

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
```

```
sudo systemctl start gvmd
```

```
sudo systemctl start gsad
```

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

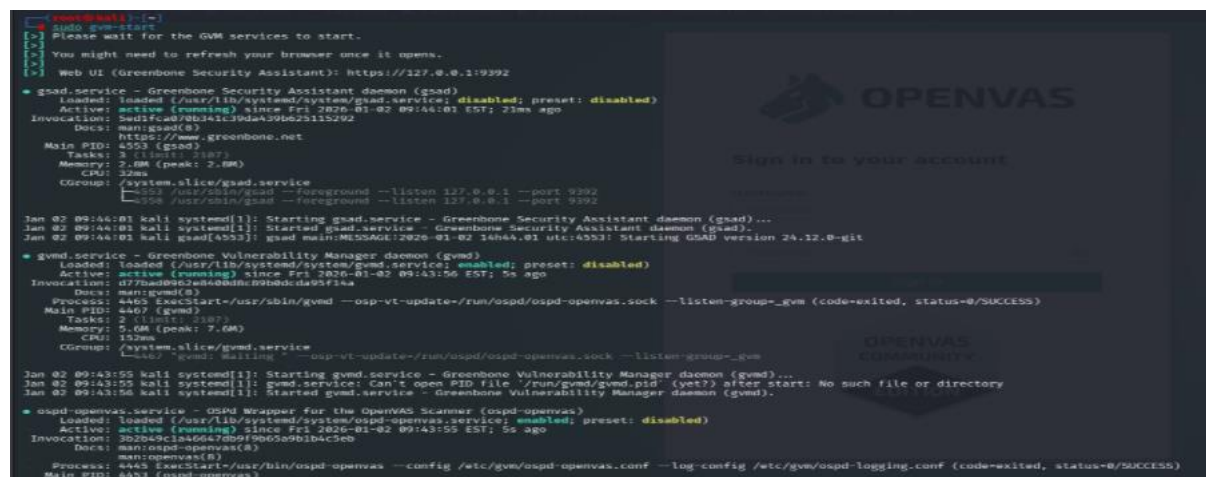
After starting those server, you must verify that there are running are not,

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

```
sudo systemctl status gvmd
```

```
sudo systemctl status gsad
```

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



```
[root@kali:~]# systemctl status gsad
● gsad.service - Greenbone Security Assistant daemon (gsad)
   Loaded: loaded (/usr/lib/systemd/system/gsad.service; disabled; preset: disabled)
   Active: active (running) since Fri 2020-01-02 09:44:01 EST; 23ms ago
     Invocation: 5e1fca878b341c19da459b623115292
       Docs: man:gsad(8)
            https://www.greenbone.net
    Main PID: 4553 (gsad)
      Tasks: 2 (limit: 2187)
     Memory: 2.0M (peak: 2.0M)
        CPU: 32ms
     CGroup: /system.slice/gsad.service
             └─4553 /usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9362
             └─4554 /usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9392

Jan 02 09:44:01 kali systemd[1]: Starting gsad.service - Greenbone Security Assistant daemon (gsad)...
Jan 02 09:44:01 kali systemd[1]: Started gsad.service - Greenbone Security Assistant daemon (gsad).
Jan 02 09:44:02 kali gsad[4553]: gsad main:RELEASE/2020-01-02 14h44.01 utc:4553: Starting GSAD version 24.12.0-git

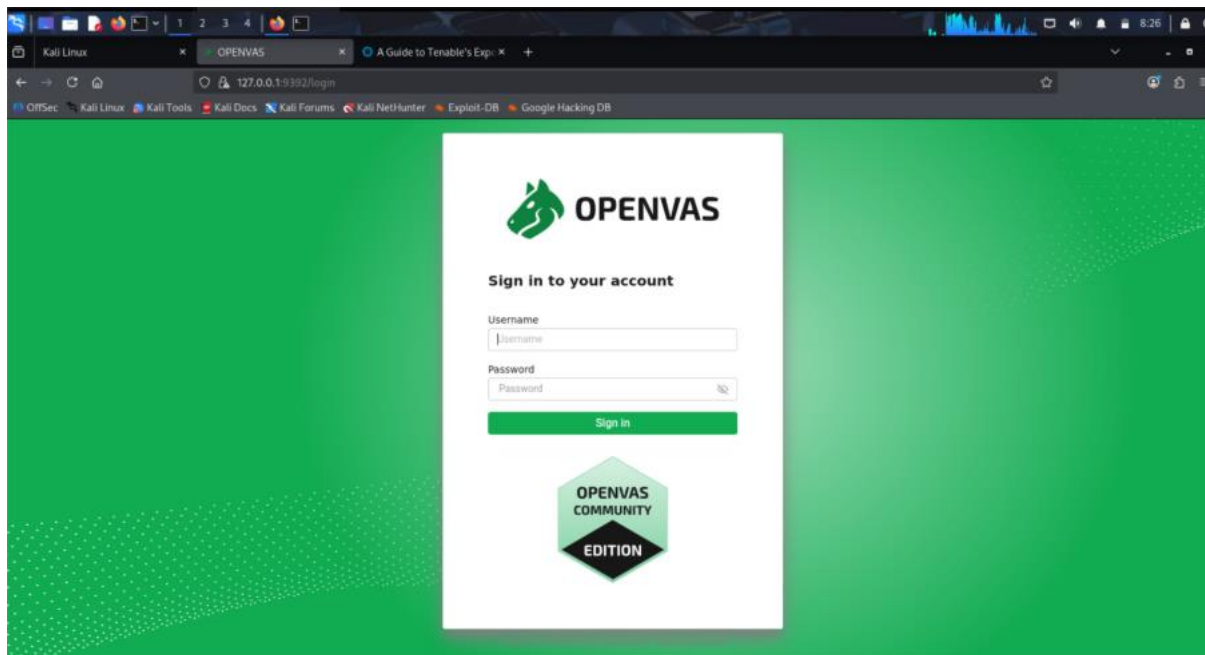
● gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)
   Loaded: loaded (/usr/lib/systemd/system/gvmd.service; enabled; preset: disabled)
   Active: active (running) since Fri 2020-01-02 09:43:56 EST; 5s ago
     Invocation: 477bade3c4a8ab0b0d8dd4d95714a
       Docs: man:gvmd(8)
    Process: 4445 ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd-openvas.sock --listen-group=_gvm (code=exited, status=0/SUCCESS)
    Main PID: 4467 (gvmd)
      Tasks: 2 (limit: 2187)
     Memory: 5.0M (peak: 7.6M)
        CPU: 152ms
     CGroup: /system.slice/gvmd.service
             └─4467 gvmd: Waiting " " --osp-vt-update=/run/ospd/ospd-openvas.sock --listen-group=_gvm

