HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Fcheck IDS alat

CCERT-PUBDOC-2000-11-06

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

Računalno bazirani sustavi za detekciju neovlaštenih aktivnosti odgovorni su za obavještavanje administratora sustava o promjenama ključnih datoteka sustava na pojedinim računalnim sustavima. Otkrivanje neovlaštenih aktivnosti korisnika predstavlja vrlo važnu komponentu sigurnosni sustava, no danas administratori računalno bazirane sustave za otkrivanje neovlaštenih aktivnosti korisnika uglavnom koriste za zapisivanje logova o promjenama koje su napravljene na sustavu da bi se kasnije mogle pregledavati aktivnosti korisnika.
Upravo zbog ovog razloga naročito je popularan bio besplatan paket za provjeru izmijenjenih datoteka na sustavu, Tripwire (http://www.tripwire.com), koji je do nedavno bio besplatan. Kako ovakav tip paketa nije ovisan o pojedinom operacijskom sustavu, moguće ga je iskoristiti na svim vitalnim dijelovima operacijskih sustava, da bi se ustanovile eventualne promjene datoteka. Fcheck, http://sites.netscape.net/fcheck/download.html, je besplatan računalno baziran sustav za otkrivanje neovlaštenih aktivnosti korisnika koji radi i pod Unix i pod Windows operacijskim sustavima. Fcheck je napisan u Perlu i zahtijeva inačicu 5 ili noviju tog interpretera.

2. Arhitektura Fcheck-a

Fcheck u potpunosti podržava filozofiju Unix programa budući da je napisan kao mali alat, koji je orijentiran ispunjavanju specificiranog zadatka i kojeg se može uključiti u veći paket sa općenitijim alatima. Fcheck može koristiti bilo koju izvršnu datoteku na sustavu ili skriptu za ispisivanje izvještaja, što mu daje veliku fleksibilnost. `Syslog` (koristeći logger komandu) ili `lpr` predstavljaju najčešće korištene metode za ispisivanje izvještaja koje koriste sustavi za otkrivanje neovlaštenih aktivnosti. Korištenje `lpr` komande i pisača daje čitavoj sigurnosti sustava novu dimenziju budući da su sigurnosni logovi zapisani na medij koji se nemože brisati, što neovlašteni korisnici obično pokušavaju napraviti nakon kompromitiranja sustava. Fcheck također koristi i vanjske programe da bi ustanovio nizove potpisa datoteka korisetći MD5 (RFC 1321) kao izbor algoritma za provjeru. Ovdje je potrebno napomenuti da ova osobina Fchecka ima i sigurnosnu rupu – izvršna datoteka od MD5 programa može biti također promijenjena tijekom kompromitacije sustava tako da zamijenjeni program daje ispravan izlaz (onaj koji Fcheck očekuje) na lažne datoteke tijekom pokretanja.
Fcheck se sastoji od `fcheck` Perl skripte, `fcheck.cfg` konfiguracijske datoteke (koja se obično nalazi u `/usr/local/etc` direktoriju), direktorija sa bazom podataka i datoteka koje se koriste da bi se ustanovilo da li su nastale kakve promjene na datotekama sustava. Fcheck nije potrebno pokretati pod administratorskim korisničkim računom budući da mu za normalan rad nisu potrebne administratorske privilegije, međutim, potrebno mu je omogućiti dozvolu čitanja datoteka nad kojima se prate promjene. No, postavljanje dozvola za čitanje na datotekama koje ih inače nemaju može biti vrlo komplicirano (u slučaju velikog broja datoteka) i u krajnjem slučaju može otvoriti nove potencijalne sigurnosne rupe tako da se ne preporučuje.
Fcheck u trenutnoj inačici koja je testirana ne omogućava praćenje promjena na pojedinačnim datotekama sa samo jednim zapisom kao što je npr. `/etc/passwd`, što može izgledati kao veliki nedostatak programa. Međutim, jednostavnost upotrebe programa i njegova brzina predstavljaju veliku prednost u odnostu na ovaj nedostatak. Da bi uklonili ovaj nedostatak, tijekom ispitivanja programa napisana je `fcheck_file_support` skripta koja stvara neophodan izlaz koji je potrebno upisati u konfiguracijsku datoteku da bi se simulirala podrška praćenja promjena na pojedinačnim datotekama. `fcheck_file_support` skripta priložena je na kraju ovog dokumenta, u točki 8.

