diritto&diritti dal 1996
diritto.it
fondatore Francesco Brugaletta

La disciplina della Computer Forensics

Autore: Guzzo Antonio
In: Diritto civile e commerciale

Per Computer Forensics si intende quella particolare disciplina concernente l'applicazione di tecniche scientifiche ed analitiche ai Sistemi Operativi ed ai filesystem al fine di recuperare prove utili e valide nell'attività processuale. Infatti quando riaccendiamo un pc significa che qualcosa all'interno dell'hard-disk viene modificato rispetto all'ultima accensione. Questa operazione rimane fondamentale per un accertamento giudiziario, e se io sequestro un pc e lo riaccendo sebbene le informazioni rimangono sul pc io non posso portarle come prova dibattimentale (cioè non posso utilizzarle nel processo). Anche il fatto di commettere delle piccole imprecisioni nell'estrazione dei dati, ciò è un motivo di invalidità della prova. La Computer Forensics nasce dal principio di scambio di Locare che si manifesta quando ogni scena del crimine lascia qualcosa sulla vittima e viceversa. (scena del crimine, vittima e sospetto). Questo principio è applicabile in ambito digitale. Attualmente la disciplina della Computer Forensics è in voga, in quanto i danni economici che essa genera sono determinanti ed hanno un impatto dirompente ed economico sui sistemi ICT (Information and Communication Technology). Infatti a tal proposito vengono usate delle tecniche di penetrazione informatica (il cosiddetto hacking). Il numero di attaccanti è notevolmente cresciuto e c'è la necessità di proteggerci dall'esterno. Noi ci occuperemo di tutto ciò che accade a valle del reato cioè a giochi fatti quando un sistema IT viene penetrato. Questo è un approccio di chiusura in quanto le aziende non vogliono fare sapere all'esterno se hanno avuto o meno degli attacchi informatici.. In questi casi il vero obiettivo di una azienda è quello di non commettere lo stesso errore due volte. I quattro passi della Computer Forensics sono i seguenti: 1) acquisizione, 2) identificazione, 3) valutazione e 4) presentazione. Supponiamo di arrivare in una scena criminosa ed analizziamo i quattro passi di cui prima. Per prima cosa dobbiamo acquisire tutte le fonti di prova che stanno sulla scena del crimine (sporgere subito denuncia e lasciare così le cose come sono (il c.d. freeze in inglese) poi successivamente si passerà all'acquisizione della prova o meglio della scena del crimine digitale. Tale processo consiste nel fare un copia esatta bit a bit della scena incriminata da un punto di vista digitale. In questi casi la polizia giudiziari andrà a refertare qualunque pc su questa rete aziendale. In pratica effettuerà il dump (cioè l'esportazione del database del pc) della memoria attualmente in uso all'interno del pc, ed infine acquisirà i meccanismi dei dispositivi di rete. Successivamente si passerà poi ad identificare qualsiasi cosa, cioè il processo deve essere scientifico e deve essere in grado di ricostruire perfettamente la scena del crimine. Si valuta, si analizza tutto questo materiale ed infine si arriva alla fase più complessa che è quella della presentazione perché bisogna far comprendere tutto ciò ad un magistrato che non ha tali competenze tecniche. Bisogna utilizzare degli strumenti di convincimento tali da essere efficaci nei confronti di un giudice. Chi ha bisogno della Computer Forensics? Essenzialmente i soggetti che ne hanno bisogno sono la vittima (ad es. il caso del bambino di Parma sequestrato al quale fu subito sequestrato il pc del papà che fu accusato di pedo-pornografia cosa rivelatasi successivamente non vera), le forze di polizia, le assicurazioni (le assicurazioni in questi casi hanno tutto l'interesse a non pagare) le aziende, il sistema

