Fedora's default security is strong, but OS hardening is essential to reduce the attack surface for production or high-security environments.

1. Account and Access Hardening

- **Enforce Strong Passwords:** Use the authselect utility to configure password requirements (length, complexity) and lockout policies in `/etc/security/faillock.conf`.
- **Disable Root Login:** Ensure the root account is locked and all administrative tasks are performed via `sudo`. Check `/etc/ssh/sshd_config` to ensure `PermitRootLogin no` is set.
- **Apply Principle of Least Privilege:** Audit the **wheel** group frequently. Remove any users who do not strictly require administrative access using `sudo gpasswd -d username wheel`.

2. Network and Firewall Security

- **Strict Firewall Zones:** Use **firewalld** to move interfaces into the `drop` or `block` zones by default, only opening specific ports in the `public` or `home` zones.
  - Command: `sudo firewall-cmd --set-default-zone=drop`
- **Disable Unused Services:** Identify unnecessary background services with `systemctl list-unit-files --state=enabled` and disable them using `sudo systemctl disable --now <service>`.
- **SSH Hardening:** Beyond disabling root login, switch to **Key-Based Authentication** only and disable password-based logins by setting `PasswordAuthentication no` in the SSH configuration.

3. File System and Kernel Security

- **Maintain SELinux:** Never disable SELinux. Use `sestatus` to confirm it is in `enforcing` mode. If an application is blocked, write a custom policy rather than disabling the entire security layer.

- **Partitioning:** Use separate partitions for `/home`, `/var`, and `/tmp`. Mount `/tmp` with `nodev`, `nosuid`, and `noexec` options in `/etc/fstab` to prevent scripts from executing in temporary directories.
- **Enable Automatic Updates:** In 2026, it is standard to use dnf-automatic to ensure security patches are applied immediately without manual intervention.

4. Auditing and Monitoring

- **Configure Auditd:** Use the Linux Audit Framework to track changes to sensitive files like `/etc/passwd` or `/etc/shadow`.
- **Centralized Logging:** Forward system logs to a remote, secure log server to prevent an attacker from deleting evidence of an intrusion on the local machine.

~Formatted with the help of gemini 3 pro.