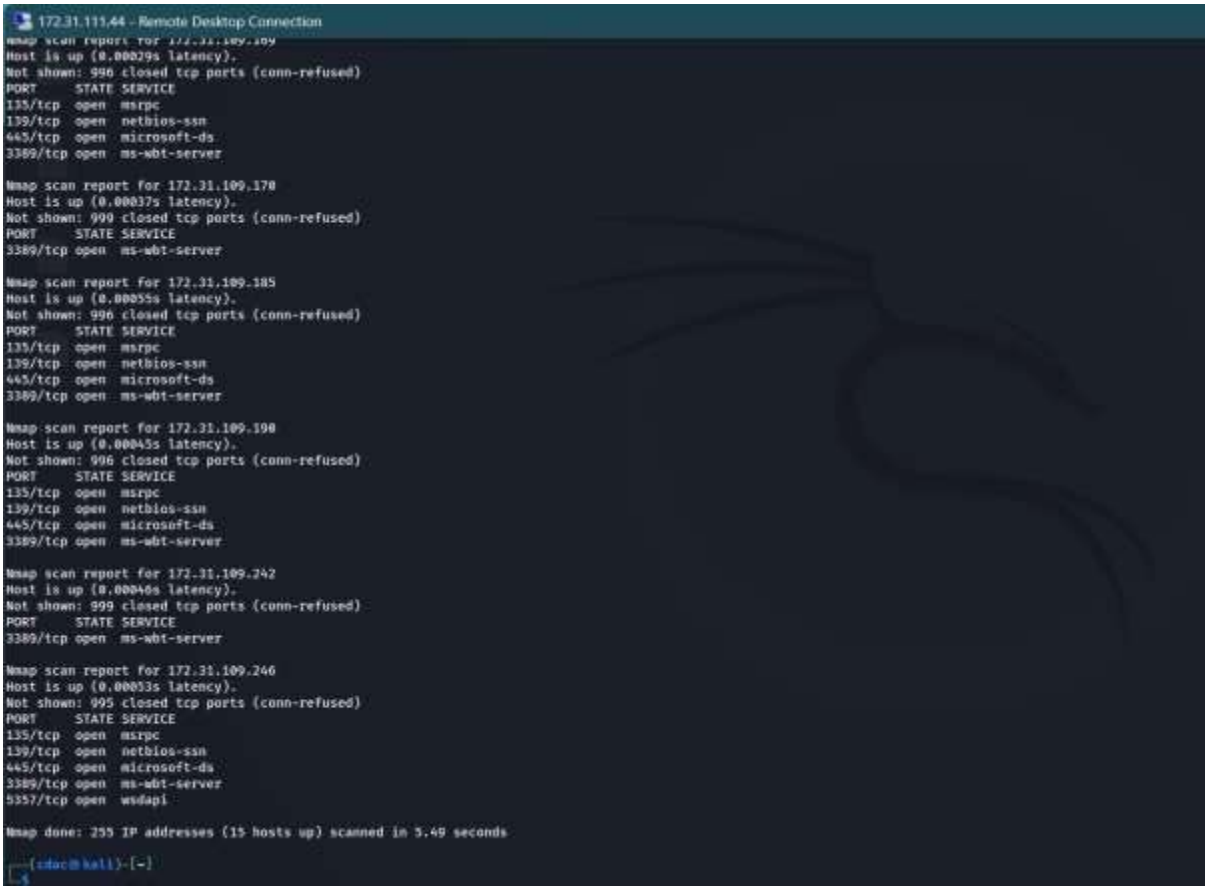
Scanning the class range using (*)



