HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

F.I.R.E Linux distribucija

CCERT-PUBDOC-2003-05-23

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

F.I.R.E. (Forensic and Incident Response Environment) je portabilna, CD-ROM bazirana, Linux distribucija, zamišljena kao jednostavan i efikasan alat za brzo provođenje forenzičke analize.
F.I.R.E nije potrebno instalirati, već se cijela distribucija prilikom podizanja s CD-ROM-a učitava u radnu memoriju računala. Ovakav pristup znatno pojednostavljuje postupak forenzičke analize kompromitiranih računala, budući da niti jedan od alata nije potrebno instalirati na računalo. Kako se distribucija temelji na inačici 2.4 jezgre Linux operacijskog sustava, podržana je široka lepeza hardvera.
Osim forenzičke analize, alati koji su dostupni na F.I.R.E CD-ROM-u, omogućuju provjeru ranjivosti sustava, antivirusno skeniranje te popravak uništenih datotečnih sustava i datoteka. Na CD-ROM-u se nalaze i aplikacije koje omogućuju analizu na pokrenutim Windows, Solaris i Linux operacijskim sustavima.
U odnosu na ostale *Open source* projekte slične namjene (Trinux, PLAC,...), F.I.R.E Linux se odlikuje vrlo jednostavnim i preglednim grafičkim sučeljem, kao i mnoštvom raznolikih paketa.

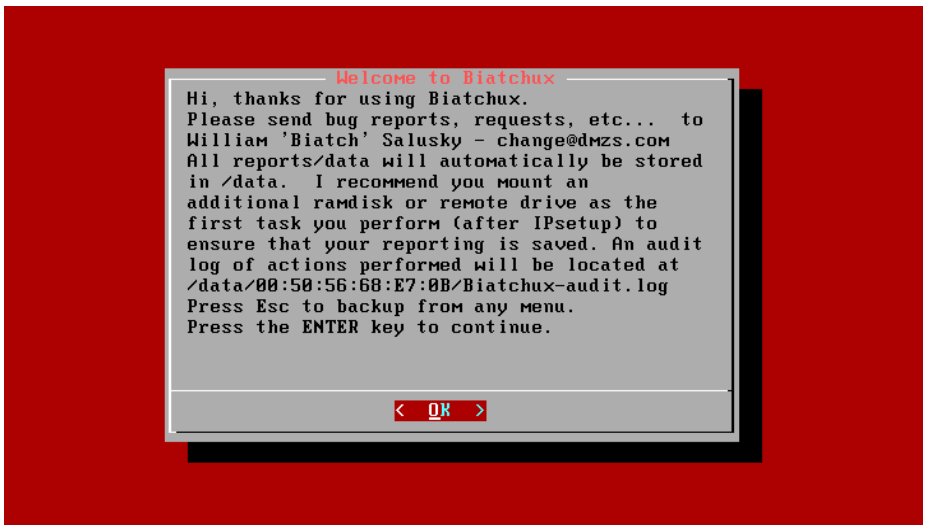
2. Pokretanje

F.I.R.E Linux nije potrebno instalirati, već ga se pokreće izravno s posebno pripremljenog CD-ROM-a. Distribucija je trenutačno dostupna isključivo kao `.iso` datoteka (http://biatchux.dmzs.com/), koju je potrebno snimiti na CD-ROM medij. Trenutačna inačica distribucije (0.4a) zauzima 578 MB. Kako bi se provjerila ispravnost dohvaćene kopije F.I.R.E Linux-a, potrebno je pomoću programa `md5sum` izračunati MD5 ključ `.iso` datoteke i usporediti ga da sadržajem `md5.txt` datoteke koja se može dohvatiti sa istog poslužitelja kao i distribucija. Postupa provjere datoteke izgleda ovako:

```
$ md5sum fire-0.3.5b.iso
fdae2b88726c6c99141c4b911350f299 *fire-0.3.5b.iso
$ cat fire-0_3_5b_md5.txt
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

fdae2b88726c6c99141c4b911350f299 *fire-0.3.5b.iso

-----BEGIN PGP SIGNATURE-----
Version: PGP 7.0.1

iQA/AwUBPearEQCUWsrXYo1REQKSdQCg5DXsok4GFDLXZQchQs7q79TZLYcAn1I8
nNJ4BWGAfGsvpPOPsydl2HzQ
=iUvO
-----END PGP SIGNATURE-----
```

