**Cybersecurity Essentials**

**Assignment-1 Day 4 / 23rd August 2020**

**Name: Nitheesh Kumar N**

**Email id.:** [**nithesh.nallarasan@gmail.com**](mailto:nithesh.nallarasan@gmail.com)

**Phone number: +919500507758**

**Q1. Find out the mail server of the following domain:**

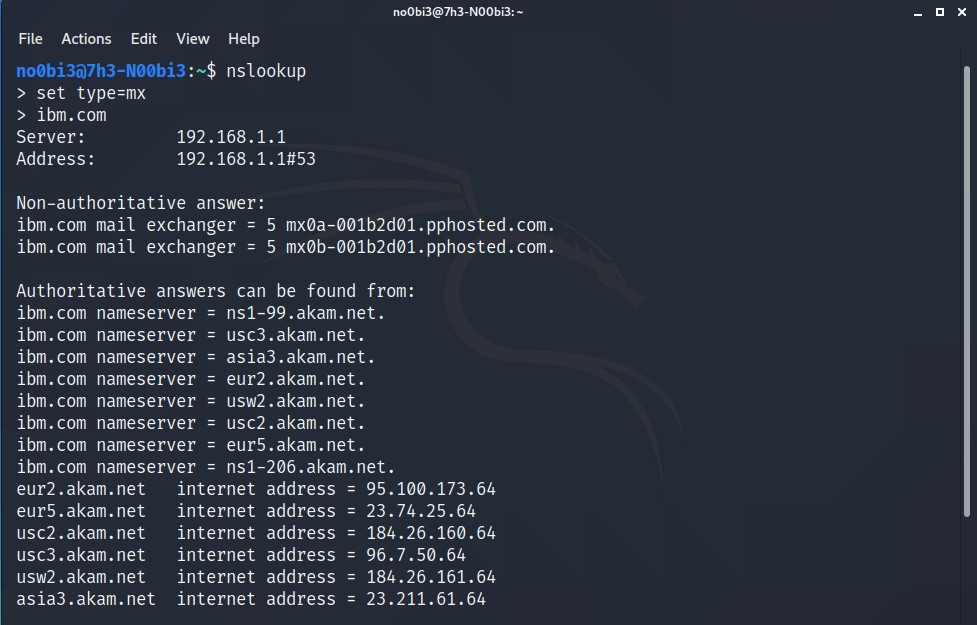
* **ibm.com**
* **Wipro.com**

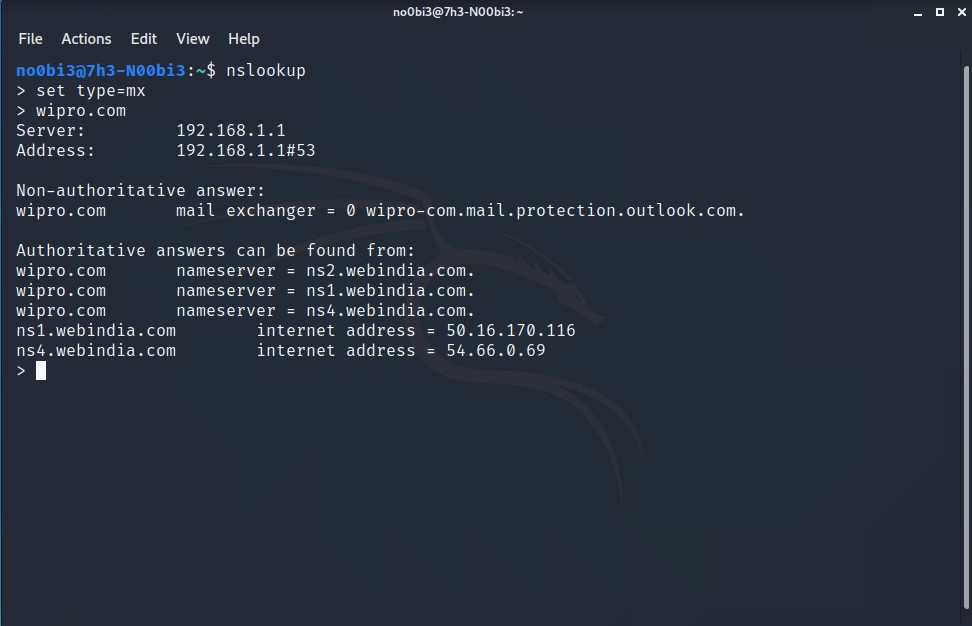
**Solution-**

1. **Open terminal in Kali**
2. **Write command nslookup and type in set type=mx**

