1.0 - Overblik over jumphost arkitektur

Information

Formålet med denne øvelse er at give dig praktisk erfaring med kontrolleret adgang til interne systemer ved brug af en jumphost placeret på LAN-siden af en firewall.

I professionelle miljøer er direkte adgang til interne systemer sjældent tilladt. I stedet anvendes en jumphost (også kaldet bastion host), som fungerer som eneste indgangspunkt til det interne netværk.

I denne øvelse:

- er adgangen til WAN-siden af OPNsense allerede etableret via skolens netværk eller via skole-VPN
- skal du konfigurere en Ubuntu Server som jumphost på LAN-siden
- skal jumphosten tildeles en fast IP-adresse via DHCP-reservation i OPNsense (Dnsmasq)
- skal du etablere SSH-adgang til jumphosten via port forwarding
- skal SSH-adgang efterfølgende begrænses til udelukkende at anvende offentlig nøgle
- skal du demonstrere forståelse for, hvorfor denne arkitektur øger systemsikkerheden

Øvelsen har fokus på adgangskontrol, netværksadskillelse og praktisk systemsikkerhed.

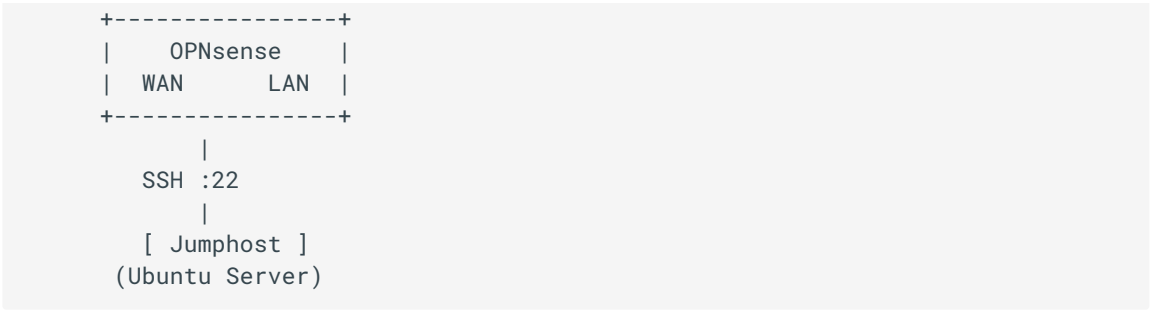
Overblik – hvad bygger du i dette øvelses forløb?

I denne øvelse skal du opbygge en kontrolleret adgangsvej til et internt system bag en firewall.

I stedet for at give direkte adgang til interne servere fra internettet, anvendes en jumphost (også kaldet en bastion host). Jumphosten placeres på LAN-siden af OPNsense og fungerer som det eneste indgangspunkt til det interne netværk.

Overordnet adgangsvej

```
[ Studerende / Windows PC ]
            |
        SSH :2222
            |
```



Forklaring

- Du forbinder udefra til OPNsense' WAN-adresse på port 2222
- OPNsense videresender forbindelsen via NAT / port forwarding
- SSH-trafikken ender på jumphosten på LAN-siden
- Der er ingen direkte adgang til LAN-netværket udefra

Jumphosten fungerer som:

- eneste indgangspunkt til det interne netværk
- kontrolpunkt for adgang
- sted for hærdning, logging og overvågning

Hvorfor denne arkitektur?

Denne arkitektur anvendes i professionelle miljøer, fordi den:

- reducerer angrebsfladen
- samler ekstern adgang ét kontrolleret sted
- gør sikker hærdning og adgangskontrol mulig
- adskiller netværkssikkerhed (firewall/NAT) fra systemsikkerhed (SSH, brugere og nøgler)

Vigtigt: At SSH-forbindelsen virker betyder ikke, at den er sikker. Først efter hærdning og verifikation i de senere trin betragtes løsningen som sikker.

Overblik over øvelsesforløbet

De følgende øvelser (1.1–1.5) gennemfører trin for trin den arkitektur, der er beskrevet ovenfor.

I forløbet vil du:

- etablere en jumphost med fast netværksidentitet på LAN-siden

- eksponere jumphosten kontrolleret via firewall og NAT
- etablere SSH-adgang via offentlig nøgle
- hærde SSH-konfigurationen og verificere effekten
- vurdere arkitekturen ud fra et systemsikkerhedsperspektiv

Hver deløvelse har sit eget fokus og afsluttes, før næste trin påbegyndes.

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