Vidljivo je da su u ovom slučaju oba ključa (izračunati i dohvaćeni) jednaki, što znači da je distribucija u cijelosti i sačuvanog integriteta prenesena s udaljenog poslužitelja. U slučaju da ključevi nisu jednaki, potrebno je ponoviti dohvat datoteke. Ispravnu `.iso` datoteku potrebno je prebaciti na CD-ROM nekim od programa za snimanje na CD-R medije (npr. cdrecord).
Minimalna hardverska konfiguracija potrebna za pokretanje ove distribucije je računalo bazirano na Intel x68 procesoru sa 48 MB radne memorije. Za korištenje grafičkog načina rada potrebna je grafička kartica koja je sposobna prikazati razlučivosti od minimalno 800x600 piksela i miš.
BIOS računala na kojemu se pokreće F.I.R.E potrebno je podesiti tako da operacijski sustav podiže s CD-ROM uređaja.
Prilikom podizanja sučelja, potrebno je odabrati vrstu sučelja F.I.R.E distribucije. Moguć je izbor između naredbenog retka, tekstualne konzole (Slika 1) i grafičkog sučelja u razlučivostima ekrana od 800x600 i 1024x768. Ukoliko se odabere pokretanje sustava u naredbenom retku, tekstualnoj konzoli uvijek je moguće pristupiti pokretanjem programa `/sbin/dlg/startmenu`.

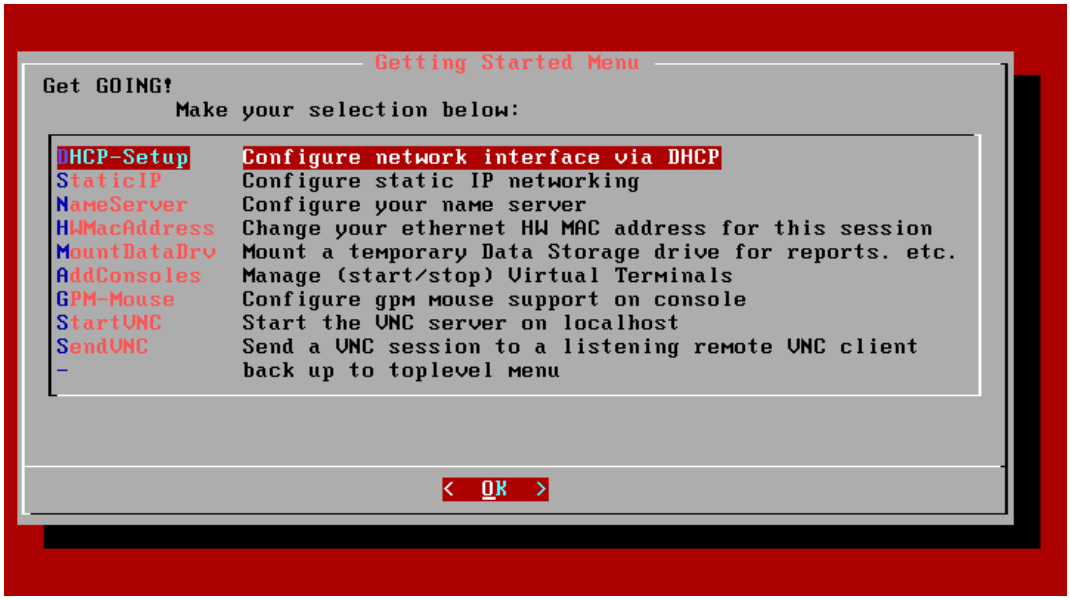
Unutar grafičkog sučelja, temeljenog na BlackBox Window Manager-u, izborniku s alatima pristupa se desnim klikom miša na radnu površinu (engl. *desktop*).
Administratorska lozinka za prijavljivanje na sustav je '`firefire`'.



