**Sadiq S.**

# Nessus

Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools. Nessus employs the Nessus Attack Scripting Language (NASL), a simple language that describes individual threats and potential attacks.

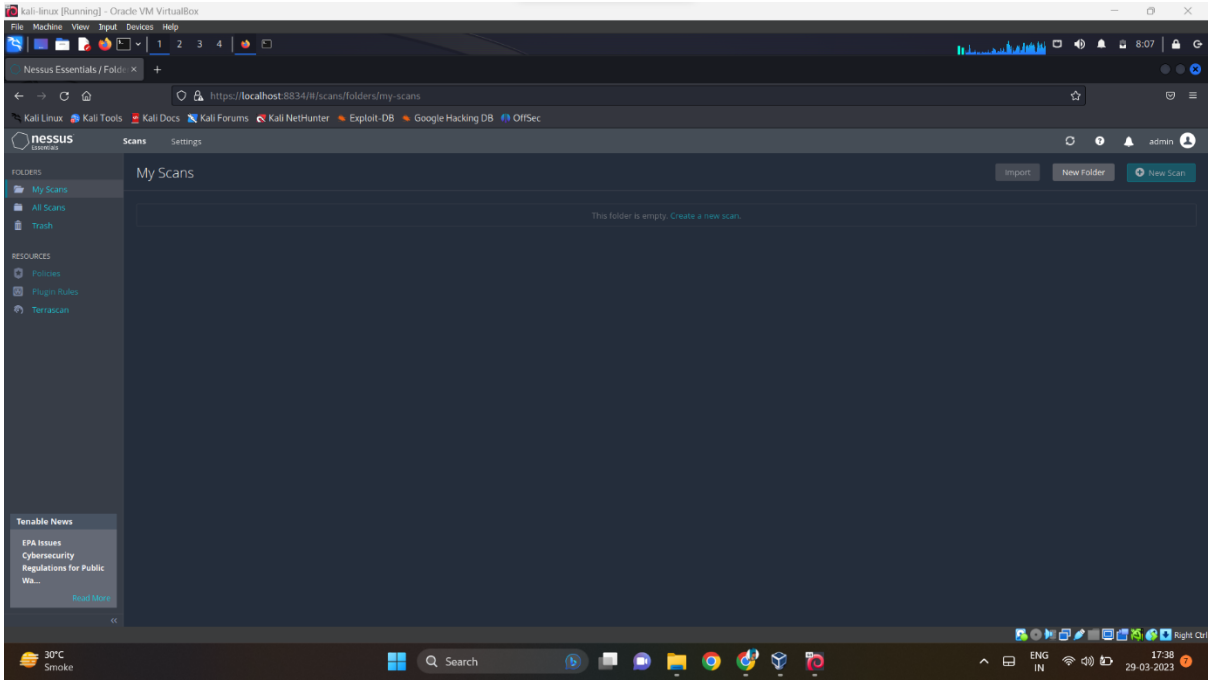
Nessus has a modular architecture consisting of centralized servers that conduct scanning, and remote clients that allow for administrator interaction. Administrators can include NASL descriptions of all suspected vulnerabilities to develop customized scans. Significant capabilities of Nessus include:

- Compatibility with computers and servers of all sizes.
- Detection of security holes in local or remote hosts.
- Detection of missing security updates and patches.
- Simulated attacks to pinpoint vulnerabilities.
- Execution of security tests in a contained environment.
- Scheduled security audits.

**I will target ‘skullcandy.com’ and my MS2 with IP Address 192.168.0.5**

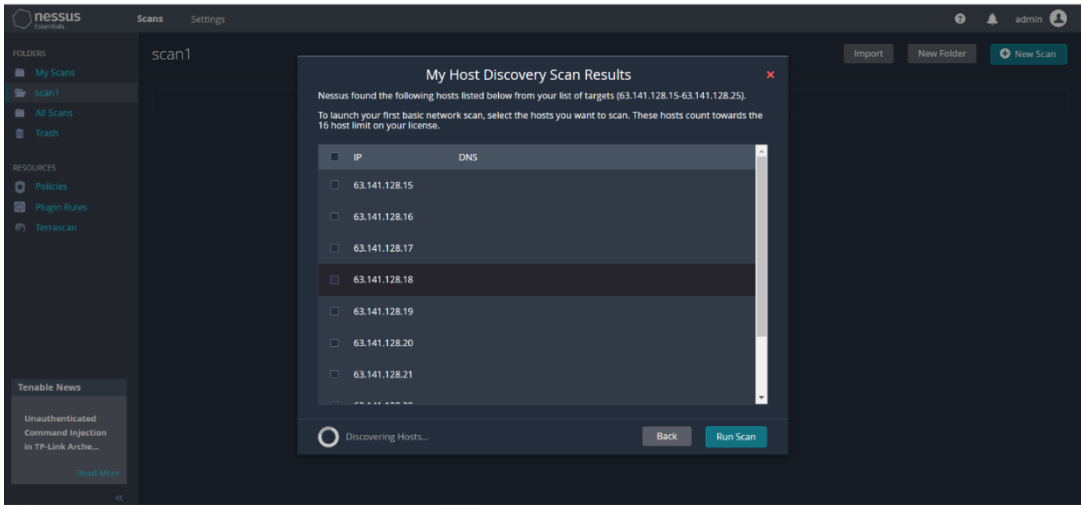
First, we have to install Nessus. Go to ‘localhost:8834’ and the Nessus will start. It will take time to download plugins. After it’s done login using username= ‘admin’ and password= ‘admin’.

