nome deve essere diverso per ogni nuovo progetto che sviluppiamo, e questo utente deve servire solo per fare questo. Tutto ciò perché i software hanno la tendenza a scrivere il nome dell'utente attivo dentro i metadati dei file che salvano, ed è meglio evitare certi recuperi inopportuni.

La ricetta "Ripristinare lo stato di una macchina virtuale a partire da un'istantanea" spiega i dettagli tecnici del primo punto. Per ciò che riguarda la creazione di un nuovo utente sulla versione di Windows che utilizziamo, crediamo di nuovo che chi ci legge sia in grado di trovare il modo di farlo attraverso il Pannello delle configurazioni.

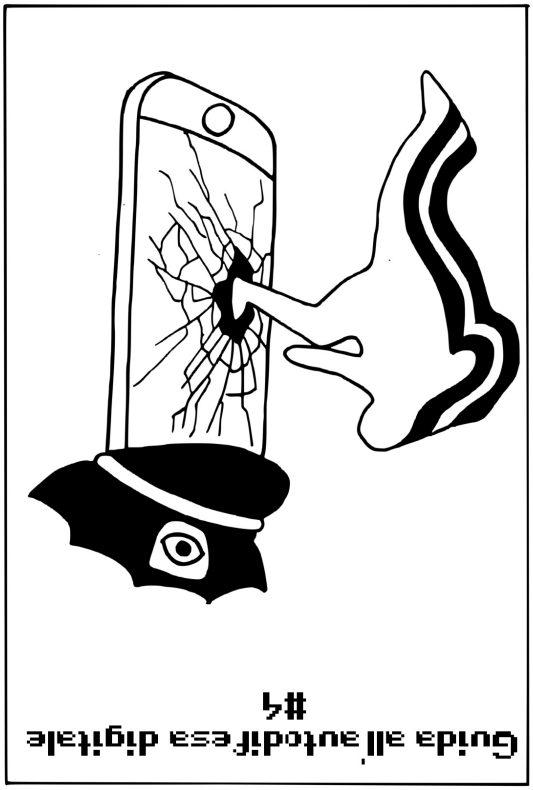
Ora che abbiamo un compartimento stagno, vediamo come aprire selettivamente delle porte, a seconda dei bisogni.

Come inviare dei documenti a un Windows imprigionato?

Dato che il Windows ospitato non ha il diritto di uscire dalla propria scatola per andare a cercarsi da solo dei file, potrebbe essere necessario fargli arrivare "dall'esterno", per esempio:

- la materia prima (bozze, immagini o testi provenienti da altre fonti);
- un software necessario al nuovo progetto, e non presente nella immagine virtuale che abbiamo scongelato.

Abbiamo già visto come procedere, ma qui ci troviamo in un caso molto particolare: l'installazione di nuovo software dentro il Windows "pulito". Condividere dei file con un Windows "sporcato" richiede per prima cosa di riflettere e prendere precauzioni, cosa che andiamo adesso a studiare.



Quello che avete tra le mani è il quinto numero della traduzione a puntate della Guide d'autodéfence numerique.
L'edizione originale integrale (in francese) è leggibile online e scaricabile liberamente qui:
http://guide.boum.org
Trovate invece le puntate precedenti della traduzione in italiano qui:
http://numerique.noblogs.org

SOMMARIO

Illustrazioni di Pinza666

Oltretutto, così facendo, le persone possono accedere agli archivi di un progetto, ma anche a quelli degli altri, il che non è molto consigliabile.

Poi, se la password è un segreto diviso, è meglio facilitare l'accesso alle persone che condividono il segreto avendo un supporto che possano trasmettersi.

Nel prossimo numero:
Le ricette: usare il terminale, scegliere una password...

Il modo di farlo è leggermente diverso, a seconda del supporto sul quale si trovano in origine i file da importare (CD, DVD, penna USB, documento presente sull'hard disk di un sistema cifrato), ma le precauzioni da usare sono le stesse:

Windows deve avere accesso soltanto ai file che vogliamo importare, solo a questo. Non dobbiamo dargli accesso a una cartella che contiene alla rinfusa vari file che riguardano vari progetti che non devono invece essere collegati tra loro. Se questo comporta il dover prima smistare e riordinare, eh oh, sarà così.

Se Windows ha bisogno di leggere (copiare) i file contenuti in una cartella, gli dobbiamo dare accesso soltanto a quella cartella. Meno permessi daremo a Windows di scrivere qui e là e meno tracce fastidiose lascerà in giro.

