Assignment: Day 4

Question 1:

Find out the mail servers of the following domain:

www.Ibm.com

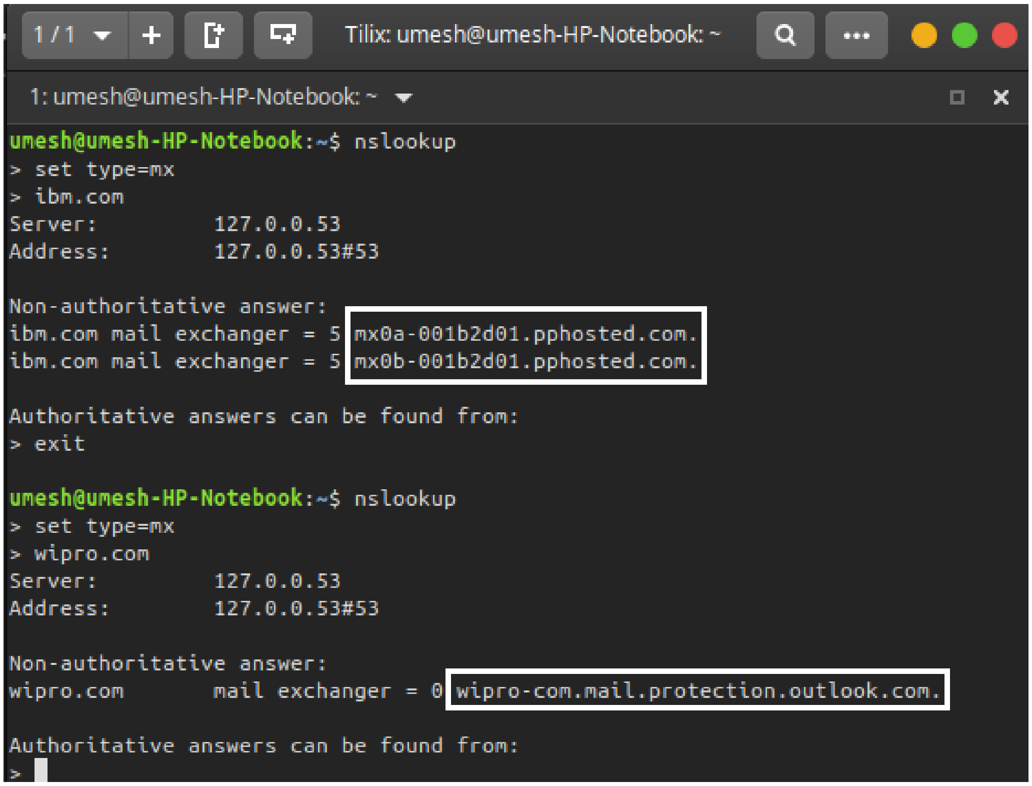
www.Wipro.com

Answer:

Note: Used Ubuntu (Debian) OS

Step1: Turn ON your Operating System.

Step2: Press ctrl+alt+T (to open Terminal) or click on terminal icon and open terminal



1 / 1
Tilix: umesh@umesh-HP-Notebook: ~
1: umesh@umesh-HP-Notebook: ~

```
umesh@umesh-HP-Notebook:~$ nslookup
> set type=mx
> ibm.com
Server:         127.0.0.53
Address:        127.0.0.53#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:
> exit

umesh@umesh-HP-Notebook:~$ nslookup
> set type=mx
> wipro.com
Server:         127.0.0.53
Address:        127.0.0.53#53

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

Authoritative answers can be found from:
>
```

Step3: type nslookup command

Step4: type set type=mx

Step5: type the domain names as specified.

Question2:

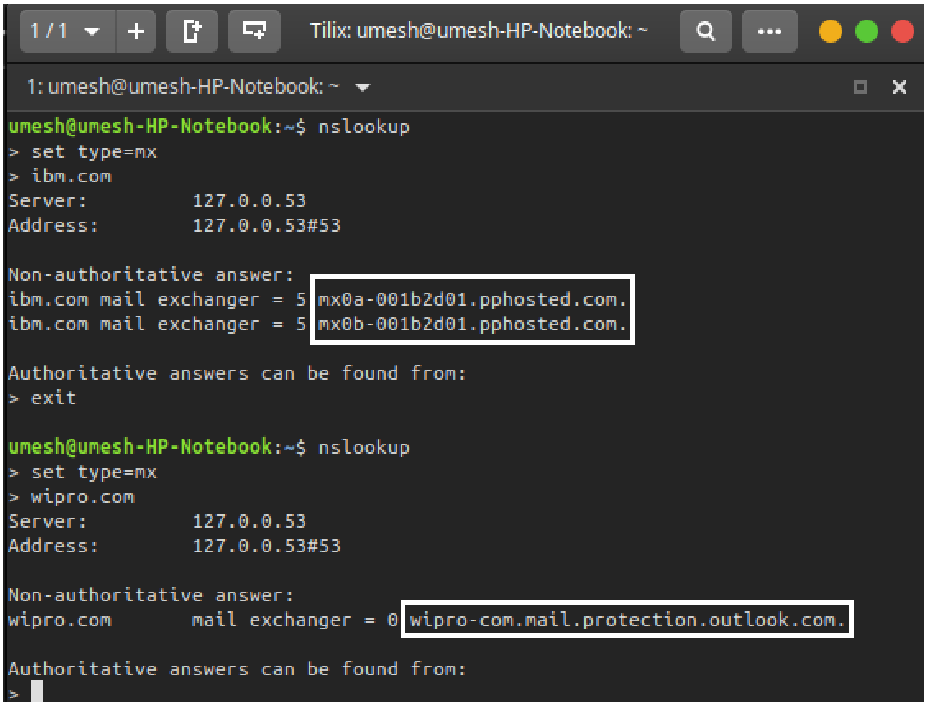
Find the location, where these email servers are hosted.

Answer:

Step1: Open Web browser.

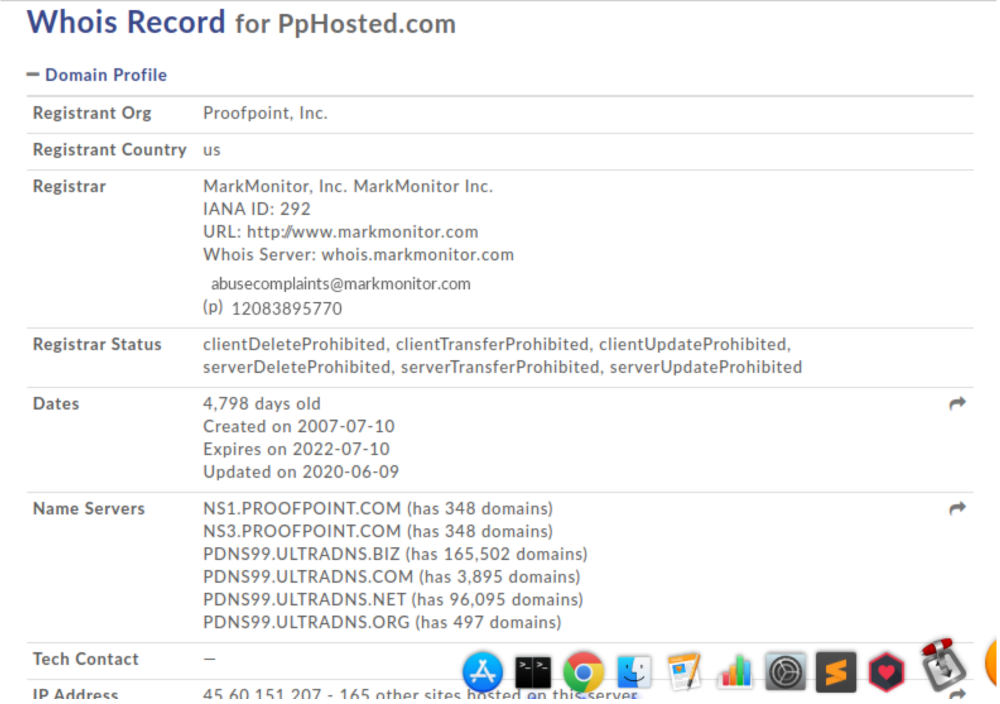
Step2: search for WhoisLookup

Step3: Copy mail exchanger and paste it in to find the location


1 / 1
Tilix: umesh@umesh-HP-Notebook: ~
1: umesh@umesh-HP-Notebook: ~

```
umesh@umesh-HP-Notebook:~$ nslookup
> set type=mx
> ibm.com
Server:         127.0.0.53
Address:        127.0.0.53#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:
> exit

umesh@umesh-HP-Notebook:~$ nslookup
> set type=mx
> wipro.com
Server:         127.0.0.53
Address:        127.0.0.53#53

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

Authoritative answers can be found from:
> 
```

