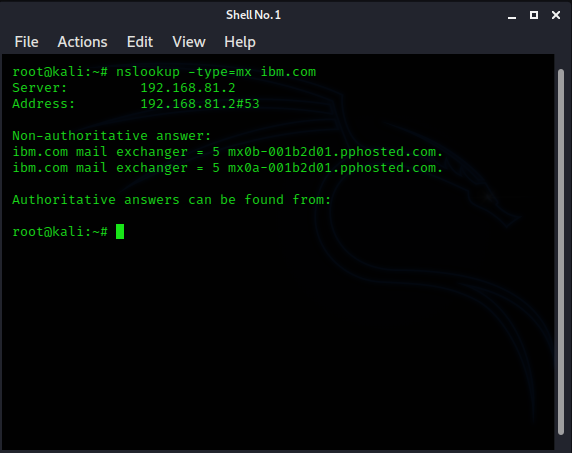
**Day 4 Assignment**

**By Krishanu Bepari (kbepari52@gmail.com)**

**(User name - kbepari529206)**

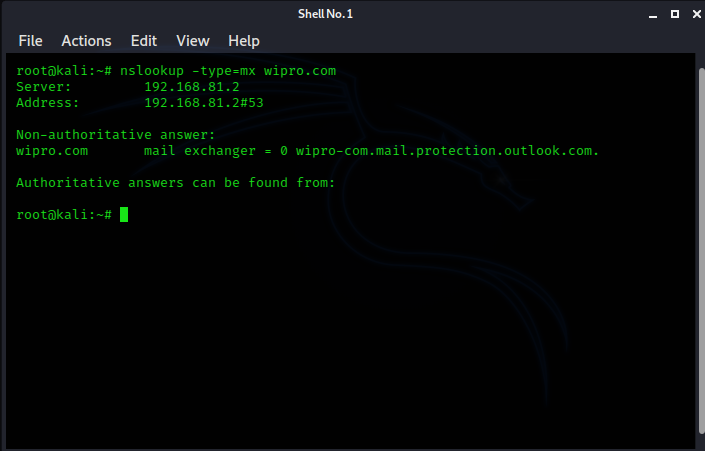
1. **Mail Servers**

* open terminal in kali Linux
* and simply type **‘nslookup -type=mx (domain name)’**
* **ibm.com**

****

So, here we can see that, there are 2 mail servers:

* **mx0b-001b2d01.pphosted.com.**
* **mx0a-001b2d01.pphosted.com.**
* **wipro.com**

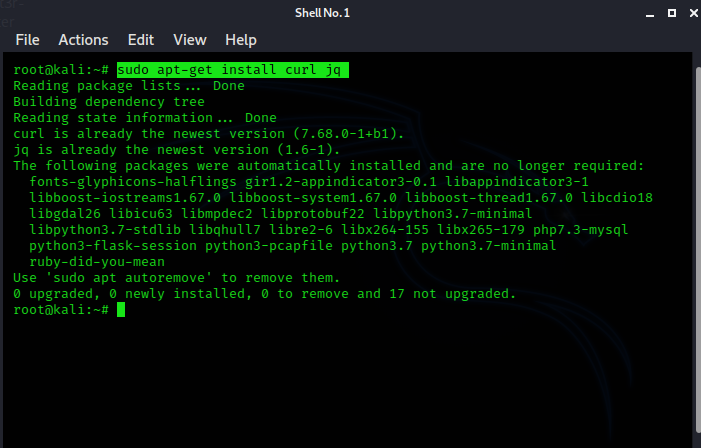
****

So, here we can see that, there are 1 mail server:

