OpenVAS on Debian 10

Installation guide with pictures

By Sanil Almeida (CPTE | CEH)

TABLE OF CONTENTS

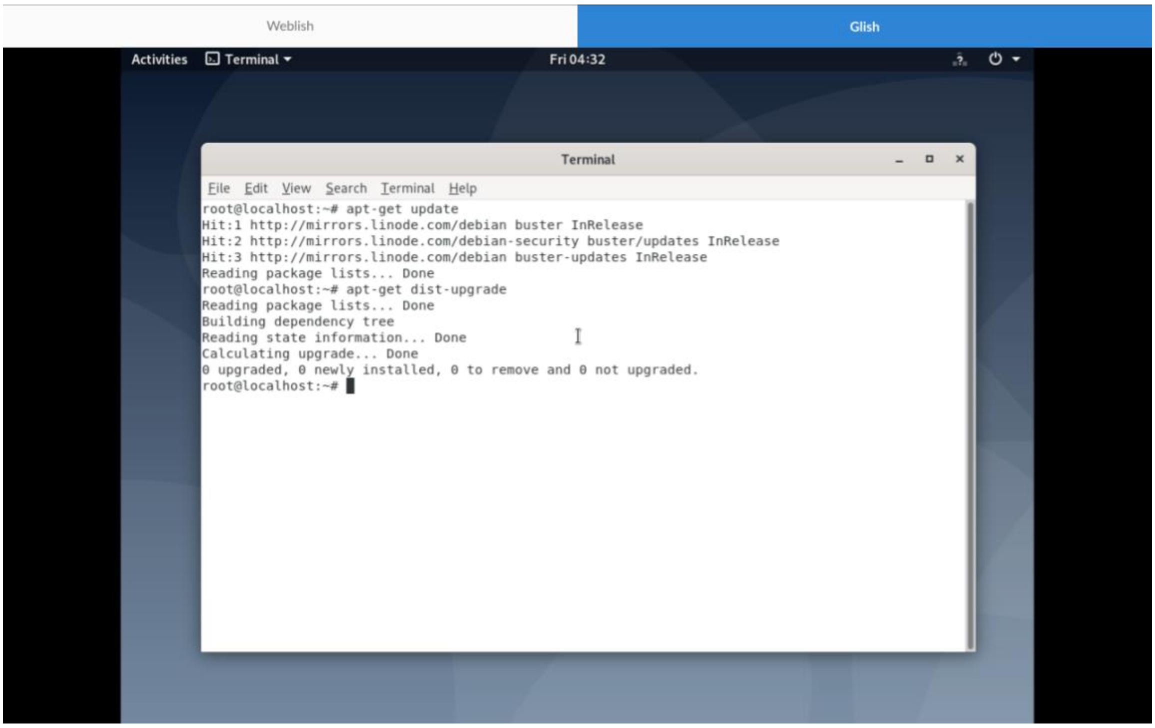
STEPS TO FOLLOW:

Step 1

On your Debian 10 machine open terminal window and type in the following commands to update and upgrade existing packages.

# sudo apt-get update

# sudo apt-get dist-upgrade



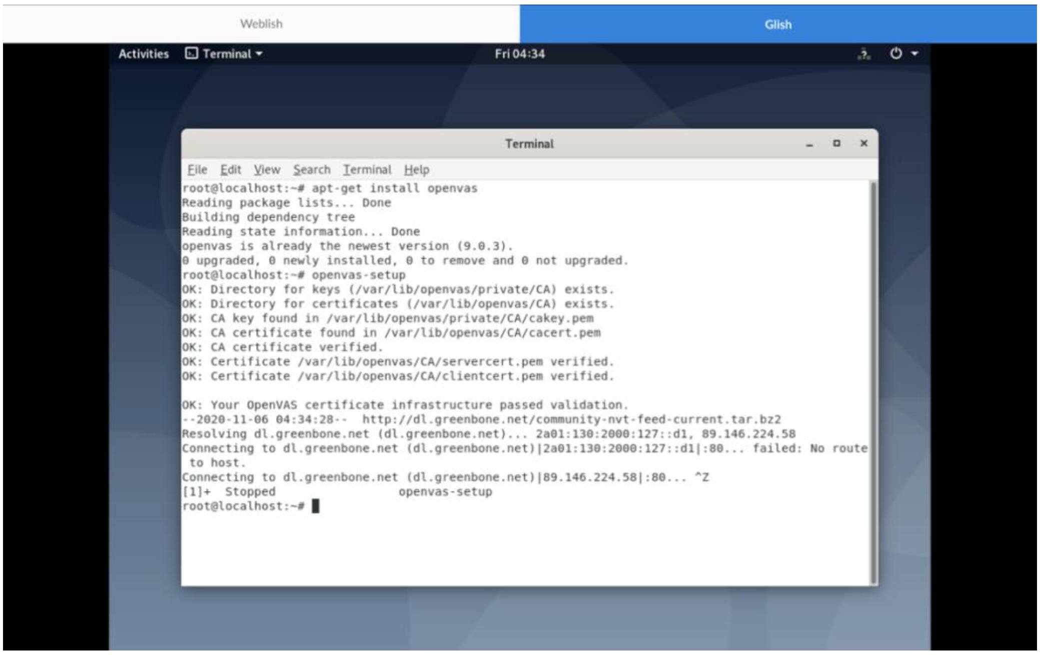
```
root@localhost:~# apt-get update
Hit:1 http://mirrors.linode.com/debian buster InRelease
Hit:2 http://mirrors.linode.com/debian-security buster/updates InRelease
Hit:3 http://mirrors.linode.com/debian buster-updates InRelease
Reading package lists... Done
root@localhost:~# apt-get dist-upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@localhost:~#
```

Step 2

After installing the packages it is time to **install** and **setup** OpenVAS. Run the following commands in the terminal.

# sudo apt-get install openvas

# sudo openvas-setup



```
root@localhost:~# apt-get install openvas
Reading package lists... Done
Building dependency tree
Reading state information... Done
openvas is already the newest version (9.0.3).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@localhost:~# openvas-setup
OK: Directory for keys (/var/lib/openvas/private/CA) exists.
OK: Directory for certificates (/var/lib/openvas/CA) exists.
OK: CA key found in /var/lib/openvas/private/CA/cakey.pem
OK: CA certificate found in /var/lib/openvas/CA/cacert.pem
OK: CA certificate verified.
OK: Certificate /var/lib/openvas/CA/servercert.pem verified.
OK: Certificate /var/lib/openvas/CA/clientcert.pem verified.

OK: Your OpenVAS certificate infrastructure passed validation.
--2020-11-06 04:34:28--  http://dl.greenbone.net/community-nvt-feed-current.tar.bz2
Resolving dl.greenbone.net (dl.greenbone.net)... 2a01:130:2000:127::d1, 89.146.224.58
Connecting to dl.greenbone.net (dl.greenbone.net)|2a01:130:2000:127::d1|:80... failed: No route
 to host.
Connecting to dl.greenbone.net (dl.greenbone.net)|89.146.224.58|:80... ^Z
[1]+  Stopped                 openvas-setup
root@localhost:~# 
```

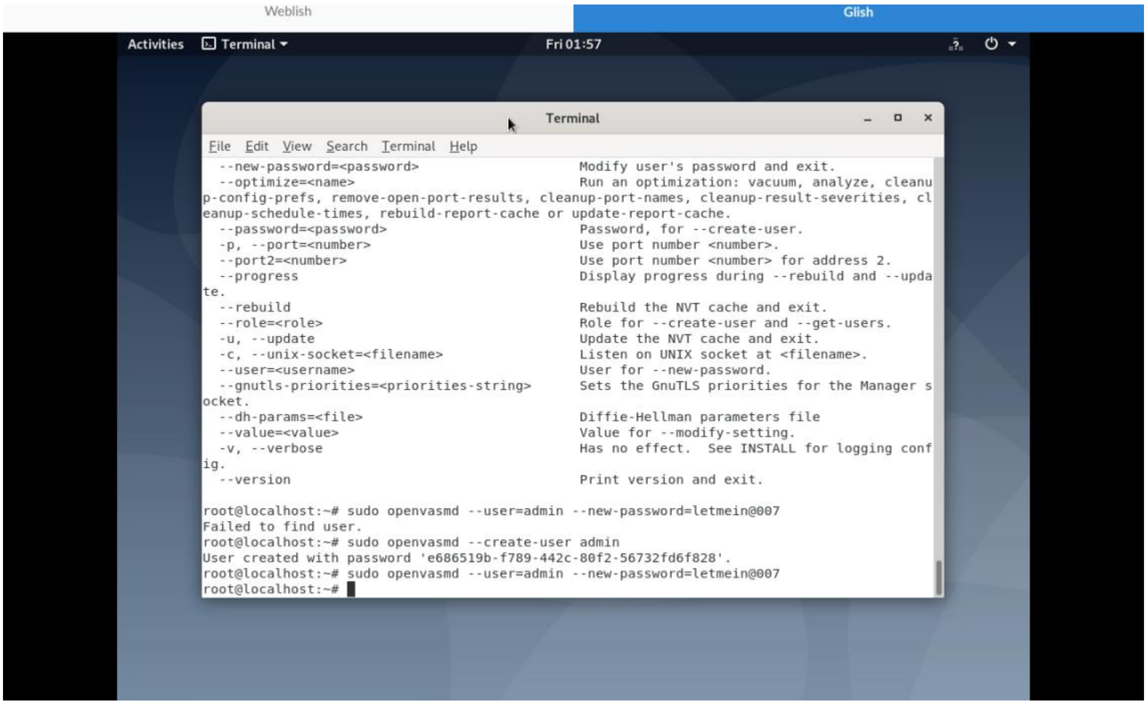
Step 3

Now, to **configure** OpenVAS and to **create** an initial **user** to access it’s services, execute followings commands in the terminal.

sudo openvasmd –create-user admin

Now, assign a **password** to the created user.

sudo openvasmd –user=admin –new-password=letmein@007



```
  --new-password=<password>                    Modify user's password and exit.
  --optimize=<name>                            Run an optimization: vacuum, analyze, cleanu
p-config-prefs, remove-open-port-results, cleanup-port-names, cleanup-result-severities, cl
eanup-schedule-times, rebuild-report-cache or update-report-cache.
  --password=<password>                        Password, for --create-user.
  -p, --port=<number>                          Use port number <number>.
  --port2=<number>                             Use port number <number> for address 2.
  --progress                                   Display progress during --rebuild and --upda
te.
  --rebuild                                    Rebuild the NVT cache and exit.
  --role=<role>                                Role for --create-user and --get-users.
  -u, --update                                 Update the NVT cache and exit.
  -c, --unix-socket=<filename>                 Listen on UNIX socket at <filename>.
  --user=<username>                            User for --new-password.
  --gnutls-priorities=<priorities-string>      Sets the GnuTLS priorities for the Manager s
ocket.
  --dh-params=<file>                           Diffie-Hellman parameters file
  --value=<value>                              Value for --modify-setting.
  -v, --verbose                                Has no effect.  See INSTALL for logging conf
ig.
  --version                                    Print version and exit.

root@localhost:~# sudo openvasmd --user=admin --new-password=letmein@007
Failed to find user.
root@localhost:~# sudo openvasmd --create-user admin
User created with password 'e686519b-f789-442c-80f2-56732fd6f828'.
root@localhost:~# sudo openvasmd --user=admin --new-password=letmein@007
root@localhost:~# 
```

Step 4

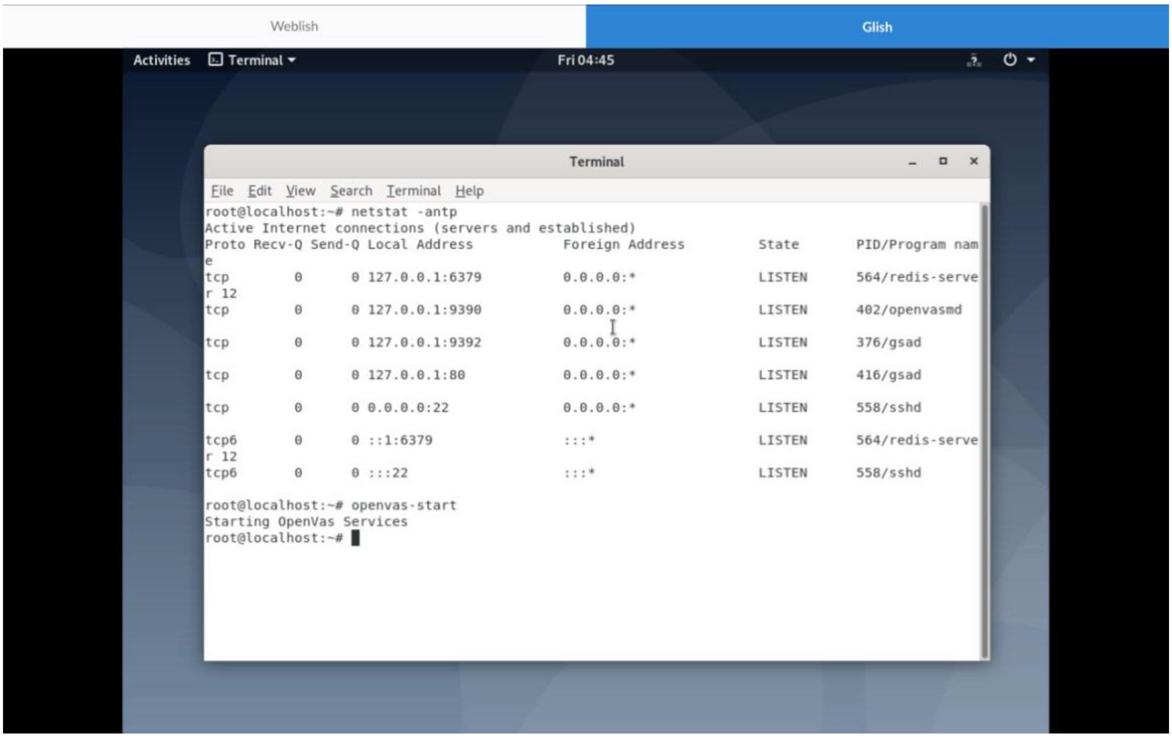
Once the user is created OpenVAS is ready to be **launched**. In order to launch OpenVAS service, we first need to check the **interface** it's running on. For that we execute the following commands.

netstat -antp

In this command '**a**' will display all active **ports**, '**n**' will give the numerical display of **address** and **port** numbers, '**t**' shows us the **download status** of active connections and '**p**' displays the connection **protocols**.

We can then start the service by executing the following command.

openvas-start



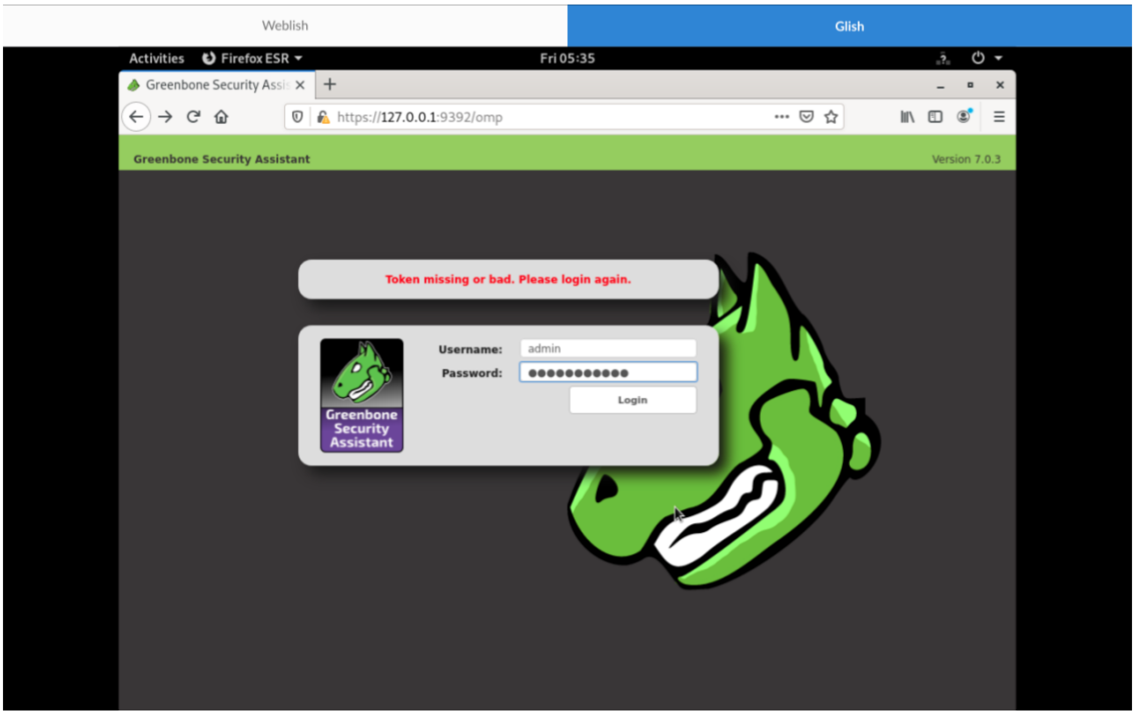
```
root@localhost:~# netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program nam
e
tcp        0      0 127.0.0.1:6379          0.0.0.0:*               LISTEN      564/redis-serve
r 12
tcp        0      0 127.0.0.1:9390          0.0.0.0:*               LISTEN      402/openvasmd

tcp        0      0 127.0.0.1:9392          0.0.0.0:*               LISTEN      376/gsad

tcp        0      0 127.0.0.1:80            0.0.0.0:*               LISTEN      416/gsad

tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      558/sshd

tcp6       0      0 ::1:6379                :::*                    LISTEN      564/redis-serve
r 12
tcp6       0      0 :::22                   :::*                    LISTEN      558/sshd

root@localhost:~# openvas-start
Starting OpenVas Services
root@localhost:~# █
```

Step 5

Once the OpenVAS service has started, navigate to **web browser** and enter the URL with **localhost IP** and **port number**. i.e. https://127.0.0.1:9392

Note: We get this **IP** and **port** number by looking at the **netstat output**. We select the one with '**gsad**' program name. (Greenbone Security Assistant Daemon)

We can then login using the credentials (admin:letmein@007) created earlier.

