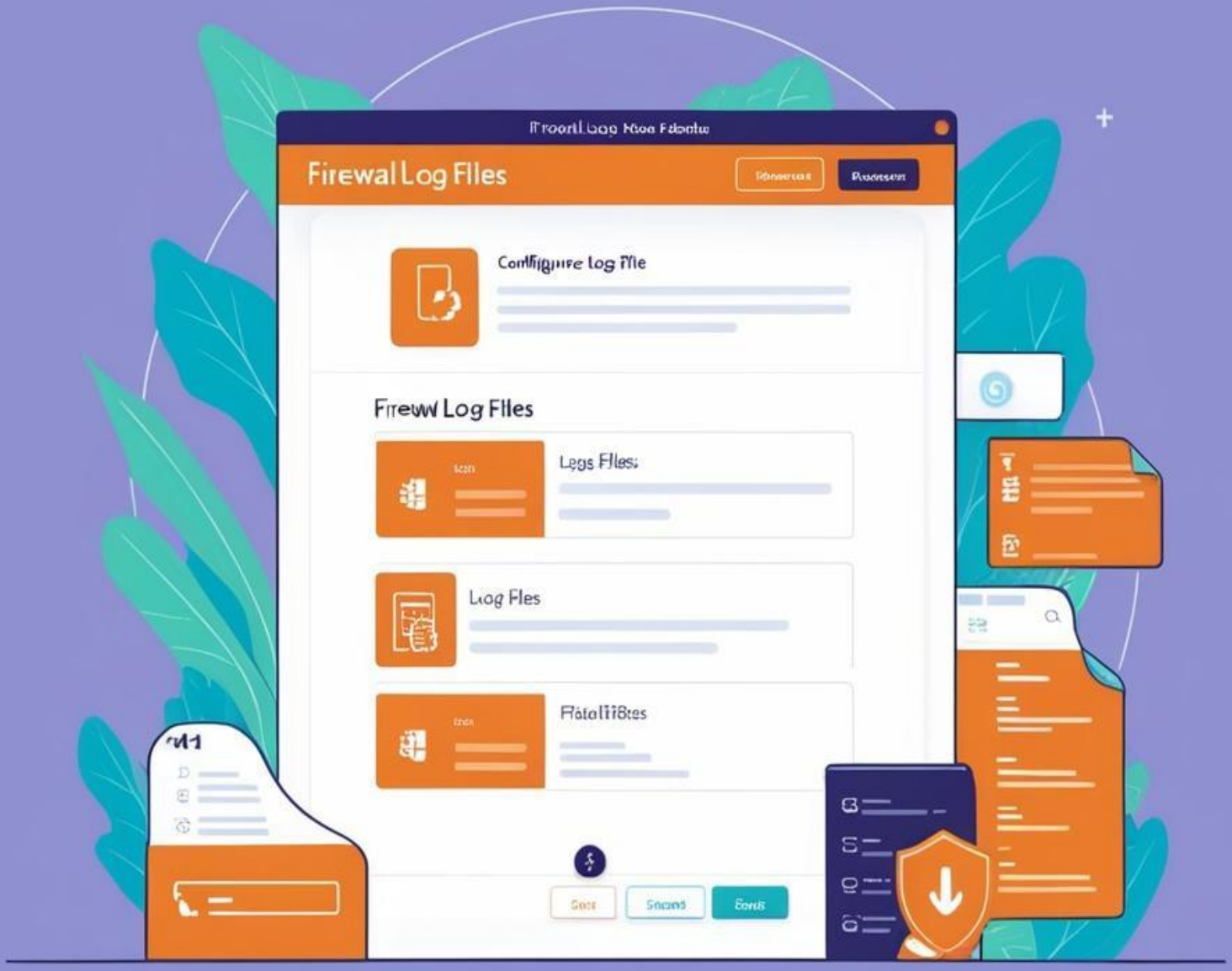
Configuración de los Ficheros log del cortafuego



Ivana Sánchez Pérez

Introducción

Los archivos de log del cortafuegos son registros detallados de las actividades que ocurren en el cortafuegos. Estos registros son esenciales para la seguridad y el monitoreo de la red, ya que permiten a los administradores identificar y analizar posibles amenazas o intrusiones.

