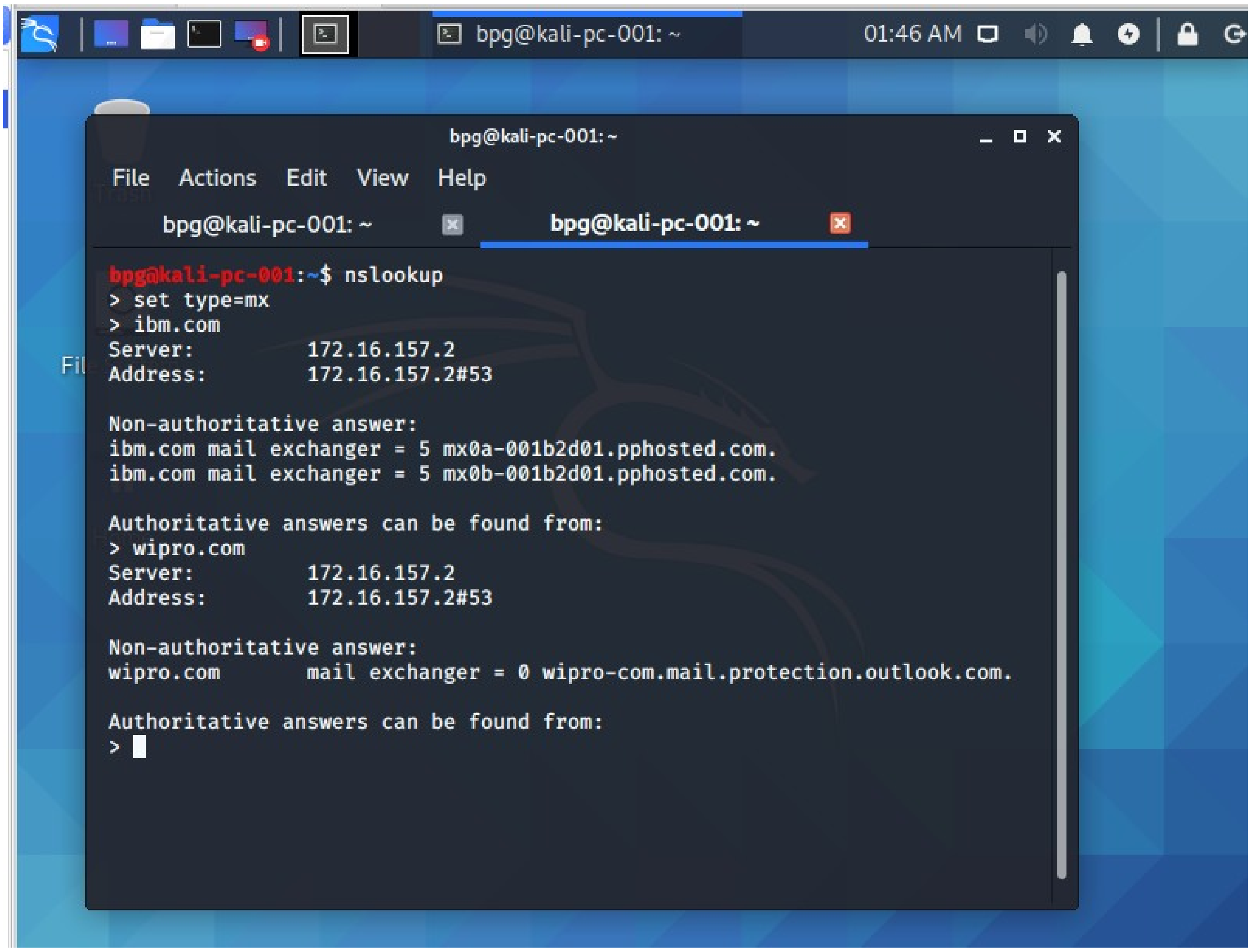
Question 1:

Find out the mail servers of the following domain :
Ibm.com
Wipro.com

- Open kali and open terminal type **nslookup** press enter and type **set type=mx** for mx record and type server address **ibm.com** and viseversa **wipro.com**

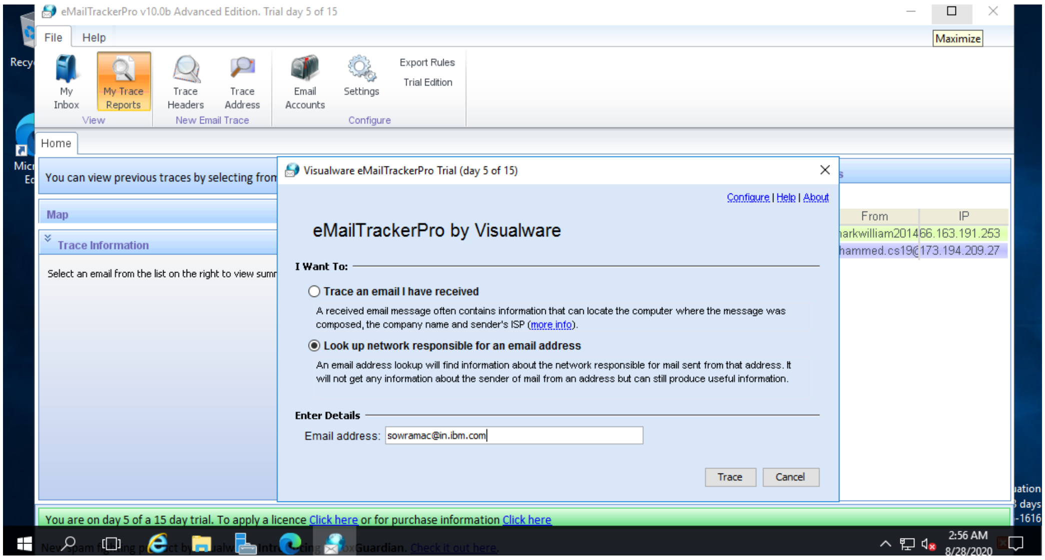


```
bpg@kali-pc-001:~$ nslookup
> set type=mx
> ibm.com
Server:         172.16.157.2
Address:        172.16.157.2#53

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
Server:         172.16.157.2
Address:        172.16.157.2#53

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

Authoritative answers can be found from:
> 
```

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

- Find any email address on google by typing
  ibm.com contact email
  wipro.com contact email
- gather it.

