

# Assignment Day 4 | 23rd August 2020

## Question 1:

Find out the mail servers of the following domain:

1) [www.lbm.com](http://www.lbm.com)

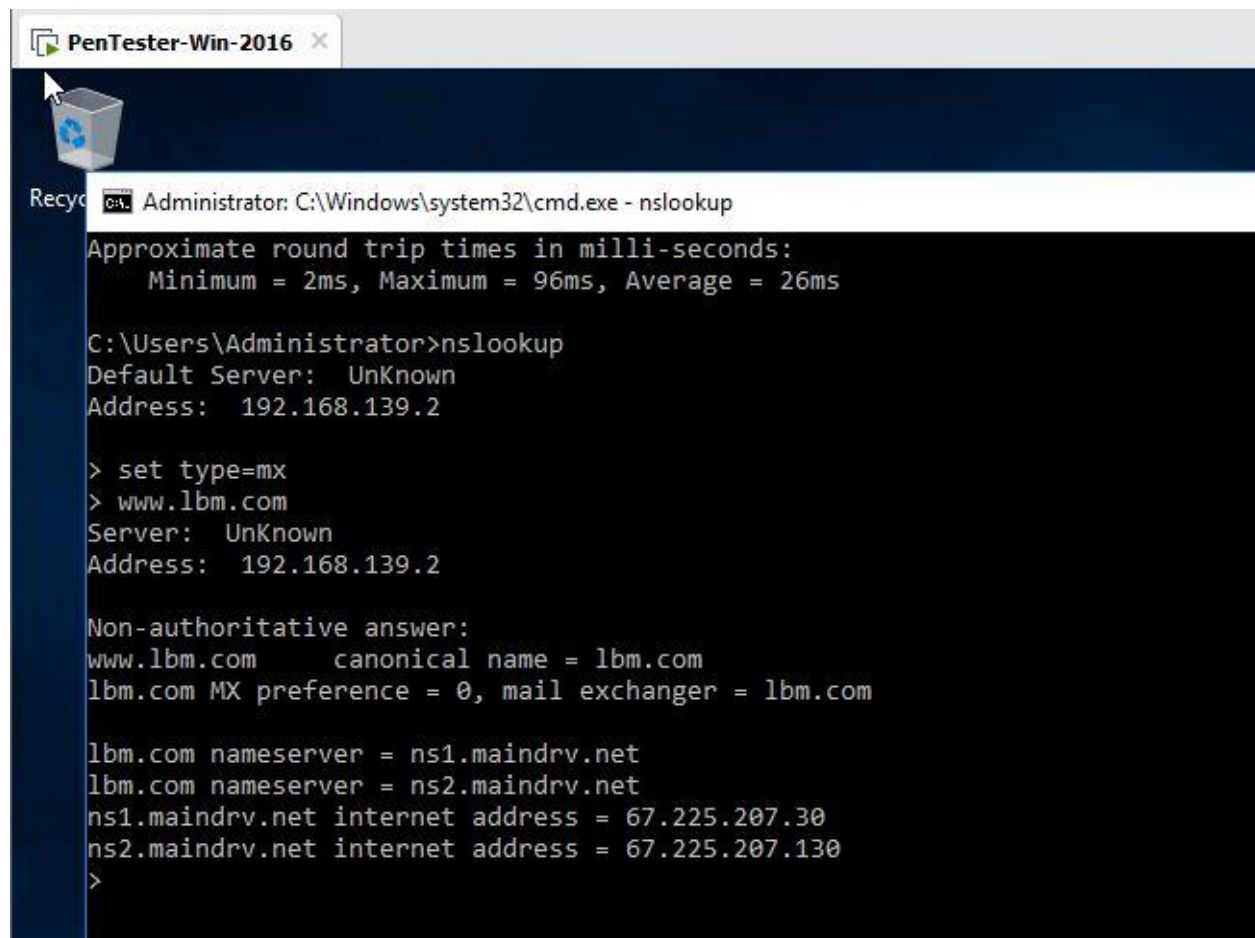
Open Command Prompt in Penchester

And type:

nslookup

set type=mx

www.lbm.com



```
PenTester-Win-2016 x
Recycle Bin
C:\Windows\system32\cmd.exe - nslookup
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 96ms, Average = 26ms

C:\Users\Administrator>nslookup
Default Server:  UnKnown
Address:  192.168.139.2

> set type=mx
> www.lbm.com
Server:  UnKnown
Address:  192.168.139.2

Non-authoritative answer:
www.lbm.com      canonical name = lbm.com
lbm.com MX preference = 0, mail exchanger = lbm.com

lbm.com nameserver = ns1.maindrv.net
lbm.com nameserver = ns2.maindrv.net
ns1.maindrv.net internet address = 67.225.207.30
ns2.maindrv.net internet address = 67.225.207.130
>
```

2) [www.wipro.com](http://www.wipro.com)

