

BloodHound Community Edition Installation and Setup on Kali Linux (Virtual Machine)

Installation Steps

Step 1: Install Docker

Docker is required to run BloodHound CE as a containerized application. Execute the following command to install Docker:

sudo apt install docker.io

```
kali@kali: ~  
$ sudo apt install docker.io  
The following packages were automatically installed and are no longer required:  
firebird3.0-common libcc++abi-19 libdirectfb-1.7-7t64 libgl1-mesa-dev libglvnd-dev libgumbo2 libbmedcrypto7t64 libtag1v5 libwebRTC-audio-processing1 python3-appdirs  
firebird3.0-common-doc libcapstone4 libegl-dev libgles-dev libgtksourceview-3.0-1 libhdfs-103-1t64 libpaper1 libtag1v5-vanilla libx265-209  
libbfl1 libconfig+9v5 libfont9 libgles1 libgtksourceview-3.0-common libhdfs-hl-100t64 libpoppler140 libtag8 openjdk-23-jre libunwind-19  
libcc++abi-19 libconfig libgeal35 libglvnd-core-dev libgtksourceviewmm-3.0-0v5 libxkb.9 libsuperluo libunwind-19 openjdk-23-jre-headless  
Use 'sudo apt autoremove' to remove them.  
Installing:  
docker.io  
Installing dependencies:  
containerd criu docker-cli libcompell libintl-perl libintl-xs-perl libmodule-find-perl libproc-processtable-perl libsort-naturally-perl needrestart python3-pycrui runc tini  
Suggested packages:  
containernetworking-plugins docker-doc aufs-tools btrfs-progs cgroupfs-mount debotstrap rinse rootlesskit xfsprogs zfs-fuse | zfsutils-linux  
Summary:  
Upgrading: 0, Installing: 14, Removing: 0, Not Upgrading: 37  
Download size: 66.2 MB  
Space needed: 261 MB / 68.0 GB available  
Continue? [Y/n] y  
Get:1 http://kali.kali.org/kali kali-rolling/main amd64 runc amd64 1.1.15+ds1-2 [2,958 kB]  
Get:4 http://kali.kali.org/kali kali-rolling/main amd64 docker.io amd64 26.1.5+dfsg1-4+b2 [22.7 MB]  
Get:6 http://kali.cs.nyu.edu.tw/kali kali-rolling/main amd64 criu amd64 4.0-3 [552 kB]  
Get:3 http://mirror.twd.com.tw/kali kali-rolling/main amd64 tini amd64 0.19.0-1 [255 kB]  
Get:5 http://kali.download/kali kali-rolling/main amd64 libcompell amd64 4.0-3 [63.8 kB]  
Get:8 http://kali.download/kali kali-rolling/main amd64 libintl-perl all 1.33-1 [720 kB]  
Get:9 http://kali.kali.org/kali kali-rolling/main amd64 libintl-xs-perl amd64 1.33-1+b3 [15.5 kB]  
Get:10 http://kali.download/kali kali-rolling/main amd64 libmodule-find-perl all 0.16-2 [18.6 kB]  
Get:13 http://kali.download/kali kali-rolling/main amd64 needrestart all 3.8-1 [65.0 kB]  
Get:11 http://kali.kali.org/kali kali-rolling/main amd64 libproc-processtable-perl amd64 0.636-1+b3 [42.3 kB]  
Get:12 http://mirror.twd.com.tw/kali kali-rolling/main amd64 libsort-naturally-perl all 1.03-4 [13.1 kB]  
Get:2 http://kali.kali.org/kali kali-rolling/main amd64 containerd amd64 1.7.24+ds1-4+b1 [31.5 MB]  
Get:7 http://kali.kali.org/kali kali-rolling/main amd64 docker-cli amd64 26.1.5+dfsg1-4+b2 [7,121 kB]  
Get:14 http://free.nhcc.org.tw/kali kali-rolling/main amd64 python3-pycrui all 4.0-3 [42.9 kB]  
Fetched 66.2 MB in 3min 24s (325 kB/s)  
Selecting previously unselected package runc.  
(Reading database ... 413163 files and directories currently installed.)  
Preparing to unpack .../00-runc_1.1.15+ds1-2_amd64.deb ...  
Unpacking runc (1.1.15+ds1-2) ...  
Selecting previously unselected package containerd.  
Preparing to unpack .../01-containerd_1.7.24+ds1-4+b1_amd64.deb ...  
Unpacking containerd (1.7.24+ds1-4+b1) ...  
Selecting previously unselected package tini.  
Preparing to unpack .../02-tini_0.19.0-1_amd64.deb ...  
Unpacking tini (0.19.0-1) ...  
Selecting previously unselected package docker.io.  
Preparing to unpack .../03-docker.io_26.1.5+dfsg1-4+b2_amd64.deb ...  
Unpacking docker.io (26.1.5+dfsg1-4+b2) ...
```

