

PRÁCTICA

NOMBRE: Analizador de Tráfico IPTRAF.			TEMA: Tres.	número	09
SUBTEMA: 3.4 Análisis de desempeño de la red: tráfico y servicios.	VALOR: 20%	LUGAR: Aula de clases			
ALUMNOS: Brenda Ciclali Ortiz Fonseca Clara Luz Milagro García Diana Paola Santiago Pelayo Ricardo Samuel Carranza Marcial	GRUPO: 803-AB	FECHA: 10/04/2025			

1. Objetivo.

Instalar iptraf en el sistema Operativo Ubuntu Server.

2. Material a usar

Hardware:

- PC, Dispositivo móvil o tableta por alumno

Software:

- Procesador de texto mínimo.
- Oracle VM Virtual Box.
- Ubuntu Server.

De apoyo:

- Internet
- Apuntes de la clase

4. Marco Teórico

Análisis de Desempeño de la Red.

Es el proceso de evaluar y medir el funcionamiento de una red de comunicaciones para garantizar que opere de manera eficiente, confiable y segura. Este análisis ayuda a identificar problemas, optimizar recursos y mejorar la experiencia del usuario.

Características Principales

- ✓ Detección temprana de cuellos de botella.
- ✓ Optimización de recursos de red.
- ✓ Mejora en la calidad de servicio (QoS).
- ✓ Prevención de fallos críticos.
- ✓ Cumplimiento de SLAs (Acuerdos de Nivel de Servicio).
- ✓ Métricas principales evaluadas: Ancho de banda, latencia, pérdida de paquetes, disponibilidad.

El análisis de desempeño de la red es esencial para mantener una infraestructura de comunicaciones estable y eficiente. Permite tomar decisiones basadas en datos para corregir problemas, planear escalamientos y asegurar una experiencia óptima para los usuarios.

Tráfico.

El tráfico de red se refiere al flujo de datos que circula a través de una red, incluyendo paquetes, señales y mensajes entre dispositivos. Este tráfico puede ser: Datos (HTTP, FTP, P2P), Voz (VoIP), Vídeo (Streaming, Videollamadas) y Mensajería (Correos, Chat).

Características principales:

- ✓ Ancho de banda: Capacidad de transmisión de la red (ej. Mbps, Gbps).
- ✓ Tasa de transferencia: Velocidad real de los datos transmitidos.
- ✓ Latencia: Tiempo que tarda un paquete en llegar desde el origen al destino.
- ✓ Jitter: Variabilidad en la latencia (afecta a VoIP y streaming).
- ✓ Pérdida de paquetes: Paquetes que no llegan a su destino.

Servicios.

Son las aplicaciones o funcionalidades que utilizan el tráfico para operar. Estos pueden ser: Servicios de Conectividad: DNS, DHCP, VPN, Servicios de Aplicación: Correo electrónico (SMTP), Web (HTTP/HTTPS), VoIP (SIP) y Servicios de Gestión: SNMP (monitoreo), QoS (Calidad de Servicio).

El tráfico determina cómo se mueven los datos, mientras que los servicios definen qué aplicaciones usan esos datos. Un buen análisis de red permite optimizar ambos para garantizar velocidad, baja latencia y alta disponibilidad.

IPTRAF es una herramienta de análisis de tráfico basada en terminal que proporciona estadísticas detalladas sobre: Tráfico por interfaz, Protocolos (TCP, UDP, ICMP), Conexiones activas (IPs remotas, puertos) y filtrado avanzado (por puerto, rango de IPs, etc.).

4. Metodología

PASOS PARA REALIZAR LA PRACTICA:

Paso 1: Instalar y configurar Iptraf en el sistema Operativo Ubuntu Server.

Paso 2: Ejecutar Iptraf.

Paso 3: Monitorear el tráfico de la red.

REPORTE DE LA PRÁCTICA

6. Desarrollo

Contestas las siguientes preguntas:

1.- Consideras que IPTRAF, nos permite monitorear el análisis de Desempeño de red. ¿Por qué?

