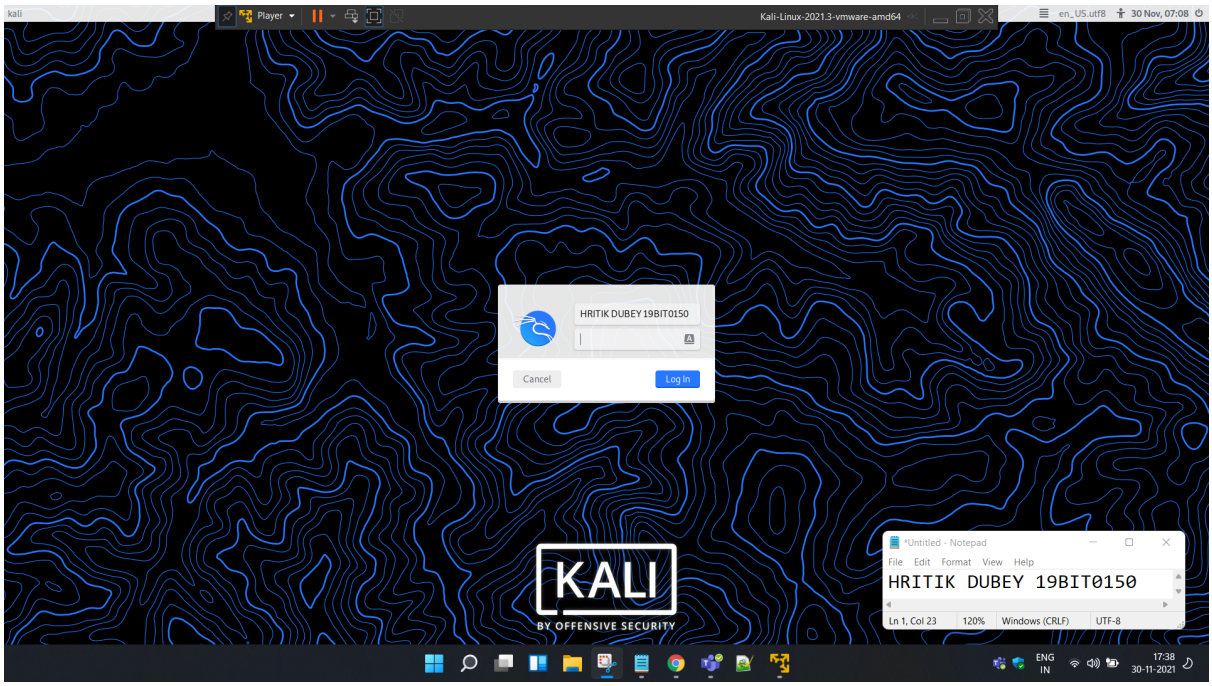
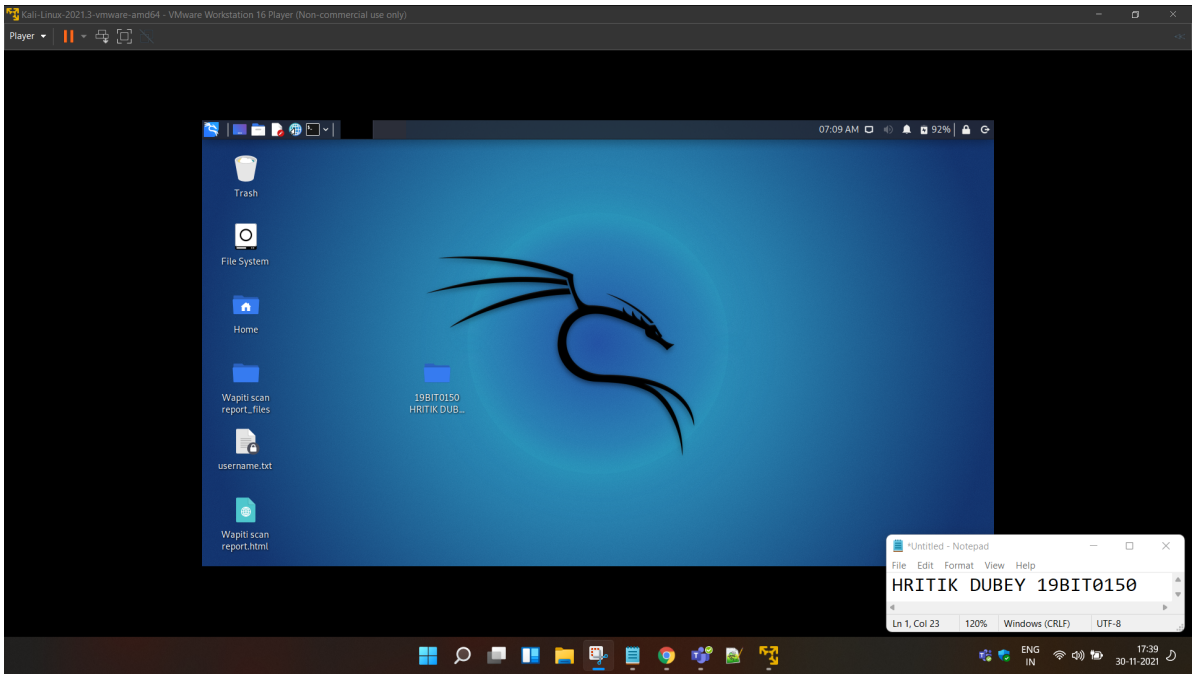
CSE3501-Information Security Analysis and Audit Lab

