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.

uto, 2009-06-30 13:16 - Željko Boroš**Kuharice:** Linux [2]
Kategorije: Servisi [3]
Vote: 0

Source URL: https://sysportal.carnet.hr/node/605

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