Per evitare di mischiare le cose, vi raccomandiamo di:

salviamo il suo stato da una parte. In seguito questa istantanea ci servirà come base di partenza per ogni altro nuovo progetto.
La ricetta "Fare un'istantanea di una macchina virtuale" spiega come effettuare questa operazione.

Nuovo progetto, nuova partenza

Mettiamo che un altro nuovo progetto necessiti dall'inizio dell'uso di Windows. Ecco come proseguire:

1. Ripristiniamo l'istantanea della macchina virtuale che contiene l'installazione del Windows "pulito";
2. Facciamo partire la macchina virtuale nel suo compartimento stagno; ci servirà esclusivamente per il nuovo progetto, e da quel momento diventerà una macchina virtuale "sporcata";
3. Dentro a questa nuova macchina virtuale sporca, viene creato un nuovo utente Windows; il

riunire più persone per poter accedere all'archivio. Bisogna però ponderare la cosa: questo metodo implica complicare l'accesso agli indesiderati, ma anche ai desiderati.

Un hard disk? Una penna? Varie penne?

A seconda delle scelte fatte precedentemente riguardo alla password, dobbiamo ora decidere quale supporto utilizzare. Tenendo conto che sul piano tecnico, la cosa più semplice al momento è quella di avere una sola password per ciascun supporto.

Un hard disk esterno può contenere più dati di una penna USB, e a volte si rende quindi necessario: per archiviare un progetto video, per esempio.
Archiviare vari progetti sullo stesso supporto permette di semplificare la cosa, ma diventa in questo modo difficile separare i progetti in base ai livelli di riservatezza che necessitano.

ESEMPIO 2 - LAVORARE SU UN DOCUMENTO SENSIBILE

1. Contesto
2. Valutazione dei rischi
3. Possibili attacchi e soluzioni praticabili

CONTESTO

Dopo la nuova partenza, il computer usato per portare avanti un progetto è stato dotato di un sistema cifrato. Bene. Mettiamo il caso allora di dover lavorare a un progetto particolare, più "sensibile", per esempio:

- scrivere un volantino;
- disegnare un manifesto;
- impaginare un libro e poi esportarlo in pdf;
- organizzare una fuga di informazioni per divulgare le meschine pratiche di un datore di lavoro;
- montare un video e metterlo su un DVD.

- creare una cartella di importazione per ciascun progetto;
- chiamare questa cartella nel modo più esplicito possibile, es. "cartella dove Windows puo' leggere";
- non condividere mai nessun'altra cartella con il Windows ospitato.

La ricetta "inviare file a un sistema virtualizzato" spiega come procedere in pratica.

Come far uscire dei file da un Windows imprigionato?

Il Windows ospitato di default non ha il permesso di lasciare tracce al di fuori del suo compartimento stagno. Ma è abbastanza inevitabile che arrivi il momento in cui sia necessario farne uscire dei file. Questi casi devono essere autorizzati esplicitamente, per esempio:

Per quanto riguarda poi l'installazione dei software all'interno di Windows: tutte le persone sufficientemente affezionate a Windows da leggere queste pagine, sono senza dubbio più competenti in materia di noi che stiamo scrivendo queste righe.

Attenzione: una volta effettuato questo passo, è imperativo non fare nient'altro all'interno di questo Windows virtualizzato.

Note:
1) Per esempio, se fosse necessario nascondere il fatto che abbiamo creato dei video, l'avere dei software di montaggio video potrebbe essere compromettente, e sarebbe più difficile da negare.

Catturare un'istantanea del Windows "pulito"

Adesso facciamo un'istantanea della macchina virtuale che abbiamo appena preparato. Ovvero,

In ciascuno di questi casi, i problemi da risolvere sono pressappoco gli stessi.

Siccome sarebbe troppo faticoso aumentare globalmente, di nuovo, il livello di sicurezza del computer, decidiamo che questo progetto in particolare deve beneficiare di un trattamento di favore.

GLOSSARIO

Nelle prossime pagine chiameremo:

- i documenti di lavoro: l'insieme dei file necessari alla realizzazione del progetto (immagini o bozze utilizzate come basi, i documenti salvati dal programma che utilizziamo, etc.);
- il progetto: il risultato finale (volantino, manifesto etc.)

La password del nostro sistema quotidiano, nel caso in cui sia cifrato (vedi ricetta “installare un sistema cifrato”), è una password che usiamo regolarmente, e quindi ha tutte le possibilità di venire ricordata.