NAME- HRITIK DUBEY REG NO-19BIT0150 SLOT- L41+L42

DIGITAL ASSIGNMENT 5 Faculty : Dr. Priya V

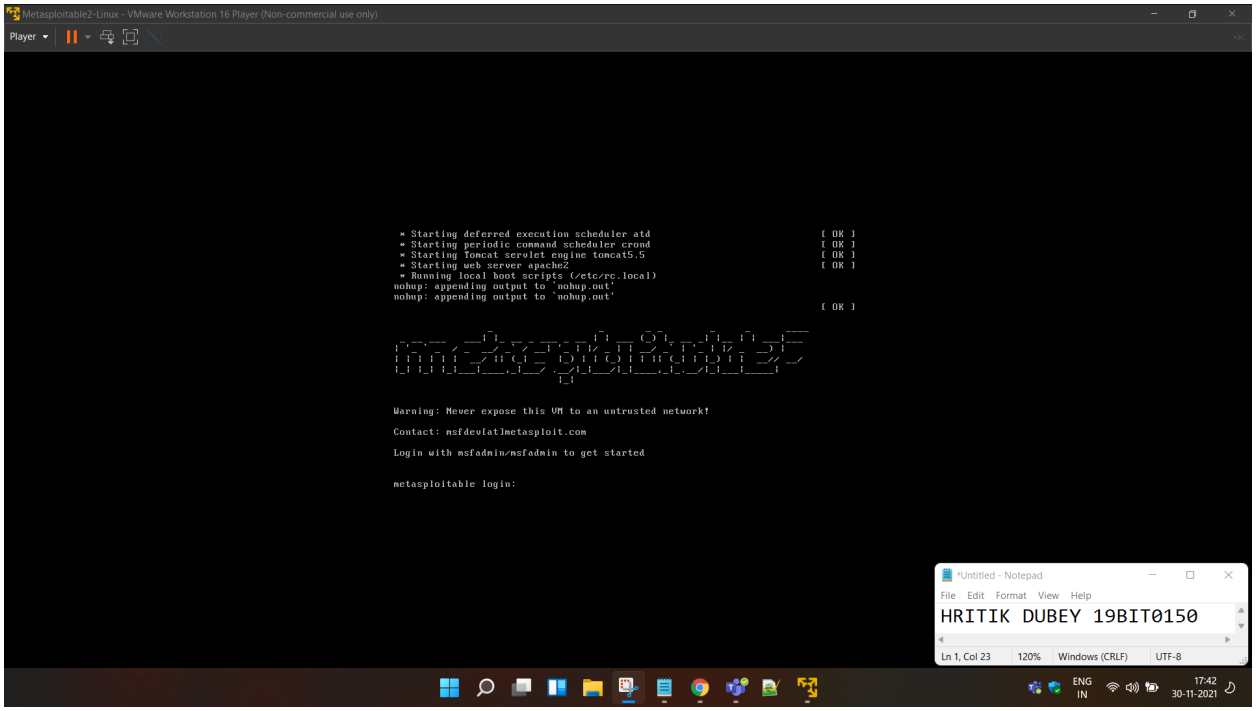
1. Install Kali Linux

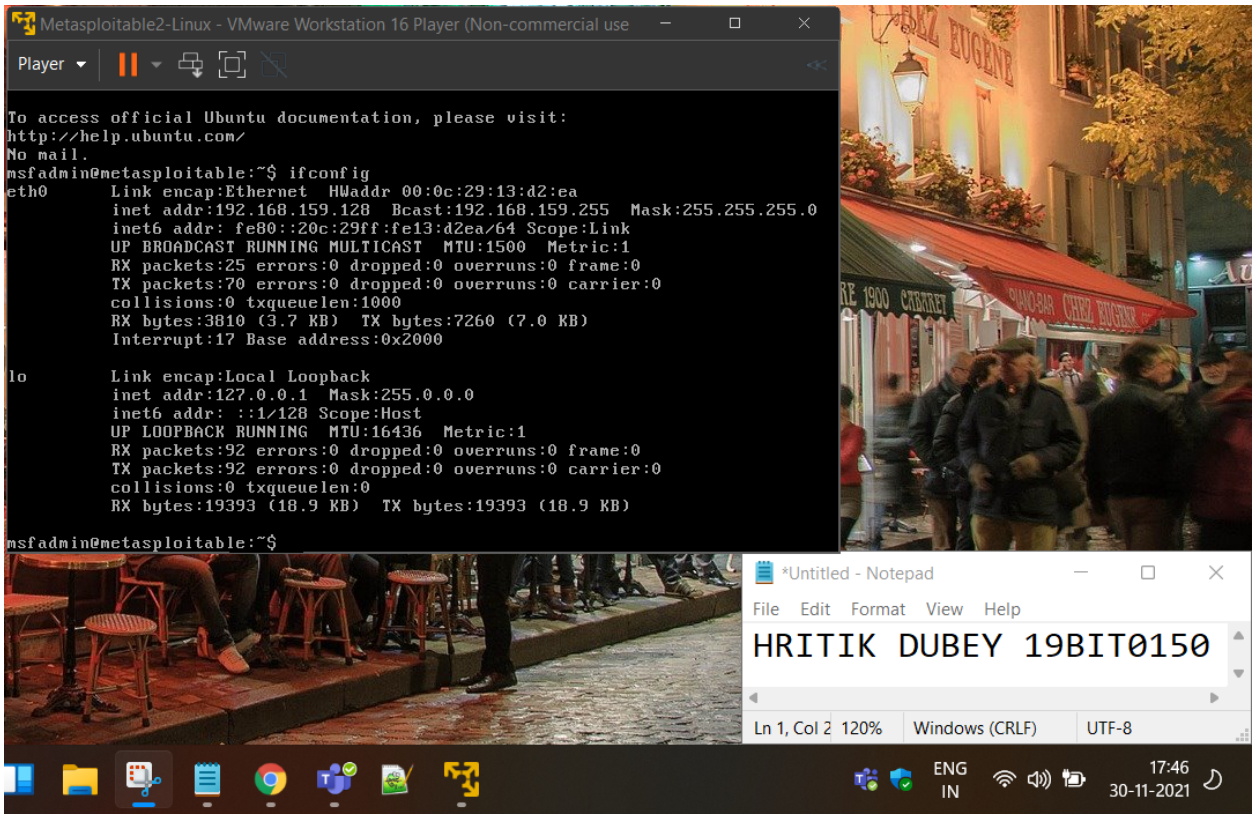




2. Install Metasploitable VM

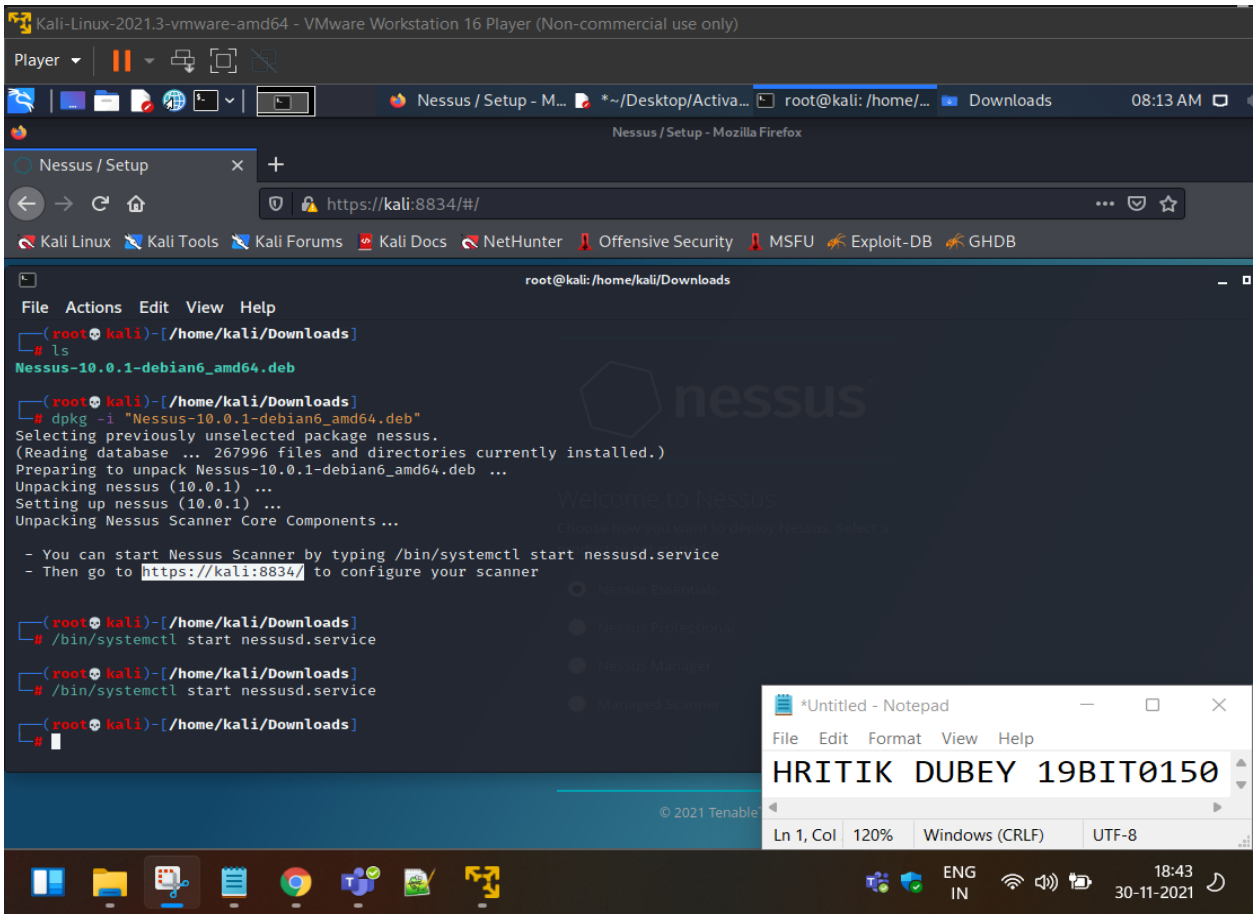
