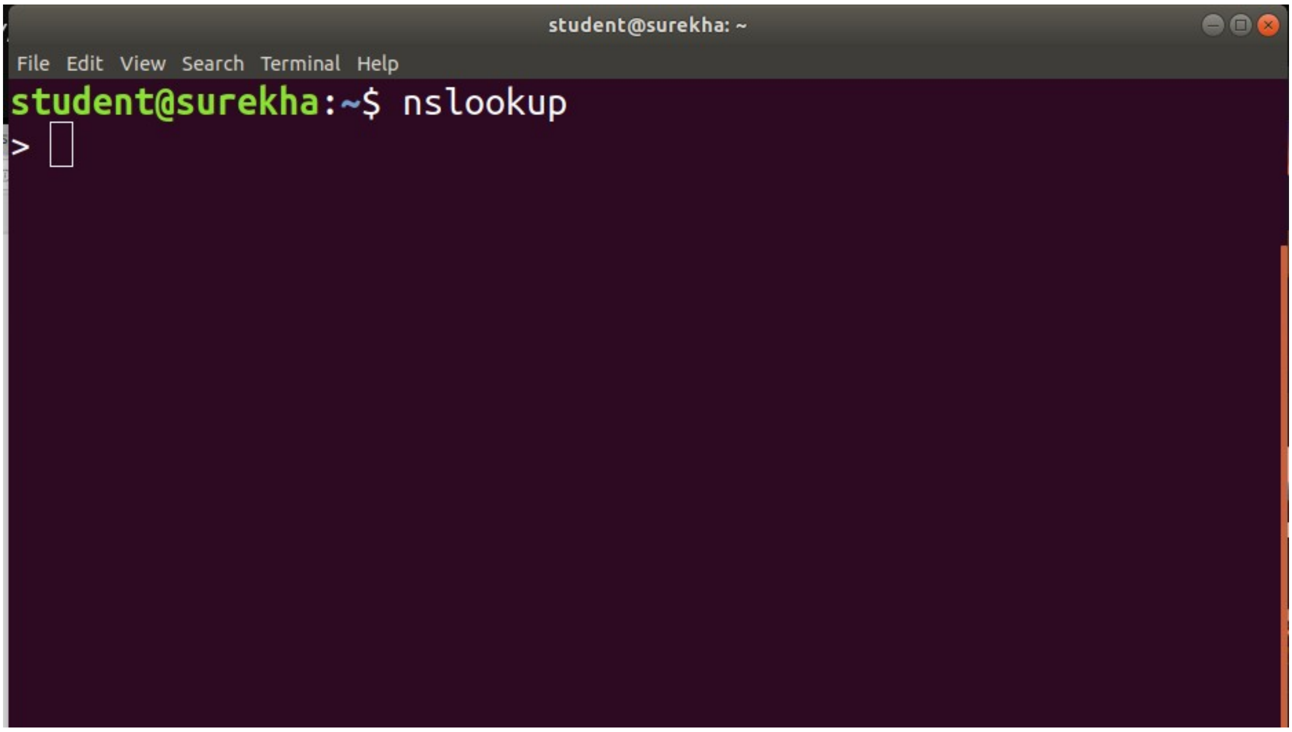
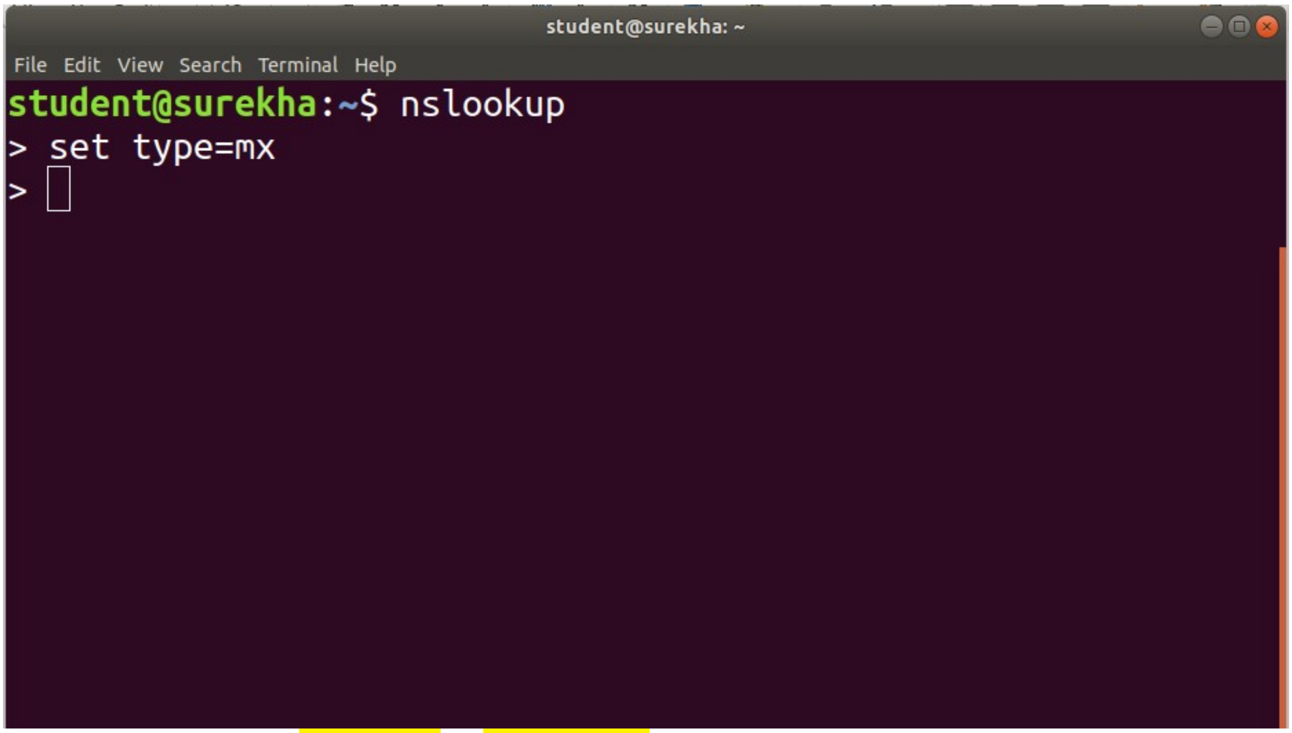
1] Find out the mail servers of the following domain:
ibm.com
wipro.com

to find the mail servers of a domain
open your terminal and type nslookup



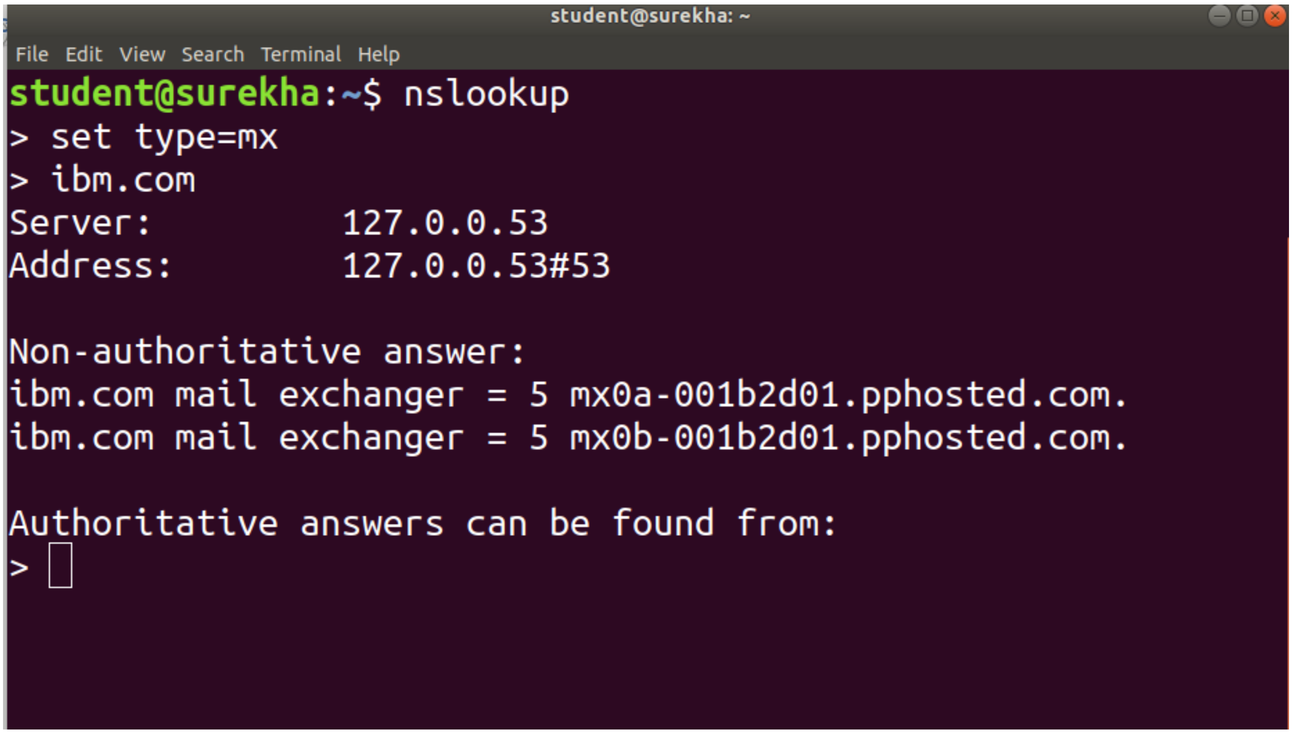
```
student@surekha:~$ nslookup
> 
```

type set type=mx this will cause nslookup to return only mail exchange records from the dns servers.

