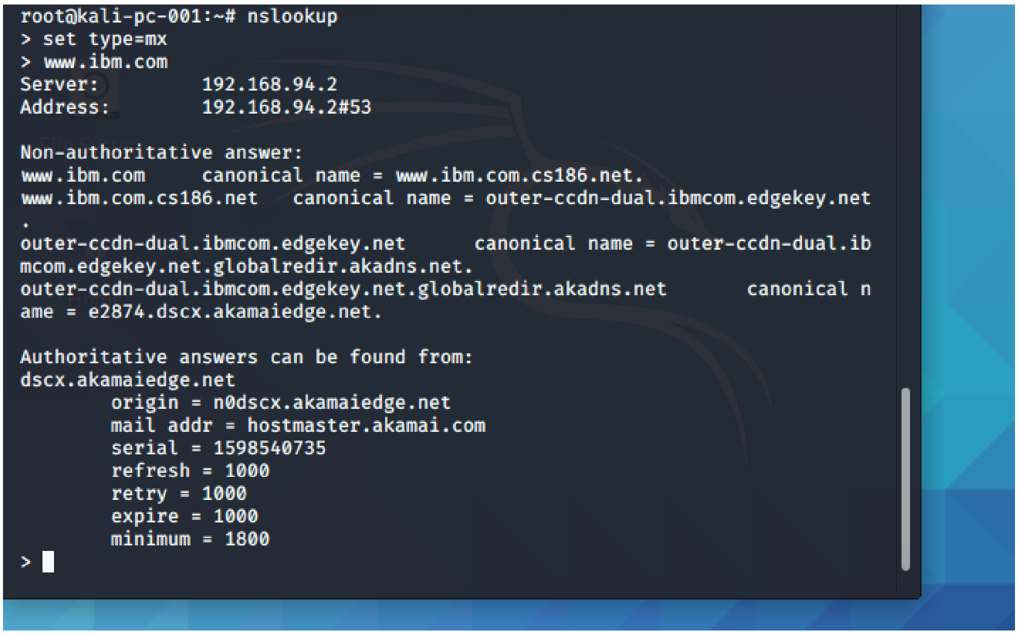
1. Find out the mail servers of the following domain :

i. Ibm.com

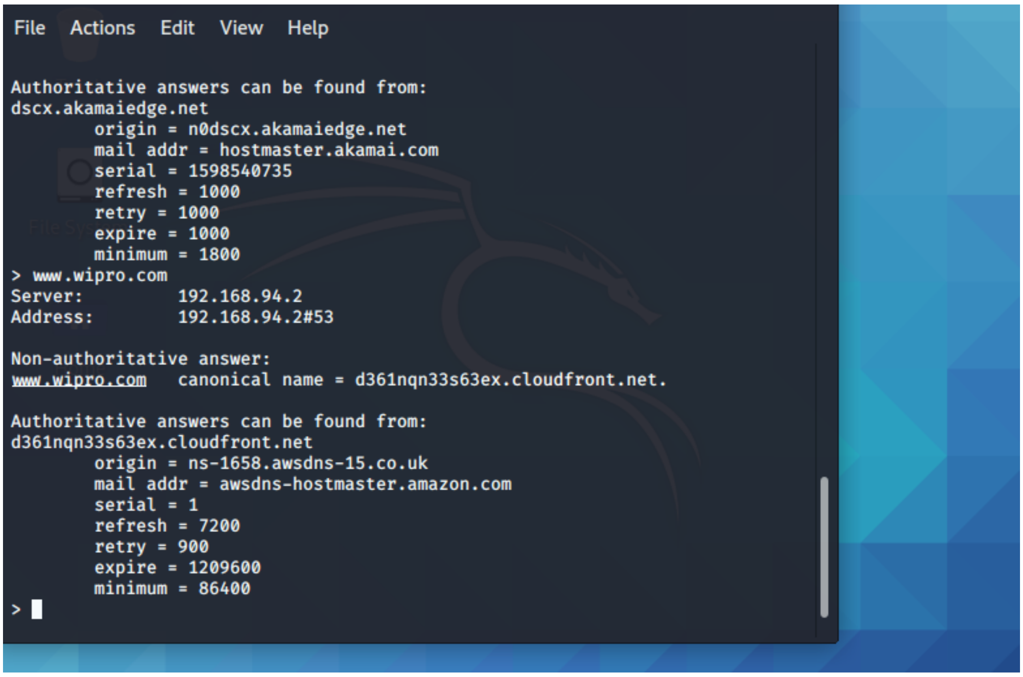


```
root@kali-pc-001:~# nslookup
> set type=mx
> www.ibm.com
Server:         192.168.94.2
Address:        192.168.94.2#53

Non-authoritative answer:
www.ibm.com     canonical name = www.ibm.com.cs186.net.
www.ibm.com.cs186.net   canonical name = outer-ccdn-dual.ibmcom.edgekey.net
.
outer-ccdn-dual.ibmcom.edgekey.net      canonical name = outer-ccdn-dual.ib
mcom.edgekey.net.globalredir.akadns.net.
outer-ccdn-dual.ibmcom.edgekey.net.globalredir.akadns.net       canonical n
ame = e2874.dscx.akamaiedge.net.

Authoritative answers can be found from:
dscx.akamaiedge.net
        origin = n0dscx.akamaiedge.net
        mail addr = hostmaster.akamai.com
        serial = 1598540735
        refresh = 1000
        retry = 1000
        expire = 1000
        minimum = 1800
> 
```

