Q.1 Find out the mail servers of the following domain:

Ibm.com

Wipro.com

Ans. 1. Open cmd.

2. Then type nslookup.

3. Now for IBM mail servers type nslookup -type=mx [www.ibm.com](http://www.ibm.com) and hit enter.

4. You will see result same as in image.



For Wipro.com follow same steps as above:

1. Open cmd.

2. Then type nslookup.

3. Now for Wipro mail servers type nslookup -type=mx [www.wipro.com](http://www.wipro.com) and hit enter.

4. You will see same result as in image.



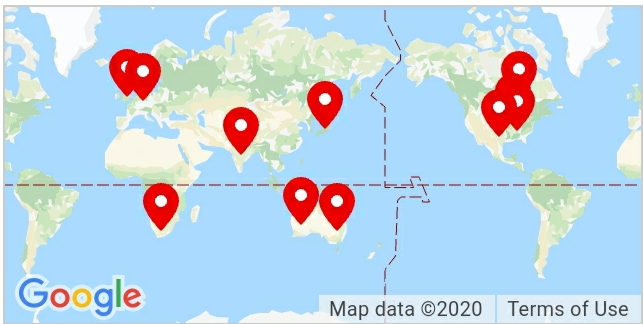
Q.2 Find the locations, where these mail servers are hosted.

Ans.

* IBM mail server location (used sowramac@in.ibm.com):



* Wipro mail server location (used info@wipro.com):



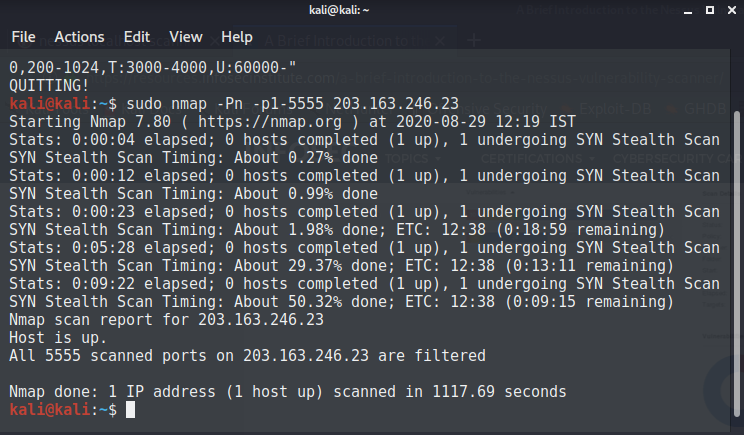
Q.3 Scan and find out port numbers open on 203.163.246.23

Ans.

* In Kali linux open up a Terminal.
* Then type sudo nmap -Pn -p1-65535 203.163.246.23 and hit enter.

And here -Pn means Treat all hosts as online .

And -p1-65535 means from port 1 to port 65535 scan all.



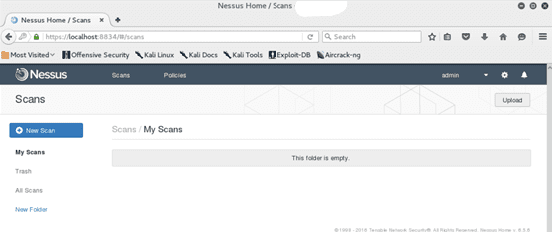
Q.4 Install nessus in a VM and scan your laptop/desktop for CVE.

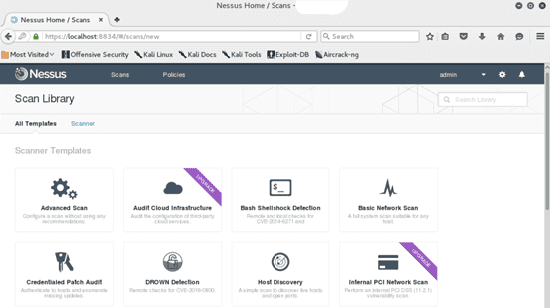
Ans. 1. Download and Install nessus from [www.tenable.com](http://www.tenable.com)

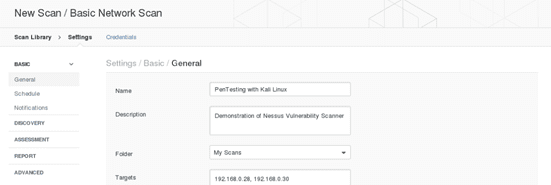
2. After Installing you need to do some basic setup, after that

3. Launching a nessus scan:

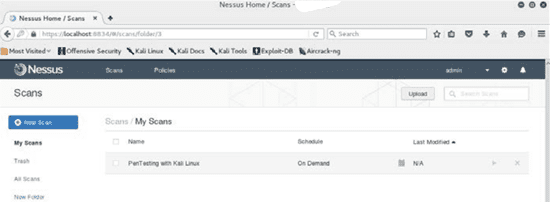
* To perform it you would need to navigate your browser to the link <https://localhost:8834>. See below:

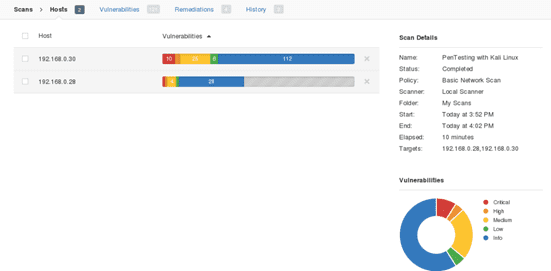


4. Hit the “New Scan” button above, then select the type of scan to perform from the numerous templates available 



5. As can be seen above, you would then issue your targets. Nessus is capable of performing scans on multiple targets separated by commas or issued in CIDR format. Once done, you will be redirected to the screen below.



6. Click the “play” icon to launch your configured scan. It is possible to have multiple configured scans, allowing you to perform multiple scans. In the screen above, we configured just one scan. Below, you can however see results from two hosts summarizing the severity and instances of issues discovered.

7. Nessus even allows you to drill down to specific hosts and vulnerabilities and get more information on how they were discovered, together with recommendations on how to patch identified risks. See below:

