Assignment Day 4 | 23rd August 2020

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

1. Ibm.com
2. Wipro.com

Solution:

1. **Ibm.com**

   To get the mail server we have to run the following command

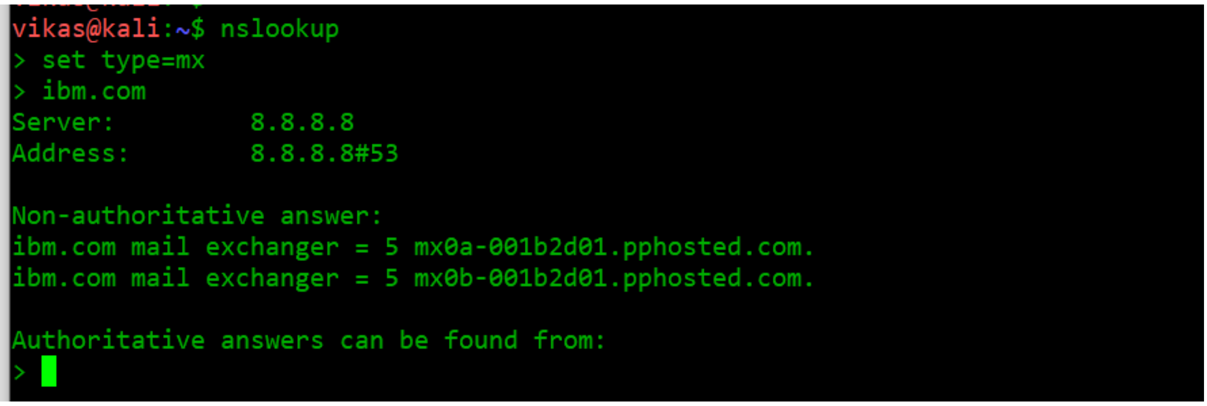
   $nslookup

   Now we have entered into nslookup prompt and set the lookup type as mx.

   > set type=mx

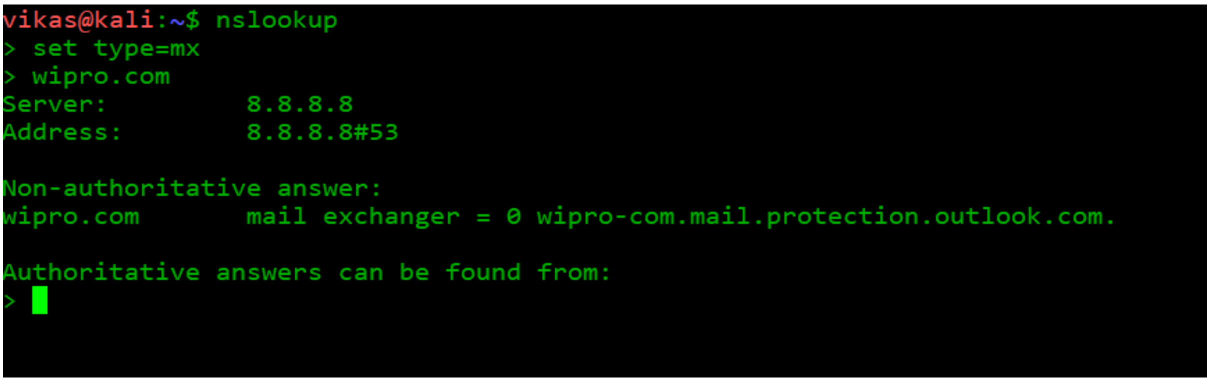
   After setting lookup type we can now enter the preferred domain to lookup.