ii. Wipro.com



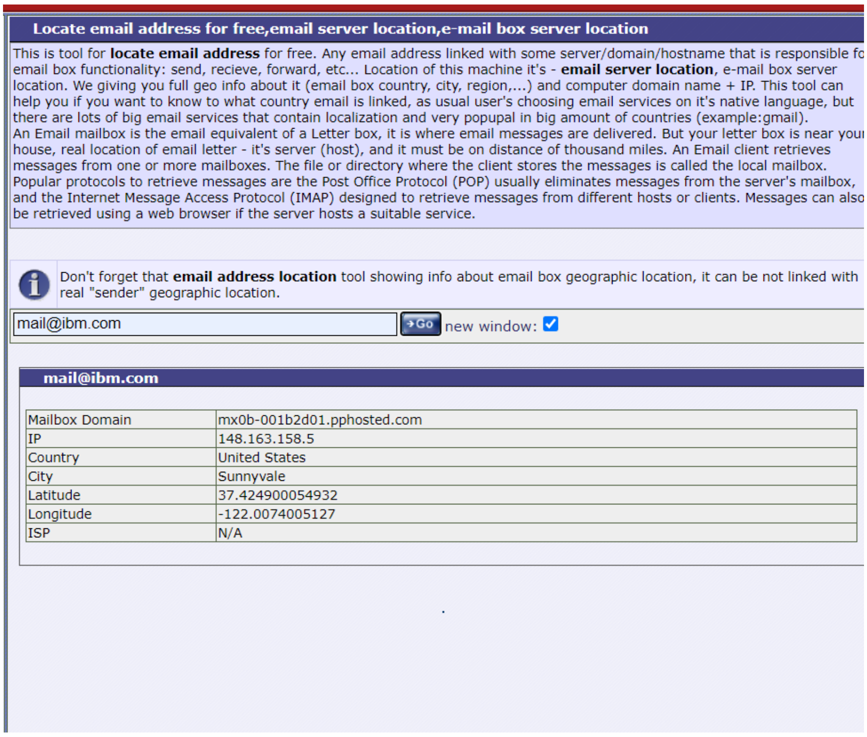
```
Authoritative answers can be found from:
dscx.akamaiedge.net
        origin = n0dscx.akamaiedge.net
        mail addr = hostmaster.akamai.com
        serial = 1598540735
        refresh = 1000
        retry = 1000
        expire = 1000
        minimum = 1800
> www.wipro.com
Server:         192.168.94.2
Address:        192.168.94.2#53

Non-authoritative answer:
www.wipro.com   canonical name = d361nqn33s63ex.cloudfront.net.

Authoritative answers can be found from:
d361nqn33s63ex.cloudfront.net
        origin = ns-1658.awsdns-15.co.uk
        mail addr = awsdns-hostmaster.amazon.com
        serial = 1
        refresh = 7200
        retry = 900
        expire = 1209600
        minimum = 86400
> 
```

2. Find the locations, where these email servers are hosted:

i. ibm.com



Locate email address for free,email server location,e-mail box server location

This is tool for **locate email address** for free. Any email address linked with some server/domain/hostname that is responsible fo email box functionality: send, recieve, forward, etc... Location of this machine it's - **email server location**, e-mail box server location. We giving you full geo info about it (email box country, city, region,...) and computer domain name + IP. This tool can help you if you want to know to what country email is linked, as usual user's choosing email services on it's native language, but there are lots of big email services that contain localization and very popupal in big amount of countries (example:gmail).
An Email mailbox is the email equivalent of a Letter box, it is where email messages are delivered. But your letter box is near you house, real location of email letter - it's server (host), and it must be on distance of thousand miles. An Email client retrieves messages from one or more mailboxes. The file or directory where the client stores the messages is called the local mailbox. Popular protocols to retrieve messages are the Post Office Protocol (POP) usually eliminates messages from the server's mailbox, and the Internet Message Access Protocol (IMAP) designed to retrieve messages from different hosts or clients. Messages can also be retrieved using a web browser if the server hosts a suitable service.

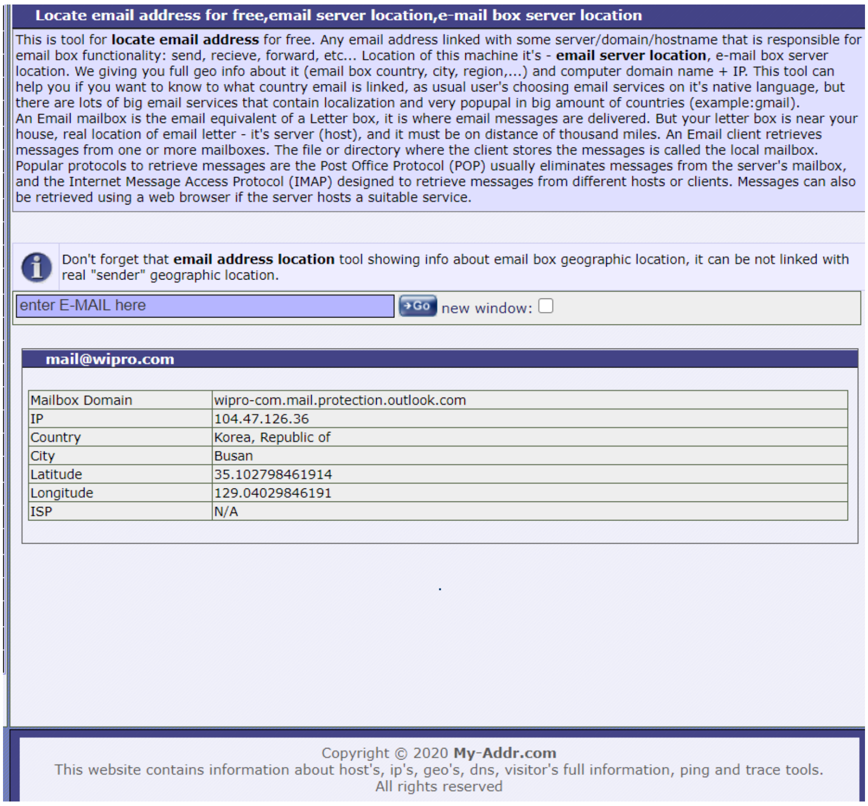
Don't forget that **email address location** tool showing info about email box geographic location, it can be not linked with real "sender" geographic location.

