IPtables kiegészítő parancsok!

Filter tábla láncai: INPUT, OUTPUT, FORWARD

A filter tábla az alapértelmezett, nem törölhető tábla az iptables-ben. Az alapvető szűréseket a kívánt útvonal alapján a megfelelő láncba kell elhelyezni.

Nat tábla: PREROUTING, POSTROUTING, OUTPUT

A NAT tábla (Network Address Translation) tábla az útvonalválasztásban használt tábla, melyben a routingnak megfelelően kell elhelyezni a szabályokat.

Mangle tábla: INPUT, OUTPUT, FORWARD, PREROUTING, POSTROUTING

A Mangle tábla (mangling = manipuláció) táblában az összes létező lánc szerepel hisz egy csomagot bárhol lehet manipulálni. Ebben a táblában kell megadni azokat a szabályokat melyek az illeszkedő csomagok tulajdonságainak átállítására szolgálnak.

Célok: (-j) ACCEPT, DROP, REJECT, QUEUE, RETURN, REDIRECT, DNAT, SNAT, IPV4OPTSSTRIP

Minden egyes iptables szabályt egy céllal, vagyis egy utasítással kell lezárni mely megadja mi történjen a csomaggal.

Accounting (számlálás) iptables –A INPUT –i eth0

Az iptables a feldolgozott csomagokat alapértelmezetten számolja, így egy forgalmi statisztikát is rendelkezésünkre bocsájt. Ahhoz, hogy a különböző láncokon áthaladó forgalmat is számolja egy egyszerű parancsot kell beszúrni.(**`iptables –A INPUT –i eth0`**)

Fontos megjegyezni, hogy ennek a parancsnak a lánc elején kell elhelyezkedni, mivel a az iptables illeszkedés esetén a csomagot feldolgozza, nem engedi tovább ezért a számláló szabályhoz lehetséges, hogy már nem jut el.

Segédprogramok:
wireshark – protokollanalízátor, grafikus felülettel rendelkező csomagvizsgáló
Nessus – biztonsági szkenner, hálózatokhoz és adatbázisokhoz
Nmap – hálózat szkenner, és hálózatfelderítő
Ping – ICMP protokoll
Tcpdump – grafikus felülettel nem rendelkező csomaganalízátor
Netstat – éppen aktuális, nyitott tcp kapcsolatok ki listázására szolgál.
Traceroute – Az ICMP ping útvonal listázására szolgál.

Iptables szabályok argumentumai:

-A hozzáad, -D töröl, -X lánc törlése, -I <sorszám> beszúrás, -N létrehoz egy láncot, -P policy állítás, -Z accounting nullázás.

-p proto

Ezzel az argumentummal adhatjuk meg milyen protokollon végezzünk vizsgálatot.

Pl: ah ipv6-auth, tcp, udp, ospf, rip, icmp, igmp, ALL,

Illeszkedés: -m

Az illeszkedés argumentummal adhatjuk meg milyen tulajdonságot figyeljen az iptables

-m state --state: ESTABLISHED, INVALID, RELATED, NEW (a csomagok állapotának vizsgálata)

-m iplimit --iplimit-above 100 –j REJECT (az egyidejűleg nyitott kapcsolatok számának korlátozása)

-m - Ipv4options --any-opt (IPv4 flagak vizsgálata)

-m length --length 1000 (csomagméret szűrés)

-m nth --every 3 --packet 0 -j DNAT –to-destination $SERVER0
-m nth --every 3 --packet 1 -j DNAT –to-destination $SERVER1
-m nth --every 3 --packet 2 -j DNAT –to-destination $SERVER2
(Round-Robin algoritmus alapján működő terhelés-elosztás)

-m --uid-owner (gid, pid) 0 –j LOG –log-prefix „root kapcsolatok” (UID, GID, PID alapján való szűrés, CSAK OUTPUT láncon működik)

-m psd (Port Scan Detector, Interface letapogatás észlelő argumentum, mely jelez ha valaki például nmap-ot használ)

-m quota --quota 65535 –j DROP (megadott mennyiségű csomag után letiltja a processzt)

-m string –string .mp3 –j DROP (a megadott sztringre keres a csomag data mezőjében.)

--ttl-eq, --ttl-set, --ttl-gt (nagyobb), --ttl-lt (kisebb) (a TTL (Time To Live) értéket figyeli, a --ttl-set egy adott értékre állítja be (csak mangle táblánál))

-m unclean (nem szokványos vagy hibásan formázott IP, ICMP, UDP, TCP)

-j LOG kiterjesztés

--log-ip-options (a naplózásba bekerül az illeszkedő csomag options bitjeinek értéke is)

--log-level $logszint (megadhatjuk milyen loglevelt használjon az iptables)

--*log-prefix $előtag* (az előtag fog szerepelni minden LOG bejegyzés előtt)

--*set-mark érték* (megjelöli a csomagot az útvonalválasztóknak (IPROUTE2, IP))

-j REJECT kiterjesztés

--*reject-with icmp-host-unreacheable, net-unreachable, tcp-reset* (különböző okok miatt történik az elutasítás)