

Kali Linux 渗透基础知识：信息搜集

1、什么是信息收集：

收集渗透目标的情报是最重要的阶段。如果收集到有用的情报资料的话，可以大大提高对渗透测试的成功性。收集渗透目标的情报一般是对目标系统的分析，扫描探测，服务查点，扫描对方漏洞，查找对方系统 IP 等，有时候渗透测试者也会用上“社会工程学”。渗透测试者会尽力搜集目标系统的配置与安全防御以及防火墙等等。

2、内容概要

网站及服务器信息

搜索引擎

Google Hacking

社交网站

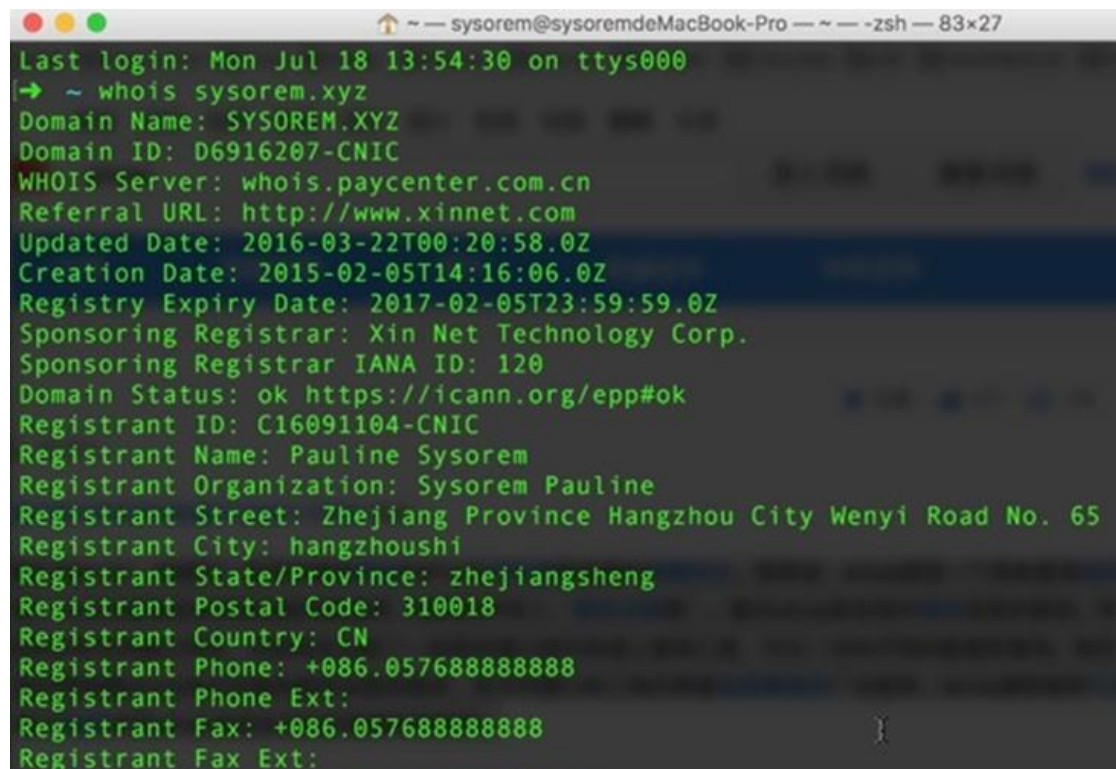
第三方未公开数据

3、whois

whois 是用来查询域名的 IP 以及所有者等信息的传输协议。简单说，whois 就是一个用来查询域名是否已经被注册，以及注册域名的详细信息的数据库（如域名所有人、域名注册商）。在 whois 查询中，注册人姓名和邮箱信息，通常

对于测试个人站点非常有用，因为我们可以通过搜索引擎，社交网络，挖掘出很多域名所有人的信息。而对于小站点而言，域名所有人往往就是管理员。

例如下面 whois www.sysorem.xyz 查看 www.sysorem.xyz 这个域名的注册信息

A terminal window on a MacBook Pro showing the output of a 'whois sysorem.xyz' command. The window title is '~ sysorem@sysoremdeMacBook-Pro ~ -zsh - 83x27'. The output text is as follows:

```
Last login: Mon Jul 18 13:54:30 on ttys000
→ ~ whois sysorem.xyz
Domain Name: SYSOREM.XYZ
Domain ID: D6916207-CNIC
WHOIS Server: whois.paycenter.com.cn
Referral URL: http://www.xinnet.com
Updated Date: 2016-03-22T00:20:58.0Z
Creation Date: 2015-02-05T14:16:06.0Z
Registry Expiry Date: 2017-02-05T23:59:59.0Z
Sponsoring Registrar: Xin Net Technology Corp.
Sponsoring Registrar IANA ID: 120
Domain Status: ok https://icann.org/epp#ok
Registrant ID: C16091104-CNIC
Registrant Name: Pauline Sysorem
Registrant Organization: Sysorem Pauline
Registrant Street: Zhejiang Province Hangzhou City Wenyi Road No. 65
Registrant City: hangzhoushi
Registrant State/Province: zhejiangsheng
Registrant Postal Code: 310018
Registrant Country: CN
Registrant Phone: +086.057688888888
Registrant Phone Ext:
Registrant Fax: +086.057688888888
Registrant Fax Ext:
```

4、DNS 服务器查询

除了 whois 查询之外，我们还可以通过 host 命令来查询 dns 服务器，

格式：

host 命令

[-aCdIriTwv]

[-c class]

[-N ndots]

[-t type]

