

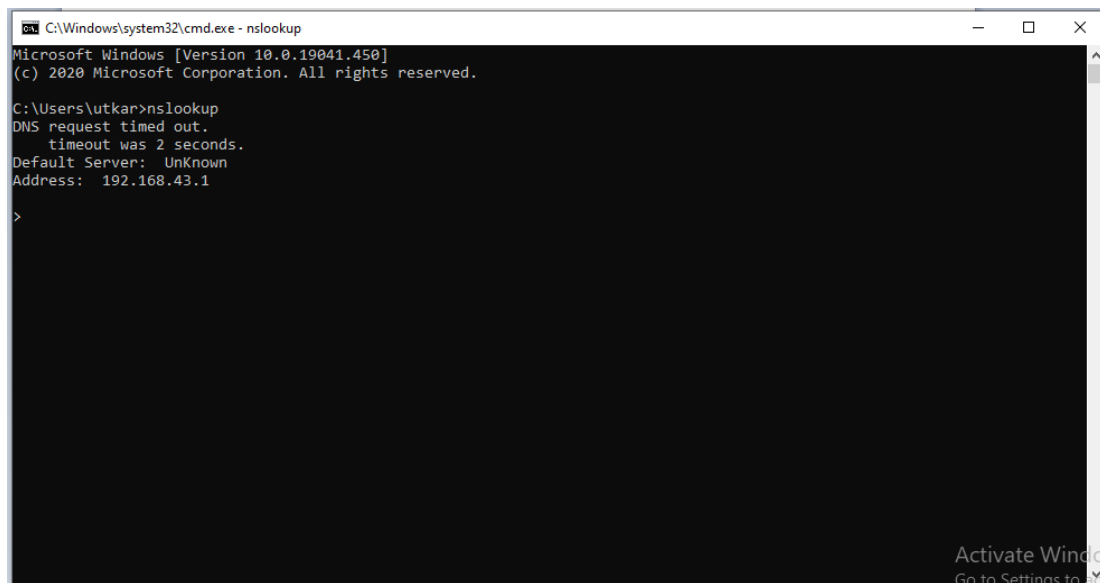
Utkarsh Rathod

Question 1: Find out the mail servers of the following domain.

- 1) ibm.com
- 2) Wipro.com

Answer:

- 1) Open CMD from run (Win + R) and type nslookup



```
C:\Windows\system32\cmd.exe - nslookup
Microsoft Windows [Version 10.0.19041.450]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\utkar>nslookup
DNS request timed out.
    timeout was 2 seconds.
Default Server:  UnKnown
Address:  192.168.43.1

>
```

- 2) Next set the search type to mail server with the help of commands:

set type=mx

```
C:\Users\utkar>nslookup
DNS request timed out.
    timeout was 2 seconds.
Default Server:  UnKnown
Address:  192.168.43.1

> set type=mx
>
```

- 3) Next enter the domain name whose mail server is required.

- a) IBM.com

```
> set type=mx
> ibm.com
Server:  UnKnown
Address:  192.168.43.1

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

b) Wipro.com

```
> set type=mx
> wipro.com
Server: UnKnown
Address: 192.168.43.1

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

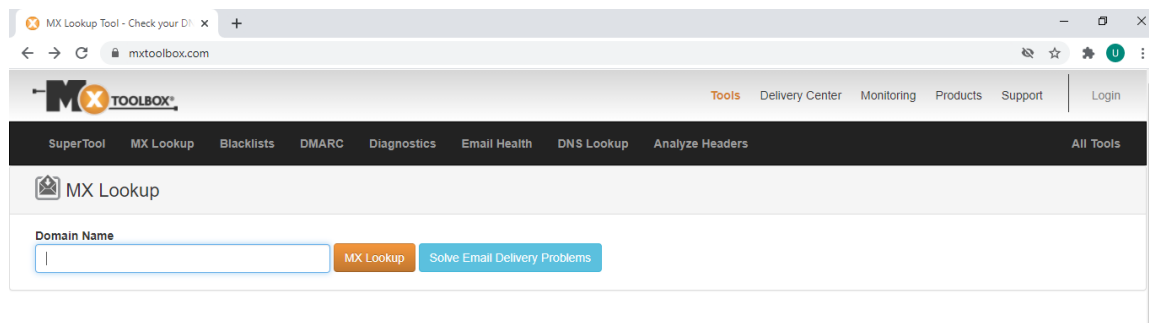
Question 2: Find the locations, of these emails servers are hosted.