You will come to this screen.

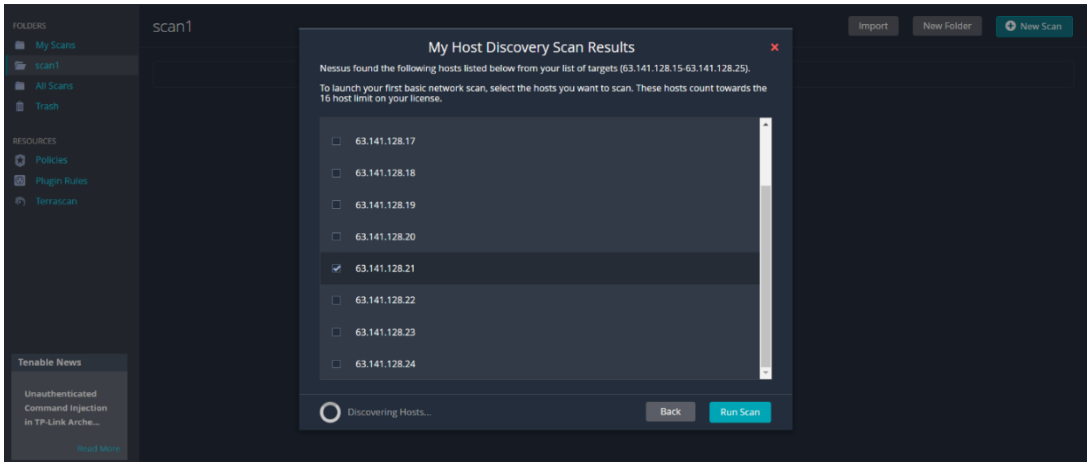


Then you scan multiple server or host and you can even scan single host.

I'll scan multiple host ranges from IP Address = 63.141.128.15 – 63.128.141.25



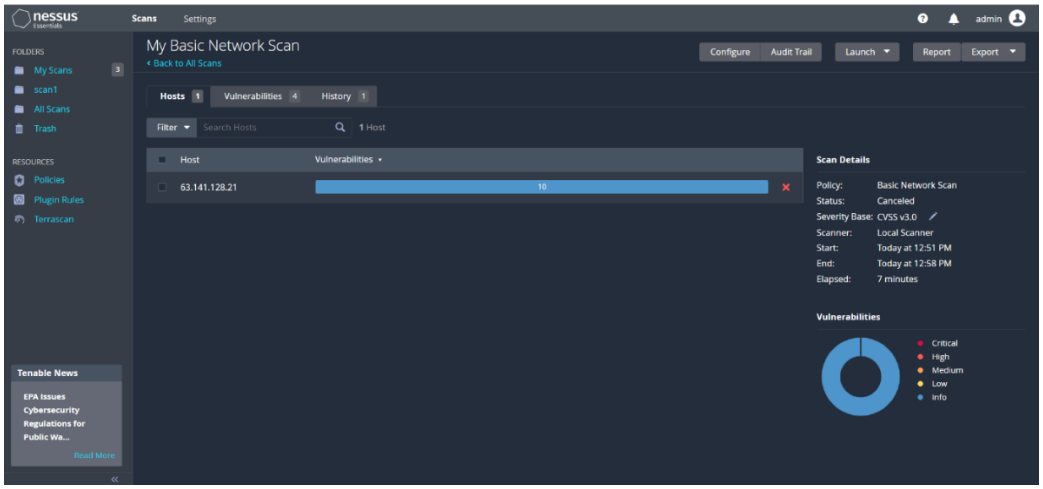

You can select a single server too.



