Fragroute

fragroute拦截、修改和重写目的地为的出口流量 对于指定的主机，实施中描述的大多数攻击 安全网络的插入、规避和拒绝服务: 躲避网络入侵检测”论文，1998年1月。

它有一个简单的规则集语言来延迟、复制、删除， 分段、重叠、打印、重新排序、分段、来源路线或否则，对所有目的地为目标的出站数据包进行欺骗 主机，最少支持随机或概率 行为。

这个工具是为了帮助网络测试而善意编写的 入侵检测系统、防火墙和基本的TCP/IP协议栈 行为。请不要滥用本软件。

示例应用程序: *测试网络入侵检测系统超时和重组参数 *测试传输控制协议/协议清理(标准、开放标准) *测试防火墙状态检查 *模拟单向延迟、丢失、重新排序和 *重传 *实现TCP代托纳(对不起，我不会发布这个) *实施传输控制协议多业务系统箝位 *避开“被动操作系统指纹”技术

在构建这个包的时候，我修改了它以使用libdumbnet，它 libdnet是否已重命名。我这样做是因为libdnet已经在内部使用了 Debian，DECnet图书馆。

此外，您必须为您所在的接口禁用欺骗保护 嗅。这由中的“欺骗保护”变量控制 /etc/network/options。在GNU/Linux下，这种行为是最有可能的 由内核控制。您可以使用以下方法设置特定的接口: echo " 0 " >/proc/sys/net/IP v4/conf/INTERFACE/RP _ filter

重要

fragtest无法在其所有配置选项上正常工作。 选项:ip-opt、frag-new和frag-timeout不能正常工作， 因为它们依赖于libpcap的一个特性 GNU/Linux系统。不过，好消息是ip-opt确实有效 在某种意义上。以下命令: fragtest ping ip-opt localhost 将会产生一个响应，但是你将不得不退出

——*Simon Law*

sfllaw@engmail.uwaterloo.ca, Sun, 8 Sep 2002 21:44:35 -0400

一，官方手册

```
用法:fragroute [-f文件]夏令时
规则:
延迟第一个|最后一个|随机<毫秒>
先放|后放|随机< prob-% >
dup第一|最后|随机< prob-% >
回声<字符串>...
ip _ chaff dup | opt | < ttl >
IP _ frag < size >[旧|新]
ip_opt lsrr|ssrr <ptr> <ip-addr >...
ip_ttl <ttl >
ip_tos <tos >
随机订购|反向订购
打印
TCP _ skill cksum | null | paws | rex MIT | seq | syn | < TTL >
tcp_opt mss|wscale <size >
```

```
TCP _ seg < size >[旧|新]
```

```
Usage: fragroute [-f file] dst
Rules:
       delay first|last|random <ms>
       drop first|last|random <prob-%>
       dup first|last|random <prob-%>
       echo <string> ...
       ip_chaff dup|opt|<ttl>
       ip_frag <size> [old|new]
       ip_opt lsrr|ssrr <ptr> <ip-addr> ...
       ip_ttl <ttl>
       ip_tos <tos>
       order random|reverse
       print
       tcp_chaff cksum|null|paws|rexmit|seq|syn|<ttl>
       tcp_opt mss|wscale <size>
       tcp_seg <size> [old|new]
```

二，相关原理及解释

提示

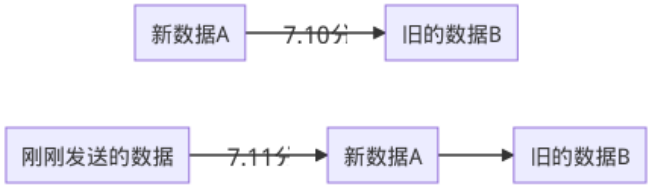
在使用fragroute前，我们需要知道fragroute在官方文档中，我们只需要知道，fragroute不提供什么华丽胡少的命令，他在帮助手册中仅仅有了两个命令，fragroute -h 和 Usage: fragroute [-f file] dst 。

配置详解

在Parrot 系统中，fragroute默认的策略组文件在/etc/fragroute.conf之中，内容为：

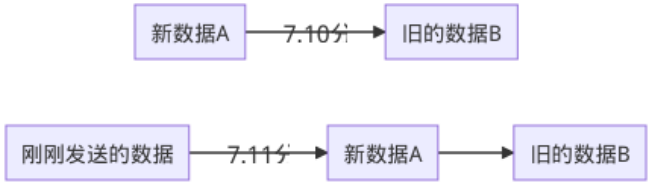
```
tcp_seg 1 new
ip_frag 24
ip_chaff dup
order random
print
```

