

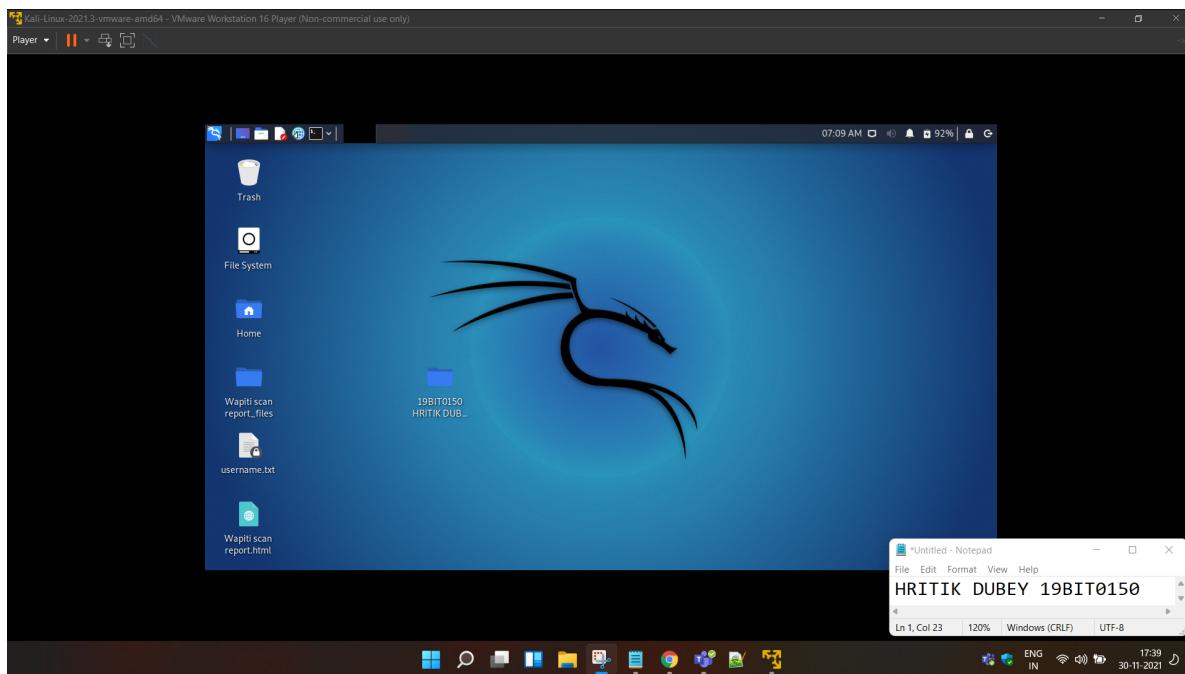
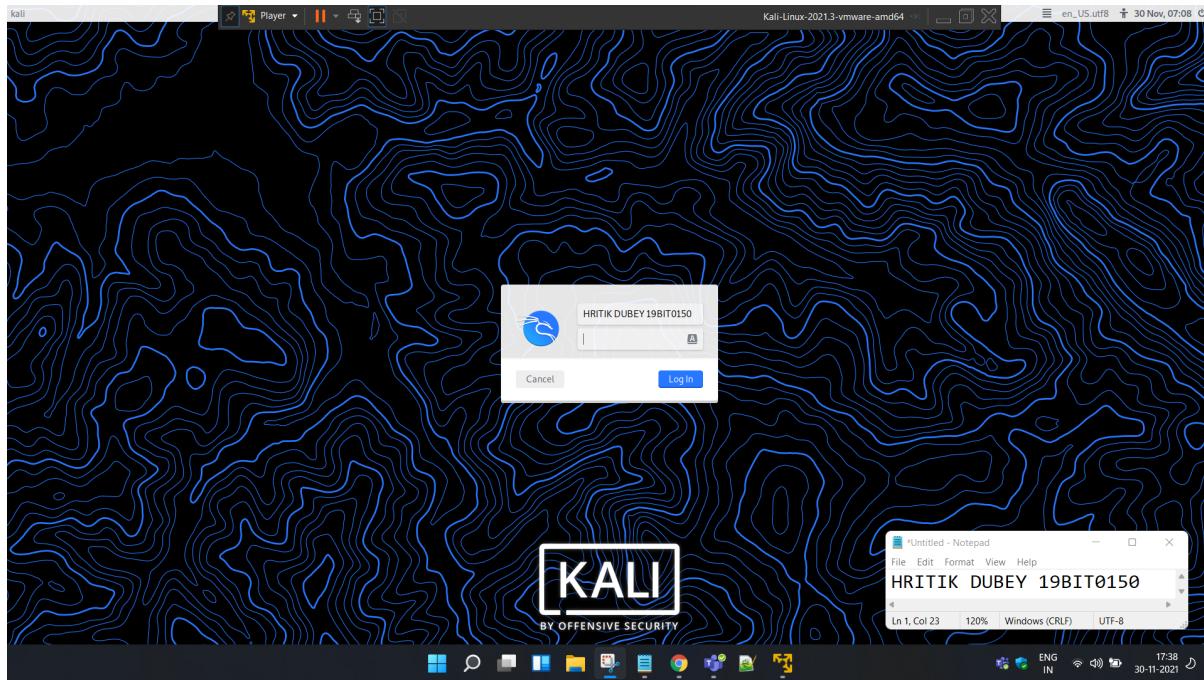
CSE3501-Information Security Analysis and Audit Lab

