**Lab 3 – Sécurisation et lookups**

1. Placer des variables confidentielles dans un fichier **secret.yaml**:

secret: |

Ceci est le message chiffré sur plusieurs lignes

Voici la seconde ligne

1. Créer un fichier contenant les mots de passe :

echo "testtest" > ~/.vault\_passwords.txt ;

chmod 600 ~/.vault\_passwords.txt

1. Chiffrer le fichier secret.yaml avec le mot de passe contenu dans l'endroit protégé ~/.vault\_passwords.txt :

ansible-vault encrypt secret.yml --vault-password-file ~/.vault\_passwords.txt

Vous pouvez afficher le contenu du secret.yaml après cette commande pour vérifier qu’il est bien crypté.

1. Ecrire un playbook **test-vault.yaml** pour afficher le contenu de la variable **secret** du secret.yaml.

Adhoc:

> ansible-vault view --vault-id @prompt secret.yml

Playbook:

---

- hosts: localhost

tasks:

- name: Read secret file

include\_vars: "secret.yml"

- name: display secret value

debug:

msg: "{{ secret }}"

1. Exécuter le playbook créé en indiquant le fichier du mot de passe de vault :

ansible-playbook test-vault.yml --vault-password-file ~/.vault\_passwords.txt

1. Utiliser le fichier csv fourni pour afficher via un playbook, exécuté sur le localhost, le mot de passe de l’utilisateur web\_server.

---

- hosts: localhost

tasks:

- name: Read secret file

include\_vars: "secret.yml"

- name: display secret value

debug:

msg: "{{ secret }}"

- name: write the secret to a csv file

copy: content="{{ secret }}" dest=debug.csv