**Cyber Security Essentials | Batch 1 | Day 4 LetsUpgrade Assignment Day 4 | 23rd August 2020**

**Question 1:**

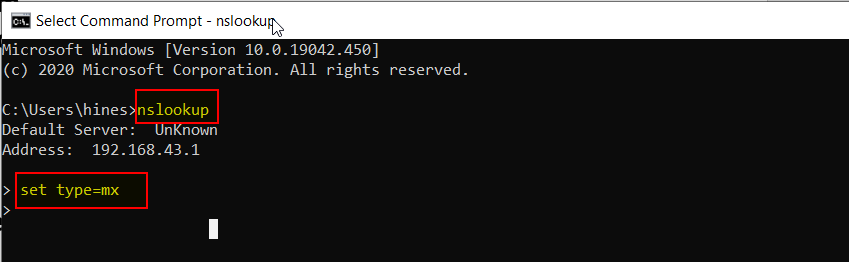
**Find out the mail servers of the following domain :**

**(1) Ibm.com**

**(2) Wipro.com**

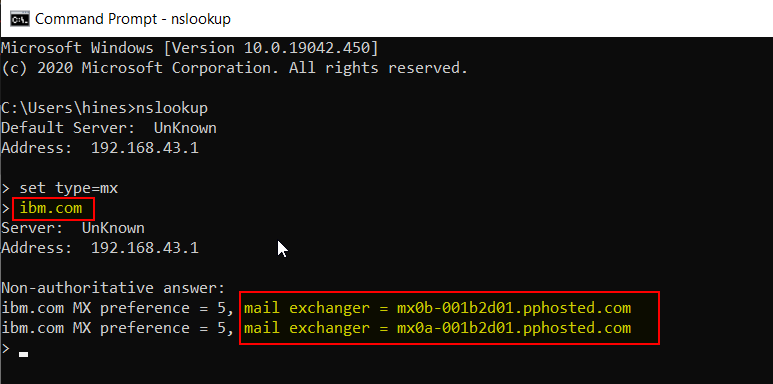
**Answer:-**

* **First Open CMD and type nslookup ,**
* **Then type set type=mx for finding mail server.**

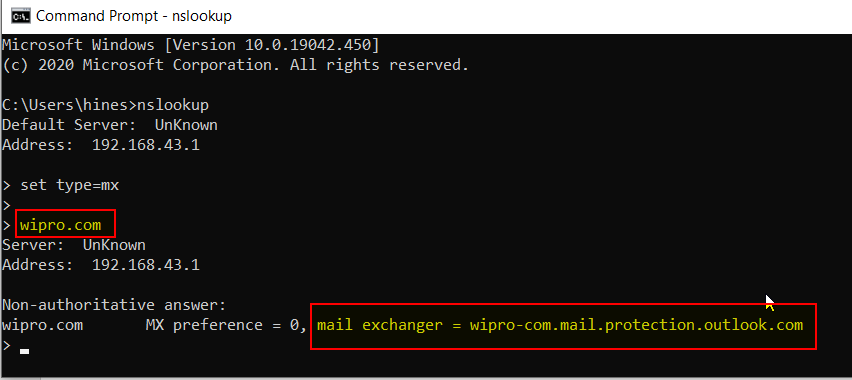
****

* **Then type the domain name that you want to find that mail server?**

**(1). Ibm.com :-**

****

**(3). Wipro.com :-**

****

**Question 2:**

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

**Answer :-**

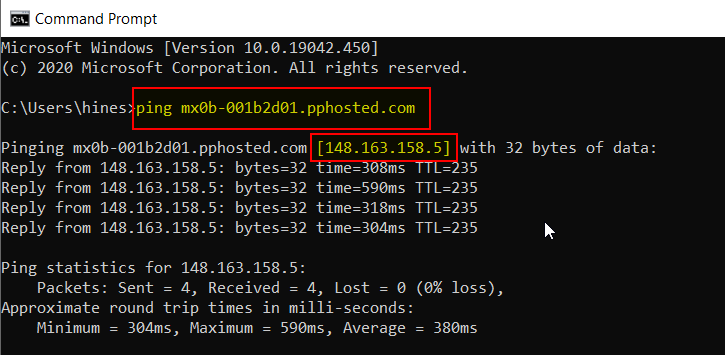
**First, in CMD using ping command find IP ADDRESS of theres mailserver.**