Ricardo Samuel Carranza Marcial: Si, ya que nos permite monitorear el desempeño de red porque capta y analiza en tiempo real el tráfico que pasa por las interfaces de red del sistema y está nos va ofreciendo datos clave que ayudan a entender cómo se está comportando la red. Como también el uso de ancho de banda, estadísticas detalladas por conexiones y la detección del tráfico de red anómalo

2.- Describe que nos muestra Iptraf, cuando ejecutamos IP Traffic Monitor.

Brenda Ciclali Ortiz Fonseca: Iptraf es una herramienta de línea de comandos que se utiliza para monitorear el tráfico de red. Cuando se ejecuta IP Traffic Monitor, Iptraf muestra información sobre las conexiones TCP y UDP, así como sobre los paquetes ICMP y IGMP. También muestra información sobre los paquetes capturados, como el número de paquetes, el número de bytes, la tasa de flujo TCP y el número de gotas. En la máquina virtual que realizamos el análisis de red muestra que hay 28 paquetes capturados, 7118 bytes, una tasa de flujo TCP de 0,00 kbps y 97 abandonos. También muestra que hay una conexión TCP activa de 192.168.1.40:22 a 192.168.1.34:56020. En este caso es nuestra red de la máquina virtual y el cmd.

3.- Consideras que el administrador de una red debe de utilizar la herramienta Iptraf.

Clara Luz Milagro García: Sí, considero que el administrador de una red debe utilizar la herramienta IPTraf, ya que es una herramienta ligera, eficiente y muy útil para el monitoreo del tráfico en tiempo real dentro de redes basadas en Linux, como Ubuntu Server. Pues ayuda a detectar cuellos de botella, identificar anomalías o comportamientos sospechosos en la red y nos ayuda a tomar decisiones rápidas para optimizar el rendimiento y la seguridad de la red.

4.- Además de analizar el tráfico de la red, que otras tareas podemos realizar con Iptraf.

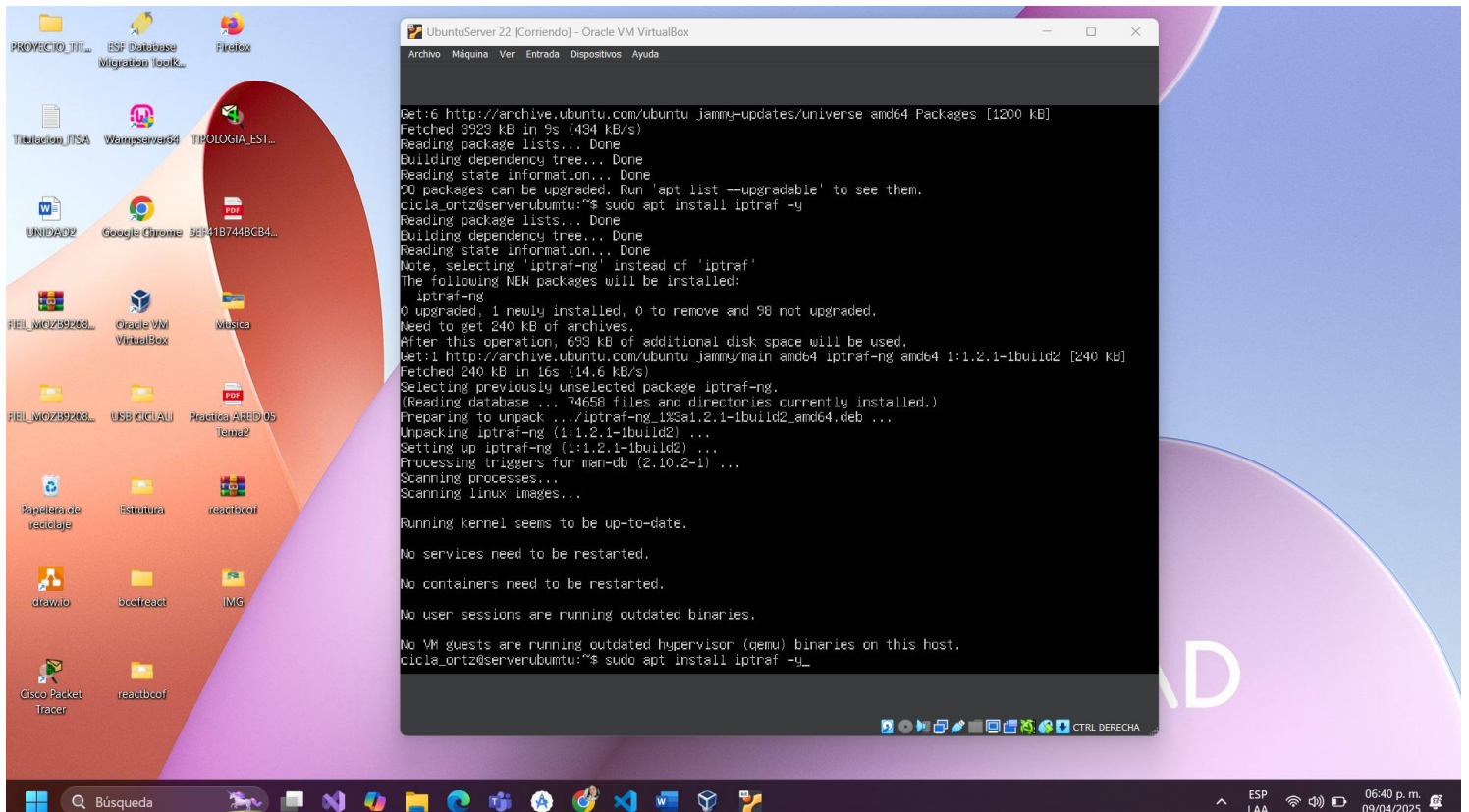
Diana Paola Santiago Pelayo: Además de analizar el tráfico de la red, con Iptraf también se pueden hacer otras cosas. Por ejemplo, se pueden ver estadísticas de cada interfaz de red, revisar las conexiones activas y ver qué protocolos se están usando. También sirve para detectar si hay algo raro en la red o si alguna conexión está usando demasiado ancho de banda. Me pareció útil porque da una visión más completa de lo que pasa en tiempo real.