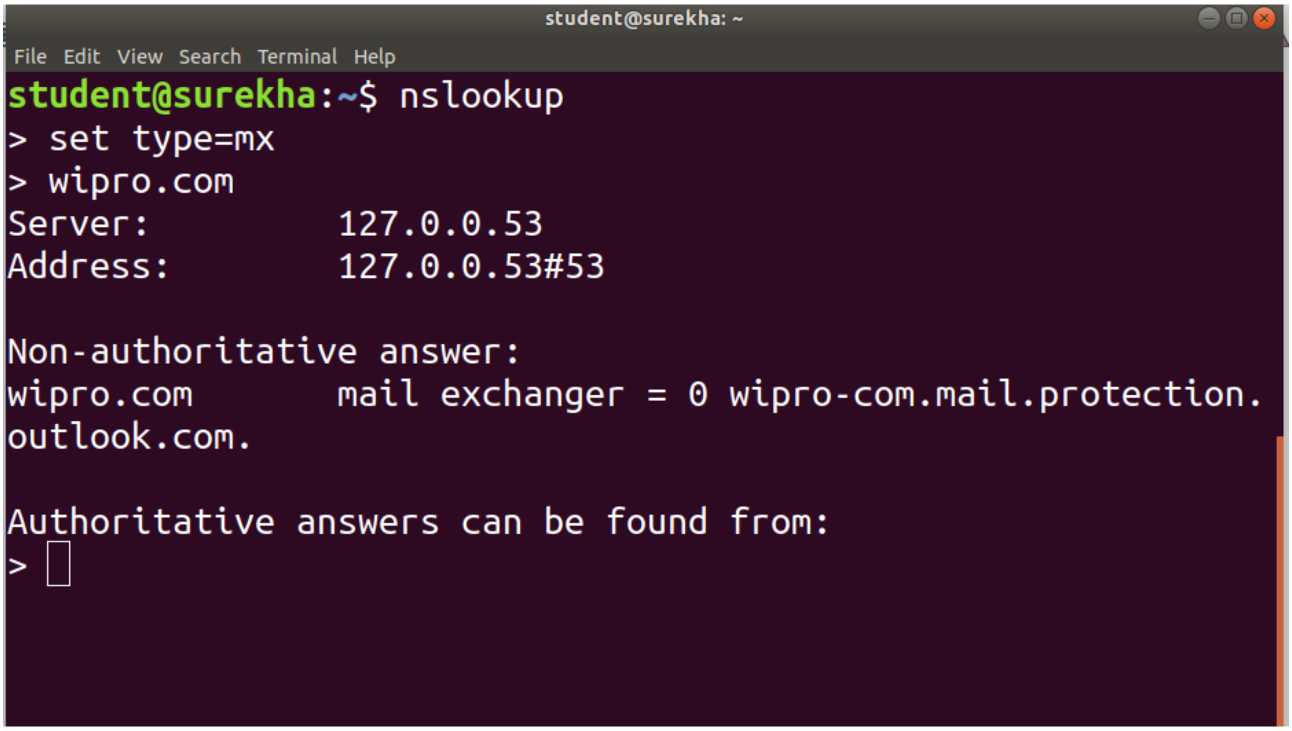


```
student@surekha:~$ nslookup
> set type=mx
> 
```

Type any domain like “ibm.com” or “wipro.com” it will return the mail servers of that domain



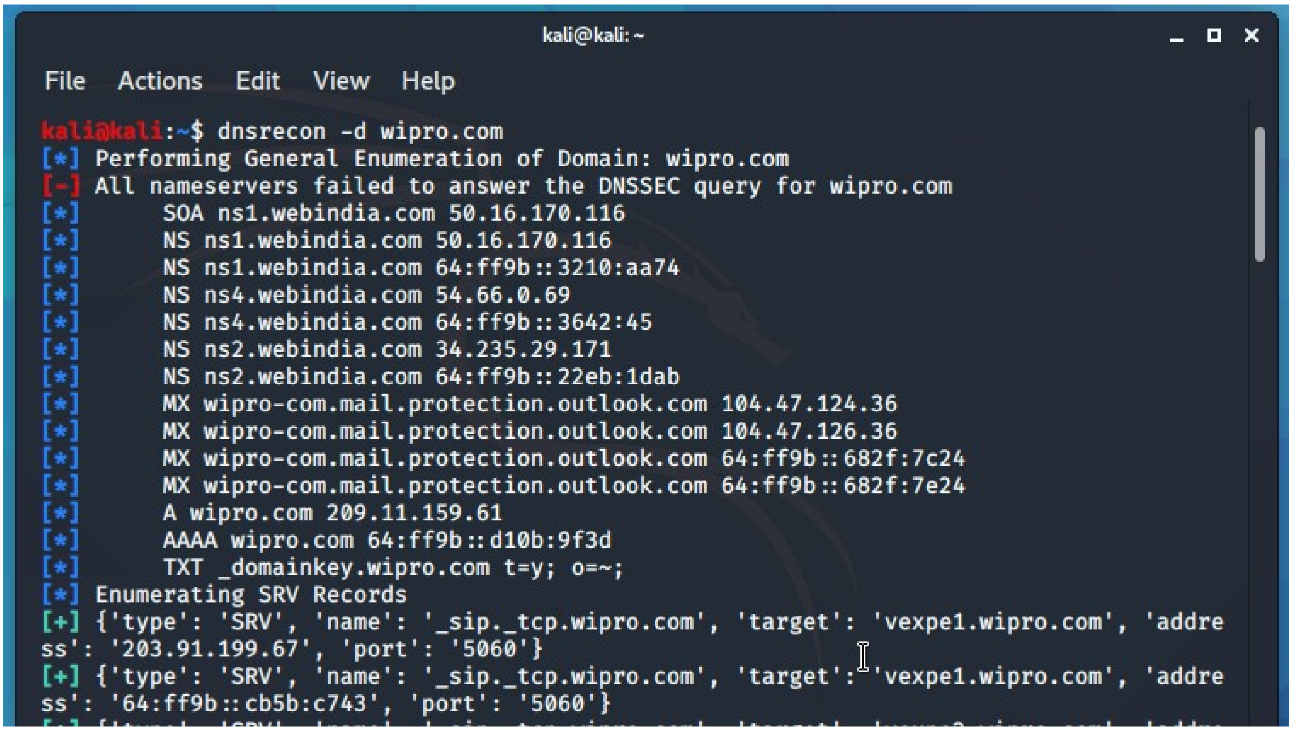
```
student@surekha:~$ nslookup
> set type=mx
> ibm.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
ibm.com mail exchanger = 5 mx0a-001b2d01.pphosted.com.
ibm.com mail exchanger = 5 mx0b-001b2d01.pphosted.com.

Authoritative answers can be found from:
> 
```



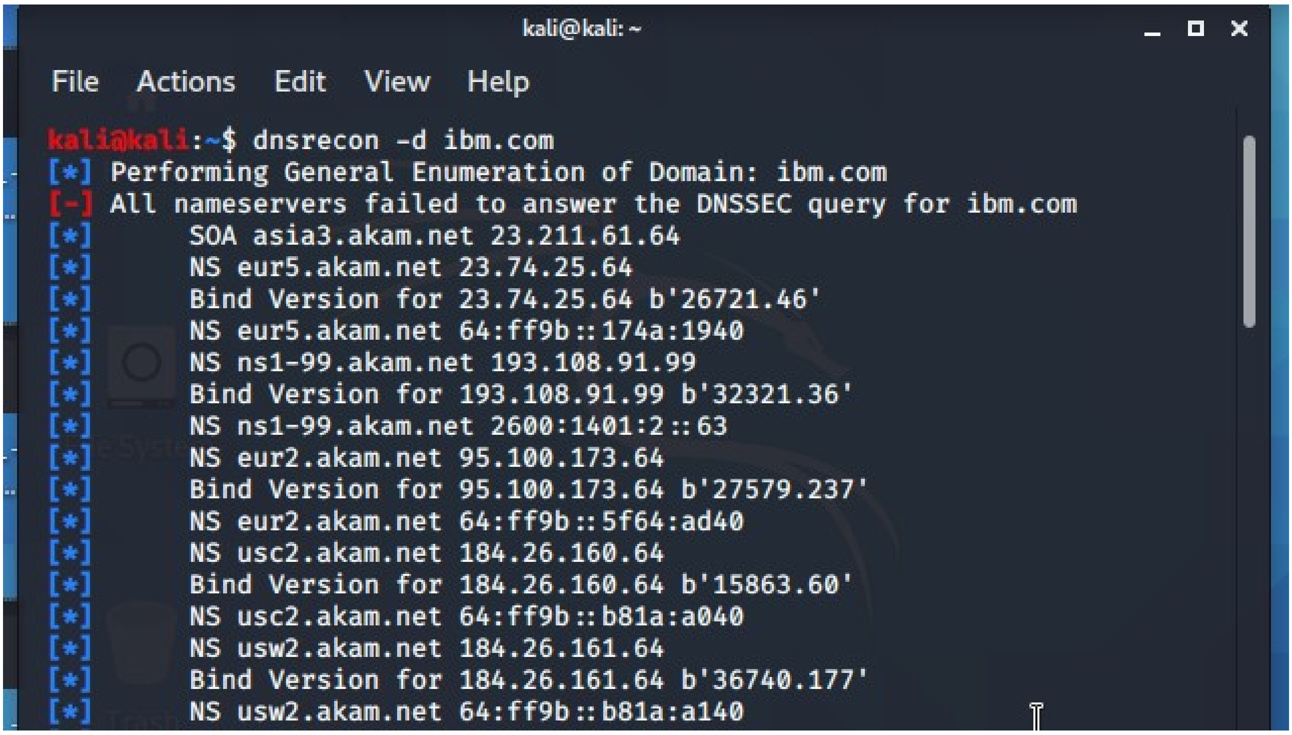
```
student@surekha:~$ nslookup
> set type=mx
> wipro.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
wipro.com       mail exchanger = 0 wipro-com.mail.protection.
outlook.com.

Authoritative answers can be found from:
> 
```