mail@ibm.com Go new window: ☑

mail@ibm.com

Mailbox Domain	mx0b-001b2d01.pphosted.com
IP	148.163.158.5
Country	United States
City	Sunnyvale
Latitude	37.424900054932
Longitude	-122.0074005127
ISP	N/A

ii. wipro.com



Locate email address for free,email server location,e-mail box server location

This is tool for **locate email address** for free. Any email address linked with some server/domain/hostname that is responsible for email box functionality: send, recieve, forward, etc... Location of this machine it's - **email server location**, e-mail box server location. We giving you full geo info about it (email box country, city, region,...) and computer domain name + IP. This tool can help you if you want to know to what country email is linked, as usual user's choosing email services on it's native language, but there are lots of big email services that contain localization and very popupal in big amount of countries (example:gmail).
An Email mailbox is the email equivalent of a Letter box, it is where email messages are delivered. But your letter box is near your house, real location of email letter - it's server (host), and it must be on distance of thousand miles. An Email client retrieves messages from one or more mailboxes. The file or directory where the client stores the messages is called the local mailbox. Popular protocols to retrieve messages are the Post Office Protocol (POP) usually eliminates messages from the server's mailbox, and the Internet Message Access Protocol (IMAP) designed to retrieve messages from different hosts or clients. Messages can also be retrieved using a web browser if the server hosts a suitable service.

Don't forget that **email address location** tool showing info about email box geographic location, it can be not linked with real "sender" geographic location.

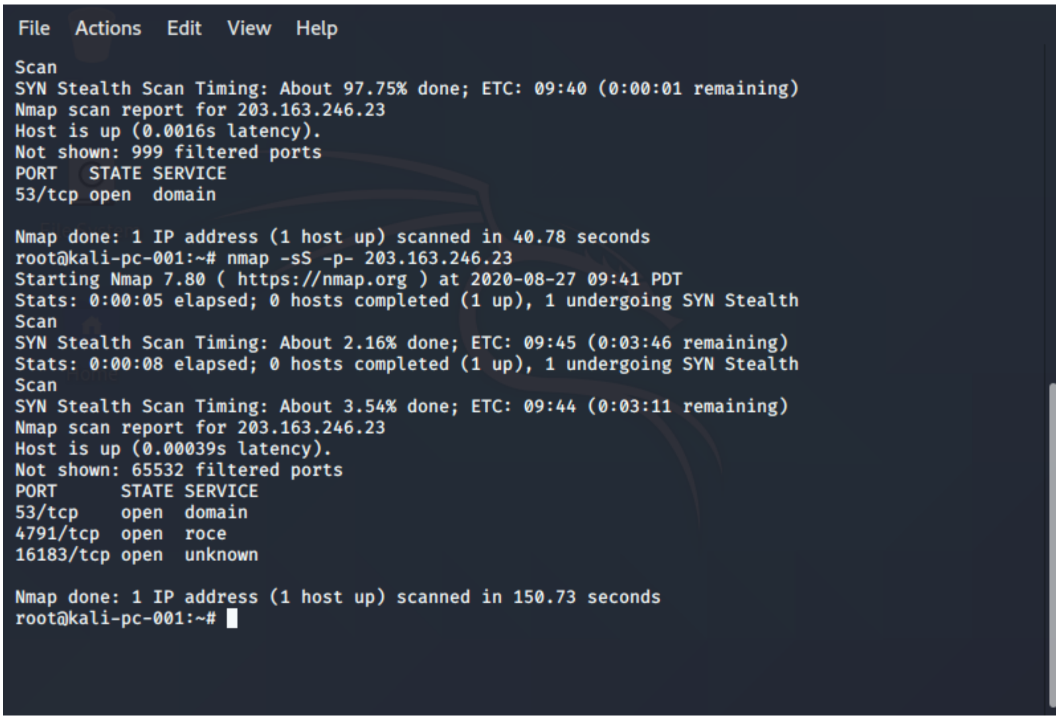
enter E-MAIL here Go new window: □

mail@wipro.com

Mailbox Domain	wipro-com.mail.protection.outlook.com
IP	104.47.126.36
Country	Korea, Republic of
City	Busan
Latitude	35.102798461914
Longitude	129.04029846191
ISP	N/A