Show the ipconfig details of the VM

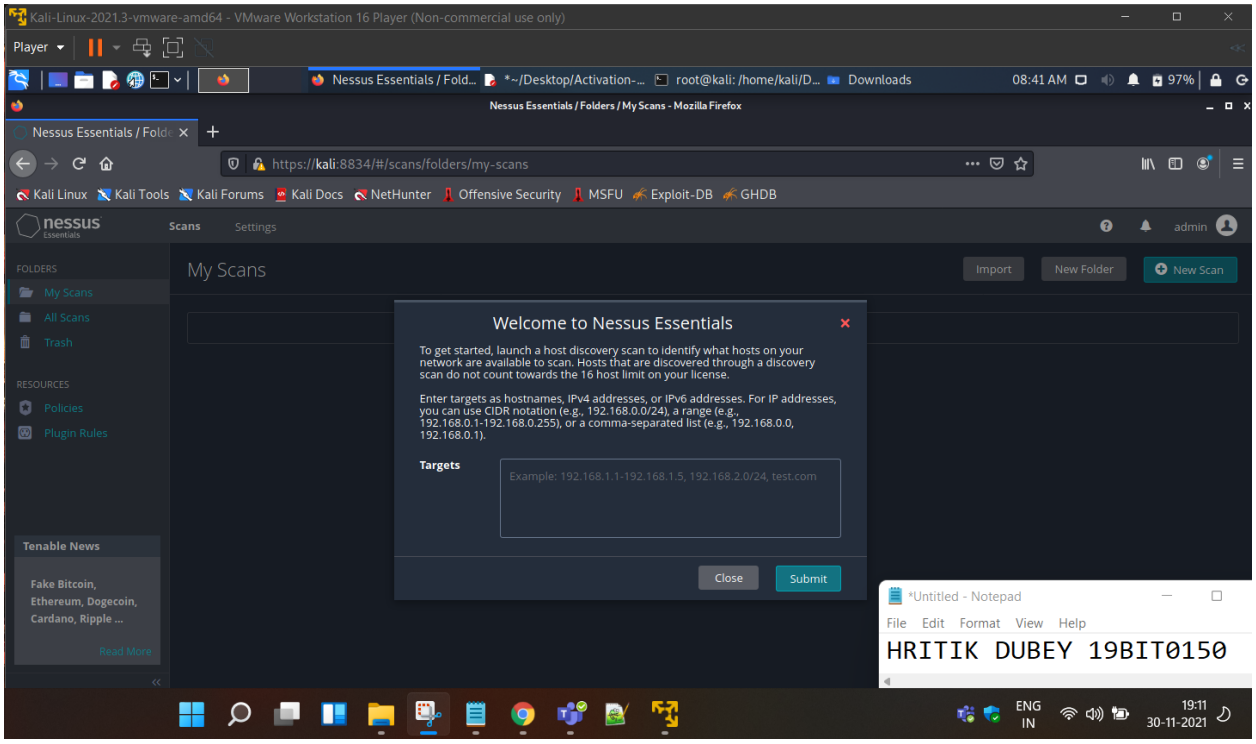




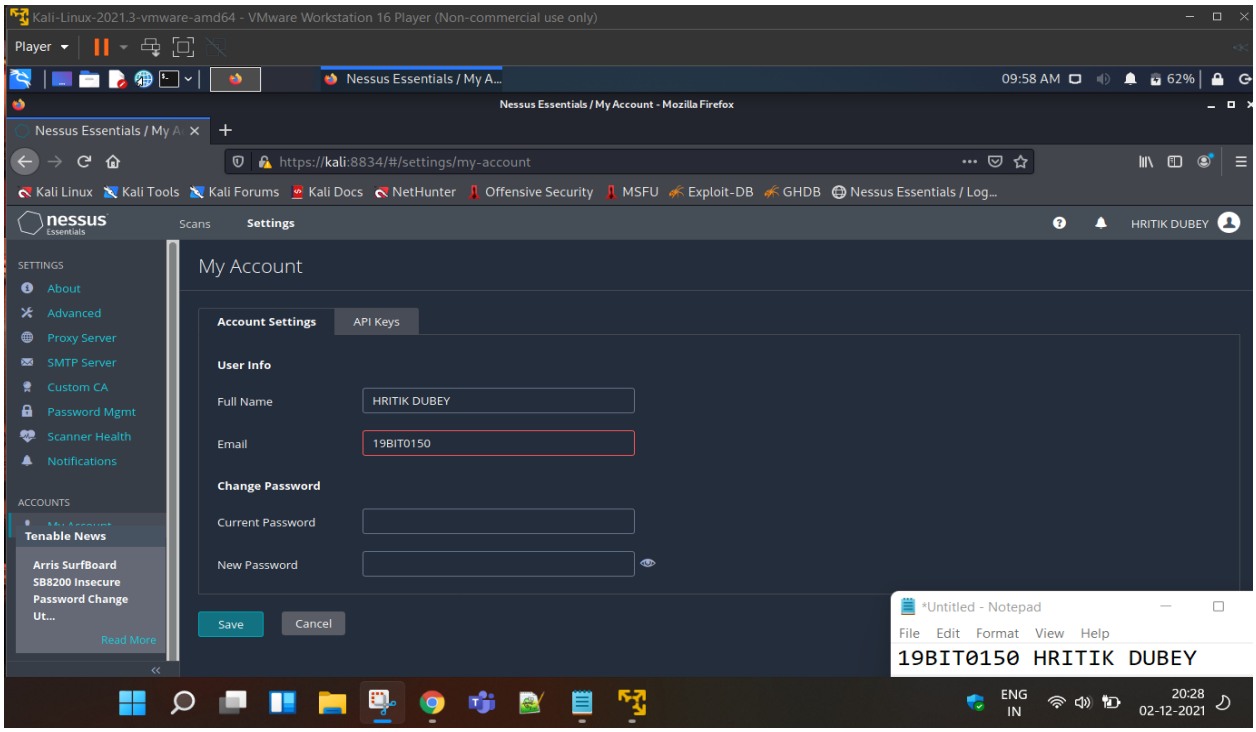
INET IP ADDR- 192.168.159.128

3. Install Nessus in Kali Linux

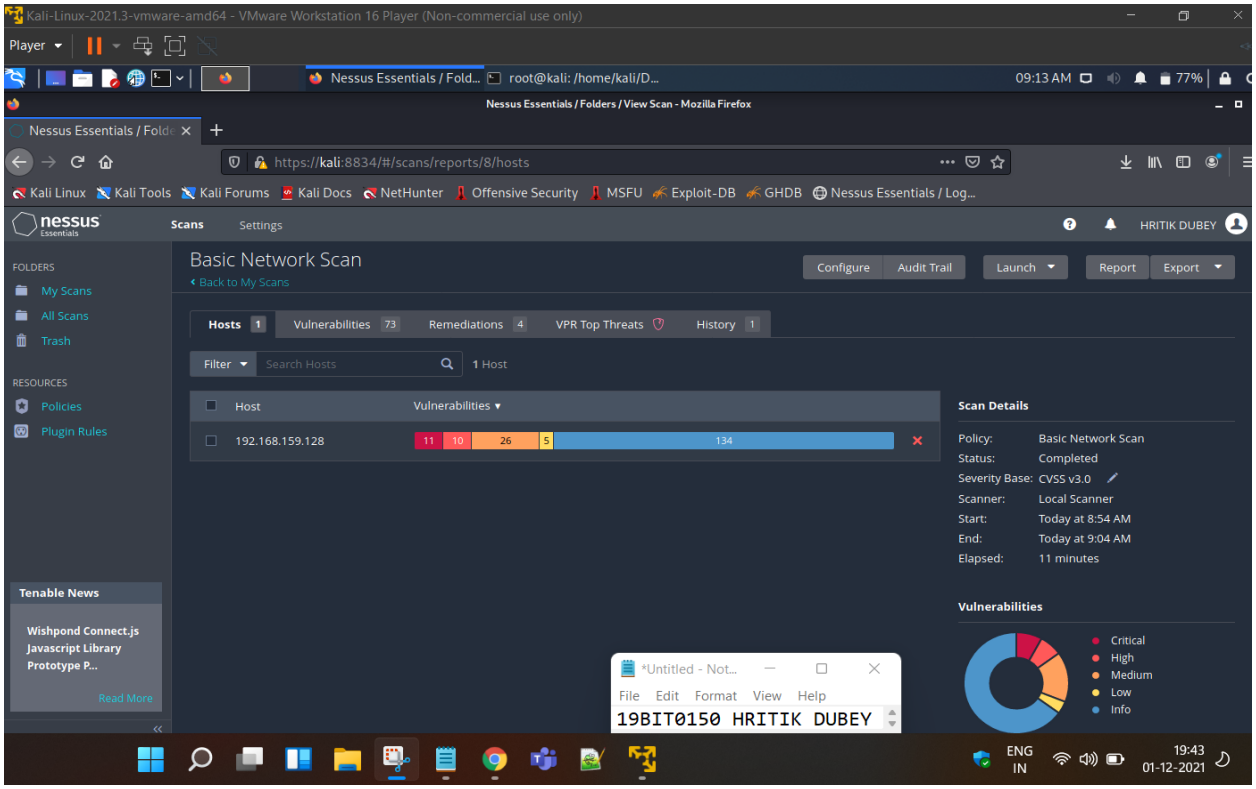


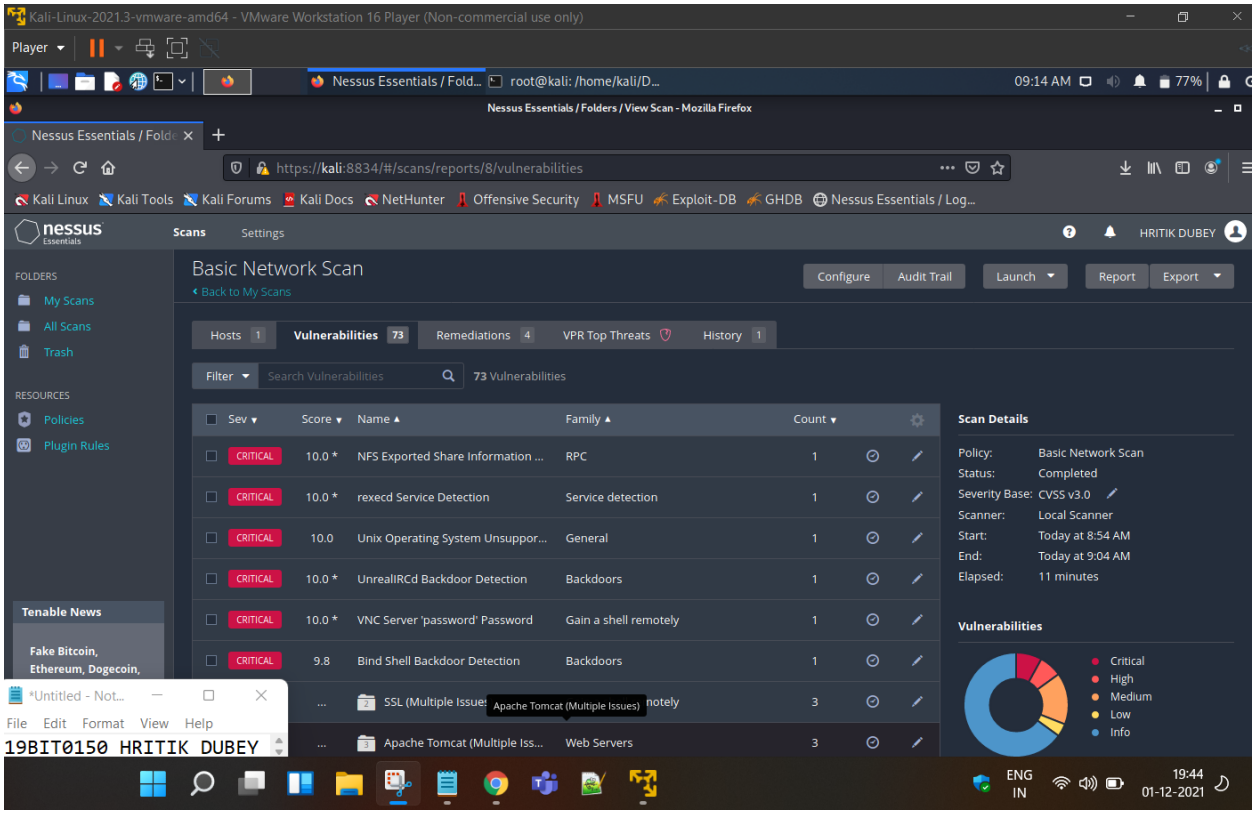


