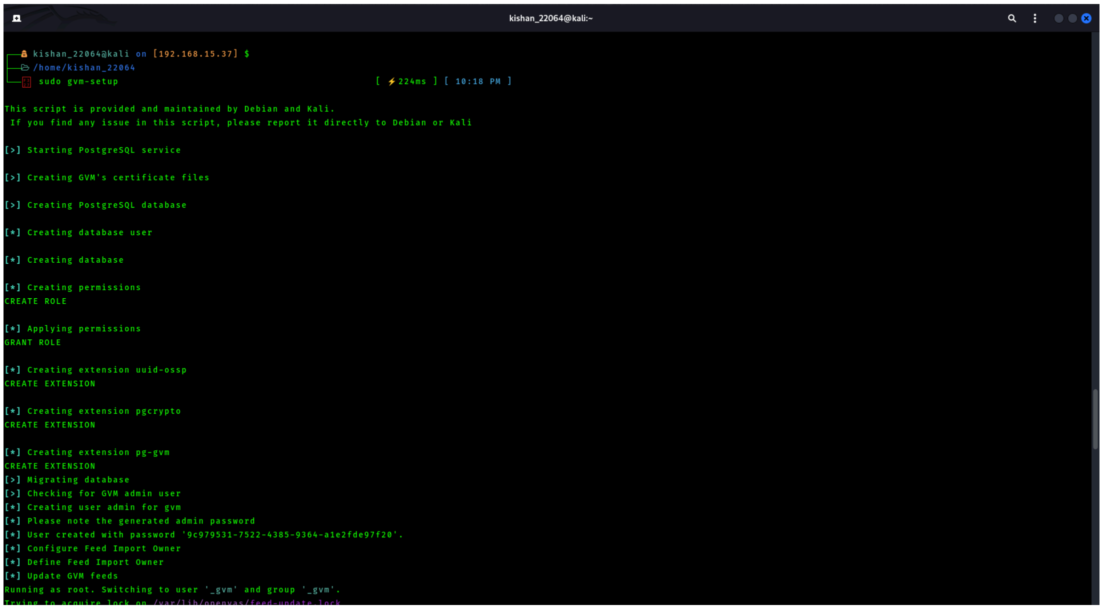
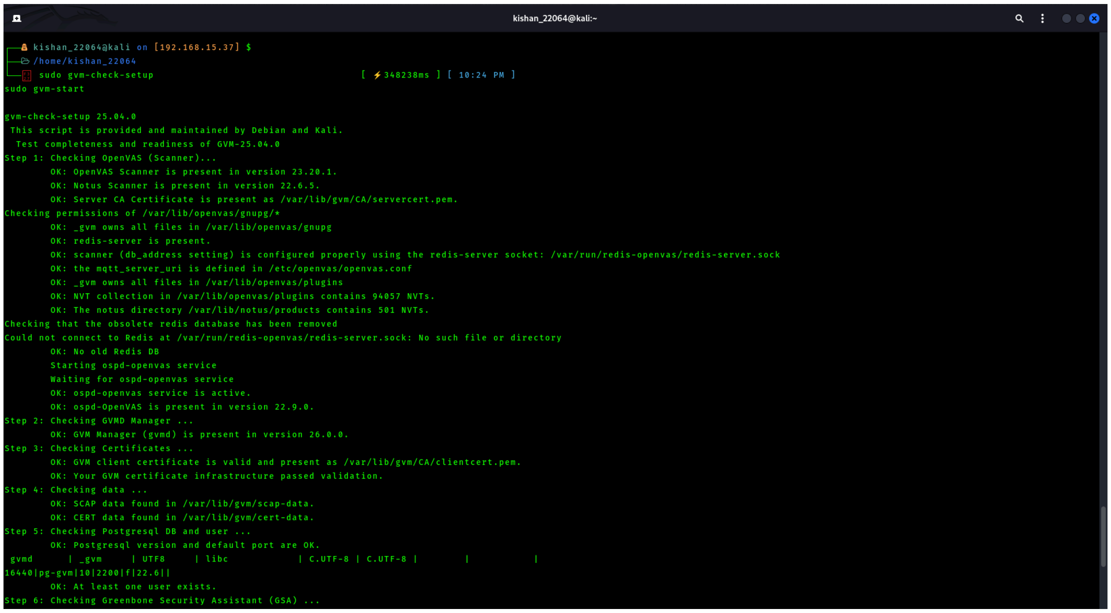
1. Install OpenVAS or Nessus Essentials



