Logcheck savjeti i trikovi

Logcheck je program koji se periodično izvršava i pregledava sistemske logove i prijavljuje bilo kakvu nepravilnost koju nađe. Kako je moguće da se pojavi veliki broj lažnih pozitiva, obično je potrebno modificirati pravila. U ovoj e-knjizi ćemo pojasniti kako to napraviti, kao i kako prilagoditi instalaciju logchecka vašim potrbama.

- Logirajte [1] se za dodavanje komentara

Logcheck, 1. dio


Iako postoje noviji, a vjerojatno i bolji *log watcheri*, logcheck je svakako jedan od najčešće korištenih kod CARNet sistem administratora. Uzrok je ovom vjerojatno činjenica da je dolazio u obliku CARNet paketa. I danas, kad imamo napredniji OSSEC sustav, koji može i puno više, je gotovo redovito instaliran na poslužiteljima CARNet članica. U tri nastavka pokušat ćemo objasniti sve "male tajne" logchecka.

Logcheck - početak i kraj

Logcheck je jedan onih programa koji je zamišljen da pomogne sistem administratorima u obavljanju svakodnevnih (dosadnih i mukotrpnih) poslova, kao što je to praćenje log datoteka. Logcheck će umjesto administratora pregledavati logove u određenom vremenskom razodoblju, odbaciti nebitne unose, te u skladu s ugrađenim pravilima slati izvješća i upozorenja administratoru.

Ne trebamo posebno napominjati da su logovi početak i kraj svakog kvalitetnijeg administriranja poslužitelja, jer *u njima sve piše*: kad je problem nastao, tko ga je prouzrokovao, a gotovo uvijek nagovještava kako problem riješiti. Ukoliko logovi ili njihov dio "nestanu", to je znak za alarm, jer je to prvo što će hacker koji je upao na sustav napraviti - **obrisati logove**.

Logcheck je bez sumnje jako koristan program, ali njegova konfiguracija može biti dosta "zapteljana". Zapravo, malo smo rekli, konfiguracija je zbog regularnih izraza prilično mukotrpna. No, ne mora uvijek biti.

Kako konfiguracija ne bi bila tako teška, treba razumjeti način na koji logcheck radi. Zato nećemo previše pažnje obraćati na opcije samog programa (koje možete u svakom trenutku vidjeti s naredbom "man logcheck"), nego na princip, logiku rada i čitanja datoteka s regularnim izrazima (više o regularnim izrazima u CARNetovom seminaru na adresi http://sistemac.carnet.hr/system/files/RegExNew.ppt [2]).

Umjesto jedne ili dvije konfiguracijske datoteke, logcheck ima cijeli niz datoteka koje određuju njegovo ponašanje, iako su samo dvije "prave" konfiguracijske datoteke (**logcheck.logfiles** i **logcheck.conf**). Ostale su datoteke popunjene regularnim izrazima prema kojima koji će biti filtrirani unosi u logovima.

Sve se konfiguracijske datoteke nalaze u direktoriju /etc/logcheck, gdje logcheck.conf određuje osnovno ponašanje programa, a logcheck.logfiles određuje koje logove logcheck provjerava (obično samo auth.log i syslog).

Nama su zanimljivi ovi direktoriji unutar /etc/logcheck direktorija:

```
drwxr-s---  2 root logcheck 1024 May 29  2005 cracking.d
drwxr-s---  2 root logcheck 1024 May 16  2004 cracking.ignore.d
drwxr-s---  2 root logcheck 1024 Apr 27 08:14 ignore.d.paranoid
drwxr-s---  2 root logcheck 2048 Apr 27 08:14 ignore.d.server
drwxr-s---  2 root logcheck 1024 Nov  5  2006 ignore.d.workstation
drwxr-s---  2 root logcheck 1024 May 29  2005 violations.d
drwxr-s---  2 root logcheck 1024 Nov  8  2006 violations.ignore.d
```

Ovakav način konfiguracije je nekima možda zbunjujuć (no sve je češći radi lakšeg održavanja i nadogradnje sustava). Objasnit ćemo što znači svaki od direktorija.

Logcheck ima tri **niza pravila**, nazvana "**Attack Alerts**", "**Security Events**" i "**System Events**", koji se redom primjenjuju za svaki redak u log datotekama.

