

Class 11 - 07/09/2023

Ports are divided into 3 types:

1. Well known Ports 0-1023
2. Registered Ports 1024-49151
3. Dynamic Ports 49152-65565

We will be learning nikto to scan web serves. Known as web servers scanners.

Speed of nikto is higher than nmap.

Accuracy of nikto is not that much.

Nmap is used for networks and web apps.

Nikto can also scan outdated technologies in the web and version specific problems and is used for security testing in web servers and web applicatons.

Find bugs and earn money:

- Bugcrowd
- Hackerone

OpenVAS tool in kali: <https://www.youtube.com/watch?v=jgVt4QgvtRc>

command → sudo apt install openvas

Task - Download OpenVAS tool on Kali linux

1. Using the command: sudo apt dist-upgrade -y

Kali [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

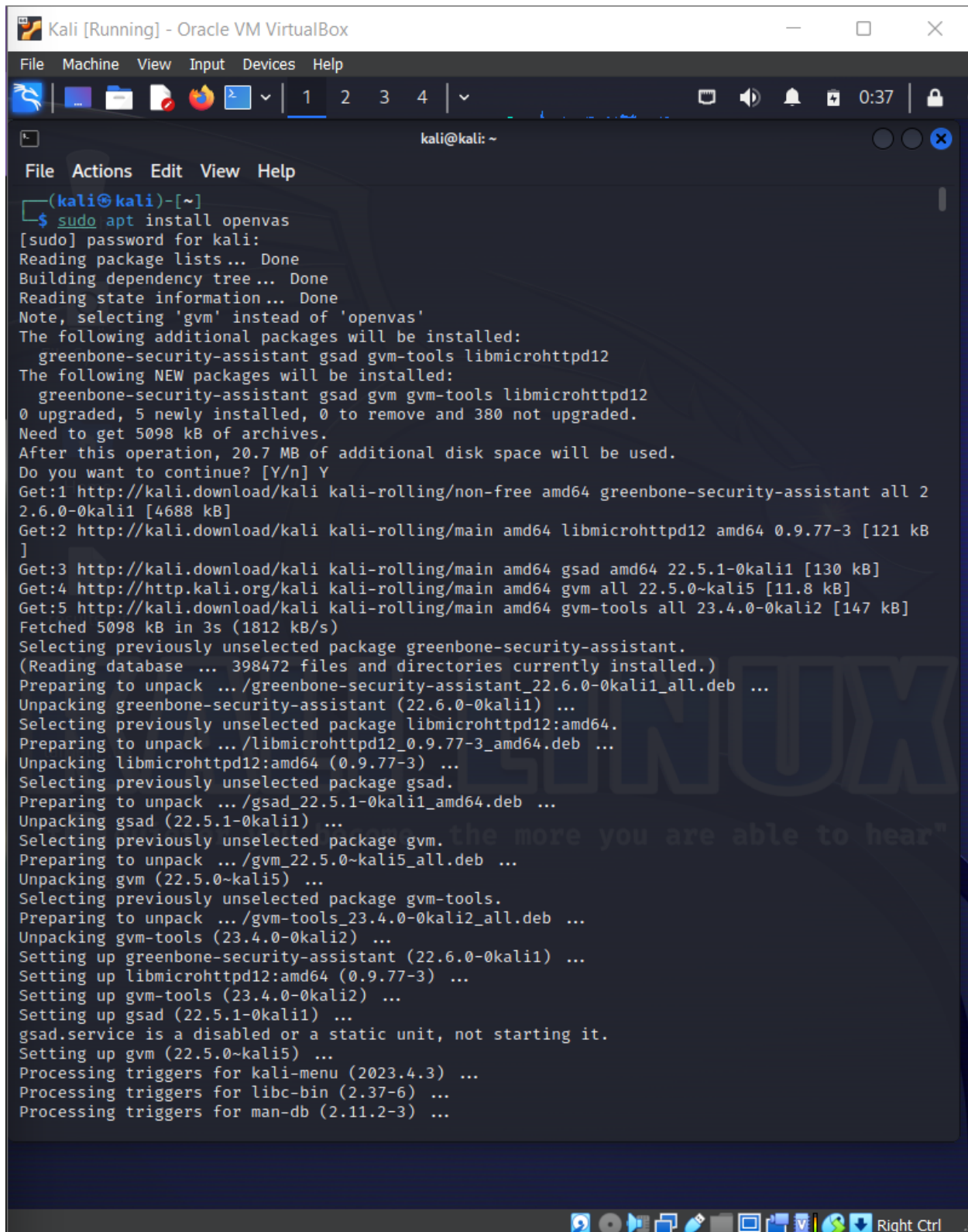
kali@kali: ~

File Actions Edit View Help

```
Get:284 http://kali.download/kali kali-rolling/main amd64 proxychains4 amd64 4.16-3 [19.9 kB]
Get:285 http://kali.download/kali kali-rolling/main amd64 libproxychains4 amd64 4.16-3 [22.7 kB]
Get:286 http://http.kali.org/kali kali-rolling/main amd64 libqt5positioning5 amd64 5.15.10+dfsg-3 [205 kB]
Get:287 http://kali.download/kali kali-rolling/main amd64 librtlsdr0 amd64 0.6.0-5 [30.2 kB]
Get:288 http://http.kali.org/kali kali-rolling/main amd64 libsdl2-2.0-0 amd64 2.28.2+dfsg-1 [636 kB]
Get:289 http://kali.download/kali kali-rolling/main amd64 libssh-4 amd64 0.10.5-3 [188 kB]
Get:290 http://kali.download/kali kali-rolling/main amd64 libtext-csv-perl all 2.03-1 [113 kB]
Get:291 http://kali.download/kali kali-rolling/main amd64 libwacom9 amd64 2.7.0-1 [21.5 kB]
Get:292 http://kali.download/kali kali-rolling/main amd64 libwacom-common all 2.7.0-1 [59.5 kB]
Get:293 http://kali.download/kali kali-rolling/main amd64 libwebsockets19 amd64 4.3.2-4 [229 kB]
Get:294 http://kali.download/kali kali-rolling/main amd64 libwireshark-data all 4.0.8-1 [1623 kB]
Get:295 http://kali.download/kali kali-rolling/main amd64 libwsutil14 amd64 4.0.8-1 [107 kB]
Get:296 http://kali.download/kali kali-rolling/main amd64 libwiretap13 amd64 4.0.8-1 [253 kB]
Get:297 http://kali.download/kali kali-rolling/main amd64 libwireshark16 amd64 4.0.8-1 [17.9 MB]
Get:298 http://kali.download/kali kali-rolling/main amd64 libwmflite-0.2-7 amd64 0.2.13-1 [75.1 kB]
Get:299 http://kali.download/kali kali-rolling/main amd64 libxatracker2 amd64 23.1.6-1 [1921 kB]
Get:300 http://kali.download/kali kali-rolling/main amd64 linux-image-6.4.0-kali3-amd64 amd64 6.4.11-1kali1 [73.5 MB]
Get:301 http://kali.download/kali kali-rolling/main amd64 linux-image-amd64 amd64 6.4.11-1kali1 [1488 B]
Get:302 http://kali.download/kali kali-rolling/main amd64 lm-sensors amd64 1:3.6.0-8 [97.4 kB]
Get:303 http://kali.download/kali kali-rolling/main amd64 mesa-va-drivers amd64 23.1.6-1 [3375 kB]
Get:304 http://kali.download/kali kali-rolling/main amd64 mesa-vgpu-drivers amd64 23.1.6-1 [3120 kB]
Get:305 http://kali.download/kali kali-rolling/main amd64 mesa-vulkan-drivers amd64 23.1.6-1 [9194 kB]
Get:306 http://http.kali.org/kali kali-rolling/main amd64 postgresql all 15+253 [10.8 kB]
Get:307 http://kali.download/kali kali-rolling/main amd64 metasploit-framework amd64 6.3.31-0kali1 [158 MB]
Get:308 http://kali.download/kali kali-rolling/main amd64 mingw-w64-common all 11.0.1-2 [5506 kB]
Get:309 http://kali.download/kali kali-rolling/main amd64 mingw-w64-i686-dev all 11.0.1-2 [2914 kB]
Get:310 http://kali.download/kali kali-rolling/main amd64 mingw-w64-x86_64-dev all 11.0.1-2 [3612 kB]
Get:311 http://http.kali.org/kali kali-rolling/main amd64 mupdf-tools amd64 1.22.2+ds1-2 [45.5 MB]
85% [311 mupdf-tools 26.5 MB/45.5 MB 58%] 1579 kB/s 1min 31s
```

