ATAQUE DE NEGACIÓN DE SERVICIO (DoS)

Trabajo de Laboratorio

Presentado por:

Samuel Alzate Echeverri

Josue Penagos

Asignatura:

Seguridad Informática

Docente:

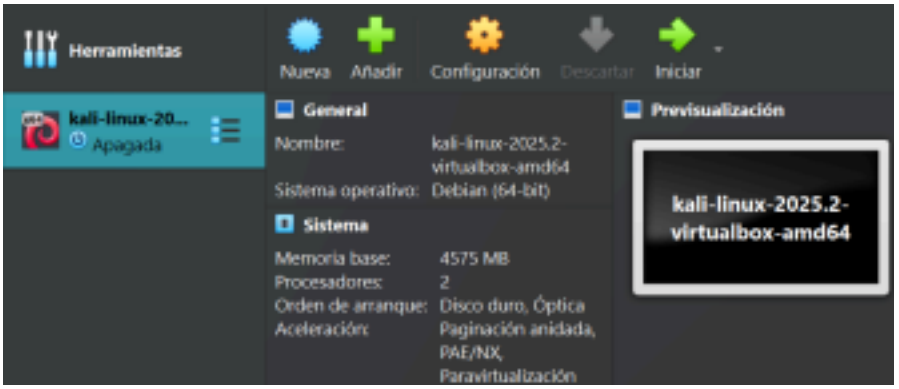
Yexid Montenegro

INSTITUCIÓN UNIVERSITARIA PASCUAL BRAVO

2025

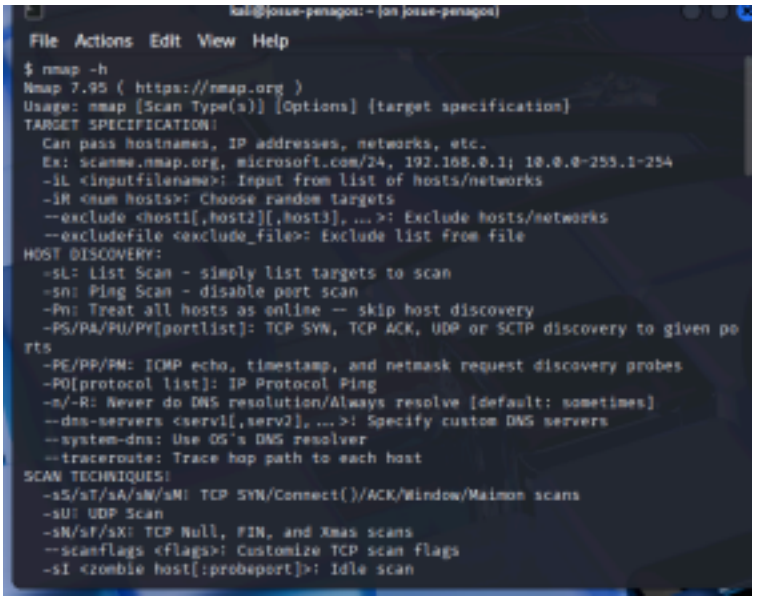
Procedimiento

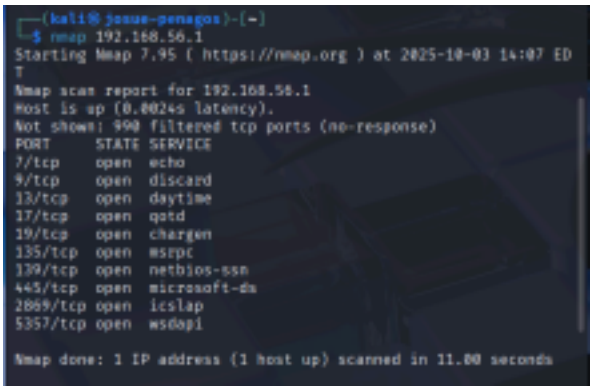
1) Trabaje en VB con Kali linux ultima version con los ultimos paquetes



Le damos los recursos necesarios para que funcione la Virtual Box

1.1) Usando Nmap (Ya instalado)





Puerto escaneado de mi maquina
Qué resultados muestra? Qué diferencia hay con respecto a lo que entrego Windows?

