**2.**

Firewalk is an active reconnaissance network security tool that attempts to determine what layer 4 protocols a given IP forwarding device will pass. Firewalk works by sending out TCP or UDP packets with a TTL one greater than the targeted gateway. If the gateway allows the traffic, it will forward the packets to the next hop where they will expire and elicit an ICMP\_TIME\_EXCEEDED message. If the gateway host does not allow the traffic, it will likely drop the packets on the floor and we will see no response.

To get the correct IP TTL that will result in expired packets one beyond the gateway we need to ramp up hop-counts. We do this in the same manner that traceroute works. Once we have the gateway hop count (at that point the scan is said to be `bound`) we can begin our scan.

**Supported OS:-**

**Windows**

**Linux**

**MAC**

**How to download Firewalk?**

Firewalk is inbuilt app in Kali Linux. If User wants to download firewalk in windows so go to <https://nmap.org/nsedocs/scripts/firewalk.html>

**How can See What Traffic Pass Through a Device?**

Step 1: Open Kali Linux and then open terminal

Step 2: #firewalk –h

Step 3:#firewalk **-d 1-65535 (34434)**

Step 4: #firewalk**-p TCP, UDP (UDP)**

Step 5: #firewalk –s 8079-8081 –i eth0 –n –pTCP 191.1.1 192.168.0.1