FTester

防火墙测试器(朋友专用)，是为测试而设计的工具 防火墙过滤策略，从0.6版开始，它还包括入侵 检测系统测试功能。基本上，ftester是由一个包组成的 生成器工具(ftest)和嗅探器(ftestd)，第一个脚本注入自定义 当嗅探器监听数据包时，数据包的数据部分带有签名 标记的数据包，嗅探器日志与注射器日志的比较 允许识别防火墙过滤规则。与普通防火墙不同 测试工具或包生成器ftester能够生成网络 看起来像防火墙或入侵检测系统的真实连接的流量 经过测试，这个特性允许我们测试状态检测防火墙(比如netfilter或ipfilter)和IDS(如snort)。这个的另一个优点是 体系结构是我们可以欺骗精心制作的数据包源地址，因为 嗅探器知道哪些数据包是由其对应方生成的，一些技巧 当模拟真实连接时，包含TTL也允许欺骗，这 被描述为“连接欺骗模式”。 ftester组件是perl脚本，因此它们可以在任何平台上执行 最新版本的perl(至少推荐5.6.1)和三种perl 模块网络::RawIP，网络::PcapUtils，网络数据包，它们可以在 www.cpan.org或使用CPAN壳。

——*Andrea Bari Sani*

< Andrea @ reverse epath . com >

一，帮助手册

配置选项:
-f <conf_file >
-c <源*ip* >:<*源*端口>:<目的*ip* >:<*目的*端口>:<标志>:<协议>:< tos >
-v <详细>

计时选项:
-d <延迟，0.25 = 250 ms >
-s <睡眠时间，1 = 1 s >

规避选项:
-e <规避方法>
-t <ids_ttl >

连接选项:
-r <重置连接>
-F <端部连接>
-g <IP片段数。4|IP片段大小。16b >
-p <传输控制协议段数。4|TCP数据段大小，es 6b >
-k <cksum值。60000 >
-m <标记>

Configuration options:
 -f <conf_file>
 -c <source_ip>:<source_port>:<dest_ip>:<dest_port>:::
 -v

Timing options:
 -d <delay, 0.25 = 250 ms>
 -s <sleep time, 1 = 1 s>

Evasion options:
 -e
 -t <ids_ttl>

Connection options:
 -r
 -F
 -g <IP fragments number, es. 4|IP fragments size, es. 16b>
 -p <TCP segments number, es. 4|TCP segments size, es 6b>
 -k <cksum value, es. 60000>
 -m

二，命令实例

此工具以不能正常使用，如有解决方法请联系 backsunli@yeah.net
感激不尽。