HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza FTimes forenzičkog alata

CCERT-PUBDOC-2003-03-08

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Prilikom analize kompromitiranog sustava, najvažnije je utvrditi što se na sustavu promijenilo, kako bi se što lakše povratilo prvobitno stanje i sustav učinio manje ranjivim. Jedna od tehnika forenzičke analize kojom je ovo moguće postići je *Baselining*. *Baselining* obuhvaća sustavno snimanje stanja sustava, kako bi se u slučaju kompromitiranja usporedbom snimki lagano analizirale promjene.

`FTimes` (engl. *File Topography and Integrity Monitoring on an Enterprise Scale*) je alat razvijen sa ciljem lakšeg provođenja *Baselining* tehnike i u svrhu lakšeg prikupljanja dokaza o kompromitiranju sustava. Prilikom pisanja programa imala se u vidu jednostavnost upotrebe, tako da program nije potrebno instalirati na računalo koje će se analizirati, već ga je dovoljno pokrenuti s diskete.

Ovaj paket općenito se koristi na dva načina, za snimku topografije datotečnog sustava i pretraživanje datoteka u potrazi za specifičnim znakovnim nizovima. Snimka topografije datotečnog sustava obuhvaća mapiranje ključnih atributa koje posjeduju odabrane datoteke i direktoriji, dok način za pretraživanje nudi mogućnost pronalaženja zadanih znakovnih nizova u određenoj strukturi direktorija i datoteka.

Izlazni rezultat opisanih radnji je u čistom tekstualnom obliku, što omogućuje lakšu i automatiziraniju interpretaciju rezultata.

`Ftimes` nudi podršku za dva radna okruženja, lokalno i klijent-poslužitelj okruženje. Lokalni način rada koristi se za pregledavanje kompromitiranog sustava i prikupljanje dokaza, dok se klijent-server način rada koristi za automatizirano provođenje analize na većem broju računala i za prikupljanje rezultata analize na centralnom poslužitelju.

Kompletnu dokumentaciju, kao i izvorni kod programa moguće je pronaći na adresi http://ftimes.sourceforge.net.

2. Karakteristike paketa

Program je pisan u C programskom jeziku i prilagođen je radu na velikom broju popularnih operacijskih sustava ako što su AIX, BSDi, FreeBSD, Linux, Solaris i Windows 98/ME/NT/2K/XP. Osim velikog broja operacijskih sustava kojima je prilagođen, jedna od prednosti klijentskog dijela `Ftimes`-a je i ta što ne zahtijeva dodatnu podršku u obliku interpretera (`Perl`,...) ili radnog okruženja (`JVM`...) za ispravan rad, što čini `Ftimes` neovisnim o konfiguraciji sustava na kojemu se pokreće.

Vrlo temeljito i precizno kreiranje log poruka olakšava analizu rada programa i otklanjanje mogućih pogrešaka u forenzičkoj analizi uzrokovanih neispravnim radom forenzičkog alata.

Ključne karakteristike ovog paketa su mogućnost pretraživanja datotečnog sustava u potrazi za specifičnim znakovnim nizovima, mogućnost kreiranja *hasheva* iz zadanog direktorija i sposobnost vrlo brze usporedbe različitih snimaka stanja sustava.

Mogućnost kreiranja *hasheva* vrlo se korisno može primijeniti na direktorijima čiji se sadržaj vrlo rijetko mijenja. Budući da *hashevi* sadrže informaciju o svim datotekama u direktoriju, njihovom letimičnom usporedbom vrlo je lako utvrditi gdje su se zbile promjene na sustavu.

3. Instalacija

`Ftimes` se sastoji od dva dijela, izvršnog programa i poslužitelja. Izvršni program služi za provođenje analize i može se primjenjivati kao samostalan alat, neovisno o poslužitelju, dok se poslužitelj koristi u slučajevima, u kojima je pogodno izlazne podatke dobivene analizom na većem broju računala prikupiti na jedno centralno mjesto.

3.1. Instalacija programa

Instalacija `Ftimes` paketa na `Unix/Linux` platformi zahtijeva `make`, `gcc` i `autoconf` programe. Budući da je u program inicijalno uključena i podrška za `SSL` protokol, na sustavu je potrebno imati instaliran i `OpenSSL` paket (http://www.openssl.org).

Na Windows operacijskim sustavima za prevođenje je programa potrebno imati Microsoft `Visual Studio`.

