Rozszerzenia Netfilter HOWTO

Fabrice Marie fabrice@celestix.com lista pocztowa netfilter-devel@lists.samba.org Wersja oryginalna: $Revision: 550 $

Orygina^3*tegodokumentuznajdujesipodadresem* : http://netfilter.samba.org/

Orygina^3*tegot*^{3}*umaczeniaznajdujesipodadresem* : http://mr0vka.eu.org/tlumaczenia/netfilter-extensions.htm

Spis treści

1 Wprowadzenie

Witam. Mam ¶wietn±*okazjbypodzikowawieluludziomzaca*^{3} ± *masczasuspdzon* ± *przykodowaniu*, *testowaniu*, *zg*^{3}*aszaniub*^{3}*dwiuywaniunetfilter*.*Dzikiwamwszystkim*!!

Ten dokument zak^3*ada*, *eprzeczyta*^{3}*e*¶*izrozumia*^{3}*e*¶*dokumentRusty*′*ego*

Filtrowanie pakietów w Linuksie 2.4 HOWTO http://www.netfilter.org/documentation/HOWTO/packet-filtering- . Zak^3*adamrwnie*, *ewieszjakprawid*^{3}*owoskompilowaizainstawowakernel*.

Dystrybucja iptables zawiera pewne rozszerzenia, które nie s±*uywaneprzezzwyk*^{3}*ychuytkownikwitaknaprawds*± *nadalwjakim*¶*stopniueksperymentalne*, *lubczekaj*±*nawprowadzeniedokernela*.*Zwykleniekompilujesiich*, *chyba*, *ejas*

Najnowsza wersja tego dokumentu powinna byæ dostêpna pod adresem

http://www.netfilter.org/documentation/index.html#HOWTO .

Celem tego HOWTO jest pomoc ludziom, którzy zaczynaj±*praczrozszerzeniaminetfilter*, *przezwyja*¶*nieniajakjezain*

(C) 2001 Fabrice MARIE. Na licencji GNU GPL.

2 Patch-O-Matic

2.1 Co to jest Patch-O-Matic ?

Plik Makefile iptables zawiera funkcjonalno¶æ nazwan±‘*patch* − *o* − *matic*′(*lub*‘*p* − *o* − *m*′).*p* − *o* − *mkierujetwoj*±*drog*±*przezprocesselekcji*^{3}*at*, *ktremoeszchciezaaplikowa*, *orazautomatyczniedodajejedokernela*.

Po pierwsze, powiniene¶ ¶ci±*gn*±*najnowszedrzewoCVS*, *bybypewnymepracujeszznajnowszymiwersjamirozszerze*.*B*

```
# cvs -d :pserver:cvs@pserver.samba.org:/cvsroot login
# cvs -z3 -d :pserver:cvs@pserver.samba.org:/cvsroot co netfilter
```

Stworzy to g^3*wnykatalog*‘*netfilter*/′*anastpnie*¶*ci* ± *gniedoniegowszystkiepotrzebnepliki*.

Upewnij siê, ¿e $\frac{1}{4}$ród^3*atwojegokernelas*±*w*‘/*usr*/*src*/*linux*/′.*Je*¶*lizjaki*¶*powodwkernel*, *ktrybdziesz*^{3}*ata*^{3}*nieznajdujes* ¶*rodowiskow* ± *KERNEL*_*DIRnakatalogzawieraj* ± *cy*$\frac{1}{4}$*rd*^{3}*akernela* :

```
# export KERNEL_DIR=/¶cie¿ka/do/linuksa
```

Upewnij siê równie¿, ¿e wykona^3*e*¶*sprawdzeniezaleno*¶*ci*(*ang*.*dependencies*).*Je*¶*liniejeste*¶*pewien* :

```
# cd /usr/src/linux/
# make dep
```

Mo¿esz teraz przej¶æ do katalogu netfilter, wej¶æ do katalogu 'userspace/' i wykonaæ p-o-m.

