Sentry: un Linux per molti usi...

[In questo breve articolo cercherò di spiegare come sfruttare Sentry: una distribuzione GNU/Linux, un po' particolare, utile per vari utilizzi e di illustrarvi una mia esperienza di installazione (seguita da un utilizzo un poco inusuale).]

Cos'è sentry:

Come definito nelle FAQ del prodotto il "Sentry Firewall CD" è un CD-ROM avviabile basato su Linux, utile per svolgere diverse funzioni: da firewall a server applicativo.
Per CD-ROM avviabile si intende un CD che contiene il sistema operativo installato e dotato di un settore di avvio in modo tale che se il BIOS del PC lo prevede è possibile avviare il computer tramite il CD-ROM.
Il vantaggio di operare tramite un CDROM e dato principalmente dall'inalterabilità del sistema e quindi dall'elevato grado di ripristino del sistema e da una sostanziale impossibilità da parte di un cracker (non haker come a volte vengono erroneamente definiti gli "intrusi" informatici) di comprometterlo in modo definitivo.
Uno dei divertimenti preferiti dei cracker infatti e l'installazione di un rootkit immediatamente dopo aver compromesso un host.
Un rootkit è in parole semplici un insieme di programmi e utility di sistema modificati in modo da consentire facile accesso, successivo, al cracker mascherandone nel contempo le attività.
Chiaramente tali programmi vengono normalmente installati nell'hard-disk del sistema compromesso e sono decisamente ostici da rimuovere richiedendo spesso di reinstallare tutto il sistema per poter ristabilire una situazione sicura.
Nel caso di Sentry il sistema operativo è memorizzato in un CD e quindi per definizione non modificabile. Il ripristino del sistema si limita quindi al riavvio del PC (e naturalmente a metterlo in sicurezza con migliore protezione).
Un'altro grande vantaggio è dato dal fatto che il sistema operativo non è contenuto sull'hard-disk che è uno dei componenti maggiormente soggetti a guasto all'interno di un computer.
A questo punto potrebbe nascere una interminabile discussione sul fatto che un lettore di CD è comunque un componente con una meccanica soggetta a guasti quanto (se non di più) degli hard-disk e che gli stessi CD sono sogetti a forme di usura. Vorrei solo far notare che di un CD si possono avere numerose copie a basso costo e che un lettore di CD ha un prezzo molto inferiore a quello di un hard-disk.

La distribuzione su cui si basava originariamente Sentry è la Slackware e questa è anche la versione che ho utilizzato. Voglio comunque segnalare la presenza di una versione di Sentry basata su Red Hat.

Preparazione del CD:

Alcuni passi che seguono sono parziali traduzioni dall'How-to di Sentry (tradotte dopo avere verificato personalmente il loro funzionamento).

1. Prelevare l'immagine ISO aggiornata del CD da www.SentryFirewall.com.
   Il file che viene prelevato è compresso in formato .gz o .bz2; bisogna quindi
2. decomprimerlo in una directory a vostra scelta:

   ```
   gzip -d sentrycd.iso.gz
   ```

3. Trattandosi di un prodotto che può essere destinato all'utilizzo come firewall è opportuno verificare l'integrità del file come segue:

   ```
   md5sum -b sentrycd.iso
   ```

4. Passare quindi alla masterizzazione

   ```
   cdrecord -v -data speed=XXX dev=YYY sentrycd.iso
   ```

dove XXX sarà la velocità di masterizzazione desiderata e YYY il percorso del device del Vostro masterizzatore.

Può capitare che siate sprovvisti di un PC con GNU/Linux (spero di no!) o che, come è capitato al sottoscritto, non abbiate il masterizzatore disponibile nel vostro PC Linux.
E`sufficiente quindi scompattare il file con uno dei tanti programmi di decompressione come ad esempio Freezip (freeware).
Masterizzare quindi il CD tramite un programma di masterizzazione adeguato: in Windows tutti i programmi di masterizzazione più noti prevedono l'opzione per la creazione di CD da immagine ISO. Pertanto è sufficiente selezionare l'immagine e far partire la masterizzazione.