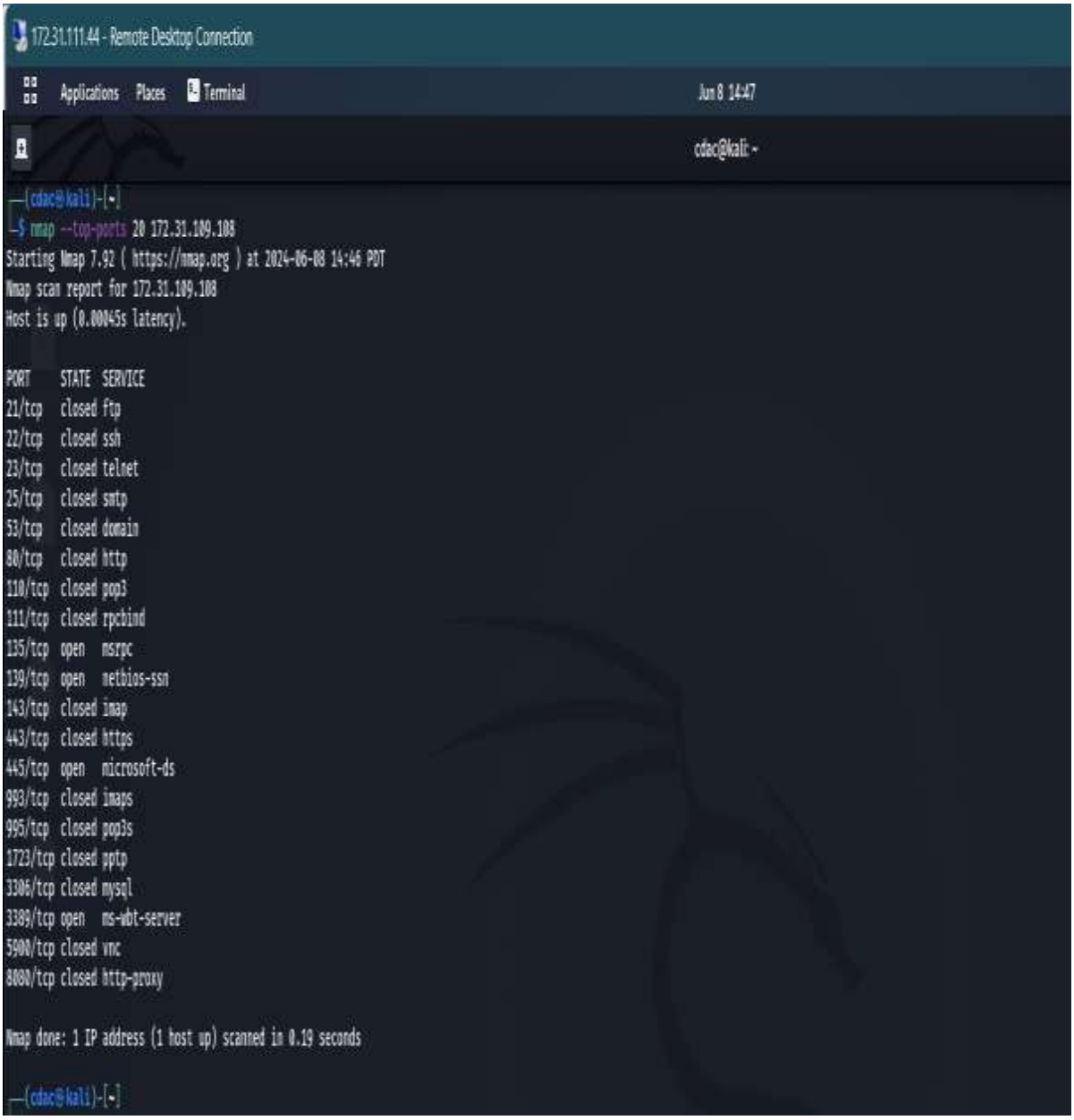


When scanning entire range we may need to exclude some IP address



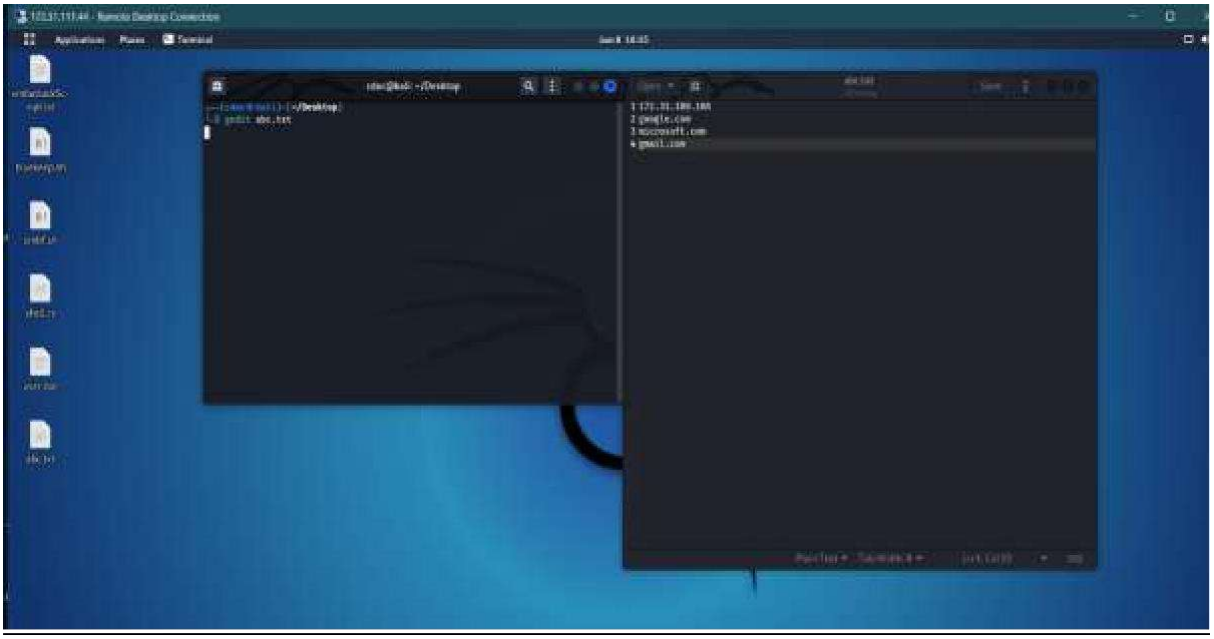


6) Scan the most popular ports.