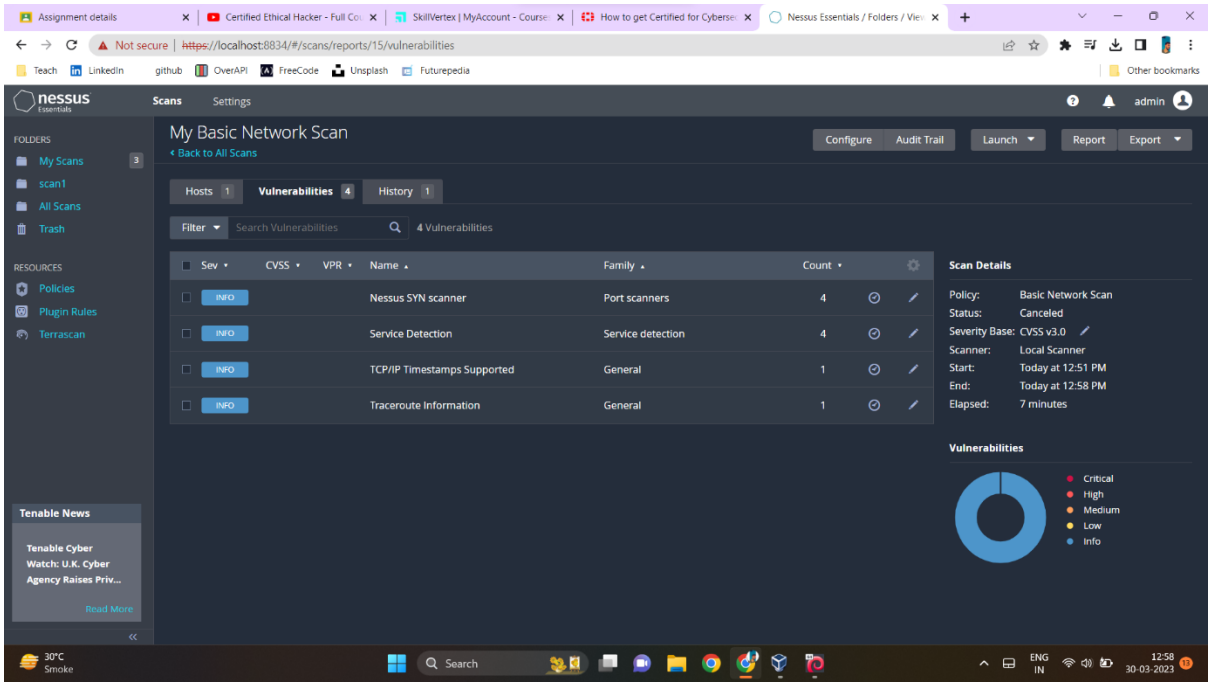

Now it will run a basic scan on the selected host.

I stopped the scan after a while and 4 very very low level vulnerability were found.

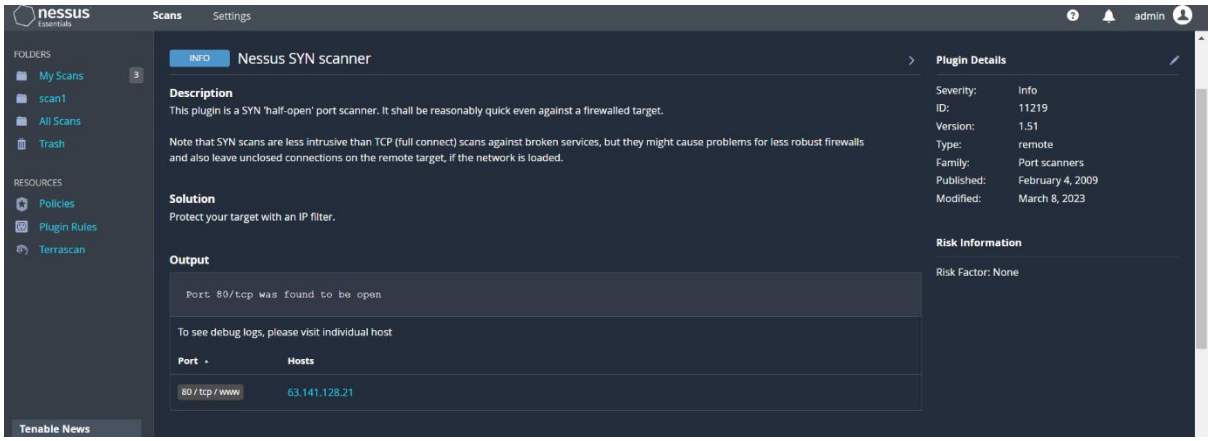
They are not vulnerability but they can be.

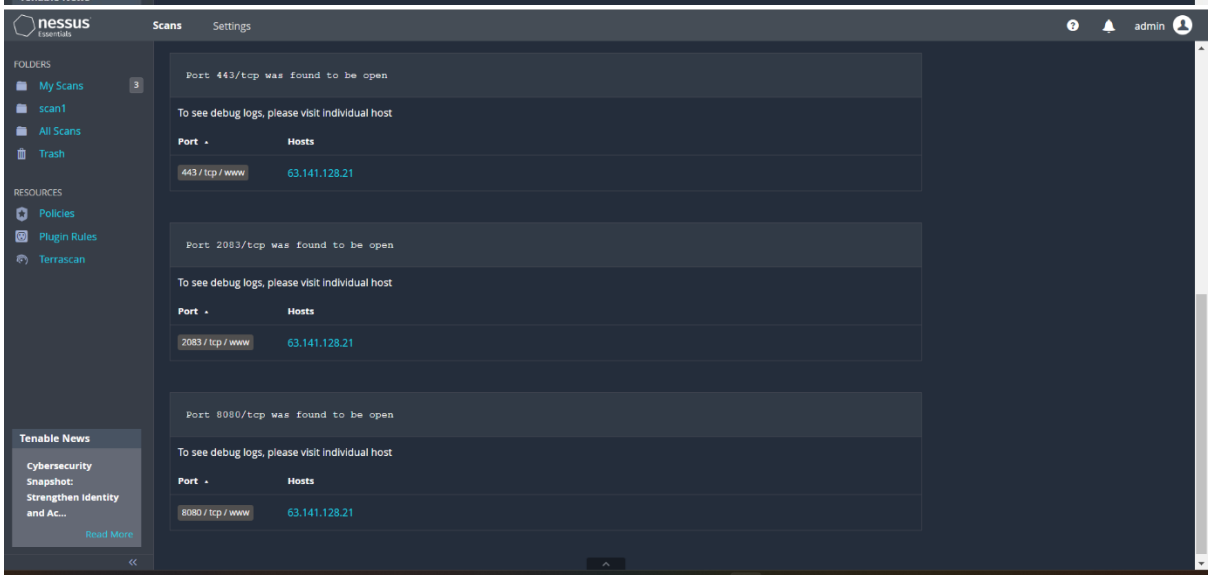


The 4 vulnerabilities were as follow:

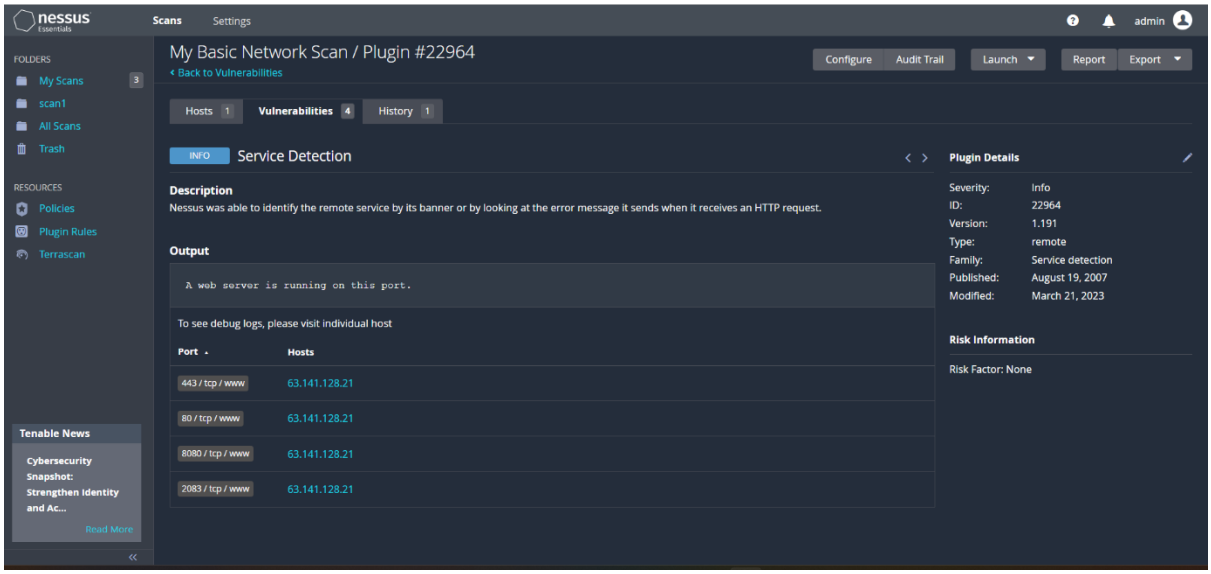



## The first vulnerability was Nessus SYN scanner.



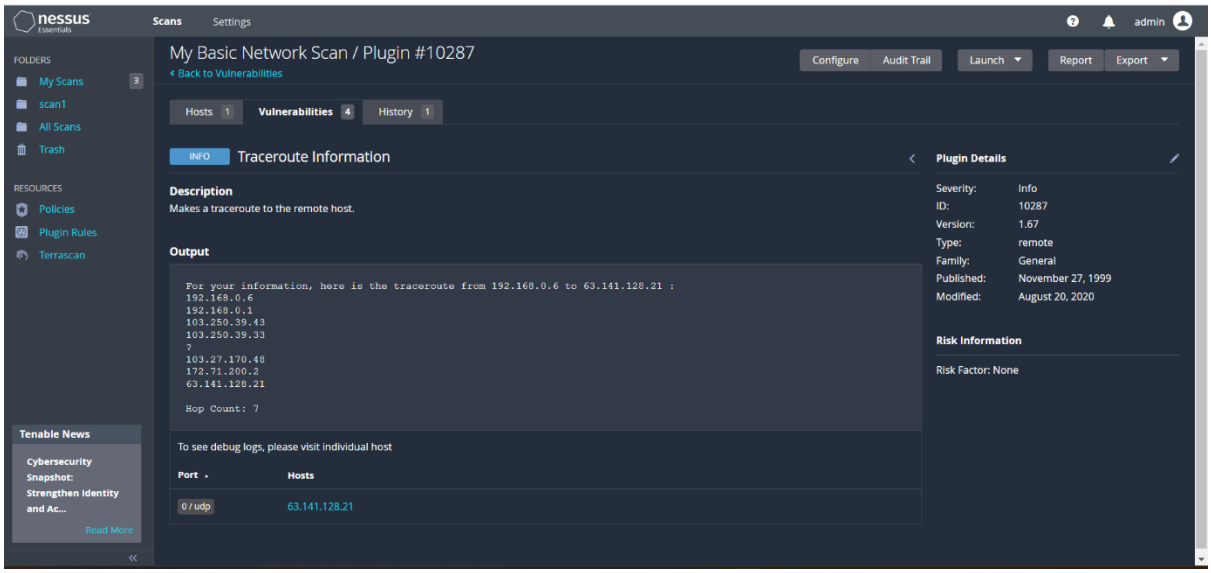



**The second vulnerability was Service Detection.**



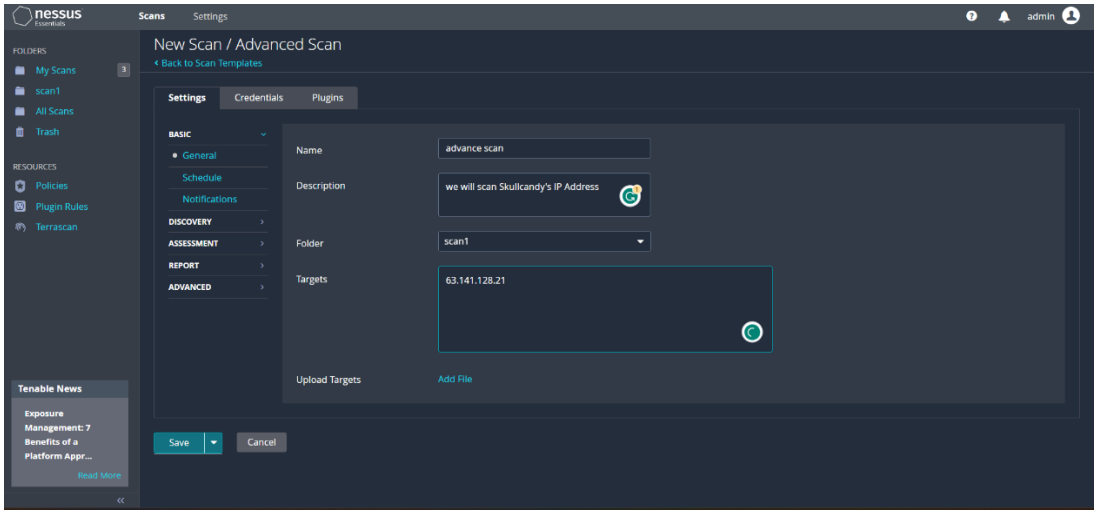

**The third vulnerability was TCP/IP Timestamps supported.