

**CAPÍTULO 6**  
**PRÁCTICA**  
**REFORZAMIENTO DE LA**  
**SEGURIDAD CON BASTILLE**  
**(*HARDENING*)**



## PRÁCTICA, REFORZAMIENTO DE LA SEGURIDAD CON BASTILLE (*HARDENING*)

### 1.- OBJETIVOS DE APRENDIZAJE

Al terminar esta práctica, el alumno:

- Comprenderá la importancia de la herramienta de seguridad Bastille Linux, para el reforzamiento del sistema operativo.
- Será capaz de realizar la instalación de Bastille Linux.
- Podrá configurar Bastille Linux para reforzar el sistema operativo de acuerdo con las políticas de seguridad que requiera.

### 2.- Conceptos teóricos

Bastille Linux es una herramienta de seguridad para el reforzamiento del sistema operativo. Se trata de un conjunto de secuencias de comandos que permiten realizar la configuración del sistema de manera simplificada, de manera que podemos obtener que nuestro sistema operativo sea lo menos vulnerable posible. Mediante una buena configuración de Bastille Linux se pueden eliminar un gran número de vulnerabilidades comunes en plataformas Linux/Unix.

De manera interactiva Bastille Linux crea una configuración segura para el sistema basado en las respuestas del usuario.

Con Bastille se pueden realizar cuatro pasos para asegurar el sistema:

- 1 Aplicar un *firewall* para prevenir el acceso a posibles servicios vulnerables.
- 2 Aplicar actualizaciones para los agujeros de seguridad conocidos.
- 3 Realizar un SUID, root audit (establecer permisos de acceso a archivos y directorios).
- 4 Desactivar o restringir servicios innecesarios.

Los anteriores pasos se subdividen en módulos que cubren cada una de las áreas anteriormente descritas.

- Módulo *ipchains*: permite la configuración de un *firewall* para filtrar el tráfico y así proteger la red.

- Módulo patch download: ayuda a mantener actualizados los servicios que se usan en el servidor. Lo más importante es aplicar actualizaciones a los agujeros de seguridad conocidos.
- Módulo file permissions: este módulo permite realizar una auditoría sobre los permisos de archivos en el sistema. Restringe o habilita permisos para el uso de servicios y archivos binarios.
- Módulo account security: con este módulo se obliga al administrador a tener “buenas prácticas” en el manejo de cuentas, además de que provee algunos trucos para realizar de una manera más efectivo el manejo de cuentas.
- Módulo boot security: en este módulo podemos habilitar ciertas opciones de arranque para hacerlo más seguro y evitar que sean aprovechadas las vulnerabilidades inherentes a los sistemas operativos tipo Linux/Unix.
- Módulo secure inetd: con este módulo podemos deshabilitar servicios que podrían significar una vulnerabilidad grave al poder ser iniciados con privilegios de root. En caso de que no se pueda deshabilitar dichos servicios por ser necesarios para los usuarios o para el sistema, entonces se restringen los privilegios. En este caso se recomienda deshabilitar telnet, ftp, rsh, rlogin y talk. Pop e imap son protocolos de correo que deben ser deshabilitados únicamente si no se requieren en el sistema.
- Módulo disable user tools: en este módulo podemos restringir el uso del compilador para que únicamente sea accesible para el usuario root.
- Módulo configure misc pam: partiendo de la idea de que un servidor debe tener únicamente los servicios y herramientas necesarias, en este módulo se pueden hacer ciertas modificaciones que harán difícil a los usuarios, incluidos los usuarios “nobody”, “web” y “ftp”, que abusen de los recursos para producir un ataque de *denegación de servicios*.
- Módulo logging: aquí manejamos y configuramos las bitácoras adicionales que contienen información del sistema, mensajes del kernel, mensajes de errores graves, etc.
- Módulo miscellaneous daemons: en este módulo se desactivan todos los demonios del sistema que no sean necesarios, los cuáles se pueden volver a activar con el comando chkconfig.
- Módulo sendmail: permite deshabilitar comandos sendmail que son usados para obtener información acerca del sistema para realizar cracking o spamming.

