**Lets Upgrade Cyber Security | August 2020**

**Assignment Day 4 | 23rd August 2020**

**Submitted By: Piyush Choudhary [ choudharypiyush08@gmail.com ]**

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

* **Ibm.com**
* **Wipro.com**

**Sol 1:**

Opened CMD in the host machine.

Used the command nslookup to open nslookup tool.

Set the type to mail exchange server to search only for mail servers using set type=mx

Next, the domain name to be searched for is given.

Mail servers of the given domains are as follows:

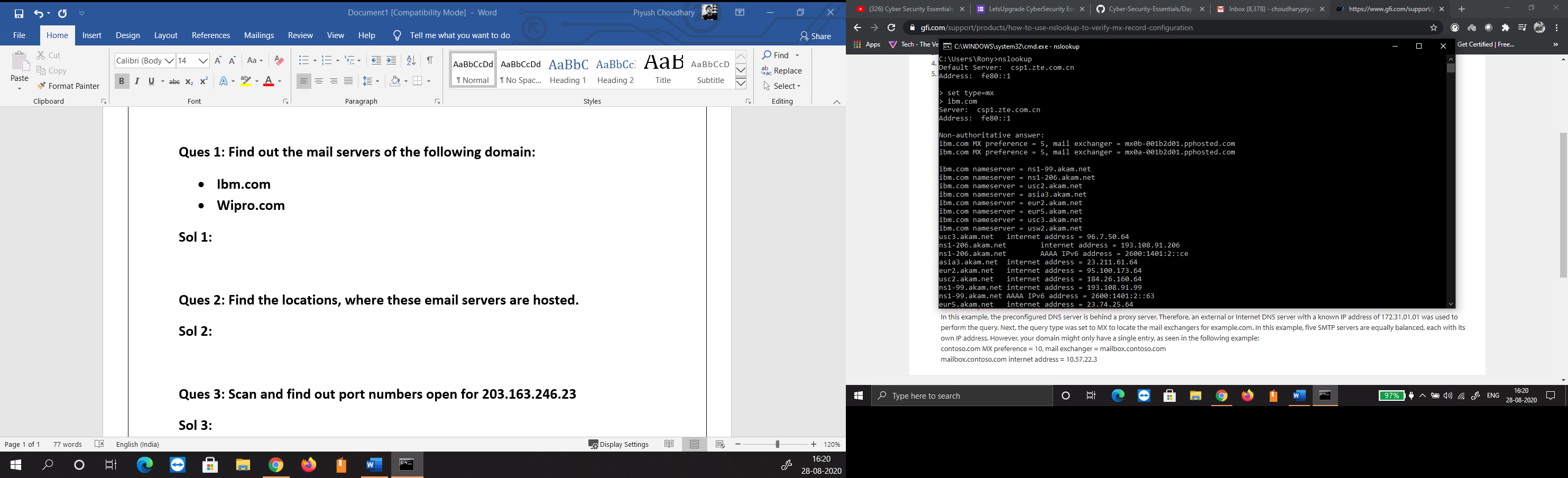


Fig 1.1 Search Results for ibm.com

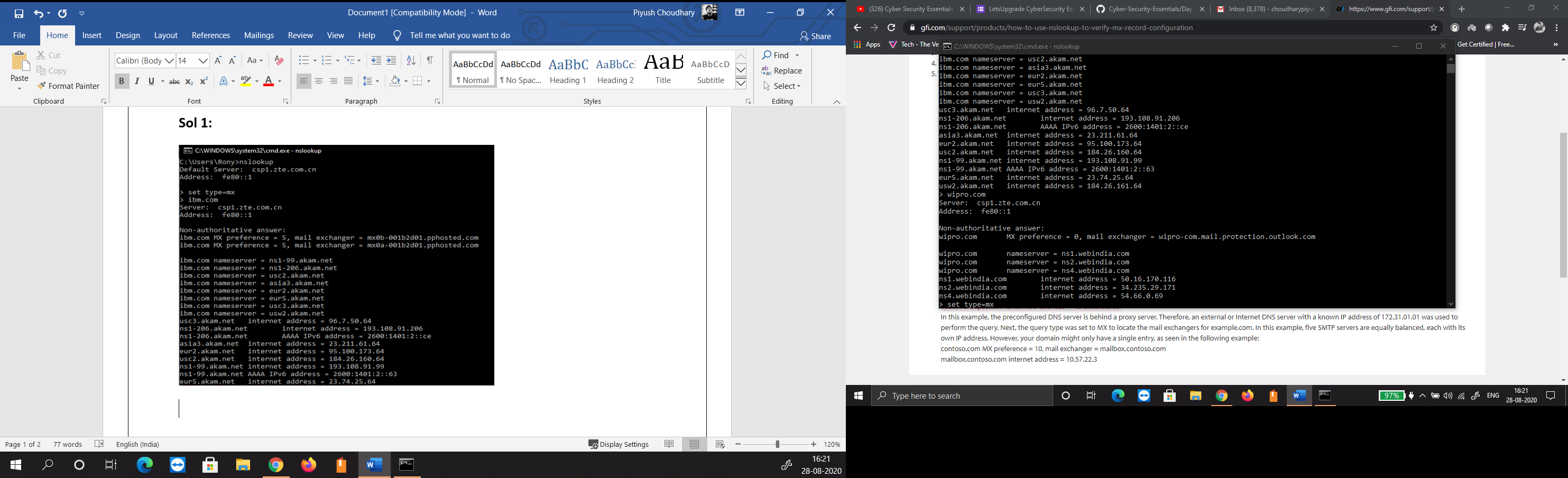


Fig 1.2 Search Results for ibm.com

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

**Sol 2:** Locations for the servers [mail@ibm.com](mailto:mail@ibm.com) and [mail@wipro.com](mailto:mail@wipro.com) are as follows:

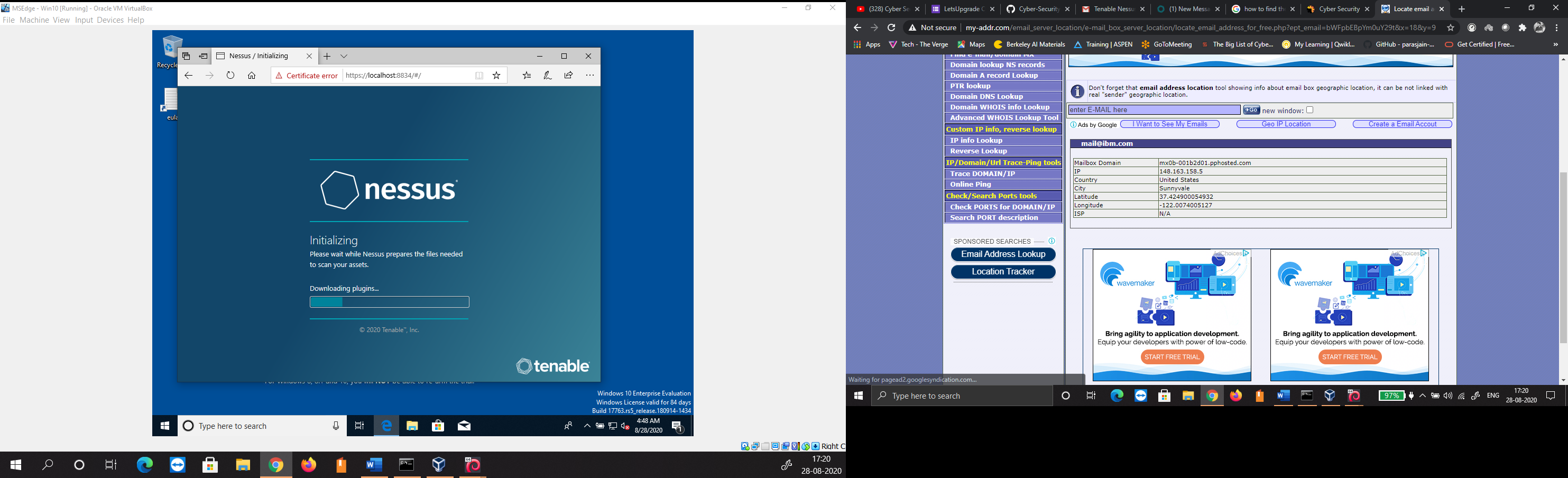


Fig 2.1 Location for the mail@ibm.com

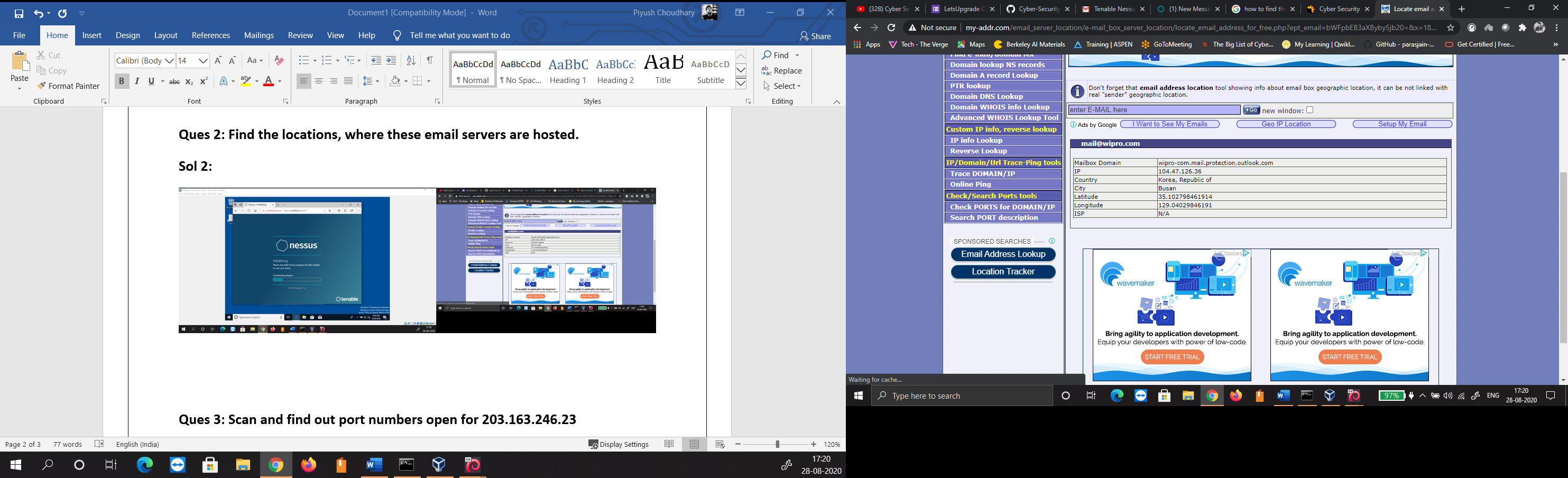


Fig 2.2 Location for the mail@wipro.com

**Ques 3: Scan and find out port numbers open for 203.163.246.23**

**Sol 3:**

Opened Terminal in Kali VM.

Used the command nmap -p1-65535 203.163.246.23 to start the scan for the given IP.

