Digital forensics

È la tipologia di computer forensics che viene effettuata sul supporto da analizzare quando il dispositivo è SPENTO, è dunque necessario acquisire i dati in maniera raw o bit a bit in modo da poter lavorare sui dati cristallizzati presenti sull'hard disk, consentendo di acquisirne tutte le memorie, inclusi slack space e file cancellati, in modo da poterne avere un clone perfetto che andrà memorizzato su un supporto esterno sterilizzato tramite la procedura wiping (di cui è bene conservare un log) o su un file immagine. FONDAMENTALE è effettuare l'analisi in ambiente virtuale e su una copia del file (anzi su una copia della copia) per consentirne la RIPETIBILITA' e non perdere i dati iniziali. In questo modo anche se viene effettuato un errore durante le varie procedure si può tornare al dato iniziale e non compromettere le indagini in corso.

L'ANALISI

Gli strumenti usati per l'**analisi** devono essere anzitutto collaudati e accettati dalla comunità degli esperti, inoltre, cosa più importante, chi li usa deve averne una conoscenza approfondita e usarli nel modo giusto, senza fretta né stress e senza farsi condizionare da opinion i personali. Se si usano strumenti nuovi allora è utile fornirne il codice sorgente. Per una maggior sicurezza dei dati trattati i dischi si custodiscono sempre in buste elettrostatiche e anticaduta e l'analisi viene eseguita in ambienti sterili.

STRUMENTI

Sono ovviamente sia strumenti HD che SW. Si possono scegliere sia TOOLS COMMERCIALI che creano problematiche come la presenza di bugs o formati troppo proprietari o OPEN SOURCE TOOLS che hanno come vantaggi indiscutibili il controllo dei bugs, formati aperti e compatibili e una sorgente aperta a tutti. Ciononostante non si deve effettuare una scelta arbitraria, essendoci dei software commerciali che effettuano operazioni che gli open source non fanno e viceversa.

Alcuni tipi di tools open source sono:

CAINE, DEFT, FORLEX, FCCU, HELIX. (software elaborati da Linux)

Mentre fra i tools closed source vi sono:

- Encase (GuidanceSoftware)
- ForensicToolkit (Acces Data) - FREEWARE
- X-waysForensic (X-Way)
- P2 Commander (Paraben Corporation)

Uno degli strumenti FONDAMENTALI per proteggere i dischi sorgente è il **WRITE BLOCKER**, dispositivo che previene delle eventuali scritture sull'hard disk oggetto di investigazione. Esso viene generalmente posto tra il disco e il computer utilizzato per esaminarlo.

Ci sono tre tipologie di write blocker:

- Firmware based: tramite il BIOS inibiscono ogni tipo di scrittura sul disco d'origine;

- Software o driver based: software a basso livello, intercettano qualsiasi interruzione hardware o software che vada a effettuare una qualsiasi scrittura sulla memoria di massa considerata. In questo caso non è più il BIOS a impedire l'alterazione, ma il sistema operativo, e dei bug presenti in esso potrebbero causare il malfunzionamento del writeblocker;

- Hardware based: sono dispositivi elettronici che tagliano il bus di comunicazione tra l'unità su cui si stanno copiando i dati e la scheda madre del computer analizzato, sono come degli intermediari che inibiscono qualsiasi fuoriuscita di dati dal dispositivo incriminato, in questo modo l'analisi viene messa al sicuro dagli errori umani e da eventuali bug.

OLTRE AGLI STRUMENTI…

È necessario però che oltre a degli strumenti adeguati anche l'operatore abbia una certa ESPERIENZA e anche un SESTO SENSO, infatti come su una vera e propria scena del crimine, le prove possono essere nascoste in posti introvabili (protette da password, nascoste dentro immagini [steganografia], server internet…). A volte per risparmiare tempo e andare a colpo sicuro nella ricerca dei reperti può essere utile un profiling del sospettato e dedicare un po' di tempo al suo profilo psicologico per riuscire a risparmiare tempo nella ricerca delle PROVE. Due approcci possono essere quello deduttivo, cioè l'idea generale che si ha del colpevole si adatta al caso specifico del crimine commesso, o induttivo, grazie a un'analisi statistica del caso particolare si può risalire a una descrizione più generale.

