SSH Hardening på Linux server för Linux- och Windows klient (Deb 13)

Bakgrund: Att säkra SSH på en server är en av de viktigaste bitarna för att skydda sig mot lösenordsattacker. Autentisering flyttas från lösenord till genererade nycklar.

Steg 1: Konfiguration

I servern, stå i användarkatalogen ~ och skapa katalog .ssh med fil authorized_keys

Sätt rättigheter
→ 700 .ssh
→ 600 authorized_keys

! säkerställ att användaren står som user- och group owner
→ chown användare:användare fil- och katalognamn

Windows
Generera nyckel på Windows 10/11 dator
→ I CMD → ssh-keygen -t ed25519 → klicka "enter" för alla steg

Detta kommer att generera en privat och publik nyckel. Filsökväg visas under skapandet.

Linux
ssh-keygen -t ed25519

Privat och publik nyckel ska finnas under /home/användare/.ssh/

Windows
Använd scp C:\Users\ANVÄNDAREl\.ssh\id_ed25519.pub
användare@ipaddress:/home/ANVÄNDARE/.ssh/pubkey

Linux
Använd ssh-copy-id användare@ipaddress. Publik nyckel hamnar direkt i filen authorized_keys. Lösenord för servern där nyckeln placeras behöver skrivas in i prompten som visas efteråt.

Redigera sedan filen /etc/ssh/sshd_config/
→ PubKeyAuthentication yes
→ AuthorizedKeysFile .ssh/authorized_keys
→ PasswordAuthentication no

Applicera ändringar med → systemctl restart ssh

Steg 2: Verifiering

Testa att använda SSH mot servern användarnamn@ipaddress, acceptera fingerprints första gången. Du ska få tillgång utan att skriva in lösenord. Logga ut och testa igen, lösenord ska ej krävas. Verifiera gärna med en annan dator. Där ska inloggningsförsöket visa Permission Denied.