- Módulo remote access: el acceso remoto se puede configurar de manera que se realice mediante *secure shell* client, un programa seguro de cifrado de información.
- Los módulos dns, *apache*, printing y ftp permiten configurar cada uno de los servicios que previamente se han asegurado en caso de que no se haya deshabilitado y establecer cierta seguridad en la forma de levantar dichos servicios.

Todos los módulos mencionados anteriormente se establecen al momento de responder a las preguntas que el script de Bastille realiza al ejecutarse, por lo que se simplifica la tarea de configuración de esta herramienta, sin embargo, es muy importante contestar dicho cuestionario de acuerdo con las políticas de seguridad establecidas por cada institución. En este caso se consideran los aspectos que generalmente se aseguran en un sistema tipo Linux, multiusuario y con características de servidor web.

### 3.- MATERIAL NECESARIO

Computadora con sistema operativo Linux con alguno de los siguientes sistemas operativos soportados por bastille:

LINUX:

'DB2.2' 'DB3.0' 'RH6.0' 'RH6.1' 'RH6.2'  
'RH7.0' 'RH7.1' 'RH7.2' 'RH7.3' 'RH8.0'  
'RH9' 'RHEL5' 'RHEL4AS' 'RHEL4ES' 'RHEL4WS'  
'RHEL3AS' 'RHEL3ES' 'RHEL3WS' 'RHEL2AS' 'RHEL2ES'  
'RHEL2WS' 'RHFC1' 'RHFC2' 'RHFC3' 'RHFC4'  
'RHFC5' 'RHFC6' 'RHFC7' 'RHFC8' 'MN6.0'  
'MN6.1' 'MN7.0' 'MN7.1' 'MN7.2' 'MN8.0'  
'MN8.1' 'MN8.2' 'MN10.1' 'SE7.2' 'SE7.3'  
'SE8.0' 'SE8.1' 'SE9.0' 'SE9.1' 'SE9.2'  
'SE9.3' 'SE10.0' 'SE10.1' 'SE10.2' 'SE10.3'  
'SESLES8' 'SESLES9' 'SESLES10' 'TB7.0'

Donde DB significa Debian, RH Red Hat, RHEL Red Hat Enterprise Linux, RHFC Red Hat Fedora Core, MN Mandriva, SE SUSE, SESLES SUSE Linux Enterprise Server.

Privilegios para realizar la instalación en dicho equipo, archivo Bastille-x.x.x.tar.bz2.

### 4.- DESARROLLO

#### 4.1 Modo de trabajo

Al principio se revisará el estado de algunos elementos importantes del sistema operativo antes de ejecutarse Bastille, posteriormente se ejecutará Bastille y se realizará la configuración recomendada más adelante en esta práctica. Finalmente se comprobará que se hayan realizado los cambios de acuerdo con la configuración realizada.

#### 4.2 Revisión del estado del sistema.

Abra una terminal o Shell (Main Menu, System Tools=> Terminal), y ejecute los siguientes comandos:

```
ls -l /bin/mount
```

```
-rwsr-xr-x 1 root root 52012 abr 6 2007 /bin/mount
```

```
ls -l /bin/ping
```

```
-rwsr-xr-x 1 root root 36140 abr 6 2007 /bin/ping
```

```
ls -l /usr/bin/at
```

```
-rwsr-xr-x 1 root root 45380 mar 27 2007 /usr/bin/at
```

Lo que se puede ver tras la ejecución del comando “ls” en los tres casos es los comandos mount, ping y at tienen el bit SUID activado. Este bit permite a un programa ser ejecutado por un usuario con los permisos de superusuario. Si bien se tiene una mejora por la facilidad de uso, esto reduce la seguridad, ya que algún usuario podría adquirir los derechos de superusuario sin estar autorizado. Se sugiere eliminar este ya que representa un problema de seguridad.

