Fail2ban - konfiguracija i uporaba, 3. dio

U prethodna dva nastavka [1] smo vam pokazali način rada, te osnovnu konfiguraciju i uporabu programa **fail2ban**. U ovom nastavku zaokružit ćemo priču, i objasniti kako napraviti svoj, odnosno prilagoditi neki postojeći filter svojim potrebama.

Kako sam fail2ban donosi filtere za većinu servisa koji će vam ikada trebati, bio nam je problem osmisliti neki novi filter. No, ipak smo se dosjetili jedne svima poznate pojave u apache logovima: tragovi potrage za bugovitim skriptama na sustavu.

Obično se traže stare inačice PHP skripti, a najčešće je to phpmyadmin. PhpMyAdmin je PHP skripta za jednostavan rad s MySql bazama podataka na vašem sustavu, ali je poznat po mnogobrojnim sigurnosnim rupama.

U vašim logovim često možete vidjeti unose slične ovima:

```
XX.YY.128.146 - - [18/Sep/2009:15:04:52 +0200] "GET
    /phpmyadmin/main.php HTTP/1.0" 404 361 "-" "-"
XX.YY.128.146 - - [18/Sep/2009:15:04:17 +0200] "GET
    /setup/phpmyadmin/main.php HTTP/1.0" 404 367 "-" "-"
XX.YY.128.146 - - [18/Sep/2009:15:04:31 +0200] "GET
    /administrator/phpmyadmin/main.php HTTP/1.0" 404 375 "-" "-"
XX.YY.128.146 - - [18/Sep/2009:15:04:31 +0200] "GET
    /admin/phpMyAdmin-2.5.6-rc2/main.php HTTP/1.0" 404 375 "-" "-"
```

Napadači žele "ispipati" imate li PhpMyAdmin, i koje je inačice. Naravno, obično se radi o *script-kiddies* korisnicima, ali koji ipak uz pomoć određenih programa mogu upasti na vaš stroj. Iz tog razloga je najbolje preventivno onemogućiti napadačevu IP adresu. Pa, krenimo redom.

U direktoriju /etc/fail2ban/filter.d napravimo novu datoteku apache-php.conf (izostavili smo komentare radi kratkoće, vi ih slobodno ostavite):

```
[Definition]
failregex = [[]client <HOST>[]] .*phpmyadmin.*$
            [[]client <HOST>[]] .*PhpMyAdmin.*$
ignoreregex = 161\.53\.XX\.\d
              161\.53\.\d\.YY
```

Umjesto XX i YY upišite IP adrese i adrese mreže svog LAN-a, i adrese vaših suradnika koji trebaju pristu PhpMyAdminu. Slično možete i za bilo koji dio IP adrese, s napomenom da oznaka '\d' označava regex [2]klasu '[0-9]', dakle obuhvaća sve brojeve od 0 do 9. Ovu sintaksu, među ostalim, rabi programski jezik Python u kojem je napisan fail2ban.

U datoteku jail.conf dodamo retke:

```
[apache-php]

enabled = true
```

```
port    = http,https
filter  = apache-php
action   = iptables[name=apache-php, protocol=tcp]
logpath  = /var/log/apache*/*error.log
maxretry = 5
```

i napravimo

```
# fail2ban-client reload
```

Što smo ovime napravili? Rezultat će biti zabrana pristupa bilo kojem klijentu (koji nije u varijabli ignoreregex), a koji pokuša više od 5 puta pristupiti PhpMyAdmin programu. Ovo će odraditi iptables.conf, no vi možete birati i između nekoliko drugih načina zaštite (primjerice preko tcp_wrappera).

Sami regularni izrazi su *case-sensitive*, i morat ćete pripaziti na velika i mala slova, što uopće nije loše kako slučajno ne bi onemogućili previše stvari odjednom.

Umjesto zabrane, možete jednostavno poslati mail sebi ili drugim kolegama da se nešto događa. U iptables.conf upišite:

```
actionban = iptables -I fail2ban-<name> 1 -s <ip> -j DROP
            printf %%b "Pozdrav,\n
            Klijent <ip> je blokiran zbog <failures> pokusaja\n
            pristupa po pravilu <name>.\n
            \n
            Vas Fail2Ban" | mail -s "[Fail2Ban] <name>: <ip> blokiran" pero@domena.hr
```

Uz zabranu, fail2ban će poslati mail s osnovnim informacijama na neku adresu. Oprezno s ovom funkcijom, kako pretjerani broj mailova ne bi napravio DDoS sam po sebi!

Na kraju, samo ćemo navesti konfigurabilne parametre koje možete rabiti u svojim "zatvorima". Iako su im imena samoobjašnjiva, radi potpunosti navest ćemo ih, zajedno s pretpostavljenim vrijednostima:

```
maxretry        3
```

Broj pokušaja, točnije, broj puta kada je neki redak u logovima odgovorao regexu koji smo postavili. Radi se o
individualnim brojevima za svaku IP adresu.

```
filter          Ime filtera (u našem slu?aju apache-php).
```

Filter se nalazi u direktoriju /etc/fail2ban/filters.d, u našem slučaju bi to bio apache-php.conf. Vrijedi napomenuti da svako pravilo unutar filtera povećava brojač (maxretry) za jedan, naravno ukoliko se redak u logu poklapa sa zadanim regularnim izrazima.

```
findtime        600 sec
```

Brojač će se vratiti na nulu, ukoliko unutar ovog vremena s iste adrese ne bude nikakve dodatne aktivnosti. Neki programi pokušavaju proći "ispod radara" i svoje pokušaje smanjuju na jedva primjetnu razinu. Neke pak treba što prije detektirati i onemogućiti, pa je namještanje ove vrijednosti

individualna potreba svakog sistemca i stroja.

```
bantime         600 sec
```

Vremenski period koliko će određena IP adresa biti zabranjena.

```
logpath         /var/log/messages
```

Jednostavno, putanja do log datoteku koju ćemo nadzirati. Može biti /var/log/syslog, ili bilo što drugo, pa čak i izvan /var/log.

Obavezno istestirajte nova pravila prvo na neprodukcijskom stroju, a ukoliko zapnete konzultirajte Wiki dokumentaciju na http://www.fail2ban.com/wiki [3], a pomoć za Python regularne izraze možete naći na http://docs.python.org/dev/howto/regex.html [4].

Za općenite regularne izraze, jako dobar izvor informacija je web sjedište http://www.regular-expressions.info/ [5].

Sretno u uporabi fail2ban sustava!

- Logirajte [6] se za dodavanje komentara

uto, 2009-10-13 00:30 - Željko Borš**Kuharice:** Linux [7]
Kategorije: Software [8]
Servisi [9]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/643

Links
[1] https://sysportal.carnet.hr/node/542
[2] https://sysportal.carnet.hr/system/files/RegExNew.ppt
[3] http://www.fail2ban.org/wiki
[4] http://docs.python.org/dev/howto/regex.html
[5] http://www.regular-expressions.info/
[6] https://sysportal.carnet.hr/sysportallogin
[7] https://sysportal.carnet.hr/taxonomy/term/17
[8] https://sysportal.carnet.hr/taxonomy/term/25
[9] https://sysportal.carnet.hr/taxonomy/term/28