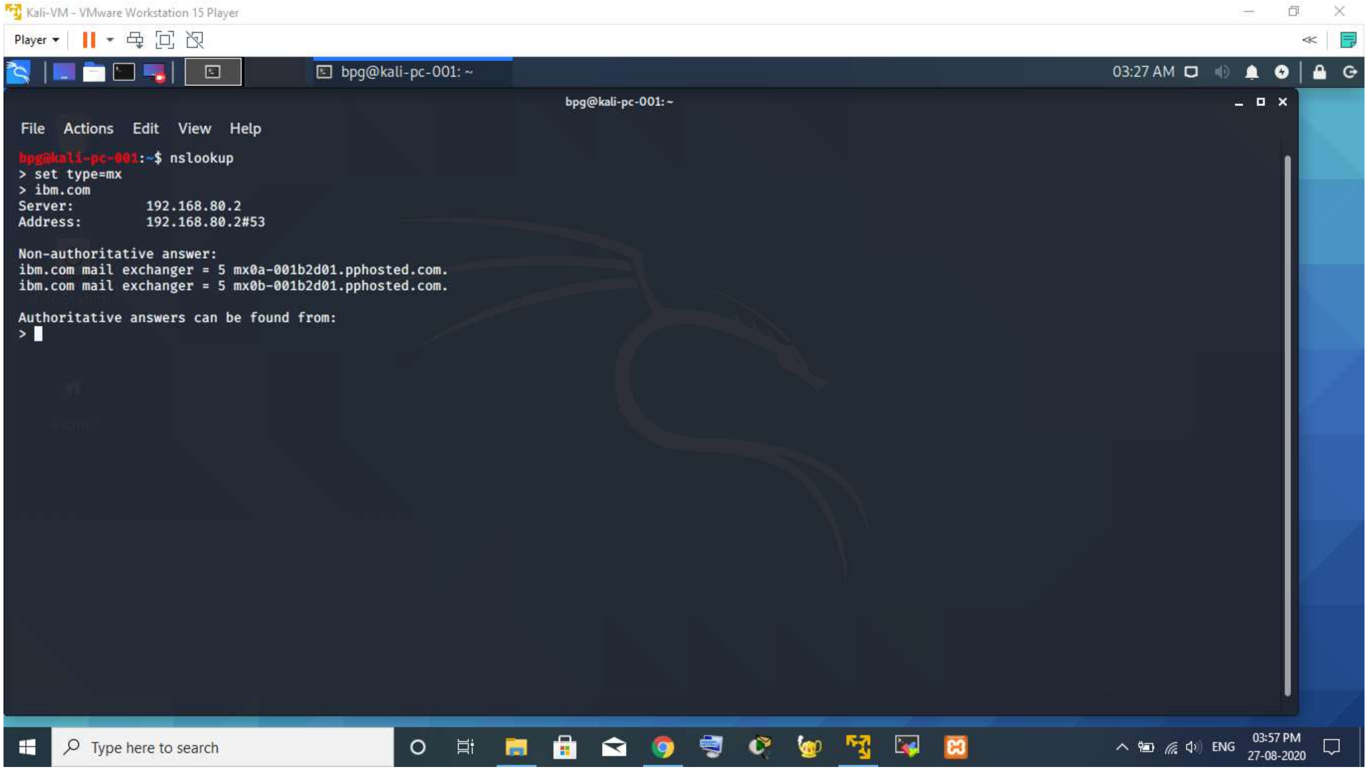
CyberSecurity Essentials Batch-1 | Day-4 Assignment

Question-1:-

Find out the mail servers of the following domain.

Ibm.com

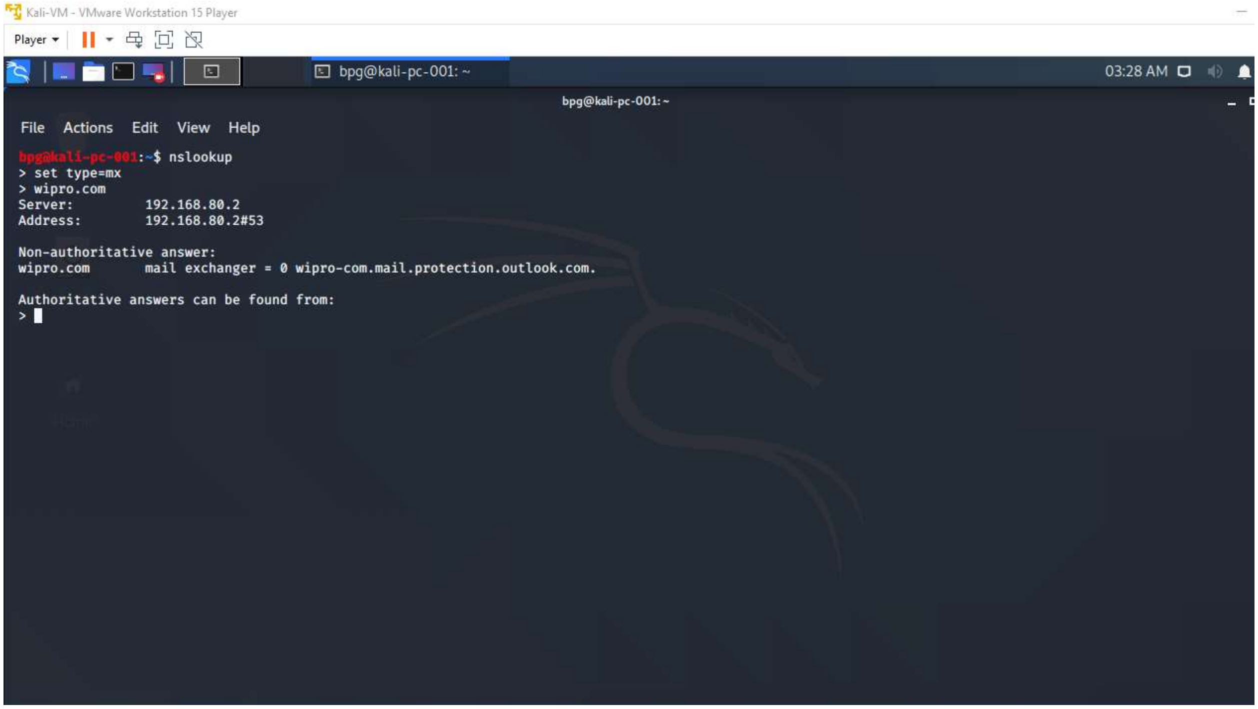
1. mx0a-001b2d01.pphosted.com
2. mx0b-001b2d01.pphosted.com



```
bpg@kali-pc-001:~$ nslookup
> set type=mx
> ibm.com
Server:         192.168.80.2
Address:        192.168.80.2#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:
> 
```