2]find the locations,where these email servers are hosted

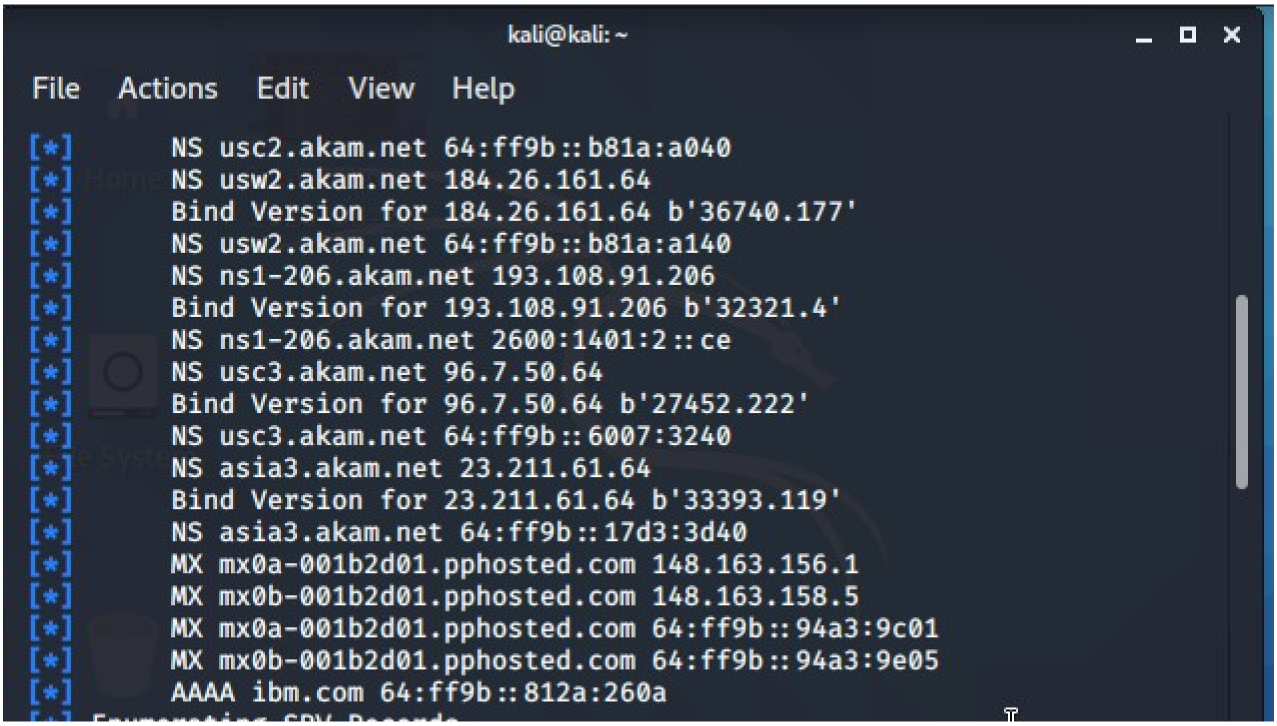
to know the location of the mail servers first we should know the ip address of that mail server for that we use dnrecon tool.
Open terminal and type dnsrecon -d <domain name>



```
kali@kali:~$ dnsrecon -d wipro.com
[*] Performing General Enumeration of Domain: wipro.com
[-] All nameservers failed to answer the DNSSEC query for wipro.com
[*]      SOA ns1.webindia.com 50.16.170.116
[*]      NS ns1.webindia.com 50.16.170.116
[*]      NS ns1.webindia.com 64:ff9b::3210:aa74
[*]      NS ns4.webindia.com 54.66.0.69
[*]      NS ns4.webindia.com 64:ff9b::3642:45
[*]      NS ns2.webindia.com 34.235.29.171
[*]      NS ns2.webindia.com 64:ff9b::22eb:1dab
[*]      MX wipro-com.mail.protection.outlook.com 104.47.124.36
[*]      MX wipro-com.mail.protection.outlook.com 104.47.126.36
[*]      MX wipro-com.mail.protection.outlook.com 64:ff9b::682f:7c24
[*]      MX wipro-com.mail.protection.outlook.com 64:ff9b::682f:7e24
[*]      A wipro.com 209.11.159.61
[*]      AAAA wipro.com 64:ff9b::d10b:9f3d
[*]      TXT _domainkey.wipro.com t=y; o=~;
[*] Enumerating SRV Records
[+] {'type': 'SRV', 'name': '_sip._tcp.wipro.com', 'target': 'vexpe1.wipro.com', 'addre
ss': '203.91.199.67', 'port': '5060'}
[+] {'type': 'SRV', 'name': '_sip._tcp.wipro.com', 'target': 'vexpe1.wipro.com', 'addre
ss': '64:ff9b::cb5b:c743', 'port': '5060'}
```

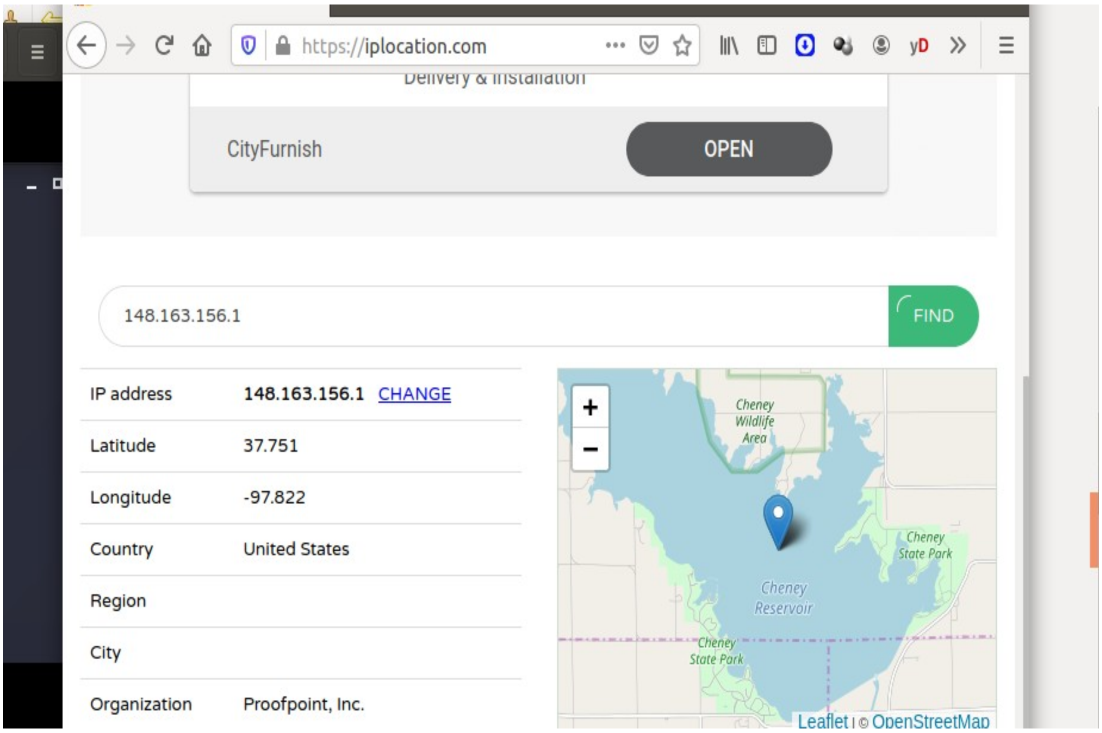


```
kali@kali:~$ dnsrecon -d ibm.com
[*] Performing General Enumeration of Domain: ibm.com
[-] All nameservers failed to answer the DNSSEC query for ibm.com
[*]      SOA asia3.akam.net 23.211.61.64
[*]      NS eur5.akam.net 23.74.25.64
[*]      Bind Version for 23.74.25.64 b'26721.46'
[*]      NS eur5.akam.net 64:ff9b::174a:1940
[*]      NS ns1-99.akam.net 193.108.91.99
[*]      Bind Version for 193.108.91.99 b'32321.36'
[*]      NS ns1-99.akam.net 2600:1401:2::63
[*]      NS eur2.akam.net 95.100.173.64
[*]      Bind Version for 95.100.173.64 b'27579.237'
[*]      NS eur2.akam.net 64:ff9b::5f64:ad40
[*]      NS usc2.akam.net 184.26.160.64
[*]      Bind Version for 184.26.160.64 b'15863.60'
[*]      NS usc2.akam.net 64:ff9b::b81a:a040
[*]      NS usw2.akam.net 184.26.161.64
[*]      Bind Version for 184.26.161.64 b'36740.177'
[*]      NS usw2.akam.net 64:ff9b::b81a:a140
```



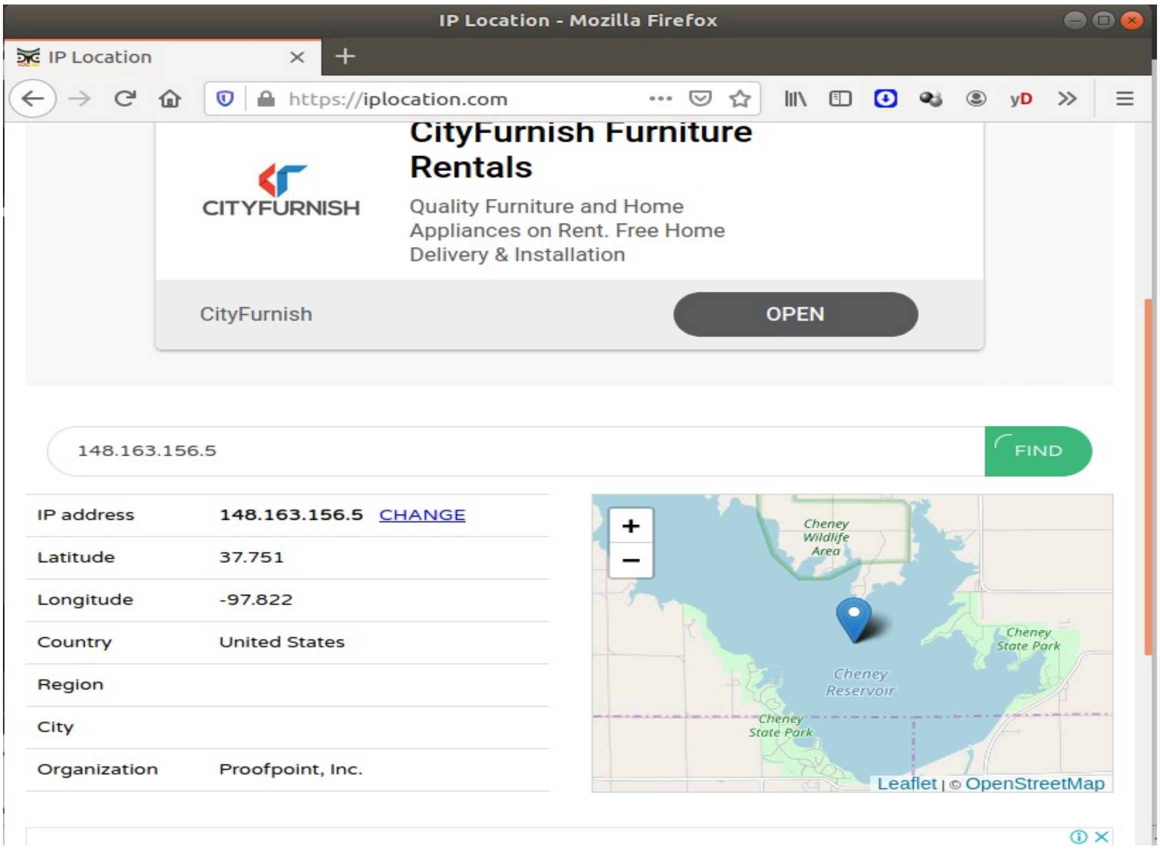
```
[*]      NS usc2.akam.net 64:ff9b::b81a:a040
[*]      NS usw2.akam.net 184.26.161.64
[*]      Bind Version for 184.26.161.64 b'36740.177'
[*]      NS usw2.akam.net 64:ff9b::b81a:a140
[*]      NS ns1-206.akam.net 193.108.91.206
[*]      Bind Version for 193.108.91.206 b'32321.4'
[*]      NS ns1-206.akam.net 2600:1401:2::ce
[*]      NS usc3.akam.net 96.7.50.64
[*]      Bind Version for 96.7.50.64 b'27452.222'
[*]      NS usc3.akam.net 64:ff9b::6007:3240
[*]      NS asia3.akam.net 23.211.61.64
[*]      Bind Version for 23.211.61.64 b'33393.119'
[*]      NS asia3.akam.net 64:ff9b::17d3:3d40
[*]      MX mx0a-001b2d01.pphosted.com 148.163.156.1
[*]      MX mx0b-001b2d01.pphosted.com 148.163.158.5
[*]      MX mx0a-001b2d01.pphosted.com 64:ff9b::94a3:9c01
[*]      MX mx0b-001b2d01.pphosted.com 64:ff9b::94a3:9e05
[*]      AAAA ibm.com 64:ff9b::812a:260a
[*] Enumerating SRV Records
```

the sentence starting with mx are the mail servers.
Now we got the mail servers ip addresses
open browser and search for “iplocation.com” there type the ip and it will give the location of that.



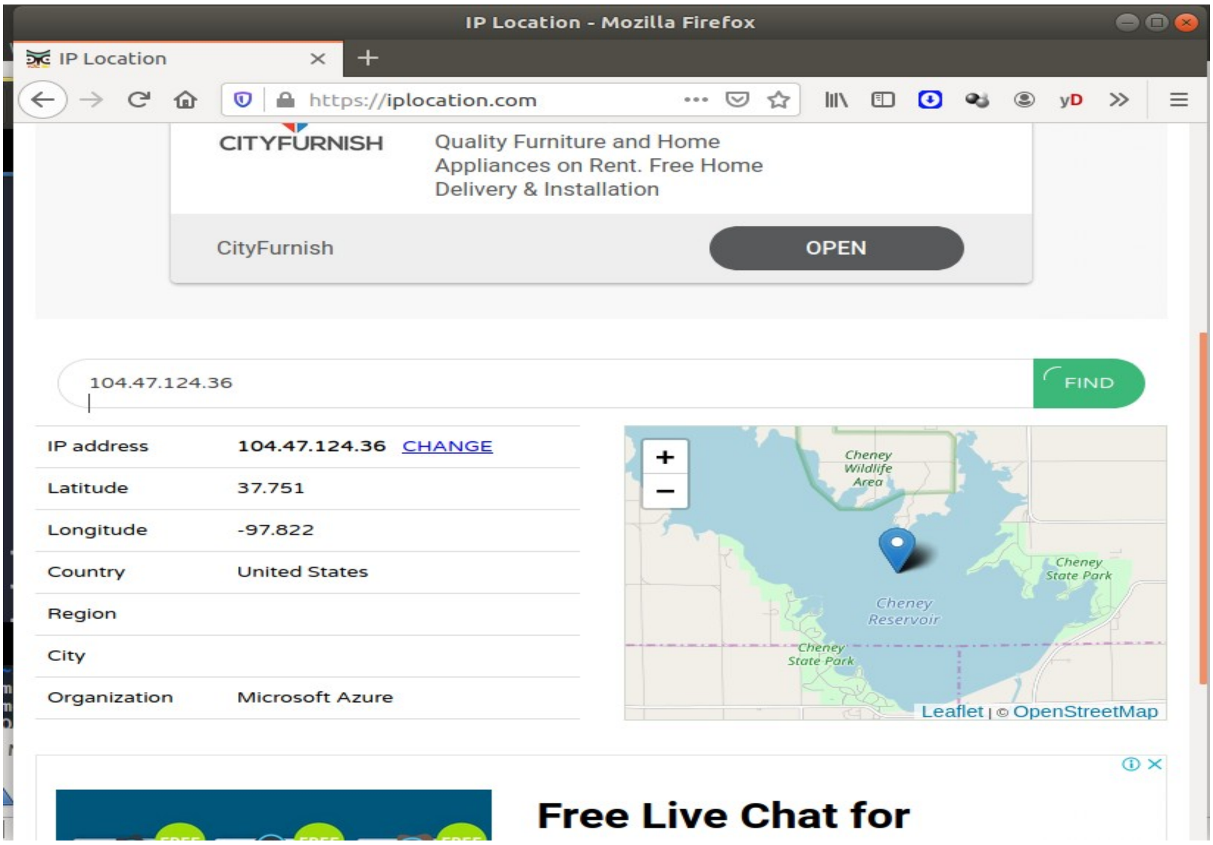
148.163.156.1

IP address	148.163.156.1 CHANGE
Latitude	37.751
Longitude	-97.822
Country	United States
Region	
City	
Organization	Proofpoint, Inc.



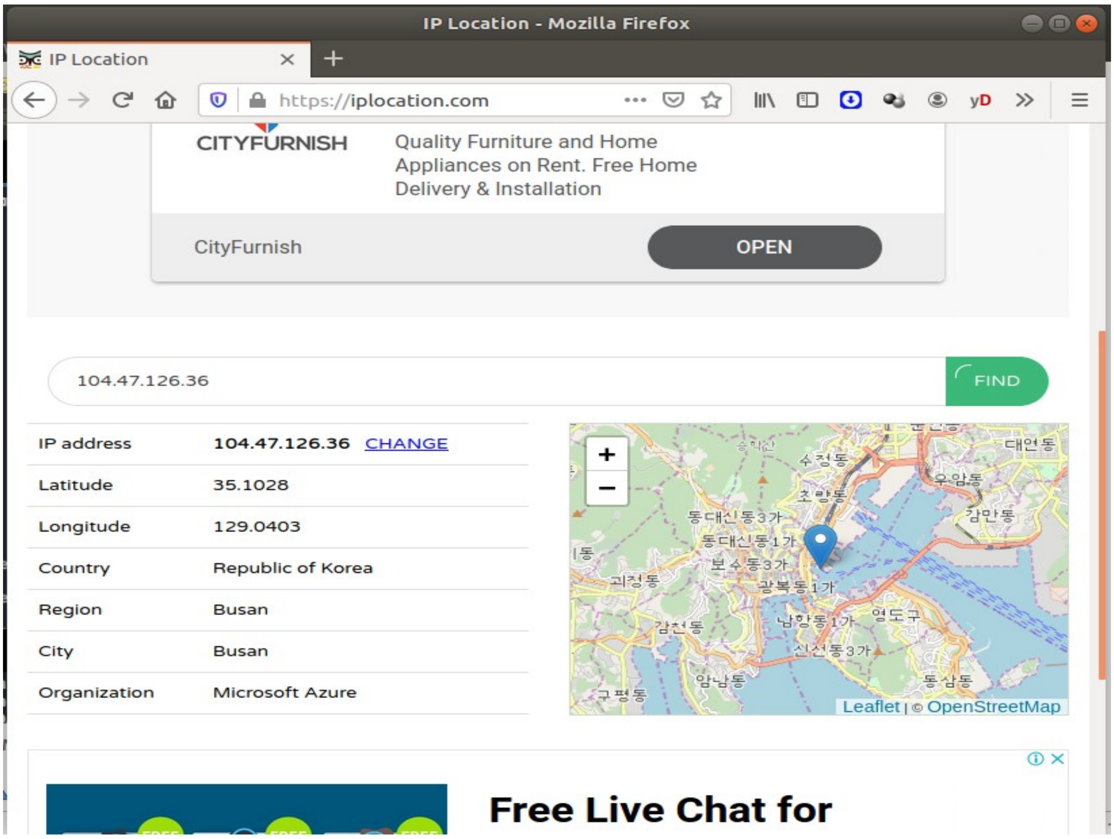
148.163.156.5

IP address	148.163.156.5 CHANGE
Latitude	37.751
Longitude	-97.822
Country	United States
Region	
City	
Organization	Proofpoint, Inc.



104.47.124.36

IP address	104.47.124.36 CHANGE
Latitude	37.751
Longitude	-97.822
Country	United States
Region	
City	
Organization	Microsoft Azure