Il rovescio della medaglia:
- se siamo costretti a rivelare la password del sistema, abbiamo rivelato anche quella dell’archivio;
- non bisogna avere una così grande fiducia nei computer attraverso i quali accederemo all’archivio. Potremmo farci beccare a nostra insaputa la password, che poi potrebbe venire usata in seguito non solo per leggere le informazioni archiviate, ma a quel punto anche tutti i dati contenuti nel computer.

Dividere il segreto con altri

Possiamo dividere il segreto con altri (vedi ricetta “dividere un segreto”). In questo modo bisogna

- per portare il file in copisteria, o dal tipografo, esportando un PDF;
- per proiettare, sotto forma di DVD, il film che abbiamo realizzato.

Per fare questa cosa, dobbiamo esportare i file dentro a una cartella vuota, dedicata a questo uso, e salvata dentro a un volume cifrato che può essere:
- una penna USB cifrata, che poi attiviamo sotto Debian scrivendo la password;
- l'hard disk cifrato di Debian che ospita anche la macchina virtuale.

Questa cartella dedicata verrà condivisa con il Windows ospitato. Insistiamo sulle parole "vuota" e "dedicata": Windows potrà leggere e modificare tutto ciò che questa cartella contiene, e non sarebbe bello permettergli di leggere altri file quando c'è bisogno di esportarne solo uno.
Se abbiamo bisogno di masterizzare un DVD, potremmo poi farlo girare su Debian.

file di installazione dei software che ci servono.

Un'operazione come questa sarà anche utile, in seguito, per inviargli qualsiasi file, e riaverli indietro. Per il momento, visto che stiamo preparando un'immagine di Windows "pulita", che ci servirà come base per qualsiasi nuovo progetto, non mischiamo tutto e accontentiamoci di mandargli soltanto ciò che gli serve per l'installazione dei software non compromettenti che abbiamo scelto.

Sul sistema ospitante, creiamo una cartella chiamata Windows, e copiamoci solo i file necessari all'installazione dei software che vogliamo

Poi condividiamo questa cartella con il Windows ospitato: la ricetta "condividere una cartella con un sistema virtuale" spiega come procedere praticamente.

sarà necessario scegliere una password (vedi ricetta relativa). Ora, visto che la destinazione è l'archiviazione, questa password non verrà utilizzata frequentemente. E una password utilizzata di rado ha tutte le possibilità del mondo di essere dimenticata.. rendendo in pratica impossibile l'accesso ai dati.

Riguardo a questo problema, possiamo studiare qualche strada.

Scrivere la password da qualche parte

Tutta la difficoltà consiste nel sapere dove scriverla, mettere questo documento in un posto dove poi lo si può trovare… senza d'altra parte far sì che altri possano ritrovarlo e capire che si tratta di una password.

Utilizzare la stessa password del nostro sistema quotidiano

VALUTAZIONE DEI RISCHI

Partendo da questo contesto, cerchiamo adesso di definire i rischi ai quali veniamo esposti.

Cosa vogliamo proteggere?

Applichiamo al caso presente le categorie definite quando abbiamo parlato della valutazione dei rischi:

- riservatezza: evitare che un occhio indiscreto arrivi troppo facilmente al progetto e/o ai documenti di lavoro;
- integrità: evitare che questi documenti vengano modificati a nostra insaputa;
- accessibilità: fare in modo che questi documenti restino accessibili quando ne abbiamo bisogno.

In questo caso accessibilità e riservatezza sono prioritarie.
Accessibilità, perché l'obiettivo principale è prima

Per evitare di mischiare (di nuovo) le cose e per limitare il contagio, vi raccomandiamo di:

- creare una cartella di esportazione del progetto;
- chiamare questa cartella nel modo più esplicito possibile, es. "cartella dove Windows può scrivere";
- non condividere mai nessun'altra cartella con il Windows ospitato, tranne che l'altra cartella delle importazioni di cui abbiamo parlato prima.

Le ricette "condividere una cartella con un sistema virtuale" e "cifrare una penna USB" spiegano come procedere in pratica.

Quando il progetto è finito

Una volta terminato il progetto, bisogna fare le pulizie, ma prima di tutto:

- esportiamo l'opera che ne è derivata su un supporto appropriato (carta, VHS, quel che

Windows dentro a un gestore di macchine virtuali tagliandogli, dall'inizio, tutti gli accessi alla rete.

A partire da questo momento, Windows sarà un sistema ospitato da una versione cifrata di Debian.