Wipro.com

1. wipro-com.mail.protection.outlook.com



Kali-VM - VMware Workstation 15 Player
Player
bpg@kali-pc-001: ~
03:28 AM
bpg@kali-pc-001: ~
File Actions Edit View Help

```
bpg@kali-pc-001:~$ nslookup
> set type=mx
> wipro.com
Server:         192.168.80.2
Address:        192.168.80.2#53

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

Authoritative answers can be found from:
> 
```

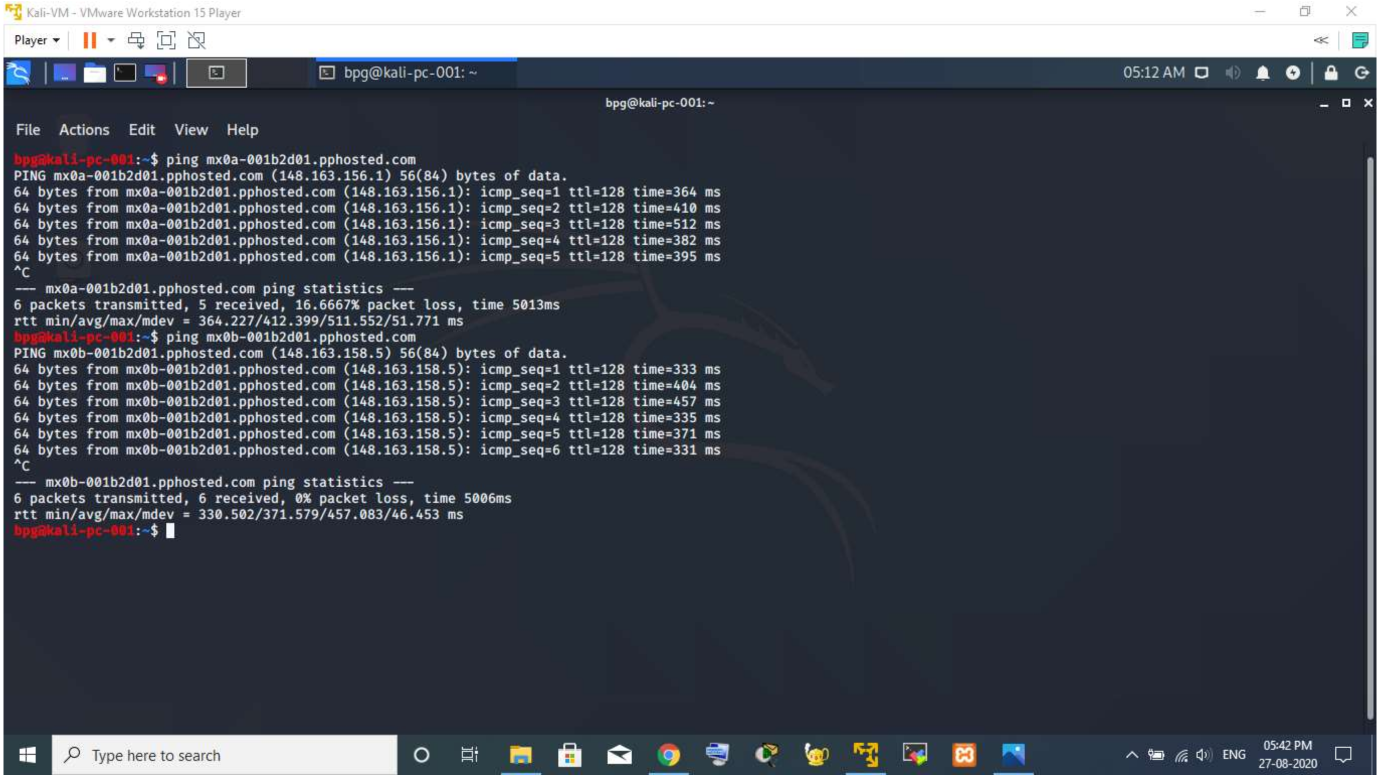
Question-2:-

Find out the locations, where these email servers are hosted.

Step-1: Find the ip addresses of the mail servers
Cmd: ping <mail-server>

Ibm.com:

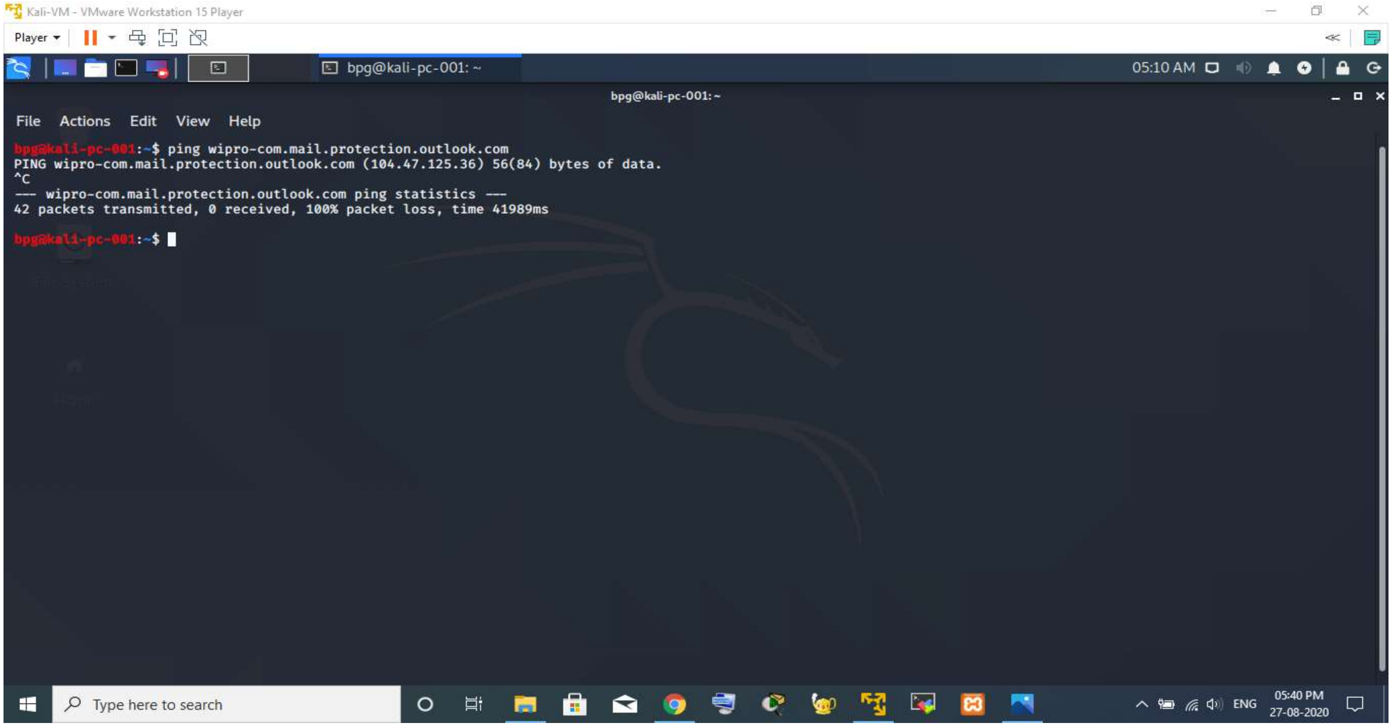
1. mx0a-001b2d01.pphosted.com - 148.163.156.1
2. mx0b-001b2d01.pphosted.com - 148.163.158.5



```
bpg@kali-pc-001:~$ ping mx0a-001b2d01.pphosted.com
PING mx0a-001b2d01.pphosted.com (148.163.156.1) 56(84) bytes of data.
64 bytes from mx0a-001b2d01.pphosted.com (148.163.156.1): icmp_seq=1 ttl=128 time=364 ms
64 bytes from mx0a-001b2d01.pphosted.com (148.163.156.1): icmp_seq=2 ttl=128 time=410 ms
64 bytes from mx0a-001b2d01.pphosted.com (148.163.156.1): icmp_seq=3 ttl=128 time=512 ms
64 bytes from mx0a-001b2d01.pphosted.com (148.163.156.1): icmp_seq=4 ttl=128 time=382 ms
64 bytes from mx0a-001b2d01.pphosted.com (148.163.156.1): icmp_seq=5 ttl=128 time=395 ms
^C
--- mx0a-001b2d01.pphosted.com ping statistics ---
6 packets transmitted, 5 received, 16.6667% packet loss, time 5013ms
rtt min/avg/max/mdev = 364.227/412.399/511.552/51.771 ms
bpg@kali-pc-001:~$ ping mx0b-001b2d01.pphosted.com
PING mx0b-001b2d01.pphosted.com (148.163.158.5) 56(84) bytes of data.
64 bytes from mx0b-001b2d01.pphosted.com (148.163.158.5): icmp_seq=1 ttl=128 time=333 ms
64 bytes from mx0b-001b2d01.pphosted.com (148.163.158.5): icmp_seq=2 ttl=128 time=404 ms
64 bytes from mx0b-001b2d01.pphosted.com (148.163.158.5): icmp_seq=3 ttl=128 time=457 ms
64 bytes from mx0b-001b2d01.pphosted.com (148.163.158.5): icmp_seq=4 ttl=128 time=335 ms
64 bytes from mx0b-001b2d01.pphosted.com (148.163.158.5): icmp_seq=5 ttl=128 time=371 ms
64 bytes from mx0b-001b2d01.pphosted.com (148.163.158.5): icmp_seq=6 ttl=128 time=331 ms
^C
--- mx0b-001b2d01.pphosted.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5006ms
rtt min/avg/max/mdev = 330.502/371.579/457.083/46.453 ms
bpg@kali-pc-001:~$
```

Wipro.com

1. wipro-com.mail.protection.outlook.com - 104.47.125.36



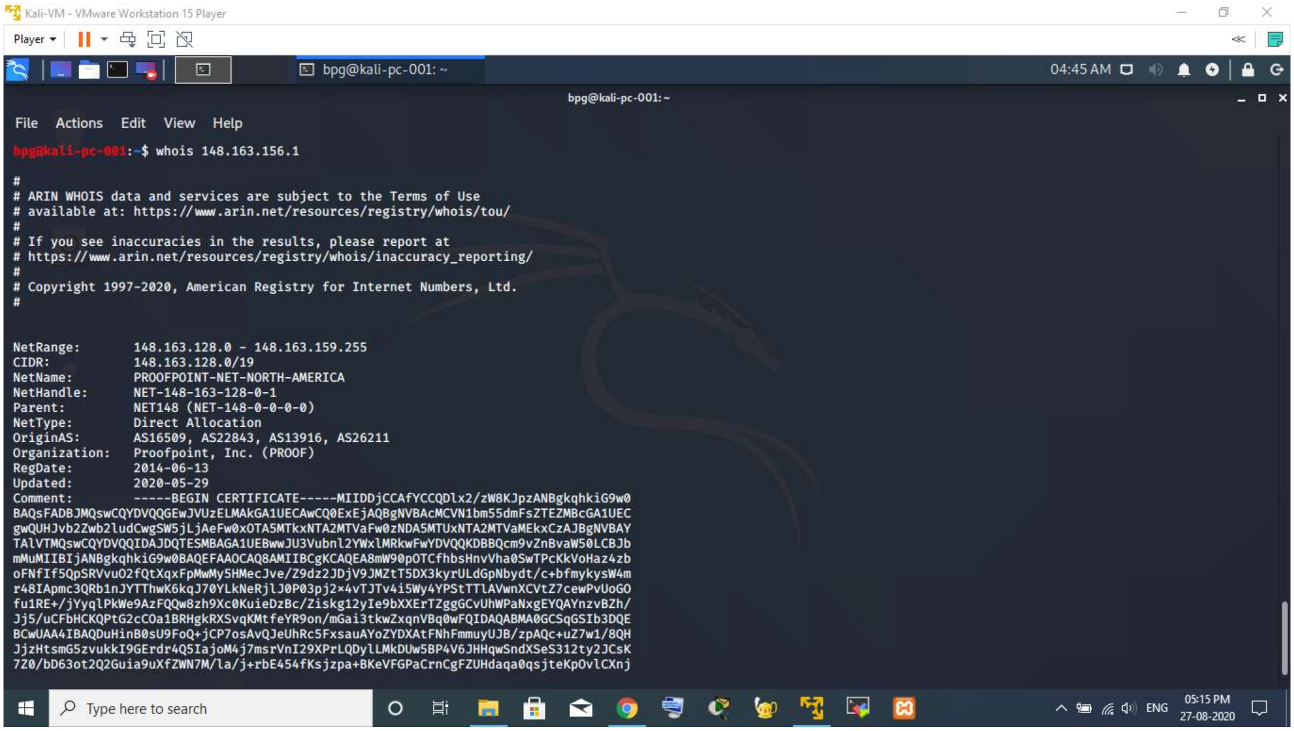
```
bpg@kali-pc-001:~$ ping wipro-com.mail.protection.outlook.com
PING wipro-com.mail.protection.outlook.com (104.47.125.36) 56(84) bytes of data.
^C
--- wipro-com.mail.protection.outlook.com ping statistics ---
42 packets transmitted, 0 received, 100% packet loss, time 41989ms

bpg@kali-pc-001:~$
```

Step-2: Find locations of that ip addresses by using whois database

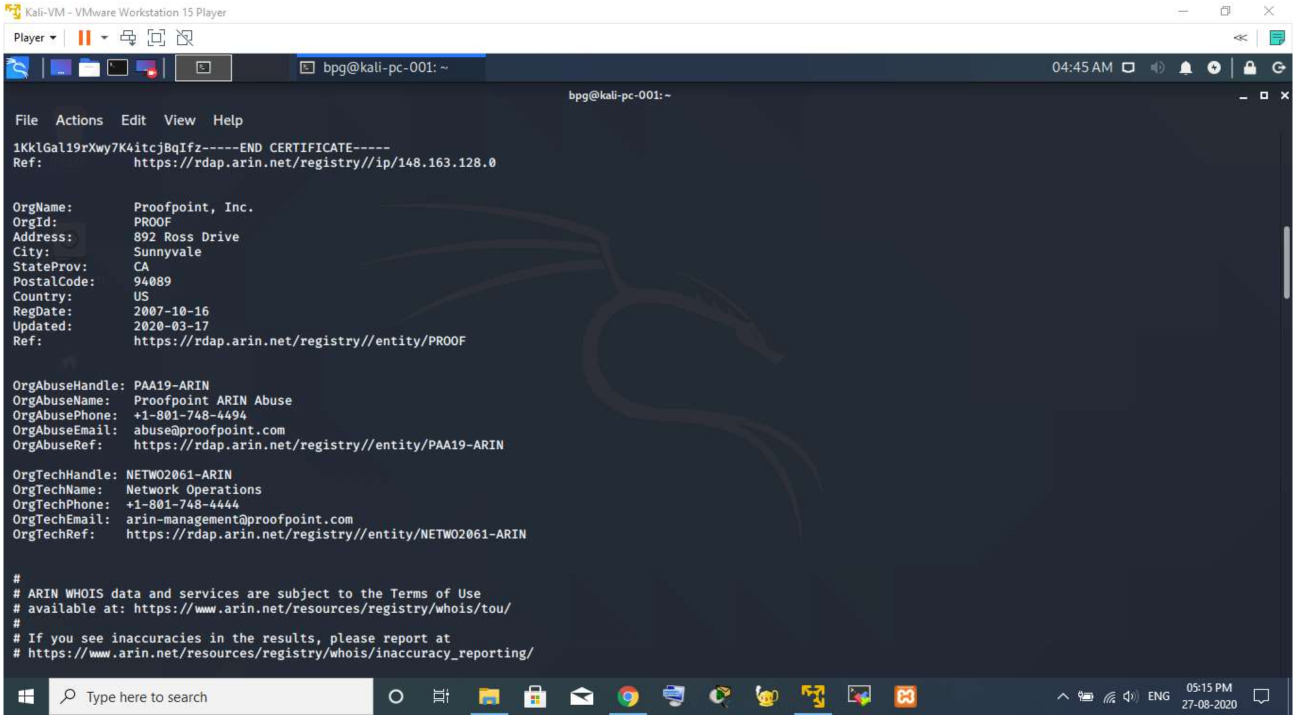
Cmd: whois <IP-address>

Ibm.com

1. mx0a-001b2d01.pphosted.com - 148.163.156.1

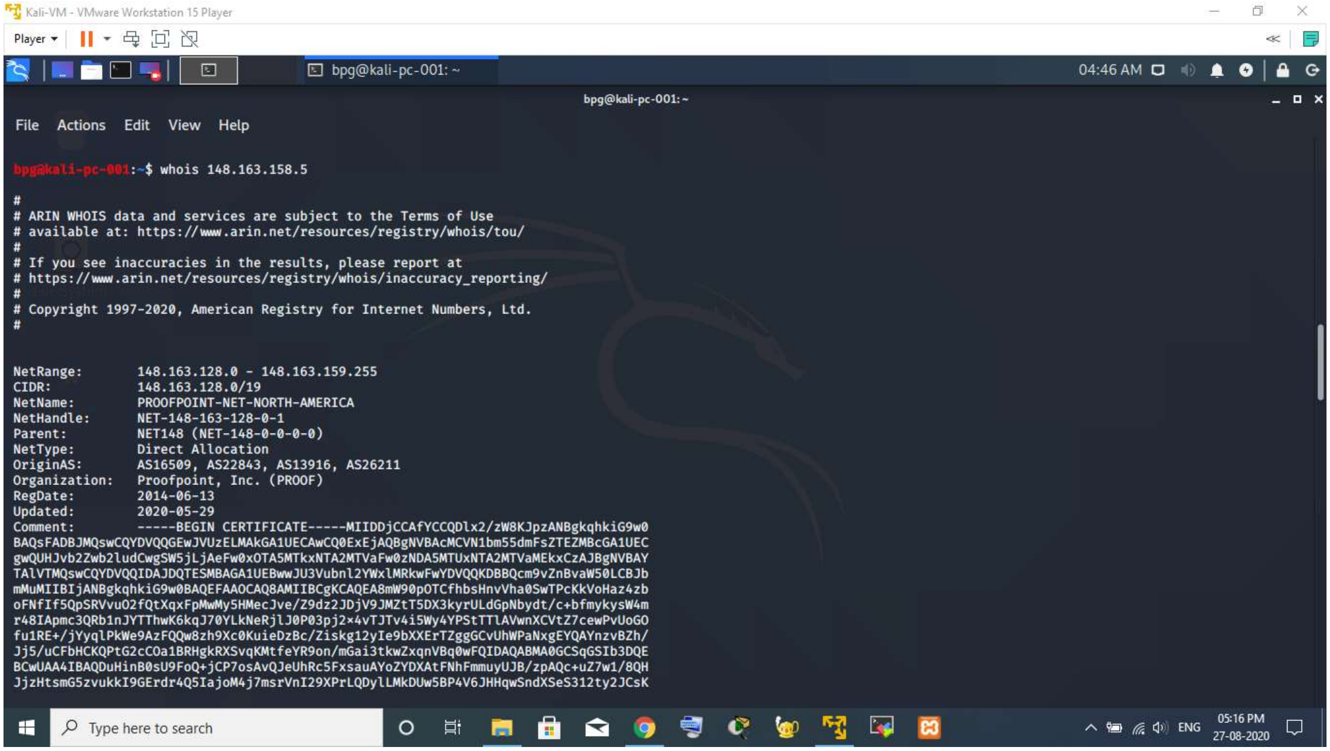


```
bpg@kali-pc-001:~$ whois 148.163.156.1

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2020, American Registry for Internet Numbers, Ltd.
#


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
Comment:        -----BEGIN CERTIFICATE-----MIIDDjCCAfYCCQDlx2/zW8KJpzANBgkqhkiG9w0
BAQsFADBJMQswCQYDVQQGEwJVUzELMAkGA1UECAwCQ0ExEjAQBgNVBAcMCVN1bm55dmFsZTEZMBcGA1UEC
gwQUHJvb2Zwb2ludCwgSW5jLjAeFw0xOTA5MTkxNTA2MTVaFw0zNDA5MTUxNTA2MTVaMEkxCzAJBgNVBAY
TAlVTMQswCQYDVQQIDAJDQTESMBAGA1UEBwwJU3Vubnl2YWxlMRkwFwYDVQQKDBBQcm9vZnBvaW50LCBJb
mMuMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA8mW90pOTCfhbsHnvVha0SwTPcKkVoHaz4zb
oFNfIf5QpSRVvuO2fQtXqxFpMwMy5HMecJve/Z9dz2JDjV9JMZtT5DX3kyrULdGpNbydt/c+bfmykysW4m
r48IApmc3QRb1nJYTThwK6kqJ70YLkNeRjlJ0P03pj2×4vTJTv4i5Wy4YPStTTlAVwnXCVtZ7cewPvUoGO
fu1RE+/jYyqlPkWe9AzFQQw8zh9Xc0KuieDzBc/Ziskg12yIe9bXXErTZggGCvUhWPaNxgEYQAYnzvBZh/
Jj5/uCFbHCKQPtG2cCOa1BRHgkRXSvqKMtfeYR9on/mGai3tkwZxqnVBq0wFQIDAQABMA0GCSqGSIb3DQE
BCwUAA4IBAQDuHinB0sU9FoQ+jCP7osAvQJeUhRc5FxsauAYoZYDXAtFNhFmmuyUJB/zpAQc+uZ7w1/8QH
JjzHtsmG5zvukkI9GErdr4Q5IajoM4j7msrVnI29XPrLQDylLMkDUw5BP4V6JHHqwSndXSeS312ty2JCsK
7Z0/bD63ot2Q2Guia9uXfZWN7M/la/j+rbE454fKsjzpa+BKeVFGPaCrnCgFZUHdaqa0qsjteKpOvlCXnj
```

