**SOURCE CODE**

**PROJECT ASSESSMENT:** To perform a security vulnerability assessment (VA) and penetration testing (PT) on the two identified systems (Windows and Debian Linux), document the VA and PT findings and provide a remediation plan to the customer.

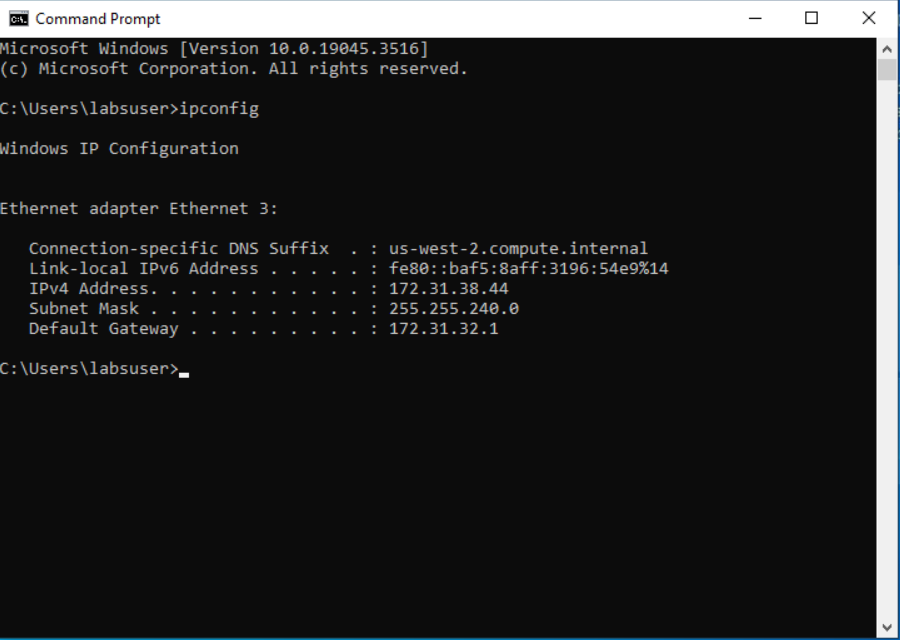
**TOOLS USED:**

* Shodan
* Nmap
* Nessus
* Metasploit

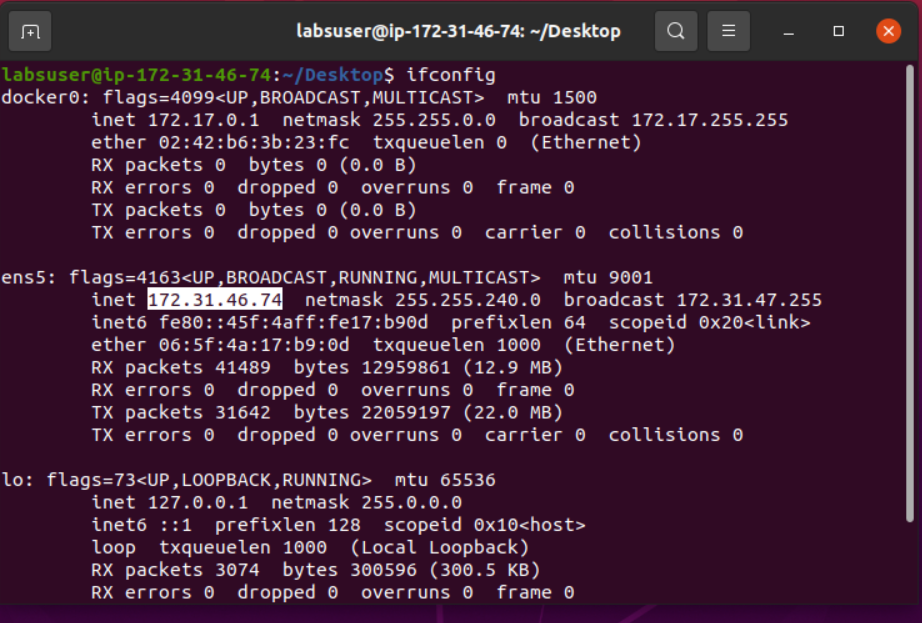
**PROCEDURE:**

From the given assessment we know that the two identified systems are Windows and Ubuntu. As we are testing it on the lab environment, we know the system’s IP addresses and the operating system used.