1) ibm.com

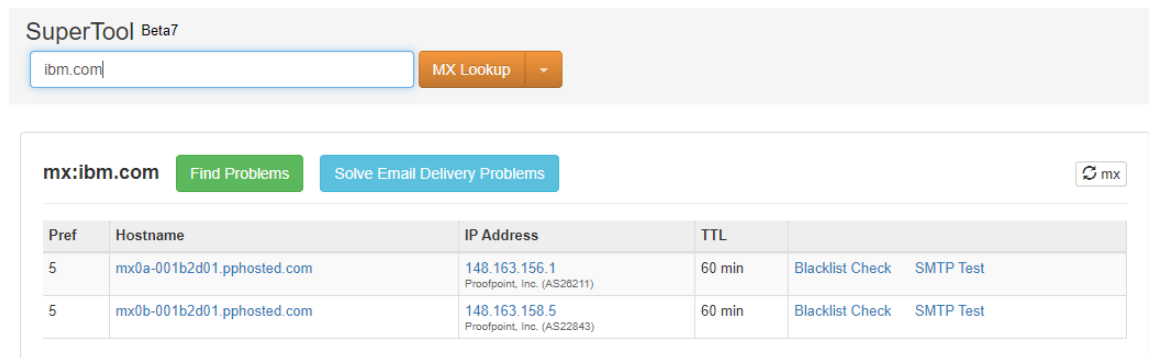
2) Wipro.com

Answer:

1) Open mxtoolbox.com in browser.



2) Type IBM.com and click the MX Lookup button.




3) We got 2 IP address now we search for these IP address to trace the location. For that we go to <https://whatismyipaddress.com/> and search the IP address.

IP Details for 148.163.156.1

This information should not be used for emergency purposes, trying to find someone's exact physical address, or other purposes that would require 100% accuracy.


[Lookup IP Address](#)

Details for 148.163.156.1

IP: 148.163.156.1
Decimal: 2493750273
Hostname: mx0a-001b2d01.pphosted.com
ASN: 26211
ISP: Proofpoint, Inc.
Organization: Proofpoint, Inc.
Services: None detected
Type: [Broadband](#)
Assignment: [Likely Static IP](#)
Blacklist: [Click to Check Blacklist Status](#)
Continent: North America
Country: United States 
Latitude: 37.751 (37° 45' 3.60" N)
Longitude: -97.822 (97° 49' 19.20" W)

Activate Wi

Details for 148.163.158.5

IP: 148.163.158.5
Decimal: 2493750789
Hostname: mx0b-001b2d01.pphosted.com
ASN: 22843
ISP: Proofpoint, Inc.
Organization: Proofpoint, Inc.
Services: None detected
Type: [Broadband](#)
Assignment: [Likely Static IP](#)
Blacklist: [Click to Check Blacklist Status](#)
Continent: North America
Country: United States 
Latitude: 37.751 (37° 45' 3.60" N)
Longitude: -97.822 (97° 49' 19.20" W)

As we see both the IP addresses are coming from North America.

Next we check for Wipro.

SuperTool | Beta7

wipro.com | MX Lookup


mx:wipro.com Find Problems Solve Email Delivery Problems

EMAILS BOUNCING? MxToolbox has your email delivery solutions

Pref	Hostname	IP Address	TTL	
0	wipro-com.mail.protection.outlook.com	104.47.125.36 Microsoft Corporation (AS8075)	60 min	Blacklist Check SMTP Test

Now we locate the IP address of the mail server for Wipro.