El escaneo con Nmap me dice que la máquina de Windows está **viva** y accesible, pero tiene puesto un *firewall* potente:

- **La Máquina Está Encendida:** Lo primero es que la IP **`192.168.56.1 (Que es la de mi pc)`** está **"up" osea que es** activa y que la red está bien configurada. ● **El Firewall Está Activado:** Nmap me dice que **990 puertos están "filtered"** (filtrados). Eso significa que el **Firewall de Windows** está activo y bloqueando casi todas las peticiones que le mando, por eso Nmap no sabe si están abiertos o cerrados.
- **Puertos Abiertos :** A pesar del *firewall*, sí encontró unos **10 puertos abiertos**. Los más importantes que me pueden servir son el **Puerto 445** (para compartir archivos en Windows) y el **Puerto 139** (NetBIOS). Son puntos débiles que el *firewall* dejó pasar.

II. Uso de DoS: con hping3

Instalación y que es y qué hace HPING.

Que es ? = Es una herramienta de red capaz de **enviar paquetes TCP/IP personalizados** (como si fuera un *ping* avanzado).

Que hace ? = Muestra las **respuestas del destino** de forma similar a como el programa `ping` lo hace con las respuestas ICMP.

Instalación en la terminal de kali linux

El paquete hping3 ya venia por defecto en mi kali linux

Ejecute con privilegios de root el siguiente comando:

Al ejecutar el comando hping3 192.168.0.103 –S –p 80 –i u1 –L eth0

Lo hare con mi ip que es 192.168.56.1

inicie el ataque puse este comando ya que el que se ponia de por si no me funciono

sudo hping3 -c 100000 -d 120 -S -w 64 -p 445 --flood --rand-source 192.168.56.1

explicacion de

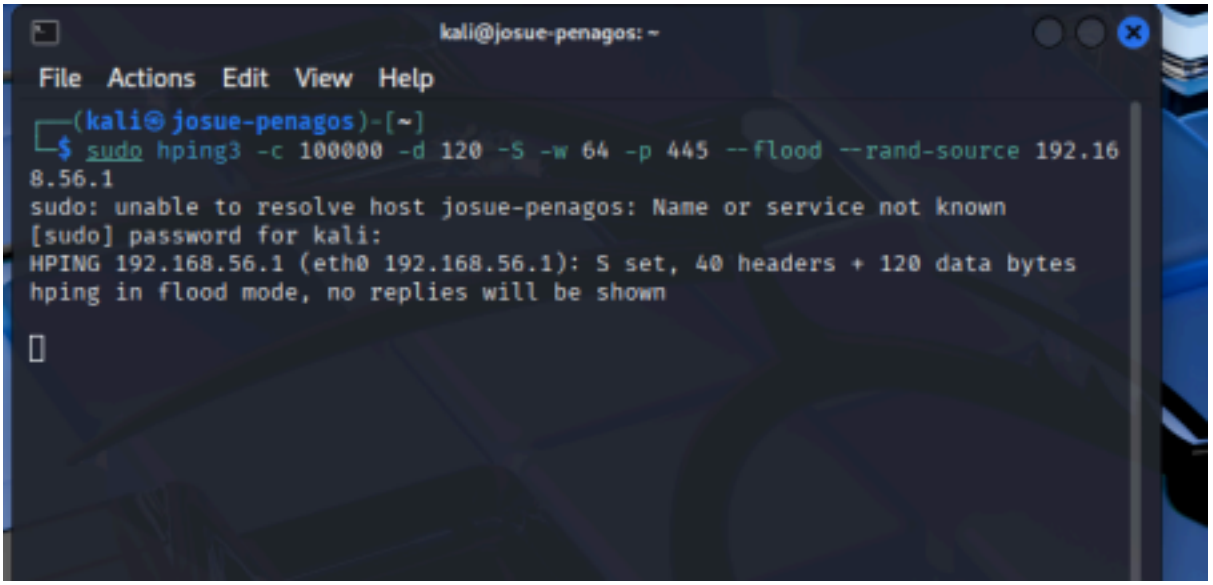
sudo hping3 -c 100000 -d 120 -S -w 64 -p 445 --flood --rand-source 192.168.56.1

el -c es el numero total de paquetes a enviar que son 100,000.

el -d que es el tamaño de los datos del paquete en 120 bytes.

