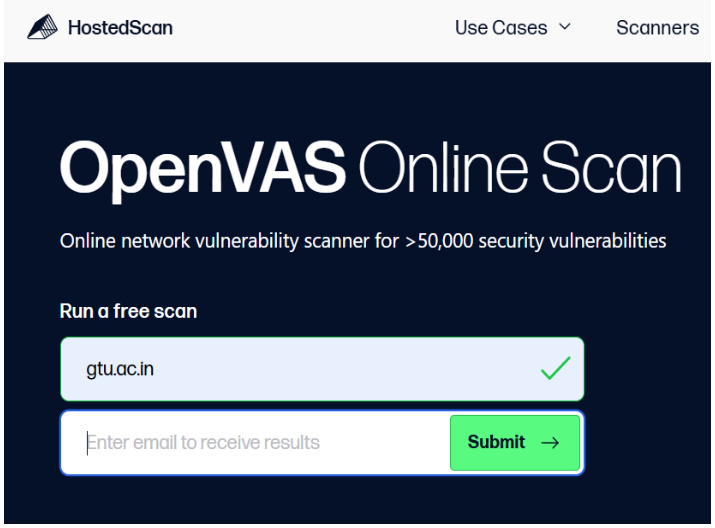
PRACTICAL – 4

AIM: Labs of Vulnerability Assessment using OpenVAS.

Online Vulnerability Assessment Link: https://hostedscan.com/openvas-vulnerability-scan



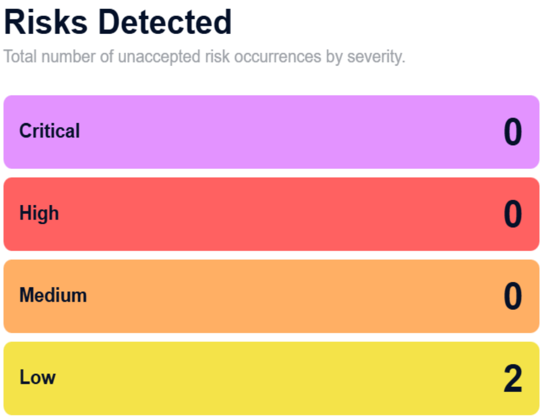
OpenVAS Online Scan

Online network vulnerability scanner for >50,000 security vulnerabilities

Run a free scan

gtu.ac.in ✓

Enter email to receive results

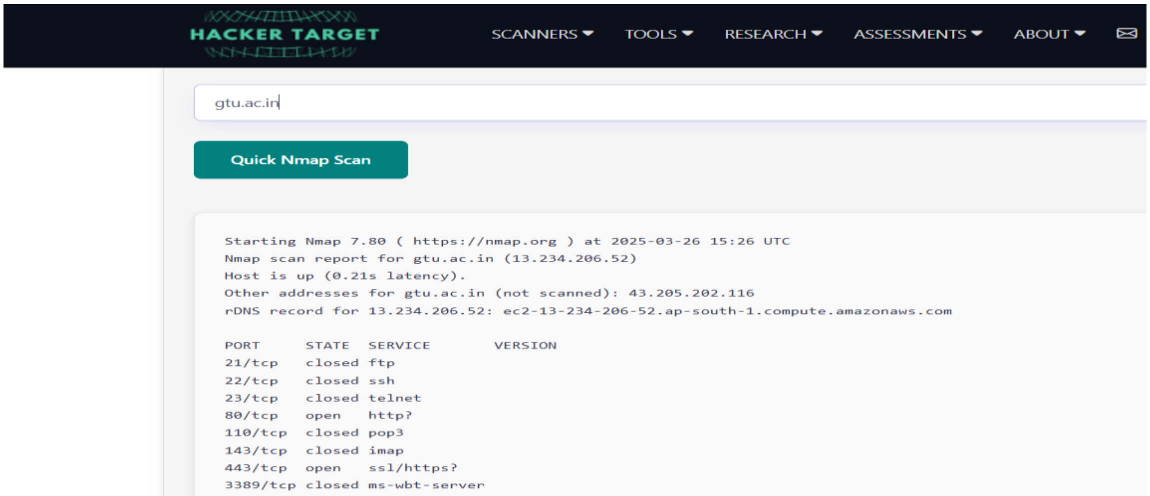


Risks Detected

Total number of unaccepted risk occurrences by severity.

Critical	0
High	0
Medium	0
Low	2

- https://hackertarget.com/



gtu.ac.in

```
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-26 15:26 UTC
Nmap scan report for gtu.ac.in (13.234.206.52)
Host is up (0.21s latency).
Other addresses for gtu.ac.in (not scanned): 43.205.202.116
rDNS record for 13.234.206.52: ec2-13-234-206-52.ap-south-1.compute.amazonaws.com

PORT     STATE  SERVICE       VERSION
21/tcp   closed ftp
22/tcp   closed ssh
23/tcp   closed telnet
80/tcp   open   http?
110/tcp  closed pop3
143/tcp  closed imap
443/tcp  open   ssl/https?
3389/tcp closed ms-wbt-server
```

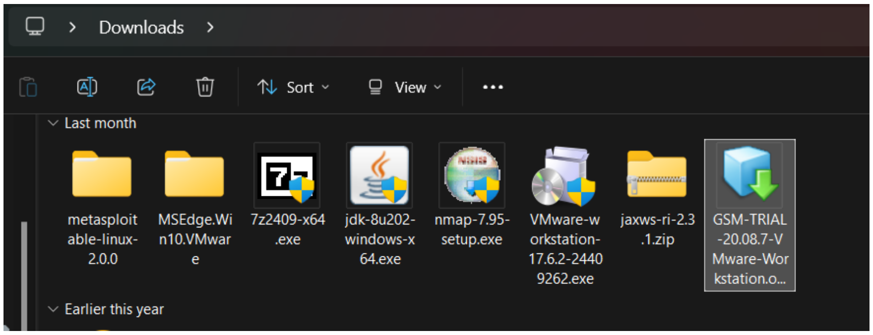
Perform following:

Configure the OpenVAS in kali Linux and perform the vulnerability assessment.

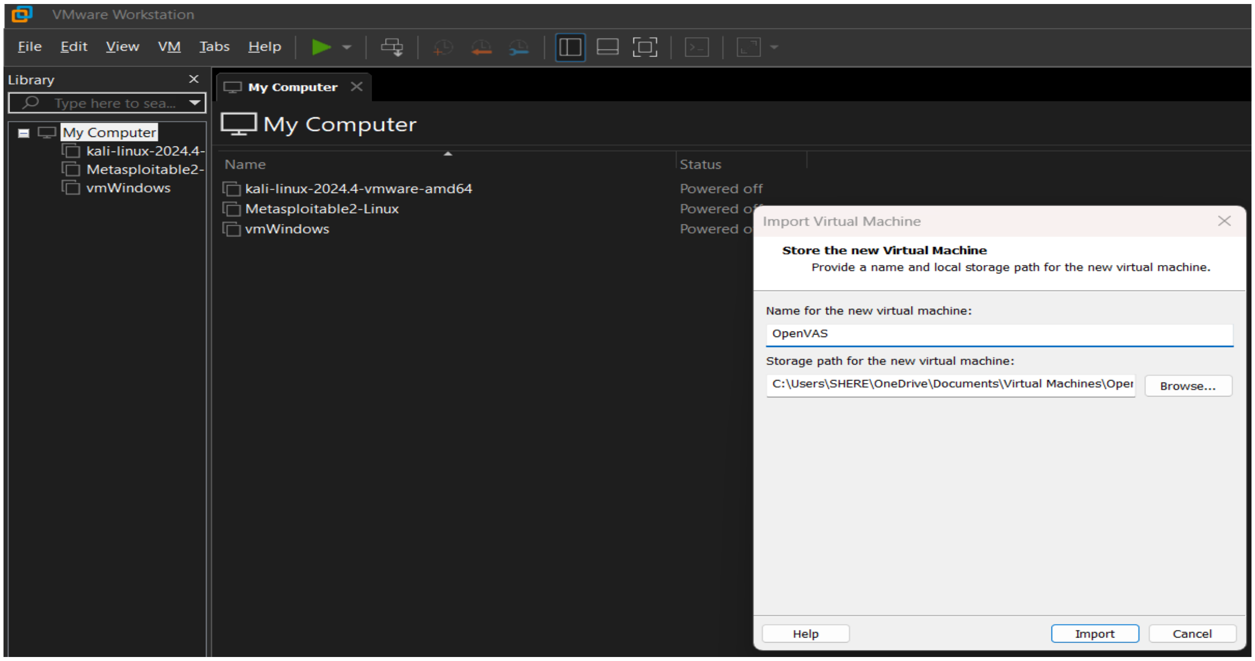
OpenVAS installation steps:

Download from: https://www.greenbone.net/en/greenbone-free/

- Open vmware and click on “Open Virtual Machine”.
- Select the Downloaded file.


Downloads
Sort
View
Last month
metasploitable-linux-2.0.0
MSEdge.Win10.VMware
7z2409-x64.exe
jdk-8u202-windows-x64.exe
nmap-7.95-setup.exe
VMware-workstation-17.6.2-24409262.exe
jaxws-ri-2.3.1.zip
GSM-TRIAL-20.08.7-VMware-Workstation.o...
Earlier this year

- Give the name “OpenVAS”

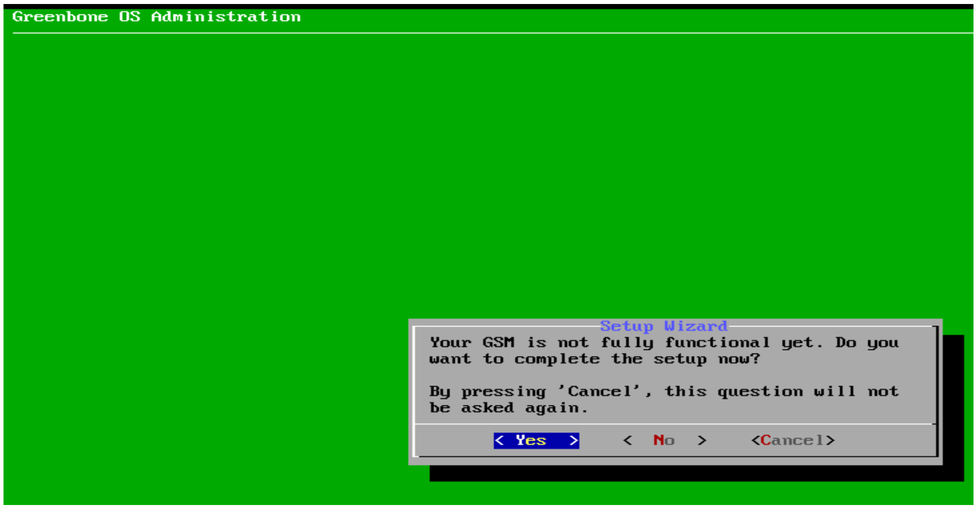


Store the new Virtual Machine
Provide a name and local storage path for the new virtual machine.

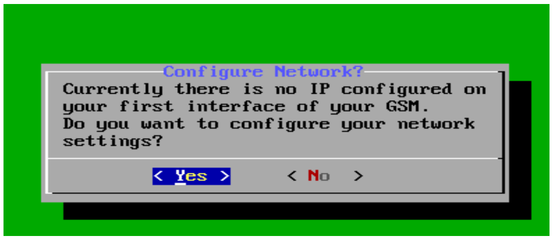
Name for the new virtual machine: OpenVAS

Storage path for the new virtual machine: C:\Users\SHERE\OneDrive\Documents\Virtual Machines\Oper

- Power on the machine and wait for some time.
- It will ask about the username and password for the Machine
- By default there is username “admin” and password is also “admin”.
- After entering the Login Credentials the OpenVAS Administrator Interface will be Visible on Screen.
- Press ok and then go to further step as following.

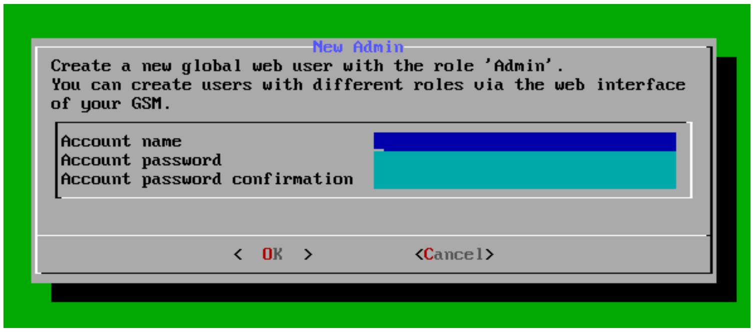


```
Greenbone OS Administration

Setup Wizard
Your GSM is not fully functional yet. Do you
want to complete the setup now?

By pressing 'Cancel', this question will not
be asked again.
```

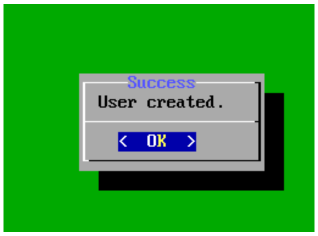


```
Configure Network?
Currently there is no IP configured on
your first interface of your GSM.
Do you want to configure your network
settings?
```

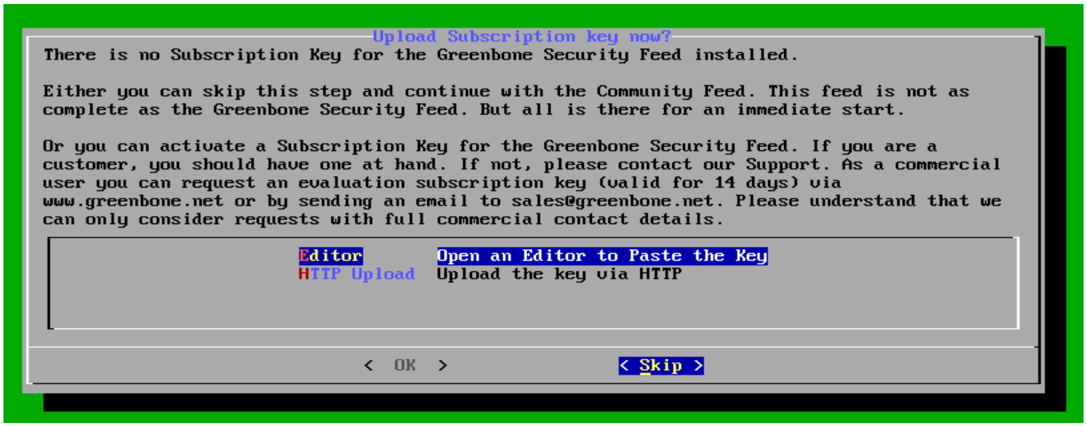
- Now we have to Create admin so enter the Account name and password.



```
New Admin
Create a new global web user with the role 'Admin'.
You can create users with different roles via the web interface
of your GSM.

Account name
Account password
Account password confirmation
```

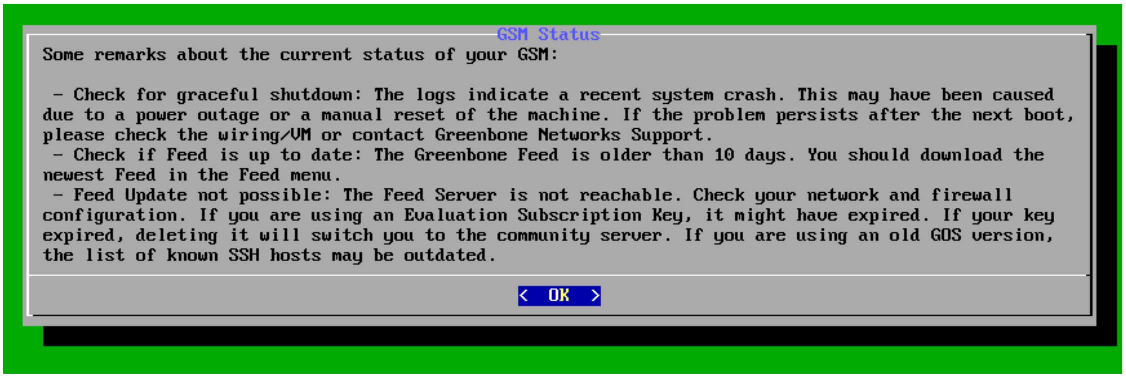


```
Success
User created.
```



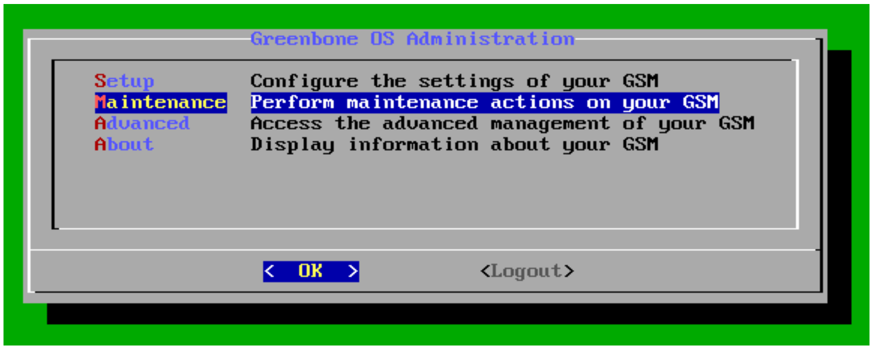
```
Upload Subscription key now?
There is no Subscription Key for the Greenbone Security Feed installed.

Either you can skip this step and continue with the Community Feed. This feed is not as
complete as the Greenbone Security Feed. But all is there for an immediate start.

Or you can activate a Subscription Key for the Greenbone Security Feed. If you are a
customer, you should have one at hand. If not, please contact our Support. As a commercial
user you can request an evaluation subscription key (valid for 14 days) via
www.greenbone.net or by sending an email to sales@greenbone.net. Please understand that we
can only consider requests with full commercial contact details.

          Editor        Open an Editor to Paste the Key
          HTTP Upload   Upload the key via HTTP
```

- After Completing the Steps one by on follow same as the following.

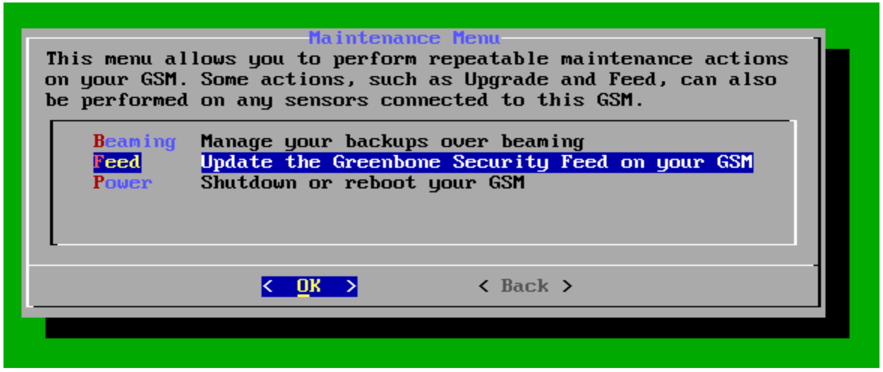


```
GSM Status
Some remarks about the current status of your GSM:

 - Check for graceful shutdown: The logs indicate a recent system crash. This may have been caused
due to a power outage or a manual reset of the machine. If the problem persists after the next boot,
please check the wiring/VM or contact Greenbone Networks Support.
 - Check if Feed is up to date: The Greenbone Feed is older than 10 days. You should download the
newest Feed in the Feed menu.
 - Feed Update not possible: The Feed Server is not reachable. Check your network and firewall
configuration. If you are using an Evaluation Subscription Key, it might have expired. If your key
expired, deleting it will switch you to the community server. If you are using an old GOS version,
the list of known SSH hosts may be outdated.

                                        < OK >
```

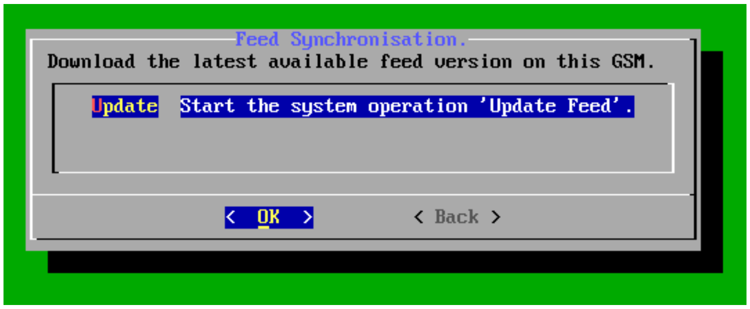
- Select the Maintenance option and update the GSM.



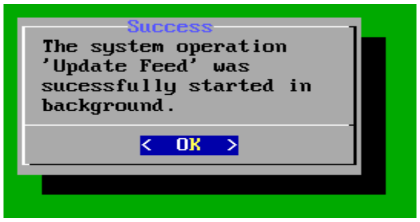
```
Greenbone OS Administration

  Setup          Configure the settings of your GSM
  Maintenance    Perform maintenance actions on your GSM
  Advanced       Access the advanced management of your GSM
  About          Display information about your GSM

              < OK >              <Logout>
```



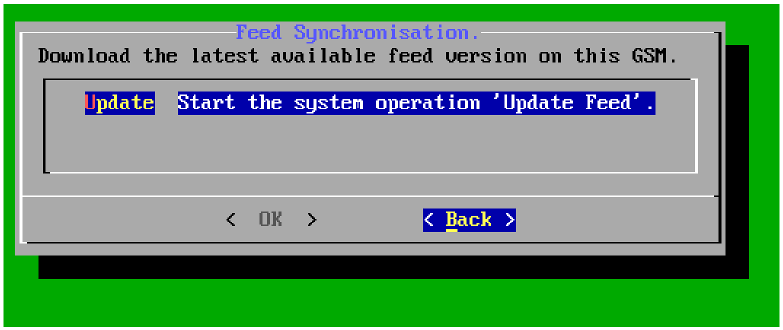
```
Maintenance Menu
This menu allows you to perform repeatable maintenance actions
on your GSM. Some actions, such as Upgrade and Feed, can also
be performed on any sensors connected to this GSM.

  Beaming    Manage your backups over beaming
  Feed       Update the Greenbone Security Feed on your GSM
  Power      Shutdown or reboot your GSM

              < OK >              < Back >
```



```
Feed Synchronisation
Download the latest available feed version on this GSM.

  Update  Start the system operation 'Update Feed'.

            < OK >            < Back >
```

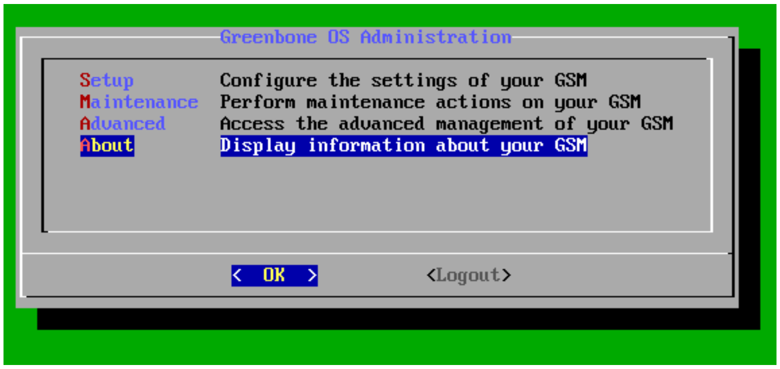


```
Success
The system operation
'Update Feed' was
sucessfully started in
background.

        < OK >
```



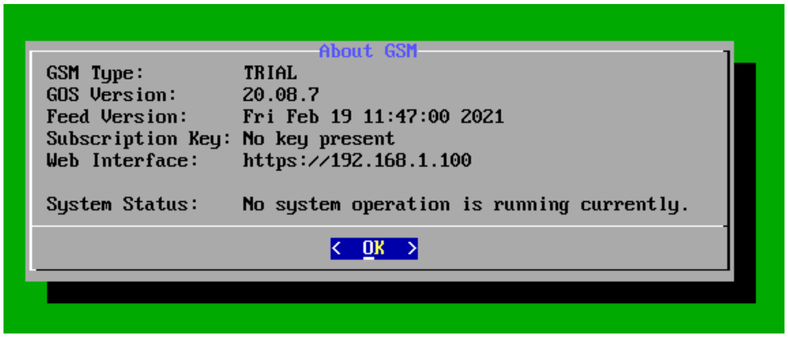
```
Feed Synchronisation
Download the latest available feed version on this GSM.

    Update   Start the system operation 'Update Feed'.

                < OK >          < Back >
```

- Then go back and Select the About Option which will Display the Information about the GSM of you Device.



```
Greenbone OS Administration

   Setup         Configure the settings of your GSM
   Maintenance   Perform maintenance actions on your GSM
   Advanced      Access the advanced management of your GSM
   About         Display information about your GSM

              < OK >          <Logout>
```

- It will also Display the Web Interface IP. Using that you can access the Web Interface of GSM. And if it shows that ip no Configured then you have to manually provide the IP range in the Setup option of the GSM.



```
About GSM
GSM Type:          TRIAL
GOS Version:       20.08.7
Feed Version:      Fri Feb 19 11:47:00 2021
Subscription Key:  No key present
Web Interface:     https://192.168.1.100

System Status:     No system operation is running currently.

                      < OK >
```

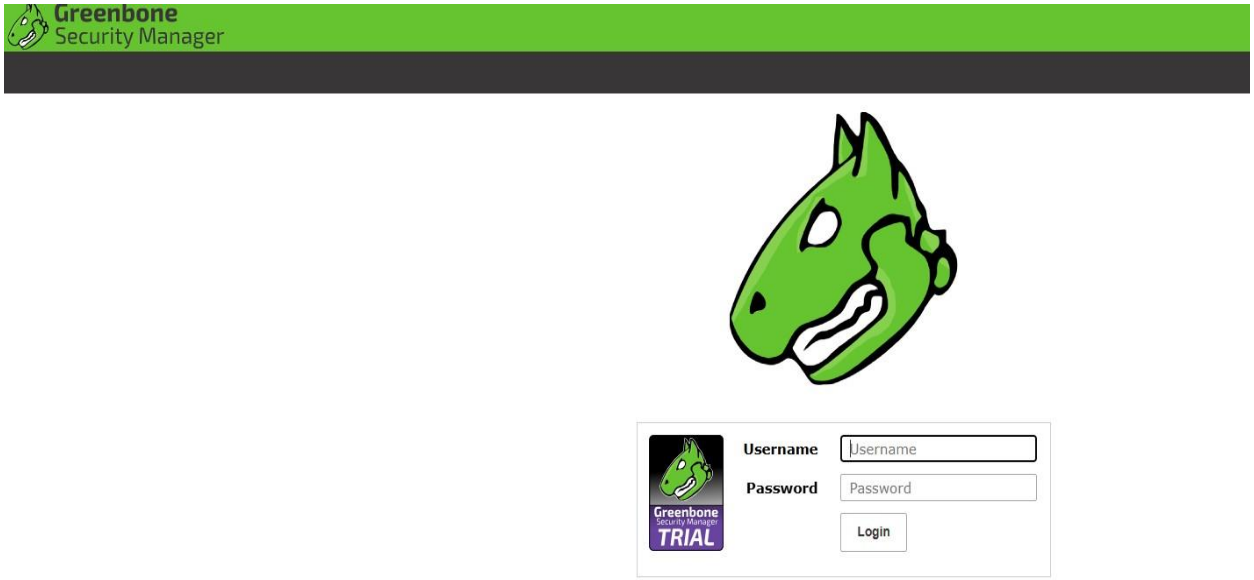
- Keep this process running and parallel, open the browser in kali or windows and open http://192.168.1.100 (Enter the user and password which you created during installation)

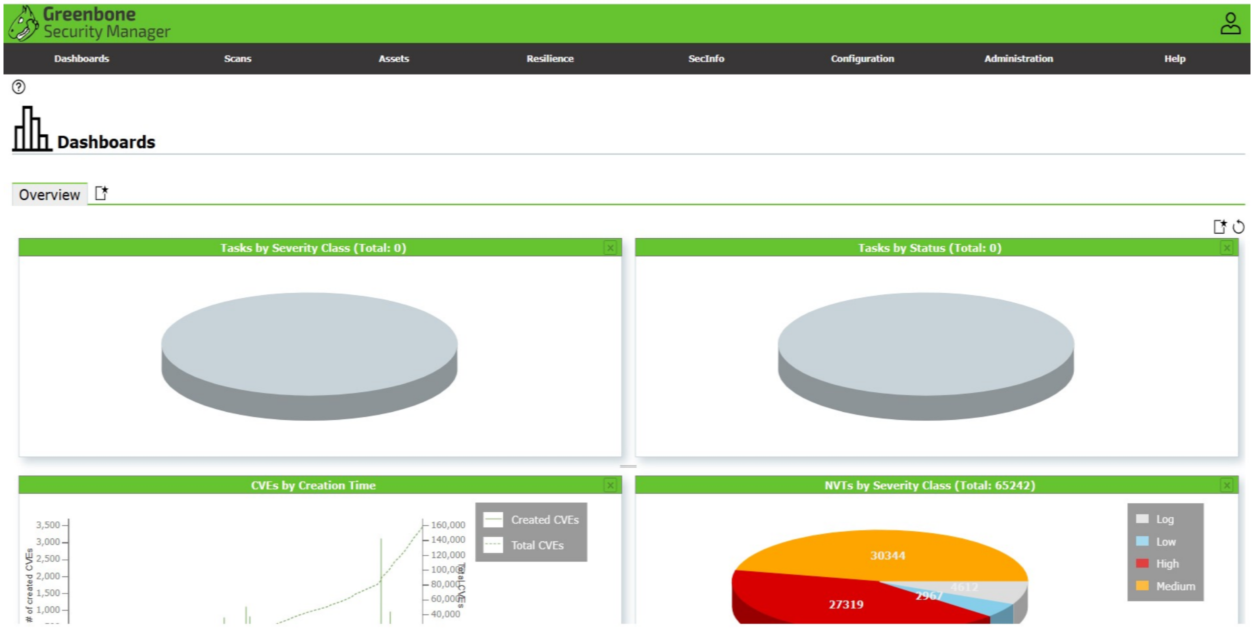
Perform the vulnerability assessment Scenario:

Attacker machine: Kali machine/Windows,

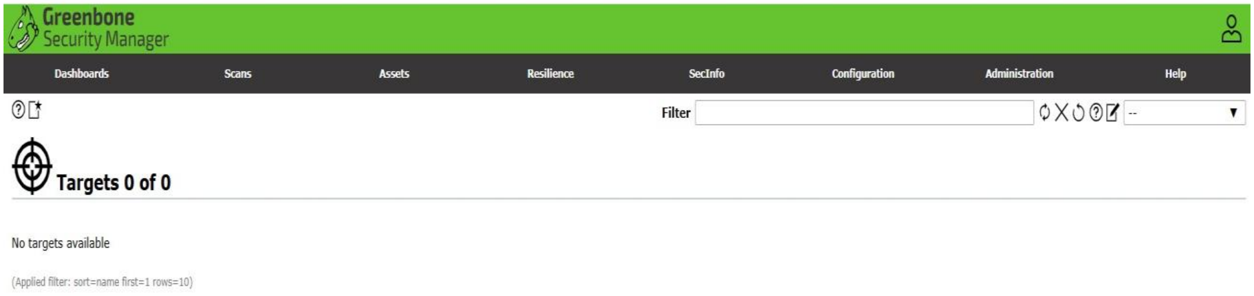
Target machine: Localhost/Windows10 / metasploitable2:

- NOTE: Check the IP address of all the machines and check the connectivity from the kali machine to the target machine using the ping command. Open the browser in the kali Windows and write the URL: https://192.168.1.100 (Note: Openvas Machine must be in running mode) and login. After Successfully login in the web interface of OpenVAS as below:





Step-1: Now go to “configuration” and click on the “target” Step-2: Click on “New target” See below:

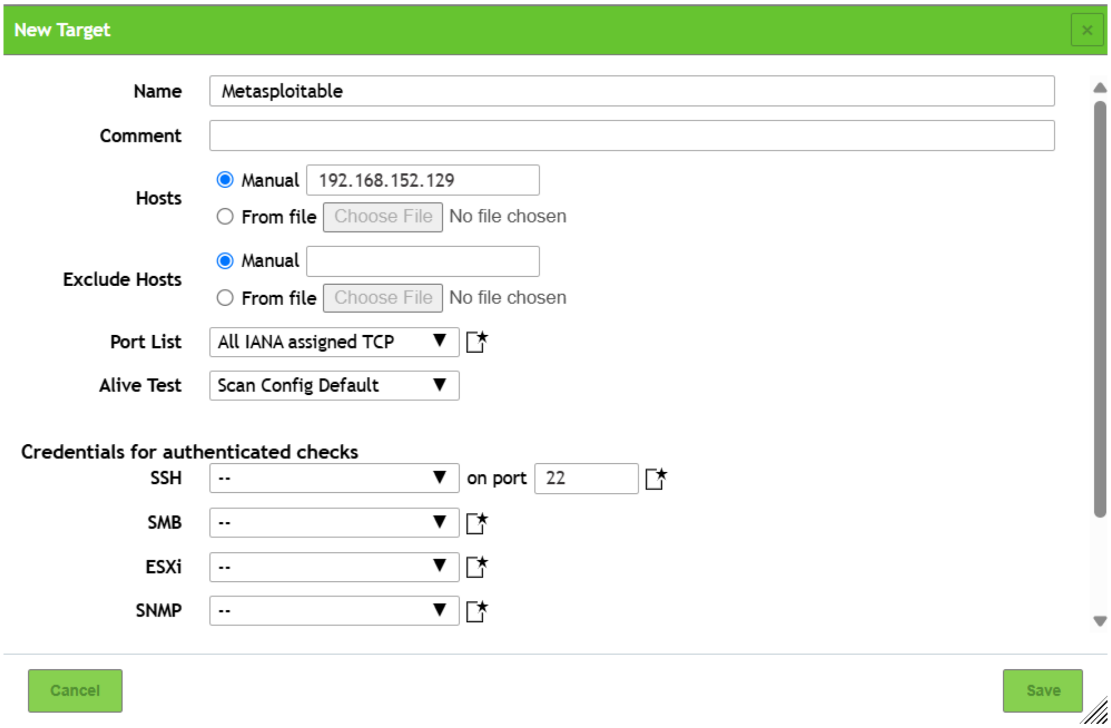


Targets 0 of 0

No targets available

(Applied filter: sort=name first=1 rows=10)

Step-3: Write the Name of scanning and in the Hosts-> Manual …..write IP address of target machine and click on the save.



New Target

Name: Metasploitable

Comment:

Hosts: ● Manual 192.168.152.129 ○ From file No file chosen

Exclude Hosts: ● Manual ○ From file No file chosen

Port List: All IANA assigned TCP

Alive Test: Scan Config Default

Credentials for authenticated checks

SSH: -- on port 22

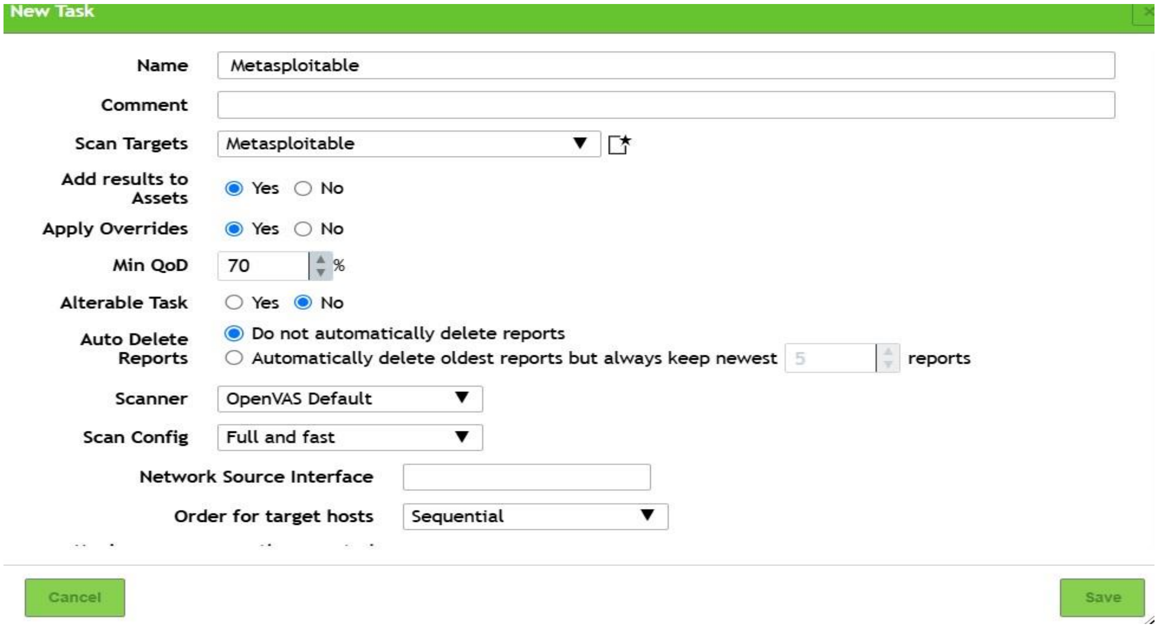
SMB: --

ESXi: --

SNMP: --

Step-4: After that go to the Scan->Tasks and add a new task from the left corner….

Provide the Name and select the scan target which we have already created in the previous step. and click on the save.



New Task

Name: Metasploitable

Comment:

Scan Targets: Metasploitable

Add results to Assets: ● Yes ○ No

Apply Overrides: ● Yes ○ No

Min QoD: 70 %

Alterable Task: ○ Yes ● No

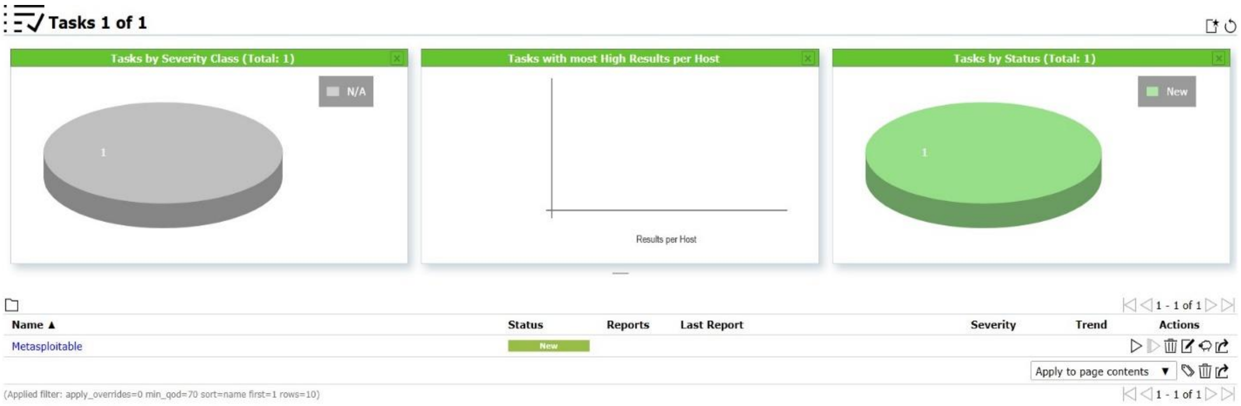
Auto Delete Reports: ● Do not automatically delete reports ○ Automatically delete oldest reports but always keep newest 5 reports

Scanner: OpenVAS Default

Scan Config: Full and fast

Network Source Interface:

Order for target hosts: Sequential

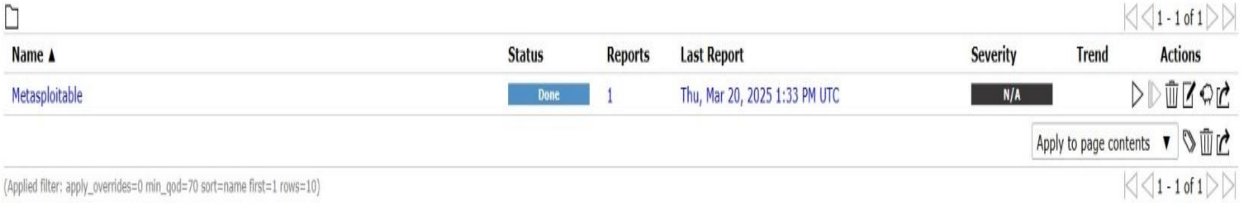

Tasks 1 of 1
Tasks by Severity Class (Total: 1)
N/A
1
Tasks with most High Results per Host
Results per Host
Tasks by Status (Total: 1)
New
1
1 - 1 of 1

Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Metasploitable	New					

Apply to page contents ▼

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

Click on the play button from the right side of the added scan to start the vulnerability scanning. Scanning started as shown below:

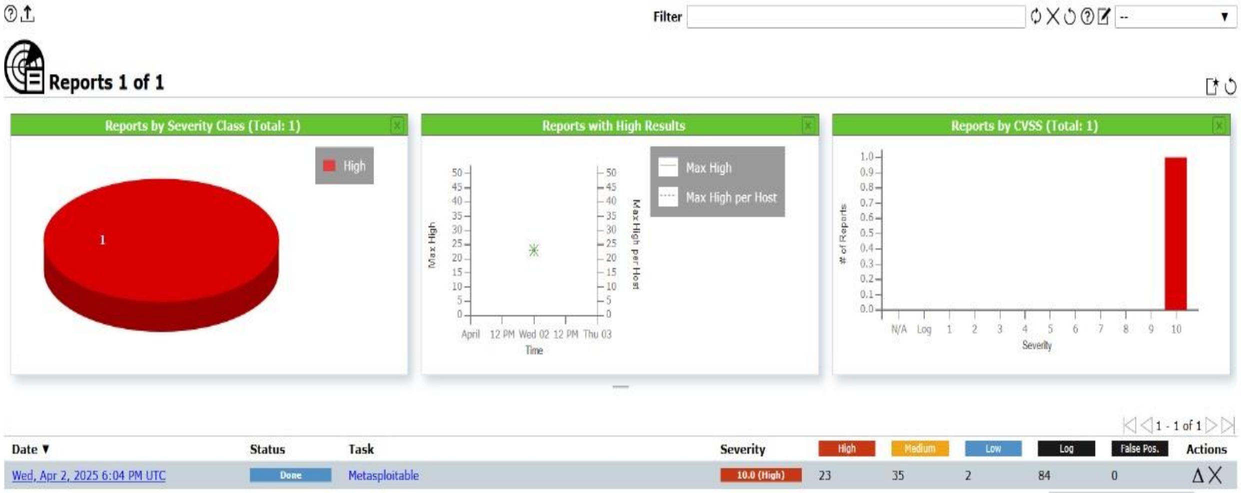


Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Metasploitable	Done	1	Thu, Mar 20, 2025 1:33 PM UTC	N/A		

Apply to page contents ▼

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

After Scanning is completed then go to the report option where you can see the report about the scan.



Date ▼	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Wed, Apr 2, 2025 6:04 PM UTC	Done	Metasploitable	10.0 (High)	23	35	2	84	0	ΔX