Otros programas que se consideran inseguros son rcp, rlogin, rsh, debido a que no cifran los datos que envían a través de la red y utilizan como método de autenticación únicamente la dirección IP, algo que se considera inadecuado. Al listar los comandos de dichos programas se puede observar que también tienen activado el bit SUID.

```
ls -l /usr/bin/rlogin
```

```
-rwsr-xr-x 1 root root 14388 abr 11 2007 /usr/bin/rlogin
```

```
ls -l /usr/bin/rsh
```

```
-rwsr-xr-x 1 root root 8940 abr 11 2007 /usr/bin/rsh
```

```
ls -l /usr/bin/rcp
```

```
-rwsr-xr-x 1 root root 18640 abr 11 2007 /usr/bin/rcp
```

```
ls -l /usr/bin/rexec
```

```
-rwsr-xr-x 1 root root 14300 abr 11 2007 /usr/bin/rexec
```

Otro factor importante es la máscara de usuario (umask), una función que establece los permisos por defecto para los nuevos archivos y directorios creados. Se puede ver la

máscara establecida al ejecutar el comando `umask`, en este caso la máscara es `0022`, lo que nos dice que los nuevos archivos y directorios creados tendrán permisos `755`.

```
umask  
0022
```

Ahora ejecute el comando `ulimit` para verificar el número de procesos que puede ejecutar un usuario.

```
ulimit  
unlimited
```

Esto también representa una vulnerabilidad ya que se puede ejecutar un ataque de *denegación de servicios* para colapsar el sistema.

Los aspectos analizados anteriormente son una pequeña parte del *hardening* (reforzamiento de la seguridad) que se debe realizar en el sistema. En Linux, esto se realiza mediante el uso de comandos y la edición de los archivos de configuración correspondiente; con Bastille Linux ya no es necesario saber exactamente que comando hay que ejecutar y que archivos modificar para asegurar el sistema, esto representa una gran ventaja si se sabe que realiza Bastille al aplicar la configuración del sistema.

### 4.3 Instalación de Bastille Linux

Encienda la computadora y elija arrancar con el sistema operativo Linux.

- Abra una terminal o Shell (Main Menu, System Tools=> Terminal)

Se requieren permisos de administrador para hacer la instalación de Bastille por lo que ejecutaremos el siguiente comando:

```
su - root
```

ahora ingresaremos la contraseña proporcionada por el profesor.

- A continuación usamos el comando `yum` (Yellow Dog Updater Modified), una herramienta para el manejo de paquetes en Linux, para instalar `perl-Curses` y `perl-TK`, dos librerías que nos permiten crear interfaces basadas en texto e interfaces gráficas. Ejecuté los siguiente comandos:

```
yum install perl-Curses*
```

```
yum install perl-Tk*
```

- En seguida copiamos el archivo de Bastille al directorio `/usr/local`, lo descomprimos y realizamos su instalación con los siguientes comandos:

```
bzip2 -d Bastille-x.x.x.tar.bz2
```

```
tar xvf Bastille-x.x.x.tar
```

