Task 14: Linux Server Hardening & Secure Configuration

11/02/2026

ABISIN RAJ

Since I’m using Fedora as my daily driver I’ll use Fedora tools . Fedora defaults to difficult tools than ubuntu

Security Checklist

- ☑ ~~System updates~~
- ☑ ~~Review User Access~~
- ☑ ~~SSH Security~~
- ☑ ~~Configure Firewall~~
- ☑ ~~Disable Unused Services~~
- ☑ ~~Check Logs for Suspicious Activity~~
- ☐

Security configuration summary

Automatic system updates - It is used to perform full system upgrade to patch known vulnerabilities ,using dnf on fedora, apt for ubuntu. Configure dnf-automatic to auto-install updates. Use sudo systemctl edit dnf-automatic.timer to edit when the system should be updated.
User management - Verified only administers have sudo access via wheel group and verified that only authorized users has shell access. SSH Configuration : Edited /etc/ssh/sshd_config to block root login.Access is now restricted to SSH keys only.
Network security - My default firewall is firewalld sometimes uses ufw, current pollicy is firewall is active and enabled on boot. The default policy is to deny all incoming traffic, with exceptions explicitly made only for:SSH (22) and HTTP/HTTPS (80/443)
Disable unused Service : Listed all running services using systemctl, Disabled unnecessary services to reduce attack surface and to save battery
Logging - Verified system integrity by checking file permissions on critical files like /etc/sahdow/ and checked journalctl logs to confirm no unauthorized access made

Commands used today

sudo dnf install dnf-automatic
sudo ss -tulpn
grep '^wheel' /etc/group
sudo firewall-cmd --state
systemctl list-unit-files --state=enabled
sudo systemctl stop service_name
sudo systemctl disable service_name
ls -l /etc/shadow