Iptables

firewall

Instalace

- Samotný firewall již je s největší pravděpodobností nainstalovaný
- Zjistíme dle parametru při použití

aptitude search iptables

```
root@debian:/home/adamek# aptitude search iptables
p   arno-iptables-firewall          - single- and multi-homed firewall script wi
i   iptables                        - administration tools for packet filtering
p   iptables-dev                    - iptables development files
p   iptables-persistent             - Simple package to set up iptables on boot
p   libiptables-chainmgr-perl       - Perl extension for manipulating iptables p
p   libiptables-ipv4-ipqueue-perl   - Perl extension for libipq
p   libiptables-parse-perl          - Perl extension for parsing iptables firewa
root@debian:/home/adamek#
```

Jak funguje

- Iptables je mocný nástroj, který umožňuje linuxovému nebo unixovému systému plně pracovat se síťovou komunikací.
- Pomocí něj si můžeme snadno postavit různé druhy firewallů (stavový, transparentní…) nebo sdílet internet, zkrátka snadno řídit velkou síťovou dopravní křižovatku na serveru.

Základní syntaxe

iptables [tabulka] [akce] [chain] [ip_část] [match] [target] [target_info]

Základní syntaxe - tabulky

- Tabulka
  - Existují pouze 3 základní:
    - filter (výchozí)
    - nat
    - mangle
- Pokud nedefinujeme žádnou tabulku, tak se automaticky použije filter, který má tyto hodnoty:
  - INPUT
  - FORWARD
  - OUTPUT
- **To, co jde přes FORWARD, neprochází pravidly INPUT ani OUTPUT!**

Základní syntaxe - tabulky

- Tabulka nat má opět výchozí 3 položky
  - PREROUTING
    - je řetěz pravidel, které se použijí na příchozí pakety, pomocí nich můžeme modifikovat cílovou adresu Destination NAT (DNAT). To se hodí hlavně tehdy, když chceme forwardovat porty (nebo celý rozsah) do neveřejné místní sítě
  - POSTROUTING
    - opak PREROUTINGu, s ním modifikujeme odchozí spojení Source NAT (SNAT),masquerade. Toho zase můžeme využít, pokud máme například jednu veřejnou IP adresu a chceme za ní skrýt více počítačů
  - OUTPUT
    - řetěz pravidel, které se uplatňují ještě před modifikací odchozích paketů (než je předáme dále).

Základní syntaxe - tabulky

- Tabulka mangle má všech pět položek, které mají filter i nat:
  - INPUT
  - OUTPUT
  - FORWARD
  - PREROUTING
  - POSTROUTING
- V nich jsou řetěze pravidel, které slouží pro úpravy hlavičky paketů, manipulace s TTL, TOS, značkování…

Základní syntaxe - akce

- -A --append - Přidání nového pravidla na konec řetězce
- -D --delete - Smaže pravidlo (buď ho zadáte ve tvaru, v němž jste ho přidávali, nebo použijete jeho číslo, to získáte rozšířenou volbou –lin)
- -R --replace - Nahradí číslo pravidla jiným pravidlem
- -I --insert - Vložení nového pravidla na začátek řetězce
- -L --list - Vypsání všech pravidel v řetězci. Pokud není zadán řetězec, vypíšou se všechny řetězce + jejich pravidla
- -F --flush - Vyprázdní všechna pravidla v řetězci (to samé, jako kdybyste to dělali po jednom)
- -N --new-chain - Vytvoříme si vlastní řetěz
- -X --delete-chain - Smažeme si vlastní řetěz (nejde smazat výchozí)
- -P --policy - Výchozí politika řetězce
- -E --rename-chain - Přejmenování vlastního řetězce

Základní syntaxe - akce

- Rozšířené volby

-v	--verbose	- Podrobnější výpis (více ukecaný)
--lin	--line-numbers	- Zobrazí čísla pravidel
-n	--numeric	- u IP adres nebude zjišťovat reverzní DNS, ale vypíše ji číselně (vhodné, když máte mnoho pravidel, abyste měli rychlejší výpis)

Praktické příklady

- sdílení internetu z eth0 do sítě 5.0 :

  iptables -t nat -A POSTROUTING -s 192.168.5.0/24 -j MASQUERADE -o eth0

- Zákaz portu 25 z lokální sítě do světa

  iptables -A FORWARD -i eth1 -o eth0 -p tcp -m tcp --dport 25 -j DROP

- Povolení ssh z určité veřejné IP

  iptables -A INPUT -i eth0 -s 81.200.59.4 -p tcp -m tcp --dport 22 -j ACCEPT

- Povolení samby z určité veřejné IP

  iptables -A INPUT -i eth0 -s 81.200.59.4 -p udp -m udp --dport 137 -j ACCEPT
  iptables -A INPUT -i eth0 -s 81.200.59.4 -p udp -m udp --dport 138 -j ACCEPT
  iptables -A INPUT -i eth0 -s 81.200.59.4 -p tcp -m tcp --dport 139 -j ACCEPT
  iptables -A INPUT -i eth0 -s 81.200.59.4 -p tcp -m tcp --dport 445 -j ACCEPT

- Zákaz všech portů mimo portu 80 do světa i lokálně pro určitý rozsah IP adres

iptables -A FORWARD -i eth1 -o eth0 -p tcp --dport ! 80 -m iprange --src-range 192.168.2.30-192.168.2.254 -j DROP
iptables -A INPUT -i eth1 -p tcp --dport ! 80 -m iprange --src-range 192.168.2.30-192.168.2.254 -j DROP