1. IP Tables alat (pregled naredbi)

1.1. Osnovne IP Tables naredbe za filtriranje paketa

U ovom poglavlju opisane su osnovne IP Tables naredbe korištene za filtriranje paketa.

S programskim paketom IP Tables dolazi program `iptables`. Taj program je namijenjen unošenju pravila za filtriranje paketa u tablice za filtriranje koje se nalaze u jezgri operativnog sustava. Program se iz komandne linije poziva kao:

```
#iptables <opcije>
```

Ovisno o opcijama navedenim iza imena programa, u tablice za filtriranje paketa se dodaju nova, brišu stara, ili modificiraju postojeća pravila. Program `iptables` moguće je pozivati direktno iz komandne linije, ali za veći skup pravila to nije praktično. Mnogo je jednostavnije napisati *shell* skriptu u kojoj se definiraju pozivi `iptables` programa sa svim željenim pravilima za filtriranje.

1.1.1. Operacije s pojedinim fazama obrade paketa

Faze obrade paketa moguće je prilagoditi potrebama. Tako je osnovni skup faza koji je opisan u prošlom poglavlju moguće proširiti novim fazama. Nove faze definiraju se npr. za obradu posebnih vrsta paketa (TCP, UDP), ili ciljnih aplikacija, odnosno korištenih protokola (Web, mail, itd.). Postojeće faze obrade paketa moguće je izostaviti ovisno o potrebama. Primjerice ukoliko se ne obavlja maskiranje ili SNAT transformacija izvorišne adrese moguće je izostaviti POSTROUTING fazu i tome slično.

1. Određivanje osnovne politike (engl. *policy*) o prihvaćanju ili neprihvaćanju paketa za pojedinu fazu obrade (moguće odluke su ACCEPT - odobri paket, REJECT - odbij zahtjev i vrati poruku da je zahtjev za konekcijom odbijen, DROP – ignoriraj zahtjev):

   ```
   -P, --policy

   #iptables –P FORWARD DROP
   ```

2. Ispis svih definiranih pravila u određenoj fazi obrade:

   ```
   -L, --list

   #iptables –L INPUT
   ```

3. Odbacivanje svih definiranih pravila u pojedinoj fazi obrade:

```
-F, --flush

#iptables –F FORWARD
```

1.1.2. Operacije s naredbama unutar pojedine faze obrade paketa

Prilikom kreiranja pojedinih faza (karika) potrebno je, ali ne i nužno, definirati pravila koja se primjenjuju na pakete koji prolaze kroz pojedinu fazu obrade.

1. Dodavanje novog pravila u određenoj fazi obrade na kraj niza postojećih pravila:

```
-A, --append

#iptables –A FORWARD –p tcp –j ACCEPT
```

2. Brisanje postojećeg pravila:

```
-D, --delete

#iptables –D FORWARD 3
```

1.1.3. Operacije s pojedinom naredbom

Da bi se paket mogao obraditi i odrediti koje je pravilo potrebno izvršiti nad njim (prosljeđivanje ili odbacivanje) potrebno ga je dobro analizirati. U tu svrhu postoje različite usporedbe.

1. Provjera korištenog protokola. Može biti TCP, UDP, ICMP ili neki drugi, iz popisa obično navedenog u datoteci `/etc/protocols`.

```
-p,–-protocol

#iptables –A FORWARD –p tcp –j ACCEPT
```

2. Analiza izvorišne IP adrese:

```
-s, --source

#iptables –I FORWARD –p udp –s 161.53.64.117 –j DROP
```

3. Analiza odredišne IP adrese:

```
-d, --destination

#iptables –I FORWARD –p udp –d 161.53.64.233 –j ACCEPT
```

4. Provjera paketa na temelju mrežnog sučelja s kojeg je pristigao (`eth0`, `eth1.1`, `eth2:1`, …):

```
-i, --in-interface

#iptables -A INPUT –i eth0 –j ACCEPT
```

5. Provjera paketa na temelju mrežnog sučelja na koje treba biti usmjeren (`eth0`, `eth1.1`, `eth2:1`, …):

```
-o, --out-interface

#iptables -A INPUT –o eth2 –j DROP
```

