

Author:bugcx or Anonymous

Url:

<http://blog.bug.cx/2012/04/25/%e5%b0%8f%e8%ae%b0%e4%b8%80%e6%ac%a1%e6%b8%97%e9%80%8f%e8%bf%>

(扫一扫) | bugcx's blog | 关注网络安全

域**服务器**的作用

1. 安全集中管理 统一**安全策略**
2. 软件集中管理 按照公司要求限定所有机器只能运行必需的办公软件。
3. 环境集中管理 利用AD可以统一客户端桌面,IE,TCP/IP等设置
4. 活动目录是企业基础架构的根本，为公司整体统一管理做基础 其它isa,exchange,防病毒**服务器**，补丁分发**服务器**，文件服务器等服务依赖于域服务器。

域控制器（Domain Controller，简写为DC）”

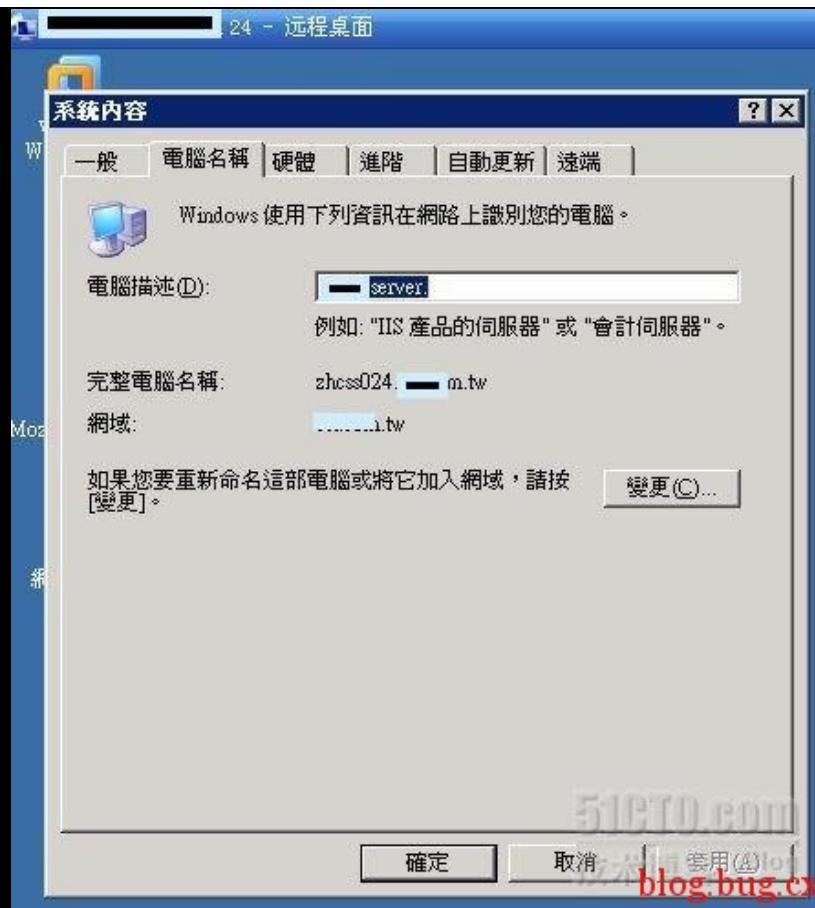
过程如下：

2天前对一台WIN2003主机做ORACLE**安全**测试，然后装了3389登陆记录软件。

然后昨天登陆看看此机的数据库设置情况时发现此机其实是DC下属的一台工作站



远程桌面登陆后查看电脑名称获得DC域名。



以前读MCSE时曾经学过如何安装和设置DC，现在知识基本都还给老师了，呵呵~~  
此机的权限在做安全测试时已经获得，但获得的用户和口令只能在本机登陆，是不能登陆DC服务器。  
于是就做了下渗透测试，看能否获得DC的最高权限，“域控管理员”。  
渗透前都要搜集信息，才好决定下一步如何进行，CMD下运行NET USER、NET LOGRUP、NET VIEW看有否当前域或工作组中计算机的列表。

```
c:\命令提示字元  
2005/03/24 下午 04:57          42,496 net.exe  
      1 個檔案          42,496 位元組  
  
C:\WINDOWS\SoftwareDistribution\Download\dbb7944a4522201d669af197ebf32816 的目  
錄  
  
2007/02/17 下午 10:35          42,496 net.exe  
      1 個檔案          42,496 位元組  
  
C:\WINDOWS\system32 的目錄  
  
2005/03/24 下午 04:57          42,496 net.exe  
      1 個檔案          42,496 位元組  
  
檔案數目總計：  
    4 個檔案          168,448 位元組  
    0 個目錄  17,082,528,768 位元組可用  
  
C:\WINDOWS>net user  
系統無法執行指定的程式。  
  
C:\WINDOWS>net1 user  
系統無法執行指定的程式。  
C:\WINDOWS>
```

