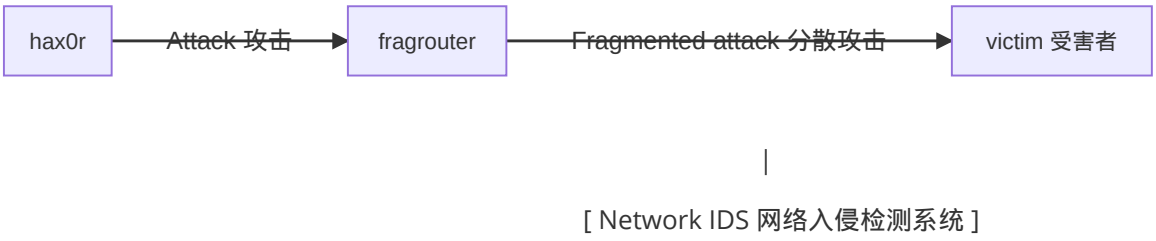
Fragrouter

Fragrouter是一个网络入侵检测规避工具箱。它实现安全网络中描述的大多数攻击插入、逃避和拒绝服务:逃避网络入侵编写这个程序是希望能进行更精确的测试方法可以应用于网络入侵领域检测，充其量也不过是一种巫术。

从概念上讲，fragrouter只是一个单向的分段路由器- IP包从攻击者发送到fragrouter，它进行转换将它们转换成碎片数据流转发给受害者。



大多数网络IDSs之所以成为这种攻击隐藏技术的受害者，是因为他们不会费心去重构一个连贯的网络数据视图(通过IP碎片和TCP流重新组装)。

——*Dug Song, Anzen Computing,Mati Aharoni*

一，帮助手册

版本1.6
用法:fragrouter [-i接口][-p] [-g hop] [-g hopcount]攻击

其中攻击是下列之一:

-B1: base-1:正常的IP转发
-F1:片段-1:有序8字节的IP片段
-F2:片段2:有序的24字节IP片段
-F3:片段-3:有序的8字节的IP片段，一个无序
-F4:片段-4:有序8字节的IP片段，一个副本
-F5:片段-5:无序的8字节片段，一个副本
-F6:片段-6:有序的8字节片段，标记最后的frag优先
-F7:片段-7:有序16字节片段，fwd-覆盖
-T1: TCP -1: 3-whs，错误的TCP校验和FIN/RST，有序的1字节段
-T3: tcp-3: 3-whs，有序的1字节段，一个副本
-T4: tcp-4: 3-whs，有序的1字节段，一次覆盖
t5: ttp -5: 3-whs，有序2字节段，fwd-覆盖
t7: ttp -7: 3-whs，有序的1字节段，交错的空段
t8: tcp-8: 3-whs，有序的1字节段，一个无序
t9: ttp -9: 3-whs，无序的1字节段

-C2: tcbc-2: 3-whs，有序的1字节段，交错的SYNs
-C3: tcbc-3:有序的1字节空段，3-whs，有序的1字节段
-R1: tcbt-1: 3-whs, RST, 3-whs，有序的1字节段
i2: ins-2: 3-whs，有序的1字节段，错误的TCP校验和
-I3: ins-3: 3-whs，有序的1字节段，没有ACK集

m1: misc-1: Windows NT 4 SP2 - http://www.dataprotect.com/ntfrag/

m2: misc-2: Linux IP链- http://www.dataprotect.com/ipchains/

Version 1.6
Usage: fragrouter [-i interface] [-p] [-g hop] [-G hopcount] ATTACK

where ATTACK is one of the following:

-B1: base-1: normal IP forwarding
-F1: frag-1: ordered 8-byte IP fragments
-F2: frag-2: ordered 24-byte IP fragments
-F3: frag-3: ordered 8-byte IP fragments, one out of order
-F4: frag-4: ordered 8-byte IP fragments, one duplicate
-F5: frag-5: out of order 8-byte fragments, one duplicate
-F6: frag-6: ordered 8-byte fragments, marked last frag first
-F7: frag-7: ordered 16-byte fragments, fwd-overwriting
-T1: tcp-1: 3-whs, bad TCP checksum FIN/RST, ordered 1-byte segments
-T3: tcp-3: 3-whs, ordered 1-byte segments, one duplicate
-T4: tcp-4: 3-whs, ordered 1-byte segments, one overwriting
-T5: tcp-5: 3-whs, ordered 2-byte segments, fwd-overwriting
-T7: tcp-7: 3-whs, ordered 1-byte segments, interleaved null segments
-T8: tcp-8: 3-whs, ordered 1-byte segments, one out of order
-T9: tcp-9: 3-whs, out of order 1-byte segments
-C2: tcbc-2: 3-whs, ordered 1-byte segments, 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, ordered 1-byte segments, bad TCP checksums
-I3: ins-3: 3-whs, ordered 1-byte segments, 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/

二，命令介绍与原理

命令实例

```
#fragrouter -i wlan0 -B1
fragrouter: base-1: normal IP forwarding
192.168.0.1 > 224.0.0.1: ip-proto-2 36 [ttl 1]
192.168.0.1 > 224.0.0.1: ip-proto-2 36 [ttl 1]
192.168.0.1 > 224.0.0.1: ip-proto-2 36 [ttl 1]
192.168.0.1 > 224.0.0.1: ip-proto-2 36 [ttl 1]
192.168.0.1 > 224.0.0.1: ip-proto-2 36 [ttl 1]
192.168.0.1 > 224.0.0.1: ip-proto-2 36 [tos 0xaa] [ttl 1]
```

fragrouter -i wlan0 -B1

使用Wlan0接口进行普通的IP转发

> fragrouter的命令非常简单，你可以根据你需要的场景进行选择即可，以下是一个例子：

> fragrouter -i 接口（你可以根据ifconfig进行查看） -参数

相关原理

> Fragrouter可以逃避入侵检测后发起IP攻击

从上面的软件介绍中可以看出Fragrouter是一种网络入侵规避工具，我们可以从上面的网络拓扑图中可以看到，在安装有"Fragrouter"被当作一个中转机。

我们假设PC1是一个攻击机，攻击Fragrouter，然后Fragrouter进行转发，这个抓发的地址有可能是你制定的地址，当然也有可能是本地局域网的预留地址。

而这一个转发的机制，可以对企业的网络造成很强的伤害，我们可以从一个追踪人员的角度来思考，当攻击者对装有FragRouter计算机或网络设备发动攻击时，往往已经拿到了该企业中的一台机器，如果直接操作FragRouter开展攻击，则会在中转机中留下很多信息，比如说日志等。

而当攻击者远程攻击中专机时，FragRouter将会不顾思考的转发给企业局域网，这就将是一个可怕的后果，而这个后果对于追踪人员来说，也许追踪会变得更加复杂。