giudiziario (il reato informatico o computer crime è quello sancito dagli art. 615 del codice penale e seguenti, bisogna capire anche qual è la differenza tra reato informatico e un reato comune perpetrato tramite la rete come ad es. il phishing.). Le vittime dei reati informatici possono essere aziende, enti governativi ed individui. Quelli che sono gestibili male sono gli individui in quanto sono privi controllo da parte dell'incident response team (il pool di persone che analizza l'evento delittuoso). Facciamo un esempio. Siamo in una grande azienda dove esiste il dipartimento sicurezza informatica cha ha l'obiettivo conclamato di proteggere e rendere sicura la rete aziendale. Se uno sprovveduto accede alla rete e non esistono delle policy di tracciatura degli accessi questo diventa un a problema enorme. Supponiamo nel caso di colpa cioè di una persona che sia ignara del pericolo, come il caso di un individuo navighi su siti consentiti e magari quel sito sia stato attaccato da pirati informatici(il fenomeno si chiama cross sight scripting).Quello che bisogna fare è di organizzare dei documenti sulle politiche di sicurezza mentre per la Computer Forensics la strategia è quella di impiantare un'infrastruttura tecnologica che ricostruisca fedelmente il momento dell'incidente sino alla situazione precedente. Bisogna quindi skillare (trovare le giuste competenze in termini di risorse umane) adeguatamente il personale IT. Dal punto di vista tecnologico è importante costituire un infrastruttura ma non è sufficiente perché bisogna anche definire delle policy di sicurezza, Gli obiettivi della Computer Forensics sono quelli di identificare il colpevole, identificare il metodo,la vulnerabilità della rete che ha consentito al colpevole di guadagnare l'accesso al sistema, condurre un assessment del danno della rete colpita, conservare correttamente la prova per l'azione giudiziaria. Il futuro attualmente è sulla tecnologia mobile (cellulari) che come dice la terminologia è always on (cioè parla sempre). Ad oggi il mobile viene refertato in modalità attiva, cioè se sono accesi il che consente di lavorare sull'interno del mobile in termini di infrastruttura tecnologica. Se è spento, in realtà bisogna fare delle considerazioni procedurali cioè analizzare il cosiddetto incidente probatorio. In realtà oggi la soluzione adottata è quella di refertare il mobile ed è possibile farlo partendo dall'SD. I tipi di richiesta forense sono l'analisi delle intrusioni (intrusion detection system o IDS), l'assessment del danno, l'esame del sospetto, i tool analysis, l'analisi dei file di log e la ricerca della prova. Passiamo ora ad a esaminare la cosiddetta analisi delle intrusioni. Nello specifico individueremo chi si è introdotto, cosa ha fatto, quando è accaduto, dove è andato, perché ha scelto questa rete, come ha fatto. Nel caso dell'assessment del danno noi andiamo ad analizzare che cosa ha visto l'intrusore, cosa ha preso, che tracce ha lasciato e dove è andato. E' necessario utilizzare degli strumenti di logging ad esempio quelli presenti nei sistemi operativi linux. Facciamo un esempio e supponiamo di avere un server apache e che io riesca ad utilizzare una exploit che mi consente di aprire una finestra di shell che sia di root. In questo caso io modifico tre log di base di linux e posso tranquillamente cancellare queste tracce e passare inosservato. Esistono però delle tecniche che evitano queste operazioni di modifica.

Esaminiamo ora le caratteristiche della prova. La prova informatica deve essere come ogni altra prova ammissibile, autentica, accurata, completa e convincente per il giudice (nella pratica succede che lo strumento più utilizzato per effettuare operazioni di Computer Forensics è quello dell'encase cioè di un software americano proprietario che è nato da una società chiamata proprio Computer Forensics la quale sviluppò alle origini un software chiamato Dibs che successivamente evolvette in encase. Questa azienda ebbe il compito di sviluppare un software (encase) che è universalmente utilizzato ed ha una percentuale di fallimento pari al 10% (molto alta). Esistono anche dei software open source che sono gratuiti i quali

Diritto & Diritti ISSN 1127-8579

hanno il vantaggio rispetto ad encase di avere un proprio codice sorgente. La prova informatica deve essere convincente, avere un valore probatorio ed un test pratico di presentazione. Per completezza esistono anche degli strumenti software open source per il mobile come ad esempio il tool Tulp2g che nasce come progetto del ministero degli interni olandesi. Esaminiamo ora quelle che sono le procedure forensi che vengono utilizzate in fase dibattimentale:

1)

congelare la scena del crimine (dare un procedimento formale per estrarre imaging);

2)

Mantenere la continuità della prova (controlled copying, controlled print-out);

3)

Raccolta testimonianze;

4)

ACPO (Association of Chief Police Officers).