kishan_22064@kali:~

```
┌── kishan_22064@kali on [192.168.15.37] $
├── /home/kishan_22064
└──  sudo gvm-setup                                              [ ⚡224ms ] [ 10:18 PM ]

This script is provided and maintained by Debian and Kali.
 If you find any issue in this script, please report it directly to Debian or Kali

[>] Starting PostgreSQL service

[>] Creating GVM's certificate files

[>] Creating PostgreSQL database

[*] Creating database user

[*] Creating database

[*] Creating permissions
CREATE ROLE

[*] Applying permissions
GRANT ROLE

[*] Creating extension uuid-ossp
CREATE EXTENSION

[*] Creating extension pgcrypto
CREATE EXTENSION

[*] Creating extension pg-gvm
CREATE EXTENSION
[>] Migrating database
[>] Checking for GVM admin user
[*] Creating user admin for gvm
[*] Please note the generated admin password
[*] User created with password '9c979531-7522-4385-9364-a1e2fde97f20'.
[*] Configure Feed Import Owner
[*] Define Feed Import Owner
[*] Update GVM feeds
Running as root. Switching to user '_gvm' and group '_gvm'.
Trying to acquire lock on /var/lib/openvas/feed-update.lock
```



kishan_22064@kali:~

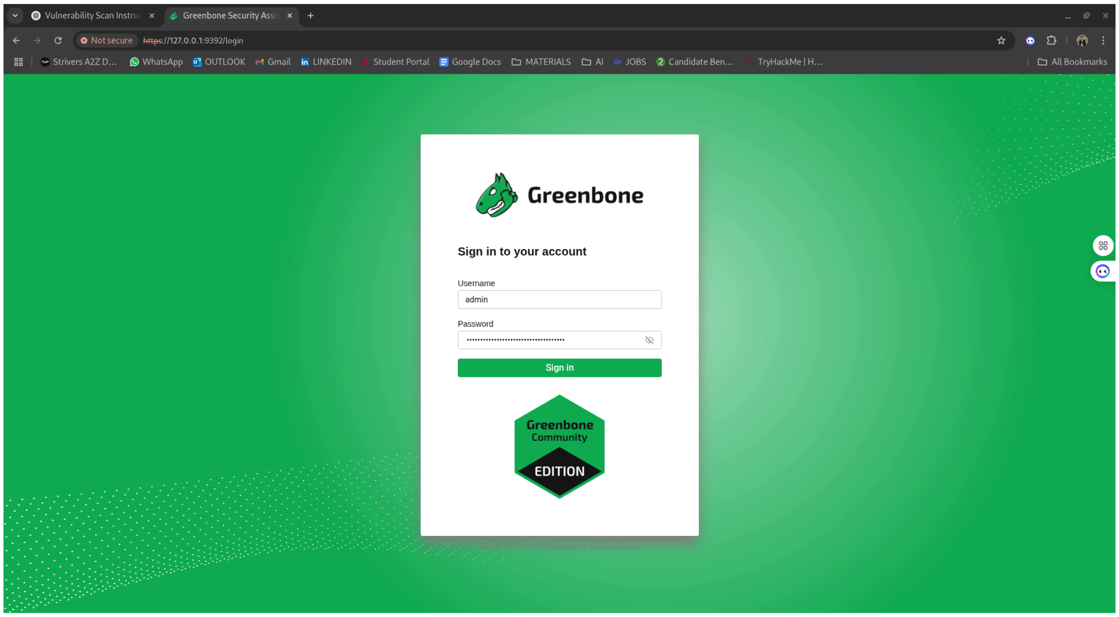
```
┌── kishan_22064@kali on [192.168.15.37] $
├── /home/kishan_22064
└──  sudo gvm-check-setup                                  [ ⚡348238ms ] [ 10:24 PM ]
sudo gvm-start

gvm-check-setup 25.04.0
 This script is provided and maintained by Debian and Kali.
  Test completeness and readiness of GVM-25.04.0
Step 1: Checking OpenVAS (Scanner)...
        OK: OpenVAS Scanner is present in version 23.20.1.
        OK: Notus Scanner is present in version 22.6.5.
        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 94057 NVTs.
        OK: The notus directory /var/lib/notus/products contains 501 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 22.9.0.
Step 2: Checking GVMD Manager ...
        OK: GVM Manager (gvmd) is present in version 26.0.0.
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     | libc            | C.UTF-8 | C.UTF-8 |        |           |
16440|pg-gvm|10|2200|f|22.6||
        OK: At least one user exists.
Step 6: Checking Greenbone Security Assistant (GSA) ...
```

OpenVAS was successfully installed, initialized, and started.