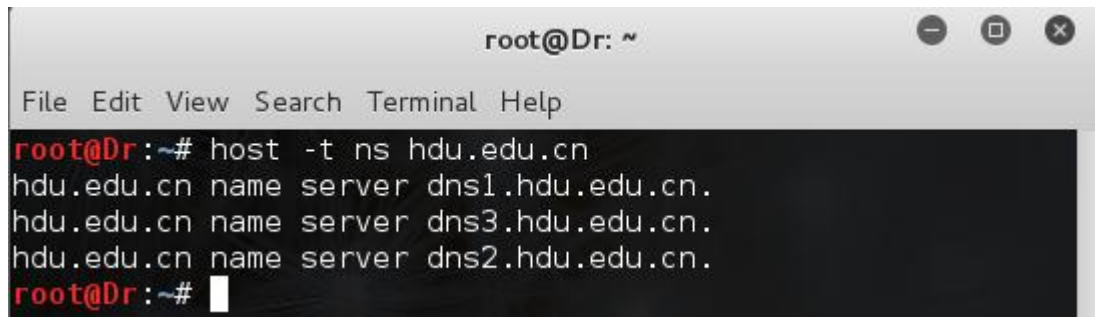
[-W time]

[-R number]

[-m flag]

hostname [server]

查询域名服务器



```
root@Dr: ~  
File Edit View Search Terminal Help  
root@Dr:~# host -t ns hdu.edu.cn  
hdu.edu.cn name server dns1.hdu.edu.cn.  
hdu.edu.cn name server dns3.hdu.edu.cn.  
hdu.edu.cn name server dns2.hdu.edu.cn.  
root@Dr:~#
```

从图中可以看到有 3 个 dns 服务器，分别为：

dns1.hdu.edu.cn

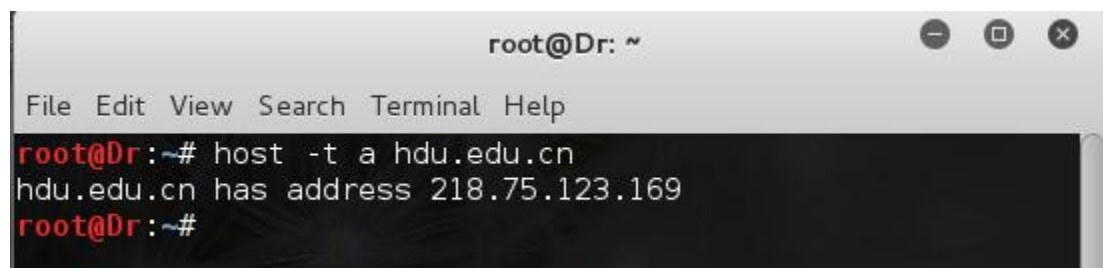
dns2.hdu.edu.cn

dns2.hdu.edu.cn

DNS 记录类型=>在买了域名后 IDC 的那个后台里，添加解析记录的地方就能看到

Type	Meaning	Value
SOA	Start of Authority	Parameters for this zone
A	IP address of a host	32-Bit integer
MX	Mail exchange	Priority, domain willing to accept email
NS	Name Server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
HINFO	Host description	CPU and OS in ASCII
TXT	Text	Uninterpreted ASCII text

例如查询 A 记录，即查 IP，如图

A terminal window titled 'root@Dr: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The command 'host -t a hdu.edu.cn' is entered, and the output is 'hdu.edu.cn has address 218.75.123.169'. The prompt 'root@Dr:~#' is shown again.

```
root@Dr: ~
File Edit View Search Terminal Help
root@Dr:~# host -t a hdu.edu.cn
hdu.edu.cn has address 218.75.123.169
root@Dr:~#
```

5、域名枚举

在得到主域名信息之后，如果能通过主域名得到所有子域名信息，再通过子域名查询其对应的主机 IP，这样我们能得到一个较为完整的信息。

使用 fierse 工具，可以进行域名列表查询：fierce -dns domainName

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# fierse -dns hdu.edu.cn  
DNS Servers for hdu.edu.cn:  
    dns1.hdu.edu.cn  
    dns2.hdu.edu.cn  
    dns3.hdu.edu.cn  
  
Trying zone transfer first...  
    Testing dns1.hdu.edu.cn  
        Request timed out or transfer not allowed.  
    Testing dns2.hdu.edu.cn  
        Request timed out or transfer not allowed.  
    Testing dns3.hdu.edu.cn  
        Request timed out or transfer not allowed.  
  
Unsuccessful in zone transfer (it was worth a shot)  
Okay, trying the good old fashioned way... brute force  
  
Checking for wildcard DNS...  
Nope. Good.  
Now performing 2280 test(s)...  
192.168.100.39  accounting.hdu.edu.cn  
192.168.100.56  appl.hdu.edu.cn  
192.168.2.253  auth.hdu.edu.cn  
192.168.101.171 jxj.split.hdu.edu.cn  
192.168.101.166 vrspace.split.hdu.edu.cn.
```

除 fierse 之外，dnsdict6、dnsenum、dnsmap 都可以进行域名枚举。

6、反向地址解析

我们经常使用到得 DNS 服务器里面有两个区域，即“正向查找区域”和“反向查找区域”，正向查找区域就是我们通常所说的域名解析，反向查找区域即是这里所说的 IP 反向解析，它的作用就是通过查询 IP 地址的 PTR 记录来得到该 IP 地址指向的域名。

由于在域名系统中，一个 IP 地址可以对应多个域名，因此从 IP 出发去找域名，理论上应该遍历整个域名树，但这在 Internet 上是不现实的。为了完成逆向域名解析，系统提供一个特别域，该特别域称为逆向解析域 in-addr.arpa。这样欲解析的 IP 地址就会被表达成一种像域名一样的可显示串形式，后缀以逆向解析域域名“in-addr.arpa”结尾。例如一个 IP 地址：222.211.233.244，其逆向域名表达方式为：244.233.221.222.in-addr.arpa

dig:使用 dig 进行反向解析的命令格式为：

dig -x ip @dnsserver #用 dig 查看反向解析

```
root@kali:~# host -t a www2.hdu.edu.cn
www2.hdu.edu.cn is an alias for www2.split.hdu.edu.cn.
www2.split.hdu.edu.cn has address 218.75.123.181
www2.split.hdu.edu.cn has address 218.75.123.182
root@kali:~# dig -x 218.75.123.181 @dns1.hdu.edu.cn