6. Preusmjeravanje paketa. Pakete je moguće preusmjeriti na neku drugu kariku (engl. *chain*), ili u stanje u kojem će paketi biti prihvaćeni (ACCEPT), odbačeni (REJECT, DROP) i slično:

```
-j, --jump

#iptables –I FORWARD –p tcp –j ISPITAJ_TCP
```

7. Provjera paketa na temelju mrežnog porta s kojeg je pristigao (1-1024: rezervirani portovi, 1025-65535: slobodni portovi). Moguće je navesti samo jedan broj koji označava samo jedan port, sve portove iznad nekog (npr. 1025:), sve portove manje od određenog (npr. :80), ili rang portova između dva porta (npr. 22:80):

```
--sport, --source-port

#iptables -A INPUT –p tcp –-sport 1024: –j ACCEPT
```

8. Provjera paketa na temelju mrežnog porta na koji treba biti usmjeren. Vrijede ista pravila kao i kod prethodno definiranog pravila:

```
--dport, --destination-port

#iptables -A INPUT –p tcp –-dport :1024 –j DROP
```

1.2. Osnovne IP Tables naredbe za pretvorbu mrežnih adresa

U ovom poglavlju opisane su osnovne IP Tables naredbe korištene za pretvorbu mrežnih adresa. Pretvorba mrežnih adresa može se obavljati na tri načina:

- DNAT – promjena odredišta
- SNAT – promjena izvorišta
- *Masquerading* – maskiranje izvorišta

DNAT transformacija koristi se za promjenu odredišne adrese i ta manipulacija ostvaruje se u PREROUTING fazi, *nat* tablice. Novo odredište može biti jednoznačno određeno, ali može biti i rang IP adresa iz kojih se novo odredište odabire slučajnim izborom. Prilikom DNAT transformacije moguće je promijeniti i odredišni port mrežnog paketa. Novi port može biti jednoznačno određen ili se može odabirati slučajnim izborom iz ranga definiranih portova.

```
-j DNAT –-to-destination

#iptables –t nat –A PREROUTING –p TCP –d 161.53.64.11
  -j DNAT –-to-destination 161.53.64.2-161.53.64.6:80-100
```

Navedena naredba svim TCP mrežnim paketima usmjerenima na IP adresu 161.53.64.11 zamjenjuje odredište sa slučajno odabranim iz ranga 161.53.64.2-161.53.64.6, ali zamjenjuje i odredišni port sa slučajno odabranim iz ranga 80-100.

SNAT transformacija koristi se za promjenu izvorišne adrese i ta manipulacija ostvaruje se u POSTROUTING fazi, *nat* tablice. Novo izvorište može biti jednoznačno određeno, ali može biti i rang IP adresa iz kojih se novo izvorište odabire slučajnim izborom. Prilikom SNAT transformacije moguće je promijeniti i izvorišni port mrežnog paketa. Novi port može biti jednoznačno određen ili se može odabirati slučajnim izborom iz ranga definiranih portova.

```
-j SNAT –-to-source

#iptables –t nat –A POSTROUTING –p TCP –s 192.168.2.0/24
  -j SNAT –-to-source 161.53.64.5-161.53.64.9:1024-1028
```

Navedena naredba svim TCP mrežnim paketima koji imaju izvorišnu IP adresu iz mreže 192.168.2.0/24, zamjenjuje izvorište sa slučajno odabranim iz ranga 161.53.64.5-161.53.64.9, ali zamjenjuje i izvorišni port sa slučajno odabranim iz ranga 1024-1028.

Masquerading transformacija koristi se za maskiranje izvorišne adrese i ta manipulacija ostvaruje se u POSTROUTING fazi, *nat* tablice. Novo izvorište postaje IP adresa izlaznog sučelja. Prilikom maskiranja moguće je promijeniti i

izvorišni port mrežnog paketa. Novi port može biti jednoznačno određen ili se može odabirati slučajnim izborom iz ranga definiranih portova.

```
-j MASQUERADE –-to-ports

#iptables –t nat –A POSTROUTING –p TCP –o eth0
  -j MASQUERADE –-to-ports 1024-2048
```

Navedena naredba svim TCP mrežnim paketima koji napuštaju računalo preko mrežnog sučelja eth0 zamjenjuje izvorište sa IP adresom mrežnog sučelja eth0. Ali zamjenjuje i izvorišni port sa slučajno odabranim iz ranga 1024-2048.