Dotazione e configurazione Hardware

Una volta ottenuto il CD sarà necessario un PC, con almeno due schede di rete, che sia in grado di effettuare il boot da CD (i BIOS più vecchi non prevedono l'opzione di avvio da CD). E` richiesto un minimo di 32Mb RAM ma sono consigliati 64Mb.
Deve essere dotato di un floppy drive con almeno un floppy per salvare la configurazione personalizzata. Sarà invece opportuno scollegare l'eventuale hard-disk presente (lo potete riciclare in un'altro PC)in modo che non possa costituire un “punto di appoggio” per la modifica “al volo” della configurazione e dei programmi.
Il PC andrà configurato (intervenendo eventualmente nel BIOS) per tentare il boot prima da CD e poi da floppy escludendo il boot da hard-disk.
Da notare che l'how-to originale prevede anche, fra i requisiti minimi, il *"facile accesso a caffè, the, soda o stimolanti equivalenti"* :-). Da parte mia consiglio invece di dotarsi di una buona dose di pazienza...e in seguito cercherò di spiegare il perchè

Configurazione e personalizzazione

La necessità di un floppy è ovvia: esso rappresenta (e contiene) la personalizzazione e la specializzazione del nostro sistema SENTRY rispetto allo standard contenuto nell'immagine iso del CD.
Il dischetto viene letto in fase di avvio e la sua configurazione sovrascrive parzialmente quella del CD.
In particolare durante la fase di avvio viene rilevata la presenza di un floppy. Se presente viene "montato" in `/floppy` e viene letto il file `sentry.conf` in esso contenuto.Tale file contiene delle istruzioni/direttive per indicare al sistema di rimpiazzare alcuni files di configurazione standard con quelli contenuti nell floppy stesso. Per il dettaglio sulle istruzioni possibili vi rimando all'ottimo How-To contenuto, fra l'altro, anche all'interno del CD.
In caso di problemi, durante la personalizzazione, potete ripartire sostituendo il dischetto e ricominciando la configurazione da zero o semplicemente eseguendo il boot da CD e poi montando il floppy per modificarne il contenuto.

Una volta avviato il sistema da CD eseguire il Login con utente `root` e password `sentry`.
Da questo momento bisogna ricordare che ogni modifica apportata al sistema e non salvata su floppy è da considerare nulla in quanto il sistema lavora su un ramdisk e qualsiasi dato scompare al riavvio.
Vi assicuro che mi sono dimenticato un numero infinito di volte di salvare la configurazione e questo comporta la necessità di ricominciare da capo ad ogni riavvio (da qui il consiglio di armarsi di molta pazienza).
Innanzitutto modifichiamo le password di default per i due utenti di standard che sono root e sentry: I comandi sono:

```
passwd root
```

e

```
passwd sentry
```

quando richiesto fornire la nuova password e confermarla con una seconda immissione.
E` necessario quindi formattare il floppy per poterci scrivere i files di configurazione:
formattiamo:

```
fdformat /dev/fd0
```

e creiamo il filesystem:

```
mkfs -t ext2 /dev/fd0
```

A questo punto possiamo sfruttare l'utility che permette di creare il file di configurazione sul floppy eseguendo il comando

```
mkconfig
```

I files di configurazione scritti nel floppy,a questo punto, conterranno anche il file delle password

```
passwd
```

con gli utenti aggiornati e le password modificate.
In alternativa è possibile creare a mano i files di configurazione copiando la struttura di default con:

```
cp ~/SENTRY/scripts/cd-config/sentry.conf /floppy/
```

Ricordarsi sempre che è necessario copiare i files man mano che vengono modificati, quindi, ad esempio, una volta cambiati utenti e password sarà necessario copiare i files relativi dal ramdisk al floppy:

```
cp /etc/passwd /floppy/config/passwd
cp /etc/shadow /floppy/config/shadow
```

