**Let’s Upgrade Assignment 1**

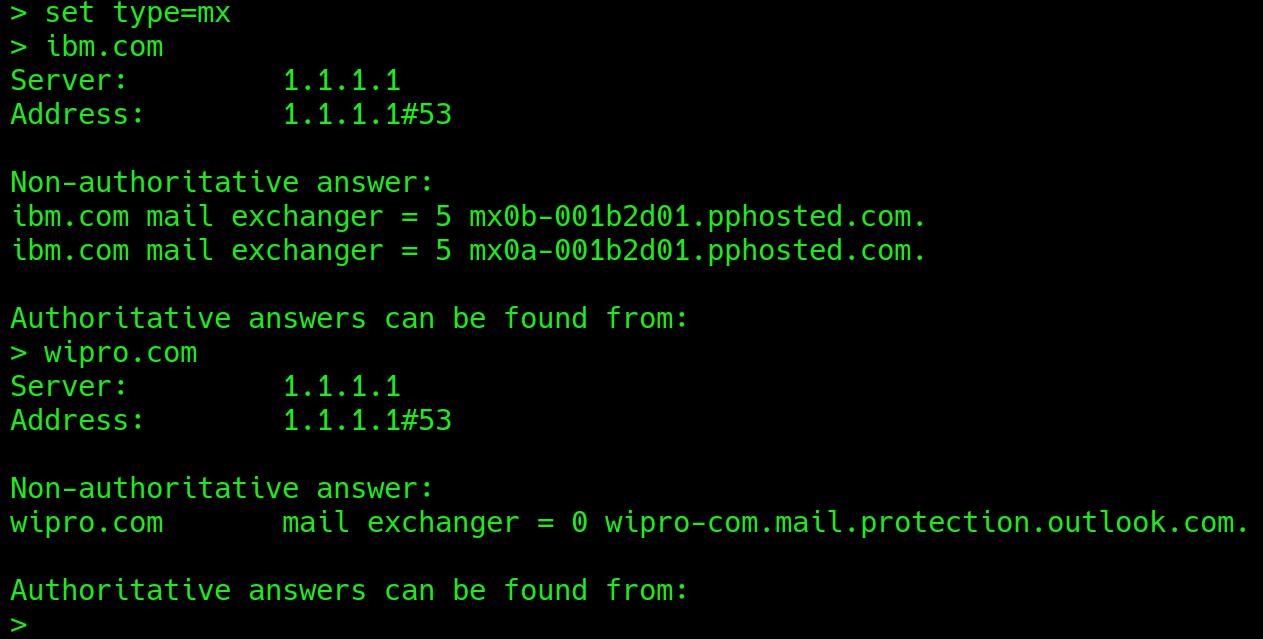
**Name:** Vedant Bhamare

Q1: Find out the mail servers of the following domain:

1. Ibm.com
2. wipro.com

Ans: We can use nslookup to find mail servers in this way:

Type nslookup in terminal, it will initiate a interactive mode, set the search type to mx (mail exchanger) so it can find mail servers of given host and then enter the hostname and there we have our result



Therefore mail servers are:

1. IBM: mx0b-001b2d01.pphosted.com

mx0a-001b2d01.pphosted.com

1. Wipro: wipro-com.mail.protection.outlook.com

Q2: Find the locations, where these email servers are hosted.

Ans: We can answer this question in two ways:

1. Search for the IP of the mail servers we just found in previous question using nslookup



These are the IP:

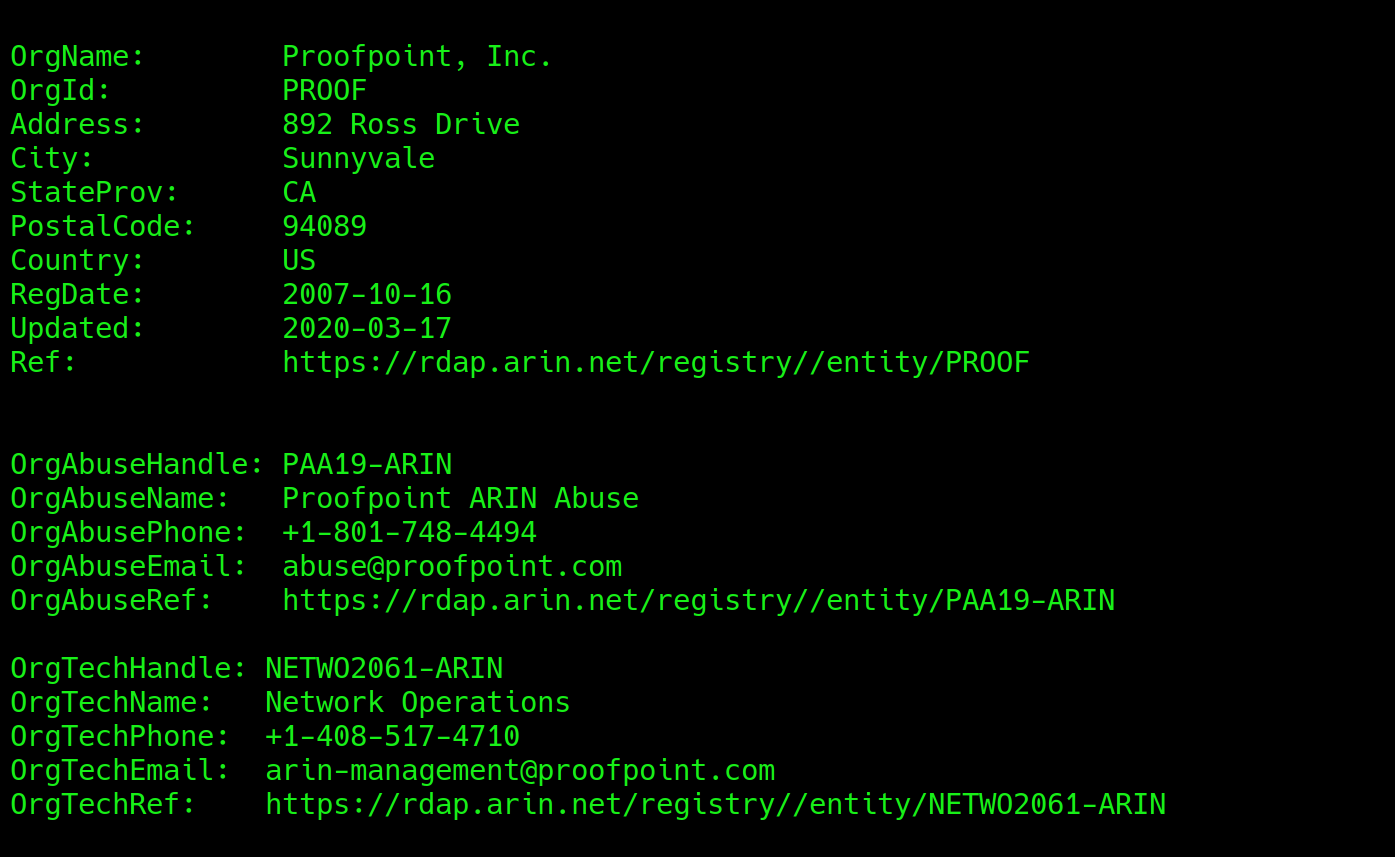
mx0b-001b2d01.pphosted.com: 148.163.158.5

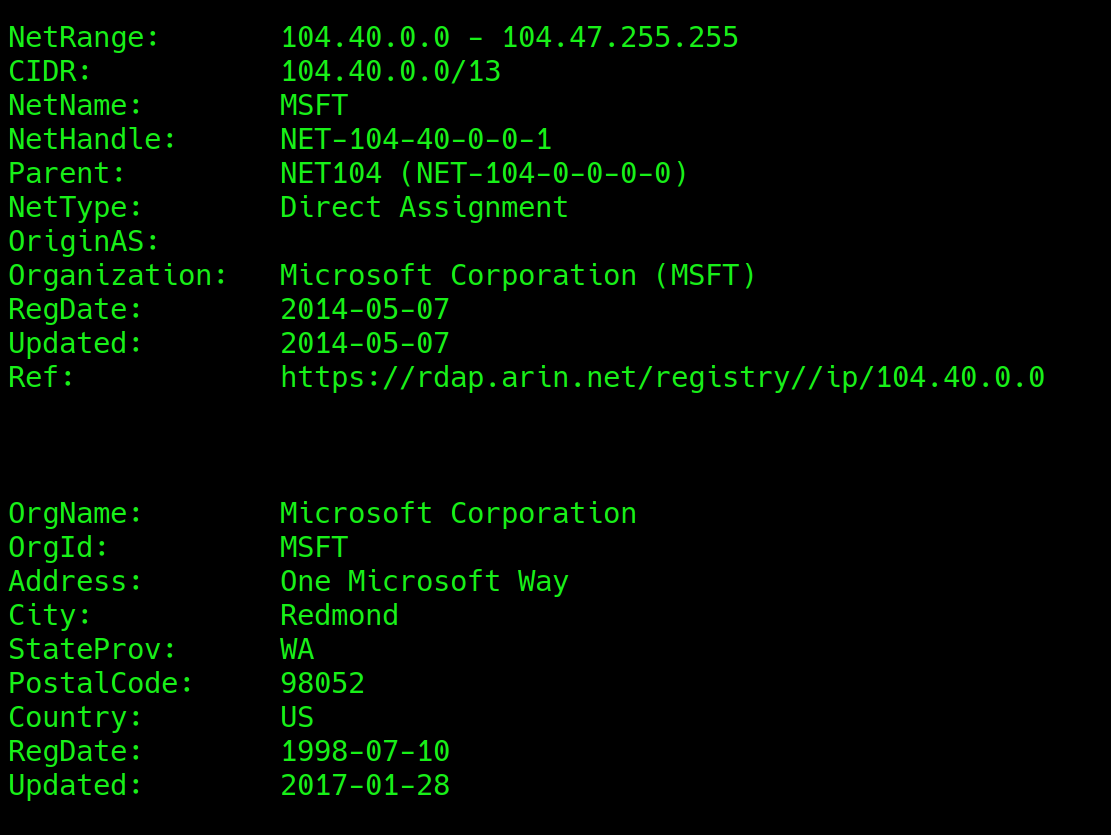
mx0a-001b2d01.pphosted.com: 148.163.156.1

