# Sesión #7 - Configuración de un Firewall en un Entorno de Red

Estudiante: Dilan Aragón

## Informe de Comandos Usados

Comandos Iniciales de Instalación y Preparación  
  
- sudo su  
 Eleva los privilegios del usuario actual a superusuario (root), permitiendo ejecutar comandos administrativos sin anteponer sudo.  
  
- apt install ufw -y  
 Instala el firewall UFW (Uncomplicated Firewall). El parámetro -y aprueba automáticamente la instalación sin solicitar confirmación.  
  
- clear  
 Limpia la pantalla del terminal para mejor visibilidad.  
  
Habilitación y Verificación de UFW  
  
- ufw enable  
 Activa el firewall UFW.  
  
- ufw status  
 Muestra el estado actual de UFW (activo/inactivo) y las reglas aplicadas.  
  
Instalación y Verificación de iptables  
  
- apt install iptables -y  
 Instala la herramienta iptables, que permite configurar reglas de filtrado de paquetes a bajo nivel en Linux.  
  
- iptables -L  
 Lista todas las reglas activas actualmente en las cadenas de INPUT, FORWARD y OUTPUT.  
  
Políticas Predeterminadas  
  
- ufw default deny incoming  
 Bloquea por defecto todas las conexiones entrantes que no estén explícitamente permitidas.  
  
- ufw default allow outgoing  
 Permite por defecto todas las conexiones salientes.  
  
- iptables -P INPUT DROP  
 Establece como política por defecto denegar (DROP) todos los paquetes entrantes en iptables.  
  
- iptables -P OUTPUT ACCEPT  
 Permite por defecto todos los paquetes salientes.  
  
Permitir Puertos Comunes (SSH, HTTP, HTTPS)  
  
- ufw allow ssh  
 Permite el tráfico entrante al puerto 22 (usado para SSH).  
  
- ufw allow http  
 Permite el tráfico entrante al puerto 80 (HTTP).  
  
- ufw allow https  
 Permite el tráfico entrante al puerto 443 (HTTPS).  
  
- iptables -A INPUT -p tcp --dport 22 -j ACCEPT  
 Permite conexiones TCP entrantes al puerto 22 (SSH) en iptables.  
  
- iptables -A INPUT -p tcp --dport 80 -j ACCEPT  
 Permite conexiones TCP entrantes al puerto 80 (HTTP).  
  
- iptables -A INPUT -p tcp --dport 443 -j ACCEPT  
 Permite conexiones TCP entrantes al puerto 443 (HTTPS).  
  
Ver Reglas Enumeradas  
  
- ufw status numbered  
 Muestra las reglas UFW en formato numerado, útil para modificar o eliminar reglas específicas.  
  
Denegar Acceso de IPs Específicas  
  
- ufw deny from 192.168.1.20  
 Bloquea todo el tráfico proveniente de la dirección IP 192.168.1.20.  
  
- ufw deny from 198.168.1.32  
 Bloquea todo el tráfico proveniente de 198.168.1.32.  
  
Permitir Acceso de IP Específica  
  
- ufw allow from 198.168.1.32  
 Permite explícitamente el tráfico desde la IP 198.168.1.32.  
  
- iptables -A INPUT -s 192.168.1.45 -j ACCEPT  
 Permite todo el tráfico entrante desde la dirección IP 192.168.1.45.  
  
Revisar y Eliminar Reglas  
  
- iptables -L –line-numbers  
 Lista las reglas de iptables incluyendo el número de línea, útil para borrarlas.  
  
- iptables -D INPUT 9  
 Elimina la regla número 9 de la cadena INPUT.  
  
Bloqueo de Puertos Específicos  
  
- ufw deny from any to any port 8080  
 Bloquea todo tráfico (de cualquier origen a cualquier destino) hacia el puerto 8080.  
  
- ufw deny from any to any port 4200  
 Bloquea el puerto 4200, comúnmente usado por servidores de desarrollo Angular.  
  
- iptables -A INPUT -p tcp --dport 8080 -j DROP  
 Agrega una regla que bloquea el tráfico TCP entrante al puerto 8080.  
  
Resumen General  
  
En este laboratorio se configuraron dos firewalls: UFW (de alto nivel, más sencillo) y iptables (de bajo nivel, más flexible). Se aplicaron reglas de denegación y permisos para proteger el sistema, así como bloqueos de puertos y filtrado por IP, configurando un entorno más seguro para los servicios en red.