Copyright © 2020 **My-Addr.com**
This website contains information about host's, ip's, geo's, dns, visitor's full information, ping and trace tools.
All rights reserved

3. Scan and find out port numbers open 203.163.246.23

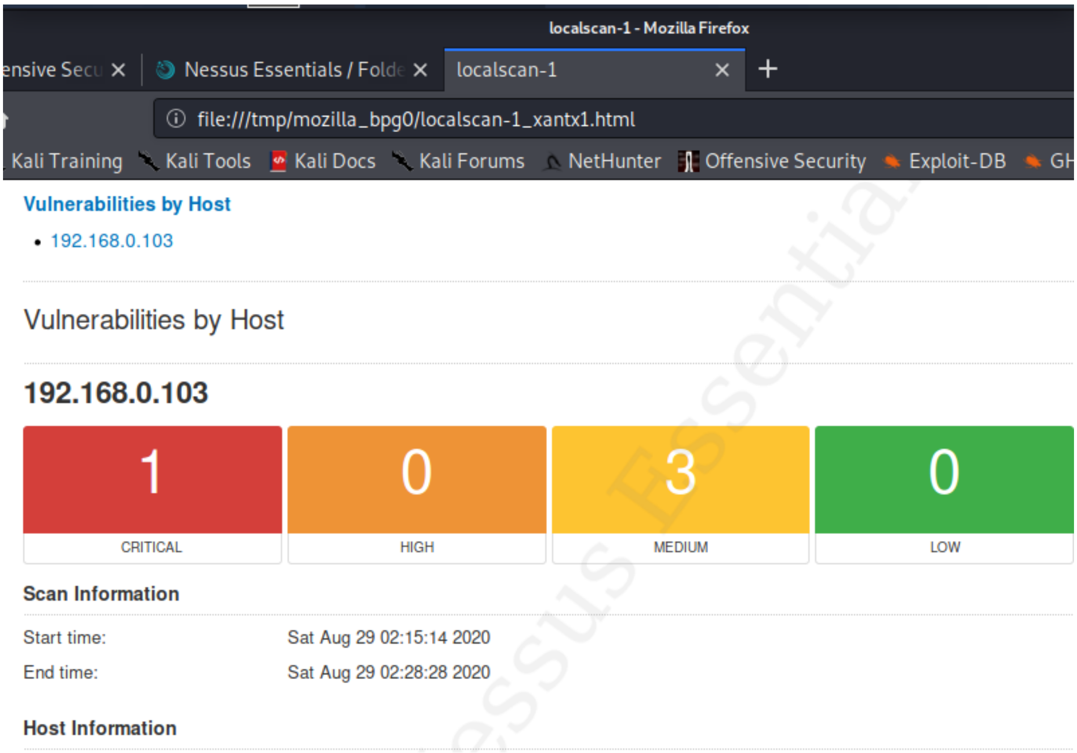


```
Scan
SYN Stealth Scan Timing: About 97.75% done; ETC: 09:40 (0:00:01 remaining)
Nmap scan report for 203.163.246.23
Host is up (0.0016s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 40.78 seconds
root@kali-pc-001:~# nmap -sS -p- 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-27 09:41 PDT
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
Scan
SYN Stealth Scan Timing: About 2.16% done; ETC: 09:45 (0:03:46 remaining)
Stats: 0:00:08 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
Scan
SYN Stealth Scan Timing: About 3.54% done; ETC: 09:44 (0:03:11 remaining)
Nmap scan report for 203.163.246.23
Host is up (0.00039s latency).
Not shown: 65532 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
4791/tcp  open  roce
16183/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 150.73 seconds
root@kali-pc-001:~# 
```

