SeguridadInformática - Práctica 2: El Firewall

Una de las mejores formas de proteger una red es mediante el uso de un firewall. Un firewall actúa como una barrera entre un dispositivo o una red y redes externas no confiables, como Internet. Su función principal es filtrar el tráfico de red y permitir o denegar el acceso a recursos según un conjunto de reglas de seguridad predefinidas. Esto con el objetivo de proteger el sistema o la red de accesos no autorizados y ataques, garantizando la confidencialidad, integridad y disponibilidad de los datos en la red.

Tipos de Firewalls

Existen varios tipos de firewalls, cada uno con sus propias características y métodos de filtrado:

1. **Firewalls de red**: Se sitúan entre la red interna y la externa, controlando el tráfico que entra y sale de la red.
2. **Firewalls de host**: Se instalan en dispositivos individuales y protegen esos dispositivos de amenazas externas.
3. **Firewalls de aplicación**: Se centran en el tráfico de aplicaciones específicas y pueden filtrar contenido a nivel de aplicación.
4. **Firewalls de estado**: Son firewalls más avanzados que mantienen un registro del estado de las conexiones y pueden tomar decisiones de filtrado basadas en el contexto de la conexión. Mientras que los otros tipos de firewalls se centran en el filtrado de paquetes individuales, los firewalls de estado son capaces de realizar un seguimiento de las conexiones activas.

Netfilter (Linux)

Netfilter es el sistema de filtrado de paquetes de Linux y proporciona las capacidades de firewall a través de **iptables**. Permite a los administradores de sistemas interceptar y manipular el tráfico de red en diferentes puntos de la pila de protocolos. Puede actuar tanto de firewall de red como de firewall de host.

Iptables (Linux)

Iptables es una herramienta de filtrado de paquetes para Linux que permite a los administradores de sistemas configurar reglas de firewall en el nivel del kernel. Utiliza una arquitectura de tablas y cadenas para definir cómo se debe tratar el tráfico de red. Las principales características de iptables incluyen:

- **Filtrado de paquetes**: Permite permitir o denegar paquetes de red en función de criterios como direcciones IP, puertos y protocolos.
- **NAT (Network Address Translation)**: Permite modificar las direcciones IP de los paquetes que atraviesan el firewall, lo que es útil para la compartición de conexiones a Internet.
- **Registro de tráfico**: Puede registrar información sobre el tráfico de red, lo que ayuda en la detección de intrusiones y el análisis de seguridad.

Por defecto, iptables no tiene reglas configuradas, lo que significa que todo el tráfico está permitido. Podemos ver las reglas actuales de iptables con el siguiente comando:

```
sudo iptables -L
```

Iptables es una herramienta poderosa, pero su configuración puede ser tediosa y compleja. Por esto, se han desarrollado herramientas como **UFW** (Uncomplicated Firewall) que simplifican la gestión de iptables.

UFW (Linux)

UFW (Uncomplicated Firewall) es una interfaz de línea de comandos para iptables diseñada para facilitar la configuración de un firewall en sistemas Linux. Proporciona un conjunto de comandos simples y fáciles de usar para permitir o denegar el tráfico de red, lo que lo hace ideal para usuarios que no son expertos en seguridad de red. Esta diseñado para ser usado como un firewall de host, aunque es perfectamente capaz de funcionar como un firewall de red con configuraciones adecuadas.

Instalación de UFW

Para instalar UFW en tu sistema, puedes utilizar el gestor de paquetes de tu distribución de Linux. Por ejemplo, en Debian, puedes instalar UFW con el siguiente comando:

```
sudo apt install ufw
```

Es recomendable hacer también un update y un upgrade de los paquetes antes de instalar cualquier paquete, como UFW:

```
sudo apt update
sudo apt upgrade
```

Activación de UFW

Servicio de UFW UFW funciona en el sistema a través de un servicio que se ejecuta en segundo plano y aplica las reglas de firewall definidas por el usuario. Para que UFW funcione correctamente, es importante que el servicio esté habilitado y en ejecución. Podemos verificar el estado del servicio UFW con el siguiente comando:

```
sudo systemctl status ufw
```