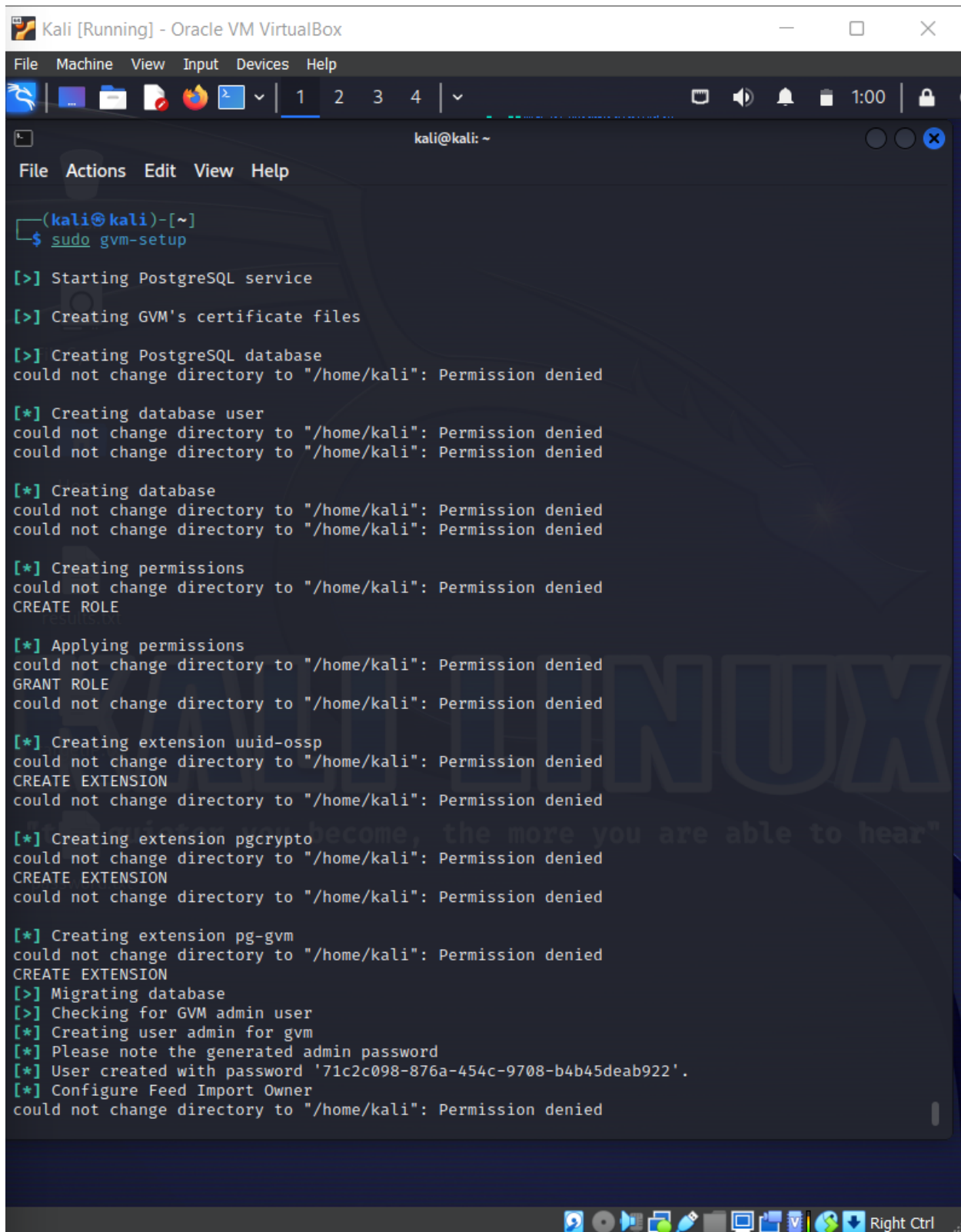
Right Ctrl

2. sudo apt install openvas



```
Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ sudo apt install openvas
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'gvm' instead of 'openvas'
The following additional packages will be installed:
  greenbone-security-assistant gsad gvm-tools libmicrohttpd12
The following NEW packages will be installed:
  greenbone-security-assistant gsad gvm gvm-tools libmicrohttpd12
0 upgraded, 5 newly installed, 0 to remove and 380 not upgraded.
Need to get 5098 kB of archives.
After this operation, 20.7 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://kali.download/kali kali-rolling/non-free amd64 greenbone-security-assistant all 2
2.6.0-0kali1 [4688 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 libmicrohttpd12 amd64 0.9.77-3 [121 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 gsad amd64 22.5.1-0kali1 [130 kB]
Get:4 http://http.kali.org/kali kali-rolling/main amd64 gvm all 22.5.0~kali5 [11.8 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 gvm-tools all 23.4.0-0kali2 [147 kB]
Fetched 5098 kB in 3s (1812 kB/s)
Selecting previously unselected package greenbone-security-assistant.
(Reading database ... 398472 files and directories currently installed.)
Preparing to unpack .../greenbone-security-assistant_22.6.0-0kali1_all.deb ...
Unpacking greenbone-security-assistant (22.6.0-0kali1) ...
Selecting previously unselected package libmicrohttpd12:amd64.
Preparing to unpack .../libmicrohttpd12_0.9.77-3_amd64.deb ...
Unpacking libmicrohttpd12:amd64 (0.9.77-3) ...
Selecting previously unselected package gsad.
Preparing to unpack .../gsad_22.5.1-0kali1_amd64.deb ...
Unpacking gsad (22.5.1-0kali1) ...
Selecting previously unselected package gvm.
Preparing to unpack .../gvm_22.5.0~kali5_all.deb ...
Unpacking gvm (22.5.0~kali5) ...
Selecting previously unselected package gvm-tools.
Preparing to unpack .../gvm-tools_23.4.0-0kali2_all.deb ...
Unpacking gvm-tools (23.4.0-0kali2) ...
Setting up greenbone-security-assistant (22.6.0-0kali1) ...
Setting up libmicrohttpd12:amd64 (0.9.77-3) ...
Setting up gvm-tools (23.4.0-0kali2) ...
Setting up gsad (22.5.1-0kali1) ...
gsad.service is a disabled or a static unit, not starting it.
Setting up gvm (22.5.0~kali5) ...
Processing triggers for kali-menu (2023.4.3) ...
Processing triggers for libc-bin (2.37-6) ...
Processing triggers for man-db (2.11.2-3) ...
```

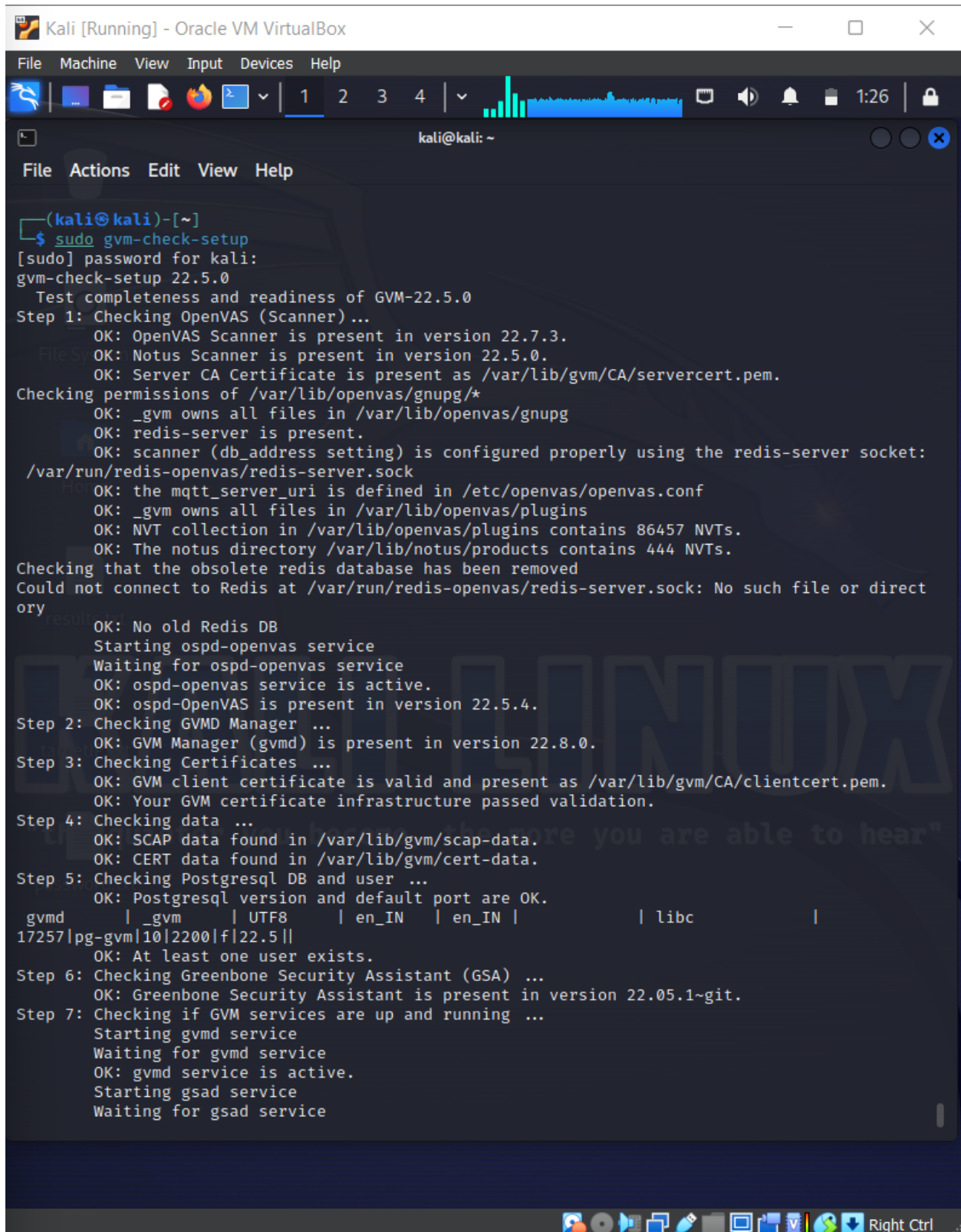
3. `sudo gvm-setup`



```
Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ sudo gvm-setup

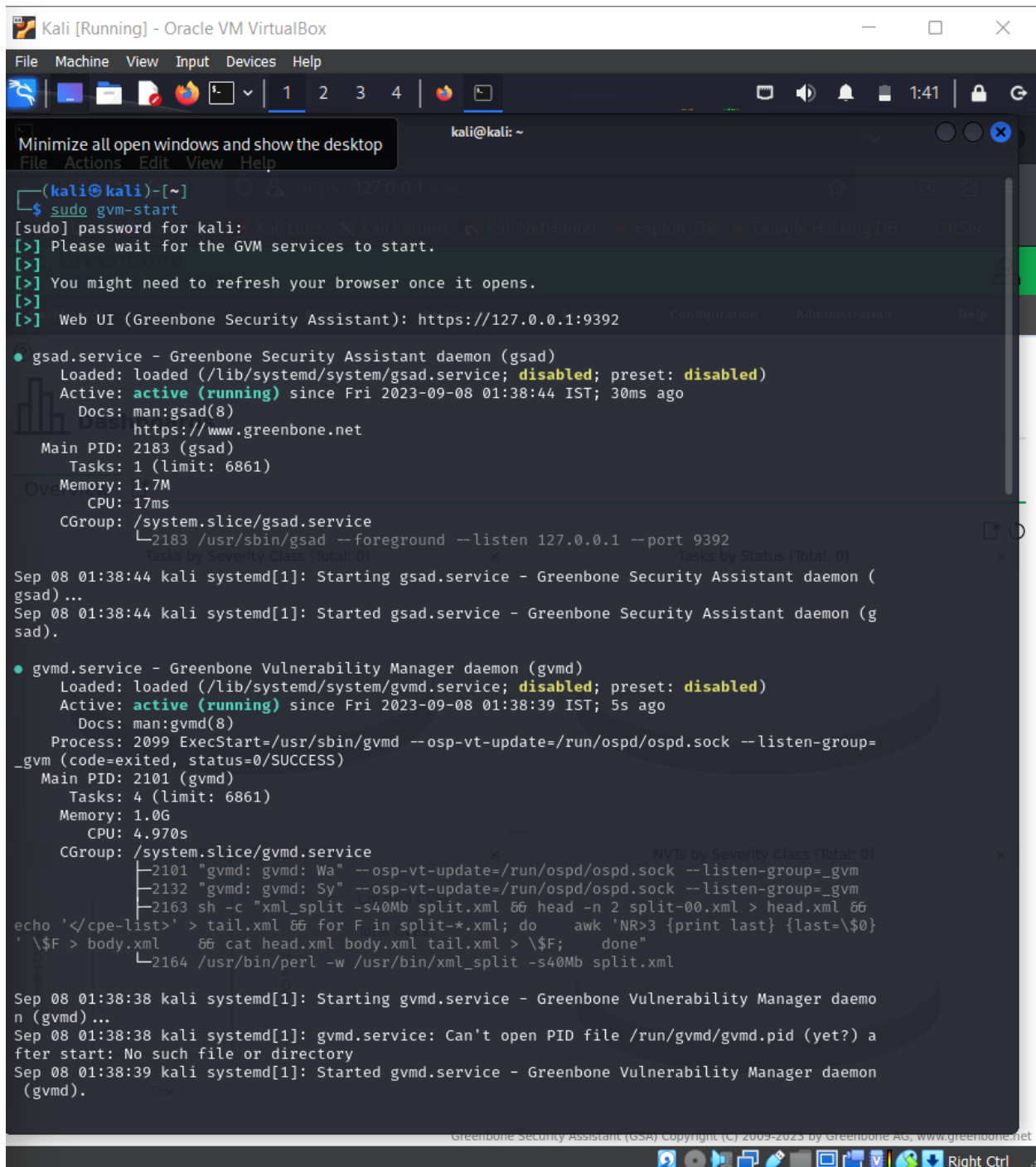
[>] Starting PostgreSQL service
[>] Creating GVM's certificate files
[>] Creating PostgreSQL database
could not change directory to "/home/kali": Permission denied
[*] Creating database user
could not change directory to "/home/kali": Permission denied
could not change directory to "/home/kali": Permission denied
[*] Creating database
could not change directory to "/home/kali": Permission denied
could not change directory to "/home/kali": Permission denied
[*] Creating permissions
could not change directory to "/home/kali": Permission denied
CREATE ROLE
[*] Applying permissions
could not change directory to "/home/kali": Permission denied
GRANT ROLE
could not change directory to "/home/kali": Permission denied
[*] Creating extension uuid-osp
could not change directory to "/home/kali": Permission denied
CREATE EXTENSION
could not change directory to "/home/kali": Permission denied
[*] Creating extension pgcrypto
could not change directory to "/home/kali": Permission denied
CREATE EXTENSION
could not change directory to "/home/kali": Permission denied
[*] Creating extension pg-gvm
could not change directory to "/home/kali": Permission denied
CREATE EXTENSION
[>] Migrating database
[>] Checking for GVM admin user
[*] Creating user admin for gvm
[*] Please note the generated admin password
[*] User created with password '71c2c098-876a-454c-9708-b4b45deab922'.
[*] Configure Feed Import Owner
could not change directory to "/home/kali": Permission denied
```