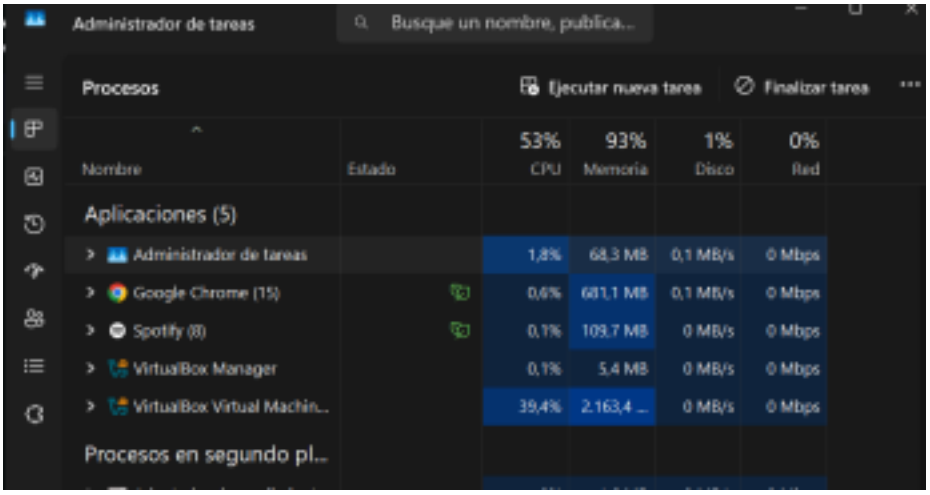
el -s que es Activa el *flag* **SYN** (Sincronización) en el encabezado TCP.

y en un lenguaje natural esto es **"Usa privilegios de *root* para enviar 100,000 paquetes TCP SYN de 120 bytes al Puerto 445 de la IP `192.168.56.1`, hazlo lo más rápido que puedas (`--flood`) y oculta mi IP (`--rand-source`)"**.

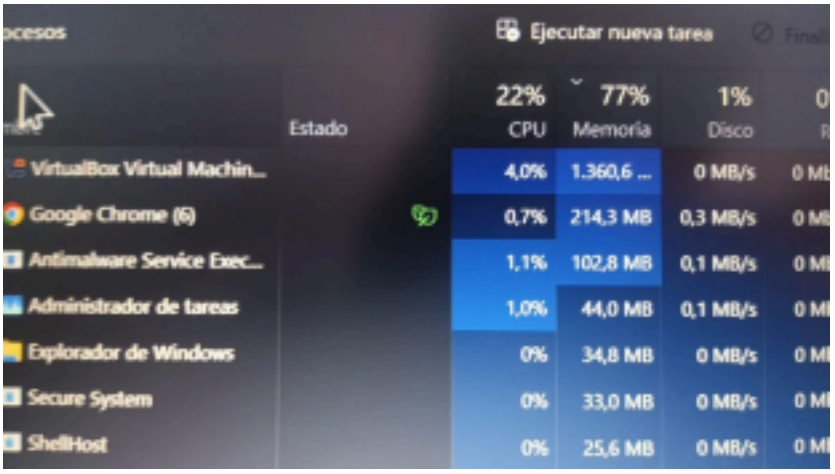


Comenzo el ataque

A. Ambiente de ataque windows



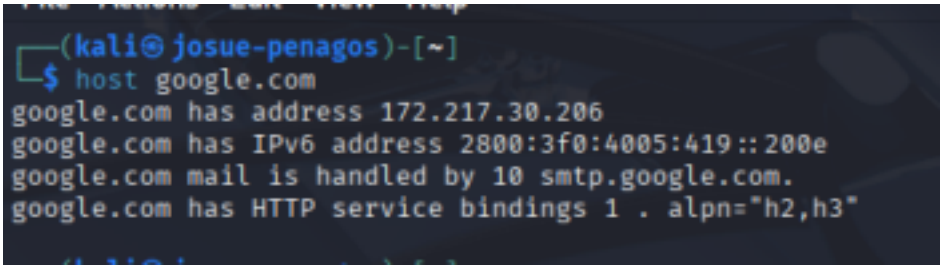
El ataque de Dos lo hice contra mi misma maquina y los primeros paquetes en enviarse me tumbaron el wifi el administrador de tareas se volvio loco y me reinicio el pc y solo pude tomar esta foto ya que no me dejaba tomarla normal



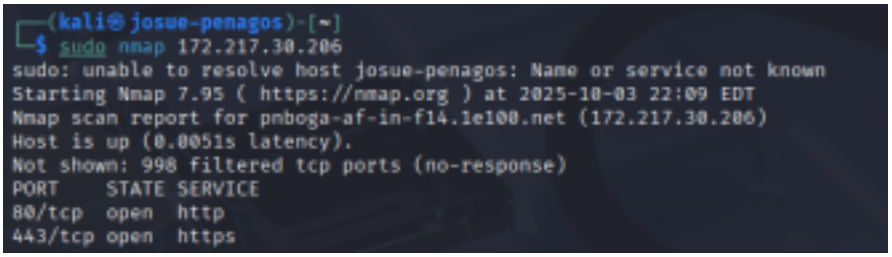
2. Obtenga la dirección IP de Windows

Al principio la IP puesta por el profesor no me funciono por unos errores con la ip entonces para esta parte del trabajo se lo hare a google

Primero ponemos el comando host en kali y ponemos el dominio



3) Con nmap ver que puertos estan abiertos



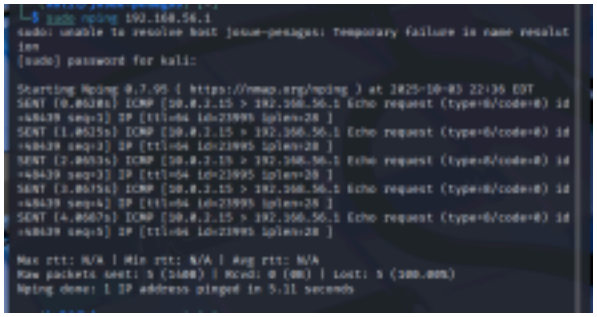
4) Me sale este error ya que el kali esta detectando como si hubiera alguna ip mas o algun infiltrado

5) sudo hping3 -c 100000 -d 120 -S -w 64 -p 445 --flood --rand-source 172.217.30.206

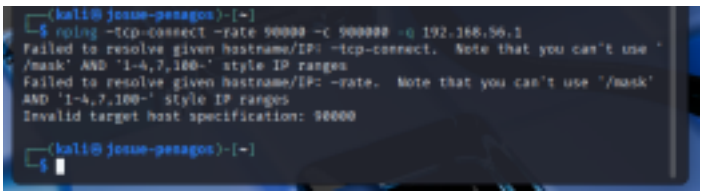
a) Empezo el ataque y ya se empezo a saturar el chrome y la vb y me toco parar ya que me dio cosita seguir y hacer algun daño minimo para ellos fue un falso positivo

b) El comportamiento fue se me cayo la conexion el chrome me iba re lag me empezo a sonar el pc como una turbina de avion y se me empezaron a cerrar las cuentas de google