* **wipro-com.mail.protection.outlook.com**

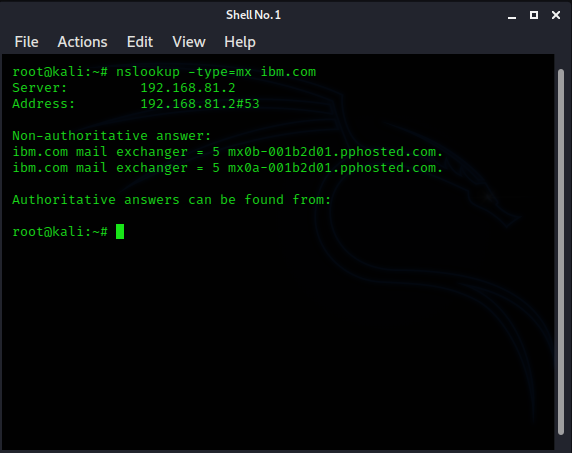
1. **Mail Servers Locations**

* First, we need to install ‘**jq’**
* **( Sudo apt-get install curl jq )**

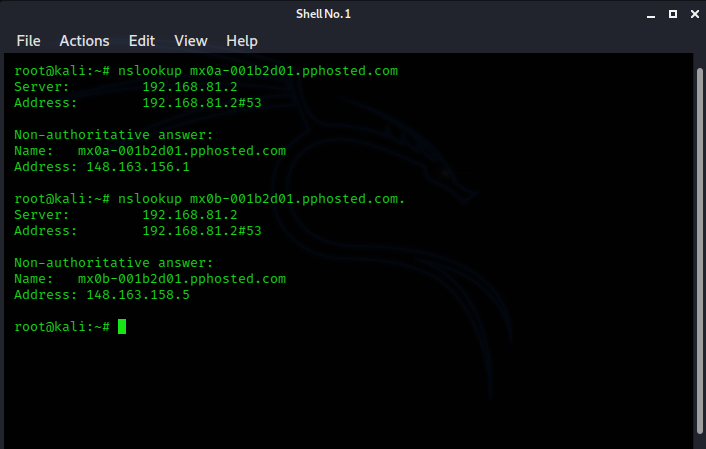
****

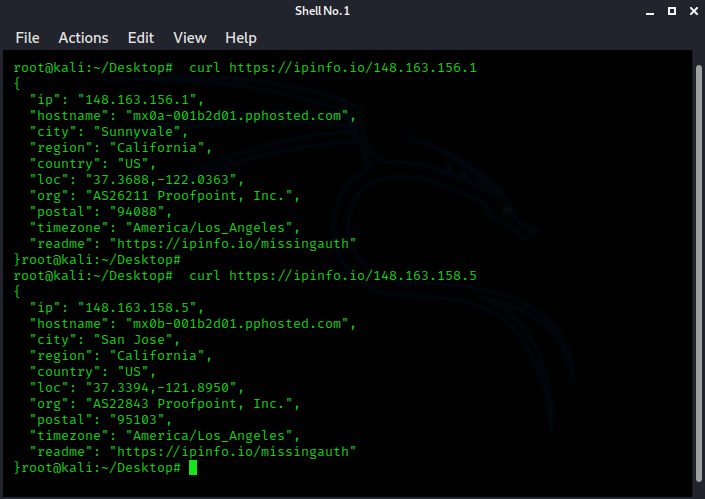
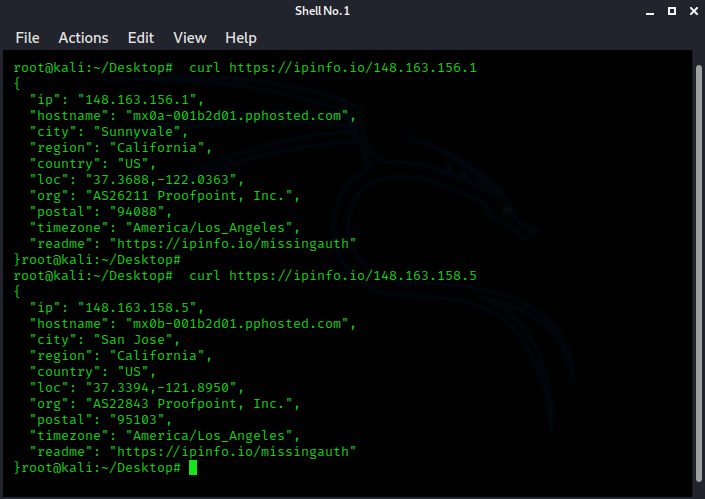
* Then simply find mx details by using **nslookup**
* Then find the mail server addresses from **nslookup**
* And then simply put it on curl **https://ipinfo.io/(address)**
* **ibm.com**