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

DIGITAL ASSIGNMENT 5

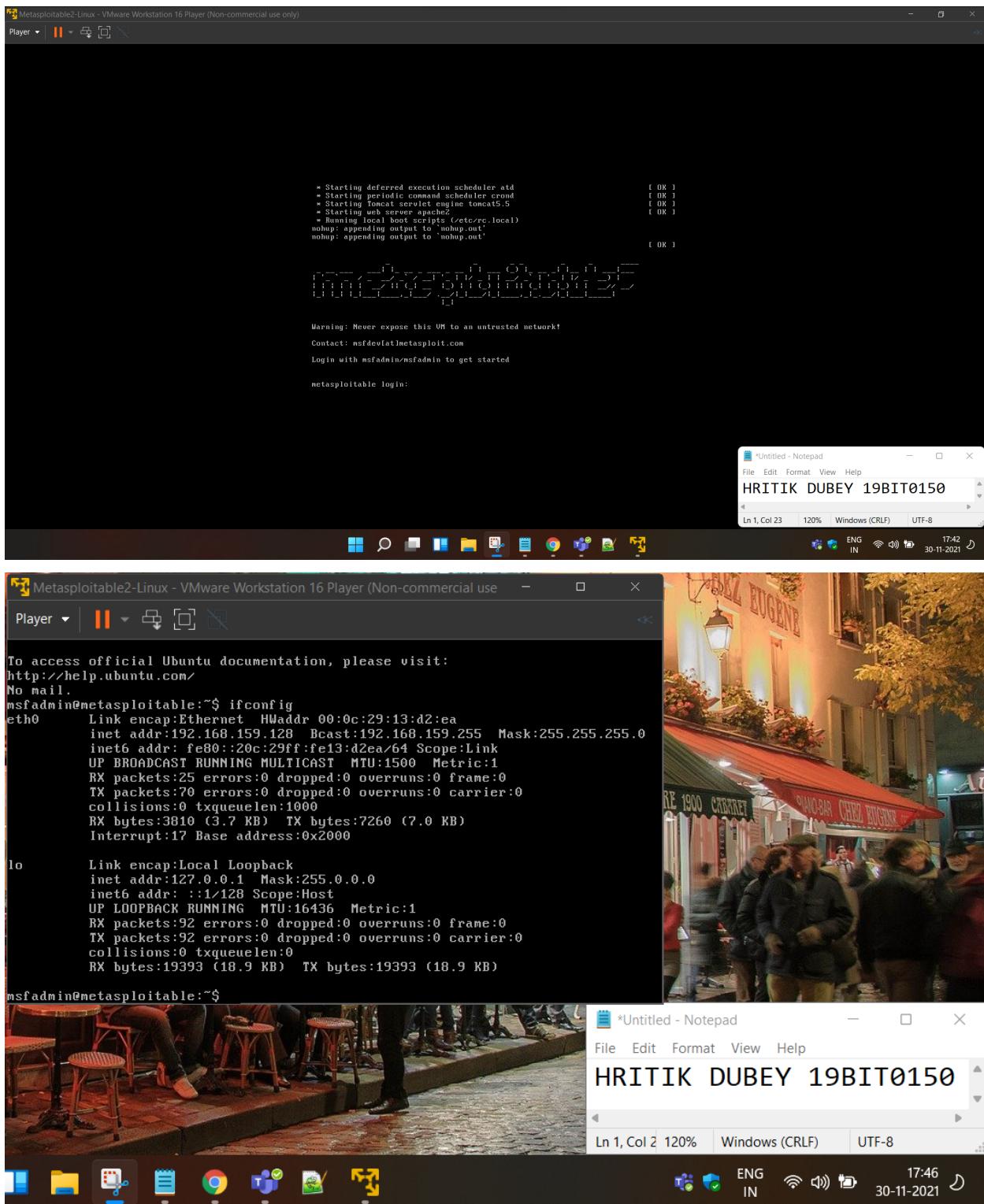
Faculty : Dr. Priya V

1. Install Kali Linux



2. Install Metasploitable VM

Show the ipconfig details of the VM



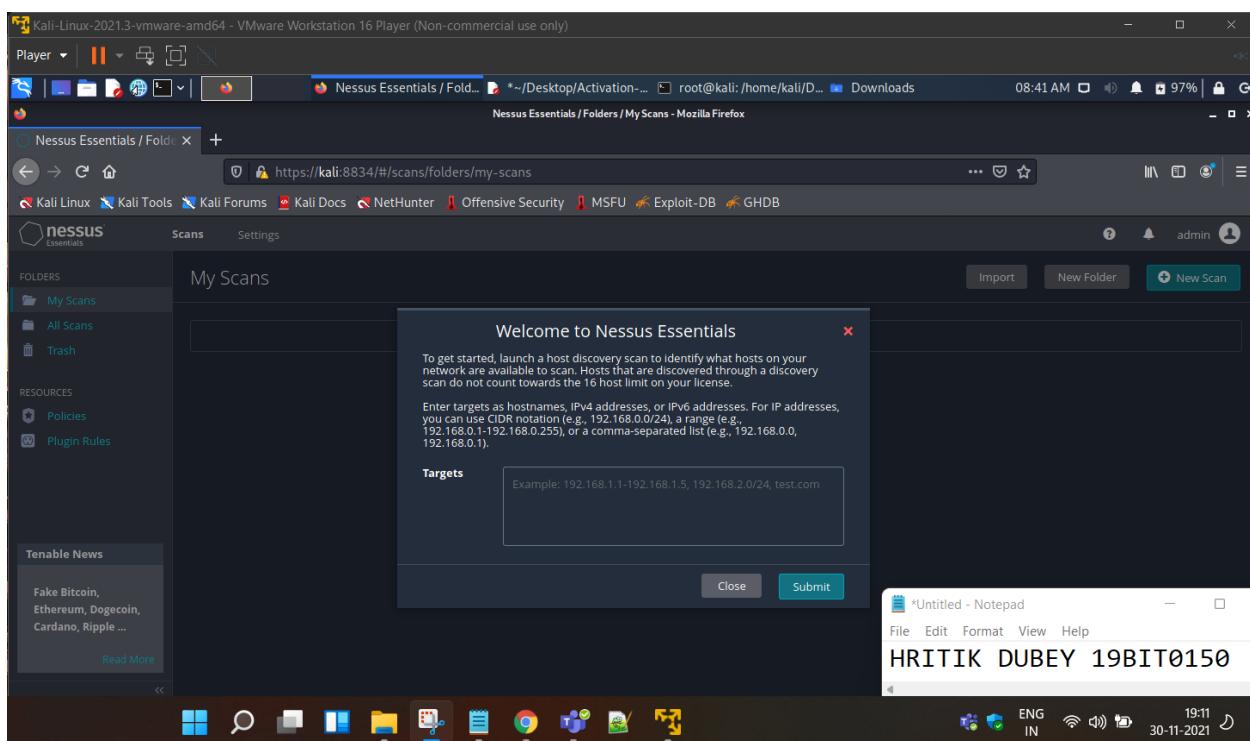
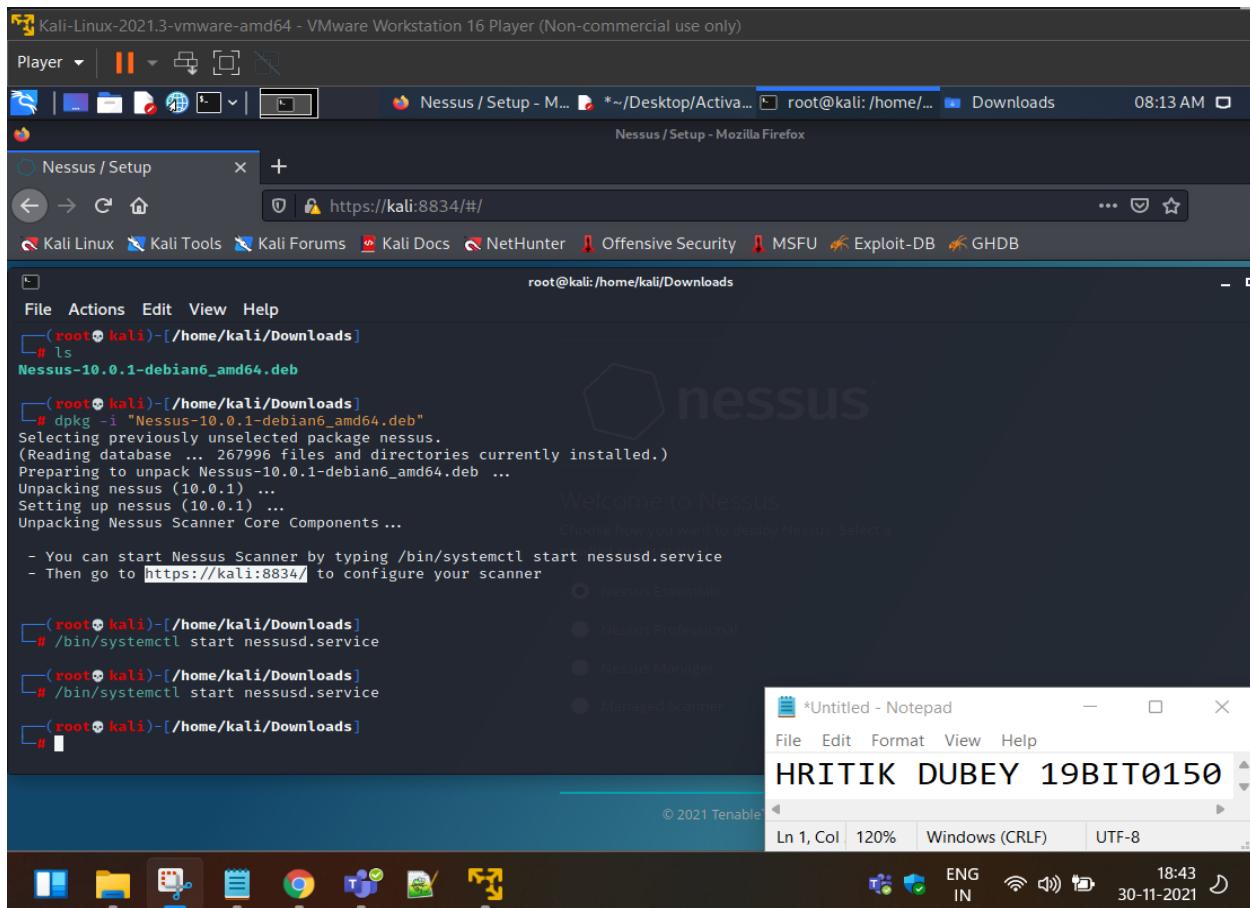
```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:13:d2:ea
          inet addr:192.168.159.128  Bcast:192.168.159.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe13:d2ea/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:25 errors:0 dropped:0 overruns:0 frame:0
            TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:3810 (3.7 KB)  TX bytes:7260 (7.0 KB)
            Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:16436  Metric:1
            RX packets:92 errors:0 dropped:0 overruns:0 frame:0
            TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$
```

INET IP ADDR- 192.168.159.128

3. Install Nessus in Kali Linux



4. Perform a Nessus scan on your Metasploitable IP-

The screenshot shows the Nessus Essentials application running in a VMware Workstation window. The main browser tab displays the 'My Account' settings page. On the left sidebar, under 'ACCOUNTS', there is a list of recent scans: 'Tenable News', 'Arris SurfBoard SB8200 Insecure Password Change Ut...', and 