# FireWalk

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

```
root@kali:~# firewalk -h
Firewalk 5.0 [gateway ACL scanner]
Usage : firewalk [options] target_gateway metric
          [-d 0 - 65535] destination port to use (ramping phase)
          [-h] program help
          [-i device] interface
          [-n] do not resolve IP addresses into hostnames
          [-p TCP | UDP] firewalk protocol
          [-r] strict RFC adherence
          [-S x - y, z] port range to scan
          [-s 0 - 65535] source port
          [-T 1 - 1000] packet read timeout in ms
          [-t 1 - 25] IP time to live
          [-v] program version
          [-x 1 - 8] expire vector
```

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

```
root@kali:~# firewalk -S8079-8081 -i eth0 -n -pTCP 192.168.1.1 192.168.0.1
Firewalk 5.0 [gateway ACL scanner]
Firewalk state initialization completed successfully.
TCP-based scan.
Ramping phase source port: 53, destination port: 33434
Hotfoot through 192.168.1.1 using 192.168.0.1 as a metric.
Ramping Phase:
 1 (TTL  1): expired [192.168.1.1]
Binding host reached.
Scan bound at 2 hops.
Scanning Phase:
port 8079: *no response*
port 8080: A! open (port not listen) [192.168.0.1]
port 8081: *no response*

Scan completed successfully.

Total packets sent:               4
Total packet errors:              0
Total packets caught              2
Total packets caught of interest  2
Total ports scanned               3
Total ports open:                 1
Total ports unknown:              0
```