   > ibm.com



```
vikas@kali:~$ nslookup
> set type=mx
> ibm.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
ibm.com mail exchanger = 5 mx0a-001b2d01.pphosted.com.
ibm.com mail exchanger = 5 mx0b-001b2d01.pphosted.com.

Authoritative answers can be found from:
> 
```

2. **Wipro.com**



```
vikas@kali:~$ nslookup
> set type=mx
> wipro.com
Server:         8.8.8.8
Address:        8.8.8.8#53

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

Authoritative answers can be found from:
> 
```

$ nslookup

> set type=mx

> wipro.com

Server: 8.8.8.8

Address: 8.8.8.8#53

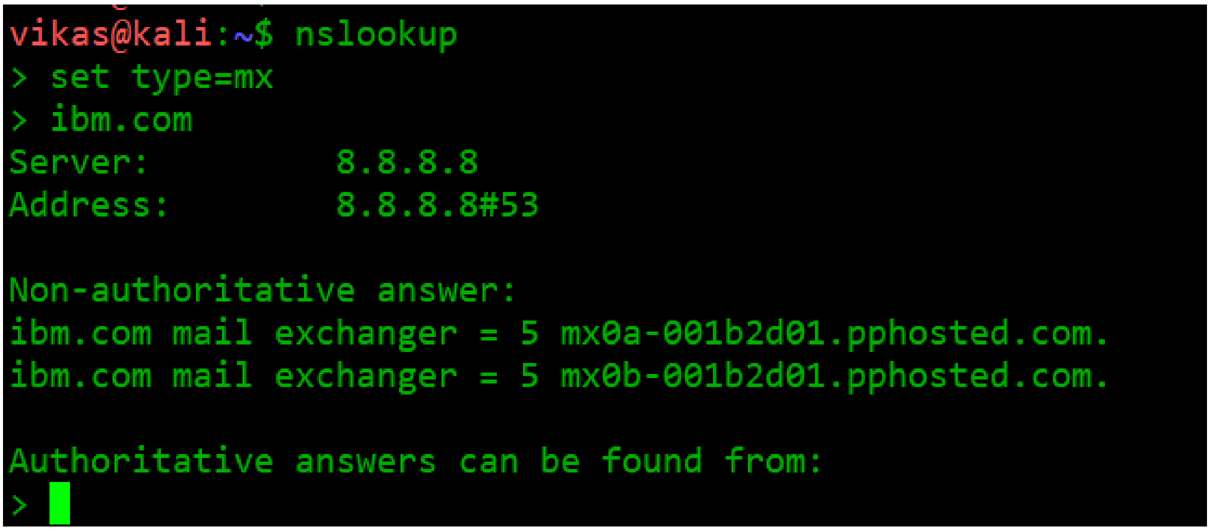
Non-authoritative answer:

wipro.com   mail exchanger = 0 wipro-com.mail.protection.outlook.com.

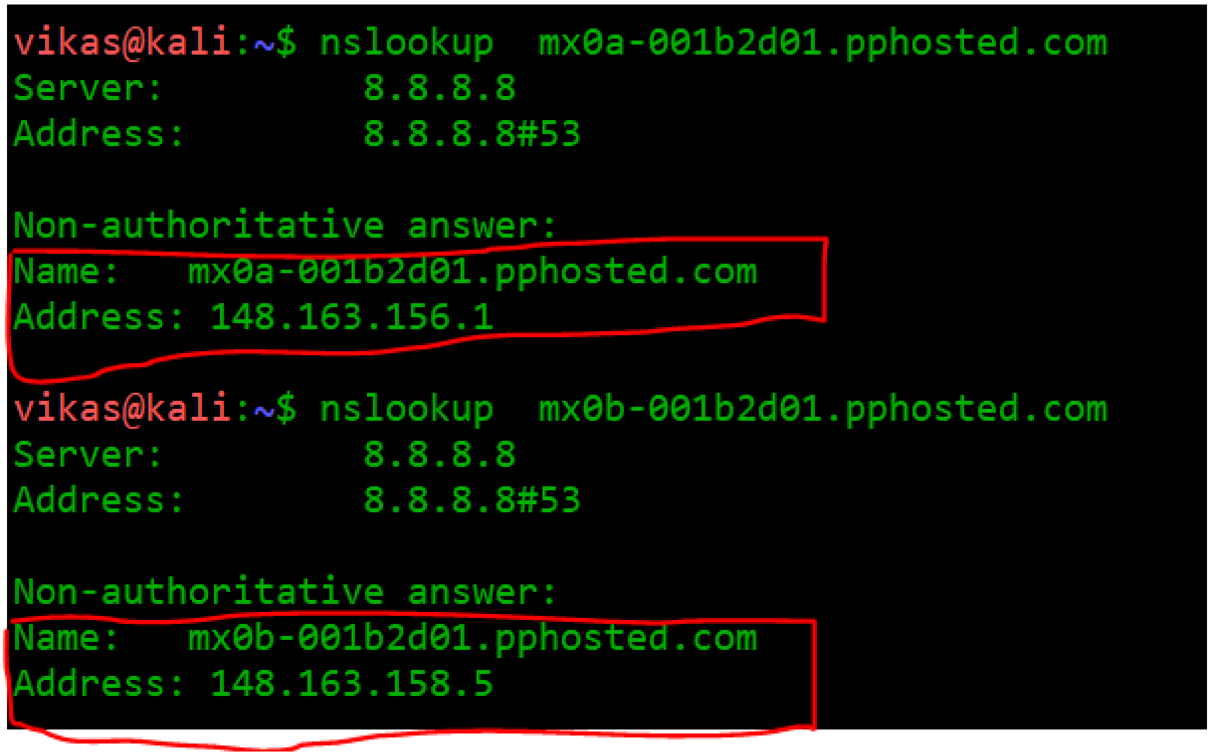
Authoritative answers can be found from:

Question 2: Find the locations, where these email servers are hosted.

1.ibm.com



```
vikas@kali:~$ nslookup
> set type=mx
> ibm.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
ibm.com mail exchanger = 5 mx0a-001b2d01.pphosted.com.
ibm.com mail exchanger = 5 mx0b-001b2d01.pphosted.com.

Authoritative answers can be found from:
> 
```



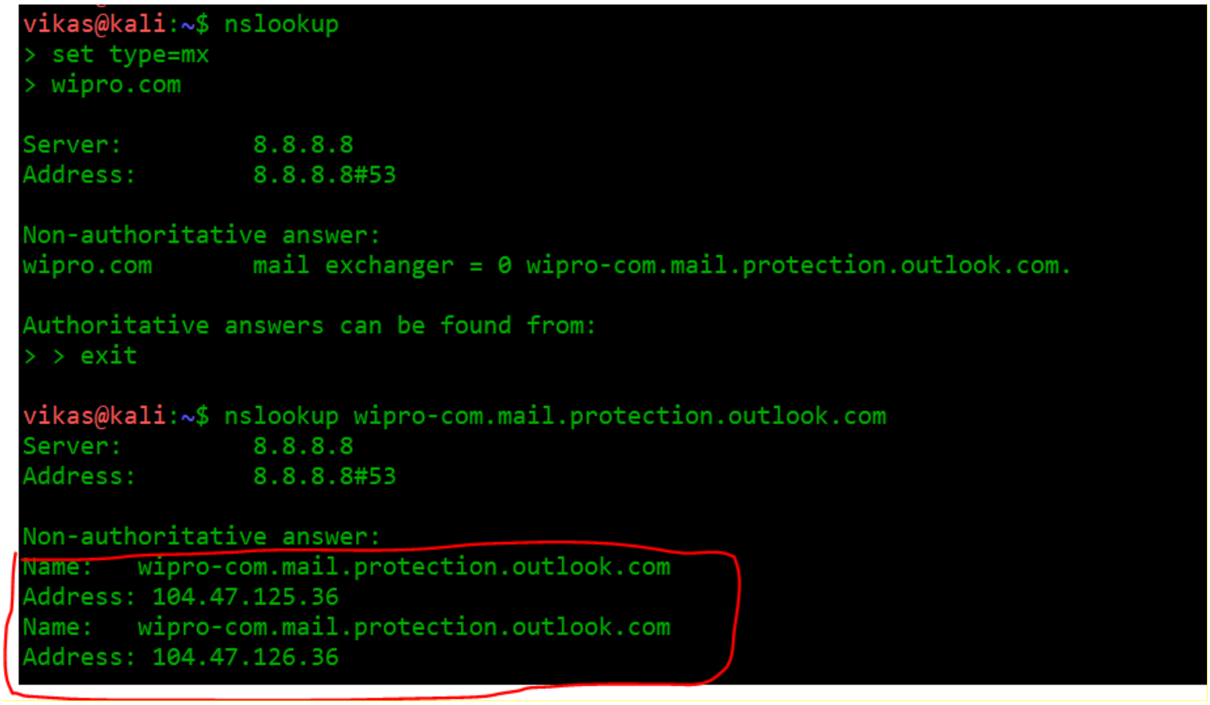
```
vikas@kali:~$ nslookup  mx0a-001b2d01.pphosted.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   mx0a-001b2d01.pphosted.com
Address: 148.163.156.1

vikas@kali:~$ nslookup  mx0b-001b2d01.pphosted.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   mx0b-001b2d01.pphosted.com
Address: 148.163.158.5
```

Now we can use look up command to find the location of these server

```
vikas@kali:~$ whois  148.163.156.1


NetRange:       148.163.128.0 - 148.163.159.255

CIDR:           148.163.128.0/19

NetName:        PROOFPOINT-NET-NORTH-AMERICA

NetHandle:      NET-148-163-128-0-1

Parent:         NET148 (NET-148-0-0-0-0)

NetType:        Direct Allocation

OriginAS:       AS16509, AS22843, AS13916, AS26211

Organization:   Proofpoint, Inc. (PROOF)

RegDate:        2014-06-13

Updated:        2020-05-29
```

```
OrgName:       Proofpoint, Inc.
OrgId:         PROOF
Address:       892 Ross Drive
City:          Sunnyvale
StateProv:     CA
PostalCode:    94089
Country:       US
RegDate:       2007-10-16
Updated:       2020-03-17
Ref:           https://rdap.arin.net/registry/entity/PROOF


OrgAbuseHandle: PAA19-ARIN
OrgAbuseName:   Proofpoint ARIN Abuse
OrgAbusePhone:  +1-801-748-4494
OrgAbuseEmail:  abuse@proofpoint.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/PAA19-ARIN

OrgTechHandle: NETWO2061-ARIN
OrgTechName:   Network Operations
OrgTechPhone:  +1-408-517-4710
OrgTechEmail:  arin-management@proofpoint.com
OrgTechRef:    https://rdap.arin.net/registry/entity/NETWO2061-ARIN
```

2.wipro.com



```
vikas@kali:~$ nslookup
> set type=mx
> wipro.com

Server:         8.8.8.8
Address:        8.8.8.8#53

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

Authoritative answers can be found from:
> > exit

vikas@kali:~$ nslookup wipro-com.mail.protection.outlook.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   wipro-com.mail.protection.outlook.com
Address: 104.47.125.36
Name:   wipro-com.mail.protection.outlook.com
Address: 104.47.126.36
```