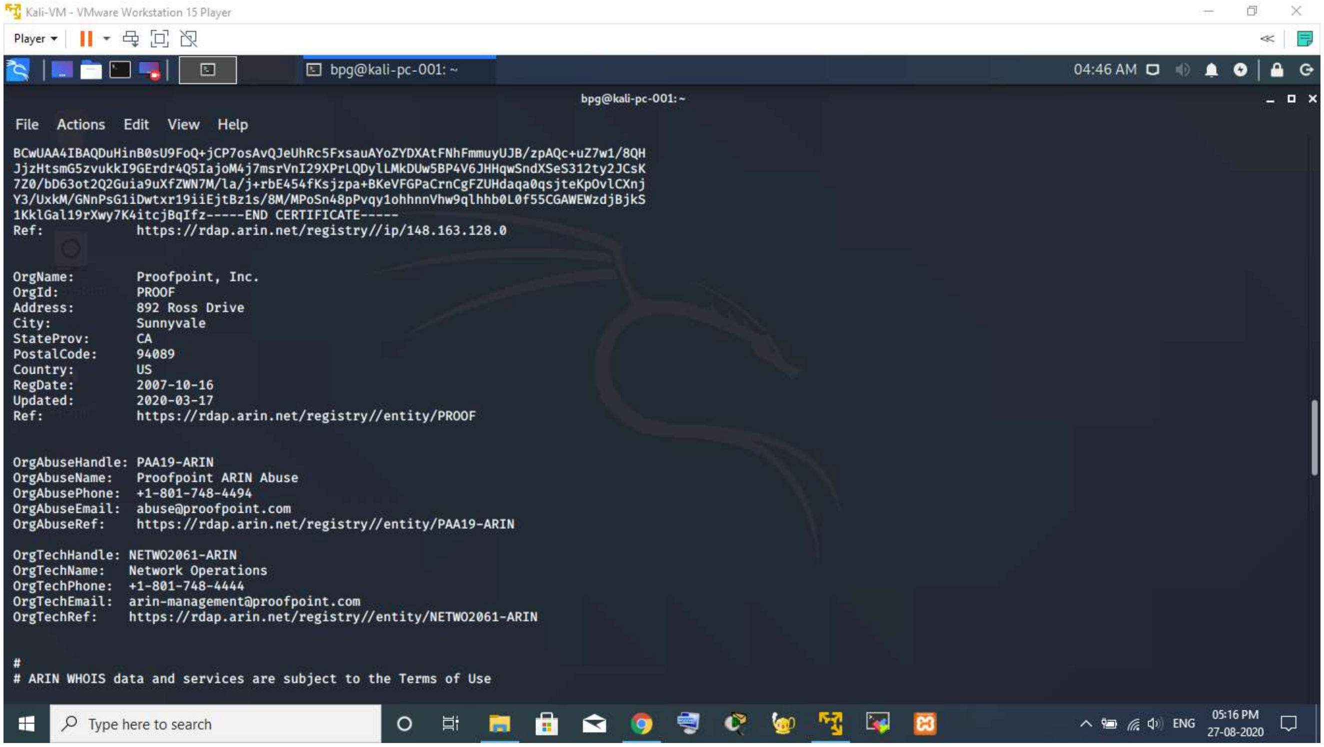


```
1KklGal19rXwy7K4itcjBqIfz-----END CERTIFICATE-----
Ref:            https://rdap.arin.net/registry//ip/148.163.128.0


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:  +1-801-748-4444
OrgTechEmail:  arin-management@proofpoint.com
OrgTechRef:    https://rdap.arin.net/registry//entity/NETWO2061-ARIN


#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
```

