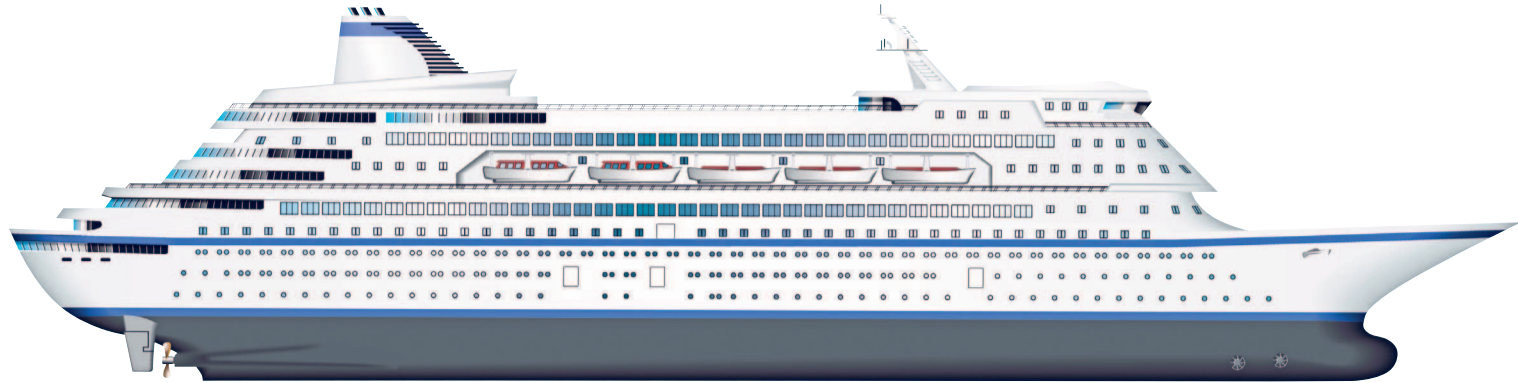


## Análisis e Informes de Problemas de Seguridad con Security Blanket

## A RAYA



Security Blanket permite analizar problemas de seguridad en unos cuantos pasos sencillos.

**POR KURT SEIFRIED**

No le conozco, pero me paso más tiempo asegurando mis servidores y asegurándome de que estén seguros del que me gustaría. Al menos una vez, hace tiempo (que yo supiera), uno de ellos estuvo comprometido. Cometí el fallo de: a) actualizar WordPress y b) asegurarme de que mi servidor estuviese seguro de modo que el acceso local no permitiese que un atacante pudiese adquirir privilegios fácilmente. El problema no era que no supiese asegurar mis servidores o que no tuviese el tiempo para ello; tenía otras cosas que hacer, e intentar llevarlo todo para adelante y mantener mi servidor seguro no es precisamente el concepto que tengo de diversión.

De modo que, ¿qué se supone que tenía que hacer yo, o cualquier otro administrador, si tenía docenas o cientos de servidores que asegurar con distintos niveles de seguridad, a los que había que aplicarles las actualizaciones, instalarles nuevo software y lidiar con los problemas básicos del día a día? Y ¿qué hay de los administradores que tienen que lidiar con estándares de seguridad como PCI-DSS o los diversos estándares gubernamentales (que son mucho menos divertidos que la lectura de los RFCs)?

### Security Blanket

Security Blanket [1] es un software de Trusted Computer Solutions, una empresa con un largo historial de trabajo en campos gubernamentales y de seguridad. La premisa básica de Security Blanket es que las herramientas automáticas facilitan la adhesión a las reglas, y las herramientas automáticas que saben a lo que necesitamos adherirnos, lo facilitan todo aún más. Security Blanket emplea un modelo cliente-consola (pueden ser múltiples consolas) que permite trabajar tanto con una máquina como con muchas de ellas (se recomienda un máximo de 1000 por consola). Conceptualmente, Security Blanket es muy similar a Puppet [2]; posee un canal de comunicaciones cifrado y una variedad de módulos en el cliente que pueden tomar acciones (por ejemplo, encender o apagar cosas, cambiar parámetros de configuración, etc). En el lado cliente de Security Blanket hay un despachador que

escucha las órdenes y envía las respuestas.

### Instalación de Security Blanket

La instalación es bastante sencilla y está bien documentada. Una vez que haya descomprimido el paquete y ejecutado el script llamado *SB\_Install*, el script le ofrecerá algunas opciones como la instalación del software cliente, la consola o ambos. Si está instalando un sistema aislado, le harán falta tanto la consola como el cliente. Si planea tener múltiples clientes y una consola, entonces la consola no tiene que tener el software cliente instalado.

A continuación se le pedirá que ejecute *cert\_gen.sh*, que normalmente se encuentra en el directorio */usr/share/security-blanket/tools*. Téngase en cuenta que un error del script de instalación requiere que se copie *cacert.pem* y *disp.pem* manualmente al directorio */var/lib/security-blanket/files/certs/* (TCS ha comentado que corregirán este fallo en una próxima versión). Una vez que tenga instalado los certificados, hay que ejecutar *SB\_Setup* del directorio */usr/share/security-blanket/tools/*. Por último, debe instalarse la clave de la licencia en la consola; es el procedimiento estándar, corte y pegue desde el

Name	Summary
CIS Benchmarks	Center for Internet Security Benchmarks
DCID	DCID 6/3
DISA UNIX STIG	UNIX Security Technical Implementation Guide
FERC CIP	Critical Infrastructure Protection
JAFAN	JAFAN 6/3
NISPOM	NISPOM Chapter 8
PCI DSS	Payment Card Industry Data Security Standard
Web Services Protection	Web Services Protection (SANS LAMP)

Figura 1: Perfiles soportados por defecto por Security Blanket.

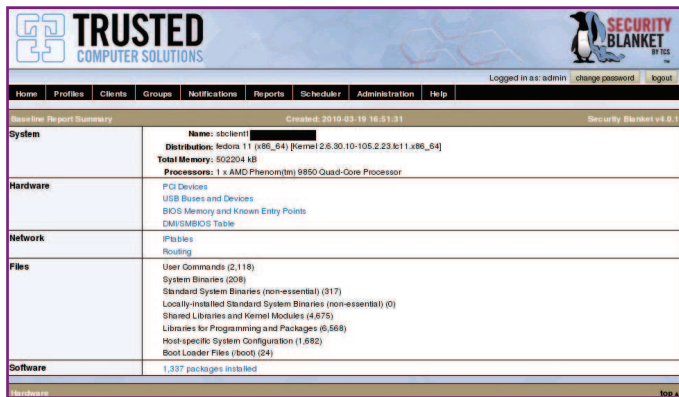


Figura 2: Resultados del análisis básico.

correo electrónico que le envíen y con eso será suficiente.

Los prerrequisitos para Security Blanket no son muy complicados. Hace falta Java para la consola (está basada en Tomcat), y para los clientes será imprescindible la librería PyXML (de lo contrario obtendrá un error diciendo que no se encuentra si intenta enviarle órdenes a los clientes).

## Configuración Básica

Una vez que tengamos una consola y algunos clientes, ¿qué hacemos ahora? Para configurar los clientes hay que añadirlos a un grupo, aplicarles algún perfil al grupo, y básicamente ya hemos terminado. Podemos elegir entre ocho perfiles por defecto (Figura 1), pudiéndose modificar o crear perfiles propios (se tratará más adelante). Una vez que haya aplicado algún perfil a un grupo y haya añadido clientes, podrá analizarlos (contra ese perfil) y aplicarles ese perfil a los sistemas en cuestión.

## Analizar

Security Blanket soporta tres tipos de análisis: análisis básico, análisis de seguridad y análisis rápido de seguridad. El análisis básico no es de seguridad (Figura 2); recolecta información acerca del host, como su nombre, distribución, dispositivos hardware, configuración de red y paquetes que tenga instalado. Los análisis de seguridad normal y rápido son lo mismo, excepto que el rápido no ejecuta módulos intensivos del sistema o módulos lentos. Sin embargo, para todos, excepto para los servidores que se encuentren sobrecargados, recomiendo encarecidamente utilizar el análisis completo, ya que el rápido podría no obviar algunos problemas.

mente, Security Blanket no posee actualmente ninguna manera de mostrar qué comandos han sido enviados y están a la espera de una respuesta, de modo que si tiene que ejecutar un comando en un host, tendrá que esperar. Una vez que haya finalizado el análisis, el cliente se conectará de nuevo a la consola, proporcionará los resultados de los análisis y creará una notificación de alerta en la interfaz web – se añadirá texto en rojo en la parte superior de la interfaz, haciéndole saber cuántas notificaciones han aparecido.

Como puede observarse a partir del primer análisis (Figura 3), una instalación por defecto de Fedora 11 no cumple precisamente el PCI-DSS (93 fallos, 47 pasados y 26 otros). Tengo que admitir que tuve curiosidad por ver cuáles eran los fallos, y lo bueno del informe es que se obtiene un listado completo de cada módulo que se ha ejecutado junto con su salida (Figura 4). Si hace clic en el título del problema, se obtendrá una descripción del mismo (por ejemplo, *rsh deshabilitado*) junto con una descripción de por qué probablemente sería una buena idea arreglarlo y qué estándares de seguridad lo requieren.