OPERATIVITA'

REPERTAMENTO

Secondo il codice di procedura penale articolo 247 par.1-bis "…Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorchè protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione. (1)". In certi casi tuttavia non è necessaria un vero e proprio sequestro del computer ma sarà sufficiente una masterizzazione delle trace pertinenti al reato.

Sia in caso di sequestro che di semplice copia dei dati vi è una procedura da rispettare:

- controllare se il PC è acceso: se vi sono volumi criptati procedere con procedura live.

- Spengere il computer con distacco dall'alimentazione

- Sequestrare computer (anche solo per la copia è comunque necessario leggere l'orario BIOS e capire l'architettura dell'hard disk)

- Sequestrare altri eventuali supporti (cd-rom, hd esterni, fax, stampanti…)

- Richiedere eventuali password e documentazione utile per capire la tipologia dell'hard disk

- Imballare tutto con guanti in lattice, fotografare tutto e portare via

- Fissare infine data per acquisizione/duplicazione dei supporti.

La procedura prevede anche che i dischi sequestrati debbano essere maneggiati con guanti elettrostatici e che tutte le fasi del repertamento siano fotografate. Inoltre tutti i dati vanno verificati con i codici hash MD5 e SHA1 (che pur essendo vulnerabili al collision attack, sono i due tipi di hash non vulnerabili ai preimage attacks, unici attacchi effettivamente praticabili su un caso reale) e ne va calcolata l'impronta hash. Durante la fase di repertamento è anche necessario rilevare sempre lo scarto orario durante le acquisizioni poiché sarà poi utile per interpretare i simboli dei log rappresentati vicino all'ora.

ANALISI DELL'HARD DISK

Per la copia dei file dal drive fisico viene usato il dispositivo hardware FORENSIC TALON, strumento creato specificatamente per l'acquisizione di dati in analisi forense. Il suo funzionamento prevede sia la copia che l'analisi dei file, con codici hash, con una velocità di scrittura che può arrivare a 4GB/min. grazie a vari tipi di adattatori e software esso può essere applicato a molteplici tipi di drive e vi possono essere memorizzati diversi formati di DD image. Da questo dispositivo si possono poi copiare i file su altri drive per ulteriori analisi.

Nella copia dell'hard disk ci si approccia in due modi, ottimistico, considerando il disco sano e tutti i settori sani, mentre se durante l'acquisizione si hanno degli errori di lettura si tenderà ad avere un'ottica più pessimistica, quindi considerando il disco con qualche settore danneggiato.

Per acquisire un hard disk in modo tale che la copia sia identica all'originale si usa il comando DD che permette di copiare un file a blocchi.

Per un primo approccio si può usare il seguente comando:

- *dd if=/dev/sdb of=/media/sdc1/disco.dd conv=noerror, sync bs=32K*

Questo leggerà blocchi di 32Kb da */dev/sdb* e li scriverà sul disco */media/sdc1* il file *disco.dd*.

L'opzione evidenziata di giallo invece permette sia di evitare sia che l'operazione si blocchi di fronte a un errore di lettura del blocco (noerror) saltando il blocco danneggiato, ma per non avere una dimensione della copia finale INFERIORE a quella originale il flag *sync* obbliga il comando dd a riempire di soli zero un blocco danneggiato per il quale la lettura risulta impossibile da effettuare. Il problema ora però risulta essere il fatto che la dimensione finale non è quella effettiva ma un multiplo del BS prescelto! Inoltre settori non danneggiati rischiano di essere azzerati se si trovano in blocchi con almeno un settore illeggibile (es. se su un blocco da 32Kb ci sono due settori danneggiati, cioè 512*2 bytes=1Kb illeggibili, i restanti 31Kb verranno azzerati e quindi persi!).

Impostare però a 512bytes (misura minima di un settore) il BS nel comando (1) risulterebbe troppo stressante per l'hard disk, perché ne imporrebbe una lettura settore per settore, operazione troppo lenta!

La soluzione risulta essere quella di usare dei tools alternativi e per l'analisi forense il migliore è **DC3DD** (basato su dd).

