Universidad Tecnológica de Panamá

Facultad de Sistemas Computacionales

Asignatura: Desarrollo de Software IV

Laboratorio Práctico 2

Profesor: Napoleón Ibarra

Estudiantes: Francisco Hernández, Roderick Muñoz

Fecha de entrega: 18/09/2025

1. Introducción

En este documento se presentan los pasos realizados en el Laboratorio Práctico 2 de la asignatura Desarrollo de Software IV. El laboratorio se enfocó en el desarrollo de un prototipo web y en la simulación de un ataque DDoS dentro de un entorno controlado de red LAN, así como en la implementación de medidas de mitigación para proteger el sistema.

2. Objetivos

• Desarrollar un sitio web básico como prototipo funcional.

• Simular un ataque DDoS en un entorno controlado usando herramientas de seguridad.

• Analizar el tráfico de red con Nmap y Wireshark.

• Documentar las evidencias del ataque y las estrategias de protección implementadas.

3. Desarrollo del Laboratorio

3.1 Caso de Estudio – Desarrollo Web

El sitio web desarrollado corresponde a la **Junta Comunal del corregimiento de Las Lomas, en David, Chiriquí, Panamá**. El objetivo principal del portal es brindar a la comunidad un medio digital donde puedan informarse sobre los distintos **servicios que ofrece la Junta Comunal**, así como conocer su **historia, proyectos comunitarios, medios de contacto y otros recursos de interés**.

Este prototipo busca facilitar la comunicación con los residentes, ofrecer un espacio accesible para la publicación de información relevante y promover la transparencia en la gestión comunitaria.


JC Las Lomas
Inicio
Visión y Misión
Servicios
Historia
Contactos
Servicios Prestados
Historia de Las Lomas
MUNICIPIO DE DAVID
JUNTA COMUNAL DE LAS LOMAS