4. Perform a Nessus scan on your Metasploitable IP-

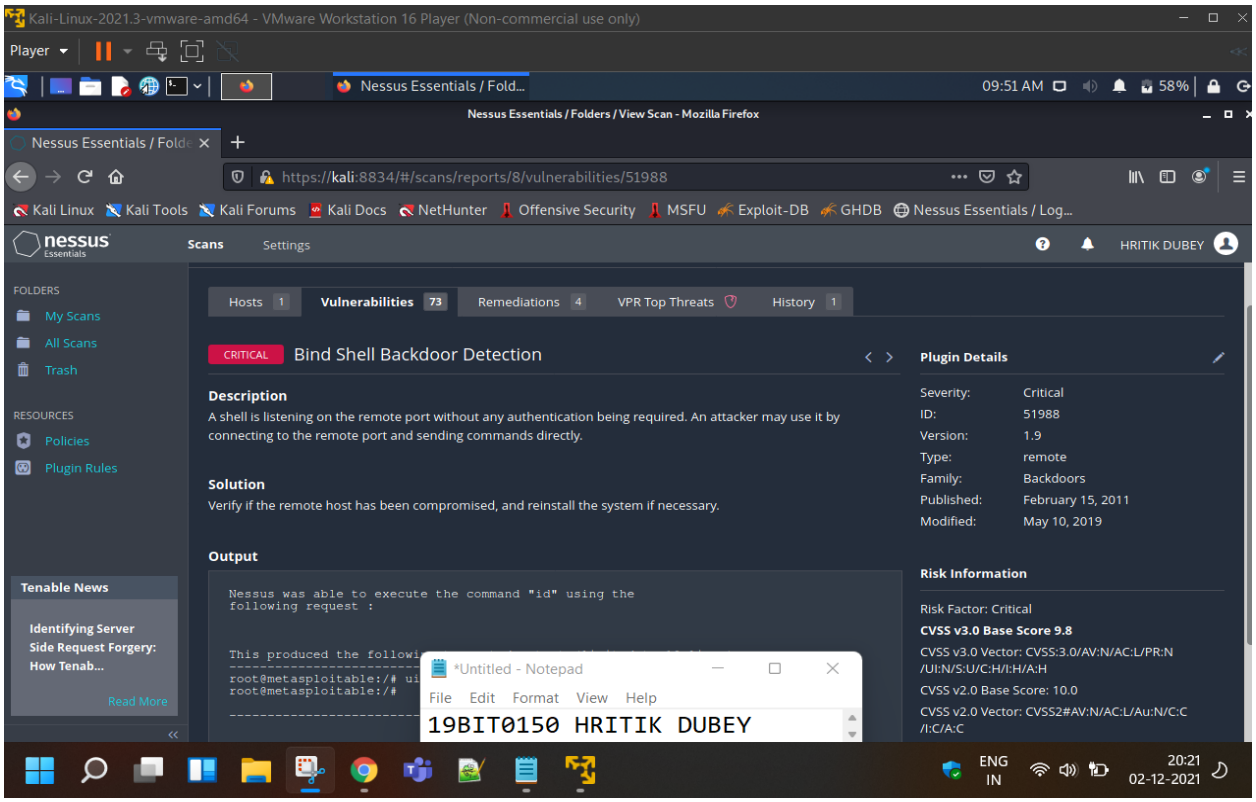


SCAN 1 BASIC NETWORK SCAN

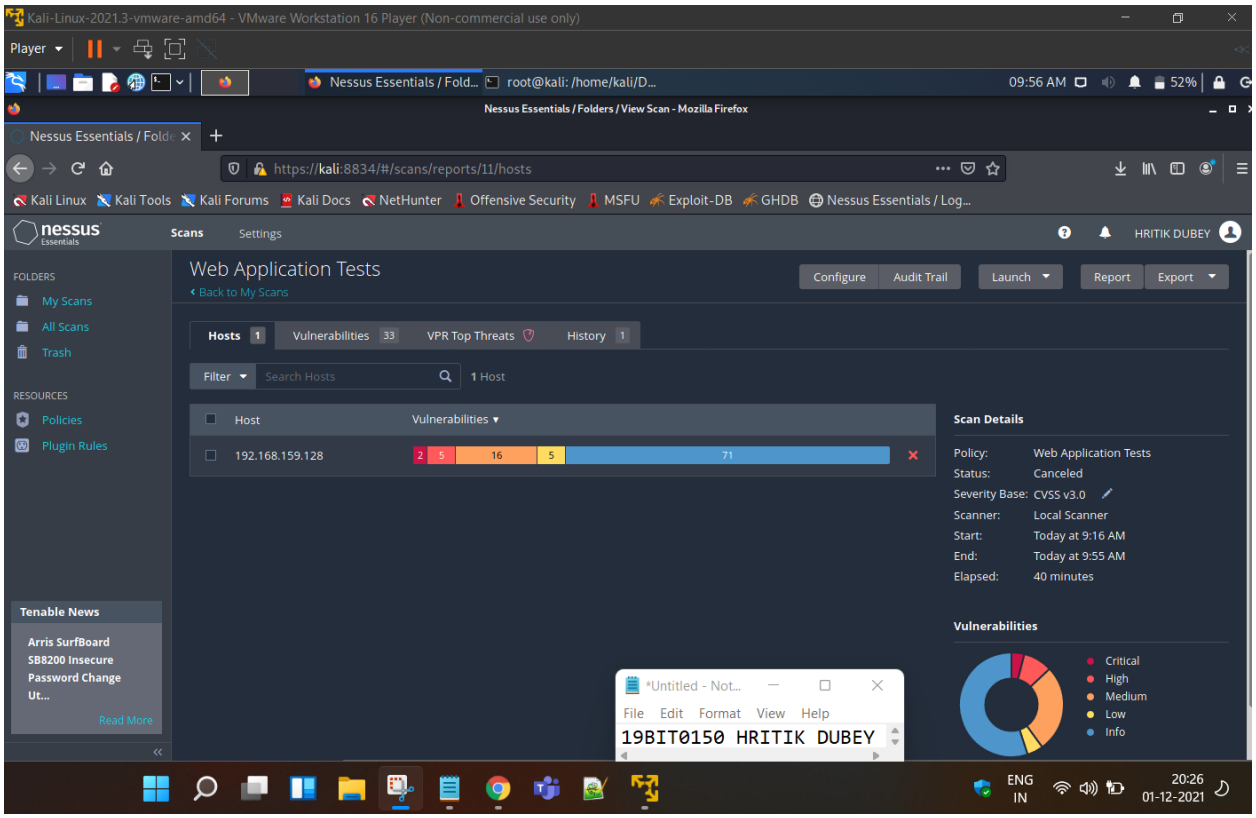


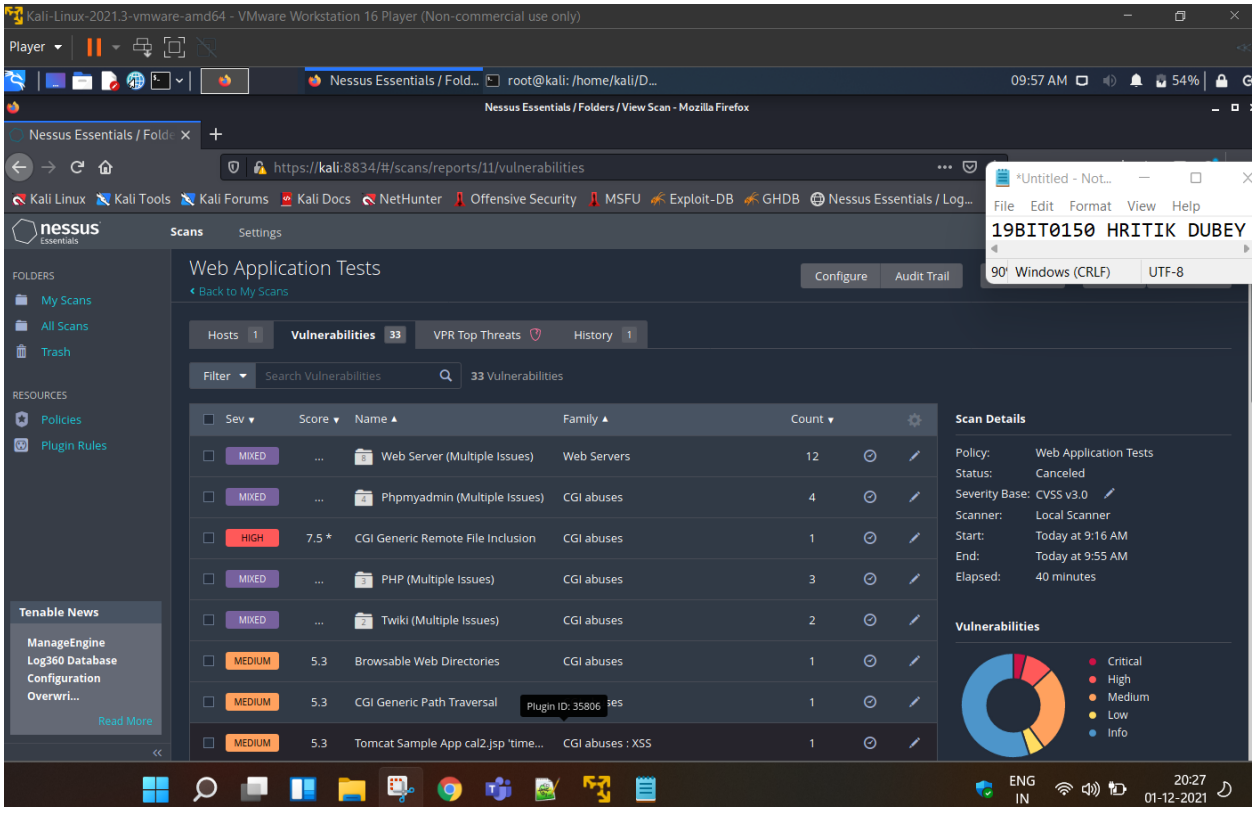


CVSS SCORE FOR BASIC NETWORK SCAN - 9.8

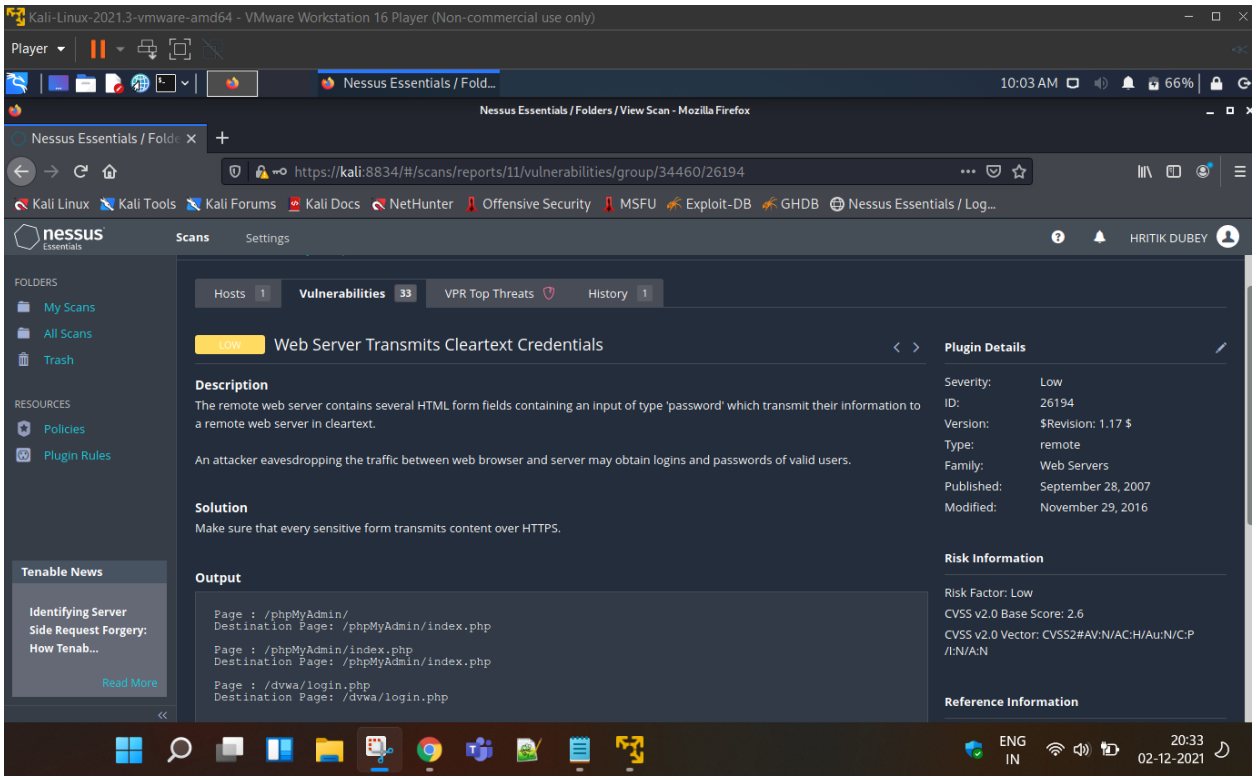