Details for 104.47.125.36

IP: 104.47.125.36
 Decimal: 1747942692
 Hostname: mail-sg2apc010036.inbound.protection.outlook.com
 ASN: 8075
 ISP: Microsoft Corporation
 Organization: Microsoft Azure
 Services: Likely [mail server](#)
 Type: [Corporate](#)
 Assignment: [Likely Static IP](#)
 Blacklist: [Click to Check Blacklist Status](#)
 Continent: Asia
 Country: Singapore 
 City: Singapore
 Latitude: 1.2929 (1° 17' 34.44" N)
 Longitude: 103.8547 (103° 51' 16.92" E)
 Postal Code: 18

Activate Wir

For Wipro the mail server is located in Singapore.

Question 3: Scan and find out the port numbers open 203.163.264.23

Answer:

```
urathod@kali:~$ sudo nmap -Pn -sS 203.163.264.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-28 14:12 IST
Stats: 0:01:41 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 49.50% done; ETC: 14:16 (0:01:43 remaining)
Stats: 0:01:41 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 49.85% done; ETC: 14:16 (0:01:42 remaining)
Stats: 0:01:42 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 50.00% done; ETC: 14:16 (0:01:42 remaining)
Stats: 0:01:56 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 57.00% done; ETC: 14:16 (0:01:28 remaining)
Stats: 0:02:25 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 71.00% done; ETC: 14:16 (0:00:59 remaining)
Stats: 0:02:26 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 71.50% done; ETC: 14:16 (0:00:58 remaining)
Stats: 0:02:45 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 81.00% done; ETC: 14:16 (0:00:38 remaining)
Stats: 0:03:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 94.00% done; ETC: 14:16 (0:00:12 remaining)
Nmap scan report for 203.163.264.23
Host is up.
All 1000 scanned ports on 203.163.264.23 are filtered
```

```
Nmap done: 1 IP address (1 host up) scanned in 203.97 seconds
```

```
urathod@kali:~$
```

Activate Windows
Go to Settings to activate Windows.

```
urathod@kali:~$ sudo nmap -Pn 203.163.264.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-28 14:17 IST
Stats: 0:00:21 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 10.00% done; ETC: 14:20 (0:03:09 remaining)
Stats: 0:01:56 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 57.00% done; ETC: 14:20 (0:01:28 remaining)
Stats: 0:02:20 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 69.00% done; ETC: 14:20 (0:01:03 remaining)
Stats: 0:02:56 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 86.50% done; ETC: 14:20 (0:00:27 remaining)
Nmap scan report for 203.163.264.23
Host is up.
All 1000 scanned ports on 203.163.264.23 are filtered

Nmap done: 1 IP address (1 host up) scanned in 203.79 seconds
urathod@kali:~$ sudo nmap -F 203.163.264.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-28 14:20 IST
Nmap scan report for 203.163.264.23
Host is up (0.062s latency).
All 100 scanned ports on 203.163.264.23 are filtered
```

```
Nmap done: 1 IP address (1 host up) scanned in 3.01 seconds
```

```
urathod@kali:~$
```

Activate Windows
Go to Settings to activate Windows.

Question 4: Install nessus in a VM and scan your Laptop/Desktop for CVE.

Answer:

We have a VM ready for the CVE scanning,

We install nessus from the official site <https://www.tenable.com/products/nessus/nessus-essentials>.
We do need to register to receive an activation code to proceed ahead with the installation of nessus.

We install Nessus like any other .exe file in the server. Here we are choosing windows server 2016 for the scanning purpose.

Once installation has been completed. It will ask to open the site from browser. Once opened, Login with the activation code.

After everything is completed, it ask us the range of IP address to scan. Please find the below screenshot for the same.

