

SELinux (Security-Enhanced Linux)

- **What it is:**

- A Linux security module developed by the US National Security Agency (NSA).
- Uses Mandatory Access Control (MAC) → strict rules about what processes, users, and applications can access.

- **How it works:**

- Even if you are root (superuser), SELinux policies can restrict what you can do.
- For example, a web server may only be allowed to read `/var/www/html` files, not `/etc/passwd`.

- **Modes:**

1. **Enforcing** → Policies are applied (strict mode).
2. **Permissive** → Violations are logged but not blocked.
3. **Disabled** → SELinux is turned off.