SCAN 2 Web Application Tests

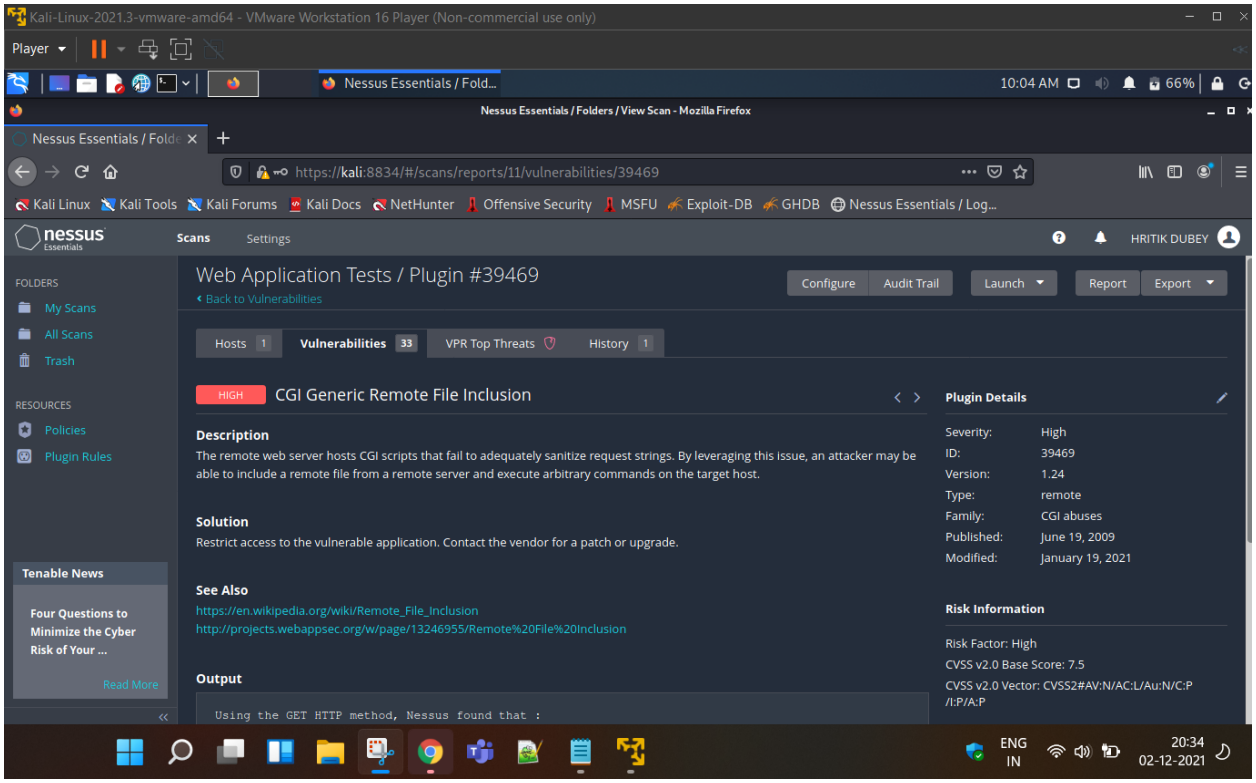




CVSS SCORE - 2.6



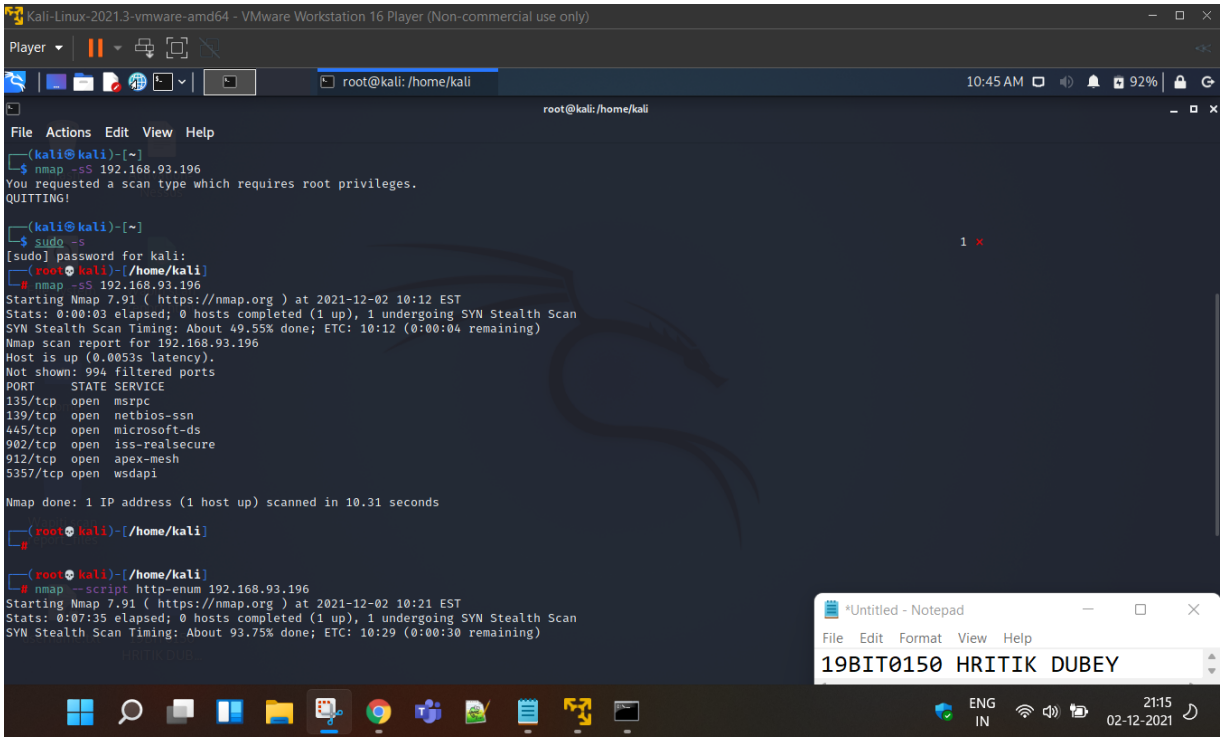
CVSS SCORE - 7.5



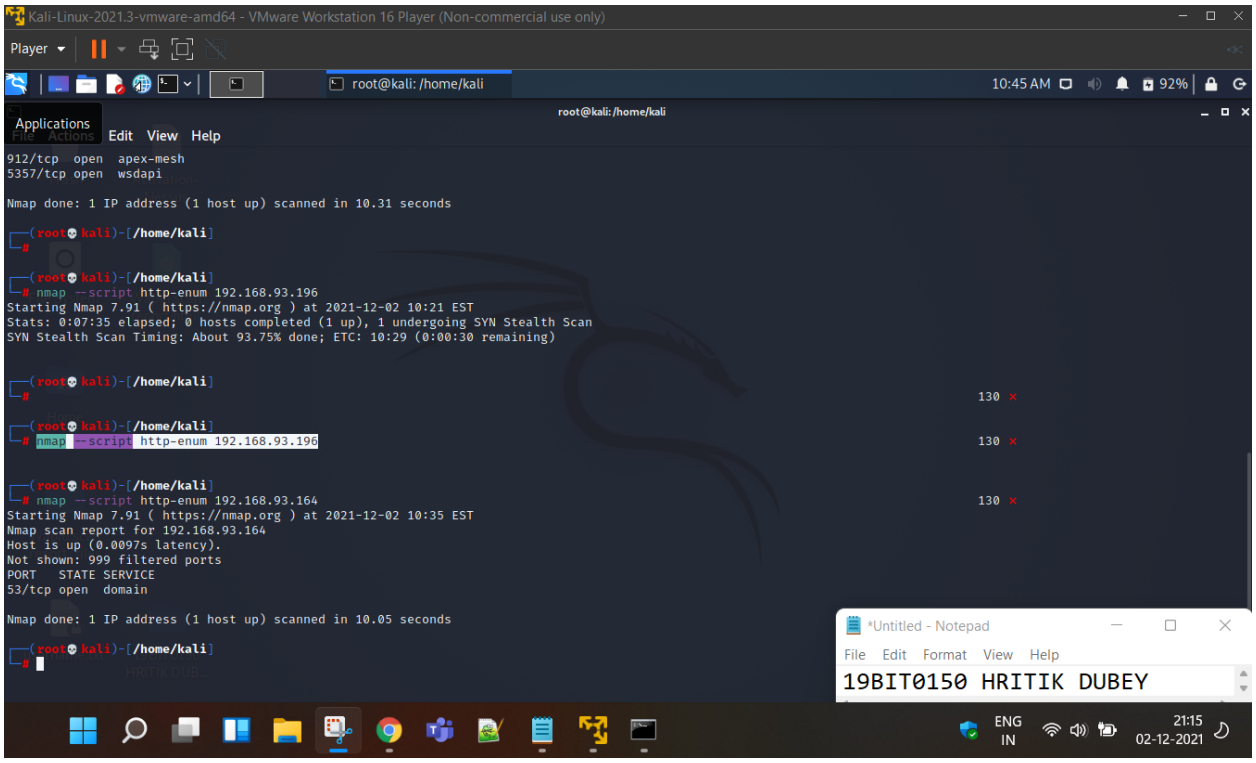
5. Perform the following scans on NMap

My system IP Address 192.168.93.196 ---- Default Gateway 192.168.93.164

