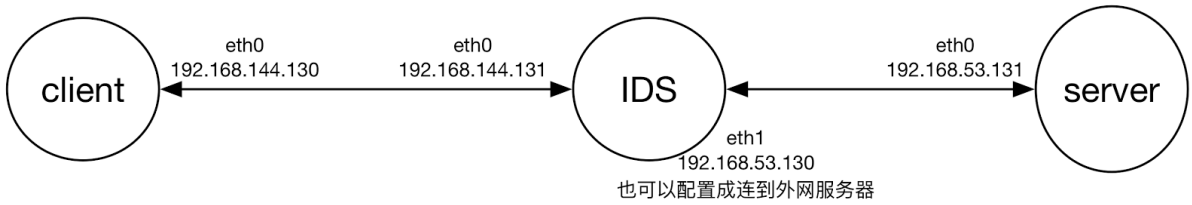
IDS 逃逸测试实验

1、实验目的：
通过本次实验，深入理解 TCP/IP 协议的数据格式、TCP 连接的建立和终止过程、对 TCP 连接的攻击方法、和逃逸技术。理解 IDS 过滤的原理，并设法绕过检测。

2、背景：
某国家级 IDS 系统会对包括敏感词的 HTTP 连接进行阻断。例如 http://mit.edu/mitmproxy.org，这个 URL 所在的页面并不存在，但是其中包含了敏感词，导致连接被阻断；而在没有 IDS 的环境下，正常的 HTTP 请求会收到 404 消息页面。

3、要求：
请结合 TCP/IP 协议相关知识，以及 IDS 实现的原理，实现绕过 IDS 的敏感词过滤，获取 http://mit.edu/mitmproxy.org 这个 URL 下返回的 404 页面。
实际实验设计可参见拓扑图结构，也可自行设计，可将 IDS 的 eth1 配置成访问外网，获取 http://mit.edu/mitmproxy.org 这个 URL 下返回的 404 页面。也可以自己在第三台机器上面自己搭建服务器，来测试收到的流量信息。

网络拓扑图结构



说明：
1. 在client 端配置路由表
2. 在IDS上开启ip forward，并设置流量网卡之间的转发，
   比如iptables –t nat –A POSTROUTING –s 192.168.144.0/24 –d 0.0.0.0/0 –o eth1 –j MASQUERADE
   # 配置源地址144网段，目标地址anywhere，从eth1网卡出
3. IDS 上面设置规则检测，检测到某字段如（GET HTTP）则向两端发送RST,(具体规则请参见教程)

可参考的方法如下：
把敏感词拆开，分在不同的 tcp segments 或 IP fragments 里面，外加不同的重叠策略，使请求能够被目标 mit.edu 正常识别、但是使 IDS 识别不出来；

在 TCP 建立连接后、发送敏感词之前，发送 RST 告诉 IDS 连接终止（从而放弃监听），但是使目标 mit.edu 不会接受这个 RST。

4、建议使用 Scapy 来实现，参考资料如下：
官方文档 - http://www.secdev.org/projects/scapy/doc/
非官方新手指南 - http://theitgeekchronicles.files.wordpress.com/2012/05/scapyguide1.pdf

使用 Scapy 进行分片 - http://www.sans.org/reading-room/whitepapers/detection/ip-fragment-reassembly-scapy-33969
snort 规则教程：http://snort.datanerds.net/writing_snort_rules.htm#first_example

提交实验报告、测试脚本，并准备在课堂上做演示。
本实验要求最好两个人组队进行实验，不然可能一个人工作量比较大。
本实验的问题可以和助教讨论：韦俊琳：weijl16@mails.tsinghua.edu.cn
关于分组的问题，可以加入微信圈互相沟通。