4. Install nessus in a VM and scan your laptop/desktop for CVE



Vulnerabilities by Host

- 192.168.0.103

Vulnerabilities by Host

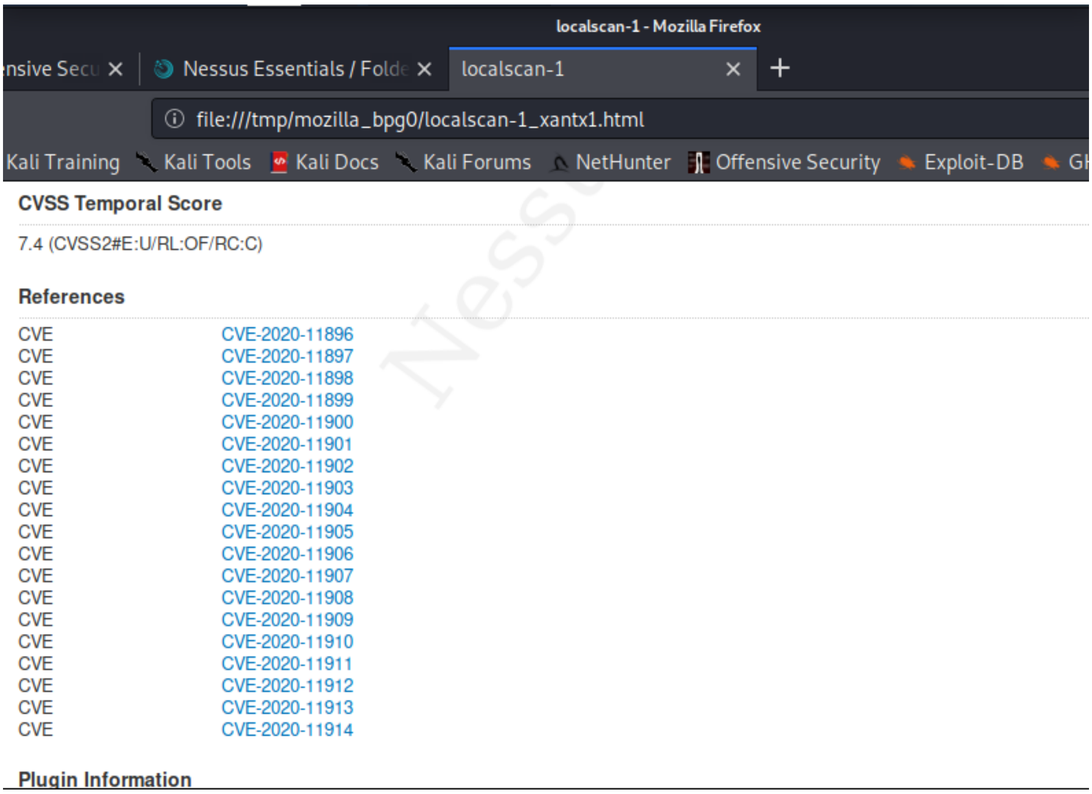
192.168.0.103

1	0	3	0
CRITICAL	HIGH	MEDIUM	LOW

Scan Information

Start time:	Sat Aug 29 02:15:14 2020
End time:	Sat Aug 29 02:28:28 2020

Host Information



CVSS Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2020-11896
CVE	CVE-2020-11897
CVE	CVE-2020-11898
CVE	CVE-2020-11899
CVE	CVE-2020-11900
CVE	CVE-2020-11901
CVE	CVE-2020-11902
CVE	CVE-2020-11903
CVE	CVE-2020-11904
CVE	CVE-2020-11905
CVE	CVE-2020-11906
CVE	CVE-2020-11907
CVE	CVE-2020-11908
CVE	CVE-2020-11909
CVE	CVE-2020-11910
CVE	CVE-2020-11911
CVE	CVE-2020-11912
CVE	CVE-2020-11913
CVE	CVE-2020-11914

Plugin Information