Step 2: Download the BloodHound CE Docker Compose File

Use the following command to download the Docker Compose file for BloodHound CE: *curl -L https://ghst.ly/getbhce > ./docker-compose.yml*

curl -L https://ghst.ly/getbhce > ./docker-compose.yml

This command retrieves the necessary configuration file required to deploy BloodHound CE containers. For more information, see the documentation:

<https://support.bloodhoundenterprise.io/hc/en-us/articles/17468450058267-Install-BloodHound-Community-Edition-with-Docker-Compose>

```
(kali@kali)-[~]
$ curl -L https://ghst.ly/getbhce > ./docker-compose.yml
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           %             %         Dload  Upload   Total   Spent    Left   Speed
100    156    100    156     0     0    168      0 --:--:-- --:--:-- --:--:--   168
100   3856    100   3856     0     0   1665      0 0:00:02 0:00:02 --:--:--  11901
```

Step 3: Pull and Run the BloodHound CE Containers

After downloading the Docker Compose file, pull the necessary container images and start the services:

`docker-compose pull && docker-compose up -d`

- `docker-compose pull`: Downloads the required Docker images.
- `docker-compose up -d`: Starts the BloodHound CE services in detached mode.

```
(kali@kali)-[~]
$ docker-compose pull && docker-compose up
Command 'docker-compose' not found, but can be installed with:
sudo apt install docker-compose
Do you want to install it? (N/y)
The following packages were automatically installed and are no longer required:
firebird3.0-common libcapstone4 libdirectfb-1.7-7t64 libgl1-mesa-dev libglvnd-dev
firebird3.0-common-doc libcapstone4 libegl-dev libgles-dev libgtksourceview-3.0-1 libgumbo2 libmbcrypto7t64 libtag1v5 libwebRTC-audio-processing1 python3-appdirs
libbrotli libconfig9 libfontconfig libglvnd-core-dev libgtksourceview-3.0-common libhdf5-hl-100t64 libpaper1 libtag1v5-vanilla libx265-209
libc++1-19 libconfig9 libgdal35 libglvnd-core-dev libgtksourceview-3.0-0v5 libhdf5-hl-100t64 libpaper1 libtag1v5-vanilla libx265-209
Use 'sudo apt autoremove' to remove them.
Installing:
docker-compose
Installing dependencies:
python3-compose python3-docker python3-dockerpty python3-texttable
Summary:
Upgrading: 0, Installing: 5, Removing: 0, Not Upgrading: 37
Download size: 270 kB
Space needed: 1,237 kB / 59.7 GB available
```

Step 4: Add Current User to Docker Group

To avoid using `sudo` for every Docker command, add your user to the Docker group:

`sudo usermod -aG docker $USER`

After making this change, activate the new group settings without logging out:

newgrp docker

Step 5: Verify Running Docker Containers

Ensure that the BloodHound CE container is running using:

docker ps

This command lists the active Docker containers.

```
(kali㉿kali)-[~]
$ sudo usermod -aG docker $USER

(kali㉿kali)-[~]
$ newgrp docker

(kali㉿kali)-[~]
$ docker ps
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
--------------	-------	---------	---------	--------	-------	-------


Step 7: Start BloodHound CE

Run the following command to start BloodHound CE using the downloaded Docker Compose file:

docker-compose -f docker-compose.yml up -d

