IDA Teams Administrator Guide

Table of Contents

Last updated on July 27th, 2022 — v0.4

1. Prerequisites

After your purchase of IDA Teams licenses, you have received an e-mail that contains links to a download area where you will find:

- an installer for the IDA Teams server (also called the "Hex-Rays Vault server")
- this guide
- an installer for IDA
- an `ida.key`

All those will be necessary, so please go ahead and download them.

You will also need `root` access on the host where you will be installing the server.

2. Installation

This chapter explains how to install two parts of IDA Teams: the vault server, and a client.

We recommend installing a client first, to be able to connect to the server immediately after installation. The very first user to connect to the server becomes the administrator.

2.1. Installing clients

There are 2 Hex-Rays Vault clients:

1. `hv`: a command-line client (which we'll use in this document)
2. `hvui`: a GUI interface to the server

Vault clients are bundled with IDA Teams installers: simply run the IDA installer and follow the instructions. That will install IDA, and the 2 clients next to it.

2.2. Installing the server

The Hex-Rays Vault server can be installed on Linux servers. We have tested it on Debian and Ubuntu, but other major flavors of Linux should be fine too.

To install the server, run the Hex-Rays Vault installer as `root` and follow the instructions (the server will not require `root` permissions; only the installer does.)

TIP If your Linux system is based on `systemd` (e.g., Debian/Ubuntu, Red-Hat, CentOS, …), it is recommended to let the installer create systemd units so that the server will start automatically at the next reboot.

Once the server is installed, it will be necessary to activate its license.

2.2.1. Activating the server license

In order for the Hex-Rays Vault server license to be activated, it must be bound to a Host ID (an Ethernet MAC address.)

From a command prompt, run `/sbin/ifconfig`, and lookup the "ether" address for the network interface through which the server will be accessible.

```
>/sbin/ifconfig
enp4s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        [...snipped...]
        ether bf:e2:91:10:58:d2  txqueuelen 1000  (Ethernet)
        [...snipped...]
```

In this case, our mac address is: `bf:e2:91:10:58:d2`

Go to https://hex-rays.com/vault_activate , and submit both the `ida.key` file and your MAC address. You will then receive

another e-mail with instructions to download the following files:

- `hexvault.crt`
- `hexvault.key`
- `hexvault.lic`

Those need to be copied in the Hex-Rays Vault installation directory. As `root`:

```
>cd /opt/hexvault
>cp .../path/to/hexvault.crt .
>cp .../path/to/hexvault.key .
>cp .../path/to/hexvault.lic .
>chown hexvault:hexvault hexvault.crt hexvault.key hexvault.lic
>chmod 640 hexvault.crt hexvault.key hexvault.lic
```

2.2.2. Creating the initial database

At this point, the server should be ready to run.

CAUTION If your system is already in production and hosts files, skip this section. Using the `--recreate-schema` option as in the example below, will re-create an empty database and lose all history.

On the first install, you will need to initialize the database the server will use:

```
>sudo -u hexvault ./vault_server --config-file hexvault.conf \
                                 --vault-dir ./files \
                                 --recreate-schema
>2022-04-14 14:30:28 Vault Server v1.0 Hex-Rays (c) 2022
>2022-04-14 14:30:28 Database initialized; exiting.
```

2.2.3. Testing the server

Now that the server is installed and has a database to work with, we can test that it works:

```
>sudo -u hexvault ./vault_server --config-file hexvault.conf \
                                 --certchain-file hexvault.crt \
                                 --privkey-file hexvault.key \
                                 --license-file hexvault.lic \
                                 --vault-dir ./files
2022-04-14 14:35:47 Vault Server v1.0 Hex-Rays (c) 2022
2022-04-14 14:35:47 Using a license with 5 seats
2022-04-14 14:35:47 Listening on 0.0.0.0:65433...
```

Good, the server appears to run! (If you are observing more worrying messages than this one, please refer to the troubleshooting section.)

At this point, you may want to either let the server run, or stop it (`Ctrl+C` will do) and restart it using systemd:

```
>systemctl restart hexvault.service
```

...and make sure it runs:

```
>ps aux | grep vault_server
hexvault  58246  0.0  0.0 ...
```

If you don't see a running `vault_server` process, please refer to the `systemd` diagnostic tools (e.g., `journalctl`) for more info.

