

# Assignment Day 4 | 23rd August 2020

## By Sameer Kulkarni

**Question 1:** Find out the mail servers of the following domain:

lbn.com

Wipro.com

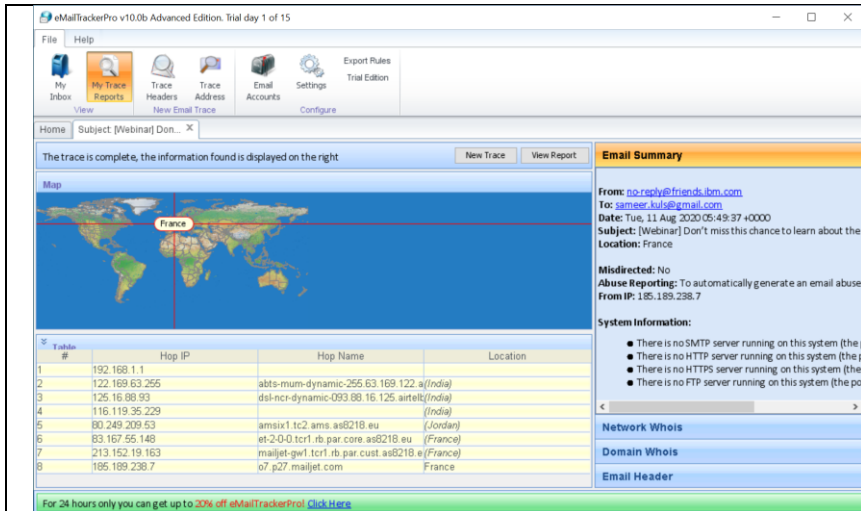
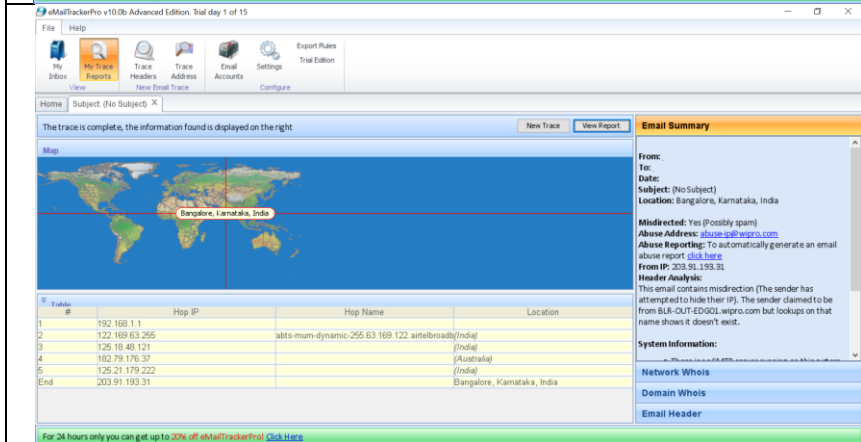
**Answer 1:** The mail servers of domains can be found with following Commands

nslookup

<pre>Administrator: Command Prompt - nslookup  C:\Users\Administrator&gt;nslookup Default Server: Unknown Address: 192.168.208.2  &gt; set type=mx &gt; www.lbn.com Server: Unknown Address: 192.168.208.2  Non-authoritative answer: www.lbn.com canonical name = www.lbn.com.cs186.net www.lbn.com.cs186.net canonical name = outer-ccdn-dual.lbncom.edgekey.net outer-ccdn-dual.lbncom.edgekey.net canonical name = outer-ccdn-dual.lbncom.edgekey.net.globalredir.akadns.net outer-ccdn-dual.lbncom.edgekey.net.globalredir.akadns.net canonical name = e2874.dscx.akamaiedge.net dscx.akamaiedge.net primary name server = n0dscx.akamaiedge.net responsible mail addr = hostmaster.akamai.com serial = 1508434187 refresh = 1000 (16 mins 40 secs) retry = 1000 (16 mins 40 secs) expire = 1000 (16 mins 40 secs) default TTL = 1800 (30 mins)  &gt;</pre>	<p>The mail server of lbn.com is hostmaster.akamai.com</p>
<pre>Administrator: Command Prompt - nslookup  C:\Users\Administrator&gt;nslookup Default Server: Unknown Address: 192.168.208.2  &gt; set type=mx &gt; www.wipro.com Server: Unknown Address: 192.168.208.2  Non-authoritative answer: www.wipro.com canonical name = d361nqn33s63ex.cloudfront.net d361nqn33s63ex.cloudfront.net primary name server = ns-1658.awsdns-15.co.uk responsible mail addr = awsdns-hostmaster.amazon.com serial = 1 refresh = 7200 (2 hours) retry = 900 (15 mins) expire = 1209600 (14 days) default TTL = 86400 (1 day)  &gt;</pre>	<p>The mail server of wipro.com is awsdns-hostmaster.amazon.com</p>

