

Assignment – Day-4

Name : Rushik kumar Avula

Email : avularushik.123@gmail.com

1)Mail servers of ibm.com and wipro.com

We should do this using the nslookup command. And the results are shown in the below screenshot.

```
C:\Users\Rushik kumar Avula>nslookup
Default Server:  csp1.zte.com.cn
Address:  fe80::1

> set type=mx
> ibm.com
Server:  csp1.zte.com.cn
Address:  fe80::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

ibm.com nameserver = ns1-206.akam.net
ibm.com nameserver = usc2.akam.net
ibm.com nameserver = usc3.akam.net
ibm.com nameserver = usw2.akam.net
ibm.com nameserver = eur5.akam.net
ibm.com nameserver = ns1-99.akam.net
ibm.com nameserver = asia3.akam.net
ibm.com nameserver = eur2.akam.net
usw2.akam.net  internet address = 184.26.161.64
asia3.akam.net internet address = 23.211.61.64
ns1-99.akam.net internet address = 193.108.91.99
ns1-206.akam.net internet address = 193.108.91.206
ns1-99.akam.net AAAA IPv6 address = 2600:1401:2::63
ns1-206.akam.net AAAA IPv6 address = 2600:1401:2::ce
> wipro.com
Server:  csp1.zte.com.cn
Address:  fe80::1

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

wipro.com nameserver = ns4.webindia.com
wipro.com nameserver = ns2.webindia.com
wipro.com nameserver = ns1.webindia.com
ns1.webindia.com internet address = 50.16.170.116
ns2.webindia.com internet address = 34.235.29.171
>
```

2) Mail servers location of ibm.com and wipro.com.

I have use the server name to search in website called NS.tools to get there locations.

The first screenshot shows the NS.Tools interface for the domain **mx0b-001b2d01.pphosted.com**. The 'MAIL' section is active, displaying 'Mail servers' information. A tooltip shows details for the selected server:

- Name: mx0b-001b
- IP: 148.163.158.5 (United States)
- Banner: 220 mx0b-001b2d01.pphosted.com ESlv

The 'WEB' section indicates there is no web server.

The second screenshot shows the NS.Tools interface for the domain **mail-pu1apc010036.inbound.protection.outlook.com**. The 'MAIL' section is active, displaying 'Mail servers' information. A tooltip shows details for the selected server:

- Name: mail-pu1apc010036.inbound.protection.outlook.com
- IP: 104.47.126.36 (South Korea)
- Banner: 220 PU1APC01FT039.mail.protection.ou

The 'Reputation' section shows Google Safe Browsing, Web of trust, Blacklists, and Virus Total all with green checkmarks. The 'SPF' section indicates there is no SPF record for this domain.

I checked one of the hackerrank's server on the emailtracker pro.

eMailTrackerPro v10.0b Advanced Edition. Trial day 1 of 15

File Help

My Inbox My Trace Reports Trace Headers Trace Address Email Accounts Settings Export Rules Trial Edition


View New Email Trace Configure

Home Subject: We Challenge ... X

The trace is complete, the information found is displayed on the right

New Trace View Report

Map



Chantilly, Virginia, USA

Table

| # | Hop IP | Hop Name | Location |
|----|-----------------|---------------------------------------|----------------------|
| 1 | 10.0.2.1 | | |
| 3 | 115.98.8.1 | | (India) |
| 4 | 202.88.190.45 | | (India) |
| 5 | 136.232.28.173 | 136.232.28.173.static.jio.com | (India) |
| 10 | 103.198.140.56 | | Singapore, Singapore |
| 11 | 103.198.140.39 | | Singapore, Singapore |
| 11 | 103.198.140.39 | | Singapore, Singapore |
| 12 | 103.198.142.245 | | Singapore, Singapore |
| 13 | 50.97.17.40 | ae6.cbs01.tl01.nyc01.networklayer.com | Dallas, TX, USA |

For 24 hours only you can get up to 20% off eMailTrackerPro! [Click Here](#)

Email Summary

From: no-reply@hackerrankmail.com
 To: avularushik.123@gmail.com
 Date: Wed, 02 Sep 2020 10:54:28 +0000
 Subject: We Challenge You to Solve The Grid Search
 Location: Chantilly, Virginia, USA

Misdirected: No
 Abuse Address: abuse@softlayer.com
 Abuse Reporting: To automatically generate an email abuse report [click here](#)
 From IP: 174.37.214.195

System Information:

- There is no SMTP server running on this system (the port is closed).
- There is no HTTP server running on this system (the port is closed).
- There is no HTTPS server running on this system (the port is closed).
- There is no FTP server running on this system (the port is closed).

Network Whois

Domain Whois

Email Header

3) Nmap scan on given Ip address.

