SEC - jednoduchý korelátor udalostí

ADRIÁN VANČO, Fakulta informatiky a informačných technológií STU, SVK

TODO.

Additional Key Words and Phrases: Jednoduchý korelátor udalostí (SEC)

ACM Reference Format:
Adrián Vančo. 2018. SEC - jednoduchý korelátor udalostí. *ACM Trans. Graph.* 37, 4, Article 111 (August 2018), 3 pages. https://doi.org/10.1145/1122445.1122456

1 FUNKČNÝ OPIS BEZPEČNOSTNÉHO NÁSTROJA

SEC je nástroj na koreláciu udalostí pre pokročilé spracovanie udalostí, ktorý možno využiť na monitorovanie denníka udalostí, na správu siete a bezpečnosti, na detekciu podvodov (napr. manipulácií so súbormi) a na akúkoľvek inú úlohu, ktorá zahŕňa koreláciu udalostí. Korelácia udalostí je postup, pri ktorom sa spracováva tok udalostí s cieľom zistiť (a reagovať na) určité skupiny udalostí, ktoré sa vyskytujú v rámci vopred definovaných časových okien. Mnoho tradičných systémov na správu (koreláciu) udalostí ukladá udalosti do databázy a vykonáva databázové dotazy na implementáciu korelácie nad udalosťami. Takéto systémy sú však ťažkými riešeniami a často zahŕňajú komplexnú databázovú infraštruktúru na vyhradenom hardvéri.

Na rozdiel od toho je SEC ľahký a na platforme nezávislý korelátor udalostí napísaný v Perl, ktorý beží ako jeden proces. Používateľ ho môže spustiť ako démona, použiť ho v shell pipeline, spustiť ho interaktívne v termináli, spustiť mnoho procesov SEC súčasne pre rôzne úlohy a použiť ho mnohými inými spôsobmi.

SEC číta riadky zo súborov, pomenovaných kanálov alebo štandardného vstupu, porovnáva riadky so vzormi (ako regulárne výrazy alebo Perl podprogramy) na rozpoznávanie vstupných udalostí a koreluje udalosti podľa pravidiel vo svojom konfiguračnom súbore (súboroch). SEC môže produkovať výstup spustením externých programov (napr. snmptrap alebo mail), zapisovaním do súborov, odosielaním údajov na servery založené na TCP a UDP, volaním predkompilovaných podprogramov Perl atď.

1.1 Konfiguračný súbor

Pravidlá sa zapisujú do konfiguračného súboru a oddeľujú sa prázdnymi riadkami alebo pomocou komentárov (začínajú symbolom „#“). To znamená, že sa tieto elementy vo vnútri samotného pravidla vyskytovať nemôžu. Pokiaľ je nejaký riadok pravidla príliš dlhý, je možné použiť symbol „\“ a pokračovať na ďalšom riadku.

Author's address: Adrián Vančo, xvancoa@stuba.sk, Fakulta informatiky a informačných technológií STU, Ilkovičova 2, 842 16 Karlova Ves, Bratislava, SVK.

0730-0301/2018/8-ART111 $15.00
https://doi.org/10.1145/1122445.1122456

1.2 SEC pravidlá

Každé pravidlo obsahuje informáciu, akého je typu.
SEC má zabudované napríklad tieto pravidlá:

- **Single** – Ak nastane zhoda, okamžite sa vykoná akcia (reakcia na udalosť), ktorá je špecifikovaná v rámci tohto pravidla. Jednoduché pravidlo, ktoré nehľadá žiadne korelácie.
- **Suppress** – Tu naopak pokiaľ zhoda nastane, tak sa žiadna akcia nevykoná. Hľadanie zhody bude však pokračovať prechádzaním ostatných pravidiel. V predvolenom nastavení totiž akonáhle SEC nájde prvú zhodu, potom už ďalšiu v pravidlách nehľadá. Toto pravidlo môže slúžiť na filtráciu udalostí.
- **Calendar** – Tento typ je špecifický, pretože ako jediný ignoruje vstupné logy. Umožňuje naplánovať nejakú akciu na konkrétny čas.
- **SingleWithScript** – Pri zhode sa spustí definovaný skript a po jeho dobehnutí sa vykoná jedna z dvoch akcií, v závislosti od výsledku tohto skriptu. Na rozdiel od tohto a predchádzajúcich, nasledujúce pravidlá už dokážu hľadať korelácie.
- **SingleWithSuppress** – Toto pravidlo sa chová podobne ako Single, avšak pri zhode tiež začne hľadanie korelácií počas T sekúnd, kde T je možné definovať v poli window. Koreláciou môže byť v tomto prípade iba rovnaká udalosť, ktorá príde neskôr. Všetky takéto udalosti budú ignorované po dobu T sekúnd. Až potom môže zhoda znovu nastať.
- **SingleWithThreshold** – Vykoná akciu, ak dôjde k N opakovaným udalostiam počas nejakej doby T. Hodnota N je špecifikovaná poľom thresh a hodnota T polom window.
- **SingleWith2Threshold** - spúšťa korelačné operácie udalostí, ktoré zareagujú, ak bolo v okne T1 sekúnd pozorovaných N1 udalostí, a potom bude v okne T2 sekúnd pozorovaných najviac N2 udalostí. Hodnoty T1, N1, T2 a N2 sú definované poľami window, thresh, window2 a thresh2.
- **EventGroup** – Ide o zovšeobecnenú verziu predchádzajúceho pravidla SingleWithThreshold. Umožňuje napočítavať ľubovoľný počet udalostí rôzneho typu v rámci spoločného intervalu (SEC používa termín okno – window).
- **Pair** – Párové pravidlo vykoná 1. akciu, pokiaľ je splnená 1. časť a 2. akcia sa vykoná, iba ak udalosť popísaná v 2. časti dorazí včas. Dobu hľadania tejto korelácie je samozrejme možné nastaviť na nekonečno. (napríklad možné využitie na odpovedanie servera, či stihol odpovedať do určitého času).
- **PairWithWindow** - spúšťa operácie korelácie udalostí na spracovanie párov udalostí počas T sekúnd. Hodnota T je definovaná poľom okna. (napríklad SSH prihlásenie užívateľa bolo neúspešné tak ak sa do určitého času prihlásenie nepodarí tak môže informovať správcu)
- **Jump** – Ak sa udalosť zhoduje s pravidlom tak v poli cfset sa nachádzajú súbory s pravidlami a aplikujú sa nad udalosťou v poradí zľava doprava.

1.3 Jednoduchý príklad konfiguračného súboru

Názov súboru je simple.conf a obsahuje nasledujúci text:

```
# Example simple.conf
# Recognize a pattern and log it.
#
type=Single
ptype=RegExp
pattern=man\s+(\S+)
desc=$0
action=logonly
```

Prvé 3 riadky sú komentáre.

type=Single - definuje typ pravidla.

ptype=RegExp - definuje typ vzoru.

pattern=man\s+(\S+) - je vzor, v tomto prípade vzor regulárneho výrazu perl a tento konkrétny vzor sa zhoduje so slovom man, za ktorým nasleduje jedna alebo viacero medzier, za ktorými nasleduje jeden alebo viacero znakov bez medzery, ako napríklad grep, install, alebo ?:SoMeThInG.

desc=$0 - desc je definícia premennej pre popis vzoru. V tomto prípade je premenná s číslom v perle $0 nastavená na celý zodpovedajúci vzor.

action=logonly - popisuje akciu vykonanú po rozpoznaní vzoru. V tomto prípade akcia logonly zapíše vzor do súboru na zaznamenávanie, ak je na príkazovom riadku uvedený, alebo na štandardný výstup, ak nie.

1.4 Spustenie názorného konfiguračného súboru

Na spustenie monitorovania vstupu pomocou tohto súboru použijete nasledujúci príkaz: **perl sec.pl -conf=simple.conf -input=-**

Ak chceme vidieť prácu SEC na súbore tak v príkaze zadefinujete **-input=suborNaMonitorovanie**

2 POŽIADAVKY NA INŠTALÁCIU A POSTUP PRI INŠTALÁCIÍ

2.1 Dostupnosť

Tento program je distribuovaný za podmienok GNU General Public License, a teda neposkytuje sa naň záruka. a možno si ho stiahnuť z https://simple-evcorr.github.io

2.1.1 GNU General Public License. Je populárna licencia pre slobodný softvér, ktorá zaručuje verejnosti slobodu:

- spúšťať program na akýkoľvek účel,
- študovať, ako program funguje a meniť ho (na to je potrebný prístup k zdrojovému kódu),
- ďalej šíriť kópie, (môžete si aj spoplatniť túto službu, ak si želáte)
- vylepšovať program a zverejňovať vylepšenia (na to je potrebný prístup k zdrojovému kódu).