Welcome to Nessus Essentials

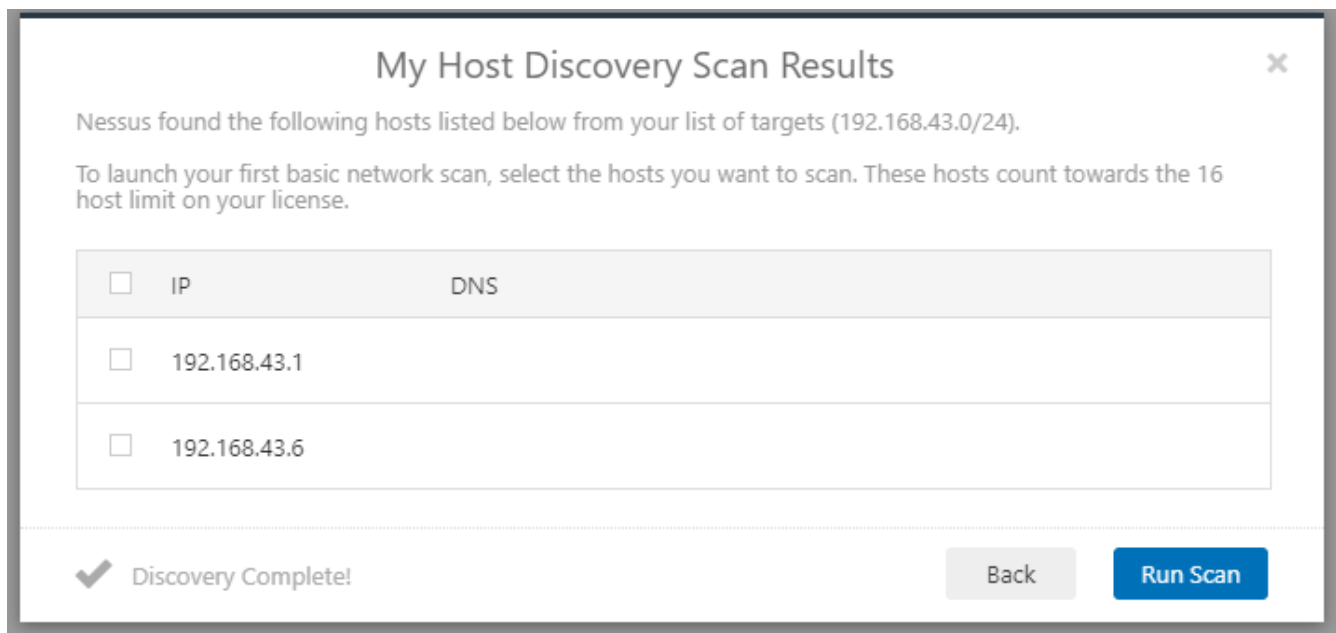
To get started, launch a host discovery scan to identify what hosts on your network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 16 host limit on your license.

Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

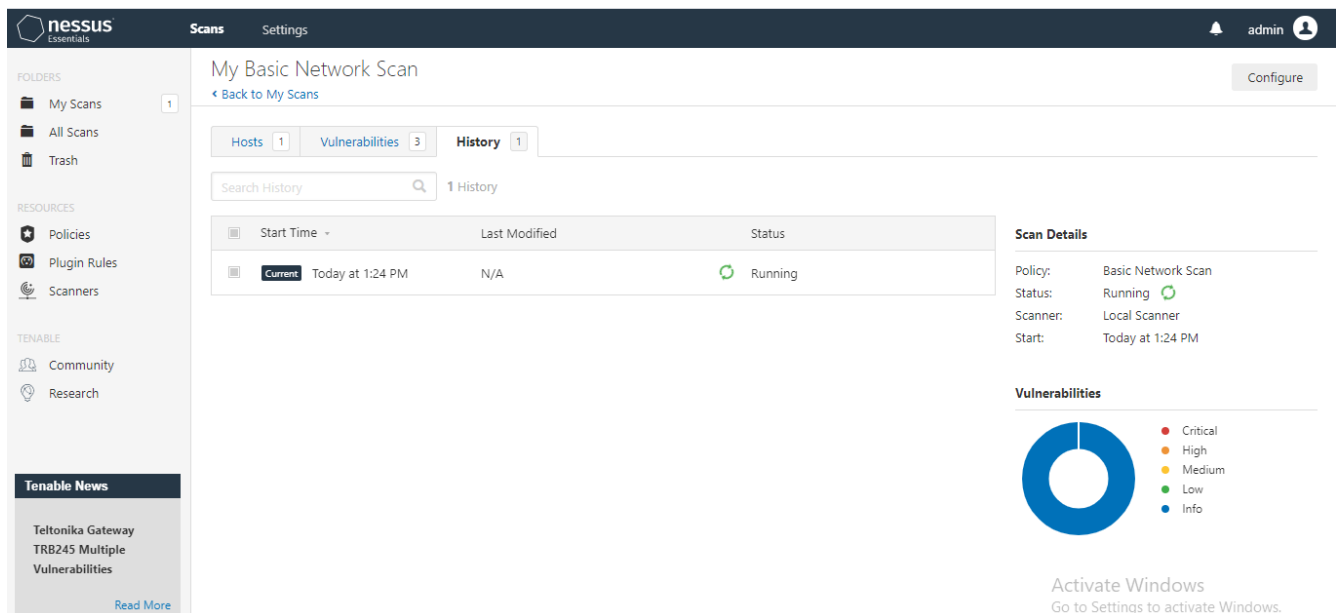
Targets

192.168.43.0/24

Submitting...



2 host have been found. We select the 2nd one for the scan.



Once the scanning is running, we found 5 vulnerabilities

nessus Essentials Scans Settings admin

My Basic Network Scan [Back to My Scans](#) [Configure](#)

Hosts 1 Vulnerabilities 5 History 1

Filter Search Vulnerabilities 5 Vulnerabilities

Sev	Name	Family	Count
INFO	DCE Services Enumeration	Windows	9
INFO	SMB (Multiple Issues)	Windows	5
INFO	Microsoft Windows (Multiple Issues)	Windows	2
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO	VMware ESX/GSX Server detection	Service detection	1

Scan Details

Policy: Basic Network Scan
 Status: Running
 Scanner: Local Scanner
 Start: Today at 1:24 PM

Vulnerabilities

Donut chart showing vulnerability distribution: Critical (0), High (0), Medium (0), Low (0), Info (5).

Tenable News

Microsoft's August 2020 Patch Tuesday Addresses 1...

When we select the vulnerabilities, it give details on it.

nessus Essentials Scans Settings admin

[Back to Vulnerability Group](#)

Hosts 1 Vulnerabilities 14 History 1

Microsoft Windows SMB Service Detection

Description
 The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Output

An SMB server is running on this port.

Port	Hosts
139 / tcp / smb	192.168.43.6

A CIFS server is running on this port.

Port	Hosts
445 / tcp / cifs	192.168.43.6

Plugin Details

Severity: Info
 ID: 11011
 Version: 1.42
 Type: remote
 Family: Windows
 Published: June 5, 2002
 Modified: August 20, 2020

Risk Information

Risk Factor: None

Vulnerability Information

Asset Inventory: True

Activate Windows
 Go to Settings to activate Windows.

Tenable News

Teltonika Gateway TRB245 Multiple Vulnerabilities [Read More](#)

It also provides medium level vulnerabilities, like

nessus

Essentials

Scans

Settings

admin

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Scanners

TENABLE

Community

Research

Tenable News

Ubiquiti UniFi Protect Username Discovery

Read More

MEDIUM

SMB Signing not required

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

See Also

<https://support.microsoft.com/en-us/help/887429/overview-of-server-message-block-signing>

<http://technet.microsoft.com/en-us/library/cc731957.aspx>

<http://www.nessus.org/u?74b80723>

<https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>

<http://www.nessus.org/u?a3cac4ea>

Output

No output recorded.

Port	Hosts
445 / tcp / cifs	192.168.43.6

Plugin Details

Severity: Medium

ID: 57608

Version: 1.18

Type: remote

Family: Misc.

Published: January 19, 2012

Modified: November 15, 2018

Risk Information

Risk Factor: Medium

CVSS v3.0 Base Score 5.3

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C

CVSS v3.0 Temporal Score: 4.6

CVSS Base Score: 5.0

CVSS Temporal Score: 3.7

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N

CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Activate Windows

Vulnerability Information

Go to Settings to activate Windows.

CPE: cpe:/o:microsoft:windows cpe:/a:samba:samba