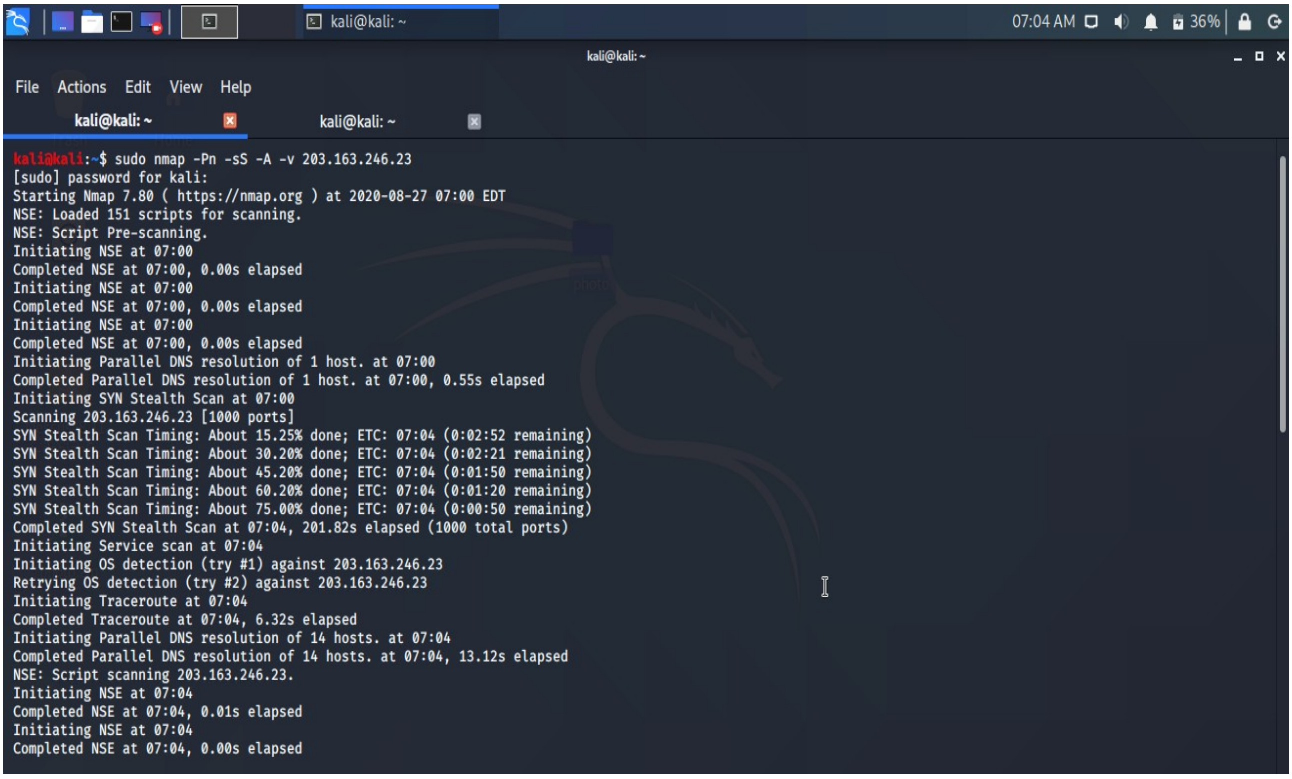


104.47.126.36 FIND

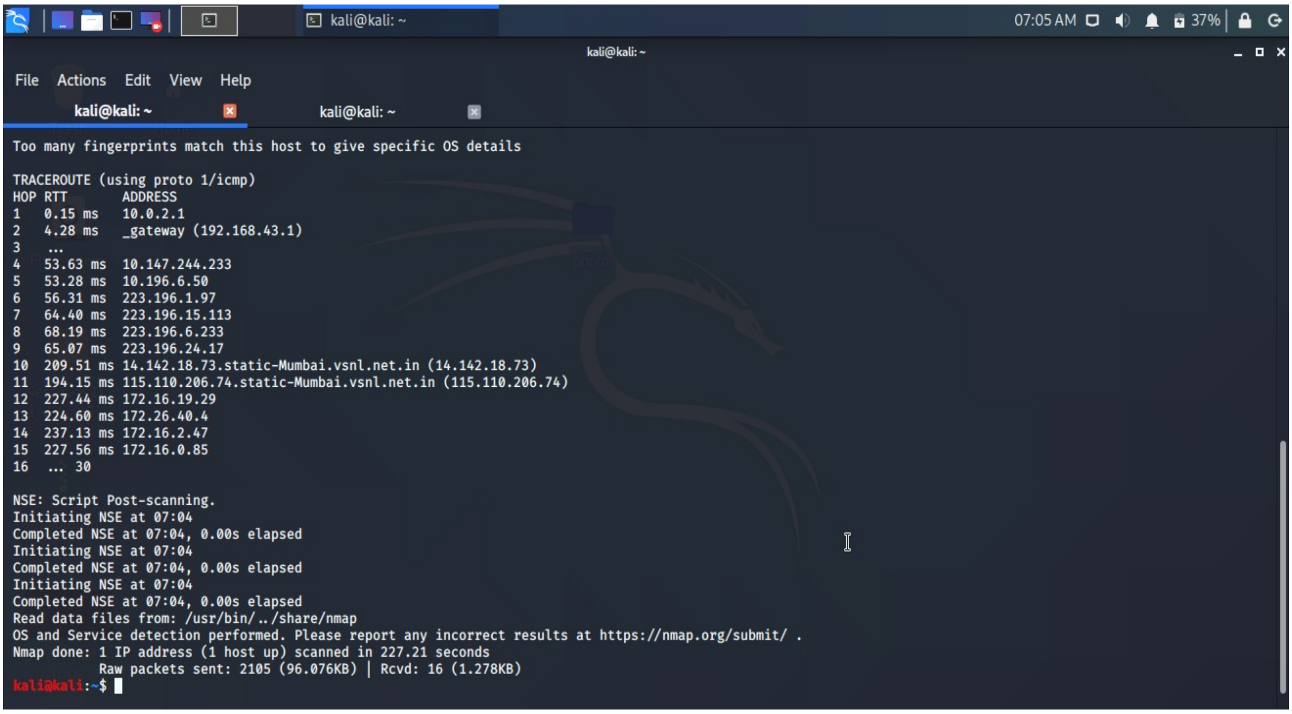
IP address	104.47.126.36 CHANGE
Latitude	35.1028
Longitude	129.0403
Country	Republic of Korea
Region	Busan
City	Busan
Organization	Microsoft Azure

3]scan and find out port numbers open 203.163.264.23

to scan the open ports we use nmap tool.
Open your terminal and type sudo nmap -Pn -sS -A -v 203.163.246.23

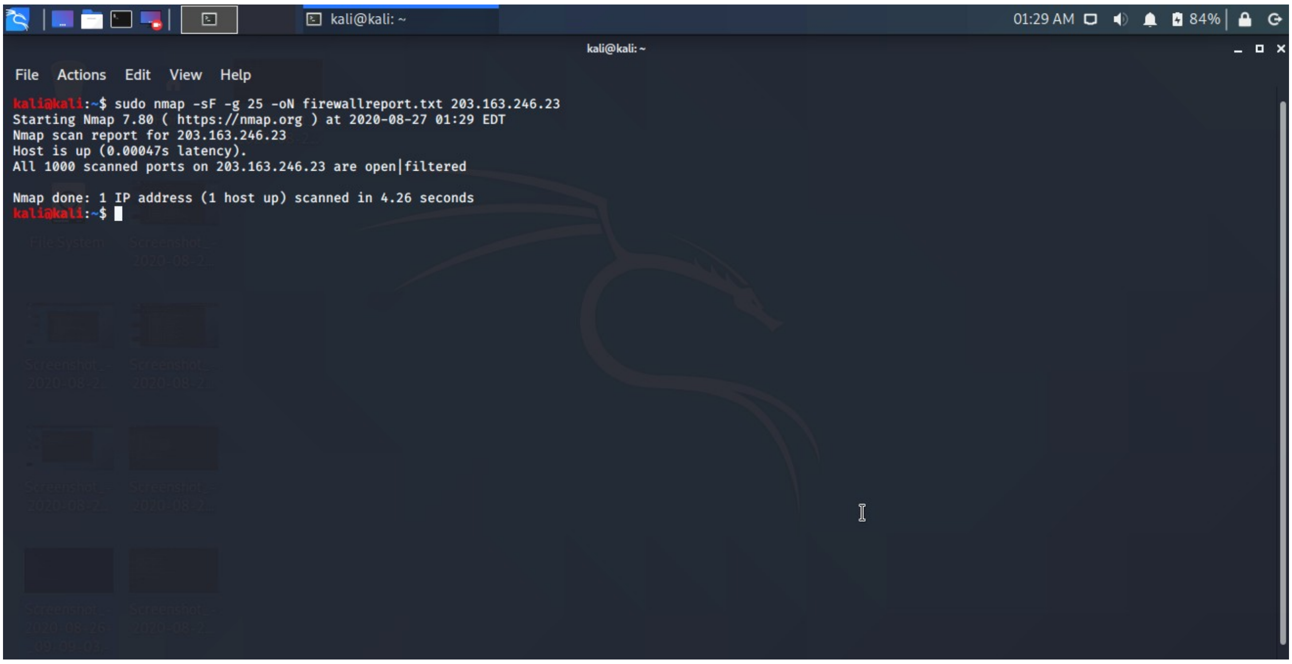


```
kali@kali:~$ sudo nmap -Pn -sS -A -v 203.163.246.23
[sudo] password for kali:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-27 07:00 EDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 07:00
Completed NSE at 07:00, 0.00s elapsed
Initiating NSE at 07:00
Completed NSE at 07:00, 0.00s elapsed
Initiating NSE at 07:00
Completed NSE at 07:00, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 07:00
Completed Parallel DNS resolution of 1 host. at 07:00, 0.55s elapsed
Initiating SYN Stealth Scan at 07:00
Scanning 203.163.246.23 [1000 ports]
SYN Stealth Scan Timing: About 15.25% done; ETC: 07:04 (0:02:52 remaining)
SYN Stealth Scan Timing: About 30.20% done; ETC: 07:04 (0:02:21 remaining)
SYN Stealth Scan Timing: About 45.20% done; ETC: 07:04 (0:01:50 remaining)
SYN Stealth Scan Timing: About 60.20% done; ETC: 07:04 (0:01:20 remaining)
SYN Stealth Scan Timing: About 75.00% done; ETC: 07:04 (0:00:50 remaining)
Completed SYN Stealth Scan at 07:04, 201.82s elapsed (1000 total ports)
Initiating Service scan at 07:04
Initiating OS detection (try #1) against 203.163.246.23
Retrying OS detection (try #2) against 203.163.246.23
Initiating Traceroute at 07:04
Completed Traceroute at 07:04, 6.32s elapsed
Initiating Parallel DNS resolution of 14 hosts. at 07:04
Completed Parallel DNS resolution of 14 hosts. at 07:04, 13.12s elapsed
NSE: Script scanning 203.163.246.23.
Initiating NSE at 07:04
Completed NSE at 07:04, 0.01s elapsed
Initiating NSE at 07:04
Completed NSE at 07:04, 0.00s elapsed
```



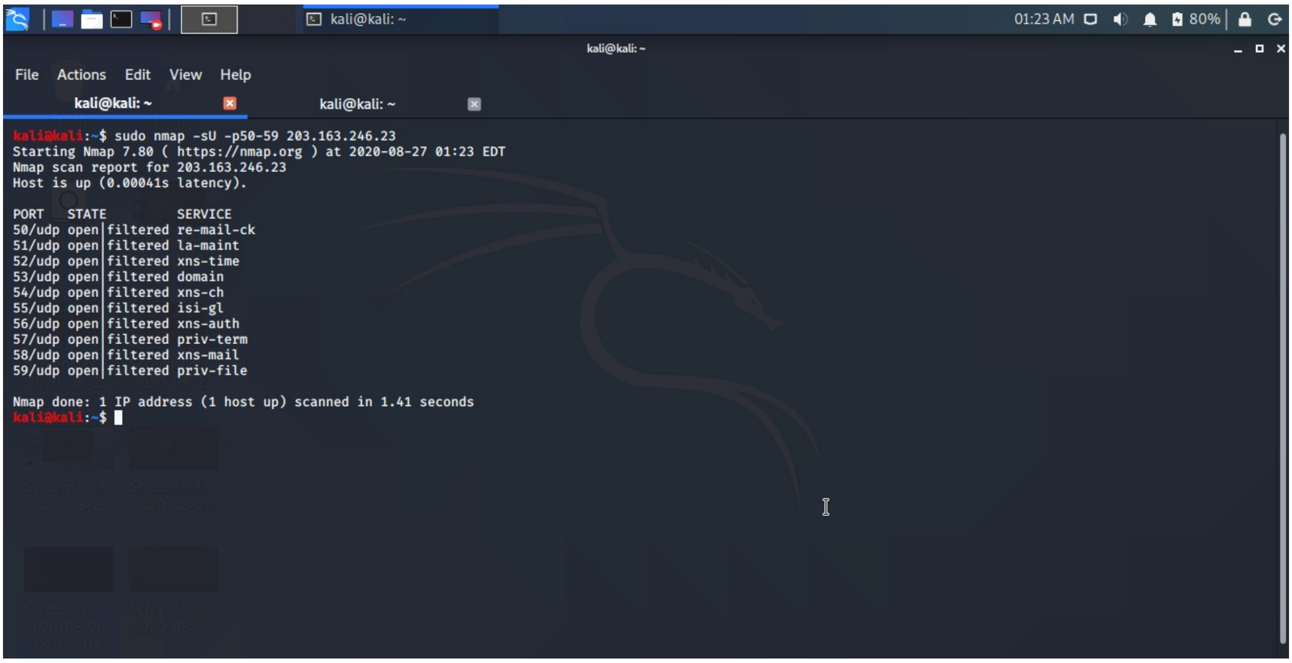
```
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using proto 1/icmp)
HOP RTT       ADDRESS
1   0.15 ms   10.0.2.1
2   4.28 ms   _gateway (192.168.43.1)
3   ...
4   53.63 ms  10.147.244.233
5   53.28 ms  10.196.6.50
6   56.31 ms  223.196.1.97
7   64.40 ms  223.196.15.113
8   68.19 ms  223.196.6.233
9   65.07 ms  223.196.24.17
10  209.51 ms 14.142.18.73.static-Mumbai.vsnl.net.in (14.142.18.73)
11  194.15 ms 115.110.206.74.static-Mumbai.vsnl.net.in (115.110.206.74)
12  227.44 ms 172.16.19.29
13  224.60 ms 172.26.40.4
14  237.13 ms 172.16.2.47
15  227.56 ms 172.16.0.85
16   ... 30

NSE: Script Post-scanning.
Initiating NSE at 07:04
Completed NSE at 07:04, 0.00s elapsed
Initiating NSE at 07:04
Completed NSE at 07:04, 0.00s elapsed
Initiating NSE at 07:04
Completed NSE at 07:04, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
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 227.21 seconds
           Raw packets sent: 2105 (96.076KB) | Rcvd: 16 (1.278KB)
kali@kali:~$ 
```

