

Configurazione “sicura” di un server web Apache in ambiente Linux

In questo documento saranno illustrate le procedure da seguire per garantire un elevato livello di sicurezza nella configurazione di un server web Apache.

In particolare verranno presi in considerazione i seguenti aspetti fondamentali:

- impostazione dei diritti di accesso alle directory ;
- gestione dei meccanismi di autenticazione;
- creazione di un ambiente di esecuzione “isolato” per il server web Apache

Prerequisiti:

- installazione di Apache 1.3.x;
- distribuzioni linux di riferimento: RedHat 6.x, 7.x – Mandrake 6.x, 7.x, 8.x;
- privilegi di superutente.

Riferimenti:

- Apache: <http://www.apache.org>
- mod_ssl: <http://www.modssl.org>
- mod_perl: <http://perl.apache.org>
- mod_php: <http://www.php.net>

1. Impostazione dei diritti di accesso alle directory

Dopo aver installato Apache è necessario modificare i permessi di alcuni file secondo le seguenti indicazioni:

```
chmod 511 /usr/sbin/httpd
chmod 750 /etc/httpd/conf
chmod 750 /var/log/httpd
```

1.1 Browsing delle directory

Se è stato abilitato il browsing delle directory (mediante l'opzione `IndexOptions` nel file `httpd.conf`) potrebbero verificarsi problemi di sicurezza in presenza di directory web prive di un file `index`; in questo caso, infatti, un qualunque browser potrebbe avere accesso a tutti i file, anche quelli non esplicitamente linkati all'interno di una pagina html.

Per ovviare a questo problema è necessario rimuovere il permesso di lettura dalle directory che non contengono un file `index`.

Es.

```
cd /home/httpd
chmod 311 MyDir
```

Con questa modifica i browser restituiranno un messaggio di errore quando tenteranno di accedere al contenuto della directory `MyDir`.

2. Meccanismi di autenticazione degli accessi

Questa feature può essere utilizzata quando esiste l'esigenza di autenticare gli accessi alle pagine web.

In alcuni casi, infatti, è necessario proteggere l'accesso ad alcune sezioni di un sito web mediante username e password.

I passi da seguire per sfruttare al meglio questa funzionalità sono i seguenti:

2.1 Creazione e aggiornamento del file `.dbmpasswd`

Il file `.dbmpasswd` contiene gli username e le password degli utenti web. Per creare o aggiornare questo file occorre utilizzare il comando `dbmmanage`. Prima di tutto è necessario cambiare i permessi di questo programma e renderlo scrivibile solo dal superutente, leggibile ed eseguibile dal gruppo e inaccessibile per tutti gli altri. Quindi:

```
chmod 750 /usr/bin/dbmmanage
```

Per creare un username e una password occorre utilizzare il seguente comando:

```
/usr/bin/dbmmanage /etc/httpd/.dbmpasswd adduser <username>
```

Per eliminare un username e una password occorre utilizzare il seguente comando:

```
/usr/bin/dbmmanage /etc/httpd/.dbmpasswd delete <username>
```

Infine, per cambiare la password di un utente:

```
/usr/bin/dbmmanage /etc/httpd/.dbmpasswd update <username>
```

2.2 Modifica del file `httpd.conf`

Editare il file `httpd.conf` ed aggiungere le seguenti righe per proteggere una determinata directory web:

```
<Directory "/home/httpd/MyDir/private">
  Options None
  AllowOverride AuthConfig
  AuthName "Area Privata"
  AuthType Basic
  AuthDBUserFile /etc/httpd/.dbmpasswd
  require valid-user
</Directory>
```

Dove `/home/httpd/MyDir/private` è la directory da proteggere e il file `/etc/httpd/.dbmpasswd` contiene l'elenco degli username e password autorizzati.