7) Scan hosts and IP addresses reading from a text file.

TEXT FILE NAME- abc.txt

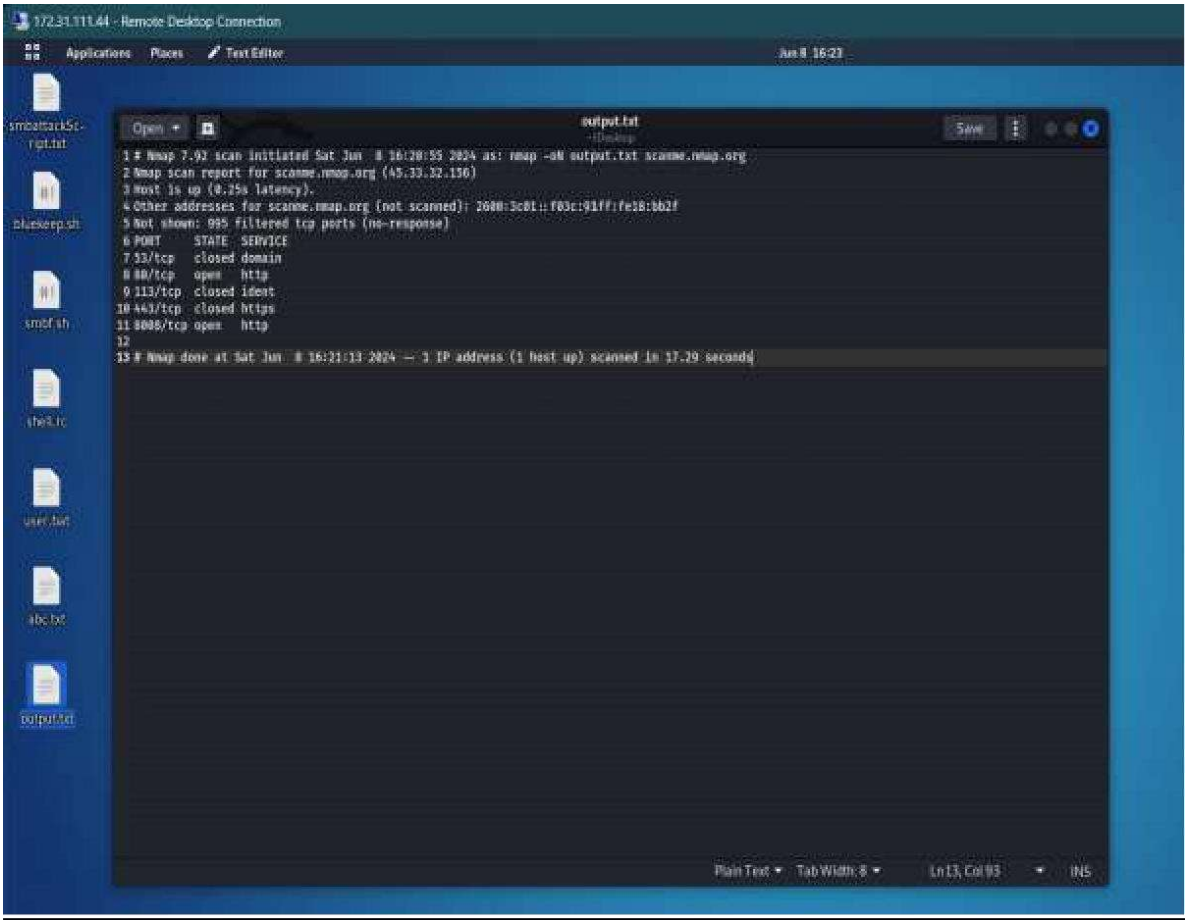


Scanning all the hosts listed.

