# 黑客攻防实战入门

## 第1章 信息搜集

网站注册信息

网管资料

共享信息

端口信息

FTP资源

常见漏洞

弱口令

搜索引擎在信息搜集中的作用

## 1.1 网站信息搜集

### 1.1.1 基本信息搜集

1. 由域名得到IP地址

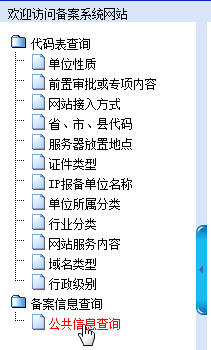
ping, nslookup

2. 由IP地址得到地理位置

[www.ip138.com](http://www.ip138.com)

3. 网站备案信息查询

一般网站底部都有“京ICP证XXXXXX号”，点这个链接，就到了<http://www.miibeian.gov.cn/>，在这里点击“公共查询”，在弹出的页面上，左侧的导航栏底部有“备案信息查询”，



点击进去，输入网站域名或许可证号码，便可以查询该网站的备案信息。

4. 网站whois信息搜集

中国万网 [www.net.cn](http://www.net.cn)

Godaddy [www.godaddy.com](http://www.godaddy.com)

例如：查询新浪的，

<http://panda.www.net.cn/cgi-bin/Whois.cgi?domain=sina&comcn=yes&refer>=

### 1.1.2 结构探测

一般来说，网站的基本结构如图1-17所示。

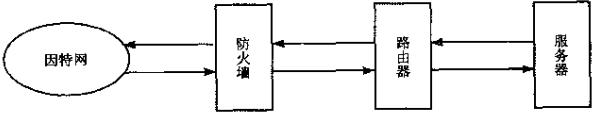


图1-17

**Linux下：**

1. cheops，<http://cheops-ng.sourceforge.net/> ，可以绘制本地或远程网络的网络图，并且也能识别主机的操作系统类型。如图1-18所示。

图1-18

**Windows下：**

2. VisualRoute，<http://www.visualroute.com/> ，

3. tracert命令，

### 1.1.3 搜索引擎

搜索引擎里可以搜索到很多有价值的信息，只要是你感兴趣的字符串，都可以搜索一下，或许会得到意想不到的信息。

搜索引擎首选Google，其次是百度，有道，搜狗，搜搜，bing, 雅虎。

## 1.2 资源搜集

### 1.2.1 共享资源简介

**1. 共享资源**

这里提及的共享资源是指Windows系统中的“共享磁盘”、“共享文件夹”、“共享文件”、“共享打印机”等。对于一般的共享，下面会有一个“托手”标志，而对于”$”为结尾的共享的没有“托手”标志，叫做“隐藏共享”。

**2. 建立共享的条件**

条件一：需要有足够的权限

条件二：已安装“Microsoft网络文件与打印机共享”组件，其界面如图1-27所示。

条件三：已安装NetBEUI协议，如图1-28所示。如果没有安装NetBEUI协议，那么只能使用IP地址来访问共享资源，如果安装了，便可以在同一局域网内使用主机名来访问共享资源。

如果满足上述条件，就可以在计算机上建立“共享资源”了。

### 1.2.2 共享资源搜索

扫描器，顾名思义，就是能够自动完成探测扫描任务的一种工具。入侵者用它来代替重复的手工劳动，实现对目标网络信息的自动搜索、整理甚至分析。

1. Angry IP Scanner

主页：<http://www.angryip.org/>

Angry IP Scanner 是一款开源、跨平台的扫描器，它主要Ping目标IP，看这台机器是否是有回应，从而判断其是否活动，更多特性请参见[这里](http://www.angryip.org/w/About)。