; <=> DiG 9.10.3-P4-Debian <=> -x 218.75.123.181 @dns1.hdu.edu.cn
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 11043
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;181.123.75.218.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
181.123.75.218.in-addr.arpa. 38400 IN     PTR      www2.hdu.edu.cn.
181.123.75.218.in-addr.arpa. 38400 IN     PTR      Symantec-server.hzlee.edu.cn.
```

在线查询也是一种办法 <http://dns.aizhan.com/>

相关站点

PING检测

IP反查域名

whois查询

whois反查

IP反查域名

请输入你要查询的IP或域名: 218.75.123.181

查询

本工具可以查看某个IP上绑定了哪些域名。

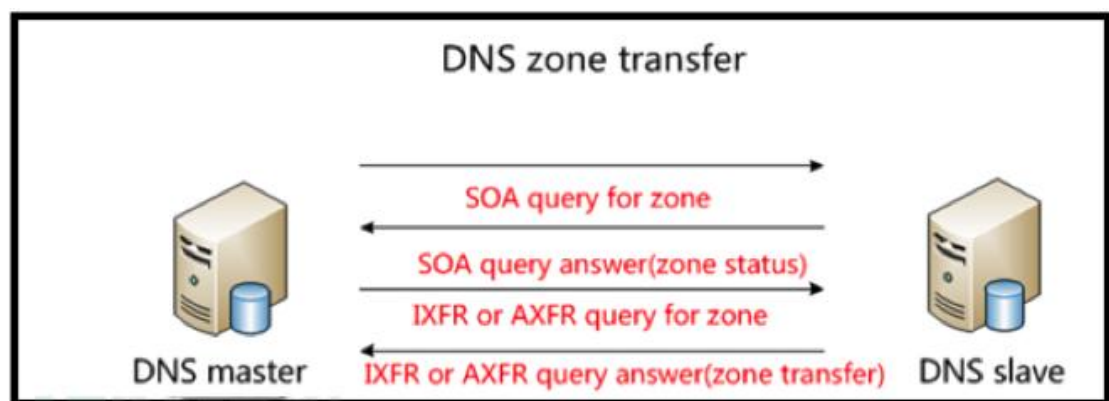
当前IP 218.75.123.181 所在地区为: 浙江省杭州市, 共有 87 个域名解析到该IP。

序号	域名	标题	PR	BR
1	www.hzlee.edu.cn	杭州电子科技大学信息工程学院	6	3
2	www.redunion.org	页面获取失败 『重试』	0	0
3	mail.jindui.com	连接网站失败! 『重试』	0	0
4	cs.hdu.edu.cn	首页 国家级实验教学示范中心电工电子实验中心	2	0

想要获得完整的信息，可以多尝试不同的工具，整合结果。很多工具无法做反向查询的原因，在于域名所有者没有添加反向解析记录。

7、关于 DNS 区域传送漏洞

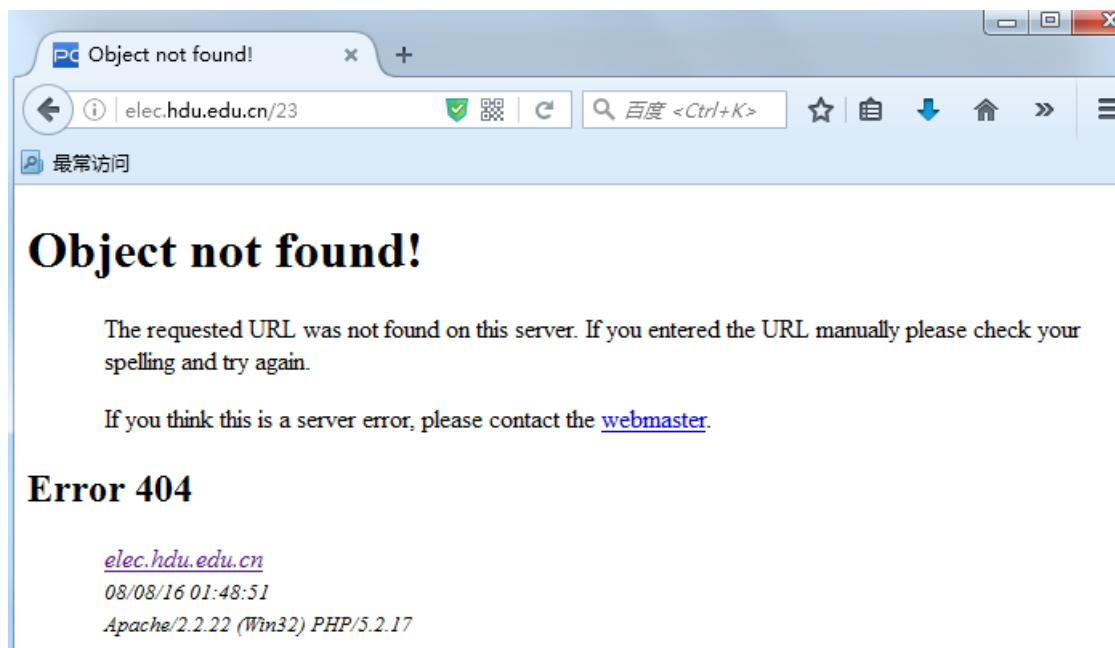
区域传送操作指的是一台后备服务器使用来自主服务器的数据刷新自己的 zone 数据库。一般来说，DNS 区域传送操作只在网络里真的有后备域名 DNS 服务器时才有必要执行，但许多 DNS 服务器却被错误地配置成只要有人发出请求，就会向对方提供一个 zone 数据库的拷贝。当一个单位没有使用公用/私用 DNS 机制来分割外部公用 DNS 信息和内部私用 DNS 信息的时候，此时内部主机名和 IP 地址都暴露给了攻击者。就像是把一个单位的内部网络完整蓝图或导航图奉送给了别人。



详细了解，[传送门](#)，感觉这位大神写的蛮清楚的，可以参考下

8、服务指纹识别

很多站点，可能没有自定义错误信息。因此在 url 上随便输入一个不存在的地址，可能会返回有用的信息。



通过上图，我们知道该站点的应用程序由 PHP 编写，Web 服务器为 Apache/2.2.22，操作系统为 Windows

9、通过端口判断服务

通过扫描服务器开放的端口判断服务器上存在的服务,nmap 具体使用在后面会讲到