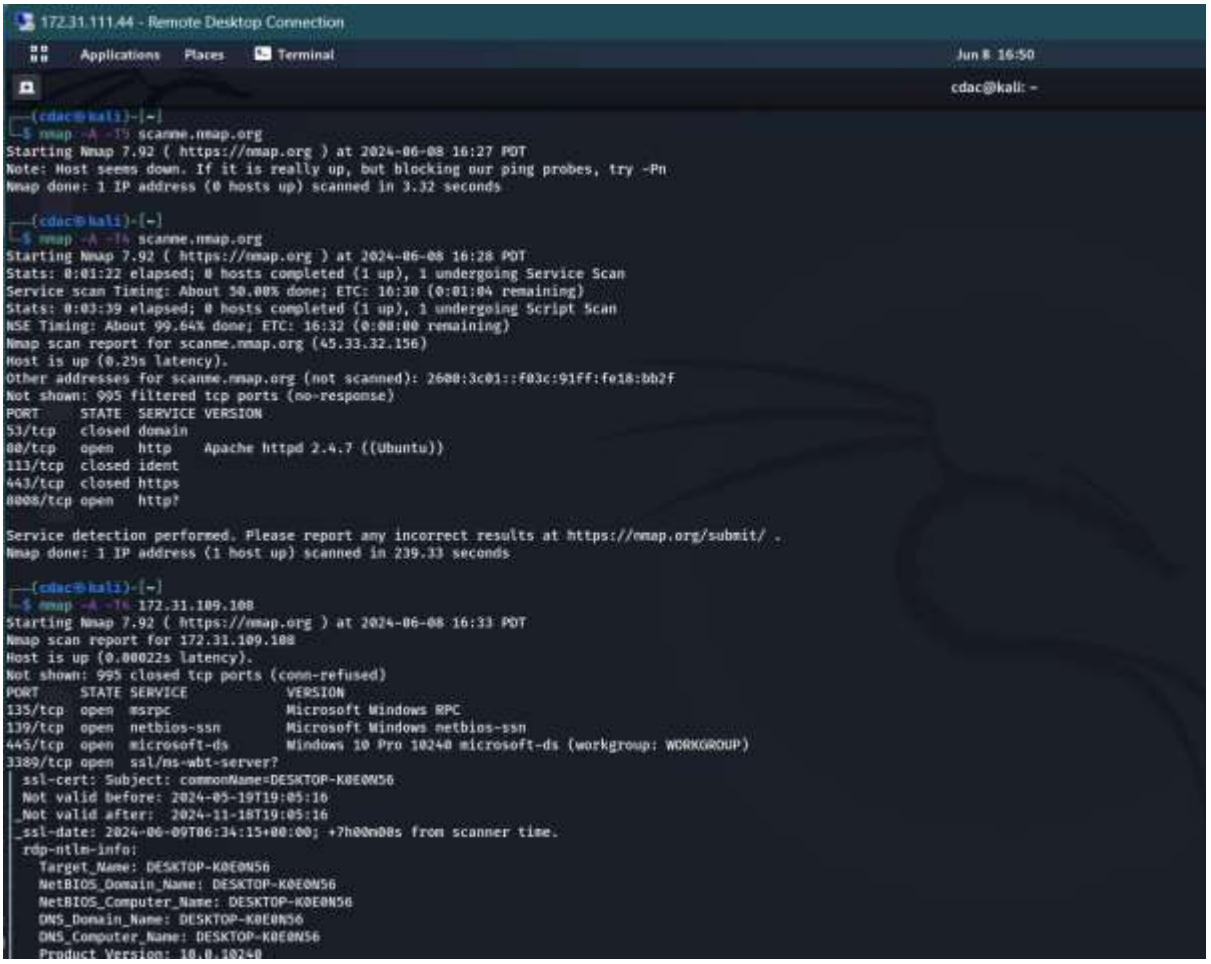
8) Save your Nmap scan results to a file.

