1.3 - SSH nøgle baseret adgang

Information

Formålet med denne øvelse er at etablere SSH-adgang baseret på offentlig nøgle i stedet for password.

Efter øvelsen vil det være muligt at logge ind på jumphosten uden password, men password-login er endnu ikke deaktiveret.

Ved Nøgle baseret autentificering anvendes et nøglepar bestående af en privat og en offentlig nøgle.

Den private nøgle forbliver på den computer som ønsker shh adgang og må aldrig deles, mens den offentlige nøgle installeres på jumphosten og bruges til at verificere identiteten ved autentificering.

Deløvelser

1 Konfigurér SSH til kun at anvende offentlig nøgle (obligatorisk – Windows / PowerShell)

I dette trin skal du sikre, at SSH-adgang til jumphosten kan ske via offentlig nøgle i stedet for password. Alle kommandoer i dette trin udføres fra den studerendes Windows-PC i PowerShell.

1. Opret SSH-nøglepar på Windows (PowerShell):

   Åbn PowerShell og kør: `ssh-keygen -t ed25519`, Accepter standardplaceringen ved at trykke Enter. Dette opretter:

   - Privat nøgle: `C:\Users\<brugernavn>\.ssh\id_ed25519`
   - Offentlig nøgle: `C:\Users\<brugernavn>\.ssh\id_ed25519.pub`

2. Overfør den offentlige nøgle til jumphosten (Windows / PowerShell)

   I dette trin kopieres den offentlige SSH-nøgle manuelt fra den studerendes Windows-PC til jumphosten. Alle kommandoer udføres fra PowerShell på Windows, medmindre andet er angivet.

3. Vis den offentlige nøgle på Windows-PC'en: `Get-Content $env:USERPROFILE\.ssh\id_ed25519.pub`

   Kommandoen viser én lang linje, der starter med: ssh-ed25519 ...

4. Kopiér hele linjen (den offentlige nøgle).

   Den offentlige nøgle kan deles frit og indeholder ingen hemmelig information. Det er kun den private nøgle, der skal beskyttes.

   Hvis den private nøgle kompromitteres, kan en angriber udgive sig for brugeren.

5. Log ind på jumphosten via SSH (stadig med password): `ssh -p 2222 bruger@<OPNsense_WAN_IP>`

6. På jumphosten: sørg for at mappen ~/.ssh findes:

   ```
   mkdir -p ~/.ssh
   chmod 700 ~/.ssh
   ```

7. Indsæt den kopierede offentlige nøgle i filen authorized_keys: `nano ~/.ssh/authorized_keys`

   Indsæt nøglen på en ny linje, gem filen, og afslut editoren.

8. Sæt korrekte rettigheder på filen: `chmod 600 ~/.ssh/authorized_keys`

   Den offentlige nøgle bør nu være installeret korrekt på jumphosten.

   SSH kræver stramme filrettigheder for at forhindre, at andre brugere kan læse eller ændre nøglemateriale.

   Hvis rettighederne er for åbne, vil SSH afvise login af sikkerhedshensyn.

9. Test login med nøgle (før hærdning) fra powershell med kommandoen: `ssh -p 2222 bruger@<OPNsense_WAN_IP>`

   Du bør nu kunne logge ind uden at indtaste password.

   Dette trin er vigtigt, før password-login deaktiveres. Hvis nøgle-login ikke testes og bekræftes før password-login deaktiveres, kan man risikere at låse sig selv ude af systemet.

Når denne øvelse er gennemført, er det muligt at logge ind på jumphosten via SSH uden at anvende password. Password-login er på dette tidspunkt stadig muligt og er endnu ikke deaktiveret. I næste øvelse (1.4) hærdes SSH-konfigurationen, og password-login deaktiveres og verificeres.

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