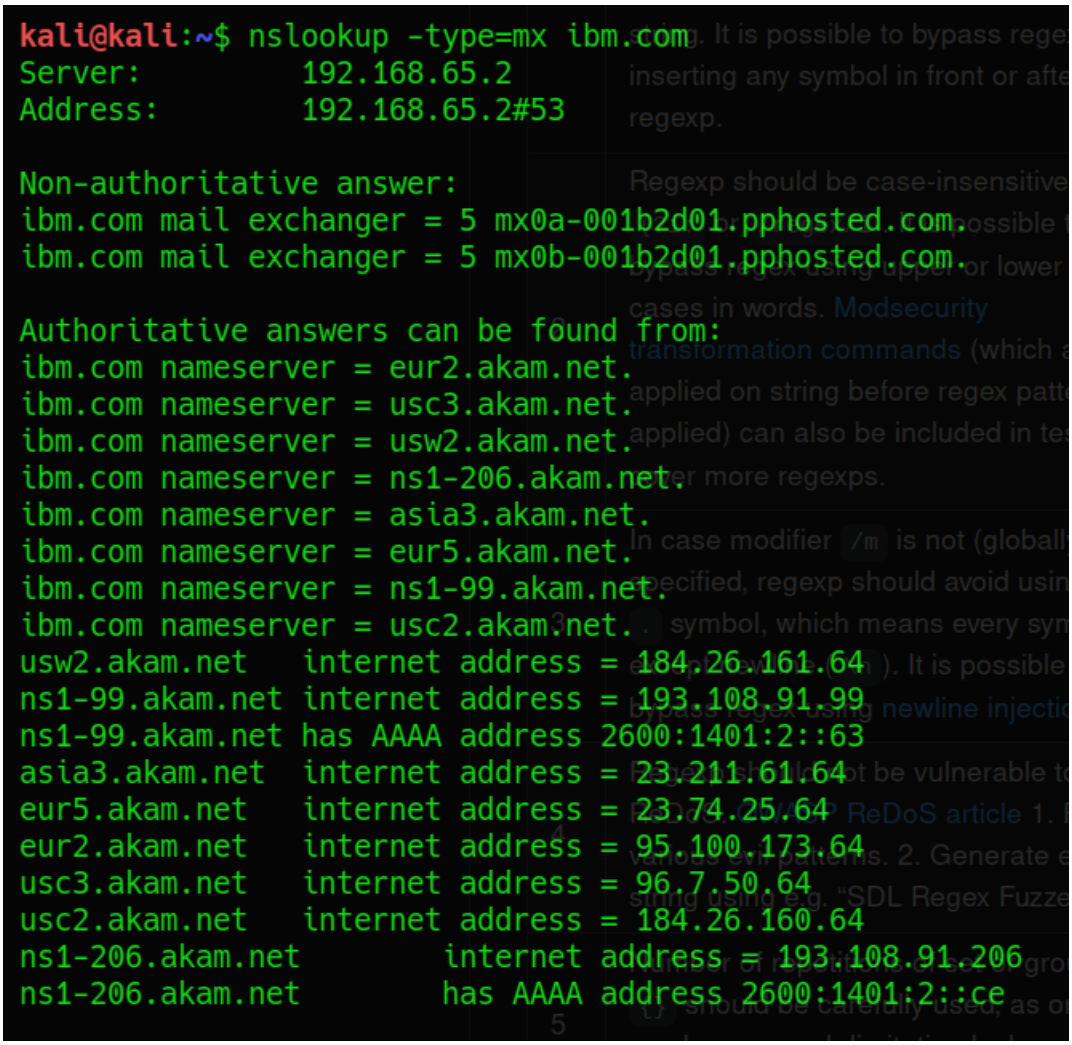
ASSIGNMENT – DAY 4

1. Mail server for

a. ibm.com



You can see in above picture that it has 2 mail servers.

mx0a-001b2d01.pphosted.com.

mx0b-001b2d01.pphosted.com.

b. wipro.com

```
kali@kali:~$ nslookup -type=mx wipro.com
Server:         192.168.65.2
Address:        192.168.65.2#53

Non-authoritative answer:
wipro.com       mail exchanger = 0 wipro-com.mail.protection.outlook.com.

Authoritative answers can be found from:
wipro.com       nameserver = ns4.webindia.com.
wipro.com       nameserver = ns1.webindia.com.
wipro.com       nameserver = ns2.webindia.com.
ns4.webindia.com        internet address = 54.66.0.69
ns2.webindia.com        internet address = 34.235.29.171
ns1.webindia.com        internet address = 50.16.170.116
```

It has only one server.