2.3 Riavvio del web server Apache

Le modifiche apportate ai punti 2.1 e 2.2 devono essere attivate con un riavvio del web server. Il comando da usare è:

```
/etc/rc.d/init.d/httpd restart
```

oppure:

```
/usr/sbin/apachectl restart
```

3. Creazione di un ambiente di esecuzione “isolato” per il server Apache

In questa sezione verrà illustrato un sistema per evitare che l’ambiente di esecuzione di Apache possa essere utilizzato (in seguito ad un attacco) per ottenere accessi non autorizzati alla macchina che ospita il server web.

Un ambiente di esecuzione “isolato” (detto **chroot jail**) consente di limitare la porzione di file-system visibile dal daemon Apache. All’interno della chroot jail dovranno essere presenti solo ed esclusivamente i file necessari all’esecuzione di Apache (file di configurazione, file di log, eseguibili, librerie, pagine web, script, ecc.).

I passi da seguire per la configurazione di Apache in una chroot jail sono i seguenti:

3.1 Creazione dell’utente www

È necessario che l’esecuzione del web server Apache in una chroot jail avvenga con i privilegi di un utente fittizio. Pertanto è possibile creare un utente “www” con il seguente comando:

```
useradd -c "Apache Server" -u 80 -s /bin/false -r -d /home/httpd www
```

(assumendo che l’ UID 80 e il GID 80 non siano stati assegnati ad altri utenti).

3.2 Inizializzazione della chroot jail

Prima di tutto occorre stoppare il daemon Apache (se questo è in esecuzione):

```
/etc/rc.d/init.d/httpd stop
```

Creare la home directory della chroot jail:

```
mkdir /chroot/httpd
```

Creare le rimanenti directory:

```
mkdir /chroot/httpd/dev
mkdir /chroot/httpd/lib
mkdir -p /chroot/httpd/usr/sbin
mkdir -p /chroot/httpd/var/run
mkdir -p /chroot/httpd/var/log/httpd
chmod 750 /chroot/httpd/var/log/httpd
mkdir -p /chroot/httpd/home/httpd
```

Copiare i seguenti file nelle directory appena create:

```
cp -r /etc/httpd /chroot/httpd/etc
cp -r /home/httpd/cgi-bin /chroot/httpd/home/httpd
cp -r /home/httpd/html /chroot/httpd/home/httpd (*)
mknod /chroot/httpd/dev/null c 1 3
chmod 666 /chroot/httpd/dev/null
cp /usr/sbin/httpd /chroot/httpd/usr/sbin
```

(*) /home/httpd/html è la document root del web server

3.3 Copia dei file di supporto per SSL nella chroot jail

Se il server Apache è stato compilato con il supporto per SSL occorre copiare nella chroot jail l'intero contenuto della directory /etc/ssl:

```
cp -r /etc/ssl /chroot/httpd/etc
chmod 600 /chroot/httpd/etc/ssl/certs/ca.crt
chmod 600 /chroot/httpd/etc/ssl/certs/server.crt
chmod 600 /chroot/httpd/etc/ssl/private/ca.key
chmod 600 /chroot/httpd/etc/ssl/private/server.key
```

3.4 Copia delle librerie dinamiche usate da httpd nella chroot jail

Per localizzare le librerie dinamiche utilizzate dall'eseguibile httpd si può usare il seguente comando:

```
ldd /usr/sbin/httpd
```

Si otterrà un output del tipo:

```
libgdbm.so.2 => /usr/lib/libgdbm.so.2 (0x2aad1000)
libpthread.so.0 => /lib/libpthread.so.0 (0x2aad8000)
libm.so.6 => /lib/libm.so.6 (0x2aaef000)
libcrypt.so.1 => /lib/libcrypt.so.1 (0x2ab10000)
libdb-3.1.so => /lib/libdb-3.1.so (0x2ab3e000)
libmm.so.1 => /usr/lib/libmm.so.1 (0x2abbb000)
libdl.so.2 => /lib/libdl.so.2 (0x2abc0000)
libc.so.6 => /lib/libc.so.6 (0x2abc4000)
/lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x2aaab000)
```