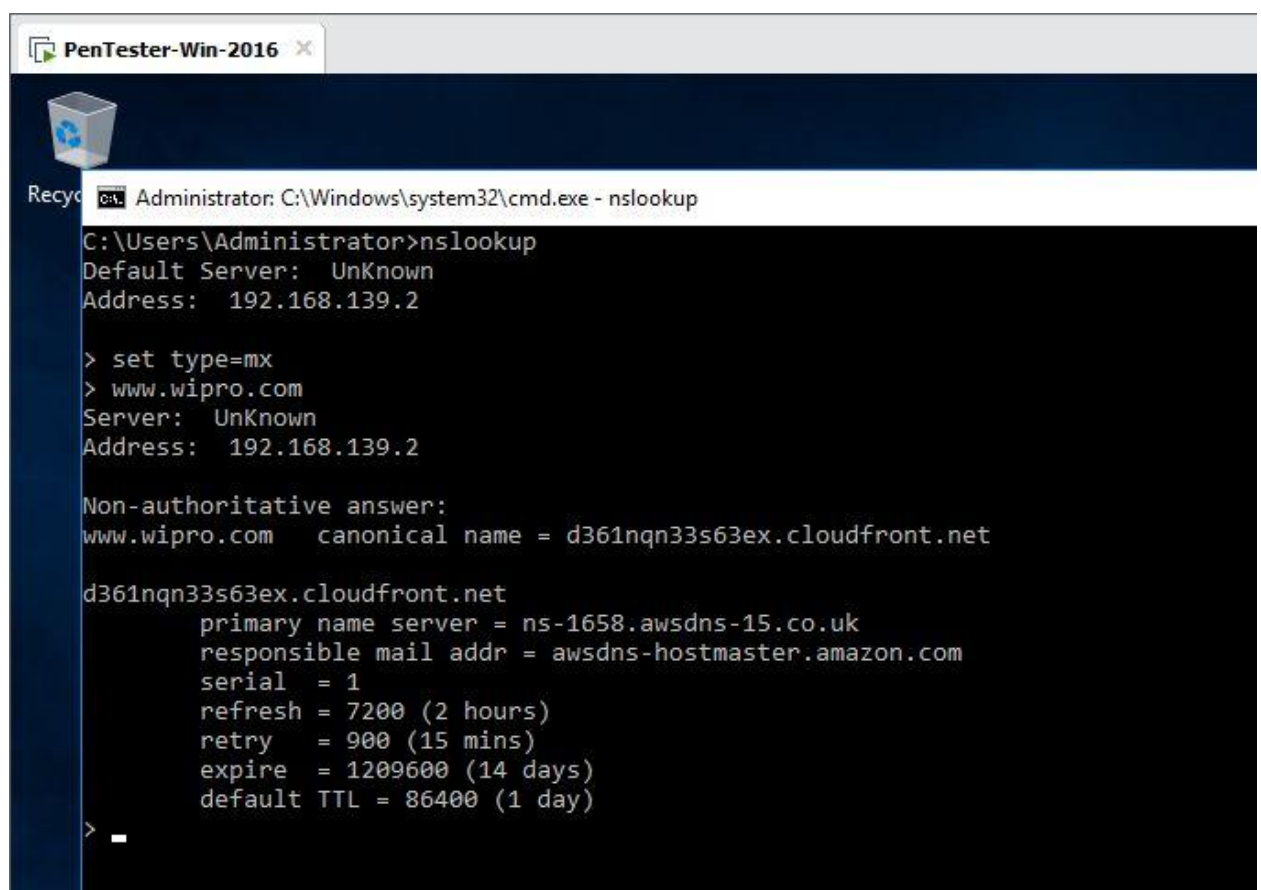
Open Command Prompt in Penchester

And type:

nslookup

set type=mx

www.wipro.com



```
PenTester-Win-2016
Recycle Bin
Administrator: C:\Windows\system32\cmd.exe - nslookup
C:\Users\Administrator>nslookup
Default Server: UnKnown
Address: 192.168.139.2

> set type=mx
> www.wipro.com
Server: UnKnown
Address: 192.168.139.2

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)
> _
```

## Question 2:

Find the locations, where these email servers are hosted.

Download Emailtrackerpro from google chrome in penchester  
copy the clipboard of email and paste in dialog box of trace header and click tracer

Home digest-noreply@quora.com X

The trace is complete, the information found is displayed on the right

New TraceView Report

Map




Table #	Hop IP	Hop Name	Location
1	192.168.139.2		
2	192.168.0.1		
3	10.0.0.1		
5	114.79.130.1	114.79.130.1.dvois.com	India
6	72.14.208.165		Mountain View, California, USA
7	209.85.241.175		USA
8	108.170.248.195		Mountain View, California, USA
9	108.170.229.13		Mountain View, California, USA
10	216.239.63.96		Mountain View, California, USA

Identification Report for 173.194.70.27

You are on day 1 of your 15-day trial period. The trial period allows you to try eMailTrackerPro without any obligation. To use eMailTrackerPro after the trial period, you will need to [purchase a product license](#) from the Visualware website or authorized reseller.