En caso de que el servicio no esté activo, puedes habilitarlo con el siguiente comando:

```
sudo systemctl enable ufw
```

Mientras que si no se esta ejecutando lo puedes iniciar con el siguiente comando:

```
sudo systemctl start ufw
```

Firewall UFW Para comenzar a utilizar UFW es necesario encender el firewall con el comando:

```
sudo ufw enable
```

Para apagar UFW, puedes usar el siguiente comando:

```
sudo ufw disable
```

Diferencia entre ufw enable/disable y el servicio ufw

La diferencia entre `ufw enable`/`ufw disable` y el servicio `ufw` es que los primeros comandos se utilizan para activar o desactivar el firewall en sí, mientras que el servicio `ufw` se refiere al proceso en segundo plano que aplica las reglas de firewall definidas por el usuario. Es posible que el servicio `ufw` esté habilitado y en ejecución, pero el firewall en sí esté desactivado. Por lo tanto, es importante asegurarse de que ambos estén configurados correctamente para que el firewall funcione de la forma esperada.

Configuración de UFW

Podemos ver las reglas actuales de UFW con el siguiente comando:

```
sudo ufw status
```

o

```
sudo ufw status verbose
```

para ver detalles adicionales sobre las reglas y su estado.

Por defecto, UFW deniega todo el tráfico entrante y permite todo el tráfico saliente. Esto significa que, a menos que se agreguen reglas específicas para permitir el tráfico entrante, se bloqueará automáticamente. Ademas, el reenvio de paquetes también está deshabilitado por defecto. Esto significa que paquetes que nos lleguen a nosotros, pero vayan destinados a otra dirección, no serán reenviados.

Podemos configurar UFW para permitir el tráfico en puertos específicos, para servicios específicos o redes y direcciones IP específicas.

Puerto:

```
sudo ufw allow 22
```

Protocolo:

```
sudo ufw allow ssh
```

Dirección IP:

```
sudo ufw allow from 192.168.1.2
```

Red:

```
sudo ufw allow from 192.168.1.0/24
```

Rango de direcciones IP:

```
sudo ufw allow from 192.168.1.0/24
```

Tambien es posible limitar el tráfico en puertos específicos, para servicios específicos o redes y direcciones IP específicas. Utilizando el comando `limit` en lugar de `allow`. Esto permite controlar la tasa de conexiones y prevenir ataques de fuerza bruta o de denegación de servicio. Concretamente, permite limitar el número de conexiones en un período de tiempo determinado. Por defecto, 6 conexiones en 30 segundos.

```
sudo ufw limit ssh
```

De igual forma, podemos impedir el tráfico en puertos específicos, para servicios específicos o redes y direcciones IP específicas. Utilizando los comandos `deny` o `reject` en lugar de `allow` o `limit`. La diferencia entre `deny` y `reject` es que `deny` simplemente bloquea el tráfico sin enviar una respuesta al remitente, mientras que `reject` envía un mensaje de error al remitente indicando que el tráfico ha sido bloqueado.

```
sudo ufw deny 22
```

```
sudo ufw reject 22
```

Tambien es posible especificar reglas `allow`, `deny` y `reject` para funcionar solamente en mensajes de entrada o salida. Esto se puede hacer utilizando las opciones `in` o `out` al definir la regla.

```
sudo ufw allow in 22
```

```
sudo ufw deny out 22
```

Con `limit` esto no se puede hacer, ya que `limit` solo aplica a las conexiones entrantes.