After the setup they have given the website link where we need to add scan and target for that website they gave username and password after the setup

2. Set up scan target as your local machine IP or localhost

The website link which was given by openvas after scan the GUI will be like this

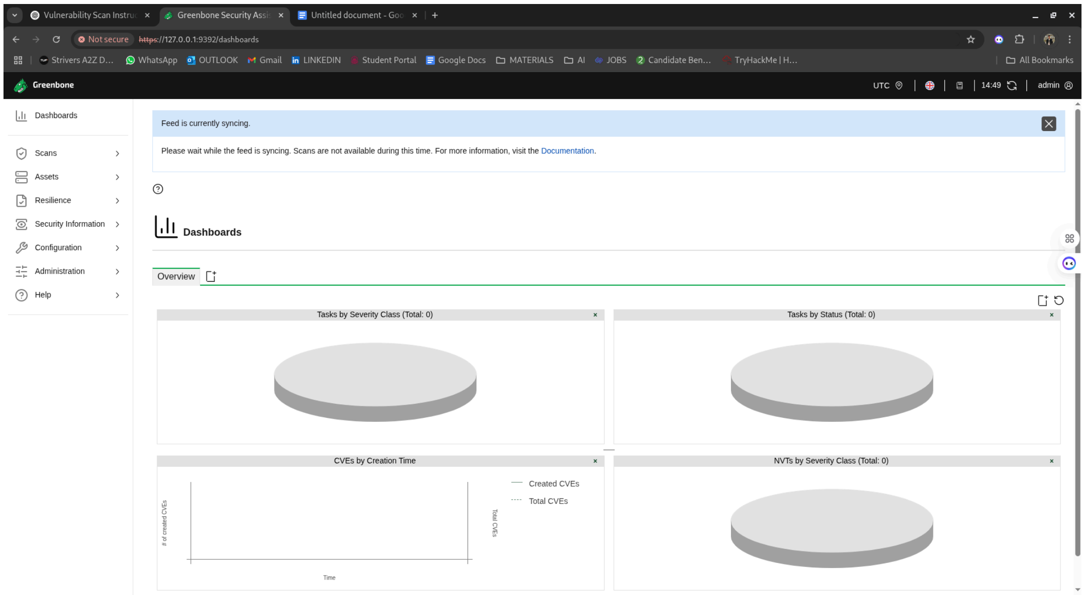


Sign in to your account

Username: admin

Password: ••••••••••••••••••••••••••••••••••

Sign in

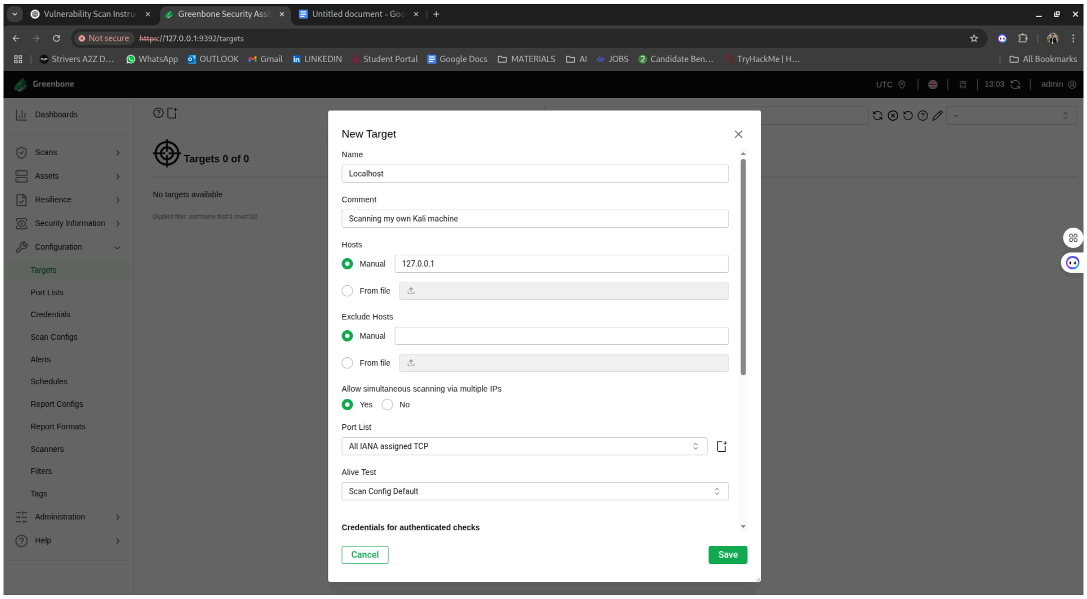


Feed is currently syncing.

Please wait while the feed is syncing. Scans are not available during this time. For more information, visit the Documentation.

I created a new Target from the GVM web UI:

- Name: Localhost
- Host IP: 127.0.0.1



New Target

Name: Localhost

Comment: Scanning my own Kali machine

Hosts: ● Manual 127.0.0.1 ○ From file

Exclude Hosts: ● Manual ○ From file

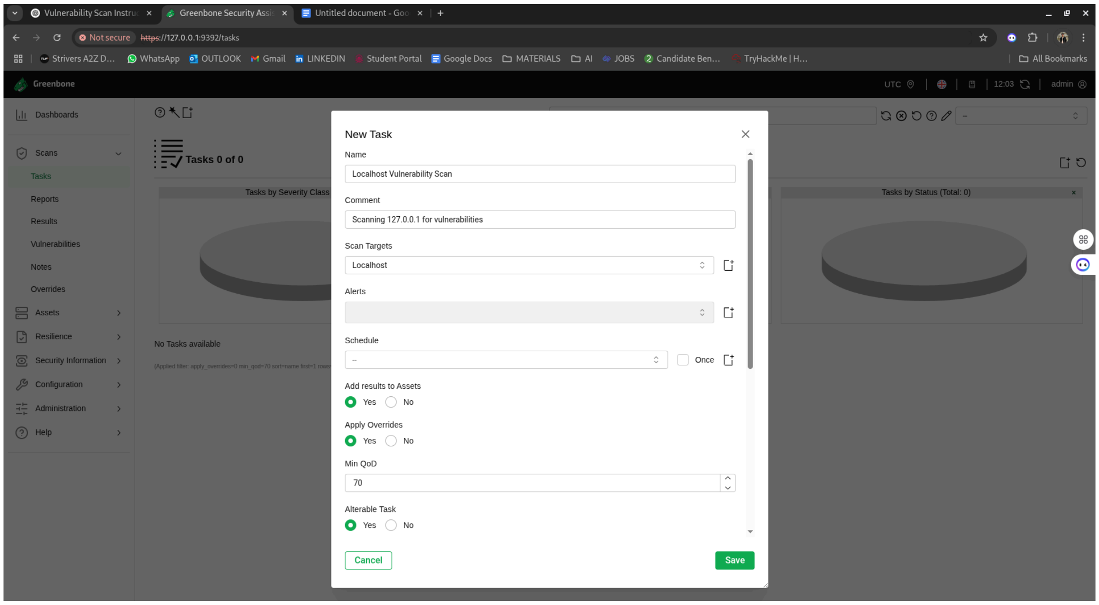
Allow simultaneous scanning via multiple IPs: ● Yes ○ No

Port List: All IANA assigned TCP

Alive Test: Scan Config Default

Credentials for authenticated checks

Cancel Save



New Task

Name: Localhost Vulnerability Scan

Comment: Scanning 127.0.0.1 for vulnerabilities

Scan Targets: Localhost

Alerts:

Schedule: -- □ Once

Add results to Assets: ● Yes ○ No

Apply Overrides: ● Yes ○ No

Min QoD: 70

Alterable Task: ● Yes ○ No

Cancel Save

3. Start a full vulnerability scan

I attempted to create a new scan task using the target, but encountered an error:

“Default Scan Config is not available. This issue may be due to the feed not having completed its synchronization.”

4. Wait for scan to complete (30–60 mins)

I could not run the scan because of missing scan configuration options (`Full and fast` etc.). So, the scan did not begin and there was no result to wait for.

5. Review the report for vulnerabilities and severity

No report was generated because the scan task was not created successfully.

However, I explored how reports in OpenVAS display:

- Vulnerability title
- Affected component
- Severity (CVSS score)
- Suggested fix or mitigation

6. Research simple fixes or mitigations for found vulnerabilities

Even without a scan result, I reviewed common vulnerabilities and how to fix them:

Weak passwords - Enforce password policies

Outdated software - Apply security updates regularly

Open ports - Close/disable unused services

Unsecured SSH settings - Disable root login, enforce keys

7. Document the most critical vulnerabilities

Since no vulnerabilities were found via the scanner, I researched typical high-severity ones:

Vulnerability Severity Fix

Open SSH with default port - High - Change default port or disable root

Conclusion:

Despite being unable to execute the scan due to a feed sync issue, I gained:

- Hands-on experience with OpenVAS/GVM
- Knowledge of feed syncing and task creation
- Awareness of common PC vulnerabilities and fixes

This task helped me understand the complete scanning process from setup to risk mitigation, even in the face of tool limitations.