sudo nmap -sF -g 25 -oN firewallreport.txt 203.163.246.23



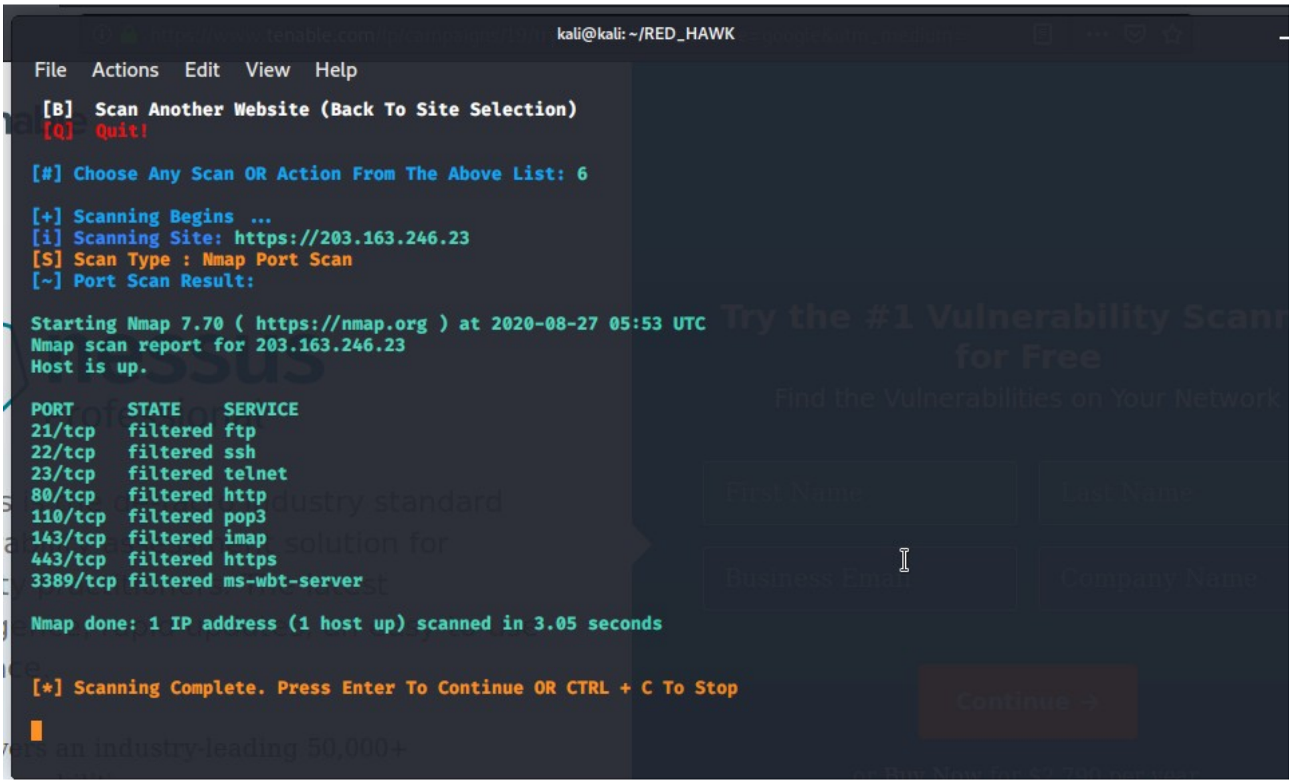
```
kali@kali:~$ sudo nmap -sF -g 25 -oN firewallreport.txt 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-27 01:29 EDT
Nmap scan report for 203.163.246.23
Host is up (0.00047s latency).
All 1000 scanned ports on 203.163.246.23 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 4.26 seconds
kali@kali:~$ 
```

the server is protected by the firewall so to get the open ports we try another command
sudo nmap -sU -p50-59 203.163.246.23



```
kali@kali:~$ sudo nmap -sU -p50-59 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-27 01:23 EDT
Nmap scan report for 203.163.246.23
Host is up (0.00041s latency).

PORT      STATE         SERVICE
50/udp open|filtered re-mail-ck
51/udp open|filtered la-maint
52/udp open|filtered xns-time
53/udp open|filtered domain
54/udp open|filtered xns-ch
55/udp open|filtered isi-gl
56/udp open|filtered xns-auth
57/udp open|filtered priv-term
58/udp open|filtered xns-mail
59/udp open|filtered priv-file

Nmap done: 1 IP address (1 host up) scanned in 1.41 seconds
kali@kali:~$
```

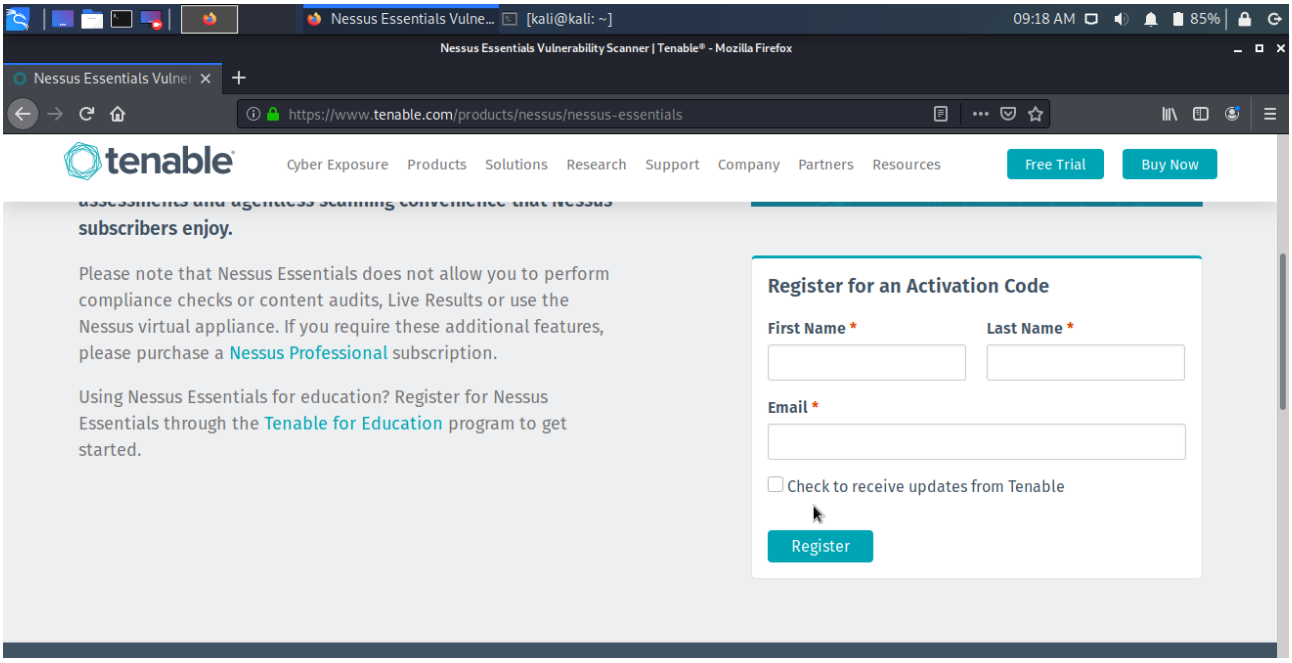
we can also use a tool called red hawk to know the open ports
commands to install and run red hawk
1.git clone https://github.com/Tuhinshubhra/RED_HAWK
2.cd RED_HAWK
3.php rhawk.php
enter the ip or domain name then find the open ports.



```
 [B]  Scan Another Website (Back To Site Selection)
 [Q]  Quit!

[#] Choose Any Scan OR Action From The Above List: 6

[+] Scanning Begins ...
[i] Scanning Site: https://203.163.246.23
[S] Scan Type : Nmap Port Scan
[~] Port Scan Result:

Starting Nmap 7.70 ( https://nmap.org ) at 2020-08-27 05:53 UTC
Nmap scan report for 203.163.246.23
Host is up.

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
80/tcp   filtered http
110/tcp  filtered pop3
143/tcp  filtered imap
443/tcp  filtered https
3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 3.05 seconds


[*] Scanning Complete. Press Enter To Continue OR CTRL + C To Stop
```

4]install nessus in a vm and scan your laptop/desktop for CVE

first of all we should install nessus
open browser and search https://www.tenable.com/products/nessus-home
register there for activation code


Nessus Essentials Vulnerability Scanner | Tenable® - Mozilla Firefox
https://www.tenable.com/products/nessus/nessus-essentials
tenable
Cyber Exposure
Products
Solutions
Research
Support
Company
Partners
Resources
Free Trial
Buy Now

subscribers enjoy.

Please note that Nessus Essentials does not allow you to perform compliance checks or content audits, Live Results or use the Nessus virtual appliance. If you require these additional features, please purchase a Nessus Professional subscription.

Using Nessus Essentials for education? Register for Nessus Essentials through the Tenable for Education program to get started.