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 09:43:56 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: 3d2b49c1a46647db9f9b05a9b1b4c5eb
       Docs: man:ospd-openvas(8)
            man:openvas(8)
    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)
```

The right side of the image shows a web browser window displaying the OpenVAS login page. The page has a dark theme with the OpenVAS logo at the top. Below the logo, it says "Sign in to your account" and "or" followed by a link to "OpenVAS Community". There are input fields for "Username" and "Password", and a "Log in" button. At the bottom, there is a link to "Forgot your password?".

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

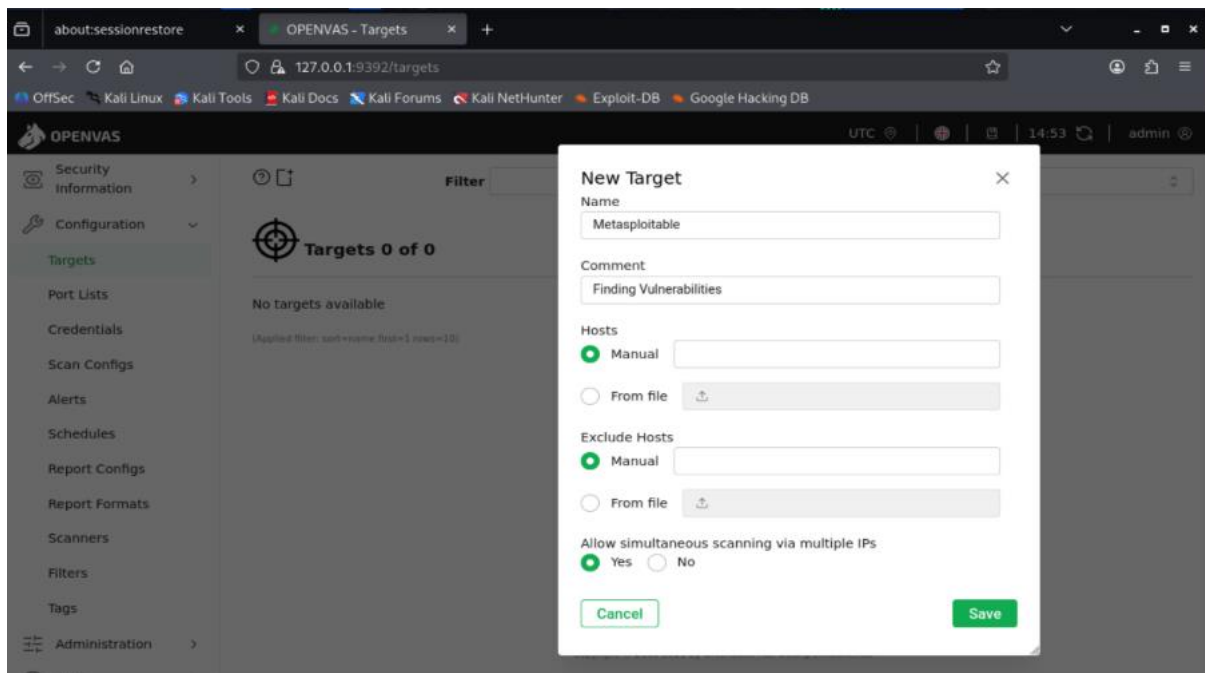


You can setup the login credentials by using the commands as

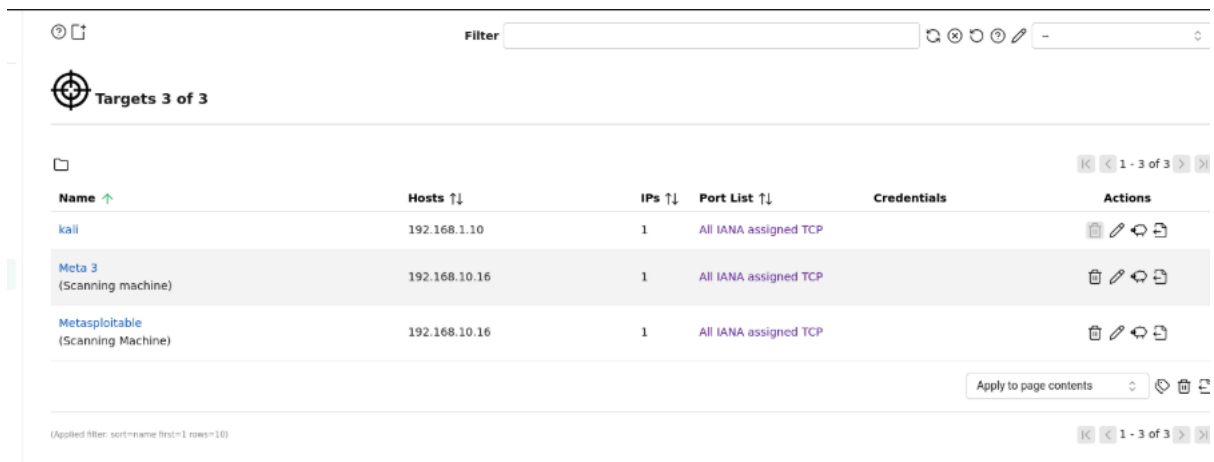
```
sudo runuser -u _gvm -- gvmcd --user=admin --new-password=1234
```

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.

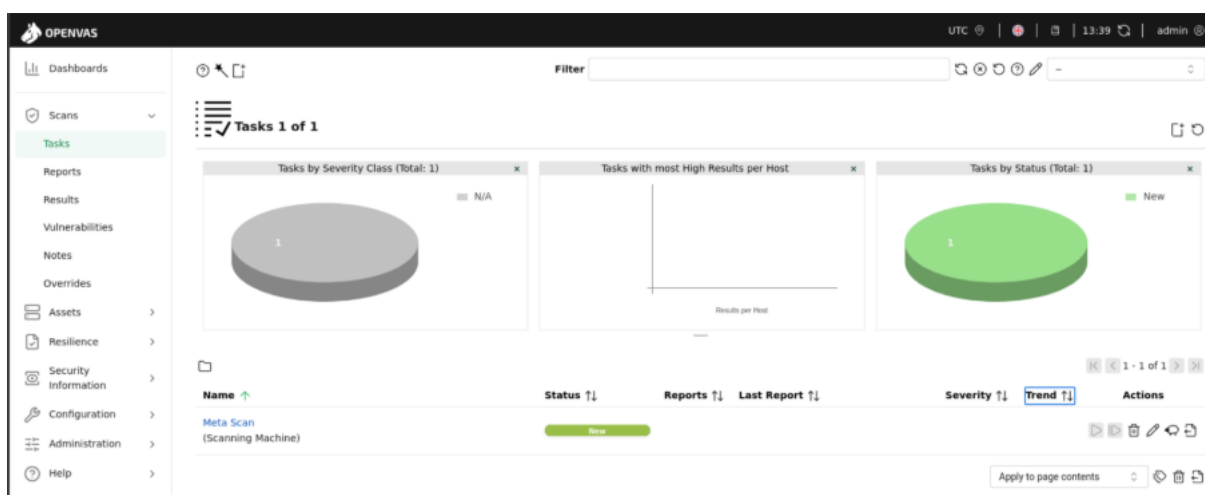


Name ↑	Hosts ↑↓	IPs ↑↓	Port List ↑↓	Credentials	Actions
kali	192.168.1.10	1	All IANA assigned TCP		
Meta 3 (Scanning machine)	192.168.10.16	1	All IANA assigned TCP		
Metasploitable (Scanning Machine)	192.168.10.16	1	All IANA assigned TCP		

Apply to page contents

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

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.



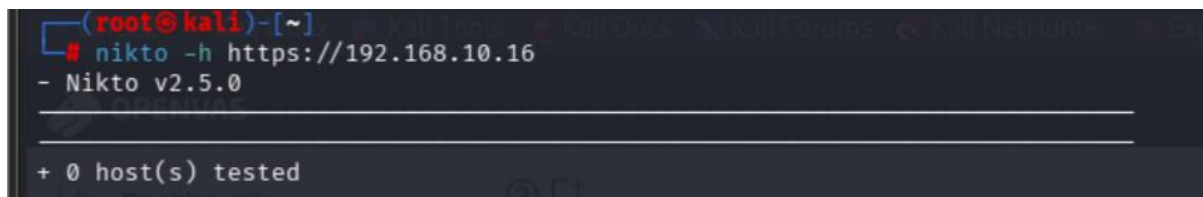
1.1 Using Nikto

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 terminal window screenshot from a Kali Linux machine. The prompt is (root@kali)-[~]. The command entered is # nikto -h https://192.168.10.16. The output shows - Nikto v2.5.0 followed by a horizontal line and + 0 host(s) tested.

```
(root@kali)-[~]  
# nikto -h https://192.168.10.16  
- Nikto v2.5.0  
+ 0 host(s) tested
```

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.