**

**The fourth vulnerability was Traceroute information.**

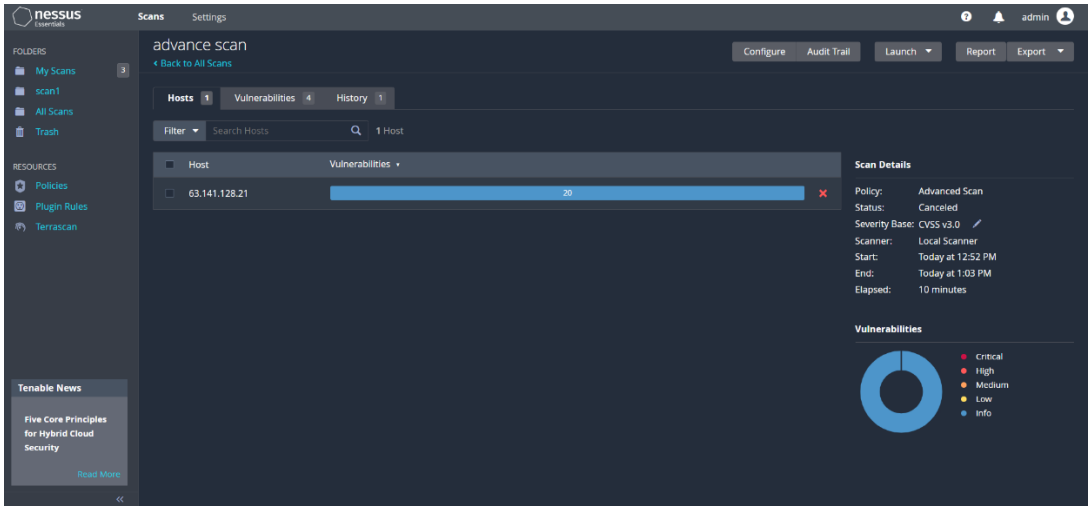



It gives us the route it followed to reach the target IP Address. And it also gives the number of hop count. i.e., the no. of network in between.

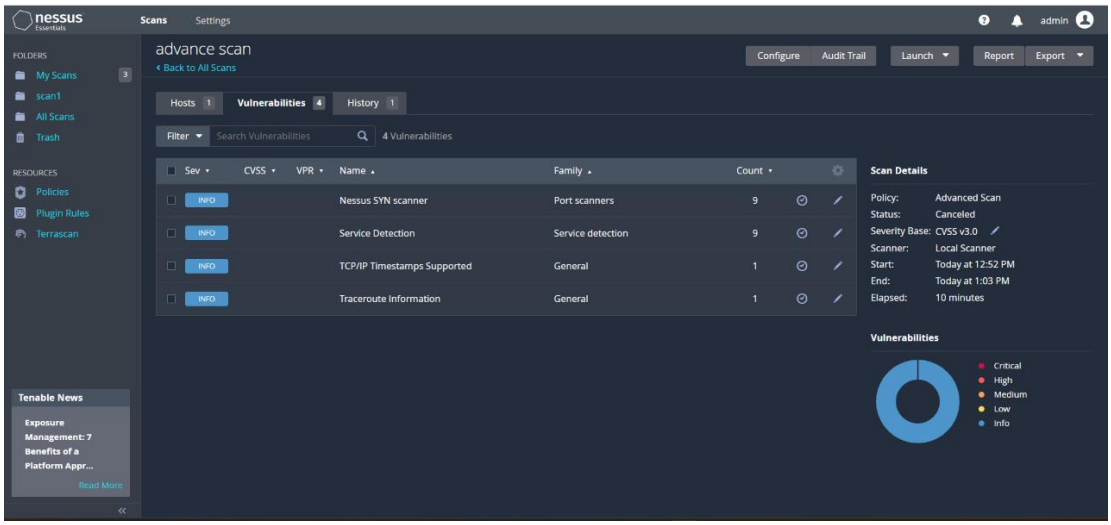
**Now I'll create a advance scan on the same port.**



