



Computer Forensics

"Introduzione alla Computer Forensics"

di

Andrea "Pila" Ghirardini, CISSP

Copyright 2002 by Pila' Security Services sas. L'opera è liberalmente distribuibile a patto di non stravolgerne il contenuto e di citarne la fonte

SIKUREZZA.ORG
Italian Security Mailing List



Computer Forensics I

L'accezione “Computer Forensics” si riferisce a quella disciplina che si occupa della preservazione, dell'identificazione, dello studio, della documentazione dei computer, o dei sistemi informativi in generale, al fine di evidenziare prove per scopi di indagine



Computer Forensics II

Questa disciplina viene erroneamente identificata come una “nuova” branca della computer security.

In realtà è semplicemente giunta alla ribalta dei media di recente, con l'aumento dei crimini informatici e, specialmente, con una presa di coscienza da parte delle aziende che, finalmente, hanno cominciato a denunciare i crimini di cui sono vittime.



Computer Forensics III

Perchè interessarsi di “Computer Forensics”?

- Richiede elevatissime conoscenze informatiche (migliora drasticamente le proprie conoscenze)
- Affina capacità di analisi, capacità di osservazione e pazienza
- Le forze dell'ordine non possiedono le figure necessarie e c'è una fortissima richiesta di consulenti esterni specializzati. La richiesta è destinata ad aumentare drasticamente



Computer Forensics: “Chain of custody” I

La preservazione in maniera corretta delle prove e dei materiali acquisiti è vitale al fine di evitare che l'intero lavoro sia invalidato per un cavillo legale.

E' vitale ricordare che, lavorando con evidenze effimere (quali possono essere i file di log o un programma in ram) è fin troppo facile distruggere una prova determinante con un semplice passo falso.



Computer Forensics: “Chain of Custody” II

Il lavoro poi è reso particolarmente arduo dal fatto che spesso, quando giungiamo sul luogo, gli amministratori di sistema, hanno già “pasticciato” sul sistema incriminato, minando quindi l'indagine in partenza.

La gestione e la raccolta delle prove richiedono disciplina, esperienza e un'attenzione quasi maniacale



Computer Forensics: “Chain of Custody III”

Sia nella raccolta sia nel mantenimento delle prove è vitale quindi tenere in considerazione:

- Deve esserci sempre un sistema per garantire che le prove non vengano alterate nel corso dell'indagine (MD5 o Digital Hash) La firma digitale deve essere ovviamente conservata in luogo diverso dal file a cui si riferisce
- Operare **SEMPRE**, ove possibile, con delle copie e non con i file originali (off-line analysis)



Computer Forensics: Competenze necessarie I

- Conoscenza approfondita dei principali Sistemi Operativi presenti (vari Windows, vari dialetti Unix e sistemi Unix like)
- Conoscenza molto approfondita dei principali file system (FAT, VFAT, FAT32, NTFS, Ext2, Veritas, Reiserfs)
- Buona conoscenza dei principali formati file (un conto è sapere che jpeg è un formato grafico un conto che la stringa “4A 46 49 46 00 01” è un pattern univoco per distinguere questi file)



Computer Forensics: Competenze necessarie II

- Ottima conoscenza sull'uso di una serie di tool di monitor, hacking ed altro quali:
 - Editor Esadecimale
 - Vari tool di computer forensics (Encase, TCT, ForensiX)
 - Debugger asm
 - Tool unix di ricerca (grep, ngrep, perl)
 - Sniffer (Ettercap, Ethereal)
 - IDS (Snort, NFR)
 - Tool per l'analisi dei file system
 - Vmware



Computer Forensics: Competenze necessarie III

- Networking (cablaggi e topologia)
- LAN & WAN
- TCP/IP, IPX/SPX
- Vari protocolli applicativi (FTP, HTTP, SMTP)
- Hacking e Hardware



Computer Forensics: Hardware necessario

Nonostante sia il primo tipo di computer che possa venire in mente un notebook o un laptop non è solitamente la scelta migliore per un computer forenser.

Le capacità di collegamento con media esterne sono solitamente troppo limitate per renderli idonei come scelta.

Diverso il discorso se intendiamo utilizzare il notebook per analizzare il traffico di rete



Computer Forensics: Hardware necessario II

- La “dream machine” di un computer forenser dovrebbe avere le seguenti caratteristiche:
 - Ampia memoria (> 512 Mb)
 - Possibilità di connettersi con svariati tipi di media (Firewire, USB 2.0, UWSCSI2, ATA133)
 - Ampio disco, con possibilità di avere supporti rimovibili
 - Connessione di rete (Ethernet, FDDI...)
 - Sistema di backup di ampia capacità
 - CD-Writer (o DVD Writer)



Computer Forensics: Hardware necessario III

- E' possibile costruire da se la propria macchina per computer forensics. In questo caso si risparmierà qualcosa ma il lavoro potrebbe occupare molto tempo con risultati non perfetti
- In caso contrario esistono, pochi, fornitori specializzati in hardware di questo genere.
 - <http://www.computer-forensics.com>
 - <http://www.forensic-computer.com>



Computer Forensics: Software di base I

- Sistemi Operativi:
 - Uno Unix Free
 - Linux è e rimane un'ottima scelta dato che dispone:
 - Ampio supporto per filesystem non nativi (26 in tutto)
 - Ottima selezione di utilities
 - Ampio supporto hardware
 - Stabilità



Computer Forensics: Software di base II

- Un sistema Windows a 32 bit (2000 o XP Professional)
 - Utile per investigare svariati tipi di formati file per i quali non ci sia un applicazione Unix in grado di importare i dati per una visualizzazione.
 - Ottimo per l'uso con Encase tende però e non rispettare i filesystem come può fare Unix. Deve essere mediato da un altro sistema per evitare che alteri informazioni vitali