¿Qué es un archivo de log del cortafuegos?

Un archivo de log del cortafuegos es un documento que registra todas las conexiones y actividades que pasan a través del cortafuegos. Estos registros pueden incluir información como:

- Direcciones IP de origen y destino
- Puertos utilizados
- Protocolos empleados
- Horarios de las conexiones
- Acciones tomadas por el cortafuegos (permitir, denegar, bloquear)

Importancia de los archivos de log del cortafuegos

1. **Monitoreo de la seguridad**: Los archivos de log permiten a los administradores monitorear las actividades de la red y detectar comportamientos sospechosos o no autorizados.
2. **Análisis de incidentes**: En caso de una brecha de seguridad, los archivos de log pueden ayudar a identificar cómo ocurrió el incidente y qué secciones de la red fueron afectadas.
3. **Cumplimiento y auditoría**: Los registros de cortafuegos son cruciales para cumplir con regulaciones y estándares de seguridad, así como para realizar auditorías internas y externas.
4. **Optimización del rendimiento**: Analizando los logs, los administradores pueden identificar patrones de tráfico y ajustar las políticas del cortafuegos para mejorar el rendimiento de la red.

Ejemplos de herramientas y sistemas de log

- **iptables**: Utilizado en sistemas Linux para configurar y gestionar reglas de cortafuegos.
- **Firewall-1 de Check Point**: Incorpora un módulo de inspección con estado (stateful inspection) que registra todas las actividades en el cortafuegos.

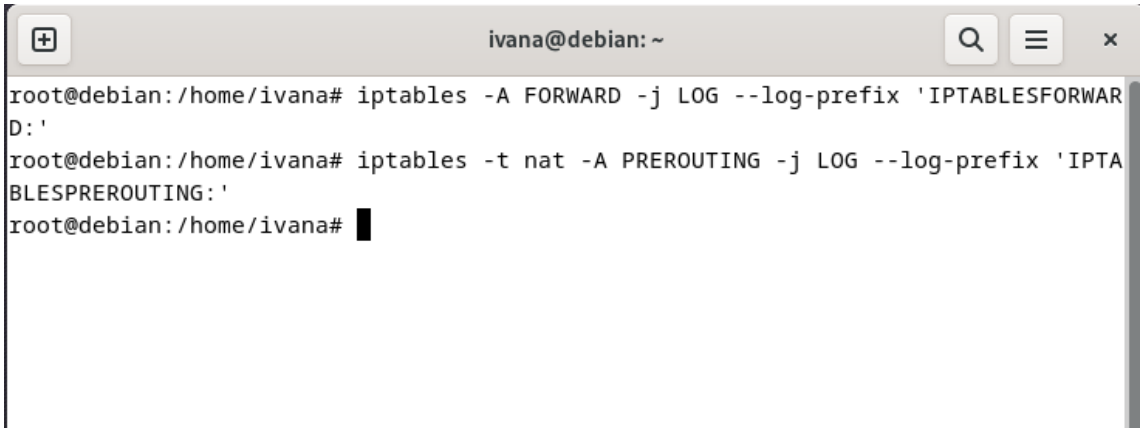
- **Cisco ASA**: Un cortafuegos de hardware que proporciona registros detallados de todas las conexiones y actividades.
- **ELK Stack (Elasticsearch, Logstash, Kibana)**: Una herramienta popular para la recolección, almacenamiento y visualización de logs de cortafuegos.