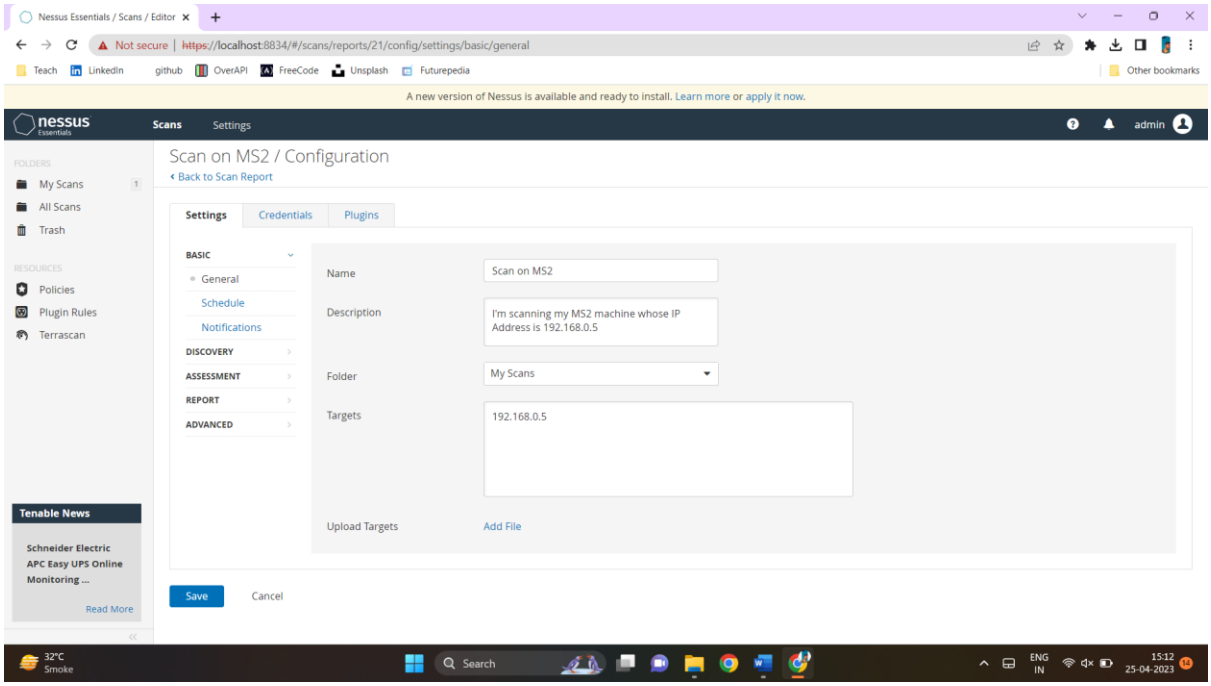

The results were same for both basic and advance scan.




The 4 same vulnerabilities were found.



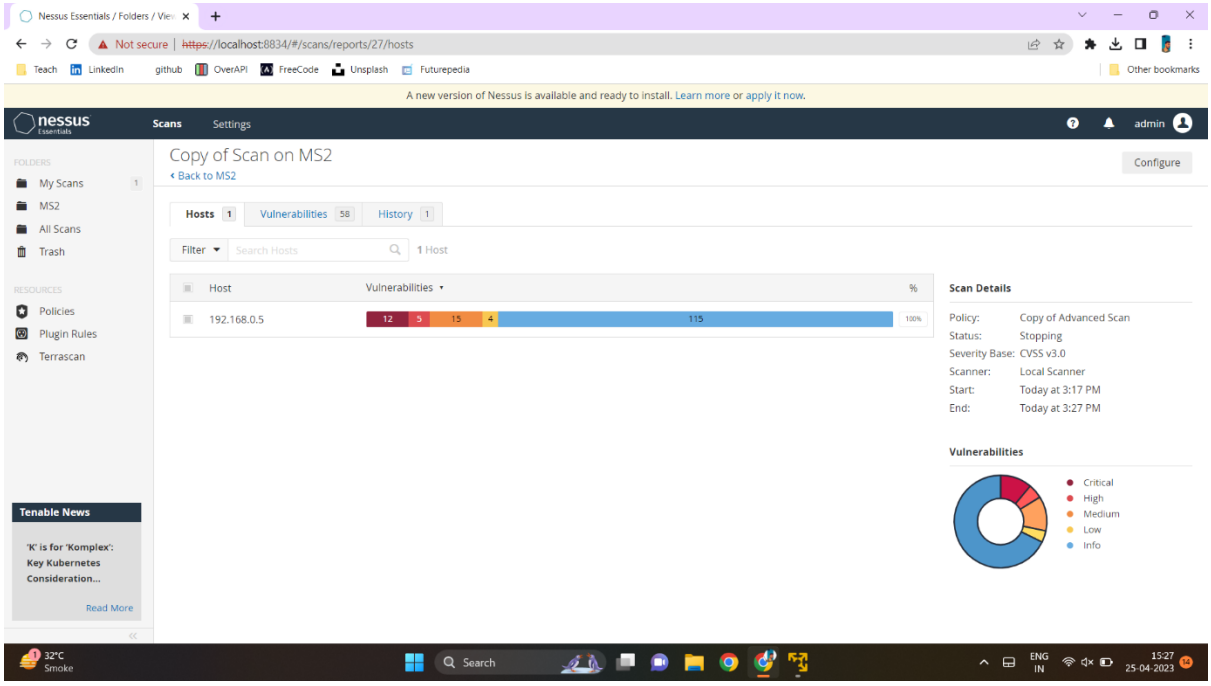
**Now we will do an Advance Scan on MS2 machine:**