- Open Pentester windows server install and open email tracker pro
- Click My Trace Reports and click Trace address
- Paste the address on Email address field
- Then click Trace Button



You can view previous traces by selecting fron

Select an email from the list on the right to view sumr

Visualware eMailTrackerPro Trial (day 5 of 15)

Configure | Help | About

eMailTrackerPro by Visualware

I Want To:

○ Trace an email I have received

A received email message often contains information that can locate the computer where the message was composed, the company name and sender's ISP (more info).

● Look up network responsible for an email address

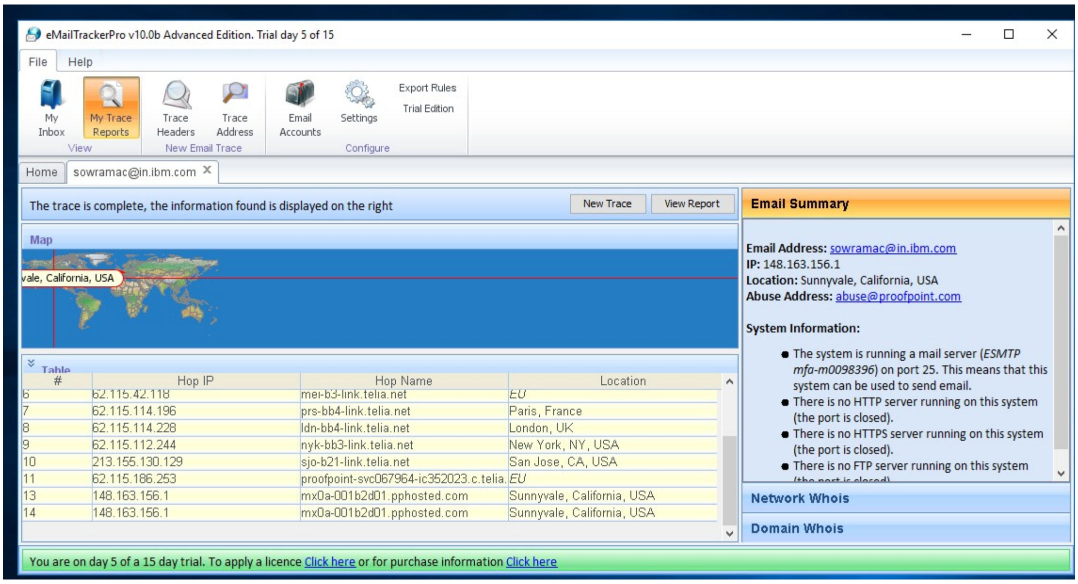
An email address lookup will find information about the network responsible for mail sent from that address. It will not get any information about the sender of mail from an address but can still produce useful information.

Enter Details

Email address: sowramac@in.ibm.com

Trace | Cancel

You are on day 5 of a 15 day trial. To apply a licence Click here or for purchase information Click here



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

#	Hop IP	Hop Name	Location
6	62.115.42.118	mei-b3-link.telia.net	*EU*
7	62.115.114.196	prs-bb4-link.telia.net	Paris, France
8	62.115.114.228	ldn-bb4-link.telia.net	London, UK
9	62.115.112.244	nyk-bb3-link.telia.net	New York, NY, USA
10	213.155.130.129	sjo-b21-link.telia.net	San Jose, CA, USA
11	62.115.186.253	proofpoint-svc067964-ic352023.c.telia.	*EU*
13	148.163.156.1	mx0a-001b2d01.pphosted.com	Sunnyvale, California, USA
14	148.163.156.1	mx0a-001b2d01.pphosted.com	Sunnyvale, California, USA

Email Summary

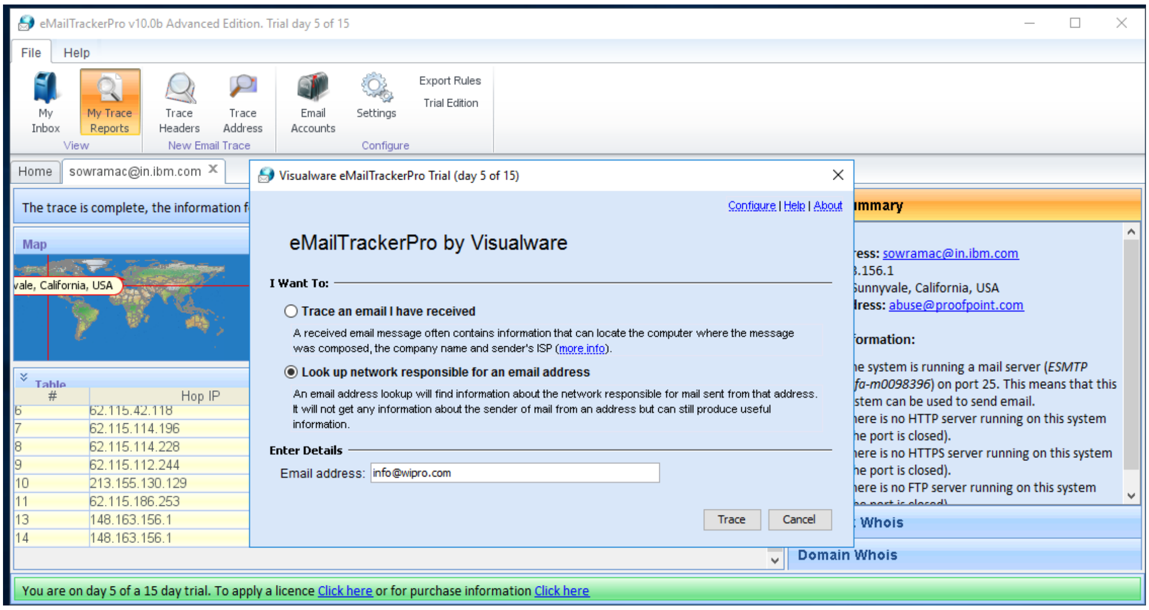
Email Address: sowramac@in.ibm.com
IP: 148.163.156.1
Location: Sunnyvale, California, USA
Abuse Address: abuse@proofpoint.com

System Information:

- The system is running a mail server (*ESMTP mfa-m0098396*) on port 25. This means that this system can be used to send email.
- 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).

