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 [1]).

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 [2] se za dodavanje komentara

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

Vaša ocjena: Nema Average: 4 (1 vote)

Source URL: https://sysportal.carnet.hr/node/604

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