Q2. Location of these servers.

a. ibm.com

for this site both servers are hosted in same place on different machines.

Mx Record	mx0a-001b2d01.pphosted.com
IP	148.163.156.1
Status	Success
Test duration(ms)	69
AS Number	AS26211
Organization	Proofpoint, Inc.
Domain	proofpoint.com
Country	United States
Abuse Contact	**Network:** 148.163.128.0/19 **Name:** Proofpoint ARIN Abuse **Email:** abuse@proofpoint.com **Phone:** +1-801-748-4494 **Address:** US, UT, Draper, 13997 S Minuteman Dr, 84020 **Country:** US

Mx Record	mx0b-001b2d01.pphosted.com
IP	148.163.158.5
Status	Success
Test duration(ms)	21
AS Number	AS22843
Organization	Proofpoint, Inc.
Domain	proofpoint.com
Country	United States
Abuse Contact	**Network:** 148.163.128.0/19 **Name:** Proofpoint ARIN Abuse **Email:** abuse@proofpoint.com **Phone:** +1-801-748-4494 **Address:** US, UT, Draper, 13997 S Minuteman Dr, 84020 **Country:** US

b. wipro.com

the server is hosted in place as shown below.

Mx Record	wipro-com.mail.protection.outlook.com
IP	104.47.126.36
Status	Success
Test duration(ms)	192
AS Number	AS8075
Organization	Microsoft Corporation
Domain	microsoft.com
Country	South Korea
Abuse Contact	**Network:** 104.40.0.0/13 **Name:** Microsoft Abuse Contact **Email:** abuse@microsoft.com **Phone:** +1-425-882-8080 **Address:** US, WA, Redmond, One Microsoft Way, 98052 **Country:** US

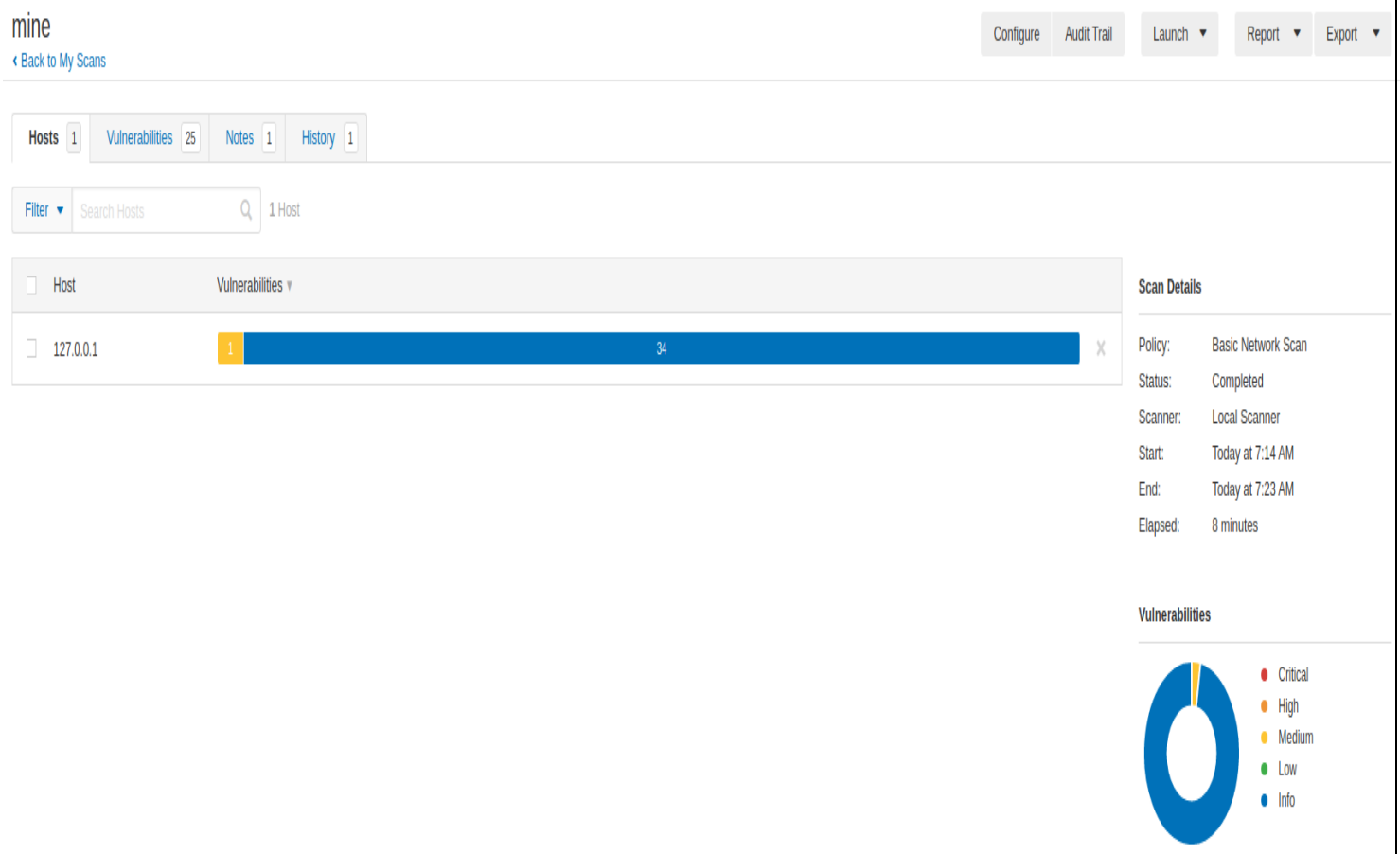
For the location I have used online tool https://dnschecker.org/mx-lookup.php