* To verify the systems IP addresses we can use the command *“****ipconfig****”* and *”****ifconfig****”* on the Windows and Ubuntu machines respectively.

**Windows**

**Fig1: Windows IP Configuration**

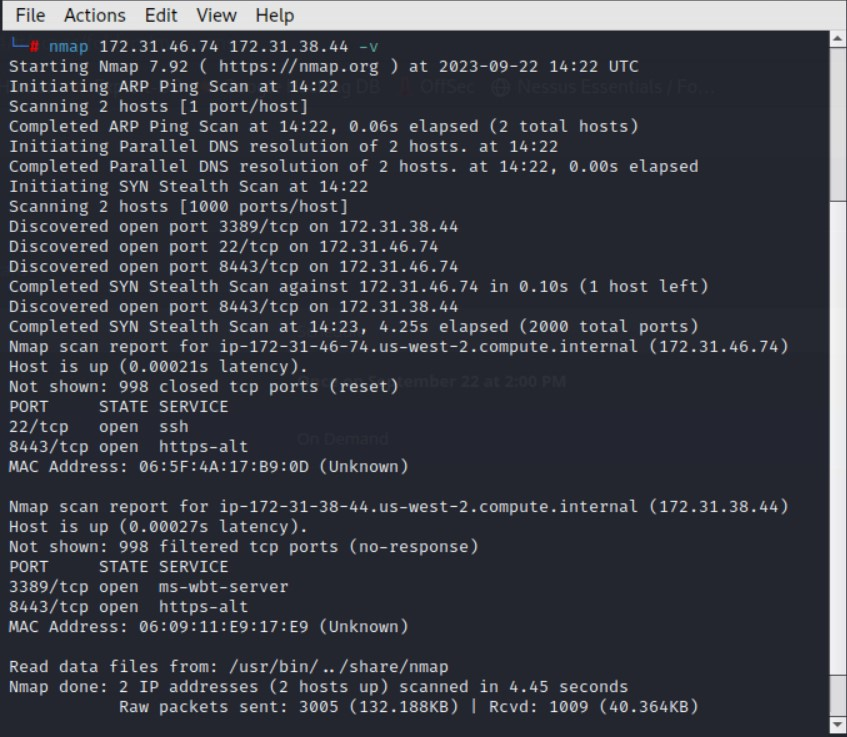
**Ubuntu  
**

**Fig2: Ubuntu IP Configuration**

Once we confirm the IP addresses of the two systems, we start by doing general scans on the two identified systems.

* As we now know the server IP’s, I used nmap to do a general scan on the IP’s. This scan is used to check for any open ports available on the IP addresses. This scan will not give any system information like the service version, operating system used, etc.

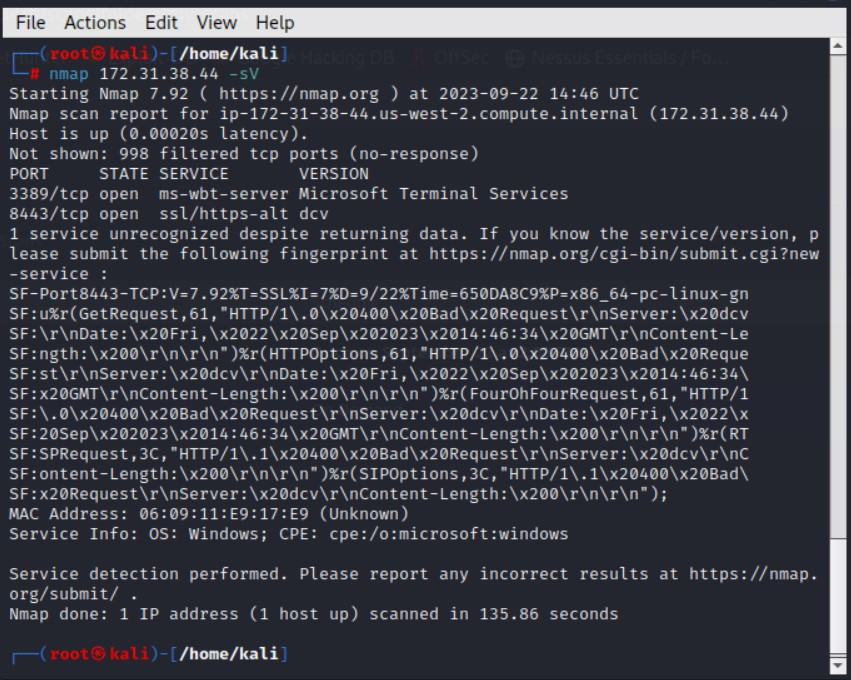
**Command used**: “*nmap 172.31.38.44 172.31.46.74”*



