Pentbox是一款网络攻击、检测平台。下面是对它的主要使用功能分析。

主要结构分析：

- 解码、密码破解工具

Base64 Encoder & Decoder

Multi-Digest (MD5, SHA1, SHA256, SHA384, SHA512, RIPEMD-160)

Hash Password Cracker (MD5, SHA1, SHA256, SHA384, SHA512, RIPEMD-160)

Secure Password Generator

- 网络测试工具

Net DoS Tester

TCP port scanner

Honeypot （蜜罐）

Fuzzer （漏洞检测）

DNS and host gathering

MAC address geolocation (samy.pl)

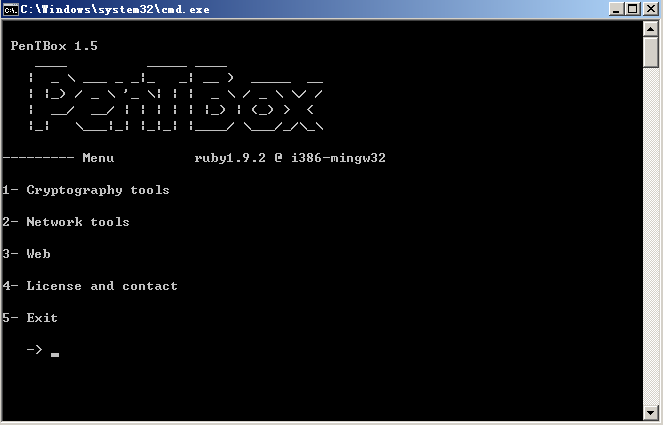
- Web安全测试工具

HTTP directory bruteforce （暴力分析HTTP下目录）

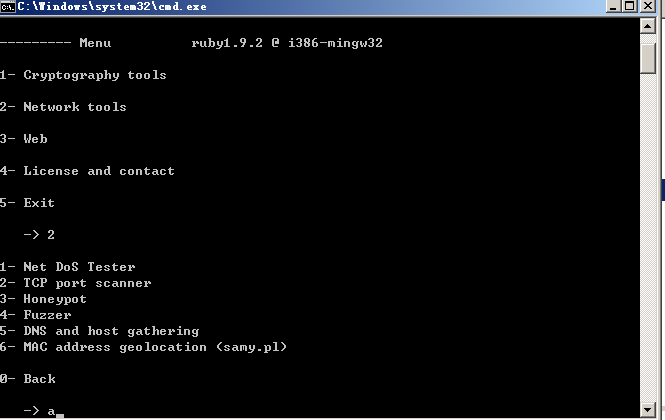
HTTP common files bruteforce （常规猜测目录）

开始测试：

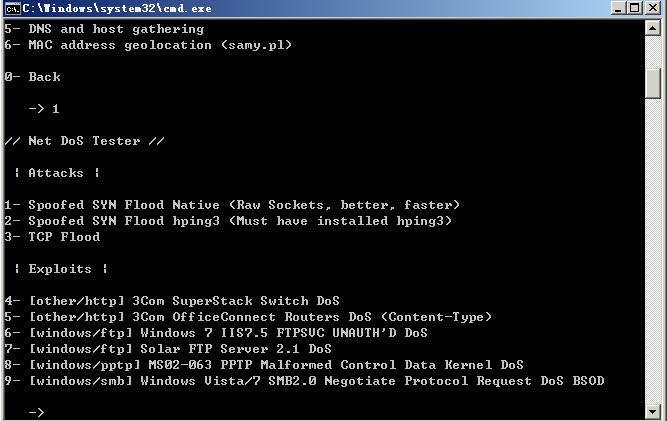
主界面选择Network tools



选择1 net dos tester



几秒后出现如下界面



// Net DoS Tester //

| Attacks |

1- Spoofed SYN Flood Native (Raw Sockets, better, faster)

2- Spoofed SYN Flood hping3 (Must have installed hping3)

3- TCP Flood

| Exploits |

4- [other/http] 3Com SuperStack Switch DoS

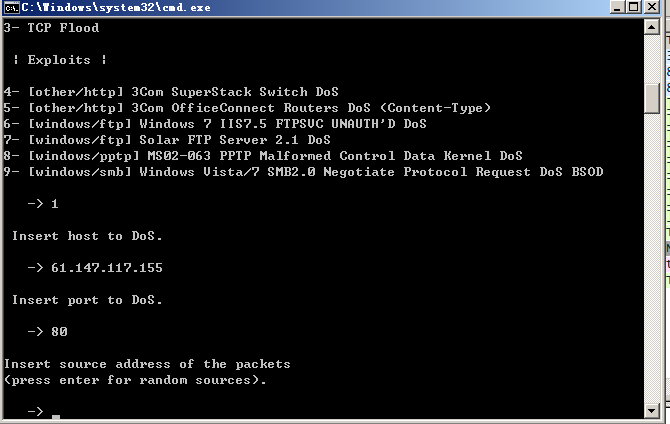
5- [other/http] 3Com OfficeConnect Routers DoS (Content-Type)

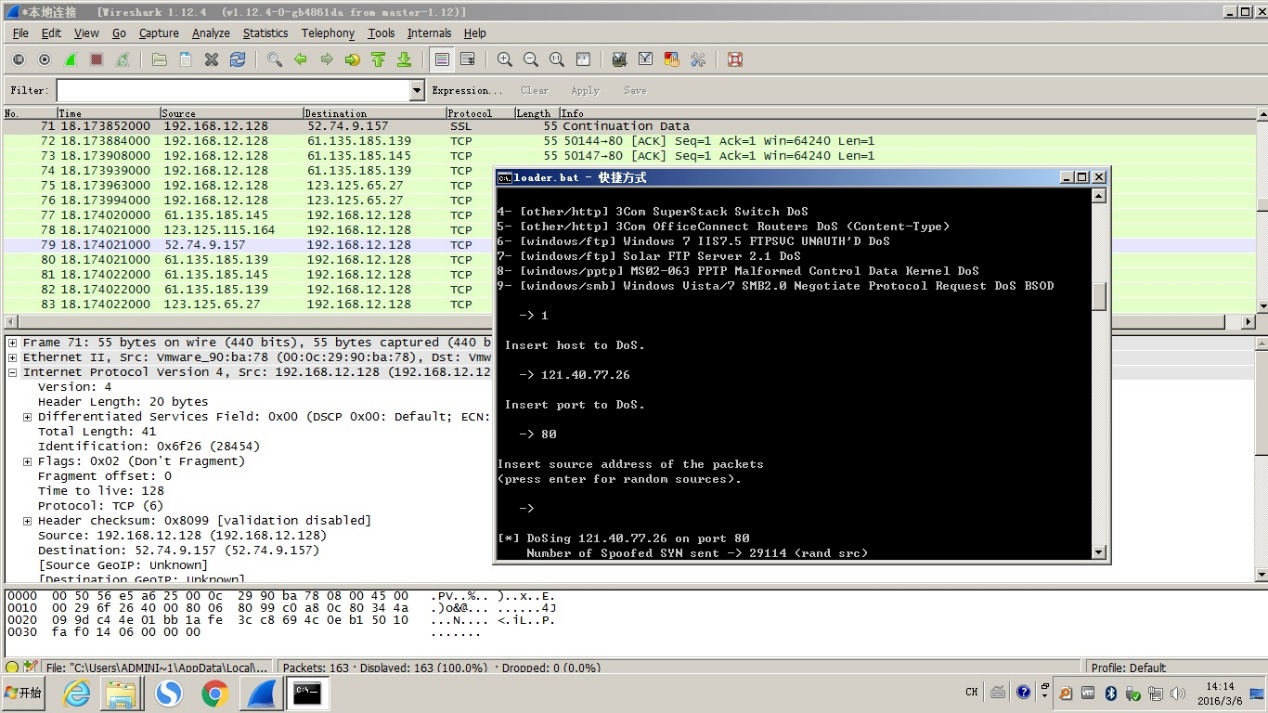
6- [windows/ftp] Windows 7 IIS7.5 FTPSVC UNAUTH'D DoS

