

## Assignment for day-4

Name:Keshav Jayakrishnan

Email:kesh.jayan@gmail.com

### Question-1:

```
C:\Users\Appu>nslookup
Default Server: dsldevice.lan
Address: 192.168.1.1

> set type=mx
> ibm.com
Server: dsldevice.lan
Address: 192.168.1.1

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: dsldevice.lan
Address: 192.168.1.1

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

wipro.com nameserver = ns1.webindia.com
wipro.com nameserver = ns2.webindia.com
wipro.com nameserver = ns4.webindia.com
>
```

The names given after 'mail exchanger' are the mail servers of the respective domains.

### Question 2:

Once the mail servers are pinged, the ip address shows up and you can run a simple online geolocation scan on it.

For ibm.com, the ip of the mail server is 148.163.158.5 or 148.163.158.1

## Technical details

IP address	148.163.158.5
Hostname	mx0b-001b2d01.pphosted.com
Type	Public
CIDR	148.163.158.5/24

## Location of IP address 148.163.158.5

Lookup information about the location associated with the IP address 148.163.158.5.

City	Sunnyvale (20% confidence)
Metrocode	807 (California, San Francisco-Oakland-San Jose CA)
Subdivision	California (CA) (60% confidence)
Country	United States (US) (99% confidence)
Postalcode	94089 (10% confidence)
Continent	North America (NA)
Time zone	America/Los_Angeles

For wipro.com, the ip of the mail server is 34.235.29.171

34.235.29.171

### LOCATION

Country	United States (US)
Continent	North America (NA)
Coordinates	37.751 (lat) / -97.822 (long)
Time	2020-08-27 06:40:40 (America/Chicago)

### NETWORK

IP address	34.235.29.171
Hostname	ec2-34-235-29-171.compute-1.amazonaws.com
Provider	AMAZON-AES
ASN	14618

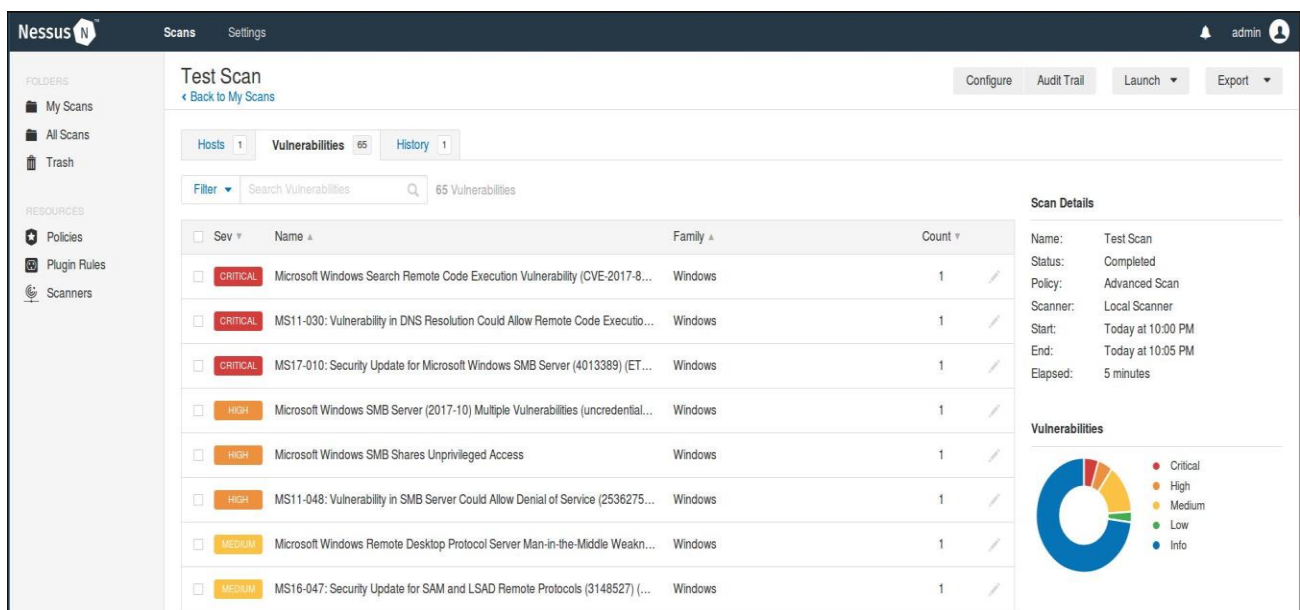
### Question 3:

A simple nmap scan can provide the open port numbers for the particular ip, but in this case, all the ports are filtered.

```
kali@kali:~$ sudo nmap -v 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-27 16:22 UTC
Initiating Ping Scan at 16:22
Scanning 203.163.246.23 [4 ports]
Completed Ping Scan at 16:22, 0.10s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:22
Completed Parallel DNS resolution of 1 host. at 16:22, 0.05s elapsed
Initiating SYN Stealth Scan at 16:22
Scanning 203.163.246.23 [1000 ports]
Completed SYN Stealth Scan at 16:22, 7.56s elapsed (1000 total ports)
Nmap scan report for 203.163.246.23
Host is up (0.041s latency).
All 1000 scanned ports on 203.163.246.23 are filtered

Read data files from: /usr/bin/../../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 8.01 seconds
Raw packets sent: 2009 (88.352KB) | Rcvd: 6 (240B)
```

### Question 4:



**Nessus** Scans Settings admin

**Test Scan**  
Back to My Scans

Configure Audit Trail Launch Export

Hosts 1 Vulnerabilities 65 History 1

Filter Search Vulnerabilities 65 Vulnerabilities

Sev	Name	Family	Count
CRITICAL	Microsoft Windows Search Remote Code Execution Vulnerability (CVE-2017-8...	Windows	1
CRITICAL	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Executio...	Windows	1
CRITICAL	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ET...	Windows	1
HIGH	Microsoft Windows SMB Server (2017-10) Multiple Vulnerabilities (uncredentia...	Windows	1
HIGH	Microsoft Windows SMB Shares Unprivileged Access	Windows	1
HIGH	MS11-048: Vulnerability in SMB Server Could Allow Denial of Service (2536275...	Windows	1
MEDIUM	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weak...	Windows	1
MEDIUM	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (...	Windows	1

**Scan Details**

Name: Test Scan  
Status: Completed  
Policy: Advanced Scan  
Scanner: Local Scanner  
Start: Today at 10:00 PM  
End: Today at 10:05 PM  
Elapsed: 5 minutes

**Vulnerabilities**

Donut chart showing vulnerability distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).