

Laboratorio 5: Redes de Computadores

Muryel Constanzo 202173525-9

Benjamín Pavez 202173628-K

Angelo Russu 202173509-7

1 de Diciembre 2024

1 Preguntas Generales

1.1 Diagrama de la interacción realizada

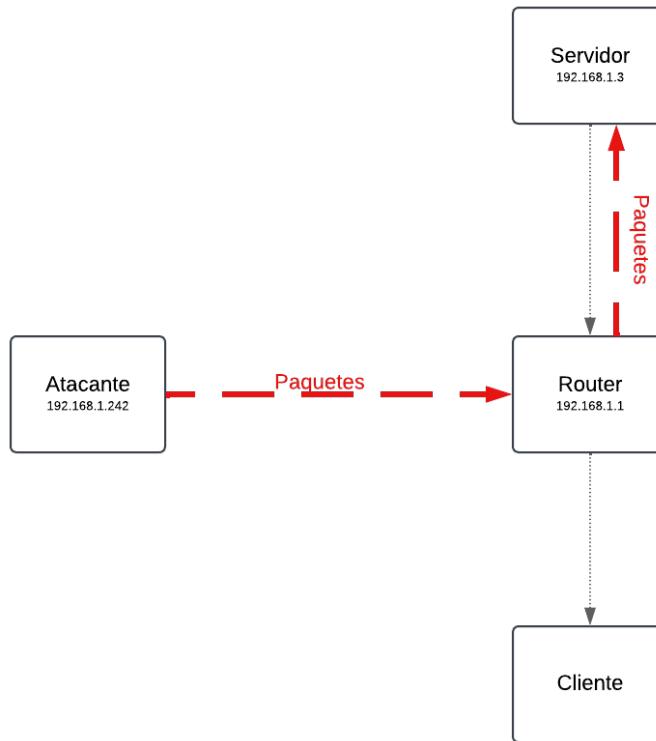


Figure 1: Diagrama que representa interacción entre el servidor, router, cliente durante ataque DoS durante el Laboratorio Presencial.

1.2 ¿En qué consisten los ataques de inundación (Flood-ing)?

Los ataques de inundación son uno de los tipos de ataques más comunes, este consisten en saturar la red mediante la generación masiva de paquetes, lo que causa la denegación del servicio (DoS). Este tipo de ataque fue el que se experimentó en el presente laboratorio, en donde en nuestro caso asumimos el rol de servidor, nos llegaron una gran cantidad de paquete en un corto periodo de tiempo, provocando problemas en la red y en la comunicación del servidor con un cliente, A continuación, se mencionarán otros tipos de inundaciones:

- **Inundación de SYN:** El atacante envía numerosas solicitudes SYN sin

completar la conexión, saturando la tabla de conexiones.

- **Inundación de Ping:** El atacante genera una gran cantidad de paquetes ICMP para ralentizar la red.
- **Inundación de ACK:** El atacante genera una gran cantidad de paquetes ACK con el fin de sobrecargar el servidor.
- **Inundación de DNS:** El atacante inunda los servidores DNS de un dominio para interrumpir la resolucion DNS de ese dominio.
- **Inundación de HTTP:** El atacante genera una gran cantidad de solicitudes HTTP al servidor con el fin de que este deje de responder.

Para mitigar las inundaciones los distintos tipos de inundaciones se puede:

- **Inundación de SYN:** Implementar SYN Cookies para validar conexiones legítimas.
- **Inundación de Ping:** Limitar el trafico ICMP en el Firewall.
- **Inundación de ACK:** Monitorear el trafico y establecer reglas en el Firewall.
- **Inundación de DNS:** Establecer un limite de consultar por direccion IP.
- **Inundación de HTTP:** Limitar solicitudes permitidas y balancear carga.

1.3 ¿Qué cambios realizarían para mejorar la seguridad y eficiencia de la red?

Algunas mejoras son:

- Activar filtrado de paquetes en el Firewall y establecer reglas con el fin de evitar el colapso de la red.
- Monitorear constantemente la red con el fin de detectar patrones que puedan afectar el trafico en la red.
- Limitar la taza de peticiones durante un tiempo para asi evitar problemas en la red.