Tar.gz arhivu je potrebno smjestiti u odabrani direktorij i otpakirati ju naredbom

```
#tar -xzvf Ftimes-3.2.1.tgz
```

Prevođenje programa tipično je za Linux/Unix platforme i obavlja se naredbama:

```
#./configure
#make
```

Budući da je podrška za SSL protokol inicijalno uključena u konfiguraciju programa, configure skripta će pokušati pronaći OpenSSL paket na sustavu. Ukoliko instalacijska skripta nije u mogućnosti pronaći OpenSSL paket, prekinuti će instalacijski postupak. U tom slučaju opcijom --with-ssl=<ime_direktorija> potrebno je specificirati lokaciju OpenSSL paketa na sustavu. Podršku za SSL moguće je i isključiti opcijom --without-ssl:

```
#./configure -without-ssl
```

Nakon prevođenja softver se instalira naredbom make install. Uobičajeni direktorij za instalaciju je /usr/local/integrity ali moguće ga je promijeniti u proizvoljni direktorij opcijom --prefix=<ime_direktorija>:

```
#./configure --prefix=<ime_direktorija>
```

Na Microsoft Windows platformi, Ftimes se instalira koristeći Microsoft Visual Studio paket. Prevođenje se svodi na podešavanje ispravne radne okoline (engl. *Environment*) i pokretanje nmake naredbe. Za Windows operacijske sustave ne postoji configure skripta koja bi ispitala konfiguraciju sustava, već se za prevođenje koristi unaprijed definirana datoteka Makefile.vs. Varijable okoline podešavaju se pokretanjem datoteke VCVARS32.BAT.

4. Konfiguracija poslužitelja

Kako bi klijent-poslužitelj komunikacija ispravno radila, na poslužiteljskom računalu potrebno je podesiti Apache Web poslužitelj tako da prihvaća zahtjeve sa klijenata na kojima se pokreće program.
Podešavanje se zapravo svodi na instalaciju skripte nph-ftimes.cgi i izmjenu konfiguracije Apache poslužitelja. Za normalan rad skripte nph-ftimes.cgi na poslužiteljskom računalu potrebno je imati instaliran Perl interpreter, što kod klijentskog dijela aplikacije nije slučaj.
Skriptu je potrebno smjestiti u proizvoljan direktorij i u konfiguracijsku datoteku Web poslužitelja dodati sljedeće linije:

```
ScriptAlias /cgi-client/ "ime_direktorija/"

<Directory "$CGI_DIR">
    AllowOverride AuthConfig
    Options None
    Order allow,deny
    Allow from all
</Directory>
```

Unutar proizvoljnog direktorija u koji će se smještati rezultati analize, potrebno je generirati sljedeću strukturu poddirektorija:

```
integrity
    |
    - incoming
    |
    - logfiles
    |
```

```
- profiles
```

Skripta `nph-ftimes.cgi` inicijalno očekuje postojanje ove strukture u korijenskom (*root*) direktoriju, ali izmjenom varijable `$baseDirectory` unutar skripte, moguće je postaviti proizvoljan put do strukture.
U kreiranoj strukturi potrebno je još napraviti i log datoteku u koju će se upisivati tijek rada programa i moguće poruke o greškama u radu. Pod pretpostavkom da je `Apache` poslužitelj na sustavu pokrenut pod korisnikom `nobody`, datoteka se kreira sljedećim naredbama:

```
#touch /integrity/logfiles/nph-ftimes.log
#chown nobody:0 /integrity/logfiles/nph-ftimes.log
#chmod 644 /integrity/logfiles/nph-ftimes.log
```

Nakon uspješnog kreiranja svih potrebnih direktorija, konačni korak instalacije poslužiteljskog dijela `Ftimes`-a je podešavanje ovlasti pristupa na razini `Apache` poslužitelja. Najlakši način za to je kreiranje jednostavne `.htaccess` datoteke u direktoriju u kojem se nalazi skripta `nph-ftimes.cgi`. Sadržaj ovakve datoteke izgledao bi otprilike ovako:

```
AuthType Basic
AuthName "Ftimes Realm"
AuthUserFile $APACHE_DIR/htusers
require valid-user
```

Naravno pomoću `htpasswd` naredbe potrebno je kreirati i valjanu lozinku za računala koja će pristupati poslužitelju.

5. Načini rada i mogućnosti Ftimes-a

Kao što je već ranije spomenuto, `Ftimes` sadrži više korisnih opcija koje se koriste prilikom provođenje forenzičke analize. U tekstu koji slijedi, ukratko će se opisati mogućnosti koje nude pojedine opcije.

