p0f is a tool that uses tcp flags (syn ack) **to fingerprint server OS and user agent** (which is often spoofed)

This tool can fingerprint the OS of a server from basically 1 syn packet

This is extremely useful for a variety of attacks such as path traversal where our payloads depend on the operating system. This is just one example the use of this tool goes FAR beyond just that.

Use:

On kali linux -> p0f -i eth0 -p -o /path/to/output.txt

<https://github.com/p0f/p0f>