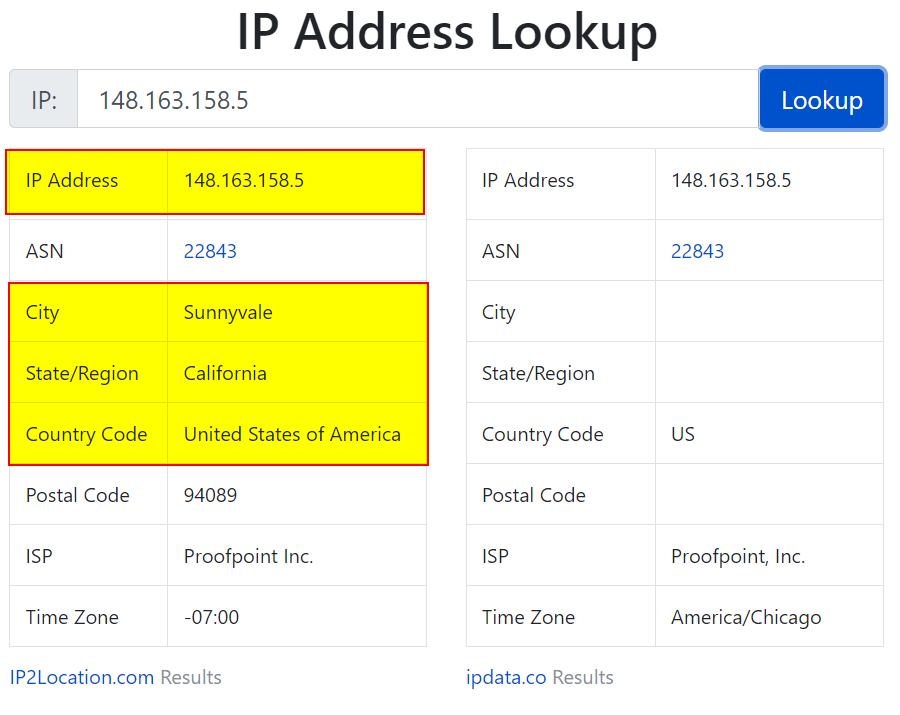
**Then using IP Address find Their Location of mail server using this link.**

