

Brain Link Dead Network HOWTO

Fabio Galvagni

fabio.galvagni@katamail.com
rhapsody@brainld.kicks-ass.org

Brain Link Dead Network HOWTO

by Fabio Galvagni

Copyright © 2004 BrainLinkDead Corporation

Noi siamo per i siti semplici, le amicizie ristrette, i programmi modulari.

Table of Contents

Introduzione	i
1. Sistema Operativo.....	1
1.1. Perchè non usare Windows?.....	1
1.2. Allora si usa Linux?	1
1.3. Ho capito, si usa Linux... ma quale distro?	1
1.4. Configurazione base di una Linux Box.....	2
1.4.1. Partizionamento dei dischi	2
1.4.2. Utenti e gruppi utenti.....	2
1.4.3. Firewall.....	3
2. Servizi di Rete	5
2.1. Quali? Quanti?	5
2.2. Web	5
2.3. FTP.....	6
2.4. SSH	6
2.5. MySQLD.....	7
2.6. Altri servizi di rete	7
2.6.1. WebChatServer.....	7
2.6.2. Ddlient	7
3. Organizzazione del FileSystem.....	8
3.1. Organizzare? Che cosa? E perchè?	8
3.2. Files personali	8
3.3. Pagine web	8
3.4. Files ed FTP	9
4. Il sito della Brain Link Dead Corporation	10
4.1. Struttura generale	10
4.2. Configurazione di Apache.....	11
4.3. Aggiunta di una sezione al sito	11

Introduzione

"Se Mussolini avesse commesso l'errore di frequentare una universita' italiana, non credo ci sarebbe stato alcun decennio fascista."

—Ezra Pound

Da rarefatto ed etereo sogno, puro ed astratto trastullo mentale di qualche sognatore Linuxfilo con molto tempo da perdere e con i piedi lunghi dall'esser saldamente piantati per terra, la rete del noto gruppo criminal-satanic-xxx-valligian-ingenerist- gnurant-birrofagus e' divenuta una realta' concreta dei fatti, con ben due server attivi ventiquattr'ore su ventiquattro (AlphaBrainld e BetaBrainld) e molti altri ancora in fase di preparazione, sperimentazione o rodaggio.

Ecco dunque il perche' di questo documento. Un si' ben fatto network non puo' certo esimersi dal costituire una serie di regole a carattere tecnico/pratico, che ne definiscano in qualche modo i tratti caratteristici fondamentali ed ne favoriscano dunque il sicuramente radioso sviluppo futuro. Troverete qui una serie di regole di fondamentale importanza, alcune riguardanti la tutela della sicurezza della rete, altre la semplice organizzazione dei nostri potenti sistemi informativi (leggi: serverini), dall'organizzazione del filesystem, alla gestione degli utenti e gruppi utenti, fino alla disposizione delle proprie pagine web personali.

L'obiettivo e' quello di creare un network (e quindi uno strumento di lavoro e/o cazzeggio) affidabile, efficiente, sicuro e, soprattutto, facile da gestire e da mantenere. Si, insomma, quello che vogliamo, da bravi ingegneri, e' sistemare tutto subito per poi cazzeggiare e basta, lo ammettiamo ;-)

Chapter 1. Sistema Operativo

1.1. Perché non usare Windows?

Perché non è sicuro. Perché non è facilmente aggiornabile (bisogna aspettare i service pack che comunque non risolvono mai nulla, anzi peggiorano la situazione). Perché è pesante, instabile, e anche piuttosto brutto. Perché non serve a nulla far girare un' interfaccia grafica se poi non la si usa. Perché Bill Gates è gay. Perché Microsoft è espressione del capitalismo demo-pluto-massonico, nonché sionista. Perché AlphaBrainld lo reggerebbe a fatica. Perché non c'è il portage tree. Perché configurare uno Unix è piu' divertente e piu' fiko. Perché se Nafta non è capace di usare Linux sono cazzi suoi, impara, no? Perché Windows è PISC.