E` necessario precisare che non tutti i files contenuti nel floppy vengono letti e vanno a sovrascrivere automaticamente le informazioni del CD, ma solo quelli specificati all'interno del file `/floppy/sentry.conf`. Innanzitutto sarà necessario specificare di leggere i nuovi utenti e le nuove password. Apriamo quindi il file attraverso un editor:

```
vi /floppy/sentry.conf
```

. ed inseriamo le modifiche seguenti:

```
--------
passwd= /floppy/config/passwd
shadow= /floppy/config/shadow
--------
```

Configurazione della rete

>Passiamo a configurare la prima interfaccia di rete. Sarà necessario modificare il file `/etc/rc.inet1` in modo da inserire alle voci

```
 IPADDR=
 NETMASK=
 NETWORK=
 BROADCAST=
```

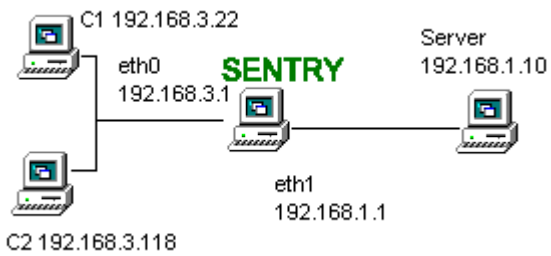
gli indirizzi IP della rete, della netmask, etc.
Copiare poi il file `/etc/rc.inet1` dal ramdisk al floppy e configurare il file `/floppy/sentry.conf` aggiungendo la riga

```
--------
rc.inet1= /floppy/config/rc.inet1
--------
```

Ripetere l'operazione per ciascuna interfaccia di rete ovvero per gli eventuali files `/etc/rc.inet2` etc.

Un applicazione...

Come accennato nell'introduzione il CD di SENTRY contiene un discreto numero di sevizi/applicativi che possono essere utili. Personalmente l'ho impiegato in una situazione in cui avevo la necessità di controllare in maniera molto rigida gli accessi ad un server applicativo da uno spezzone all'altro della mia intranet.
Lo schema che segue può essere utile per chiarire la cosa:



Mi era infatti necessario limitare il numero di utenti che potessero accedere al server, misurare il traffico e in caso di necessità poter interrompere "al volo" il servizio.Inoltre veniva richiesto che gli accessi fossero possibili solo in una determinata fascia oraria.

Vista la particolarità del caso ho ritenuto opportuno collegare fra il server ed il resto della rete un PC che avesse la funzione di "filtro". Avevo sentito parlare di SENTRY e mi sembrava il caso opportuno per verificarne il funzionamento.

Ho deciso quindi di dividere la intranet in due aree e utilizzare il PC con SENTRY come router tra le due. In realtà un'area è rappresentata dal solo server applicativo ma isolarlo significava poterne regolare l'accesso in maniera migliore.

Per prima cosa ho verificato che il PC SENTRY non avesse dei servizi attivi non necessari. Non fidandomi del solo controllo "a vista" della configurazione, sono ricorso ad un buon scanner di rete (NESSUS) per testare il sistema. La buona notizia è che SENTRY non attiva nessun servizio come predefinito (ovvero se volete qualcosa di attivo dovete esplicitamente configurarlo). Nel mio caso non avevo proprio bisogno di alcun servizio se non il funzionamento di base della rete e avevo già configurato le due interfacce di rete come sopra riportato.
Giusto per dare un po' di nomi alle cose il lato dei clients corrispondeva alla scheda di rete eth0 di SENTRY configurata come segue:

```
IPADDR=192.168.3.1
NETMASK=255.255.255.0
NETWORK=192.168.3.0
BROADCAST=192.168.3.255
```

mentre il lato server corrispondeva alla eth1 di SENTRY configurata come segue:

```
IPADDR=192.168.1.1
NETMASK=255.255.255.0
NETWORK=192.168.1.0
BROADCAST=192.168.1.255
```

d il server aveva `IPADDR=192.168.1.10` mentre i due client di test erano:
C1 con `IPADDR=192.168.3.22` e C2 con `IPADDR=192.168.3.118`