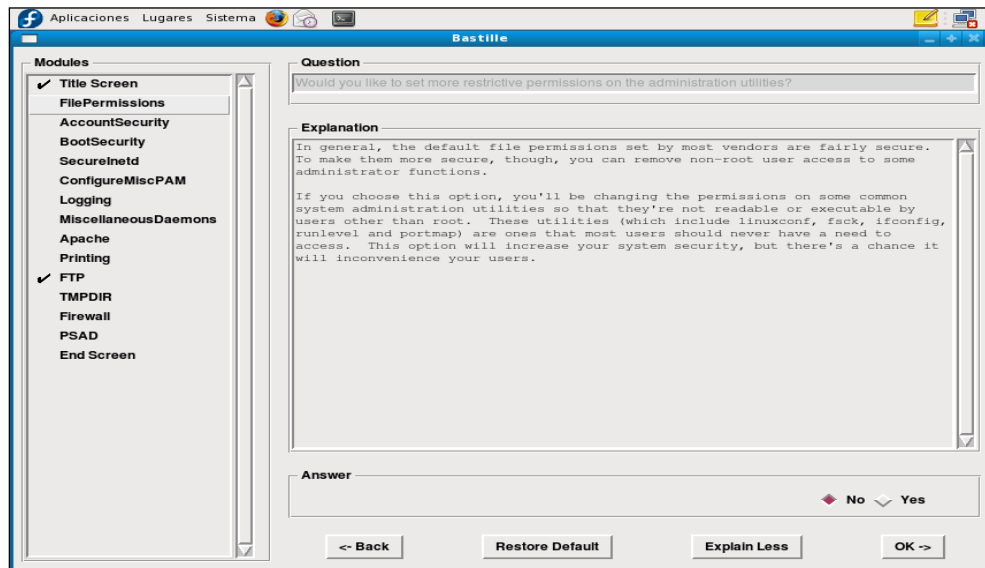
```
cd Bastille
```

```
sh Install.sh
```

```
bastille -x
```

```
accept
```

- Al ejecutar el comando “bastille -x” se abre la interfaz de configuración de Bastille Linux y podemos comenzar a configurar Bastille Linux, figura 6.1.



6.1, Configuración de Bastille Linux

En esta práctica se realizará la configuración de Bastille para asegurar el sistema operativo sin incluir la configuración del *firewall*, ya que se considera que el *firewall* es una parte del sistema de defensa tan importante que requiere una instalación y configuración independiente.

Ahora, por cada pregunta que nos presenta Bastille Linux, tenemos que ingresar una respuesta del tipo “Y” (si) o “N” (no), lo cual haremos a continuación, además, se deben completar las razones por las cuáles se responde Y o N, en su caso, donde aparezca la línea continúa:

## FILE PERMISSSIONS

- ***Would you like to set more restrictive permissions on the administration utilities? [N]***

Útil en máquinas con múltiples cuentas de usuario pero en este caso se trata de una máquina dedicada para establecer el sistema de seguridad.

- ***Would you like to disable SUID status for mount/umount? [Y]***
- ***Would you like to disable SUID status for ping? [Y]***
- ***Would you like to disable SUID status for at? [Y]***

Se deshabilitarán los programas SUID para evitar que usuarios sin privilegios ejecuten programas con permisos de administrador. El atributo setuid es un permiso que se asigna a archivos o directorios, para ser ejecutados por los usuarios del sistema con privilegios elevados temporalmente, para hacer una tarea específica.

- ***Would you like to disable the r-tools? [Y]***

r-tools son un conjunto de utilidades para la administración remota de equipos que usan las direcciones IP como método de autenticación y no usan encriptación para el intercambio de información.

- ***Would you like to disable SUID status for usernetctl? [Y]***

## ACCOUNT SECURITY

- ***Should Bastille disable clear-text r-protocols that use IP-based authentication? [Y]***

Las llamadas r-tools son un conjunto de utilidades para la administración remota de equipos. El problema con ellas es que no usan encriptación para el intercambio de datos y usan las direcciones IP como método de autenticación. Esta carencia de confidencialidad y la facilidad para falsificar las direcciones IP de origen han llevado a que se desaconseje el uso de las r-tools y se usen en su lugar alternativas más seguras.

- ***Would you like to enforce password aging? [Y]***

Se habilitará un tiempo de caducidad para las contraseñas, por default 180 días. Se deberá cambiar la contraseña antes de este plazo, de otra forma la cuenta será bloqueada.

- ***Do you want to set the default umask? [Y]***



El umask son los permisos por defecto que el sistema asigna a los archivos que se van creando.

- ***What umask would you like to set for users on the system? [077]***

Continuación de la pregunta anterior, lo mejor es usar la opción **077** para que únicamente el dueño de los archivos y nadie más pueda escribir o leer sobre ellos.