'Read More'. The central panel shows 'Account Settings' with fields for 'Full Name' (HRITIK DUBEY) and 'Email' (19BIT0150). Below these are 'Change Password' fields for 'Current Password' and 'New Password'. At the bottom are 'Save' and 'Cancel' buttons. To the right of the browser, a small Notepad window is open with the text '19BIT0150 HRITIK DUBEY'. The system tray at the bottom right shows the date as 02-12-2021.

SCAN 1 BASIC NETWORK SCAN

The screenshot shows the Nessus Essentials application running in a VMware Workstation window. The main browser tab displays the 'Basic Network Scan' results. The left sidebar shows 'FOLDERS' with 'My Scans' selected, and 'RESOURCES' with 'Policies' and 'Plugin Rules'. The central panel shows a table of vulnerabilities for a single host, 192.168.159.128, with 11 Critical, 10 High, 26 Medium, 5 Low, and 134 Info level findings. To the right, 'Scan Details' provide information about the completed scan: Policy (Basic Network Scan), Status (Completed), Severity Base (CVSS v3.0), Scanner (Local Scanner), Start (Today at 8:54 AM), End (Today at 9:04 AM), and Elapsed (11 minutes). A 'Vulnerabilities' chart at the bottom indicates the distribution of findings. A small Notepad window is open with the text '19BIT0150 HRITIK DUBEY'. The system tray at the bottom right shows the date as 01-12-2021.