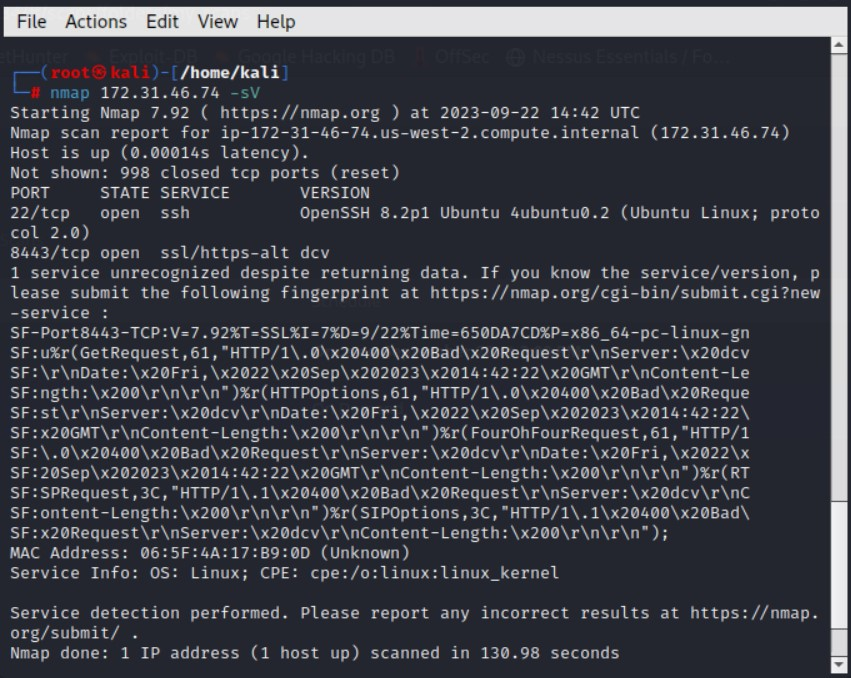
**Fig3: nmap results for both Windows and Ubuntu machine**

* To get more details on the systems, we can use *“-sV”* which is to check for service version

