Lab A4 – Privilege Delegation and Administrative Hardening on RHEL

Ayoub Zouargui
Master 1 – Networks and Embedded Systems
University of Algiers 1 (2025–2026)
https://github.com/AyoubSecurity

Objective

The objective of this lab is to configure secure privilege delegation using `sudo` on Red Hat Enterprise Linux. The lab demonstrates how administrative access can be granted without direct root usage, while enforcing accountability, auditability, and the principle of least privilege.

Lab Environment

Operating System: Red Hat Enterprise Linux

Machine: Single RHEL administrative workstation

Users: root, ayoub.admin, devuser1

Step 1: Verification of Existing Sudo Permissions

```
sudo -l
```

This command was used to verify which commands each user is authorized to execute with elevated privileges.

Step 2: Full Administrative Privileges for ayoub.admin

```
/etc/sudoers entry:
ayoub.admin ALL=(ALL) ALL
```

This configuration grants unrestricted administrative access via sudo while preserving logging and authentication.

Verification Output

```
User ayoub.admin may run the following commands on localhost:
    (ALL) ALL
    (ALL) ALL
```

Summary: The user `ayoub.admin` is authorized to execute any command as any user through sudo.

Step 3: Restricted Privileges for devuser1

```
/etc/sudoers entry:
devuser1 ALL=(root) /usr/bin/systemctl status
```

This configuration limits the user to a single read-only administrative command.

Verification Output

```
User devuser1 may run the following commands on localhost:
    (root) /usr/bin/systemctl status
```

Summary: The user `devuser1` is restricted to viewing service status and cannot modify system state.

Security Observations

Administrative privileges are explicitly defined and not implicit

Sudo enforces authentication and command-level control

Privilege escalation risks are reduced through restriction

All privileged actions remain auditable

Skills Demonstrated

Secure sudo configuration using `visudo`

Fine-grained privilege delegation

Verification of administrative permissions

Application of least-privilege principles

Linux system hardening fundamentals

Professional Relevance

The configurations implemented in this lab reflect real-world enterprise Linux administration practices, where direct root access is avoided and privileges are carefully delegated to minimize security risks.