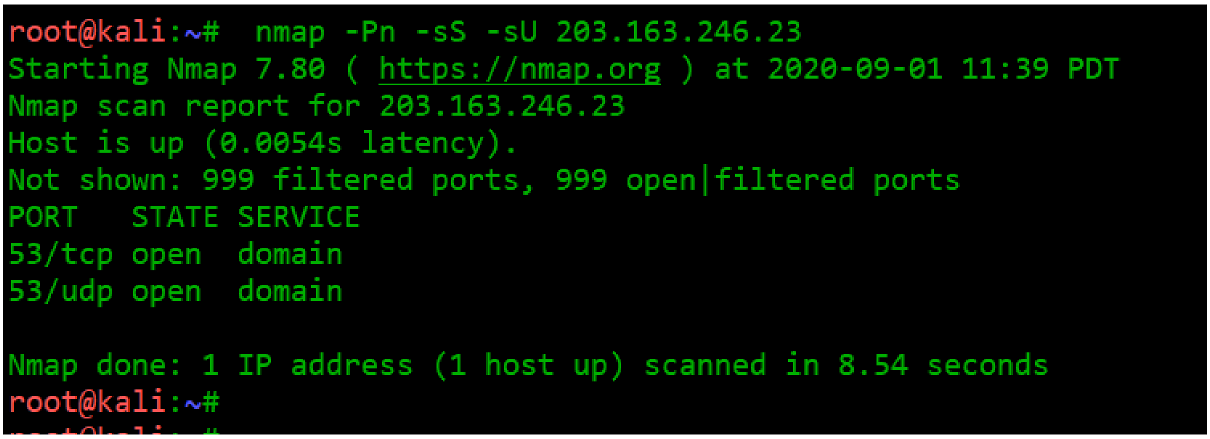
For location we use whois command

```
vikas@kali:~$ whois 104.47.125.36

NetRange:       104.40.0.0 - 104.47.255.255

CIDR:           104.40.0.0/13

NetName:        MSFT

NetHandle:      NET-104-40-0-0-1

Parent:         NET104 (NET-104-0-0-0-0)

NetType:        Direct Assignment

OriginAS:

Organization:   Microsoft Corporation (MSFT)

RegDate:        2014-05-07

Updated:        2014-05-07

Ref:            https://rdap.arin.net/registry/ip/104.40.0.0
```

```
OrgName:       Microsoft Corporation

OrgId:         MSFT

Address:       One Microsoft Way

City:          Redmond

StateProv:     WA

PostalCode:    98052

Country:       US

RegDate:       1998-07-10

Updated:       2017-01-28

Comment:       To report suspected security issues specific to traffic emanating from
Microsoft online services, including the distribution of malicious content or other illicit or
illegal material through a Microsoft online service, please submit reports to:

Comment:       * https://cert.microsoft.com.

Comment:

Comment:       For SPAM and other abuse issues, such as Microsoft Accounts, please
contact:

Comment:       * abuse@microsoft.com.

Comment:

Comment:       To report security vulnerabilities in Microsoft products and services, please
contact:

Comment:       * secure@microsoft.com.

Comment:

Comment:       For legal and law enforcement-related requests, please contact:

Comment:       * msndcc@microsoft.com

Comment:

Comment:       For routing, peering or DNS issues, please

Comment:       contact:

Comment:       * IOC@microsoft.com

Ref:           https://rdap.arin.net/registry/entity/MSFT
```

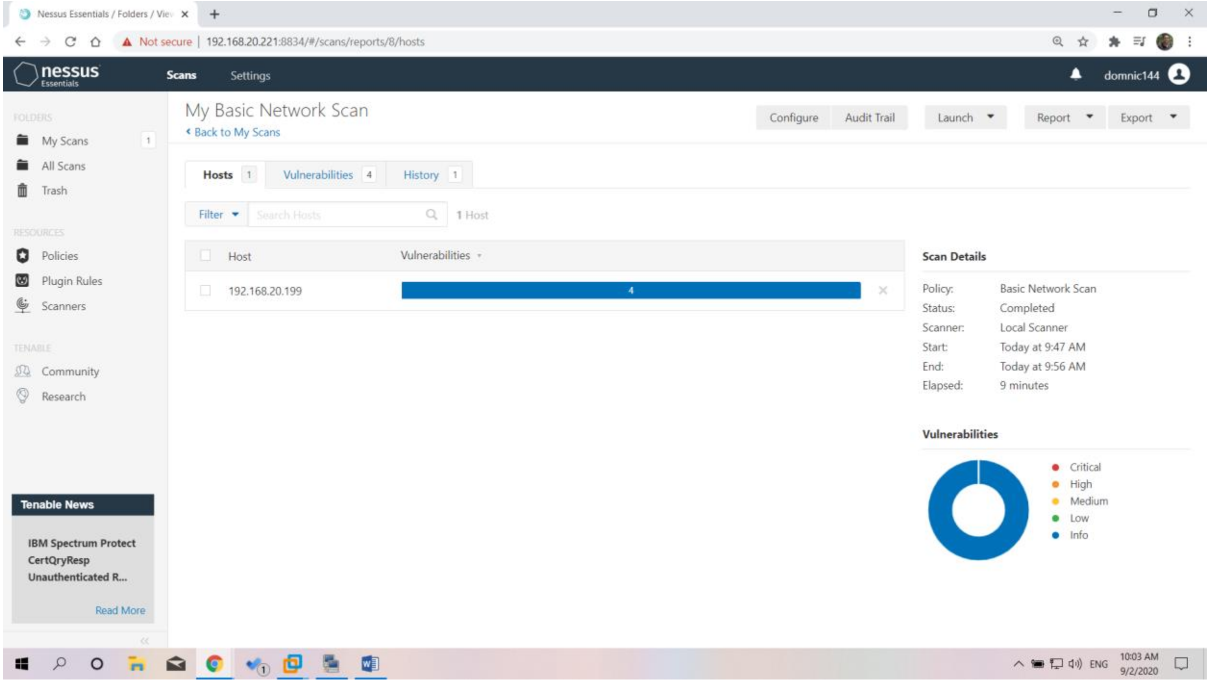
```
OrgAbuseHandle: MAC74-ARIN

OrgAbuseName:   Microsoft Abuse Contact

OrgAbusePhone:  +1-425-882-8080

OrgAbuseEmail:  abuse@microsoft.com

OrgAbuseRef:    https://rdap.arin.net/registry/entity/MAC74-ARIN


OrgTechHandle: MRPD-ARIN

OrgTechName:   Microsoft Routing, Peering, and DNS

OrgTechPhone:  +1-425-882-8080

OrgTechEmail:  IOC@microsoft.com

OrgTechRef:    https://rdap.arin.net/registry/entity/MRPD-ARIN
```

