OpenWEEKEND

Linux firewalling

LINUX IPTABLES

Pavol Lupták, P.Luptak@sh.cvut.cz

1 Firewall Configuration

Firewall Hardware Configuration

- Single machine, one NIC/modem
- Single machine, two interfaces - Internet on one, internal network on other
- Pseudo-DMZ: One machine, three NICs, one for internal network, two for servers
- Real DMZ: Two firewall boxes, each with two NICs

2 iptables

Robustný prostriedok na administráciu IP paketového filtra, nástupca ipchains/ipfwadm.

2.1 Výhody

- Rýchly, flexibilný, lacný (stačia 486 alebo pomalé Pentium pre malú sieť)
- Flexibilná zmena pravidiel (bez potrebného rebootu ;-)

2.2 Nevýhody

- Analyzujú sa len hlavičky a parametre paketu, nejde o ’content filter’
- Hlavičky môžu byť upravené
- Pravidlá pre veľkú sieť môžu byť neprehľadné (je potrebné stále vedieť, čo chcem a čo robím)

2.3 Ideálny paranoidný systém

Linux firewall box s nakonfigurovanými IPTables, žiadnymi bežiacimi servermi, navyše so spusteným content filtrom (Snort, Hogwash) bežiacimi worm-findermi (ramen-find).

3 IPTables vs. IPChains

- IPChains umožňoval len kontrolu zhody SYN flagu, IPTables umožňuje match na SYN, ACK, FIN, RST, URG, PSH, ALL, NONE
- Stavovosť, povoľuje blokovanie neautorizovaných nových spojení cez firewall aj napriek tomu, že tieto pakety by boli inak povolené. Aplikovateľné na všetky protokoly, nielen TCP

3.1 Stavová politika

Routovacie rozhodnutia môžu byť založené na nasledujúcich stavoch:

- NEW: vytváranie nového spojenia (SYN flag), nepovoľujeme na INPUT chain, pokým nebeží server
- RELATED: spojenie vzťahujúce sa nejakým spôsobom na už existujúce spojenie

  - ESTABLISHED: súčasť existujúceho spojenia
  - INVALID: nepatriace žiadnemu spojeniu (info v hlavičke je poškodené)

```
iptables -A FORWARD -m state --state ESTABLISHED, RELATED
-j ACCEPT
```

- Adresový preklad (NAT), IPChains umožňoval len Maškarádu, IPTables podporuje DNAT, SNAT, REDIRECT, MASQUERADE
- Podpora ”Packet Mangling” - zmena ”mangling” informácie v hlavičkách paketov počas routovacieho procesu (TOS, Marking, ..)
- Ochrana pred log-floodingom DOS útokmi limitovaním množstvom prípadnych zhôd v priebehu minúty (aplikovateľné nielen na LOG), podpora LOG prefixu a warning levelov (schopnosť logovania detailov)

```
iptables -A INPUT -s 192.168.0.0/16 -m limit --limit 1/s
-j LOG
iptables -A INPUT -s 192.168.0.0/16 -j LOG --log-level warn
--log-prefix "spojenie:"
```

- Možnosť kontroly (matchovania) paketov na základe rôznych kritérií (MAC, TOS, LENGTH, TTL, ...)
- modul LOG je separovaný ”target” a nemôže byť kombinovaný naraz v jednom pravidle ako to bolo možné v IPChains, musí byť vytvorené nové pravidlo (viac pravidiel = väčšia flexibilita, možnosť použiť vlastné chainy na logovanie, dropovanie, ..)
- REJECT bol zahrnutý do externého modulu

4 Kernel setup

Networking options

- CONFIG_NETFILTER
- CONFIG_IP_NF_CONNTRACK
- CONFIG_IP_NF_FTP
- CONFIG_IP_NF_IRC[1]
- CONFIG_IP_NF_IPTABLES
- CONFIG_IP_NF_MATCH_LIMIT
- CONFIG_IP_NF_MATCH_MAC
- CONFIG_IP_NF_MATCH_MARK
- CONFIG_IP_NF_MATCH_MULTIPORT
- CONFIG_IP_NF_MATCH_TOS
- CONFIG_IP_NF_MATCH_LENGTH[2]
- CONFIG_IP_NF_MATCH_TTL[3]
- CONFIG_IP_NF_MATCH_TCPMSS

[1] kernel 2.4.14
[2] kernel 2.4.14
[3] kernel 2.4.14

- CONFIG_IP_NF_MATCH_UNCLEAN
- CONFIG_IP_NF_MATCH_OWNER
- CONFIG_IP_NF_MATCH_STATE
- CONFIG_IP_NF_FILTER
- CONFIG_IP_NF_TARGET_REJECT
- CONFIG_IP_NF_TARGET_MIRROR
- CONFIG_IP_NF_NAT
- CONFIG_IP_NF_TARGET_MASQUERADE
- CONFIG_IP_NF_TARGET_REDIRECT
- CONFIG_IP_NF_TARGET_LOG
- CONFIG_IP_NF_TARGET_TOS
- CONFIG_IP_NF_TARGET_TCPMSS
- CONFIG_IP_NF_COMPAT_IPCHAINS
- CONFIG_IP_NF_COMPAT_IPFWADM

5 Vytváranie firewallu

- Firewall vytvárame vždy technikou všetko zakáž a niečo povoľ, nie naopak!!!

```
iptables -F
iptables -F -t nat
iptables -X
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

- Maškarádovanie vnútornej siete