Le librerie così identificate dovranno essere copiate nella chroot jail:

```
cp /usr/lib/libgdbm.so.2 /chroot/httpd/lib
cp /lib/libpthread.so.0 /chroot/httpd/lib
cp /lib/libm.so.6 /chroot/httpd/lib
cp /lib/libcrypt.so.1 /chroot/httpd/lib
cp /lib/libdb-3.1.so /chroot/httpd/lib
cp /usr/lib/libmm.so.1 /chroot/httpd/lib
cp /lib/libdl.so.2 /chroot/httpd/lib
cp /lib/libc.so.6 /chroot/httpd/lib
cp /lib/ld-linux.so.2 /chroot/httpd/lib
```

Inoltre dovranno essere copiate nella chroot jail le seguenti librerie aggiuntive:

```
cp /lib/libnss_compat* /chroot/httpd/lib
cp /lib/libnss_dns* /chroot/httpd/lib
cp /lib/libnss_files* /chroot/httpd/lib
```

3.5 Creazione dei file passwd e group nella chroot jail

Nella directory /chroot/httpd/etc creare il file passwd contenete l'unica entry:

```
www:x:80:80::/home/www:/bin/false
```

e il file group contenente l'unica entry:

```
www:x:80:
```

3.6 Copia dei file di configurazione di rete nella chroot jail

Copiare nella directory /chroot/httpd/etc i seguenti file:

```
cp /etc/resolv.conf /chroot/httpd/etc
cp /etc/hosts /chroot/httpd/etc
cp /etc/nsswitch.conf /chroot/httpd/etc
```

3.7 Impostazione dei flag di immutabilità

Per un maggiore livello di sicurezza è possibile attribuire il flag di immutabilità ai seguenti file di configurazione:

```
chattr +i /chroot/httpd/etc/passwd
chattr +i /chroot/httpd/etc/group
chattr +i /chroot/httpd/etc/httpd/conf/httpd.conf
chattr +i /chroot/httpd/etc/resolv.conf
chattr +i /chroot/httpd/etc/hosts
chattr +i /chroot/httpd/etc/nsswitch.conf
```

3.8 Copia del file `/etc/localtime` nella chroot jail

Affinché le date e gli orari degli eventi registrati nei log file siano coerenti con le impostazioni della propria “timezone” è necessario copiare nella chroot jail il file “localtime”:

```
cp /etc/localtime /chroot/httpd/etc/
```

3.9 Rimozione di file non necessari

I seguenti file non sono più necessari in quanto sono stati copiati nella chroot jail e quindi possono essere tranquillamente rimossi:

```
rm -rf /var/log/httpd
rm -rf /etc/httpd
rm -rf /home/httpd
rm -f /usr/sbin/httpd
```

3.10 Nuova impostazione del syslogd

Normalmente i processi “dialogano” con il syslogd attraverso il dispositivo virtuale “/dev/log”. Nella chroot jail questo dispositivo non esiste ma può essere creato modificando nello script di inizializzazione `/etc/rc.d/init.d/syslog` la linea:

```
daemon syslogd -m 0
in :
daemon syslogd -m 0 -a /chroot/httpd/dev/log
```

3.11 Modifica dello script di inizializzazione del server Apache

Editare il file `/etc/rc.d/init.d/httpd` e cambiare la linea:

```
daemon httpd
in:
/usr/sbin/chroot /chroot/httpd/ /usr/sbin/httpd
```

e la linea:

```
rm -f /var/run/httpd.pid
in:
rm -f /chroot/httpd/var/run/httpd.pid
```

3.12 Configurazione dello script di rotazione dei log

Editare il file `/etc/logrotate.d/apache` e cambiare ogni riferimento alla directory:

```
    /var/log  
in:  /chroot/httpd/var/log
```

3.13 Restart del syslogd e start del server Apache

Per attivare le modifiche apportate in precedenza occorre fare il restart del syslogd col comando:

```
/etc/rc.d/init.d/syslog restart
```

e far partire il server Apache col comando:

```
/etc/rc.d/init.d/httpd start
```