Opgave 23 - Tillad indgående trafik fra specifikke ICMP-beskeder

Information

Formålet med denne øvelse, er at vise hvor firewallen kan arbejde med specifikke protokoller, såsom ICMP protokollen.

Pakker sendt med ICMP protokollen bruges til såkaldte "ping requests" og anvendes ofte af angribere i rekognosceringsfasen, hvor netværket bliver skannet. Man kan skjule sin vært ved at blokere ICMP-pakker. At blokere ICMP-pakker er ikke i sig selv en foranstaltning mod et angreb, men det besværliggør dog angriberens arbejde en smule i rekognosceringsfasen. Nogle enkelte typer af ICMP-pakker er dog belejlige at kunne modtage, og er ofte anvendt ved fejlfinding mellem enheder på et netværk.

I øvelsen skal tre typer af ICMP-pakker tillades, til den eksisterende regelkæde, der blev bygget i forrige øvelse.

Instruktioner

1. Tillad ICMP-pakker af type 3 med kommandoen `sudo iptables -A INPUT -p icmp --icmp-type destination-unreachable -m conntrack --ctstate NEW,ESTABLISHED,RELATED -j ACCEPT`.
2. Tillad ICMP-pakker af type 11 med kommandoen `sudo iptables -A INPUT -p icmp --icmp-type time-exceeded -m conntrack --ctstate NEW,ESTABLISHED,RELATED -j ACCEPT`.
3. Tillad ICMP-pakker af type 12 med kommandoen `sudo iptables -A INPUT -p icmp --icmp-type parameter-problem -m conntrack --ctstate NEW,ESTABLISHED,RELATED -j ACCEPT`.
4. Udskriv regelkæden. Kan du finde fejlen? Og hvordan kan den rettes?
5. De ICMP-pakker, der er blevet tilladt, er hver især af en bestemt type. Undersøg hvad hver af de tre typer betyder.

Vi har åbnet for ICMP-pakker af type 3, 11 og 12, som er nyttige til fejlfinding. Nu er regelkæden komplet.

Bonus øvelse.

Når du har afsluttet alle øvelserne med iptables, bør du eksperimenter med *Uncomplicated firewall(UFW)*. Dokumentation der kan hjælpe dig igang, kan du finde her.

Links

ICMP Types

2025-04-03 05:55:59