2.2 Praca z Patch-O-Matic

Uruchommy w katalogu 'userspace/' p-o-m :

```
# make patch-o-matic

Welcome to Rusty's Patch-o-matic!

Each patch is a new feature: many have minimal impact, some do not.
Ka¿da ³ata to nowa funkcjonalno¶æ: wiele z nich wnosi niewielkie zmiany, ale niektre nie.
Almost every one has bugs, so I don't recommend applying them all!
Prawie ka¿da ma jakie¶ b³êdy, wic nie rekomenduj nak³adania ich w ogle!
------------------------------------------------------

Already applied: 2.4.1 2.4.4
Ju¿ na³oone: 2.4.1 2.4.4
Testing... name_of_the_patch NOT APPLIED ( 2 missing files)
Testuje... nazwa_³atki NIE NA£O¯ONA ( znaleziono 2 brakuj±ce pliki )
The name_of_the_patch patch:
nazwa_³atki:
   Here usually is the help text describing what
   Tutaj znajduje siê zwykle tekst obja¶niaj±cy
   the patch is for, what you can expect from it,
   do czego jest ³ata, czego moesz si po niej spodziewa,
   and what you should not expect from it.
   a czego nie.
Do you want to apply this patch [N/y/t/f/q/?]
Czy chcesz na³oy ³atk
```

p-o-m przejdzie przez wszystkie ³aty.Je¶lizosta³yjuna³oone, zobaczysznapis'Alreadyapplied :' wpierwszejlinii.Je¶linie, wy¶wietlinazw³atyzkrtkimobja¶nieniem.p − o − mpoinformujerwnieotym, cosidzieje : 'NOTAPPLIED(nmissingfiles)'oznaczapoprostu, e³atyjeszczeniena³oono, a'

1. £ata nie mo¿e byæ na³oona, lube³atajuzosta³aw³ ± czonadokernela, ktryprbujesz³ata.retryingtopatch.

   Na koniec, zapyta o twoj±decyzj − ³ataczynie.

   2. Naci¶nij po prostu Enter je¶li nie chcesz jej aplikowaæ.

   - Naci¶nij 'y' je¶li chcesz by p-o-m przetestowa³33atizaaplikowa³j±; je¶litestsiniepowiedzie, poinformujeotymizapp

- Naci¶nij 'f' by p-o-m wymusi³zainstalowanie³aty.Moeszrwnienacisn ± 'q', je¶lichceszopu¶cip − o − m.

  Dobr±zasad±jestprzeczytanieopisu³atyzanimsij±na³oy.Poniewaobecniejestbardzoduoficjalnych³atdlapatch− o−matic(iprawdopodobniejeszczewicejnieoficjalnych)absolutnieniezalecamstosowaniaichwszystkich!Powiniene¶po

  Stworzono now±wersjpatch − o − matic, ktrapokazujetylko³atyoktrychwiadomo, ena³o ± sibezproblemowo, lubprzynajmniejniezniszcz ± efektuinnych³at.Byj ± wywo³a, napisz :

  - # make most-of-pom

Dzia^3*atotaksamojakpatch – o – matic, je¶lichodzio*^{3}*atanie.Zaoszczdziszsobiepoprostuogl ± dania*^{3}*attylkodlaprogramistw.*

2.3 A co dalej ?

W momencie gdy na^3*oy*^{3}*e¶juwszystkie*^{3}*aty, ktrechcia*^{3}*e¶, nastpnymkrokiembdzierekompilacjakernelaizainstalowanie*

Linux Kernel HOWTO http://www.linuxdoc.org/HOWTO/Kernel-HOWTO.html .

Podczas konfiguracji swojego kernela, zauwa¿ysz nowe opcje w 'Networking Options -> Netfilter Configuration'. Wybierz opcje, których potrzebujesz, przekompiluj i zainstaluj nowy kernel.

Je¶li ju¿ siê to sta^3*o, moeszzainstalowapaczk'iptables'zkatalogu'userspace/'wtensposb* :

```
# make && make install
```

I to wszystko! Twoje nowe `iptables` zosta^3*ow*^{3}*a¶niezainstalowane!Terazczasnazabawznow ± funkcjonalno¶ci* ± .