Emails from 173.194.70.27 are passed to the server identified on the Internet by **173.194.70.27**. This report details that server, which is probably owned or maintained by the sender's company or Internet service provider. If you would like information on the computer on which the email was actually composed, then use eMailTrackerPro's Advanced Email Trace facility).

Note that email addresses are very easy to fake. If you have received a spam or scam email pertaining to be from **173.194.70.27**, then it almost certainly does **not** come from that address. You can find the real source of the email using the Advanced Email Trace facility.

Computer **173.194.70.27** has been found. It is almost certainly located in **Portage, Wisconsin, USA** as it has an exact match in the eMailTrackerPro database.

This system is a mail server (click [here](#) for details).

**Network Contact Information:** The following details refer to the network that the system is on.

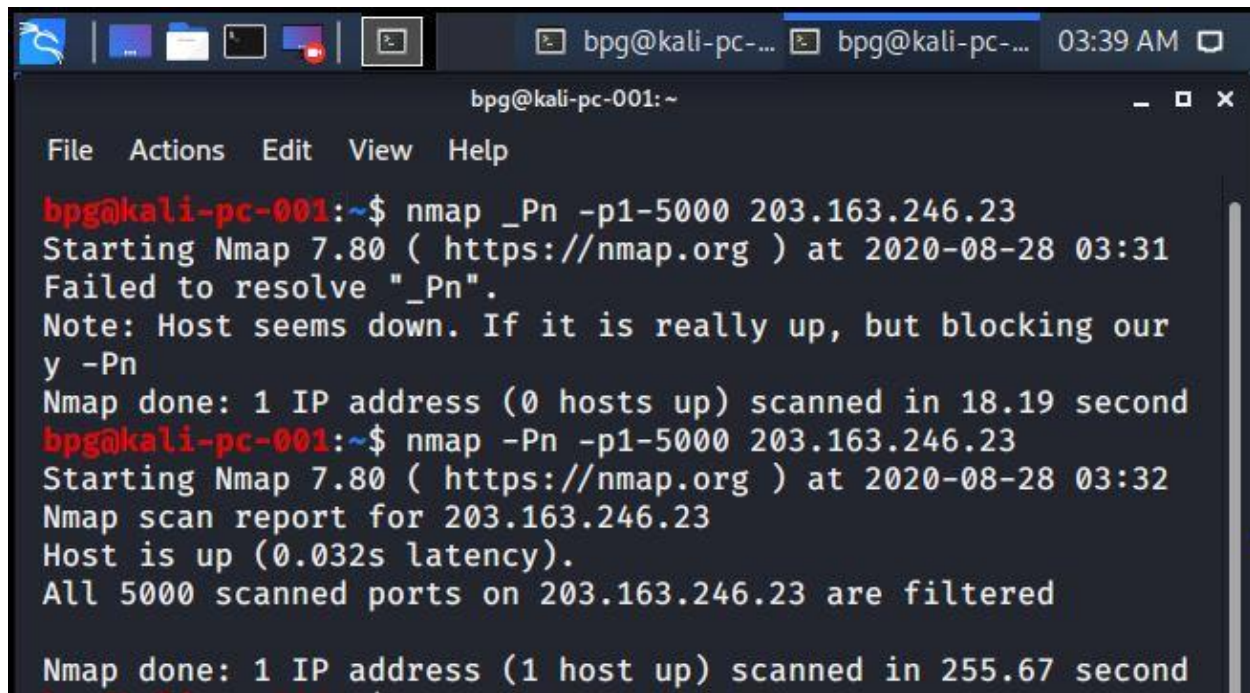
### Question 3:

Scan and find out port numbers open 203.163.246.23

Open terminal in Kali

Type Following code:

```
nmap -Pn -p1-65535 203.163.246.23
```



```
bpg@kali-pc-001: ~  
File Actions Edit View Help  
bpg@kali-pc-001:~$ nmap -Pn -p1-5000 203.163.246.23  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-28 03:31  
Failed to resolve "_Pn".  
Note: Host seems down. If it is really up, but blocking our  
y -Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 18.19 second  
bpg@kali-pc-001:~$ nmap -Pn -p1-5000 203.163.246.23  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-28 03:32  
Nmap scan report for 203.163.246.23  
Host is up (0.032s latency).  
All 5000 scanned ports on 203.163.246.23 are filtered  
  
Nmap done: 1 IP address (1 host up) scanned in 255.67 second
```

#### Question 4:

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

Download nessus from google chrome. Open Domain controller and power on it.

Open Command prompt in kali

type following command:

ipconfig

open terminal in kali

type following command:

ip a

sudo su -

nmap -Pn sS -A -v 192.168.103.129

Open prompt in Penchester command

type following command:

ping 192.168.103.129

Open Google Chrome In Penchester

localhost:8834

Sign in in the nessus. advanced scan. fill the information click on And launch it