```
root@kali:~# nmap -O www.hdu.edu.cn

Starting Nmap 7.12 ( https://nmap.org ) at 2016-07-18 04:55 EDT
Nmap scan report for www.hdu.edu.cn (218.75.123.182)
Host is up (0.011s latency).
Other addresses for www.hdu.edu.cn (not scanned): 218.75.123.181
Not shown: 993 closed ports
PORT      STATE      SERVICE
80/tcp    open      http
85/tcp    open      mit-ml-dev
135/tcp   filtered  msrpc
139/tcp   filtered  netbios-ssn
443/tcp   open      https
445/tcp   filtered  microsoft-ds
1433/tcp  filtered  ms-sql-s
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4.37
OS details: DD-WRT v24-sp2 (Linux 2.4.37)
```

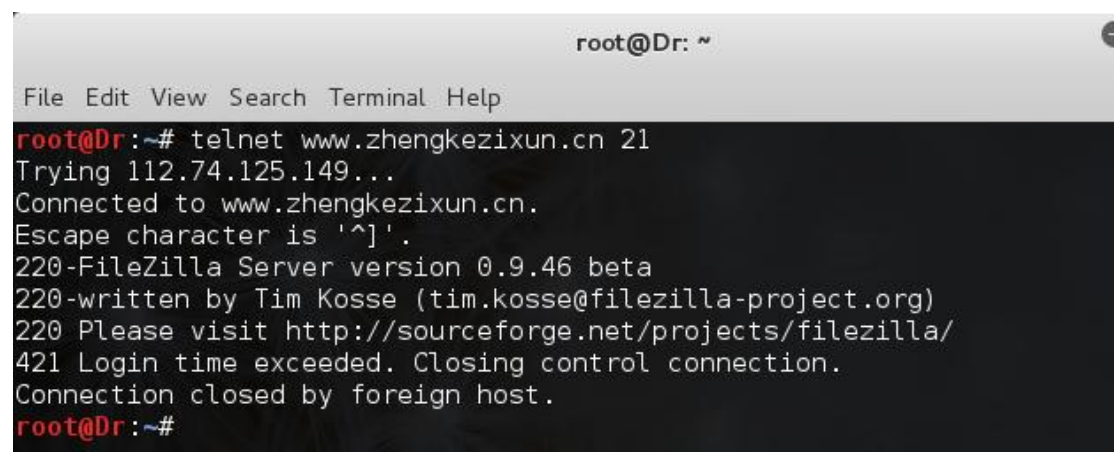

从图中可以看出该服务器搭建了 http(Web)、msrpc(文件共享)、MSSQL 数据库等

10、操作系统指纹识别

识别目标主机的操作系统，首先，可以帮助我们进一步探测操作系统级别的漏洞从而可以从这一级别进行渗透测试。其次，操作系统和建筑在本系统之上的应用一般是成套出现的，例如 LAMP 或者 LNMP。操作系统的版本也有助于我们准确定位服务程序或者软件的版本，比如一般情况下 windows server 2003 搭载的 IIS 为 6.0，windows server 2008 R2 搭载的是 IIS7.5。

Banner 抓取

banner 抓取是应用程序指纹识别而不是操作系统指纹识别。Banner 信息并不是操作系统本身的行为，是由应用程序自动返回的，比如 apache、exchange。而且很多时候并不会直接返回操作系统信息，幸运的话，可能会看到服务程序本身的版本信息，并以此进行推断。下图可以看出 ftp 服务器软件为 FileZilla 及版本等信息

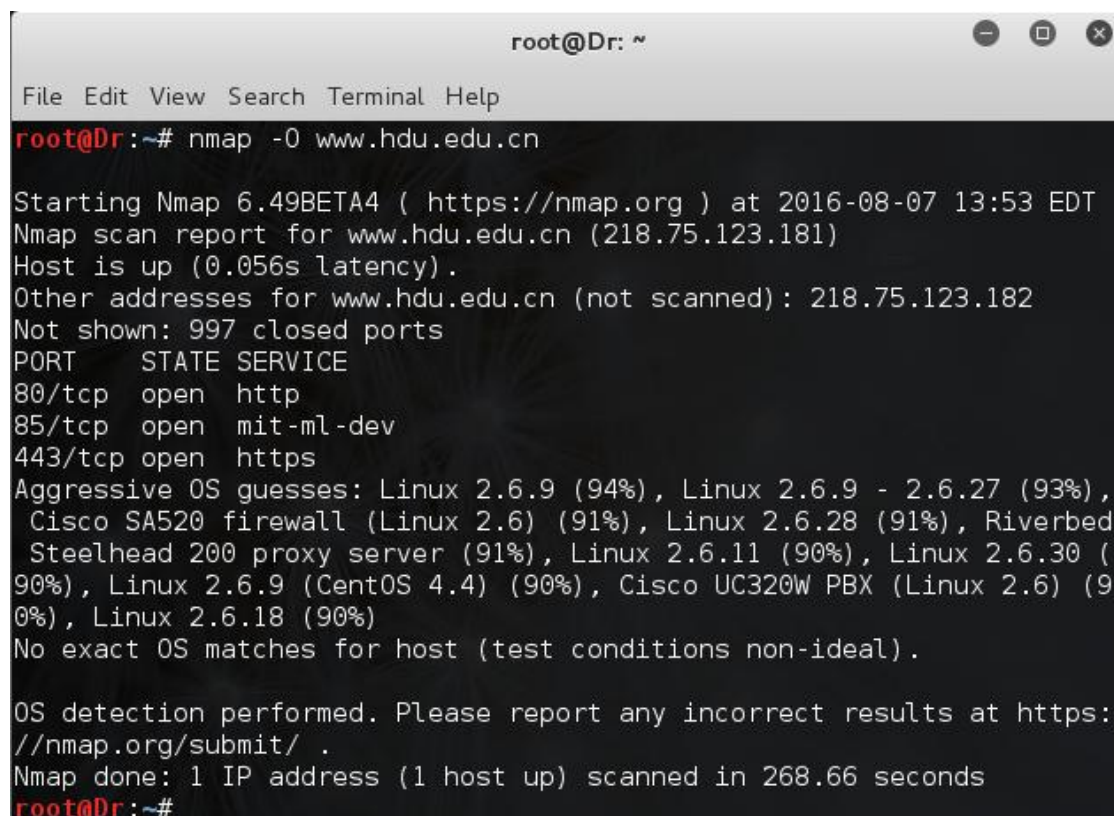


```
root@Dr: ~  
File Edit View Search Terminal Help  
root@Dr:~# telnet www.zhengkezixun.cn 21  
Trying 112.74.125.149...  
Connected to www.zhengkezixun.cn.  
Escape character is '^]'.  
220-FileZilla Server version 0.9.46 beta  
220-written by Tim Kosse (tim.kosse@filezilla-project.org)  
220 Please visit http://sourceforge.net/projects/filezilla/  
421 Login time exceeded. Closing control connection.  
Connection closed by foreign host.  
root@Dr:~#
```

使用 Nmap 进行操作系统探测

使用 Nmap 识别操作系统最简单的方法为使用-O 参数

格式 `nmap -O URI`,从图中可以看到服务器操作系统为 Linux



```
root@Dr: ~  
File Edit View Search Terminal Help  
root@Dr:~# nmap -O www.hdu.edu.cn  
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-08-07 13:53 EDT  
Nmap scan report for www.hdu.edu.cn (218.75.123.181)  
Host is up (0.056s latency).  
Other addresses for www.hdu.edu.cn (not scanned): 218.75.123.182  
Not shown: 997 closed ports  
PORT      STATE SERVICE  
80/tcp    open  http  
85/tcp    open  mit-ml-dev  
443/tcp   open  https  
Aggressive OS guesses: Linux 2.6.9 (94%), Linux 2.6.9 - 2.6.27 (93%),  
Cisco SA520 firewall (Linux 2.6) (91%), Linux 2.6.28 (91%), Riverbed  
Steelhead 200 proxy server (91%), Linux 2.6.11 (90%), Linux 2.6.30 (90%),  
Linux 2.6.9 (CentOS 4.4) (90%), Cisco UC320W PBX (Linux 2.6) (90%),  
Linux 2.6.18 (90%)  
No exact OS matches for host (test conditions non-ideal).  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 268.66 seconds  
root@Dr:~#
```

使用 p0f 进行操作系统探测

p0f 是一款被动探测工具，通过分析网络数据包来判断操作系统类型。同时 p0f 在网络分析方面功能强大，可以用它来分析 NAT、负载均衡、应用代理等。下面命令的含义为监听网卡 eth0，并开启混杂模式。这样会监听到每一个网络连接，部分结果摘录如下：`p0f -i eth0 -p`

```

.-[ 172.16.211.128/52452 -> 218.75.123.182/80 (http request) ]-
client  = 172.16.211.128/52452
app     = Firefox 10.x or newer
lang    = English
params  = none
raw sig  = 1:Host,User-Agent,Accept=[image/png,image/*;q=0.8,*/*;q=0.5],Accept-Language=[en-US,en;q=0.5],Accept-Encoding=[gzip, deflate],?Referer,?Cookie,Connection=[keep-alive]:Accept-Charset,Keep-Alive:Mozilla/5.0 (X11; Linux i686; rv:45.0) Gecko/20100101 Firefox/45.0

```

使用 Xprobe2 进行操作系统探测

Xprobe2 是一款使用 ICMP 消息进行操作系统探测的软件，探测结果可以和 Nmap 互为参照。但是该软件目前公开版本为 2005 年的版本，对老的操作系统探测结果较为准确。简单用法：xprobe2 -v URI (这个平时用用我基本也扫不出什么东西 233333)

```

root@Dr: ~
File Edit View Search Terminal Help
[+] Primary guess:
[+] Host 218.75.123.181 Running OS: "Linux Kernel 2.4.19" (Guess probability: 100%)
[+] Other guesses:
[+] Host 218.75.123.181 Running OS: "Linux Kernel 2.4.23" (Guess probability: 100%)
[+] Host 218.75.123.181 Running OS: "FreeBSD 5.2.1" (Guess probability: 100%)
[+] Host 218.75.123.181 Running OS: "Linux Kernel 2.4.29" (Guess probability: 100%)
[+] Host 218.75.123.181 Running OS: "Apple Mac OS X 10.2.2" (Guess probability: 100%)

```

抓取操作系统指纹的工具还有很多，如 miranda 等，不过多举例。

11、WAF 检测

WafW00f 是 Python 脚本，用于检测网络服务是否处于网络应用防火墙保护状态，极其有用。使用 WafW00f 检测网络服务器和网络传输之间是否存在网

络应用防火墙，这不仅可以发展测试战略，而且还能开发出绕过网络应用防火墙的高级技术。简单用法 wafw00f URL

```
File Edit View Search Terminal Help
root@Dr:~# wafw00f www.baidu.com

      ^          ^
    // // // . ' \ // // // // // // // // // // 
   | V V // o // // | V V // 0 // 0 // // // // // 
   |_n_, ' _n_// // |_n_, ' \ , ' \ , ' \ // // // 
                                <
                               ...'