4. Verifying the installation: gvm-check-setup



```
(kali@kali)~$ sudo gvm-check-setup
[sudo] password for kali:
gvm-check-setup 22.5.0
Test completeness and readiness of GVM-22.5.0
Step 1: Checking OpenVAS (Scanner) ...
OK: OpenVAS Scanner is present in version 22.7.3.
OK: Notus Scanner is present in version 22.5.0.
OK: Server CA Certificate is present as /var/lib/gvm/CA/servercert.pem.
Checking permissions of /var/lib/openvas/gnupg/*
OK: _gvm owns all files in /var/lib/openvas/gnupg
OK: redis-server is present.
OK: scanner (db_address setting) is configured properly using the redis-server socket:
/var/run/redis-openvas/redis-server.sock
OK: the mqtt_server_uri is defined in /etc/openvas/openvas.conf
OK: _gvm owns all files in /var/lib/openvas/plugins
OK: NVT collection in /var/lib/openvas/plugins contains 86457 NVTs.
OK: The notus directory /var/lib/notus/products contains 444 NVTs.
Checking that the obsolete redis database has been removed
Could not connect to Redis at /var/run/redis-openvas/redis-server.sock: No such file or directory
OK: No old Redis DB
Starting ospd-openvas service
Waiting for ospd-openvas service
OK: ospd-openvas service is active.
OK: ospd-OpenVAS is present in version 22.5.4.
Step 2: Checking GVM Manager ...
OK: GVM Manager (gvmd) is present in version 22.8.0.
Step 3: Checking Certificates ...
OK: GVM client certificate is valid and present as /var/lib/gvm/CA/clientcert.pem.
OK: Your GVM certificate infrastructure passed validation.
Step 4: Checking data ...
OK: SCAP data found in /var/lib/gvm/scap-data.
OK: CERT data found in /var/lib/gvm/cert-data.
Step 5: Checking PostgreSQL DB and user ...
OK: PostgreSQL version and default port are OK.
gvmd | _gvm | UTF8 | en_IN | en_IN | | libc |
17257|pg-gvm|10|2200|f|22.5||
OK: At least one user exists.
Step 6: Checking Greenbone Security Assistant (GSA) ...
OK: Greenbone Security Assistant is present in version 22.05.1~git.
Step 7: Checking if GVM services are up and running ...
Starting gvmd service
Waiting for gvmd service
OK: gvmd service is active.
Starting gsad service
Waiting for gsad service
```


