

# Diario di un computer forenser

## Contrabbando, cui prodest?

### Alzataccia

Sono su una spiaggia assolata, all'ombra di una palma da cocco che si allunga sulla sabbia (odio il sole), di lato a me mia moglie si cuoce al sole con quel bikini ridottissimo che poco spazio lascia all'immaginazione e molto alla contemplazione. Sorseggio un bibita e... suona la sveglia. Le 3 e 50. Insisto, c'è qualcosa di sottilmente perverso nello svegliarsi all'ora in cui, solitamente, si va dormire.

Cerco di connettere, indosso qualcosa e mi trascino in cucina per il primo caffè della solita, innumerevole fila che sorseggerò durante la giornata. Una luce filtra dalla finestra. Oh, ma insomma, sono già di sotto che mi aspettano, il lampeggiante blu che lancia bagliori sinistri a intervalli regolari. Chissà che cosa penseranno i vicini. Sono tre anni che abito qui e non conosco i nomi di nessuno di essi. Le varie forze dell'ordine sotto casa a orari impossibili e il postino che mi guarda male quando mi consegna l'ennesimo atto giudiziario in quella busta verde che tutti vogliono toccare il meno possibile.

Scendo, saluto i ragazzi della finanza chiedendomi come fanno a essere così freschi a quest'ora impossibile. Carico tutta la mia robbaccia nel baule della 156 e mi sistemo dietro (la prossima volta mi faccio anche ammanettare, così i vicini parleranno per mesi). Si parte veloci in autostrada. Dormo, con loro lo si può fare, non sono dei folli nella guida come quelli dei reparti ROS dei Carabinieri (però viaggiare con questi ultimi a 250 km/h ha un certo fascino).

### Il quesito

Quando comincia ad albeggiare siamo prossimi al posto dove dobbiamo arrivare. Il Pubblico Ministero mi ha chiesto di coadiuvare la Guardia di Finanza nel trovare delle prove per una compravendita di materiale di contrabbando. Durante la perquisizione nella casa di uno degli indagati è stato trovato un portatile su cui c'erano delle mail decisamente compromettenti. Arrivavano tutte dal server di questa ditta piantata in mezzo a questa nebbiosa pianura.

Negli scorsi giorni ci ho perso un po' di tempo. Il server di mail non è altro che una macchina in hosting presso un provider della provincia. Un giretto con `nmap` mi ha permesso di vedere che è una workstation Linux con attivi solo i servizi di SMTP (con postfix) e un pop3 server (`pop3d`, un classico). Non merita attenzione: al 90% è solamente un posto di transito. Ci farò un saltino finito il lavoro, giusto per precauzione.

## Si comincia

Aprono i cancelli ed entriamo. Me ne sto in disparte, lascio fare alle Fiamme Gialle il loro lavoro, che svolgono in maniera efficiente. La scena è sempre la stessa, entrano dall'entrata principale e dal magazzino contemporaneamente, prendono il primo che capita a tiro e gli notificano l'atto firmato dal PM. Anche le reazioni di sgomento/panico/incredulità dall'altra parte sono un classico. Io mi defilo e cerco la sala macchine. In una ditta di questo genere di solito è uno sgabuzzino delle scope con qualche macchina, uno switch e un condizionatore. Lascio accesi i server ma provvedo a spegnere gli switch e a isolare i router dalla rete, giusto per ulteriore precauzione. Ci sono delle linee ISDN che si infilano direttamente nel cablaggio strutturato. Via anche quelle che non si sa mai, ovviamente previa foto del tutto ed etichettatura dei cavi per rimettere poi le cose com'erano prima del mio arrivo. Chiedo al maresciallo di impedire a chiunque di toccare un computer.

Parto dal server. Se sono fortunato magari quello esterno è un semplice relay e la posta aziendale è tutta qui. Il problema è, come sempre, fare tutto senza modificare alcunché. Il server è un Dell piuttosto recente e ben carrozzato. Bene, con i server Dell non ho mai avuto incompatibilità con Linux.

Inizialmente accendo il monitor e il salvaschermo di Windows 2000 Server mi guarda sornione. La frase ribelle "Burn all the flags" acquista un significato tutto nuovo... Beh, mi faciliterà il compito.