WAFW00F - Web Application Firewall Detection Tool

By Sandro Gauci && Wendel G. Henrique

Checking http://www.baidu.com
Generic Detection results:
The site http://www.baidu.com seems to be behind a WAF
Reason: The server returned a different response code when a string t
rigged the blacklist.
Normal response code is "200", while the response code to an attack i
s "302"
Number of requests: 12
root@Dr:~# █
```

从图中可以看到该网站处于 Waf 保护状态

12、搜索引擎

Google 搜索技术融合了用于执行 Google 的详细搜索的高级搜索技术。在 Google 首页右下角可以点击 “Settings” -> “Advanced search” 进行详细设置

Advanced Search

Find pages with...

all these words:

this exact word or phrase:

any of these words:

none of these words:

在高级设置页面可以设置“所有字”、“精确的字或短语”、“含以下任何字”、“不含以下任何字”、“数字范围”、“语言”、“地区”、“最新更新”、“网站或域名”、“关键字出现位置”、“安全搜索”、“阅读级别”、“文件类型”、“使用权限”等等，更精确的搜索

Then narrow your results by...

language:

any language

region:

any region

last update:

anytime

site or domain:

terms appearing:

anywhere in the page

SafeSearch:

Show most relevant results

file type:

any format

usage rights:

not filtered by license

Advanced Search

由于一些众所周知的原因，我们在不能欢快滴科学上网的时候，会用到国内的一些搜索引擎。同样也是可以设置的，不过相对而言没 Google 强大。



[新闻](#) [网页](#) [音乐](#) [图片](#) [视频](#) [地图](#) [知识](#) [更多](#)

☐ 不拆分关键词

在指定站内搜索

搜索词位于

☒ 网页的任何地方 ☐ 仅在标题中 ☐ 仅在正文中 ☐ 仅在网址中

搜索结果排序方式

☒ 按相关性排序 ☐ 按时间排序

指定文件格式

☐ word(.doc) ☐ PDF(.pdf) ☐ PPT(.ppt)
☐ excel(.xls) ☐ RTF(.rtf) ☐ 全部文档 ☒ 全部网页

每页显示

10条结果

搜狗搜索

[返回首页](#) [个性设置](#)

渗透测试中还有一些非常好用的搜索引擎，比如

shodan(<https://www.shodan.io/>)

下面是搜索 sogou.com 的返回结果

Exploits

Maps

TOP COUNTRIES

Kenya
Hqals: 0

China	51
United States	2
Taiwan, Province of China	2
Japan	1

TOP SERVICES

Kerberos	33
HTTP	17
NAS Web interfaces	4
HTTPS	2

TOP ORGANIZATIONS

China Unicom Beijing	4
China Telecom Hunan	4
Hangzhou Alibaba Advertisin...	3
HiNet	2
China Telecom ningxia	2

Total results: 56

113.247.42.148

China Telecom Hunan

Added on 2016-07-18 09:36:05 GMT

China, Changsha

Details

HTTP/1.0 307 Temporary Redirect

Content-Length: 0

Content-Type: text/html

Date: Fri, 02 Jan 1970 09:14:09 GMT

Expires: Fri, 02 Jan 1970 09:14:09 GMT

Server: Mikrotik HttpProxy

Proxy-Connection: close

Location: <http://113.247.42.148/771084-2463>

error page

162.82.31.150

Allyun Computing Co., LTD

Added on 2016-07-17 22:08:47 GMT

China, Hangzhou

Details

HTTP/1.0 404 Not Found

Date: Sun, 17 Jul 2016 22:08:46 GMT

Content-Type: text/html

Content-Length: 121

Connection: keep-alive