Slika 1: Uvodni prozor forenzičke konzole F.I.R.E Linux distribucije

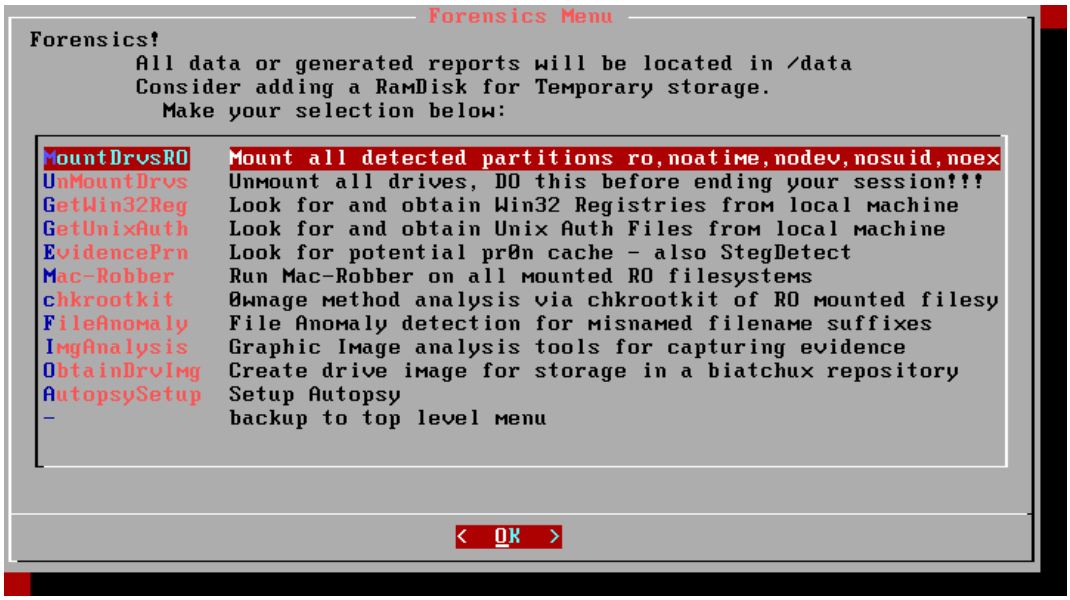
3. Forenzička analiza i spašavanje podataka

Prije pokretanja ozbiljne forenzičke analize, potrebno je odrediti neke osnovne postavke sustava. Postavke se mogu podešavati u Start-Here izborniku forenzičke konzole. Unutar ovog izbornika moguće je odabrati podešavanje mrežnih sučelja na sustavu, postavljanje dodatnog diskovnog prostora, podešavanje miša, upravljanje virtualnim konzolama, itd.



Slika 2: Podešavanje osnovnih postavki sustava

Kada je sustav ispravno podešen može se pristupiti forenzičkoj analizi. U izborniku Forensics nalaze se najpotrebniji alati za provođenje forenzičke analize.



Slika 3: Izbornik sa programima za provođenje forenzičke analize

Naravno, u izborniku se ne nalaze svi dostupni programi za provođenje forenzičke analize, već im je potrebno pristupiti i iz naredbenog retka. Neki od poznatijih programa za provođenje forenzičke analize i spašavanje podataka koji se nalaze u distribuciji su:

- The Autopsy Forensic Browser – grafičko sučelje za TASK grupu forenzičkih aplikacija
- biew – preglednik datoteka s podrškom za pregledavanje binarnih i heksadecimalnih datoteka
- chkrootkit – alat za pronalaženje rootkit aplikacija instaliranih na sustavu
- editreg – Linux aplikacija za pregledavanje Windows Registry datoteka
- fatback – aplikacija za spašavanje datoteka sa FAT32 diskovnih particija
- FTimes – vrlo koristan *baselining* alat
- Linux Disk Editor – alat za pregledavanje i editiranje sadržaja tvrdog diska
- StegDetect – alat za automatsku detekciju steganografskih sadržaja unutar JPEG slika
- TCT – kolekcija alata za forenzičku analizu
- TestDisk – alat za spašavanje uništenih particija tipa FAT12, FAT16, FAT32, Linux, Linux SWAP (inačice 1 i 2), NTFS (Windows NT), BeFS (BeOS), UFS (BSD), Netware i ReiserFS
- The Sleuth Kit (TASK) – popularan set aplikacija za forenzičku analizu