Installare i software necessari al Windows "pulito"

Installare per prima cosa tutto il software non compromettente (1) che ci servirà a realizzare i nostri progetti: questo eviterà di doverlo rifare ogni volta quando si inizia un nuovo progetto.. e eviterà, lo sottolineiamo bene, di utilizzare un'immagine di Windows "sporcata" per un nuovo progetto, una volta che magari siamo di fretta.

Visto che il Windows ospitato non ha il diritto di uscire dalla sua scatola per andare a cercarsi da solo i file, occorre fargli arrivare "dall'esterno" i

di tutto quello di realizzare il progetto.
Per quanto riguarda invece la riservatezza, dipende tutto da quanto il progetto vuole essere pubblico. Approfondiamo quindi la questione.

Opera a diffusione ristretta
Se il contenuto del progetto non è completamente pubblico, ovvero perfettamente segreto, si tratta di nascondere sia il progetto che i documenti di lavoro.

Opera a diffusione pubblica
Se il progetto vuole essere pubblico, la questione della riservatezza si restringe a quella dell'anonimato.

Sono allora principalmente i documenti di lavoro che devono passare sotto silenzio: in effetti, trovarli all'interno di un computer potrebbe far dedurre che il suo proprietario abbia realizzato il progetto.. con tutte le conseguenze spiacevoli che questo potrebbe comportare.

POSSIBILI ATTACCHI E SOLUZIONI PRATICABILI

Il metodo più semplice al momento è:
creare una penna USB o un hard disk cifrato; (vedi ricetta relativa) copiare i file da archiviare dentro questa periferica; eliminare e cancellare “davvero” il contenuto dei file di lavoro. (vedi ricetta per cancellare “davvero” i file)

Una volta effettuate queste operazioni, la penna o l’hard disk potranno essere riposti altrove rispetto al luogo dove utilizziamo normalmente il computer.
Si potrebbe anche studiare l’uso del CD o del DVD, per il loro basso costo, ma al momento è più complesso cifrare correttamente dei dati su questi supporti piuttosto che su delle chiavi USB, che sono ormai moneta corrente e facili da procurarsi.

Quale password?
Dato che i file saranno salvati sotto forma cifrata,

L’idea è insomma quella di far funzionare Windows all’interno di un compartimento stagno, dentro a un sistema Debian cifrato come quelli che abbiamo imparato a usare nell’esempio precedente. Ciò che farà da hard disk per Windows, sarà un grosso file salvato sull’hard disk del nostro sistema Debian cifrato.

Installare il gestore di macchine virtuali

La ricetta "installare il gestore di macchine virtuali" vi spiega come installare il software di gestione per virtual machine, che ci servirà a lanciare Windows dentro a un compartimento stagno.

Installare una versione "pulita" di Windows dentro il gestore di macchine virtuali.

Prepariamo un'immagine del nostro disco virtuale: la ricetta "installare una versione di Windows virtualizzata" spiega come installare

sia…), aiutandosi con quello che abbiamo detto precedentemente per spiegare come far uscire dei file dal Windows ospitato;
- i file di lavoro, se necessario, potrebbero dover essere archiviati (guarda caso il prossimo esempio riguarda proprio questo).

A questo punto viene il momento delle grandi pulizie, che elimineranno dal sistema ospitante la maggior parte possibile delle tracce lasciate dal progetto:
- ripristiniamo l'immagine del disco al suo stato "pulito" con l'aiuto della ricetta "Ripristinare lo stato di una macchina virtuale a partire da un'istantanea";
- dopo aver verificato un'ultima volta che tutto ciò che deve essere conservato sia stato archiviato bene altrove, cancelliamo "davvero" i file condivisi con Windows;
- cancelliamo "davvero" le tracce lasciate sull'hard disk;
(cfr. ricetta per cancellare "davvero" i file)

informazioni che vogliamo proteggere.
Aggiungiamo a questi rischi la possibilità che il libro o il film prodotto non piaccia a qualche commissario, ministro, CEO, o simili. Può succedere. Poniamo che:
questa autorità abbia avuto degli indizi che gli permettano di supporre chi sia l'autore del capolavoro; questa autorità sia in grado di disporre di una temibile squadra di uomini dotati di armi e uniformi, di poter agire la mattina presto e di sapere il domicilio delle persone sospettate.

Una tale inopportuna intrusione porterà, come minimo, in modo evidentemente anche fastidioso, al sequestro di tutto il materiale informatico che verrà trovato. Questo materiale verrà consegnato dagli intrusi nelle mani di qualcun'altro di fiducia che metterà in pratica una specie di autopsia volta a riesumare i dati presenti.. o che erano presenti in passato.