**Command used:** *“nmap <system IP> -sV”*

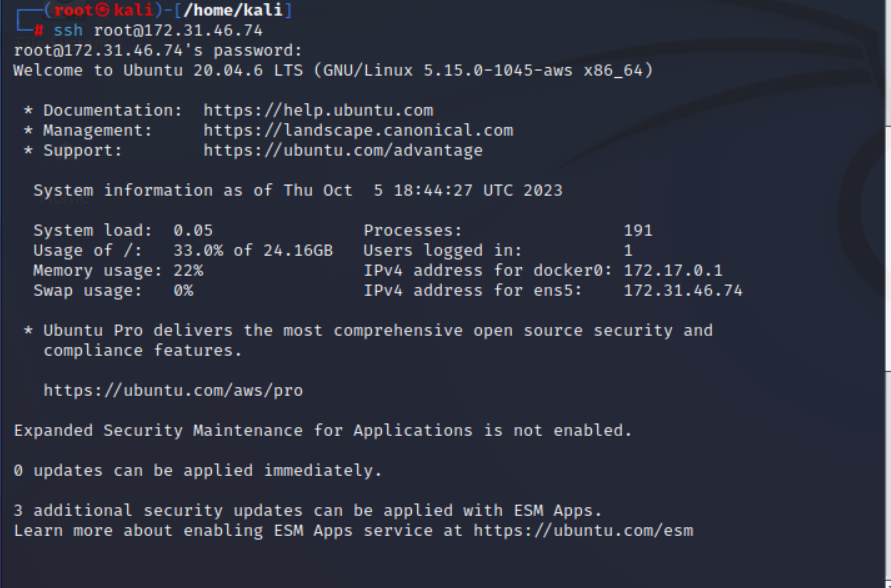
**Windows**  


**Fig4: Windows**

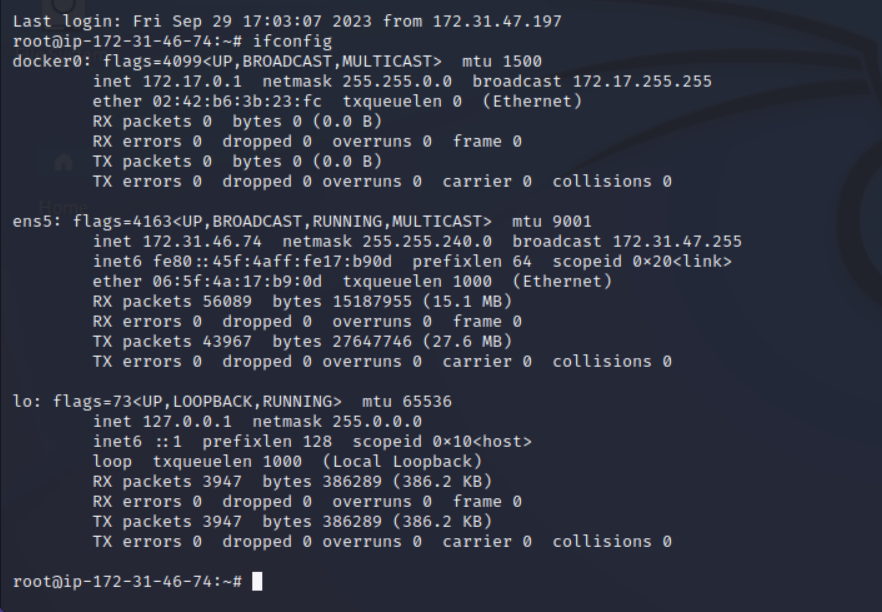
**Ubuntu**  


**Fig4b: Ubuntu**

* As we see some open ports, we can check if we can connect remotely to the systems

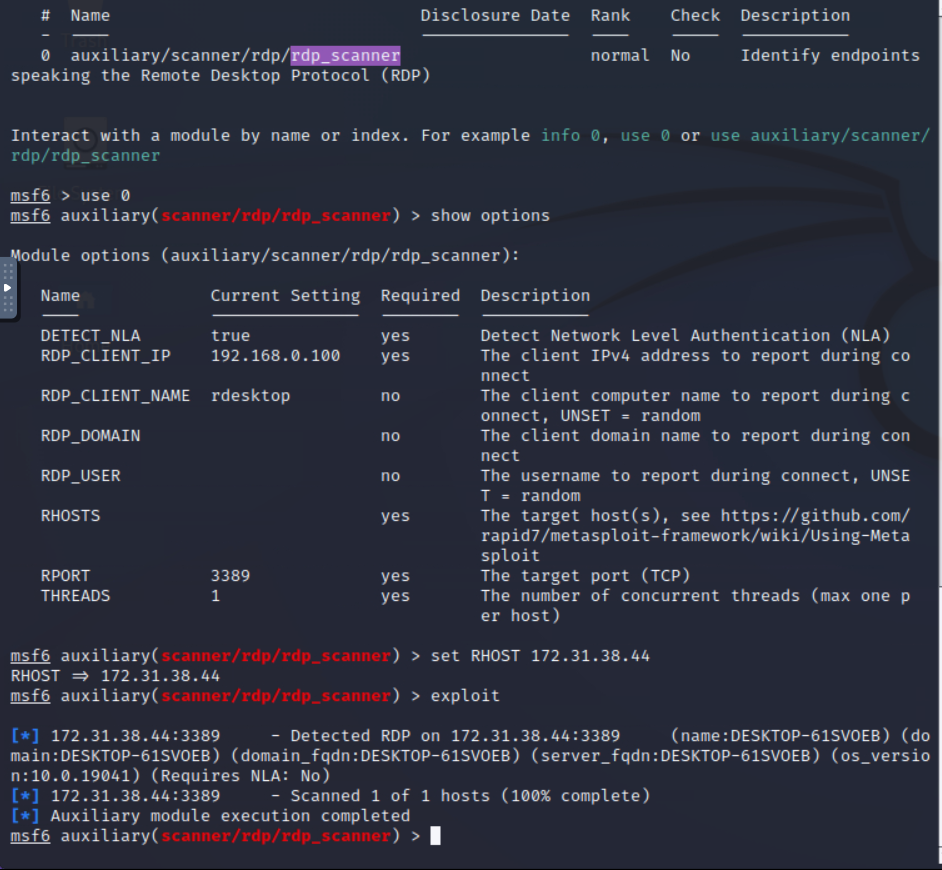
**Ubuntu** 

**Fig5a: Successful SSH into Ubuntu**

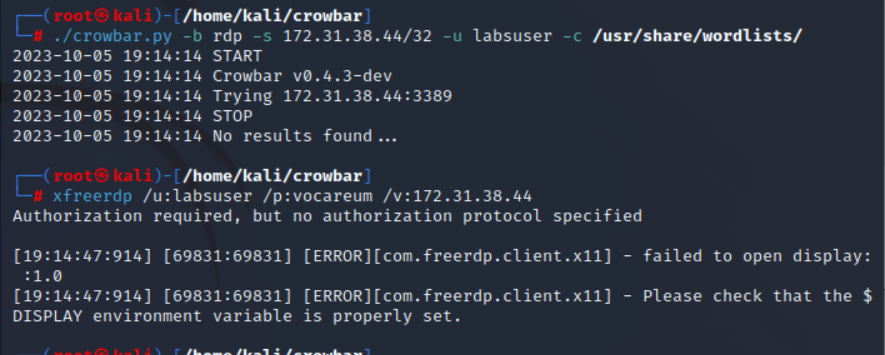


**Fig5b: PoC of logging in Ubuntu**

**Windows**



**Fig6a: Exploiting open port 3389 using Metasploit**

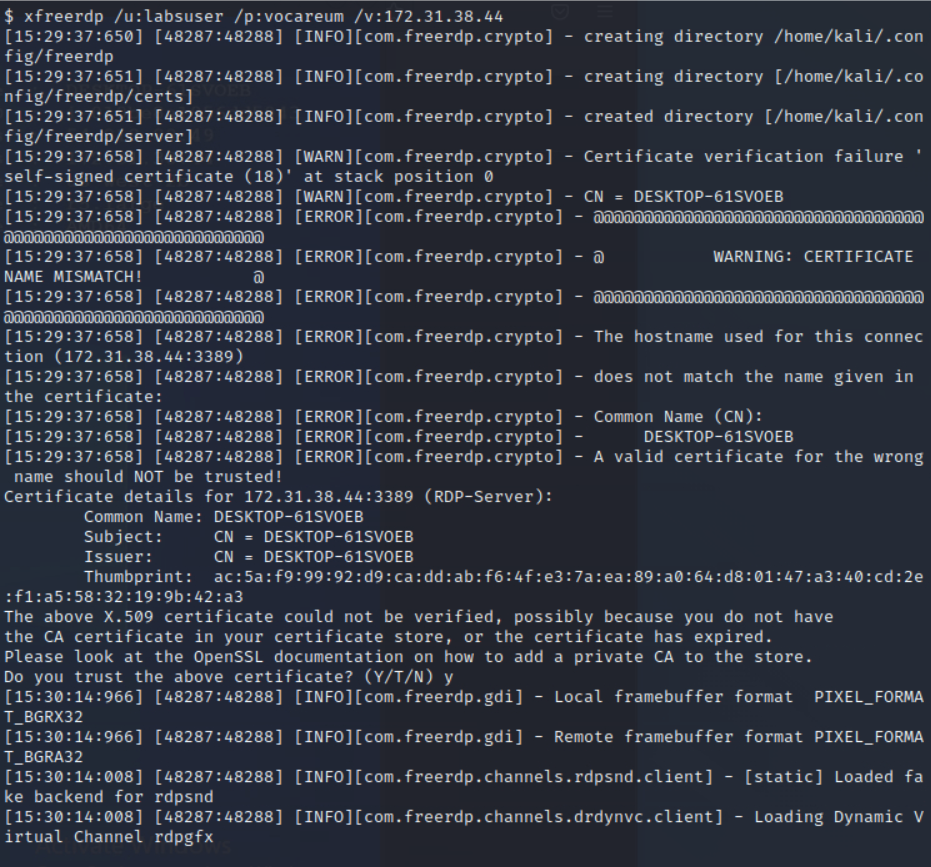


**Fig6b: Brute forcing the RDP service**

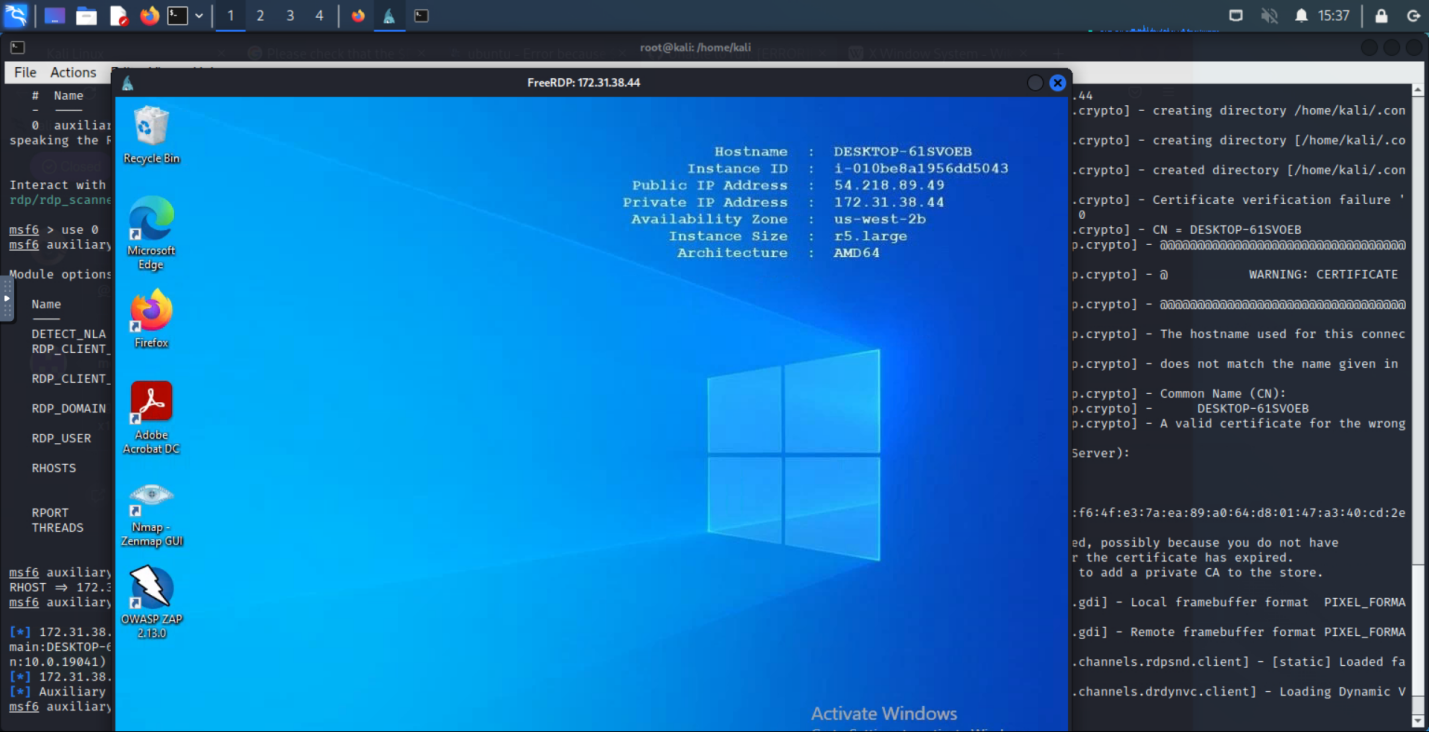
Tried to connect to windows but there were some authorization issues. The output also said that the *“$DISPLAY environment variable is not properly set”.*

This was because the FreeRDP was run with administrative privileges.

Hence I once again ran the FreeRDP tool without any administrative privilege and was successful.



