CAA 23-24

Lab #1

20-09-2023

1 Introduction

The goal of this lab is to use the Vault software[1] to manage a PKI in a company infrastructure. Vault is a software that provides the management and storage of secret information, allows to do precise access control, and has further advanced functionalities like certificate and one-time passwords generation. In particular, Vault is great to **centralize** secrets in a company. It allows easy access revocation as well as auditing (who accessed what and when). In this lab, we are going to follow some basic tutorials about Vault and use it in a industrial scenario.

2 Submission

You have to provide the following:

- A **script** setting-up Vault for the scenario described. **Do not forget to provide as well the policy files.** For steps that are not scriptable, you can explain what you do in a comment. If you prefer, you can also describe what you did in a report (with screenshots).
- A **report** in which you answer all the questions asked.
- Provide all the **certificates** and all the **private keys** that you generated in a zip.
- The lab is due on the **3rd of October** at 23h55.

3 Installation and Introduction

You can install Vault on most operating systems. Follow the installation tutorial `https://learn.hashicorp.com/tutorials/vault/getting-started-install` to install it on your platform. You can interact with Vault in three manners: with the command line interface (CLI) (which is what will mostly put forward in this lab), with API calls using curl[2], and with a Web UI[3].

4 Starting the Vault Server

Vault can be executed in `dev` mode and in production mode. The `dev` mode is insecure and not recommended. In this lab, launch the server in **production mode**. Your company has **6 security officers** and the server needs to be unsealed by at least **two security officers**. For simplicity, we will interact with the Vault server using HTTP even though it is **not** recommended.

4.1. What is the goal of the unseal process. Why are they more than one unsealing key?

4.2. What is a security officer. What do you do if one leaves the company?

[1] `https://www.vaultproject.io`
[2] If interested, read about it `https://learn.hashicorp.com/tutorials/vault/getting-started-apis`
[3] If interested, read about it `https://learn.hashicorp.com/tutorials/vault/getting-started-ui`

5 Policies

Read about policies in Vault: https://learn.hashicorp.com/tutorials/vault/policies. Create an **admin** policy that will be used instead of the root policy.

6 PKI

We are now going to manage a small PKI for the HEIG-VD: https://learn.hashicorp.com/tutorials/vault/pki-engine

- Update the admin policy so that it can handle PKI.
- Create an admin token.
- Follow the PKI tutorial to create an `HEIG-VD Root` certificate, an `HEIG-VD Intermediate` certificate.
- Create a role to manage the website `intra.heig-vd.ch` and **only this website**.
- Create a policy `intra` that is **only** dedicated to obtaining certificates for `intra.heig-vd.ch`.
- Generate a certificate for `intra.heig-vd.ch`.
- Generate a wildcard certificate for all the `heig-vd.ch` subdomains.

6.1. Why is it recommended to store the root certificate private key **outside of Vault** (we did not do this here)?

6.2. Where would you typically store the root certificate private key?

6.3. What do you need to do in Vault to store the root certificate private key outside of Vault?

6.4. How is the intermediate certificate private key secured?

6.5. In the certificate for `intra.heig-vd.ch`, what is its duration of validity? What is the name of its issuer?

6.6. What do you need to do concretely for the `intra.heig-vd.ch` certificate to be accepted by browsers?

6.7. What is a wildcard certificate? What are its advantages and disadvantages?

7 Users

Finally, we are going to create a user using the `userpass` method: https://www.vaultproject.io/docs/auth/userpass.

- Create a user `toto` with password `titi` that can **only** obtain certificates for `intra.heig-vd.ch`
- Create a user `admin` with password `admin` that has the admin policy.
- Try doing admin tasks with the `toto` user and show a screenshot of what happens.

8 Final Questions

8.1. How is the *root key* and the *encryption key* used to secure Vault?

8.2. What is *key rotation* and when is it done?

8.3. What can you say about the confidentiality of data in the storage backend? How is it done?

8.4. What can you say about the security of Vault against an adversary that analyses the memory of the server that runs Vault?