You are on day 5 of a 15 day trial. To apply a licence Click here or for purchase information Click here

- Ibm.com Email server located under location **Synnyvale, California, USA**



The trace is complete, the information f

#	Hop IP
6	62.115.42.118
7	62.115.114.196
8	62.115.114.228
9	62.115.112.244
10	213.155.130.129
11	62.115.186.253
13	148.163.156.1
14	148.163.156.1

Visualware eMailTrackerPro Trial (day 5 of 15)

eMailTrackerPro by Visualware

I Want To:

○ **Trace an email I have received**

A received email message often contains information that can locate the computer where the message was composed, the company name and sender's ISP (more info).

● **Look up network responsible for an email address**

An email address lookup will find information about the network responsible for mail sent from that address. It will not get any information about the sender of mail from an address but can still produce useful information.

Enter Details

Email address: info@wipro.com

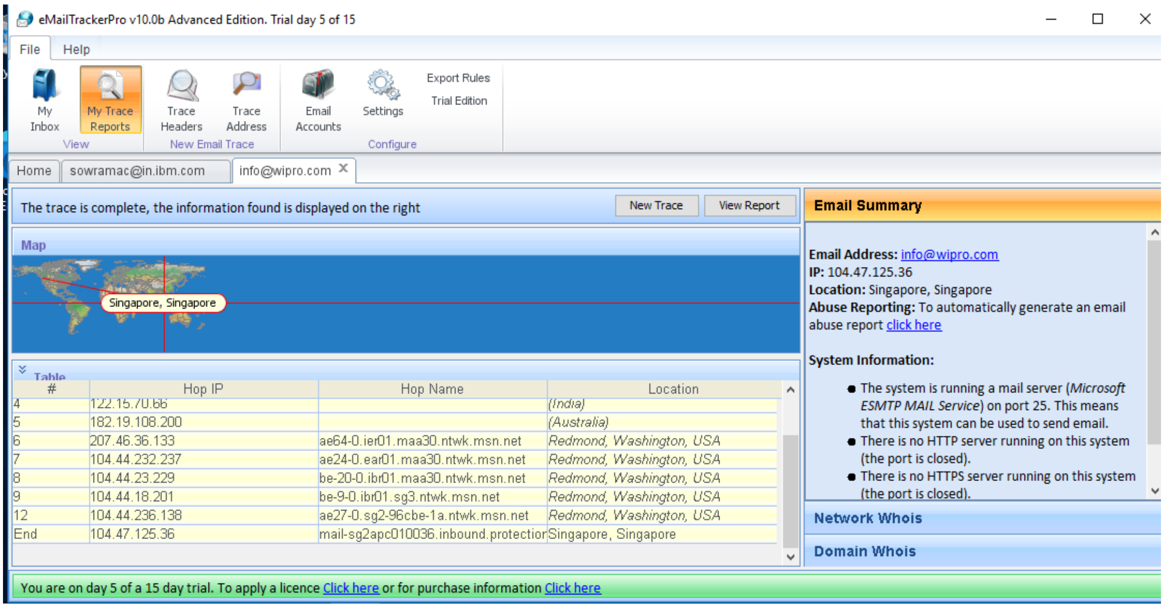
ımmary

ess: sowramac@in.ibm.com
.156.1
Sunnyvale, California, USA
Iress: abuse@proofpoint.com

ormation:

he system is running a mail server (*ESMTP fa-m0098396*) on port 25. This means that this stem can be used to send email.
here is no HTTP server running on this system he port is closed).
here is no HTTPS server running on this system he port is closed).
here is no FTP server running on this system

You are on day 5 of a 15 day trial. To apply a licence Click here or for purchase information Click here



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

#	Hop IP	Hop Name	Location
4	122.15.70.66		*(India)*
5	182.19.108.200		*(Australia)*
6	207.46.36.133	ae64-0.ier01.maa30.ntwk.msn.net	*Redmond, Washington, USA*
7	104.44.232.237	ae24-0.ear01.maa30.ntwk.msn.net	*Redmond, Washington, USA*
8	104.44.23.229	be-20-0.ibr01.maa30.ntwk.msn.net	*Redmond, Washington, USA*
9	104.44.18.201	be-9-0.ibr01.sg3.ntwk.msn.net	*Redmond, Washington, USA*
12	104.44.236.138	ae27-0.sg2-96cbe-1a.ntwk.msn.net	*Redmond, Washington, USA*
End	104.47.125.36	mail-sg2apc010036.inbound.protectior	Singapore, Singapore

Email Summary

Email Address: info@wipro.com
IP: 104.47.125.36
Location: Singapore, Singapore
Abuse Reporting: To automatically generate an email abuse report click here

System Information:

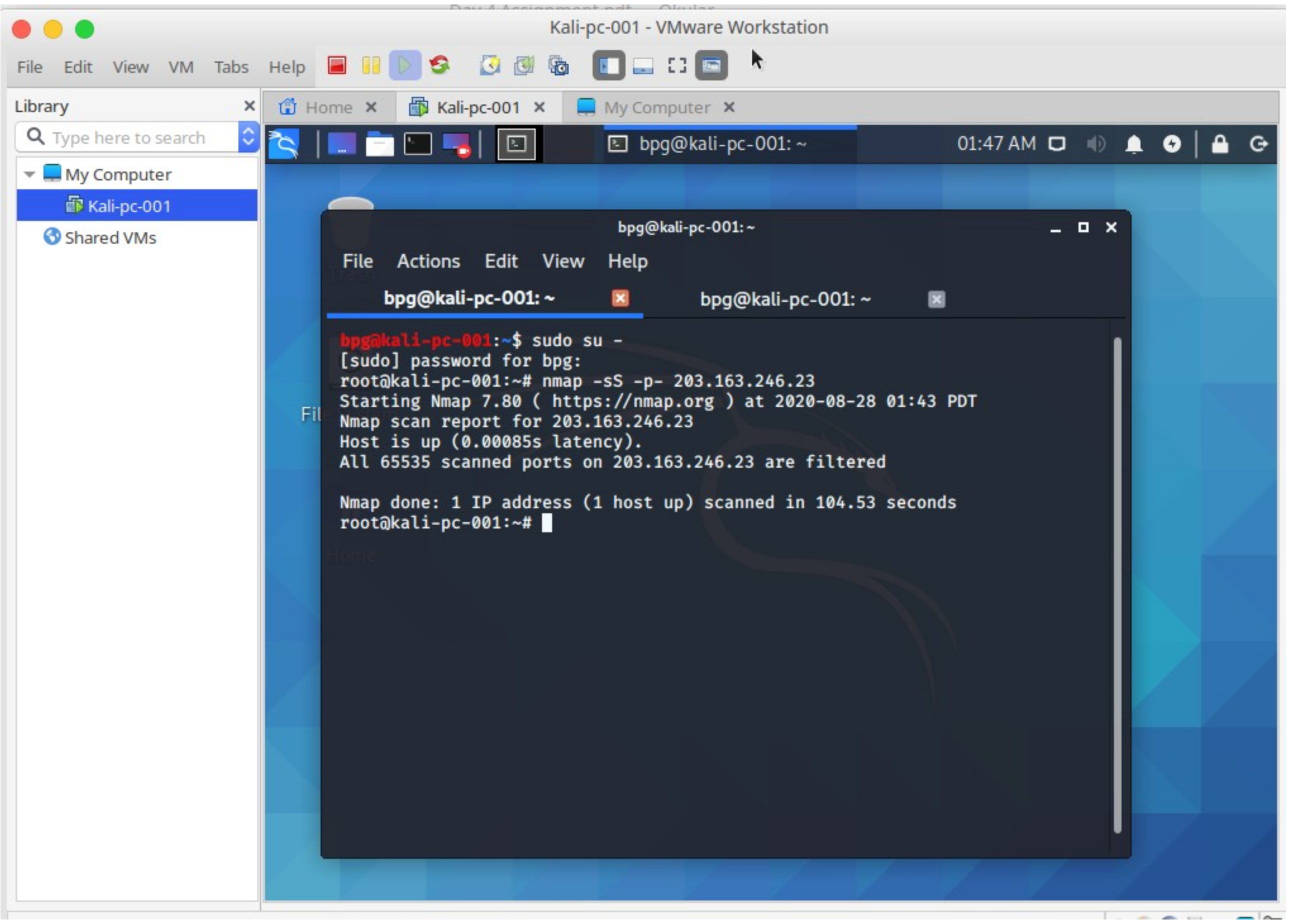
- The system is running a mail server (*Microsoft ESMTP MAIL Service*) on port 25. This means that this system can be used to send email.
- There is no HTTP server running on this system (the port is closed).
- There is no HTTPS server running on this system (the port is closed).

You are on day 5 of a 15 day trial. To apply a licence Click here or for purchase information Click here

- Wipro.com Email server located under location **Singapore, Singapore**

Question 3:
Scan and find out port numbers open 203.163.246.23

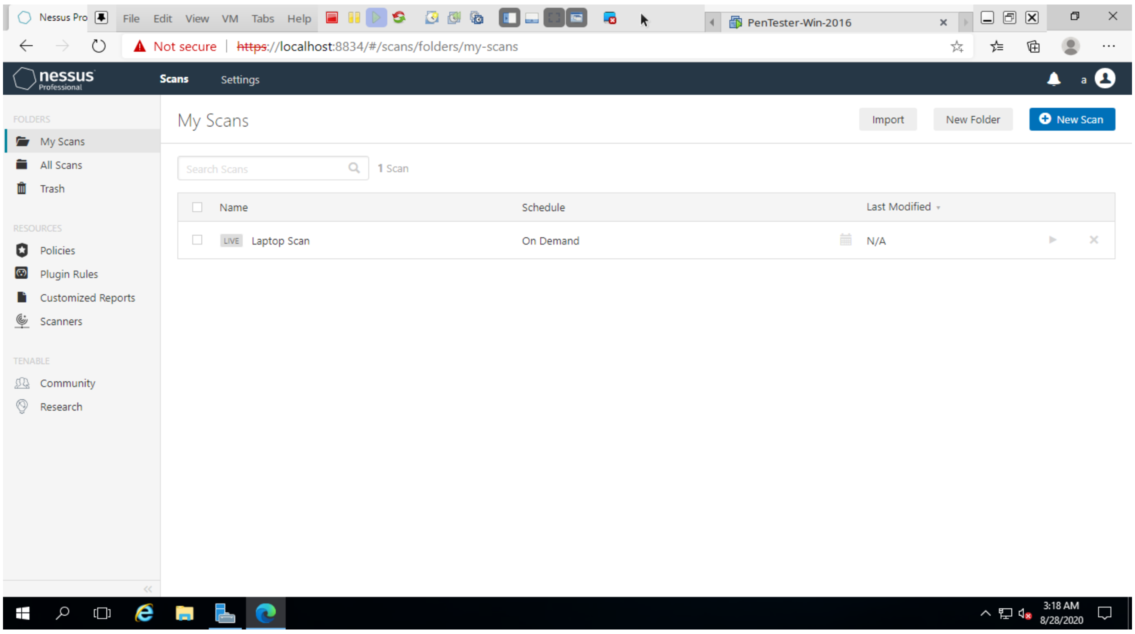
- Open Kali and open terminal and type **sudo su -**
- then type **nmap -sS -p- 203.163.246.23**
- See the result
- No open port found



```
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 2020-08-28 01:43 PDT
Nmap scan report for 203.163.246.23
Host is up (0.00085s latency).
All 65535 scanned ports on 203.163.246.23 are filtered

Nmap done: 1 IP address (1 host up) scanned in 104.53 seconds
root@kali-pc-001:~# 
```

