

Se ejecutó el script:

packet\_attack.py

Acciones realizadas por el Red team:

1. El script construyó paquetes TCP con bandera SYN utilizando la librería *Scapy*.
2. Se enviaron solo 3 SYN controlados hacia la dirección y puerto objetivo, cumpliendo la regla:

*“No romper servicios, no causar denegación de servicio.”*

3. Se utilizó el modo seguro con el parámetro `--simulate` para validar la ejecución sin generar tráfico real, y posteriormente se hizo una prueba con envío real controlado.

### Simulación de envíos de paquetes

```
C: > Users > kamilla > Downloads > packet_attack.py > ...
1  #!/usr/bin/env python3
2
3  from scapy.all import IP, TCP, send
4  import argparse
5  import time
6  import sys
7  from datetime import datetime
8
9
10 def validate_ip(ip):
11     """Valida formato básico de dirección IP."""
12     parts = ip.split('.')
13     if len(parts) != 4:
14
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS

PS C:\Users\kamilla\Downloads\SYNsimple> python packet_attack.py 192.168.0.12 80 --simulate
[INFO] Iniciando SYN test hacia 192.168.0.12:80 (simulate=True)
[SIMULACION] Enviaria paquete SYN #1
[SIMULACION] Enviaria paquete SYN #2
[SIMULACION] Enviaria paquete SYN #3
[INFO] Prueba finalizada.
PS C:\Users\kamilla\Downloads\SYNsimple> |
```

1. El programa indica que inició la prueba hacia la IP 192.168.0.12 en el puerto 80.
2. Como se activó `--simulate`, el script no envía paquetes reales, sino que muestra mensajes indicando qué habría enviado:
  - Paquete SYN #1
  - Paquete SYN #2
  - Paquete SYN #3

3. Finalmente indica que la prueba terminó.

### Prueba con envío real de paquetes (controlado).

Se muestra el envío de paquetes a la IP 192.168.100.1:80.

```
C:\Users\User\OneDrive\Documentos\juegos\images\PROGRA_INTERMEDIA\PROGRA_AVANZADA\proyecto_ciberseguridad\red_team>python packet_attack.py -t 192.168.100.1 -p 80

=====
Red Team - SYN Attack Tool
=====
Target: 192.168.100.1:80
Packets: 3
Mode: ATTACK
Delay: 1.0s
=====

[ATTACK] Iniciando envío de paquetes SYN...
[SENT] Paquete #1/3 - SYN enviado a 192.168.100.1:80
[SENT] Paquete #2/3 - SYN enviado a 192.168.100.1:80
[SENT] Paquete #3/3 - SYN enviado a 192.168.100.1:80
=====

Ataque completado: 3/3 paquetes
Log guardado en: attack_log.txt
=====
```

Con WireShark se verifica que los paquetes fueron recibidos.

The screenshot shows the Wireshark network protocol analyzer interface. The top pane displays a list of captured packets, with three TCP SYN packets (No. 252, 254, and 259) selected, all destined for 192.168.100.1:80. The middle pane shows the packet details for the selected packet (No. 259), including Ethernet II, Internet Protocol Version 4, and TCP. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
252	30.830005	192.168.100.34	192.168.100.1	TCP	54	20 → 80 [SYN] Seq=0 Win=8192 Len=0
254	31.835273	192.168.100.34	192.168.100.1	TCP	54	[TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=0
259	32.837334	192.168.100.34	192.168.100.1	TCP	54	[TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=0

Frame 259: Packet, 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF...  
Section number: 1  
Interface id: 0 (\Device\NPF\_{7024433A-EABF-4608-B6A5-CDDF8BF9C812})  
Encapsulation type: Ethernet (1)  
Arrival Time: Dec 7, 2025 19:58:16.745120000 Hora estándar, América Central  
UTC Arrival Time: Dec 8, 2025 01:58:16.745120000 UTC  
Epoch Arrival Time: 1765159096.745120000  
[Time shift for this packet: 0.000000000 seconds]  
[Time delta from previous captured frame: 20.422000 milliseconds]  
[Time delta from previous displayed frame: 1.002061000 seconds]  
[Time since reference or first frame: 32.837334000 seconds]  
Frame Number: 259  
Frame Length: 54 bytes (432 bits)  
Capture Length: 54 bytes (432 bits)  
[Frame is marked: False]  
[Frame is ignored: False]  
[Protocols in frame: eth:ethertype:ip:tcp]  
[Coloring Rule Name: Bad TCP]  
[Coloring Rule String: tcp.analysis.flags && !tcp.analysis.window\_update && !tcp.analysis.keep\_alive]  
▼ Ethernet II, Src: Intel\_ee:50:9d (e4:0d:36:ee:50:9d), Dst: HuaweiTechno\_a0:bd:af (f8:bf:09:a0:bd:af)  
... 0 ... = 10 bit: Globally unique address (factory default)  
... 0 ... = 10 bit: Individual address (unicast)  
▼ Source: Intel\_ee:50:9d (e4:0d:36:ee:50:9d)  
... 0 ... = 10 bit: Globally unique address (factory default)  
... 0 ... = 10 bit: Individual address (unicast)  
Type: IPv4 (0x0000)  
[Stream index: 1]  
▼ Internet Protocol Version 4, Src: 192.168.100.34, Dst: 192.168.100.1  
0100 ... = Version: 4  
... 0101 = Header Length: 20 bytes (5)  
▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total length: 40  
Identification: 0x0001 (1)  
000 ... = Flags: 0x0  
... 0 0000 0000 0000 = Fragment Offset: 0  
Time to Live: 64

## Resultado

El ataque fue ejecutado de forma segura y sin afectar la disponibilidad de los servicios del laboratorio.

Se pudo observar los paquetes desde las herramientas de monitoreo sin recibir un impacto negativo en el sistema.