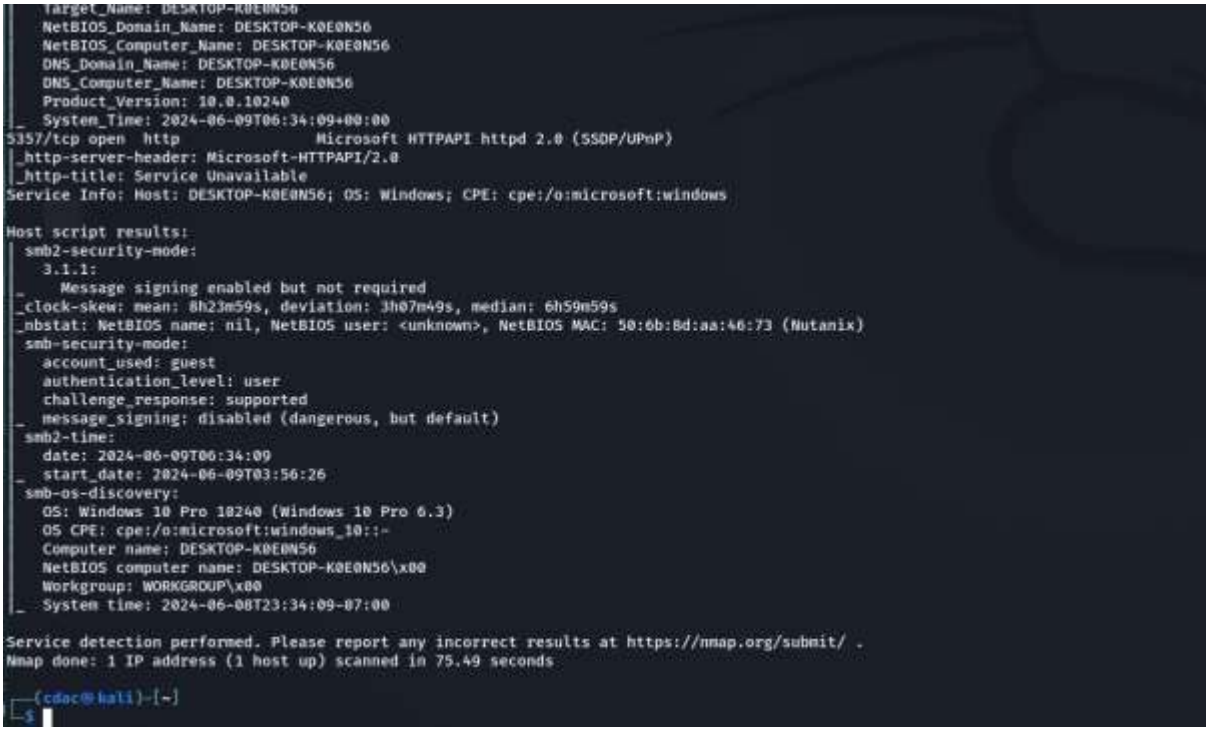
```
Nmap done: 4 IP addresses (4 hosts up) scanned in 30.18 seconds

┌──(cdac㉿kali)-[~/Desktop]
└─$ nmap -oN output.txt scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-08 16:20 PDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE  SERVICE
53/tcp   closed domain
80/tcp   open   http
113/tcp  closed ident
443/tcp  closed https
8008/tcp open   http

Nmap done: 1 IP address (1 host up) scanned in 17.29 seconds

┌──(cdac㉿kali)-[~/Desktop]
└─$
```