**Fig7a: FreeRDP X11 client**



**Fig7b: PoC of successful RDP session**

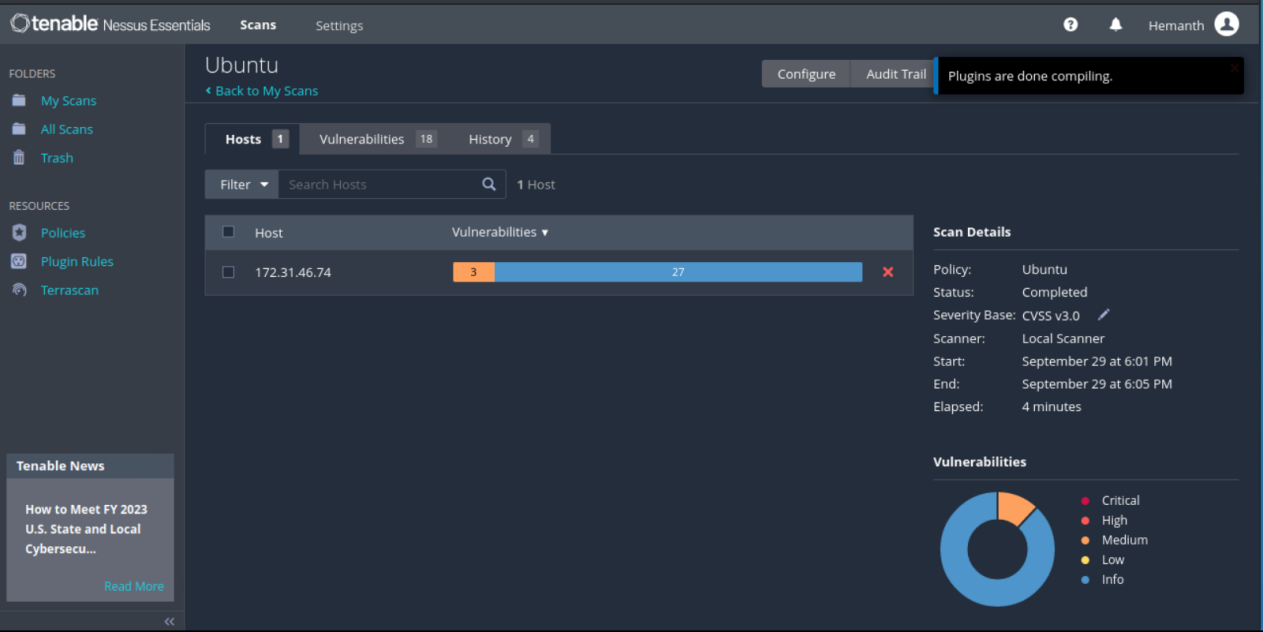
To check for vulnerabilities, I used Nessus. Nessus is a tool used for vulnerability assessment. On the Nessus tool, the following steps we followed:

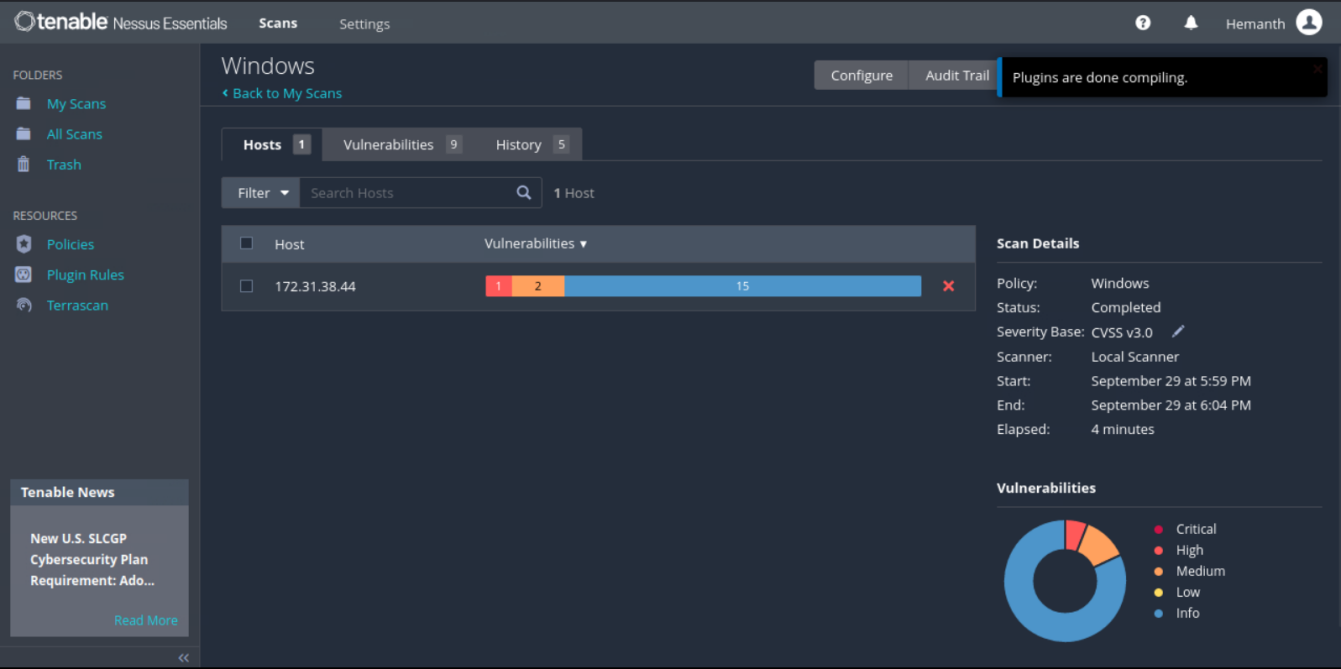
* Go to policies > New Policy > Advanced scan
* Give the details of the policy and save
* Next go to My Scan > New Scan > User Defined > Choose the policy that was created > Add the target that must be scanned