Ad ogni modo, per usare Windows bisognerebbe possederne una licenza (vera). In caso contrario, un server pubblico rischia grosso...

1.2. Allora si usa Linux?

E chi lo ha mai detto? Non esiste solo Linux... ci sono anche FreeBSD, NetBSD, OpenBSD, Minix, MacOSX, GNU/Hurd... certo bisognerebbe imparare ad usarli bene. L'importante è lavorare con sistemi Unix, per garantire la intro-compatibilita' ai server della Brainld network...

Le uniche alternative possibili sono 2: Linux o FreeBSD. Quest'ultimo, forse, potrebbe essere la scelta migliore: ` piu' stabile, piu' 'collaudato' ('meno giocattoloso' di Linux), piu' veloce, piu' efficiente... e poi il diavoletto fa piu' fiko del pinguino con gli occhi da strafatto di Linux.

FreeBSD ha pero' un difetto, un grosso difetto. Non supporta iptables. Nemmeno ipchains. Nossignore. Siamo ancora fermi ad ipadwf. Un guaio. Un grosso guaio per un sistema che dovrebbe fare da server ma contemporaneamente esporsi come Bastion Host...

1.3. Ho capito, si usa Linux... ma quale distro?

Quella che vuoi. Basta che non sia Debian. La ODIO. Tutti la odiano. Tutti la dovrebbero odiare. E anche tu la odi adesso, vero?

Warning

Non provare assolutamente ad usare Debian. So chi sei, e dove abiti. Ti vedo.

Gentoo Linux è senza dubbio quella piu' performante dal punto di vista delle prestazioni (e dato l'hardware che abbiamo a disposizione, la cosa non è da poco). Certo risulta tediosa da installare e configurare, richiede competenze tecniche non da poco... e per aggiornare un software scarica, ricompila quarant'anni e il tutto a partire dai sorgenti. Ma in fondo, lo facciamo noi o il povero serverino?

Slackware e' una distribuzione grandiosa. Semplice, pulita, bella. Certo, bisogna scordarsi gli aggiornamenti automatici, anche se c'è emerde... ma non si fa prima allora ad usare Gentoo?

Fedora? Ma si, puo' andare... ora che Red Hat si è tolta dalle palle, la distro è stata ripulita per benino. Eppoi il sistema rpm non funziona mica male, in fondo. Sempre meijo di quello di Debian (va beh che non ci vuole molto).

Se avete altre idee, scrivetemi. Io mi trovo bene a smanettare con Gentoo, e vorrei imparare per benino FreeBSD. Suggestimenti, insulti, prediche, saranno da me sempre gradite. Amen.

1.4. Configurazione base di una Linux Box

1.4.1. Partizionamento dei dischi

Sicuramente una bella partizioncina di swap da almeno 500MB. Eppoi /home dovrebbe risiedere su un disco o almeno su una partizione separata...

Warning

/home DEVE risiedere in una partizione separata da quella di root (/)!!! In /home risiede /home/ftp, e se, nel riempirvi l'ftp, vi dovessero riempire la / perchè siete stati coglioni e non avete configurato bene il vostro sys... sono cazzi!

usando il comando e2fsck si fa una bella scansione delle partizioni. Farla spesso aiuta a risolvere molti problemi...

1.4.2. Utenti e gruppi utenti

Ogni utente dovrebbe essere identificato in modo univoco, all'interno del network. Suggestisco i seguenti nicknames:

- Rhapsody (Io)
- Frasten (Piccy Barba)
- Nightwakth (Piccy Rosso, meglio di RedManBrainld)

- Mordeth (Iora)
- Pedro (quando cazzo ti decidi a scegliere un nick decente?)
- Nafta (Nafta)
- Chrome (Sergio di Rio... ma entra poi o no?)
- Giala83 (Teo, ma che nick di merda... suggerisco 'Winnie Pooh')
- Satana (Alessio)

E, speriamo, tanti altri...

L'utente root, è ovviamente, riservato all'/agli amministratore/i del server. Cio' significa che la password deve rimanere segreta, per questioni di sicurezza internazionale, anche all'interno della Brainld, e condivisa con i soli diretti interessati alla manutenzione del server.