**This will let us know the mail exchanger used by the domain.**

1. **Enter the domain ibm.com and follow the same process for wipro.com to obtain their respective mail servers**

****

****

**Therefore we can find out**

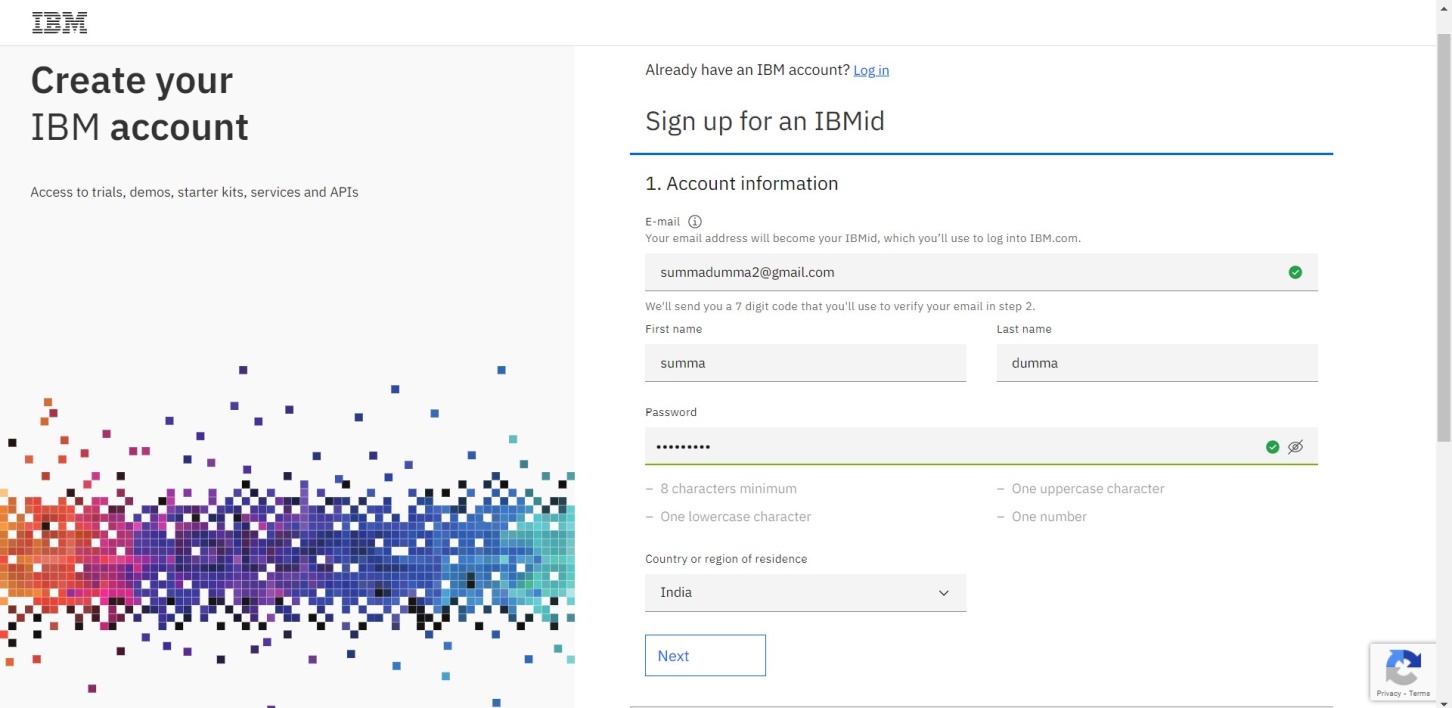
**The mail server of ibm.com:- mx0a-001b2d01.pphosted.com**

