Opgave 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 giver mulighed for at filtrere netværkstrafik på mange måder. Som udgangspunkt giver den mulighed for at åbne op for kommunikation på specifikke netværksporte eller lukke ned for kommunikation på specifikke netværksporte. Som udgangspunkt bør man lukke for kommunikation på alle porte og derefter åbne for de specifikke porte, der er behov for. Altså, tilgangen er "Allow list", hvor udgangspunktet er, at intet er tilladt.

Dette betyder, at alle porte og forbindelser er 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 'Deny 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. Udskriv regelkæden og notér, hvordan den ser ud. (Regelkæden blev tidligere udskrevet i opgave 19, trin 4.)
2. Lav en regel i slutningen af regelkæden, som dropper alt trafik, med kommandoen `sudo iptables -A INPUT -j DROP`.
3. Udskriv regelkæden igen og notér forskellen fra trin 1. *Bemærk der komme en fejl, som unable to resolve host . Det fordi loopback adressen er blokeret. Det løser vi i næste øvelse*
4. Forsøg at pinge hosten (F.eks. fra din Kali instans), kommer der noget svar?

Fordelen ved at som udgangspunkt at bloker alt trafik, er at tilgangen er *allow list*, altså alt bliver blokeret. Med undtagelse af det vi specificer er tilladt. Dog har vi blokeret alt, også muligheden for at lave udadgående forbindelser da vi ikke længere kan modtage svar på de forspørgelser vi sender ud. Derudover kan Linux ikke længere bruge loopback adressen til at kommuniker med sig selv længere. Alt dette løse vi i næste øvelse, ved at tillade noget trafik.

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

Bonusopgave

Du kan prøve at anvende en netværksscanner som f.eks. *nmap* til at scanne dine netværksporte før og efter, du opsætter firewall-regler.
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

2025-04-03 05:55:59