Basic Network Scan

Vulnerabilities 73

Sev	Score	Name	Family	Count
Critical	10.0 *	NFS Exported Share Information ...	RPC	1
Critical	10.0 *	rexed Service Detection	Service detection	1
Critical	10.0	Unix Operating System Unsuppor...	General	1
Critical	10.0 *	UnrealRCd Backdoor Detection	Backdoors	1
Critical	10.0 *	VNC Server 'password' Password	Gain a shell remotely	1
Critical	9.8	Bind Shell Backdoor Detection	Backdoors	1

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 8:54 AM
- End: Today at 9:04 AM
- Elapsed: 11 minutes

Vulnerabilities

ENG IN 19:44 01-12-2021

CVSS SCORE FOR BASIC NETWORK SCAN - 9.8

Bind Shell Backdoor Detection

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Output

```
Nessus was able to execute the command "id" using the following request :

This produced the following output:
root@metasploitable:~# id
root@metasploitable:~#
```

Risk Information

Risk Factor: Critical
CVSS v3.0 Base Score 9.8
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/I/U/S:U/C:H/I:H/A:H
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I/C:A/C

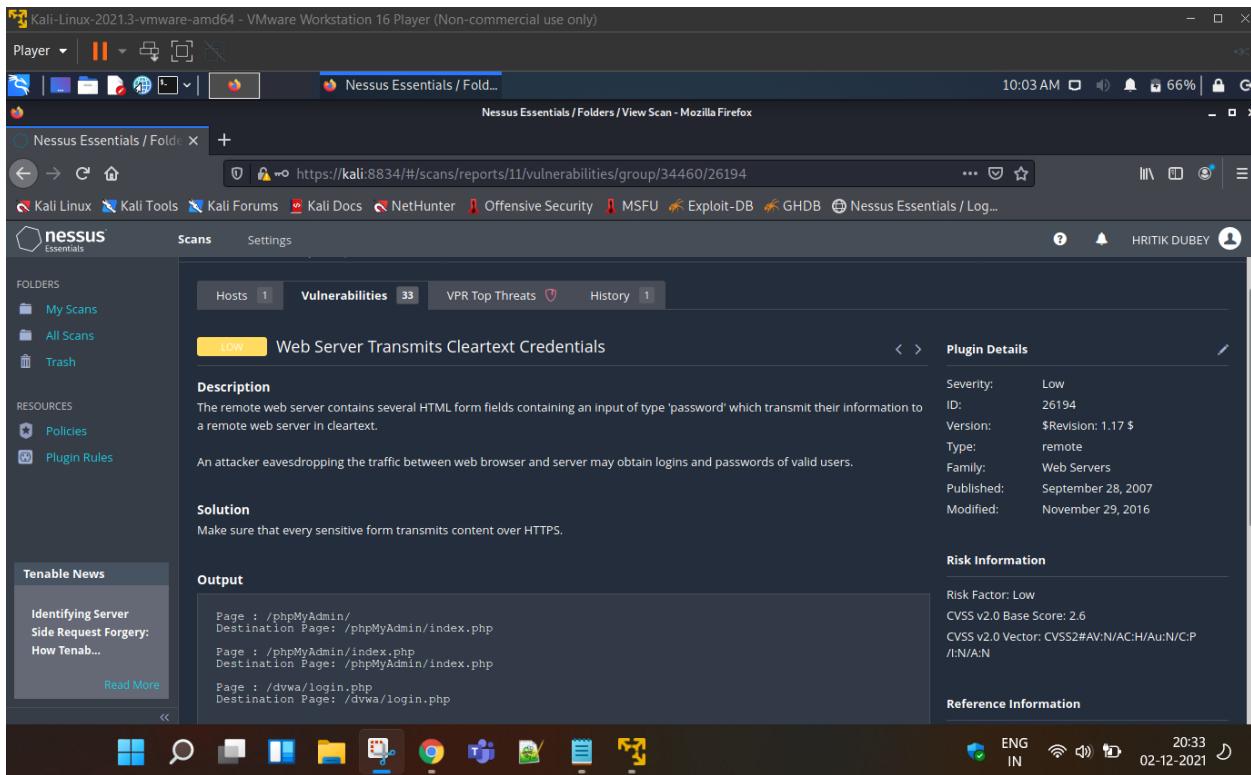
ENG IN 20:21 02-12-2021

SCAN 2 Web Application Tests

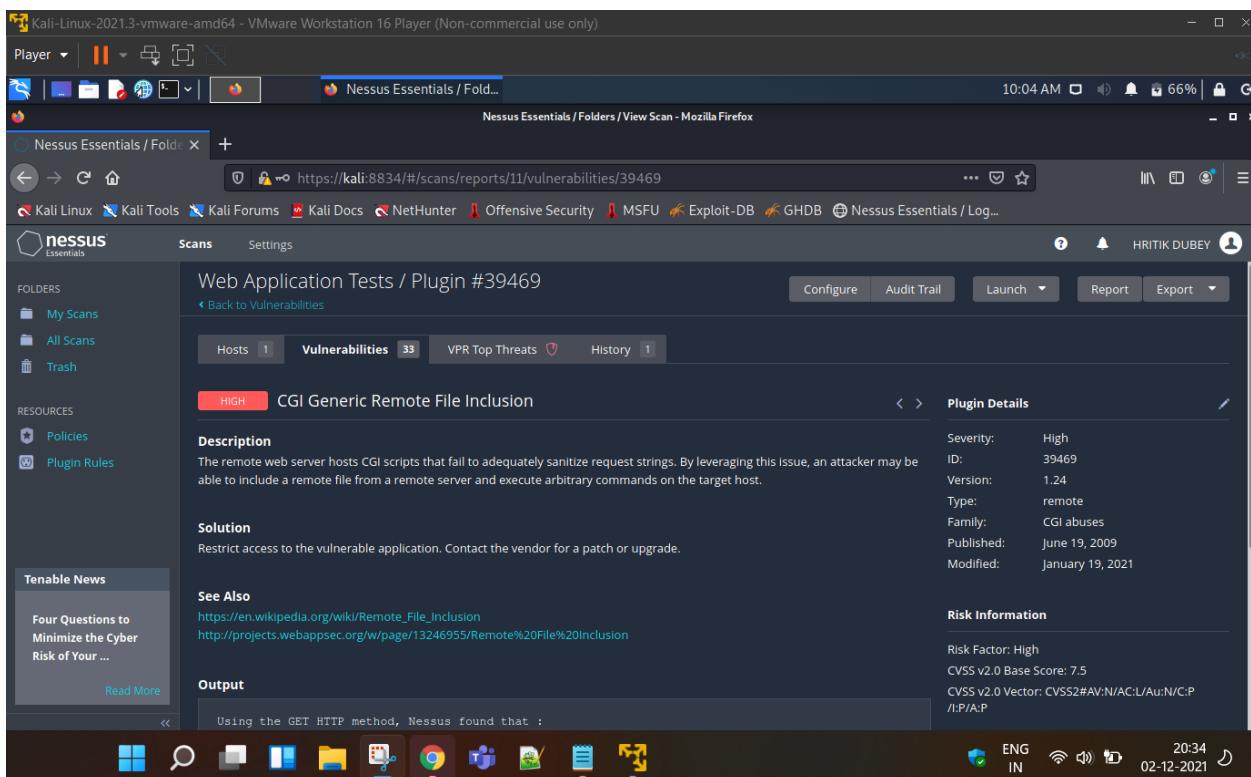
The screenshot shows the Nessus Essentials interface after a scan has been completed. The main window displays the 'Web Application Tests' section with a summary table showing one host (192.168.159.128) with 71 vulnerabilities across five severity levels (Critical, High, Medium, Low, Info). A 'Scan Details' panel on the right provides information about the scan policy, status, and timing. A 'Vulnerabilities' chart is also present. A small terminal window in the foreground shows the command '19BIT0150 HRITIK DUBEY'.

This screenshot shows a detailed view of the 'Vulnerabilities' tab from the previous scan. It lists 33 vulnerabilities across various families, including 'Web Server (Multiple Issues)', 'Phpmmyadmin (Multiple Issues)', 'CGI Generic Remote File Inclusion', 'PHP (Multiple Issues)', 'Twiki (Multiple Issues)', 'Browsable Web Directories', 'CGI Generic Path Traversal', and 'Tomcat Sample App cal2.jsp?time...'. The 'Scan Details' panel on the right is identical to the first screenshot. A terminal window in the foreground shows the command '90% Windows (CRLF) - UTF-8'.

