

## 1.4 - SSH hærkning og verifikation

### □ Information

Formålet med denne øvelse er at hærde SSH-konfigurationen på jumphosten, så password-login deaktiveres, og kun offentlig nøgle accepteres.

Øvelsen har fokus på korrekt konfigurationsmetode og verifikation af den effektive SSH-konfiguration.

### □ Deløvelser – SSH-hærkning og verifikation

#### 1□ Hærkning: Deaktiver password-login i SSH (Match all)

På Ubuntu kan SSH-konfigurationen blive overskrevet af inkluderede filer i

`/etc/ssh/sshd_config.d/`, herunder cloud-init-konfigurationer. Derfor må password-login ikke deaktiveres direkte i `/etc/ssh/sshd_config` alene.

I stedet oprettes en dedikeret hardening-konfigurationsfil, som eksplicit overskriver alle tidligere indstillinger ved hjælp af "Match all".

1. Opret en ny SSH-hardening-fil: `sudo nano /etc/ssh/sshd_config.d/99-hardening.conf`

2. Indsæt følgende indstillinger i filen:

```
Match all
PasswordAuthentication no
KbdInteractiveAuthentication no
ChallengeResponseAuthentication no
PubkeyAuthentication yes
PermitRootLogin no
```

3. Gem filen og afslut editoren.

Denne konfiguration vil overstyre eventuelle modstridende indstillinger, herunder dem der er sat af cloud-init (fx `50-cloud-init.conf`).

#### □ 2□ Aktivér ændringer: Genstart SSH-tjenesten

1. Genstart SSH-tjenesten for at aktivere ændringerne: `sudo systemctl restart ssh`

#### □ 3□ Verifikation: Kontrollér effektiv SSH-konfiguration

1. Verificér den effektive SSH-konfiguration: `sudo sshd -T | egrep -i "passwordauthentication|kbdinteractiveauthentication"`

Forventet output:

```
passwordauthentication no
kbdinteractiveauthentication no
```

## 4 Genindlæsning: Sikr at ændringer er aktivt anvendt

1. Genstart SSH-tjenesten på jumphosten: `sudo systemctl restart ssh`

## 5 Kontroltest: Verificér at password-login afvises

I dette trin skal du dokumentere, at SSH-adgang med password er deaktiveret, og at kun offentlig nøgle accepteres.

1. Test login med offentlig nøgle (skal virke): `ssh -p 2222 bruger@<OPNsense_WAN_IP>` Du skal kunne logge ind uden at blive spurgt om password.
2. Afbryd forbindelsen igen.
3. Tving SSH til at forsøge password-login fra PowerShell: `ssh -p 2222 -o PreferredAuthentications=password bruger@<OPNsense_WAN_IP>`
4. Observer resultatet.

Forventet resultat:

- SSH afviser forbindelsen
- Du får enten beskeden: "Permission denied (publickey)."

Dette dokumenterer, at password-login er deaktiveret, og at jumphosten kun accepterer login via offentlig nøgle.

---

Når denne øvelse er gennemført, er password-login deaktiveret på jumphosten, og SSH-adgang er udelukkende baseret på offentlig nøgle.

Konfigurationen er både implementeret og verificeret.

I næste øvelse (1.5) vurderes arkitekturen og de anvendte sikkerhedstiltag ud fra et systemsikkerhedsperspektiv.

---

Last update: 2026-03-20 13:58:28