**IDS and IPS Evasion**

## **TTL Manipulation**

Send some packets with a TTL enough to arrive to the IDS/IPS but not enough to arrive to the final system. And then, send another packets with the same sequences as the other ones so the IPS/IDS will think that they are repetitions and won't check them, but indeed they are carrying the malicious content.

**Nmap option:** --ttlvalue <value>

## Avoiding signatures

Just add garbage data to the packets so the IPS/IDS signature is avoided.

**Nmap option:** --data-length 25

## **Fragmented Packets**

Just fragment the packets and send them. If the IDS/IPS doesn't have the ability to reassemble them, they will arrive to the final host.

**Nmap option:** -f

## **Invalid** ***checksum***

Sensors usually don't calculate checksum for performance reasons. So an attacker can send a packet that will be **interpreted by the sensor but rejected by the final host.** Example:

Send a packet with the flag RST and a invalid checksum, so then, the IPS/IDS may thing that this packet is going to close the connection, but the final host will discard the packet as the checksum is invalid.

## **Uncommon IP and TCP options**

A sensor might disregard packets with certain flags and options set within IP and TCP headers, whereas the destination host accepts the packet upon receipt.

## **Overlapping**

It is possible that when you fragment a packet, some kind of overlapping exists between packets (maybe first 8 bytes of packet 2 overlaps with last 8 bytes of packet 1, and 8 last bytes of packet 2 overlaps with first 8 bytes of packet 3). Then, if the IDS/IPS reassembles them in a different way than the final host, a different packet will be interpreted. Or maybe, 2 packets with the same offset comes and the host has to decide which one it takes.

* **BSD**: It has preference for packets with smaller *offset*. For packets with same offset, it will choose the first one.
* **Linux**: Like BSD, but it prefers the last packet with the same offset.
* **First** (Windows): First value that comes, value that stays.
* **Last** (cisco): Last value that comes, value that stays.

## Tools

* <https://github.com/vecna/sniffjoke>