

---

## Analisi di sistemi compromessi (ricerca di “rootkit”, backdoor, ...)

---

**Massimo Bernaschi**

Istituto per le Applicazioni del Calcolo “Mauro Picone”

Consiglio Nazionale delle Ricerche

Viale del Policlinico, 137 - 00161 Rome - Italy

<http://www.iac.cnr.it/>

e-mail: [m.bernaschi@iac.cnr.it](mailto:m.bernaschi@iac.cnr.it)

---

## Alcuni strumenti utili

### **nc:** (netcat)

`http://www.vulnwatch.org/netcat/nc110.tgz`

Come prepararlo: `tar zxvf nc110.tgz; make linux;`

**Attenzione:** a volte è necessario commentare la `res_init()`

**dd:** `http://www.gnu.org/software/fileutils/fileutils.html`

(aggiunto alle “core” utilities)

**netstat, arp, route:** `http://freshmeat.net/projects/net-tools/`

Come prepararli: `bzip2 -d net-tools-1.60.tar.bz2; tar xvf`

`net-tools-1.60.tar; make config; make CC=“gcc -static”;`

come verificarli: `file netstat arp route o ldd netstat arp route`

**lsof:** `ftp://lsof.itap.purdue.edu/pub/tools/unix/lsof/lsof.tar.gz`

Come prepararlo: `tar zxvf lsof.tar.gz; cd lsof_4.73_src;`

tar xvf lsof\_4.73\_src.tar; ./Configure linux; make CC="gcc -static";  
come verificarlo: lsof -h;

**module\_hunter.o:** [http://www.phrack.org/phrack/61/p61-0x03\\_Linenoise.txt](http://www.phrack.org/phrack/61/p61-0x03_Linenoise.txt)

Per rendere il modulo più indipendente rimuovere le seguenti linee dal codice sorgente:

```
#ifdef CONFIG_MODVERSIONS
#define MODVERSIONS
#include <linux/modversions.h>
#endif
```

È possibile caricare questo modulo su altri kernel rimuovendo MODVERSIONS

Come prepararlo: gcc -c module\_hunter.c -I/usr/src/linux/include/  
(fare attenzione al path di include).

**dmesg:** <http://ftp.cwi.nl/aeb/util-linux/util-linux-2.12.tar.gz>

Come prepararlo: ./configure; make CC="gcc -static";  
come verificarlo: file dmesg o ldd dmesg

Questi strumenti dovrebbero essere caricati su un CD per un'analisi “a caldo” del sistema compromesso. Esistono già “pronti” allo scopo:

- **Knoppix**
- **F.I.R.E.** disponibile su  
<http://biatchux.dmzs.com/?section=main>
- **Professional Hacker Linux Assault Kit** disponibile su  
<http://www.phlak.org/>
- **Auditor security collection** disponibile su:  
<http://moser-informatik.ch/?page=products&lang=eng>

Una serie di strumenti tipici Unix/Linux (*e.g.*, `grep`, `find`,...) sono stati portati in ambiente Windows all'interno del progetto `gnuwin32`: <https://sourceforge.net/projects/gnuwin32>.

Un'alternativa più semplice, anche se i singoli pacchetti sono meno aggiornati, è disponibile da <http://unxutils.sf.net>.

Altri importanti tool “Unix-like” per Windows:

- `dd.exe`;
- `md5sum.exe`;
- `wipe.exe` (“sterilizza” un disco);
- `Volume_dump.exe` (fornisce informazioni su un volume);
- `nc.exe`.

sono disponibili su <http://users.erols.com/gmgarner/forensics/>

**TCPView** disponibile su

<http://www.sysinternals.com/ntw2k/source/tcpview.shtml>

mostra informazioni dettagliate su porte TCP e UDP

(compresi i nomi dei processi che utilizzano le porte).