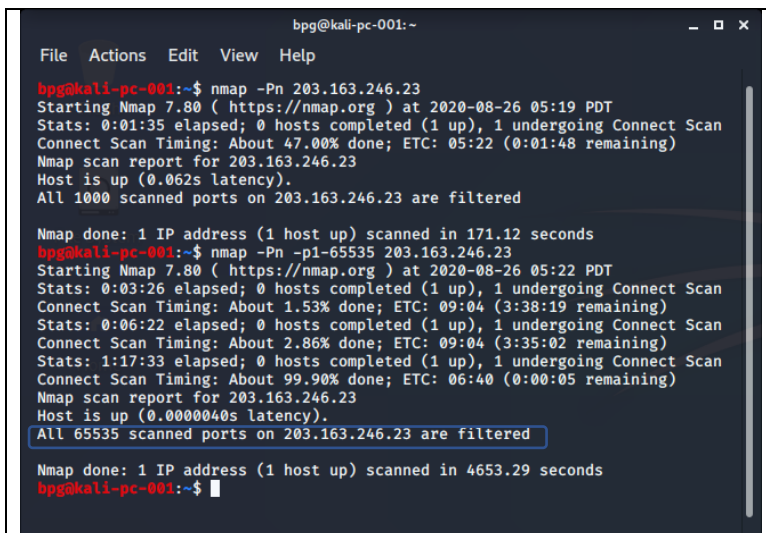
**Question 2:** Find the locations, where these email servers are hosted.

**Answer 2:**

	<p>I had a mail from IBM Watson. The email header was used in emailtrackerpro. The mail server of ibm.com is located in France.</p>
	<p>The email header was used in emailtrackerpro. The mail server of wipro.com is located in Bangalore, India.</p>