Ma non è tutto: se il progetto, o le sue versioni intermedie, sono salvate su questo computer (in un pdf etc) la loro data di creazione è probabilmente registrata nel file system e nei metadati. Il fatto che questa data sia anteriore alla pubblicazione del progetto può facilmente portare degli avversari a trarre delle scomode conclusioni circa la sua generazione.

Da chi vogliamo proteggerci?

Per farla semplice, riprendiamo le possibilità descritte nell'esempio che abbiamo fatto in precedenza sulla nuova partenza: il computer utilizzato per realizzare il progetto potrebbe venire rubato, più o meno casualmente, sia da degli sbirri che da dei ladri che lavorano per conto proprio.

Terzo passo: attacchi possibili e contromisure

L'ipotesi che abbiamo descritto finora si basa sull'utilizzo, come sistema ospitante, della Debian cifrata che abbiamo spiegato nel primo passo dell'esempio "una nuova partenza". Tutti gli attacchi che riguardano questa Debian sono quindi applicabili a questa soluzione.

Tracce lasciate sulla nostra Debian cifrata.

La maggior parte delle tracce più evidenti di questo progetto sono separate dal resto del sistema: tutti i file di lavoro sono salvati dentro la cartella che contiene l'immagine del disco virtuale. Sul nostro sistema Debian vengono però lasciate delle tracce che riguardano il nome della macchina virtuale, la sua configurazione, i tempi di utilizzo.

materiali e logiche che permettono di far funzionare, su un solo computer, più sistemi operativi, in modo separato l'uno dall'altro, più o meno come se funzionassero su macchine diverse.

Ormai è anche relativamente facile far funzionare Windows all'interno di un sistema GNU/Linux, tagliandogli allo stesso tempo tutti gli accessi alla rete, e in particolare isolandolo da Internet.

Attenzione: vi consigliamo di leggere questo capitolo per intero prima di precipitarvi sulle ricette pratiche; la descrizione dell'ipotesi seguente è abbastanza lunga, e i suoi limiti sono elencati alla fine di questo capitolo, in cui suggeriamo anche delle contro misure. Sarebbe un po' un peccato passare quattro ore a seguire queste ricette, per poi rendersi conto che c'è tutta un'altra soluzione in realtà più adatta.

Cominciamo riassumendo l'ipotesi.

POSSIBILI ATTACCHI E SOLUZIONI PRATICABILI

Dipendenza da Windows?
Il primo problema che si pone è: quale sistema operativo usare? Dipende, evidentemente, dal software utilizzato per il progetto:

Se funziona sotto GNU/Linux, continuiamo nella lettura per studiare le varie possibilità che abbiamo.

Se funziona esclusivamente sotto Windows, peccato. Vi proponiamo però lo stesso una via praticabile che permette di limitare i danni. Potete andare direttamente a leggere quella strada, saltando i capitoli che arrivano ora, dedicati invece a GNU/Linux.

Il sistema live senza ricordi

I problemi riguardo a come iniziare, sono gli stessi del precedente esempio "una nuova

Cosa ci dicono le categorie definite quando parliamo di valutazione del rischio, applicate a questo caso?
riservatezza: evitare che un occhio indiscreto arrivi troppo facilmente al progetto e/o ai documenti di lavoro; integrità: evitare che questi documenti vengano modificati a nostra insaputa; accessibilità: fare in modo che questi documenti restino accessibili quando ne abbiamo bisogno.

Qui, l'accessibilità è secondaria rispetto alla riservatezza: l'idea che sta alla base dell'archiviazione è quella di scendere a un compromesso, rendendo l'accesso ai dati più difficile per tutti, per offrire una maggiore riservatezza.

Da chi vogliamo proteggerci?
I rischi studiati nell'esempio "una nuova partenza" valgono anche qui: un furto, una perquisizione che abbia dei motivi che possono anche non essere direttamente legati alle

Adesso passiamo alle cose serie.

Secondo passo: rinchiudere Windows in un compartimento (quasi) stagno

Quella che comincia ad assomigliare a una soluzione seria, è il far funzionare Windows all'interno un compartimento stagno, nel quale quando serve e con coscienza di causa, possiamo aprire una porta per permettergli di comunicare con l'esterno in un modo strettamente limitato.