7. Resultados

(Agregar capturas de pantalla de los pasos 1,2,3.

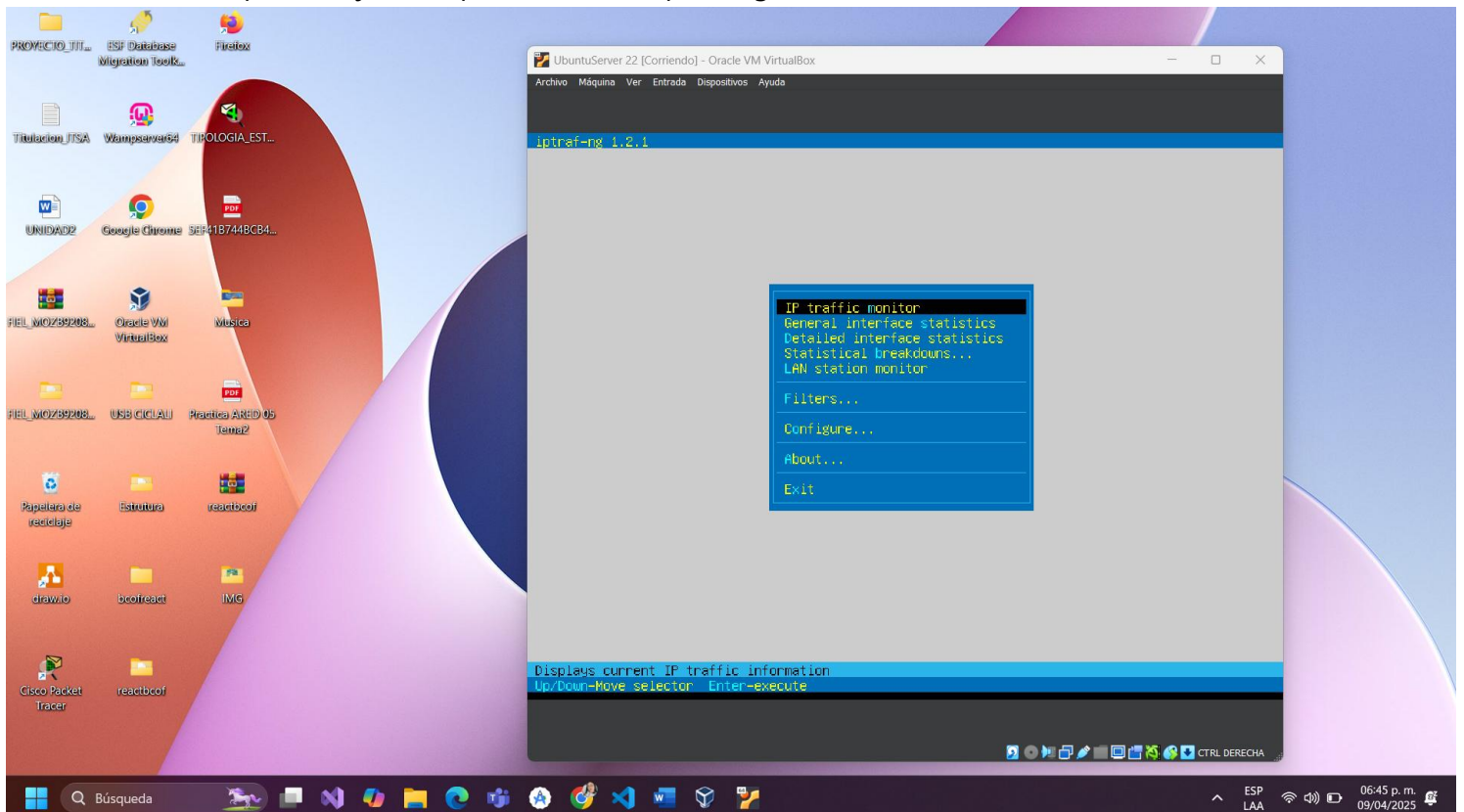
Paso 1: Instalar Iptraf

Iptraf está disponible en los repositorios estándar de Ubuntu. Para instalarlo: `sudo apt install iptraf -y`