Q3 Scanning open ports for 203.163.246.23

All the ports were behind firewall, i.e filtered.

```
kali@kali:~$ sudo nmap -sS -Pn 203.163.246.23 -p1-4000
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-01 03:33 EDT
Stats: 0:02:32 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 18.99% done; ETC: 03:46 (0:10:53 remaining)
Stats: 0:05:27 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 40.75% done; ETC: 03:46 (0:07:57 remaining)
Stats: 0:09:22 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 70.00% done; ETC: 03:46 (0:04:01 remaining)
Stats: 0:09:50 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 73.50% done; ETC: 03:46 (0:03:33 remaining)
Stats: 0:11:27 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 85.62% done; ETC: 03:46 (0:01:56 remaining)
Stats: 0:11:43 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 87.62% done; ETC: 03:46 (0:01:39 remaining)
Stats: 0:13:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 97.45% done; ETC: 03:46 (0:00:20 remaining)
Nmap scan report for 203.163.246.23
Host is up.
All 4000 scanned ports on 203.163.246.23 are filtered
```

Q4 Scanning my own machine with NESSUS



I didn’t find any know CVEs in my scan , but the scan showed my other info and medium vulnerabilities

127.0.0.1

0	0	1	0	32
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 33

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
INFO	N/A	12634	Authenticated Check : OS Name and Installed Package Enumeration
INFO	N/A	110695	Authentication Success - Local Checks Not Available
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	55472	Device Hostname
INFO	N/A	54615	Device Type
INFO	N/A	25203	Enumerate IPv4 Interfaces via SSH
INFO	N/A	25202	Enumerate IPv6 Interfaces via SSH
INFO	N/A	33276	Enumerate MAC Addresses via SSH
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	10147	Nessus Server Detection
INFO	N/A	58651	Netstat Active Connections
INFO	N/A	64582	Netstat Connection Information

INFO	N/A	14272	Netstat Portscanner (SSH)
INFO	N/A	11936	OS Identification
INFO	N/A	97993	OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	22964	Service Detection
INFO	N/A	42822	Strict Transport Security (STS) Detection
INFO	N/A	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	56468	Time of Last System Startup
INFO	N/A	20094	VMware Virtual Machine Detection

It detected my vmware and the kali os I was running on it.

mine / Plugin #20094

‹ Back to Vulnerabilities

Hosts 1 | **Vulnerabilities 25** | Notes 1 | History 1

INFO VMware Virtual Machine Detection

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Output

```
The remote host is a VMware virtual machine.
```

Port ▲	Hosts
N/A	127.0.0.1

mine / Plugin #11936

‹ Back to Vulnerabilities

Hosts 1 | **Vulnerabilities 25** | Notes 1 | History 1

INFO **OS Identification**

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Output

```
Remote operating system : Linux Kernel 5.4.0-kali3-amd64
Confidence level : 99
Method : uname

The remote host is running Linux Kernel 5.4.0-kali3-amd64
```

Port ▲	Hosts
N/A	127.0.0.1

----------X----------

NAME- VISHAL KUMAR SINGH