En este caso, se nos asignó el rol de servidores por lo que se cumplió con el rol de defender. A continuacion se responderán las preguntas asociadas a este rol:

2 Preguntas para Defensores

2.1 ¿En qué consiste y qué funciones cumple el reenvío de puertos?

El reenvío de puertos, o port forwarding, es una técnica que permite redirigir el tráfico entrante desde un dispositivo externo hacia uno interno en una red local. Entre sus funciones principales se encuentra el acceso remoto, que permite conectarse a servicios internos desde Internet, como servidores web, servidores de archivos o dispositivos IoT. Por ejemplo, un NAS en una red interna podría ser accedido remotamente reenviando el puerto 8080 hacia su dirección IP local, facilitando la gestión y acceso a archivos desde fuera de la red.

2.2 ¿Qué tipos de reglas de firewall pueden configurarse para proteger ante ataques de inundación?

- **Bloqueo de puertos:** Cerrar puertos que no sean importantes o que no estén en uso para así evitar accesos no deseados.
- **Limitación de conexiones por IP:** Establecer reglas en el Firewall bloqueando IPs sospechosas.

Otros enfoques para evita, mitigar o resolver serian:

- **Monitoreo:** Monitorear constantemente la red en busca de dispositivos intrusos.
- **IDS/IPS:** Detección y prevención automática de intrusiones.
- **Limitar:** Limitar la cantidad de solicitudes permitidas.
- **Balanceo de carga:** Distribuye la carga entre múltiples servidores.

3 Anexo

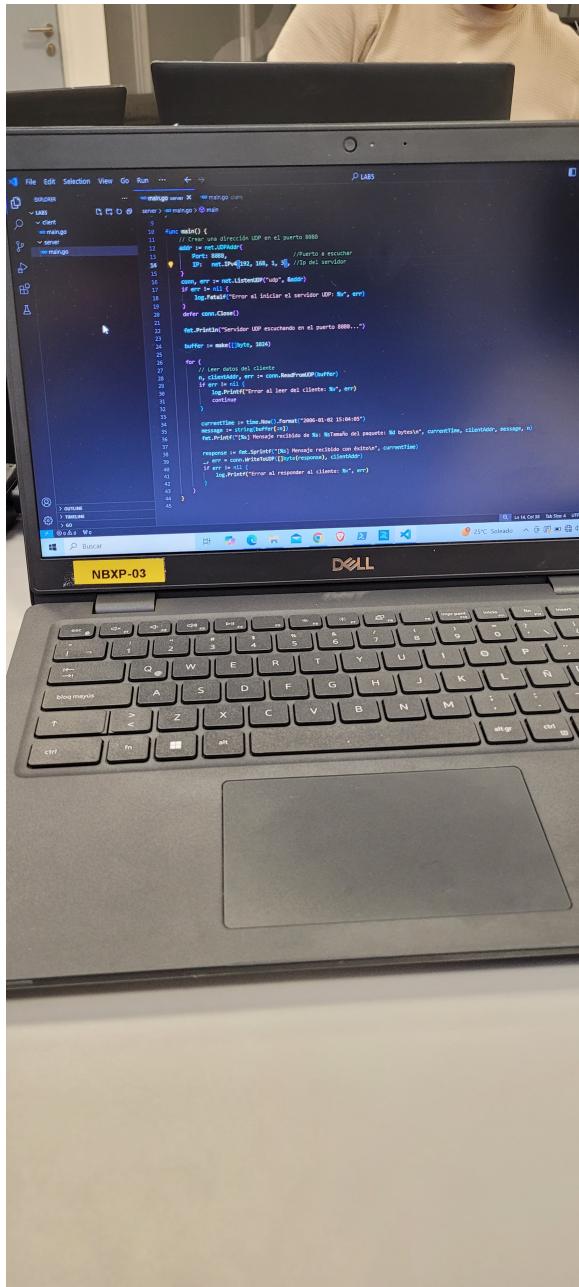


Figure 2: Se configura el main.go de server con la IP y el puerto para comenzar a recibir ataques.