Conclusión

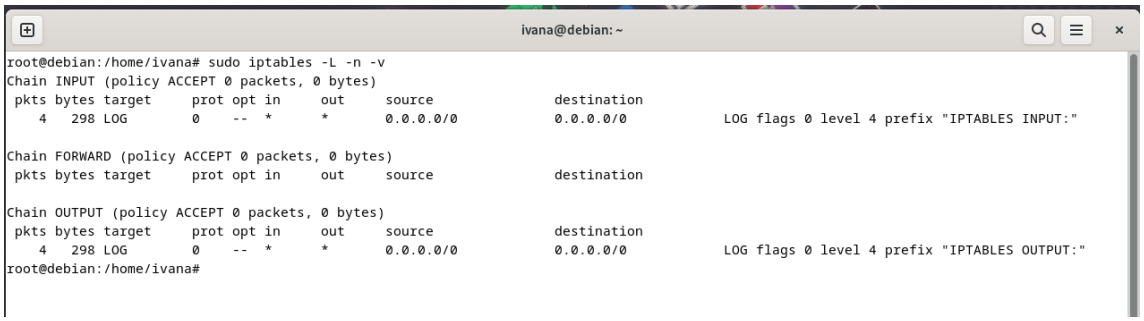
Los archivos de log del cortafuegos son una herramienta fundamental para la seguridad de la red. Permiten a los administradores monitorear, analizar y optimizar el rendimiento del cortafuegos, así como cumplir con regulaciones y realizar auditorías.

Configuración de los archivos log

1- Agregamos las reglas de iptables para registrar paquetes y almacenarlas en el archivo logs con:
   - sudo iptables -A FORWARD -j LOG --log-prefix 'IPTABLESFORWARD: '
   - sudo iptables -t nat -A PREROUTING -j LOG --log-prefix 'IPTABLESPREROUTING: '



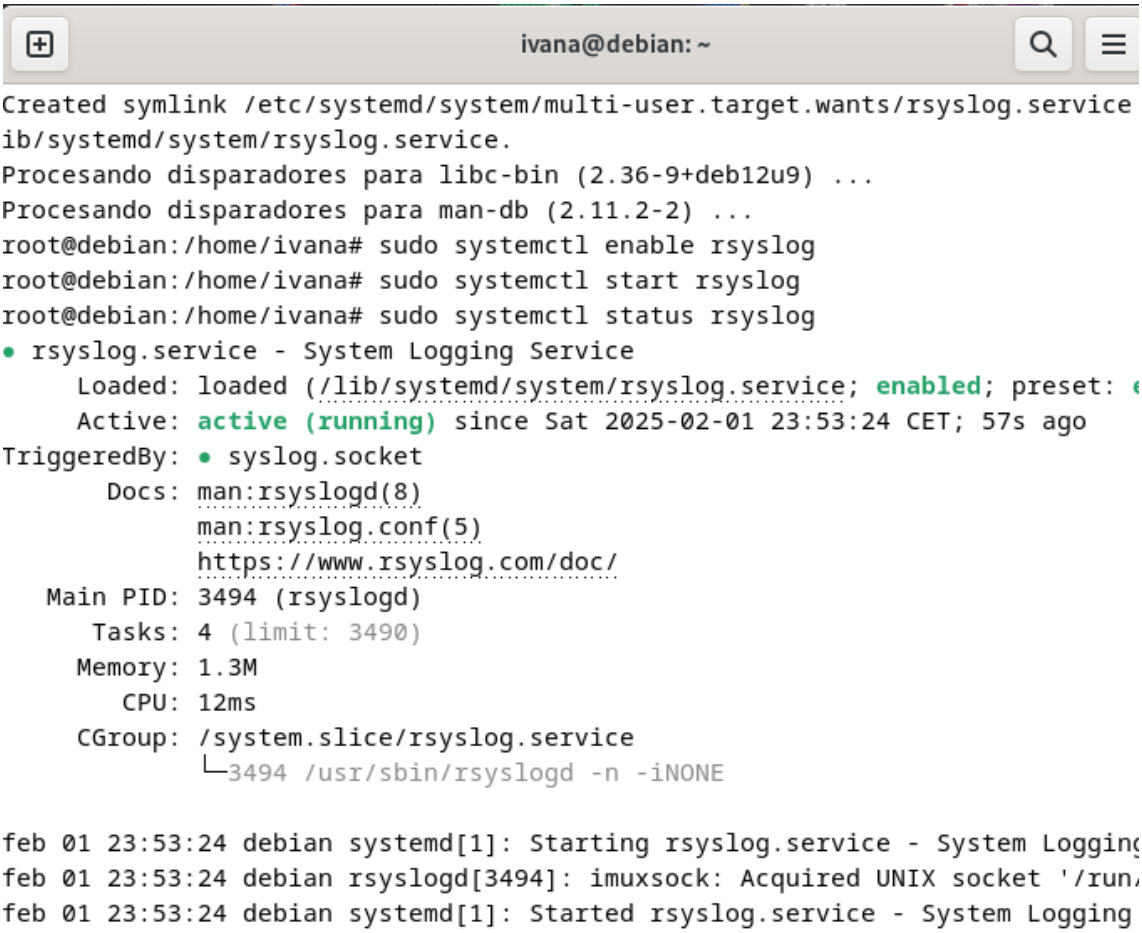
Con las reglas anteriores no se han añadido reglas en las cadenas INPUT o OUTPUT, que son esenciales para registrar tráfico entrante o saliente directamente relacionado con nuestro sistema. Por lo que procedo a ajustar y completar la configuración.