**Link:-** <https://www.whatismyip.com/ip-address-lookup/>

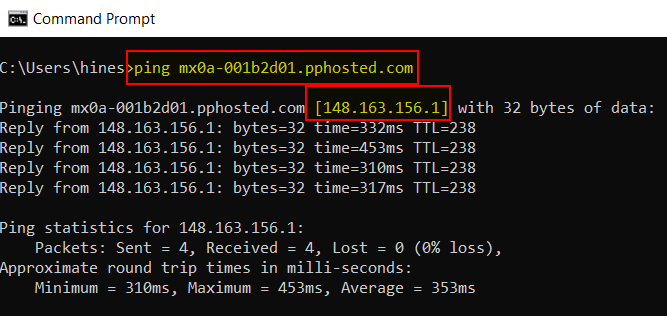
**1.Location Ibm.com mailserver :-**

1.mx0b-001b2d01.pphosted.com:-

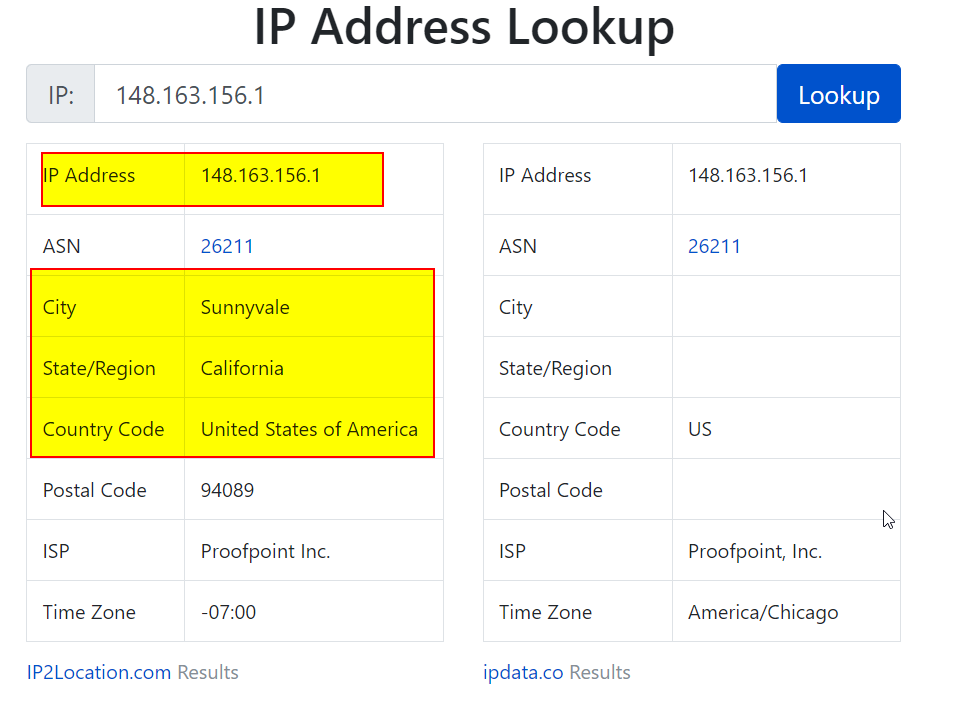


**Then Using IP Address find their location:-** ****

2.mx0a-001b2d01.pphosted.com:-

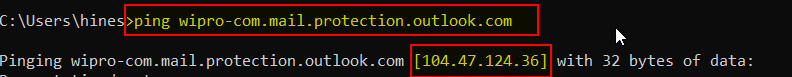
****

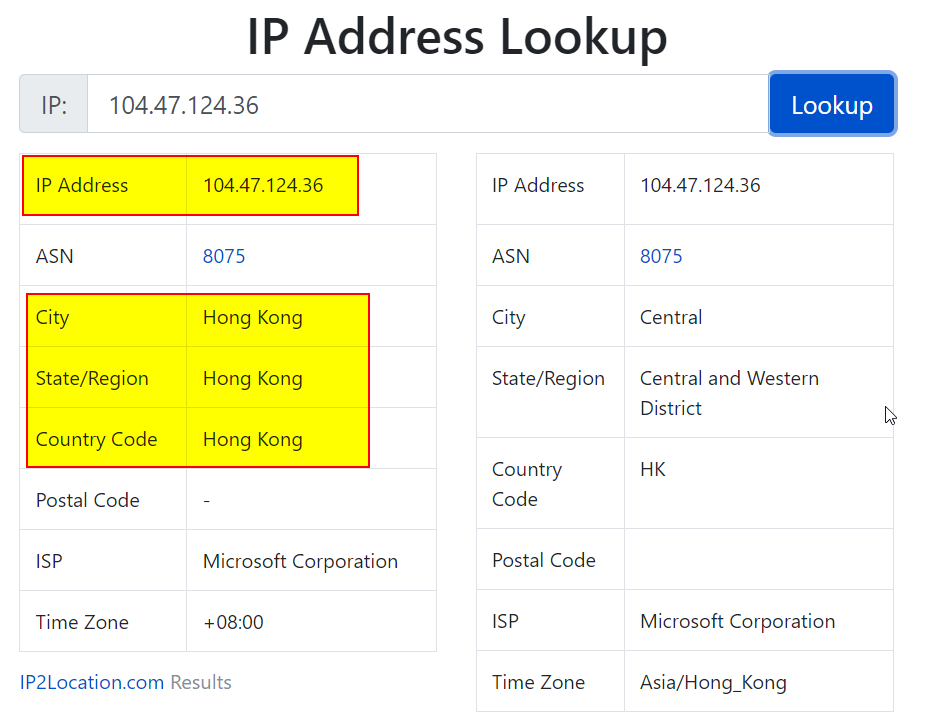
**Then Using IP Address find their location:-**



