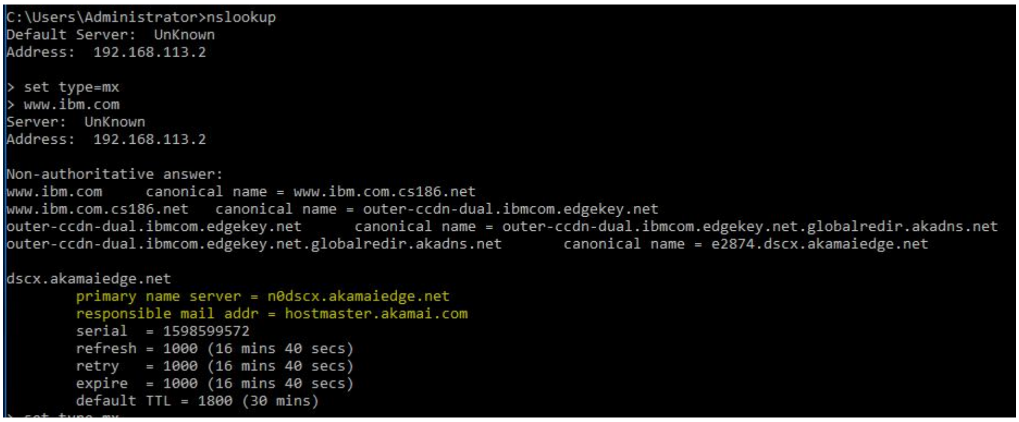
LETSUPGRADE - CYBERSECURITY ESSENTIALS ASSIGNMENT DAY 4

Question 1:

Find out the mail servers of the following domain :
Ibm.com
Wipro.com

Solution:

Open Win2016, Open cmd, Type nslookup
Then set type=mx
And then type the website. This will lookup on those websites for their mail servers.



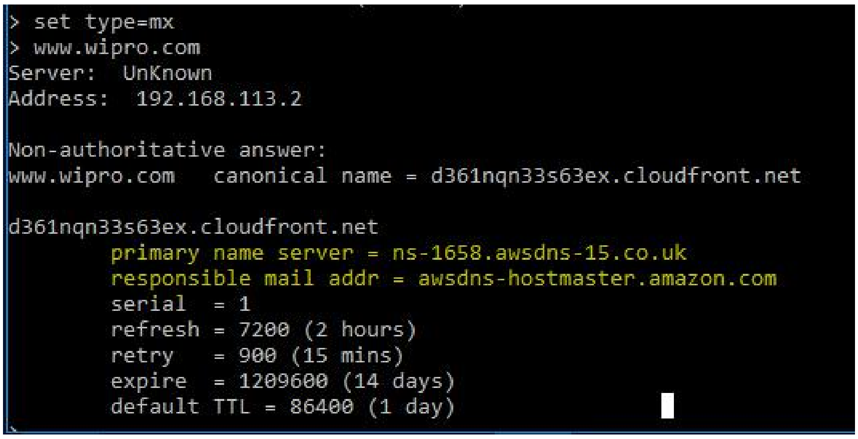
```
C:\Users\Administrator>nslookup
Default Server:  UnKnown
Address:  192.168.113.2

> set type=mx
> www.ibm.com
Server:  UnKnown
Address:  192.168.113.2

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.ibmcom.edgekey.net.globalredir.akadns.net
outer-ccdn-dual.ibmcom.edgekey.net.globalredir.akadns.net       canonical name = e2874.dscx.akamaiedge.net

dscx.akamaiedge.net
        primary name server = n0dscx.akamaiedge.net
        responsible mail addr = hostmaster.akamai.com
        serial  = 1598599572
        refresh = 1000 (16 mins 40 secs)
        retry   = 1000 (16 mins 40 secs)
        expire  = 1000 (16 mins 40 secs)
        default TTL = 1800 (30 mins)
```

When I searched for www.ibm.com, its gave n0dscx.akamaiedge.net



```
> set type=mx
> www.wipro.com
Server:  UnKnown
Address:  192.168.113.2

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

d361nqn33s63ex.cloudfront.net
        primary name server = ns-1658.awsdns-15.co.uk
        responsible mail addr = awsdns-hostmaster.amazon.com
        serial  = 1
        refresh = 7200 (2 hours)
        retry   = 900 (15 mins)
        expire  = 1209600 (14 days)
        default TTL = 86400 (1 day)
```