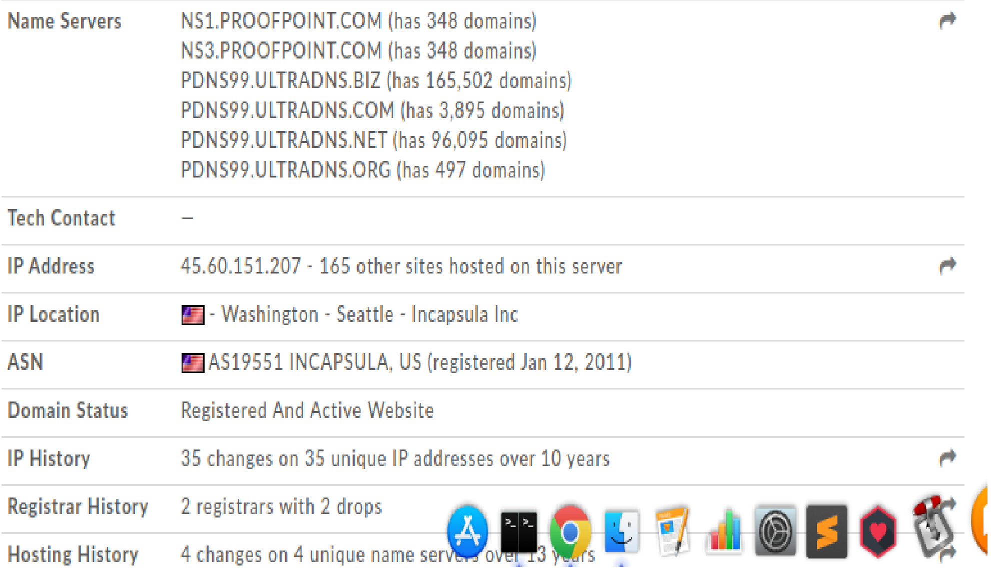
Address 1: (IBM)



Whois Record for PpHosted.com

— Domain Profile

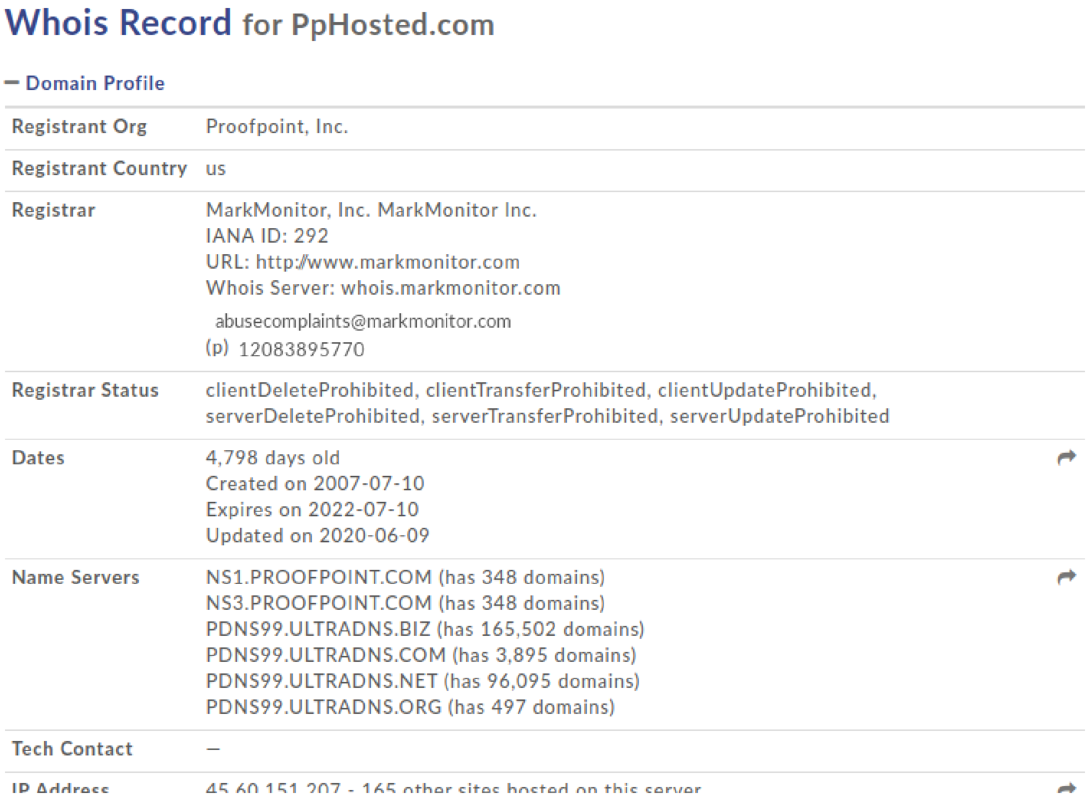
Registrant Org	Proofpoint, Inc.
Registrant Country	us
Registrar	MarkMonitor, Inc. MarkMonitor Inc. IANA ID: 292 URL: http://www.markmonitor.com Whois Server: whois.markmonitor.com abusecomplaints@markmonitor.com (p) 12083895770
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited
Dates	4,798 days old Created on 2007-07-10 Expires on 2022-07-10 Updated on 2020-06-09
Name Servers	NS1.PROOFPOINT.COM (has 348 domains) NS3.PROOFPOINT.COM (has 348 domains) PDNS99.ULTRADNS.BIZ (has 165,502 domains) PDNS99.ULTRADNS.COM (has 3,895 domains) PDNS99.ULTRADNS.NET (has 96,095 domains) PDNS99.ULTRADNS.ORG (has 497 domains)
Tech Contact	–
IP Address	45.60.151.207 - 165 other sites hosted on this server