1. **these are our mail servers:**

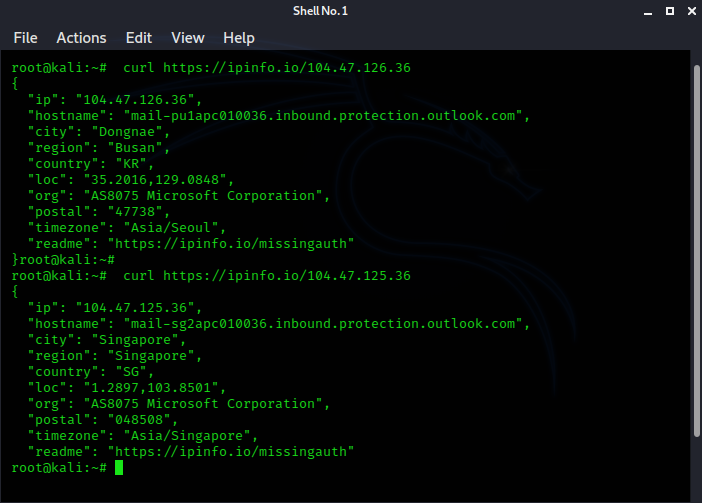
****

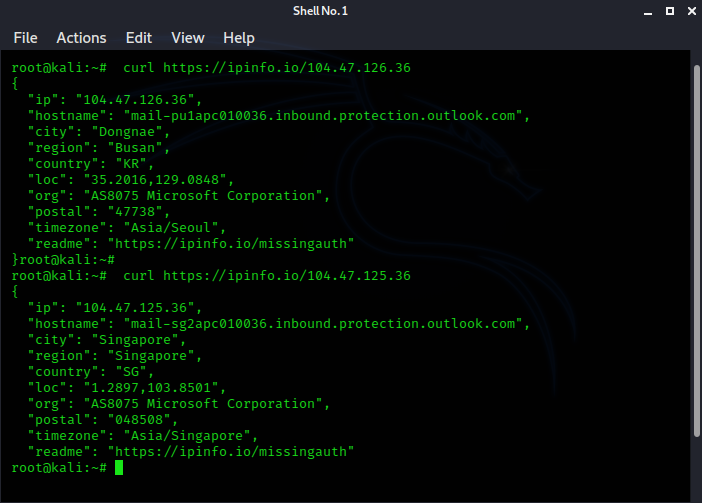
1. **Now find addresses of each mail server:**

****

1. **Now we gonna find each mail servers locations:**

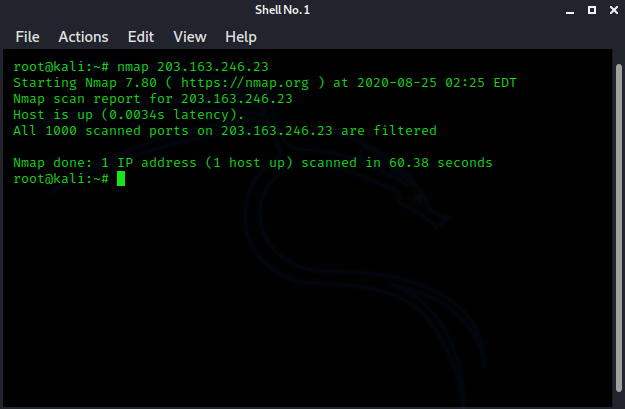
* **wipro.com**

1. **now at the same way we gonna find Wipro mail server address.**
2. **Here we got 2 address. Now we gonna find each addresses location.**



**3) port scanning of 203.163.246.23**

* For port scanning we use **Nmap.**

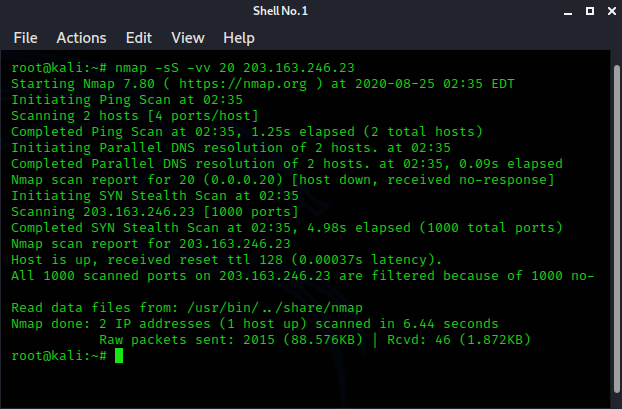
1. **first, we try to scan normally**

**And here we got this. It shows us that ‘host is up’ and all 1000 ports are filtered but doesn’t listed. That means firewall is activate and it block our request.**