Caution

Silenzio! Il nemico ci ascolta...

Per quanto riguarda i gruppi utenti, ciascun membro della Brainld corp dovrà appartenere al gruppo 'brainld' presente su ciascun server, ma anche al gruppo riservato alla rete locale (per esempio l'utente 'rhapsody' su betabrainld appartiene sia al gruppo 'brainld' che a quello 'galvagni').

settaggio gruppi utenti

```
groupadd [nomegruppo]  
useradd -m -G [nomeutente] -s /bin/bash
```

1.4.3. Firewall

E qui son dolori. Perchè di iptables me ne intendo davvero troppo poco, e quelle quattro righe che ho scritto sono veramente un firewall penoso e pieno di buchi. Ma nemmeno Iora sembra cavarsela meglio... almeno a giudicare dagli attacchi subiti da AlphaBrainld, che è stato aperto come burro...

Forse Sergio di Rio ci puo' dare una mano. Forse è lui l'uomo del momento. Sergio, se ci sei, batti un colpo!

Warning

Gigante, aiutaci tu!

Comunque, io opterei per un firewall minimalista. Tutto chiuso, tranne quello che voglio stia aperto. Tutto cio' che non è esplicitamente concesso è proibito (tranne la birra ed il sesso).

Chapter 2. Servizi di Rete

2.1. Quali? Quanti?

Essenzialmente quattro: web, ftp, mysql, ssh. Piu' altre diavolerie che potrebbero disgraziatamente venire in mente (tipo server strani per controllori Campi-like...). Ah, dimenticavo. La mia splendida chat in java.

Caution

La mia chat in java girera' su AlphaBrainId, oh se girera'. Ora la RAM c'è. altrimenti... sara' AlphaBrainId a girare.

2.2. Web

Un nome solo: Apache. Meglio la versione 2.

Sicuramente DEVE esserci il supporto php. La quasi totalita' dei siti ospitati su BrainId sono scritti in php. Il MIO sito è scritto in php.

Important: Sgombrate la mente dalle cazzate che ha sparato Nafta a riguardo. Php non è un 'servizio di rete' nè un server. È semplicemente l'interprete di un simpatico linguaggio sul quale si appoggia (talvolta, se lo deve usare per interpretare qualche pagina!) il server web Apache. Non spaventatevi dunque se, dopo aver installato mod_php, nmappando non si intravede alcuna voce 'php'...

Se avete Gentoo, emerge mod_php. Meijo tenere php come modulo di apache... fa meno danni.

configurazione per mod_php di apache2.conf

```
LoadModule php4_module /usr/lib/apache2-extramodules/libphp4.so
```

```
AddType application/x-httpd-php .php
```

Important: Apache andrebbe anche configurato in modo tale da permettere l'accesso alle pagine web personali di ciascun utente in questo modo: <http://xxxbrainid.kicks-ass.org/~username/>

E non dimenticate di settare Apache nel runlevel di default...

2.3. FTP

Eh, lo so, è comodo. Poi, con la possibilità di loggarsi come utente e di lavorare via ftp sulla propria home...

Ma è insicuro. La coppia nome_utente/password viene trasmessa IN CHIARO! Non viene applicato alcun algoritmo di cifratura nella trasmissione dei dati. Insomma, una vera porcheria. E' piu' sicuro raccontare i propri cazzi ad una vecchia di paese.

Usiamo SSH, va la', che e' meglio. Piu' scomodo, soprattutto per gli utenti Windows, ma...

Note: Cazzi loro.

2.4. SSH

Beh, sicuramente deve esserci un bel demonino sshd in giro per la memoria del nostro server. Anzi, al dire il vero, il server che si espone come Bastion Host (cioè quello che fornisce l'accesso ad internet tramite NAT firewallato agli host della rete interna) dovrebbe in teoria far girare solo sshd... a volte nemmeno quello. Ma cio', per noi, significherebbe dover avere uno spazio di indirizzamento almeno /31 per la rete perimetrale esterna, e un ip statico... impossibile.