OUTPUT FILE- output.txt



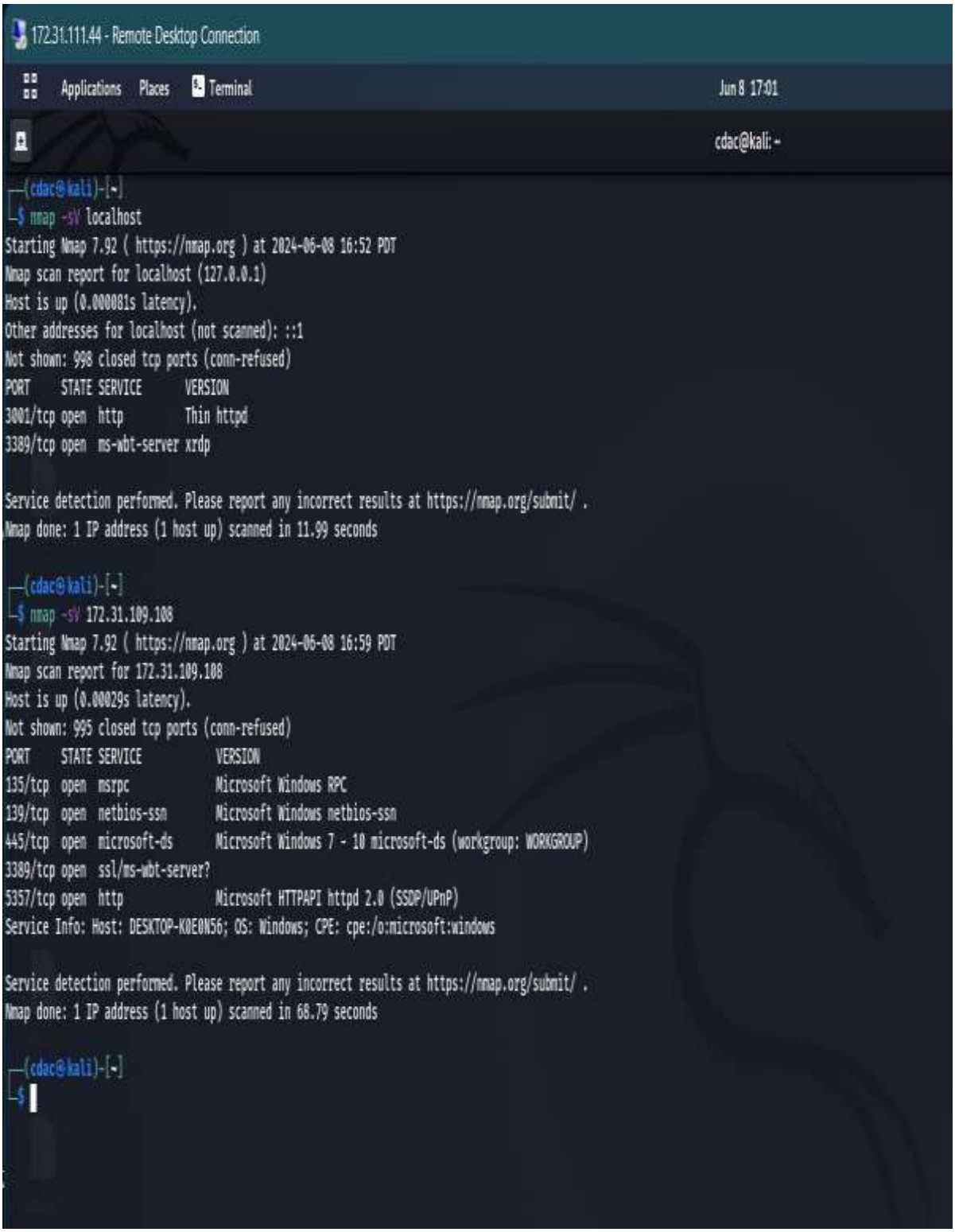
9) Scan + OS and service detection <u>with fast execution</u>.





nmap may control the speed of scanning also (very slow (-T0) to extremely aggressive (-T5)).

10) Detect service/daemon versions.