Name Servers	NS1.PROOFPOINT.COM (has 348 domains) NS3.PROOFPOINT.COM (has 348 domains) PDNS99.ULTRADNS.BIZ (has 165,502 domains) PDNS99.ULTRADNS.COM (has 3,895 domains) PDNS99.ULTRADNS.NET (has 96,095 domains) PDNS99.ULTRADNS.ORG (has 497 domains)
Tech Contact	–
IP Address	45.60.151.207 - 165 other sites hosted on this server

IP Location	🇺🇸 - Washington - Seattle - Incapsula Inc
ASN	🇺🇸 AS19551 INCAPSULA, US (registered Jan 12, 2011)
Domain Status	Registered And Active Website
IP History	35 changes on 35 unique IP addresses over 10 years
Registrar History	2 registrars with 2 drops
Hosting History	4 changes on 4 unique name servers over 13 years

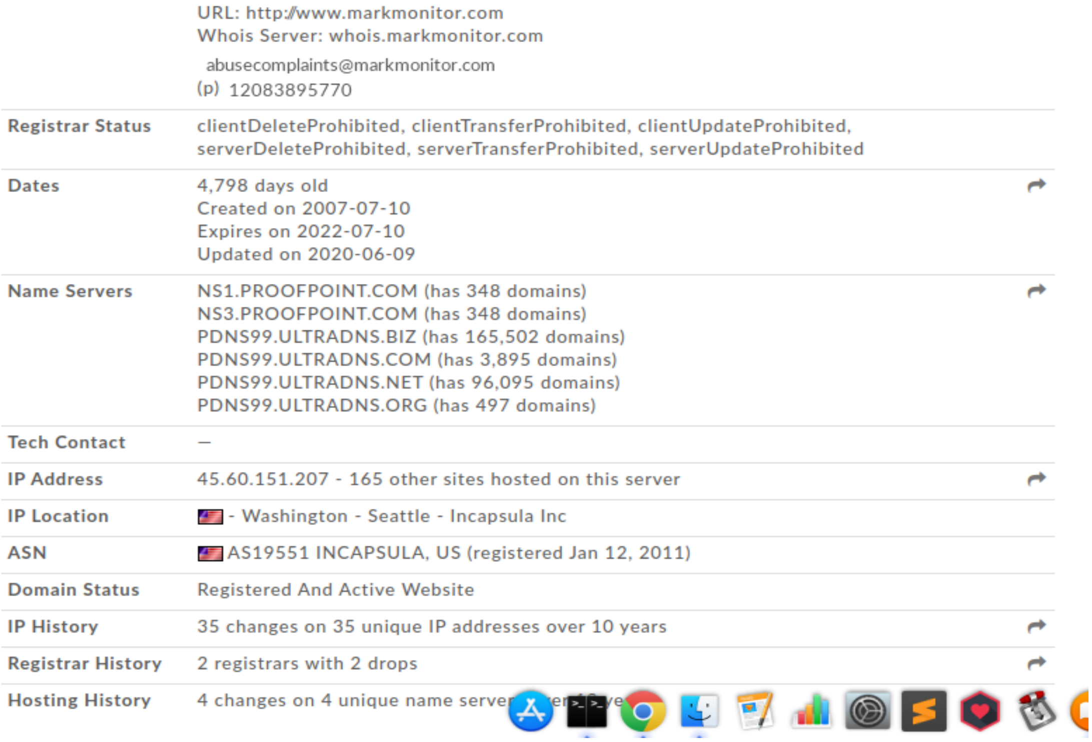
Address 2: (IBM)



