Deploy de Servidores Web con **Jack The Stripper v 2.7**

JackTheStripper v 2.7 (estable)
Autor: Eugenia Bahit <eugenia.bahit@laeci.org>
Licencia: GNU GPL v3.0
Plataforma: Debian 7.x

Resumen
JackTheStripper es una herramienta que facilita la instalación, configuración, optimización y aseguramiento de sistemas operativos Debian 7.x destinados a funcionar como servidores Web. El fuerte de JacTheStripper se encuentra en las medidas de seguridad que configura e implementa.

Tareas que realiza JackTheStripper

1. Configuración de Hostname (opcional)
2. Configuración de zona horaria
3. Actualización del sistema
4. Creación de un nuevo usuario
5. Configuración de acceso remoto por SSH para el nuevo usuario, mediante llave de acceso RSA
6. Aseguramiento del servidor OpenSSH
7. Asignación manual de puerto para conexiones SSH
8. Configuración del firewall iptables
9. Creación de demonio de recuperación de reglas de iptables para el arranque del sistema
10. Instalación y configuración de fail2ban para prevención de ataques por fuerza bruta
11. Instalación, configuración y optimización del servidor de bases de datos MySQL
12. Instalación, configuración y optimización del servidor Web Apache
13. Instalación, configuración y optimización de PHP
14. Instalación del módulo de seguridad para Apache, ModSecurity
15. Instalación de la batería de reglas de seguridad de OWASP para ModSecurity
16. Instalación y configuración de ModEvasive para prevención de ataques de denegación de servicio (DoS)
17. Instalación de paquetes adicionales para desarrolladores:
    1. Sistema de control de versiones para deploy de aplicaciones Web (Bazaar)
    2. Driver MySQL para Python (python-mysqldb)
    3. Módulo de Apache WSGI para aplicaciones Web Python
    4. PIP (Python Package Index)
    5. Vim, optimizado para trabajar como IDE
    6. Framework para pruebas unitarias en PHP, PHP Unit
    7. CLI alternativo para PHP (phpcli)
18. Optimización de la shell de GNU Bash
19. Precarga optimizada de los archivos de configuración de Vim, Nano y GNU Bash en /etc/skel (para que al crear nuevos usuarios, conserven todas las plantillas de configuración y la optimización de los programas)
20. Agregado de tarea de actualización diaria del sistema en el crontab
21. Instalación y configuración de PortSentry (detector y bloqueador de escaneos de puerto)
22. Creación de comando para bloqueo y desbloque manual de Ips (blockip y unblockip)
23. Creación de comando para montaje rápido, seguro y optimizado de VirtualHosts de Apache
24. Aseguramiento del Kernel contra ataques de red (aporte de Jason Soto)
25. Instalación opcional de NewLab, herramienta para montaje de laboratorios chroot enjaulados (aporte de Marcos Leal Sierra)

Herramientas propias incorporadas por JackTheStripper

phpcli

CLI alternativo para PHP. Su principal característica es que acumula las instrucciones en una pila que puede ser ejecutada o editada en cualquier momento.

Autor: Eugenia Bahit <http://www.eugeniabahit.com>

Uso:

```
phpcli
```

Comandos internos:

```
h, -h, --help    Muestra ayuda en pantalla
_                Ejecuta la pila
.                Vacía la pila
:                Muestra la pila y permite eliminar elementos
q                Sale del programa
> FILENAME       Exporta la pila al archivo FILENAME
< FILENAME       importa un archivo FILENAME a la pila
```

Atajos de teclado disponibles:

```
<Ctrl><l>        Limpia la pantalla
<Ctrl><r>        Busca una instrucción en el historial
```

vhostadd

Creación de nuevo VirtualHost de Apache. Crea la estructura de directorios, el repositorio y VirtualHost para una nueva aplicación Web, en el directorio /srv/websites

Autor: Eugenia Bahit <http://www.eugeniabahit.com>

Uso:

```
vhostadd -s <servername> [-l <php|python>]
```

Para más ayuda visite la página man:

```
man vhostadd
```

blockip

Permite un bloqueo rápido y permanente de forma manual de una IP atacante

Autor: Eugenia Bahit <http://www.eugeniabahit.com>

Uso:

```
blockip IP
```

Para más ayuda visite la página man:

```
man blockip
```

unblockip
Permite el desbloqueo manual de una dirección IP previamente bloqueada.

Autor: Eugenia Bahit <http://www.eugeniabahit.com>

Uso:
```
unblockip IP
```

Para más ayuda visite la página man:
```
man unblockip
```

NewLab
Herramienta para montaje de jaulas chroot diseñadas para el deploy y mantenimiento de aplicaciones Web independientes mediante Bazaar habilitando acceso remoto por SSH mediante llave RSA.

Con NewLab es posible crear un nuevo usuario enjaulado con todo el entorno necesario para que monte y administre su propia aplicación Web, dentro de una jaula chroot que oculta el verdadero filesystem al usuario.

Autor: Marcos Leal Sierra <http://marcos.laeci.org>

Uso:
```
newlab USUARIO php|python
rmlab USUARIO
```

Argumentos:
```
USUARIO          El nuevo del nuevo usuario enjaulado a crear
php              Crea un VirtualHost para montar una aplicación Web
                 con el módulo PHP de Apache
python           Crea un VirtualHost para montar una aplicación Web
                 con el módulo WSGI de Apache
```

Obtener JackTheStripper
Las versiones oficiales de JackTheStripper se encuentran disponibles en el FileServer de LAECI: http://bit.ly/JackTheStripperOficial

Instalar un servidor con JackTheStripper:
1. Descargue la versión de JackTheStripper desde http://bit.ly/JackTheStripperOficial

2. Descomprima el archivo: `tar -xzvf <archivo>`
   ```
   tar -xzvf jackthestripper2_7-for-debian-7_official-version.tar.gz
   ```

3. Ingrese en la carpeta donde se han descomprimido los archivos:
   ```
   cd jts-debian-7
   ```

4. Ejecute el archivo `dms.sh`
   En modo principiante: `./dms.sh`
   En modo avanzado (solo administradores de sistemas): `./dms.sh –custom`
   (en el modo pausa, elija 'off' para ejecutar el script sin interrupciones u 'on' para hacerlo con pausas step-by-step)

PROBLEMAS COMUNES

En el paso 5, el script le dará instrucciones precisas para:

1. Generar una llave RSA en su equipo local
2. Enviar la llave RSA desde su equipo local al servidor remoto

Habitualmente, el envío de la llave RSA falla por omisión del carácter final del comando scp. Note que la instrucción para copiar archivos con el comando scp finaliza con dos puntos. Si olvida copiar los dos puntos finales, la llave RSA se copiará localmente en su propio equipo y no será enviada al servidor. Esto le impedirá volver a conectarse al servidor.

Ejemplo de instrucción de copiado con scp:

```
scp archivo-origen usuario@123.456.78.90:
```

Note los **dos puntos** del final. No olvide **copiarlos**. Si no copia los dos puntos rojos, perderá el acceso al servidor.