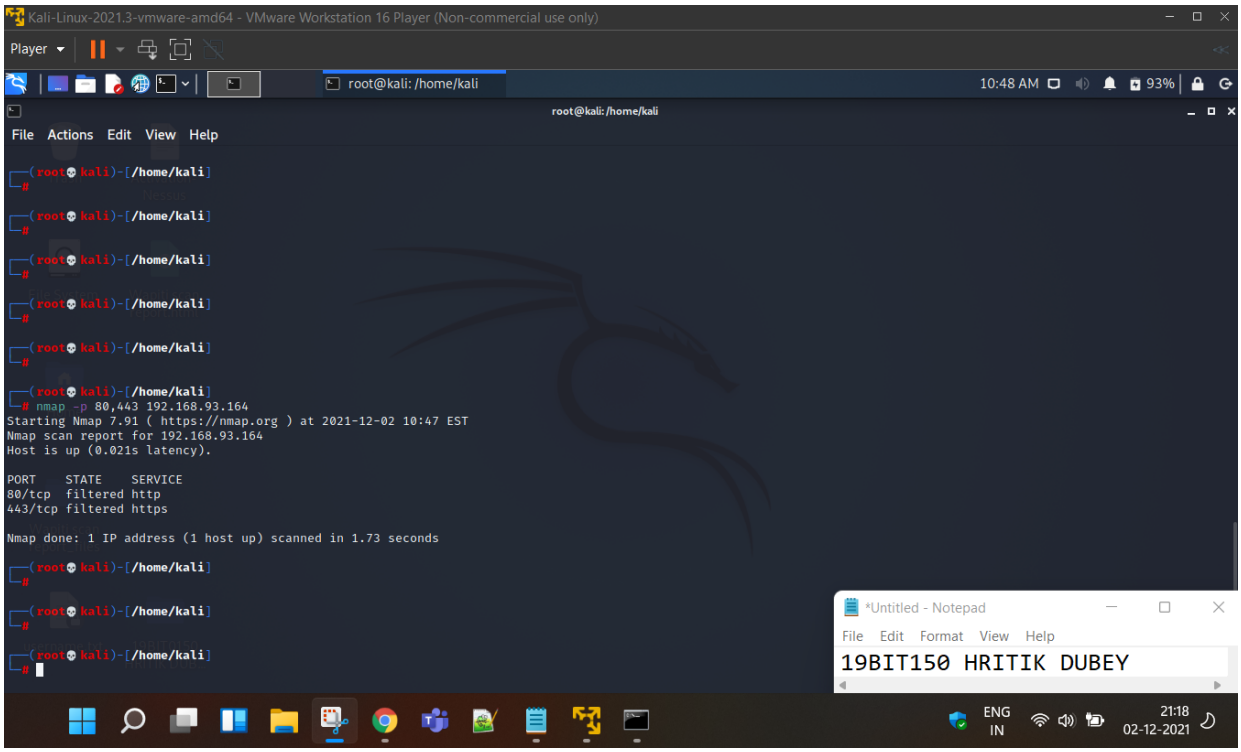
1. nmap –sS ipaddr



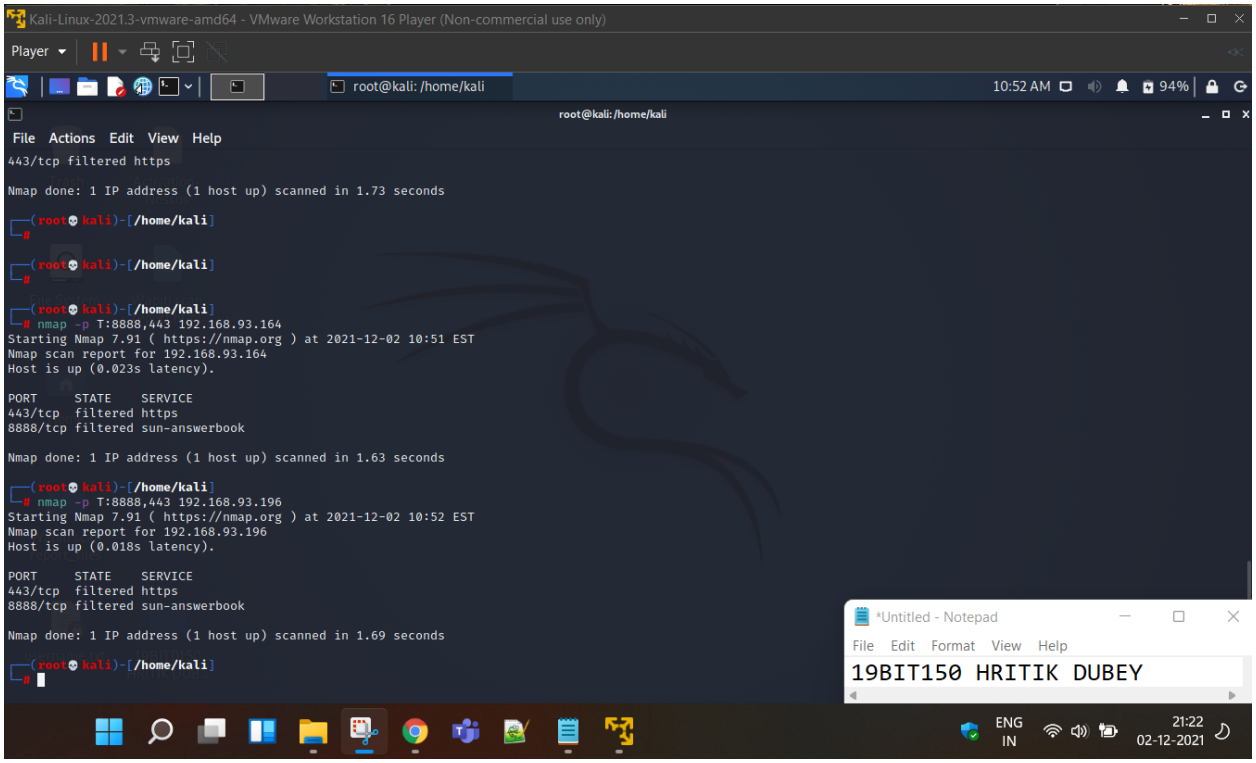
2. nmap --script http-enum ipaddr



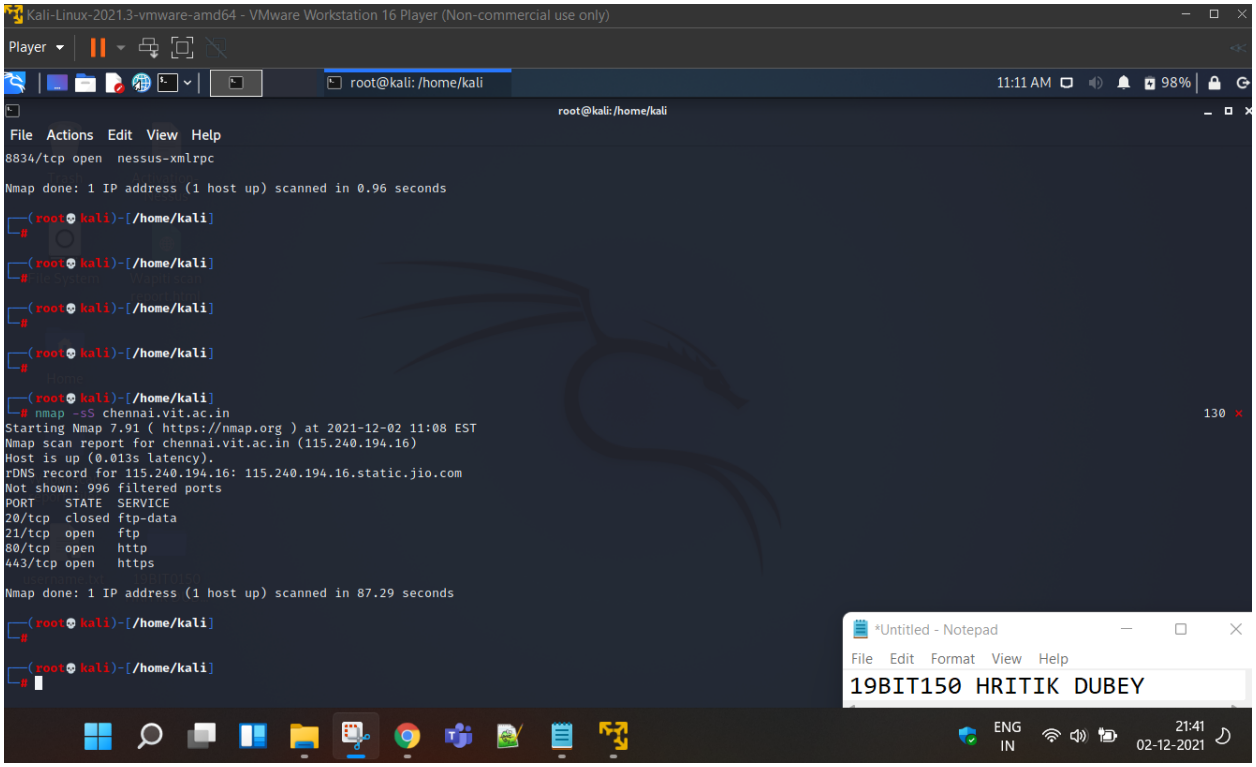
3. nmap -p 80,443 ipaddr OPEN PORT 80/tcp 443/tcp