```
(kali㉿kali)-[~]
$ docker-compose -f docker-compose.yml up
```

```
Creating network "kali_default" with the default driver
Creating volume "kali_neo4j-data" with default driver
Creating volume "kali_postgres-data" with default driver
Pulling app-db (docker.io/library/postgres:16) ...
16: Pulling from library/postgres
c29f5b76f736: Pull complete
c48f75705ee4: Pull complete
37f0f01afa08: Pull complete
bc9c351d2177: Pull complete
0a56f421ffcf: Pull complete
e2addc4ceae4: Pull complete
34985e29ac4e: Pull complete
ed284837e3c6: Pull complete
dce7ed737d87: Pull complete
4edf6f9d6bbd: Pull complete
9e5fea6c52a5: Pull complete
efd72fc59b95: Pull complete
4618de3d69f3: Pull complete
b3e17255218b: Pull complete
Digest: sha256:a35ec42526e3c522eb13b4d82eddaee875d0ac6ca9eb5cc5607e412854478c71
Status: Downloaded newer image for postgres:16
Pulling graph-db (docker.io/library/neo4j:4.4) ...
```



BLOODHOUND
COMMUNITY EDITION

ⓘ Your Account Password Has Expired
Please provide a new password for this account to continue.

If password cannot be seen try `sudo docker-compose -f docker-compose.yml logs`

After successfully establishing a server connection, an auto-generated password will be provided which will serve as the initial password upon logging in.