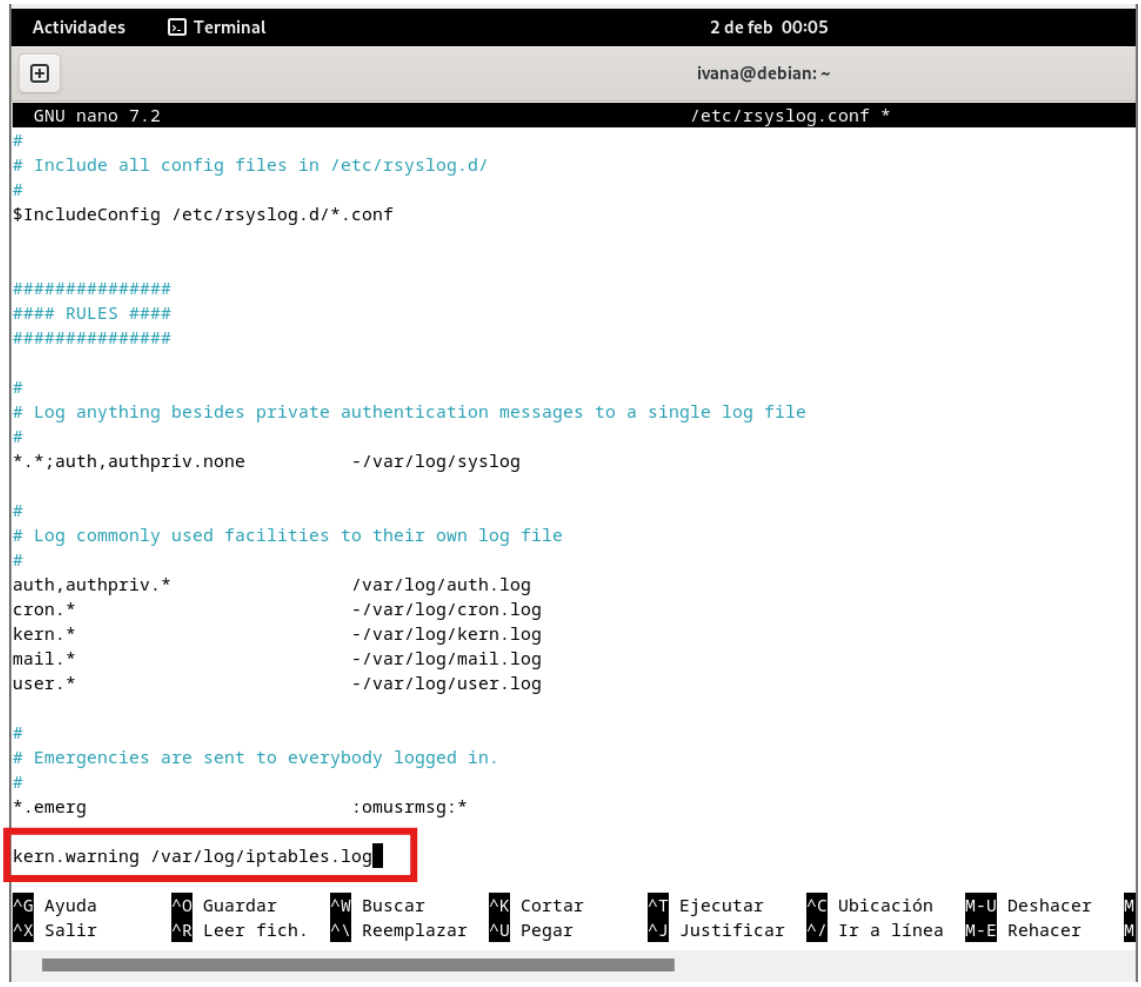
Explicación:

- -A FORWARD: Agrega una regla a la cadena FORWARD.
- -t nat -A PREROUTING: Agrega una regla en la tabla NAT antes de reenviar paquetes.
- -j LOG: Indica que los paquetes deben ser registrados en los logs.
- --log-prefix: Agrega un prefijo a los registros para identificarlos fácilmente.

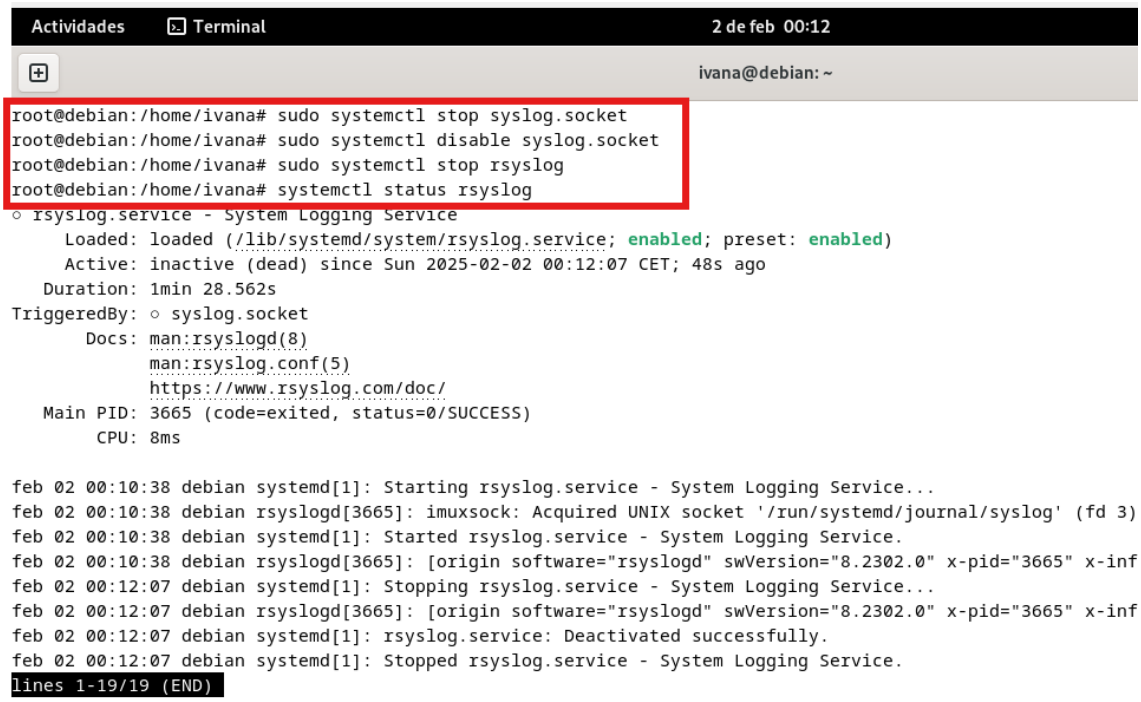
2- Configuramos el sistema de logs. Para ello primero instalamos e iniciamos el sistema rsyslog.