3. Instalacija

Instalacija Fcheck programa vrlo je jednostavna. Testirana instalacija pokrenuta je na računalu sa RedHat 6.2 operacijskim sustavom i Perl 5.005.03 inačicom interpretera, no instalacija i na ostalim inačicama Unix operacijskih sustava jednaka je opisanoj. U idealnom slučaju, svaki sustav za detektiranje neovlaštenih aktivnosti korisnika treba biti instaliran odmah nakon završene instalacije

operacijskog sustava na tom računalnom sustavu, što, na žalost, obično nije slučaj. Za vrijeme provođenog testiranja aktualna inačica Fcheck programa bila je 2.7.51, za koju vrijedi sve napisano u ovom dokumentu.
Na početku je potreno skinuti Fcheck paket sa adrese:

http://sites.netscape.net/fcheck/Fcheck_2.07.51.tar.gz

i postaviti u `/usr/local/src` ili drugo mjesto na sustavu. Ako je riječ o tek instaliranom operacijskom sustavu, preporuka je ne koristiti mrežu dok se ne postave određene sigurnosne postavke već se u tom slučaju paket na to računalo može prenijeti korištenjem disketa. Kako je paket vrlo mali, veličine oko 100 kb, ovaj postupak ne bi trebao predstavljati problem.
Nakon što se distribucijski paket nalazi na računalu potrebno je raspakirati arhivu:

```
$ cd /usr/local/etc
$ gzip -cd Fcheck_2.07.51.tar.gz | tar -xvf -
```

Perl skripte `fcheck` i `fcheck.cfg` koje dolaze sa paketom potrebno je postaviti na pravo mejsto unutar datotečnog sustava. Ovdje je preporuka napraviti novi direktorij u kojem će se držati samo datoteke od Fcheck programa, no kako je riječ samo o dvije datoteke može se slijediti i preporuka autora koja kaže da se `fcheck` skripta postavi u `/usr/local/bin/` direktorij, a `fcheck.cfg` u `/usr/local/etc/` direktorij:

```
$ cp /usr/local/src/fcheck/fcheck /usr/local/bin/
$ cp /usr/local/src/fcheck/fcheck.cfg /usr/local/etc/
```

Nakon ovoga potrebno je provjeriti prvu liniju `/usr/local/bin/fcheck` skripte koja mora pokazivati na izvršnu datoteku perl interpretera na sustavu (`#!/usr/bin/perl`). Na kraju, potrenno je još i napraviti direktorij u koji će Fcheck stavljati svoje podatke:

```
$ mkdir /usr/local/data/
```

Mjesto ovog direktorija na datotečnom sustavu može se promijeniti u `/usr/local/etc/fcheck.cfg` datoteci tako da se pronađe zapis "`DataBase = /usr/local/data`" i promijeni u željenu vrijednost.

4. Pokretanje Fcheck-a

Prije pokretanja Fcheck-a, na probnoj instalaciji praćene su promjene na datotekama koje se nalaze u /etc direktoriju. Da bi se ovaj direktorij pratio potrebno je promijeniti zapis u `/usr/local/etc/fcheck.cfg` datoteci "`Directory = /tmp`" u "`Directory = /etc`". Ukoliko se na kraju direktorija ostavi / Fcheck će provjeravati i sve poddirektorije. U ovom slučaju to je izostavljeno, tako da su se provjeravale samo datoteke koje se nalze u `/etc` direktoriju.
Fcheck je pokrenut na slijedeći način:

```
$ /usr/local/bin/fcheck -acs
```

Gdje je značenje parametara slijedeće:

- a – Automatsko pregledavanje konfiguracije direktorija.
- c – Stvaranje inicijalne baze podataka sa kojom će se uspoređivati datoteke prilikom kasnijih testiranja.
- s – Stvaranje potpisa datoteka. Dokumentacija koja dolazi sa Fcheck paketom ne ističe da je potrebno koristiti –s opciju, no ispitivanja na stvarno kompomitiranim sustavima pokazala su da je korisno imati i potpis svih datoteka budući da neovlašetni korisnici mogu nakon kompromitacije sustava proizvoljno mijenjati parametre datoteka kao što su dozvole, vrijeme

i veličina datoteke. Fcheck će za stvaranje potpisa datoteke koristiti program koji je definiran u `$Signature` parametru u `fcheck.cfg` konfiguracijskoj datoteci.