The screenshot shows a Microsoft Visual Studio Code (VS Code) interface with the following details:

- File Explorer:** Shows a project structure with a file named `main.go` selected.
- Code Editor:** Displays the content of `main.go`. The code initializes a UDP server on port 8080, listening for connections from a specified IP address (192.168.1.3). It includes error handling for connection setup.
- Terminal:** Shows the output of running the application. It lists network interfaces (Adaptador de LAN inalámbrica, Adaptador de LAN inalámbrica Wi-Fi), their states (desconectados), and specific DNS suffixes. It also shows the configuration for the Ethernet connection (Dirección IPv6, Dirección IPv6 temporal, Vinculo: dirección IPv6 local, Dirección IP4, Máscara de subred, Puerta de enlace predeterminada).
- Bottom Status Bar:** Provides information about the current file (Ln 14, Col 38), encoding (UTF-8), and system status (CRLF, Go, 17:44, 27-11-2024).

Figure 3: Se configura el main.go de server con la IP y el puerto para comenzar a recibir ataques.

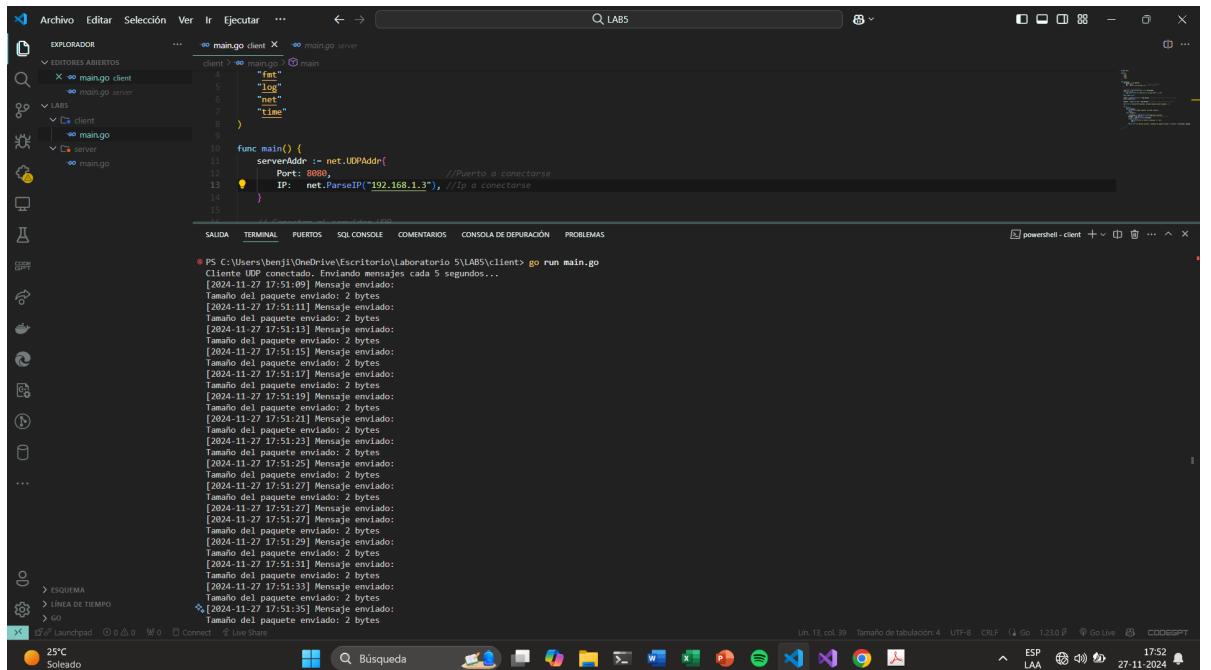


Figure 4: De otro PC en la red se envia un paquete al PC servidor para verificar que lleguen.



Figure 5: Los paquetes enviados llegan correctamente, verificando que esta listo el servidor para recibir ataques.