2. mx0b-001b2d01.pphosted.com - 148.163.158.5



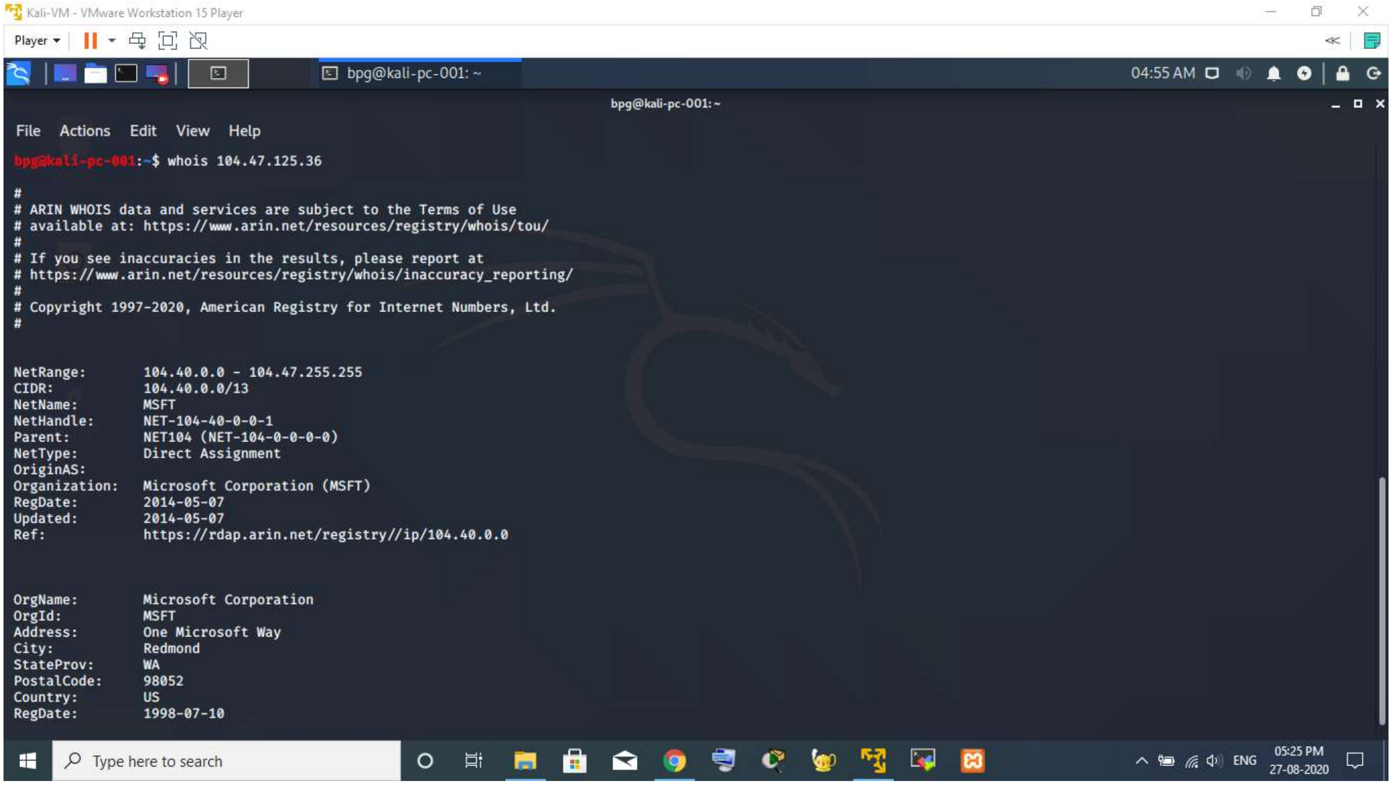
```
bpg@kali-pc-001:~$ whois 148.163.158.5

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2020, American Registry for Internet Numbers, Ltd.
#


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
Comment:        -----BEGIN CERTIFICATE-----MIIDDjCCAfYCCQDlx2/zW8KJpzANBgkqhkiG9w0
BAQsFADBJMQswCQYDVQQGEwJVUzELMAkGA1UECAwCQ0ExEjAQBgNVBAcMCVN1bm55dmFsZTEZMBcGA1UEC
gwQUHJvb2Zwb2ludCwgSW5jLjAeFw0xOTA5MTkxNTA2MTVaFw0zNDA5MTUxNTA2MTVaMEkxCzAJBgNVBAY
TAlVTMQswCQYDVQQIDAJDQTESMBAGA1UEBwwJU3Vubnl2YWxlMRkwFwYDVQQKDBBQcm9vZnBvaW50LCBJb
mMuMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA8mW90pOTCfhbsHnvVha0SwTPcKkVoHaz4zb
oFNfIf5QpSRVvuO2fQtXqxFpMwMy5HMecJve/Z9dz2JDjV9JMZtT5DX3kyrULdGpNbydt/c+bfmykysW4m
r48IApmc3QRb1nJYTThwK6kqJ70YLkNeRjlJ0P03pj2×4vTJTv4i5Wy4YPStTTlAVwnXCVtZ7cewPvUoGO
fu1RE+/jYyqlPkWe9AzFQQw8zh9Xc0KuieDzBc/Ziskg12yIe9bXXErTZggGCvUhWPaNxgEYQAYnzvBZh/
Jj5/uCFbHCKQPtG2cCOa1BRHgkRXSvqKMtfeYR9on/mGai3tkwZxqnVBq0wFQIDAQABMA0GCSqGSIb3DQE
BCwUAA4IBAQDuHinB0sU9FoQ+jCP7osAvQJeUhRc5FxsauAYoZYDXAtFNhFmmuyUJB/zpAQc+uZ7w1/8QH
JjzHtsmG5zvukkI9GErdr4Q5IajoM4j7msrVnI29XPrLQDylLMkDUw5BP4V6JHHqwSndXSeS312ty2JCsK
```



```
BCwUAA4IBAQDuHinB0sU9FoQ+jCP7osAvQJeUhRc5FxsauAYoZYDXAtFNhFmmuyUJB/zpAQc+uZ7w1/8QH
JjzHtsmG5zvukkI9GErdr4Q5IajoM4j7msrVnI29XPrLQDylLMkDUw5BP4V6JHHqwSndXSeS312ty2JCsK
7Z0/bD63ot2Q2Guia9uXfZWN7M/la/j+rbE454fKsjzpa+BKeVFGPaCrnCgFZUHdaqa0qsjteKpOvlCXnj
Y3/UxkM/GNnPsG1iDwtxr19iiEjtBz1s/8M/MPoSn48pPvqy1ohhnnVhw9qlhhb0L0f55CGAWEWzdjBjkS
1KklGal19rXwy7K4itcjBqIfz-----END CERTIFICATE-----
Ref:            https://rdap.arin.net/registry//ip/148.163.128.0


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:  +1-801-748-4444
OrgTechEmail:  arin-management@proofpoint.com
OrgTechRef:    https://rdap.arin.net/registry//entity/NETWO2061-ARIN


#
# ARIN WHOIS data and services are subject to the Terms of Use
```

Wipro.com

1. wipro-com.mail.protection.outlook.com - 104.47.125.36



```
bpg@kali-pc-001:~$ whois 104.47.125.36

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2020, American Registry for Internet Numbers, Ltd.
#


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
```