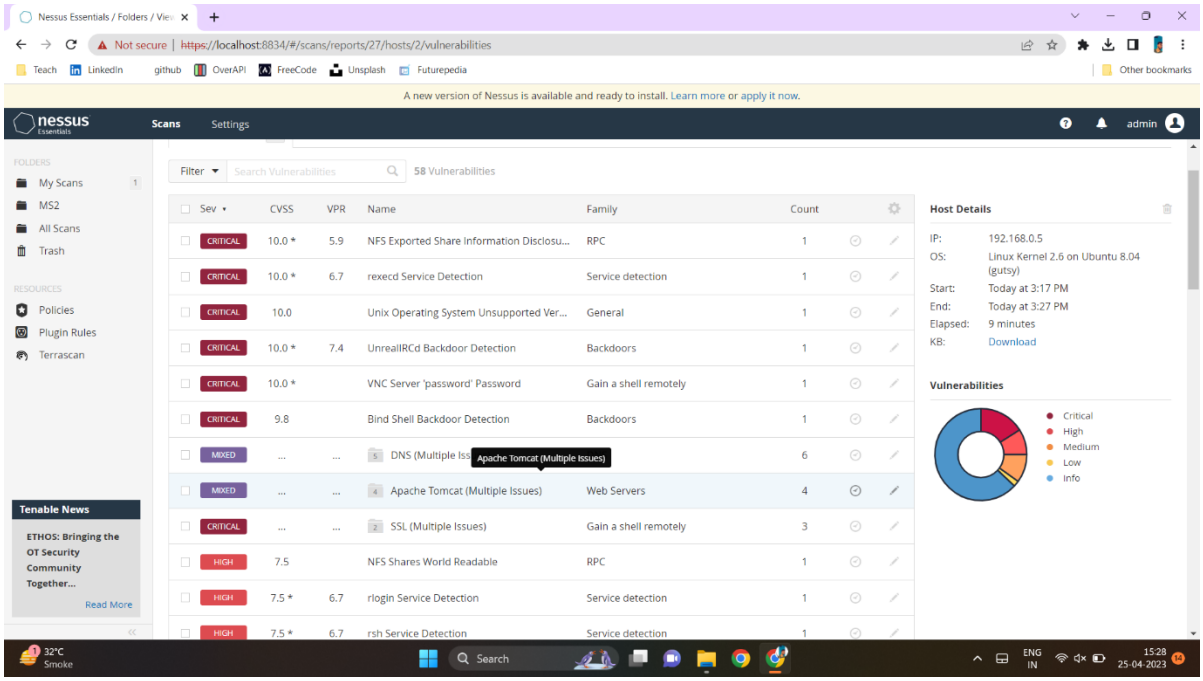



**After creating a scan, I launched.**

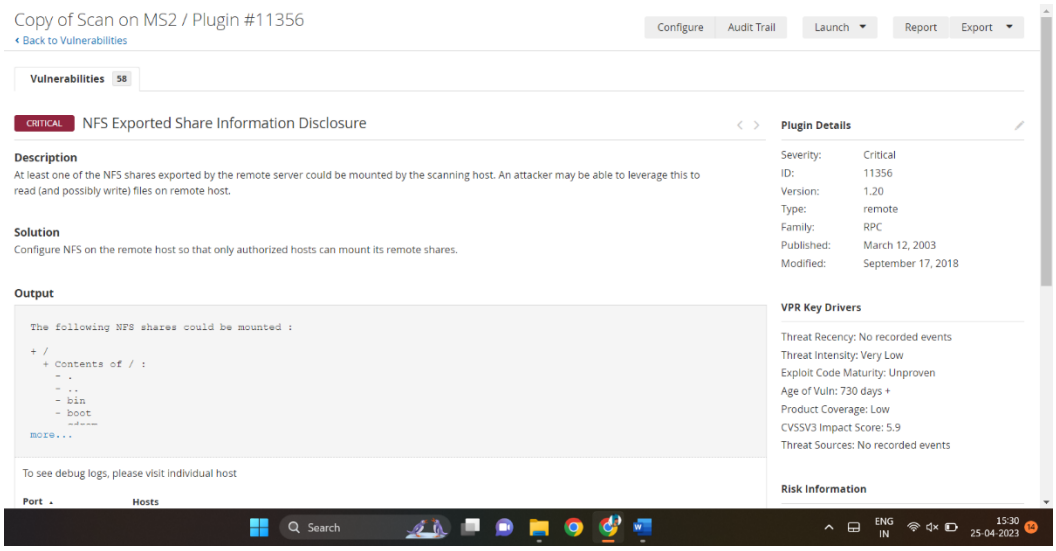
**As metasploitable is purposely made vulnerability we got a lot of vulnerabilities and I had to stop the scan because it will take a lot of time.**

