

1.Vulnerability Scanning

Use the open-source tool called Openvas to scan and identify the vulnerabilities and also you can use nikto for web application scanning.

Before setting up the openvas tool you have to start the services in your kali Linux

```
sudo systemctl start osap-openvas
```

```
suso systemctl start gvm
```

```
sudo systemctl start gsad
```

```
sudo systemctl start redis-server
```

After starting those server, you must verify that there are running are not,

```
sudo systemctl status osap-openvas
```

```
suso systemctl status gvm
```

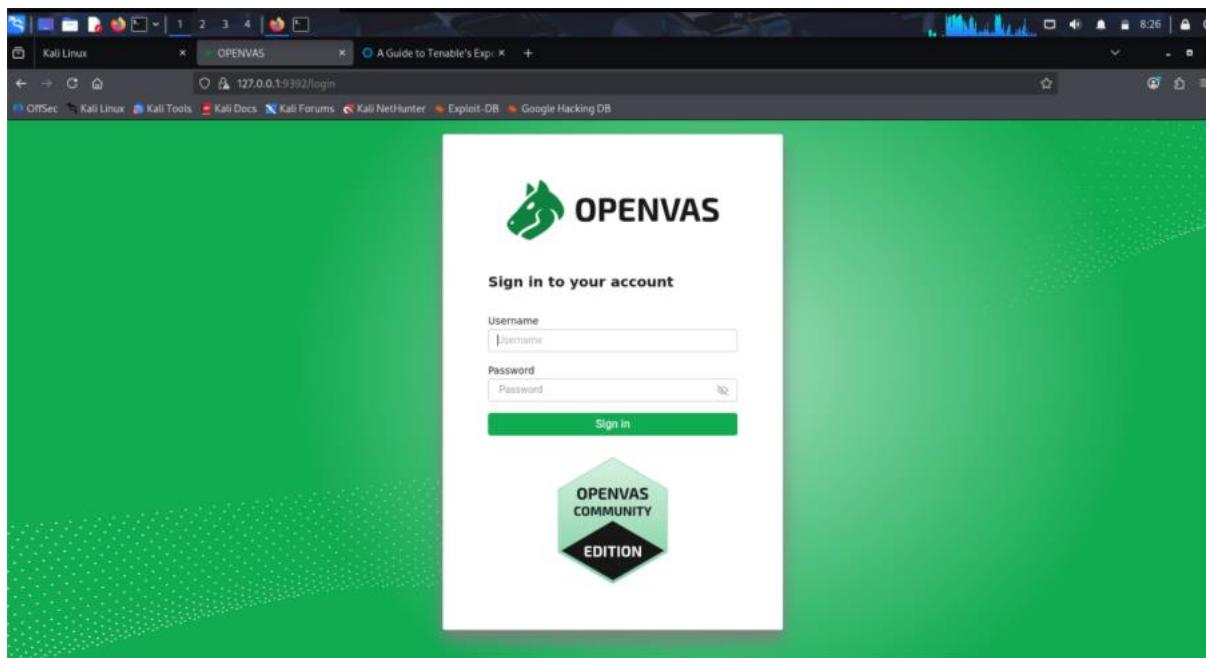
```
sudo systemctl status gsad
```

```
sudo systemctl status redis-server
```



```
[root@kali ~]# sudo gvm-start
Please wait for the GVM services to start.
You might need to refresh your browser once it opens.
Web UI (Greenbone Security Assistant): https://127.0.0.1:9392
● gsd-service - Greenbone Security Assistant daemon (gsad)
  Loaded: loaded (/usr/lib/systemd/system/gsd.service; disabled; preset: disabled)
  Active: active (running) since Fri 2020-01-02 09:44:01 EST; 23ms ago
  Invocation-Id: 70242c39daea5b622115292
  Docs: man:gsad(8)
  Main PID: 4553 (gsad)
  Memory: 2.0M (peak: 2.0M)
  CPU: 0.2ms
  CGroup: /system.slice/gsd.service
          └─ 4553 /usr/sbin/gsd --foreground --listen 127.0.0.1 --port 9392
              ├─ 4558 /usr/sbin/gsd --foreground --listen 127.0.0.1 --port 9392
Jan 02 09:44:01 kali systemd[1]: Starting gsd.service - Greenbone Security Assistant daemon (gsad)...
Jan 02 09:44:01 kali systemd[1]: Started gsd.service - Greenbone Security Assistant daemon (gsad).
Jan 02 09:44:01 kali gsd[4553]: gsd main:MESSAGE[0x20-01-02 14h44.81 utc:4553]: Starting GSAD version 24.12.0-git
● gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)
  Loaded: loaded (/usr/lib/systemd/system/gvmd.service; enabled; preset: disabled)
  Active: active (running) since Fri 2020-01-02 09:43:56 EST; 5s ago
  Invocation-Id: d77bd0962e4040fcfb0bdcdd495f1a
  Docs: man:gvmd(8)
  Main PID: 4467 (gvmd)
  Tasks: 2 (limit: 2187)
  Memory: 2.0M (peak: 7.0M)
  CPU: 152ms
  CGroup: /system.slice/gvmd.service
          └─ 4467 /usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd-openvas.sock --listen-group=_gvm (code=exited, status=0/SUCCESS)
Jan 02 09:43:55 kali systemd[1]: Starting gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)...
Jan 02 09:43:55 kali systemd[1]: gvmd.service: Can't open PID file '/run/gvmd/gvmd.pid' (yet?) after start: No such file or directory
Jan 02 09:43:55 kali systemd[1]: Started gvmd.service - Greenbone Vulnerability Manager daemon (gvmd).
● ospd-openvas.service - OSPD Wrapper for the OpenVAS Scanner (ospd-openvas)
  Loaded: loaded (/usr/lib/systemd/system/ospd-openvas.service; enabled; preset: disabled)
  Active: active (running) since Fri 2020-01-02 09:43:55 EST; 5s ago
  Invocation-Id: 3b20491ca6647db9f9b65a9b1b4c5eb
  Docs: man:ospd-openvas(8)
  Main PID: 4445 (ospd)
  Process: 4445 ExecStart=/usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-config /etc/gvm/ospd-logging.conf (code=exited, status=0/SUCCESS)
  Main PID: 4453 (ospd-openvas)
```

After starting it will be directly open in the browser and it will be look as

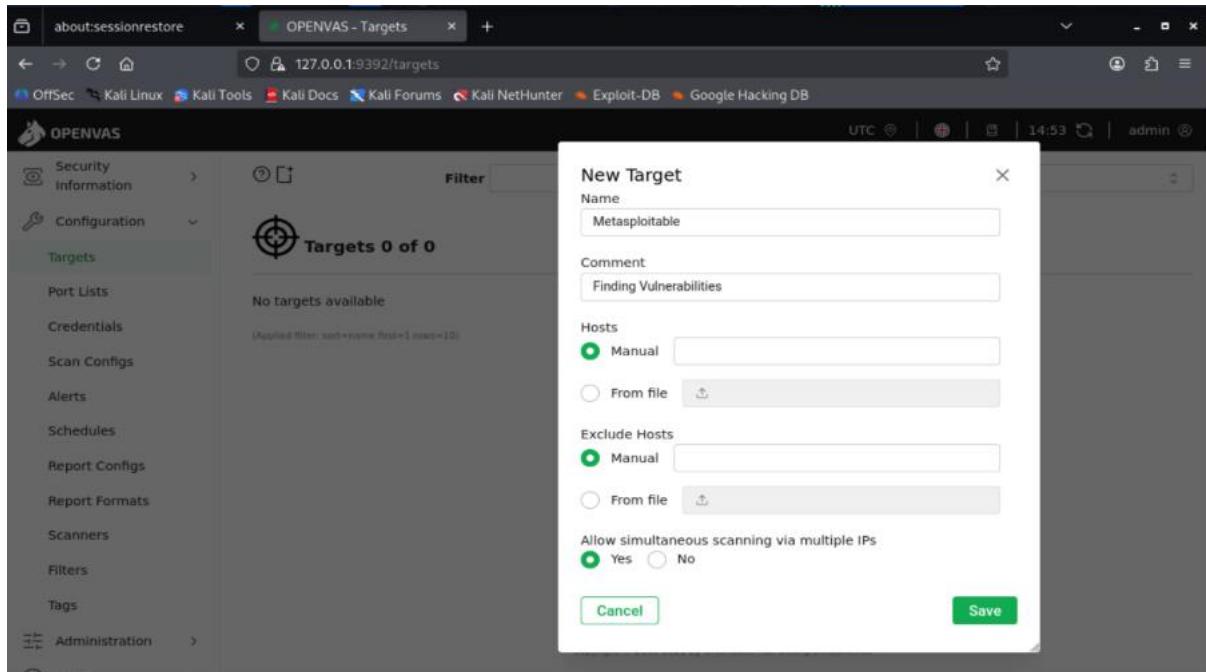


You can setup the login credentials by using the commands as

```
sudo runuser -u _gvm -- gvmd --user=admin --new-password=1234
```

After login into the openvas you have to create the target to scan the machine which was setup before called metasploitable 3

Go to configurations -> Target -> New target and provide the details of the machine like Ip address and any particular ports.



I have created the two targets under the configuration in which that will be scan the machines through the IP address you provided.

The screenshot shows the 'Targets' section of the OpenVAS web interface. At the top, there is a header with a search bar labeled 'Filter' and various navigation icons. Below the header, a title 'Targets 3 of 3' is displayed next to a target icon. A table lists three targets:

Name	Hosts	IPs	Credentials	Actions
kali	192.168.1.10	1	All IANA assigned TCP	
Meta 3 (Scanning machine)	192.168.10.16	1	All IANA assigned TCP	
Metasploitable (Scanning Machine)	192.168.10.16	1	All IANA assigned TCP	

At the bottom of the table, there is a note '(Applied filter: sort=name first=1 rows=10)' and a page navigation bar with links for '1 - 3 of 3'.

After setting up the target navigate to Scans -> tasks -> new task and create the new task, in scan targets select the target before you created. I have created a task and that will be added in the img below.

The screenshot shows the 'Tasks' section of the OpenVAS web interface. On the left, a sidebar menu includes 'Dashboards', 'Scans', 'Tasks' (which is selected and highlighted in green), 'Reports', 'Results', 'Vulnerabilities', 'Notes', 'Overrides', 'Assets', 'Resilience', 'Security Information', 'Configuration', 'Administration', and 'Help'. The main content area has a header 'Tasks 1 of 1' with a search bar and navigation icons. Below the header, there are three donut charts and a table:

- Tasks by Severity Class (Total: 1)**: Shows 1 N/A.
- Tasks with most High Results per Host**: Shows 1 host with 1 result.
- Tasks by Status (Total: 1)**: Shows 1 New task.

Name	Status	Reports	Last Report	Severity	Trend	Actions
Meta Scan (Scanning Machine)	New					

At the bottom of the table, there is a note 'Apply to page contents' and a page navigation bar with links for '1 - 1 of 1'.

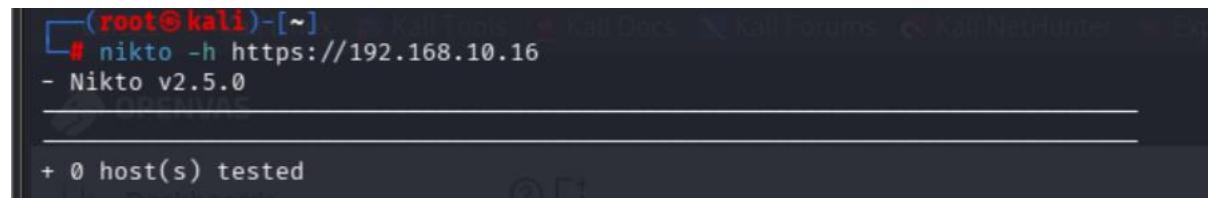
1.1 Using Nikto

First, i have installed the nikto in my kali Linux by using the command as

```
sudo apt install nikto
```

I have scanned the metasploitable 3 using the nikto in my kali Linux but i didn't get the results from that because the firewalls are fully protected to that machine.

```
nikto -h https://192.168.101.6
```

A screenshot of a terminal window titled '(root@kali)-[~]'. It shows the command '# nikto -h https://192.168.10.16' being run. The output indicates 'Nikto v2.5.0' and '+ 0 host(s) tested'. The background of the terminal window has a watermark for 'Kali Linux'.

I have scanned the Metasploitable 3 using the OpenVAS but i didn't get any results and i have tried a lot but i didn't get any results.

I got a lot of errors for the services which are in the kali Linux while setting up the OpenVAS. I tried a lot and i get the web UI working but the results didn't get.