5. Starting OpenVas: sudo gvm-start



The screenshot shows a Kali Linux terminal window titled "Kali [Running] - Oracle VM VirtualBox". The terminal output for the command `sudo gvm-start` is as follows:

```
(kali@kali)-[~]
$ sudo gvm-start
[sudo] password for kali: 
[>] 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

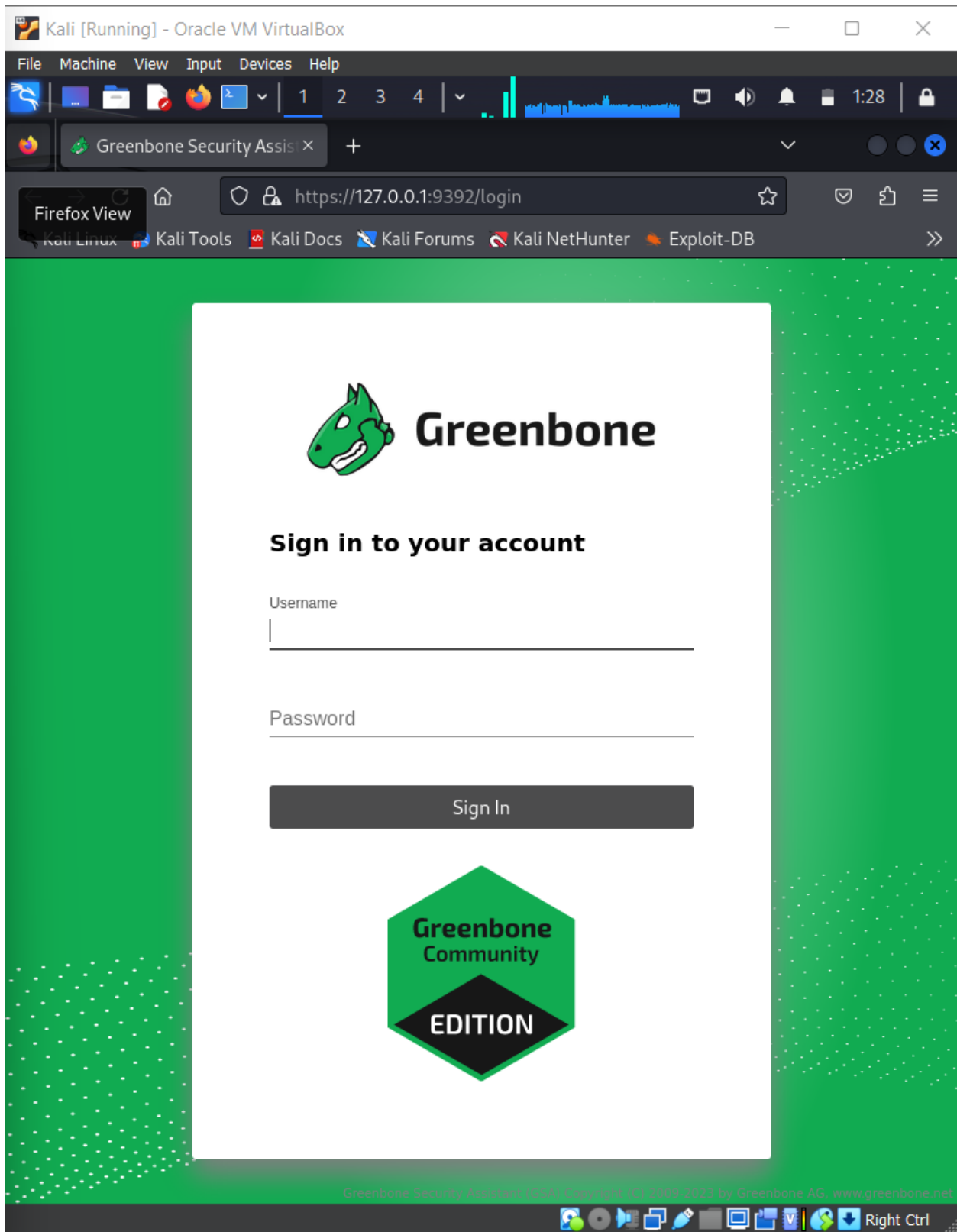
• gsad.service - Greenbone Security Assistant daemon (gsad)
  Loaded: loaded (/lib/systemd/system/gsad.service; disabled; preset: disabled)
  Active: active (running) since Fri 2023-09-08 01:38:44 IST; 30ms ago
    Docs: man:gsad(8)
           https://www.greenbone.net
  Main PID: 2183 (gsad)
    Tasks: 1 (limit: 6861)
  Memory: 1.7M
    CPU: 17ms
  CGroup: /system.slice/gsad.service
          └─2183 /usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9392

Sep 08 01:38:44 kali systemd[1]: Starting gsad.service - Greenbone Security Assistant daemon (gsad) ...
Sep 08 01:38:44 kali systemd[1]: Started gsad.service - Greenbone Security Assistant daemon (gsad).

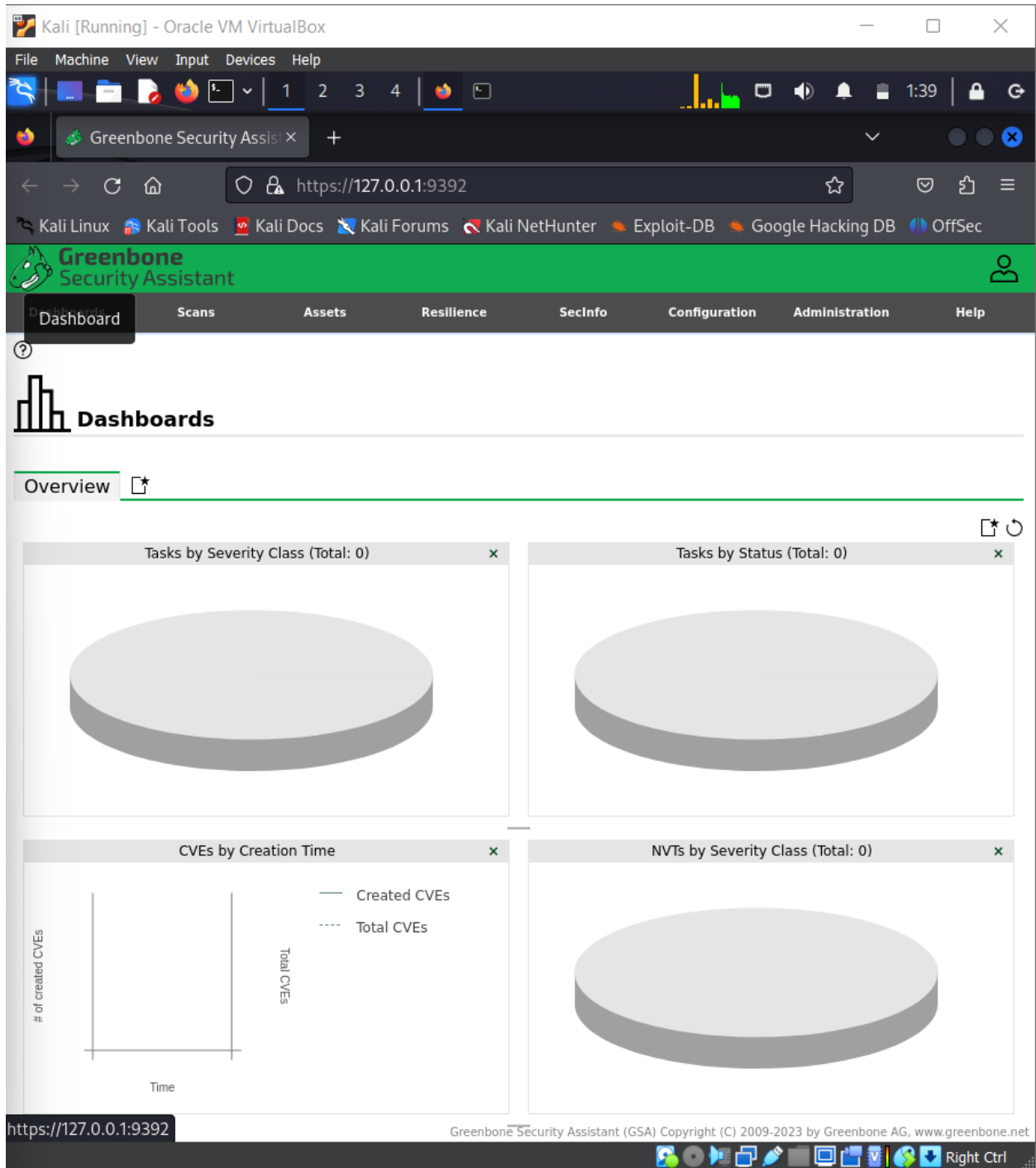
• gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)
  Loaded: loaded (/lib/systemd/system/gvmd.service; disabled; preset: disabled)