Question 3: Scan and find out port numbers open 203.163.246.23.



```
root@kali:~#  nmap -Pn -sS -sU 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-01 11:39 PDT
Nmap scan report for 203.163.246.23
Host is up (0.0054s latency).
Not shown: 999 filtered ports, 999 open|filtered ports
PORT    STATE SERVICE
53/tcp open   domain
53/udp open   domain

Nmap done: 1 IP address (1 host up) scanned in 8.54 seconds
root@kali:~#
```

Question 4: Install nessus in a VM and scan your laptop/desktop for CVE



My Basic Network Scan

‹ Back to My Scans

Host	Vulnerabilities
192.168.20.199	4

Scan Details

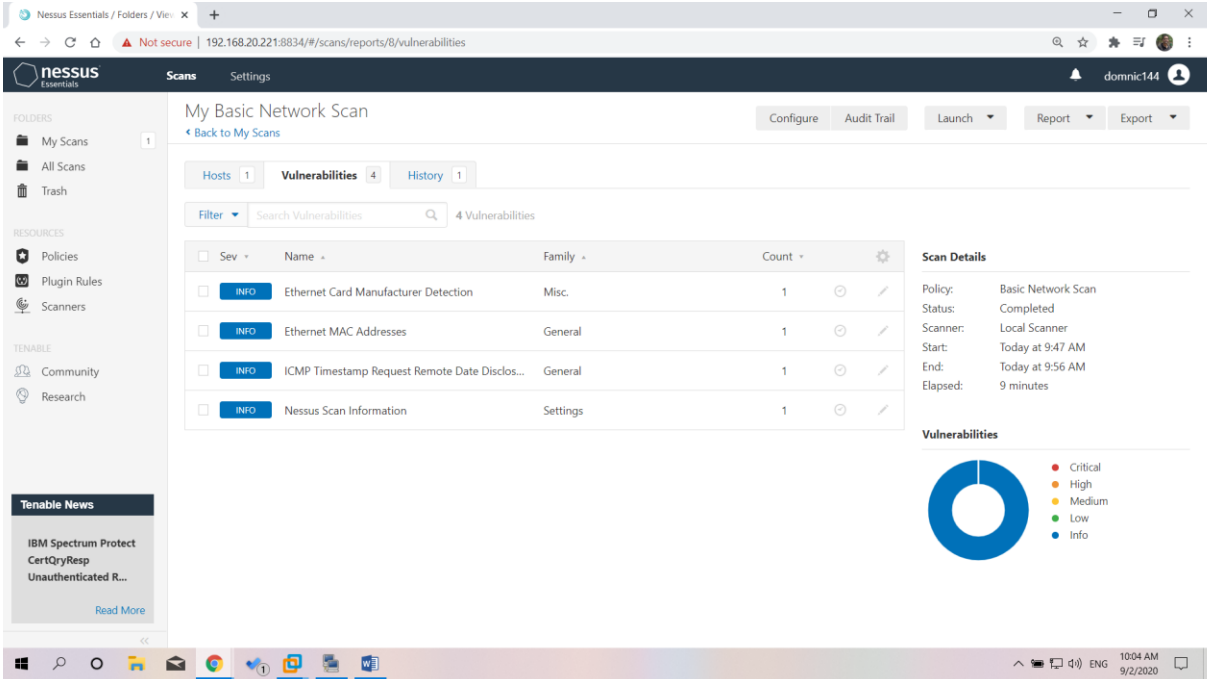
Policy:	Basic Network Scan
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 9:47 AM
End:	Today at 9:56 AM
Elapsed:	9 minutes

Vulnerabilities

Tenable News

IBM Spectrum Protect CertQryResp Unauthenticated R...