CVSS SCORE - 2.6



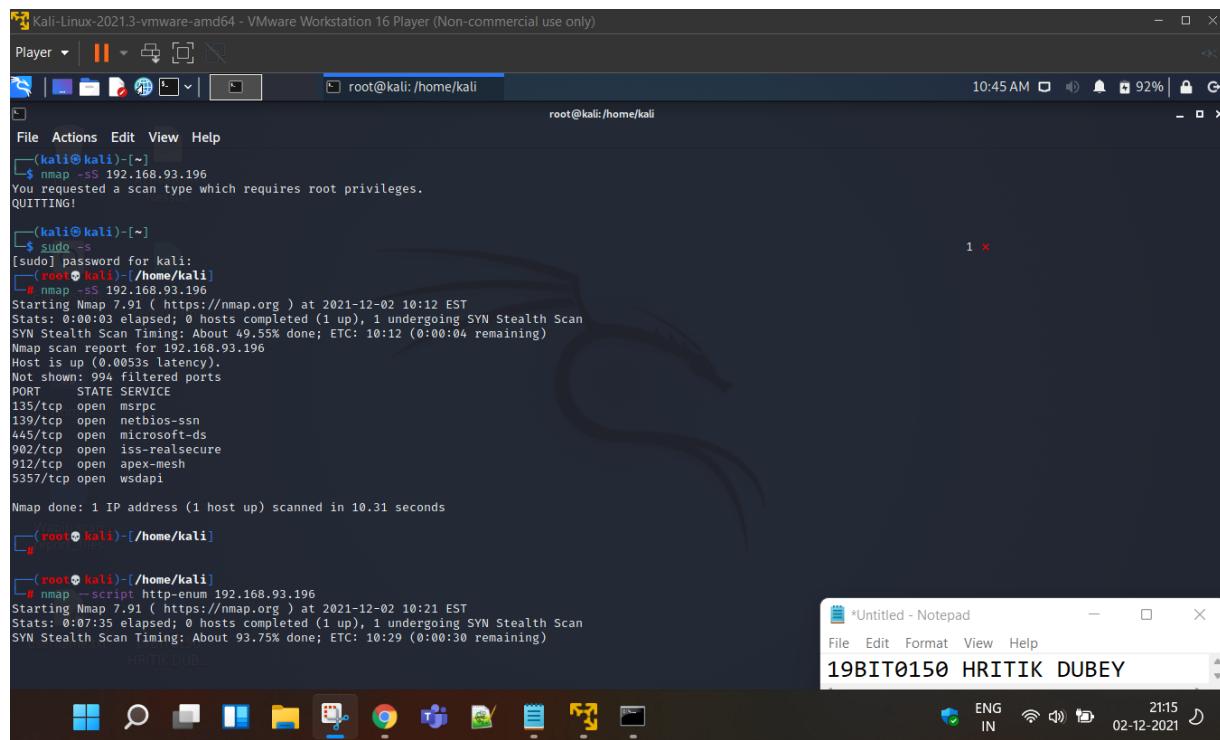
CVSS SCORE - 7.5



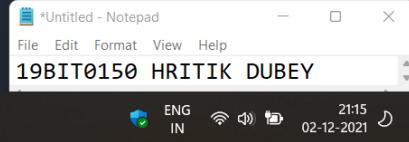
5. Perform the following scans on NMap

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

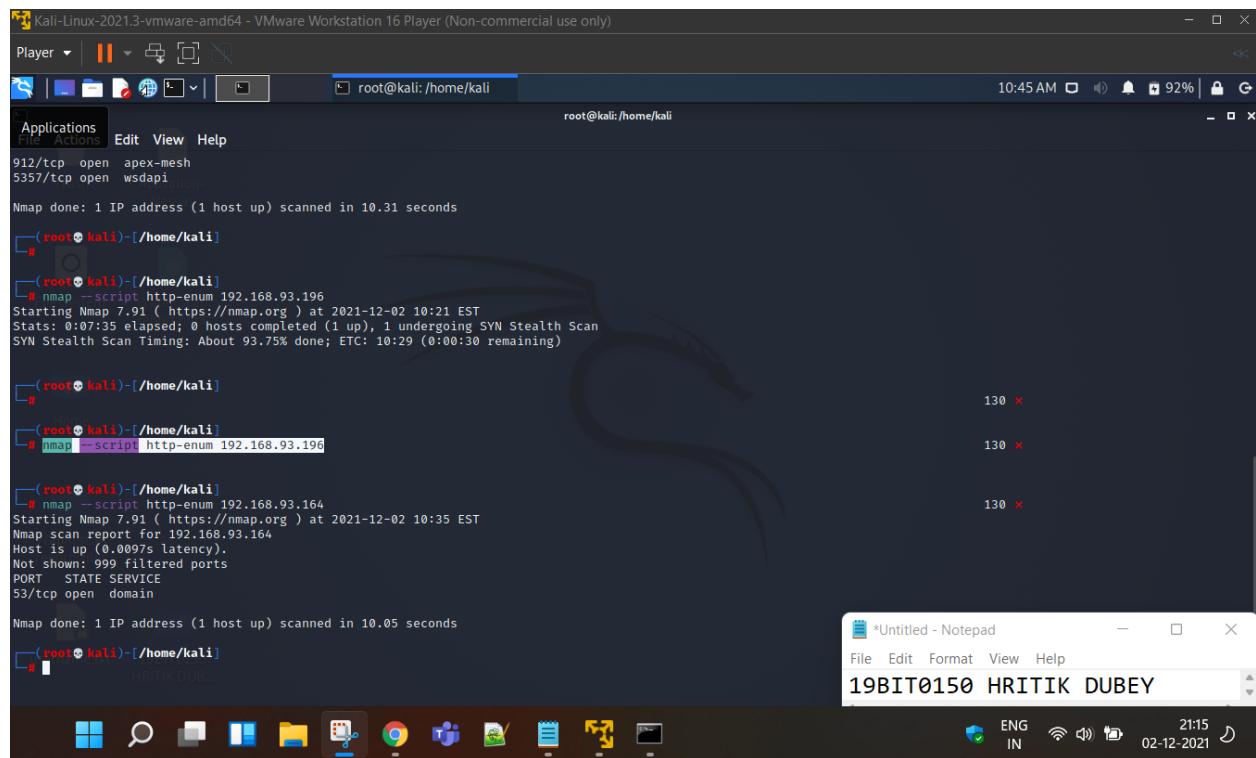
1. nmap -sS ipaddr



```
[root@kali:~/home/kali]# nmap -sS 192.168.93.196
You requested a scan type which requires root privileges.
QUITTING!
[~]
[sudo] password for kali:
[root@kali:~/home/kali]# nmap -sS 192.168.93.196
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-02 10:12 EST
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 49.55% done; ETC: 10:12 (0:00:04 remaining)
Nmap scan report for 192.168.93.196
Host is up (0.0053s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
902/tcp    open  iss-realsecure
912/tcp    open  apex-mesh
5357/tcp   open  wsdd
Nmap done: 1 IP address (1 host up) scanned in 10.31 seconds
[~]
[root@kali:~/home/kali]# nmap --script http-enum 192.168.93.196
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-02 10:21 EST
Stats: 0:07:35 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 93.75% done; ETC: 10:29 (0:00:30 remaining)
```



2. nmap --script http-enum ipaddr

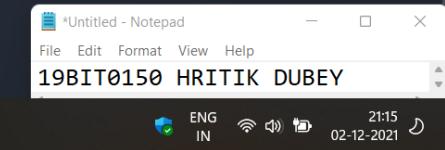


```
[root@kali:~/home/kali]# nmap --script http-enum 192.168.93.196
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-02 10:21 EST
Stats: 0:07:35 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 93.75% done; ETC: 10:29 (0:00:30 remaining)

[~]
[root@kali:~/home/kali]# nmap --script http-enum 192.168.93.196
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-02 10:35 EST
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.0097s latency.

Nmap scan report for 192.168.93.164
Host is up (0.0097s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain

Nmap done: 1 IP address (1 host up) scanned in 10.05 seconds
[~]
[root@kali:~/home/kali]#
```



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

Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)

Player | || | ☰

root@kali: /home/kali

File Actions Edit View Help

8834/tcp open nessus-xmlrpc

Nmap done: 1 IP address (1 host up) scanned in 0.96 seconds

(root@kali)-[~/home/kali]

#

(root@kali)-[~/home/kali]

#

(root@kali)-[~/home/kali]

#

(root@kali)-[~/home/kali]

#

(root@kali)-[~/home/kali]

#

Home

(root@kali)-[~/home/kali]

nmap -sS chennai.vit.ac.in

Starting Nmap 7.91 (https://nmap.org) at 2021-12-02 11:08 EST

Nmap scan report for chennai.vit.ac.in (115.240.194.16)

Host is up (0.013s latency).

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

Not shown: 996 filtered ports

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

Using NSE scripts. 0.00s to connect to each host.