Svakom nizu pravila pripada odgovarajući direktorij:

Attack: **cracking.d** i **cracking.ignore.d**
Security: **violations.d** i **violations.ignore.d**
System: **ignore.d.paranoid**, **ignore.d.server**, **ignore.d.workstation**

(zašto nizovi pravila nemaju isto ime kao i direktoriji, što bi sigurno olakšalo snalaženje i konfiguraciju, treba pitati autore).

No, to nije sve. Tri direktorija koji počinju s **ignore.d.*** ujedno označavaju i razinu prijave problema (**REPORTLEVEL**, podešava se u datoteci /etc/logcheck/logcheck.conf).

Postojeće razine izvještavanja su:

Paranoid

Primjenjuje se samo osnovna pravila za filtriranje, što nužno dovodi do većeg izvješća. Zato je ova razina prikladna samo na sustavima sa malim brojem servisa (na vatrozidu, primjerice)

Server

Na ovoj razini filtriraju se samo osnovne i repetitivne poruke, kako bi ispis bio pregledan, a potencijalni napadi uočljiviji. Ipak, sve bitne poruke ostaju, pa je ova razina pogodna za produkcijske poslužitelje.

Workstation

Ova razina je pogodna za poslužitelje koji nisu kritični za produkciju, i kao što ime sugerira, korisnička računala pod linuxom.

Za tipični poslužitelj u CARNetu, ni ne možemo rabiti drugu opciju do "**server**".

U sljedećem nastavku, opisat ćemo na koji način logcheck radi, te u koje datoteke treba upisivati vlastita pravila, kako nas logcheck ne bi stalno "bombardirao" lažnim upozorenjima.

- Logirajte [1] se za dodavanje komentara

pon, 2009-06-29 22:05 - Željko Borš**Kuharice:** Linux [3]
Kategorije: Servisi [4]
Vote: 4

Vaša ocjena: Nema Average: 4 (1 vote)

Logcheck, 2. dio

Kako logcheck zapravo radi?

Pomoću pomoćnog programa "**logtail**", iz sistemskih logova **auth.log** i **syslog** izdvajaju se linije koje do tog trenutka nisu bile nijednom pregledane (**logtail** vodi o tome računa). Daljnje izvršavanje preuzima egrep, proširena inačica naredbe grep (budimo iskreni i recimo da je to samo skripta koja pokreće grep sa posebnom opcijom -E).

Ukratko ćemo objasniti naredbu (e)grep. Ona iz linija teksta u datoteci ili proslijeđenih preko STDIN-a (standardnog ulaza) izdvaja one linije koje odgovaraju zadanim uvjetima. Uvjet je obično fiksni niz znakova, ali egrep zna raditi i sa regularnim izrazima, što logcheck bogato koristi. I negativna selekcija je moguća, dakle mogu se izdvojiti linije koje ne odgovaraju zadanim uvjetima.

Egrep će iz proslijeđenih mu linija logova izdvojiti sve one koje odgovaraju regularnim izrazima upisanim u datotekama u direktoriju **cracking.d**. Ukoliko je tako konfigurirano u logcheck.conf (**SUPPORT_CRACKING_IGNORE=1**), sada se iz izvješća brišu linije koje odgovaraju unosima u datotekama u direktoriju cracking.ignore.d. Važno je napomenuti da se linije koje se ovdje definiraju neće prenijeti u niže slojeve, nego će biti potpuno ignorirani od strane logchecka.

One linije koje su prepoznate pojavit će se u mail izvješću pod naslovom "**Security Alerts**" (zašto se ne zove "**Attack Alerts**", treba pitati autore).

U normalnim situacijama, izvješće "**Security Alerts**" će rijetko postojati. Postavlja se pitanje je li u tom trenutku provala već izvršena, te je ovo samo suvišna obavijest? S druge strane, svaki će "pošteni" hacker prvo obrisati kompromitirajuće logove, ne dajući šansu logchecku da upozori sistem administratora.

Zatim, slijedi procesiranje logova u sloju "**Security Events**", koji služi za praćenje manje bitnih unosa u logovima (nisu toliko kritični), ali mogu ukazati na neki problem.