Register for an Activation Code

First Name *

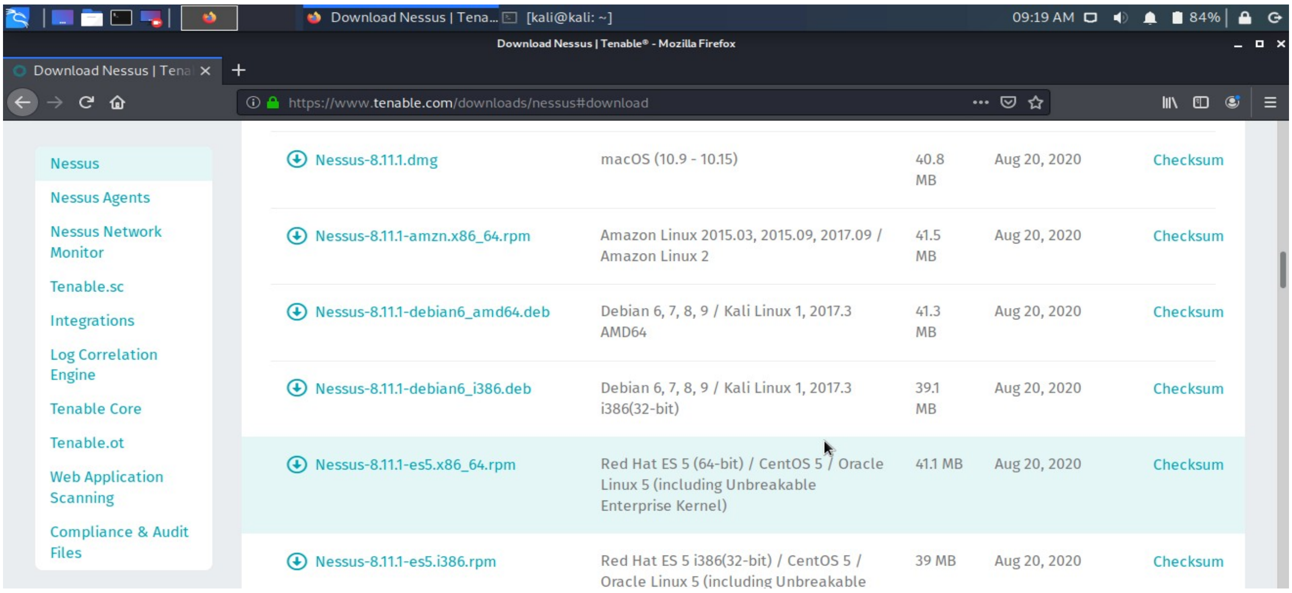
Last Name *

Email *

□ Check to receive updates from Tenable

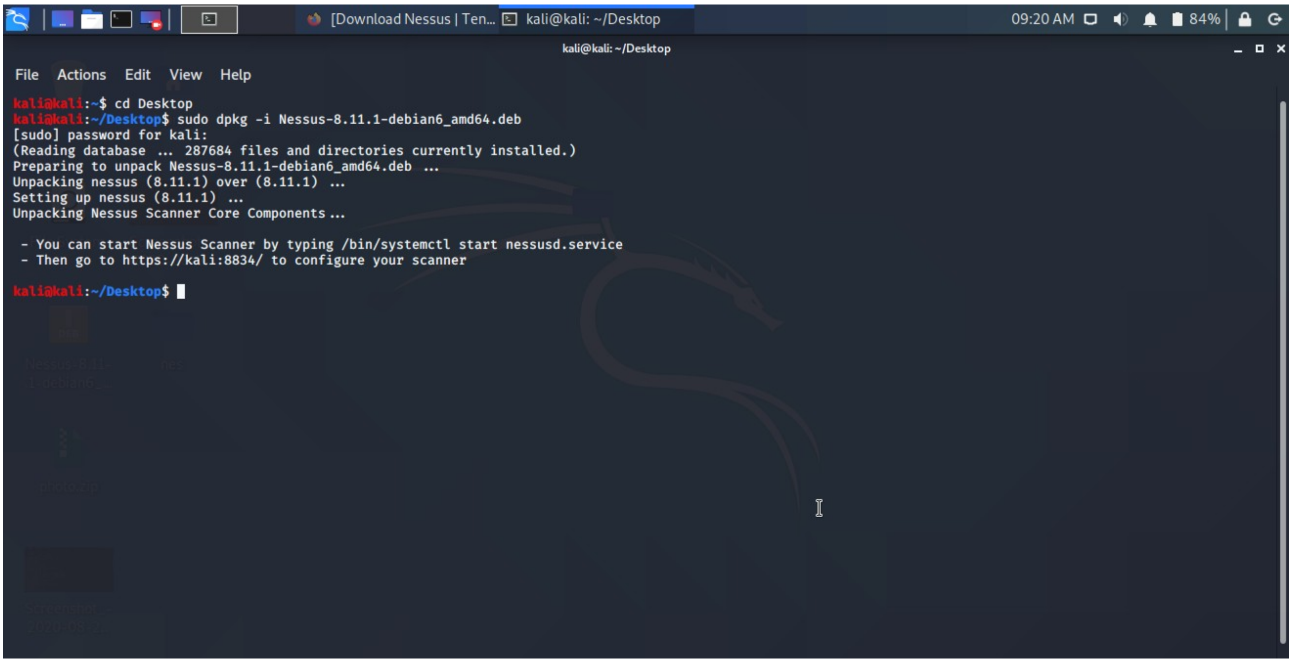
Register

you will get an email with activation code.
Open https://www.tenable.com/downloads/nessus#download
download the file which is suitable for your os



Nessus-8.11.1.dmg	macOS (10.9 - 10.15)	40.8 MB	Aug 20, 2020	Checksum
Nessus-8.11.1-amzn.x86_64.rpm	Amazon Linux 2015.03, 2015.09, 2017.09 / Amazon Linux 2	41.5 MB	Aug 20, 2020	Checksum
Nessus-8.11.1-debian6_amd64.deb	Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 AMD64	41.3 MB	Aug 20, 2020	Checksum
Nessus-8.11.1-debian6_i386.deb	Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 i386(32-bit)	39.1 MB	Aug 20, 2020	Checksum
Nessus-8.11.1-es5.x86_64.rpm	Red Hat ES 5 (64-bit) / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel)	41.1 MB	Aug 20, 2020	Checksum
Nessus-8.11.1-es5.i386.rpm	Red Hat ES 5 i386(32-bit) / CentOS 5 / Oracle Linux 5 (including Unbreakable	39 MB	Aug 20, 2020	Checksum

open your terminal and navigate to the folder where you have the downloaded file.
And enter dpkg -i <file name>



```
kali@kali:~$ cd Desktop
kali@kali:~/Desktop$ sudo dpkg -i Nessus-8.11.1-debian6_amd64.deb
[sudo] password for kali:
(Reading database ... 287684 files and directories currently installed.)
Preparing to unpack Nessus-8.11.1-debian6_amd64.deb ...
Unpacking nessus (8.11.1) over (8.11.1) ...
Setting up nessus (8.11.1) ...
Unpacking Nessus Scanner Core Components...

 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
 - Then go to https://kali:8834/ to configure your scanner

kali@kali:~/Desktop$ 
```

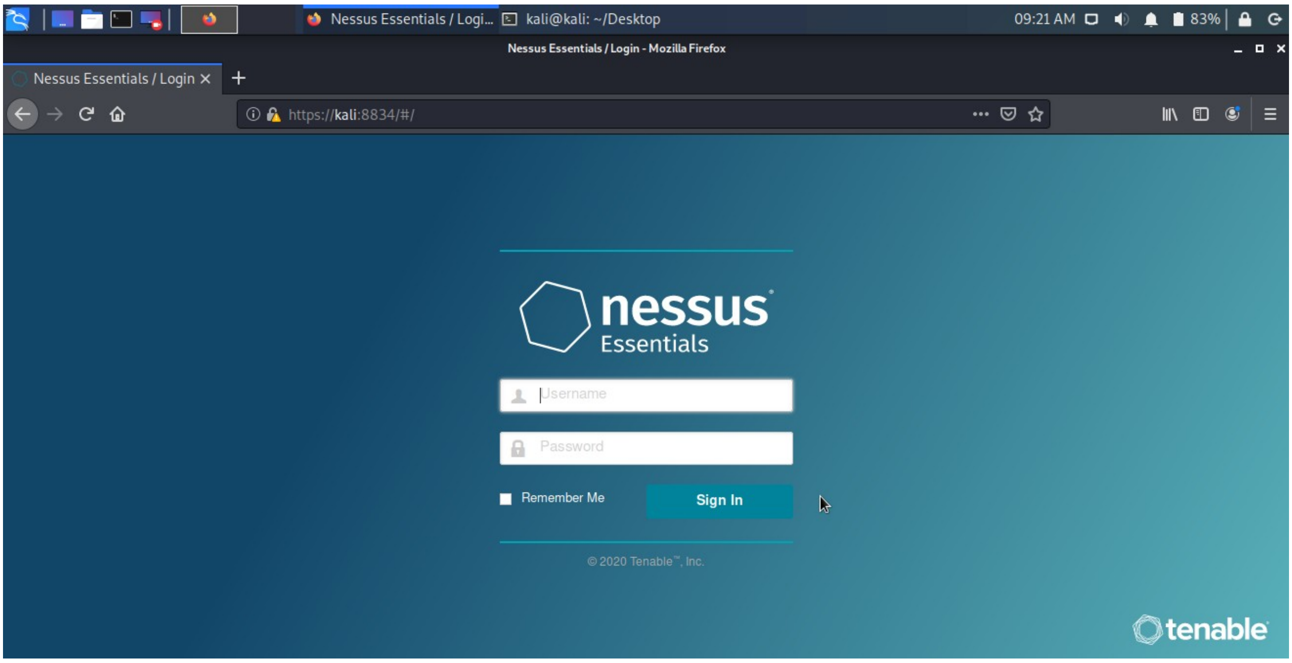
now type the cammand which you get in the terminal prompt.for me it is */bin/*systemctl start nessusd.service