Read More



My Basic Network Scan

‹ Back to My Scans

Sev	Name	Family	Count
INFO	Ethernet Card Manufacturer Detection	Misc.	1
INFO	Ethernet MAC Addresses	General	1
INFO	ICMP Timestamp Request Remote Date Disclos...	General	1
INFO	Nessus Scan Information	Settings	1

Scan Details

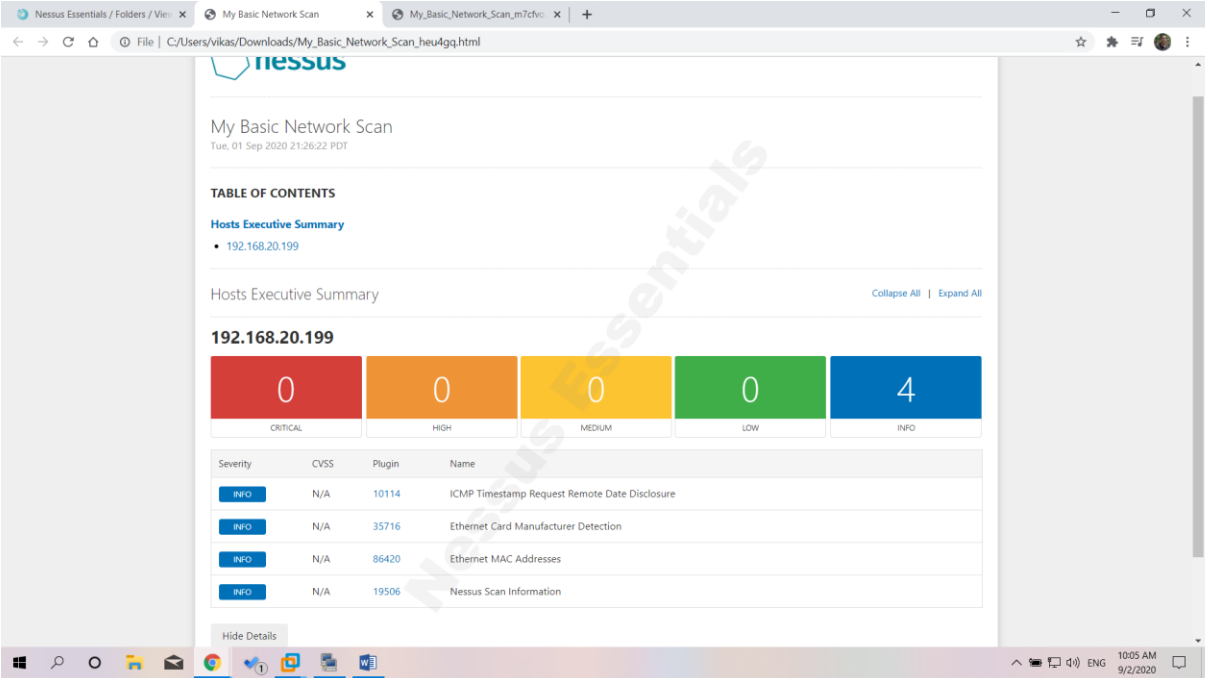
Policy:	Basic Network Scan
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 9:47 AM
End:	Today at 9:56 AM
Elapsed:	9 minutes

Vulnerabilities

Tenable News

IBM Spectrum Protect CertQryResp Unauthenticated R...

