

Soultion 1:-Mail servers of the given domain

- Ibm.com
- Wipro.com

```
Non-authoritative answer:
ibm.com MX preference = 5, mail exchanger = mx0b-001b2d01.pphosted.com
ibm.com MX preference = 5, mail exchanger = mx0a-001b2d01.pphosted.com
> Wipro.com
Server: UnKnown
Address: ██████████

Non-authoritative answer:
Wipro.com MX preference = 0, mail exchanger = wipro-com.mail.protection.outlook.com
>
```

Solution 2: Finding location of the email-servers of the given above domain

--- Since it's not possible to track the location of the email-servers of the above domain just by the url rather than using the email-header.

Solution 3:- The List of open ports of 203.163.246.23

---Three of the ports were opened for 203.163.246.23.

- 21---tcp
- 554---tcp
- 1723---tcp

```
warlock@kali:~$ sudo nmap -v -sS -sV 203.163.246.23
[sudo] password for warlock:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-27 17:21 EDT
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 17:21
Scanning 203.163.246.23 [4 ports]
Completed Ping Scan at 17:21, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:21
Completed Parallel DNS resolution of 1 host. at 17:21, 0.74s elapsed
Initiating SYN Stealth Scan at 17:21
Scanning 203.163.246.23 [1000 ports]
Discovered open port 554/tcp on 203.163.246.23
Discovered open port 1723/tcp on 203.163.246.23
Discovered open port 21/tcp on 203.163.246.23
Increasing send delay for 203.163.246.23 from 0 to 5 due to 11 out of 28 dropped probes since last increase.
Completed SYN Stealth Scan at 17:22, 76.66s elapsed (1000 total ports)
Initiating Service scan at 17:22
Scanning 3 services on 203.163.246.23
Completed Service scan at 17:22, 3.07s elapsed (3 services on 1 host)
NSE: Script scanning 203.163.246.23.
Initiating NSE at 17:22
Completed NSE at 17:22, 3.07s elapsed
Initiating NSE at 17:22
Completed NSE at 17:22, 0.01s elapsed
Nmap scan report for 203.163.246.23
Host is up (0.034s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  tcpwrapped
554/tcp   open  tcpwrapped
1723/tcp  open  tcpwrapped

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 84.82 seconds
Raw packets sent: 3032 (133.260KB) | Rcvd: 1677 (67.104KB)
```

Solution 4: Nessus report of one of my VM Machine for CVE

my VM

[Back to My Scans](#)

Configure

Audit Trail

Launch

Report

Export

Hosts1Vulnerabilities18History1

Filter

Search Vulnerabilities

18 Vulnerabilities

<input type="checkbox"/>	Sev	Name	Family	Count		
<input type="checkbox"/>	MIXED	4	Microsoft Windows (Multiple Issu...	Windows	4	
<input type="checkbox"/>	MEDIUM	SMB Signing not required	Misc.	1		
<input type="checkbox"/>	INFO	7	SMB (Multiple Issues)	Windows	8	
<input type="checkbox"/>	INFO	DCE Services Enumeration	Windows	7		
<input type="checkbox"/>	INFO	Authenticated Check : OS Name and I...	Settings	1		
<input type="checkbox"/>	INFO	Authentication Failure - Local Checks ...	Settings	1		
<input type="checkbox"/>	INFO	Common Platform Enumeration (CPE)	General	1		
<input type="checkbox"/>	INFO	Device Type	General	1		
<input type="checkbox"/>	INFO	Ethernet MAC Addresses	General	1		

Scan Details

Policy: Advanced Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 8:20 PM
End: Today at 8:26 PM
Elapsed: 6 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

my VM

[Back to My Scans](#)

Configure

Audit Trail

Launch

Report

Export

Hosts1Vulnerabilities18History1

Filter

Search Hosts

1 Host

<input type="checkbox"/>	Host	Vulnerabilities
<input type="checkbox"/>		<div><div>121</div><div>30</div></div>

Scan Details

Policy: Advanced Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 8:20 PM
End: Today at 8:26 PM
Elapsed: 6 minutes

Vulnerabilities

Critical

High

Medium

Low

Info