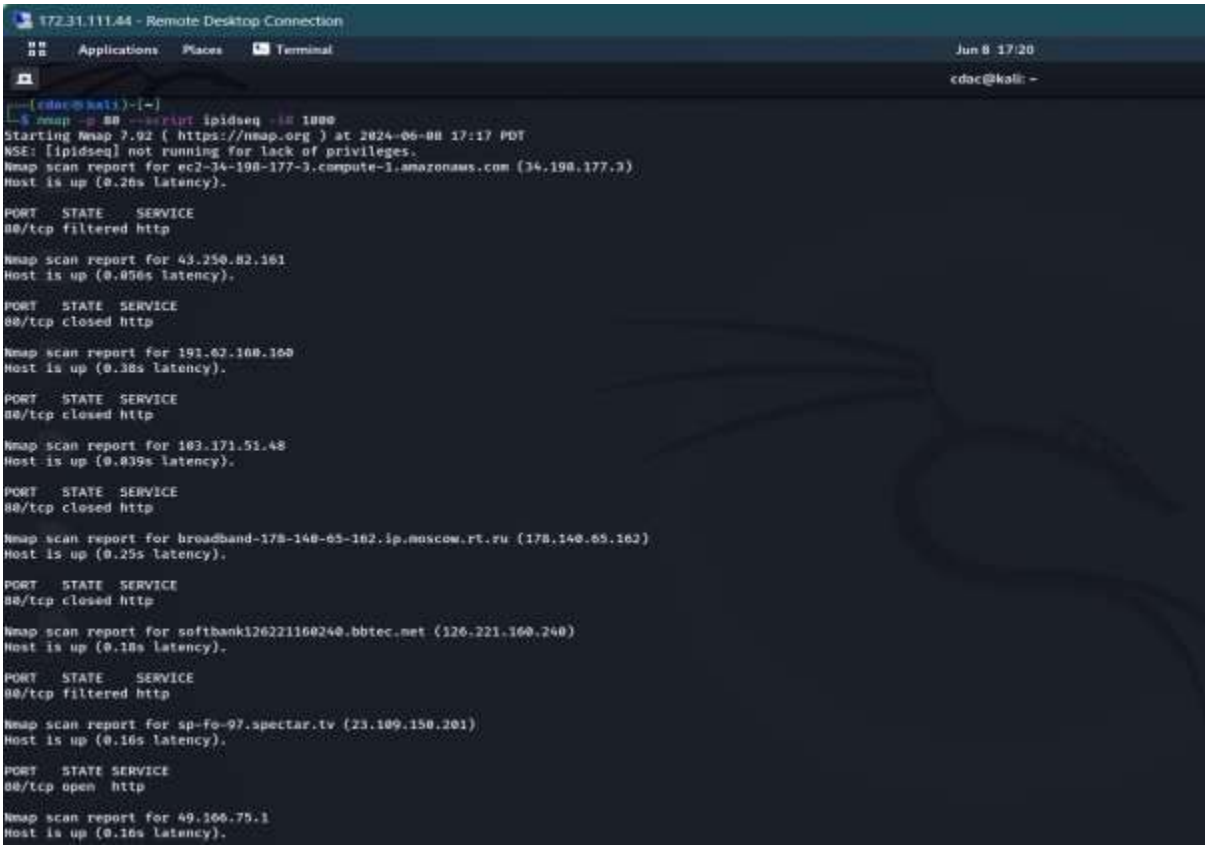
11) Scan using TCP or UDP protocols.

TCP protocol:

UDP Protocol:

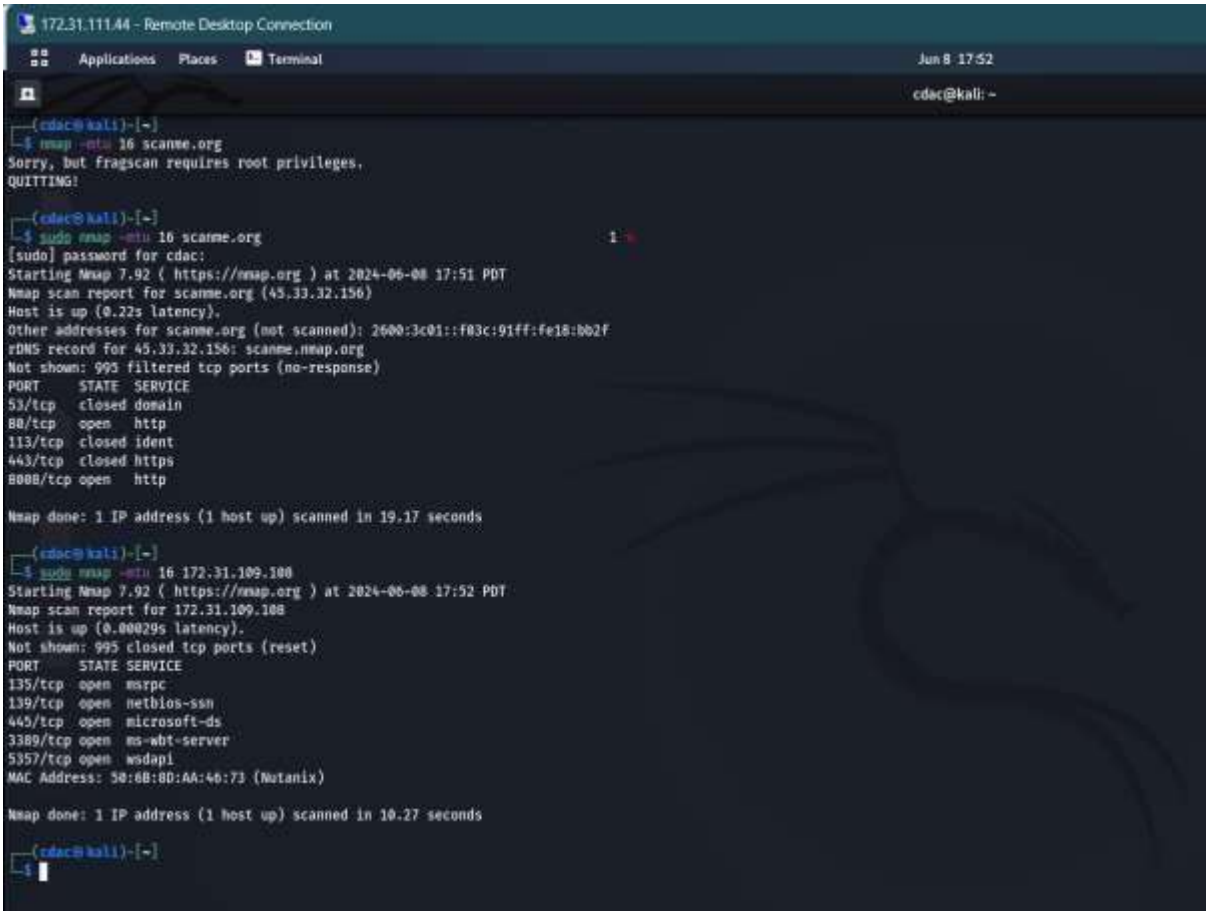
12) Finding <u>multiple live hosts</u> in the network.