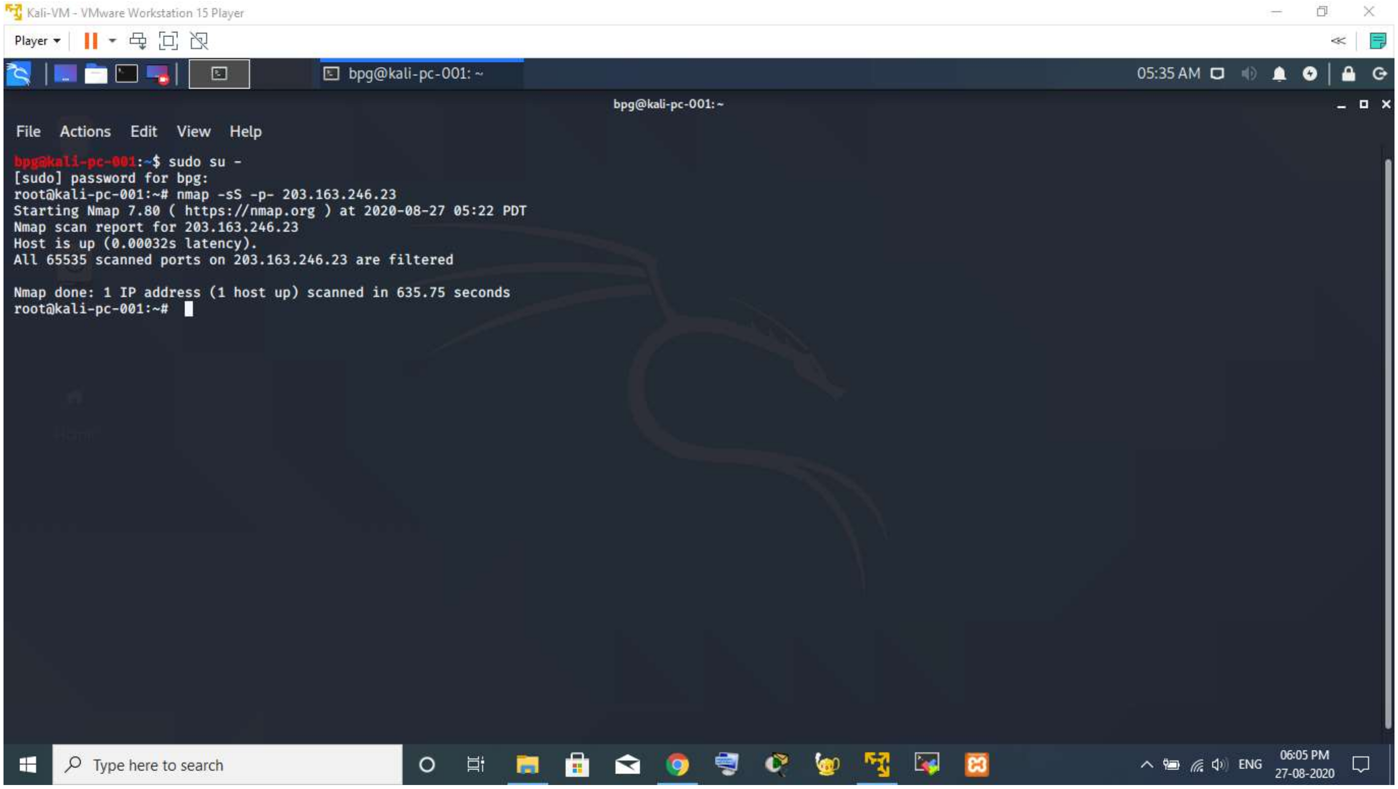
Question-3:-

Scan and find out port numbers open 203.163.246.23

All ports on 203.163.246.23 are filtered.

Cmd: 1. sudo su -

2. nmap -sS -p- 203.163.246.23

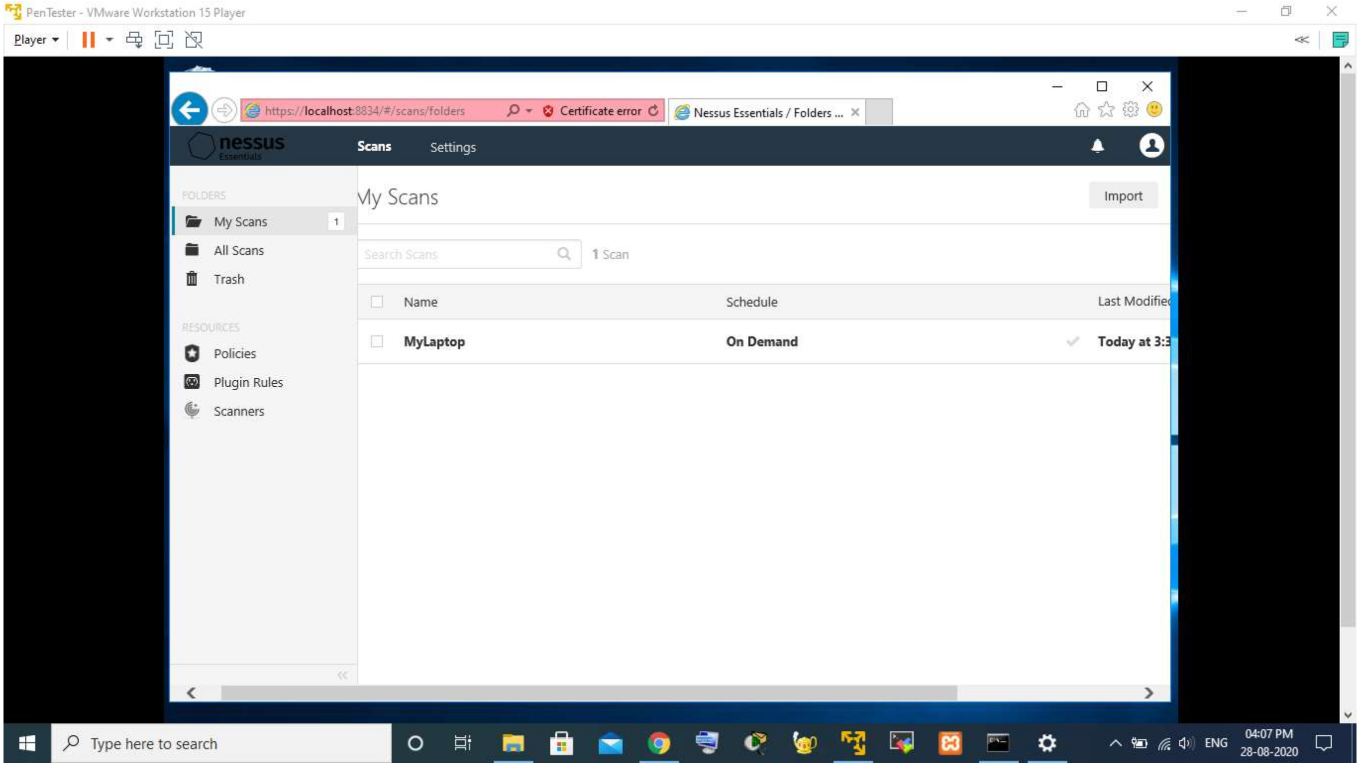


```
bpg@kali-pc-001:~$ sudo su -
[sudo] password for bpg:
root@kali-pc-001:~# nmap -sS -p- 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-27 05:22 PDT
Nmap scan report for 203.163.246.23
Host is up (0.00032s latency).
All 65535 scanned ports on 203.163.246.23 are filtered

Nmap done: 1 IP address (1 host up) scanned in 635.75 seconds
root@kali-pc-001:~#
```

