

Fortalecimiento de la seguridad

BanCoppel

Ismael Flores

Consultant Senior

Fernando López

Project Manager

Diciembre 3, 2021

Agenda

- ▶ Objetivo
- ▶ Revisión del registro de Linux (1.4.1)
- ▶ Revisión del servicio OpenSSH (1.4.9, 1.4.10)
- ▶ Revisión de puertos abiertos y servicios de red (1.4.11)
- ▶ Revisión y documentación de cuentas privilegiadas (1.4.12)
- ▶ Eliminación de los Shells innecesarios o no utilizados (1.4.15)
- ▶ Limpieza y verificación del sistema operativo



Objetivo

Revisar y ajustar la configuración de 30 servidores RHEL v6.x o superior seleccionados, para realizar una serie de ajustes en la configuración que permitan fortalecer las defensas de estos contra posibles ataques de seguridad

Fortalecimiento de la seguridad

Revisión del registro de Linux (1.4.1)

- ▶ Configurar el sistema de syslog
- ▶ Revisar de la configuración de iptables
- ▶ Configurar el paquete: sudoers
- ▶ Limitar el uso del crontab únicamente para usuarios con privilegios
- ▶ Configurar del cliente de Red Hat Insights
- ▶ Verificar que las bitácoras de los servidores se archiven y reenvíen a un SIEM (el cliente debe contar con un SIEM)
- ▶ Verificar que los servidores estén configurados para registrar y retener información
- ▶ Preparar documentación con el detalle de la validación

Fortalecimiento de la seguridad

Revisión del servicio OpenSSH (1.4.9, 1.4.10)

- ▶ Revisar de la configuración de OpenSSH
- ▶ Verificar niveles de accesos para las cuentas y grupos accesibles
- ▶ Verificar niveles de accesos restringidos para procesos automatizados y accesos remotos
- ▶ Verificar niveles de accesos restringidos a usuarios autenticados
- ▶ Verificar puerto al que escucha el demonio sshd y hacer ajustes de esta configuración
- ▶ Configurar los niveles de accesos con privilegios mínimos para todas las cuentas y grupos accesibles
- ▶ Limitar el acceso al servidor sólo a cuentas de usuarios autenticados ajenos a root
- ▶ Preparar documentación con el detalle de la validación

Fortalecimiento de la seguridad

Revisión de puertos abiertos y servicios de red (1.4.11)

- ▶ Desactivar puertos de red identificados como no necesarios
- ▶ Desactivar servicios de red identificados como no necesarios
- ▶ Bloquear las direcciones IP, los puertos y los sinkholes de nombres de dominio que hayan sido identificados
- ▶ Verificar que las comunicaciones de salida y sistemas críticos se pueden denegar de forma predeterminada
- ▶ Validar que todo el tráfico de salida de red aprobado bajo excepción se registra
- ▶ Verificar que se está utilizando un firewall basado en host como iptables para restringir el acceso a servicios que no son necesarios
- ▶ Deshabilitar el acceso fuera de BanCoppel de los protocolos FTP y Telnet
- ▶ Preparar documentación con el detalle de la validación

Fortalecimiento de la seguridad

Revisión y documentación de cuentas privilegiadas (1.4.12)

- ▶ Revisar y documentar las cuentas configuradas
- ▶ Revisar y documentar las cuentas que tienen privilegios de root
- ▶ Validar la documentación de las cuentas privilegiadas
- ▶ Eliminar usuarios que no correspondan o no estén autorizados de acuerdo a las recomendaciones con con las aplicaciones
- ▶ Verificar que el único usuario configurado en un sistema con UID 0 sea la cuenta predeterminada de root
- ▶ Habilitar las opciones "Password is Required" y "Sensitive account and cannot be delegated" en las cuentas ya existentes
- ▶ Eliminar el atributo "Admin SDHolder" de todas las cuentas que no están en grupos privilegiados
- ▶ Imponer la caducidad de las contraseñas en las cuentas privilegiadas
- ▶ Preparar documentación con el detalle de las mejoras

Fortalecimiento de la seguridad

Eliminación de los Shells innecesarios o no utilizados (1.4.15)

- ▶ Eliminar todos aquellos Shells que no se utilicen o no estén autorizados
- ▶ Verificar si el shell predeterminado de la cuenta root no ha sido reemplazado por otro binario de shell
- ▶ Verificar los shells de inicio
- ▶ Preparar documentación con el detalle de las mejoras

Fortalecimiento de la seguridad

Limpieza y verificación del sistema operativo


- ▶ Verificar que el sistema operativo tenga los parches requeridos
- ▶ Verificar que el sistema opera haya actualizado el antivirus (firmas) y se haya completado un análisis total del disco
- ▶ Verificar que se hayan restablecido todas las contraseñas de las cuentas locales del sistema
- ▶ Preparar documentación con el detalle de las mejoras

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

 linkedin.com/company/red-hat

 facebook.com/redhatinc

 youtube.com/user/RedHatVideos

 twitter.com/RedHat