České vysoké učení technické

Fakulta informačních technologií

Forensic Analyzer

Instalační a uživatelská příručka

Jan Lejnar

12. května 2017

Obsah

1 Instalační příručka

1.1 Požadavky

Aplikace *Forensic Analyzer* je určená pro operační systém Linux. Pro úspěšnou instalaci je potřeba mít nainstalované tyto balíčky:

- make
- g++
- qt-sdk
- doxygen
- graphviz

Balíček instalujte příkazem: `sudo apt-get install <název balíčku>`

1.2 Instalace

Pro instalaci otevřete příkazový řádek v adresáři se souborem `Makefile` a zadejte příkaz `make`. Součástí instalace je také snaha přiřadit práva na spouštění přidružené aplikace SEC+ s relativní adresou `./res/sec+`. Tento soubor, prosím, nemažte ani jej nepřesouvejte na jiné umístění.

1.3 Možnosti Makefilu

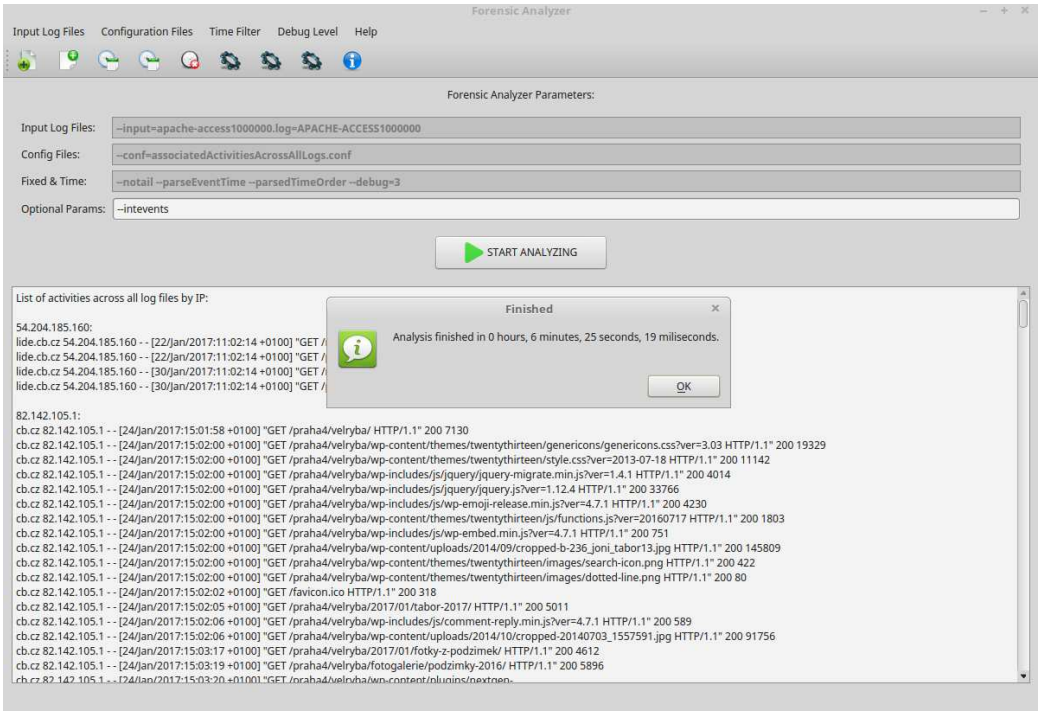
`Makefile` má definováno více zajímavých návěští, které můžete připsat za `make`:

- all – Výchozí návěští, pokud není explitně specifikováno jinak. Nainstaluje aplikaci a vygeneruje programátorskou příručku.
- run – Spustí aplikaci. Při spuštění již nejsou potřeba administrátorská práva.
- doc – Vygeneruje programátorskou příručku do složky `doc`. Pro spuštění HTML verze příručky otevřete soubor `doc/index.html`.
- count – Počítá počet řádků kódu všech souborů s příponami `.h` a `.cpp`
- clean – Odinstaluje aplikaci a odstraní programátorskou příručku.

Př.: Pouze pro vygenerování programátorské příručky zadejte: `make doc`

2 Uživatelská příručka

2.1 Hlavní obrazovka



Obrázek 1: Hlavní okno aplikace

Po spuštění *Forensic Analyzeru* se dostanete na hlavní obrazovku, viz 1. Tato hlavní obrazovka je rozdělena na dvě části:

1. Část s parametry, které definují, jak bude forenzní analýza probíhat.
2. Okno pro zobrazení výsledků, ať už čistě pro zobrazení nalezených korelací nebo detailnější záznam průběhu analýzy.