Whois Record for PpHosted.com

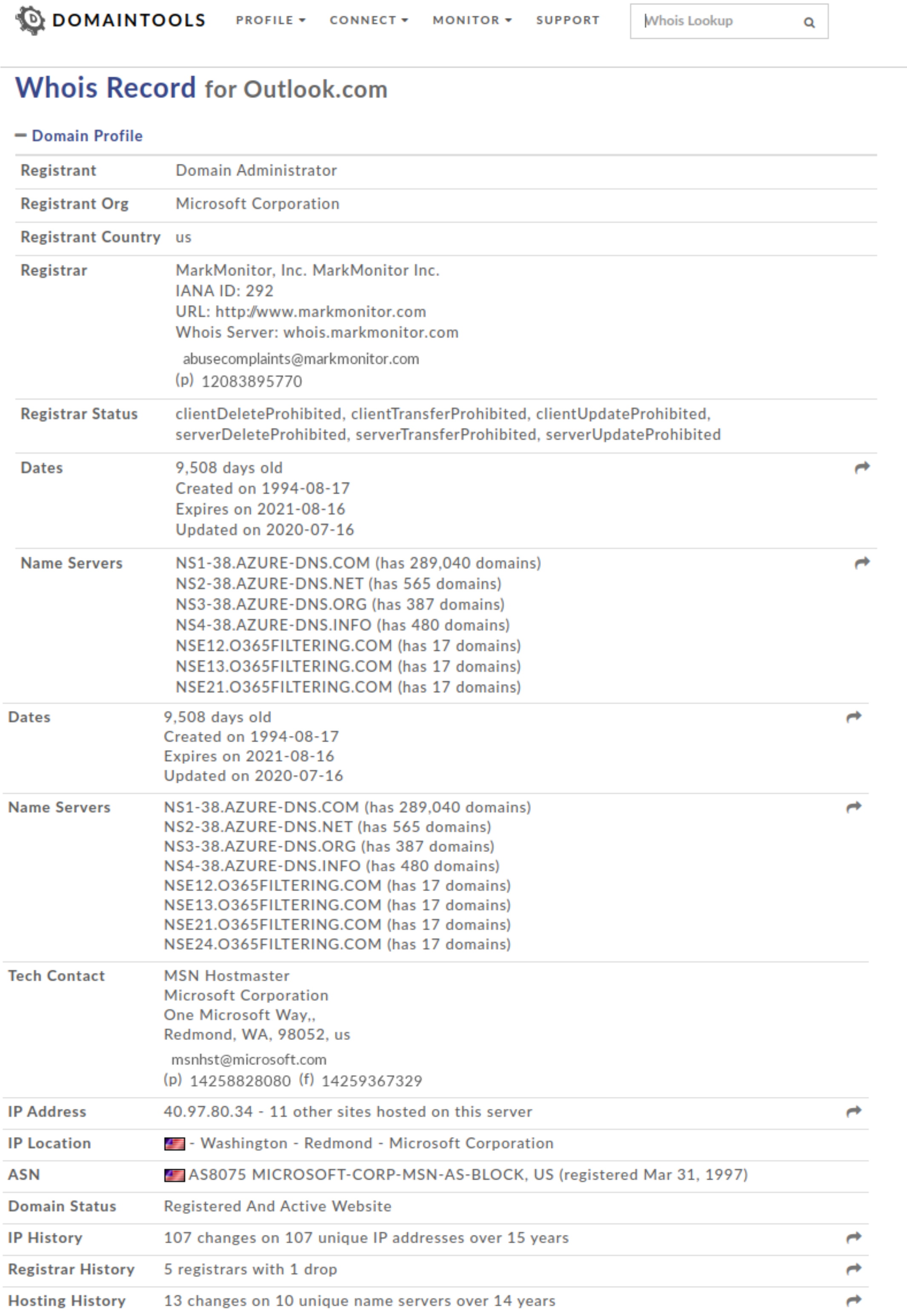
— Domain Profile

Registrant Org	Proofpoint, Inc.
Registrant Country	us
Registrar	MarkMonitor, Inc. MarkMonitor Inc. IANA ID: 292 URL: http://www.markmonitor.com Whois Server: whois.markmonitor.com abusecomplaints@markmonitor.com (p) 12083895770
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited
Dates	4,798 days old Created on 2007-07-10 Expires on 2022-07-10 Updated on 2020-06-09
Name Servers	NS1.PROOFPOINT.COM (has 348 domains) NS3.PROOFPOINT.COM (has 348 domains) PDNS99.ULTRADNS.BIZ (has 165,502 domains) PDNS99.ULTRADNS.COM (has 3,895 domains) PDNS99.ULTRADNS.NET (has 96,095 domains) PDNS99.ULTRADNS.ORG (has 497 domains)
Tech Contact	—
IP Address	45.60.151.207 - 165 other sites hosted on this server



	URL: http://www.markmonitor.com Whois Server: whois.markmonitor.com abusecomplaints@markmonitor.com (p) 12083895770
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited
Dates	4,798 days old Created on 2007-07-10 Expires on 2022-07-10 Updated on 2020-06-09
Name Servers	NS1.PROOFPOINT.COM (has 348 domains) NS3.PROOFPOINT.COM (has 348 domains) PDNS99.ULTRADNS.BIZ (has 165,502 domains) PDNS99.ULTRADNS.COM (has 3,895 domains) PDNS99.ULTRADNS.NET (has 96,095 domains) PDNS99.ULTRADNS.ORG (has 497 domains)
Tech Contact	—
IP Address	45.60.151.207 - 165 other sites hosted on this server
IP Location	🇺🇸 - Washington - Seattle - Incapsula Inc
ASN	🇺🇸 AS19551 INCAPSULA, US (registered Jan 12, 2011)
Domain Status	Registered And Active Website
IP History	35 changes on 35 unique IP addresses over 10 years
Registrar History	2 registrars with 2 drops
Hosting History	4 changes on 4 unique name serve

Address 3: (Wipro)



