Red Hat Certified Specialist in Security: Linux

Content

1. Red Hat Ansible Engine Management

- Install and configure **Ansible Engine** on a control node.
- Set up managed nodes and configure simple inventories.
- Run playbooks on specified nodes for system management.

2. Automation Controller Access

- Create and restrict an inventory for a specific automation controller user.
- Restrict credentials or projects for user access.
- Allow users to create and launch templates.

3. Intrusion Detection

- Install and configure **AIDE** to monitor critical system files for changes.

4. Encrypted Storage Configuration

- Encrypt/decrypt storage using **LUKS** and ensure persistence with **NBDE**.
- Change passphrases for encrypted storage.

5. USB Device Restriction

- Install **USBGuard** and write policy rules to manage USB devices.

6. System Login Security (PAMs)

- Set password quality standards and failed login policies.
- Modify **PAM** configuration files and parameters.

7. System Auditing

- Write rules to log specific auditable events.
- Enable prepackaged rules and generate audit reports.

8. SELinux Configuration

- Enable **SELinux** and analyze violations for corrective actions.
- Map and restrict user activities using **SELinux**.

9. Security Compliance (OpenSCAP)

- Install **OpenSCAP** and scan hosts for security compliance.
- Tailor and apply security policies with customized remediation playbooks.