```

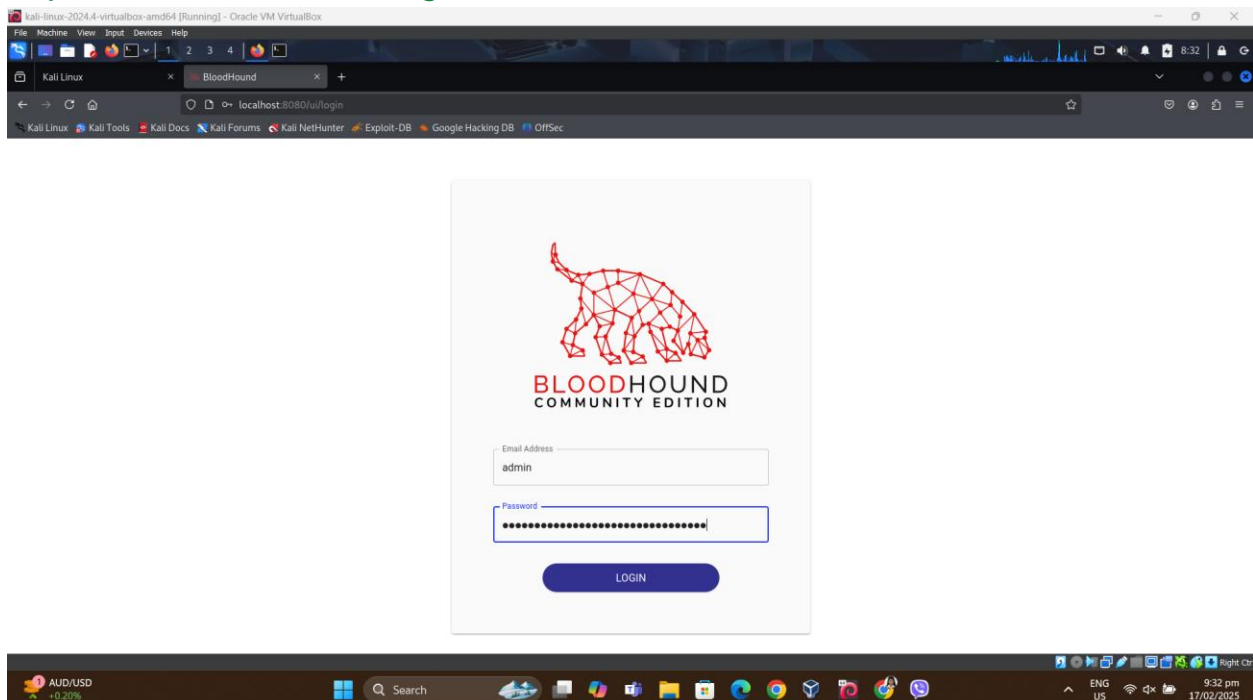
[2025-02-17T13:29:19.8549312Z] level=INFO message=Executing SQL migrations for v5.8.2.0"
[2025-02-17T13:29:19.85958437Z] level=INFO message=Executing SQL migrations for v5.11.0"
[2025-02-17T13:29:19.90283653Z] level=INFO message=Executing SQL migrations for v5.12.0"
[2025-02-17T13:29:19.914295817Z] level=INFO message=Executing SQL migrations for v5.13.0"
[2025-02-17T13:29:19.915959617Z] level=INFO message=Executing SQL migrations for v5.13.1"
[2025-02-17T13:29:19.92680896Z] level=INFO message=Executing SQL migrations for v5.14.0"
[2025-02-17T13:29:19.9272227Z] level=INFO message=Executing SQL migrations for v5.15.0"
[2025-02-17T13:29:19.9481142Z] level=INFO message=Executing SQL migrations for v6.0.0"
[2025-02-17T13:29:19.9517874Z] level=INFO message=Executing SQL migrations for v6.1.0"
[2025-02-17T13:29:19.968417189Z] level=INFO message=Executing SQL migrations for v6.2.0"
[2025-02-17T13:29:19.9715889Z] level=INFO message=Executing SQL migrations for v6.3.0"
[2025-02-17T13:29:19.97816263Z] level=INFO message=Executing SQL migrations for v6.4.0"
[2025-02-17T13:29:28.42913628Z] level=INFO message=#####
[2025-02-17T13:29:28.42939977Z] level=INFO message=#####
[2025-02-17T13:29:28.42934623Z] level=INFO message=# Initial Password Set To: _00rFaPsXUZnFE1UampgTZO9m2tBvsc #
[2025-02-17T13:29:28.42934863Z] level=INFO message=# #
[2025-02-17T13:29:28.42935138Z] level=INFO message=#####
[2025-02-17T13:29:28.43059786Z] level=INFO message=Adding index azuser_tenantid_index to labels AZUser on properties tenantid using native-btree-1.0"
[2025-02-17T13:29:49.862650839Z] level=INFO message=Adding index gp_tenantid_index to labels GPO on properties tenantid using native-btree-1.0"
[2025-02-17T13:29:54.578761503Z] level=INFO message=Adding index azapp_tenantid_index to labels AZApp on properties tenantid using native-btree-1.0"
[2025-02-17T13:29:54.580000000Z] level=INFO message=Adding index aztenantid_name_index to labels AZTenant on properties name using lucene-native-3.0"
[2025-02-17T13:29:53.087656828Z] level=INFO message=Adding index azfunctionapp_name_index to labels AZFunctionApp on properties name using lucene-native-3.0"