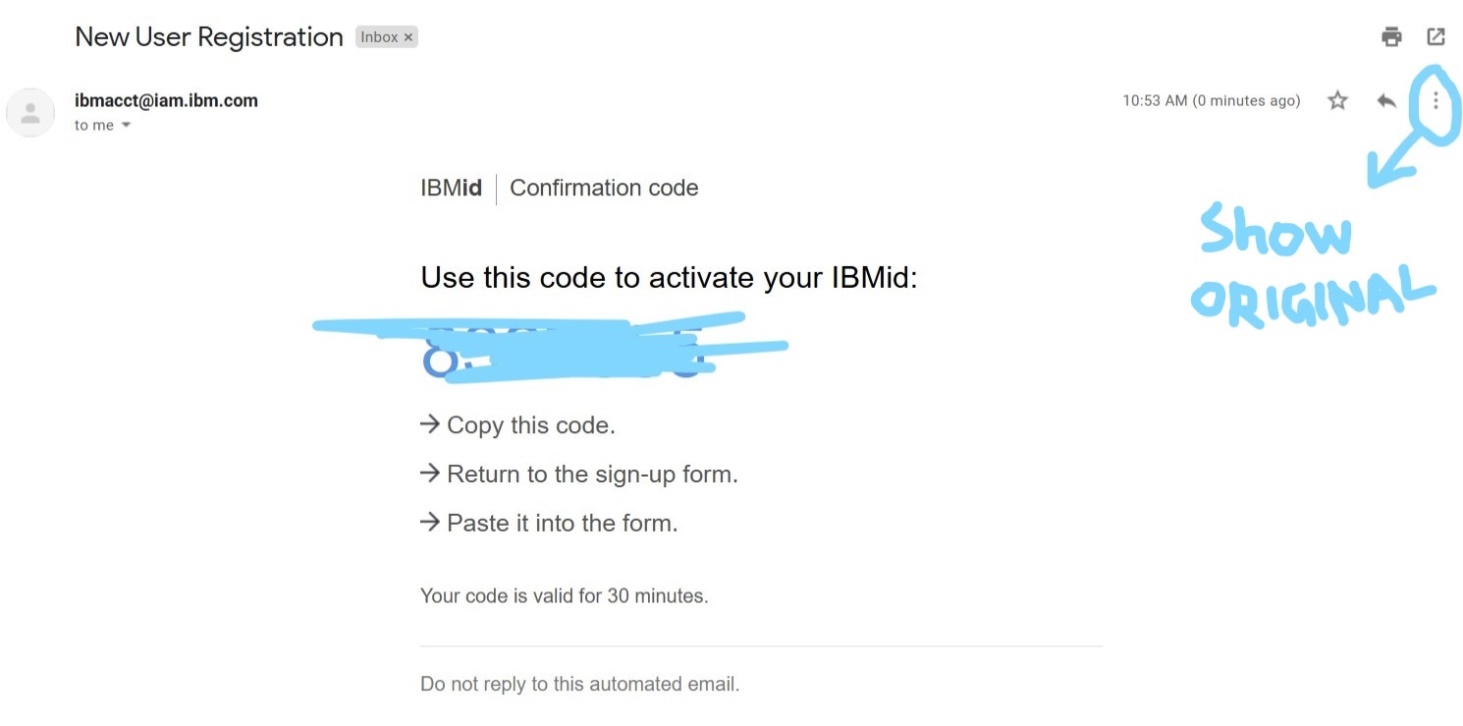
**The mail server of wipro.com: wipro-com.mail.protection.outlook.com.**

Q2. Find the location, where these mail servers are located

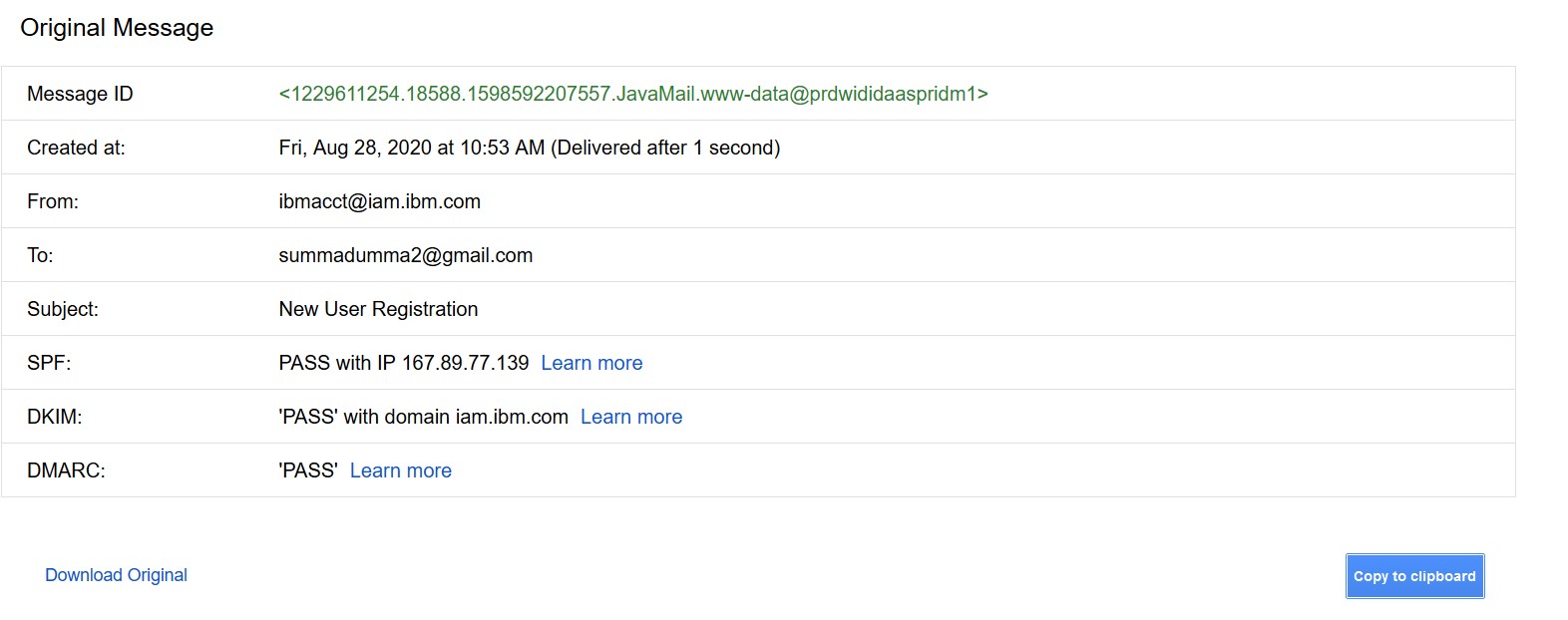
Solution:

1. To find the location of the mail servers we need to receive email from the domain in order to obtain the Email Headers
2. Hence Go to ibm.com and register for credentials to receive a mail with confirmation code

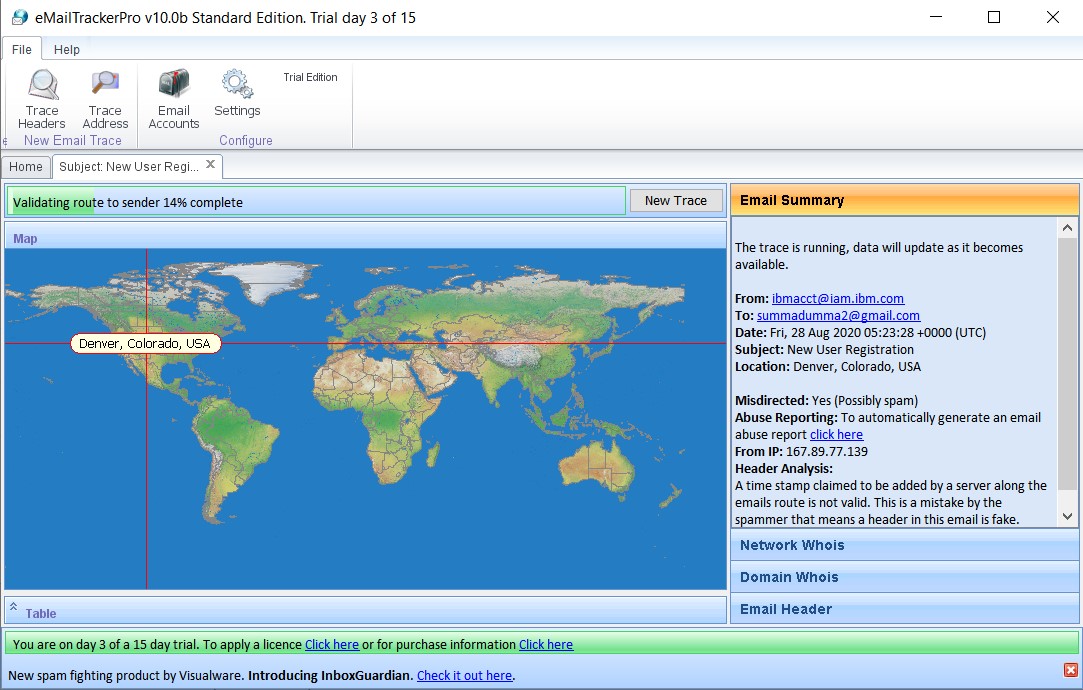




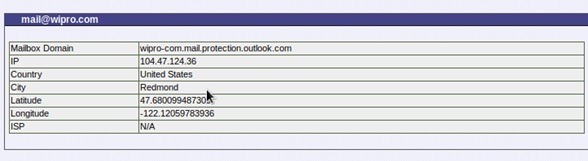
1. In the mail, we can click on SHOW ORIGINAL option to get the headers of the mail, which will look like this, Click Copy to clipboard



1. Open eMailTrackerPro and click Trace headers and paste the headers to obtain the location of mail server



1. Repeat the same for wipro.com and obtain the location



Therefore

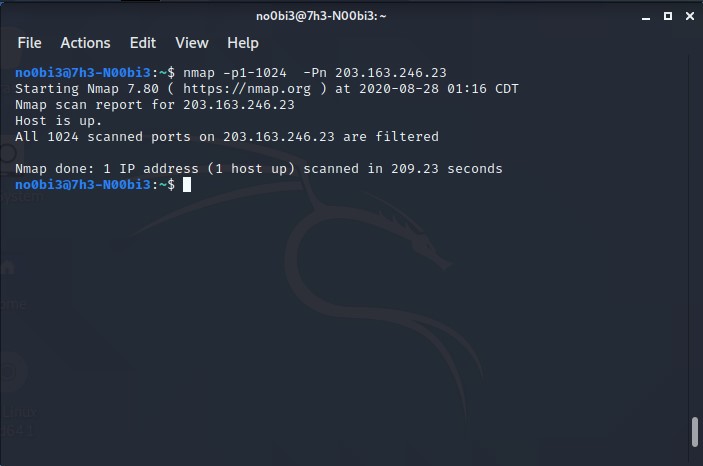
We can obtain the location of these mails server which are listed below:

|  |  |
| --- | --- |
| **DOMAIN** | **MAIL SERVER LOCATION** |
| Ibm.com | Denver,Colorado,USA |
| Wipro.com | Redmond, USA |

Q3:Scan and find out the port numbers open 203.163.246.23

Solution:

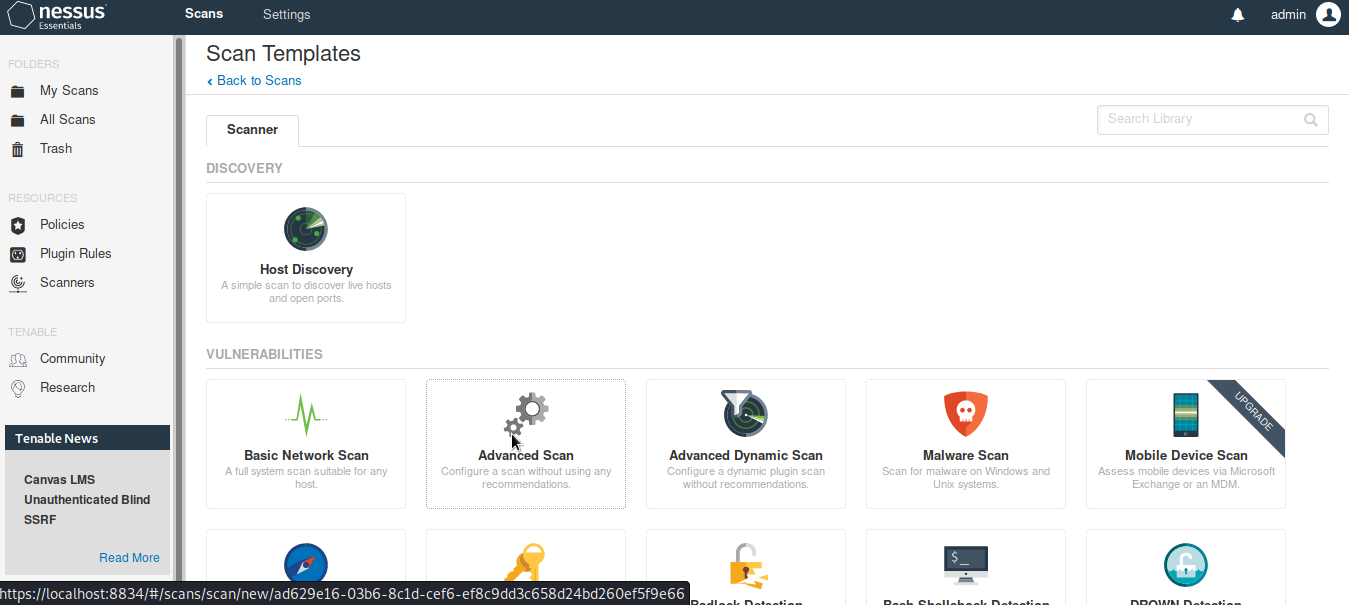
1. Open terminal in Kali linux
2. We will use nmap to find ports that are open on the target IP
3. Type nmap p1-1024 –Pn 203.163.246.23
4. We can find that there are no open ports and all ports have been filtered