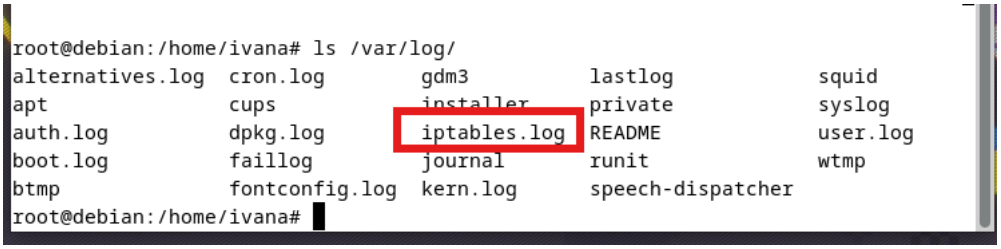


Y posteriormente editamos el archivo de configuración de rsyslog para asegurarnos que el sistema almacene los registros en un archivo separado. Hacemos un sudo nano /etc/rsyslog.conf y le añadimos la línea kern.warning /var/log/iptables.log al final del mismo. Esta línea nos indica que los mensajes de nivel "warning" generados por el kernel se guardaran en el archivo iptables.log.

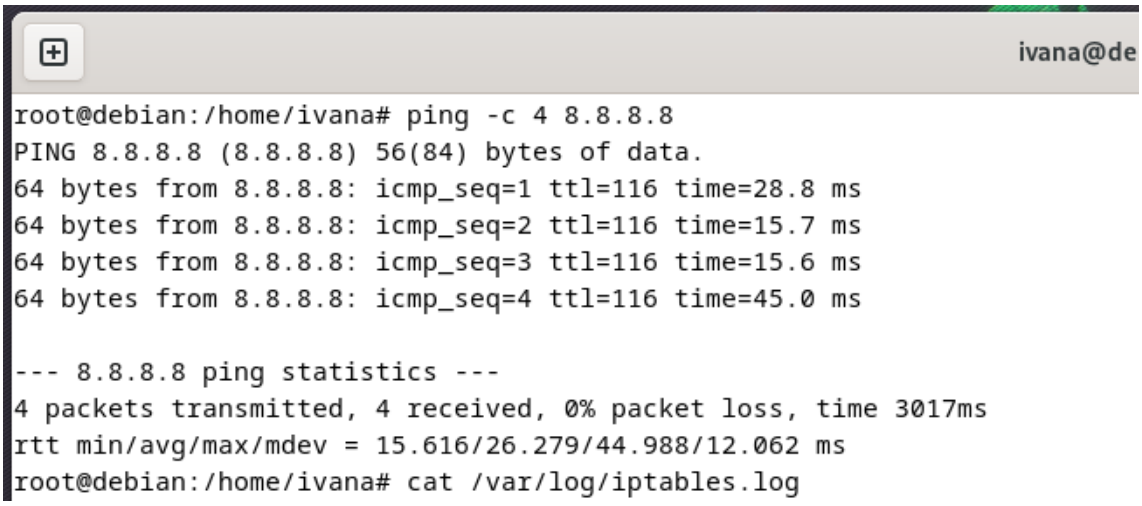


Reiniciamos y verificamos el servicio

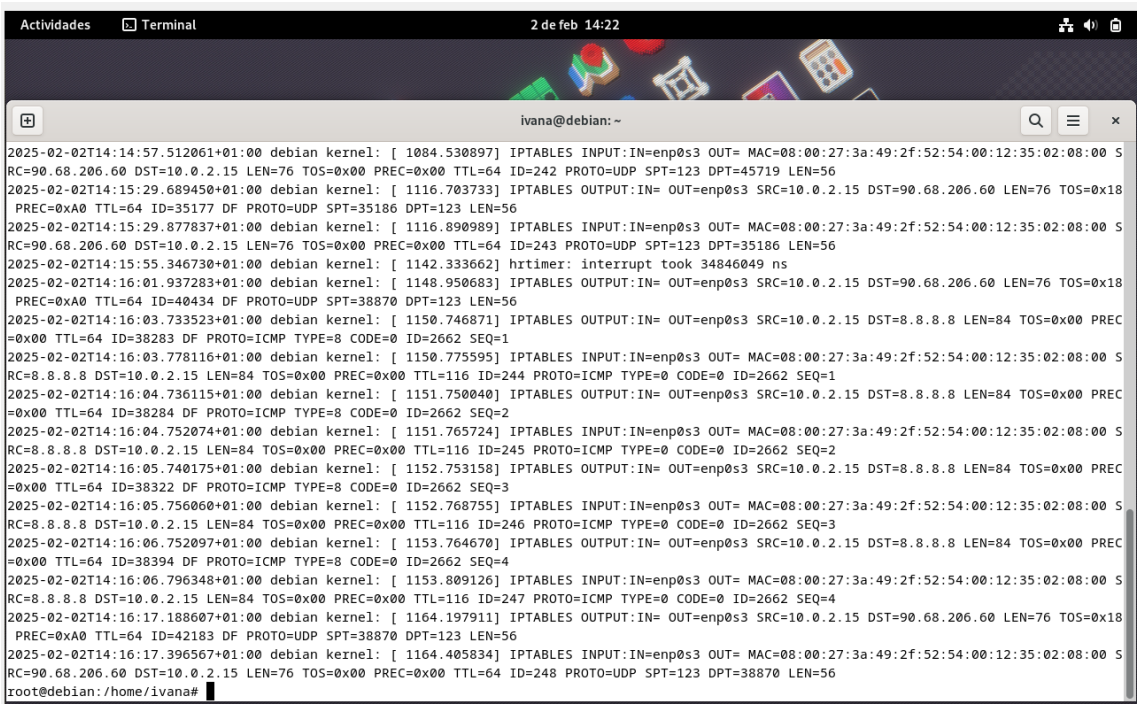




Verificamos que los logs se están generando. Si no lo vemos inmediatamente, generamos el tráfico para que iptables tenga algo que registrar. Y ahora ya podemos verificar que iptables está registrando con el comando sudo tail -f /var/log/iptables.log. También lo podemos ver con un cat /var/log/iptables.log



Analizamos los registros. Cada línea en el log contiene información clave



Explicación de los datos registrados:

1. **Fecha y hora** → 2025-02-02 14:14:57
2. **Nombre del equipo** → debian
3. **Código del log del kernel** → kernel:
4. **Prefijo personalizado** → [IPTABLES INPUT]
5. **Interfaces de red** → IN=enp0s3

6. **Direcciones MAC** → OUT =MAC=08:00:27:3a:49:2f:52:54:00:12:35:02:08:00
7. **Dirección IP de origen** → SRC=90.68.206.60
8. **Dirección IP de destino** → DST=10.0.2.15
9. **Longitud del paquete** → LEN=76
10. **Tipo de servicio (ToS)** → TOS=0x00 PREC=0x00
11. **Tiempo de vida (TTL)** → TTL=64
12. **ID de reensamblaje** → ID=242
13. **Protocolo de transporte** → PROTO=UDP
14. **Puerto de origen** → SPT=123
15. **Puerto de destino** → DPT=45719 LEN=56