

## Letsupgrade -CyberSecurity - Batch 1- Assignment1(Day4)

Name : Sundeep

date : 26/aug/2020

mail: sundeepsanju29@gmail.com

Q1) Finding Mail servers of wipro and ibm

sol) command prompt -> nslookup -> set type =mx -> ibm.com/wipro.com

```
C:\Users\davinci>nslookup
Default Server:  kaveri.hathway.com
Address:  202.88.174.6

> set type=mx
> ibm.com
Server:  kaveri.hathway.com
Address:  202.88.174.6

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

ibm.com nameserver = usc2.akam.net
ibm.com nameserver = asia3.akam.net
ibm.com nameserver = usw2.akam.net
ibm.com nameserver = ns1-99.akam.net
ibm.com nameserver = usc3.akam.net
ibm.com nameserver = ns1-206.akam.net
ibm.com nameserver = eur2.akam.net
ibm.com nameserver = eur5.akam.net
eur5.akam.net internet address = 23.74.25.64
asia3.akam.net internet address = 23.211.61.64
ns1-206.akam.net internet address = 193.108.91.206
ns1-99.akam.net AAAA IPv6 address = 2600:1401:2::63
>
```

```
> Wipro.com
Server:  kaveri.hathway.com
Address:  202.88.174.6

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 = ns3.webindia.com
ns1.webindia.com internet address = 50.16.170.116
ns2.webindia.com internet address = 34.235.29.171
ns3.webindia.com internet address = 216.55.142.32
>
```

Q2) Finding locations of obtained mail servers


sol) chrome -> iplocator -> paste the obtained domains

You've entered a domain name. We've found an IP address from the domain name you've entered. Your translated IP address is **148.163.158.5**

Geolocation data from [IP2Location](#) (Product: DB6, updated on 2020-9-1)

Domain Name	Country	Region	City
mx0b-001b2d01.pphosted.com	United States of America 	California	Sunnyvale
ISP	Organization	Latitude	Longitude
Proofpoint Inc.	Not Available	37.4012	-122.0075

Geolocation data from [ipinfo.io](#) (Product: API, real-time)

Domain Name	Country	Region	City
mx0b-001b2d01.pphosted.com	United States 	California	San Jose
ISP	Organization	Latitude	Longitude
<a href="#">Proofpoint, Inc.</a>	Proofpoint, Inc. ( <a href="#">proofpoint.com</a> )	37.3394	-121.8950

You've entered a domain name. We've found an IP address from the domain name you've entered. Your translated IP address is **104.47.125.36**

Geolocation data from [IP2Location](#) (Product: DB6, updated on 2020-9-1)

Domain Name	Country	Region	City
wipro-com.mail.protection.outlook.com	Singapore 	Singapore	Singapore
ISP	Organization	Latitude	Longitude
Microsoft Corporation	Not Available	1.2897	103.8501

Geolocation data from [ipinfo.io](#) (Product: API, real-time)

Domain Name	Country	Region	City
wipro-com.mail.protection.outlook.com	Singapore 	Singapore	Singapore
ISP	Organization	Latitude	Longitude
<a href="#">Microsoft Corporation</a>	Microsoft Corporation ( <a href="#">microsoft.com</a> )	1.2897	103.8501

Q3) Nmap scan on 203.163.246.23

sol ) Kali -> terminal -> su -> enter pass for root acc -> nmap -sS -v -Pn 203.163.246.23      No open ports

```
File Actions Edit View Help
bpg@kali-pc-001:~$ sudo su -
[sudo] password for bpg:
root@kali-pc-001:~# nmap -sS -v -Pn -g 88 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 08:31 PDT
Initiating Parallel DNS resolution of 1 host. at 08:31
Completed Parallel DNS resolution of 1 host. at 08:31, 0.49s elapsed
Initiating SYN Stealth Scan at 08:31
Scanning 203.163.246.23 [1000 ports]
SYN Stealth Scan Timing: About 15.50% done; ETC: 08:34 (0:02:49 remaining)
SYN Stealth Scan Timing: About 30.00% done; ETC: 08:34 (0:02:22 remaining)
SYN Stealth Scan Timing: About 45.00% done; ETC: 08:34 (0:01:51 remaining)
SYN Stealth Scan Timing: About 59.50% done; ETC: 08:34 (0:01:22 remaining)
SYN Stealth Scan Timing: About 74.50% done; ETC: 08:34 (0:00:52 remaining)
Completed SYN Stealth Scan at 08:34, 203.60s elapsed (1000 total ports)
Nmap scan report for 203.163.246.23
Host is up, received user-set.
All 1000 scanned ports on 203.163.246.23 are filtered because of 1000 no-responses

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 204.44 seconds
Raw packets sent: 2000 (88.000KB) | Rcvd: 0 (0B)
root@kali-pc-001:~# nmap -6 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 08:36 PDT
Warning: Hostname 203.163.246.23 resolves, but not to any IPv6 address. Try scanning without -6
Failed to resolve "203.163.246.23".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds
root@kali-pc-001:~# nmap -p 22,25,135 -Pn -v -b 203.163.246.23 scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 08:38 PDT
Resolved FTP bounce attack proxy to 203.163.246.23 (203.163.246.23).
Failed to resolve "scanme.nmap.org".
```

#### Q4) nessus Scan fot find CVE

sol ) browser-> localhost:8834 : login with bgp credentials -> new scan ->advance scan -> fill domain name and ip  
-> window ->fill details and start scan

The screenshot displays the Nessus Essentials web interface. The left sidebar contains navigation links for 'OLDERS' (My Scans, All Scans, Trash), 'RESOURCES' (Policies, Plugin Rules, Scanners), and 'ENABLE' (Community, Research, Tenable News). The main content area shows the 'pentester scan' details. At the top, there are tabs for 'Hosts' (1), 'Vulnerabilities' (6), and 'History' (1). Below these is a 'Search History' search bar and a table with columns for 'Start Time', 'Last Modified', and 'Status'. The table contains one entry: 'Current' (Today at 8:00...), 'Today at 8:13 AM', and 'Completed'. To the right of the table are 'Configure' and 'Audit Trail' buttons. On the far right, the 'Scan Details' section lists: Policy: Advanced Scan, Status: Completed, Scanner: Local Scanner, Start: Today at 8:08 AM, End: Today at 8:13 AM, and Elapsed: 5 minutes. Below this is a 'Vulnerabilities' section with a donut chart showing the distribution of vulnerability severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue). The chart shows a high proportion of 'Info' vulnerabilities.

Start Time	Last Modified	Status
Current Today at 8:00...	Today at 8:13 AM	Completed

**Scan Details**

- Policy: Advanced Scan
- Status: Completed
- Scanner: Local Scanner
- Start: Today at 8:08 AM
- End: Today at 8:13 AM
- Elapsed: 5 minutes

**Vulnerabilities**

- Critical
- High
- Medium
- Low
- Info