Tramite ssh, che è un protocollo dello strato Sessione, si possono fare cose molto interessanti. SSH fornisce servizi di crittografia dei dati, che le applicazioni dello strato superiore possono utilizzare senza grossi problemi. Per esempio l'applicativo 'scp' ('pscp' sotto Windows) permette, sfruttando il protocollo SSH, di trasferire files dal sistema locale a quello remoto, viceversa, e persino da/verso due sistemi remoti!

uso di scp (pscp sotto Windows)

```
scp utente@host.dominio:nomefile nomefile ( remoto->locale )
```

```
scp nomefile utente@host.dominio:nomefile ( locale->remoto )
```

```
scp utente1@host1.dominio1:nomefile utente2@host2.dominio2:nomefile ( remoto->remoto )
```

Note: il percorso è sempre relativo alla home dell'utente specificato; se ci si vuole riferire alla root directory (/), è necessario specificarlo: utente@host.dominio:/path/filename... (avete i permessi per farlo?)

2.5. MySQLD

In realta' SQL non sarebbe un vero e proprio servizio di rete... il team di mysql ha deciso di implementare il proprio database come tale.

Ma anche MySQL non è troppo sicuro. Anche qui la coppia nome_utente/pwd è trasmessa in chiaro...

2.6. Altri servizi di rete

2.6.1. WebChatServer

Lo farete girare. Vivi o morti.

Supporta piu' chatrooms, quindi chiunque puo' implementarlo all'interno del proprio sito senza per questo 'disturbare' le altre stanze virtuali che girano sul server. La chatroom (una per ciascun sito=implementazione) è impostata per essere passata come parametro alla applet.

2.6.2. Ddlient

È il programma utilizzato per mantenere il dominio statico di secondo livello xxxbrainld.kicks-ass.org a partire dall'indirizzo dinamico fornito dalla connessione dial-up dei nostri meravigliosi server.

Note: Qualcuno potrebbe spiegarmi per cortesia come fa a funzionare se non apre alcun socket, nè UDP nè TCP su nessuna porta???

Chapter 3. Organizzazione del FileSystem

3.1. Organizzare? Che cosa? E perchè?

È già' dura mantenere sincronizzati e funzionanti 2 server. Se poi si incomincia a far casino con le directory... caos totale. Pisc.

AlphaBrainld è, e DEVE rimanere il server principale (PRIMARY). Quando un server Secondary come BetaBrainld modifica il proprio contenuto (pubblico, cioè condiviso dalla Brainld) o necessita di aggiornamento, deve riferirsi SOLO ed ESCLUSIVAMENTE al il primary server. Un minimo di gerarchia ci vuole. Gli altri secondary server si aggiorneranno da li' in seguito.

sincronizzazione di due directory tramite RSync(locale <-> remoto)

```
rsync -av dir_locale/ utente@host.dominio:dir_remota/
```

3.2. Files personali

I files personali sono ovviamente contenuti nella propria home, non vedo in che altro posto. Le homes, ovviamente, andrebbero sincronizzate. Di questo, pero', dovrebbe occuparsi l'utente...

Note: Esiste la possibilita' di far sincronizzare ai server tutto automaticamente? E questo richiederebbe che il server memorizzi la pwd di ciascun user da qualche parte, vero? Se sapete qualcosa, fatevi vivi...

3.3. Pagine web

Warning

I propri siti andrebbero posti in \$HOME_DIR/public_html. Ma i collegamenti al sito personale dovrebbero riferirsi a \$HOME_DIR/public_html/mywb/!!! (altrimenti come fa il visitatore a sapere qual'è il sito personale effettivo di un determinato membro della BrainLD???)

Non c'è molto altro da dire; qualche consiglio sulla programmazione in php del proprio sito, che deve essere il piu' possibile indipendente dalla locazione in cui viene posto.. per esempio il mio si calcola di volta in volta dove si trova (tramite funzioncina stupidissima),

Dimenticavo: il sito 'ufficiale' del server (che dovrebbe essere uguale per tutti i nodi della rete BrainLD, e scritto in php per adattarsi a ciascuna macchina) andrebbe posto in /var/www/htdocs.

