Sesión #7 - Configuración de un Firewall en un Entorno de Red (Resuelto)

Título del Laboratorio: Configuración de un Firewall en un Entorno de Red
Duración: 2 horas

Objetivos del Laboratorio:

1. Implementar políticas de filtrado de tráfico entrante y saliente.
2. Configurar reglas de seguridad para servicios específicos.
3. Monitorear y ajustar la configuración del firewall.

Materiales Necesarios:

- Repositorio en GitHub
- Acceso a Academia Cisco
- Computador
- Acceso a internet

Estructura del Laboratorio:

Parte 1: Introducción al Firewall y Entorno de Configuración
Paso 1: Revisión de la Configuración de Red Actual

- Ejecutar ip a o ifconfig para ver la interfaz activa.
- Confirmar la IP asignada y puerta de enlace con ip route.
- Verificar conectividad con ping 8.8.8.8 y ping google.com.

Paso 2: Instalación y Verificación del Firewall

- Instalar UFW en Ubuntu:
- sudo apt update
- sudo apt install ufw
- sudo ufw status verbose

Parte 2: Configuración Básica del Firewall
Paso 3: Configuración de Políticas por Defecto

sudo ufw default deny incoming

sudo ufw default allow outgoing

Paso 4: Permitir Tráfico para Servicios Específicos

sudo ufw allow ssh

sudo ufw allow http

sudo ufw allow https

sudo ufw enable

Parte 3: Configuración Avanzada del Firewall
Paso 5: Crear Reglas de Filtrado por IP

sudo ufw deny from 192.168.0.100

sudo ufw allow from 192.168.0.50 to any port 22

Paso 6: Configuración de Reglas para Redes Internas y Externas

sudo ufw allow from 192.168.0.0/24

sudo ufw deny from 203.0.113.0/24

Parte 4: Monitoreo y Ajustes del Firewall
Paso 7: Monitoreo de Logs del Firewall

sudo less /var/log/ufw.log

sudo ufw logging on

Paso 8: Ajuste de Reglas Basado en Monitoreo

sudo ufw deny from [IP_sospechosa]

sudo ufw status numbered

sudo ufw delete [número_regla]