Ak však distribuujete kópie takéhoto programu, či bezplatne alebo za poplatok, musíte koncovému užívateľovi poskytnúť všetky práva, ktoré vyplývajú z licencie. Teda kópia musí obsahovať aj túto licenciu a užívateľovi musia byť ukázané tieto podmienky. Aby vedel svoje práva a zmluvu podpísal. A môžete podľa vlastného uváženia ponúknuť záručnú ochranu výmenou za poplatok.

Oproti tomu iné druhy licencií – licencie pre koncových používateľov, ktoré zvyčajne používajú tvorcovia proprietárneho softvéru zriedkakedy zaručujú akékoľvek slobody koncovému užívateľovi, a dokonca obmedzujú aktivity zvyčajne neobmedzené zákonom, ako reverse engineering. Primárny rozdiel medzi GPL a „voľnejšími“ licenciami slobodného softvéru, ako licencia BSD je, že u GPL sa hore uvedené slobody zachovávajú aj pre tzv. odvodené práce. Toto sa deje pomocou právneho mechanizmu nazývaného copyleft vynájdeného Richardom Stallmanom, ktorý vyžaduje, aby odvodené práce boli taktiež zverejňované pod licenciou GPL. Kritici opisujú copyleft licencie ako virulentné (viral). Napríklad licencie typu BSD dovoľujú distribuovať odvodené práce aj ako proprietárny softvér.

2.2 Platformová závislosť

SEC bol primárne testovaný na Linuxe a Solarise, ale keďže je napísaný v Perle a nepoužíva kód závislý od platformy, mal by fungovať na akejkoľvek modernej platforme UNIX. Je známe, že SEC funguje aj v systéme Windows, hoci niektoré funkcie, ktoré sú natívne pre UNIX, budú vypnuté.

2.2.1 Perl. Perl (Practical Extraction and Report Language) je univerzálny, interpretovaný (t.j. netreba ho kompilovať) programovací jazyk, vyvinutý v roku 1987, Larrym Wallom, lingvistom, ktorý pracoval ako správca systémov v NASA. Zámerom bolo spraviť jazyk praktický (ľahko používateľný, výkonný, kompletný) a nie nevyhnutne pekný (elegantný, minimalistický).

Pôvodne bol Perl vyvinutý na manipuláciu textu, dnes sa používa v mnohých oblastiach, od správy systémov, programovanie webov, sieťové programovanie, vývoj GUI, programovanie hier (napr. Construder) a 3D grafiku pomocou OpenGL, až po webové aplikácie, akou je napríklad Wikipédia. Perl 5 beží na viac ako 100 platformách od prenosných zariadení až po mainframy.

Medzi hlavné črty Perl-u patrí:

- masívna knižnica použiteľného kódu
- kultúra najlepšej praxe a testovania
- vľúdna a otvorená komunita

Programovať v Perl-e sa dá rôznymi štýlmi v závislosti na projekte, dostupnom čase, očakávanej potreby údržby programu, osobnom štýle. Moto jazyka je TIMTOWTDI (There's more than one way to do it), čo umožňuje tvoriť pekný kód ale aj ťažko čitateľný neporiadok.

Keďže SEC nie je testovaný proti starým vydaniam Perlu, odporúča sa spustiť SEC aspoň s Perlom 5.8 (najnovšie stabilné vydanie Perl nájdete na https://www.perl.org). Okrem Perlu nie je SEC závislý od iného softvéru. Používa Perl Getopt, POSIX, Fcntl, Socket, IO::Handle, Sys::Syslog a moduly JSON::PP, ktoré sú súčasťou štandardnej inštalácie Perlu (prítomnosť Sys::Syslog a JSON::PP je voliteľné).

2.3 Postup inštalácie na Ubuntu

(1) **Aktualizácia systému** Ako prvé treba nainštalovať Perl ak ho ešte nemáte, ale ešte pred samotným príkazom na inštaláciu Perl sa odporúča aktualizovať váš systém zadaním nasledujúcich príkazov cez terminál.
sudo apt update - tento príkaz stiahne informácie o balíkoch zo všetkých nakonfigurovaných zdrojov (/etc/apt/sources.list). Takto potom váš systém vie, ktoré balíky sú dostupné na aktualizáciu a kde je možné tento softvér získať.

sudo apt upgrade - potom môže na základe týchto informácií konať a aktualizovať všetky nainštalované balíky na ich najnovšie verzie.