Paso 2: Ejecutar Iptraf

Una vez instalado, puedes ejecutar Iptraf con: `sudo iptraf-ng`



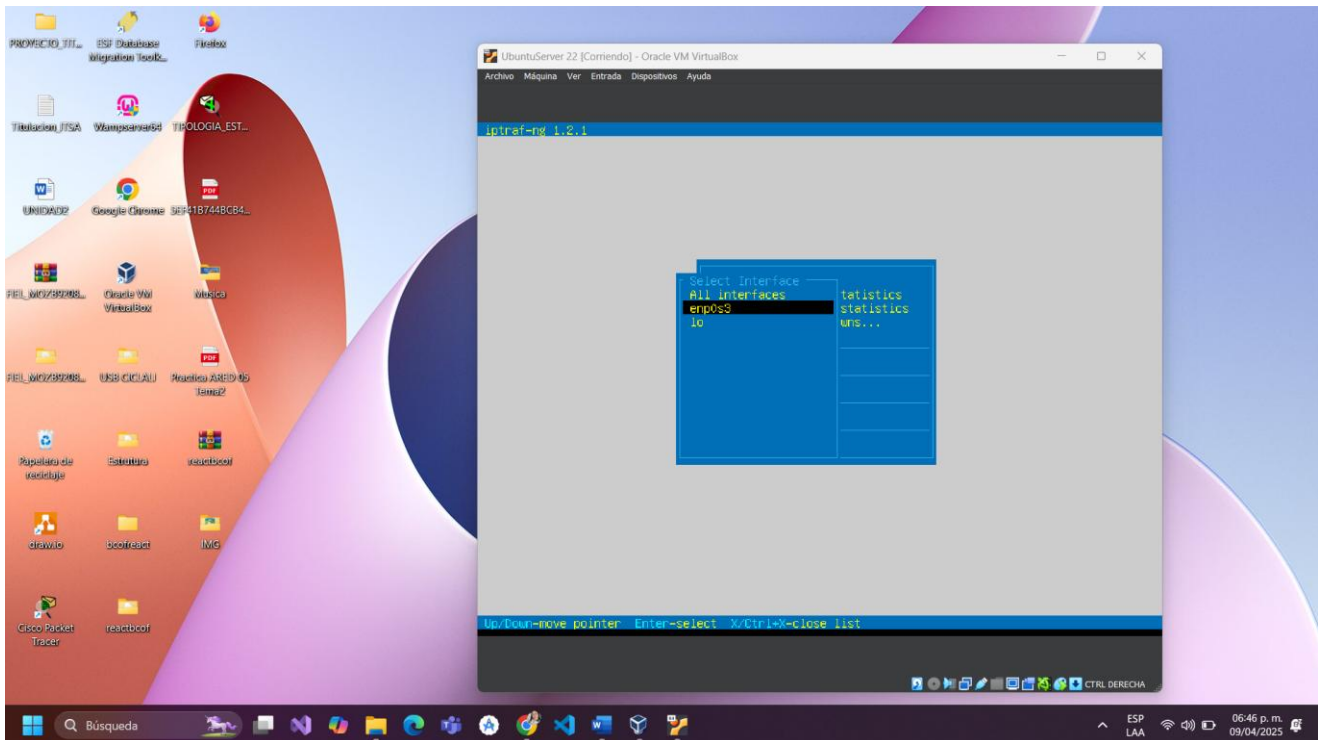
Paso 2: Monitorear el Tráfico de Red

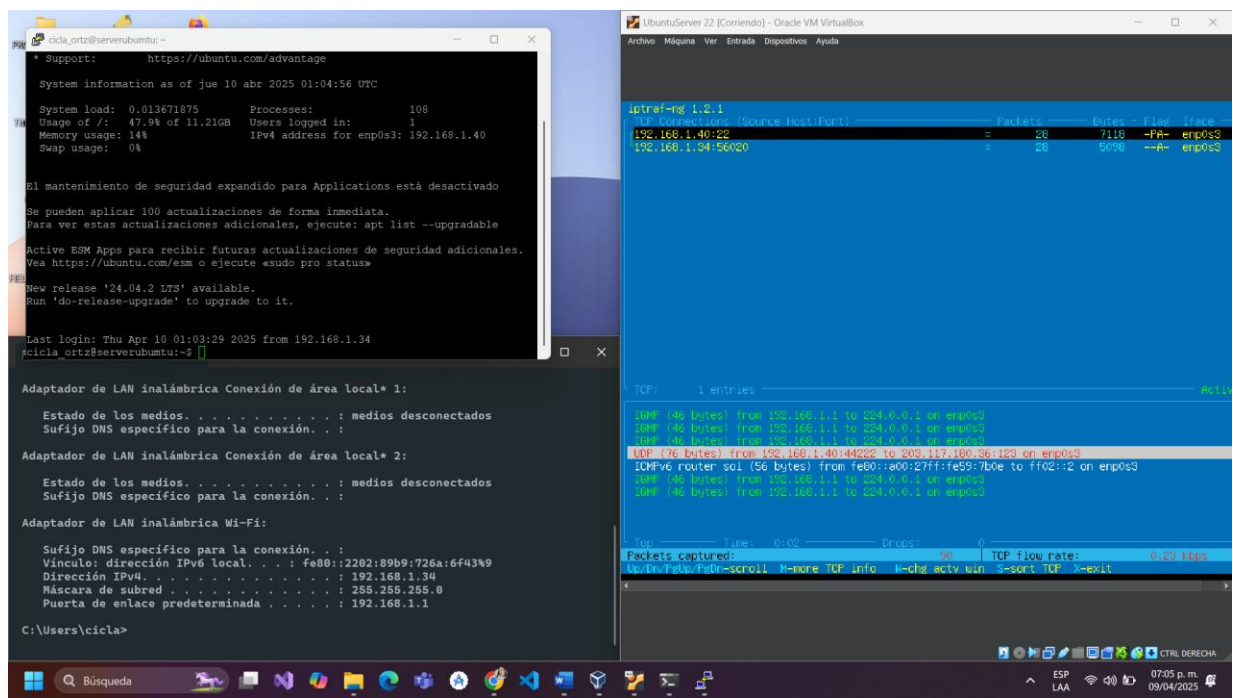
Opción 1: Monitorear el Tráfico IP General