In altri termini, mettere in piedi una soluzione basata su una logica del tipo lista autorizzata: a priori niente potrà entrare o uscire da Windows, e a partire da questa regola generale, autorizzeremo delle eccezioni, caso per caso, riflettendo sul loro impatto.

La virtualizzazione permette di mettere in atto questo tipo di sistema. E' un insieme di tecniche

Se la catastrofe arriva mentre stiamo realizzando il progetto

L'hard disk del computer utilizzato contiene i file di lavoro contenuti nell'immagine del disco virtuale.

Se la catastrofe arriva dopo

L'immagine del disco virtuale dovrebbe essere stata ripulita nel momento in cui il progetto è finito, se la catastrofe (cedere di fronte alla legge, la scoperta di un problema nel sistema crittografico..) arriva dopo il fatto, le tracce residue sull'hard disk saranno meno evidenti e meno numerose che se avessimo proceduto normalmente.

Se la catastrofe arriva prima della fine del progetto, cioè prima della pulizia che abbiamo consigliato, anche in questo caso sarebbe azzardato sentirsi protetti, perché come spiegato

Visto che un sistema è tanto più suscettibile di essere attaccato quanto più lo si utilizza frequentemente, si possono togliere via dal computer che usiamo tutti i giorni le informazioni utilizzate raramente. Inoltre è più facile riuscire a negare ogni legame con dei file, se questi sono salvati su una penna USB seppellita in mezzo a un bosco, piuttosto che se vengono trovati archiviati sull'hard disk del nostro computer di casa.

E' così necessario?
La prima domanda da porsi prima di archiviare questo tipo di file è la seguente: è davvero necessario conservarli? Quando non si dispone più del tutto di una informazione, possono anche insistere, ma nessuno sarà in grado di darla, e questa a volte è la migliore soluzione.

VALUTAZIONE DEI RISCHI

Cosa vogliamo proteggere?

partenza". Ma prima di mettere in campo le eventuali policy di sicurezza, lanciamoci in un rapido tour degli strumenti e dei metodi disponibili.

Liste bloccate vs liste autorizzate

Visto che abbiamo già un sistema Debian cifrato, potremmo in un primo momento immaginare di configurarlo in modo specifico per fargli conservare il minor numero possibile di tracce delle nostre attività sull'hard disk. Il problema di questo approccio è lo stesso che vale per il metodo "lista bloccata", e ne abbiamo spiegato i limiti nelle puntate precedenti: per quanto tempo ci dedicheremo, qualunque esperto ci lavori, anche con una comprensione particolarmente approfondita dei meandri del sistema operativo usato, ci dimenticheremo sempre una piccola opzione nascosta bene, resteranno sempre delle tracce non volute alle quali non avevamo pensato.

all'inizio di questo esempio, l'inconveniente peggiore del metodo descritto qui è quello dell'essere basato sul principio della lista bloccata, principio abbondantemente descritto in queste pagine... e quindi resteranno sempre delle tracce indesiderate alle quali non avevamo pensato, oltre a quelle che ormai conosciamo bene: log, memoria viva e memoria virtuale, salvataggi automatici.

Se nonostante queste preoccupazioni, l'ipotesi che vi stiamo descrivendo vi sembra un compromesso accettabile, tenete presente anche i limiti condivisi tra tutte le soluzioni studiate in questo esempio, limiti che descriveremo poco più avanti.

Altrimenti, approfondiamo un po'.

Spingersi più lontano

Ammettiamo che uno degli attacchi descritti a

riservatezza desiderata;
- La nostra autodisciplina deve essere perfettamente rigorosa. Se ci dimentichiamo, o non abbiamo il tempo di "ripulire" l'hard disk quando non ci serve più, e il problema si presenta proprio in quel momento, abbiamo perso: fine dei giochi.

Esistono degli strumenti per cifrare i dati su Windows. Possiamo fidarci o no, ma resta il fatto che essi si appoggiano per forza alle funzionalità di quella scatola nera che è Windows. Non possiamo far altro quindi che diffidarne, e in ogni caso Windows avrà accesso ai nostri dati in chiaro e nessuno sa cosa potrebbe farci.

Per concludere questo piccolo giro nel cuore dei miracoli improbabili, aggiungiamo che la sola "soluzione" possibile nell'esempio in cui ci troviamo è usare un approccio a lista bloccata, di cui abbiamo già precedentemente spiegato l'inefficacia.

Al contrario, certi sistemi live funzionano in base al principio della "lista autorizzata": a meno che noi non lo chiediamo esplicitamente, non viene lasciata nessuna traccia sull'hard disk.