Figure 6: Comienzan a enviar paquetes los atacantes en la red.

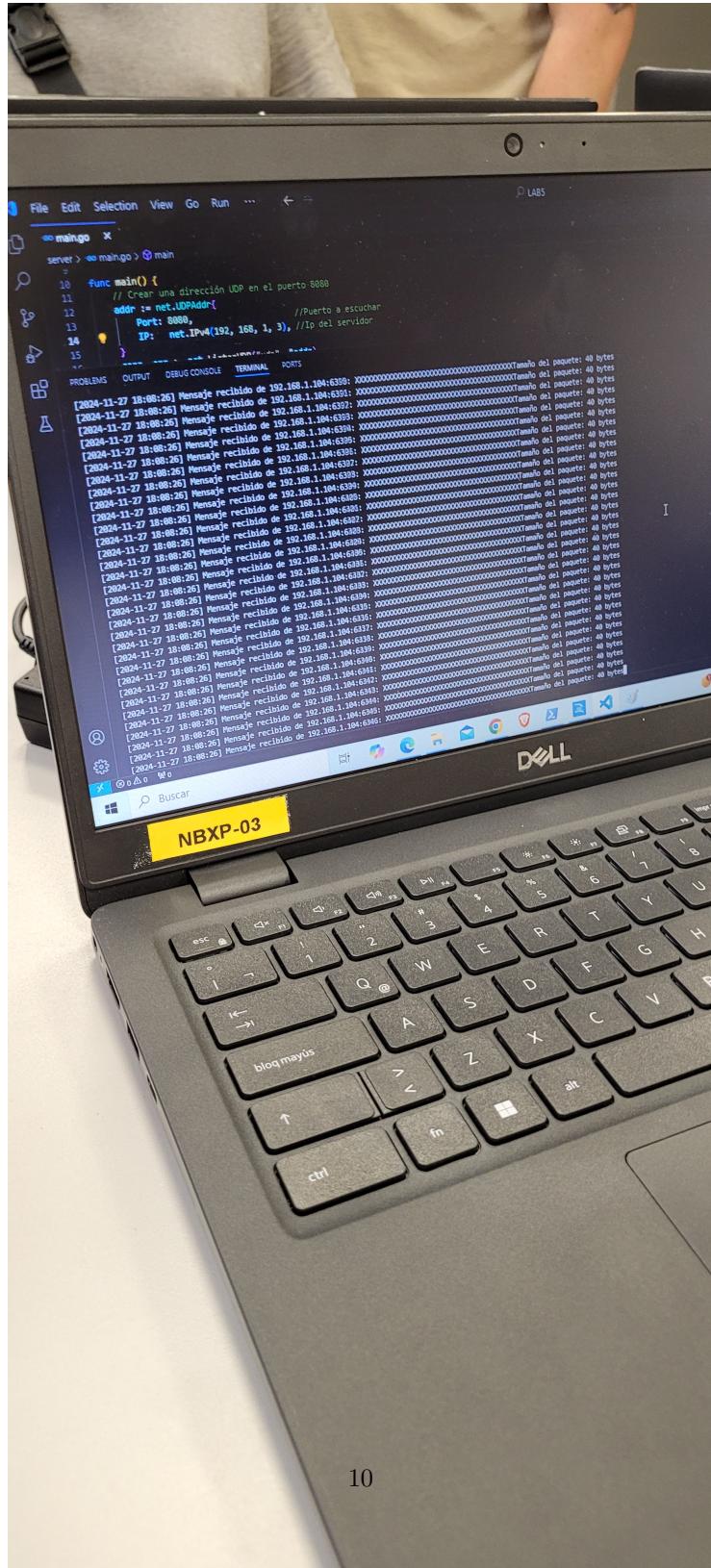


Figure 7: Comienzan a enviar más paquetes los atacantes en la red.