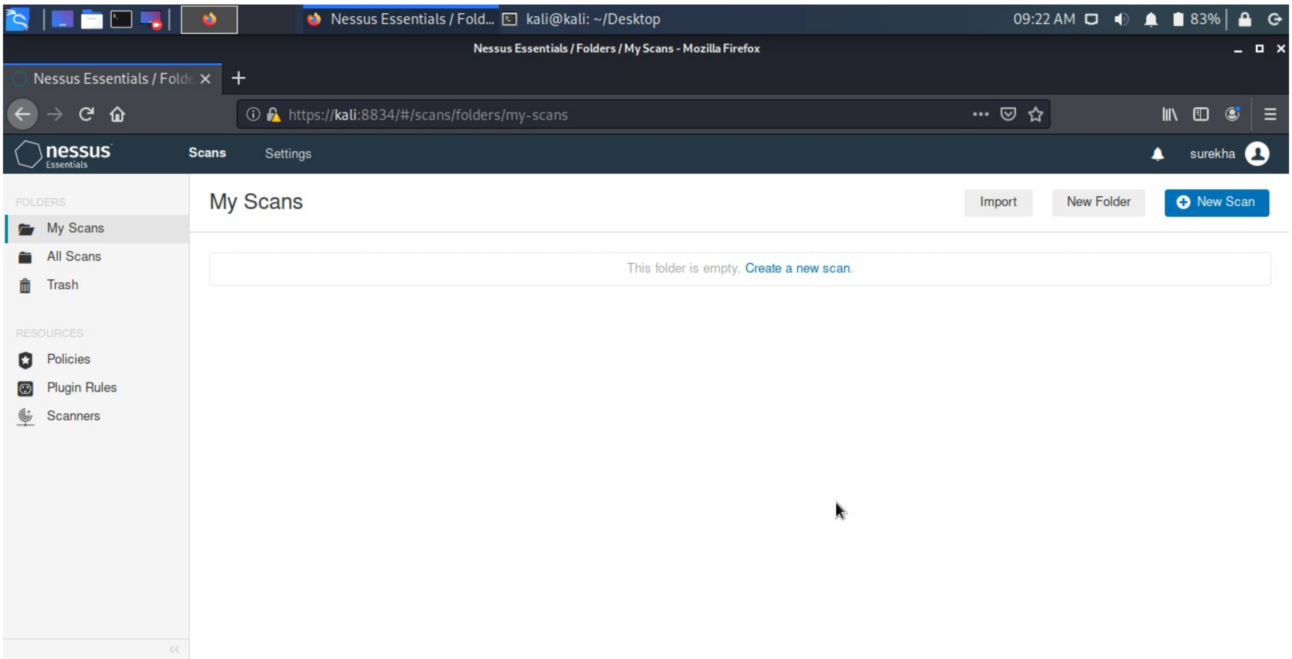
open browser and type https://kali:8834/

there you should enter your activation code

then you can set your username and password.

Login to you account with your details.

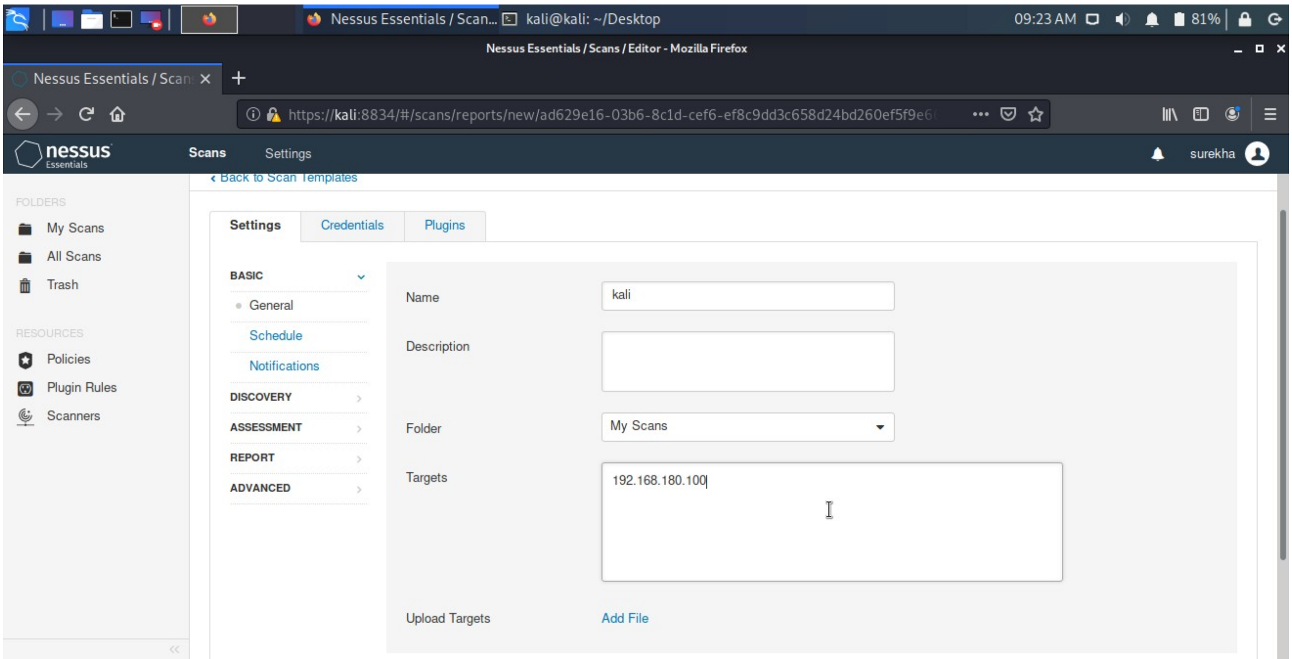




My Scans

This folder is empty. Create a new scan.

Click on new scan
type the name and target ip address



Name: kali

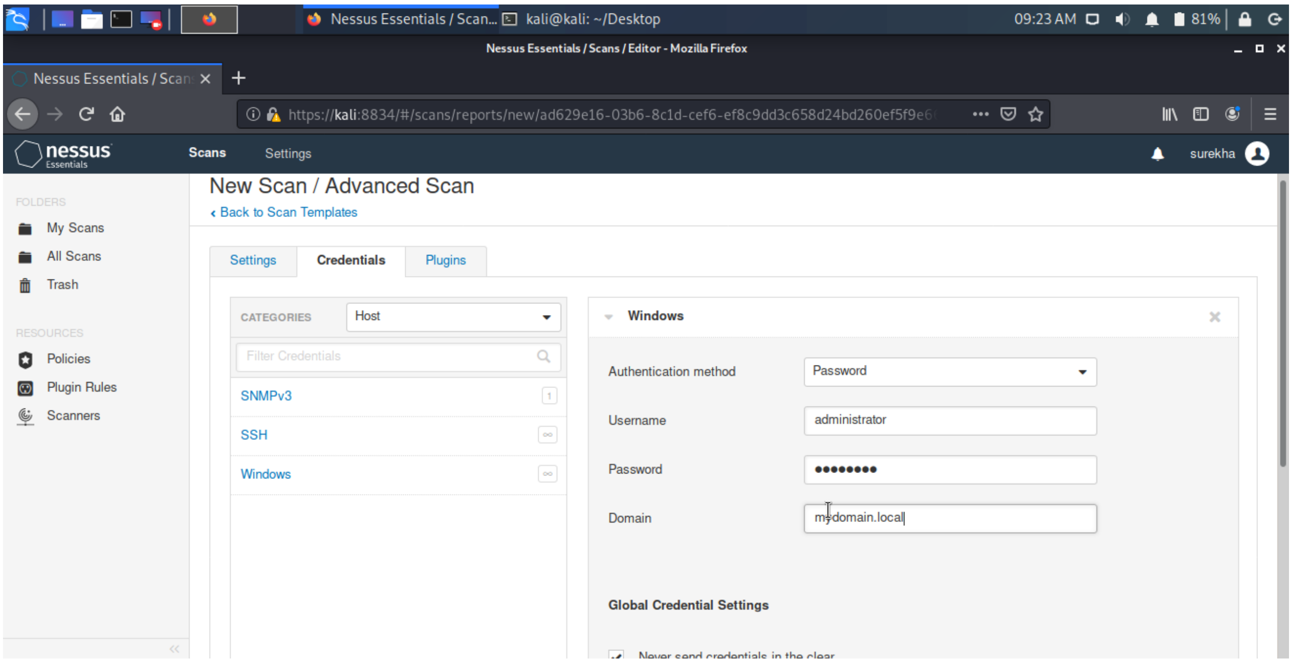
Description:

Folder: My Scans

Targets: 192.168.180.100

Upload Targets: Add File

go to credential and give the details



New Scan / Advanced Scan

‹ Back to Scan Templates

CATEGORIES: Host

Windows

Authentication method: Password

Username: administrator

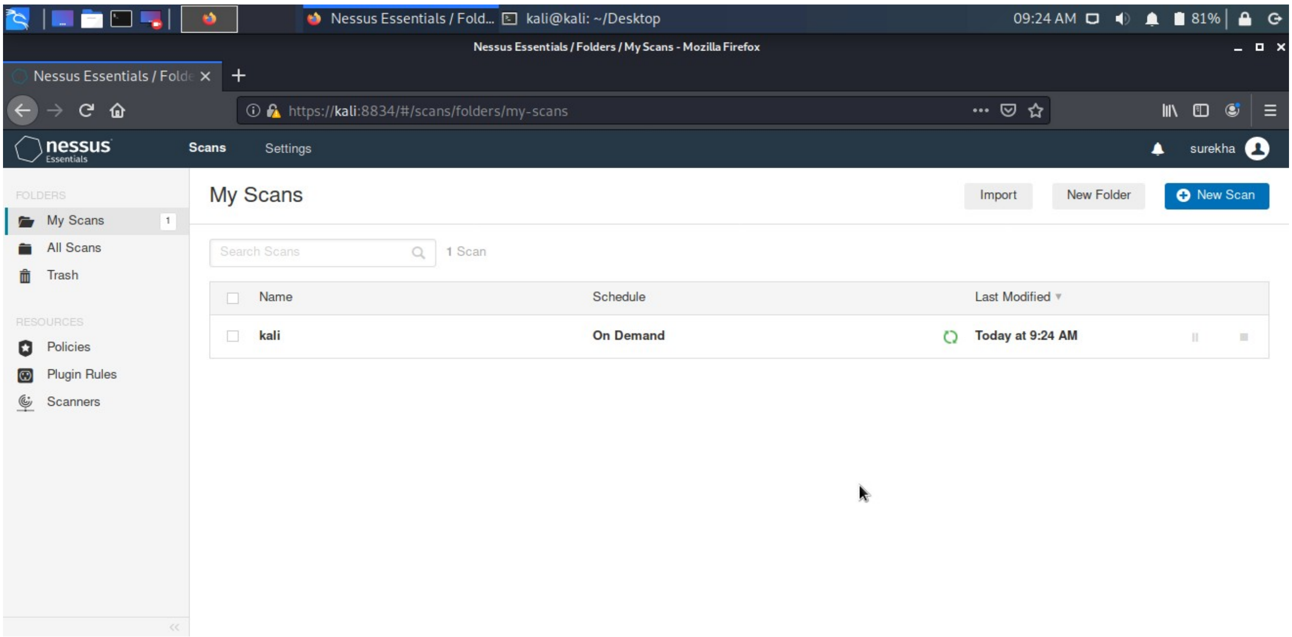
Password: ••••••••

Domain: mydomain.local

Global Credential Settings

☑ Never send credentials in the clear

save the state and launch it.
It will take some time to run and will give the results.



My Scans

1 Scan

	Name	Schedule	Last Modified
□	kali	On Demand	Today at 9:24 AM