Elegantno protiv napada grubom silom na SSH

Ne tako davno pojavili su se i postali vrlo česti pokušaji neovlaštenog pristupa SSH protokolom metodom grube sile. Napadači jednostavnim skriptama, koje usmjeravaju na cijele mreže, pokušavaju pristupiti na poslužitelje iskušavanjem velikog broja korisničkih imena i/ili lozinki. Gotovo svaki dan u logovima pojave se deseci, pa i stotine zapisa o pokušajima prijavljivanja na poslužitelj s pojedine IP adrese. Tijekom napada, svake minute zlonamjernici iskušaju i po 20 imena i/ili lozinki. Slijedi jedan skraćeni primjer iz logova:

```
Mar 6 02:49:10 stroj sshd[5210]: Illegal user mat from 141.5.9.6
Mar 6 02:49:12 stroj sshd[5210]: Illegal user rolo from 141.5.9.6
Mar 6 02:49:15 stroj sshd[5273]: Illegal user ice from 141.5.9.6
Mar 6 02:49:18 stroj sshd[2827]: Illegal user horde from 141.5.9.6
Mar 6 02:49:21 stroj sshd[2689]: Illegal user cyrus from 141.5.9.6
Mar 6 02:49:24 stroj sshd[6844]: Illegal user www from 141.5.9.6
Mar 6 02:49:27 stroj sshd[3144]: Illegal user run from 141.5.9.6
Mar 6 02:49:30 stroj sshd[4021]: Illegal user matt from 141.5.9.6
Mar 6 02:49:33 stroj sshd[7440]: Illegal user test from 141.5.9.6
Mar 6 02:49:35 stroj sshd[2140]: Illegal user test from 141.5.9.6
Mar 6 02:49:38 stroj sshd[2541]: Illegal user test from 141.5.9.6
Mar 6 02:49:41 stroj sshd[8455]: Illegal user devil from 141.5.9.6
Mar 6 02:49:55 stroj sshd[2402]: Illegal user tim from 141.5.9.6
```

Ako je na vaš poslužitelj instaliran CARNetov paket kernel-cn, imate sve potrebno, i posao je biti gotov za nekoliko minuta. Dovoljno je kopirati sljedeću skriptu i pokrenuti je. Ako već imate skriptu kojom postavljate pravila iptables, onda ćete znati koji dio trebate dodati u svoju skriptu. Samo pripazite da taj dio umetnete na odgovarajuće mjesto. Slijedi skripta:

----POČETAK----

```
#!/bin/sh
set -e
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Ciscenje FILTER tabela
iptables -t filter -F
iptables -t filter -X

# Svi kojima vjerujemo idu u odgovarajucu bijelu listu
TRUSTED_SSH="161.53.0.0/16"
iptables -N SSH_WHITELIST
iptables -F SSH_WHITELIST

iptables -A SSH_WHITELIST -s $TRUSTED_SSH -m recent --remove --name SSH -j ACCEPT
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --set --name SSH
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -j SSH_WHITELIST

# Rezanje pristupa i logiranje adresa s kojih dolaze SSH brute force napadi
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --update --seconds
 60 --hitcount 4 \
     --rttl --name SSH -m limit --limit 2/sec -j LOG --log-prefix "SSH_brute_force:"
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --update --seconds
 60 --hitcount 4 \
     --rttl --name SSH -j DROP
```

----KRAJ----

Nakon kreiranja nove ili unesenih promjena u staru, pokrećemo skriptu koja će tabele napuniti pravilima. Možemo odmah provjeriti rezultat:

```
# iptables -nL -v
```

I ne zaboravimo spremiti promjene kako bi se nova pravila učitala pri pokretanju poslužitelja:

```
# /etc/init.d/iptables save active
```

Što gornja pravila zapravo rade?

Sve navedeno omogućio nam je iptables modul "recent" (ipt_recent). Pomoću njega odredili smo, ako s neke IP adrese prema našem SSH portu 22 (--dport 22) stignu više od tri (--hitcount 4) nova (-m state --state NEW) TCP/IP paketa koji žele uspostaviti novu SSH konekciju, da se ta IP adresa blokira 60 sekundi (--seconds 60). Novi SSH paketi se ponovno počnu propuštati samo ako ih nije bilo u zadnjih 60 sekundi od zadnjeg pristiglog (--update).

Pravilom koje prethodi opisanom, logiramo samo po dva pokušaja svake sekunde (-m limit --limit 2/sec -j LOG) kako bismo spriječili DoS. Sve linije koje se zapisuju u logove imat će premetak (--log-prefix "SSH_brute_force:").

Više o opcijama koje pruža modul "recent" saznat ćete ovako:

```
# iptables -m recent --help
```

Nezaobilazni linkovi o ovoj temi su:

http://www.netfilter.org **[1]**

http://www.snowman.net/projects/ipt_recent **[2]**

- Logirajte [3] se za dodavanje komentara

sub, 2005-03-12 15:47 - Uredništvo**Kuharice:** Linux [4]
Kategorije: Sigurnost [5]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr./node/71

Links
[1] http://www.netfilter.org/
[2] http://www.snowman.net/projects/ipt_recent
[3] https://sysportal.carnet.hr./sysportallogin

[4] https://sysportal.carnet.hr./taxonomy/term/17
[5] https://sysportal.carnet.hr./taxonomy/term/30