5.1. Compare

U `compare` načinu rada, program uspoređuje dvije snimke stanja sustava prema zadanim atributima. Rezultat usporedbe ispisuje se na standardni izlaz u sljedećem formatu:

```
kategorija|ime_datoteke|promjena|ostalo
```

Polje kategorija može poprimiti sljedeće vrijednosti, C (promijenjen), M (nedostaje), N (nov), U (nepoznat), X (promijenjen i nepoznat). U polju promjena, upisani su atributi koji su se promijenili, dok polje ostalo sadrži listu atributa koji zbog nedostatka informacija nisu mogli biti uspoređeni.
Sintaksa za pokretanje programa u `compare` načinu rada je:

```
#ftimes --compare maska baseline snapshot
```

Pod maskom se podrazumijeva popis atributa datoteke koji će se uspoređivati. Moguće vrijednosti su `ALL` i `NONE` koje obuhvaćaju sve atribute ili niti jedan. Na vrijednosti `ALL` i `NONE`, atributi se dodaju ili oduzimaju znakom + ili −. Tako će npr. `ALL-mtime`, značiti usporedbu svih atributa osim `mtime`.
Tablica 1: prikazuje moguće vrijednosti atributa.

Atribut	Operacijski sustav	Značenje
`volume`	Windows	Serijski broj diska
`findex`	Windows	Serijski broj datoteke
`attributes`	Windows	Datotečni atributi

Atribut	Operacijski sustav	Značenje
atime	Windows	Vrijeme posljednjeg pristupa
mtime	Windows	Vrijeme posljednje izmjene
ctime	Windows	Vrijeme kreiranja datoteke
size	Windows	Veličina datoteke
magic	Windows	Vrsta datoteke
md5	Windows	MD5 hash datoteke
dev	Unix	Identifikacijski broj diska
inode	Unix	Identifikacijski broj datoteke
mode	Unix	Datotečni atributi i dozvole
nlink	Unix	Broj linkova na datoteku
uid	Unix	Korisnička oznaka
gid	Unix	Oznaka grupe
rdev	Unix	Tip uređaja
atime	Unix	Vrijeme posljednjeg pristupa
mtime	Unix	Vrijeme posljednje izmjene
ctime	Unix	Vrijeme posljednje promjene statusa
size	Unix	Veličina datoteke
magic	Unix	Vrsta datoteke
md5	Unix	MD5 hash datoteke

Tablica 1: Popis atributa koji se koriste uz compare naredbu

Rezultate usporedbe program ispisuje na standardni izlaz, pa ih je poželjno preusmjeriti u datoteku:

```
#[root@cecilija bin]# ./ftimes --compare NONE+mtime+uid+size+ctime
baseline sminka > usporedba
```

U našem slučaju, datoteka se zove `snimka`, i njen sadržaj je sljedeći:

```
category|name|changed|unknown
N|"/home/spajic/jolt2.c~"||
N|"/home/spajic/SYSADMIN/133-002.htm"||
C|"/home/spajic/jolt2.c"|mtime,ctime,size|
C|"/home/spajic/shell_skripte.doc"|uid,ctime|
N|"/home/spajic/wget_upute.html"||
C|"/home/spajic/samba_exploit"|uid,ctime|
C|"/home/spajic"|mtime,ctime|
M|"/home/spajic/wget.html"||
M|"/home/spajic/sysadmin/133-002.htm"||
M|"/home/spajic/radius.ps"||
M|"/home/spajic/template.zip"||
```

Pažljivim odabirom parametara moguće je izvršiti vrlo selektivne usporedbe nad velikim brojem datoteka, što olakšava uočavanje neovlaštenih radnji na sustavu.

5.2. Digauto

`Digauto` koristi uobičajenu konfiguraciju za pretraživanje datotečnog sustava i pronalaženje datoteka koje sadrže određene znakovne nizove. Primjer pokretanja programa u `digauto` načinu rada je :

```
#ftimes --digauto datoteka [lista_datoteka]
```

"`Datoteka`" u ovom slučaju sadrži listu znakovnih nizova koji će se tražiti u datotekama navedenima listom. Ukoliko lista datoteka nije specificirana, `Ftimes` će pretražiti kompletan

datotečni sustav, uključujući i udaljene dijeljene direktorije. U nastavku je dan tipičan rezultat pretraživanja datotečnog sustava (tražila se riječ `address`):

```
name|offset|string
"/share/exploit/crash/synflood.c"|93|address
"/share/exploit/crash/dos_new_code.tgz"|22109|address
"/share/exploit/dos.htm"|7829|address
"/share/exploit/dos.htm"|8337|address
```

5.3. Digfull

Za razliku od `digauto` načina rada, u `digfull` načinu rada `Ftimes` koristi konfiguracijsku datoteku koja je specificirana prilikom pokretanja naredbe. Na taj način moguće je mnogo preciznije prilagoditi pretraživanje datotečnog sustava.
Opis mogućih parametara u konfiguracijskoj datoteci opisan je u dokumentaciji programa.

