

SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

[Área personal](#) / [Mis cursos](#) / [SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN](#) / [Unidad No. 2 - Control de Accesos](#)
/ [Tarea No. 6 \(1er Parcial \)](#)

Tarea No. 6 (1er Parcial)

Apertura: Thursday, 15 de June de 2023, 22:00

✓ Hecho

I N S T R U C C I O N E S

Del siguiente sitio web --> https://docs.oracle.com/cd/E24842_01/html/E23286/rbac-1.html

Con sus propias palabras explicar el contenido del mismo. O lo que es lo mismo, ¿ Qué parte del documento en cuestión es la que le pareció más interesante y Por qué ?

Esta actividad estará habilitada desde las 22h00 del 15 de Junio hasta las 22h00 del 20 de Junio del 2023. No hay opción a prórroga alguna. Esta actividad la realizará directamente en la plataforma. NO hay que generar ningún tipo de archivo.

Estado de la entrega

Estado de la entrega	Enviado para calificar
Estado de la calificación	Calificado
Última modificación	Tuesday, 20 de June de 2023, 21:39

Texto en línea

Control de acceso basado en roles

El Control de Acceso Basado en Roles (RBAC, por sus siglas en inglés) es una función de seguridad que se utiliza para controlar el acceso de los usuarios a tareas restringidas que normalmente solo pueden ser realizadas por el superusuario. Mediante la aplicación de atributos de seguridad a usuarios y procesos, el RBAC permite dividir las capacidades del superusuario entre varios administradores.

En el RBAC, los derechos de los procesos se gestionan a través de privilegios, mientras que los derechos de los usuarios se gestionan a través de roles. Los privilegios son derechos específicos que se pueden otorgar a comandos, usuarios, roles o al sistema en general. Por ejemplo, el privilegio "proc_exec" permite a un proceso llamar a la función "execve()". Los privilegios permiten que un proceso realice operaciones que normalmente están prohibidas para los usuarios comunes.

Por otro lado, los roles son identidades especiales que pueden asumir los usuarios para realizar tareas que requieren capacidades de superusuario. Un rol puede incluir uno o varios perfiles de derechos, que son colecciones de capacidades administrativas. Los perfiles de derechos pueden contener autorizaciones, comandos con atributos de seguridad y otros perfiles de derechos complementarios. Al asignar un rol a un usuario, este adquiere las capacidades asociadas con ese rol.

El RBAC ofrece una alternativa más segura al modelo de superusuario tradicional en sistemas UNIX. En lugar de tener un único superusuario con amplios privilegios, se pueden crear roles específicos con capacidades limitadas que se asignan a usuarios confiables. De esta manera, cada usuario tiene solo los privilegios necesarios para realizar su trabajo, lo que reduce el riesgo de abuso de privilegios y mejora la seguridad del sistema.


El RBAC se implementa en Oracle Solaris, un sistema operativo basado en UNIX. Proporciona autorizaciones predefinidas y perfiles de derechos que se pueden utilizar para crear roles con diferentes niveles de acceso. Además, permite la asignación de privilegios y autorizaciones directamente a usuarios y roles, lo que brinda flexibilidad en la configuración de la seguridad.

Me pareció más importante como redacta las consideraciones de seguridad al asignar atributos, porque en estas situaciones priorizar la seguridad es importante debido a la cantidad y calidad de precios que manejamos.

Comentarios de la entrega

▶ [Comentarios \(0\)](#)

Comentario

Calificación	10,00 / 10,00
Calificado sobre	Wednesday, 21 de June de 2023, 22:23
Calificado por	 OTTO RODRIGO GONZALEZ MENDOZA

◀ [Taller No. 5 \(1er Parcial \)](#)

Ir a...

[Examen del 1er Parcial ▶](#)

Español - Internacional (es)

English (en)

Español - Internacional (es)

Resumen de retención de datos

Descargar la app para dispositivos móviles