**2.Location wipro.com mailserver :-**

wipro-com.mail.protection.outlook.com:-

**Then Using IP Address find their location:-**

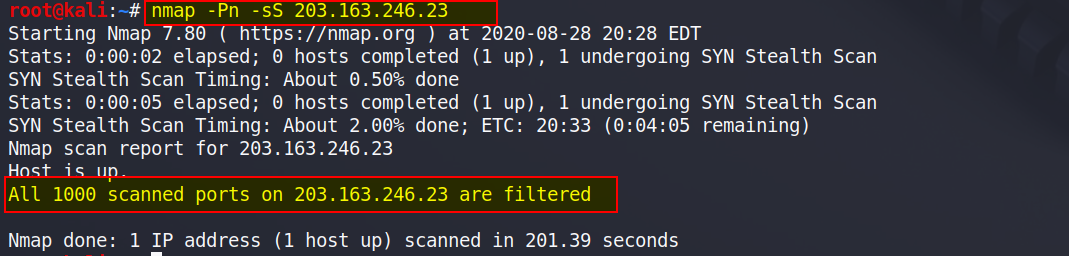


**Question 3:**

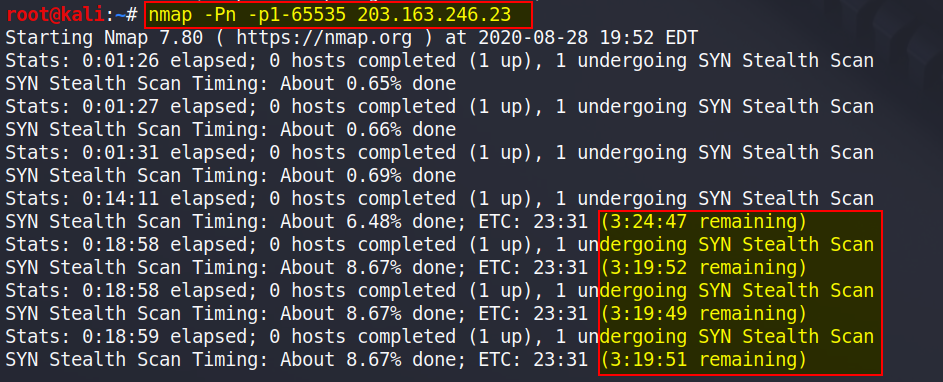
**Scan and find out port numbers open 203.163.246.23**