3 Nowe testy netfilter

W tej sekcji postaram siê omówiæ u¿ycie nowych testów. £aty wymieniane bêd±*wkolejno¶cialfabetycznej.Nieporuszymy*^{3}*at, ktrepowoduj ± uszkadzanieinnych*^{3}*at, chobymoekiedy¶taksistanie.*

Ogólnie rzecz bior±*c, moeszuzyskapomocdlatestwwpisuj* ± *c* :

```
# iptables -m test_o_który_ci_chodzi --help
```

Wy¶wietli to normaln±*pomociptables, orazdodatkoweinformacjedotycz ± ce'testu_o_ktry_ci_chodzi'nakocu.*

3.1 £ata ah-esp

Przygotowana przez Yon Uriarte <yon@astaro.de> dodaje dwa nowe testy:

- 'ah' : pozwala dopasowywaæ pakiety AH na podstawie **Indeksu Parametrów Bezpieczeñstwa** (ang.*Security Parameter Index, SPI*)
- 'esp': pozwala dopasowywaæ pakiety ESP na podstawie ich SPI

£ata bêdzie u¿yteczna dla ludzi u¿ywaj±*cychIPSEC, ktrzychc ± kontrolowapo*^{3} ± *czenianapodstawieichSPI.*

Na przyk^3*ad, byodrzucipakietyAHktremaj* ± *SPIrwne*500 :

```
# iptables -A INPUT -p 51 -m ah --ahspi 500 -j DROP

# iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       ipv6-auth--  anywhere             anywhere           ah spi:500
```

Opcje dostêpne dla testu ‘ah’ to:

- `--ahspi [!] spi[:spi]`
  -> match spi (zakres)

Test ‘esp’ dzia^3*adok*^{3}*adnietaksamo* :

```
# iptables -A INPUT -p 50 -m esp --espspi 500 -j DROP

# iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       ipv6-crypt--  anywhere             anywhere           esp spi:500
```

Opcje dostêpne dla testu ‘esp’ to:

- `--espspi [!] spi[:spi]`
  -> match spi (zakres)

Nie zapomij podaæ w^3*a*¶*ciwegoprotoko*^{3}*u*, *czyli*‘−*p*50′*lub*‘−*p*51′(*dlaodpowiednio*‘*esp*′*i*‘*ah*′), *poniewawinnymprzypadkun*

3.2 £ata iplimit

£ata przygotowana przez Gerd Knorr <kraxel@bytesex.org> dodaje nowy test, pozwalaj±*cynaograniczaniejednoczesnychpo*^{3} ± *czeTCPzkonkretnejsiecilubkomputera*.

Na przyk^3*ad*, *ograniczmyilo*¶*jednoczesnychpo*^{3} ± *czeHTTPwykonywanychprzezpojedyczyadresIPdo*4 :

```
# iptables -A INPUT -p tcp --syn --dport http -m iplimit --iplimit-above 4 -j REJECT

# iptables --list
Chain INPUT (policy ACCEPT)
target   prot opt source    destination
REJECT   tcp  --  anywhere  anywhere     tcp dpt:http flags:SYN,RST,ACK/SYN #conn/32 > 4 reject-with icmp-
```

Mo¿esz równie¿ ograniczyæ liczbê jednoczesnych po^3 ± *czenaprzyk*^{3}*addlaca*^{3}*ejklasyA* :

```
# iptables -A INPUT -p tcp --syn --dport http -m iplimit --iplimit-mask 8 --iplimit-above 4 -j REJECT

# iptables --list
Chain INPUT (policy ACCEPT)
target   prot opt source    destination
REJECT   tcp  --  anywhere  anywhere     tcp dpt:http flags:SYN,RST,ACK/SYN #conn/8 > 4 reject-with icmp-p
```

Opcje dostêpne dla testu ‘iplimit’ to:

- `[!] --iplimit-above n`
  - pasuje je¶li ilo¶æ istniej±*cychpo*^{3} ± *czeniejestwyszanin*
- `--iplimit-mask n`

- grupuje komputery przez u¿ycie maski