Il disco al momento è paciosamente in stand-by. Strappo il cavo di alimentazione. Lo so, non è uno shutdown regolare ma è il modo migliore di preservare lo *status quo*. Riaccendo la macchina, entro nel BIOS e annoto data e ora e lo scostamento dalla mia sveglia, uno di quei modelli della Oregon Scientific che prendono l'ora dall'orologio atomico di Francoforte. Modifico i valori per il boot così che il server parta solo da CD-ROM. Mi appunto le modifiche sul registratore vocale (mi sembra sempre di essere Dana Scully durante un'autopsia).

Prendo la Knoppix 3.7, la infilo nel drive e parto. Utilizzo spesso la distribuzione standard per questi compiti, anche se non disdegno la sua variante Helix. Utilizzata anche dal SANS per i suoi corsi di Computer Forensics, usa dei parametri più restrittivi al boot loader (per evitare modifiche sia dei dati sia dei metadati), un supporto hardware più ampio della Knoppix standard (comprese molte periferiche RAID e SATA) e un desktop (Xfce) decisamente più leggero, utile con macchine non particolarmente dotate di RAM. Al boot modifico la lingua della tastiera e presto attenzione a specificare il parametro `noswap` così da evitare che il sistema modifichi anche un solo byte del disco. Evito inoltre il ricorso all'interfaccia grafica, specificando di fermarsi al runlevel 2. Due console testuali sono tutto quello che mi serve.

Esamino i programmi contenuti all'interno della macchina. Sono indeciso se esultare oppure piombare nello sconforto più profondo. La buona notizia è che c'è installato un

server di posta elettronica, la pessima è che lo stesso è Microsoft Exchange 2000. Questo significa dover passare un po' di tempo in laboratorio litigando con Active Directory e affini, oltre, ovviamente, con il DB di Exchange, noto per non essere avvezzo a smantamenti non previsti.

Esamino la configurazione hardware. Il server ha un RAID 5 e il controller è integrato in piastra. Non ho un controller simile sul mio server, quindi acquisirò i dati via rete. È un metodo più lento dello smontare i dischi ma almeno eviterò di riempirmi, come al solito, di polvere. Inoltre così potrò acquisire il drive logico nella sua interezza invece dei singoli tre dischi e poi impazzire una settimana in laboratorio cercando di capire come quel diavolo di un controller abbia sparso i dati sui singoli hard disk.

I ferri del mestiere sono tutti Open Source. Continuo a chiedermi chi sia così pazzo da comprarsi uno dei quei duplicatori hardware da migliaia di dollari. `dd` e `netcat` mi permettono di ottenere una copia bit a bit perfettamente identica all'originale senza patemi. Lancio `netcat` in listen mode sul mio server e poi `dd` in pipe con `netcat` sulla macchina da acquisire. Sulla macchina di acquisizione ho montato tre schede di rete Gigabit su PCI-X, così da poter acquisire contemporaneamente più computer a una velocità umana. Ora c'è solo da attendere che abbia finito. Chiudo a chiave la stanza e do le chiavi a uno dei finanziari pregandolo di controllare che nessuno tenti di ficcare il naso.

Faccio il giro dei client, non prima di aver preso il terzo o quarto caffè. O era il quinto? La procedura è simile, boot con una Knoppix e montaggio del file system in read only. Benissimo, l'unico programma di posta installato è Outlook ovunque e i file PST sono vuoti. Ergo la posta rimane sul server e il client si occupa solamente della visualizzazione. Unica eccezione: i due portatili del presidente e dell'amministratore delegato. Foto con la digitale e poi li rimuovo per portarmeli in sala macchine.

Di sotto mi aspetta un tipo alto e allampanato sulla quarantina con un completo gessato. Dato che non è il becchino, l'unica altra alternativa è che si tratti dell'avvocato di fiducia. È un incrocio tra Learch e Snoopy con il papillon e la borsa di cuoio (come lo disegnava Schulz per fargli fare la parte del principe del foro). Mi chiede spiegazioni lanciandosi in una prolissa arringa sul fatto che non posso sequestrare le macchine della ditta dato che causerebbe loro "un ingente danno economico". Giusto per chiarire subito le cose gli sventolo sotto il naso la nomina del PM, e poi gli spiego il concetto di copia "bit a bit" abbinato a quello di algoritmo di hash. Farò una copia integrale di tutti i dischi fissi che contengono materiale rilevante ai fini d'indagine. Tutte le copie saranno verificate sia con MD5 sia con SHA1. Ogni cosa sarà annotata sul verbale di acquisizione. I supporti su cui saranno salvate le indagini saranno a disposizione in Procura e io lavorerò su un'ulteriore copia. La sua espressione alla fine mi lascia il dubbio che non abbia capito proprio ogni dettaglio...

Torno al mio server. La copia è finita. Do un `Crtl+C` (il programma non esce da solo) sul client, do un "sync" sulla macchina di acquisizione e lancio `sha1` e `md5` per la verifica. Ho imparato a mie spese che se non seguo questa esatta sequenza la verifica fallirà miseramente. Il numero delle macchine da acquisire è limitato, perciò posso permettermi una verifica con tutti e due gli algoritmi di hash. Intanto scrivo il verbale e metto i portatili in copia con la stessa trafila. O lavori in multitasking oppure rischi di invecchiare aspettando.

Dopo qualche ora tutto è finito. Consegno i verbali, spiego le ultime cosettine all'avvocato, poi ricollego switch e router. Si prendano pure loro la responsabilità di riaccendersi le macchine. Anche le Fiamme Gialle hanno finito la loro parte. Come sempre, prima di me. Prendo un caffè prima di andarmene.

Tappa dal provider, per confermare la mia tesi del relay. C'è un po' di posta in attesa di essere prelevata, per cui riscarico tutta l'attrezzatura e procedo alla copia. Altro verbale, altra trafila, altro caffè.

Arrivo a casa dopo cena. Mia moglie dorme sul divano. Devo proprio portarla su quella spiaggia e regalarle quel bikini...

## Lo scienziato pazzo nel suo anatro

Il giorno dopo mi aspetta il laboratorio e i 500 GB recuperati. La prima volta che ho dovuto recuperare della posta da un backup di un server Exchange avrei voluto uccidere qualcuno, solamente per sfogare la frustrazione accumulata. Avevo già individuato la vittima designata, quello che ha scritto quel maledetto modulo di System Attendant, che ha la fragilità di un cristallo di Boemia.

Pare infatti che i backup di Exchange siano stati fatti apposta per essere recuperati sulla *stessa* macchina su cui sono stati fatti. Nessuno ha pensato che questa potrebbe rompersi catastroficamente. Exchange pretende infatti che la macchina su cui si recuperano i dati abbia:

1. lo stesso nome;
2. lo stesso dominio;
3. la stessa versione di sistema operativo;
4. la stessa *identica* versione di Exchange, né minore né maggiore

Anche se queste condizioni sono rispettate, va comunque eseguita una complessa quanto fragile sequenza di operazioni (disponibili sulla Knowledge base di Microsoft) per riuscire a recuperare le mailbox.

Stavolta ho le immagini dei dischi del server (in due copie, per sicurezza), Vmware GSX e un po' di esperienza. Creo quindi un disco virtuale con una copia dell'immagine acquisita ed effettuo il boot di una macchina virtuale con il sistema operativo originale. Resetto la password di Administrator e quelle di tutti gli utenti. Dopodiché configuro un client, sempre virtuale, di Outlook per estrarre (con un paio di programmi di supporto per automatizzare il salvataggio di mail e attachment) il contenuto delle mailbox dei singoli utenti. Tutto questo mi occupa un paio di giorni di elaborazione e solo una decina di imprecazioni. Continuo a ringraziare il giorno in cui ho deciso di comprare una macchina con due Opteron.

Ovviamente questo procedimento, se effettuato sull'originale, avrebbe alterato le informazioni in esso contenute. Ma ho lavorato su una copia della copia e documentato ogni singolo passo su un apposito verbale. Ergo l'operazione è ripetibile dalla controparte partendo dalla copia depositata in Procura subito dopo l'acquisizione.

Alla fine la posta è su un supporto inalterabile in un formato decisamente più umano, sia dal punto di vista della possibilità di visualizzarlo sia per il fatto che mbox è decisamente più standard di quell'accrocchio di database di Exchange. Aggiungo la posta contenuta nei portatili, augurando come sempre un'orchite a chi ha scritto le specifiche dei file PST. Relazione, firme, scartoffie, e consegno tutto agli inquirenti. Il mese dopo un articolo sul giornale mi conferma che non ho fatto tutto per niente. Interessante quel trafiletto che dice "...determinanti le prove acquisite dai sistemi informatici...".