Logcheck, 3. dio

Kreiranje i testiranje pravila

Testiranje vaših pravila možete napraviti preko naredbe:

```
sed -e 's/[[:space:]]*$//' /var/log/syslog | egrep -i 'Access Denied'
```

(ovdje naredba sed samo filtrira prazna retke, koji su opasni jer će uključiti baš svako pravilo i odgovarajući alarm).

Ukoliko se redak iz loga pokaže, vaše pravilo je napisano kako treba. Ako ovo pravilo upišete u neki od ignore direktorija, unosi će biti ignorirai. Ukoliko ga pak upišete u **violations.d** ili **cracking.d**, navedeni redak će biti upisan u odgovarajućoj sekciji izvještaja (**System Events** i **Security Events**).

Treba svakako napomenuti da se datoteke s pravilima iščitavaju preko standardnog run-parts mehanizma, što znači da možete pojedina pravila privremeno izbaciti iz uporabe tako da im dodate nastavak **.disabled**. Također, backup pojedinih editora se ignorira (popularni editor **joe** dodaje tildu na kraj stare inačice datoteke, primjerice **apache~**)

Primjer 1

U izvješću se često pojavljuju neki unosi koje ne želimo vidjeti, jer nisu oznaka napada niti problema. Primjerice, anacron ostavlja dosta logova:

```
Jun 13 07:30:02 server anacron[24367]: Anacron 2.3 started on 2007-06-13
Jun 13 07:30:02 server anacron[24367]: Will run job `cron.daily' in 5 min.
Jun 13 07:30:02 server anacron[24367]: Will run job `cron.weekly' in 10 min.
Jun 13 07:30:02 server anacron[24367]: Jobs will be executed sequentially
Jun 13 07:35:02 server anacron[24367]: Job `cron.daily' started
Jun 13 07:35:02 server anacron[24411]: Updated timestamp for job `cron.daily' to
  2007-06-13
```

Ovi nam unosi ne znače ništa posebno, osim možda nakon instaliranja tog paketa da se uvjerimo da radi. Zato ćemo u /etc/logcheck/ignore.d.server/anacron upisati:

```
^\w{3} [ :0-9]{11} [._[:alnum:]-]+ anacron\[[0-9]+\]: Anacron [.[:alnum:]]+ started o
n [0-9-]+$
^\w{3} [ :0-9]{11} [._[:alnum:]-]+ anacron\[[0-9]+\]: Jobs will be executed sequentia
lly$
^\w{3} [ :0-9]{11} [._[:alnum:]-]+ anacron\[[0-9]+\]: Normal exit \([0-9]+ jobs* run\
)$
^\w{3} [ :0-9]{11} [._[:alnum:]-]+ anacron\[[0-9]+\]: Will run job `[._[:alnum:]-]+'
in [0-9]+ min\.$
^\w{3} [ :0-9]{11} [._[:alnum:]-]+ anacron\[[0-9]+\]: Job `[._[:alnum:]-]+' started$
^\w{3} [ :0-9]{11} [._[:alnum:]-]+ anacron\[[0-9]+\]: Job `[._[:alnum:]-]+' terminate
d$
```

```
^\w{3} [ :0-9]{11} [._[:alnum:]-]+ anacron\[[0-9]+\]: Job `[._[:alnum:]-]+' terminate
d \(mailing output\)$
^\w{3} [ :0-9]{11} [._[:alnum:]-]+ anacron\[[0-9]+\]: Updated timestamp for job`[._[:
alnum:]-]+' to [0-9-]+$
```

Navedeni upisi se mogu naći u datoteci **/etc/logcheck/ignore.d.workstation/anacron**, pa se može od tamo jednostavno prekopirati.

Primjer 2

```
Jun 18 08:29:08 linux named[15362]: client 161.53.XXX.86#1054: update 'institucija.hr
/IN' denied
```

Ovo je poruka koja označava da Windows klijenti pokušavaju nadopuniti DNS bazu, što po defaultu nije dopušteno. Jedino pravo rješenje je preko Group Policya ili ručno na klijentu isključiti opciju "Register this connection (...) in DNS".

No, u logchecku ovu poruku možemo filtrirati preko ovog regularnog izraza:

```
.*named.*client.*update.*denied
```

Problem s ovim filterom je taj što će filtrirati i ovakve unose, koji mogu predstavljati napad na resurse vašeg poslužitelja:

```
Jun 18 08:43:10 linux named[15362]: client 89.172.XXX.YYY#56419: update 'domena.hr/IN
' denied
```

Regularni izrazi mogu pomoći u ovakvim slučajevima:

```
.*named.*client \[161\.53\.XXX\.[0-9]+\].*update.*denied
```

Ovaj izraz će filtrirati samo klijente s adresom koja počinje s 161.53.XXX (naravno, ovdje stavite svoju adresu), dok će sve ostale biti prikazane u izvješću.

Primjer 3

Jun 18 08:07:30 linux pop3-login: Login: korisnik [161.53.XXX.YYY]

```
^\w{3} [ :0-9]{11} [._[:alnum:]-]+ pop3-login: Login: [.[:alnum:]-]+\[[0-9.]+\]$
```

Puni regularni izraz je predugačak i teško razumljiv, možda je bolje skratiti cijeli izraz:

```
.*pop3-login: Login:.*
```

Potreban je oprez kod skraćivanja, kako ne bismo previše toga isfiltrirali i na taj način previdjeli prave napade i upozorenja.

S ovim člankom smo završili s analizom logchecka. Na vama je da stečeno znanje primjenite na vašem poslužitelju i u vašem okruženju.

- Logirajte [1] se za dodavanje komentara

sri, 2009-07-01 08:27 - Željko Boroš**Kuharice:** Linux [2]
Kategorije: Servisi [3]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr./node/606

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