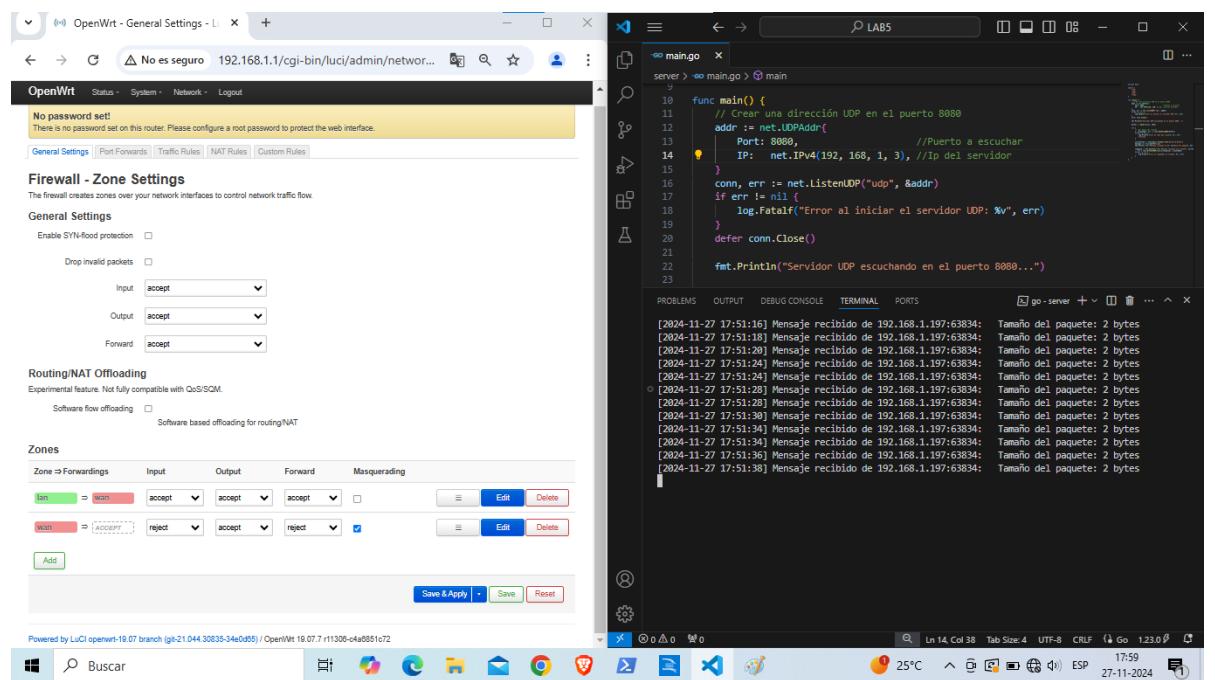


Figure 8: Se abre la configuración del router para setear reglas de port forwarding.