填入目标网络起始IP和结束IP，点击“Start”按钮开始扫描。扫描结果如图1-29所示。其中红色的是不在线的主机，蓝色的是在线的主机。

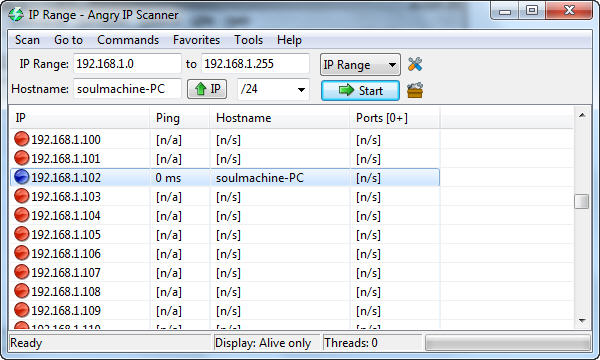


图1-29

2. Legion

下载地址：<http://www.packetstormsecurity.org/groups/rhino9/>

### 1.2.3 利用共享资源入侵

**1. autorun.inf**

[autorun]

open=hack.exe

**2. 开机启动**

### 1.2.4 破解Windows 9x共享密码

PQwak2

### 1.2.5 FTP资源扫描

sftp

## 1.3 端口扫描

### 1.3.1 网络基础知识

TCP三次握手，见谢希仁《计算机网络（第5版）》

### 1.3.2 端口扫描原理

**1．端口扫描原理**

尝试与目标主机的某些端口建立连接，如果目标主机该端口有回复（见三次握手中的第二次），则说明该端口开放，即为“活动端口”。

**2．扫描原理分类**

（1）全TCP连接

这种扫描方法使用三次握手，与目标计算机建立标准的TCP连接。需要说明的是，这种古老的扫描方法很容易被目标主机记录。

（2）半打开式扫描（SYN扫描）

在这种扫描技术中，扫描主机自动向目标计算机的指定端口发送SYN数据段，表示发送建立连接请求。

a．如果目标计算机的回应TCP报文中SYN=1，ACK=1，则说明该端口是活动的，接着扫描主机传送一个RST给目标主机拒绝建立TCP连接，从而导致三次握手过程的失败。

b．如果目标计算机的回应是RST，则表示该端口为“死端口”，这种情况下，扫描主机不用做任何回应。

由于扫描过程中，全连接尚未建立，所以大大降低了被目标计算机的记录的可能性，并且加快了扫描的速度。

（3）FIN扫描

在前面介绍过的TCP报文中，有一个字段为FIN，FIN扫描则依靠发送FIN来判断目标计算机的指定端口是否活动。

发送一个FIN=1的TCP报文到一个关闭的端口时，该报文会被丢掉，并返回一个RST报文。但是，如果当FIN报文到一个活动的端口时，该报文只是简单的丢掉，不会返回任何回应。

从FIN扫描可以看出，这种扫描没有涉及任何TCP连接部分，因此，这种扫描比前两种都安全，可以称之为秘密扫描。

（4）第三方扫描

第三方扫描又称“代理扫描”，这种扫描是利用第三方主机来代替入侵者进行扫描。这个第三方主机一般是入侵者通过入侵其他计算机而得到的，该“第三方”主机常被入侵者称之为“肉鸡”。这些“肉鸡”一般为安全防御系数极低的个人计算机。

### 1.3.3 端口扫描工具

**1. X-Port**

**2. PortScanner**

**3. SuperScan**

主页：<http://www.foundstone.com/us/resources/proddesc/superscan.htm> ，

### 1.3.4 操作系统识别

每种操作系统都开放有不同的端口供系统间通信使用，因此从端口号上也可以大致判断目标主机的操作系统。一般认为开有135、139端口的主机为Windows系统。如果除了135、139外，还开放了5000端口，则该主机为Windows XP操作系统。

## 1.4 综合扫描

### 1.4.1 X-Scan

### 1.4.2 流光Fluxay

### 1.4.3 X-Way

### 1.4.4 扫描器综合性能比较

## 第2章 基于认证的入侵