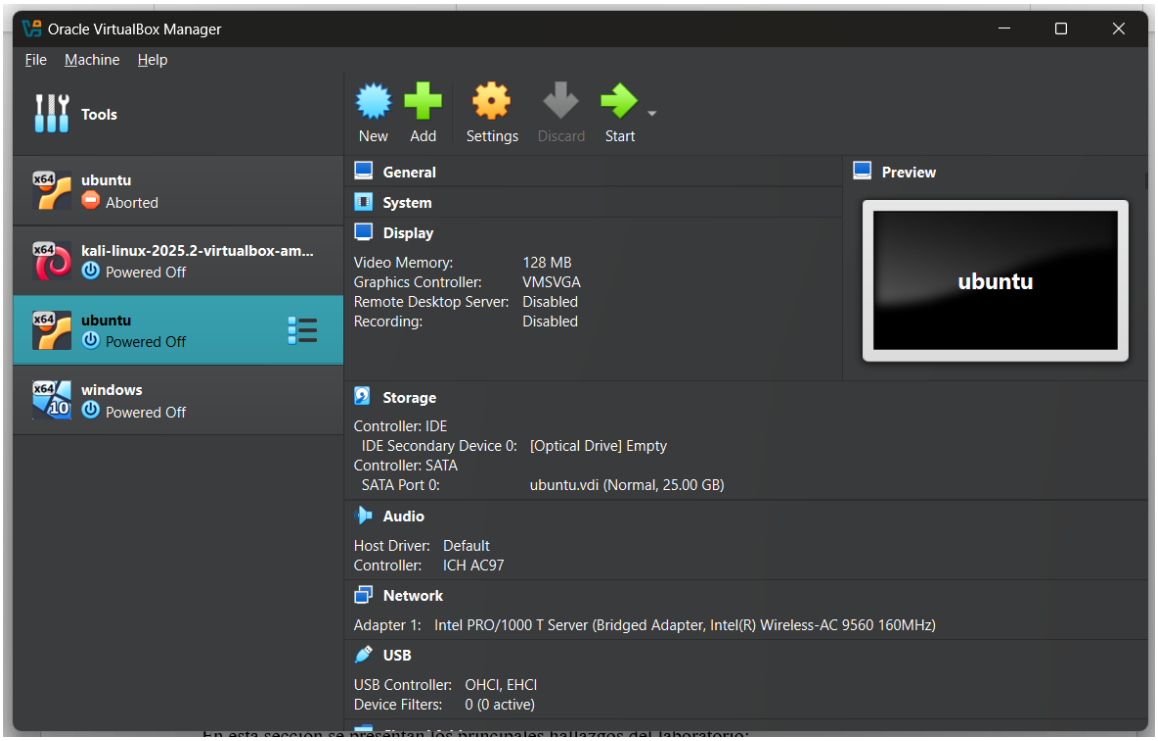

JC Las Lomas
Inicio
Visión y Misión
Servicios
Historia
Contactos
Servicios Prestados
Servicios Prestados
Consulta los servicios específicos ofrecidos por la Junta Comunal de Las Lomas, sus costos estimados y requisitos.
Buscar servicio...
Servicio
Descripción
Costo Estimado
Requisitos
Área Responsable
Solicitar
Certificado de Residencia
Documento oficial para trámites personales y legales.
Gratuito
Cédula y comprobante de domicilio.
Administración
Solicitar
Recepción de Denuncias Comunitarias
Atención y canalización de reportes sobre problemas locales.
Gratuito
Formulario de denuncia o contacto directo.
Atención Ciudadana
Solicitar
Organización de Actividades Cívicas
Inscripción y participación en eventos, ferias y jornadas comunitarias.
Gratuito
Inscripción previa según evento.
Cultura y Deportes
Solicitar
Solicitud de Apoyo para Proyectos Locales
Gestión de mantenimiento de caminos, parques y espacios públicos.
Gratuito
Solicitud formal y descripción del proyecto.
Infraestructura
Solicitar
Constancia de Domicilio
Documento para trámites escolares, bancarios o laborales.
Gratuito
Cédula y solicitud en oficina.
Administración
Solicitar

3.2 Configuración del Entorno

Para la simulación del laboratorio se utilizaron dos sistemas operativos en máquinas virtuales:

Kali Linux, instalado en la computadora del compañero Roderick, el cual se empleó para ejecutar los escaneos de red y lanzar los ataques DDoS simulados.

Ubuntu, instalado en la computadora del compañero Francisco que fue configurado para correr el servidor web donde estaba alojado el sitio de la Junta Comunal de Las Lomas.



De esta manera, el entorno reproducía un escenario realista en el que un equipo atacante (Kali Linux) intentaba inhabilitar el servicio web, mientras otro equipo (Ubuntu) actuaba como servidor objetivo dentro de la red LAN controlada.

3.3 Monitoreo de Tráfico con Wireshark

Para analizar el comportamiento del servidor durante la simulación se utilizó Wireshark como herramienta de captura y análisis de tráfico en la máquina que ejecutaba el servidor (Ubuntu en la computadora de Francisco). Wireshark permitió registrar paquetes entrantes y salientes, identificar patrones de tráfico anómalos durante el ataque DDoS simulado y obtener evidencias que respaldan los resultados del laboratorio.

Procedimiento realizado:

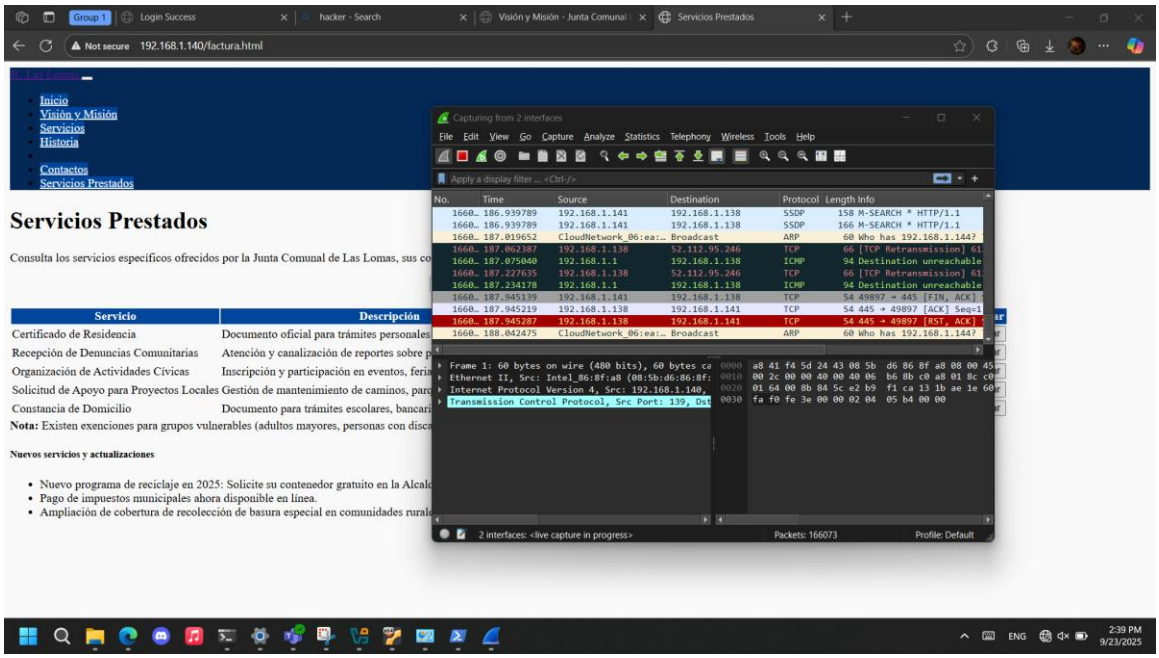
Selección de la interfaz: Se eligió la interfaz de red de la VM/host donde corría el servidor y se inició la captura en modo promiscuo para registrar todo el tráfico de la LAN controlada.