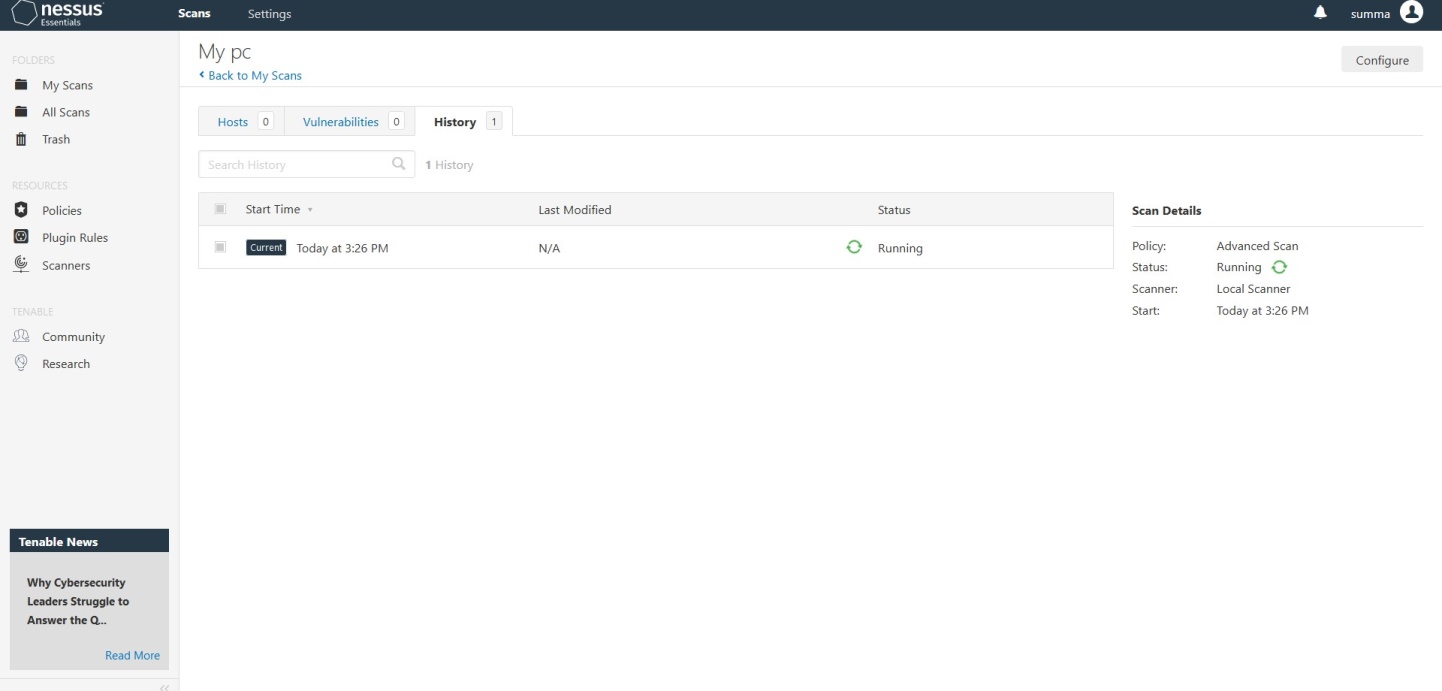
Q4: Install Nessus in a VM and scan your laptop/desktop for CVE

Solution:

1. Register and download Nessus from tenable
2. Click on New scan
3. Choose Advance scan and enter you laptop/desktop IP address for CVE scan



1. Wait for the scan to complete



Thus we can see the results as follows:

