Øvelse 20 – Bloker alt indgående trafik

Information

Formålet med denne øvelse, er at give en grundlæggende introduktion til hvordan tilføjer en regel til firewal'en.

En firewall anvendes til at filtrere netværkstrafik baseret på definerede regler. Den kan eksempelvis tillade eller blokere kommunikation på specifikke netværksporte, protokoller eller IP-adresser.

En grundlæggende sikker tilgang er at blokere al trafik som standard og derefter eksplicit tillade den kommunikation, der er nødvendig. Denne tilgang kaldes en allow list og bygger på *sikkerhedsprincippet failsafe defaults*.

Princippet indebærer, at hvis en konfiguration fejler eller er ufuldstændig, vil systemets standardtilstand være restriktiv – altså at ingen trafik er tilladt.

Dette betyder, at alle porte og forbindelser bør være blokeret som standard. Først når du eksplicit åbner en port, er kommunikationen tilladt. Denne tilgang giver bedre sikkerhed, da kun de nødvendige porte er åbnet, og alt andet er blokeret. Det står i kontrast til en 'Block list'-tilgang, hvor alle forbindelser er tilladt som standard, og kun de usikre eller uønskede forbindelser bliver blokeret.

Firewall-regler behandles ofte én ad gangen i rækkefølge. Dette kaldes en regelkæde. Reglerne i en regelkæde håndhæves typisk i kronologisk rækkefølge. Dette betyder, at den første regel i kæden bliver evalueret først. Hvis en regel tillader eller blokerer en forbindelse, stopper vurderingen der, og de efterfølgende regler bliver ikke evalueret for den pågældende trafik. Hvis en forbindelse ikke er matchet af de første regler, vil den blive evalueret mod de næste regler i rækkefølgen.

For eksempel:

- Regel 1: Tillad TCP-forbindelser på port 80.
- Regel 2: Forbyd alle UDP-forbindelser.
- Regel 3: Forbyd alle TCP-forbindelser.
- Regel 4: Tillad UDP-forbindelser på port 53.

I dette tilfælde kommer regel 1 før regel 3, og derfor tillader firewallen oprettelsen af TCP-forbindelser på port 80. Omvendt kommer regel 2 før regel 4, og derfor er UDP-forbindelser på port 53 ikke tilladte.

Når man bruger `-A`-muligheden til at indsætte en regel, bliver den tilføjet sidst i regelkæden. Når firewall-reglerne eksekveres kronologisk, bør en 'drop alt trafik'-regel altid placeres sidst i regelkæden for at sikre, at al uønsket trafik bliver afvist.

Instruktioner

1 Gennemgang af eksisterende regler

1. Udskriv regelkæden og notér, hvordan den ser ud.
   (Regelkæden blev tidligere udskrevet i øvelse 19, trin 4.)

---

2 Bloker al indgående trafik

1. Lav en regel i slutningen af regelkæden, som dropper alt trafik, med kommandoen: `sudo iptables -A INPUT -j DROP`
2. Udskriv regelkæden igen og notér forskellen fra trin 1.

---

3 Test af firewall-reglen

1. Forsøg at pinge hosten på loopback adressen 127.0.0.1. Kommer der noget svar?
2. Forsøg at pinge hosten fra en anden host (f.eks. fra din Kali-instans hvis den er på samme netværk).
   Kommer der noget svar?

Fordelen ved som udgangspunkt at blokere alt trafik, er at tilgangen er *allow list*, altså alt bliver blokeret – med undtagelse af det, vi specifikt tillader.

Dog har vi blokeret alt, også muligheden for at lave udadgående forbindelser, da vi ikke længere kan modtage svar på de forespørgsler, vi sender ud. Derudover kan Linux ikke længere bruge loopback-adressen til at kommunikere med sig selv.

Alt dette løses i næste øvelse, ved at tillade noget trafik.

Behold reglen om at droppe alt trafik – vi skal bruge den i næste øvelse.

Bonusøvelse

Du kan prøve at anvende en netværksscanner som f.eks. *nmap* til at scanne dine netværksporte før og efter, du opsætter firewall-regler, men det kræver at der er noget der lytter på portene (F.eks. SSH server).

Med *nmap* kan du lave en såkaldt port scanning for at identificere åbne porte på din maskine. Før du opsætter firewall-regler, vil *nmap* vise dig en liste over åbne porte. Efter du har opsat din 'drop alt trafik'-regel, vil du opdage, at *nmap* ikke længere kan finde nogen åbne porte, hvilket viser, at firewallen effektivt har blokeret al trafik.

Links

- iptables man page

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