Trabajo Práctico – Seguridad en Sistemas Operativos

Alumnos:

- Federico Garcia – garcia.federico@outlook.com
- Federico Garcia Bengolea - feddericogarciaa@gmail.com

Materia:

Arquitectura y Sistemas Operativos

Profesor: Diego Lobos

Tutor: Nicolas Carcaño

Fecha de Entrega: 05 de junio de 2025

Introducción

La seguridad en los sistemas operativos es fundamental no solo para garantizar la integridad y confidencialidad de los datos en el sistema, sino también para resguardar la integridad del mismo sistema operativo y así garantizar su buen funcionamiento.

Para esto contamos con diversas herramientas y procedimientos que nos pueden ayudar a prevenir accesos no autorizados, detectar operaciones maliciosas o minimizar los posibles riesgos de ataque.

A lo largo del trabajo práctico abordaremos conceptos de seguridad informática y desarrollaremos un caso práctico utilizando Linux Ubuntu.

Marco Teórico

La necesidad de proteger los sistemas, redes y datos de caer en manos de posibles usuarios malintencionados hace de la seguridad informática un punto crucial a tener en cuenta al momento de estructurar nuestros sistemas.

Esta necesidad se ve intensificada en los tiempos que corren debido a la gran disponibilidad de servicios en la nube y a la crítica masa de usuarios que utilizan estos servicios día a día.

Como pilares de la seguridad informática podemos nombrar:

- **Confidencialidad**: Garantizar que solo usuarios autorizados accedan a la información.
- **Integridad**: Asegurar que los datos no sean alterados de forma indebida.
- **Disponibilidad**: Mantener los datos y servicios accesibles cuando se necesiten.
- **Autenticación**: Verificar la identidad de los usuarios que acceden al sistema.

Herramientas de prevención:

- **Firewall**: Controla y filtra el tráfico de red para bloquear accesos no autorizados. En Linux, se usan herramientas como iptables y firewalld para definir reglas que permitan o bloqueen conexiones según criterios específicos.
- **Antivirus**: Detecta y elimina software malicioso (malware). En Linux, ClamAV es un antivirus libre y ampliamente utilizado, que puede instalarse y ejecutarse fácilmente desde la terminal.
- **Gestión de permisos y usuarios**: La asignación correcta de permisos con comandos como chmod, chown y la gestión de usuarios con sudo ayuda a limitar el acceso a archivos y funciones críticas, reduciendo las posibilidades de ataque.

Si todas estas herramientas llegaran a fallar, el monitoreo de actividades nos permite identificar comportamientos sospechosos, modificaciones inusuales en el sistema o accesos no autorizados, con el fin de poder actuar rápidamente ante este tipo de situaciones.

Caso Práctico: Configuración Básica de Seguridad en Linux Ubuntu

En este caso práctico configuraremos un firewall (firewalld), instalaremos un antivirus (ClamAV) y haremos configuraciones básicas de permisos de usuarios.
Todo esto se realizará en un entorno Linux Ubuntu 24.04.2 LTS instalado en una máquina vistual de VirtualBox.

Pasos:

1. Configuración del Firewall con firewalld
    a. Instalar y activar firewalld

```
sudo apt update
sudo apt install firewalld
sudo systemctl start firewalld
sudo systemctl enable firewalld
```

    b. Permitir acceso SSH (puerto 22) para administración remota

```
sudo firewall-cmd --permanent --add-service=ssh
sudo firewall-cmd --reload
```

    c. Bloquear un puerto, por ejemplo, el 8080

```
sudo firewall-cmd --permanent --remove-port=8080/tcp
sudo firewall-cmd --reload
```

    d. Verificar puertos abiertos

```
sudo firewall-cmd --list-all
```

2. Instalación y uso básico de ClamAV
    a. Instalar ClamAV

```
sudo apt install clamav
```

    b. Actualizar la base de datos de virus

```
sudo freshclam
```

c. Escanear un directorio o archivo (por ejemplo, la carpeta Descargas)

```
clamscan -r /home/usuario/Descargas
```

3. Gestión de permisos y usuarios
    a. Crear un usuario nuevo

```
sudo adduser [nombre_del_usuario]
```

b. Intentar ingresar a la carpeta del usuario recién creado

```
cd [usuario_creado]/
```

c. Cambio de usuario

```
su [usuario_creado]
password: [constraseña_del_usuario_creado]
```

d. Volver a intentar el ingreso a la carpeta del usuario

```
cd [usuario_creado]/
```

Metodología Utilizada

- Se realizó una búsqueda de información (videos tutoriales, artículos publicados en internet, documentación oficial).
- Se virtualizó un entorno Linux Ubuntu en una máquina virtual utilizando Virtual Box.
- Se realizaron pruebas y se llevó adelante el caso práctico en el entorno controlado que ofrece la máquina virtual.
- Se analizaron las respuestas obtenidas de los comandos ejecutados en la terminal.

Resultados Obtenidos

- El firewall y su configuración nos permite controlar el acceso a determinados servicios (como por ejemplo la comunicación SSH). Por otro lado, la posibilidad de permitir o denegar la conexión por determinados puertos reduce considerablemente la posibilidad de ataques o accesos no autorizados.

- La instalación de un antivirus nos da la posibilidad de poder escanear directorios en busca de malware. Es imprescindible para el óptimo funcionamiento contar con la base de datos del antivirus actualizada. En entornos Linux, podemos utilizar herramientas como cron, para poder automatizar tanto la actualización de la base de datos como la posibilidad de hacer un escaneo completo del sistema en determinados momentos para asegurar que esto no quede en desuso.
- La gestión de permisos, usuarios y grupos en entornos Linux nos da la posibilidad de mantener restricciones muy específicas en cuanto a la privacidad de archivos, la posibilidad de ejecución de servicios o la manipulación del sistema en general.

Conclusiones

La seguridad en sistemas operativos es más que simplemente un conjunto de herramientas. Las herramientas deben ser utilizadas, mantenidas y actualizadas constantemente. La seguridad en los sistemas es un riguroso procedimiento que debe ejecutarse constantemente. Hay que considerar la cantidad de servicios disponibles en la nube, la cantidad de usuarios que están interactuando constantemente con estos servicios y la gran masa de datos que se manejan a cada hora en la red. Todos estos factores hacen de la seguridad informática y de los procedimientos que la componen a ser una parte fundamental para garantizar la integridad de nuestros servidores.

Bibliografía

- Universidad Cataluña. Seguridad informática: La importancia y lo que debe saber.
- SPConnet. Guía Completa para Principiantes en Ciberseguridad.
- Ciberseguridad Tips. Ejemplos de la seguridad informática: 7 medidas clave.
- Manual práctico de IPTABLES. TLDP.
- YouTube. ClamAV un antivirus para Ubuntu 16.04 LTS y derivados.

Anexos

Se anexan a este documento otro archivo con todas las capturas de pantalla de las operaciones realizadas y una breve descripción de cada una de ellas.