Note: Gentoo Linux colloca di default i documenti html in /var/www/localhost/htdocs

3.4. Files ed FTP

I documenti esportati tramite FTP con logging 'anonymous' devono riferirsi semplicemente all'utente ftp (quindi si devono trovare in /home/ftp). Deve anche esserci certamente una directory per gli uploads (per ex. /home/ftp/uploads).

Warning

Okkio ai permessi! Questi vanno settati sia nel file di configurazione di proftpd (proftpd.conf), sia a livello di permessi (chmod!!!)

Oltre ad un accesso di tipo 'anonymous', trascurando l'aspetto della sicurezza nella trasmissione della coppia username/login, andrebbe impostato anche l'accesso ftp per ciascun utente. In questo modo il contenuto di ogni \$HOME risulterebbe accessibile da remoto e facilmente modificabile.

Chapter 4. Il sito della Brain Link Dead Corporation

Warning

Il sito è stato opportunamente progettato in modo tale da non richiedere alcuna modifica se collocato su un nuovo server appartenente alla BrainLD Network (purché il nome del server sia stato opportunamente configurato in apache2.conf e il file 'config.inc.php' ne preveda la presenza nel network).

4.1. Struttura generale

Si tratta di una struttura relativamente semplice, imperniata su tre script php di base (config.inc.php, header.php, footer.php). Il sito è stato implementato in modo tale da non richiedere alcuna modifica al codice (nè a quello di 'base', nè a quello relativo ai contenuti 'secondari').

'config.inc.php' contiene le variabili necessarie al funzionamento del sito, fra le quali gli array contenenti i nomi dei membri (ed il loro corrispettivo identificativo ICQ) e i riferimenti alle sezioni presenti sul sito e accessibili fra i link 'fondamentali' (nome file + nome link). È richiamato direttamente da 'header.php'.

'header.php' richiama 'config.inc.php' ma anche 'library.php'. Va aggiunto DOPO aver dichiarato la variabile \$sub_title (il titolo della sezione/pagina). Segue il contenuto vero e proprio della pagina, ed infine il 'footer.php', che chiude la pagina.

'library.inc.php' contiene alcune funzioni di base, fra le quali image(\$path).

Warning

Le immagini vanno aggiunte NON DIRETTAMENTE, ma attraverso la funzione image(): in questo modo vengono automaticamente calcolate (e dichiarate nel tag IMG generato dall'interprete php) le dimensioni orizzontali e verticali dell'immagine, eliminando lo sgradevole effetto di 'caricamento' della pagina (il browser, infatti, essendo a priori a conoscenza delle dimensioni effettive di ciascuna immagine da caricare in una pagina, ne imposta il 'rettangolo' prima ancora di aver cominciato il caricamento).

Warning

Le immagini vanno INTERLACCIADE!!! In questo modo si ottiene il piacevole effetto di progressivo 'sfuocamento' che, unitamente alla tecnica descritta dal 'warning' precedente, rendono complessivamente piu' gradevole (e meno pesante) il caricamento della pagina.

4.2. Configurazione di Apache

E' sufficiente attivare il supporto per il php ed impostare il nome del server come xxxxBrainLD. Ovviamente, se si aggiunge un nuovo server alla BrainLD Network, bisognera' opportunamente modificare l'array 'network' contenuto in 'config.inc.php'...

4.3. Aggiunta di una sezione al sito

Semplicemente si deve creare un file .php e scrivere il contenuto dopo aver richiamato 'header.php' e prima di richiamare 'footer.php'.

Per fare invece in modo tale che la nuova pagina/sezione appaia nel menu dei links, è necessario che nel file config.inc.php vengano modificati due array: si deve aggiungere il nome del corrispondente file in sections[], e il nome della sezione (quello che apparira' effettivamente nel menu) in sections_name[].