Nmap done: 1 IP address (1 host up) scanned in 87.29 seconds

(root@kali)-[~/home/kali]

#

(root@kali)-[~/home/kali]

#

*Untitled - Notepad

File Edit Format View Help

19BIT150 HRITIK DUBEY

ENG IN 21:41 02-12-2021

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)

Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)

Player ▾ || ⌂ ⌂ ⌂ root@kali: /home/kali

root@kali: /home/kali

File Actions Edit View Help

Other addresses for cloudflare.com (not scanned): 104.16.132.229 2606:4700::6810:85e5 2606:4700::6810:84e5

Not shown: 997 filtered ports

PORT STATE SERVICE VERSION

80/tcp open http Cloudflare http proxy

|_http-server-header: cloudflare

|_http-title: Did not follow redirect to https://www.cloudflare.com/

443/tcp open ssl/http Cloudflare http proxy

|_http-server-header: cloudflare

|_http-title: Did not follow redirect to https://www.cloudflare.com/

|_ssl-cert: Subject: commonName=cloudflare.com/organizationName=Cloudflare, Inc./stateOrProvinceName=California/countryName=US

Subject Alternative Name: DNS:cloudflare.com, DNS:*.cloudflare.com, DNS:*.staging.cloudflare.com, DNS:*.dns.cloudflare.com, DNS:*.amp.cloudflare.com

|_Not valid before: 2021-06-04T00:00:00

|_Not valid after: 2022-06-03T23:59:59

_ssl-date: 2021-12-02T16:15:40+00:00; 0s from scanner time.

tls-alpn:

| h2

| http/1.1

- tls-nextprotoneg:

| h2

| http/1.1

8080/tcp open http Cloudflare http proxy

|_http-server-header: cloudflare

|_http-title: Did not follow redirect to https://www.cloudflare.com/

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Aggressive OS guesses: Actiontec M142WR-GEN3 WAP (96%), Linux 3.2 (96%), DD-WRT v24-sp2 (Linux 2.4.37) (95%), Linux 4.4 (95%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (92%), Microsoft Windows XP SP3 (92%), BlueArc Titan 2100 NAS device (91%), VMware Player virtual NAT device (91%), Pirelli DP-10 VoIP phone (87%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

1 0.14 ms 192.168.159.2

2 0.09 ms 104.16.133.229

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 88.13 seconds

(root@kali)-[/home/kali]

*Untitled - Notepad

File Edit Format View Help

19BIT150 HRITIK DUBEY

ENG IN 21:52 02-12-2021

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)

The screenshot shows a Kali Linux VM running in VMware Workstation. The terminal window displays the results of an nmap scan. The scan was run with the command `nmap -Pn --script vuln 192.168.93.196`. The output indicates that 998 ports were closed and 53 ports were open. One port, 514/tcp, was filtered. The scan took 144.55 seconds. A Notepad window titled "Untitled - Notepad" is also visible, containing the text "19BIT0150 HRITIK DUBEY". The desktop taskbar at the bottom shows various application icons.

```
[root@kali:~/home/kali]# nmap -Pn --script vuln 192.168.93.196
[...]
# valid after: 2022-08-03T23:59:59
# update: 2021-12-02T01:51:40+00:00; 6s from scanner time.
[...]
# http
# http/1.1
[...]
# http/1.1
# http proxy
[...]
# connect to https://www.cloudflare.com/
[...]
# reliable because we could not find at least 1 open and 1 closed port
# 192.168.93.196 ( https://nmap.org ) at 2021-12-02 11:43 EST
# Nmap scan report for 192.168.93.196
# Host is up (3.1s latency).
# Not shown: 998 closed ports
# PORT      STATE    SERVICE
# 53/tcp    open     domain
# 53/tcp    open     domain. Please report any incorrect results at https://nmap.org/submit/
# 514/tcp   filtered shell (1 host up) scanned in 48.13 seconds
# Nmap done: 1 IP address (1 host up) scanned in 144.55 seconds
# 192.168.93.196
[...]
# All addresses will be marked 'up' and scan times will be slower.
# Setting scan type to 'tiny' (https://nmap.org/) at 2021-12-02 11:28 EST
# Nmap scan report for 192.168.93.196
# 192.168.93.196:514/tcp filtered shell
# 192.168.93.196
# All addresses will be marked 'up' and scan times will be slower.
[...]
# 192.168.93.196:514/tcp filtered shell (10)
# 192.168.93.196
# Discovery disabled (--discover). All addresses will be marked 'up' and scan times will be slower.
# Setting scan type to 'tiny' (https://nmap.org/) at 2021-12-02 11:35 EST
# Nmap scan report for 192.168.93.196
# 192.168.93.196:514/tcp filtered shell (10)
# 192.168.93.196
```