Nakon pokretanja programa, u `/usr/local/database` direktoriju moguće je vidjeti da je Fcheck napravio datoteku u kojoj se nalazi popis datoteka čiji se integritet prati kao i informacija o njima te digitalnim potpisom u istoj liniji. Ime datoteke je u formatu `ime_računala._direktorij` i obična je tekstualna datoteka koja se može pročitati sa bilo kojim Unix programom koji prihvaća tekstualne datoteke kao ulazne podatke.

Tijekom ispitivanja u slijedećem smo koraku napravili promjenu koju je Fcheck trebao detektirati. Kako smo gledali integritet `/etc/passwd` datoteke promijenili smo zaporku jednog od korisnika koristeći `passwd` komandu. Ovdje smo upisali staru zaporku – bilo je potrebno samo promijeniti kriptirani dio tako da se izazove akcija Fchecka prilikom promatranja integriteta datoteke.

Nakon toga ponovno je pokrenut Fcheck program, ovaj put samo sa –a argumentom:

```
$ /usr/local/bin/fcheck -a
```

Što je rezultiralo sa slijedećim izvještajem programa:

```
PROGRESS: validating integrity of /etc
STATUS:
 WARNING: [lefty] /etc/passwd
 Inode       Permissions Size  Created On        Name
 293999      -rw-r--r--   707   Oct 01 08:11 2000 /etc/passwd
 ** Was modified to reflect the following: **
 294000      -rw-r--r--   707   Oct 01 11:35 2000 /etc/passwd

 WARNING: [lefty] /etc/passwd-
 Inode       Permissions Size  Created On        Name
 293243      -rw-r--r--   707   Oct 01 08:11 2000 /etc/passwd-
 ** Was modified to reflect the following: **
 293243      -rw-r--r--   707   Oct 01 11:35 2000 /etc/passwd-

 WARNING: [lefty] /etc/shadow
 Inode       Permissions Size  Created On        Name
 294000      -rw-r--r--   707   Oct 01 08:11 2000 /etc/shadow
 ** Was modified to reflect the following: **
 294001      -rw-r--r--   707   Oct 01 11:35 2000 /etc/shadow

 WARNING: [lefty] /etc/shadow-
 Inode       Permissions Size  Created On        Name
 293772      -rw-r--r--   707   Oct 01 08:11 2000 /etc/shadow
 ** Was modified to reflect the following: **
 293772      -rw-r--r--   707   Oct 01 11:35 2000 /etc/shadow
```

Ovdje se vidi da je izlaz programa bio na terminal radne stanice budući da je korišten –a argument prilikom pokretanja. Da je bio upisan –l argument, sav izlaz iz Fcheck-a bio bi poslan na program koji je definiran u `Logger` polju unutar `fcheck.cfg` konfiguracijske datoteke. Naravno, standard output se može preusmjeriti na bilo koji drugi program tako da administratori sustava mogu koristiti slijedeću komandu:

```
$ /usr/loca/bin/fcheck -a | mail root@localhost
```

da bi dobili izvještaj programa e-mailom. Izlaz programa se može također usmjeriti i na nekij medij na koji je moguće samo pisati, poput pisača, ili CD-R uređaja što je poželjno za računalne sustave na kojima je sigurnost integriteta podataka od iznimne važnosti.

5. Konfiguracija

U fcheck.cfg konfiguracijskoj datoteci postoji šest jednostavnih parametara. Aktivne parametre moguće je lako izlistati slijedećom komandom:

```
$ grep –v ^# /usr/local/etc/fcheck.cfg | grep –v ^$
```

Što će dati izlaz sličan slijedećem:

```
Directory = /etc
DataBase = /usr/local/data
Logger = /usr/bin/logger –tfcheck
TimeZone = CET+1
$Signature = /usr/bin/md5sum
```