When I searched for www.wipro.com, it gave ns-1658.awsdns-15.co.uk

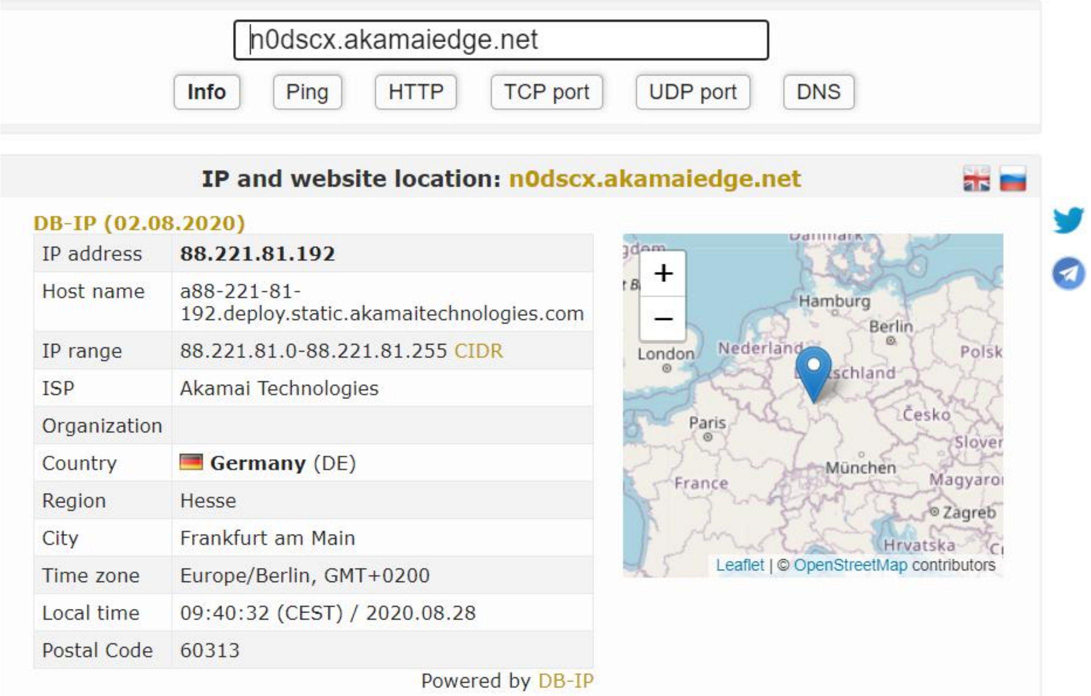
Question 2:

Find the locations, where these email servers are hosted.

Solution:

Head over to https://check-host.net/ip-info?host= to get the location of those domains.

When I typed n0dscx.akamaiedge.net, I got its location as Frankfurt, Germany.



n0dscx.akamaiedge.net

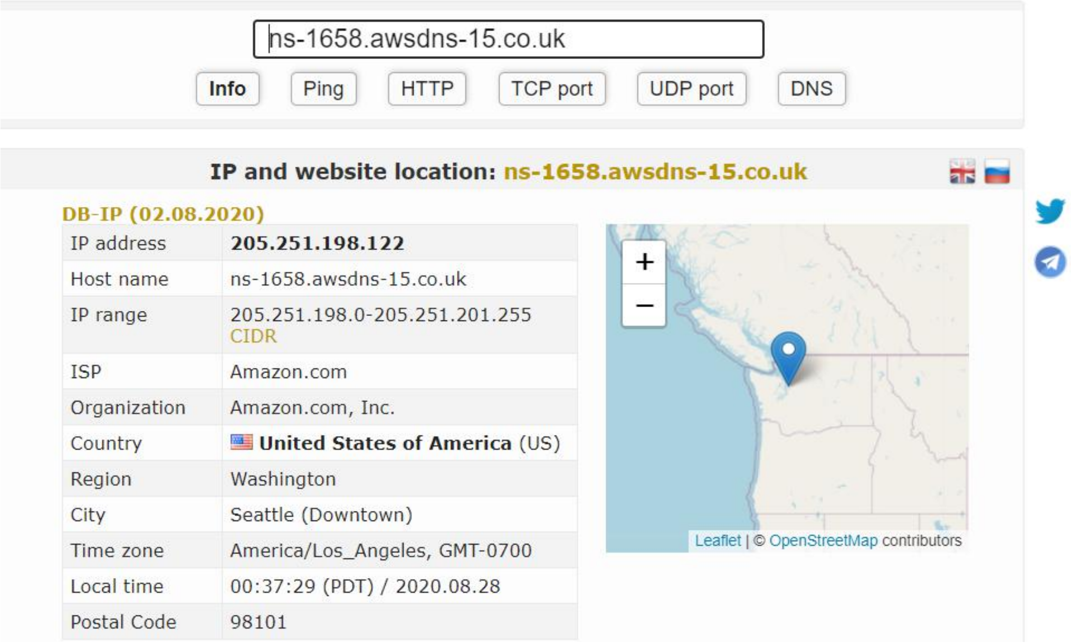
IP and website location: n0dscx.akamaiedge.net

