OS Fingerprinting

OS fingerprinting involves sending specially crafted packets to the target system and analyzing the responses to determine what OS is running. This is based on the fact that different OSes have unique TCP/IP stack implementations that respond differently to certain packets.

We can perform OS Fingerprinting with the help of Nmap using -O flag.

```
sudo nmap -sS -O IP
```

To detect the OS running on the target system, nmap sends bunch of probe packets and then analyze their response with its database of over 2600 known OS fingerprints. If it found a match, it will print out the OS details. Sometimes, nmap guesses the target Operating System version. This happens more in Windows hosts as there different version of windows. We can also confirm the OS details by analyzing other software an services running on the target.