7- [windows/ftp] Solar FTP Server 2.1 DoS

8- [windows/pptp] MS02-063 PPTP Malformed Control Data Kernel DoS

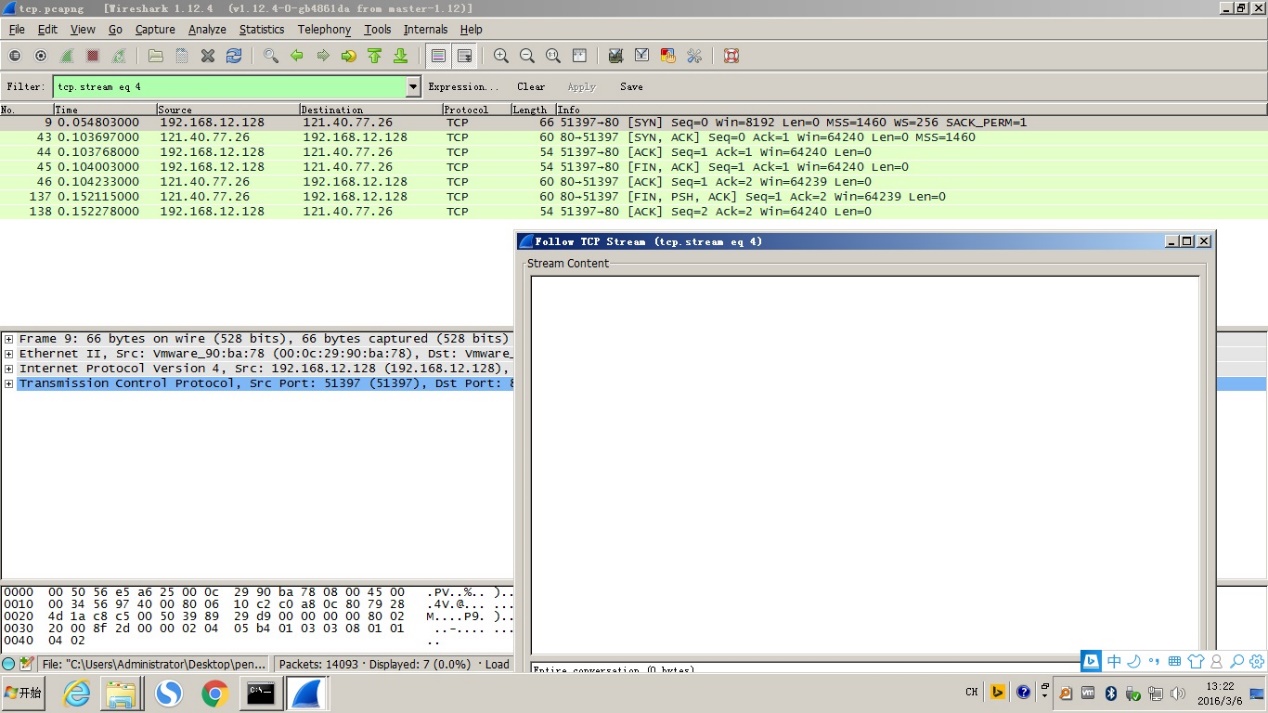
9- [windows/smb] Windows Vista/7 SMB2.0 Negotiate Protocol Request DoS BSOD



然后我用Spoofed SYN Flood Native (Raw Sockets, better, faster)进行攻击，但是wireshark抓不到我攻击的网站的数据包。（抓包文件）

第二种攻击方式（2- Spoofed SYN Flood hping3 (Must have installed hping3)

）和第一种是一样的结果。抓不到发送给目标服务器的数据包。

第三种攻击方式（flood tcp）抓包截图如下

可以看到，软件对目标服务器不断进行tcp的连接和断开。分析Tcp stream没有数据。（抓包文件）