Occupandosi soltanto del criterio della "riservatezza", il metodo live batte quindi l'altro 10 a 0. La distanza viene un po' accorciata se consideriamo invece anche tempi e difficoltà di attuazione.

La botte piena o la moglie ubriaca?

Un sistema live è effettivamente senza ricordi; alcune sono pensate proprio per questo, ma questa proprietà ha anche degli inconvenienti. Per esempio, nel caso in cui la nostra live preferita non fornisca un particolare software, che è invece indispensabile per il progetto, dovremmo a scelta:

- installare il software nella live ogni volta che

onde radio, nonché agli effetti dei vari spioni. (Vedi Guida in italiano #0 e #1)

ESEMPIO 3 : ARCHIVIARE UN PROGETTO FINITO

1. Contesto
2. Valutazione dei rischi
3. Possibili attacchi e soluzioni praticabili

CONTESTO

Siamo arrivati in fondo a un progetto sensibile, per esempio un libro è stato impaginato e stampato, un video è stato montato, compresso e caricato su un DVD.

In generale, da adesso non sarà più necessario poter accedere ai file di lavoro (immagini in alta risoluzione, bozze non compresse..). Però potrebbe essere utile poterli ritrovare in seguito, per esempio per una riedizione, o un aggiornamento.

- Dobbiamo avere fortuna. Basta che il problema (una perquisizione, un furto…) si presenti al momento sbagliato per vanificare tutta la azzardata:

Questo cerotto è basato su due ipotesi un po' Un hard disk si può ogni volta smontare e nascondere. Certo. Ma ci sono i periodi in cui lo usiamo, a volte per molti giorni o settimane di fila.

Proviamo ad appiccicare qualche cerotto su questo colabrodo. Eccone un rapido elenco.

Partiamo dal classico computer munito di un hard disk con sopra Windows. Non vogliamo farla pesante, la prima parte di questa guida ha già abbondantemente descritto i molteplici problemi che questa situazione comporta. Un colabrodo insomma, pieno di buchi di sicurezza.

Cosa abbiamo: un colabrodo e una scatola di cerotti vecchi

Un'idea è quella di salvare fuori dal disco del sistema ospitante l'immagine del disco virtuale

Non salvare l'immagine del disco virtuale dentro l'hard disk del sistema ospitante

Prendiamo in considerazione dunque due strade che permettono di limitare i danni. Una è del tipo "lista bloccata", l'altra del tipo "lista autorizzata".

parire dal terzo passo dell'esempio "una nuova partenza" vi sembri credibile. Se esso riuscisse, il contenuto dell'hard disk cifrato del sistema ospitante sarebbe leggibile, in chiaro, dall'attaccante. Ora, i nostri file di lavoro sono, ricordiamolo, contenuti dentro l'immagine del disco virtuale usato dal nostro Windows ospitato… il che non è nient'altro se non uno stupido file salvato sull'hard disk del nostro sistema ospitante. Quindi questi file di lavoro, e tutte le tracce dei software usati dentro Windows, diventano leggibili dall'attaccante.

Limiti comuni a queste policy di sicurezza

Tutte le policy di sicurezza che abbiamo studiato in questo esempio sono vulnerabili a un certo numero di attacchi. Sia quelle basate su un sistema live, che quelle che prevedono di incatenare l'infame Windows.

I passi 4 e 5 dell'esempio "una nuova partenza", studiano alcuni attacchi che ci sono venuti in mente, più o meno fantascientici, a seconda del momento storico, del luogo, dei protagonisti e delle circostanze in ballo. E' il momento di ridargli una lettura.

Inoltre, la parte "problematica" di questa parte della Guida è indirizzata, in un modo relativamente generico, ai molti metodi di sorveglianza che può essere bene ristudiare alla luce della situazione concreta di cui ci occupiamo. Facciamo attenzione in particolare alle questioni su elettricità, campi magnetici e

iniziamo una nuova sessione di lavoro;
- creare una penna USB avviabile live che includa il nostro software all'interno di una partizione persistente;
- convincere gli autori della live ad aggiungere quel software;

L'utilizzo di un sistema live è la soluzione più sicura e, in questo caso, la meno difficile da attuare. Passiamo quindi a studiare una policy di sicurezza basata su questo tipo di sistema.

E' anche possibile installare una Debian in una virtual machine, per rispondere a esigenze come questa, ma questa soluzione è abbastanza complessa e quindi non ne parleremo.