Question-4:-

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

1.Scanning on nessus

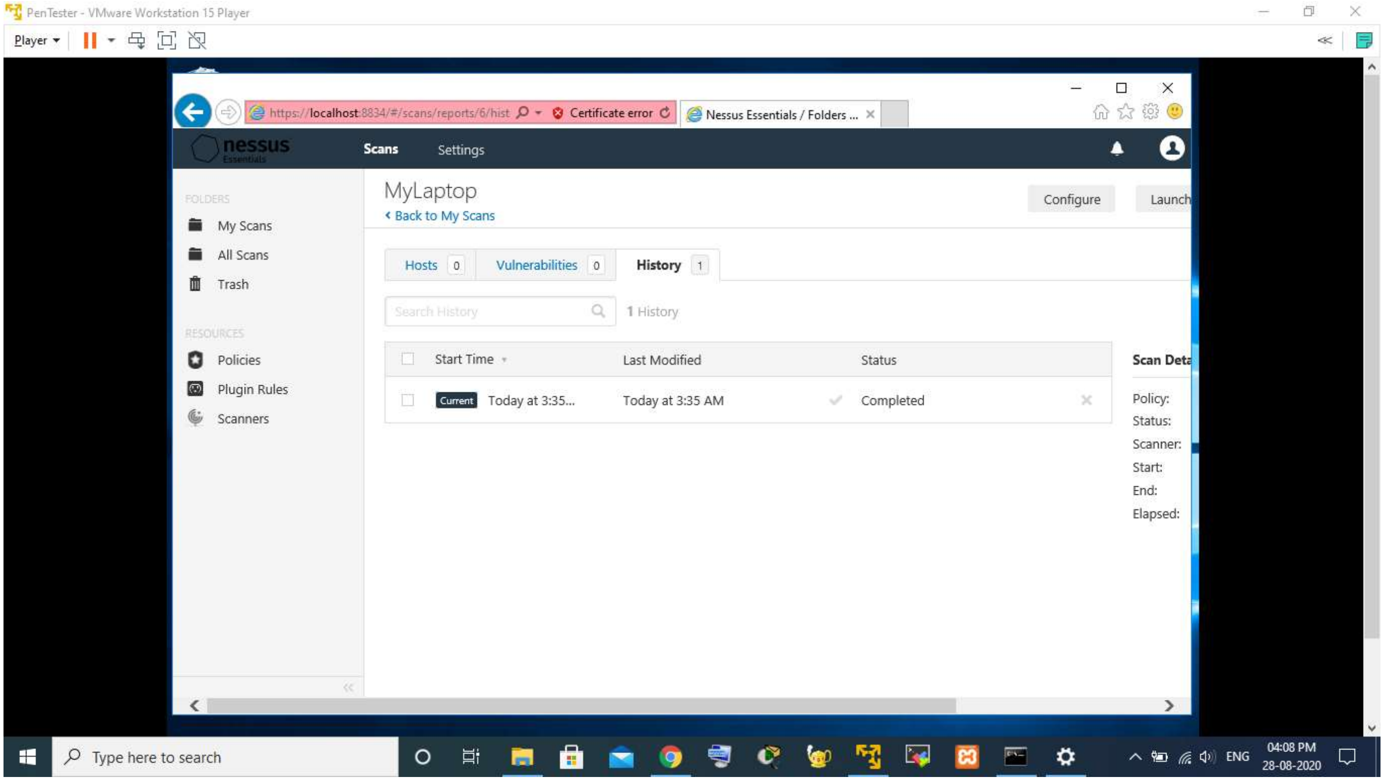


My Scans

1 Scan

□	Name	Schedule	Last Modifie
□	MyLaptop	On Demand	✓ Today at 3:3

2. Scanning Completed



MyLaptop

‹ Back to My Scans

Hosts 0 | Vulnerabilities 0 | History 1

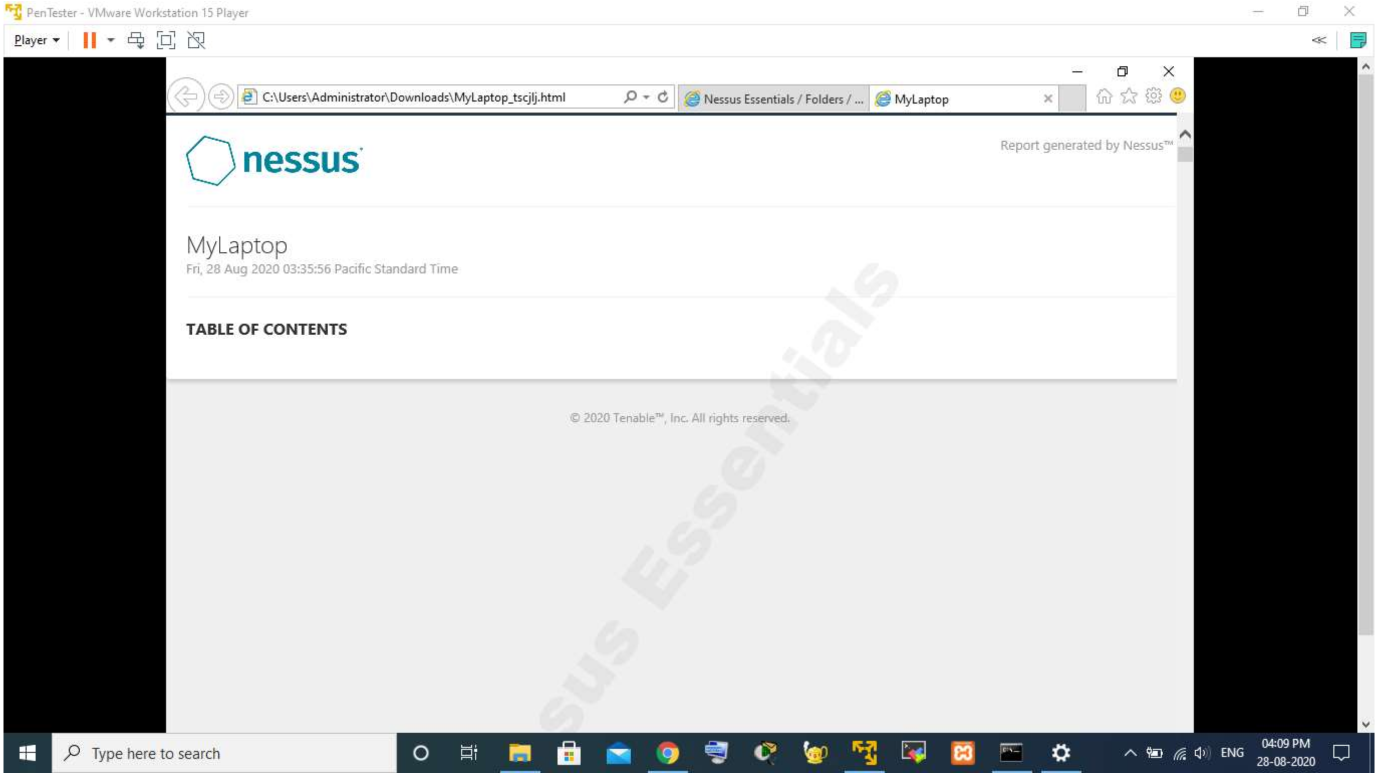
1 History

□	Start Time	Last Modified	Status	
□	Current Today at 3:35...	Today at 3:35 AM	✓ Completed	×

Scan Deta

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

3. Html report: No vulnerabilities on my System


PenTester - VMware Workstation 15 Player
Player
C:\Users\Administrator\Downloads\MyLaptop_tscjlj.html
Nessus Essentials / Folders / ...
MyLaptop
nessus
Nessus Essentials
Type here to search
ENG
04:09 PM
28-08-2020

Report generated by Nessus™

MyLaptop

Fri, 28 Aug 2020 03:35:56 Pacific Standard Time

TABLE OF CONTENTS

© 2020 Tenable™, Inc. All rights reserved.