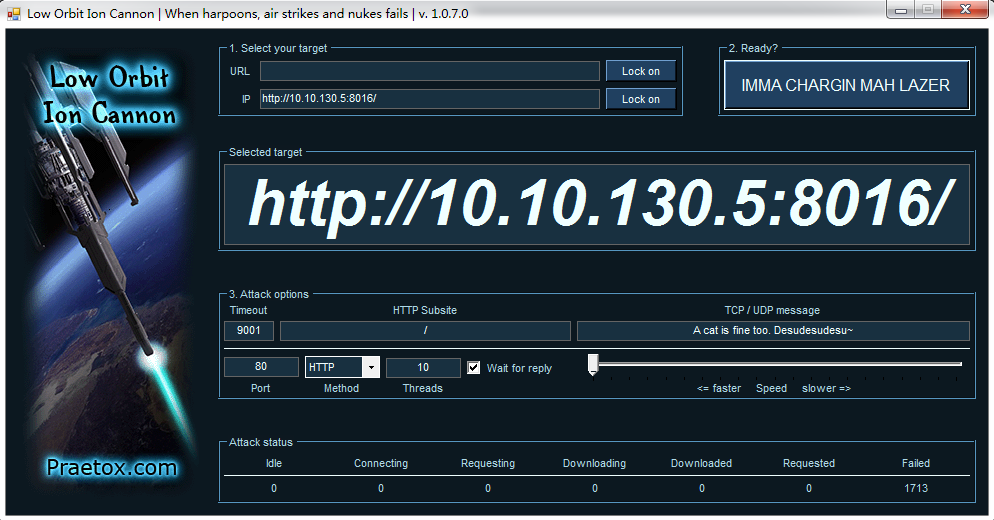
1. 试图安装并采用ddos的测试攻击工具，对实际网站进行模拟攻击，并捕获其数据包，试图理解其原理并对今后的测试可行度进行分析。
2. 下载运行**(LOIC) (Low Orbit Ion Canon)**

此工具由c#编写，下载地址<http://sourceforge.net/projects/loic/>

压缩包下载完后杀毒软件会报毒

国内某网站也提供此工具下载，但压缩包不能解压（解压会有劫持注册表的木马，本机曾惨遭毒手）

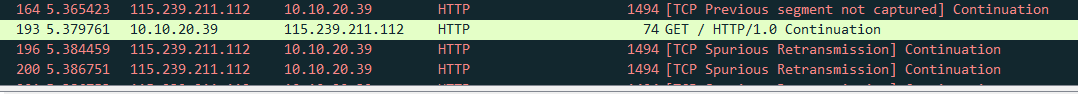
界面如图：

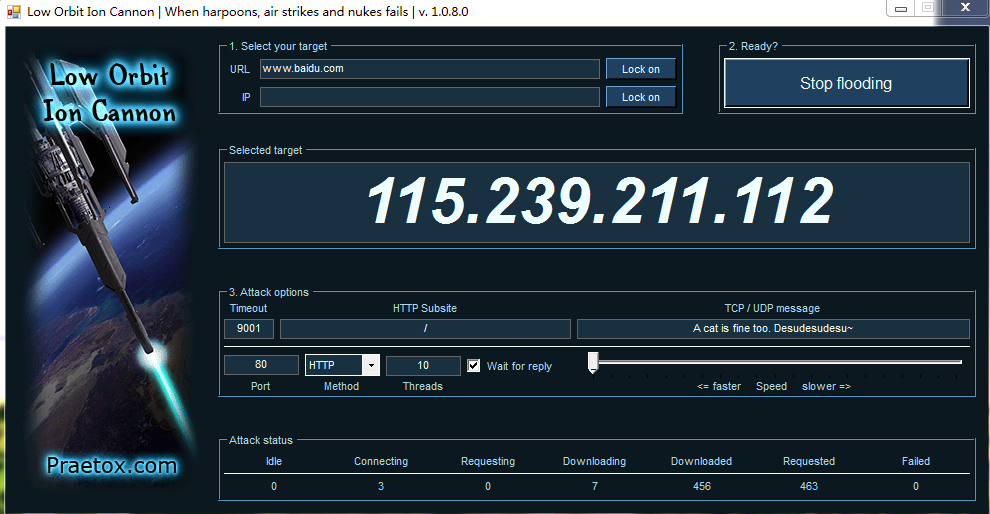


模拟攻击的网站为鹰潭职业技术学院的网站项目

但无论攻击方式选用http（tcp/udp），其攻击状态一直为failed数量递增（udp/tcp模式不起作用），使用wireshark并未捕获到其攻击所用的数据包。

原因分析：鹰潭职业技术学院的网站项目部署在公司域网服务器，没有域名（固定IP）无法从外网以http等协议访问(或者通过局域网时遭遇什么阻碍？)

证明：将攻击目标改为[www.baidu.com](http://www.baidu.com),工具有效，wireshark能捕获其攻击请求：



但该服务器无法做到监控资源和连接等状态异常，故如需要实际验证需要一个具有外网环境的且能监控服务器的测试目标

3.下载安装**DDOSIM-Layer**

工具由c++编写,并且在Linux系统上运行。

<http://sourceforge.net/projects/ddosim/> 下载源码包

使用SSH Secure File Transfer Client传送至本机virtual box的linux虚拟机:

在linux安装

tar zxvf ddosim-0.2.tar.gz –C /usr/test/

./configure

（显示缺少g++环境）

yum install g++

（命令执行失败显示没有源包）

yum install gcc-c++

（安装g++成功，命令差别执行结果不同原因不明）

./configure

（显示缺少libpcab库）

yum install libpcab-devel

（安装成功）

./configure

（显示缺少libnet0库）

Yum install libnet0-devel

（执行失败，显示没有源包，至此各种百度都无法解决，此工具安装破产）

4.其余ddos攻击工具：（仅提供可以下载到源码安装运行的）

**Tor's hammer****（python环境）**http://packetstormsecurity.com/files/98831/

**DAVOSET（perl环境）**http://packetstormsecurity.com/files/123084/DAVOSET-1.1.3.html

**GoldenEye（python环境）**

http://packetstormsecurity.com/files/120966/GoldenEye-HTTP-Denial-Of-Service-Tool.html