**Cybersecurity Essentials**

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

Name – Tharshan R

Email Id: - tharshan25throckstar@gmail.com

Ph. No - +91 9750551101

**Q**1. Find out the mail servers of the following domain:

* Ibm.com
* Wipro.com

Sol-

ALL THE PROCESS I AM DOING IN KALI MACHINE (terminal and termux)

Step 1 open terminal in kali

Step 2 write command nslookup.

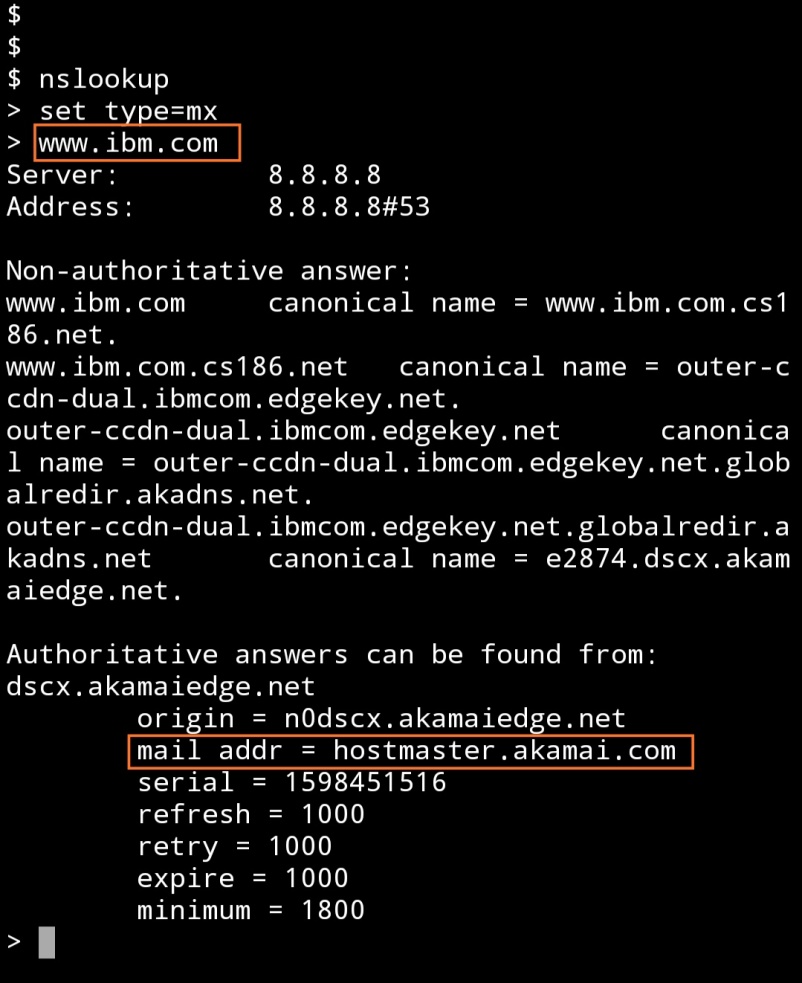
It will opens the nslookup in terminal

Step 3 type command “set type=mx” and then type site name

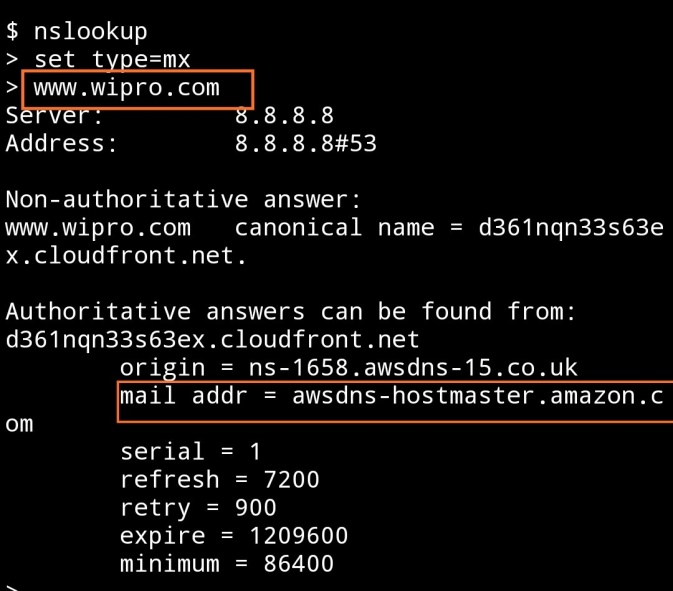


“set type=mx” this command is used to get mail servers of our targets

THE MAIL SERVER OF ibm.com is as follows:

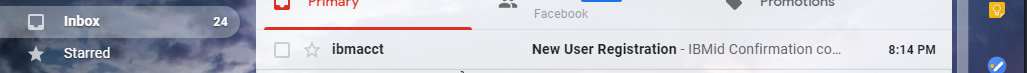


Step 4 same for wipro.com.



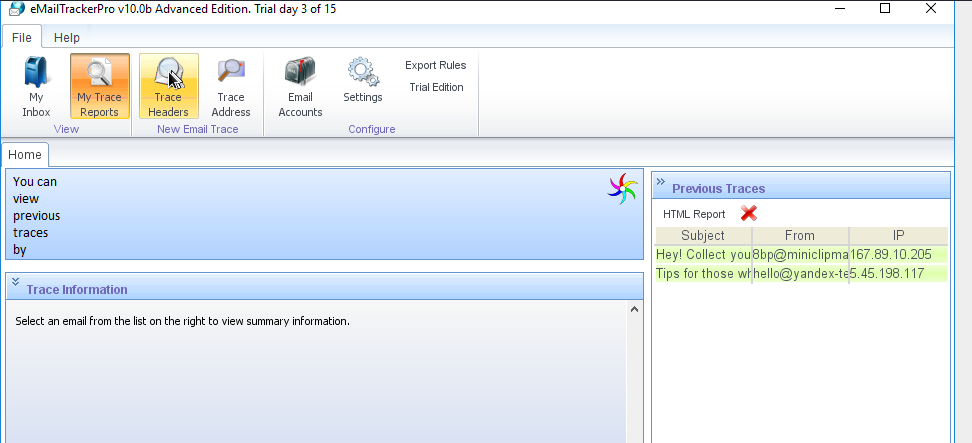
**Q**2. **Find the location, where these email servers are hosted.**

Sol.**To find location of these email servers we have to get an email from site. To do so we can register on one of the sites ibm.com.**

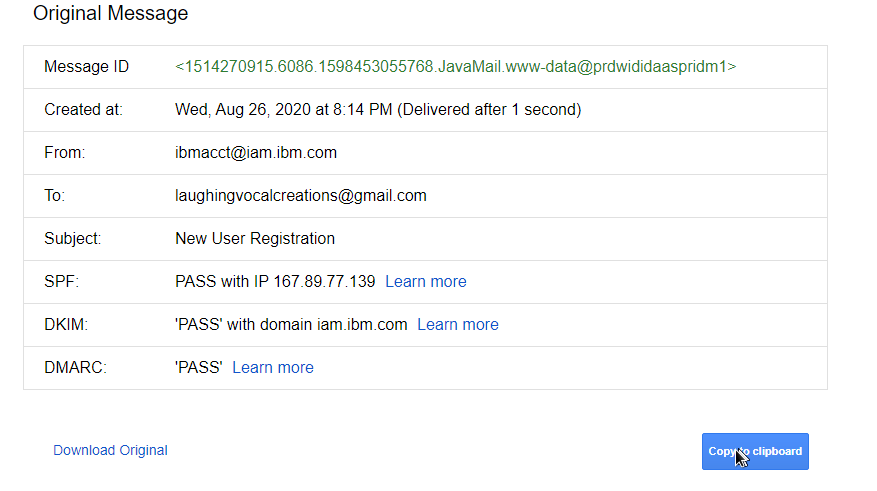


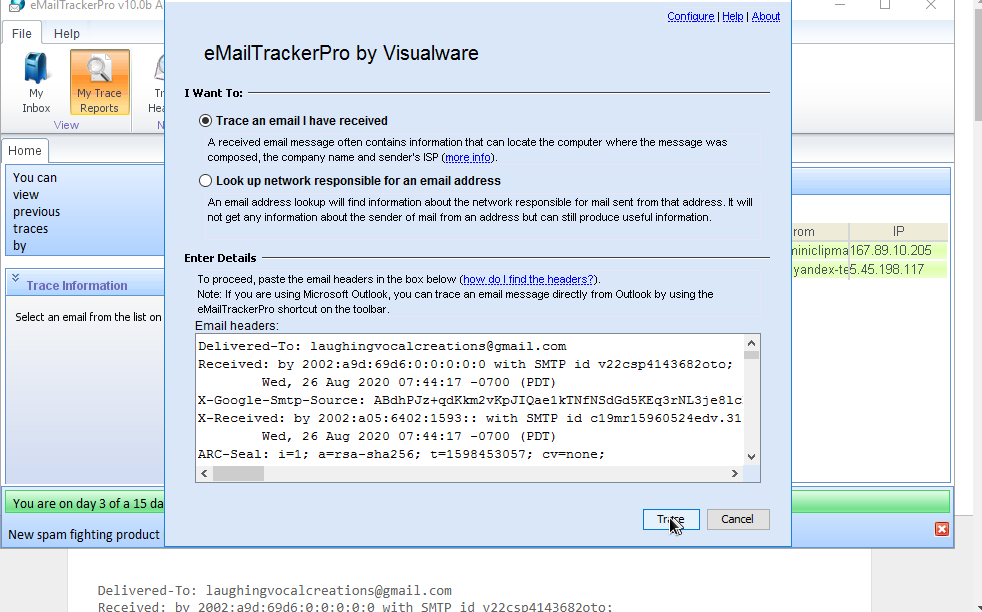
Open mail. And choose show original option.

Open email tracer and chose option trace headers.

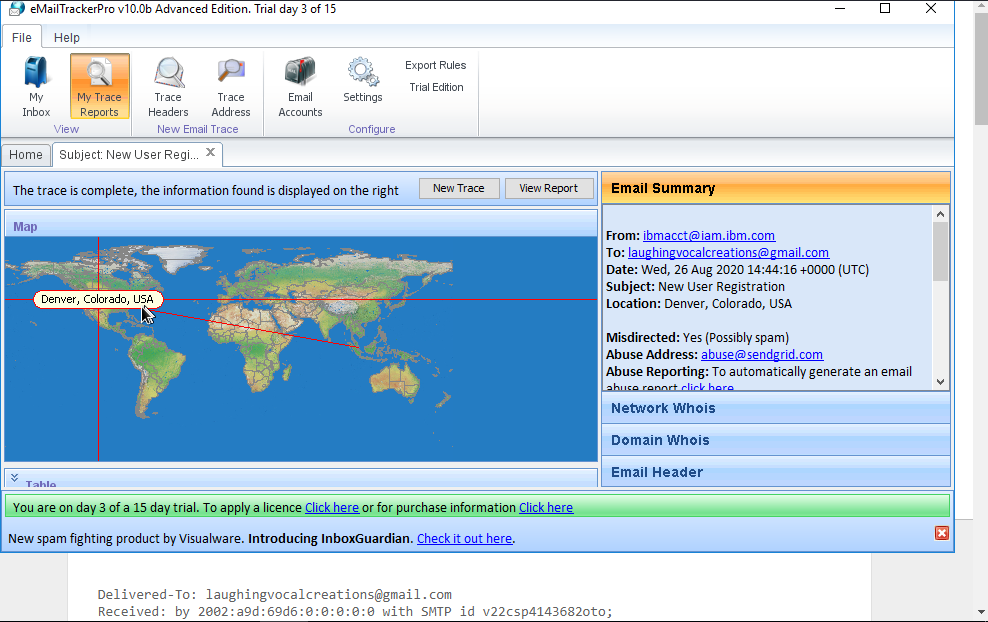


**Open mail and select option copy to clipboard and paste it in email tracer.**



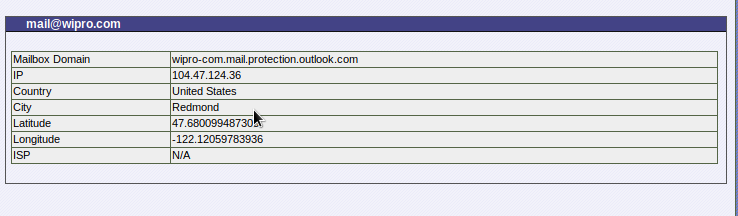


And press trace.



And we get the location i.e. Denver, Colorado, USA.

Or we can use website i.e. my-addr.com



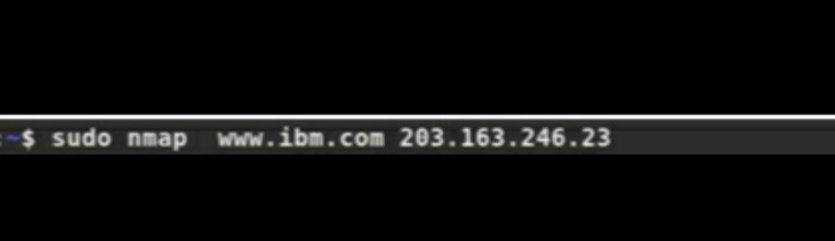
We get result for wipro.com i.e. Redmond, us.

**Q**3. **Scan and find out port numbers open 203.163.246.23.**

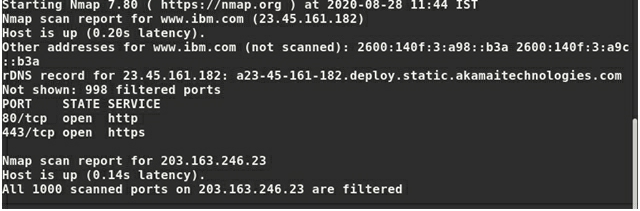
Sol. To scan port, we use Nmap

1. In kali linux we have tool called Nmap scanner to scan open ports

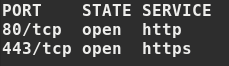
1. Open terminal in kali Linux and type command “nmap [www.ibm.com](http://www.ibm.com/) 203,163,246,23”



1. THE two ports are opened in ibm.com



1. Doing same for wipro.com.

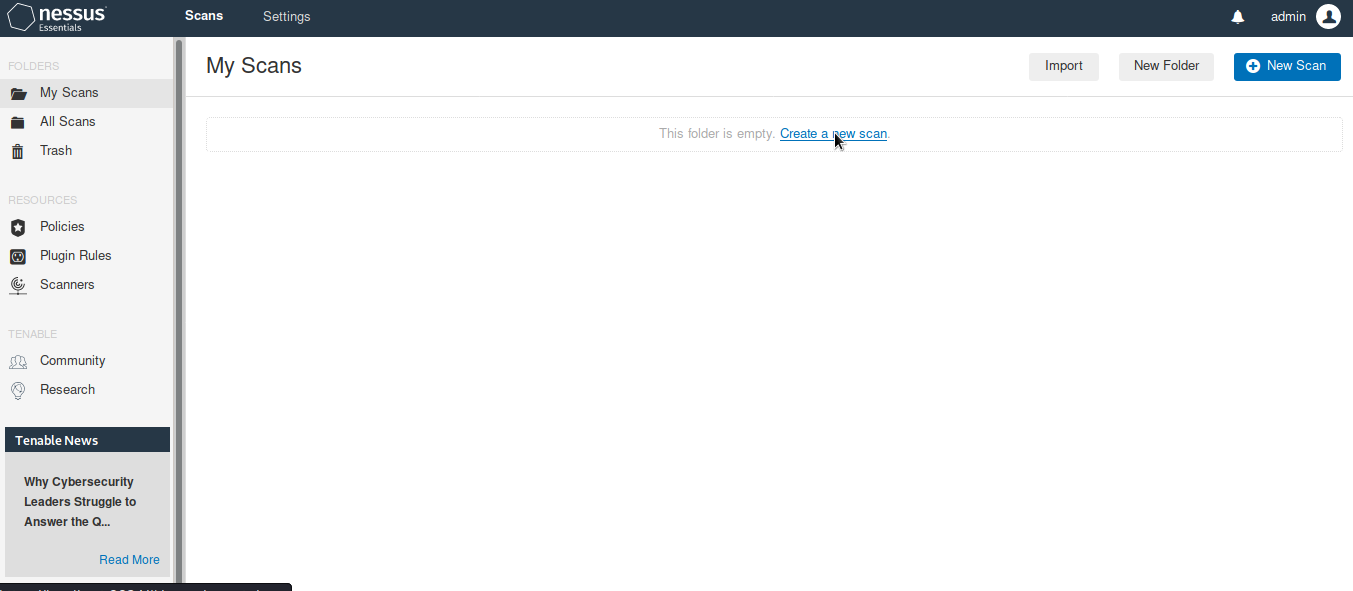


1. As we can see ports given above two ports are open for in wipro.com.

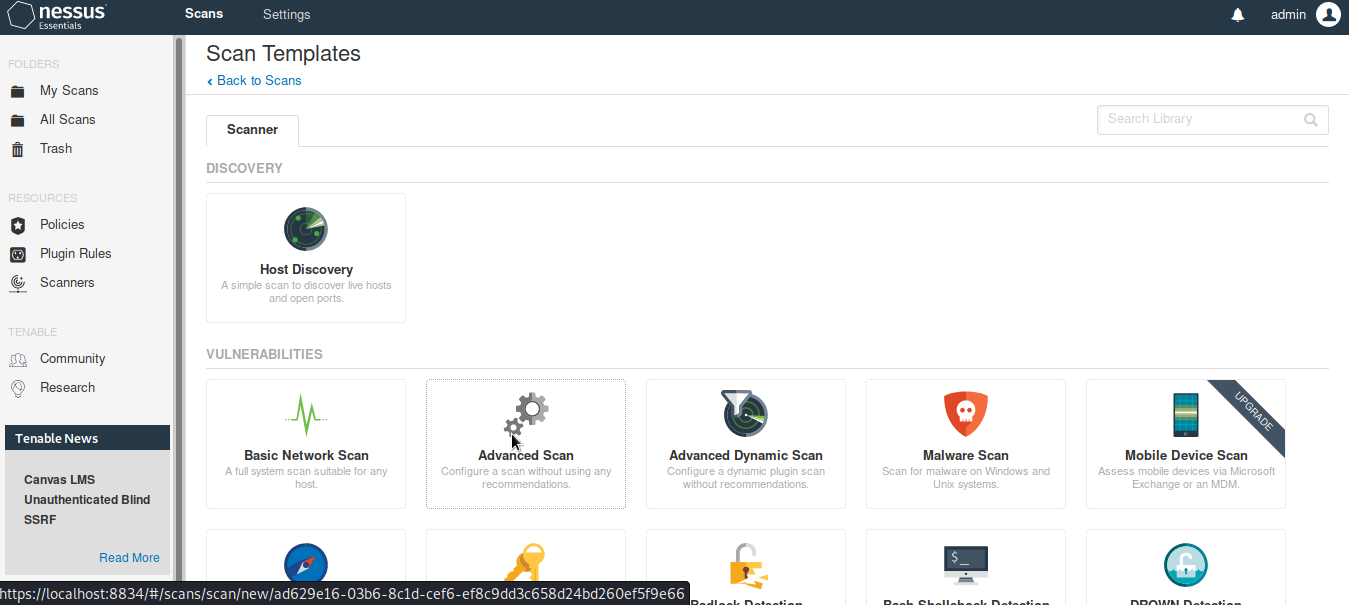
**Q**4. **Install Nessus in a VM and scan your laptop/desktop for CVE.**

Sol.

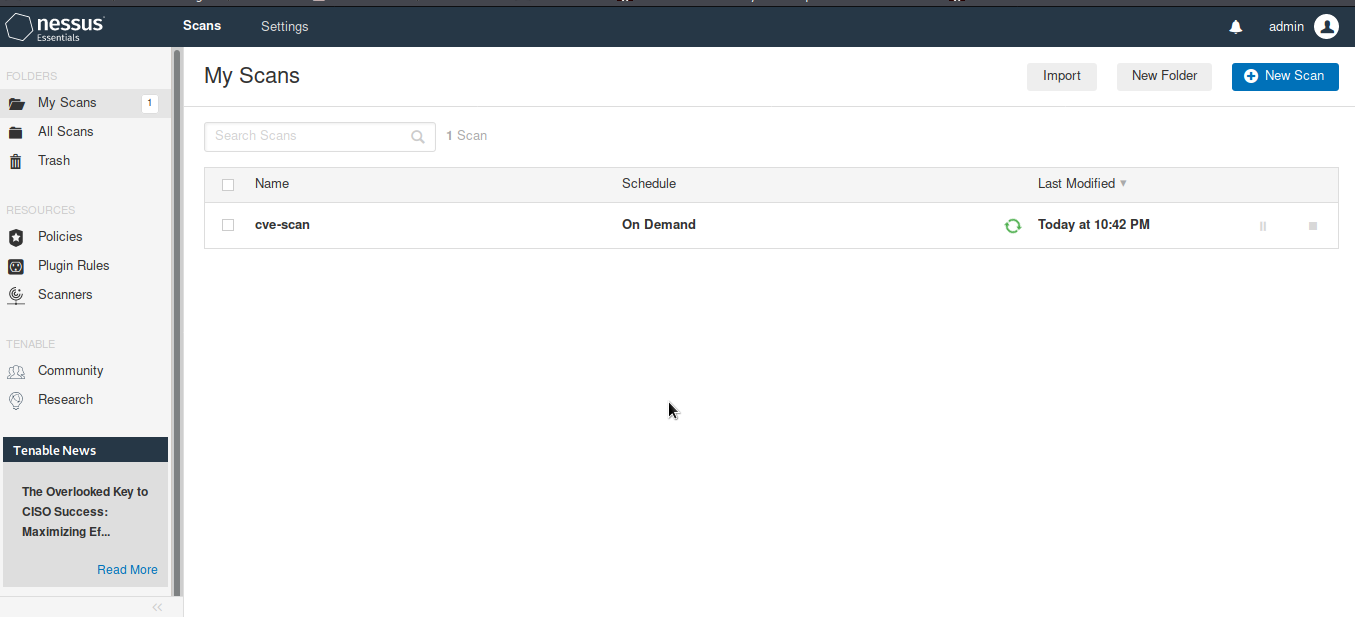
1. Install Nessus in your virtual machine open it .



1. Click on new scan.
2. Then click on advance scan .

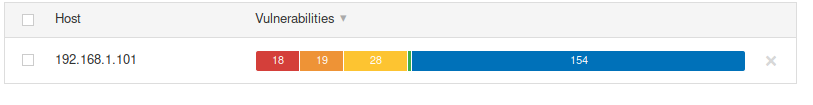


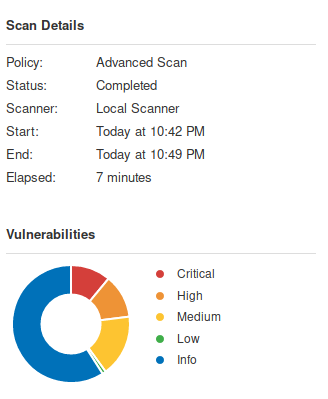
1. Now, fill name description and target ip which is 192.168.1.101 in this case.
2. And then click on scan.

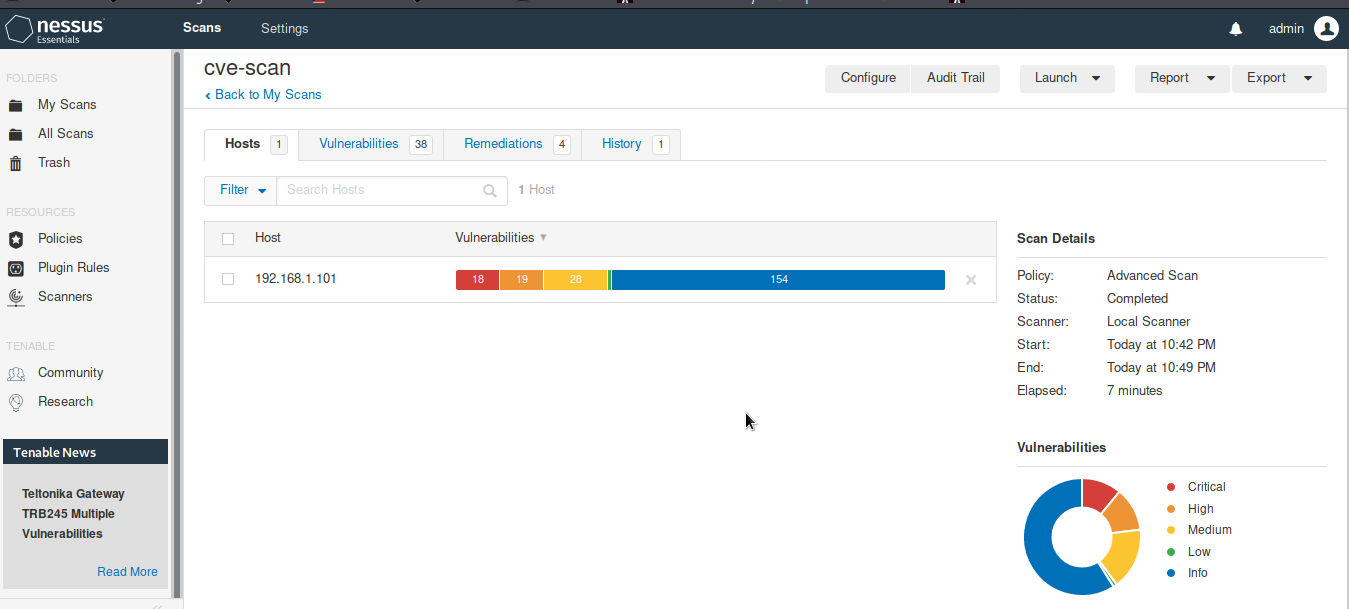


1. After scan complete we can see all the vulnerabilities index as –

* Critical
* High
* Medium
* Low
* Info







As we can see we have –

* 18 critical
* 19 high
* 28 medium vulnerabilities.