OSSEC: Kako ignorirati ugrađena pravila i dodati svoja?

OSSEC je multiplatformski sustav za detekciju napada otvorenog koda, i već dulje vrijeme je u ponudi CARNetovih paketa. U potpunosti je spreman za autonoman rad nakon instalacije, a za početak je dovoljno upoznati se s njegovim pravilima ("*rules*"), točnije kako ignorirati pravila koja generiraju lažne pozitive, te dodati svoja vlastita pravila. Kako ignorirati određena pravila smo ovlaš spomenuli u članku http://sistemac.carnet.hr/node/625 [1], koji se tiče ignoriranja određenih unosa u logovima koje generira BIND. No, postoji mnogo više mogućnosti od ove.

U članku smo naveli ovaj primjer:

```
<rule id="100131" level="0">
  <if_sid>1002</if_sid>
  <program_name>^named</program_name>
  <match>denied</match>
  <description>BIND denied upozorenja</description>
</rule>
```

SID koji se spominje u direktivi **<if_sid>** se odnosi na broj pravila na koje želite utjecati, a njega ćete dobiti u mail poruci, npr. "Rule: 1002 fired" . Vi dodavanjem ovog pravila pravite "*child rule*", preko kojeg možete utjecati na krajnji rezultat (koji bi se dogodio da niste uveli svoje pravilo).

Što se tiče određivanja vašeg vlastitog broja, morat ćete poštovati odluku razvijatelja da korisnička pravila rabe brojeve veće od sto tisuća (100000).

Svoja pravila upišite u datoteku **/var/ossec/rules/local_rules.xml**. Kako je tamo već dodana CARNetova modifikacija ugrađenih pravila, nemojte upisivati ništa unutar bloka "**Begin update by CARNet...**" i "**End update by CARNet...**".

Svoja pravila stavite unutar **<group></group>** oznaka ispred ili iza CARNetovog bloka. Ukoliko grupa ne postoji, možete kreirati svoju:

```
<group name="local">
  <rule id=...>
   ...
  </rule>
</group>
```

Još samo trebate zapamtiti da brojevi pravila moraju biti jedinstveni, a dalje ih samo nanižite numerički jedan iza drugog, povećavajući broj za jedan, 100001, 100002 itd.

Isto kako možemo modificirati postojeća pravila unutar OSSEC-a, tako imamo i mogućnost da dodamo svoja vlastita pravila, u istoj datoteci gdje smo upisivali modifikacije postojećih pravila (local_rules.xml).

OSSEC zapise u logovima raščlanjuje na sljedeći način:

```
Jun  5 11:42:39 posluzitelj saslauthd[3020]: pam_unix(smtp:auth):
```

```
authentication failure; logname= uid=0 euid=0 tty= ruser= rhost=
```

time -> Jun 5 11:42:39
hostname -> posluzitelj
program_name -> saslauthd
log -> pam_unix(smtp:auth): authentication failure; logname= uid=0 euid=0 tty= ruser= rhost=

Nakon ovoga, moguće je dodatno dekodiranje (definirano preko decoders.xml) pa možete dobiti još ključnih riječi, poput srcip, dstip, id, srcport i tako dalje. Za većinu slučajeva, bit će dovoljno i ovo što imamo do sada. Nakon rašćlanjivanja dobit ćemo ključne riječi, odnosno varijable s kojima možemo dalje raditi i rafinirati naše pravilo.

U navedenom primjeru imamo direktive **<program_name>** i **<match>**. S <program_name> možemo ograničiti djelovanje pravila na točno određeni program, u ovom slučaju saslauthd. <Match>, i njegov moćniji "partner" <regex> (koji omogućava uporabu regularnih izraza) se odnose isključivo na "log" dio, u ovom slučaju na dio retka "pam_unix(smtp:auth): authentication failure...".

Ovo je jako bitno zapamtiti kod pravljenja svojih pravila, da ne bi pokušavali "matchirati" od početka retka u logu (konretno, to je datum i vrijeme).

Ostalo je za objasniti još samo "**level**". OSSEC podržava petnaestak razina ozbiljnosti događaja ("severity"). Sve razine od 7 nadalje će generirati mail administratoru (ovo se može promijeniti u datoteci ossec.conf), dok će razina 0 poništiti bilo koju drugu razinu, ukoliko pravite "child" pravilo. To je upravo ono što želimo, ugasiti poruke za koje smo utvrdili da nam ne znače ništa i samo zatrpavaju sandučić elektroničke pošte.

Ukoliko želimo promijeniti razinu kod koje se šalju upozorenja mailom, u datoteci /var/ossec/etc/ossec.conf promijenite unos unutar oznaka **<email_alert_level>**:

```
<email_alert_level>7</email_alert_level>
```

u neku drugu, višu ili nižu, razinu. Ovo možda nije za preporučiti dok se bolje ne upoznate sa sustavom, pa jednostavno možete unutar vašeg pravila dodati unos

```
<options>alert_by_email</options>
```

pa će vaše pravilo uvijek generirati upozorenje mailom, bez obzira na globalnu postavku razine definirane unutar ossec.conf.

Kao primjer, navest ćemo rješenje za konkretan upit koji smo dobili od kolege sistem-inženjera kako da OSSEC šalje upozorenja ako se aktivira zaštita iptablesa, koju smo opisali u članku http://sistemac.carnet.hr/node/71.

Ovo je lako učiniti, sada kada znamo na koji način OSSEC raščlanjuje unose u logovima. Odgovarajući redak je:

```
Jun  9 14:35:00 posluzitelj kernel: [1296546.520971] SSH_brute_force:IN=eth0 OUT=
   MAC=00:0e:0c:ab:64:cd:00:1b:90:a0:00:46:08:08 SRC=161.53.XX.YYY
   DST=161.53.ZZZ.ZZ LEN=60 TOS=0x00 PREC=0x00 TTL=62 ID=6790
   DF PROTO=TCP SPT=16075 DPT=22 WINDOW=5840 RES=0x00 SYN URGP=0
```

Nakon raščlanjivanja, imamo:

time -> Jun 9 14:35:00
hostname -> posluzitelj
program_name -> kernel
log -> [1296546.520971] SSH_brute_force:IN=eth0...

Od ovih informacija, lako možemo napraviti pravilo:

```
<rule id="100001" level="7">
 <program_name>^kernel</program_name>
 <match>SSH_brute_force</match>
 <description>Javlja da se uklju?ilo SSH_brute_force pravilo</description>
</rule>
```

Ovo pravilo upišite u svoju grupu pravila (između vlastitih <group></group> pravila), i restartajte OSSEC. Sada biste trebali početi dobijati obavijesti u trenutku kada se uključi zaštita zbog prekomjernih pokušaja spajanja na SSH daemon.

Naravno da ovakva pravila možete napisati za bilo koji servis, te ih možete imati neograničen broj. Nemojte ni pretjerivati, jer ćete početi ignorirati preveliku količinu ovakvih mailova sa sigurnosnim upozorenjima.

- Logirajte [2] se za dodavanje komentara

čet, 2010-06-10 13:59 - Željko Boroš**Kuharice:** Linux [3]
Kategorije: Servisi [4]
Vote: 5

Vaša ocjena: Nema Average: 5 (2 votes)

Source URL: https://sysportal.carnet.hr/node/751

Links
[1] https://sysportal.carnet.hr/node/625
[2] https://sysportal.carnet.hr/sysportallogin
[3] https://sysportal.carnet.hr/taxonomy/term/17
[4] https://sysportal.carnet.hr/taxonomy/term/28