All the 65535 ports for the given IP are filtered thus NMAP is unable to detail it as Open or Closed. Scan report for the given IP is as follows:

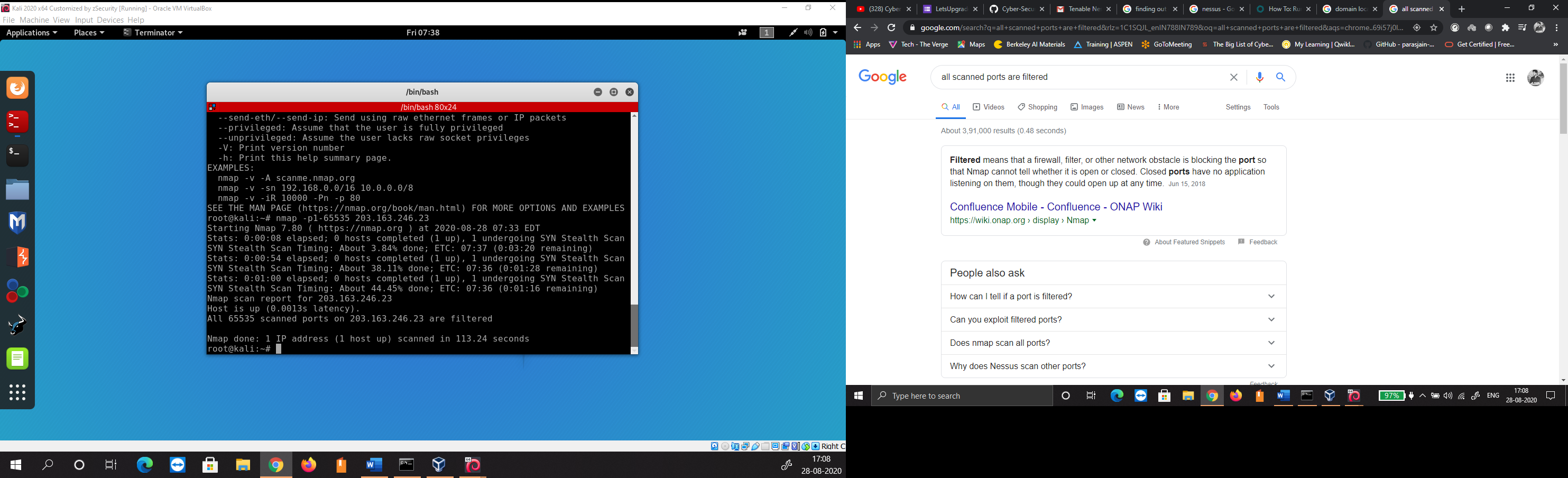


Fig 3.1 Scan Results for 203.163.246.23

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

**Sol 4:**

Opened Windows10 VM.

Downloaded Nessus and Installed it.

Scanned the host machine for CVE using Nessus in VM as follows:

Setting up an advanced scan for the target 10.0.2.13 -

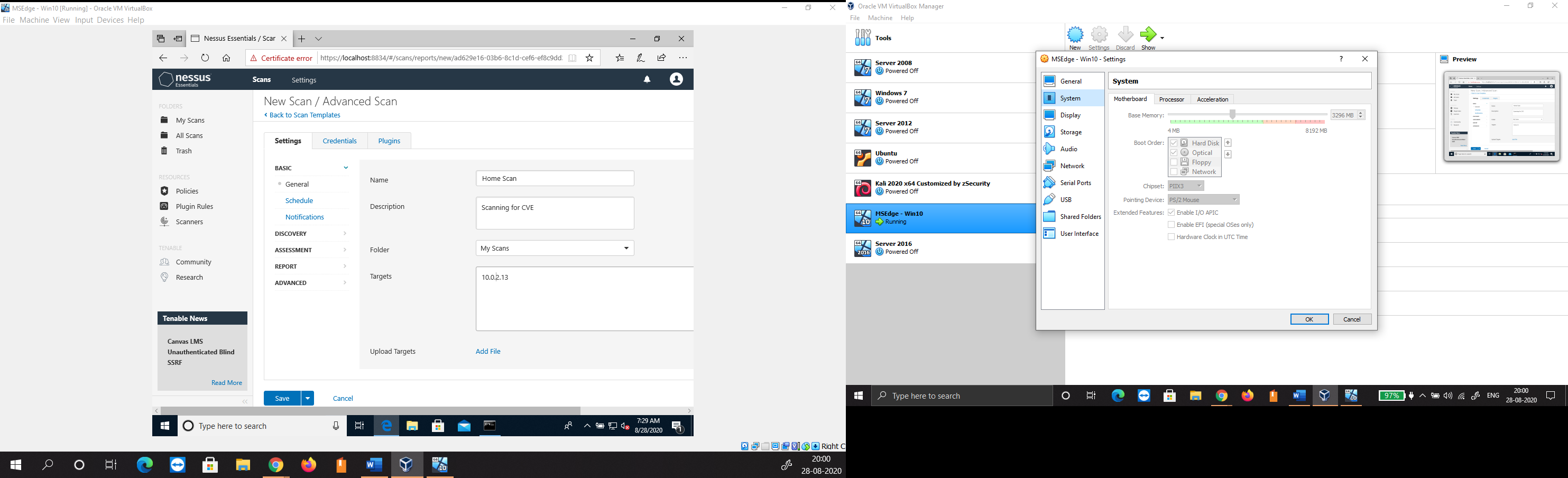


Fig 4.1 Setting up an advanced scan

Scan Generated -

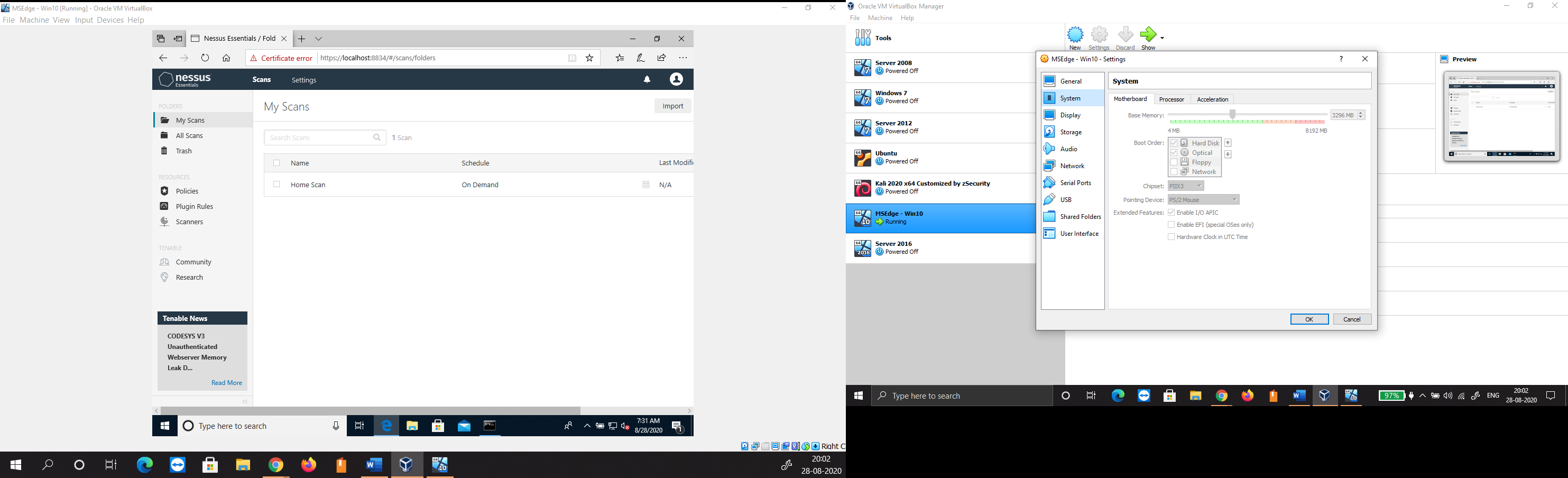


