Chapter 9: Security & Access Control

1. Why Security Matters in Linux (Interview Context)

Linux is a **multi-user and network-connected operating system**.
Security ensures:

- Only authorized users access the system
- Applications run with minimum required privileges
- System files remain protected
- Damage is contained if something goes wrong

Interview insight:

Linux security is based on layers, not a single control.

2. su vs sudo (VERY IMPORTANT)

su (Switch User)

Definition

`su` allows switching to another user account (usually root).

Example:

```
su -
```

Characteristics:

- **Requires target user’s password**
- **Full root shell**
- **No command-level logging by default**

sudo (Superuser Do)

Definition

`sudo` allows a user to execute specific commands with elevated privileges.

```
sudo systemctl restart nginx
```

Characteristics:

- **Requires user’s own password**
- **Fine-grained access control**
- **Commands are logged**

---

su vs sudo Comparison

Feature	su	sudo
Password	Target user	Current user
Granularity	Full access	Command-based
Logging	Limited	Yes
Security	Lower	Higher

Interview line:

sudo is safer than su because it provides controlled privilege escalation.

---

3. SSH (Secure Shell)

What Is SSH?

Definition

SSH is a secure protocol used to access remote systems over a network.

Default port:

- 22

Why SSH Is Secure

- Encrypted communication
- Prevents eavesdropping
- Supports key-based authentication

Interview insight:

SSH is the primary way to manage Linux servers remotely.

---

4. Securing SSH (Very Common Interview Question)

Best Practices

- **Disable root login**
- **Use key-based authentication**
- **Change default port (optional)**
- **Limit user access**
- **Use firewall rules**

Key configuration file:

```
/etc/ssh/sshd_config
```

Interview line:

SSH security is improved by disabling root login and using keys.

---

5. Firewall in Linux

What Is a Firewall?

Definition

A firewall controls incoming and outgoing network traffic based on rules.

Purpose of Firewall

- Block unauthorized access
- Allow required services only
- Protect against network attacks

Common Firewall Tools

- iptables
- firewalld
- ufw

Interview insight:

Firewalls enforce network-level security.

---

6. Restricting User Access

Common Techniques

- Strong passwords
- Group-based access
- sudo rules
- File permissions
- SSH access control

Interview line:

Linux access control is achieved using users, groups, permissions, and sudo.

---

7. PAM (Pluggable Authentication Modules)

Definition

PAM provides a flexible authentication framework for Linux.

What PAM Controls

- User login
- Password policies
- Authentication rules

Configuration directory:

```
/etc/pam.d/
```

Interview explanation:

PAM allows administrators to define authentication behavior centrally.

---

8. SELinux (Security-Enhanced Linux)

What Is SELinux?

Definition

SELinux is a mandatory access control (MAC) system that restricts what processes can do.

Why SELinux Exists

- Prevents compromised applications from harming the system
- Adds an extra security layer beyond permissions

Interview insight:

SELinux enforces security policies even for root processes.

---

9. SELinux Modes (VERY IMPORTANT)

Enforcing

- Policies are enforced
- Violations are blocked

Permissive

- Policies are logged
- No blocking

Disabled

- SELinux is off

Interview line:

Enforcing blocks, permissive logs, disabled turns SELinux off.

---

10. AppArmor vs SELinux

AppArmor

- Path-based
- Easier to configure
- Used by Ubuntu

SELinux

- Label-based
- More powerful
- Used by RHEL-based systems

Comparison Table

Feature	SELinux	AppArmor
Policy type	Label-based	Path-based
Complexity	High	Lower
Default distro	RHEL	Ubuntu

Interview line:

SELinux is stricter; AppArmor is simpler.

---

11. Real-Life Production Scenarios

Scenario 1: Service Not Starting

- Check file permissions
- Check SELinux logs
- Temporarily set permissive mode

Scenario 2: User Cannot SSH

- Check SSH service
- Check firewall
- Check user permissions
- Check SELinux

Scenario 3: Application Access Denied

- Permissions look correct
- SELinux blocking access

Interview insight:

If permissions look fine, always check SELinux.

Chapter 9: Interview Takeaways

After this chapter, you should confidently explain:

- su vs sudo
- SSH and SSH security
- Firewall purpose
- User access restriction
- PAM basics
- SELinux concepts and modes
- AppArmor vs SELinux