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

- Download and install nessus in pentest windows 2016 server and configure
- open chrome browser (install) and type https://localhost:8834/ to open nesus dashboard
- On Dashboard click **New Scan**

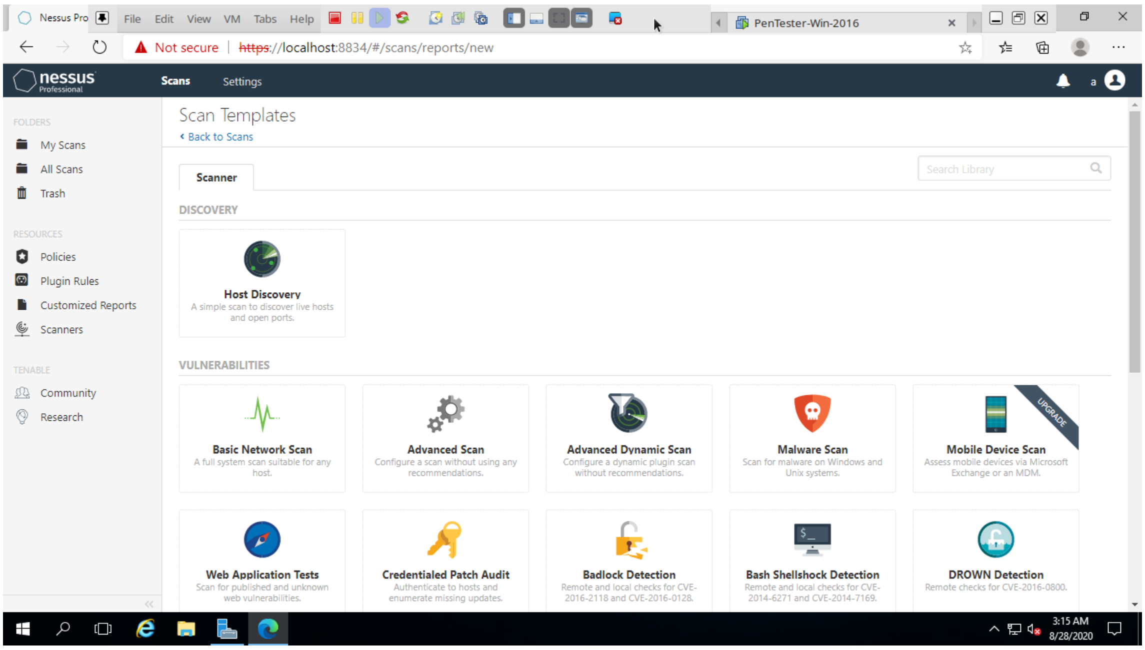


My Scans

1 Scan

Name	Schedule	Last Modified
LIVE Laptop Scan	On Demand	N/A

- On New Scan window click **Advanced Scan**



Scan Templates

DISCOVERY

Host Discovery
A simple scan to discover live hosts and open ports.

VULNERABILITIES

Basic Network Scan
A full system scan suitable for any host.

Advanced Scan
Configure a scan without using any recommendations.

Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.

Malware Scan
Scan for malware on Windows and Unix systems.

Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

Web Application Tests
Scan for published and unknown web vulnerabilities.

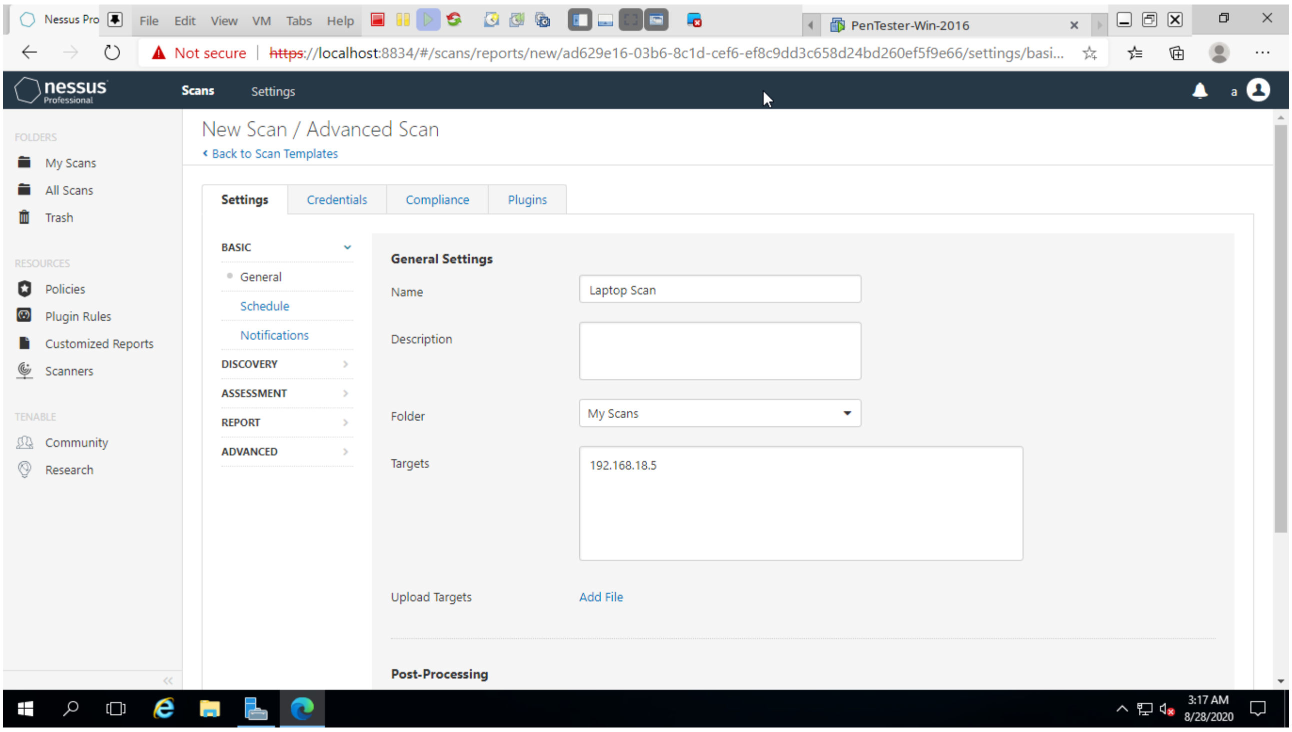
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

DROWN Detection
Remote checks for CVE-2016-0800.