Lavorare su un documento sensibile... dentro a un sistema live

Dopo aver spiegato il contesto all'inizio di questo esempio, e aver deciso di utilizzare un sistema

- informarsi sui limiti comuni a tutte le soluzioni

Per seguire questa strada:

usato dal sistema Windows ospitato. Per esempio, su un disco esterno cifrato. In questo modo, anche se il disco ospitante viene decifrato, i nostri file di lavoro restano inaccessibili.. sempre che il disco esterno che li contiene sia in quel momento tenuto "ordinato".

Questo approccio è del tipo "lista bloccata", con tutte le problematiche relative. I file di lavoro e il sistema Windows si trovano sì da un'altra parte rispetto all'hard disk del sistema ospitante, ma non dobbiamo dimenticare che questi dati saranno comunque utilizzati da un software che gira nel sistema ospitante stesso. In particolare, il gestore delle macchine virtuali. Come abbiamo spiegato nel capitolo "tracce da tutte le parti" (Guida in italiano #1 NDR), rimangono lo stesso diverse tracce, inevitabilmente.

Dopo aver presentato il contesto all'inizio di questo esempio e una volta deciso, malgrado tutti i problemi che questo comporta, di utilizzare Windows, proviamo adesso a trovare un modo per limitare un po' i danni.

Lavorare su un documento sensibile... sotto Windows

Alcuni limiti, comuni sia a questo metodo che a quello basato sull'uso di Windows, verranno esposti nelle prossime puntate.

Limiti

In seguito dovremmo distruggere il volume della persistenza (vedi ricetta).

Una volta terminato il nostro progetto, stampato o pubblicato online, potremmo volerlo archiviare (vedi ricetta).

Distruggere il sistema live

live, non ci resta altro che mettere in pratica questa soluzione.. e studiarne i limiti.

Scaricare e installare il sistema live

Non tutte le distribuzioni live sono necessariamente pensate per delle pratiche "sensibili". Occorre quindi scegliere un sistema concepito in particolare per (provare a) non lasciare traccia sull'hard disk del computer che stiamo usando.

Se non si dispone ancora di una copia dell'ultima versione di Tails, seguite la ricetta per scaricare e installare un sistema live "discreto". (vedi ricetta relativa)
A partire dalla prima periferica Tails appena creata, possiamo poi creare una penna USB dedicata solo al nostro progetto. Per fare questo, bisogna far partire il sistema live appena installato (vedi ricetta "avviare da supporto esterno")

Poi seguiamo le istruzioni per clonare una penna Tails (vedi ricetta "clonare un sistema Tails") e poi quelle per creare e configurare un volume persistente dentro Tails (vedi ricetta "creare la persistenza"). Attiviamo soltanto l'opzione "Dati personali".

Installare un eventuale software aggiuntivo

Se abbiamo bisogno di utilizzare un software che non è incluso dentro Tails e che non vogliamo installare ogni volta, basta seguire la ricetta "Installare un software aggiuntivo dentro Tails".

Utilizzare il sistema live

Ogni volta che dobbiamo lavorare sul nostro documento, basterà avere con sé la penna usb contenente la nostra live e la sua persistenza cifrata per farcelo girare sopra. Per fare questo bisognerà attivare il volume della persistenza (vedi ricetta relativa).

Ripulire i metadati di un documento finito

Una volta che il nostro documento è finito, esportiamolo in un formato adatto allo scambio di documenti (per esempio un PDF nel caso in cui dobbiamo stampare un testo, un file AVI o Ogv se si tratta di un video da caricare su Internet, etc.).

Mettiamo che stiamo pubblicando il nostro documento senza prendere altre precauzioni più ampie: un avversario in questo caso può prima di tutto molto semplicemente scaricarsi il documento e cercare eventuali metadati che lo possano condurre al suo autore.

Malgrado le precauzioni che abbiamo già preso, sarà bene ripulire gli eventuali metadati presenti (vedi ricetta: "ripulire i metadati").

studiate in questo esempio;
- rifarsi alla ricetta per cifrare un hard disk esterno.

Utilizzare un sistema live come sistema ospitante

L'appendice di questo approccio a "lista bloccata" è una soluzione di tipo "lista autorizzata", che coniuga l'utilizzo di un sistema live con il salvataggio dell'immagine del disco virtuale su un hard disk esterno cifrato.

Per seguire questa strada:

- informarsi sui limiti comuni a tutte le soluzioni studiate in questo esempio;
- rifarsi alla ricetta per cifrare un hard disk esterno, e a quella che spiega come utilizzare un sistema live.