Universidad de las Fuerzas Armadas ESPE

Departamento de Ciencias de la Computación

Aplicación de Sistemas Operativos

Nombre: Freddy Leonel Pachacama **NRC:** 10035

Fecha: 16/08/2023

- **Seguridad multinivel – Bell – La Padula**

  Es un enfoque utilizando en la seguridad de sistemas de información y redes para garantizar que los datos y la información se manejen y compartan de manera segura en entornos con diferentes niveles de clasificación o acceso. Bell La Padula es uno de los modelos de seguridad multinivel más conocidos y utilizados, que se rige por dos propiedades fundamentales:

  1. **Regla de la no divulgación (No Read Up):** Esta regla establece que un sujeto con un nivel de seguridad inferior no puede leer información en un objeto con un nivel de seguridad superior, en otras palabras, la información solo fluye hacia abajo, desde niveles superiores de seguridad a niveles inferiores.
  2. **Regla de la no modificación (No Write Down):** Esta regla establece que un sujeto con un nivel de seguridad superior no puede escribir información en un objeto con un nivel de seguridad inferior.

- **¿Cómo implementar un modelo de seguridad multinivel en Windows y Linux?**

  1. **Implementación en Windows:**
     - **Identificación de Niveles de Seguridad:** Define los niveles de seguridad según las clasificaciones de datos y recursos en tu entorno.
     - **Asignación de Niveles de Seguridad a Objetos:** Configura los permisos de acceso a archivos, carpetas y otros objetos de acuerdo con el modelo Bell-La Padula. Asigna niveles de seguridad apropiados a los objetos y asegúrate de que los usuarios solo puedan acceder a objetos con niveles de seguridad iguales o inferiores.
     - **Políticas de Grupos y Usuarios**: Utiliza grupos de usuarios para asignar niveles de seguridad y permisos específicos. Asegúrate de que los usuarios tengan acceso solo a grupos y recursos correspondientes a sus niveles de seguridad.
     - **Control de Acceso:** Configura las políticas de seguridad de Windows para limitar el acceso a los recursos basándote en el modelo Bell-LaPadula. Utiliza ACLs

(Listas de Control de Acceso) y políticas de seguridad avanzadas para controlar quién puede acceder a qué objetos.

2. **Implementación en Linux:**
    - **SELinux (Security-Enhanced Linux**): SELinux es una tecnología de control de acceso obligatorio (MAC) que puede implementar políticas de seguridad multinivel en Linux. Puedes configurar políticas SELinux para limitar el acceso a objetos basados en niveles de seguridad.
    - **Políticas de Grupos y Usuarios:** Similar a Windows, utiliza grupos y usuarios para gestionar el acceso a recursos. Asegúrate de asignar grupos y niveles de seguridad adecuados.
    - **Configuración de Permisos:** Configura los permisos de archivos y directorios para reflejar las reglas del modelo Bell-La Padula. Utiliza comandos como chmod y chown para establecer permisos y propietarios adecuados.
    - **Políticas de Firewall**: Además de los controles de acceso en el nivel de archivos, considera configurar políticas de firewall para restringir la comunicación entre diferentes niveles de seguridad.