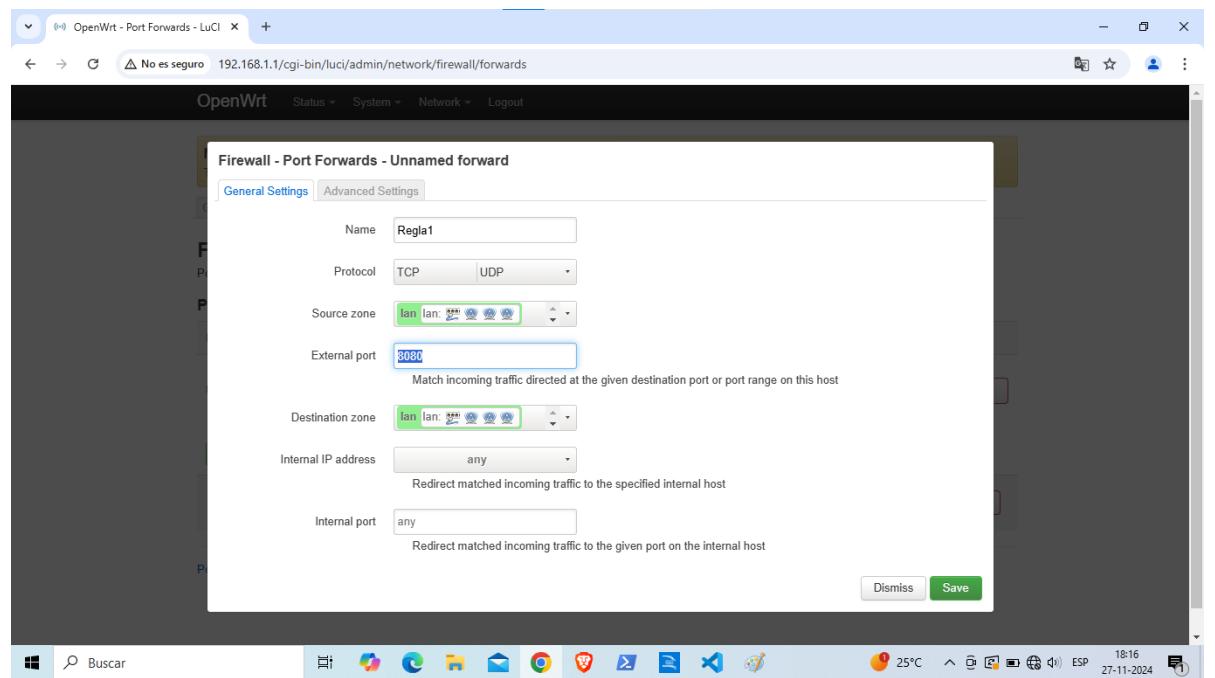


Figure 9: Se crea una regla para evitar más ataques al servidor.

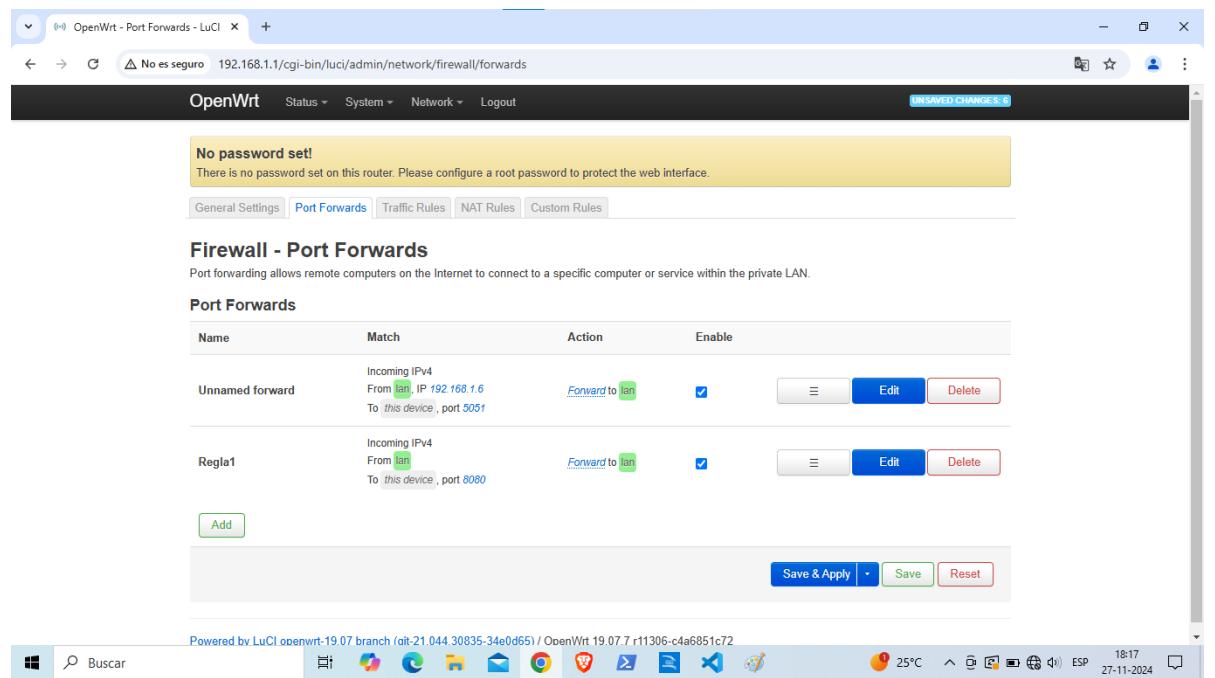


Figure 10: La regla se creo para disminuir la cantidad de paquetes a nuestra IP.