- On Advanced Scan Type **Name** and **Target IP** (Laptop IP – get using ifconfig/ipconfig)



New Scan / Advanced Scan

‹ Back to Scan Templates

General Settings

Name: Laptop Scan

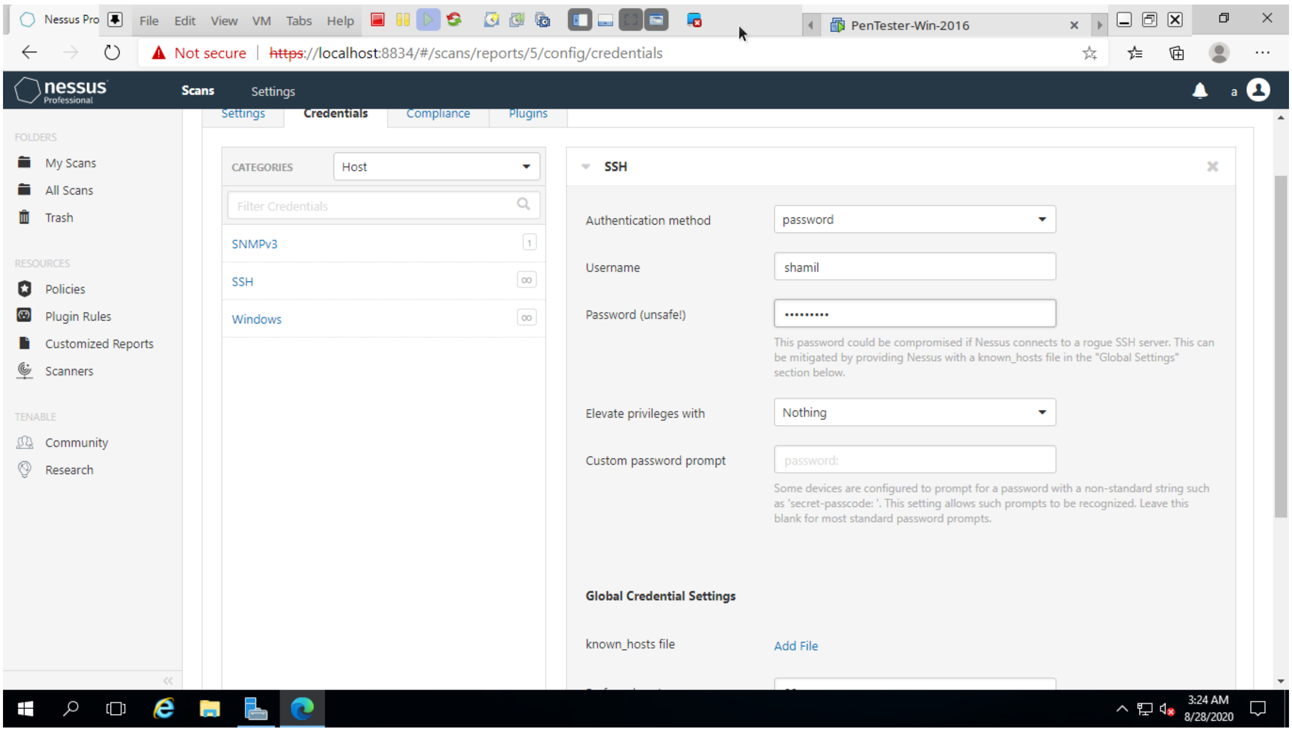
Description:

Folder: My Scans

Targets: 192.168.18.5

Upload Targets: Add File

- Open Credentials Tab and select **SSH** (for linux) and Type **Username** and **Password**



Authentication method: password

Username: shamil

Password (unsafe!): •••••••••

This password could be compromised if Nessus connects to a rogue SSH server. This can be mitigated by providing Nessus with a known_hosts file in the "Global Settings" section below.

Elevate privileges with: Nothing

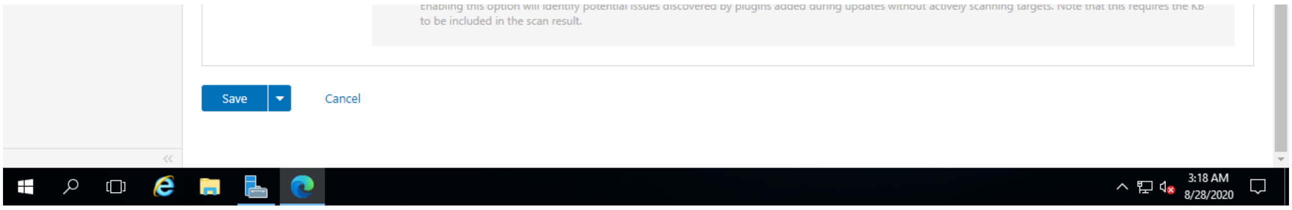
Custom password prompt: password:

Some devices are configured to prompt for a password with a non-standard string such as 'secret-passcode: '. This setting allows such prompts to be recognized. Leave this blank for most standard password prompts.