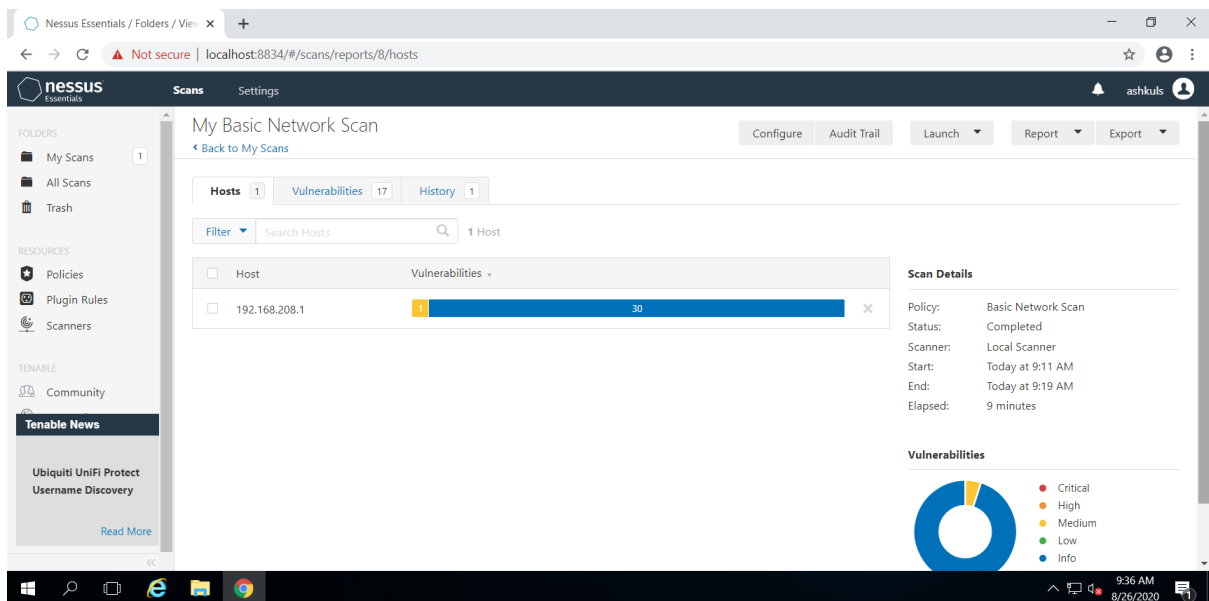
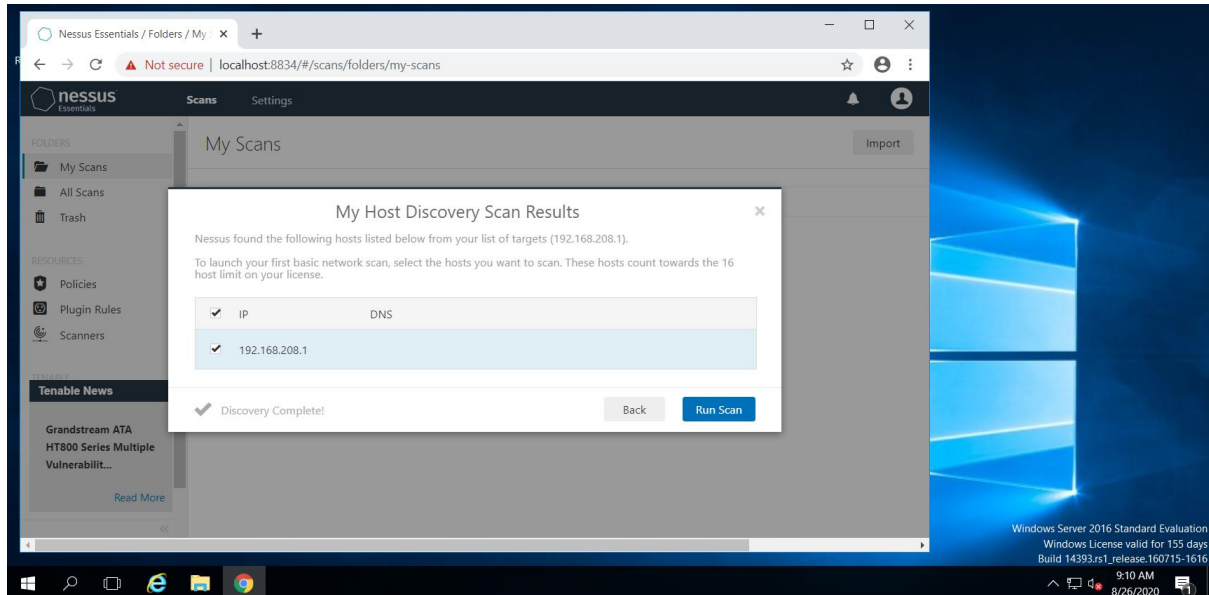
**Question 3:** Scan and find out port numbers open 203.163.246.23

**Answer 3:** The ports open for any system can be found out with **nmap**.

	<p>The open ports found with the nmap command are as follows: Nil Open Ports. All are filtered.</p>
---	---

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

**Answer 4:** Nessus was installed in VM and my laptop was scanned for CVE. The screenshots are as follows:



There was only one Medium vulnerability about SMB Signing not required, which is irrelevant for my Windows 10 Home edition without domain and hence was not resolved.