14) Finding the system with incremental ip-id.



15) Performing idle scanning using nmap(zombie scanning).

16) Bypassing firewall using fragmentation.

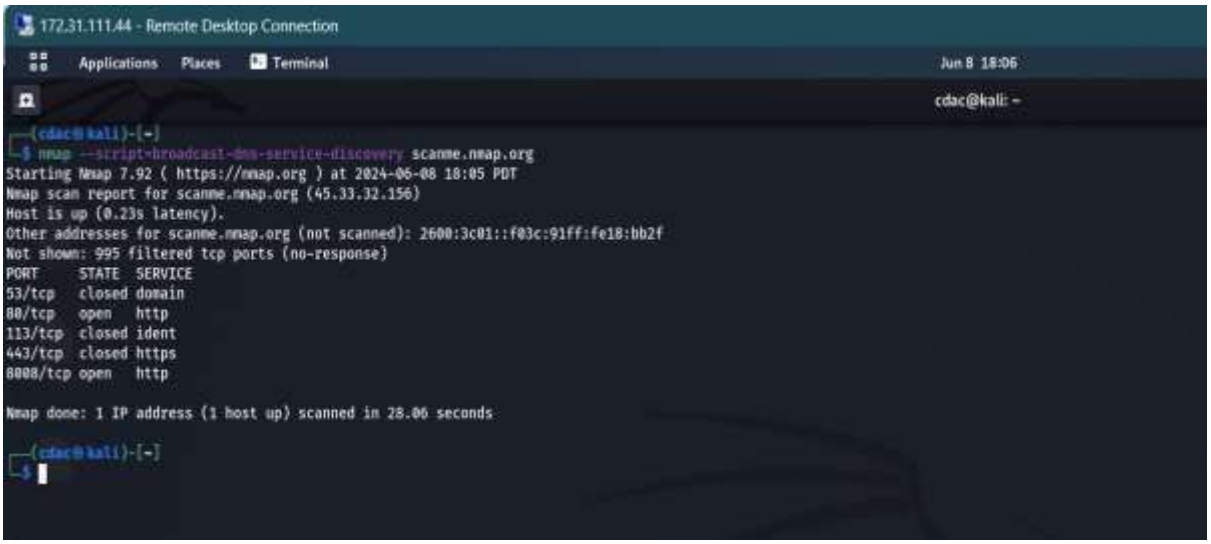


17) Stealthy scan to avoid firewall detection.

18) Using Nmap Script engine.

USING:

19) DNS Enumeration.



Trying to enumerate DNS hostnames by brute force guessing of common subdomains.