Opgave 21 - Tillad indgående trafik fra etablerede forbindelser

Information

Formålet med denne øvelse, er at vise hvordan en *stateful* firewall kan benyttes til at sikre svar på udadgående kommunikation.

Iptables er en *"stateful"* firewall. Det betyder, at den blandt andet kan holde styr på, hvilke forbindelser operativsystemet har oprettet til andre enheder på netværket. Dette gør det muligt for iptables at tillade svar på forbindelser, som din maskine selv har initieret, samtidig med at den blokerer al uautoriseret indgående trafik. I denne øvelse skal vi arbejde med netop dette.

I forrige øvelse blev alt indadgående trafik blokeret. Hvilket kan være en smule uhensigtmæssigt. Det bloker nemlig for alt trafik, heriblandt og for trafik på *loopback interfacet*, og det forhindre svar på de udadgående forbindelser vi forsøger at etablere. Så i denne øvelse, skal vi tillade den trafik vi ønsker

Instruktioner

1. Eksekver kommandoen `sudo iptables -F`
   - Flusher (rydder) alle eksisterende iptables-regler, så vi starter fra en ren konfiguration.
2. Eksekver kommandoen `sudo iptables -A INPUT -i lo -j ACCEPT`
   - Tillader trafik på loopback-interface (`lo`), hvilket sikrer, at systemet kan kommunikere med sig selv.
3. Eksekver kommandoen `sudo iptables -A OUTPUT -o lo -j ACCEPT`
   - Tillader udgående trafik på loopback-interface, så interne processer fungerer korrekt.
4. Eksekver kommandoen `sudo iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT`
   - Tillader udgående HTTP-trafik (port 80), som bruges til at hente websider via `curl` eller en browser.
5. Eksekver kommandoen `sudo iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT`
   - Tillader udgående HTTPS-trafik (port 443), som er nødvendig for sikre webforbindelser.
6. Eksekver kommandoen `sudo iptables -A OUTPUT -p udp --dport 53 -j ACCEPT`

- Tillader udgående DNS-opslag via UDP (port 53), hvilket er nødvendigt for at oversætte domænenavne til IP-adresser.

7. Eksekver kommandoen `sudo iptables -A OUTPUT -p tcp --dport 53 -j ACCEPT`
   - Tillader udgående DNS-opslag via TCP (port 53), som bruges til større DNS-forespørgsler.
8. Eksekver kommandoen `sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT`
   - Tillader indkommende pakker, der er en del af eksisterende eller relaterede forbindelser (så svar på forespørgsler kommer tilbage).
9. Eksekver kommandoen `sudo iptables -A OUTPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT`
   - Tillader udgående pakker, der hører til allerede etablerede forbindelser.
10. Eksekver kommandoen `sudo iptables -A INPUT -j DROP`
    - Blokerer al anden indgående trafik, hvilket øger sikkerheden ved at afvise uønskede forbindelser.

med `-m conntrack` (conntrack = connection tracking), ved iptables at der skal holdes styr på, hvilke forbindelser der er etableret, og hvem der har initieret dem. Med `--ctstate ESTABLISHED,RELATED -j ACCEPT`, tillades indadgående pakker fra servere, hvor klienten (OS) selv har oprettet forbindelsen.

Efter at have tilføjet reglen, vil iptables tillade indgående trafik fra eksterne servere, der er svar på forbindelser, din maskine selv har oprettet. Dette betyder, at du kan få svar på webanmodninger, SSH-forbindelser eller andre tjenester, som du selv har startet, mens indgående forbindelser udefra, som du ikke selv har initieret, vil blive blokeret.

i øvelsen har i indtil videre arbejdet udfra *allow list* tilgangen, hvor der specificeret konkret, hvornår der må etableres netværks forbindelser til og fra hosten.

Test med curl

Efter du har oprettet reglen, kan du teste dens funktionalitet ved at prøve at etablere en forbindelse til en tjeneste, såsom en webserver. Brug et værktøj som Curl til at sende en anmodning til en ekstern server (F.eks. www.google.com) og se, om svaret kommer igennem, mens en uautoriseret indgående forbindelse (f.eks. en ping) bliver afvist.

Du kan læse mere om iptables i forberedelsen til idag, eller ip tables man page

I næste øvelse bygges der videre på denne øvelse.

Links

- iptables man page
- Curl

2025-04-03 05:55:59