Fig 4.2 Scan Generated

Scan Initiated -

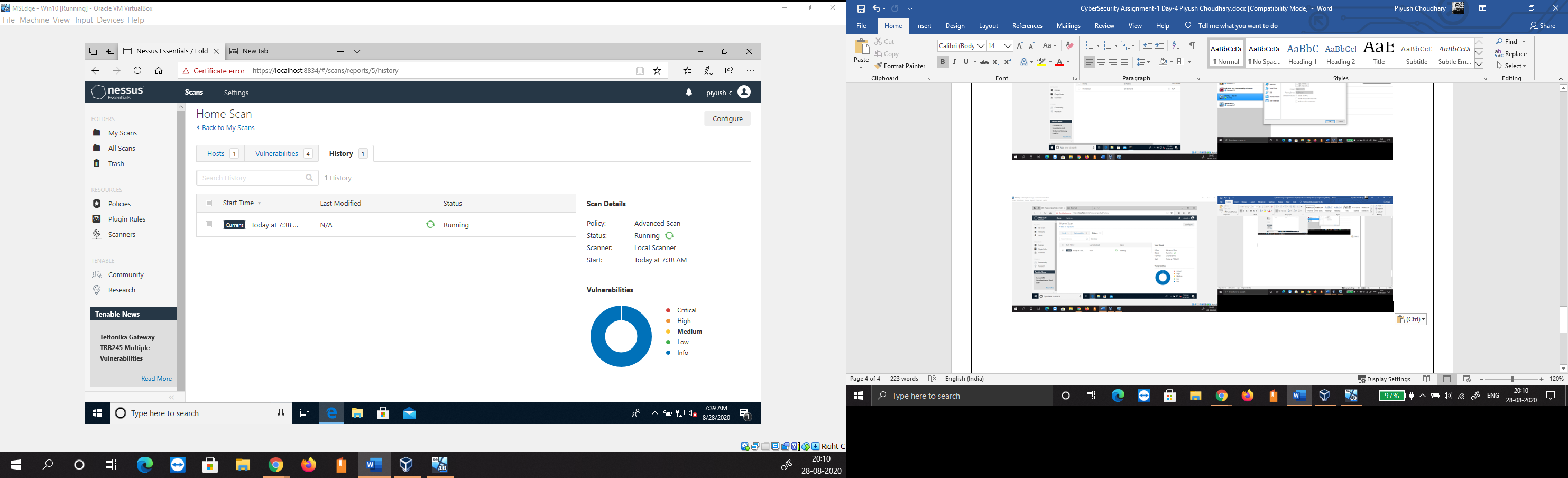


Fig 4.3 Scan Initiated

Scan Completed -



Fig 4.4 Scan Completed