5.4. Getmode

`Getmode` način rada može se koristiti u slučaju klijent-poslužitelj komunikacije. Pomoću njega je moguće sa poslužitelja dohvatiti konfiguracijsku datoteku prema kojoj će se vršiti snimka analize sustava. Prilikom korištenja `getmode` opcije programu je potrebno pomoću posebne datoteke prenijeti ključne podatke za uspješno spajanje na poslužitelj (adresa, lozinka,...).
U ovisnosti o konfiguraciji, nakon dohvata datoteke moguće su tri akcije. `Ftimes` može dohvaćenu datoteku ispisati na standardni izlaz, zapisati je na disk ili se pokrenuti u `digfull` ili `mapfull` načinu rada koristeći dohvaćenu konfiguraciju.

5.5. Mapauto

Kao što je u uvodu spomenuto, dva glavna načina rada `Ftimes` paketa su pretraživanje datotečnog sustava i izrada topografije datoteka i direktorija. Sintaksa za pokretanje programa u mapauto načinu rada je:

```
#ftimes --mapauto maska [lista_direktorija]
```

Nakon pokretanja program će izraditi mapu datotečnog sustava, prikupljajući informacije o atributima definiranim zadanom maskom. Način korištenja maske identičan je onome opisanom kod opcije `compare`. Ukoliko lista datoteka i direktorija nije specificirana, `Ftimes` će pretražiti kompletan datotečni sustav, uključujući i udaljene dijeljene direktorije.
Budući da se rezultat inicijalno ispisuje na standardni izlaz, potrebno ga je preusmjeriti u datoteku. Pokretanjem `Ftimes`-a sa `mapauto` opcijom i preusmjeravanjem njegovog izlaza u datoteku, dobije se sljedeći sadržaj datoteke:

```
name|dev|inode|mode|nlink|uid|gid|rdev
"/home/spajic/tmp"|775|64769|40700|2|501|501|0
"/home/spajic/.screenrc"|775|32386|100644|1|501|501|0
"/home/spajic/.bash_logout"|775|32387|100644|1|501|501|0
"/home/spajic/.bash_profile"|775|32388|100644|1|501|501|0
"/home/spajic/.bashrc"|775|32389|100644|1|501|501|0
"/home/spajic/.mailcap"|775|32390|100644|1|501|501|0
"/home/spajic/.wmrc"|775|32391|100644|1|501|501|0
```

Zbog preglednosti, iz ispisa su izbačeni neki atributi.

5.6. Mapfull

Ovaj način rada, za razliku od `mapauto` moda, koristi korisnički definiranu konfiguracijsku datoteku umjesto uobičajene konfiguracije.

5.7. Putmode

`Putmode` opcija koristi se za spremanje rezultata analize na centralni poslužitelj. Budući da se sva komunikacija između poslužitelja i klijenta obavlja preko sigurnog (kriptiranog) kanala, centralni poslužitelj se može nalaziti i izvan lokalne računalne mreže.

5.8. Korištenje gotovih konfiguracijskih skripti

Na Web stranici `Ftimes` projekta (http://ftimes.sourceforge.net/FTimes/Cookbook.shtml) mogu se pronaći gotove konfiguracijske skripte za izvođenje većine uobičajenih analiza.
Osim jednostavnijih primjera, na istoj adresi mogu se pronaći i skripte koje su npr. sposobne preprocesirati dobivene podatke i spremiti ih u `MySQL` bazu podataka, olakšavajući time daljnju analizu.

6. Zaključak

Zbog mnoštva opcija koje nudi, kao i zbog visokog stupnja neovisnosti o sustavu na kojemu se pokreće, `Ftimes` se pokazao kao vrlo koristan forenzički alat. Rezultati njegove analize uvelike ubrzavaju otkrivanje izvora problema na kompromitiranom računalu i prikupljanje potrebnih dokaza. Faktor brzine koji `Ftimes` donosi vrlo je značajan u slučajevima analize poslužitelja koji se iz određenih razloga ne smiju ugasiti i detaljno ispitivati.
Mogućnost spremanja rezultata analize na centralni poslužitelj čini ovaj program vrlo poželjnim pri provođenju forenzičkih analiza većeg razmjera.