A questo punto è necessario attivare il routing fra le due reti. Sul PC SENTRY aggiungiamo quindi le seguenti regole:

```
route add 192.168.1.10 eth1
route add default 192.168.1.0
route add 192.168.3.22 eth0
route add 192.168.3.118 eth0
```

questo indica al PC come raggiungere gli altri host e solo quelli, non solo abbiamo imposto che di default i pacchetti uscenti vengono indirizzati alla eth1 ove non specificato altrimenti. In questo modo si escludono tutti gli host del lato client non specificati.
Continuo a ricordare che le modifiche inserite permangono solo fino al riavvio della macchina. Per evitare un buon mal di testa, dopo avere eseguito i test con risultato positivo, ricordatevi di trascrivere le modifiche stesse nel floppy. Per mia scelta personale ho trascritto le righe relative al routing alla fine del file `rc.inet1= /floppy/config/rc.inet1` ove era comunque presente una direttiva riguardante la rete di default.
Aggiungiamo quindi nelle tabelle host le dovute specifiche: in `/etc/hosts` le righe relative ai due clients e al server...

```
---------
C1 192.168.3.22
C2 192.168.3.118
Server 192.168.1.10
---------
```

Nella tabella `/etc/hosts.deny` inseriamo la riga che segue:

```
deny ALL:ALL
```

che, di fatto, vieta l'accesso a qualsiasi attività è servizio di rete per gli hosts non indicati nella tabella `/etc/host.allow` nella quale appunto indichiamo:

```
192.168.1.10 ALL
192.168.3.22 ALL
192.168.3.118 ALL
```

anche in questo caso bisogna ricordarsi di copiare i files dalla directory /etc/ al floppy (in `/floppy/config/`) in modo da non perdere le modifiche e configurare il file `/floppy/sentry.conf` in modo che i files siano caricati all'avvio.

Per limitare gli accessi in maniera drastica ho scelto una soluzione banale: ho schedulato con cron due comandi che ad una determinata ora "spengono" la rete dall'interno:

```
ifconfig eth0 down
ifconfig eth1 down
```

Avrei dovuto poi schedulare altri due comandi per il riavvio della rete ma ho preferito invece effettuare un `reboot` programmato 5 minuti prima dell'orario di inizio lavoro. Naturalmente ho provveduto a sostituire la tabella cron di default con quella salvata nel floppy.
A questo proposito vi devo riportare che la versione di SENTRYin mio possesso aveva un errore nella direttiva di sostituzione della tabella cron e ho fatto ricorso a una serie di scripts per ovviare all'incoveniente. Tale errore è stato in seguito corretto e la versione attuale mi risulta essere priva di tale bug.

Il risultato dell'operazione sopra indicata è un PC che permette ai soli client indicati di collegarsi al server. In caso di necessità posso modificare le tabelle di route e quelle degli hosts per aggiungere o rimuovere accessi ad altri PC o limitare l'utilizzo di solo alcuni protocolli di rete. Grazie ad una copia del CD e ad un backup aggiornato del floppy posso attivare (in caso di guasto) un PC con la stessa funzione di filtro in pochi minuti (il tempo di trasferire le schede di rete o trovarne un paio di compatibili con la configurazione). Se lo ritenessi opportuno niente mi impedirebbe di sfruttare i servizi di firewall a disposizione nel CD in modo da "rafforzare le difese".
Come ultima nota segnalo la presenza di un utility (`netwatch`)che permette di visualizzare, in modalità testo, i contatori dei pacchetti che viaggiano nella rete evidenziando il traffico fra i due segmenti.
Chi ne fosse capace inoltre può eseguire il mount dell'immagine del CD copiarla in un disco e modificarne le parti che ritiene opportune. Ne otterrà un sistema personalizzato, pronto all'uso, che potrà eventualmente riconvertire in CD.
Per le applicazioni possibili l'unico limite è dato dalla vostra fantasia...

di Rudi Giacomini Pilon