Computer Forensics: Tool necessari I

- Tool per la copia bit-a-bit del file system
 - Unix
 - DD
 - Ddrescue
 - Windows
 - Norton Ghost
 - Partition Magic
 - Image Magic Foresinc Solo



Computer Forensics: Tool necessari II

- Tool di Computer Forensics
 - Unix
 - ForensiX (<http://www.all.net>)
 - TCT (<http://www.fish.com/tct>)
 - Windows
 - Encase (commerciale)
 - NTI Tools



Computer Forensics: Tool necessari III

- Tool generici
 - Vari Comandi Unix (porting su Windows tramite Cygwin)
 - Perl
 - Editor Esadecimali
 - NT Resource Kit
 - Gestore archivi compressi
 - File viewer (Quick View Plus della Jasc)



Computer Forensics: Accessori

- Cavi vari
- Fotocamera digitale
- Victorinox Cybertool
- Blocco notes o meglio PDA
- Registratore digitale o a cassette (o PDA)
- Etichette adesive e buste di plastica
- Floppy Disk nuovi e CDR



Computer Forensics: Una macchina Windows

Premessa:

Siete stati chiamati per analizzare un computer Windows 2000 che si pensi sia stato utilizzato per la diffusione di immagini pedopornografiche.



Computer Forensics: Una macchina Windows II

- Iniziate subito ad annotare tutte le operazioni che compite, con data e ora di ognuna di esse
- Iniziate a smontare la macchina (di fronte a testimoni) e a rimuovere il disco fisso.
NON FATE MAI UN BOOT DAL COMPUTER INCRIMINATO
- Collegate il disco fisso alla stazione da computer forensics ed effettuate una copia bit-a-bit delle partizioni presenti



Computer Forensics: Una macchina Windows III

- Per mantenere la “Chain of Custody” fate un hash dei file di output, annotate il valore e consegnate una copia dei file di hash all'autorità
- Per tutto il resto dell'indagine è **VITALE** non modificare mai le immagini delle partizioni
- Montare quindi le partizioni in readonly via loopback device su uno Unix Free ed esportare il mount point via samba verso una macchina Windows (sia essa reale o virtuale). Si evita che Windows modifichi le immagini.



Computer Forensics: Una macchina Windows IV

- Cominciare la ricerca ad alto livello utilizzando gli strumenti classici messi a disposizione del SO, se si ha fortuna la cosa finisce in fretta
- In caso contrario scendere di livello e cominciare ad esaminare nell'ordine:
 - Archivi zip
 - Contenuto del cestino
 - Esame delle signature (nel caso l'estensione non sia coerente)
 - Esame dello spazio non allocato (alla ricerca di file cancellati)



Computer Forensics: Una macchina Windows V

- Controllare i file di log e gli eseguibili presenti per verificare se esistono sistemi per la diffusione dei file
- Documentare ogni passo e stendere la relazione finale



Computer Forensics: Una macchina Unix

Premessa:

Siete stati chiamati per esaminare una macchina Unix che si sospetta sia stata violata da un cracker per essere utilizzata come “testa di ponte” per un successivo hack



Computer Forensics: Una macchina Unix II

L'analisi può passare da un medio livello di difficoltà and un vero “incubo”, dipende dall'abilità del cracker che ha violato la macchina.

Dobbiamo tenere conto di una nuova serie di fattori che potrebbero intervenire come l'installazione di una backdoor o di un rootkit e la cancellazione dell'eseguibile un volta lanciato in memoria



Computer Forensics: Una macchina Unix III

Questo è uno di quei casi in cui dobbiamo aggiungere all'analisi “off-line” anche un'analisi “live” per esaminare la memoria RAM.

Molti cracker infatti lanciano i programmi che usano per creare le backdoor in memoria per poi cancellare l'eseguibile dal file system.



Computer Forensics: Una macchina Unix IV

Per eseguire la parte “live” dell'analisi è indispensabile utilizzare comandi e tool provenienti da un nostro CD o generati da un'altra macchina con lo stesso hardware o lo stesso SO.

Non possiamo infatti sapere a priori se il cracker abbia cambiato i comandi del sistema operativo per nascondere le sue tracce



Computer Forensics: Una macchina Unix V

Per evitare alterazioni della memoria la prima operazione che dobbiamo compiere è il dump della RAM, utilizzando tool appositi oppure il /proc file system per quegli Unix che lo implementano.

Successivamente possiamo controllare, evitando alterazioni, i processi attivi, i moduli a livello kernel caricati, le connessioni in essere al momento.



Computer Forensics: Una macchina Unix VI

Successivamente potremmo spegnere la macchina (brutalmente), o mandarla in freeze per quelle workstation che implementano tale funzione (le Sun ad esempio con STOP-A), ed effettuare una copia bit-a-bit del disco fisso del computer.

Procederemo poi ad un'analisi “off-line”.



Computer Forensics: Una macchina Unix VII

C'è la possibilità che la maggior parte dei log siano stati cancellati quindi, tramite TCT o altri tool, dovremmo preovvedere ad esaminare lo spazio non allocato alla ricerca dei file cancellati.

L'analisi potrebbe richiedere un tempo relativamente lungo per essere portata a termine.



Computer Forensics: Una macchina Unix VIII

Potremmo agire anche seguendo un diverso *modus operandi*, trasformando la macchina violata in una honeypot e sorvegliando la connessione di rete tramite un sistema di Intrusion Detection System per tracciare le connessioni effettuate dal cracker.



Computer Forensics

Domande
e
Risposte