Ipset, 1. dio

Bez zaštite poslužitelja vatrozidom (*firewallom*, ako vam je tako draže) odavno se ne može. Na mreži je previše ljudi s hakerskim sposobnostima, ali i onih koji samo misle da ih imaju. No, svi oni mogu uspješno napasti vaše poslužitelje i napraviti probleme, samo ako se odluče za to.

Iako postoje automatizirani sustavi zaštite, a ovdje prvenstveno mislimo na popularne fail2ban i OSSEC programe, nekad je pametno napraviti preventivnu zaštitu. Recimo, na poslužitelj vašeg kolege je provaljeno iz zemlje X. Iz određenih razloga pretpostavljate da će se možda pokušati provaliti i na vaše poslužitelje, pa želite spriječiti bilo koga iz te cijele zemlje da pristupi, primjerice, vašem webu.

Iako uopćeno govoreći, nije baš razborito blokirati cijele zemlje, ponekad je to jedino što možete učiniti, jer zaštita nije poznata ili moguća.

Problem nastaje u trenuku kada zaista želite blokirati neku zemlju. Ovdje se može raditi o desecima i stotinama raspona adresa, pa je problem u održavanju popisa tih adresa. Iako se za iptables može napraviti više datoteka u kojima će biti navedene adrese koje želite blokirati, nije praktično s njima baratati - većina se ipak zadovoljava standardnim *saved-active-inactive* kombincijama. Ovdje u pomoć dolazi ipset.

Pomoću ovog modula unutar iptablesa možete si olakšati način na koji rabite iptables. Možete imati osnovni vatrozid, koji brani samo ono najbitnije, a ostatak uključujete po potrebi. To izgleda ovako:

```
iptables -A INPUT -m set --set moja_pravila src -j DROP
```

Opcija -m uključuje dodatne module, primjerice "recent", "cluster", a u ovom slučaju "ipset". Da biste mogli rabiti ipset, morate ga instalirati jer ne dolazi u standardnoj instalaciji:

```
# apt-get install ipset ipset-source
...
The following extra packages will be installed:
  module-assistant
The following NEW packages will be installed:
  ipset-source module-assistant
...
Setting up ipset (2.5.0-1) ...
Setting up module-assistant (0.11.3) ...
Setting up ipset-source (2.5.0-1) ...
```

No, to nije sve. Sljedeća operacija se mora izvesti kako bi modul ipset ugradili u kernel. Restart poslužitelja nije potreban. Napravite:

```
# module-assistant auto-install ipset
```

ili jednostavnije:

```
# m-a a-i ipset

Updated infos about 1 packages
Getting source for kernel version: 2.6.32-5-686-bigmem
apt-get install linux-headers-2.6.32-5-686-bigmem
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  linux-headers-2.6.32-5-common linux-kbuild-2.6.32
The following NEW packages will be installed:
  linux-headers-2.6.32-5-686-bigmem linux-headers-2.6.32-5-common
  linux-kbuild-2.6.32

Done with /usr/src/ipset-modules-2.6.32-5-686-bigmem_2.5.0-1+2.6.32-45_i386.deb
dpkg -Ei /usr/src/ipset-modules-2.6.32-5-686-bigmem_2.5.0-1+2.6.32-45_i386.deb
Selecting previously deselected package ipset-modules-2.6.32-5-686-bigmem.
(Reading database ... 87619 files and directories currently installed.)
Unpacking ipset-modules-2.6.32-5-686-bigmem (from .../ipset-modules-2.6.32-5-68
Setting up ipset-modules-2.6.32-5-686-bigmem (2.5.0-1+2.6.32-45) ...
```

Zato što se radi o modulima unutar kernela, morali ste na ovaj način skinuti module assistant, izvorni kod kernela, modula ipset i još po koju sitnicu. No, ne morate duboko ulaziti u cijelu problematiku, dovoljno je da slijedite upute koje smo ovdje naveli.

Dobro, kako dalje? Kako se uopće prave setovi? Ništa lakše:

```
ipset --create moja_pravila nethash
ipset --add moja_pravila 109.228.64.0/18
ipset --add moja_pravila 79.140.144.0/20
ipset --add moja_pravila 195.66.160.0/19
ipset --add moja_pravila 85.94.96.0/19
ipset --add moja_pravila 77.222.0.0/19
ipset --add moja_pravila 78.155.32.0/19
ipset --add moja_pravila 95.155.0.0/18
ipset --add moja_pravila 109.228.64.0/18
ipset --add moja_pravila 46.33.192.0/19
...
```

U navedenom popisu mogu biti na stotine, pa i tisuće adresa. Pazite da to budu mrežne adrese, odnosno rasponi, ne miješajte ovdje i adrese hostova. Odnosno, probajte, dobit ćete:

```
ipset v2.5.0: Out of range cidr `109.228.113.111/32' specified
```

Sada kada ste napravili set pravila "moja_pravila", vrlo je jednostavno ubaciti taj set u iptables:

```
# iptables -A INPUT -m set --set moja_pravila src -j DROP
# iptables -L -n  | grep moja_pravila
DROP       all  --  0.0.0.0/0            0.0.0.0/0           match-
set   moja_pravila src
```

S jednim retkom koda blokirali ste tisuće adresa, na elegantan i brz način. U primjeru smo rabili

zastavicu "**src**", što naravno određuje da se pravila primjenjuju na dolazne adrese. Analogno, zastavica "**dst**" određuje da se radi o odredišnim adresama.

Dobro, a po čemu je to bolje od standardnog načina, to sve mogu i preko "običnih" iptables pravila, pitate se.

Iptables su moćna stvar, ali je rukovanje s velikim brojem pravila je nespretno, jer morate paziti na njihov poredak koji je jako bitan. Zbog toga može doći do neželjnih kombinacija, što može dopustiti vanjskim adresama više nego što ste htjeli, odnosno može čak i međusobno poništiti vašu prvobitnu namjeru. O tome u nastavku, gdje ćemo navesti i neke dodatne primjere koji će vam olakšati uporabu ipset modula.

- Logirajte [1] se za dodavanje komentara

pet, 2012-09-28 11:32 - Željko Borš**Kuharice:** Linux [2]
Kategorije: Software [3]
Operacijski sustavi [4]
Servisi [5]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr/node/1110

Links
[1] https://sysportal.carnet.hr/sysportallogin
[2] https://sysportal.carnet.hr/taxonomy/term/17
[3] https://sysportal.carnet.hr/taxonomy/term/25
[4] https://sysportal.carnet.hr/taxonomy/term/26
[5] https://sysportal.carnet.hr/taxonomy/term/28