(2) **Inštalácia Perl** Po dokončení aktualizácie vášho systému nainštalujete Perl nasledujúcim príkazom.
sudo apt install perl
Po dokončení inštalácie Perl môžete skontrolovať nainštalovanú verziu Perl nasledujúcim príkazom.
perl -v
(prípadne aj príkazom na zobrazenie všetkých nainštalovaných balíkov Perl: **apt list –installed | grep -i perl**)
Ako môžete vidieť na nižšie uvedenej snímke obrazovky, verzia Perl „v5.30.0“ je nainštalovaná na mojom systéme.

(3) **Otestovanie** či Perl funguje spravíme nasledujúcim príkazom. **/usr/bin/perl -e 'print join "\n", @INC' -/usr/bin/perl** je cesta, kde je Perl bežne nainštalovaný.

Inštalácia nástroja Z nasledujúcej stránky https://simple-evcorr.github.io/ si stiahnete **sec-2.9.0.tar.gz** v sekcií Download. Prejdete do priečinku Downloads, kde sa vám uložil stiahnutý súbor, otvoríte v tomto priečinku terminál a nasledujúcim príkazom rozbalíte súbor.
tar -xvzf sec-2.9.0.tar.gz

Po zadaní príkazu **ls** môžete vidieť že sa súbor rozbalil.

Ak sa pozriete na obsah môžete vidieť:

- COPYING - kópia GNU General Public License
- ChangeLog - zmeny začínajúce od verzie 1.0
- README - tento súbor
- contrib - príspevky používateľov SEC
- sec - program SEC
- sec.man - manuálová stránka SEC

Ak váš nainštalovaný Perl sa nachádza inde ako v adresári /usr/bin/ treba zmeniť prvý riadok v súbore sec.

Teraz treba premiestniť program SEC a manuálovú stránku SEC do príslušných adresárov, ako je v README súbore napísané, môže to byť napríklad:

sudo cp sec /usr/local/bin - príkaz na premiestnenie programu SEC do adresára /usr/local/bin

sudo cp sec.man /usr/local/share/man/man1/sec.1 - príkaz na premiestnenie manuálovej stránky SEC do adresára /usr/local/share/man/man1/sec.1

Následne príkazom sudo mandb aktualizuje zoznam manuálov a na konci výpisu by ste mali vidieť pridanie manuálu pre SEC.

A ak zadáme príkaz man sec zobrazí sa nám manuálová stránka SEC

3 EXPERIMENTOVANIE A OVERENIE ZÁKLADNÝCH FUNKCIONALÍT BEZPEČNOSTNÉHO NÁSTROJA

TODO

4 DOKUMENTOVANIE EXPERIMENTOVANIA S NÁSTROJOM

5 HODNOTENIE BEZPEČNOSTNÉHO NÁSTROJA

SEC vyniká v monitorovaní záznamových súborov udalostí. Pomocou vhodného súboru pravidiel je možné nakonfigurovať SEC tak, aby monitoroval tieto súbory pre jedného hostiteľa, malú skupinu alebo celý podnik. A keďže pravidlá sú jednoducho textové súbory, kedykoľvek je potrebné nové pravidlo, môže byť rýchlo vytvorené a pridané do SEC za behu.

Výhody:

- Dokáže čítať dáta z mnohých zdrojov: zo súborov, zo štandardného vstupu až po pomenované rúry.
- Používa konfiguračný súbor (súbory) pre definíciu podozrivých aktivít. Tieto podozrivé aktivity dokáže popísať pomocou mnohých predpripravených typov pravidiel.
- Pre administráciu konfiguračného súboru nie je potrebná znalosť programovacieho jazyka.
- Veľmi mocná je možnosť špecifikácie ako podozrivých aktivít, tak reakcie na ne pomocou Perl.
- Podporuje regulárne výrazy, ktorými je možné popísať mnoho hľadaných vzorov.
- Umožňuje definovať kontexty, ktoré dokážu spojiť jednoduché regulárne výrazy alebo definovať ďalšie udalosti, ktoré musia nastať, aby sa jednalo o podozrivú aktivitu. Umožňujú napríklad pridať podmienky, z ktorého záznamu musí udalosť prísť, v akom časovom intervale a pod.
- Dokáže definovať, aká reakcia na podozrivú aktivitu sa má vykonať.
- Obsahuje napríklad zabudovanú možnosť spúšťať externé programy, napr. mail – na odoslanie upozorňovacieho e-mailu správcovi servera.
- Dobrá dokumentácia.
- Jednoduchá inštalácia.
- Napísaný v Perl, teda platformovo nezávislý.

Nevýhody:

- Absencia GUI.
- SEC nie je testovaný proti starým vydaniam Perlu

6 ZOZNAM ZÁKLADNÝCH POUŽITÝCH PRAMEŇOV

TODO