3. Initial configuration

This chapter explains how to perform the initial configuration of the vault server.

For the sake of the examples below, we'll imagine the following fictional group of users:

- Jane Smith, the department admin/IT head
- Fred Bloggs, senior reverse engineer

In addition, we'll assume:

- the company name is `Acme`
- the Hex-Rays Vault server has been installed on the company's LAN, on the host `hexvault.acme.com`

3.1. Creating the administrator

IMPORTANT The very first user to log into the server becomes the first administrator. S/he can create new administrators and otherwise manage the server.

Once the server is up and running, login to server using a username and password of your choice (`hv` is the vault client utility, it is installed as part of the client package.)

NOTE We will assume Jane installed IDA (and thus `hv`) in `/home/jane/idateams`.

```
>cd /home/jane/idateams
>./hv -hhexvault.acme.com -ujane -psecr3t info

Hex-Rays Vault Server v1
Vault time: 2022-04-14 15:28:03, up since 2022-04-14 15:17:25
License user : Jane Smith, Test IDA Ultimate
License email: jane@acme.com
License: IDAULTTM; 1 users out of 5; expires on 2023-04-05
MAC address: xx:xx:xx:xx:xx:xx
Vault directory: /opt/hexvault/files
Client name: jane *ADMIN*
Client site:
Client host: 127.0.0.1
Client root:
Login time : 2022-04-14 15:28:03
Last active: 2022-04-14 15:28:03
```

TIP Please note that there is no space between the command line switches and values.

Since Jane is the first user to login to the server, the credentials she provided, will be used to create the server's primary administrator.

You can verify that you are the only user by checking the user list:

```
>./hv -hhexvault.acme.com -ujane -psecr3t users

LastActive Adm    Login       License          Email
---------- --- ------------ --------------- ------------
2022-04-14  *  jane          <>
```

You may also add information (like your real name) to your user record by issuing:

```
>./hv -hhexvault.acme.com -ujane -psecr3t user edit jane "Jane Smith" jane@acme.com 1 "" 48-XXXX-XXXX-XX
>./hv -hhexvault.acme.com -ujane -psecr3t users

LastActive Adm    Login       License          Email
---------- --- ------------ --------------- ------------
2022-04-14  *  jane         48-XXXX-XXXX-XX Jane Smith <jane@acme.com>
```

3.2. Useful environment variables

To facilitate using hv, you may consider defining the following environment variables:

```
export VAULT_HOST=hexvault.acme.com
export VAULT_USER=jane
export VAULT_PASS=secr3t
```

After that, you can connect to the server effortlessly. For example, this command will print information about the server and the client:

```
>./hv info

Hex-Rays Vault Server v1
Vault time: 2022-04-14 15:36:29, up since 2022-04-14 15:17:25
...
```

TIP if you login to the server using `hvui` and save the login information in the registry, hv will re-use the saved information. In this scenario, there is no need to set the environment variables.

3.3. Adding users

To be able to connect to the vault server, users need to be added to the server. That can be done with the user add command:

```
>./hv user add fred "Fred Bloggs" fred@acme.com 0 "" 48-XXXX-XXXX-XX
>./hv users

LastActive Adm    Login       License          Email
---------- --- ------------ --------------- ------------
Never          fred         48-XXXX-XXXX-XX Fred Bloggs <fred@acme.com>
2022-04-14  *  jane         48-XXXX-XXXX-XX Jane Smith <jane@acme.com>
```

3.3.1. Setting the new user's password

Then, we need to set the user's password, using the passwd command:

```
>./hv passwd stea1thy fred
```

3.4. Adding groups

To facilitate user management, sometimes it makes sense to make user groups. All users of a group then can be granted or denied access to certain files on the server.

Let's add a few groups:

```
>./hv group add org
>./hv group add analysts
```

Using the groups command, we can see the new groups are still empty:

```
>./hv groups
analysts:
org:
```

We can now add group members:

```
>./hv group edit org jane 1
>./hv group edit org fred 1
>./hv group edit analysts fred 1
>./hv groups
analysts: fred
org: fred jane
```

Groups are especially useful for managing permissions.

4. Management

This chapter explains in detail how to perform regular administrator tasks.