c:\ 命令提示字元  
2007/02/17 下午 10:35 42,496 net.exe  
1 個檔案 42,496 位元組  
C:\WINDOWS\system32 的目錄  
2005/03/24 下午 04:57 42,496 net.exe  
1 個檔案 42,496 位元組  
檔案數目總計：  
4 個檔案 168,448 位元組  
0 個目錄 17,082,528,768 位元組可用  
C:\WINDOWS>net user  
系統無法執行指定的程式。  
C:\WINDOWS>net1 user  
系統無法執行指定的程式。  
C:\WINDOWS>net group  
系統無法執行指定的程式。  
C:\WINDOWS>net group /domain  
系統無法執行指定的程式。  
C:\WINDOWS>

51CTO.com  
技术博客 Blog  
blog.bug.cx

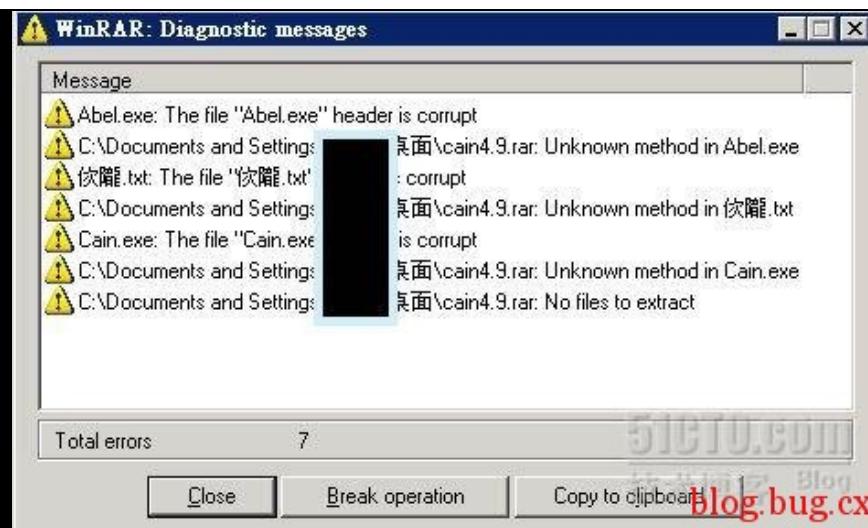
图显示，管理员居然做了“活动目录策略--组策略--软件限制策略”

NET和NET1都被限制了权限。既然做了限制策略，那很多常用的方法应该都行不通了，理了下思路，首先要弄清楚DC服务器的IP地址才行，连DC的地址都不知道，咋弄？但NET VIEW被限制了，怎么才能查看到？翻资料，想办法，找到个VBS的，也失败了。



那嗅探行不？传了cain上去，被可爱的MCAFEE杀掉了。。。关掉MACFEE也不行。我还以为文件损坏，但同一文件在我电脑里正常解压和运行。这是什么原因？

知道的大牛希望教我一下。



思考。。。在CMD里输入指令，发现netstat能用，ipconfig也能用，显示了网卡信息，这个命令没做限制，

```
命令提示字元
Windows IP Configuration

Ethernet adapter VMware Network Adapter VMnet8:
  Connection-specific DNS Suffix . :
  IP Address . . . . . : 192.168.14.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

Ethernet adapter VMware Network Adapter VMnet1:
  Connection-specific DNS Suffix . :
  IP Address . . . . . : 192.168.195.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

Ethernet adapter [區域連線]:
  Connection-specific DNS Suffix . :
  IP Address . . . . . : 10.10.1.24
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :
```

