BRS08. Tarea Online

Título de la tarea: Configuración de dispositivos para la instalación 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

- **RA6.** Configura dispositivos para la instalación de sistemas informáticos minimizando las probabilidades de exposición a ataques.

Contenidos

1.- Precauciones previas a la instalación de un sistema informático: aislamiento, configuración del control de acceso a la BIOS, bloqueo del orden de arranque de los dispositivos, otros.
    1.1.- Control de configuración BIOS/UEFI.
    1.2.- Secuencia de arranque.
    1.3.- Puertos de conexión: Ethernet, Wifi, Bluetooth,…
    1.4.- Puertos de conexión: USB.
2.- Seguridad en el arranque del sistema informático, configuración del arranque seguro.
3.- Seguridad de los sistemas de ficheros, cifrado, particionado, entre otros.

1.- Descripción de la tarea.

¿Qué te pedimos que hagas?

El departamento de I+D tiene unos resultados extraordinarios por lo logros conseguidos en el descubrimiento de un nuevo sistema de propulsión eléctrica en los coches fabricados por la compañía. Existen intereses económico de empresas de la competencia y actores externos por hacerse con esta información para poder aplicarla a sus modelos.

El CISO de la compañía quiere que se investigue si el sistema donde se guarda la información sensible y crítica es segura. Por lo que ha pedido que se revisen las medidas de seguridad relativas a estos sistemas. Buscando:

- Los directorios que tienen permisos de escritura.
- Los directorios que tienen permisos de ejecución.
- Ficheros con el SUID o SGID activado, que permitan ejecutar los ficheros con permisos de root, incluyendo si existe algún fichero con permisos de root entre los de la siguiente lista: https://gtfobins.github.io
- Los ficheros de la variable PATH, comprobando qué usuarios tienen acceso de escritura en esos directorios.
- Las carpetas compartidas mal configuradas que permiten realizar acciones no controladas.
- Las particiones que tienen permisos para ejecutar ficheros y otras características que tienen impacto sobre la seguridad.
- Borrado seguro de archivos.

El escenario se puede realizar con un sistema operativo Linux Ubuntu.

2.- Información de interés.

Recursos necesarios y recomendaciones

Referencias de interés para desarrollar el trabajo:

- https://gtfobins.github.io
- https://payatu.com/guide-linux-privilege-escalation
- http://ntfs.com/ntfs-permissions.htm
- https://proyectoa.com/borrado-seguro-de-ficheros-y-particiones-en-linux-con-shred/
- https://www.hackingarticles.in/linux-privilege-escalation-using-path-variable/
- https://zsecurity.org/linux-privilege-escalation-using-path-variable-and-suid/

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_BRS08_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 octava unidad del MP de BRS**, debería nombrar esta tarea como...

sanchez_manas_begona_BRS08_Tarea

3.- Evaluación de la tarea.

Criterios de evaluación implicado

Criterios de evaluación RA6

- a) Se ha configurado la BIOS para incrementar la seguridad del dispositivo y su contenido minimizando las probabilidades de exposición a ataques.
- b) Se ha preparado un sistema informático para su primera instalación teniendo en cuenta las medidas de seguridad necesarias.
- c) Se ha configurado un sistema informático para que un actor malicioso no pueda alterar la secuencia de arranque con fines de acceso ilegítimo.
- d) Se ha instalado un sistema informático utilizando sus capacidades de cifrado del sistema de ficheros para evitar la extracción física de datos.
- e) Se ha particionado el sistema de ficheros del sistema informático para minimizar riesgos de seguridad.

La evaluación de esta tarea es saber tener la capacidad de buscar los directorios que tienen mal configurados los permisos de los archivos tanto las debilidades en:

- Directorios con permisos de escritura.
- Directorios con permisos de ejecución.
- Buscar ficheros con SUID que permitan ejecutar los ficheros con permisos de root.
- Buscar ficheros con SGID que permitan ejecutar los ficheros con permisos de grupo de root.
- Ver si existe algún fichero con permisos de root entre los de la siguiente lista: https://gtfobins.github.io.
- Analizar los ficheros de la variable PATH, y comprobar qué usuarios tienen acceso a para escribir en esos directorios.
- Los permisos en las carpetas compartidas
- Los permisos en las particiones a través de la configuración de las mismas.
- Borrado seguro de ficheros para evitar o dificultar la recuperación de ficheros por "carving".

¿Cómo valoramos y puntuamos tu tarea?

Rúbrica de la tarea	
Apartado 1: Directorios con permisos de escritura.	0,5 puntos
Apartado 2: Directorios con permisos de ejecución	0,5 puntos
Apartado 3: Buscar ficheros con SUID o SGID que permitan	0,5 puntos

ejecutar los ficheros con permisos de root.	
Apartado 4: Ver si existe algún fichero con permisos de root entre los de la siguiente lista: https://gtfobins.github.io	0,5 puntos
Apartado 5: Analizar los ficheros de las variable PATH, y comprobar qué usuarios tienen acceso a para escribir en esos directorios	2 puntos
Apartado 6: Los permisos en las carpetas compartidas	2 puntos
Apartado 7: Los permisos en las particiones a través de la configuración de las mismas.	3 puntos
Apartado 8: Borrado seguro de ficheros	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.