(In our case it’s the systems IP addresses)

* Save and launch

Once the scanning is completed, it will show the vulnerabilities that were detected.

  
**Fig8a: Ubuntu vulnerabilities on Nesses**

  
**Fig8b: Windows vulnerabilities on Nessus**

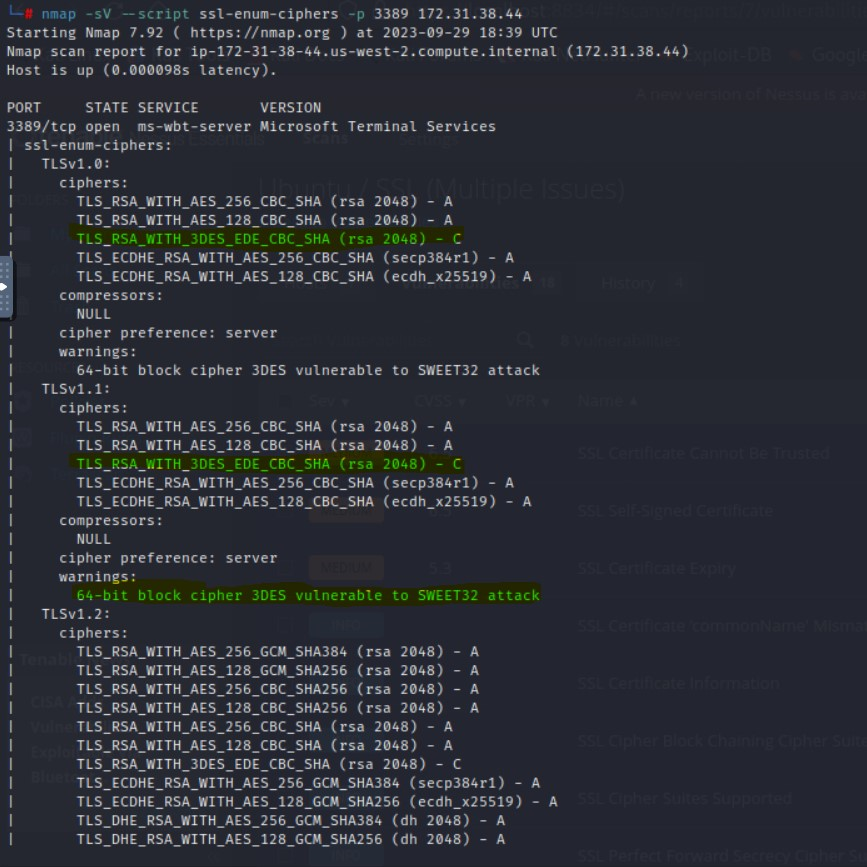
* Here we can click on the vulnerability option and check
* Each vulnerability has its CVSS Score which tells the *Risk Information*
* Each vulnerability also has a CVE number.

CVE stands for Common Vulnerabilities and Exposures. The system provides a method for publicly sharing information on cybersecurity vulnerabilities and exposures.

The CVE’s are stored in NVD(National Vulnerability Database)

From this we can get information about the vulnerabilities.

The vulnerabilities that were observed when testing were of incorrect SSL certificate. Some of them were Self-signed SSL certificate, SSL certificate cannot be trusted, SSL certificate expiry. These were checked and confirmed using nmap scripts ***“nmap -sV --script ssl-enum-ciphers -p <port number> <IP address>”***

  
**Fig9: SSL Ciphersuit results**