接着加参数 /all 查看详细。获知DNS是：10.10.1.1和10.10.1.2 网关是：10.10.1.252，接着再试nslookup反向查询10.10.1.2，这命令也没做限制，得知是同一域内的O2号机。

```
C:\命令提示字元
Ethernet adapter 區域連線:

Connection-specific DNS Suffix . . . . . : 
Description . . . . . : HP NC373i Multifunction Gigabit Server Adapter
Physical Address . . . . . : 00-19-BB-CE-B9-68
DHCP Enabled. . . . . : No
IP Address . . . . . : 10.10.1.24
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.10.1.252
DNS Servers . . . . . : 10.10.1.2
                           10.10.1.1
Primary WINS Server . . . . . : 10.10.0.1
Secondary WINS Server . . . . . : 10.10.1.8

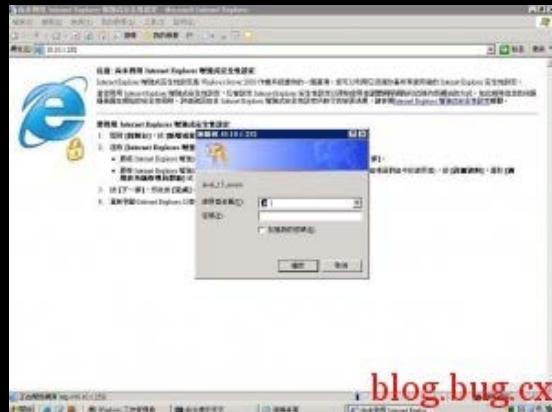
C:\WINDOWS>nslookup 10.10.1.2
Server: [REDACTED].tw
Address: 10.10.1.2

Name: [REDACTED].tw
Address: 10.10.1.2

C:\WINDOWS>
```

51CTO.com  
技术博客 blog.bug.cx

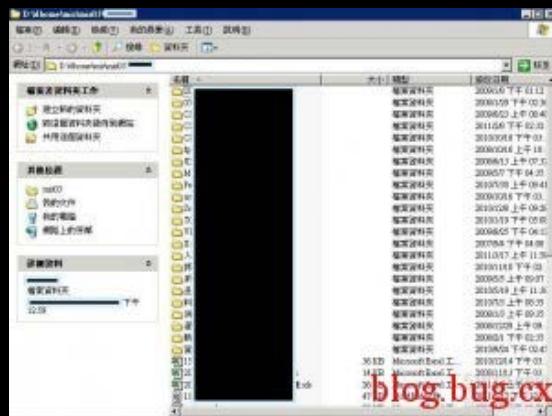
用IE打开网关IP，看提示15级权限应该是CISCO了。先不管它。



blog.bug.cx

那IP: 10.10.1.1应该就是DC

用已获得的用户名和口令登陆失败，看来此帐号没加入到 DOMAIN USER，只好在本机查看硬盘里有什么可以利用的？



blog.bug.cx

翻遍了都是些资料，驱动，应用软件等等。找不着头绪。。。很多命令被限制，嗅探也被杀，传说gsecdump可以抓DC的HASH，但我想这应该也会被

MACFELL杀掉，所以就不尝试了。由于才疏学浅，还真想不到其他方法了。

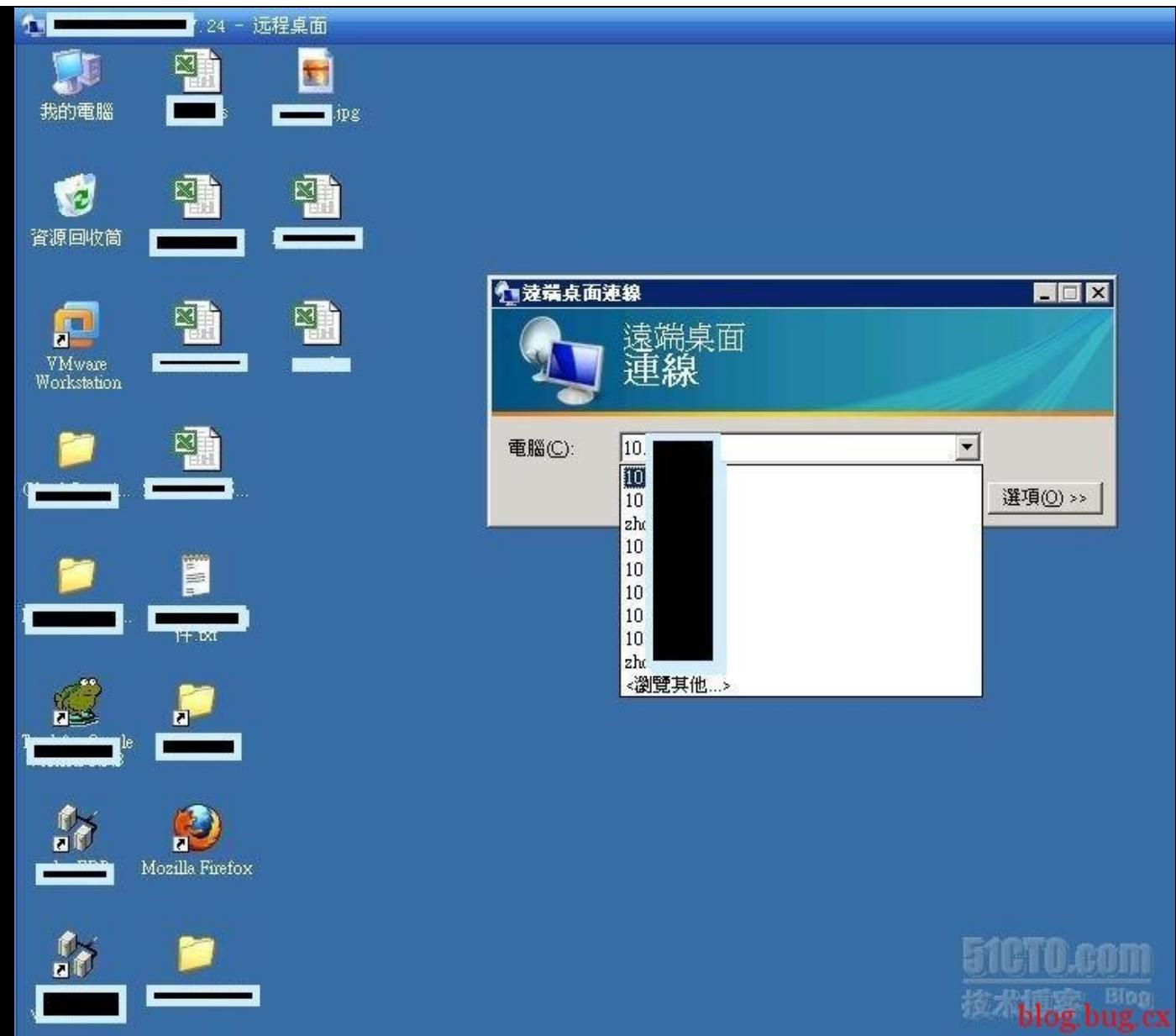
退出远程桌面，洗澡去。边洗边想，猛然想起昨天安了3389登陆记录。洗完出来赶紧查看记录，显示本机系统管理员登陆过，还有1个用户用这台机登陆，

而且登陆的DOMAIN不同。

```
Time:2011 [REDACTED]
IP: [REDACTED]
TSPort:3389↓
Domain:ZHCSS024↓
UserName:Administrator↓
Password: [REDACTED]
=====
↓
↓
↓
=====
Time:2011 [REDACTED]
IP: [REDACTED]
TSPort:3389↓
Domain:ZHCS↓
UserName: [REDACTED]
Password: [REDACTED]
```

51CTO.COM  
技术博客 Blog  
[blog.bug.cx](http://blog.bug.cx)

于是用这用户登陆本机，看有否新的信息可利用，桌面的[远程](#)桌面有很多连接记录，看来这用户不是普通权限啊。



好，抱着试一下的心情，登陆刚才查到的DNS地址10.10.1.2 结果真是踏遍铁鞋弄不到，天涯何处无芳草得来全不费功夫。。。 (什么文采啊？)



然后在用NET VIEW指令，这下没有限制了。

命令提示字元

C:\>Documents and Settings\<redacted>>net view  
伺服器名稱 說明

\\NC400  
\\NC492  
\\NC500  
\\NC508  
\\NC528  
\\NC542  
\\NC641  
\\NC647  
\\NC665  
\\NC670 [redacted] 系統  
\\NC751  
\\NC816  
\\NC823  
\\NC844  
\\NC899  
\\NC911  
\\NC970  
\\NC971  
\\NC972  
\\NC989  
\\<redacted>B4CB2605614  
\\<redacted>22  
\\D017  
\\D019  
\\D053  
\\D087  
\\D091  
\\D718  
\\<redacted>USER  
\\NIPC11  
\\NIPC13  
\\NIPC14  
\\NIPC20  
\\NOAPP1

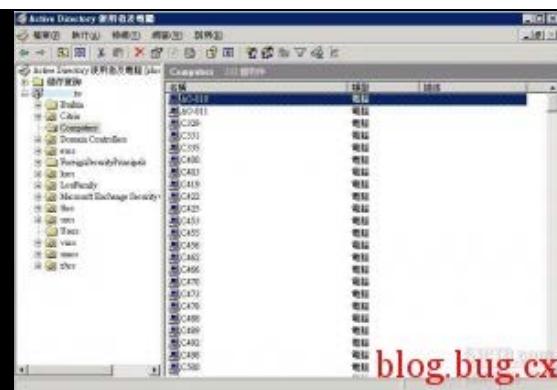
51CTO.com  
技术博客 Blog  
blog.bug.cx

NET USER查看用户，有几百个用户。



blog.bug.cx

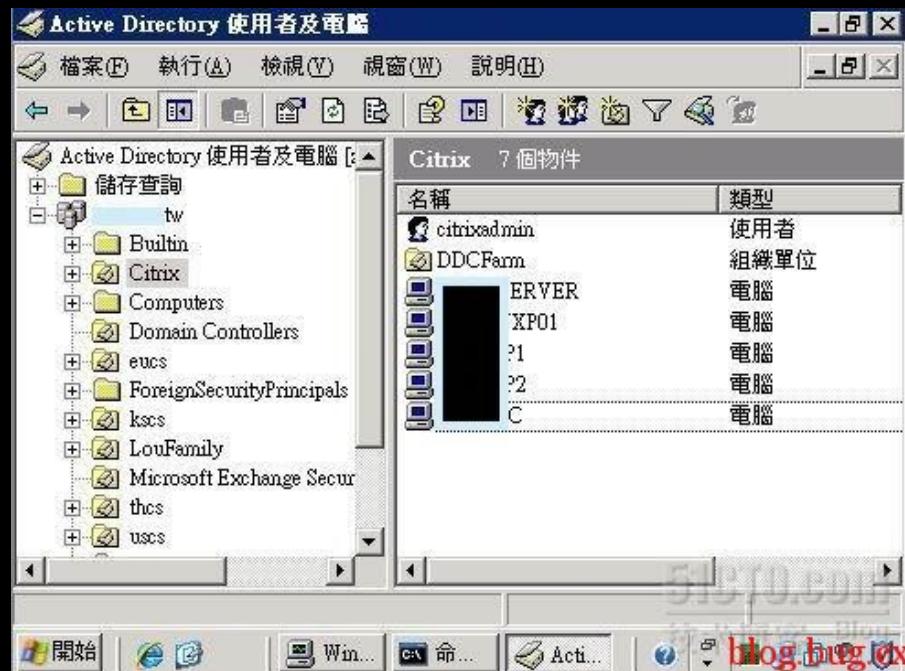
那么多用户，这内网有多少台机呢？接着用AD查,COMPUTERS 300+台主机



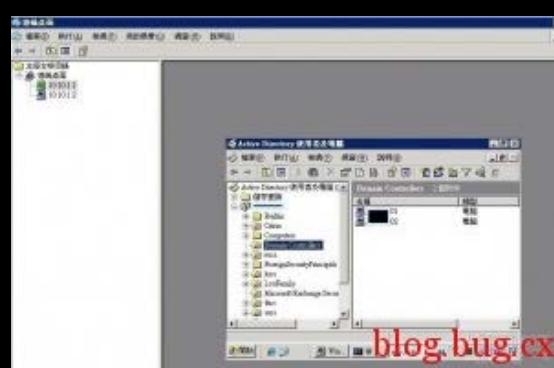
这内网，还用到思杰服务器虚拟化：

思杰官方：

<http://www.citrix.com.cn/products/server-virtualization.aspx>



有2台控制器分别就是：10.10.1.1和10.10.1.2



该企业在美国、日本、英国、泰国都有分公司，做橡胶产品的。由于域名被天朝屏蔽，输入IP就可以查看网页。

小结：

因为嗅探软件发挥不了作用，所以3389记录起到了关键的作用，这是一次没什么技术含量的渗透测试过程。让各位大牛见笑了。测试完毕后，帮管理员把ORACLE漏洞修复。其他一切操作恢复原样。

时间不早了，就写到这。

最新文章

相关文章

热评文章

Waiting

Waiting

[webhook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)