```
echo 1 > /proc/sys/net/ipv4/ip_forward

# pri dynamicky pridelovanej IP (DHCP, PPP, ..)
iptables -t nat -A POSTROUTING -o eth0 -j MASQUARADE

# pri pevnej statickej IP
iptables -t nat -A POSTROUTING -s $INT_NETWORK -o eth0
-j SNAT --to $EXT-INTERFACE

# povolenie odpovedi a vztahujucich spojeni
iptables -A FORWARD -m state --state ESTABLISHED, RELATED
-j ACCEPT
iptables -A FORWARD -o $EXT-INTERFACE -s $INT-NETWORK
-j ACCEPT
```

- Povolenie v INPUT chaine príslušných serverov (DNS, SSH, FTP, HTTP, ..)
- Aplikovanie DROP, REJECT, LOG na všetky neprepustené pakety

6 FW na psilocybus.sh.cvut.cz

```
IPTABLES="/usr/local/sbin/iptables"
LOIF="lo"
NETIF="eth0"
MASQIF="eth1"
TUNNELIF="netb"
# /sbin/depmod -a

modprobe ip_conntrack_ftp
modprobe ip_nat_ftp
echo "1" > /proc/sys/net/ipv4/ip_forward
# zmazame obsah vsetkych chainsov
$IPTABLES -F -t nat
$IPTABLES -F
# zmazame jednotlive chainsy
$IPTABLES -X
# nastavime default POLICY pre incoming packety na DROP
$IPTABLES -P INPUT DROP
$IPTABLES -P FORWARD DROP
$IPTABLES -N icmp_packets
$IPTABLES -N tcp_packets_ext
$IPTABLES -N irc_allowed
$IPTABLES -N udpincoming_packets
echo Starting IPTables...
$IPTABLES -N allowed
# povolime len novovytvorene spojenia (SYN), uz vytvorene
# (ESTABLISHED) a suvisiace s vytvorenymi (RELATED, ftp-data napr.)
$IPTABLES -A allowed -p TCP --syn -j ACCEPT
$IPTABLES -A allowed -p TCP -m state --state ESTABLISHED,RELATED
-j ACCEPT
# zvysne TCP spojenia dropneme (vecicka koli portscannom)
$IPTABLES -A allowed -p TCP -j DROP
# Povolime Echo reply, Destinantion Unreachable, Redirect, Echo a
```

```
# Time Exceeded
$IPTABLES -A icmp_packets -p ICMP -s 0/0 --icmp-type 0 -j ACCEPT
$IPTABLES -A icmp_packets -p ICMP -s 0/0 --icmp-type 3 -j ACCEPT
$IPTABLES -A icmp_packets -p ICMP -s 0/0 --icmp-type 5 -j ACCEPT
$IPTABLES -A icmp_packets -p ICMP -s 0/0 --icmp-type 8 -j ACCEPT
$IPTABLES -A icmp_packets -p ICMP -s 0/0 --icmp-type 11 -j ACCEPT
# povolime TCP connect na SSH a SMTP (pre vonkajsi interfejs)
$IPTABLES -A tcp_packets_ext -p TCP -s 0/0 -m multiport
--dport 21,22,25,465,993,995,1234,8080 -j allowed
$IPTABLES -A tcp_packets_ext -p TCP -s 147.32.112.0/20
--dport 139 -j allowed
# povolime connect na nas identd z irc serverov
$IPTABLES -A irc_allowed -p TCP -s 194.1.128.5 --dport 113
-j allowed
$IPTABLES -A irc_allowed -p TCP -s 195.146.134.62 --dport 113
-j allowed
$IPTABLES -A irc_allowed -p TCP -s 194.1.128.5 --sport 6667
-j allowed
$IPTABLES -A irc_allowed -p TCP -s 195.146.134.62 --sport 6667
-j allowed
# povolime UDP reply z DNS serverov (nutne koli resolvovaniu)
$IPTABLES -A udpincoming_packets -p UDP -s 0/0 --source-port 53
-j ACCEPT
$IPTABLES -A udpincoming_packets -p UDP -s 0/0 -m multiport
--dport 53,517,518 -j ACCEPT
# pridame politiku icmp_packets, tcp_packets, udpincoming_packets
$IPTABLES -A INPUT -p ICMP -j icmp_packets
$IPTABLES -A INPUT -p UDP -j udpincoming_packets
$IPTABLES -A INPUT -p TCP -j irc_allowed
$IPTABLES -A INPUT -p TCP -j tcp_packets_ext
# povolime lokalne spojenie
$IPTABLES -A INPUT -i lo -j ACCEPT
# inak povolime uz vytvorene spojenia (ESTABLISHED)
# a suvisiace s vytvorenymi
$IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
# co neprejde, to zalogujeme
#$IPTABLES -A INPUT -j LOG --log-level 4
#--log-prefix "IPT INPUT packet died: "
# a pretoze sme slusni, tak odpovieme icmp-port-unreachable
$IPTABLES -A INPUT -j REJECT
# pripadna maskarada
$IPTABLES -t nat -A POSTROUTING -p all -s 192.168.0.0/24 -j SNAT
--to 147.32.114.77
# Source/Destination NAT pre tunnel
$IPTABLES -t nat -A POSTROUTING -p all -s 10.0.1.1 -j SNAT
--to 194.160.28.125
$IPTABLES -t nat -A PREROUTING -p all -d 194.160.28.125 -j DNAT
--to 10.0.1.1
```

Linky:

- http://wilder.sk/iptables.ps
- http://wilder.sk/nat.ps
- http://netfilter.samba.org
- http://people.unix-fu.org/andreasson/iptables-tutorial/iptables-tutorial.html
- http://www.malibyte.net/iptables/
- http://www.malibyte.net/security/fwscripts.html
- http://linuxguruz.org/iptables/

ĎAKUJEM ZA POZORNOSŤ.

OpenWEEKEND