Actually when I ping the given target it is not connecting. So I scanned one of my devices.

```
C:\Users\Rushik kumar Avula>nmap -p 1-65535 -A 157.240.23.35
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-02 19:02 India Standard Time
^C
C:\Users\Rushik kumar Avula>nmap -p 1-65535 -A 192.168.1.3
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-02 19:06 India Standard Time
Nmap scan report for 192.168.1.3
Host is up (0.057s latency).
All 65535 scanned ports on 192.168.1.3 are closed
MAC Address: D4:1A:3F:F6:A2:25 (Guangdong Oppo Mobile Telecommunications)
Device type: storage-misc|phone|general purpose|media device
Running: Buffalo embedded, Google Android 6.X, Linux 2.6.X|3.X, Sony embedded
OS CPE: cpe:/o:google:android:6.0.1 cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3.13 cpe:/o:google:android
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 56.88 ms 192.168.1.3

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 86.81 seconds

C:\Users\Rushik kumar Avula>
```

```

C:\Users\Rushik kumar Avula>nmap -p 1-65535 -A 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-02 19:00 India Standard Time
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 5.80 seconds

C:\Users\Rushik kumar Avula>ping 203.163.246.23

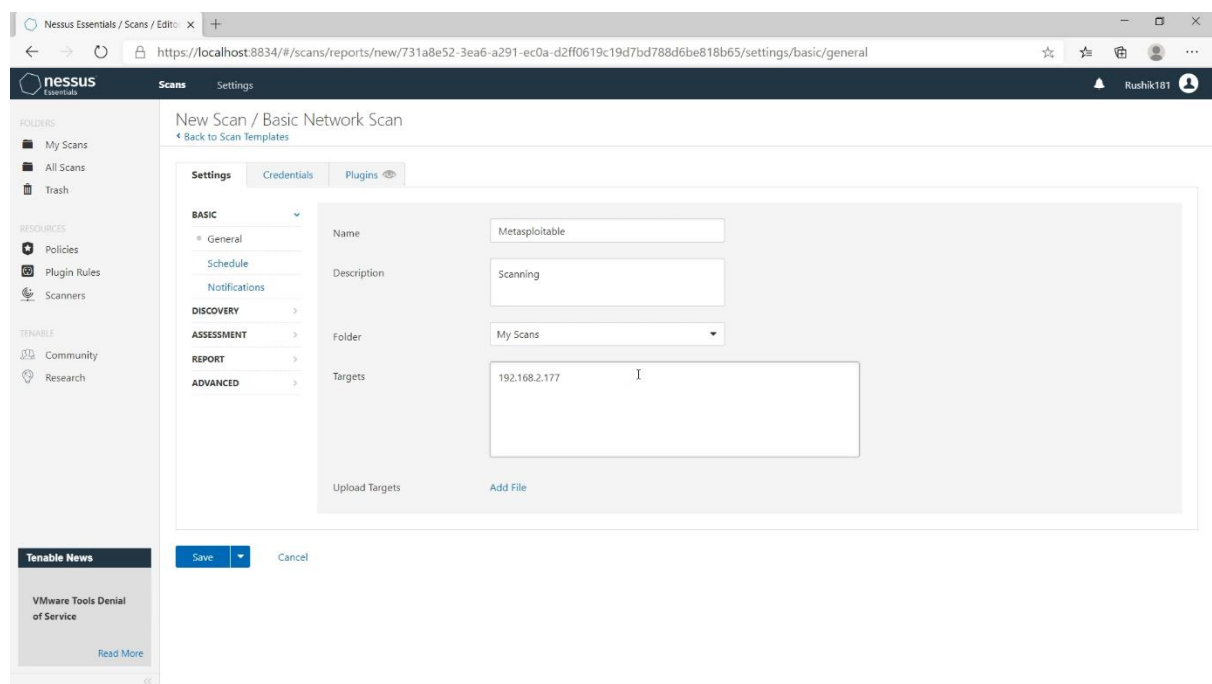
Pinging 203.163.246.23 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 203.163.246.23:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\Rushik kumar Avula>ping facebook.com

```

4) Nessus on my device.

A) Actually I have used metasploitable server on my virtual box to scan as there are not much interesting facts about the my laptop or my devices. Hope you accept this.



Nessus Essentials / Folders / View

https://localhost:8834/#/scans/reports/16/vulnerabilities

nessusEssentials

ScansSettings

Rushik181

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Scanners

TENABLE

Community

Research

Tenable News

CVE-2020-5902: Critical Vulnerability in FS BIG-IP...
[Read More](#)

Metasploitable

Back to My Scans

Configure

Hosts1

Vulnerabilities9

History1

FilterSearch Vulnerabilities9 Vulnerabilities

| Sev | Name | Plugin ID: 11356 | Family | Count |
|----------|---|------------------|-------------------|-------|
| CRITICAL | NFS Exported Share Information Disclosure | | RPC | 1 |
| INFO | Nessus SYN scanner | | Port scanners | 25 |
| INFO | RPC Services Enumeration | | Service detection | 10 |
| INFO | SMB (Multiple Issues) | | Windows | 5 |
| INFO | RPC (Multiple Issues) | | RPC | 2 |
| INFO | NFS Share Export List | | RPC | 1 |
| INFO | Samba Server Detection | | Service detection | 1 |
| INFO | Samba Version | | Misc. | 1 |
| INFO | WMI Not Available | | Windows | 1 |

Scan Details

Policy: Basic Network Scan
Status: Running
Scanner: Local Scanner
Start: Today at 5:57 PM

Vulnerabilities

Critical

High

Medium

Low

Info

nessusEssentials

ScansSettings

Rushik181

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Scanners

TENABLE

Community

Research

Tenable News

CVE-2020-5902: Critical Vulnerability in FS BIG-IP...
[Read More](#)

Metasploitable / Plugin #61708

Back to Vulnerabilities

Configure

Audit Trail

Launch

Report

Export

Hosts1

Vulnerabilities70

Remediations4

History1

CRITICAL

VNC Server 'password' Password

<>

Plugin Details

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

Output

Nessus logged in using a password of "password".

| Port | Hosts |
|------------------|---------------|
| 5900 / tcp / vnc | 192.168.2.177 |

Risk Information

Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

Default Account: true
Exploited by Nessus: true