(2) dc3dd if=/dev/sdb of=/media/sdc1/disco.dd conv=noerror,sync bs=32k

iflag=direct

(3) dc3dd if=/dev/sdb of=/media/sdc1/disco.dd conv=noerror,sync bs=32k /dev/rdisk

Le due stringhe sono comandi che permettono di leggere dei blocchi di dimensioni maggiori di 512bytes (il default blocksize è di 32Kb) al fine di aumentare la performance, ma nel momento in sui si trova di fronte a un errore, essendo il paramentro *conv=sync,noerror* impostato, allora dc3dd rilegge il blocco dall'inizio, settore per settore, così da mantenere i settori non danneggiati e sostituire SOLO i settori illeggibili con una serie di 0s. Così facendo si avrà una lettura più veloce ma senza perdere i blocchi di dati che circondano un bad sector e mantenendo così anche la stessa dimensione del disco sorgente nel file immagine creato.

I parametri evidenziati in verde invece servono a bypassare la ***page cache***, luogo in cui viene mantenuta in RAM una copia dei dati, per poter accedere direttamente al disco, abilitando cioè il direct I/O mode, per poter considerare effettivamente la dimensione minima del settore. [(2) viene usata per Linux, mentre (3) per Mac OS X].

Per clonare un disco:

(4) dd if=/dev/hda of=/dev/sdb

mentre su (1) la destinazione era /media/sdb, usando /dev, dd copia il disposotivo fisico di origine su un altro dispositivo fisico, altrimenti sarebbe come copiarlo su una cartella, il che è impossibile.

Azzeramento dell'hard disk:

(5) dd if=/dev/zero of=/dev/hda

ANALISI FISICA

L'analisi fisica comporta il recupero dei dati non solo su tutto il sistema operativo, ma su tutto il drive fisico, quindi è un'analisi che non presuppone alcuna organizzazione logica.

I metodi applicabili sono tutti metodi di ricerca e estrazione, che hanno delle limitazioni perché non possono essere fatti sector by sector in quanto un'analisi di questo tipo impiegherebbe anni per essere conclusa!

I metodi applicabili sono tre:

- keyword searching,
- **file carving** (si basa sull'estrazione dei file da una base binaria utilizzando gli header e i footer noti),
- estrazione delle tabelle di ripartizione e dello spazio inutilizzato sul drive fisico.

CARVING

Carving manuale: per estrarre un file di cui sono noti sia l'header che il footer basta rintracciare il settore in cui è memorizzato l'header in questione e marcarlo e successivamente marcare la prima occorrenza del footer, infine basterà copiare l'intero blocco di dati compreso fra questi due settori marcati. Per esempio, per ricercare un file JPG con un editor esadecimale basta aprire il file che contiene le jpg e cercare l'header FFD8, marcare il blocco e cercare da dove siamo il primo footer FFD9, marcando di

nuovo il blocco si sarà ottenuto un intero insieme di dati che basterà copiare su un altro editor esadecimale.

Carving non manuali sono foremost e scalpel che estraggono tutti i file automaticamente.

Esempio:

foremost –t jpg –i /media/disco.dd –o /media/sda1/output

REPORTING

Tutta la procedura di analisi deve essere documentata con dei moduli standard o dei verbali che compongono una CHAIN OF CUSTODY (catena di custodia) grazie alla quale una prova sarà sempre e facilmente rintracciabile durante tutto il processo. Questa catena comprende tutti i momenti che vanno dall'individuazione del crimine commesso sino alla consegna dei risultati nell'aula del tribunale o nelle mani di chi di competenza (PM, avvocati …) che vanno descritti nei minimi particolari (spostamenti, custodi, manipolazioni della memoria principale …). Questo report finale dovrà però essere scritto in modo chiaro e comprensibile anche a un profano, quindi andrà evitato l'utilizzo esclusivo di un linguaggio informatico, accessibile solo agli esperti.

Il report dovrà contenere:

- premessa (con quesiti e descrizione dell'incarico)
- operazioni svolte
- risposta ai quesiti
- conclusioni

Le prove vanno inoltre registrate su supporti ottici/magnetici e inoltre devono essere codificate con hash MD5 e SHA1 e questi codici vanno memorizzati con un file che dovrà a sua volta essere criptato così da evitare alterazioni. A fine incarico inoltre i dati acquisiti vengono generalmente distrutti in modo sicuro tramite soprascrittura multipla.

Queste operazioni garantiscono l'INTEGRITA', la RISERVATEZZA e la DISPONIBILITA' dei dati trattati, anche in un eventuale ri-masterizzazione.