Lab A1: User, Group, and Privilege Management on Red Hat Enterprise Linux

Objective

The objective of this lab is to practice fundamental system administration tasks related to user management, group-based access control, and privilege delegation on Red Hat Enterprise Linux (RHEL). The lab focuses on applying enterprise security principles such as least privilege, accountability, and access auditing.

Lab Environment

The lab was conducted on the following environment:

Operating System: Red Hat Enterprise Linux

Primary Node: `rhel-admin`

Optional Secondary Node: `rhel-server1`

Access Method: Local console and SSH

All administrative tasks were performed using root privileges or sudo where appropriate.

Enterprise Context

In enterprise environments, Linux systems host critical services and are accessed by users with different operational roles. Direct root access is typically restricted, and privileges are delegated using role-based access control. This lab simulates such an environment by creating multiple user roles and enforcing controlled administrative access.

Tasks Performed

User and Group Management

Dedicated groups were created to represent operational roles:

`sysadmins`

`netops`

`devops`

Users were created and assigned to their respective groups based on responsibility. Each user was provided with a dedicated home directory and a standard login shell.

Password Policy Enforcement

Password aging policies were configured to enforce security best practices. Maximum password age, minimum password age, and warning periods were defined globally and applied to existing users.

Privilege Delegation Using sudo

Privilege escalation was configured using drop-in sudoers files under `/etc/sudoers.d/`. Full administrative access was granted only to the `sysadmins` group. Restricted command-level sudo access was configured for the `netops` group to allow network-related operations without granting full root privileges.

Account Locking and Access Control

User accounts were locked and unlocked to simulate incident response scenarios, such as compromised credentials or inactive accounts.

Default User Environment Hardening

Default shell settings were configured to enforce secure file creation permissions and improve command history auditing for newly created users.

Verification and Auditing

User access and authentication activity were verified using standard Linux auditing commands, including login history and failed authentication tracking. Configuration correctness was validated by testing both authorized and unauthorized privilege escalation attempts.

Screenshots

The following screenshots were captured as evidence of successful configuration and validation:

User group membership verification

Successful sudo execution for authorized users

Denied sudo access for restricted users

Password aging policy verification

```
root@localhost:/home/ayoubsco/Desktop# id ayoub.admin
uid=1001(ayoub.admin) gid=1004(ayoub.admin) groups=1004(ayoub.admin),1001(sysadmins)
```

Figure 1: Verification of administrative user group membership

```
root@localhost:/home/ayoubsco/Desktop# su - ayoub.net
Last login: Tue Dec 23 15:20:28 CET 2025 on pts/1
ayoub.net@localhost:~$ sudo nmcli device status
[sudo] password for ayoub.net:
DEVICE  TYPE      STATE                   CONNECTION
enp0s3  ethernet  connected               enp0s3
lo      loopback  connected (externally)  lo
```

Figure 2: Successful sudo command execution by authorized user

Lessons Learned

This lab demonstrated the importance of structured user management and controlled privilege delegation in Linux systems. Implementing role-based access and enforcing password policies significantly reduces the attack surface while maintaining operational efficiency.

Conclusion

Through this lab, enterprise-grade user and privilege management practices were implemented and validated on Red Hat Enterprise Linux. These configurations form the foundation for secure system administration and are essential in production environments.

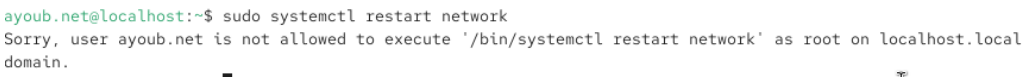

Figure 3: Denied sudo access for restricted user