1. Selecciona la opción 1. IP traffic monitor (presiona 1 y luego Enter).
2. Elige la interfaz de red ens33.

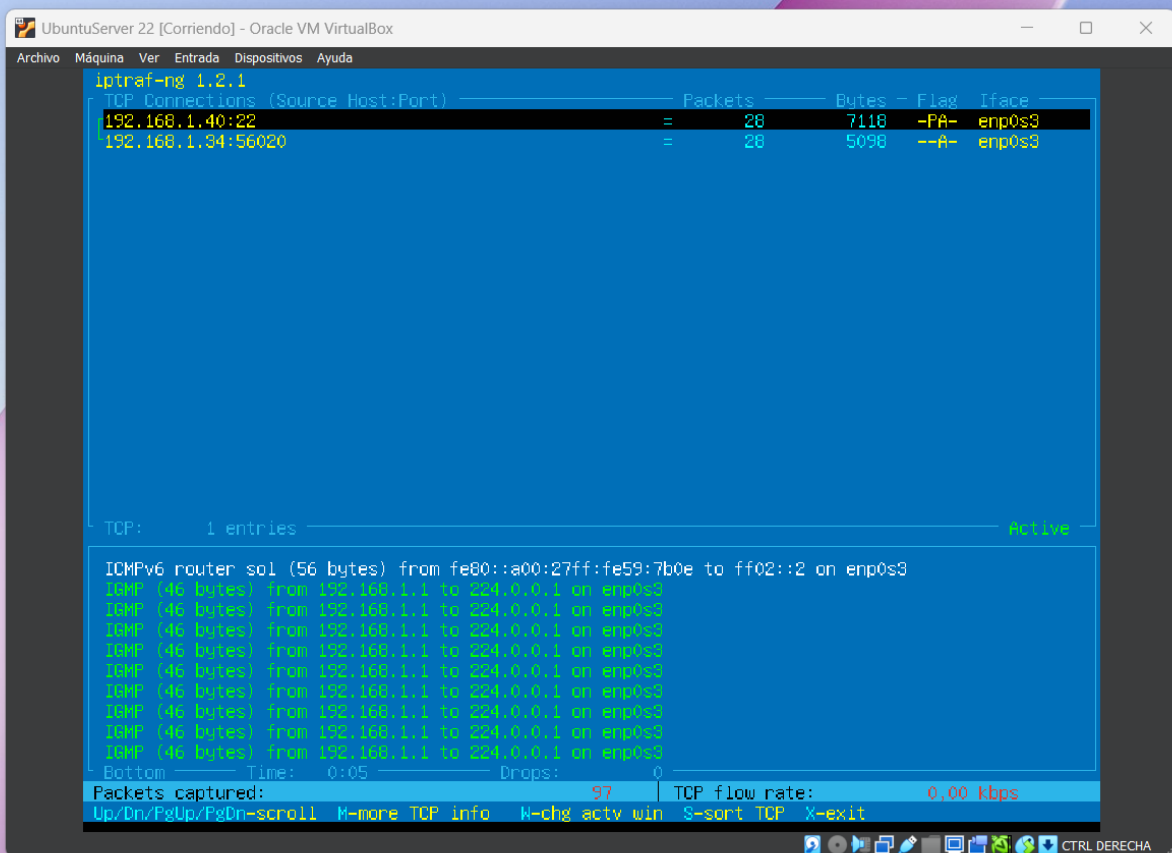
Verás en tiempo real:

- Conexiones activas (TCP/UDP)
- Direcciones IP origen/destino
- Paquetes enviados/recibidos
- Ancho de banda utilizado





Si probamos a descargar un fichero desde internet, veremos como muestra la ip desde donde se está descargando, con todos los paquetes y bytes recibidos.