1.TCP _ seg < size >[old|new]



列中的TCP数据分割为size大小的TCP报文段，后面两个设置是数据覆盖方式的选择，（old | new）因为目标系用的覆盖方式很难掌握，在一般的情况下不管是UNIX还是Windows系统都是由新到的数据覆盖到的数据。

2.ip_frag <size> [old |new]



> IP碎片重叠

把队列中的所有数据包分成大小为 size 的碎片，并在地一个碎片中包含完整的传输层包头。这个模块还支持IP碎片重叠，有系统是会以后的碎片的数据覆盖到先到的碎片数据，对于这种系统需要使用 new 如果不是则使用 old。

3.ip_chaff dup | opt | <ttl>

为队列中的所有数据包都制作一个负载不用（数据都是随机填充）的副本.，主要分为dup 和 opt 及 <ttl> 。

使用dup选项，fragroute将会延迟1微秒，投递数据包副本。

使用ope选项，fragroute会在数据包副本中设置无效的IP选项，

使用<ttl>选项，fragoute就会吧数据包副本的TTL值设置为较小的值

最后是chaff 应为是玩笑的、愚弄的、戏弄的。

3.order random | reverse

队列中的数据包重新以随机(random) 或 反向(reverse) 的方式排序

4.print

以Tcpdump的风格想标准输出设备输出队列中的所有数据包

5.delay first | last | random <ms>

把队列中第一个(first)、最后一个(last)或随机(random)总选择一个，延迟到 ms 微秒之后才投递出去。

在配置的时候需要带具体的毫秒数值，单位可写也可不写，随机不代表时间也随机，需要手工写入，否则将提示参数无效。

6.drop first | last | random <prob-%>

模拟数据包丢失情况，以 prob% 的记录丢掉队列中的第一个（first），最后一个(last)或随机(random)选择数据包

例如: drop first 30 意思为以30%的几率丢掉队列中的第一的数据包，drop last 100读掉队列中最后的一个数据包

7.dup first | last | random <prob-%>

以prob%的几率重复队列中地一个(first)，最后一个(last)，或者随机选择一个数据包。

例如：dup first 100，在队列中复制第一个数据包的一个副本。

dup last 100，在队列中复制最后一个数据包的一个副本。

8.echo <string>

输出字符，每一个数据输出就会打印信息，而<string>中包含的字符内容。

9.ip_opt lsrr | ssrr <ptr> <ip-addr>

在每个数据包中设置的IP选项，松散源路由（lsrr），或者严格源路由（ssrr），<ptr> 最小是4,而且必须是4的倍数，而 ip-add 则是一系列的IP地址。

10.ip_ttl <ttl>

把每个数据包的生春时间设置为 <ttl> 比如 ip_ttl 60

11.tos <tos>

把每个数据包的服务类型域（type-of-server）的值设置为tos，最小值为0，最大为7（0 ~ 7）

12.tcp_chaff cksum | null | paws | rexmit | seq | syn | <ttl>

在队列中交错插入每个 TCP 报文段的副本，负载和原来的报文段不同，其中副本报文段可以有无效的校验和（cksum），空的控制标志（null），旧的时间戳（paws）一针对序列号回卷保护（Protection Aginst Wrapped Sequence number , PAWS）伪造的重传调度（rexmit），超出窗口的序列号（seq），在TCP数据流中间的重新同步序列号的请求（syn）或者短的生存期值（ttl），是一个大于0小于265的整数。

13.tcp_opt mss | wscale <size>

为每个TCP报文段添加选项，设置期最大报文段长度（0—65535）或者窗口放大因子的大小为（0—255）为size.

例如：tcp_opt mss 3137 ，tcp_opt wscale 255

三，基本命令使用

> 首先使用fragroute的前提是你需要和他建立一个“握手”，因为Fragroute能够截取，修改，重写向外发送的保温，包括IP、TCP层的数据碎片以及数据包数据重叠技术等，他主要根据配置文件的配置来进行相关的运行。

> Fragroute的使用非常简单，就只有一句话，此时你需要对 36.110.164.37 建立握手，当然就是 ping 36.110.164.37

fragroute -f /etc/fragroute.conf 36.110.164.37

使用fragroute.conf文件定制的规则对36.110.164.37进行截取，其他的只需要根据配置文件进行配置即可。