4. nmap -p T:8888,443 ipaddr || 8888/tcp service name sun-answerbook



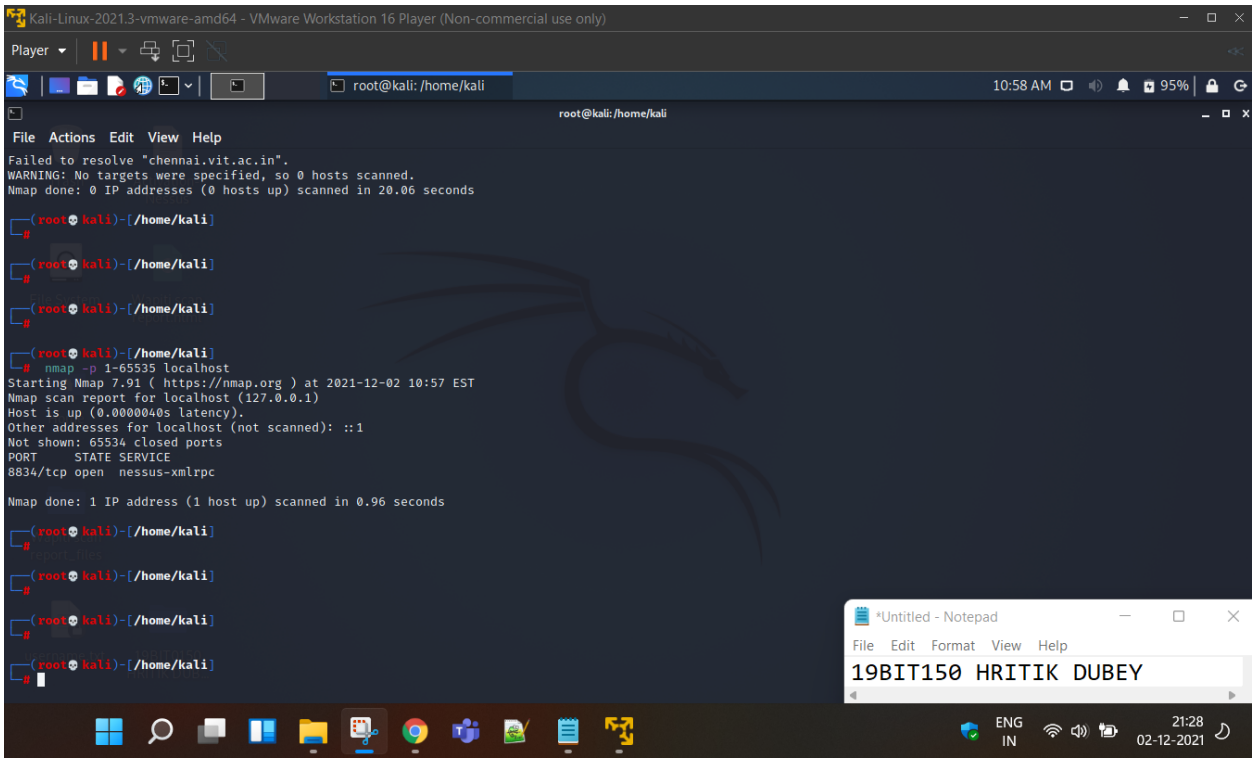
5. Nmap -sS Chennai.vit.ac.in



rDNS record for 115.240.194.16: 115.240.194.16.static.jio.com

PORT STATE SERVICE
20/tcp closed ftp-data
21/tcp open ftp
80/tcp open http
443/tcp open https