  Active: active (running) since Fri 2023-09-08 01:38:39 IST; 5s ago
    Docs: man:gvmd(8)
  Process: 2099 ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm (code=exited, status=0/SUCCESS)
  Main PID: 2101 (gvmd)
    Tasks: 4 (limit: 6861)
  Memory: 1.0G
    CPU: 4.970s
  CGroup: /system.slice/gvmd.service
          └─2101 "gvmd: gvmd: Wa" --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm
              └─2132 "gvmd: gvmd: Sy" --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm
                  └─2163 sh -c "xml_split -s40Mb split.xml && head -n 2 split-00.xml > head.xml &&
                      echo '</cpe-list>' > tail.xml && for F in split-*.xml; do awk 'NR>3 {print last} {last=\\$0}
                      '\\$F > body.xml && cat head.xml body.xml tail.xml > \\$F; done"
                      └─2164 /usr/bin/perl -w /usr/bin/xml_split -s40Mb split.xml

Sep 08 01:38:38 kali systemd[1]: Starting gvmd.service - Greenbone Vulnerability Manager daemon (gvmd) ...
Sep 08 01:38:38 kali systemd[1]: gvmd.service: Can't open PID file /run/gvmd/gvmd.pid (yet?) after start: No such file or directory
Sep 08 01:38:39 kali systemd[1]: Started gvmd.service - Greenbone Vulnerability Manager daemon (gvmd).
```