**Answer:-**

**There are no found any open ports of 203.163.246.23 IP Address.All scan ports are filtered.**

****

**Note:- All ports scanning take more than 4 hours of time. So, I did not use it.**

****

**Question 4:**

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

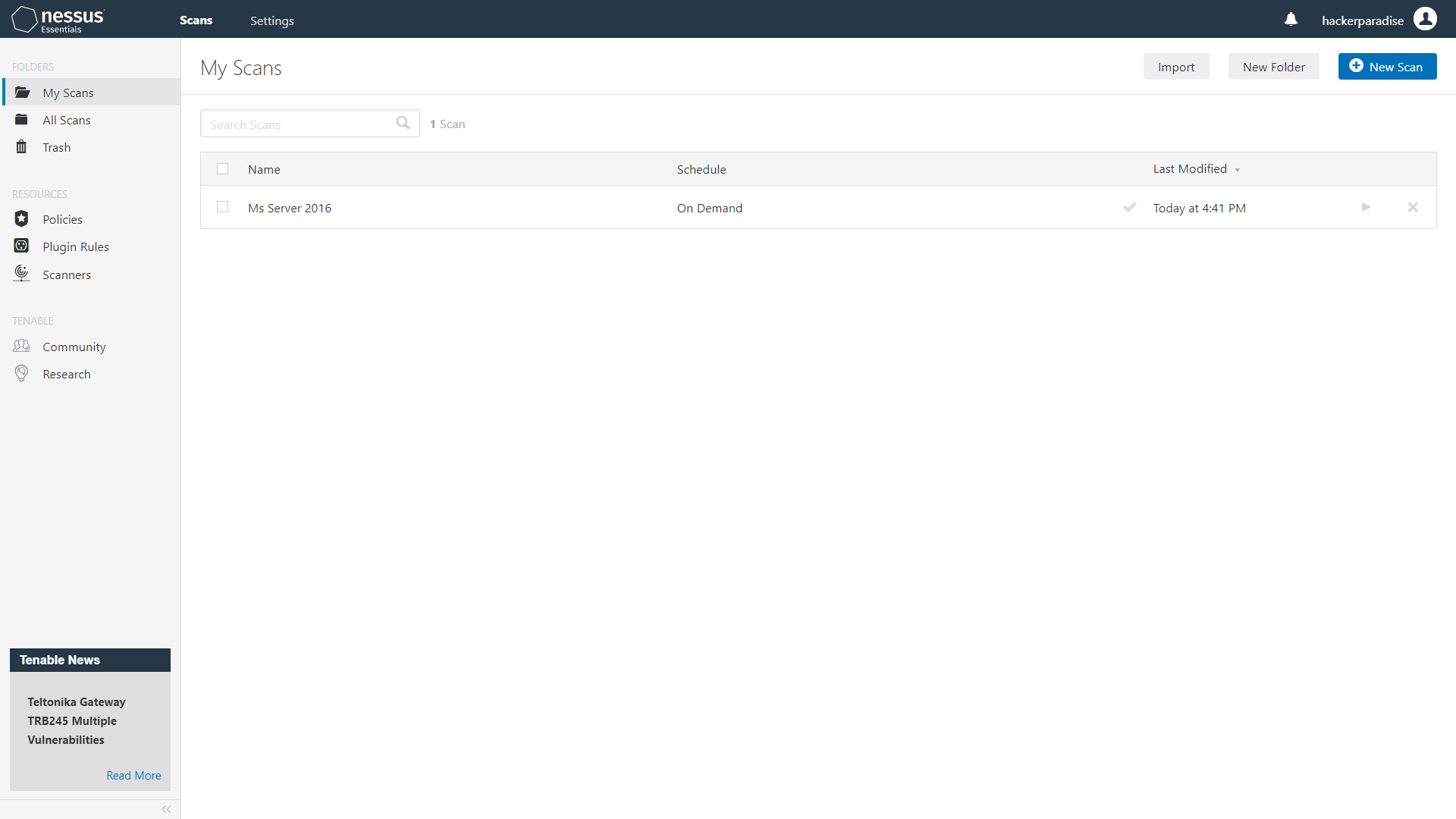
**Answer:-**

**First download and install Nessus in Windows Virtual Machine.**

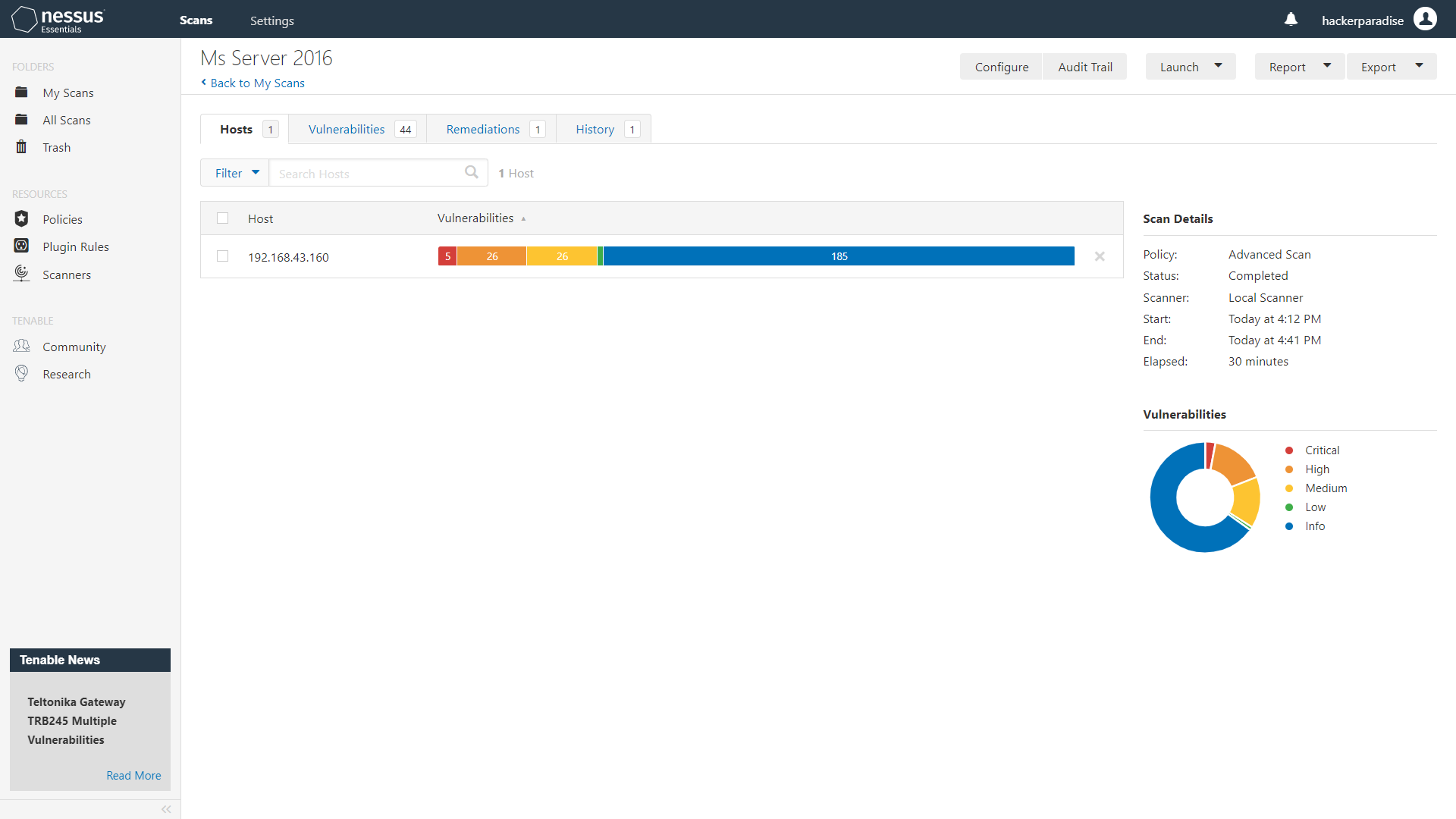
**Then Open Nessus in browser through the link then put licence key and start services.**