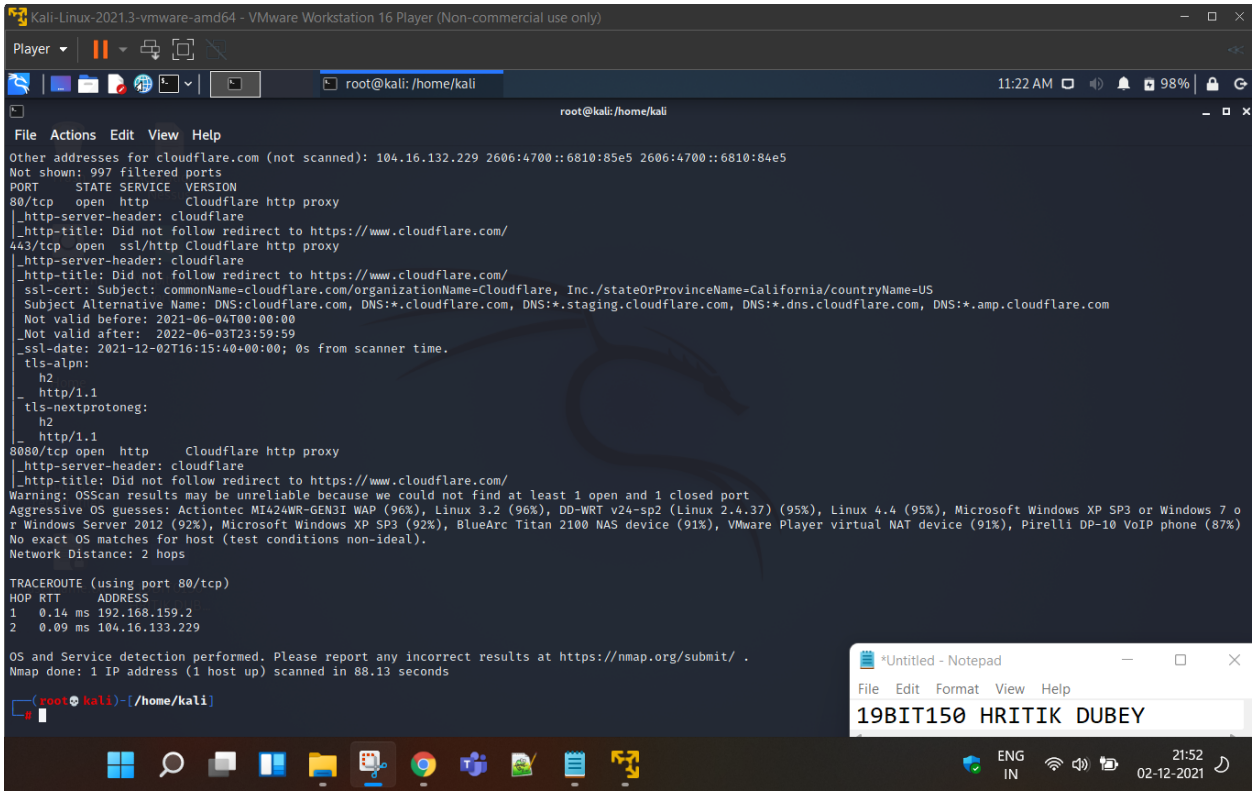
6. nmap -p 1-65535 localhost



Starting Nmap 7.91 (https://nmap.org) at 2021-12-02 10:57 EST
Nmap scan report for localhost (127.0.0.1)

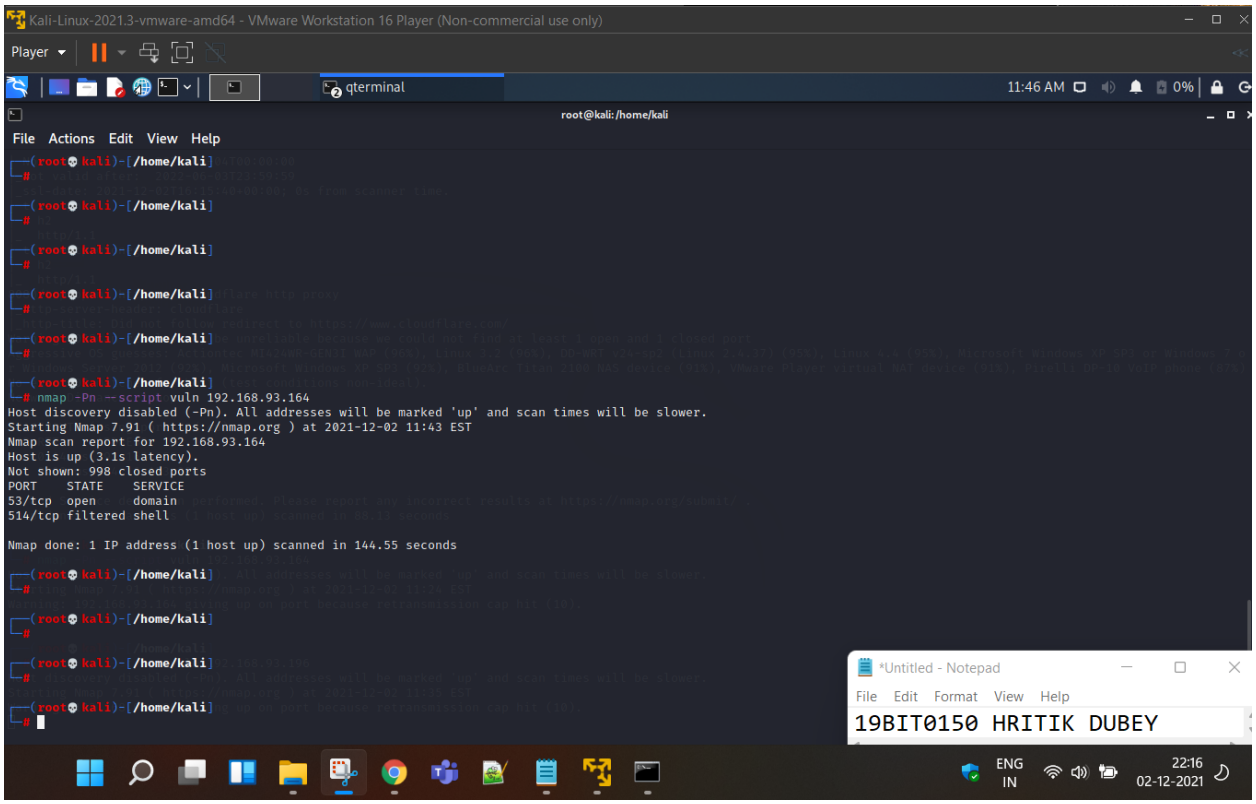
Not shown: 65534 closed ports
PORT STATE SERVICE
8834/tcp open nessus-xmlrpc

7. nmap -T4 -A cloudflare.com (from the complete output, give only the trace route result)



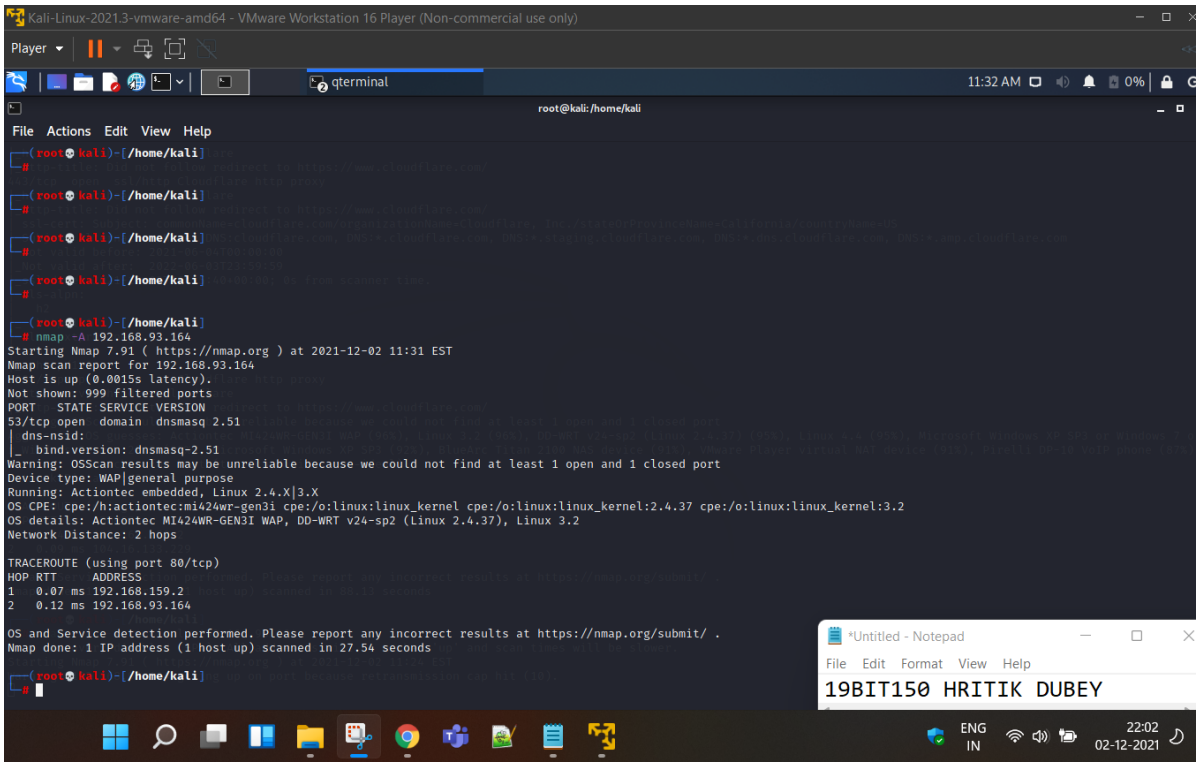
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 0.14 ms 192.168.159.2
2 0.09 ms 104.16.133.229

8. nmap -Pn --script vuln ipaddr (how many ports are filtered)



Not shown: 998 closed ports
PORT STATE SERVICE
53/tcp open domain
514/tcp filtered shell

9. nmap -A ipaddr



10. Command to scan IPv6 address (ADD -6)