Análisis en tiempo real: Durante la ejecución del ataque se observó un aumento abrupto en el número de paquetes y en la tasa de conexiones hacia los puertos del servicio web (ej. puerto 80/5000), lo cual fue evidente en las gráficas de “Packets/sec” y en la columna de tiempo entre paquetes.

Guardado de evidencia: Las capturas relevantes se guardaron en formato .pcap y se exportaron pantallazos de los momentos clave (picos de tráfico, filtros aplicados, y detalles de paquetes sospechosos) para incluir en el informe.

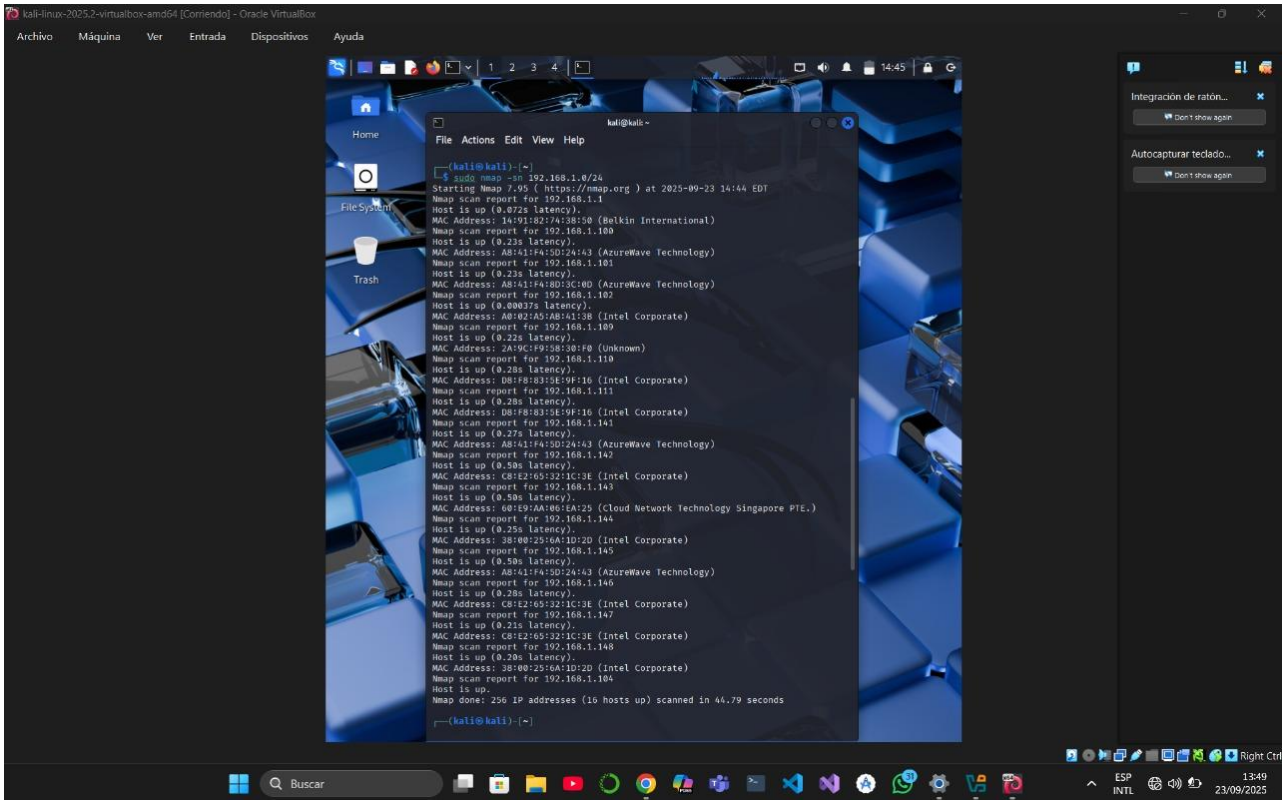
Observaciones importantes obtenidas:

Wireshark facilitó diferenciar tráfico legítimo de tráfico malicioso por la frecuencia y la naturaleza de las solicitudes (muchas conexiones cortas o solicitudes repetitivas en poco tiempo).

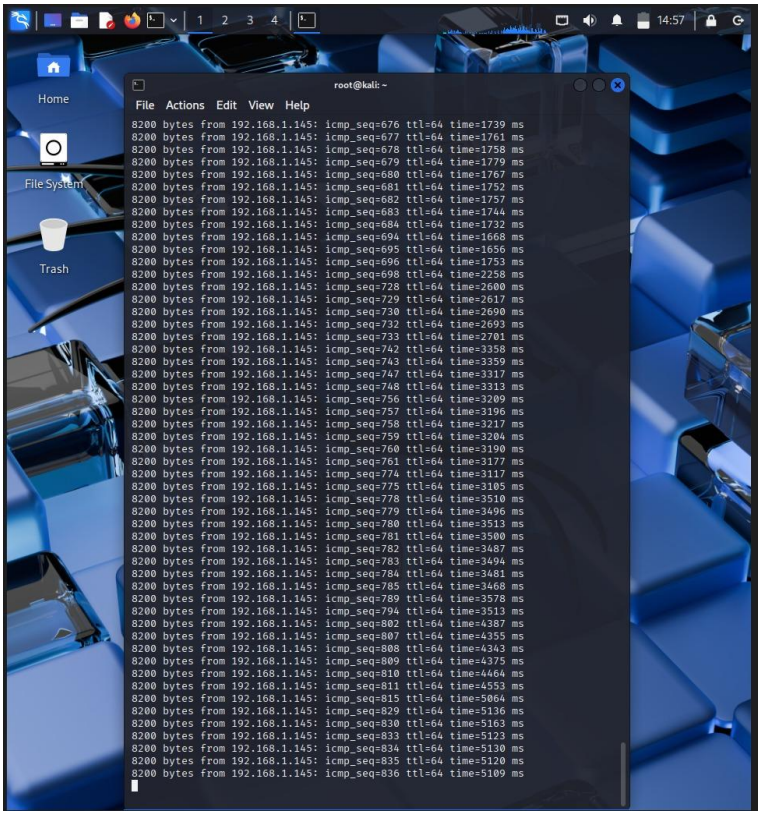


3.4 Simulación del Ataque DDoS

Primero se utilizó el comando **`sudo nmap -sn 192.168.1.0`** , para localizar las distintas direcciones IP, de los compañeros y así saber a cuál <<atacar>>.



Mas adelante, se utilizó el comando para enviar los paquetes y saturar las distintas páginas web



4. Resultados

Durante el laboratorio se obtuvieron evidencias claras del comportamiento del servicio web ante la simulación de un ataque DDoS y de la efectividad parcial de las medidas de mitigación aplicadas. A continuación se resumen los hallazgos más relevantes:

Evidencias principales

Las capturas de Wireshark muestran un aumento abrupto en el número de paquetes dirigidos a la IP del servidor durante la ventana temporal del ataque, con picos visibles en la métrica de paquetes por segundo.

El escaneo inicial con Nmap permitió identificar los puertos y servicios expuestos del servidor objetivo, lo que facilitó la focalización del ataque.

Durante la ejecución del ataque (originado desde la VM Kali, en la máquina de Roderick), el servidor hospedado en Ubuntu (mi equipo, Francisco) presentó conectividad intermitente y en ciertos momentos dejó de responder a solicitudes HTTP, evidenciado por pings con pérdida y tiempos de respuesta elevados.