Whois Record for Outlook.com

— Domain Profile

Registrant	Domain Administrator
Registrant Org	Microsoft Corporation
Registrant Country	us
Registrar	MarkMonitor, Inc. MarkMonitor Inc. IANA ID: 292 URL: http://www.markmonitor.com Whois Server: whois.markmonitor.com abusecomplaints@markmonitor.com (p) 12083895770
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited
Dates	9,508 days old Created on 1994-08-17 Expires on 2021-08-16 Updated on 2020-07-16
Name Servers	NS1-38.AZURE-DNS.COM (has 289,040 domains) NS2-38.AZURE-DNS.NET (has 565 domains) NS3-38.AZURE-DNS.ORG (has 387 domains) NS4-38.AZURE-DNS.INFO (has 480 domains) NSE12.O365FILTERING.COM (has 17 domains) NSE13.O365FILTERING.COM (has 17 domains) NSE21.O365FILTERING.COM (has 17 domains)
Dates	9,508 days old Created on 1994-08-17 Expires on 2021-08-16 Updated on 2020-07-16
Name Servers	NS1-38.AZURE-DNS.COM (has 289,040 domains) NS2-38.AZURE-DNS.NET (has 565 domains) NS3-38.AZURE-DNS.ORG (has 387 domains) NS4-38.AZURE-DNS.INFO (has 480 domains) NSE12.O365FILTERING.COM (has 17 domains) NSE13.O365FILTERING.COM (has 17 domains) NSE21.O365FILTERING.COM (has 17 domains) NSE24.O365FILTERING.COM (has 17 domains)
Tech Contact	MSN Hostmaster Microsoft Corporation One Microsoft Way,, Redmond, WA, 98052, us msnhst@microsoft.com (p) 14258828080 (f) 14259367329
IP Address	40.97.80.34 - 11 other sites hosted on this server
IP Location	- Washington - Redmond - Microsoft Corporation
ASN	AS8075 MICROSOFT-CORP-MSN-AS-BLOCK, US (registered Mar 31, 1997)
Domain Status	Registered And Active Website
IP History	107 changes on 107 unique IP addresses over 15 years
Registrar History	5 registrars with 1 drop
Hosting History	13 changes on 10 unique name servers over 14 years