**Next, step go to new scan then advance scan**

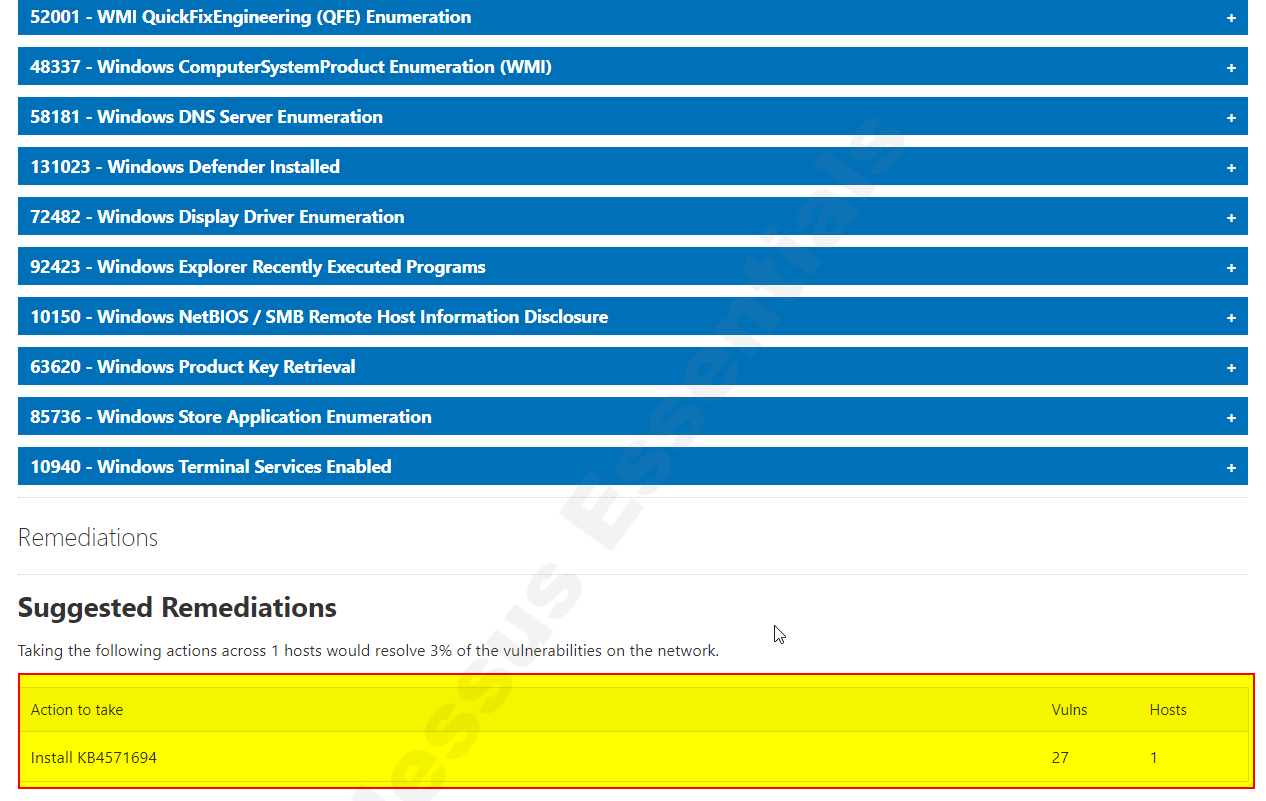
**Then fill up necessary details and then scan and scanning is started:-**

****

**After scanning completed click on scanning process and see your system report:-**

****

**To generate report click on Report and then custom and report generate in HTML file and find your vulnerability remediation at bottom of the report:-**

****