U ovom sloju se obrađuju sve preostale linije koje su prošle "**Attack Alerts**" filter. Ovo će izvješće biti znatno bogatije, i biti poslano pod dijelom nazvanim "**Security Events**". Vrijede i druge odrednice utvrđene u prethodnom sloju, s tim da su odgovarajući direktoriji za ovaj sloj **violations.d** i **violations.ignore.d**.

Treba dodati da ako postoje posebne datoteke za pojedine pakete u **cracking.d** i **violations.d**, u izvješću će se pojaviti dodatna zaglavlja, "Security Alerts for paket" i "Security Events for paket". Ako se u logovima pronađe
redak koji odgovara pravilima u tim datotekama, onda ti retci neće biti duplicirani u izvješću.

Sljedeći sloj, "**System Events**" ima samo odgovarajuće "ignore" direktorije, jer se sve preostale linije iz loga biti poslane u ovaj sloj i pojaviti se u izvješću. Logično, ovo bi potencijalno mogao biti velik broj linija, zato su
ignore.d.* direktoriji i najnapučeniji, kako bi se broj linija u izvješću sveo na minimum.

Datoteke za konfiguraciju filtera

Svaki od filtera ima regularne izraze za određivanje što treba prijaviti, a što treba ignorirati. Ostatak linija ide u niži sloj, a nakon obrade ide u zadnji, koji ima samo set pravila za ignoriranje pravila (**ignore.d.***).

Ovdje su autori odlučili dodatno zakomplicirati život korisnicima njegovog paketa. Naime, ovdje treba razlikovati tri vrste datoteka (plus još dvije vrste datoteka koje imaju veću važnost od drugih):

1. ./paket, npr. apache

One sadržavaju regularne izraze za pojedine pakete, koji će pojedine unose u log datotekama prepoznati kao napade, ili će ignorirati bezopasne unose.

Filteri u ovim datotekama nikada ne utječu na filtere u datotekama za druge pakete. Ako imate filter koji će ignorirati niz znakova "access denied" u datoteci "apache", ona neće utjecati da se taj niz znakova ignorira u
log unosima koje kreiraju drugi paketi.

Podrazumijeva se da ove datoteke postavlja paket **logcheck-database**, i njih u principu ne treba dirati.

2. ./logcheck i ./logcheck-paket

U "logcheck" datoteci se nalaze generička pravila, odnosno pravila koja vrijede za sve pakete. Ova pravila, kako smo gore i napisali, imaju prednost nad pojedinačnim pravilima u paketskim datotekama. Tako, ako je isti filter naveden i u "logcheck" i u "apache" datoteci, "logcheck" ima prednost i obavijest će ipak biti poslana. Ukoliko ipak želite da specifične paketske datoteke imaju prednost nad generičkim pravilima navedenim u datoteci "logcheck", možete upotrijebiti format "logcheck-paket". Filteri u ovako formiranim datotekama imaju
prednost nad generičkim pravilima.

3. ./local i ./local-paket

Ove datoteke su najzanimljive sistem administratorima. Razlog je jednostavno taj što ove datoteke nisu dio paketa i nikad neće biti "pregažene" novim inačicama i nadogradnjama. Datoteke koje dolaze s paketom su označene kao "Conffile" i kod nadogradnje za svaku promjenu ćete biti upitani želite li instalirati inačicu iz paketa ili zadržati staru.

Dakle, ukoliko želite mijenjati pravila, najbolje je da to činite preko local-* datoteka, jer time ne gubite promjene prilikom nadogradnji. Format "local-paket" rabite kad želite da vaša pravila imaju prednost na paketskim, ali i generičkim pravilima. Jedino treba pripaziti da vaša pravila ne budu previše generička i na taj način sakriju unose koje bi svakako trebalo vidjeti.

U sljedećem, posljednjem nastavku, ćemo opisati kako trebaju izgledati datoteke s pravilima.

- Logirajte [1] se za dodavanje komentara

uto, 2009-06-30 13:16 - Željko Boroš**Kuharice:** Linux [3]

Kategorije: Servisi [4]
Vote: 0

No votes yet

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 [3]
Kategorije: Servisi [4]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr./node/694

Links
[1] https://sysportal.carnet.hr./sysportallogin
[2] https://sysportal.carnet.hr./system/files/RegExNew.ppt
[3] https://sysportal.carnet.hr./taxonomy/term/17
[4] https://sysportal.carnet.hr./taxonomy/term/28