

## **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.

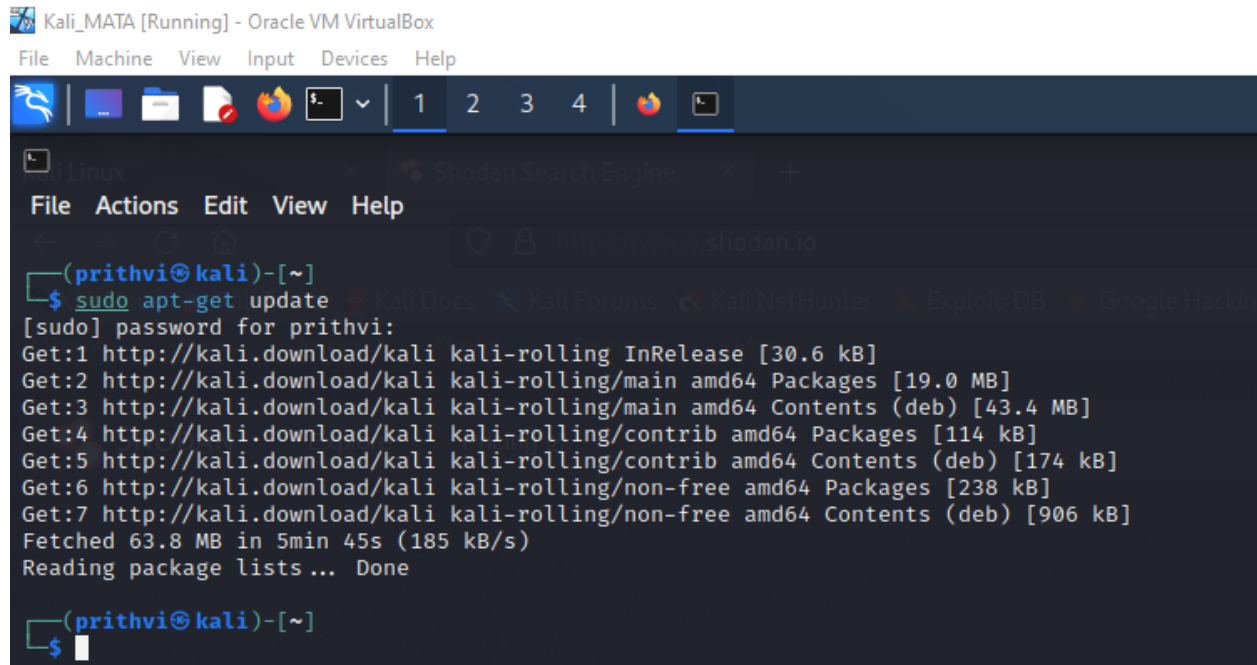
**PORT:- 8834**

#### **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**



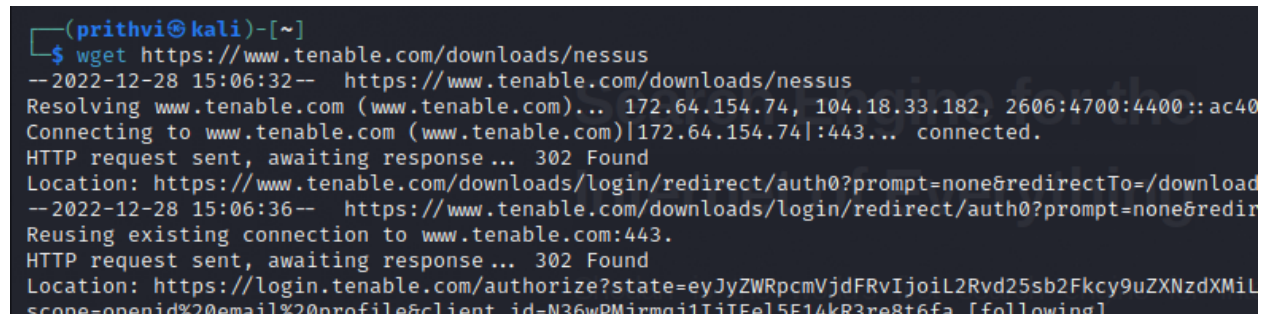
The screenshot shows a Kali Linux terminal window titled 'Kali\_MATA [Running] - Oracle VM VirtualBox'. The terminal displays the output of the command 'sudo apt-get update'. The output shows the system is fetching package lists from various sources, including kali-rolling InRelease, main amd64 Packages, and non-free amd64 Packages. The total size of the fetched packages is 63.8 MB, and the process took 5 minutes and 45 seconds at a rate of 185 kB/s.

```
(prithvi@kali)-[~]
$ sudo apt-get update
[sudo] password for prithvi:
Get:1 http://kali.download/kali kali-rolling InRelease [30.6 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.0 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [43.4 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [114 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [174 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [238 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [906 kB]
Fetched 63.8 MB in 5min 45s (185 kB/s)
Reading package lists... Done

(prithvi@kali)-[~]
$
```

## Step-2:-Download Nessus

\$ wget <https://www.tenable.com/downloads/nessus>



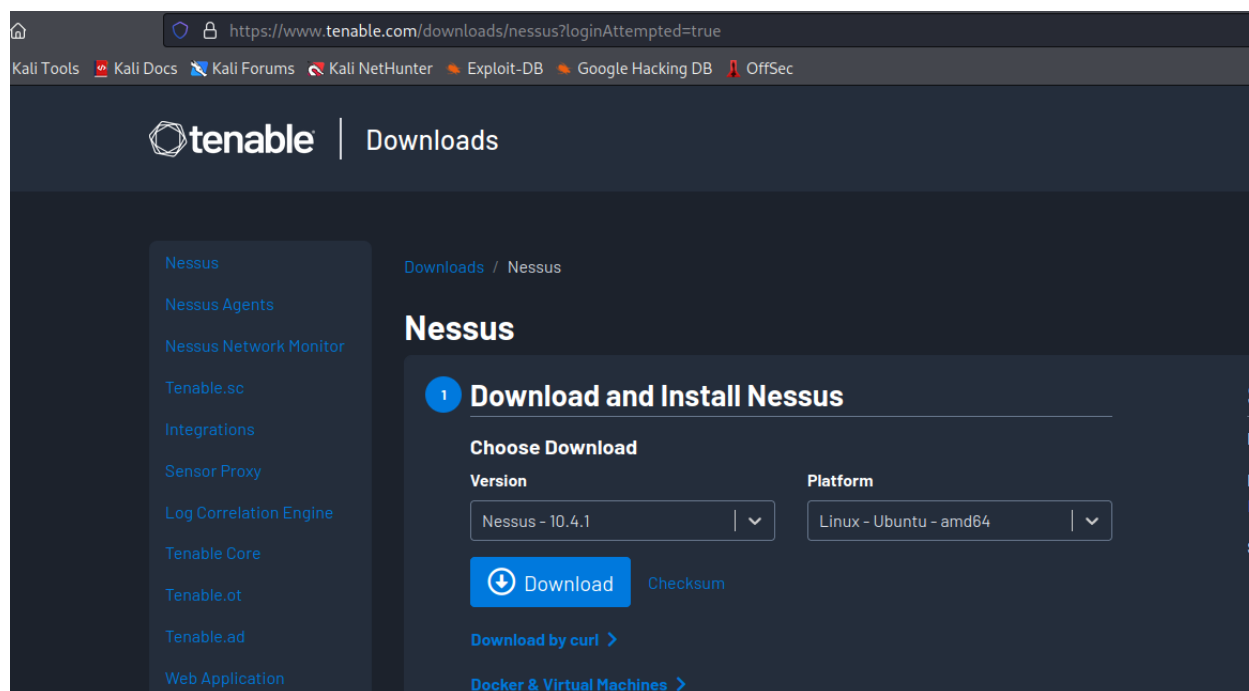
The screenshot shows a Kali Linux terminal window running the command 'wget https://www.tenable.com/downloads/nessus'. The output shows the wget process resolving the URL, connecting to the server, and receiving a 302 Found response. The location is redirected to 'https://login.tenable.com/authorize?state=eyJyZWVpcVjdFRvIjoil2Rvd25sb2Fkcy9uZXNzdXMiL...'. The process is still ongoing, as indicated by the '[following]' at the end of the output.

```
(prithvi@kali)-[~]
$ wget https://www.tenable.com/downloads/nessus
--2022-12-28 15:06:32-- https://www.tenable.com/downloads/nessus
Resolving www.tenable.com (www.tenable.com)... 172.64.154.74, 104.18.33.182, 2606:4700:4400::ac40
Connecting to www.tenable.com (www.tenable.com)|172.64.154.74|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://www.tenable.com/downloads/login/redirect/auth0?prompt=none&redirectTo=/download
--2022-12-28 15:06:36-- https://www.tenable.com/downloads/login/redirect/auth0?prompt=none&redir
Reusing existing connection to www.tenable.com:443.
HTTP request sent, awaiting response... 302 Found
Location: https://login.tenable.com/authorize?state=eyJyZWVpcVjdFRvIjoil2Rvd25sb2Fkcy9uZXNzdXMiL...
scope=openid%20email%20profile&client_id=N36wPMirmqil1iITe15E14kR3re8t6fa [following]
```

[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**

```
(prithvi@kali) - [~/Downloads]
$ ls
nessus  Nessus-10.4.1-ubuntu1404_amd64.deb

(prithvi@kali) - [~/Downloads]
$ sudo dpkg -i Nessus-10.4.1-ubuntu1404_amd64.deb
[sudo] password for prithvi:
Selecting previously unselected package nessus.
(Reading database ... 311015 files and directories currently installed.)
Preparing to unpack Nessus-10.4.1-ubuntu1404_amd64.deb ...
Unpacking nessus (10.4.1) ...
Setting up nessus (10.4.1) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
```

### Step-4:- Start the Nessus Service

**\$ sudo systemctl start nessusd**

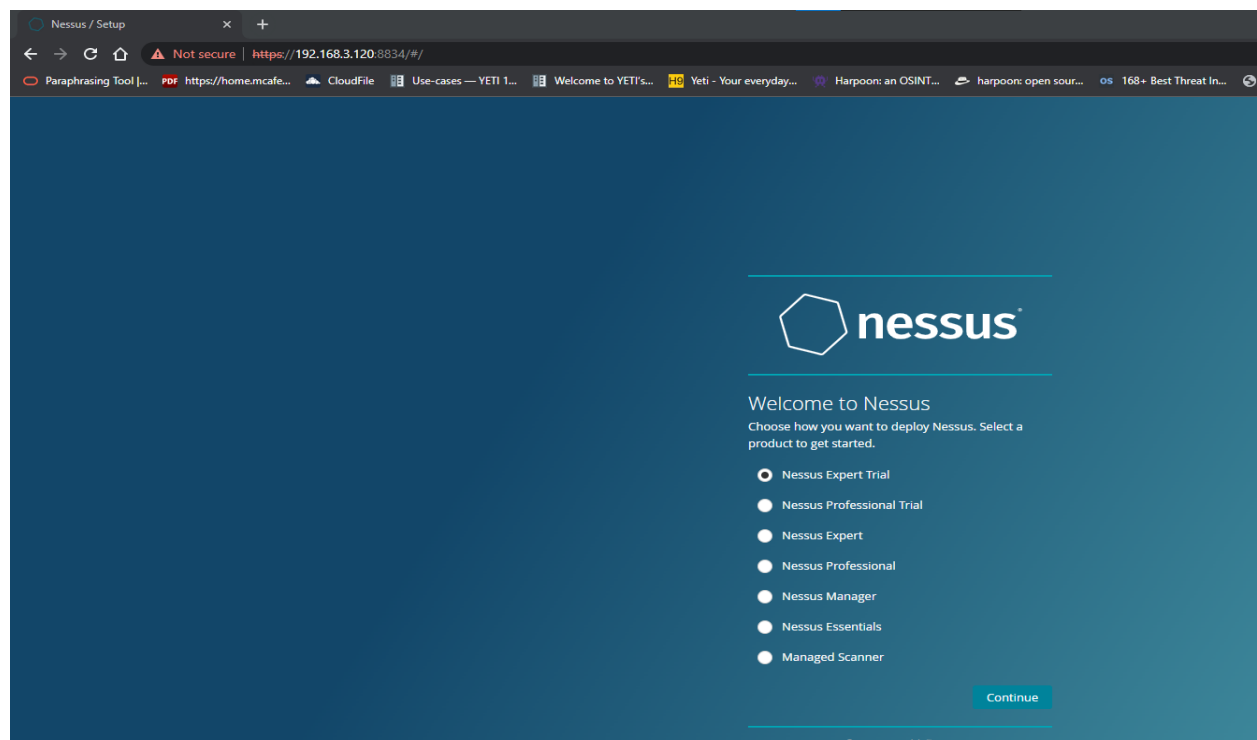
```
(prithvi@kali)-[~/Downloads]
$ systemctl start nessusd

(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

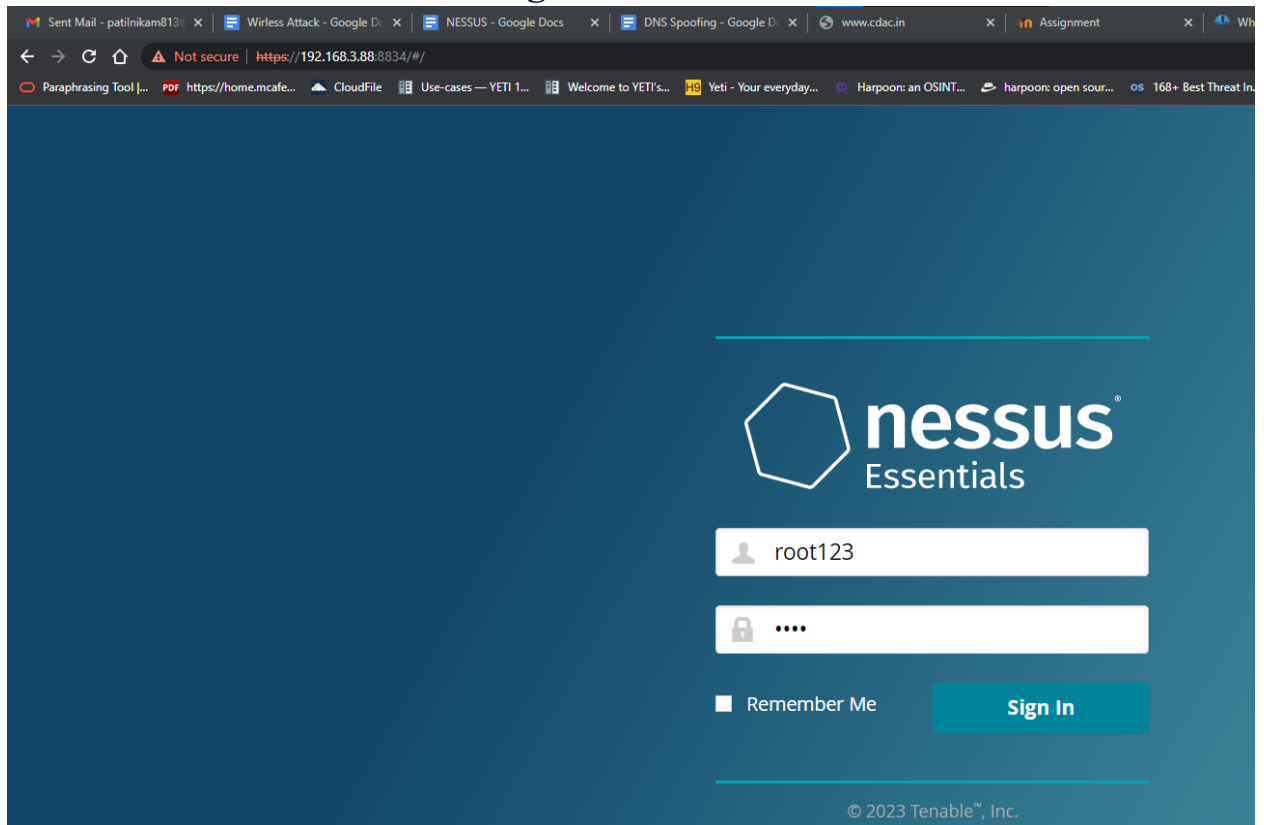
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 0  bytes 0 (0.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 0  bytes 0 (0.0 B)
    TX errors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

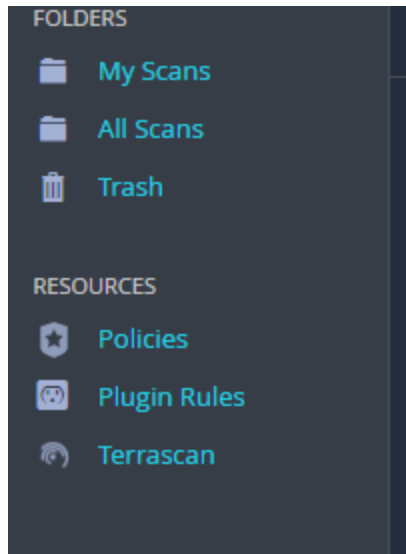


- Select “Nessus Essential “ (only Accept 16 ip address)
- Create Nessus Account and Login

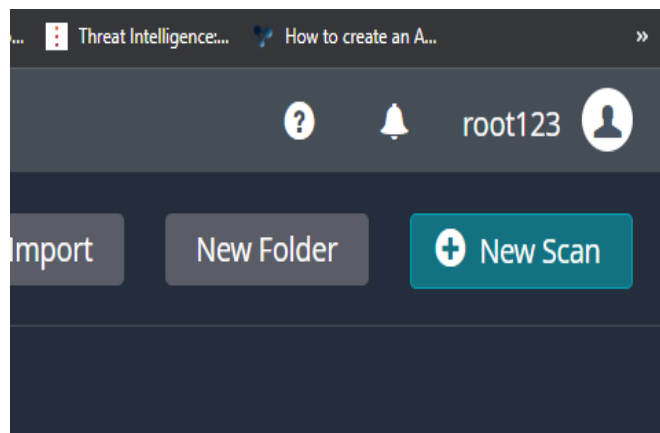


- Download Plugins
    - > On GUI
    - [OR]
    - > Through command
- ```
$ sudo rm -rf /opt/*
$ reboot
$ sudo dpkg -i Nessus-10.4.1-ubuntu1404_amd64.deb
$ sudo systemctl start nessusd
$ sudo opt/nessus/sbin/nessuscli update
```

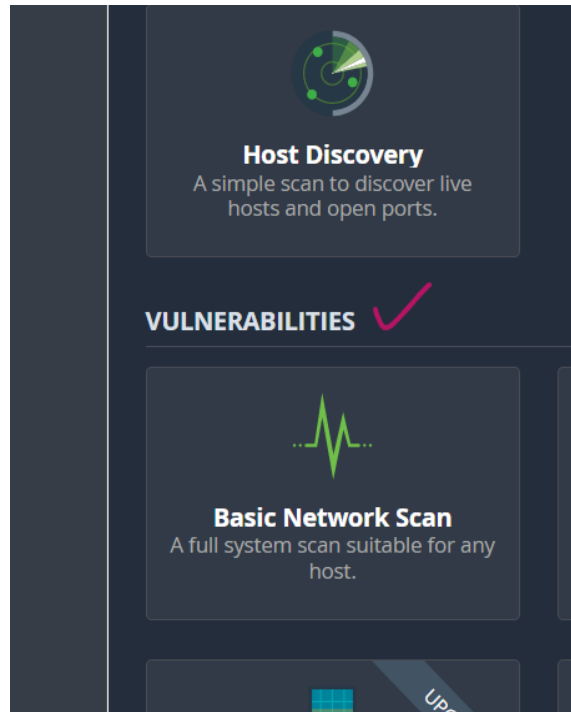
**Step-6:- After Login Downloaded Plugin show Following Figure**



**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>**

Scans Settings

## New Scan / Basic Network Scan

[← Back to Scan Templates](#)

Settings Credentials Plugins

**BASIC**

- General
- Schedule
- Notifications

**DISCOVERY**

**ASSESSMENT**

**REPORT**

**ADVANCED**

Name: TEST

Description: Any Description you can write here

Folder: My Scans

Targets: 192.168.3.88

Upload Targets [Add File](#)

Save Cancel

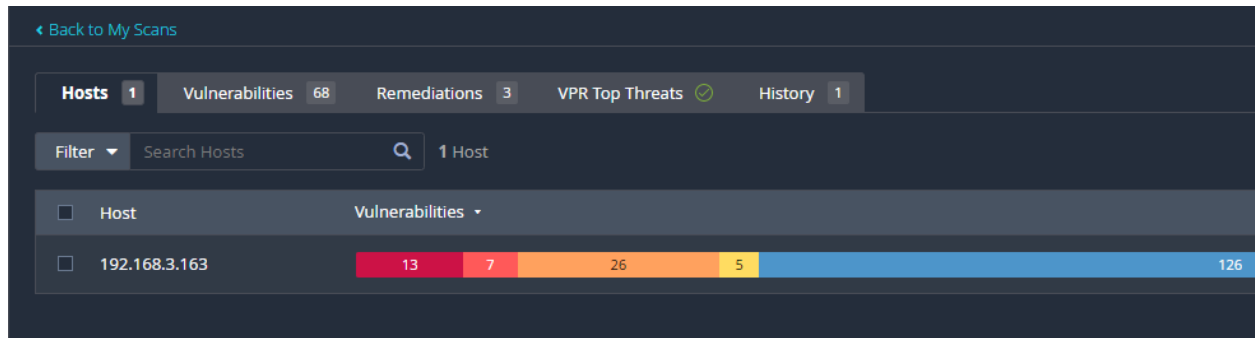
**Step-10:-After saving scanning is running way**

Search Scans [Q](#) 1 Scan

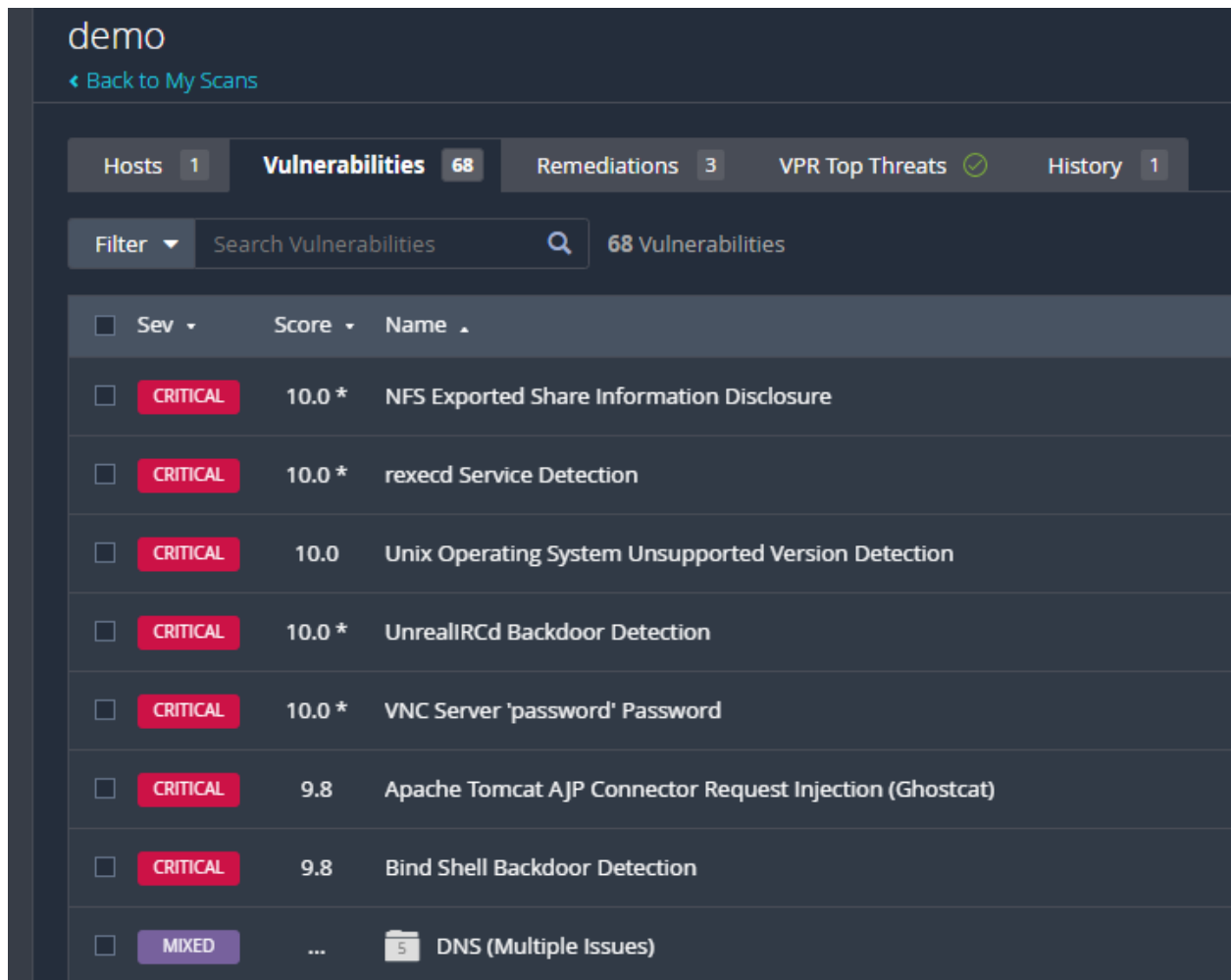
| <input type="checkbox"/> | Name |
|--------------------------|------|
| <input type="checkbox"/> | demo |

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

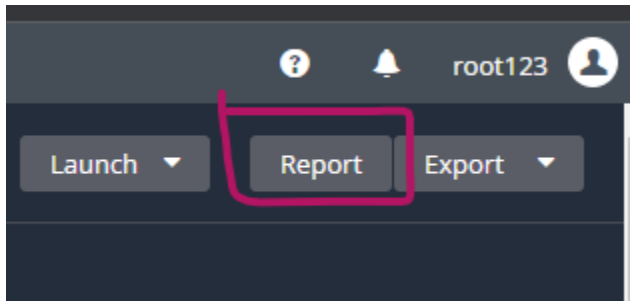




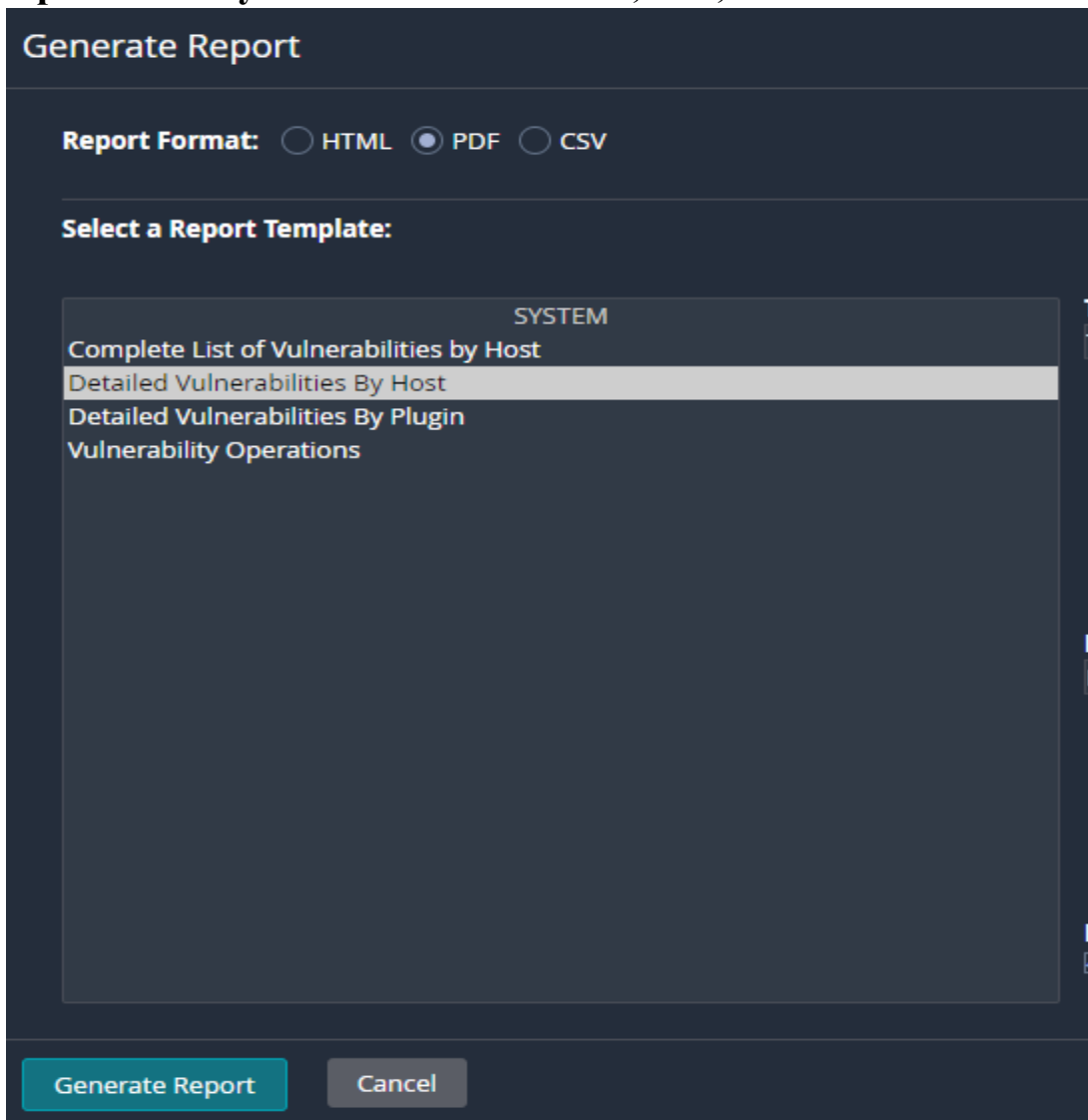
**Step-12:- Click Vulnerabilities option that can be show many scanned vulnerabilities**



**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**

A screenshot of a 'Generate Report' dialog box. The title bar says 'Generate Report'. Below the title, there is a 'Report Format' section with three radio buttons: 'HTML', 'PDF' (which is selected), and 'CSV'. Below this is a 'Select a Report Template:' section. It contains a list of templates under the heading 'SYSTEM': 'Complete List of Vulnerabilities by Host', 'Detailed Vulnerabilities By Host' (which is highlighted), 'Detailed Vulnerabilities By Plugin', and 'Vulnerability Operations'. At the bottom of the dialog, there are two buttons: 'Generate Report' and 'Cancel'.

## Step-15:- Open the Downloaded Report