**So, we have to apply different method.**

1. **Now at this time we use SYN mode (stealth mode) and verbose mode:**

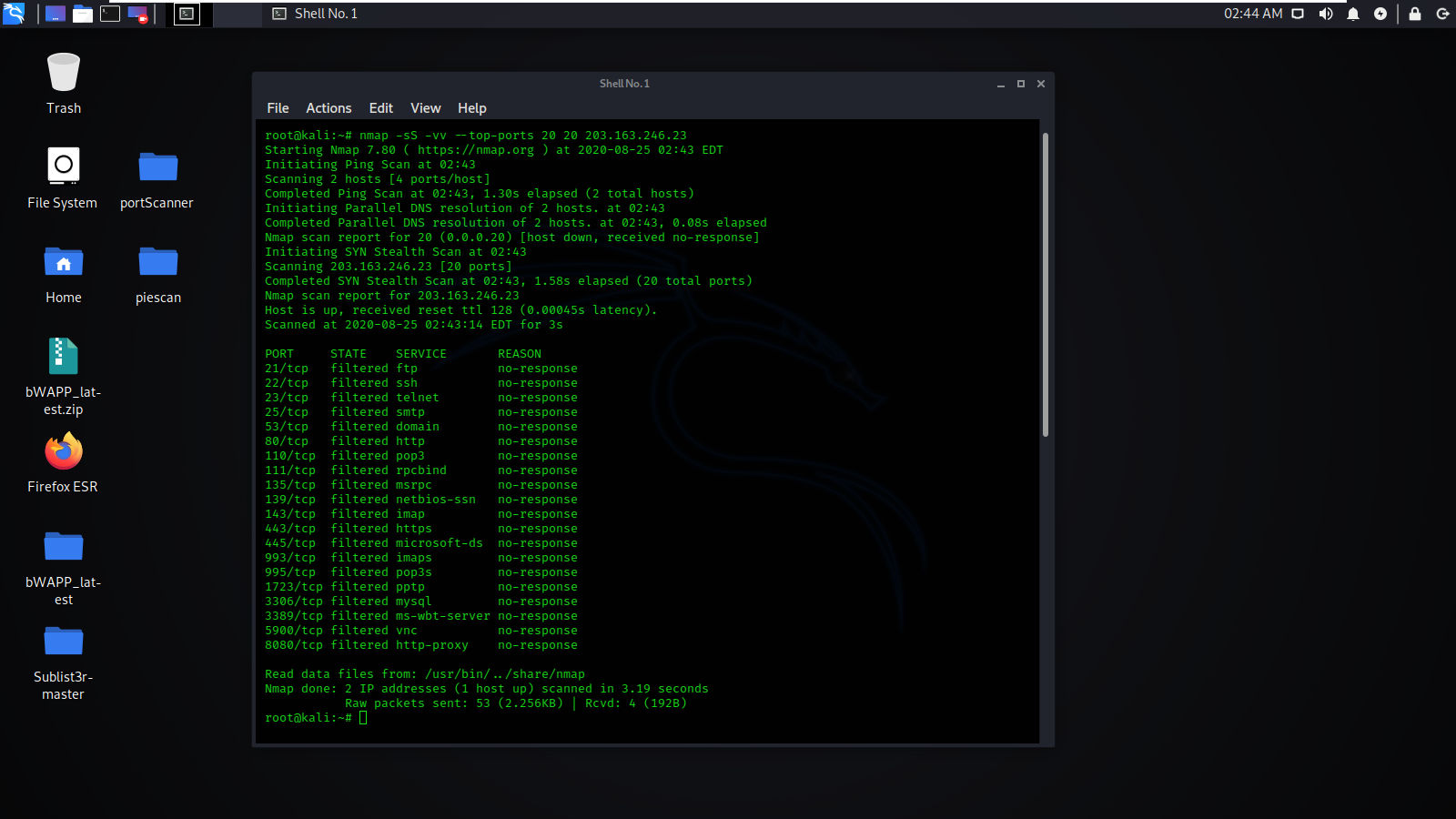
**nmap -sS -vv 20 203.163.246.23**

****

**But at this also the same result, we don’t get the port list.