Global Credential Settings

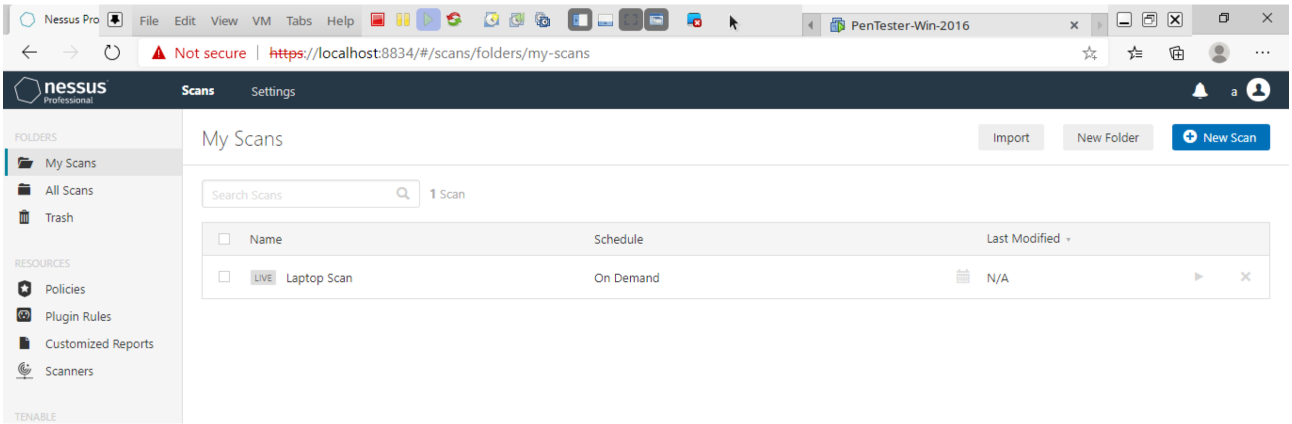
known_hosts file: Add File

- Click save buttton



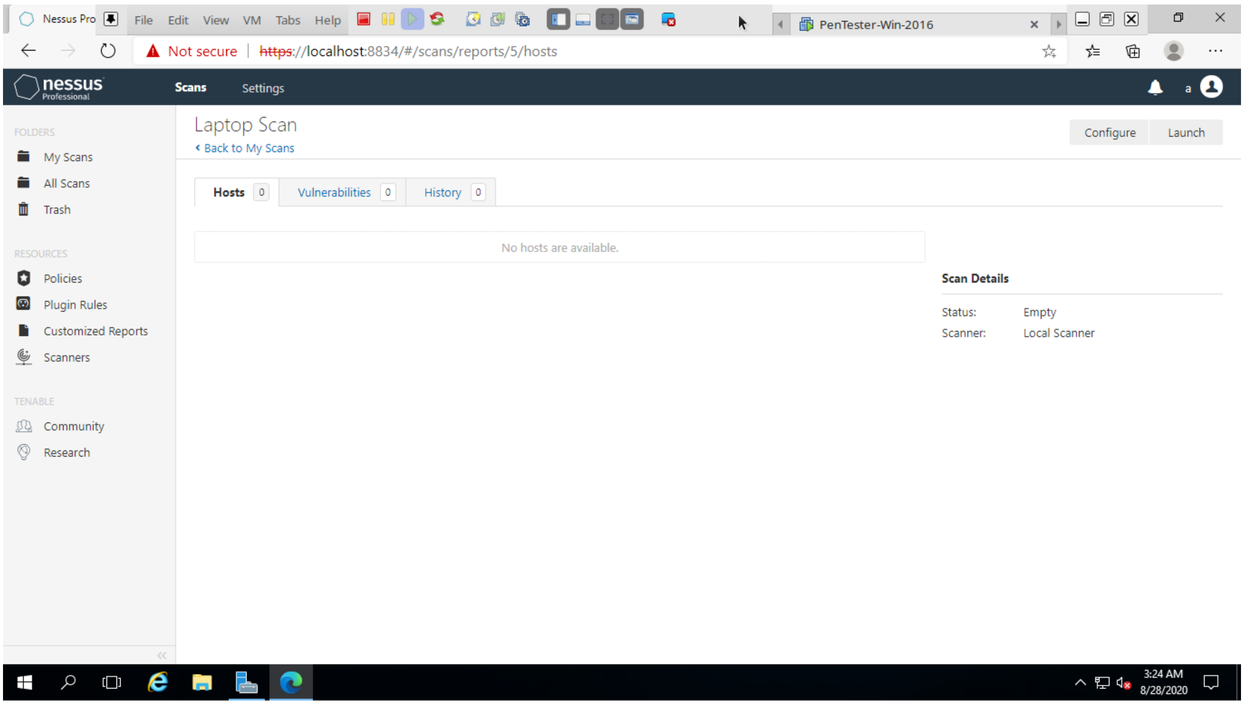
Enabling this option will identify potential issues discovered by plugins added during updates without actively scanning targets. Note that this requires the KB to be included in the scan result.