4.1. Managing permissions

If you want to limit access to the files that will be stored on the vault server, you can specify who can access what. By default, the permission table grants all users access to all files:

```
>hv perm get
# The permission for each vault file is determined as the result of applying
# all matching lines, from the beginning of the permission table to the end.
# An empty permission table grants all access to everyone.
# A non-empty permission table starts by denying all access to everyone.
```

You will need to prepare a new permission table and put it into a file. The permission table consists of lines with the following format:

```
ACTION CATEGORY WHO PERM PATH
```

where:

ACTION
: one of "grant" or "deny"

CATEGORY
: one of "user" or "group"

WHO
: name of the user or group to match

PERM
: one of "list", "read", "write"

PATH
: path pattern that the rule is for

Below is a sample permission table:

NOTE We'll assume the server has been in use for a while, and holds some files in the directories `subdir-for-fred/`, `local-secret/`, and `subdir/for/idbs/`.

```
# The permission for each vault file is determined as the result of applying
# all matching lines, from the beginning of the permission table to the end.
# An empty permission table grants all access to everyone.
# A non-empty permission table starts by denying all access to everyone.

# Fred can freely list, read, and modify all files inside "subdir-for-fred"
grant user fred write //subdir-for-fred/

# The "remote" group cannot even see "local-secret":
deny group remote list //local-secret

# The analysts can work on IDBs:
grant group analysts write //subdir/for/idbs/

# Everyone else may read them:
grant user * read //subdir/for/idbs/
```

The permissions have the following order:

- Adding the `read` permission also adds the `list` permission.
- Adding the `write` permission also adds the `list` and `read` permissions.
- Removing the `read` permission also removes the `write` permission.
- Removing the `list` permission also removes the `read` and `write` permissions.

Once the permission table is ready and stored in a file, we can install it:

```
>hv perm set @path/to/permission-file
```

After setting the permissions, it is a good idea to verify them. For example, this is how we can get a full list of files that `fred` can see, with the `rw` or `r-` prefixes, depending on the permissions:

```
>hv perm check fred //
rw //subdir-for-fred/afile
rw //subdir-for-fred/anotherfile
r- //subdir/for/idbs/malware.idb
```

Or we could limit our check to a particular file:

```
>hv perm check fred //local-secret
```

The empty output means that `fred` cannot see `local-secret` even though it exists.

4.2. Backup and restore

Currently, there is no dedicated procedure to back up the vault contents. It can be done by temporarily stopping the vault server and making a copy of the sqlite3 database as well as the files. The server must be stopped only during the backup of the sqlite3 database and then can be immediately restarted. It is ok to let the server run when making copies of the vault files. In the worst case some additional files will get copied in the backup, which normally will not cause problems. Since we never modify vault files but always create new revisions, there is no danger of copying inconsistent data.

Alternatively, it is possible to use sqlite3 backup functionality to make a backup of the database. Vault files can be copied using any Linux command (e.g. rsync or tar).

4.3. Managing vault files

We plan to introduce additional functionalities like:

- obliteration of files
- periodic vault self-verification
- periodic backups
- usage stats

5. hv command reference

This chapter explains the syntax, and details about common hv commands

5.1. Adding users

```
>hv user add USERNAME REALNAME EMAIL IS_ADMIN NOTES LICENSE_ID
```

where:

USERNAME
: is the user's login name of your choice. It may contain only alphanumeric symbols or underscore, max 16 characters. The first symbol cannot be a digit.

REALNAME
: is the user's real name

EMAIL
: is the user's email address

IS_ADMIN
: is 0 or 1. 1 means that the user has admin rights.

NOTES
: is an arbitrary text about the user. it is visible to all users.

LICENSE_ID
: is the user's license id. It has the following form: 48-XXXX-XXXX-XX, where X is a hexadecimal number.

You can add as many users as your license seat count specifies. Once this limit is reached, it is not possible to add new users.

5.2. Setting a user's passwords

```
>hv passwd PASSWORD USERNAME
```

where:

PASSWORD
: is the new password

USERNAME
: is the user's login name. If omitted, this command sets the password of the current user.

Users can use it to also set their own password.

5.3. Editing a user

```
>hv user edit USERNAME REALNAME EMAIL IS_ADMIN NOTES LICENSE_ID
```

where the meaning of the various fields, is the same as in the user add command.

5.4. Deleting a user

```
>hv user del USERNAME
```

Deleting a user does not interrupt his existing connections to the server. However, all of his sites are deleted.