**

1. **So Now we try to scan top 20 ports**

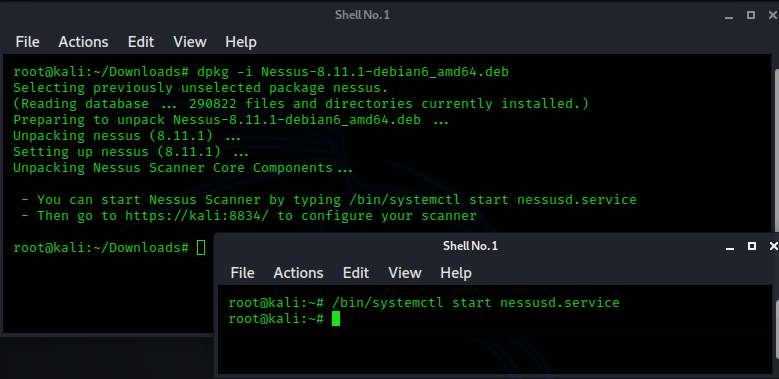
**nmap -sS -vv --top-ports 20 20 203.163.246.23**

****

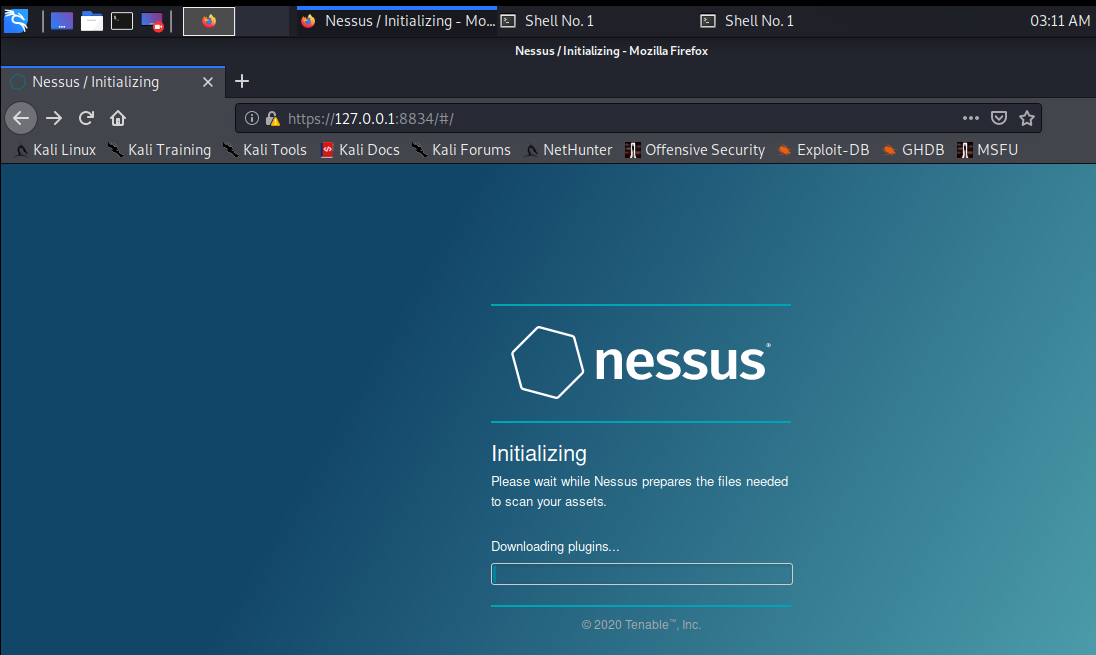
**So, finally we got the port list. But due to firewall, all ports are filtered.**