DB-IP (02.08.2020)

IP address	**88.221.81.192**
Host name	a88-221-81-192.deploy.static.akamaitechnologies.com
IP range	88.221.81.0-88.221.81.255 CIDR
ISP	Akamai Technologies
Organization	
Country	**Germany** (DE)
Region	Hesse
City	Frankfurt am Main
Time zone	Europe/Berlin, GMT+0200
Local time	09:40:32 (CEST) / 2020.08.28
Postal Code	60313

Powered by DB-IP

And when I typed ns-1658.awsdns-15.co.uk, I got the location as Seattle, United States.



ns-1658.awsdns-15.co.uk

IP and website location: ns-1658.awsdns-15.co.uk

DB-IP (02.08.2020)

IP address	**205.251.198.122**
Host name	ns-1658.awsdns-15.co.uk
IP range	205.251.198.0-205.251.201.255 CIDR
ISP	Amazon.com
Organization	Amazon.com, Inc.
Country	**United States of America** (US)
Region	Washington
City	Seattle (Downtown)
Time zone	America/Los_Angeles, GMT-0700
Local time	00:37:29 (PDT) / 2020.08.28
Postal Code	98101

Question 3:

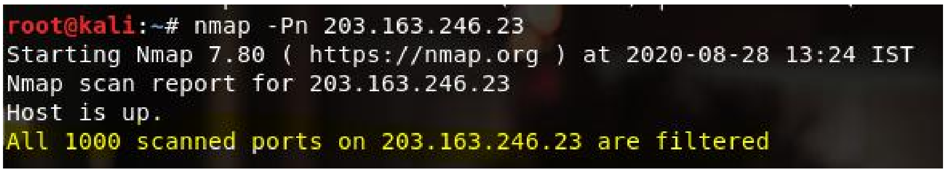
Scan and find out port numbers open 203.163.246.23

Solution:

Open kali in VM, because we need to use nmap to scan open ports.

Open terminal

Type nmap -Pn 203.163.246.23



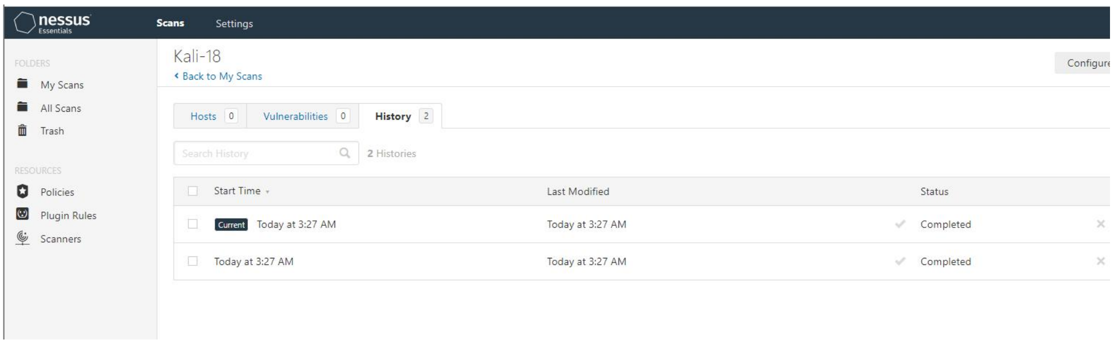
```
root@kali:~# nmap -Pn 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-28 13:24 IST
Nmap scan report for 203.163.246.23
Host is up.
All 1000 scanned ports on 203.163.246.23 are filtered
```

-Pn is a command to scan ports behind firewalls or that are protected by firewalls.

When we run the command we see there were 1000 scanned ports and are filtered. That means are the port are protected by firewall.
I even used the command, nmap -Pn -sS -A -v 203.163.246.23 . But there results were same. All 1000 ports are filtered.

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

Solution:
I installed nessus on my Windows server 2016. Then scanned my kali linux. I found 0 Vulnerabilities.



Kali-18

2 Histories

Start Time	Last Modified	Status
Current Today at 3:27 AM	Today at 3:27 AM	✓ Completed
Today at 3:27 AM	Today at 3:27 AM	✓ Completed