Tutte le analisi forensics che noi faremo saranno effettuate solo su una copia dell'hard-disk e cioè sulla sua immagine. Da questo momento in poi inizia la catena di custodia che sta alla base del procedimento di acquisizione della copia, cioè deve garantire che il reperto non sia stato manomesso. Una volta in possesso della copia originale del dispositivo, occorre documentare come si conserva. Bisogna sapere dove è memorizzata, chi ne ha avuto accesso e quale operazioni sono state effettuate su di essa. Questa è la catena di custodia, che fornisce la documentazione provante che l'integrità dei dati è stata preservata e non c'è stata alcuna modifica, seppur casuale. Tecnicamente la catena di custodia si ottiene con la

documentazione, con gli hashes (per hash si intende una funzione univoca operante in un solo senso ossia, che non può essere invertita, atta alla trasformazione di un testo di lunghezza arbitraria in una stringa di lunghezza fissa, relativamente limitata. Tale stringa rappresenta una sorta di "impronta digitale" del testo in chiaro, e viene detta valore di hash, checksum crittografico o message digest. In informatica, la funzione di trasformazione che genera l'hash opera sui bit di un file qualsiasi, restituendo una stringa di bit di lunghezza predefinita. Spesso il nome della funzione di hash include il numero di bit che questa genera: ad esempio, SHA-256 genera una stringa di 256 bit. Oggi le funzioni di hash vengono utilizzate dalla firma digitale che garantisce l'integrità, l'autenticità ed il non ripudio) e il timestamps (ricevuta temporale). I tipi di dispositivi che si utilizzano sono i cd, dvd, floppies, hard driver, flash ram (smart media, memory stick, mmc, secure digital), pda (palmari), cellulari.

Passiamo ora ad effettuare l'analisi del disco fisso di un pc. Per prima cosa iniziamo a lavorare sull'image o sulla copia sicura. Successivamente passiamo ad effettuare l'interpretazione del dato e poi la sua successiva valutazione. I dati possono essere estratti in forma binaria. Si passa poi a processare i dati per convertire la copia in forma comprensibile (reverse engineer per estrarre informazioni dalle partizioni dei dischi, dal file system, directory e file – esistono software per questi scopi). Infine si passa poi ad interpretare i dati mediante ricerca per parole chiave, frasi, etc. Ma quali problemi tuttavia si riscontrano? I problemi aperti sono quelli relativi all'uso di tool proprietari per forze di polizia, del disclosure del metodo, dell'open source, della parità di armi con la difesa. Esaminiamo ora il cosiddetto Network Monitoring, cioè il monitoraggio della rete che è consentito quando il sistema è compromesso e si sta effettuando un controllo al fine di localizzare ed identificare un intruso, ovverosia quando il monitoraggio è esplicitato e consentito dagli utenti (AUP) e dove le leggi lo consentono. Come abbiamo detto in precedenza la prova informatica è modificabile in quanto un intruso potrebbe aggiungere,rimuovere,modificare il contenuto dei log oppure potrebbe compromettere i componenti del sistema che ospita i log ed infine potrebbe modificare qualcosa durante l'investigazione. E' possibile effettuare il recupero di file cancellati, di file nascosti, di slack space, di bad blocks. Si analizzano alcune tecniche di cifratura per l'analisi di
file cifrati e di partizioni nascoste.

Passiamo ora identificare la prova informatica. La prova si identifica essenzialmente nell'hard disk che si esplicita nella forma di swap files, temporary files, spazio del disco non allocato, spazio del file slack. La prova si identifica anche nella memoria e nei processi accesi nel sistema operativo, nei floppy disk, cd roms, dvd zip e dischi jaz, nastri di back-u p, file di log, schede RAID e back-up. Ad esempio esiste un software chiamato snort che fa intrusion detection (è uno strumento di intrusion detection cioè di controllo di eventuali accessi non autorizzati). Passiamo ora ad esaminare l'analisi dei file di log mediante l'utilizzo di trip-wire che è un software di tipo host intrusion detection system cioè si basa su un database come my sql dove inserisce tutti i digest cioè le impronte dei file di sistema di default. Un altro strumento da cui bisogna difendersi è il rootkit che è un programma silente che si installa nel sistema operativo ed ha l'obiettivo di sostituirsi a dei programmi/processi fondamentali per l'uso del sistema operativo. Il rootkit ha come obiettivo quello di effettuare un accesso da remoto su un determinato host e qui entra in gioco tripwire che tiene traccia di tutti questi accessi. Nell'analisi dei file di log vengono esaminati degli