Se guardaron archivos .pcap y capturas de pantalla de los momentos críticos (picos de tráfico, filtros aplicados y seguimiento de flujos TCP) que sirven como evidencia reproducible para la sustentación.

Impacto sobre el servicio

El servicio web experimentó degradación de rendimiento: aumento de latencia, incremento en la tasa de reintentos por parte de clientes y accesos fallidos en períodos de mayor intensidad del ataque.

En los momentos más críticos el sitio quedó parcialmente no disponible para usuarios legítimos, lo que demuestra cómo un volumen sostenido de tráfico malicioso puede afectar la disponibilidad de un servicio sin mitigación adecuada.

Efectividad de las medidas de protección

Las medidas preventivas básicas (filtros de firewall y restricciones simples de conexión) mostraron efecto limitado frente al patrón del ataque simulado: redujeron parcialmente el impacto pero no eliminaron la indisponibilidad en picos altos.

Las observaciones indican que soluciones adicionales —como limitación de tasa por IP, reglas más estrictas en el firewall, y la colocación de un reverse proxy con protección contra conexiones excesivas— mejorarían significativamente la resiliencia del servicio.

Lecciones aprendidas y recomendaciones

Monitoreo continuo: Mantener capturas periódicas y alertas (logs, métricas de packets/sec y uso de CPU/memoria) permite detectar anomalías antes de que el servicio se degrade severamente.

Hardenización del servidor: Cerrar puertos innecesarios y aplicar reglas de firewall precisas reduce la superficie de ataque detectada por escáneres.

Mitigación activa: Implementar rate limiting, fail2ban y/o un reverse proxy que maneje conexiones masivas para proteger el servicio web.

Pruebas escalonadas: Realizar simulaciones controladas con distintos volúmenes y vectores de ataque para evaluar umbrales y ajustar reglas de protección.

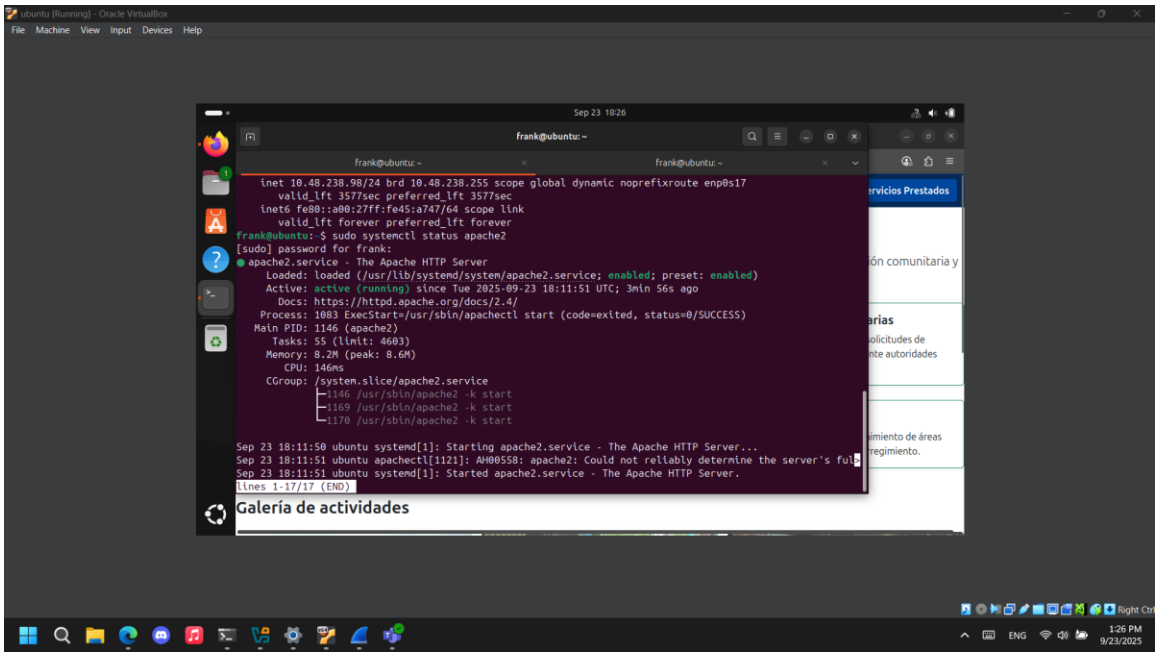
Estrategias de disponibilidad: Considerar balanceo de carga, escalado de recursos y/o uso de servicios de mitigación (CDN/WAF) para entornos productivos.