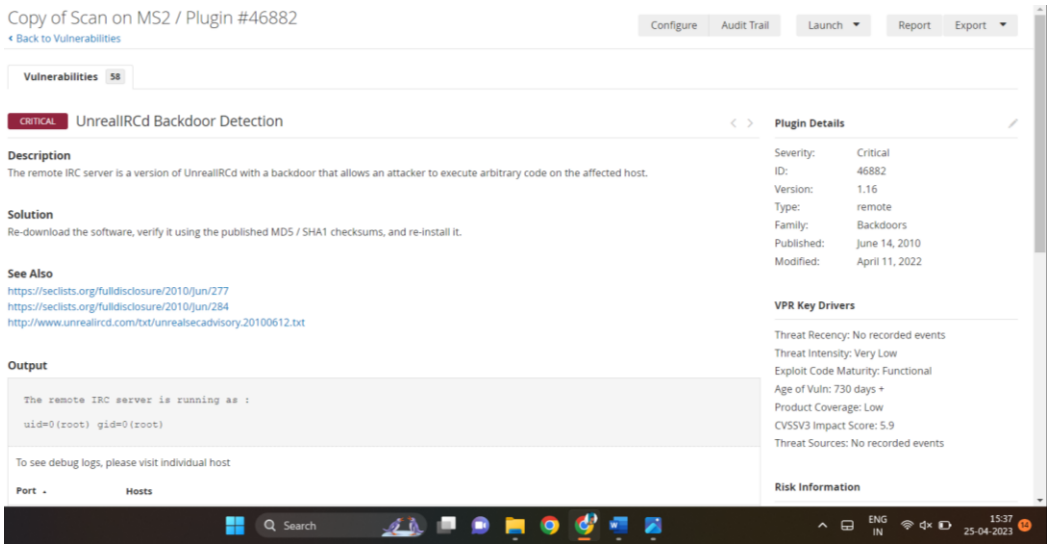
**12 Critical, 5 High, 15 Medium, 4 Low, 115 Info, Vulnerabilities were found.**

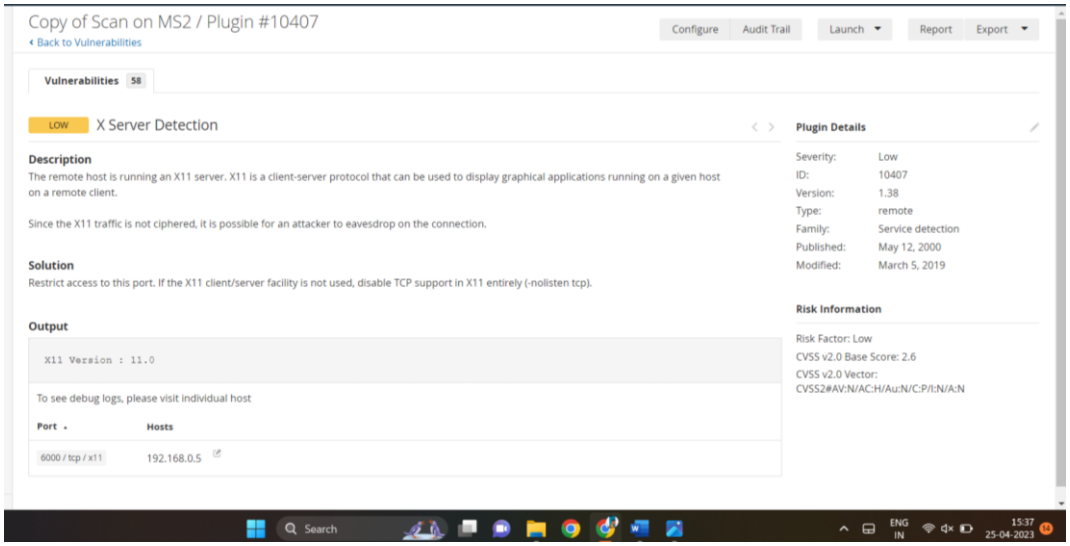




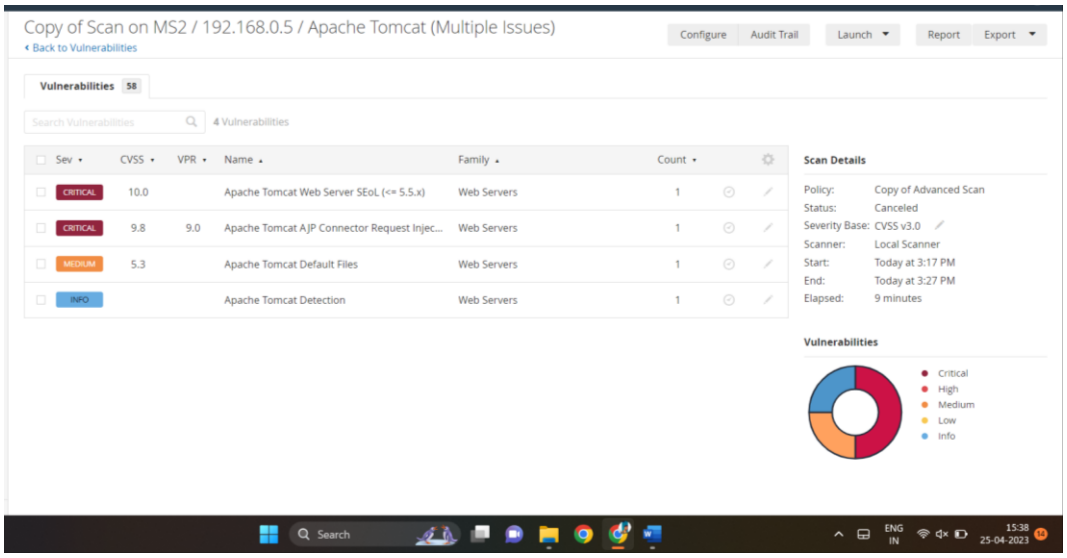

With the vulnerability name, the solution is also given for that vulnerability.






It will also group vulnerabilities together.




Here, all these vulnerabilities are of Apache Tomcat server, so they are group together.