Rozszerzenia Netfilter HOWTO

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

Orygina³*tegodokumentuznajdujesipodadresem* : http://netfilter.samba.org/

Orygina³*tegot*³*umaczeniaznajdujesipodadresem* : http://mr0vka.eu.org/tlumaczenia/netfilter-extensions.html

Spis treści

1 Wprowadzenie

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

Ten dokument zak³*ada, eprzeczyta*³*e*¶*izrozumia*³*e*¶*dokumentRusty′ego*

Filtrowanie pakietów w Linuksie 2.4 HOWTO http://www.netfilter.org/documentation/HOWTO/packet-filtering-HOWTO.html . Zak³*adamrwnie, ewieszjakprawid*³*owoskompilowaizainstawowakernel.*

Dystrybucja `iptables` zawiera pewne rozszerzenia, które nie s±*uywaneprzezzwyk*³*ychuytkownikwitaknaprawds*± *nadalwjakim*¶*stopniueksperymentalne, lubczekaj*±*nawprowadzeniedokernela.Zwykleniekompilujesiich, chyba, ejasnosobietegozayczysz.*

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*¶*nieniajakjezainstalowaanastpnieuywa.*

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.Bytozrobi, wykonaj* :

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

Stworzy to g³*wnykatalog*'*netfilter*/′*anastpnie*¶*ci* ± *gniedoniegowszystkiepotrzebnepliki.*

Upewnij siê, ¿e $\frac{1}{4}$ród³*atwojegokernelas*±*w*'/*usr*/*src*/*linux*/′.*Je*¶*lizjaki*¶*powodwkernel, ktrybdziesz*³*ata*³*nieznajdujesiwtymkatalogu, musiszustawizmienn*± ¶*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¶ : 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¶ b³dy, 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£OONA ( 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 ^{3}*aty.Je¶lizosta*^{3}*yjuna*^{3}*oone, zobaczysznapis'Alreadyapplied :' wpierwszejlinii.Je¶linie, wy¶wietlinazw*^{3}*atyzkrtkimobja¶nieniem.p − o − mpoinformujerwnieotym, cosidzieje : 'NOTAPPLIED(nmissingfiles)'oznaczapoprostu, e*^{3}*atyjeszczeniena*^{3}*oono, a'NOTAPPLIED(nrejectsoutofnhunks)'oznaczageneralnie, e :*

1. £ata nie mo¿e byæ na^3*oona, lube*^{3}*atajuzosta*^{3}*aw*^{3} ± *czonadokernela, ktryprbujesz*^{3}*ata.retryingtopatch.*

Na koniec, zapyta o twoj±*decyzj* − ^{3}*ataczynie.*

- Naci¶nij po prostu Enter je¶li nie chcesz jej aplikowaæ.
- Naci¶nij 'y' je¶li chcesz by p-o-m przetestowa^{33}*atizaaplikowa*^{3}*j*±; *je¶litestsiniepowiedzie, poinformujeotymizapytaponownieodecyzj*; *je¶liwszystkopjdziedobrze, zobaczysznazw*^{3}*atkiitekst'AlreadyApplied'.Naci¶nij't'je¶lichcesztylkoprzetestowa*^{3}*at.*

- Naci¶nij 'f' by p-o-m wymusi^3*zainstalowanie*^{3}*aty.Moeszrwnienacisn* ± *'q', je¶lichceszopu¶cip − o − m.*

Dobr±*zasad*±*jestprzeczytanieopisu*^{3}*atyzanimsij*±*na*^{3}*oy.Poniewaobecniejestbardzoduoo ficjalnych*^{3}*atdlapatch−o−matic(iprawdopodobniejeszczewicejnieoficjalnych)absolutnieniezalecamstosowaniaichwszystkich!Powiniene¶powanieprzemy¶leswjwybrina*^{3}*oytylkote, ktrychfaktyczniepotrzebujesz, nawetje¶lioznaczatorekompilacjnetfiltergdybdzieszpotrzebowa*^{3}*wicej*^{3}*at.*

Stworzono now±*wersjpatch − o − matic, ktrapokazujetylko*^{3}*atyoktrychwiadomo, ena*^{3}*o* ± *sibezproblemowo, lubprzynajmniejniezniszcz* ± *efektuinnych*^{3}*at.Byj* ± *wywo*^{3}*a, 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¶, nastpnymkrokiembdzierekompilacjakernelaizainstalowaniego.ToHOWTOtegonieobja¶ni, przeczytaj*

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_ktôry_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*‘$-p50'$*lub*‘$-p51'$*(dlaodpowiednio*‘*esp*$'$*i*‘*ah*$'$*), poniewawinnymprzypadkuniepowiedziesidopisanieregu*^{3}*ydo*^{3}*acucha*.

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-port-unreachable
```