Až budete mít všechny parametry specifikované, stiskněte tlačítko `START ANALYZING`, popřípadě klávesovou zkratku `Ctrl + R`. Následně proběhne forenzní analýza zadaných logů dle definovaných konfiguračních souborů. Po dokončení analýzy se objeví výsledky a informace o době běhu.

2.1.1 Parametry Forensic Analyzeru

Parametry jsou logicky rozdělené do 4 kategorií:

1. Parametry popisující jaké jsou vstupní logovací soubory, ve kterých se budou podezřelé aktivity hledat.

2. Parametry popisující z jakých konfiguračních souborů se bude vytvářet sada pravidel, která definuje podezřelé aktivity.

3. Fixní parametry, což jsou přednastavené parametry, které zaručují správnou funkcionalitu pro offline analýzu logů.

4. Volitelné parametry, které slouží pro pokročilé uživatele se znalostmi další parametrizace aplikace SEC, které zde lze uplatnit.

Můžete si všimnout, že parametry z kategorie 1–3 jsou šedé. To značí, že je nelze ručně editovat. Generují se automaticky dle aktuálního stavu aplikace.

Parametry z kategorie 4 je možné editovat. Lze použít veškeré parametry příkazové řádky, které podporuje nástroj SEC – viz [**?**, **?**]. Ve výchozím nastavení je nastaven parametr `--intvents`, který vynutí generování interních událostí SEC, kterých lze také využívat při psaní pravidel v konfiguračních souborech.

2.1.2 Menu lišta a panel nástrojů

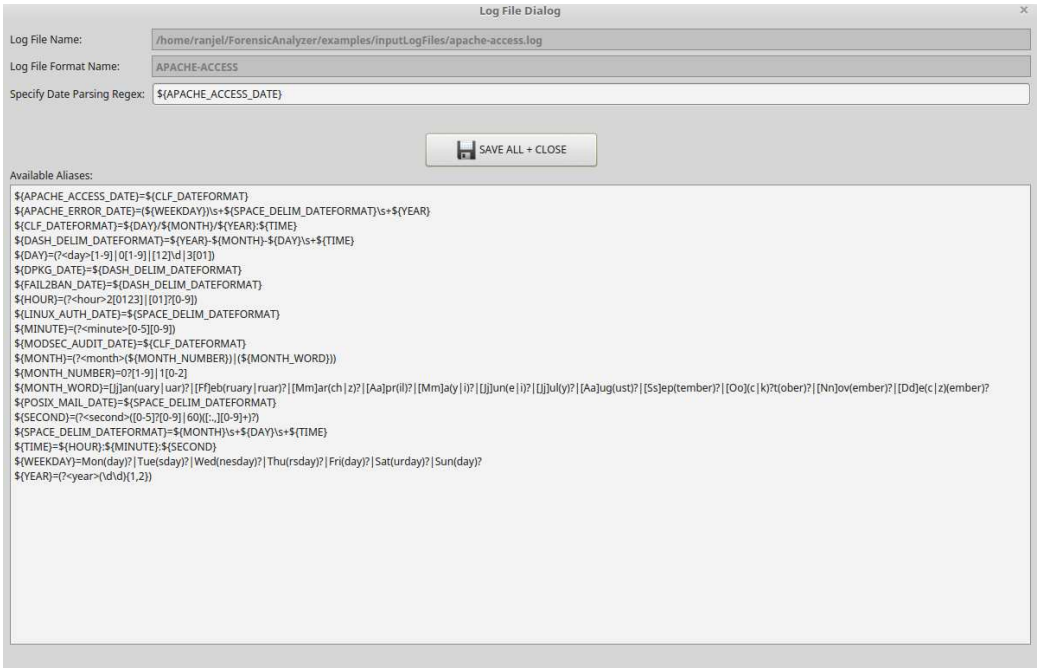
Panel nástrojů poskytuje rychlejší přístup k některým prvkům menu lišty. Tento panel nástrojů není fixní a lze jej přemístit na jiný okraj aplikace. Většina operací, které zde nebo v menu najdete, má přiřazené alternativní klávesové zkratky, které mohou zrychlit používání aplikace.

V menu se nachází možnost specifikovat časové filtry, které umožní definovat interval, ve kterém chcete hledat podezřelé aktivity a jejich korelace. Události mimo tento interval budou ignorovány. Pomocí kalendáře lze specifikovat horní nebo dolní mez, popřípadě obě současně.

