Module:- SECURITY CONCEPT

(NESSUS)

Name:-Prithviraj Nikam

NESSUS

What is NESSUS and How Does it Work?

Nessus is a proprietary vulnerability scanner developed by Tenable, Inc. Tenable.io is a subscription-based service.Tenable also contains what was previously known as Nessus Cloud, which used to be Tenable Software-as-a-Service Solution.Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools.

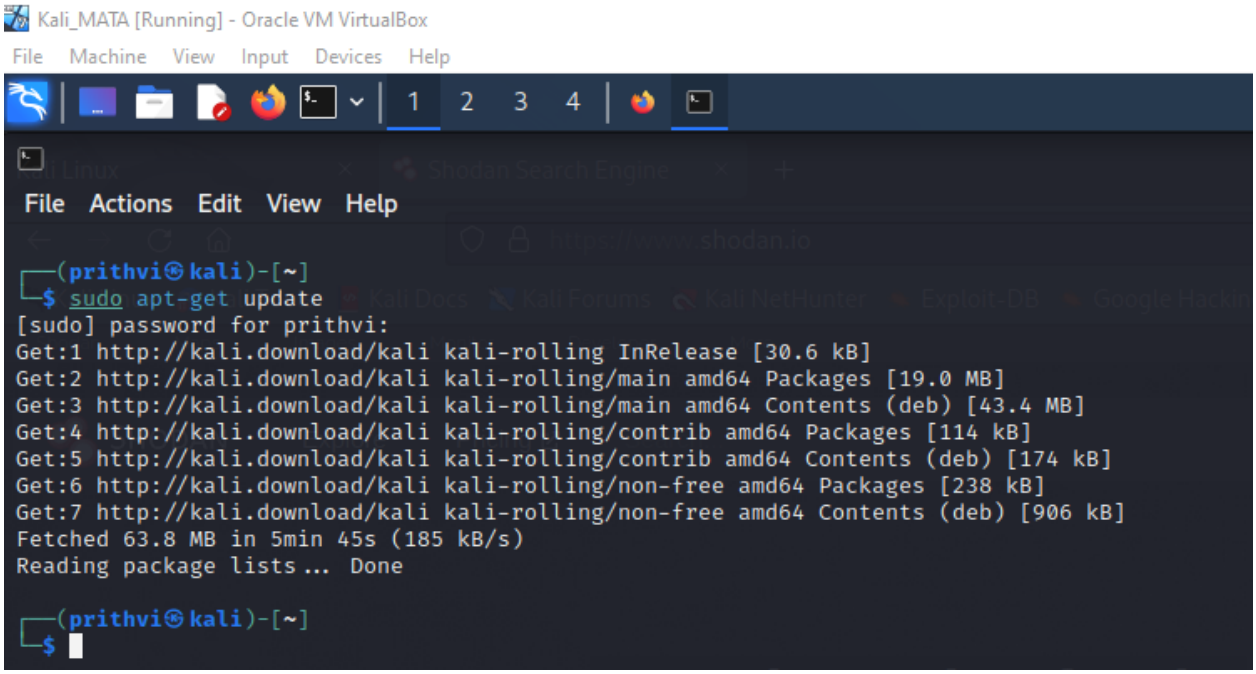
PORT:- 8834

Nessus can scan these vulnerabilities and exposures

- Vulnerabilities that could allow unauthorized control or access to sensitive data on a system
- Misconfiguration (e.g. open mail relay)
- Denials of service (Dos) vulnerabilities
- Default passwords, a few common passwords, and blank/absent passwords on some system accounts

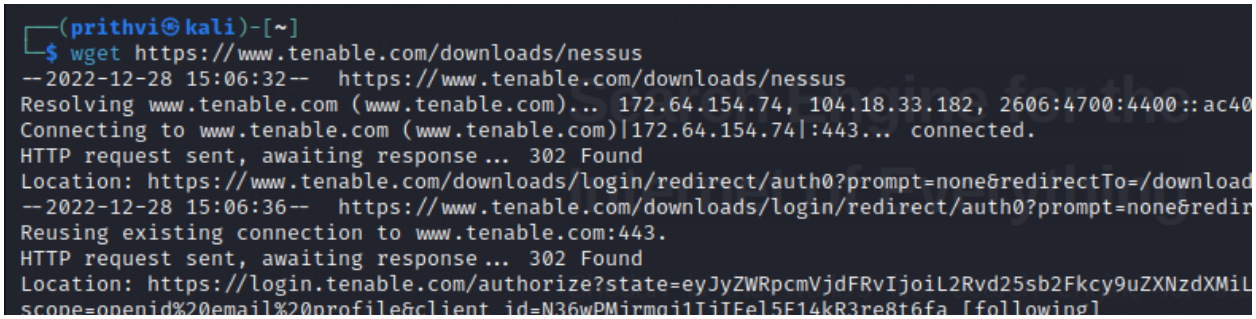
Step-1:- Update the libraries

 # sudo apt-get update



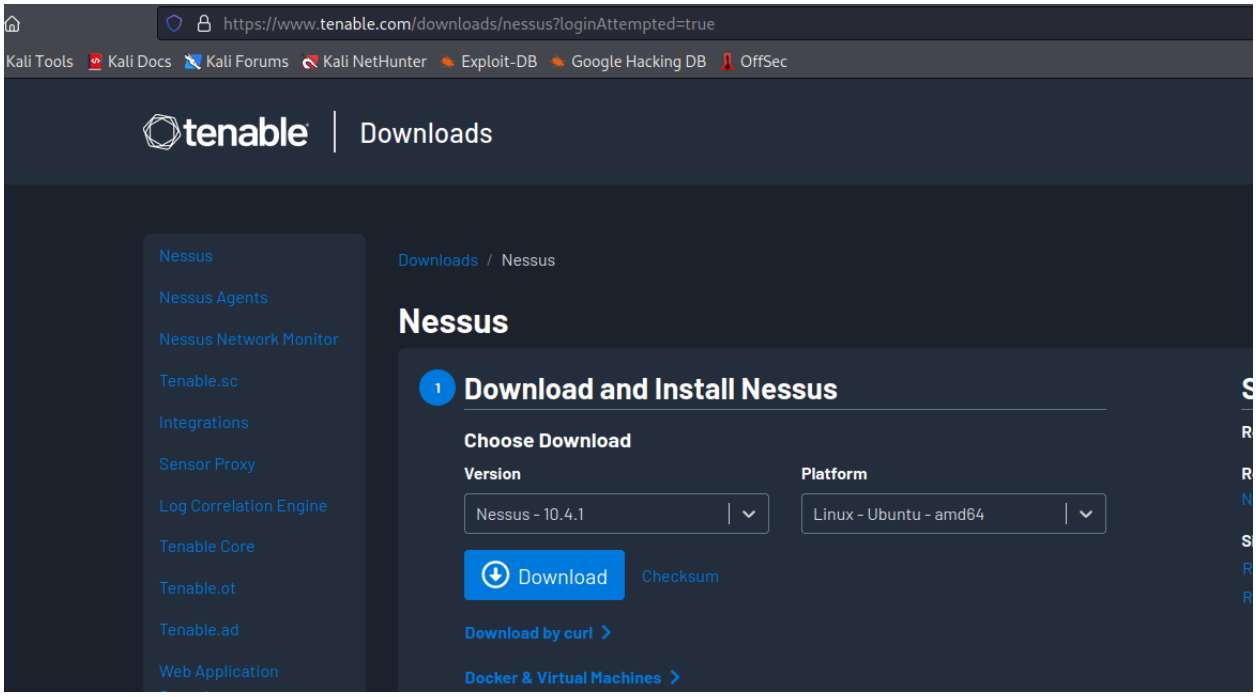
Step-2:-Download Nessus

$ wget https://www.tenable.com/downloads/nessus

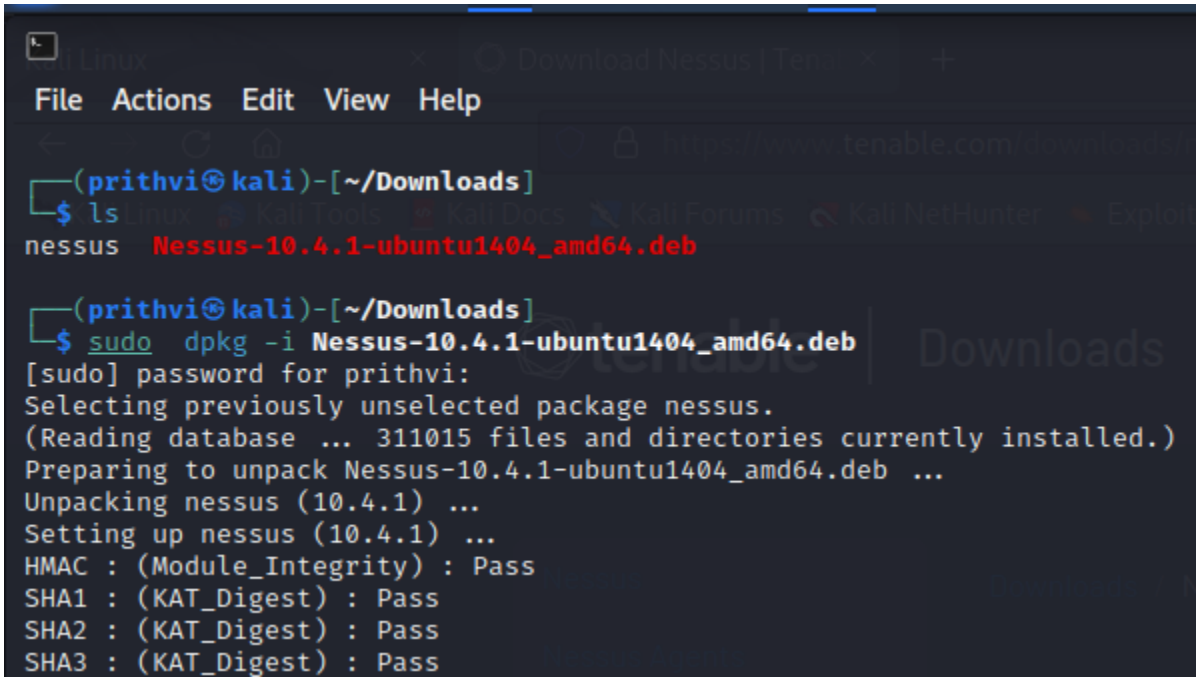


[OR]

Go to website
https://www.tenable.com/downloads/nessus



Step-3:-Install Nessus in Kali Machine
$ sudo dpkg -i Nessus-10.4.1-ubuntu1404_amd64.deb

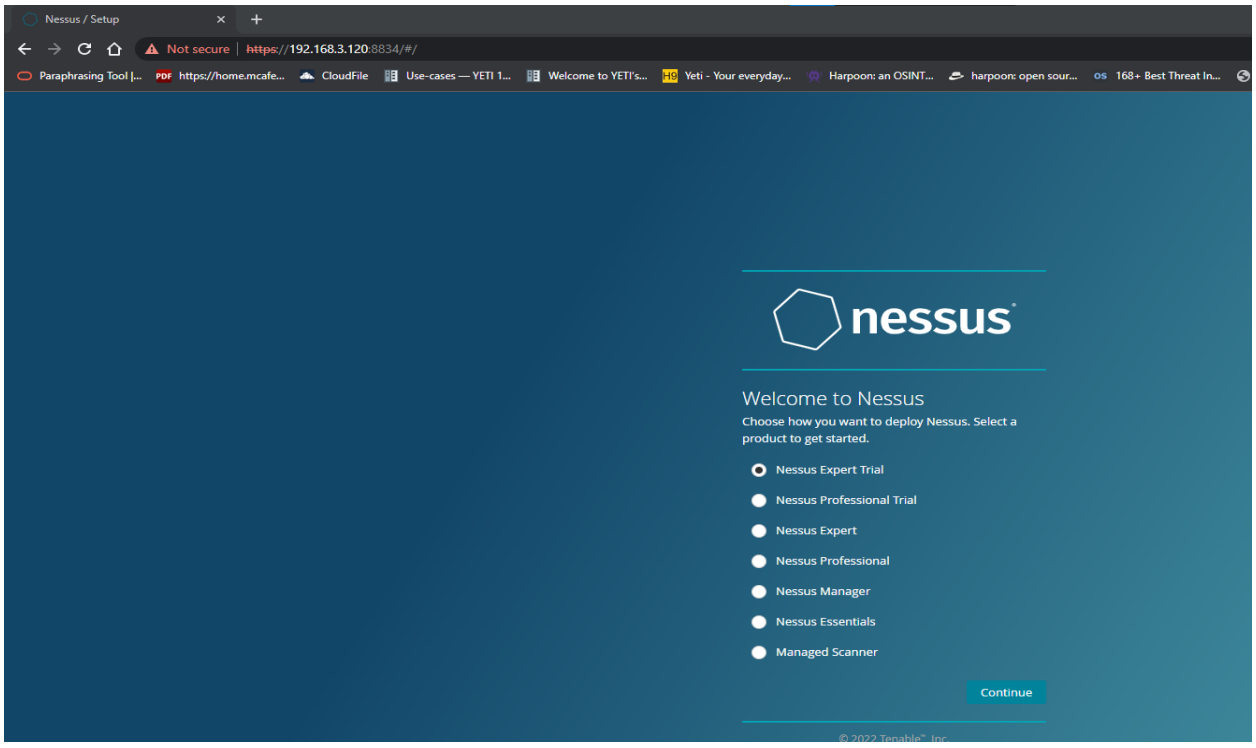


Step-4:- Start the Nessus Service
$ sudo systemctl start nessusd

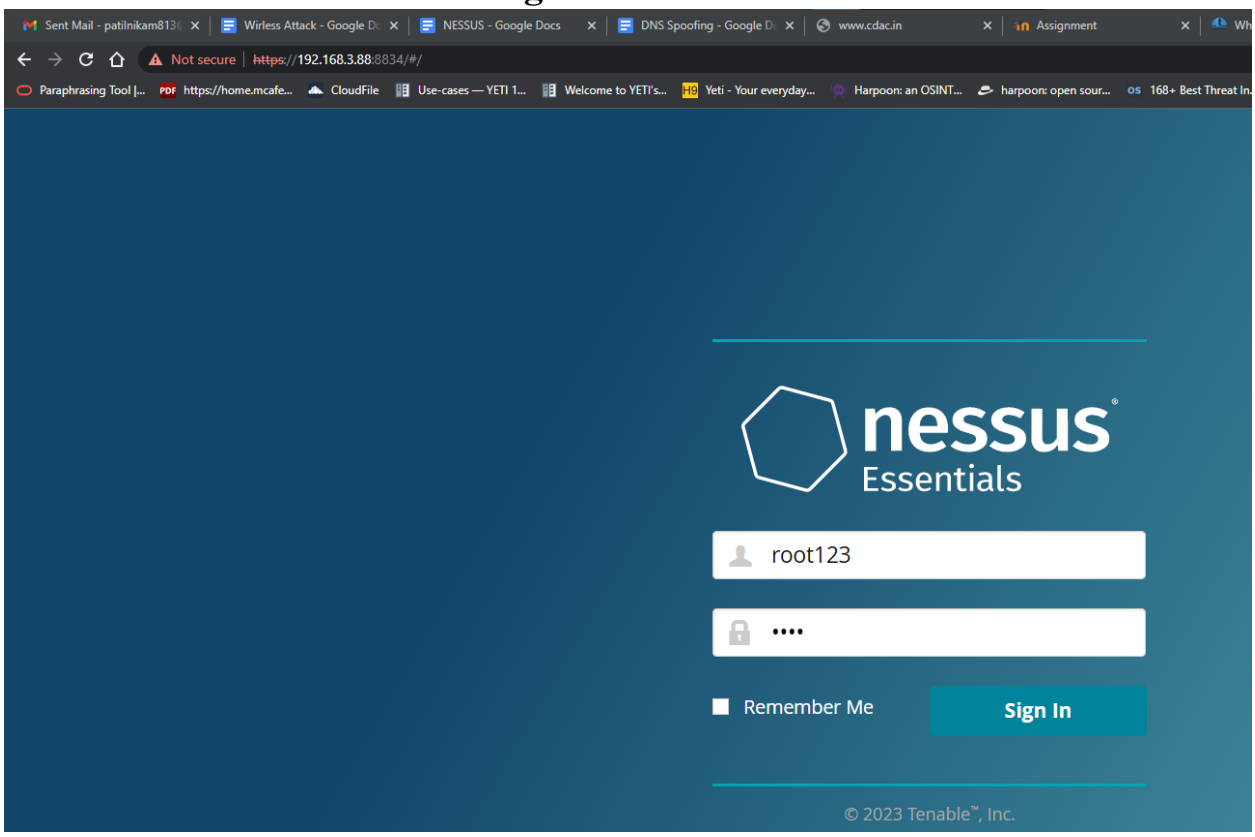
```
┌──(prithvi㉿kali)-[~/Downloads]
└─$ systemctl start nessusd

┌──(prithvi㉿kali)-[~/Downloads]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.3.120  netmask 255.255.255.0  broadcast 192.168.3.255
        inet6 fe80::a00:27ff:fe6a:eca1  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:6a:ec:a1  txqueuelen 1000  (Ethernet)
        RX packets 226364  bytes 151549631 (144.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 116504  bytes 9183205 (8.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Step-5:-Go to Browser and Type
http:// 192.168.3.88:8834

Kali IP **Port No**



- **Select “Nessus Essential “ (only Accept 16 ip address)**
- **Create Nessus Account and Login**



- **Download Plugins**

  —-> On GUI

  [OR]

  ——---> Through command

  $ sudo rm -rf /opt/*

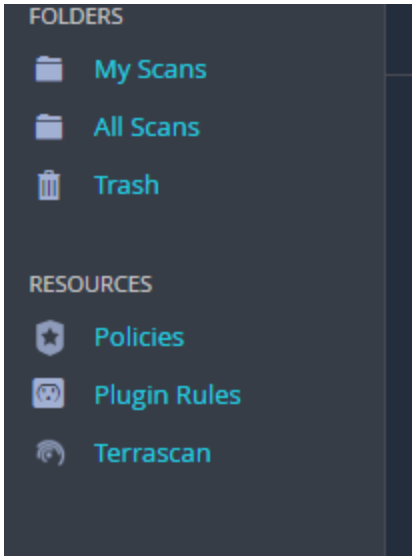
  $ reboot

  $ sudo dpkg -i Nessus-10.4.1-ubuntu1404_amd64.deb

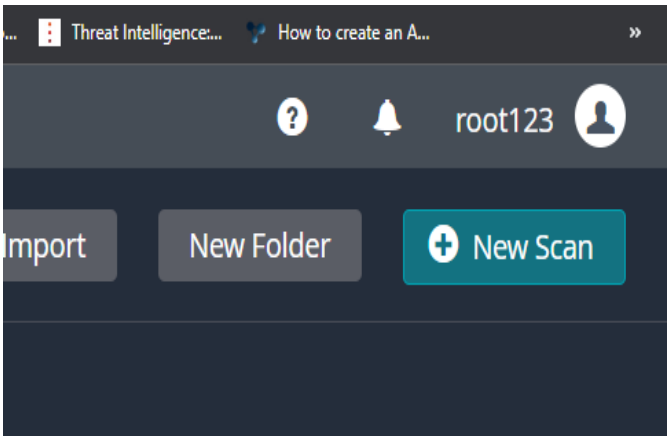
  $ sudo systemctl start nessusd

  $ sudo opt/nessus/sbin/nessuscli update

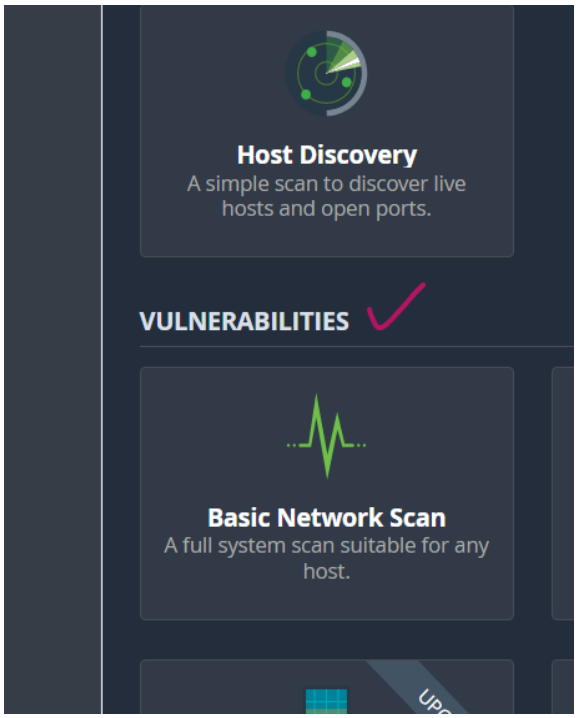
Step-6:- After Login Downloaded Plugin show Following Figure



Step-7:- After Login go to New Scan Option



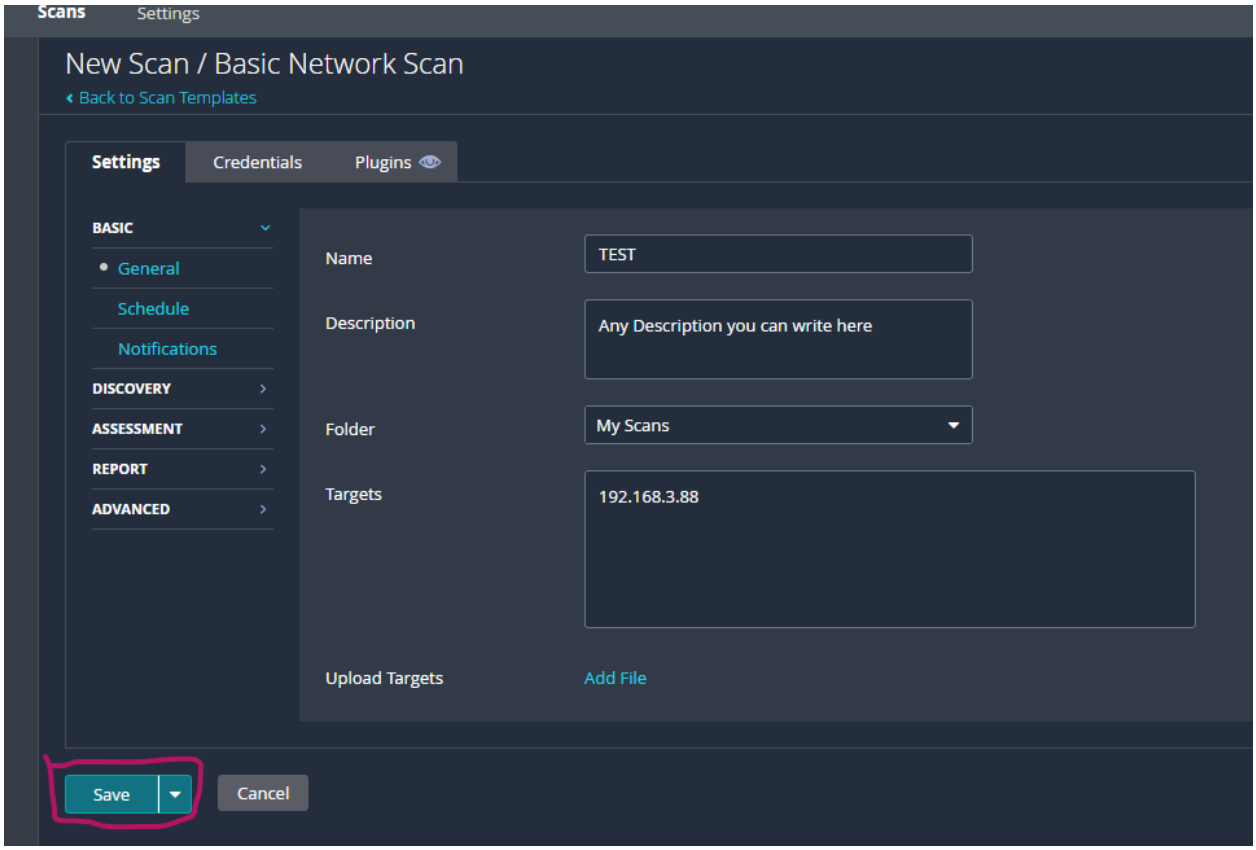
Step-8:-Select Basic Network Scan in Vulnerabilities



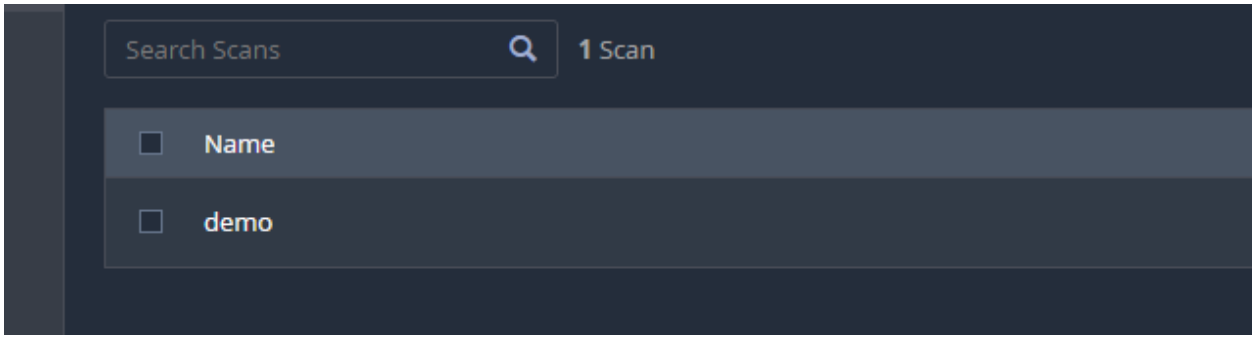
Step-9:- After Network scan selection feel the following Details and save it
Name: Demo (Any)
Description: Any Description you can write here
Folder:- My Scans
Target : 192.168.3.163
Metasploit Machine ip

Note :- Download the Metasploit Machine and in Virtual BOX

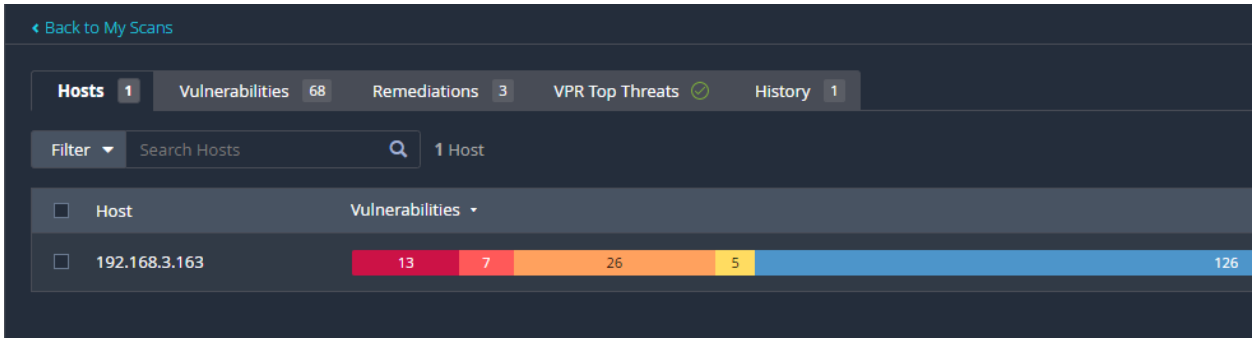
https://sourceforge.net/projects/metasploitable/files/latest/download



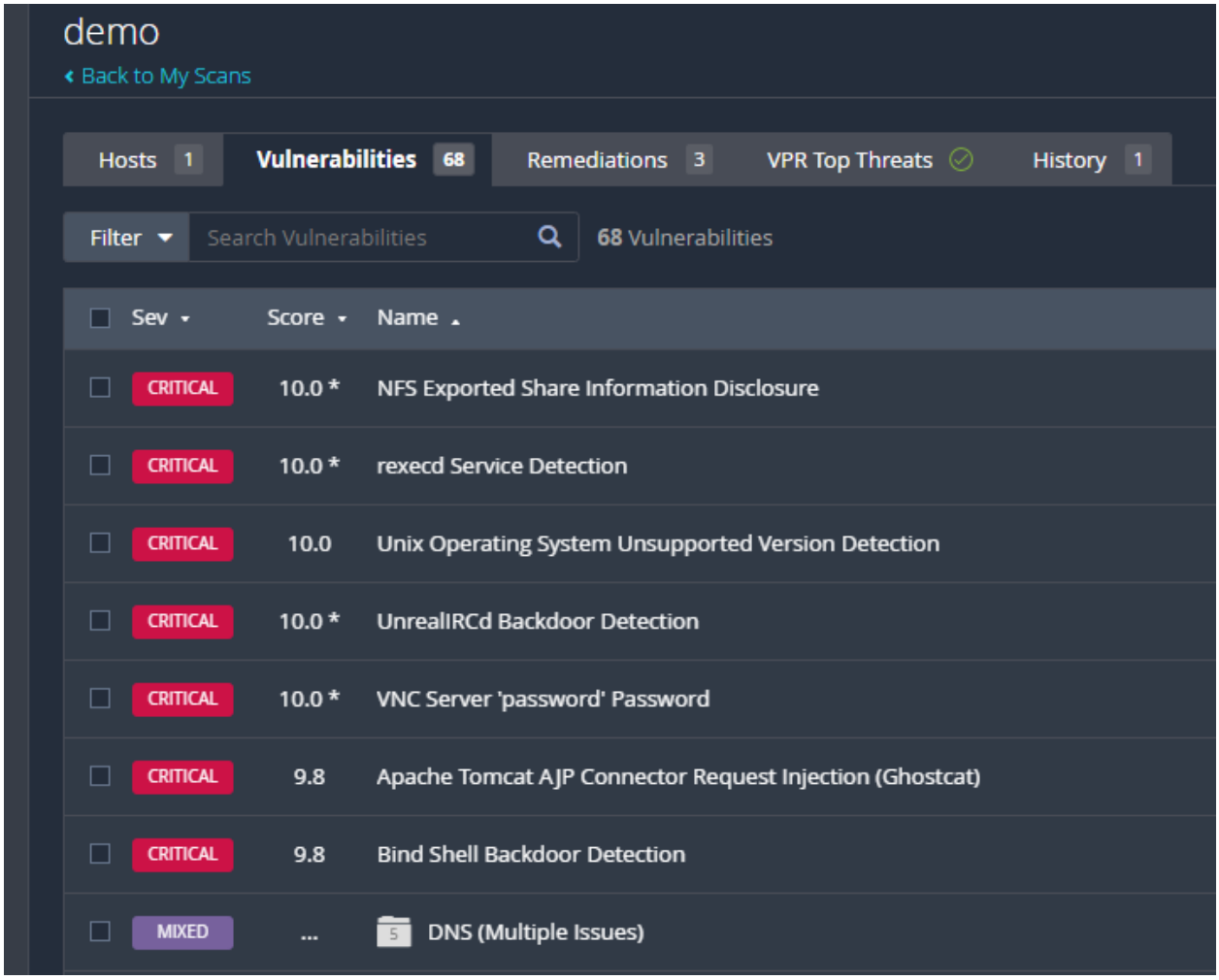
Step-10:-After saving scanning is running way



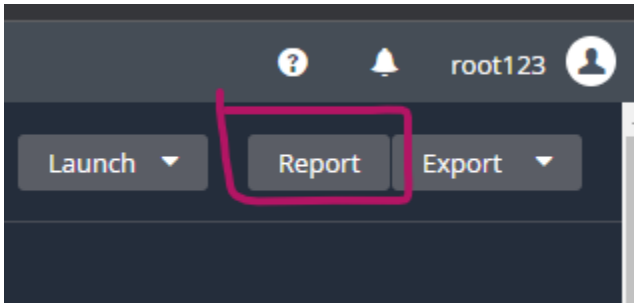
Step-11:- Scanning will be finished then click the Scanned “Demo “ Hosts



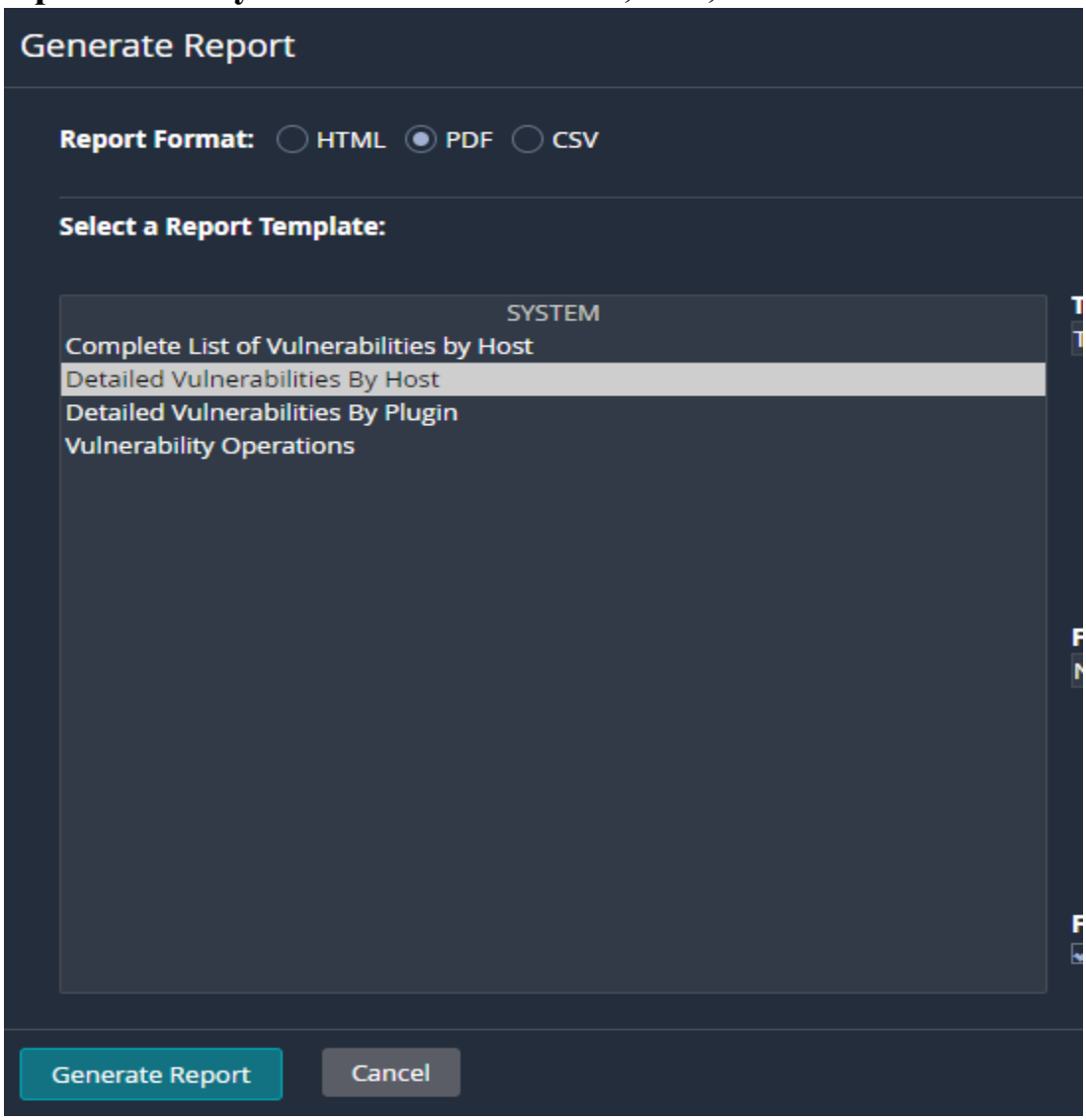
Step-12:- Click Vulnerabilities option that can be show many scanned vulnerabilities



Step-13:- Now select the “Report” Generate Option



Step-14:- Here you can select any system option that can be generate report in many extension like HTML,PDF,CSV



Step-15:- Open the Downloaded Report

192.168.3.163

CRITICAL	HIGH	MEDIUM	LOW	INFO
13	7	26	5	126

Scan Information

Start time:	Thu Dec 29 15:17:23 2022
End time:	Thu Dec 29 15:30:31 2022

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.3.163
MAC Address:	08:00:27:FF:39:3E
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities

134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

Synopsis

There is a vulnerable AJP connector listening on the remote host.

Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).