Uno strumento simile è **Fport**, disponibile su

<http://www.foundstone.com/knowledge/proddesc/fport.htm>

**DumpReg** disponibile su <http://www.systemtools.com/somarsoft/>

effettua un *dump* del Registry che permette di effettuare più facilmente ricerche, ad esempio, delle ultime chiavi inserite o modificate.

## Pacchetti per l'analisi di sistemi compromessi

Linux offre la possibilità di usare un filesystem contenuto in un file. È possibile quindi montare un'immagine contenuta in un file XYZ.dd nel seguente modo:

```
mount -o ro,loop -t vfat XYZ.dd /t
```

Il supporto nativo di Linux non permette di montare un'immagine di disco che contenga più partizioni. In questo caso si può

1. estrarre le partizioni individuali con il comando `dd`:

```
dd if=host_hda.dd of=host_hda1.dd bs=512 skip=63 count=15119937
```

le informazioni specifiche su numero di blocchi, punto di inizio, *etc.*, possono essere ottenute con il comando:

```
fdisk -lu host_hda.dd
```

2. utilizzare l'*enhanced loopback driver* che permette di accedere

l'intero hard disk come un dispositivo di loopback. Il software è disponibile da:

`ftp://ftp.hq.nasa.gov/pub/ig/ccd/enhanced_loopback`

Il Coroner's Toolkit, sviluppato da Dan Farmer e Wietse Venema, è disponibile su <http://www.fish.com/security/forensics.html>.

I principali programmi nel TCT sono:

- **grave-robber**: uno strumento per la raccolta di informazioni, tipicamente informazioni su *i-node*:

```
grave-robber -d /tmp
```

- **unrm** e **lazarus**: strumenti per il recupero di file cancellati o l'accesso allo swap space.

```
unrm /dev/hdXX > /data/victim.hdXX.unrm
```

Su `/data` deve essere disponibile una quantità di spazio disco pari, almeno, a quella che risulta libera sulla partizione in esame.

- **mactime**: ordina file e directory nel file system sulla base delle informazioni sui tempi di Modifica, Accesso, Cambio (“MAC”) reperite nell'*i-node*:

```
./mactime -d /tmp -R 07/01/2003 | tac | less
```

- **ils**: fornisce informazioni sugli *i-node* di file rimossi

```
./ils -r -f ext2fs /dev/hda4 | less
```

- **icat**: per recuperare il contenuto del file corrispondente ad uno degli *i-node*:

```
./icat -hf ext2fs /dev/hda4 XXXX
```

per recuperare tutti i file (con nomi **non** contenenti caratteri speciali) cancellati:

```
./ils -rf ext2fs /image/dev_hda1.img | awk -F '|' '($2=="f") {print $1}' |  
while read i; do ./icat /image/dev_hda1.img $i > /tmp/deleted/$i; done
```

- **pcat**: permette di copiare la memoria di un processo attivo.

## Sleuthkit ed Autopsy

Un'evoluzione del TCT è rappresentata dal pacchetto “*SleuthKit*”:  
<http://www.sleuthkit.org/sleuthkit> o <http://sleuthkit.sourceforge.net>  
per il quale è disponibile un'interfaccia (“*autopsy*”) via browser:  
<http://www.sleuthkit.org/autopsy> o <http://autopsy.sourceforge.net>.  
In particolare, *SleuthKit* supporta una serie di file systems più ampia  
del TCT (**ext3**, **HFS**, **NTFS**, ...).

- È possibile sperimentare questi tool su immagini di disco di diverso tipo (NTFS, EXT3, FAT) disponibili su <http://dftt.sourceforge.net> oppure da <http://project.honeynet.org/challenge/images.html>.
- È possibile sperimentare direttamente su un'immagine di disco accedendo la partizione corrispondente (/dev/hda1 o /dev/hda4 ad esempio).