Question3:

Scan and find out the port number open 203.163.246.23

Answer:

For this question we have use nmap tool of Ubuntu

Step1: open terminal

Step2: type command nmap -Pn -p 1-65535 203.168.246.23

(-Pn to bypass Firewall)

Step3: All 1000 ports as filtered of above IP address

Question4:

Install Nessus in a VM and scan your laptop/desktop for CVE

Answer:

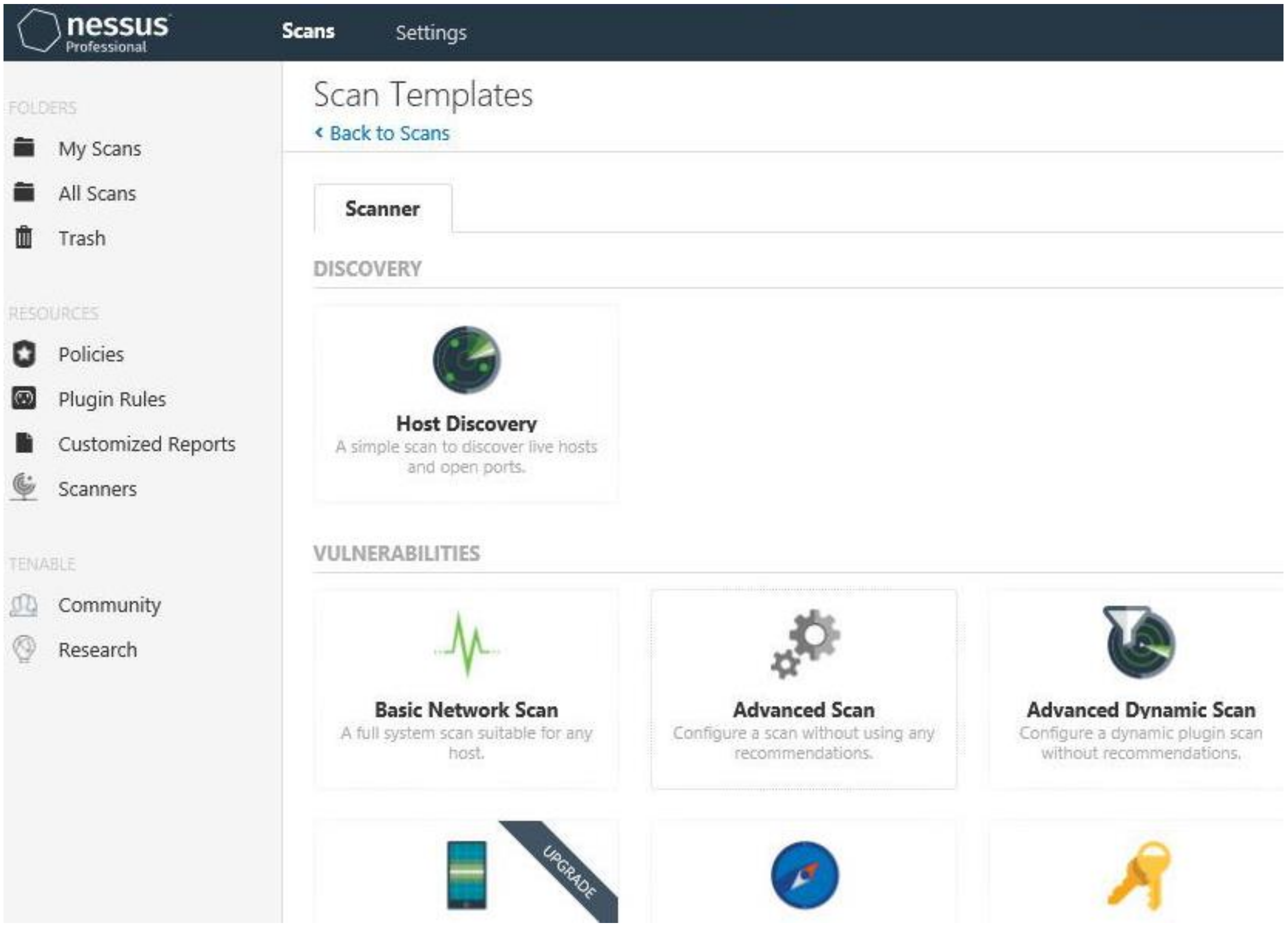
Step1: Open PenTester in VMware workstation

