**Lab 7: Ansible Vault for Secure Secrets Management\*\***

### Step 1: Create an Encrypted Variable File

* Create an Ansible Vault encrypted variable file that will store your sensitive data. You can do this using the ansible-vault create command:

| ansible-vault create sensitive\_data.yml |
| --- |

Inside the sensitive\_data.yml file, define your sensitive variables, for example:

yaml

| db\_password: my\_secret\_password api\_key: my\_api\_key |
| --- |

### Step 2: Edit the Encrypted Variable File

| ansible-vault edit sensitive\_data.yml |
| --- |

### Step 3: Create a Playbook That Uses Encrypted Variables

Now, you can create a playbook that uses the encrypted variables from the sensitive\_data.yml file.

| --- - name: Use Encrypted Variables  hosts: localhost # You can specify the target hosts as needed  gather\_facts: no # Disable gathering facts   tasks:  - name: Load Encrypted Variables  include\_vars:  file: sensitive\_data.yml  name: sensitive\_data # Define a variable name to access the encrypted data   - name: Display Encrypted Variables  debug:  var: sensitive\_data |
| --- |

In this playbook:

* include\_vars task is used to load the encrypted variables from sensitive\_data.yml into the sensitive\_data variable.
* debug task displays the content of the sensitive\_data

### Step 4: Run the Playbook

| ansible-playbook my\_playbook.yml --ask-vault-pass |
| --- |

### 

### 

To run the playbook, use the ansible-playbook command: