

**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.

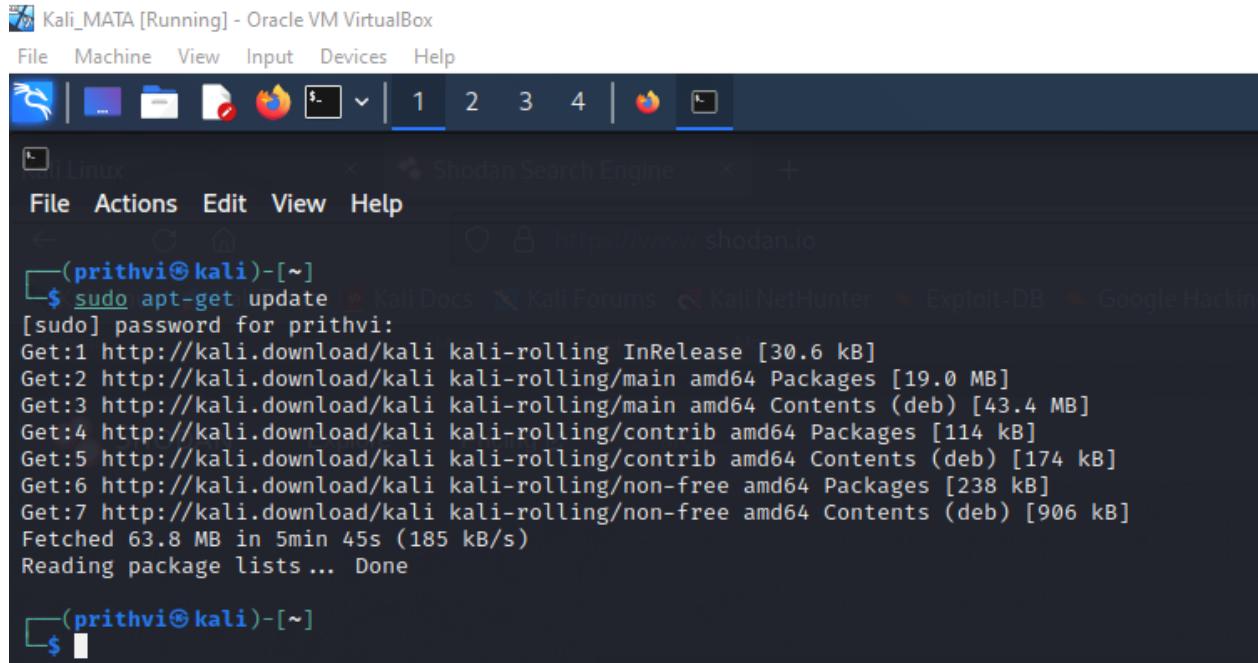
PORT:- 8834

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

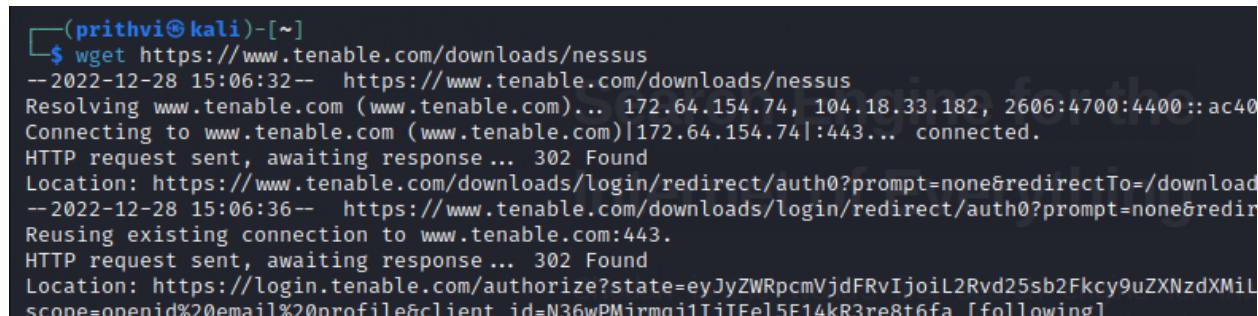


```
(prithvi㉿kali)-[~]
$ sudo apt-get update
[sudo] password for prithvi:
Get:1 http://kali.download/kali kali-rolling InRelease [30.6 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.0 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [43.4 kB]
Get:4 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
```



```
(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&redirectTo=/download
Reusing existing connection to www.tenable.com:443.
HTTP request sent, awaiting response ... 302 Found
Location: https://login.tenable.com/authorize?state=eyJyZWRpcmVjdFRvIjoil2Rvd25sb2Fkcy9uZXNzdXMlL
scope=openid%20email%20profile&client_id=N36wPMirmqj1TiJFcl5F14kR3re8t6fa [following]
```

[OR]

Go to website

<https://www.tenable.com/downloads/nessus>

The screenshot shows the Tenable Downloads page for Nessus. On the left, there's a sidebar with links like Nessus, Nessus Agents, Nessus Network Monitor, Tenable.sc, Integrations, Sensor Proxy, Log Correlation Engine, Tenable Core, Tenable.ot, Tenable.ad, and Web Application. The main content area has a breadcrumb path 'Downloads / Nessus' and the title 'Nessus'. Below it is a section titled '1 Download and Install Nessus' with a 'Choose Download' form. The 'Version' dropdown is set to 'Nessus - 10.4.1' and the 'Platform' dropdown is set to 'Linux - Ubuntu - amd64'. There are buttons for 'Download' (with a checksum link), 'Download by curl', and 'Docker & Virtual Machines'.

Step-3:-Install Nessus in Kali Machine

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

The terminal window shows the user navigating to their Downloads directory and running the command to install the Nessus deb package. The output of the command shows the package being selected, unpacked, and configured.

```
(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
[Templeton]

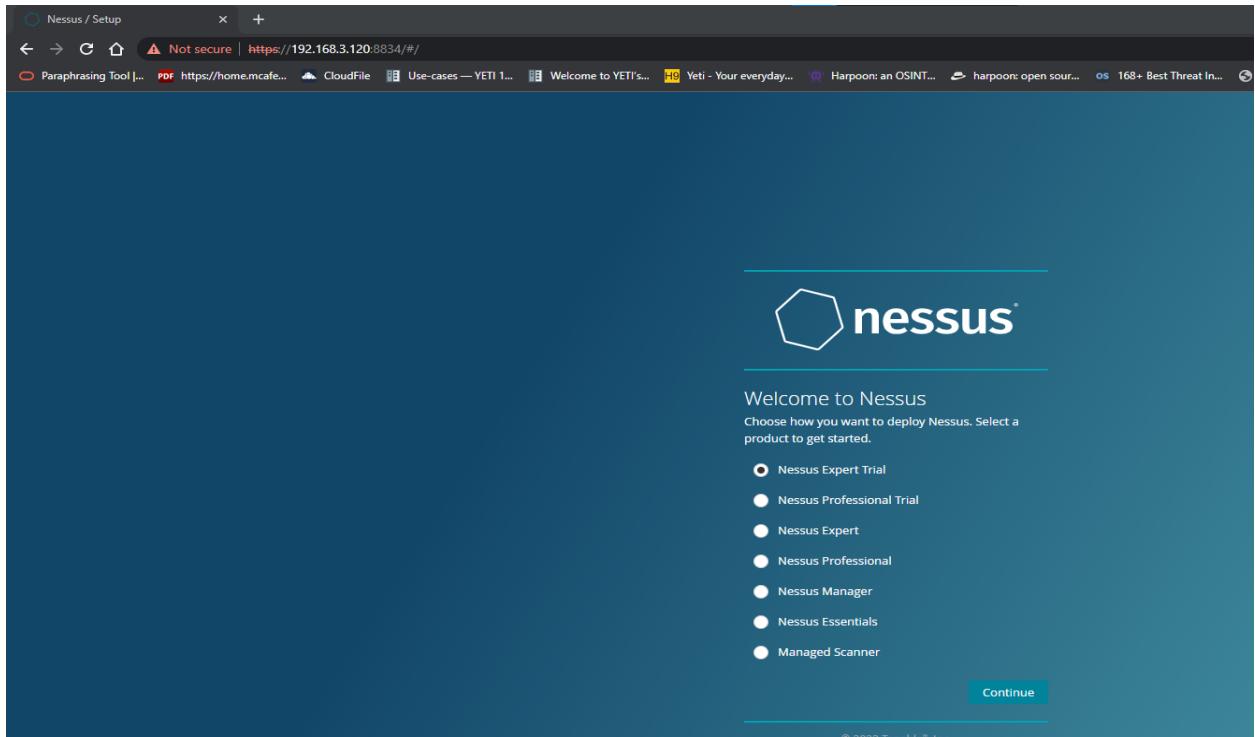
└──(prithvi㉿kali)-[~/Downloads] Integrations
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.3.120 netmask 255.255.255.0 broadcast 192.168.3.255
        inet6 fe80::a00:27ff:fe6a:ec1 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:6a:ec:a1 txqueuelen 1000 (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

```

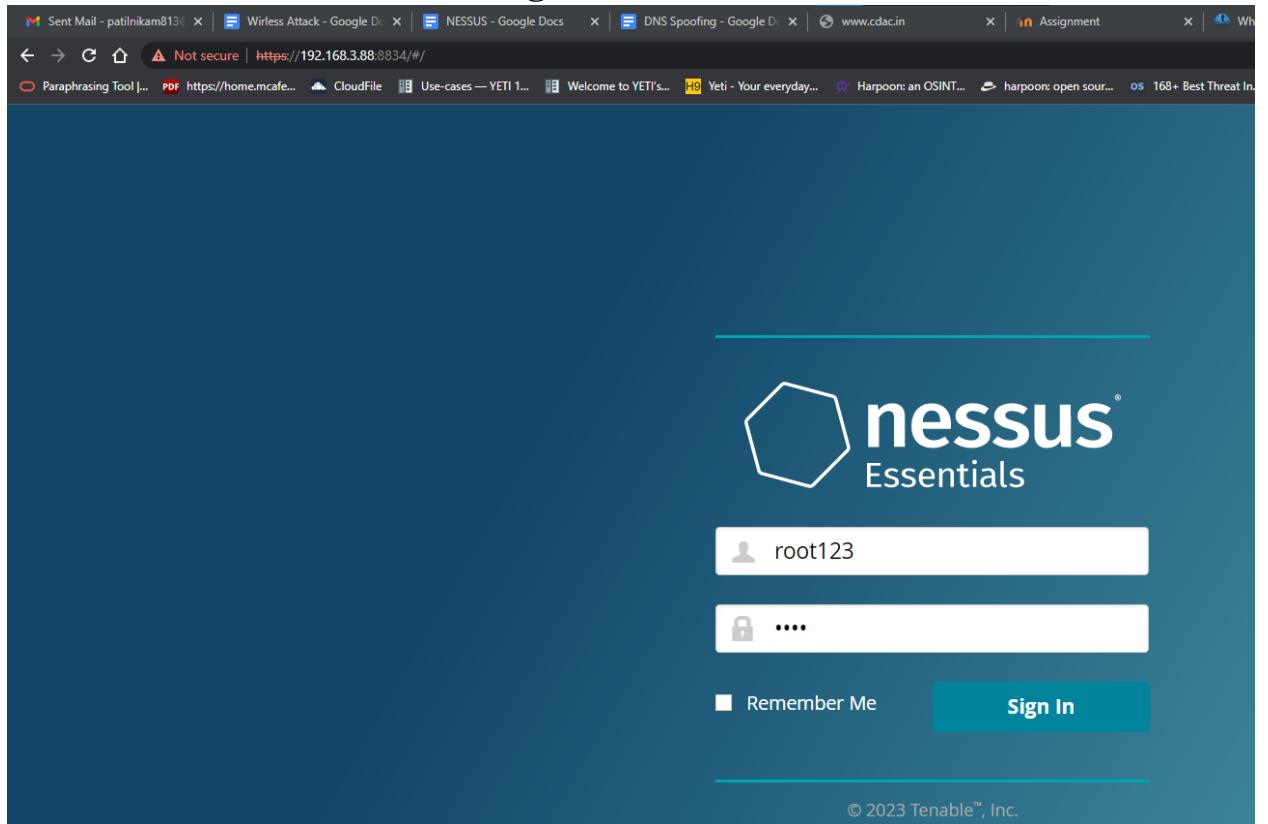
Step-5:-Go to Browser and Type

<http://192.168.3.88:8834>

Kali IP Port No

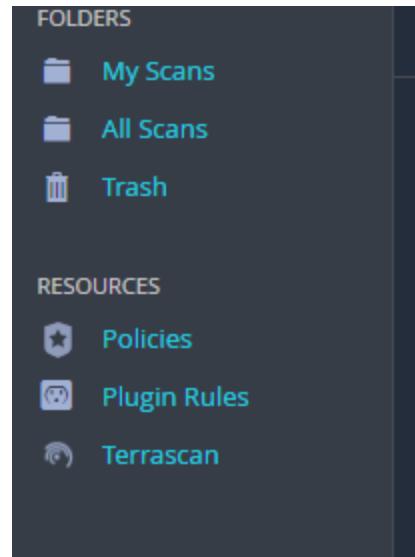


- Select “Nessus Essential “ (only Accept 16 ip address)
- Create Nessus Account and Login

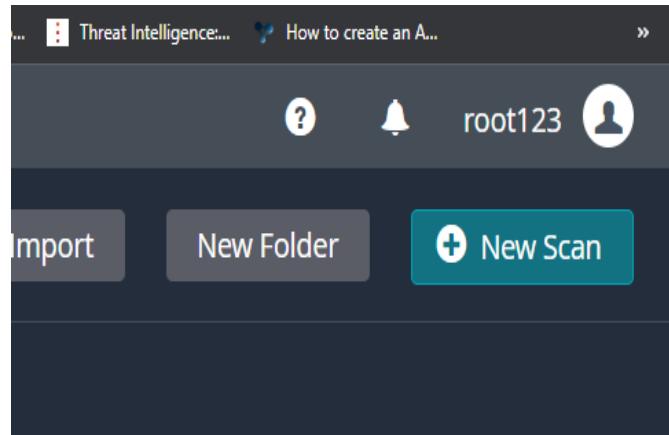


- Download Plugins
 - > On GUI
 - [OR]
 - > Through command
- ```
$ sudo rm -rf /opt/*
$ reboot
$ sudo dpkg -i Nessus-10.4.1-ubuntu1404_amd64.deb
$ sudo systemctl start nessusd
$ sudo opt/nessus/sbin/nessuscli update
```

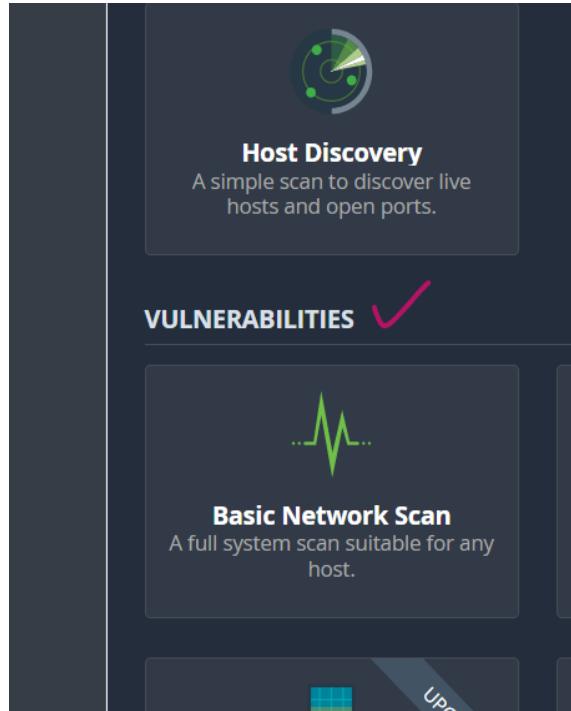
**Step-6:- After Login Downloaded Plugin show Following Figure**



**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 (selected)
- 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 1 Scan

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

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

[◀ Back to My Scans](#)

Hosts 1 | Vulnerabilities 68 | Remediations 3 | VPR Top Threats ⓘ | History 1

Filter ▾ Search Hosts  1 Host

| Host          | Vulnerabilities |
|---------------|-----------------|
| 192.168.3.163 | 13 7 26 5 126   |

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

demo

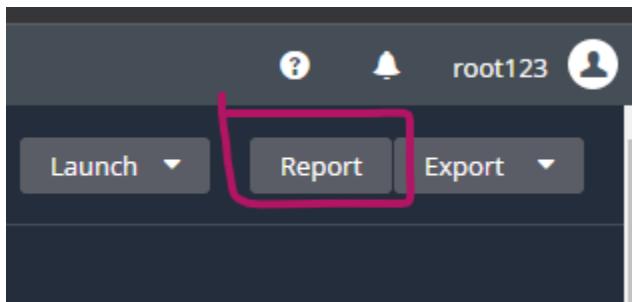
[◀ Back to My Scans](#)

Hosts 1 | **Vulnerabilities 68** | Remediations 3 | VPR Top Threats ⓘ | History 1

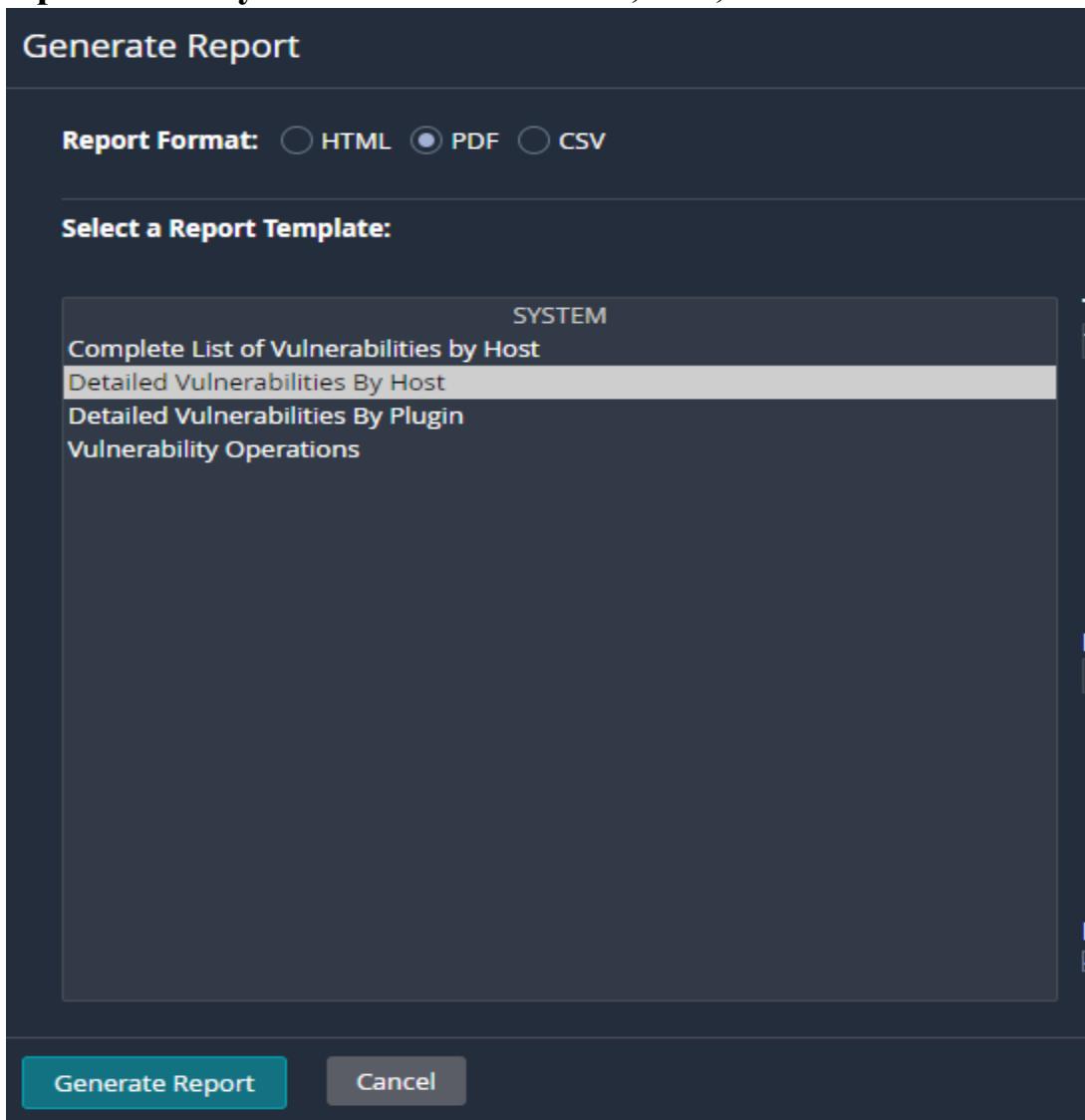
Filter ▾ Search Vulnerabilities  68 Vulnerabilities

| Sev      | Score  | Name                                                     |
|----------|--------|----------------------------------------------------------|
| CRITICAL | 10.0 * | NFS Exported Share Information Disclosure                |
| CRITICAL | 10.0 * | rexecd Service Detection                                 |
| CRITICAL | 10.0   | Unix Operating System Unsupported Version Detection      |
| CRITICAL | 10.0 * | UnrealIRCd Backdoor Detection                            |
| CRITICAL | 10.0 * | VNC Server 'password' Password                           |
| CRITICAL | 9.8    | Apache Tomcat AJP Connector Request Injection (Ghostcat) |
| CRITICAL | 9.8    | Bind Shell Backdoor Detection                            |
| MIXED    | ...    | DNS (Multiple Issues)                                    |

**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