Další položkou je volba podrobnosti výpisu. Čím vyšší úroveň, tím více informací o průběhu analýzy bude zobrazeno. Výchozím nastavením je úroveň 3. Úroveň 1 zobrazuje pouze nalezené podezřelé aktivity a druhým extrémem je úroveň 6, která detailně popisuje všechny důležité momenty analýzy.

Jak podrobnost výpisu, tak časové filtry se připisují do parametrů kategorie 3. Pokud budete chtít přidávat parametry kategorie 4 může být praktické si zobrazit veškerou dostupnou parametrizaci SEC+ (například pomocí klávesové zkratky `Ctrl + U`).

Zbývají 2 nejdůležitější položky menu, které si rozebereme podrobněji.



Obrázek 2: Dialog se vstupním logovacím souborem

2.2 Správa vstupních logovacích souborů

V první záložce na hlavním okně naleznete přehled aktivních a neaktivních vstupních logů. Aktivní logy jsou zaškrtnuté a tedy se také nachází v parametrech kategorie 1. První tři akce tohoto menu jsou vyhrazené pro možnost přidat, editovat nebo smazat vstupní log. Akce smazat log (popřípadě konfigurační soubor) pouze odstraní evidenci tohoto souboru z aplikace, neprovádí fyzické smazání z disku.

Pokud zvolíte akci přidat log, zobrazí se vám dialog, ve kterém vyberte logovací soubor, který budete chtít zkoumat. Následovat bude dialog z obrázku 2, ve kterém je potřeba doplnit potřebné informace o logovacím souboru.

2.2.1 Aliasy

Největší část je věnována pro uživatelem definované aliasy, které slouží k zjednodušení a zvýšení přehlednosti zápisu regulárních výrazů.

Alias se definuje zápisem `${<jmémo proměnné>}=<hodnota>`. Vyhodnocování probíhá rekurzivně, dokud `<hodnota>` není obyčejný řetězec.

Listing 1: Příklad definice tří aliasů

```
${SECOND}=(?<second>([0-5]?[0-9]|60)([:.,][0-9]+)?)
${MINUTE}=(?<minute>[0-5][0-9])
${TIME}=(?<hour>2[0123]|[01]?[0-9]):${MINUTE}:${SECOND}
```

2.2.2 Popis data a času

Je nutné specifikovat regulární výraz, podle kterého bude možné z každé události získat datum a čas. Tento regulární výraz navíc musí obsahovat tzv. *named capture groups*. [**?**]

Vyžaduji specifikovat přesně tyto skupiny:

- year[1]
- month
- day
- hour
- minute
- second

Každá skupina musí být obalena zleva `?<` a zprava `>`.

Listing 2: Příklad regulárního výrazu získávající datum a čas z události

```
(?<month>(0?[1-9]|1[0-2]))\s+(?<day>[1-9]|0[1-9]|
[12]\d|3[01])\s+(?<hour>2[0123]|[01]?[0-9]):(?<minute>
[0-5][0-9]):(?<second>([0-5]?[0-9]|60)([:.,][0-9]+)?)
```

Pokud bude skupina pojmenovaná například `month`, aplikace očekává, že v této skupině nalezne údaj o tom, jaký je právě měsíc. Nemusí to být ovšem jen číselná informace. Validní je také například „Jan“ nebo „January“.

Pojmenovaná skupina `year` je jediná nepovinná, protože některé logy zkrátka rok neevidují. Pokud tato informace není dostupná, aplikace vezme nejpravděpodobnější rok dle dnešního data. Pokud je například 16. dubna 2017 a bude analyzován log, ve kterém je měsíc specifikován jako „Nov“, pak aplikace vyhodnotí, že se jedná o listopad roku 2016, ne roku 2017.

Lze zde využít výše zmíněné aliasy.

[1] Tato skupina je nepovinná.

2.2.3 Formát logu

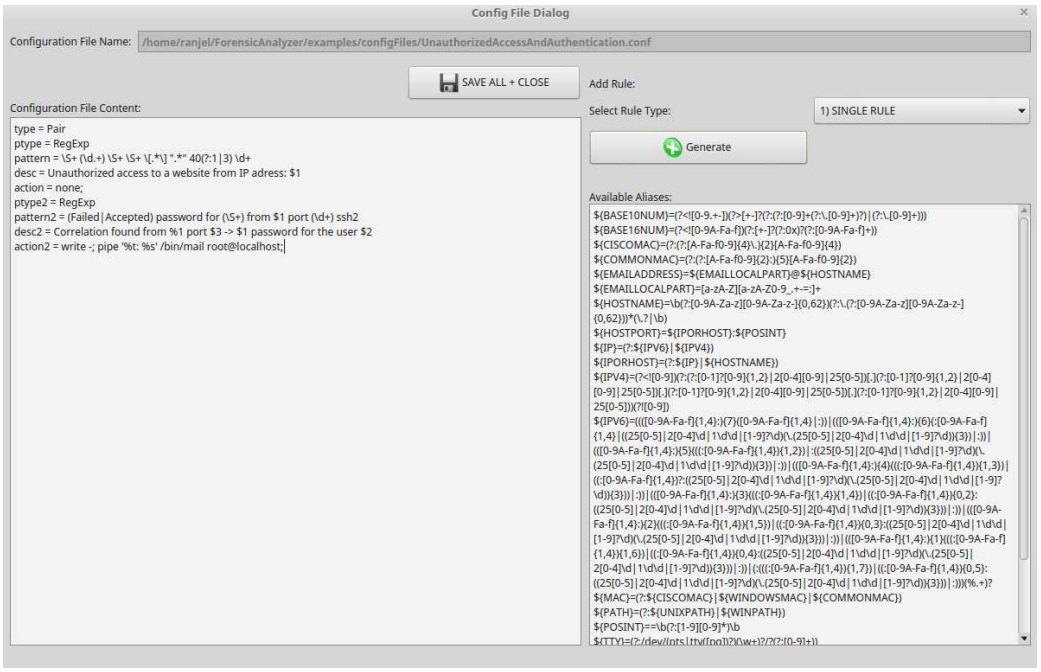
V horní části okna se nachází další dvě pole. V prvním je absolutní cesta k právě spravovanému souboru. V druhém poli je generovaný název formátu logu, pro který se automaticky vytváří alias `${<název formátu>}=<zadaný vstup od uživatele>`, který bude možné použít později pro jiný logovací soubor stejného formátu.

2.2.4 Uložení změn a ukončení

Uložení změn v tomto okně se provede příslušným tlačítkem `SAVE ALL + CLOSE`, případně klávesovou zkratkou `Ctrl + S`. Pokud okno zavřete křížkem v pravém horním rohu, změny nebudou uloženy.

Nově přidaný log je automaticky považován za aktivní.

2.3 Správa konfiguračních souborů



Obrázek 3: Dialog s konfiguračním souborem

Logika správy konfiguračních souborů je velice podobná správě vstupních logovacích souborů. Zmíním tedy jen odlišnosti.

Na obrázku 3 je zachycen dialog po výběru konfiguračního souboru. Vpravo naleznete opět seznam aliasů. Tyto aliasy jsou oddělené od předchozích a lze je uplatnit v levé části, která zobrazuje obsah daného konfiguračního souboru.

2.3.1 Pravidla z konfiguračního souboru

Jednotlivá pravidla musí být oddělena minimálně jedním prázdným řádkem. Pravidla mohou být různých typů, viz [**?**]. Lze si zvolit typ pravidla, které chcete přidat, a kliknout na tlačítko `Generate`, popřípadě stisknout klávesovou zkratku `Ctrl + G`. Takto je možné vygenerovat všechny povinné položky, které dané pravidlo vyžaduje specifikovat.

Můžete si všimnout, že je automaticky generována akce „`write -`“[2]. Tuto akci nemažte, jinak hledanou podezřelou aktivitu program sice nalezne, ale v přehledu ji nezobrazí. Je možné přidávat více akcí, stačí je oddělovat středníkem.

2.4 Zálohovací soubory

Aplikace si i po vypnutí pamatuje mnoho informací z předchozího běhu a automaticky je načítá při spuštění. Jedná se například o seznam definovaných logovacích a konfiguračních souborů nebo seznam definovaných aliasů. Tato evidence je uložena v zálohovacích souborech ve složce `backup`.
Pokud chcete rychle získat čistou verzi *Forensic Analyzeru*, můžete celou tuto složku smazat. Aplikace je ovšem dodána s přednastavenými aliasy, které by byla škoda nevyužít.

[2]Spojovník (`-`) je zkratka pro standardní výstup.
Akce `write` má signaturu: `write <soubor> [<obsah>]`. Podrobněji zde [**?**].