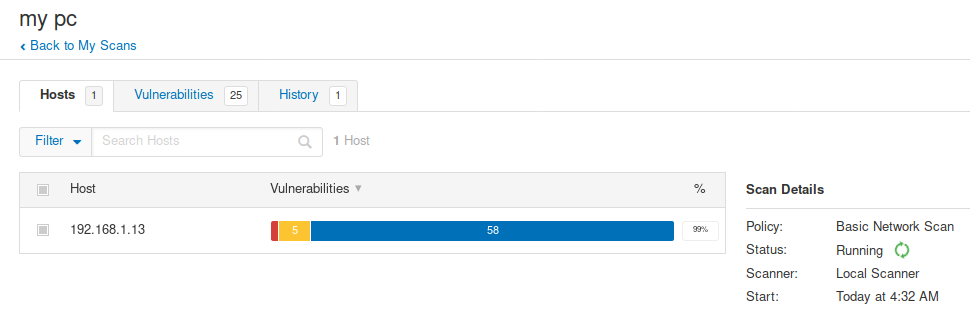
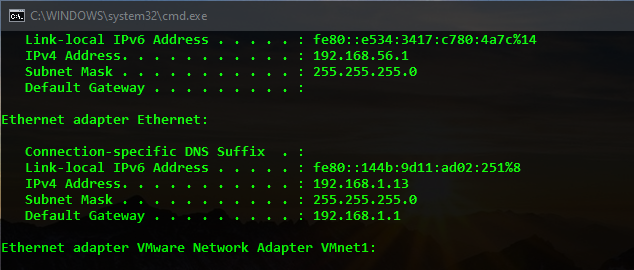
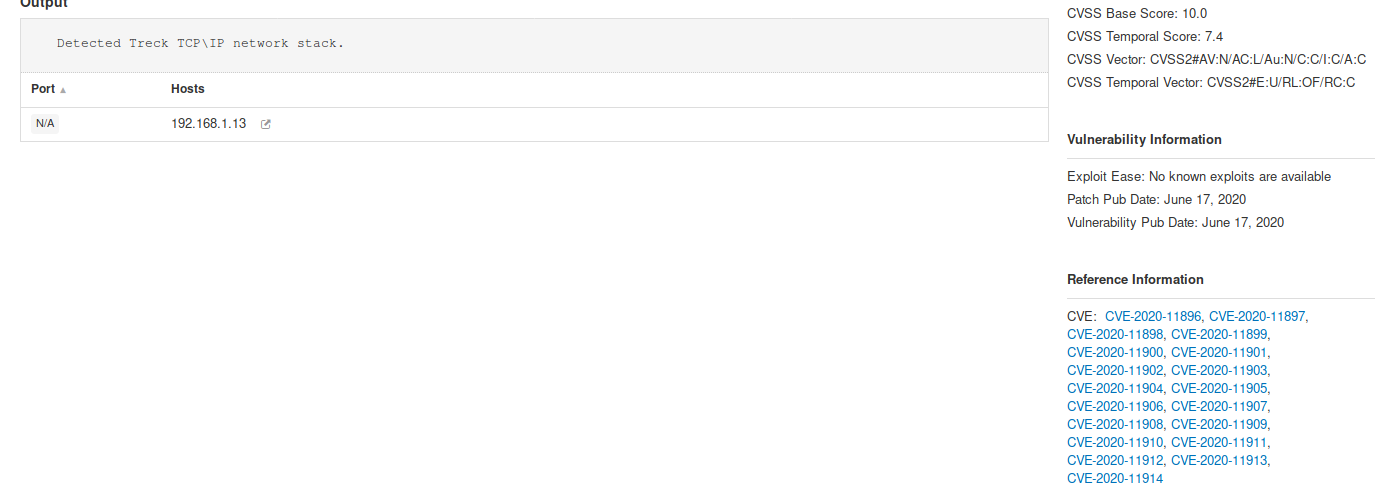
1. **Installing Nessus In A VM And Scan Your Laptop/Desktop For CVE.**

* **Here I install the Nessus on my kali machine:**

****

* **And then I configure it:**

****

* **Now I’m gonna find my pc’s IP for scan**
* ******So, now I have to scan this IP on Nessus: 192.168.1.13**
* **And at finally, we got the CVE**