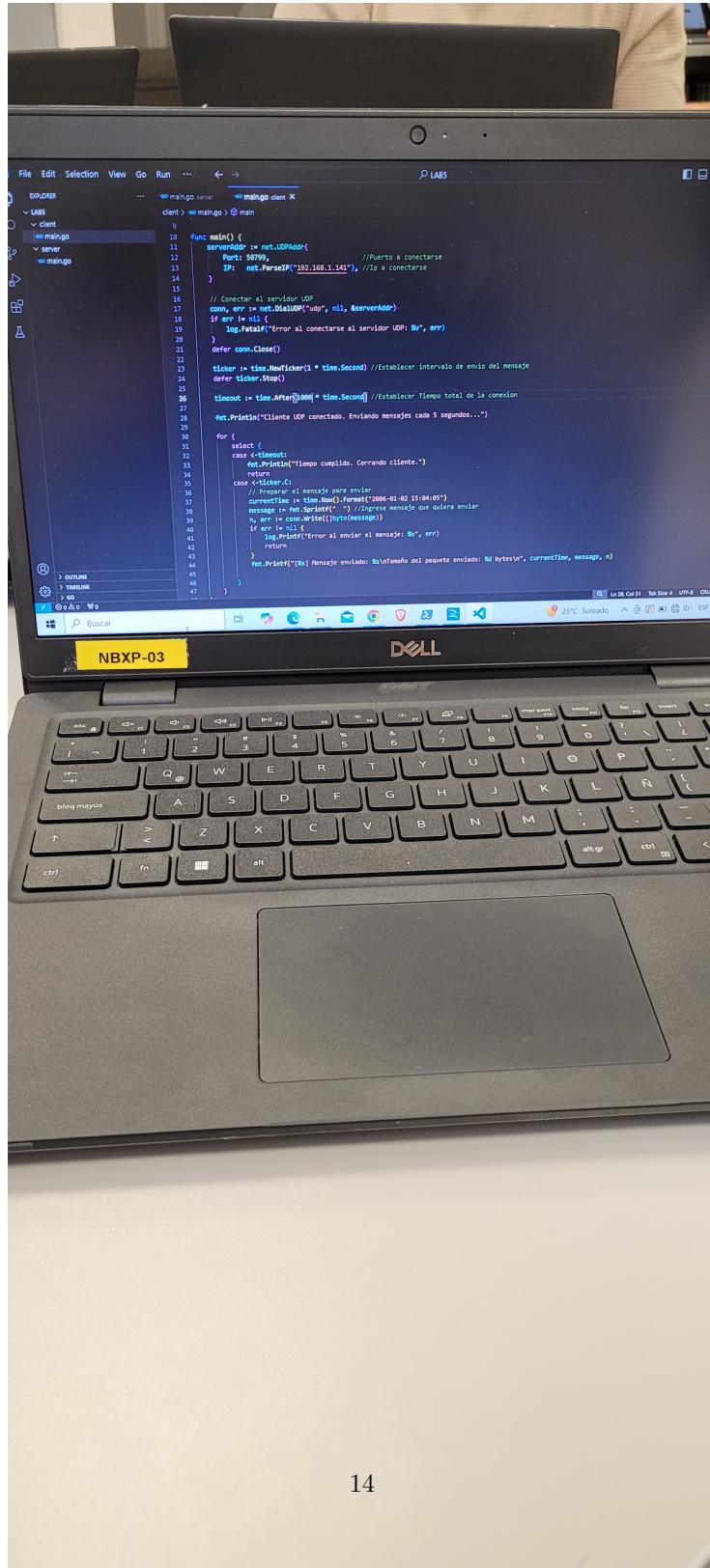


Figure 11: Se realiza un ataque del PC servidor a otro PC del laboratorio.