**Assignment cybersecurity essential**

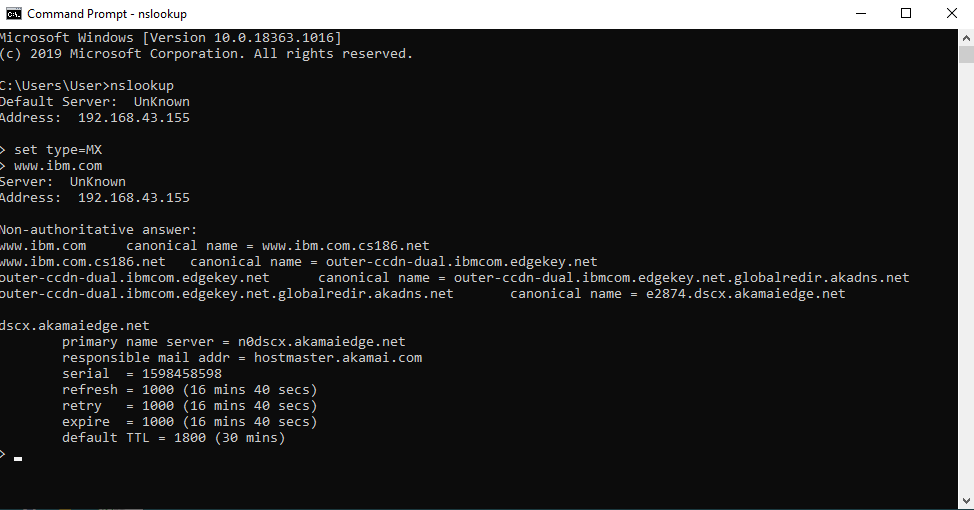
Question1:

Find out the mail servers of following domains:

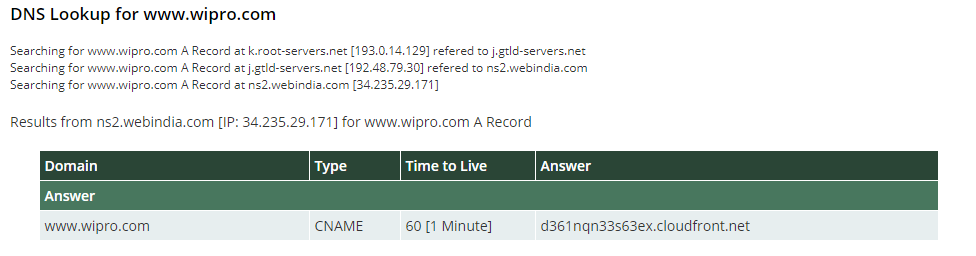
1. Ibm.com
2. Wipro.com

For ibm.com use nslookup and type set=MX

And then enter the particular domain



Similarly wipro also

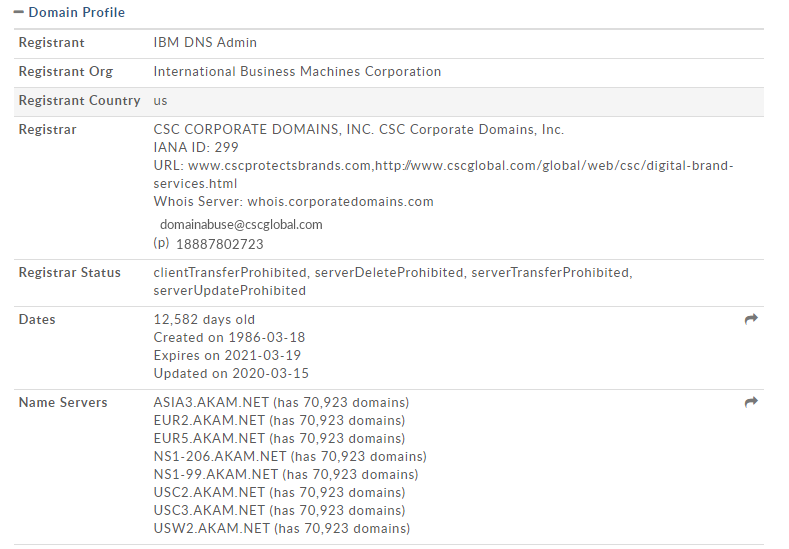


And use resource nslookup.