Gestión de reglas

UFW permite gestionar las reglas de firewall de manera sencilla. Algunas de las operaciones más comunes son:

- **Listar reglas**: Para ver las reglas actuales de UFW, puedes usar el siguiente comando:

```
sudo ufw status
```

o

```
sudo ufw status verbose
```

- **Eliminar reglas**: Para eliminar una regla existente, puedes usar el siguiente comando:

```
sudo ufw delete allow 22
```

- **Ver reglas numeradas**: Para ver las reglas actuales de UFW con números de línea, puedes usar el siguiente comando:

```
sudo ufw status numbered
```

- **Eliminar reglas numeradas**: Para eliminar una regla existente utilizando su número de línea, puedes usar el siguiente comando:

```
sudo ufw delete 1
```

- **Borrar todas las reglas**: Para eliminar todas las reglas existentes de UFW, puedes usar el siguiente comando:

```
sudo ufw reset
```

Politicas por Defecto

UFW aplica políticas por defecto que determinan cómo se maneja el tráfico no especificado por ninguna regla. Las políticas por defecto son:

- **Política de entrada**: Denegar todo el tráfico entrante, a menos que se permita explícitamente.
- **Política de salida**: Permitir todo el tráfico saliente, a menos que se deniegue explícitamente.

Se pueden modificar las políticas por defecto utilizando `default` y `incoming` o `outgoing`:

```
sudo ufw default allow outgoing
```

```
sudo ufw default deny incoming
```

Windows Firewall

El Firewall de Windows es una herramienta de seguridad integrada en el sistema operativo Windows que ayuda a proteger el equipo contra accesos no autorizados y amenazas externas. Algunas de sus características son:

- **Activación y desactivación**: El Firewall de Windows se puede activar o desactivar desde el Panel de Control o la Configuración de Windows.
- **Configuración de reglas**: Se pueden crear reglas para permitir o denegar el tráfico en función de la aplicación, el puerto o la dirección IP.
- **Perfiles de red**: El Firewall de Windows permite configurar diferentes reglas según el perfil de red activo (público, privado o de dominio).
- **Registro de eventos**: El Firewall de Windows puede registrar eventos relacionados con el tráfico bloqueado o permitido, lo que facilita la supervisión y el análisis de la seguridad.

Para acceder al Firewall de Windows, abre el buscador de Windows y busca Windows Defender Firewall con seguridad avanzada. Tambien puedes pulsar windows + R, escribir “firewall.cpl” y pulsas enter.

Para agregar una regla de entrada o salida, puedes seguir estos pasos:

1. En el Firewall de Windows, haz clic en “Configuración avanzada” en el panel izquierdo.
2. Selecciona “Reglas de entrada” o “Reglas de salida” según sea necesario.
3. Haz clic en “Nueva regla” en el panel derecho y sigue el asistente para crear la regla.
4. Configura los parámetros de la regla y haz clic en “Finalizar” para guardarla.

La regla nueva aparecerá en la lista de reglas de entrada o salida, dependiendo de la opción seleccionada.

Entregable

Para esta práctica debereis crear una serie de reglas tanto en Linux con UFW como en Windows con el Firewall de Windows. Despues me tendreis que hacer y enviar una serie de capturas. En UFW me tendreis que hacer las siguientes reglas:

1. Permitir el tráfico de entrada SSH (puerto 22).
2. Limitar el tráfico de entrada HTTP (puerto 80).
3. Permitir el tráfico de entrada desde la dirección IP 192.168.1.100.
4. Denegar el tráfico de salida hacia la dirección IP 192.168.1.200.

En el Firewall de Windows me tendreis que hacer las siguientes reglas:

1. Permitir el tráfico de entrada RDP (puerto 3389).
2. Limitar el tráfico de entrada ICMP (ping).
3. Permitir el tráfico de entrada desde la dirección IP 192.168.1.100.
4. Denegar el tráfico de salida hacia la dirección IP 192.168.1.200.

Capturas a entregar

- Captura de pantalla del estado del servicio UFW.
- Captura de pantalla del estado de UFW con las reglas creadas.
- Captura de pantalla del estado del Firewall de Windows con las reglas de entrada creadas.
- Captura de pantalla del estado del Firewall de Windows con las reglas de salida creadas.