- ***Should we disallow root login on ttys 1-6 ? [N] -***

Esta opción es extremadamente útil con equipos a los que se pueda acceder por SSH sin limitación en cuanto a la IP de origen. En este caso no se limitará el acceso ya que se considera que la configuración del SSH lo contempla.

## BOOT SECURITY

- ***Would you like to password-protect the GRUB prompt? [N]***

Si se tiene acceso físico al equipo cualquier persona podría reiniciar el equipo y obtener una consola de administrador pasándole ciertos parámetros al GRUB, por lo que se debe proteger con una contraseña. Para efectos de la práctica responderemos con [N].

- ***Would you like to password protect single-user mode? [N]***

Este modo (mono-usuario) permite arrancar el sistema de manera que solamente puede acceder el administrador del equipo. Generalmente no solicita autenticación por lo que se recomienda proteger este modo mediante una contraseña.

En esta práctica responderemos con [N].

## SECURE INETD

- ***Would you like to set a default-deny on TCP Wrappers and xinetd? [N]***

Se permitirá que se ejecuten estos servicios de conectividad a internet.

TCP Wrappers es un sistema que se usa para filtrar el acceso de red a servicios de protocolos de Internet. Xinetd es un servicio de Linux que sirve para administrar la conectividad basada en Internet.

- ***Should Bastille ensure the telnet service does not run on this system? [Y]***

Se desactivará el servicio telnet ya que es obsoleto y supone un riesgo grave de seguridad del sistema al transmitir datos sin cifrarlos.

- ***Should Bastille ensure inetd's FTP service does not run on this system? [Y]***

Lo mismo que telnet, ftp es un servicio inseguro, por lo que se deshabilitará.

- ***Would you like to display "Authorized Use" messages at log-in time? [N]***

Esta opción se puede activar para mostrar un mensaje con las restricciones para uso del sistema.

Si la respuesta fuera [Y] Bastille preguntará el nombre del responsable del uso del equipo, con lo que creará un mensaje que se alojará en /etc/issue, mensaje que se puede modificar de acuerdo con las especificaciones de la organización a la que pertenece el equipo que se está configurando.

#### CONFIGURE MISCPAM

- ***Would you like to put limits on system resource usage?[Y]***

Con esta medida establecemos un límite de 150 procesos por usuario, suficiente para trabajar y evita un ataque por denegación de servicio.

AL DAR CLICK EN OK => System resource limits have been set in the file /etc/security/limits.conf, which you can edit later as necessary.

- ***Should we restrict console access to a small group of user accounts? [N]***

Permite denegar el acceso a la consola excepto a un grupo determinado de cuentas.

- ***Would you like to add additional logging? [N]***

Aunque no representa un peligro tener dos registros adicionales, no se considera necesario en este equipo.

#### LOGGING

- ***Do you have a remote logging host? [N]***

Solo se activa en caso de tener un host remoto.

- ***Would you like to set up process accounting? [N]***

Esta opción permite establecer la contabilidad de procesos y saber quién ejecutó cierto proceso y cuando, aunque parece útil esto puede consumir muchos recursos del sistema y crear bitácoras muy grandes en poco tiempo.

#### MISCELLANEOUS DAEMONS

- ***Would you like to deactivate NFS and Samba? [Y]***

El Network File System (Sistema de archivos de red), o NFS, es un protocolo utilizado para sistemas de archivos distribuidos. Posibilita que distintos sistemas conectados a una misma red accedan archivos remotos como si se tratara de locales. Samba es una implementación libre del protocolo de archivos compartidos de Windows, antiguamente llamado SMB, fue renombrado recientemente para sistemas de tipo Unix.

- ***Would you like to deactivate the HP OfficeJet (hpoj) script on this machine? [Y]***

Este script inicia el sistema de soporte en Linux para los dispositivos HP all in one.

- ***Would you like to deactivate ISDN script on this machine? [Y]***

ISDN es un método para conectar equipos a Internet, con una velocidad de 128 kbps ha sido sustituido por IDSL otro tipo de conexión más rápida.