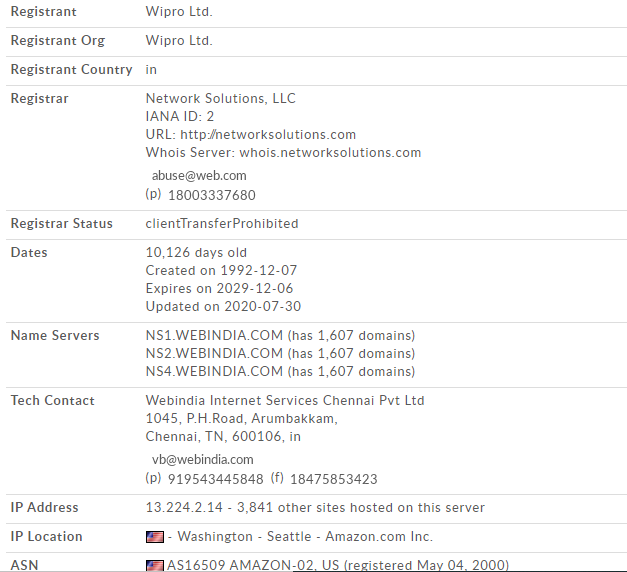
Question2:

Find these location where these email servers hosted: I used domain tool in that did whois lookup

* ibm



* wipro



Question3. Scan and find out port numbers open 203.163.246.23

nmap –Pn 203.163.246.26



Question 4.Install Nessus in your VM and scan our laptop/desktop for CV

nmap -sV --script=vulscan/vulscan.nse 192.168.1.105

Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-24 11:24 -03

Nmap scan report **for** 192.168.1.105 (192.168.1.105)

Host **is** up (0.000061s latency).

Not shown: 999 closed ports

PORT STATE SERVICE VERSION

53/tcp open domain dnsmasq 2.80

| vulscan: VulDB - https://vuldb.com:

| [49778] Thekelleys dnsmasq up to 2.32 tftp.c tftp\_request memory corruption

| [43410] The Kelleys dnsmasq 2.43 Crash denial **of** service

| [43287] Thekelleys dnsmasq 2.25 Crash denial **of** service

| MITRE CVE - https://cve.mitre.org:

| [CVE-2013-0198] Dnsmasq before 2.66test2, **when** used with certain libvirt configurations, replies to queries **from** prohibited interfaces, which allows remote attackers to cause a denial **of** service (traffic amplification) via spoofed TCP based DNS queries. NOTE: **this** vulnerability exists because **of** an incomplete fix **for** CVE-2012-3411.

| [CVE-2012-3411] Dnsmasq before 2.63test1, **when** used with certain libvirt configurations, replies to requests **from** prohibited interfaces, which allows remote attackers to cause a denial **of** service (traffic amplification) via a spoofed DNS query.

| [CVE-2009-2958] The tftp\_request function **in** tftp.c **in** dnsmasq before 2.50, **when** --enable-tftp **is** used, allows remote attackers to cause a denial **of** service (NULL pointer dereference **and** daemon crash) via a TFTP read (aka RRQ) request with a malformed blksize option.

| SecurityFocus - https://www.securityfocus.com/bid/:

| [31017] Dnsmasq DCHP Lease Multiple Remote Denial Of Service Vulnerabilities

| [17662] DNSmasq Broadcast Reply Denial Of Service Vulnerability

| [12897] Dnsmasq Multiple Remote Vulnerabilities

Nmap done: 1 IP address (1 host up) scanned **in** 11.25 seconds

[research@securitytrails.com ~]#