6. Uso del nping ahora si con mi ip que es 192.168.56.1



segun esto todos los packetes que se envian se pierden

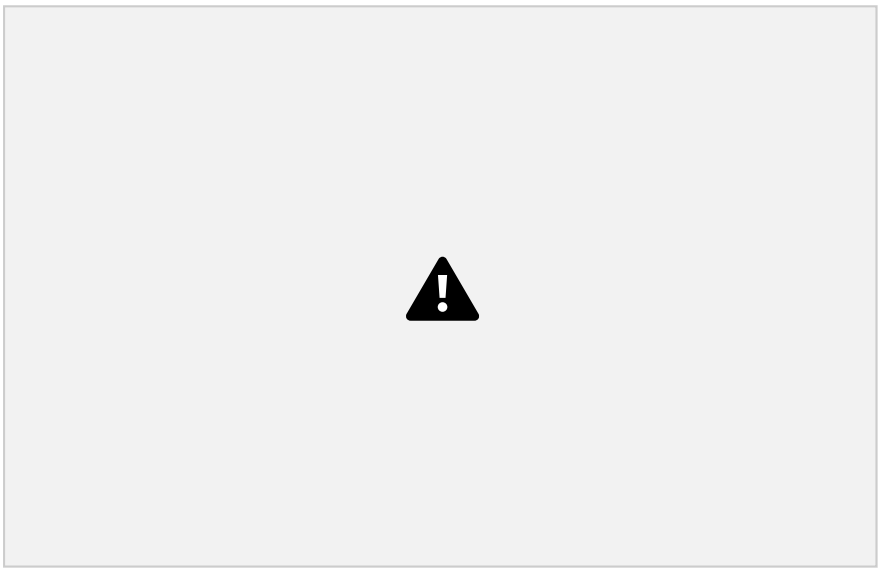


que se pierden todos los paquetes ya que el firewall esta bloqueando el ping

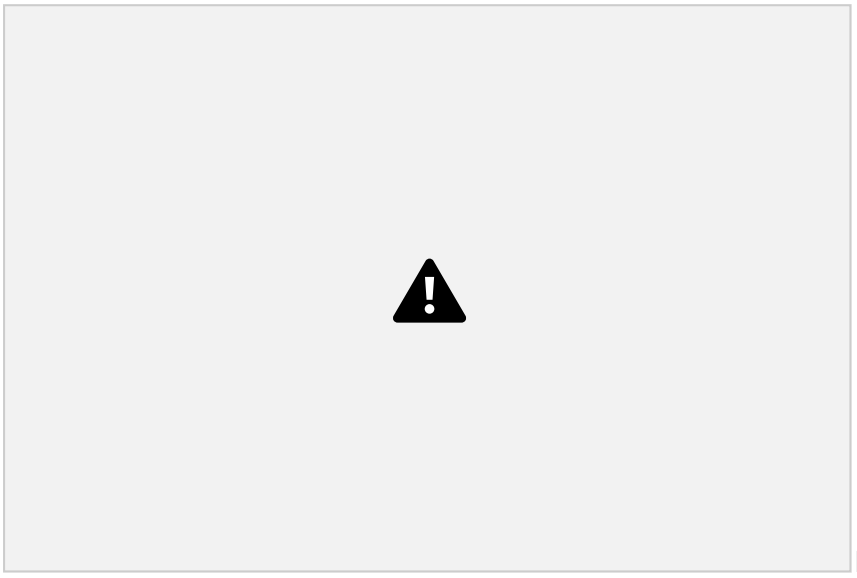
7) me sale el mismo error

Ambiente de proteccion

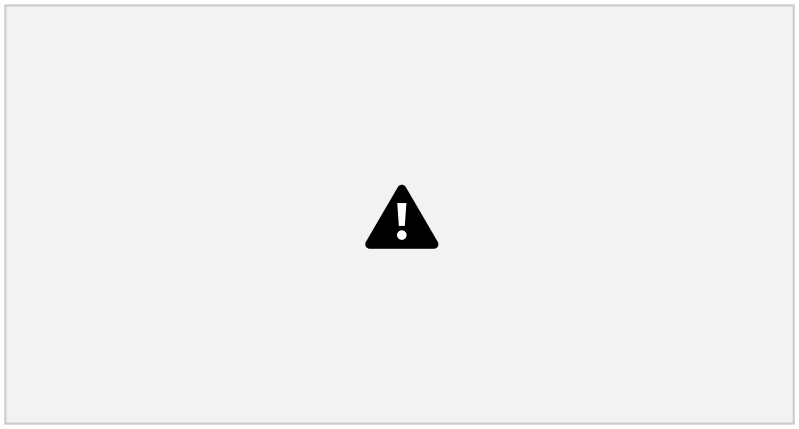
aca le damos en configuracion avanzada



Le damos en nueva regla



le damos en

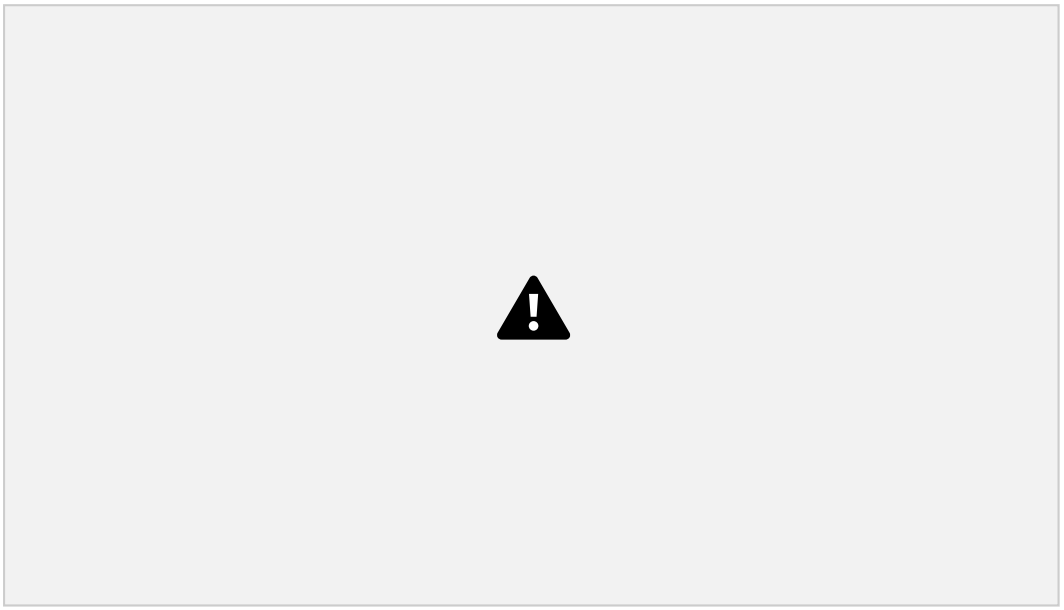


puerto

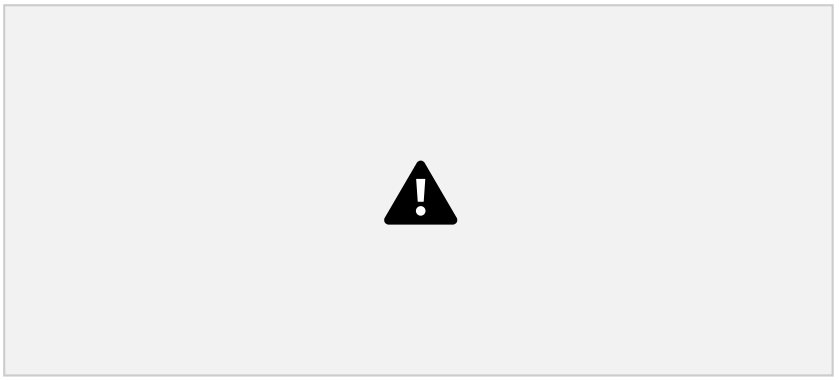
le damos en tcp ya que : protocolo **TCP (Transmission Control Protocol)** porque el ataque que realizaste (**SYN Flood**) es intrínsecamente un ataque TCP.

y por que puertos locales especificos ? : Se elige **"Puertos locales específicos"** en lugar de "Todos los puertos locales" para aplicar el principio de **mínimo privilegio y mínimo impacto**.

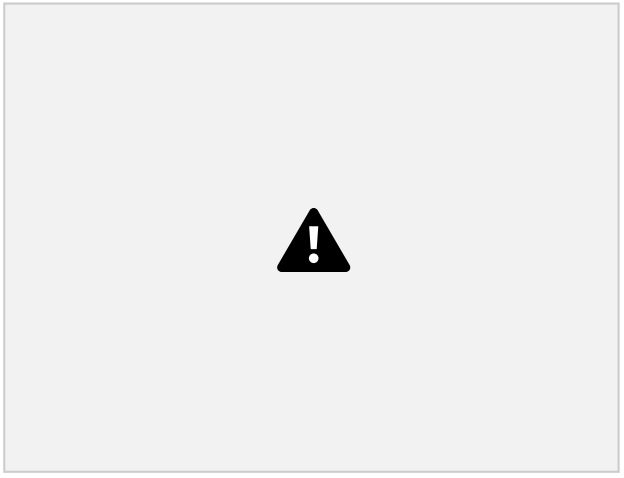
y se pone el puerto atacado ya que fue el punto de vulnerabilidad que fue el 445


hay que bloquear el puerto y continuar ponerle un nombre y una descripción y asi se cierran los puertos

¿Qué comportamiento observa?


Al escanear con nmap

el puerto sigue abierto pero solo en el localhost y cerre mas puertos con esta


regla

Conclusión

Este laboratorio demostró de manera práctica la **vulnerabilidad crítica** que representa un **Ataque de Denegación de Servicio (DoS)** basado en SYN Flood. Se utilizó la herramienta **hping3** para saturar el puerto abierto del sistema Windows, lo que provocó el agotamiento de los recursos (CPU y Memoria) y, consecuentemente, la inestabilidad y el reinicio de la máquina.

Finalmente, el ejercicio permitió implementar un mecanismo de defensa efectivo al configurar una **regla de bloqueo TCP específica** en el **Firewall de Windows** contra el puerto atacado, demostrando que una configuración de seguridad adecuada es vital para prevenir la interrupción del servicio y mitigar el potencial daño de estos ataques.