#### APACHE

- ***Would you like to deactivate the Apache web server? [N]***

En este responderemos con N, pero si el equipo no se utiliza como servidor web debe deshabilitarse.

Se puede habilitar nuevamente con el comando `/sbin/chkconfig httpd on`

- ***Would you like to bind the Web server to listen only to the localhost? [N]***

Esto es muy útil cuando se hace desarrollo web, ya que permite editar un sitio web localmente antes de que se cargue en otro servidor.

- ***Would you like to bind the Web server to a particular interface? [N]***

En caso de que se permita el acceso al servidor web únicamente a la red interna se tiene que contestar [Y] e ingresar la ip del equipo que se quiere asociar y el puerto que debe escuchar.

- ***Would you like to deactivate the following of symbolic links? [Y]***

En general trataremos de limitar la información del servidor web que puede ser vista por los usuarios. Al desactivar la opción de seguimiento de ligas simbólicas se previene el que un visitante web pueda leer o modificar archivos que no se encuentran en el directorio de publicación web.

#### TMPDIR

- ***Would you like to install TMPDIR/TMP scripts? [N]***

Esto nos permitiría crear directorios temporales alternativos al directorio /tmp con la ventaja de ejecutar scripts cuando los usuarios accedieran a dichos directorios.

Activar esta opción hará que Bastille instale unos scripts en las cuentas de los usuarios que configuren las variables TMPDIR y TMP de tal manera que utilicen directorios de ficheros temporales completamente individuales, en vez de que todos usen el /tmp lo que puede ser extremadamente peligroso en entornos multiusuarios.

#### PRINTING

- ***Would you like to disable printing? [Y]***

No usaremos impresoras en este equipo por lo tanto deshabilitamos las funciones de impresión, ya que dejarlas activas supone un riesgo de seguridad.

Esto se puede revertir con los siguientes comandos:

```
/bin/chmod 06555 /usr/bin/lpr /usr/bin/lprm
```

```
/sbin/chkconfig lpd on
```

- ***Would you like to disable CUPS'legacy LPD support? [N]***

Para efectos de la práctica contestaremos [N], pero si el equipo realizará funciones de impresión, se puede deshabilitar el soporte para el protocolo LPD del sistema de impresión común de Unix.

#### FTP

## FIREWALL

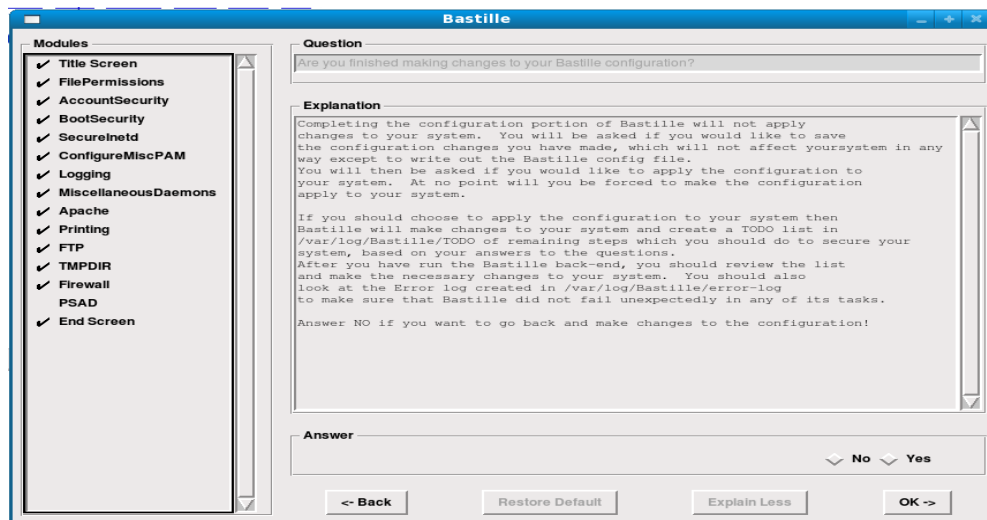
- *Would you like to run the packet filtering script? [N]*

Esta opción activaría el *firewall* nativo de Linux, en este caso no se activará porque se recomienda que el *firewall* se configure por separado y con otras herramientas específicas para la configuración del mismo.

