LESSON 10

site.yml

```
$ ansible-vault create vault.yml
db_password: "{{ vault_db_password }}"
no_log: true
```

YAML

Vault & Windows

Learn it all @MyWebUniversity



A FREE MYWEBUNIVERSITY COURSE

ANSIBLE & DEVOPS

LESSON 10

Secrets, Privilege and Windows Hosts

ansible-vault, no_log, become, managing Windows with WinRM and win_ modules

ansible-vault

terminal

```
$ ansible-vault create group_vars/db/vault.yml
$ ansible-vault edit group_vars/db/vault.yml
$ cat group_vars/db/vault.yml
$ANSIBLE_VAULT;1.1;AES256
623138633635626130383 6...
$ ansible-playbook site.yml --ask-vault-pass
```

- Never commit passwords in plain text. ansible-vault encrypts a whole file, or a single …
- Edit encrypted files with ansible-vault edit, and supply the password when running with …

01

A Clean Vault Pattern

group_vars/db/vars.yml

- db_user: school
- db_password: "{{ vault_db_password }}"

group_vars/db/vault.yml 🔒

- vault_db_password: S3cret!
- (encrypted with AES-256)

- Keep two files per group: vars.yml with normal variables that point to vault_ variables, …
- Anyone can still search for which variables exist without decrypting anything. Add no_log …

02

become and Privilege

db.yml

```yaml
- name: Create application database
  community.postgresql.postgresql_db:
    name: school
  become: true
  become_user: postgres

- name: Create database user
  community.postgresql.postgresql_user:
    db: school
    name: "{{ db_user }}"
    password: "{{ db_password }}"
  become: true
  become_user: postgres
  no_log: true
```

- become runs tasks with elevated rights, by default with sudo as root. Set it per play or ...
- Grant only what is needed: become at task level is safer than everywhere.

03

Managing Windows

group_vars/windows.yml

```
ansible_connection: winrm
ansible_port: 5986
ansible_winrm_transport: ntlm
ansible_winrm_server_cert_validation: validate
ansible_user: CORP\\ansible-svc
ansible_password: "{{ vault_win_password }}"

# ansible windows -m ansible.windows.win_ping
```

- Ansible manages Windows over WinRM, or SSH on newer systems. The control node still runs …
- win_ping tests the connection, just like ping for Linux.

04

Windows Modules

iis.yml

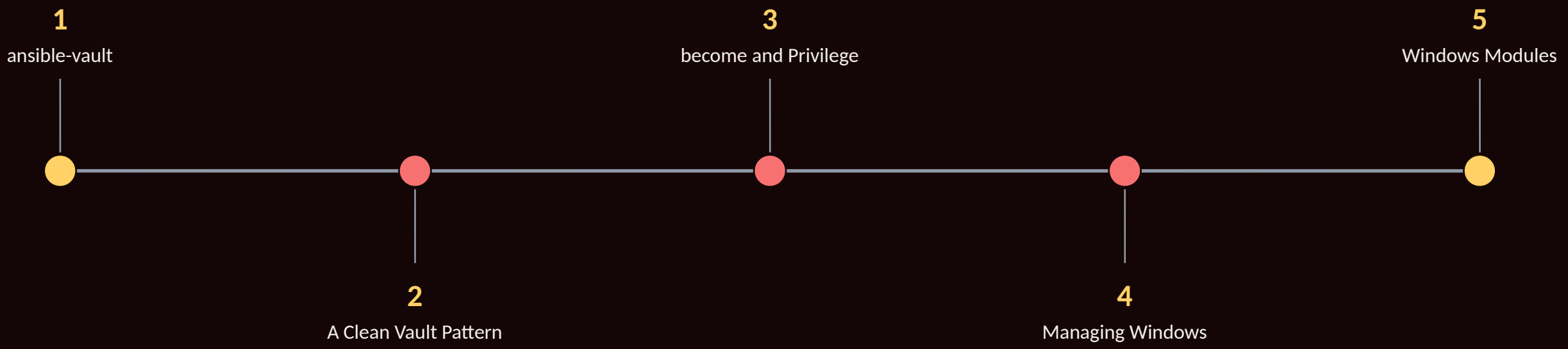
```
- hosts: windows
  tasks:
    - name: Install IIS
      ansible.windows.win_feature:
        name: Web-Server
        include_management_tools: true

    - name: Install security updates
      ansible.windows.win_updates:
        category_names: [SecurityUpdates]
        reboot: true
```

- The ansible.windows and community.windows collections provide win_feature for roles and …
- One playbook can patch and configure hundreds of Windows servers.

05

Lesson Map


1
ansible-vault
2
A Clean Vault Pattern
3
become and Privilege
4
Managing Windows
5
Windows Modules

Sources and Further Reading

terminal

```
$ ansible-vault create group_vars/db/vault.yml
$ ansible-vault edit group_vars/db/vault.yml
$ cat group_vars/db/vault.yml
$ANSIBLE_VAULT;1.1;AES256
623138633635626130383 6...
$ ansible-playbook site.yml --ask-vault-pass
```

ANSIBLE & DEVOPS · 10

db.yml

```
- name: Create application database
  community.postgresql.postgresql_db:
    name: school
  become: true
  become_user: postgres

- name: Create database user
  community.postgresql.postgresql_user:
    db: school
    name: "{{ db_user }}"
    password: "{{ db_password }}"
  become: true
  become_user: postgres
  no_log: true
```

Thank you for watching

MyWebUniversity.com

Free technical education since 2000 — English and Dari

@MyWebUniversity · @MyWebUniversity-Dari