BRS09. Tarea online

Título de la tarea: Configuración de Sistemas Informáticos

Curso de Especialización y módulo: Ciberseguridad en Entornos de las Tecnologías de la Información - Bastionado de Redes y Sistemas.

¿Qué contenidos o resultados de aprendizaje trabajaremos?

Resultados de aprendizaje

- **RA7.** Configura sistemas informáticos minimizando las probabilidades de exposición a ataques.

Contenidos

1.- Reducción del número de servicios, Telnet, RSSH, TFTP, entre otros.
    1.1.- Telnet.
    1.2.- TFTP/FTP.
    1.3.- RSSH/SSH.
2.- Hardening de procesos (eliminación de información de depuración en caso de errores, aleatorización de la memoria virtual para evitar exploits, etc.).
3.- Eliminación de protocolos de red innecesarios (ICMP, entre otros).
4.- Securización de los sistemas de administración remota.
5.- Sistemas de prevención y protección frente a virus e intrusiones (antivirus, HIDS, etc.).
6.- Configuración de actualizaciones y parches automáticos.
7.- Sistemas de copias de seguridad.
8.- Shadow IT y políticas de seguridad en entornos SaaS.
    8.1.- Shadow IT.

1.- Descripción de la tarea.

¿Qué te pedimos que hagas?

Responsable de la Seguridad de la empresa ha decido que este servicio crítico y tan utilizado por los administradores tiene que ser bastionado, de cara aumentar el nivel de seguridad de las tareas asociada a la utilización del SSH. Por lo que ha decidido que se implementen las siguientes medidas de seguridad:

1. No será posible el acceso remoto con el usuario root.
2. Si la sesión permanece sin actividad durante 5 minutos se bloqueará.
3. Los usuarios deberán acceder al servicio con una clave público/privada. Las claves privadas de los usuarios deberá tener configurados los permisos correctamente para que un usuario no pueda manipular claves privadas de otros usuarios.
4. Sólo está permitido el acceso al servicio para cierto usuario
5. Sólo está permitido el acceso al servicio para cierto IPs. Basar la confianza de los equipos en parámetros de filtrado host de SSH en lugar del fichero .rhosts
6. Se debe implementar la versión segura del protocolo.
7. No es posible que a través del servicio se realice “Port-forwarding” ni ”X11 Forwarding”.
8. Los usuario recibirán en el inicio de sesión recibirán un mensaje indicando al tipo de sistema que están accediendo y las obligación de cumplir con la normativa interna de la empresa.
9. Se establecerán como protocolo de cifrado SHA2-512, SHA2-256.
10. Los logs del servicio están activados para poder enviárselos al SOC.

2.- Información de interés.

Recursos necesarios y recomendaciones

Referencias de interés para desarrollar el trabajo:

- https://www.ssh.com/academy/ssh/protocol
- https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3674-ccn-stic-619-implementacion-de-seguridad-sobre-centos7/file.html
- https://nvlpubs.nist.gov/nistpubs/ir/2015/nist.ir.7966.pdf
- https://www.ssi.gouv.fr/en/guide/openssh-secure-use-recommendations/
- https://github.com/jtesta/ssh-audit
- https://sergiobelkin.com/posts/como-usar-certificados-ssh-para-autenticar/
- https://www.digitalocean.com/community/tutorials/how-to-create-an-ssh-ca-to-validate-hosts-and-clients-with-ubuntu

Indicaciones de entrega

Una vez realizada la tarea, el envío se realizará a través de la plataforma. El archivo se nombrará siguiendo las siguientes pautas:

Apellido1_Apellido2_BRS09_Tarea

Asegúrate que el nombre no contenga la letra ñ, tildes ni caracteres especiales extraños. Así por ejemplo la alumna **Begoña Sánchez Mañas para la novena unidad del MP de BRS**, debería nombrar esta tarea como...

sanchez_manas_begona_BRS09_Tarea

3.- Evaluación de la tarea.

Criterios de evaluación implicado

Criterios de Evaluación RA7

- a) Se han enumerado y eliminado los programas, servicios y protocolos innecesarios que hayan sido instalados por defecto en el sistema.
- b) Se han configurado las características propias del sistema informático para imposibilitar el acceso ilegítimo mediante técnicas de explotación de procesos.
- c) Se ha incrementado la seguridad del sistema de administración remoto SSH y otros.
- d) Se ha instalado y configurado un Sistema de detección de intrusos en un Host (HIDS) en el sistema informático.
- e) Se han instalado y configurado sistemas de copias de seguridad.

Propuesta de Herramientas:

- Máquina con sistema operativo Linux: Centos, Debian, Ubuntu,...
- Servicio de SSH corriendo en la máquina Linux: OpenSSH
- Máquina que permita la conexión al servicio para realizar las pruebas de seguridad. Se podrá utilizar una máquina asociado al pentesting (Ej: Kali Linux) o una herramienta gráfica de un entorno Windows (Ej: Putty, MobaXTerm,…)
- Opcional. Herramientas de auditoría de seguridad del servicio: nmap, metasploit, hydra, scripts de github

Cada tarea relativa al bastionado se evaluará con 1 punto. Deberá existir una evidencia de la pruebas de que la medida de protección funciona con una antes y un después de aplicar la medida. Se dará cada punto cómo válido si se evidencia la protección a través de parámetros de configuración del servicio.

¿Cómo valoramos y puntuamos tu tarea?

Rúbrica de la tarea	
Apartado 1: No será posible el acceso remoto con el usuario root.	1 punto
Apartado 2: Si la sesión permanece sin actividad durante 5 minutos se bloqueará.	1 punto
Apartado 3: Los usuarios deberán acceder al servicio clave público/privadas. Las claves privadas de los usuarios deberá	1 punto

tener configurados los permisos correctamente para que un usuario no pueda manipular claves privadas de otros usuarios.	
Apartado 4:Sólo está permitido el acceso al servicio para cierto usuario	1 punto
Apartado 5:Sólo está permitido el acceso al servicio para cierto IPs. Basar la confianza de los equipos en parámetros de filtrado host de SSH en lugar del fichero .rhosts	1 punto
Apartado 6: Se debe implementar la versión segura del protocolo.	1 punto
Apartado 7: No es posible que a través del servicio se realice “Port-forwarding” ni ”X11 Forwarding”.	1 punto
Apartado 8: Los usuario recibirán en el inicio de sesión recibirán un mensaje indicando al tipo de sistema que están accediendo y las obligación de cumplir con la normativa interna de la empresa.	1 punto
Apartado 9: Se establecerán como protocolo de cifrado SHA2-512, SHA2-256	1 punto
Apartado 10: Los logs del servicio están activados para poder enviárselos al SOC.	1 punto
Redacción clara y correcta, sin errores ortográficos	Se resta 0,1 puntos por cada error ortográfico o expresiones incorrectas.

NOTA IMPORTANTE

Aquellos apartados/subapartados en los que las capturas de pantalla no sean claras o no tengan como fondo de pantalla la plataforma con tu usuario mostrando claramente la foto de tu perfil, no serán corregidos.