- *Are you finished answering the questions, i.e. may we make the changes? [Y]*

Respondemos afirmativamente para que se apliquen los cambios en el sistema.

Guardar la configuración y después aplicarla al sistema, figura 6.2.



6.2, Guardar configuración.

Se ha terminado de configurar Bastille Linux, además de aplicarse los cambios en el sistema operativo.

Ahora con una cuenta de usuario sin privilegios probaremos que la configuración anterior funciona correctamente, en este caso probaremos ciertos puntos en el sistema operativo, que deben estar protegidos por la configuración hecha con Bastille Linux:

Los comandos mount, ping y at no deben tener activo el bit SUID

```
ls -l /bin/mount
```

```
-rwr-xr-x 1 root root 52012 abr 6 2007 /bin/mount
```

```
ls -l /bin/ping
```

```
-rwr-xr-x 1 root root 36140 abr 6 2007 /bin/ping
```

```
ls -l /usr/bin/at
```

```
-rwr-xr-x 1 root root 45380 mar 27 2007 /usr/bin/at
```

Otros programas que inseguros como rcp, rlogin, rsh también deben tener desactivado el bit SUID.

```
ls -l /usr/bin/rlogin
```

```
-rwr-xr-x 1 root root 14388 abr 11 2007 /usr/bin/rlogin
```

```
ls -l /usr/bin/rsh
```

```
-rwr-xr-x 1 root root 8940 abr 11 2007 /usr/bin/rsh
```

```
ls -l /usr/bin/rcp
```

```
-rwr-xr-x 1 root root 18640 abr 11 2007 /usr/bin/rcp
```

```
ls -l /usr/bin/rexec
```

```
-rwsr-xr-x 1 root root 14300 abr 11 2007 /usr/bin/rexec
```

La máscara de usuario (umask), función que establece los permisos por defecto para los nuevos archivos y directorios creados debe tener el nuevo valor (077)

```
umask
```

```
0077
```

El número de procesos por usuario debe estar restringido a 150, y eso se comprueba con el comando ulimit.

```
ulimit -a
```

```
max user processes (-u) 150
```

Por lo que el sistema se encuentra protegido si un ataque de saturación de buffer o *denegación de servicios* intenta hacer una replicación infinita de procesos.

El reforzamiento de la seguridad con Bastille Linux se debe verificar en otros aspectos que en este caso no fueron analizados, para ello es necesario saber que archivos se van a modificar o que comandos se ejecutarán mediante la configuración hecha con este programa, pero al revisar estos aspectos básicos podemos darnos una idea de las ventajas de utilizar un software de este tipo.

## 5.- CUESTIONARIO

- 1.- ¿Cuáles son los cuatro pasos que se pueden hacer con Bastille para asegurar el sistema operativo?
- 2.- ¿Qué son las r-tools y qué método de autenticación utilizan?
- 3.- ¿Qué problema de seguridad presenta el servicio Telnet?
- 4.- ¿Por qué es importante establecer un límite de procesos que puede ejecutar un usuario?
- 5.- ¿Cuál es la ventaja de utilizar Bastille para asegurar el sistema operativo?

## 6.- CUESTIONARIO PREVIO

- 1.- Investigue ¿Qué medidas para reforzar un sistema operativo tipo Linux existen?
- 2.- ¿Qué función tiene el comando “umask”?  
¿qué permisos se deben establecer en un sistema para que se considere seguro?
- 3.- ¿Qué servicios remotos se consideran inseguros en un sistema tipo Linux y por qué?
- 4.- ¿Qué es la denegación de servicios?
- 5.- Investigue ¿Qué herramientas para el reforzamiento del sistema operativo conoce y cuáles son sus características?