**Passive Fingerprinting – OS Identification**

**OS Identification**

Passive fingerprinting requires indistinct variations in the network unless it will be very difficult to achieve accuracy in network analysis. One of the method that we have used to identify the operating system is with Initial time to live (TTL) in IP header and the TCP window size of the first packet in a TCP session which means SYN and SYN+ACK packet.

TTL values differ with OS and there is no particular standard to put any fixed value of TTL, however recommended value for Internet Protocol (IP) is 64 and this recommendation has been made in RFC 1700 [1]. Initial TTL value captured will have done some number of router hops before it has been captured, hence its bit tricky to analyze the value of initial TTL.

Few examples of identified OS with the help of initial TTL and TCP Window size.

|  |  |  |
| --- | --- | --- |
| **Initial TTL** | **TCP Window Size** | **Operating System** |
| 128 | 65535 | Windows XP |
| 128 | 8192 | Windows 7, Vista |
| 255 | 4128 | Cisco Router (IOS 12.4) |
| 64 | 5840 | Linux – Kernel 2.4, 2.6 |
| 64 | 5720 | Google Linux (Customized) |

**References:**

1. https://tools.ietf.org/html/rfc1700