Normally, the user's worklists must be deleted before deleting the user. This is done to protect against accidental deletion of an actively working user. To automatically delete the user's worklists, use the -f switch:

```
>hv user del -f USERNAME
```

An admin can delete any user, excluding himself:

5.5. Showing user list

```
>hv users
```

Sample output:

```
LastActive Adm    Login       License          Email
---------- --- ------------ --------------- ------------
1970-01-01     user1        48-1111-2222-33 Simple User <simple@example.com>
1970-01-01  *  user2        48-1111-2222-33 <very.common@example.com> User notes...
1970-01-01     user5        48-1111-2222-33 <fully-qualified-domain@example.com>
1970-01-01     user7        48-1111-2222-33 <x@example.com>
1970-01-01     user9        48-1111-2222-33 <test/test@test.com>
1970-01-01     userB        48-1111-2222-33 <example@s.example>
1970-01-01     userD        48-1111-2222-33 Old Pal <user%example.com@example.org>
```

Columns

LastActive
: The last time the user issued a request to the server

Adm
: A star in this column denotes an administrator

Login
: The user's login name

License
: The license ID

Email
: The user's email address and additional notes

5.6. Adding groups

```
>hv group add GROUPNAME
```

where:

GROUPNAME
: the group name of your choice. It may contain only alphanumeric symbols or underscore, max 16 characters. The first symbol cannot be a digit.

5.7. Editing groups (i.e., add, or remove group members)

```
>hv group edit GROUPNAME USERNAME ADD
```

where:

GROUPNAME
the name of an existing group

USERNAME
the name of an existing user

ADD
1 means to add to the group; 0 means to remove from the group

5.8. Deleting groups

```
>hv group del GROUPNAME
```

where:

GROUPNAME
the name of an existing group

Deleting a non-empty group is not possible, you have to remove its members first.

5.9. Showing contents of a group

```
>hv group show GROUPNAME
```

where:

GROUPNAME
the name of an existing group

5.10. Listing groups

```
>hv groups
```

6. Troubleshooting

This chapter explains how to solve typical problems with the vault server.

6.1. Connection issues

By default, the vault server listens on the TCP port 65433 on all interfaces. Please ensure that this port is enabled in your firewalls.

The vault server uses secure TLS connections with the clients. The TLS layer requires the certificate (.crt) and private key (.key) files. Usually, they are attached to the email message with the activation information.

6.2. Lost admin password

A lost admin password can be reset by following these steps:

- Stop the running server
- Launch the server with the `--set-admin` command line switch
- Start the server

In practice it may look like this:

```
>systemctl stop hexvault.service
>vault_server --config-file hexvault.conf --set-admin USERNAME:PASSWORD
>systemctl start hexvault.service
```

The uppercase USERNAME and PASSWORD placeholders should be replaced by the desired values. The user name and the password are separated by a colon.

The specified user must exist. If sh/e was not an admin before, s/he will be promoted to an admin by this command.

TIP If you do not know any valid users of the vault, use the `sqlite3` command line utility to list the users. They are stored in the `users` table.

6.3. Site verification

The following command:

```
>hv md5 PATH REVISION
```

can be used to retrieve MD5 checksums of the specified files.

PATH
path pattern to retrieve checksums from

REVISION
optional file revision. If not specified, the checksum of the last revision is reported

6.4. The server complains about a "world-accessible" file, and exits

The following files shouldn't be readable by everyone on the system, but only by `root` and `hexvault`:

- `hexvault.conf`: this file file holds the connection string to the database the server will use, and might contain credentials.
- `hexvault.crt`: the certificate chain
- `hexvault.key`: the private key file
- `hexvault.lic`: the license file

As a precaution, the Hex-Rays Vault server will refuse to start if these files are readable by unauthorized users.

Please make sure they:

- have `hexvault:hexvault` ownership: `chown hexvault:hexvault hexvault.crt hexvault.key hexvault.lic hexvault.conf`
- are not world-accessible: `chmod chmod 640 hexvault.crt hexvault.key hexvault.lic hexvault.conf`

6.5. Licensing

The hexvault.lic file is tied to the MAC address of the first network interface. If they do not match, the server will not start. To change the MAC address, please contact support@hex-rays.com

6.6. Restoring from backups

There are no special precautions to take: restoring the sqlite3 database and vault files from a backup should be enough.