wipro-com.mail.protection.outlook.com: 104.47.126.36

Now search these IP’s in whois database using this command in terminal whois <IP> and these are the results that we get:

For both mail servers of ibm.com we get same result:

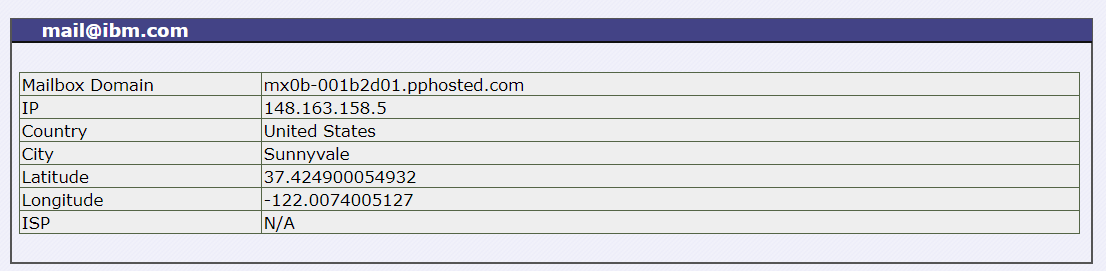


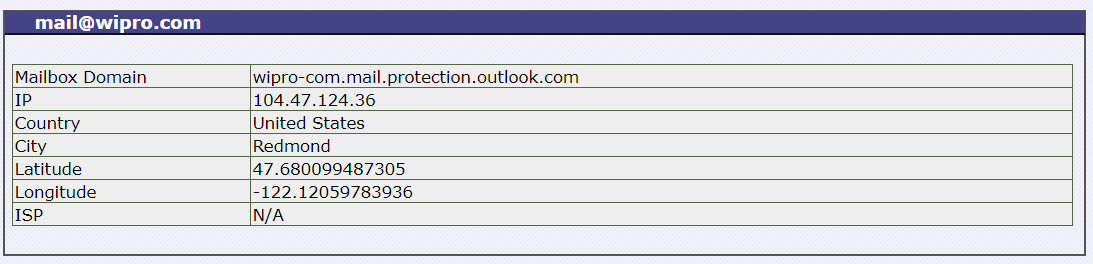
For wipro mail server:

1. Now the second way to do this is through this site:

|  |
| --- |
| <https://my-addr.com/email_server_location/e-mail_box_server_location/locate_email_address_for_free.php> |

Enter [mail@ibm.com](mailto:mail@ibm.com) for ibm and [mail@wipro.com](mailto:mail@wipro.com) for wipro.com in email address box and check the mail server with what we got in nslookup and note the location.





And that’s how we can get location of mail servers:

**Therefore IBM mail servers are located at 892 Ross drive, Sunnyvale, California, United States and**

**Wipro mail server is located at One Microsoft way, Redmond, Washington, United States.**

Q3: Scan and find out port numbers open 203.163.246.23

|  |
| --- |
| # Nmap 7.80 scan initiated Thu Aug 27 17:13:21 2020 as: nmap -Pn -vv -oN nmap.txt 203.163.246.23  Nmap scan report for 203.163.246.23  Host is up, received user-set (0.0072s latency).  Scanned at 2020-08-27 17:13:22 EDT for 59s  Not shown: 998 filtered ports  Reason: 996 no-responses and 2 host-unreaches  PORT STATE SERVICE REASON  25/tcp closed smtp conn-refused  110/tcp open pop3 syn-ack  Read data files from: /usr/bin/../share/nmap  # Nmap done at Thu Aug 27 17:14:21 2020 -- 1 IP address (1 host up) scanned in 59.11 seconds |

**Therefore** **110 port is open and it is running pop3 service**

Q4: Install nessus in a VM and scan your laptop/desktop for CVE.

Ans: Now for this question I wasn’t able to install nessus because it is showing me error of disk space, I increased the disk space upto 80 gb still it is showing same error. So I downloaded a report I found somewhere on internet and I’m attaching that report over here.