## Aplicando un Perfil de Seguridad

Obviamente tengo un problema (93 fallos) que ha de resolverse. La solución es tan sencilla como pulsar el botón “apply” y esperar unos pocos minutos. Cuando se ejecuta “apply”, es

Una vez que haya pulsado el botón *Scan*, la consola enviará un comando al despachador que se ejecuta en el cliente. Una vez que le haya mandado un comando al cliente, debe completarse antes de poder mandarle uno nuevo. Desafortunada-

como si se ejecutase un análisis; el comando es enviado al cliente, y éste lo ejecuta y devuelve los resultados a la consola y luego crea un evento de notificación. Si ocurriese algún error (por ejemplo, que un módulo falle), aparecerá en la pantalla de notificación y en el informe.

Como puede ver, un análisis tras aplicar un perfil muestra muchos menos fallos (Figura 6). En mi caso, falló (el soporte de Fedora no ha concluido aún) a la hora de tratar con *su* de forma adecuada; además, hubo un error con SNMP y surgieron algunos problemas con los permisos en los registros del sistema.

## Resumen

Security Blanket hace lo que dice en el envoltorio; es fácil de instalar y configurar; y su uso es... digamos... simple (pulsar *Scan*, pulsar *Apply* y personalizar los perfiles que se necesiten).

De modo que, ¿Por qué hay que gastarse el dinero en un producto como este pudiendo utilizarse Puppet, que es de código abierto y libre? Diversas características hacen que valga la pena gastarse el dinero en Security Blanket. Las siguientes secciones resaltan algunas de las razones por las que Security Blanket merece la pena.

## Perfiles

La primera y más importante de las características que hacen que merezca la pena la inversión en Security Blanket son los perfiles predefinidos de seguridad [3][4][5][6][7][8][9]. (No pude encontrar en línea la política SANS LAMP). Por diversión, me descargué el estándar PCI-DSS y comencé a leerlo. Algunas partes son bastante claras, como la del Requisito

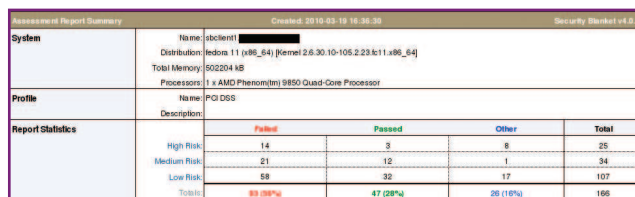


Figura 3: Resultados del análisis de unos cuantos hosts (muchos problemas).

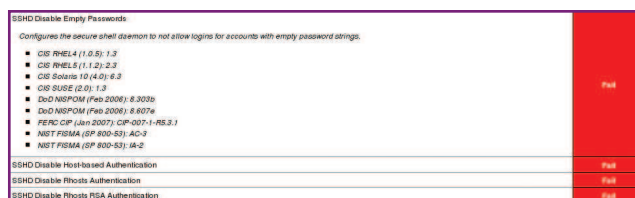


Figura 4: Resultados SSH, expandidos.

5: “Use y actualice regularmente el software y los programas antivirus”. Esta parte es autoexplicativa.

Sin embargo, la sección 8.5, más que tratar con una docena de problemas específicos, trata de contraseñas, tocando temas que van desde la fortaleza mínima de una contraseña hasta el tiempo de bloqueo de una cuenta (30 minutos) y el tiempo que debe permanecer una sesión ociosa (15 minutos). La implementación de estas restricciones con las contraseñas podría significar tener que realizar multitud de ajustes – desde las políticas de contraseñas hasta los salvapantallas (bloqueo de sesiones ociosas) – y servicios específicos que soporten conexiones (como FTP). Al disponer de perfiles predefinidos y módulos que implementan estas modificaciones, permiten un ahorro considerable de tiempo.

### Conforme a la Regulación

De nuevo, la temida palabra “C” – Conforme a. La realidad es que en la mayoría de las organizaciones que se rigen por conformidad a alguna regla o ley, no les importa cómo de bien asegures sus sistemas a menos que pueda probarse que se haya hecho según un informe de auditoría. Esto requiere, primero, alguna clase de mecanismos que permitan analizar las máquinas y, segundo, una lista de elementos a analizar – algo que no se encuentra en productos como Puppet, por lo que yo sepa.

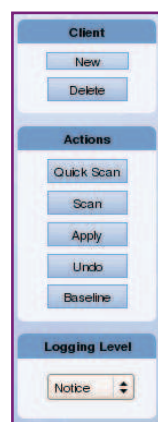
Security Blanket también informa de vulnerabilidades categorizadas (de riesgo alto, medio y bajo) y proporciona una salida numérica, algo que le encanta a los jefes. (La teoría de negocios más común que he oído dice que si se pueden obtener números, se podrá medir y por tanto controlar – matiz de 6 Sigma y Total Quality).

### Automatización

Una de mis características favoritas de Security Blanket, sin embargo, es su habilidad para programar acciones, especialmente las cadenas de acciones. Por ejem-

plo, se puede programar un grupo de hosts para que ejecute un análisis, seguido por un comando *Apply*, y luego seguido de un segundo análisis digamos a las cuatro de la mañana todos los días. Con esto podremos saber si los hosts están cambiando (por ejemplo, antes de pulsar *Apply*, había nuevos problemas de seguridad) y asegurarse de que las actualizaciones de los sistemas y otros cambios no deshacen las medidas de seguridad tomadas (y si las deshacen, se pueden reparar e informar).

La realidad es que cualquier tarea de seguridad o cualquier copia de seguridad que no esté automatizada probablemente no se hará (como mi fallo a la hora de actualizar WordPress en el fin de semana).



**Figura 5:** Comandos del cliente de Security Blanket.

### Deshacer

Ni siquiera conocía esta funcionalidad hasta que pregunté a uno de los ingenieros de soporte por qué se deshabilitaban los programas simplemente eliminando el bit de ejecución (en vez de eliminar el fichero, desinstalarlo, etc.). Resulta que lo hacen así porque Security Blanket puede deshacer casi todo lo que hace.

De modo que si accidentalmente se ponen muy estrictos los niveles de seguridad, o se estropea algo en uno de los servidores críticos, rápidamente se pueden deshacer los cambios. Esto significa que dispondremos de más tiempo para averiguar la causa por la que ha ido mal, sin tener que perder el tiempo en reparar el fallo bajo presión y luego averiguar la causa que lo produjo.

### Qué le Falta

Algo que he visto en muchas revisiones de productos es que sólo se escuchan las cosas buenas, los redactores no mencionan lo que no funciona o no incluye el producto. Entonces ¿qué es lo que no es tan bueno o falta en Security Blanket? Mi mayor deseo sería

algo diferente a los informes de análisis. Realmente no quiero ver el informe entero cada vez (mis ojos empiezan a cansarse); en su lugar, me gustaría bastante más tener un *diff* del informe actual donde se vean las diferencias con respecto al informe anterior. He visto que aparece en la hoja de ruta y espero que se realice, ya que sería una gran característica (realmente compactaría la cantidad de información que habría que ver).

### Conclusión

¿Debería gastarse el dinero en este producto? Si tiene que vérselas con problemas de auditorías y regulaciones, le será realmente de ayuda. Y, si se encuentra atascado con estándares gubernamentales, entonces probablemente sea una buena idea adquirirlo.

Incluso si no tiene que enseñar las pruebas, (por ejemplo, que no esté obligado a cumplir estos estándares), realmente me gusta la base de partida que proporcionan estas políticas y la facilidad con la que pueden ser modificadas para ajustarse a una instalación específica.

También me sorprendió un poco que la mayoría de los productos no dispongan de la función deshacer (nunca utilizaría un procesador de textos que no la tuviera, así que si voy a administrar mis sistemas, me gustaría tener una buena seguridad). Ante todo, me gusta este producto – sobre todo porque realmente hace lo que promete que hará y lo hace sin complicaciones. ■

System		Report Statistics			
Name:	labclient1	Failed	Passed	Other	Total
Distribution:	fedora 11 (x86_64) [kernel 2.6.30-105.2.23.fc11.x86_64]	0	17	8	25
Total Memory:	802204 MB	Medium Risk	1	32	34
Processors:	1 x AMD Phenom(tm) 9850 Quad-Core Processor	Low Risk	3	87	107
Profile Name:	PCI DSS	Total	4 (2%)	136 (82%)	26 (10%)
Description:					

**Figura 6:** Resultados del análisis de unos cuantos hosts tras aplicar los perfiles de seguridad.

## RECURSOS

- [1] Trusted Computer Solutions – Security Blanket: <http://www.trustedcs.com/Security-Blanket/SecurityBlanket.html>
- [2] Puppet: <http://projects.puppetlabs.com/projects/puppet>
- [3] CIS benchmarks: <http://cisecurity.org/>
- [4] DCID 6/3: [http://www.fas.org/irp/offdocs/DCID\\_6-3\\_20Manual.htm](http://www.fas.org/irp/offdocs/DCID_6-3_20Manual.htm)
- [5] DISA Unix STIG: <http://iase.disa.mil/stigs/stig/unix-stig-v5r1.pdf>
- [6] FERC CIP: <http://www.ferc.gov/industries/electric/indus-act/reliability/cip.asp>
- [7] JAFAN 6/3: [http://www.lazarusalliance.com/horsewiki/images/f/fa/JAFAN\\_6\\_3.pdf](http://www.lazarusalliance.com/horsewiki/images/f/fa/JAFAN_6_3.pdf)
- [8] NISPOM: [http://www.fas.org/sgp/library/nispom/5220\\_22m2.pdf](http://www.fas.org/sgp/library/nispom/5220_22m2.pdf)
- [9] PCI-DSS: <https://www.pcisecuritystandards.org/>