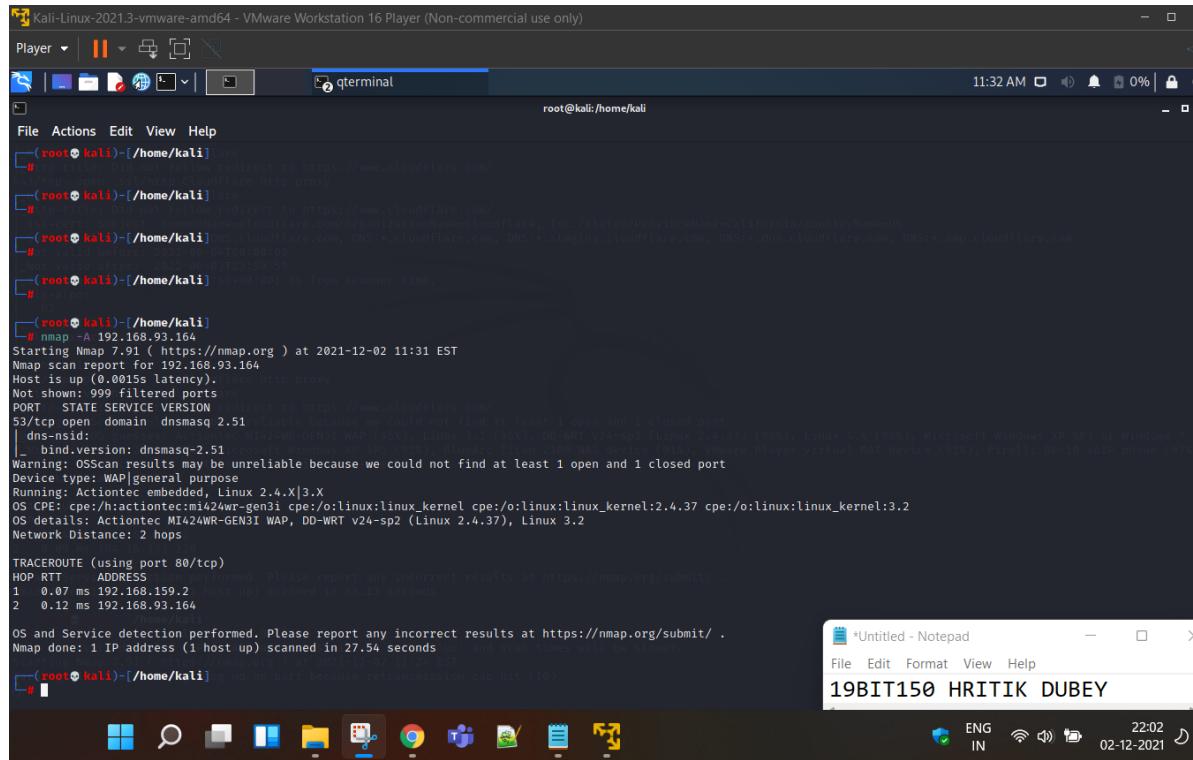
Not shown: 998 closed ports

PORT STATE SERVICE

53/tcp open domain

514/tcp filtered shell

9. nmap -A ipaddr

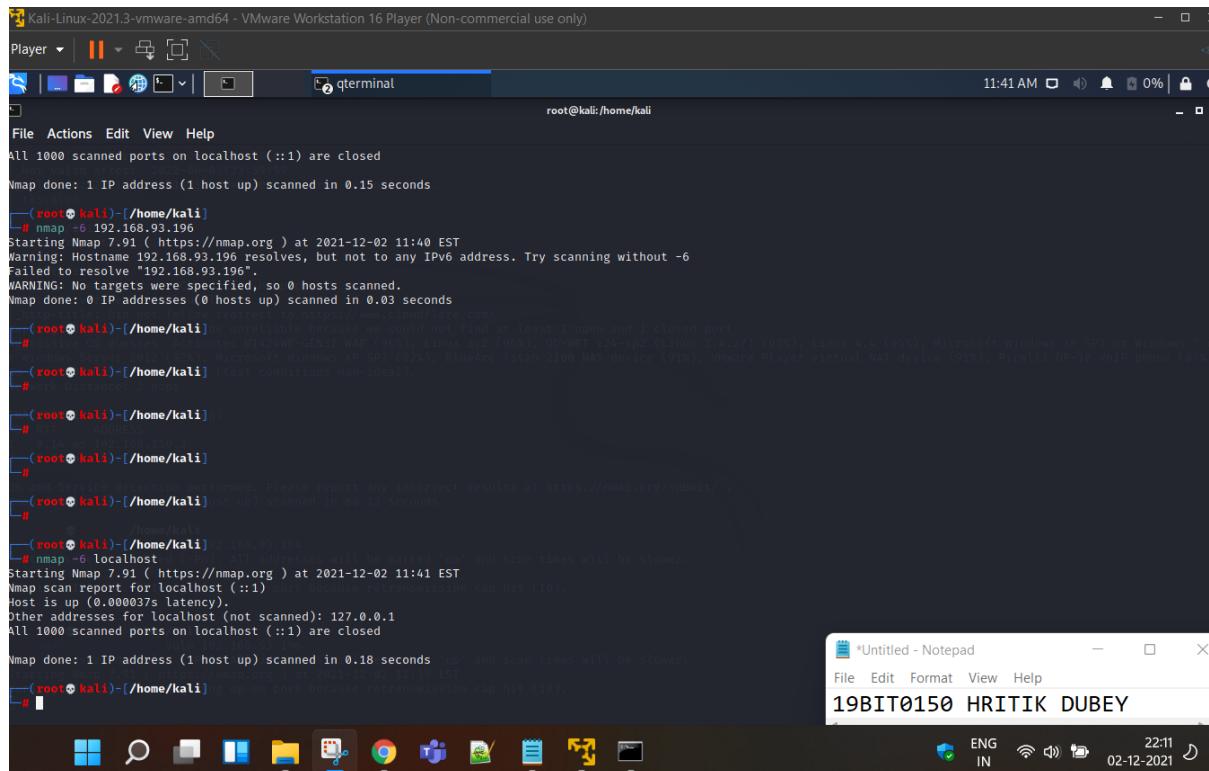


```
# nmap -A 192.168.93.196
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-02 11:31 EST
Nmap scan report for 192.168.93.196
Host is up (0.0015s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
53/tcp    open  domain dnsmasq 2.51
          bind.version: dnsmasq-2.51
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose
Running: Actiontec embedded, Linux 2.4.X|3.X
OS CPE: cpe:/h:actiontec:mi24wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2
OS details: Actiontec MI24WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  0.07 ms  192.168.159.2 (host up) scanned in 88.11 seconds
2  0.12 ms  192.168.93.196

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 27.54 seconds
#
```

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



```
All 1000 scanned ports on localhost (::1) are closed
Warning: Hostname 192.168.93.196 resolves, but not to any IPv6 address. Try scanning without -6
Failed to resolve "192.168.93.196".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (@ hosts up) scanned in 0.03 seconds

# nmap -6 192.168.93.196
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-02 11:40 EST
Warning: Hostname 192.168.93.196 resolves, but not to any IPv6 address. Try scanning without -6
Failed to resolve "192.168.93.196".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (@ hosts up) scanned in 0.03 seconds

# nmap -6 localhost
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-02 11:41 EST
Nmap scan report for localhost (::1)
Host is up (0.000037s latency).
Other addresses for localhost (not scanned): 127.0.0.1
All 1000 scanned ports on localhost (::1) are closed

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
#
```