Parametar `Directory` je objašnjen ranije i u njemu je napisano koji se direktorij, odnosno integritet datoteka u njemu želi promatrati. Kao što je već rečeno, ukoliko ime direktorija završava sa / Fcheck će promatrati i integritet svih datoteka u direktorijima koji su ispod ovog zadanog. Parametar `DataBase` govori programu gdje je potrebno pohraniti rezultate. Parametar `Logger` govori programu koji će se vanjski program koristiti za logiranje rezultata. Ovaj se parametar koristi samo ako je Fcheck pokrenut sa –l argumentom sa komandne linije.`TimeZone` parametar omogućava ignoriranje lokalne vremenske zone za ispisivanje izvještaja i na kraju `$Signature` parametar specificira koji će se vanjski program koristiti za izračunavanje digitalnog potpisa datoteke. Ovaj se vanjski program koristi samo ako je Fcheck pokrenut sa –s argumentom sa komandne linije. Zadnji parametar koji se koristi u konfiguracijskoj datoteci i koji nije ispisan na primjeru je `Exclusion` parametar, koji dozvoljava administratoru definiranje imena datoteka i direktorija koji će se ignorirati.

6. Preporuka za pokretanje

Određivanje datoteka čiji će se integritet promatrati može biti kompliciran zadatak, koji se dodatno otežava na sustavima koji se često mijenjaju. Općenita preporuka je promatranje integriteta svih datoteka sustava koje su pohranjene u `/etc` direktoriju, kao i binarnih datoteka koje se nalaze u `/bin` i `/sbin` direktorijima. Ako računalni sustav predstavlja centralizirani poslužitelj na kojem se vrlo malo podataka mijenja tijekom rada, moguće je proširiti popis datoteka čiji se integritet promatra. Promatranje većeg broja datoteka neprimjetno usporuje rad programa.
Stvaranje datoteke u kojoj se nalaze potpisi datoteka treba shvatiti ozbiljno, pogotovo u slučajevima kada se promatra integritet binarnih datoteka i onih koje služe za autentikaciju (datoteke sa zaporkama ili poslužiteljima kojima se vjeruje). Ako na računalnom sustavu koji se promatra postoji puno promjena u smislu dodavana i micanja korisnika potrebno je postaviti zasebni Fcheck sustav koji će odgovarati onome na poslužitelju. Jedan proces može promatrati integritet datoteke sa zaporkama na dnevnoj bazi (ako je potrebno), dok drugi Fcheck proces može promatrati integritet datoteka sustava i konfiguracijskih datoteka. Ovdje se može koristiti –f parametar koji govori Fcheck programu koju će konfiguracijsku datoteku koristiti. Datoteke drugog procesa trebale bi biti postavljene u zasebnu hijerarhiju direktorija.
Moguće je i postavljanje crontab-a tako da se Fcheck program poziva svakih određeni broj minuta. Prema dokumentaciji programa preporučeno je pozivanje svakih deset minuta, što odgovara većini računalnih sustava.

7. Zaključak

Fcheck programski paket nije još uvijek dorađen do kraja ali predstavlja dobru pomoć za mnoge administratore sustava. Program je vrlo jednostavan i javno je dostupan izvorni kod programa, što ga čini vrlo zanimljiv za uporabu.

8. Dodatak: fcheck_file_support skripta

Iako dokumentacija Fcheck programskog podataka ističe da je on u stanju promatrati integritet pojedinih datoteka, prilikom testiranja to se nije uspjelo provesti. Zbog toga je napisana mala skripta koja je priložena i omogućava simuliranje promatranja integriteta pojdinih datoteka na sustavu. Nakon postavljanja skripte na određeno mjesto (`/usr/local/bin`) i potrebnih dozvola, moguće ju je pokrenuti sa dva parametra: imenom direktorija i imenom datoteke čiji će se integritet promatrati. Skripta će zatim ispisati listu Exclusion parametara koje je potrebno upisati u konfiguracijsku datoteku Fcheck programa. Također je potrebno postaviti i `Directory` parametar na istu vrijednost koja je upisana u fcheck_file_support skriptu.

```
#!/bin/bash
# fcheck_file_support

if echo $1 | grep -v \/$ >/dev/null
then
  dir="$1/"
else
  dir="$1"
fi

for i in 'ls $1'
do
  echo "Exclusion   = $dir$i" | grep -v "/$2"
done
```