Read More


Nessus Essentials / Folders / View
My Basic Network Scan
My_Basic_Network_Scan_m7cfvo
File | C:/Users/vikas/Downloads/My_Basic_Network_Scan_heu4gq.html
ENG
10:05 AM
9/2/2020

nessus

My Basic Network Scan

Tue, 01 Sep 2020 21:26:22 PDT

TABLE OF CONTENTS

Hosts Executive Summary

- 192.168.20.199

Hosts Executive Summary

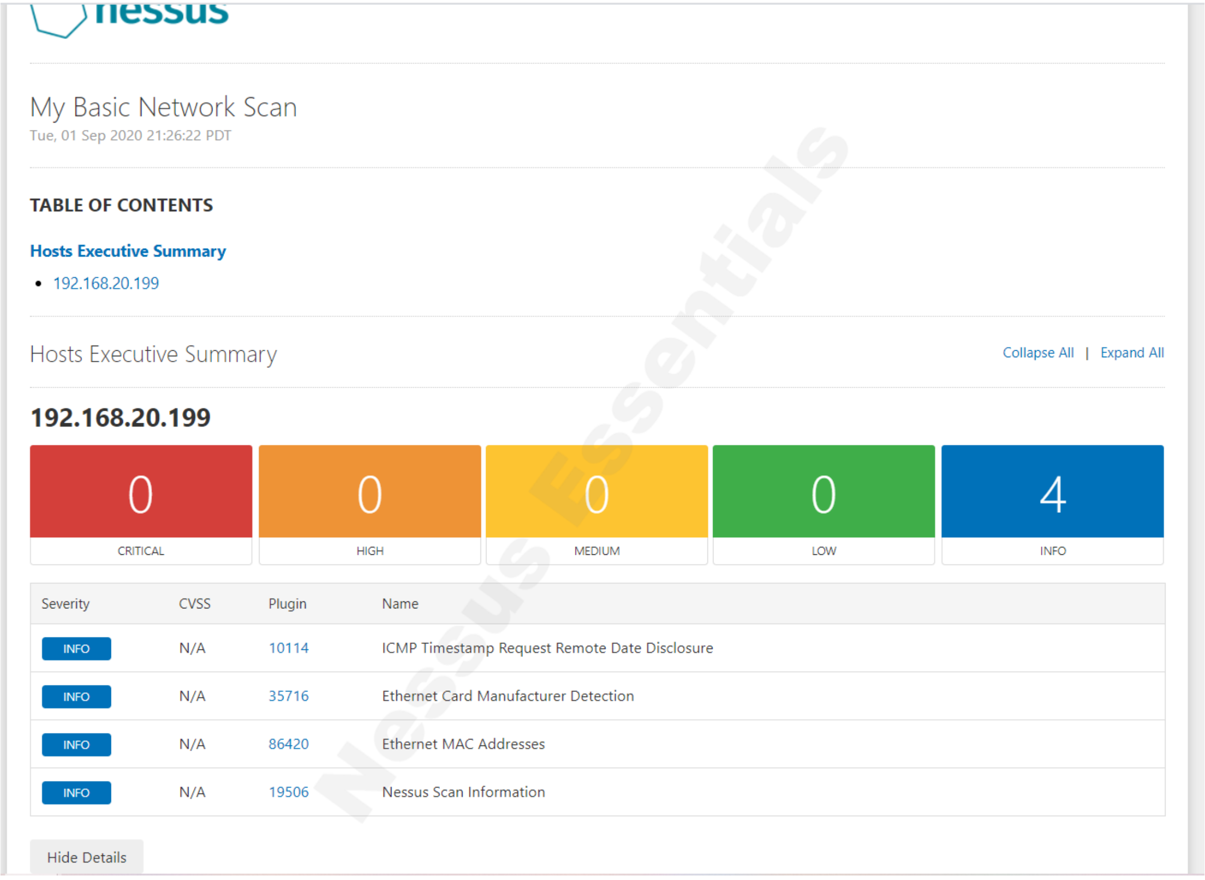
Collapse All | Expand All

192.168.20.199

0	0	0	0	4
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS	Plugin	Name
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	19506	Nessus Scan Information

Hide Details


nessus

My Basic Network Scan

Tue, 01 Sep 2020 21:26:22 PDT

TABLE OF CONTENTS

Hosts Executive Summary

- 192.168.20.199

Hosts Executive Summary

Collapse All | Expand All

192.168.20.199

0	0	0	0	4
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS	Plugin	Name
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	19506	Nessus Scan Information

Hide Details