Etag: "551e2fde-79"

Server: Apache

Set-Cookie: CXID=015EFBF243688499A1195283CE8FAA28; expires=Mon, 17-Jul-17 22:08:46 GMT; max-age=31536000; path=/;

点击第一个结果的 Details 可以查看详细信息，包括地理位置、服务器开放的端口等等

113.247.42.148

City	Changsha
Country	China
Organization	China Telecom Hunan
ISP	China Telecom Hunan
Last Update	2016-07-18T09:36:05.466558
ASN	AS4134

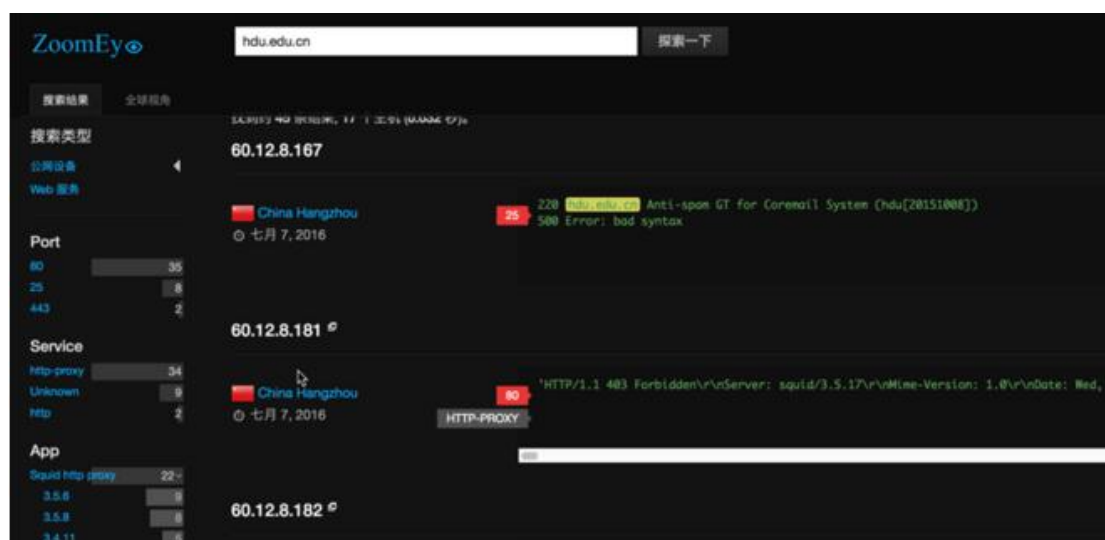
Ports

- 80

Services

- 80
tcp
http
- MikroTik http proxy**
HTTP/1.0 307 Temporary Redirect
Content-Length: 0

除了 shodan 之外，当然还不得不提知道创宇的“钟馗之眼” ->
ZoomEye 分分钟吊炸天有木有？



推荐余弦的[《ZoomEye 高级黑》](#)

13、Google hacking

对于普通的用户而言，Google 是一个强大的搜索引擎；而对于黑客而言，则可能是一款绝佳的黑客工具。正因为 google 的检索能力强大，黑客可以构造特殊的关键字语法，使用 Google 搜索互联网上的相关隐私信息。通过 Google，黑客甚至可以在几秒钟内黑掉一个网站。这种利用 Google 搜索相关信息并进行入侵的过程就叫做 Google Hack。下面介绍一些常用的所谓“谷歌黑客语法”。

例如批量查找学校网站的后台 输入如下关键字

site:hdu.edu.cn intext:管理|后台|登录|用户名|密码|验证码|系统|账号|后台管理|后台登录

欢迎登录

www.lib.hdu.edu.cn/DBList/GotoDB.aspx?dbid=cff97ee9-6e65... ▼ Translate this page

欢迎登录. 用户名: . 密码: . 手动下载图形控件. 教育部·国家知识产权局·教育部科技发展中心·知识产权出版社·中国教育和科研计算机网·中国教育在线. 主办: 教育 ...

主编登录 - 杭州电子科技大学学报

journal.hdu.edu.cn/JournalX/editorInChiefLogOn.action?mag_id... ▼ Translate this page

您的初始账号由编辑部设置, 会写在您邮件中。2. 登录后您可以修改您的账号信息。3. 本系统的用户名密码是大小写敏感的。请使用IE6. ... 请在下面输入邮件中标明的用户名和密码, 登录本刊审稿系统。用户名: . 密码: . 验证码: 验证码(均为数字) ...

登录-信息管理后台

foreignedu.hdu.edu.cn/ht ▼ Translate this page

登录. 管理员账号. 管理员密码. 忘记密码请联系管理员: 13675888422. 登录.

intext: 把网页中的正文内容中的某个字符做为搜索条件.

例如在 google 里输入:intext:杭电.将返回所有在网页正文部分包含“杭电”的网页

allintext:使用方法和 intext 类似.

intitle: 搜索网页标题中是否有我们所要找的字符.

例如搜索:intitle:杭电.将返回所有网页标题中包含“杭电”的网页.同理
allintitle:也同 intitle 类似.

cache: 搜索 google 里关于某些内容的缓存,有时候往往能找到一些好东西.

define: 搜索某个词的定义,例如搜索:define:杭电,将返回关于“杭电”的定义.

filetype: 搜索制定类型的文件，例如：filetype:doc.将返回所有以 doc 结尾的文件 URL.

info: 查找指定站点的一些基本信息.

inurl: 搜索我们指定的字符是否存在于 URL 中.

例如输入:inurl:admin,将返回 N 个类似于这样的连接:<http://xxx/admin>,

常用于查找通用漏洞、注入点、管理员登录的 URL

allinurl:也同 inurl 类似,可指定多个字符.

linkurl: 例如搜索:inurl:hdu.edu.cn 可以返回所有和 hdu.edu.cn 做了链接的 URL.

site: 搜索指定域名,如 site:hdu.edu.cn.将返回所有和 hdu.edu.cn 有关的 URL.

还有一些*作符

+ 把 google 可能忽略的字列如查询范围

- 把某个字忽略

~ 同意词

. 单一的通配符

* 通配符，可代表多个字母

"" 精确查询

实际操作时需根据情况组合使用，下面列举些常用的：

intext:to parent directory

inurl:upload.php

intitle:powered by xxx

index of/upload

Filetype:txt

inurl:robots.txt

index of /passwd

site:xxx.com filetype:mdb|ini|php|asp|jsp

....

14、社交网站