At the bottom of the terminal window, there is a copyright notice: "Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.net".



After logging in:



6. To stop the OpenVas: `sudo gvm-stop`

```
Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ sudo gvm-stop
[+] Stopping GVM services
o gsad.service - Greenbone Security Assistant daemon (gsad)
  Loaded: loaded (/lib/systemd/system/gsad.service; disabled; preset: disabled)
  Active: inactive (dead)
  Docs: man:gsad(8)
        https://www.greenbone.net

Sep 08 01:38:44 kali systemd[1]: Starting gsad.service - Greenbone Security Assistant daemon (gsad) ...
Sep 08 01:38:44 kali systemd[1]: Started gsad.service - Greenbone Security Assistant daemon (gsad).
Sep 08 01:40:25 kali systemd[1]: Stopping gsad.service - Greenbone Security Assistant daemon (gsad) ...
Sep 08 01:40:25 kali systemd[1]: gsad.service: Deactivated successfully.
Sep 08 01:40:25 kali systemd[1]: Stopped gsad.service - Greenbone Security Assistant daemon (gsad).

o gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)
  Loaded: loaded (/lib/systemd/system/gvmd.service; disabled; preset: disabled)
  Active: inactive (dead)
  Docs: man:gvmd(8)

Sep 08 01:38:38 kali systemd[1]: Starting gvmd.service - Greenbone Vulnerability Manager daemon (gvmd) ...
Sep 08 01:38:38 kali systemd[1]: gvmd.service: Can't open PID file /run/gvmd/gvmd.pid (yet?) after start: No such file or directory
Sep 08 01:38:39 kali systemd[1]: Started gvmd.service - Greenbone Vulnerability Manager daemon (gvmd).
Sep 08 01:40:25 kali systemd[1]: Stopping gvmd.service - Greenbone Vulnerability Manager daemon (gvmd) ...
Sep 08 01:40:25 kali systemd[1]: gvmd.service: Deactivated successfully.
Sep 08 01:40:25 kali systemd[1]: Stopped gvmd.service - Greenbone Vulnerability Manager daemon (gvmd).
Sep 08 01:40:25 kali systemd[1]: gvmd.service: Consumed 1min 46.196s CPU time.

o ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas)
  Loaded: loaded (/lib/systemd/system/ospd-openvas.service; disabled; preset: disabled)
  Active: inactive (dead)
  Docs: man:ospd-openvas(8)
        man:openvas(8)

Sep 08 01:38:23 kali systemd[1]: Starting ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas) ...
Sep 08 01:38:26 kali systemd[1]: Started ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas).
Sep 08 01:40:25 kali systemd[1]: Stopping ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas) ...
Sep 08 01:40:25 kali systemd[1]: ospd-openvas.service: Deactivated successfully.

Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.net
```