eventi ed il loro monitoraggio, nello specifico vengono esaminati quali sono i record degli eventi, i file di log di firewall/IDS/Router/server. Si utilizzano in questi casi dei software come Tripwire database. Infine si fa una analisi di alcuni strumenti che si utilizzano per identificare una prova quali il modem, l'utilizzo ftp, gli accessi in modalità telnet e gli accessi RAS. Nella prossima lezione infine esamineremo un paio di casi di azione investigativa informatica mediante tecniche di computer forensics. L'esempio che verrà fatto sarà di phishing (In ambito informatico il **phishing** ("**abboccaggio**", in italiano) è una attività truffaldina che sfrutta una tecnica di ingegneria sociale, ed è utilizzata per ottenere l'accesso a informazioni personali o riservate con la finalità del furto di identità mediante l'utilizzo delle comunicazioni elettroniche, soprattutto messaggi di posta elettronica fasulli o messaggi istantanei, ma anche contatti telefonici. Grazie a questi messaggi, l'utente è ingannato e portato a rivelare dati personali, come numero di conto corrente, numero di carta di credito, codici di identificazione, ecc. Il termine phishing è una variante di fishing (letteralmente "pescare" in lingua inglese),e allude all'uso di tecniche sempre più sofisticate per "pescare" dati finanziari e password di un utente.)e di spamming (Il principale scopo dello spamming è la pubblicità, il cui oggetto può andare dalle più comuni offerte commerciali a proposte di vendita di materiale pornografico o illegale, come software pirata e farmaci senza prescrizione medica, da discutibili progetti finanziari a veri e propri tentativi di truffa. Uno **spammer**, cioè l'individuo autore dei messaggi spam, invia messaggi identici (o con qualche personalizzazione) a migliaia di indirizzi e-mail. Questi indirizzi sono spesso raccolti in maniera automatica dalla rete mediante spambot ed appositi programmi, ottenuti da database o semplicemente indovinati usando liste di nomi comuni. Per definizione lo spam viene inviato senza il permesso del destinatario ed è un comportamento ampiamente considerato inaccettabile dagli Internet Service Provider (ISP) e dalla maggior parte degli utenti di Internet. Mentre questi ultimi trovano lo spam fastidioso e con contenuti spesso offensivi, gli ISP vi si oppongono anche per i costi del traffico generato dall'invio indiscriminato. Un gran numero di spammer utilizza intenzionalmente la frode per inviare i messaggi, come l'uso di informazioni personali false (come nomi, indirizzi, numeri di telefono) per stabilire account disponibili presso vari ISP. Per fare questo vengono usate informazioni anagrafiche false o rubate, in modo da ridurre ulteriormente i loro costi. Questo permette di muoversi velocemente da un account a un altro appena questo viene scoperto e disattivato dall'ISP. Gli spammer usano software creato per osservare connessioni Internet con scarsa sicurezza, che possono essere facilmente dirottate in modo da immettere i messaggi di spam direttamente nella connessione dell'obiettivo con il proprio ISP. Questo rende più difficile identificare la posizione dello spammer e l'ISP della vittima è spesso soggetto di aspre reazioni e rappresaglie da parte di attivisti che tentano di fermare lo spammer. Entrambe queste forme di spamming "nascosto" sono illegali, tuttavia sono raramente perseguiti per l'impiego di queste tattiche. I mittenti di e-mail pubblicitarie affermano che ciò che fanno non è spamming. Quale tipo di attività costituisca spamming è materia di dibattiti, e le definizioni divergono in base allo scopo per il quale è definito, oltre che dalle diverse legislazioni. Lo spamming è considerato un reato in vari paesi e in Italia l'invio di messaggi non sollecitati è soggetto a sanzioni..

(a cura del Dottor Antonio Guzzo Responsabile CED del Comune di Praia a Mare).

Diritto & Diritti ISSN 1127-8579

https://www.diritto.it/la-disciplina-della-computer-forensics/

Diritto & Diritti ISSN 1127-8579