Trabajo Práctico N° 7

Temas: Conceptos Fundamentales. Llamadas al sistema de seguridad. Implementación de la seguridad. El problema de la seguridad. Amenazas relacionadas con los programas. Amenazas del sistema y de la red. La Criptografía como herramienta de seguridad. Autenticación de usuarios. Implementación de defensas de seguridad. Cortafuegos para proteger los sistemas y las redes. Clasificación de la seguridad informática.

Fecha de Presentación: jueves 04/07/2024

Modalidad: Grupal

Consignas

1. Defina con sus palabras los términos protección y seguridad.
2. ¿Qué es un dominio de protección? Explique de qué manera se implementa el control de los objetos que pertenecen a un dominio.
3. ¿Cómo puede violarse la seguridad en un sistema? Explique algunas formas de acceso mal intencionado.
4. Explique algunos métodos para validar los usuarios en el sistema.
5. ¿Qué recomendaciones daría para la selección de las contraseñas del sistema? ¿Cuáles son los errores más comunes que se cometen?
6. ¿Qué entiende por criptografía? Cite las ventajas de cifrar los datos almacenados en el sistema de computación. Mencione el algoritmo de encriptación de claves que utiliza Linux
7. ¿Qué es un ACL? ¿Cómo se utilizan? ¿En qué sistemas operativos esta soportado?
8. Menciones dos aspectos por lo que considera que el So Linux es más seguro que el SO Windows.

Práctica (Seguridad en GNU/Linux – Servidor AWS)

1. El comando login verifica el *username* y la clave de acceso. ¿En qué archivo hace esta verificación?
2. ¿Un usuario puede cambiar su clave de acceso? ¿Qué comando usaría?
3. ¿Qué usuario puede cambiar la clave de otros usuarios? ¿Con qué comando?
4. ¿Qué usuarios tienen autorización para modificar los permisos de un determinado archivo?

5. ¿Qué operación/es podemos realizar sobre un directorio si éste tiene el permiso de ejecución asignado?
6. Comenzar la sesión de trabajo y visualice los permisos otorgados a los siguientes archivos y explíquelos.

   /etc/passwd : _

   /etc/shadow : _

   /bin/login : _

   /bin/ls : _
7. Cree un archivo llamado copiaclave que contenga el archivo /etc/shadow y verifique los permisos que posee y compare.

   ```
   cat /etc/shadow > copiaclave
   ls –l copiaclave
   ```
8. Cambie los permisos del archivo creado (copiaclave) usando el modo simbólico, otorgándole permisos de lectura solamente al propietario, al grupo y a los demás usuarios. Verifique los cambios realizados.

   ```
   chmod ugo+r-wx copiaclave
   chmod a+r-wx copiaclave
   ls –l copiaclave
   ```

   Deberá obtener los siguientes permisos: r - - r - - r - -
9. Haga una copia del archivo copiaclave llamado copiaclave2 y usando el modo absoluto modifique los permisos del nuevo archivo otorgándole derechos de lectura y ejecución al propietario, solamente de lectura al grupo y ningún derecho al resto. Muestre los permisos modificados.

   ```
   cp copiaclave copiaclave2
   chmod u=rx,g=r,o=- copiaclave2
   ls –l copiaclave2
   ```

   Deberá obtener los siguientes permisos: r - x r - - - - -
10. Otorgue los mismos derechos del punto anterior al archivo copiaclave, pero utilice el modo numérico (octal).

    ```
    chmod 540 copiaclave
    ls –l copiaclave
    ```
11. Cree un subdirectorio llamado "prueba". Compruebe los derechos que se le otorgaron.

    ```
    mkdir prueba
    ls –l | grep prueba
    ```

12. Modifique los permisos del directorio prueba de manera que se vean como: r- - r - - - - -, utilice cualquier método. Luego verifique los cambios con: ls -la
13. Visualice los permisos otorgados a los siguientes archivos y explíquelos.
    /etc/crontab: _
    /bin/cat : _
    /usr/bin/yes: _
14. Cree un archivo llamado comandos que contenga los archivos de /bin, y verifique el contenido del archivo y los permisos que posee.

```
ls /bin > comandos
cat comandos
ls –l comandos
```

15. Utilizando el modo absoluto modifique los permisos del archivo comandos otorgándole derechos de lectura y ejecución al propietario, solamente de lectura al grupo y al resto de los usuarios. Muestre los permisos modificados.

```
chmod u=rx,g=r,o=r comandos
ls –l comandos
```

    Deberá obtener los siguientes permisos: r - x r - - r - -
16. Otorgue al archivo comandos todos los permisos para el dueño, y para el grupo y rsto de los usuario solo lectura y ejecución utilizando el modo numérico (octal).

```
chmod 755 comandos
ls –l comandos
```

    Deberá obtener los siguientes permisos: r w x r - x r – x
17. Realice un enlace duro del archivo comandos como comandos ln y verifique los permisos de ambos.

```
ln comandos comandosln
ls -li comandos comandosln
```

18. Modifique los permisos del archivo comandosln de manera que se vean como: r—r-----, utilice cualquier método. Luego verifique los cambios con: ls –l ¿Qué sucedió con los permisos de los archivos comandos y comandosln? ¿Por qué?

Nota: Para cada punto es suficiente una captura de pantalla que visualice los comandos ejecutados y el resultado