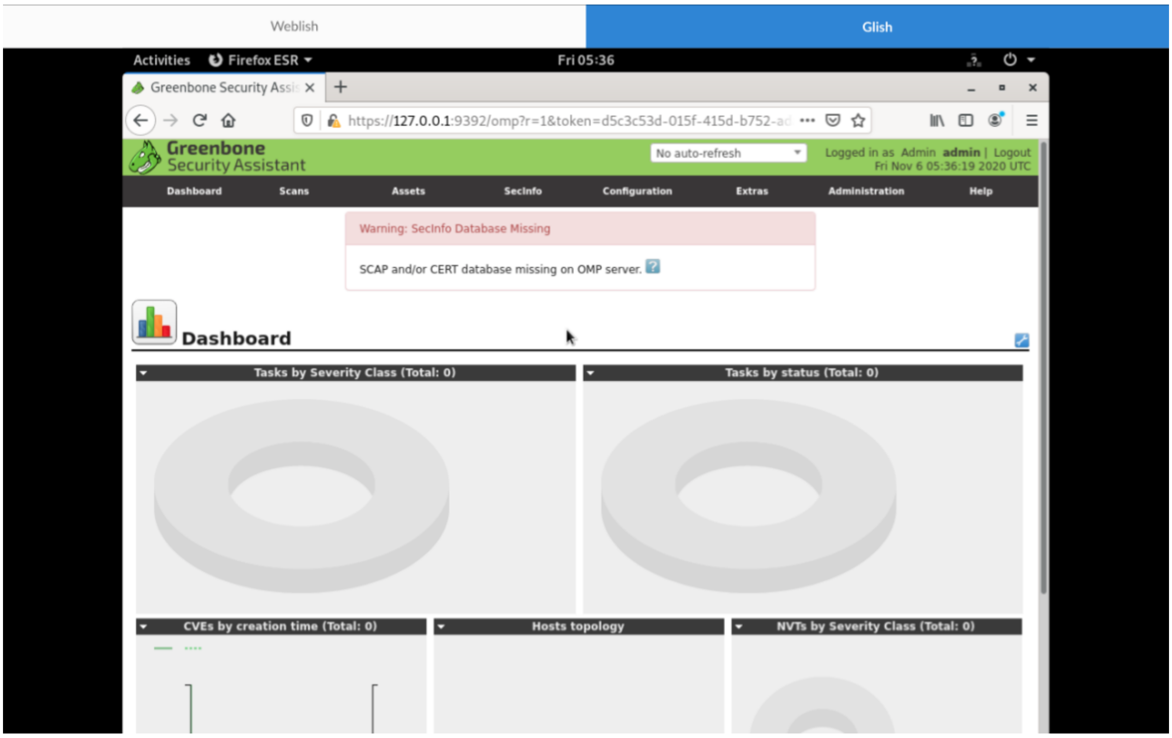


Token missing or bad. Please login again.

Username: admin
Password: ●●●●●●●●●●●

Step 6

After logging into the dashboard. We can navigate and use the services needed.


Weblish
Glish
Activities
Firefox ESR
Fri 05:36
Greenbone Security Assi
https://127.0.0.1:9392/omp?r=1&token=d5c3c53d-015f-415d-b752-ac
Greenbone Security Assistant
No auto-refresh
Logged in as Admin admin | Logout
Fri Nov 6 05:36:19 2020 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Dashboard
Tasks by Severity Class (Total: 0)
Tasks by status (Total: 0)
CVEs by creation time (Total: 0)
Hosts topology
NVTs by Severity Class (Total: 0)

Warning: SecInfo Database Missing

SCAP and/or CERT database missing on OMP server.

REFERENCES & USEFUL LINKS:

- *Ubuntu Manpage Repository - http://manpages.ubuntu.com/manpages/bionic/man8/gsad.8.html*
- *Greenbone Community – https://community.greenbone.net/t/about-the-greenbone-source-edition-gse-category/176*
- *Live Greenbone Demo -*

  https://www.greenbone.net/en/live-demo/
- *Installation Steps on Kali Org – https://www.kali.org/penetration-testing/openvas-vulnerability-scanning/*