Vulnerabilities Found – Total = 13

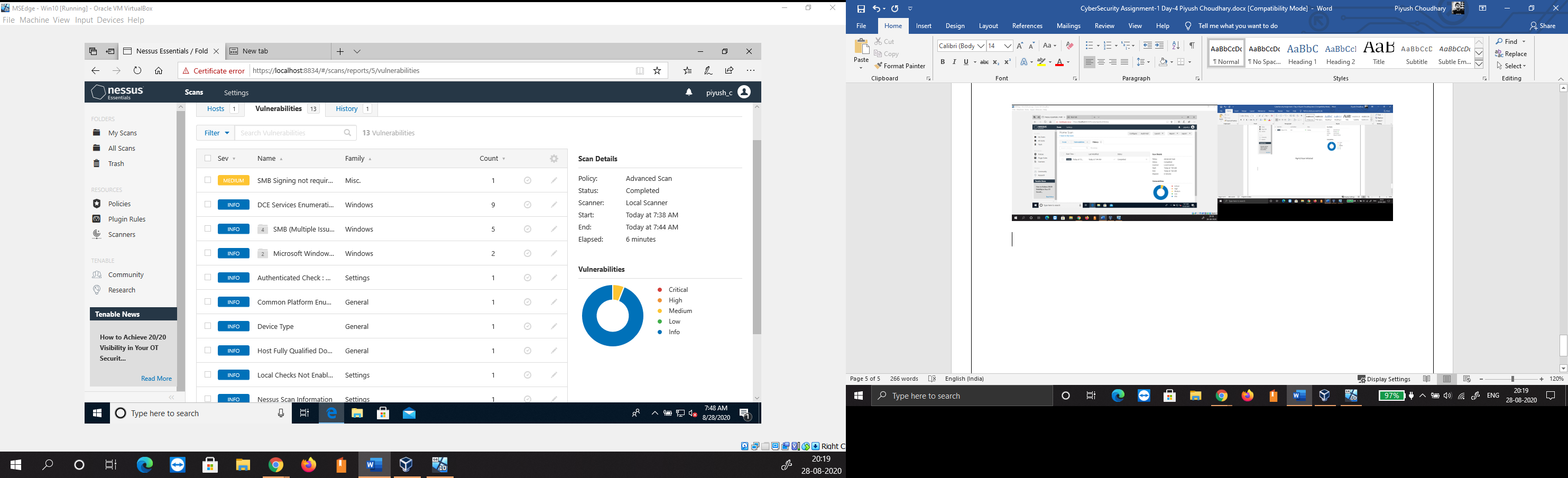


Fig 4.5 Vulerabilities Found

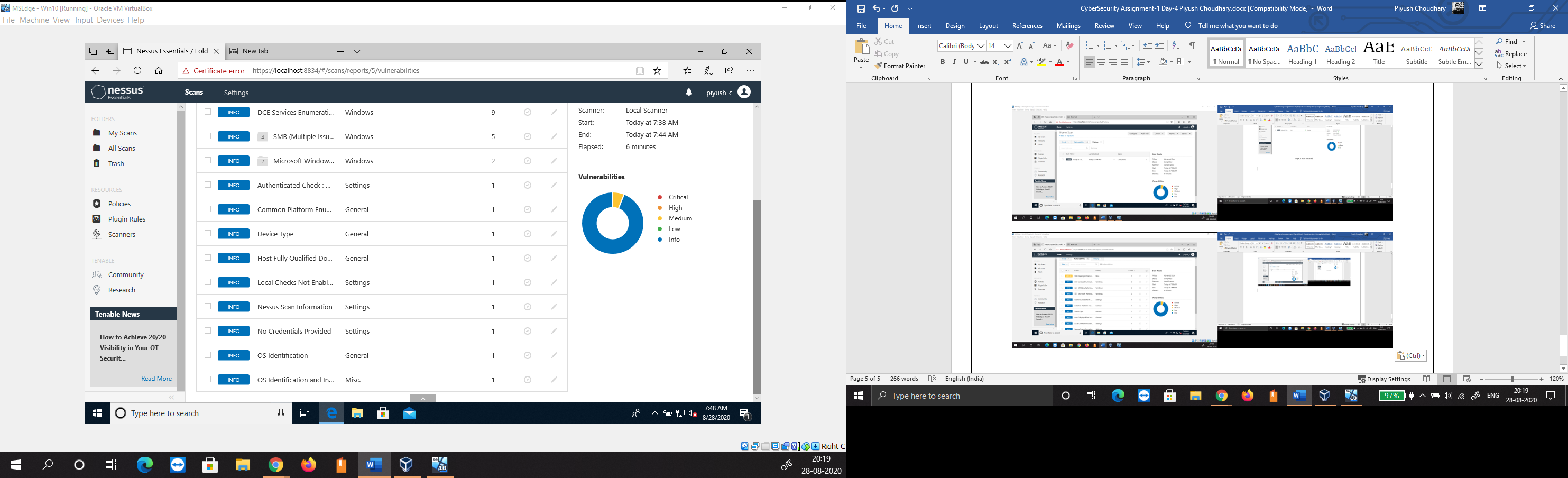


Fig 4.6 Vulerabilities Found