[2025-02-17T13:29:54.67172225Z] level=INFO message=Adding index azsaga_system_tags_index to labels AISA on properties system_tags using lucene-native-3.0"
[2025-02-17T13:29:54.6717225Z] level=INFO message=Adding index adocuser_system_tags_index to labels ADUser on properties system_tags using lucene-native-3.0"
[2025-02-17T13:29:54.685772051Z] level=INFO message=Adding index azmscaleout_system_tags_index to labels AZMScaleout on properties system_tags using lucene-native-3.0"
[2025-02-17T13:29:55.09419066Z] level=INFO message=Adding index group_domainid_index to Labels Group on properties domainid using native-btree-1.0"
[2025-02-17T13:29:55.21707252Z] level=INFO message=Adding index ou_tenantid_index to Labels OU on properties tenantid using native-btree-1.0"
[2025-02-17T13:29:55.21707252Z] level=INFO message=Adding index aztenantid_group_name_index to Labels Group on properties system_tags using lucene-native-3.0"

```

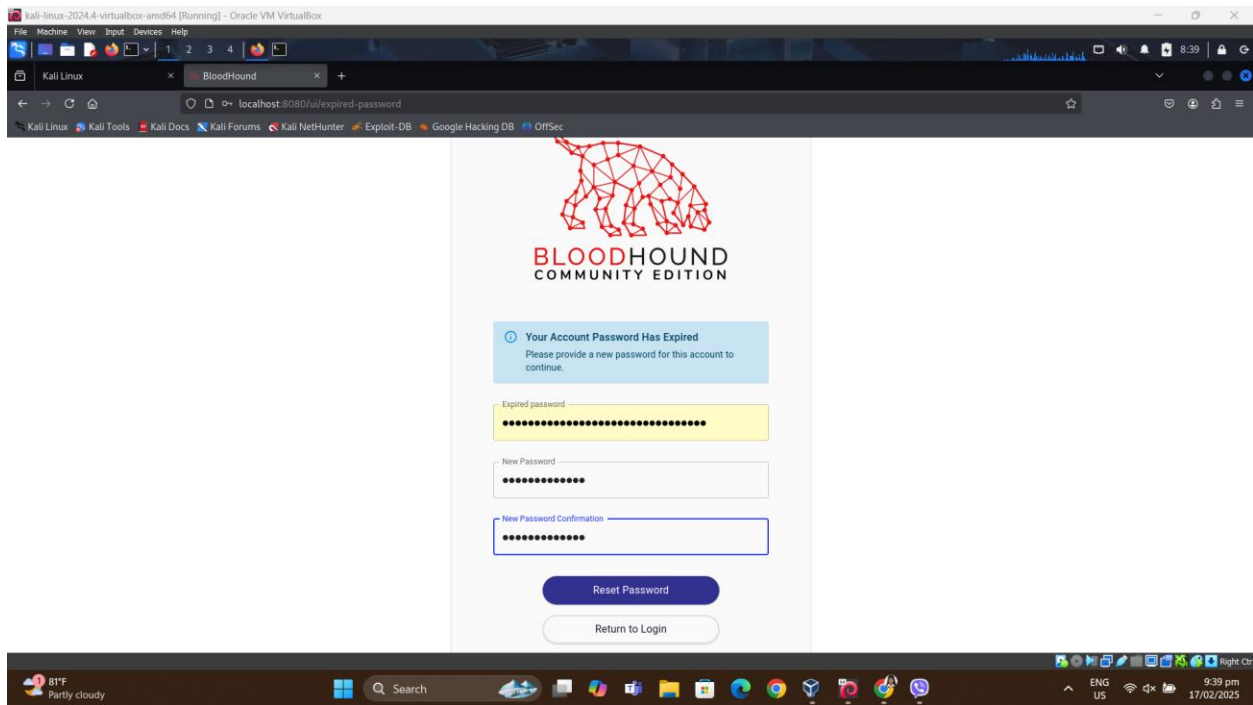
Step 8: Access BloodHound CE Web Interface

Once the containers are running, open your web browser and navigate to:

<http://localhost:8080/ui/login>



The default email address is “admin” and enter the initial password that has been provided. After successfully logging in, you will be asked to create a new password.



Step 10: BloodHound CE Dashboard

Finally, you will be redirected to the BloodHound dashboard, where you can start using the application.

The screenshot shows the BloodHound web interface. The sidebar on the left contains the following navigation links:

- Data Collection**
 - File Ingest (selected)
 - Data Quality
 - Database Management
- Users**
 - Manage Users
- Authentication**
 - SSO Configuration
- Configuration**
 - BloodHound Configuration
 - Early Access Features
- Bottom icons: Document, Magnifying Glass, Person, List

The main content area is titled "File Ingest". It contains the following text:

Upload data from SharpHound or AzureHound offline collectors. Check out our [Getting Started](#) documentation for more information.

Below the text is a table with the following columns: User, Start Time, End Time, Duration, Status, and Status Message. The table is currently empty. At the bottom right of the table, it says "Rows per page: 10 0-0 of 0". Above the table is a blue button labeled "Upload File(s)".