社交网站往往是我们公开信息最多的地方，比如我们常用的 QQ、QQ 空间、微信朋友圈、微博等。能获取到的信息可能有姓名、年龄、生日、星座、爱好、照片、人际交往关系、甚至邮箱、手机、住址、身份证等等隐私、敏感信息。还

有一些招聘求职网站也往往是信息泄露最严重的地方。对这些信息加以利用，总能得到一些惊喜。

比如看上一个妹子，看她空间很朋友圈，基本上都能知道她的生活规律就能摸的很清楚，她长什么样，喜欢什么，闺蜜有哪些、平时去哪里玩，有时候还能推算出此时此刻她正在做什么。朋友圈那种输入名字算各种的，大部分妹子都会输入自己的名字生日等。。

既然有看上的妹子，那就花半天时间了解了解妹子。。



辅之一些必要社工手段，

个人编号	██████	卡号	██████
帐号	██████	身份	本专科生
姓名	██████	性别	女
部门	██████	状态	有效卡
证件类型		证件号码	
有效期	██████	卡片类型	M1
修改			

照片
饭卡 学号
班级
....

██████	M1	商务收费	第五餐厅-总公司	智能控制器 (下沙3站)	11	-5.60	2016-03-22 12:12	1号线包	1
██████	M1	商务收费	仙鹤校园饮食	智能控制器 (下沙2站)	38	-12.50	2016-03-22 18:56	1号线包	1
██████	M1	商务收费	第五餐厅-总公司	智能控制器 (下沙3站)	11	-1.50	2016-03-23 09:21	1号线包	1
██████	M1	商务收费	第三餐厅-总公司	智能控制器 (下沙2站)	21	-4.80	2016-03-23 12:45	1号线包	1
██████	M1	商务收费	第五餐厅-总公司	智能控制器 (下沙3站)	4	-4.30	2016-03-23 17:35	1号线包	1
██████	M1	商务收费	第五餐厅-总公司	智能控制器 (下沙3站)	5	-1.50	2016-03-24 08:06	1号线包	1

消费记录->
平时基本都去三
餐和三餐吃饭

最后，最后一不小心就得到：

学号：[REDACTED]
姓名：[REDACTED]
性别：女
单位：[REDACTED]
身份：本科生
身份证号：43012119921210129
出生时间：[REDACTED]
发证地点：[REDACTED]县

id [REDACTED]
pwd [REDACTED]
手机：15737177020
固定电话 [REDACTED]

[REDACTED]，女，计算机专业，学号 [REDACTED] 3,qq
2015 —2016学年 第一学期 优秀学生奖学金获奖名单公示，[REDACTED]，[REDACTED] 等奖学金
高中毕业 [REDACTED] 学(中考准考证号 [REDACTED]，该中学定向生)
2015 —2016学年 第一学期单项奖学金社会实践奖

推荐一本书《欺骗的艺术》，在渗透实战中，我们可以通过社会工程学的手段获取管理员的信息，比如 QQ 号、邮箱、常用密码等等。比如可以想办法登录某网站域名注册的平台，直接修改域名解析（亲身经历），可能能达到瘫痪整个网络服务的效果...

Maltego 社工神器:Maltego 是用来对来自互联网的信息进行收集、组织、可视化的工具。它可以收集某个人的在线数据信息 一包括电子邮件地址、博客、Facebook 中的朋友 ,个人爱好、地理位置、工作描述 ,然后可以一种更为有用、全面的形式展现出来。



不过这个对国外的效果可能会好一点吧

15、第三方未公开数据

“社工库”是运用社会工程学进行攻击的时候积累的各方面数据的结构化数据库。这个数据库里有大量信息，甚至可以找到每个人的各种行为记录，比如酒店开房记录、个人身份证、姓名和电话号码。

例如查询某 QQ 号老密码。findmima.com(要爬墙)

精确匹配: User and Email

试试吧!

为了遵守国家道德法规，查询结果关键字段，已经用星号隐藏，敬请放心，本站不会记录和传播你的任何信息；

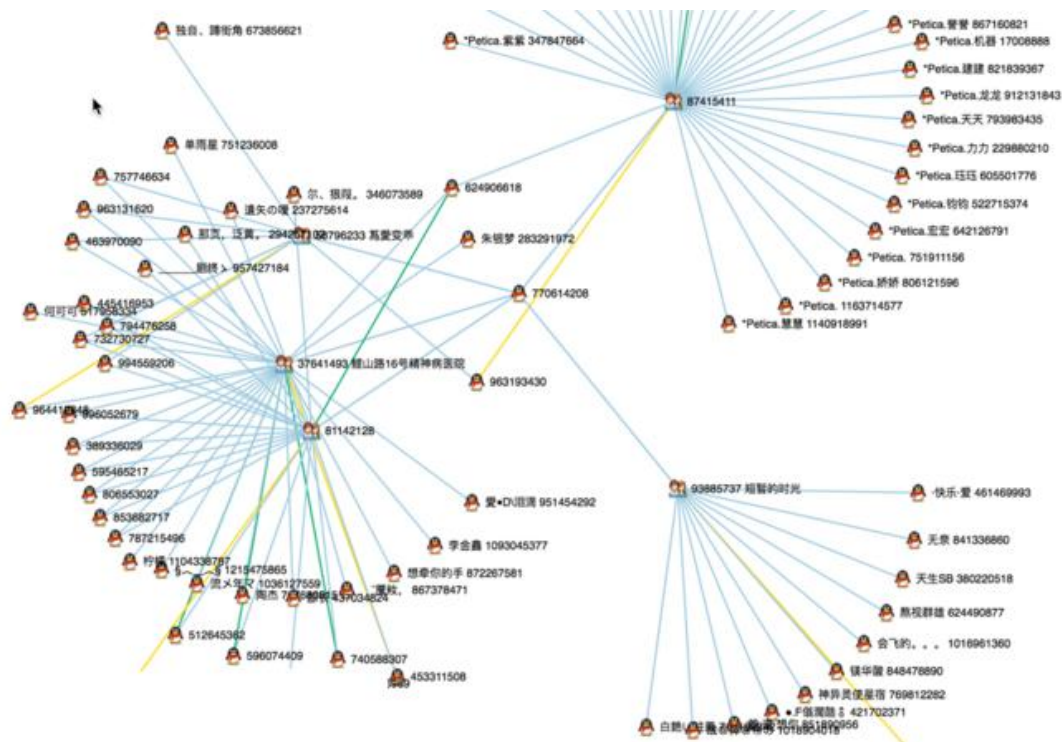
所有数据由华西安全网整理，并提供免费查询服务，数据约4.7亿，主要为多年前泄露的老密码，源自几年前已公开的搜云社工库，且不会涉及身份证等隐私信息；

本站十多年信誉保证，不做任何违法黑产谋利，不窃取任何信息，数据来自互联网，旨在找回遗忘密码，或对已泄露密码进行修改防范，请勿非法使用，否则一切后果自负。

查询完毕 数据量:1条 耗时:2604毫秒

用户名/账号	邮箱	密码/密文	来源
		zha****hen	qq_old_password

某 QQ 号的群关系



某社工库网站可查询以下数据，

名称	条数	备注
qun	1,410,000,000	14.1亿企鹅群关系
qq	153,953,672	企鹅老密，无IP
qq	91,605,619	企鹅老密，带IP（部分重复）
tianya	29,233,001	天涯社区
24buy	22,219,977	成都时时购
gfan	21,258,536	机锋Android手机交流网
ipart	19,318,000	iPart-爱情公寓
开房记录	19,238,496	传说中的2000W
unknown	18,935,844	一堆乱七八糟汇总的
hiapk	17,130,246	hiapk安卓版网
000web	15,047,799	000webhost.com著名免费空间
52pk1	14,001,237	52pk游戏网
houdao	12,885,277	猴岛游戏论坛

通过这些数据库可能可以查到 QQ 密码、邮箱密码等信息，这样在有些时候能帮助猜解管理员相关的信息。第一部分就先写到这里了，后面还会带来新的内容，敬请关注。