- On Dashboard Click the saved scan Laptop Scan



Name	Schedule	Last Modified
LIVE Laptop Scan	On Demand	N/A

- On Laptop Scan click Launch



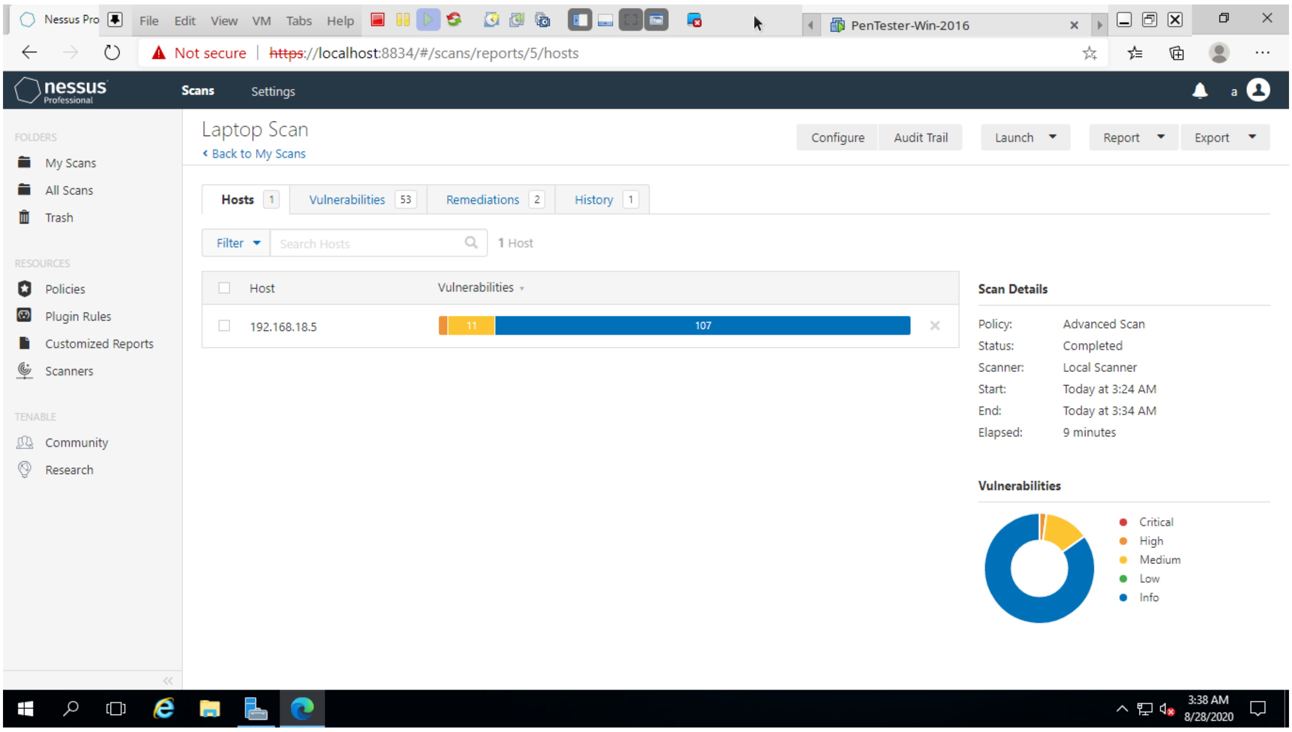
No hosts are available.

Scan Details

Status: Empty

Scanner: Local Scanner

- After Scan Complete See the **Scan Details**



Laptop Scan

‹ Back to My Scans

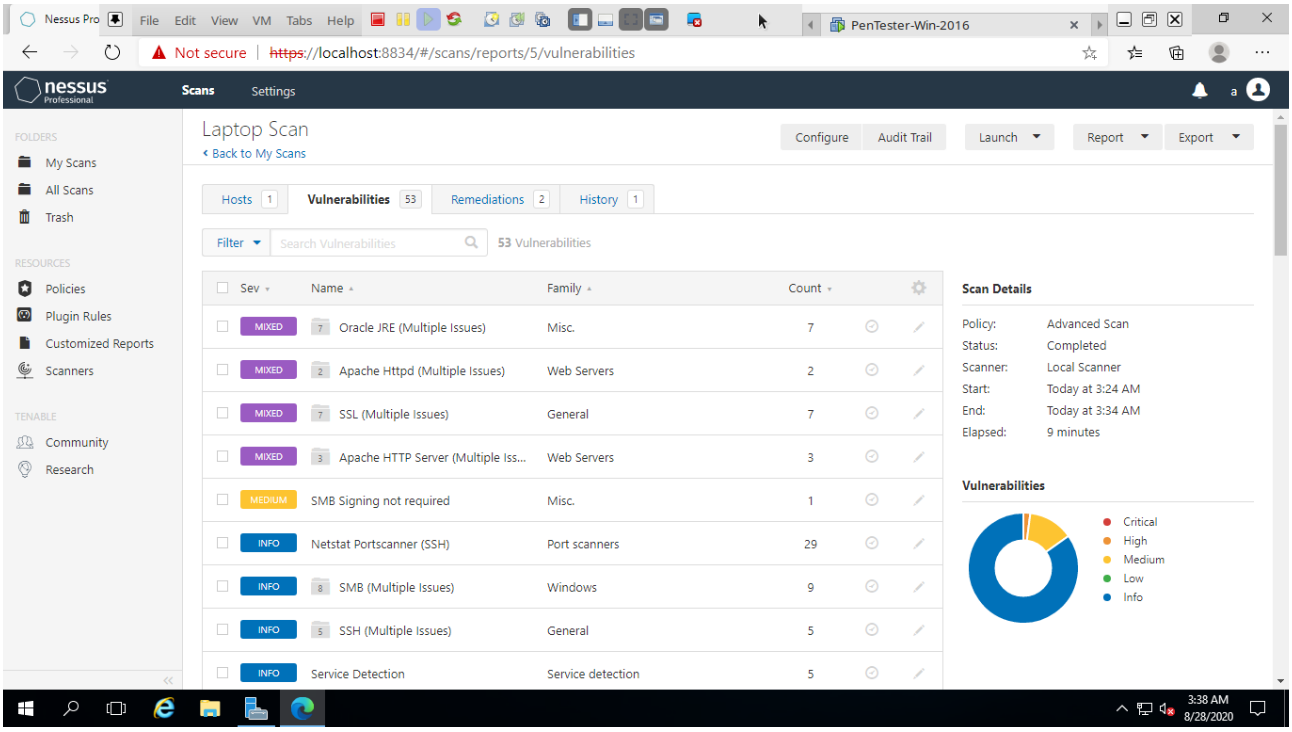
□	Host	Vulnerabilities
□	192.168.18.5	11 107

Scan Details

Policy:	Advanced Scan
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 3:24 AM
End:	Today at 3:34 AM
Elapsed:	9 minutes

Vulnerabilities

Total Vulnerabilities



Laptop Scan

‹ Back to My Scans

□	Sev	Name	Family	Count
□	MIXED	7 Oracle JRE (Multiple Issues)	Misc.	7
□	MIXED	2 Apache Httpd (Multiple Issues)	Web Servers	2
□	MIXED	7 SSL (Multiple Issues)	General	7
□	MIXED	3 Apache HTTP Server (Multiple Iss...	Web Servers	3
□	MEDIUM	SMB Signing not required	Misc.	1
□	INFO	Netstat Portscanner (SSH)	Port scanners	29
□	INFO	8 SMB (Multiple Issues)	Windows	9
□	INFO	5 SSH (Multiple Issues)	General	5
□	INFO	Service Detection	Service detection	5

Scan Details

Policy:	Advanced Scan
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 3:24 AM
End:	Today at 3:34 AM
Elapsed:	9 minutes

Vulnerabilities