Version 1.6

Usage: fragrouter [-i interface] [-p] [-g hop] [-G hopcount] ATTACK

格式: fragrouter [-i 接口] [-p] [-g hop] [-G 跳数] 攻击

where ATTACK is one of the following:

-B1: base-1: 正常的IP转发

-F1: frag-1: 命令字节的IP碎片

-F2: frag-2: 有序24字节的IP碎片

-F3: frag-3: 命令字节的IP碎片 one out of order

-F4: frag-4: 命令字节的IP碎片 one duplicate

-F5: frag-5: 无序的8字节的片段，one duplicate

-F6: frag-6: 命令字节的片段, marked last frag first

-F7: frag-7: 有序16字节片段, fwd-overwriting

-T1: tcp-1: 3-whs, bad TCP checksum FIN/RST, ordered 1-byte segments

-T3: tcp-3: 3-whs, 命令字节段， one duplicate

-T4: tcp-4: 3-whs, 命令字节段， one overwriting

-T5: tcp-5: 3-whs, 命令字节段， fwd-overwriting

-T7: tcp-7: 3-whs, 命令字节段，, interleaved null segments

-T8: tcp-8: 3-whs, 命令字节段， one out of order

-T9: tcp-9: 3-whs, out of order 1-byte segments

-C2: tcbc-2: 3-whs, 命令字节段， interleaved SYNs

-C3: tcbc-3: ordered 1-byte null segments, 3-whs, ordered 1-byte segments

-R1: tcbt-1: 3-whs, RST, 3-whs, ordered 1-byte segments

-I2: ins-2: 3-whs, 命令字节段，, bad TCP checksums

-I3: ins-3: 3-whs, 命令字节段，, no ACK set

-M1: misc-1: Windows NT 4 SP2 - http://www.dataprotect.com/ntfrag/

-M2: misc-2: Linux IP chains - <http://www.dataprotect.com/ipchains/>

实例：

Using interface eth0 (-i eth0), send ordered 8-byte IP fragments (-F1):

使用接口eth0（我是），发送命令字节的IP碎片（F1）：

root@kali:~# fragrouter -i eth0 -F1  
fragrouter: frag-1: ordered 8-byte IP fragments