- Per utilizzare al meglio questi strumenti è richiesta una certa familiarità con il formato interno dei diversi file system.
  - Informazioni di base sul formato dei file system Windows (**FAT** e **NTFS**) sono disponibili su:  
<http://www.sleuthkit.org/sleuthkit/docs/>.
  - Informazioni sui formati Linux **ext2** ed **ext3** sono disponibili su <http://e2fsprogs.sourceforge.net/ext2intro.html>.  
Poiché **ext3** è sostanzialmente identico all'**ext2** con l'aggiunta delle funzionalità di *journaling* è sufficiente consultare le FAQ su  
<http://batleth.sapientisat.org/projects/FAQs/ext3-faq.html>

I tool forniti dallo Sleuthkit possono essere divisi in 5 categorie:

1. comandi che mostrano informazioni su filesystem completi o partizioni: `fsstat` e `mmls`;
2. comandi che permettono di accedere dati nei file: `dcalc`, `dcat`, `dls`, `dstat`;
3. comandi che permettono di accedere i “metadati” associati ai file: `icat`, `ifind`, `ils`, `istat`;
4. comandi che permettono di svolgere compiti come creare liste di file o cercare file: `fls`, `ffind`;
5. comandi che permettono di ordinare i file per tipo: `file`, `sorter`.

Il comando `mactime` mostra gli eventi sul file system in ordine cronologico.

```
fls -f ntfs -r /dev/hda1 -m / | mactime 01/01/2001 | tac | less
```

Il recovery dei file è analogo a quello del TCT:

```
#!/bin/bash
ils -f fat32 -r /dev/hda1 | tail +4 | awk -F '|' '$11 > 0 {print $1}' | \
while read in; do
    icat -f fat32 /dev/hda1 $in > /tmp/rectmp/$in
done
./file /tmp/rectmp/* | egrep "Office"
```

**Autopsy** permette di accedere via browser gli strumenti dello Sleuthkit.

- L'installazione di Autopsy deve essere effettuata **dopo** quella dello Sleuthkit in quanto viene richiesto il nome della directory dove è installato.
- È consigliabile creare una directory per salvare i diversi “casi” che vengono creati con Autopsy.
- Quando viene fatto partire **autopsy**, viene mostrato un *URL* (`http://...`) che può essere acceduto con un qualsiasi browser.
- La sequenza di operazioni standard eseguita attraverso il browser è la seguente:
  1. creazione di un nuovo “caso”;
    - viene creata la directory che conterrà tutte le informazioni specifiche sul caso.

2. definizione del sistema(i) che verrà analizzato (*add host*);
3. definizione dell'immagine di disco che verrà analizzata (*add image*)
  - **è possibile analizzare direttamente la partizione fisica** (ad esempio: `/dev/hda1`);
4. a questo punto inizia l'analisi vera e propria selezionando *File Activity Time Lines*:
  - vanno prima estratte le informazioni che costituiscono il *body* attraverso la scelta *Create Data File*.  
In pratica vengono utilizzati i comandi `fls` ed `ils` dello Sleuthkit.
  - la scelta *Create Timeline* mostra la sequenza di operazioni sul file system in ordine cronologico.

Autopsy offre anche altre funzionalità come l'ordinamento dei file per tipo o la ricerca di parole chiave (*keyword searching*).

- Dopo che è stata completata la creazione della *timeline* è possibile accedere alle altre funzionalità selezionando dalla schermata dei casi i *details* dell'immagine desiderata (sotto **HOST MANAGER**)
- Nella schermata successiva è possibile scegliere di estrarre i dati non allocati oppure di andare direttamente alla schermata di gestione del file system da dove si accede l'ordinamento dei file per tipo, la ricerca di stringhe, i “metadati” del file system.
  - Fare attenzione se viene utilizzata la feature di *keyword searching* di Autopsy perché viene effettuata in sostanza una ricerca “fisica”. In altre parole non si considera la struttura logica ma l'immagine viene vista come un unico blocco di dati.