En conjunto, el laboratorio permitió reproducir de forma controlada el efecto de un ataque DDoS sobre un prototipo web y confirmó que, sin mecanismos de mitigación adecuados, la disponibilidad del servicio puede verse seriamente comprometida. Las medidas aplicadas redujeron parcialmente el impacto, pero se requieren soluciones adicionales para garantizar la continuidad en un escenario real.

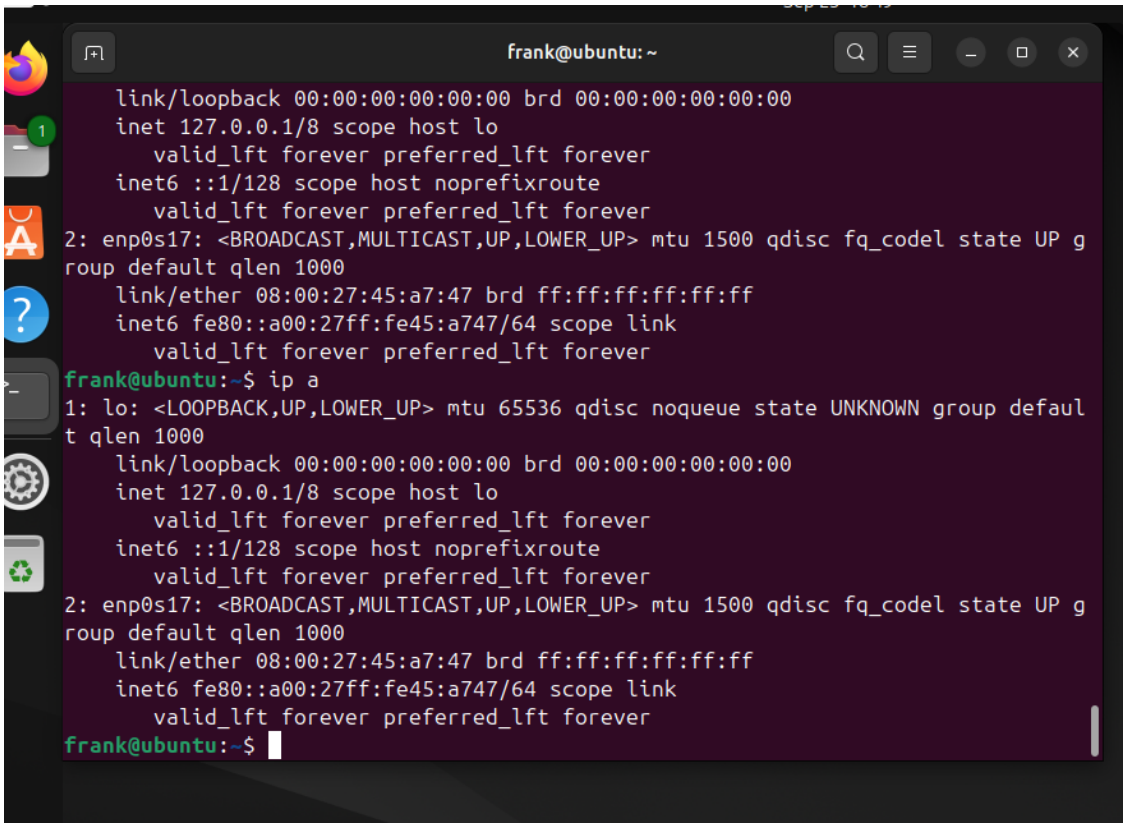
5. Conclusiones

El laboratorio permitió comprender de manera práctica cómo un ataque DDoS puede afectar la disponibilidad de un servicio web y la importancia de contar con mecanismos de protección adecuados. Se reforzó el uso de herramientas como Nmap y Wireshark para el análisis de red, así como la necesidad de aplicar medidas de seguridad en servidores expuestos. La experiencia demostró que, aunque se pueden implementar mitigaciones básicas, en escenarios reales se requiere una defensa más robusta para garantizar la continuidad del servicio.

6. Anexos



Levantando el servidor de Apache



`ip a`, para conseguir la dirección IP