4. Analiza na pokrenutom operacijskom sustavu

U određenim situacijama nije poželjno zaustavljati rad poslužitelja radi provođenja forenzičke analize na operacijskom sustavu. Budući da postoji sumnja u integritet sustava, za analizu nije poželjno koristiti naredbe koje već postoje na sustavu, zbog opravdane bojazni da je napadač ispravne inačice naredbi zamijenio malicioznima.

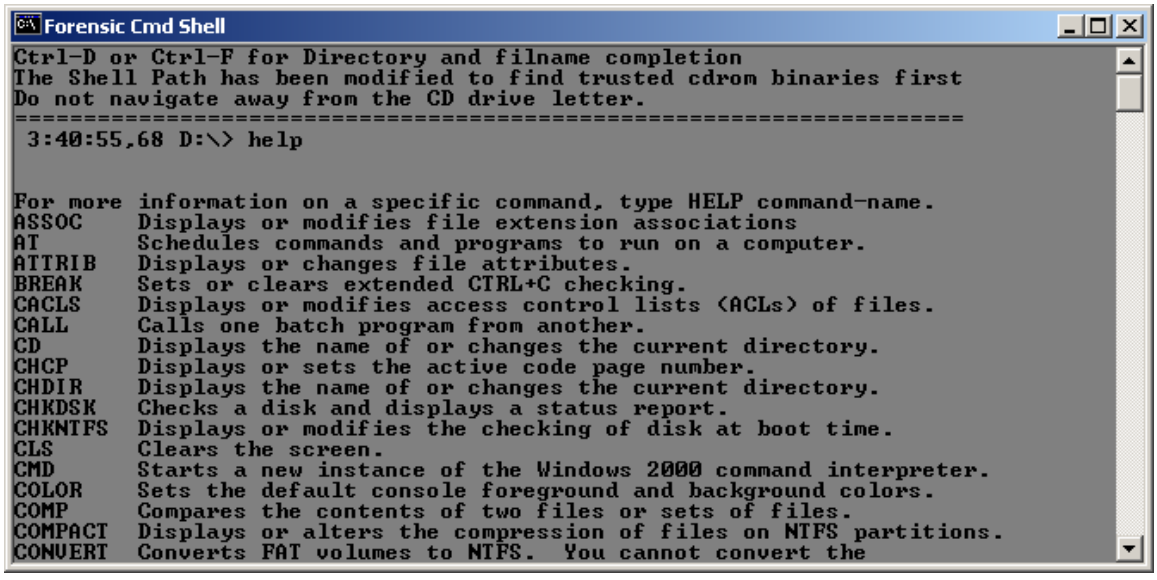
Za takve slučajeve, F.I.R.E Linux sadrži setove osnovnih sistemskih naredbi koje su prevedene tako da se mogu pokretati izravno s CD-ROM-a na Windows, Linux i Solaris operacijskim sustavima. Tek pomoću tih, "sigurnih", inačica naredbi, administratoru je omogućen potpun uvid u stanje kompromitiranog sustava.

Na Linux i Solaris operacijskim sustavima, "sigurne" naredbe se pokreću iz naredbenog retka, a nalaze se u direktoriju `/statbins` na CD-ROM-u.

Kod korisnika Windows operacijskih sustava, prilikom pokretanja CD-ROM-a pojavljuje se forenzički izbornik (Slika 4), unutar kojega je osim naredbene konzole (Slika 5) ugrađena i podrška za VNC terminalski rad i podrška za IRC.

Slika 4: Forenzički izbornik za Windows operacijski sustav

Kod pokretanja naredbene konzole, varijable okoline na sustavu postavljaju se tako da se "sigurne" naredbe pokreću prije izvornih sistemskih naredbi. Prilikom provođenja analize poželjno je ne izlaziti iz korijenskog direktorija CD-ROM-a.



Slika 5: Naredbena konzola za provođenje analize na Windows operacijskim sustavima

5. Antivirusni alati

Kao antivirusni alat, u F.I.R.E distribuciju je uključen program F-prot tvrtke FRISK (http://www.f-prot.com/). Ovaj, inače komercijalan proizvod, za Linux operacijske sustave dostupan je kao besplatna probna inačica. Pomoću ovog alata na kompromitiranom sustavu moguće je detektirati velik broj virusa, crva i trojanskih konja za Windows, DOS i Linux operacijske sustave. Provjeravane tvrde diskove (ili particije) je prije skeniranja potrebno postaviti naredbom `mount`.

Prednost ovakvog pristupa skeniranju je ta što virus prilikom skeniranja nije aktivan (budući da operacijski sustav nije podignut) te nije u mogućnosti ometati rad antivirusnog alata.
Budući da se novi virusi i trojanski konji pojavljuju gotovo svakodnevno, program podržava mogućnost dohvata datoteka s definicijama novih virusa (*signature* datoteke) preko mreže (http://www.f-prot.com/download/) ili sa diskete. Kako se cijela distribucija temelji na memorijskom disku, prilikom dohvata *signature* datoteka potrebno je osigurati dodatan prostor na tvrdom disku (postavljanjem dodatnih particija), kako bi se datoteke mogle uspješno pohraniti.

6. Provjera ranjivosti

Kao dodatna opcija, u distribuciju je uključena i mogućnost provjere ranjivosti ostalih računala na mreži. U tu svrhu mogu se koristiti sljedeći alati:

- ADMsmb – alat za provođenje *brute force* napada
- darkstat – analizator mrežnog prometa
- ethereal – analizator mrežnih protokola
- Firewalk – aplikacija za provjeravanje sigurnosti vatrozida
- hping2 – mrežni alat za kreiranje proizvoljnih TCP paketa
- john – alat za provjeru sigurnosti korisničkih zaporki
- nessus –trenutno najpopularniji *open source* alat za provjeru ranjivosti
- Nikto – alat za provjeru sigurnosti Web poslužitelja
- nmap – popularni alat za pregledavanje portova
- nsat – jednostavan i brz alat za provjeru ranjivosti
- packit – jednostavna aplikacija za generiranje proizvoljnih TCP paketa
- Pandora – set alata za ispitivanje sigurnosti računalnih mreža baziranih na Novell Netware operacijskom sustavu
- smtpscan – alat za otkrivanje inačice SMTP poslužitelja
- snort – popularan IDS sustav
- ssldump – analizator mrežnog prometa za SSL protokol
- whisker – alat za provjeru ranjivosti CGI skripti instaliranih na Web poslužitelju
- zodiac – alat za provjeru sigurnosti DNS poslužitelja

Nabrojanoj skupini alata potrebno je dodati stotinjak manje poznatih i manje korisnih aplikacija, koje su zbog duljine popisa izostavljene. Navedene aplikacije nisu primarno namijenjene forenzičkoj analizi, ali se mogu pokazati vrlo korisnima prilikom analize incidenata na nepoznatoj računalnoj mreži.

7. Zaključak

Testirana Linux distribucija pokazala se kao koristan alat za brzu forenzičku analizu kompromitiranih računala. Jednostavnost upotrebe CD-ROM baziranih distribucija omogućuje nenapadnu forenzičku analizu kompromitiranih sustava u vrlo kratkom vremenskom roku i bez značajnih zahvata na hardveru analiziranog računala. Također, set alata prevođen za pokretanje na različitim operacijskim sustavima (Linux, Windows, Solaris), omogućuje jednostavno provođenje analize na računalima čija je dostupnost kritična.
Nešto veći hardverski zahtjevi, u odnosu na ostale distribucije iste namjene mogu se opravdati velikim brojem paketa i iznimno dobrim grafičkim sučeljem.