También hay un apartado para ver las estadísticas de la interfaz de red.

Trabaja en...
Desarrolla...
172.16.1.1
Descarga...
Nueva...

cidla_ortz@serverubuntu: ~
Des:1 http://archive.ubuntu.com/ubuntu jammy-updates
e-8.0 amd64 8.0.41-0ubuntu0.22.04.1 [2.716 kB]
Descargados 2.716 kB en 3s (926 kB/s)
Seleccionando el paquete mysql-client-core-8.0 prev
(leyendo la base de datos ... 74794 ficheros o dire
e.)
Preparando para desempaquetar .../mysql-client-core
amd64.deb ...
Desempaquetando mysql-client-core-8.0 (8.0.41-0ubun
Configurando mysql-client-core-8.0 (8.0.41-0ubuntu0
Procesando disparadores para man-db (2.10.2-1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu)
cidla_ortz@serverubuntu:~\$

UbuntuServer 22 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Iptraf-ng 1.2.1
Iface Total IPv4 IPv6 NonIP BadIP Activity
enp0s3 3082 3082 0 0 0 0,00 kbps
lo 12 12 0 0 0 0,00 kbps

Time: 0:01 Total: 0,00 kbps / 0 pps Drops: 0
Up/Down/PsUp/PsDn-scroll window X=exit

Compartir
Complementos
Complementos
8. Conclusiones
e lo contrario el valor de la

NOTA: La conclusión deberá estar formada de al menos 6 líneas, de lo contrario el valor de la conclusión será de 0 puntos.

Brenda Ciclali Ortiz Fonseca: En esta práctica realice una instalación y utilice **IPTRAF** en **Ubuntu Server**, una herramienta clave para el monitoreo y análisis del tráfico de red. A través de su interfaz, pudimos observar métricas esenciales como el ancho de banda, las conexiones activas y el comportamiento de los protocolos, lo que refuerza su utilidad en el **análisis de desempeño de red**. En mi experiencia demostré que estas herramientas son fundamentales para identificar posibles cuellos de botella, optimizar recursos y garantizar una red eficiente. Además, esta práctica consolide mis conocimientos sobre el monitoreo de tráfico, reforzando la importancia de evaluar constantemente la red para mantener su estabilidad y seguridad.

Diana Paola Santiago Pelayo: Durante esta práctica observé cómo se instaló y configuró Iptraf en Ubuntu Server. Aunque no lo hice personalmente, seguí cada paso y entendí cómo funciona esta herramienta para monitorear el tráfico de red en tiempo real. Pude ver cómo muestra datos como direcciones IP, protocolos y cantidad de información transmitida. Esto me ayudó a comprender mejor la importancia de analizar el comportamiento de la red para detectar problemas o mejorar el rendimiento y entendí que herramientas como Iptraf pueden ser clave para el análisis del rendimiento y la seguridad en sistemas Linux.

Clara Luz Milagro García: Durante esta práctica realizamos el análisis del desempeño de una red utilizando la herramienta IPTraf en un sistema Ubuntu Server. Esta herramienta nos permitió monitorear de forma detallada el tráfico de red, visualizar las conexiones activas, protocolos utilizados y la actividad en tiempo real. Gracias a esta práctica, reforzamos la importancia de contar con herramientas de monitoreo como IPTraf para mantener redes estables y tomar decisiones informadas. También comprendimos la relación entre el tráfico y los servicios de red, y cómo un buen monitoreo permite mejorar la calidad del servicio.

Ricardo Samuel Carranza Marcial: En esta práctica, pude comprender cómo instalar, configurar y utilizar la herramienta Iptraf en un entorno Ubuntu Server. La instalación fue sencilla mediante el uso del gestor de paquetes, y una vez ejecutado el programa, me sorprendió la interfaz clara que ofrece para monitorear el tráfico de red en tiempo real. A través del monitoreo, observé las conexiones activas, el uso del ancho de banda y otros detalles importantes del tráfico entrante y saliente. Esta experiencia me permitió valorar la utilidad de Iptraf como una herramienta ligera pero poderosa para la administración y supervisión de redes en servidores Linux.