Step2: Install Google Chrome

Step3: Install Nessus

Step4: Create a new Scan

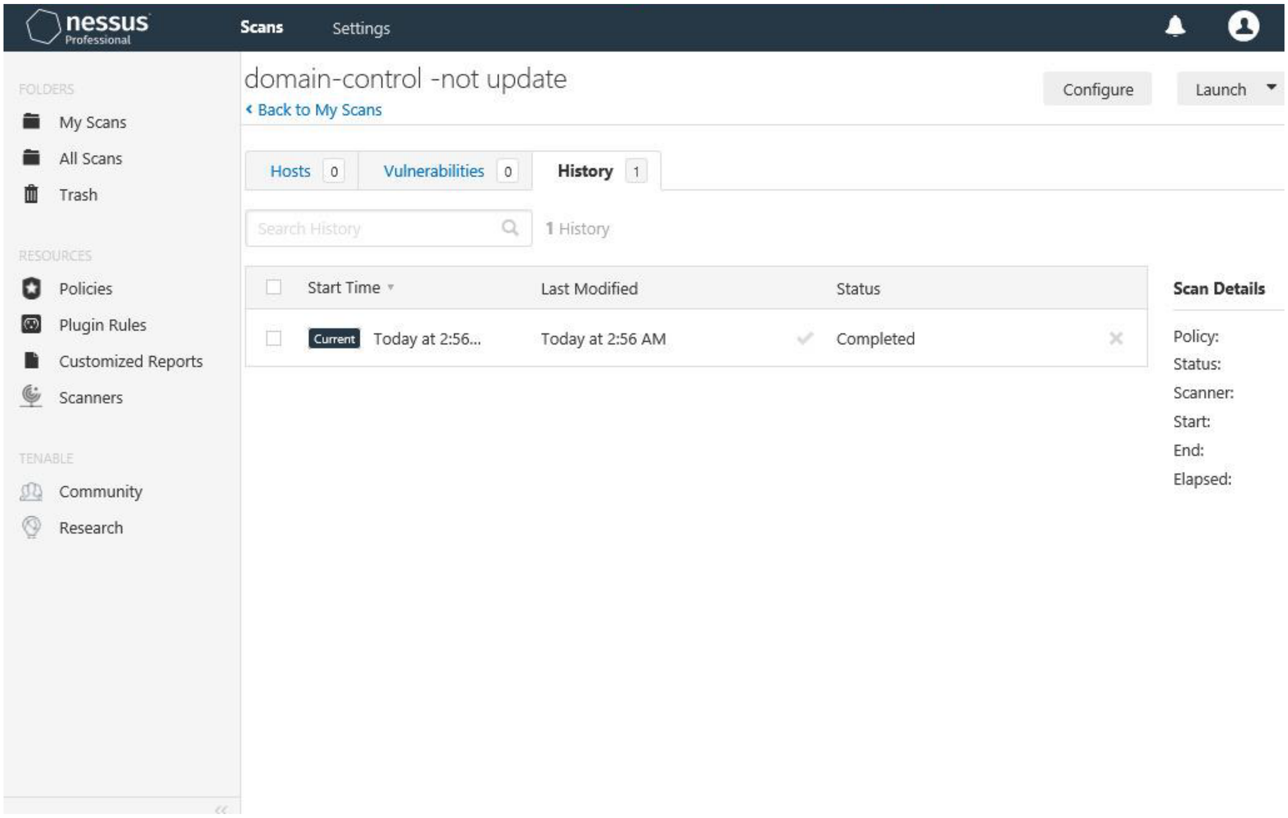
Step5: Click Advanced Scan



Step6: on Setting tab fill the domain and IP of Target

Step7: Click on credentials tab and select Windows

Step8: Fill the credentials & launch



domain-control -not update

□	Start Time	Last Modified		Status	
□	Current Today at 2:56...	Today at 2:56 AM	✓	Completed	✕

Scan Details

Policy:
Status:
Scanner:
Start:
End:
Elapsed: