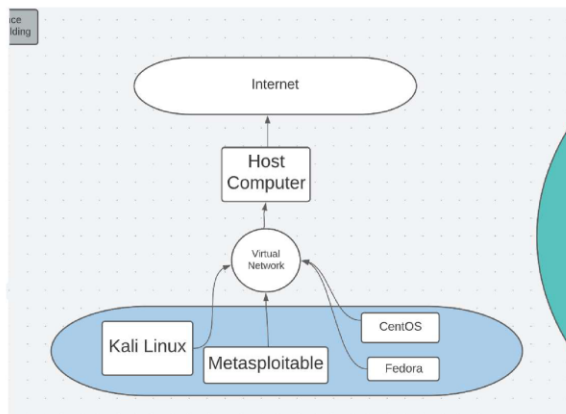
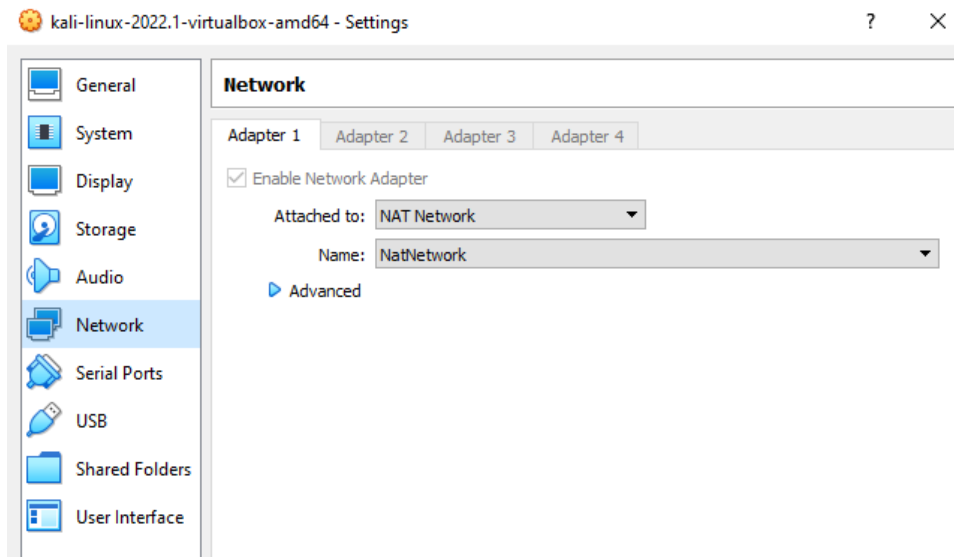


## 1. Set-up NAT Network within planned VMs. Connect VMs to NAT network



### Metasploitable

Step 1:

Use ifconfig command in Metasploitable to identify IP address for metasploitable

## 2. Download and configure OpenVAS on Kali Linux

Use command : `sudo apt-get update`  
`sudo apt-get dist-upgrade`

3. Start target OS and run command `ifconfig` to get the ip address.

4. ping target ip within kali to make sure they are connected on NAT Network.

```
(kali㉿kali)-[~]
$ ping 192.168.139.132
PING 192.168.139.132 (192.168.139.132) 56(84) bytes of data:
64 bytes from 192.168.139.132: icmp_seq=1 ttl=64 time=15.5 ms
64 bytes from 192.168.139.132: icmp_seq=2 ttl=64 time=2.03 ms
64 bytes from 192.168.139.132: icmp_seq=3 ttl=64 time=1.79 ms
64 bytes from 192.168.139.132: icmp_seq=4 ttl=64 time=1.47 ms
64 bytes from 192.168.139.132: icmp_seq=5 ttl=64 time=1.32 ms
64 bytes from 192.168.139.132: icmp_seq=6 ttl=64 time=1.80 ms
```

5. Get password from initial configuration and start OpenVAS. Start OpenVAS with `sudo gvm-start`.

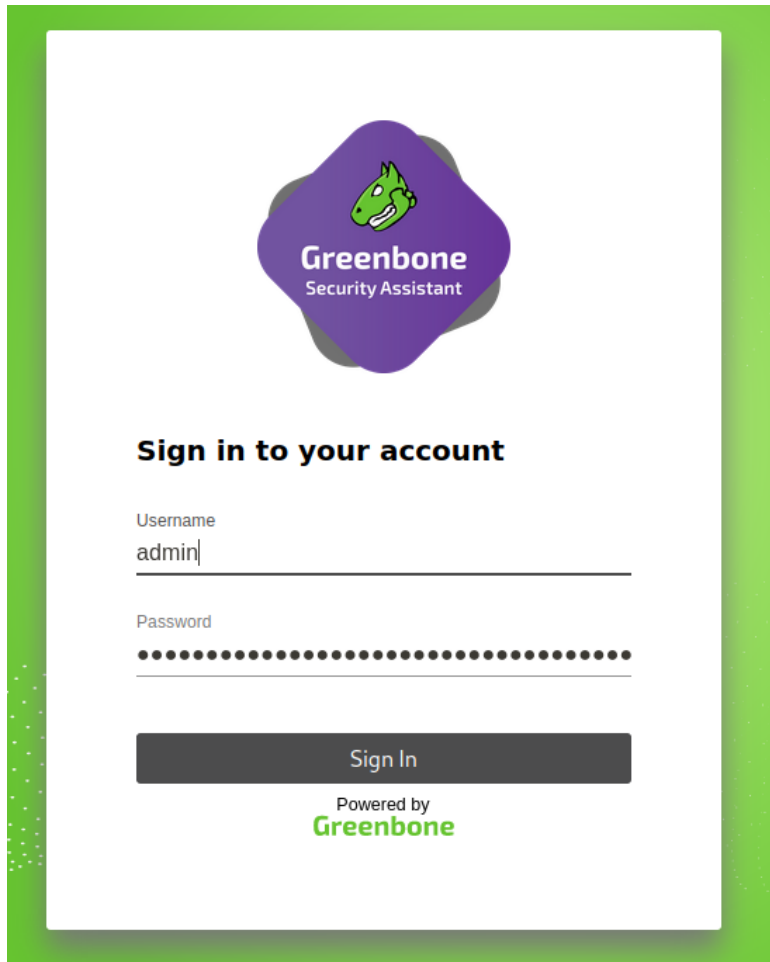
```
(kali㉿kali)-[~]
$ sudo gvm-start
[*] Please wait for the GVM / OpenVAS services to start.
[*] You might need to refresh your browser once it opens.
[*] Web UI (Greenbone Security Assistant): https://127.0.0.1:9392

• greenbone-security-assistant.service - Greenbone Security Assistant (gsad)
  Loaded: loaded (/lib/systemd/system/greenbone-security-assistant.service; disabled; vendor preset: disabled)
  Active: active (running) since Fri 2021-02-12 12:24:11 UTC; 43ms ago
  Docs: man:gsad(8)
         https://www.greenbone.net
  Process: 33117 ExecStart=/usr/sbin/gsad --listen=127.0.0.1 --port=9392 (code=exited, status=0/SUCCESS)
  Main PID: 33118 (gsad)
  Tasks: 1 (limit: 4546)
  Memory: 1.7M
  CGroup: /system.slice/greenbone-security-assistant.service
          └─33118 /usr/sbin/gsad --listen=127.0.0.1 --port=9392

Feb 12 12:24:11 kali systemd[1]: Starting Greenbone Security Assistant (gsad)...
Feb 12 12:24:11 kali gsad[33117]: Oops, secure memory pool already initialized
Feb 12 12:24:11 kali systemd[1]: Started Greenbone Security Assistant (gsad).

• gvm.service - Greenbone Vulnerability Manager daemon (gvmd)
  Loaded: loaded (/lib/systemd/system/gvmd.service; disabled; vendor preset: disabled)
  Active: active (running) since Fri 2021-02-12 12:24:06 UTC; 5s ago
  Docs: man:gvmd(8)
  Process: 33071 ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd.sock (code=exited, status=0/SUCCESS)
  Main PID: 33073 (gvmd)
  Tasks: 2 (limit: 4546)
  Memory: 3.1M
  CGroup: /system.slice/gvmd.service
```

6. Login with admin and the provided password.



7. Select new task and enter the target OS details

New Task

Name

Comment

Scan Targets  ▼ ☐ \*

Alerts  ▼ ☐ \*

Schedule  ▼ ☐ Once ☐ \*

Add results to Assets ☒ Yes ☐ No

Apply Overrides ☒ Yes ☐ No

Min QoD  %

Alterable Task ☐ Yes ☒ No

Auto Delete Reports ☒ Do not automatically delete reports  
☐ Automatically delete oldest reports but always keep newest  reports

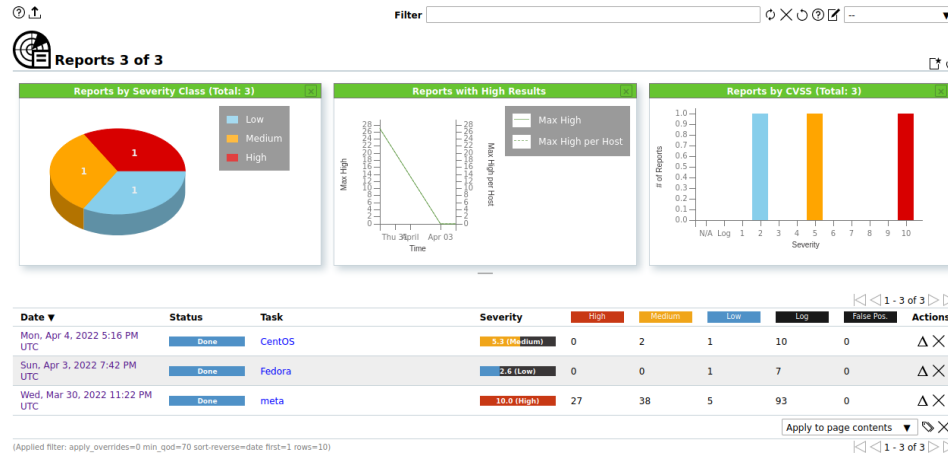
Scanner  ▼

Scan Config  ▼

8. save task then click the arrow to run a scan.



9. Go to reports and select the specific report to get details on the scan.



**Report: Mon, Apr 4, 2022 5:16 PM UTC** Done ID: 540ff68b-0a83-4a14-9657-r86303a6de12 Created: Mon, Apr 4, 2022 5:17 PM UTC Modified: Mon, Apr 4, 2022 5:27 PM UTC Owner: admin

Information	Results (3 of 22)	Hosts (1 of 1)	Ports (1 of 1)	Applications (1 of 1)	Operating Systems (1 of 1)	CVEs (0 of 0)	Closed CVEs (0 of 0)	TLS Certificates (0 of 0)	Error Messages (0 of 0)	User Tags (0)
-------------	-------------------	----------------	----------------	-----------------------	----------------------------	---------------	----------------------	---------------------------	-------------------------	---------------

Task Name: CentOS  
Scan Time: Mon, Apr 4, 2022 5:17 PM UTC - Mon, Apr 4, 2022 5:27 PM UTC  
Scan Duration: 0:09 h  
Scan Status: Done  
Hosts scanned: 1  
Filter: apply\_overrides=0 levels=hml min\_qod=70  
Timezone: Coordinated Universal Time (UTC)

10. Download report for the OS scan and upload onto Github

11. repeat steps 3-4 and 7-10 for each target OS