



Seguridad con Bastille

Filth (filth@tux.cl)

Bastille Linux no es una distribución de GNU/Linux. Es una serie de herramientas automatizadas, que su finalidad es configurar los servicios más cruciales de nuestro Linux, ayudando notablemente a la seguridad de éste.

1. Que es Bastille

Bien vamos por parte, primero que nada Bastille es un proyecto desarrollado por Jon Lasser en conjunto con Jay Beale. En definitiva es una suite de seguridad creada para sistemas Red Hat y Mandrake, también se puede utilizar en otros sistemas GNU/Linux, pero se pueden tener problemas con las paths.

Esta suite se encarga de securitizar nuestro Linux Box mediante scripts en sh y Perl, para este fin se usan módulos los cuales cumplen funciones tales como

- Configuración de Ipchains
- Establecer permisos sobre archivos
- Securitizar cuentas de usuario
- Securitizar el booteo del sistema
- Configuración de Inetd
- Deshabilitar compiladores para usuarios
- Configuración de PAM
- Activar y desactivar demonios
- Securitizar Send Mail
- Instalar SSH
- Securitizar Named
- Securitizar Apache
- Deshabilitar Impresoras
- Securitizar Ftpd
- Securitizar HP-UX
- Detector de scaneos de puertos

Para estos propósitos Bastille cuenta con 19 módulos. La configuración de Bastille se presenta mediante una interfaz en modo texto para consola.

1.1 Módulo Ipchains

Permite configurar scripts ipchains, servicios udp, tcp, icmp, métodos reject, permitir accesos con verificaciones de ip, requerimientos a interfaces DHCP.

1.2 Módulo Patch Download

Instala los últimos rpms actualizados de Bastille

1.3 Módulo File Permissions

Establece restricciones para utilidades de administración del sistema, quita modo SUID a ficheros con posible riesgos de seguridad.

1.4 Módulo Account Security

Crea cuentas con uid 0, deshabilita protocolos r, crea cuentas no root, restringe el uso de "cron" solo para cuentas de administradores de sistema.

1.5 Módulo Boot Security

Establece seguridad en el booteo, protege con password el LILO, reduce tiempos de espera para booteos en LILO, deshabilita reseteos mediante interrupción de teclado (CTRL-ALT-DEL), protege con password el nivel de inicio 1 (Single user mode: linux init 1).

1.6 Módulo Secure Inetd

Establece seguridad para inetd y optimiza hosts.allow para su uso con inetd, configura SSH para aceptar conexiones solo de una lista de ip.

1.7 Módulo User Tools

Deshabilita el uso de compiladores para usuarios que no tengan privilegios de administrador en el sistema.

1.8 Módulo Misc Pam

Limita el uso de procesos para usuarios, restringe la entrada a consolas, permitiendo el ingreso solo a ciertos grupos de cuentas de usuarios.

1.9 Módulo Logging

Permite logear a hosts remotos, mediante una cuenta de usuario.

1.10 Módulo MiscellaneousDaemons

Deshabilita demonios apdm, nfs, samba, atd, servicios pcmcia, dhcpd, gpm, news server, nis, snmpd.

1.11 Módulo Send Mail

Habilita a Send Mail para funcionar como demonio, deshabilita comandos VRFY y EXPN.

1.12 Módulo Remote Access

Baja e instala Secure Shell (SSH).

1.13 Módulo DNS

Deja chroot a named y quita SUID al demonio.

1.14 Módulo Apache

Deshabilita apache, desactiva Server Side Includes, CGI scripts e indexes.

1.15 Módulo Printing

Deshabilita el demonio de impresion.

1.16 Módulo FTP

Utilizable solo para Wu-FTPD (por sus problemas de seguridad). Deshabilita la cuenta ANONYMOUS y quita privilegios de ejecución para este demonio.

1.17 Módulo PSAD (Port Scan Attack Detector)

Modulo PSAD (Port Scan Attack Detector)

1.18 Módulo HP-UX

1.19 Módulo HP-API

Estos modulos son betas de la version 1.3.0. Estos modulos hacen hardening en sistemas HP-UX.

2. Instalación

Todos los módulos mencionados anteriormente cuentan con la extensión *.pm y se encuentran en /usr/lib/Bastille/.

La instalación de Bastille es sumamente simple, se procede a descomprimir el archivo en un directorio y luego se ejecuta un script en perl, el cual inicia el UI (User Interface). El funcionamiento de Bastille requiere de 3 archivos:

Bastille-1.3.0.tar.bz2

En el caso de usar Bastille en modo texto:

```
Bastille-Curses-module-1.2.0-1.1mdk.noarch.rpm  
perl-Curses-1.05-10.i386.rpm
```

O en el caso de usar Bastille en modo grafico para X Windows

```
Bastille-Tk-module-1.2.0-1.1mdk.noarch.rpm  
perl-Tk-800.022-11.i386.rpm
```

Instalando Bastille:

```
$ ls  
Bastille-1.3.0.tar.bz2  
Bastille-Curses-module-1.2.0-1.1mdk.noarch.rpm  
perl-Curses-1.05-10.i386.rpm  
Bastille-Tk-module-1.2.0-1.1mdk.noarch.rpm  
perl-Tk-800.022-11.i386.rpm  
  
$ tar xvj Bastille-1.3.0.tar.bz2  
  
$ rpm -ivh Bastille-Curses-module-1.2.0-1.1mdk.noarch.rpm  
  
$ rpm -ivh perl-Curses-1.05-10.i386.rpm  
  
$ tar xpvf Bastille-1.3.0.tar  
  
$ cd Bastille  
  
$ sh Install.sh --> Instala Bastille en las determinadas Paths  
  
$ ./InteractiveBastille --> ejecutar el script InteractiveBastille  
  
Usage: InteractiveBastille [ -x | -c ] [--norequires]  
-x : use the Perl/Tk (X11) GUI  
-c : use the Curses (non-X11) GUI  
--norequires : ask all questions, even ones that do not apply to the current system configuration
```

Claramente podemos apreciar que se dan las opciones tanto para modo texto como para X Windows.

Modo Texto :

```
./InteractiveBastille -c
```

Modo Gráfico :

```
./InteractiveBastille -x
```

Bien con esto se inicia la configuración de Bastille en nuestro equipo.

La configuración es bastante simple, solo con responder "yes" o "no", además de algunas paths y nombres de usuarios tendremos configurado Bastille en nuestro equipo. Ahora si se desea desinstalar Bastille existe un script para ese fin, se llama "UndoBastille" y se encuentra en <http://www.bastille-linux.org/UndoBastille>

3. Cual es la idea de usar Bastille, si todo lo puedo hacer a mano?

La única razón sería por tiempo, ya que muchos admin nunca andan con tiempo, o simplemente no se quieren dar la tarea de hacer todo a mano, además para algunos usuarios resulta muy cómodo usar Bastille, por lo versátil que es este.

