
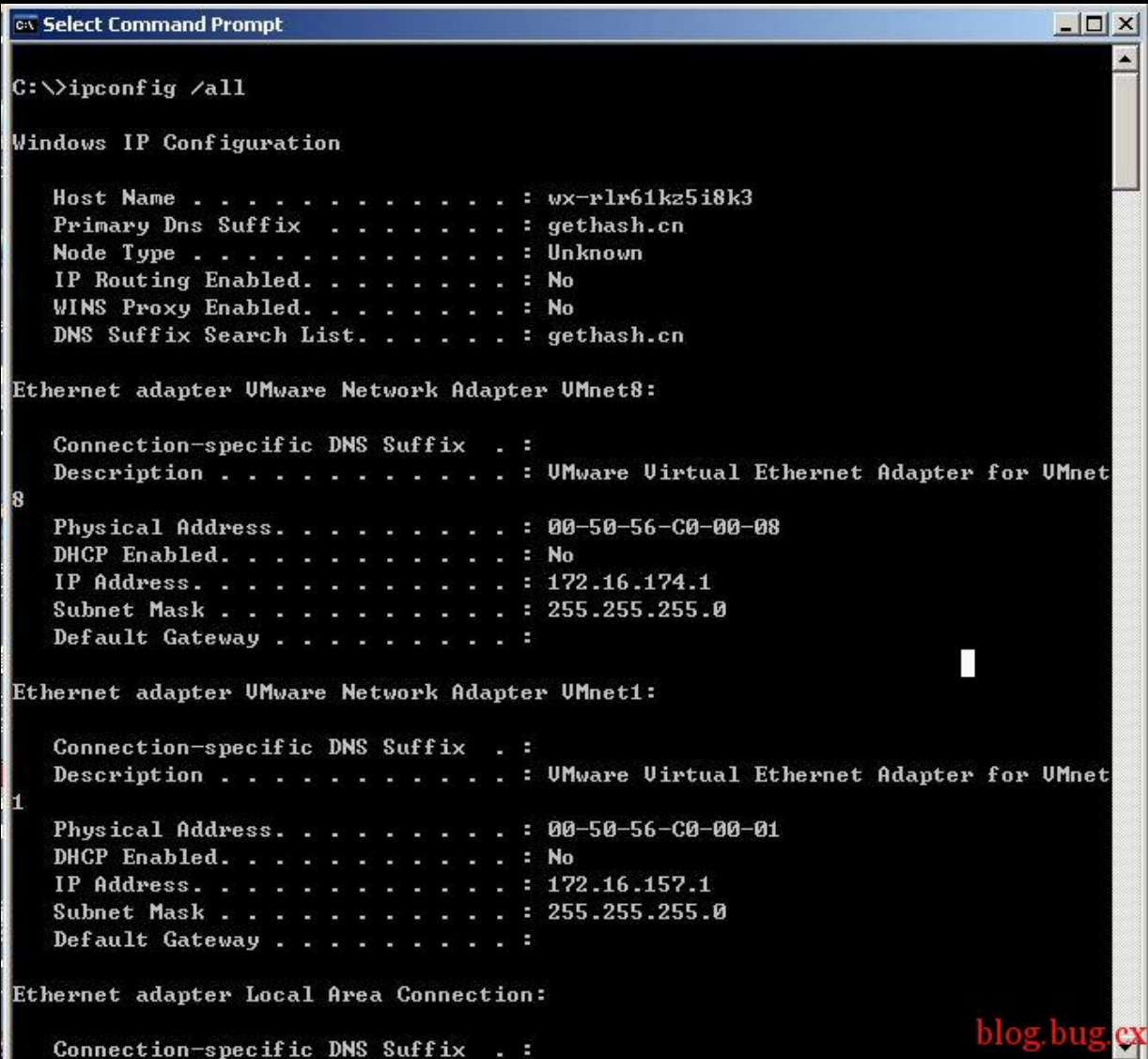


Author:bugcx or Anonymous
 Url:
 http://blog.bug.cx/2012/04/25/%e5%9f%9f%e5%86%85%e7%bd%91%e4%b8%ad%e7%9a%84%e4%bf%a1%e6%81%
 (撸一撸) | bugcx's blog | 关注网络安全

作者: **lcx**

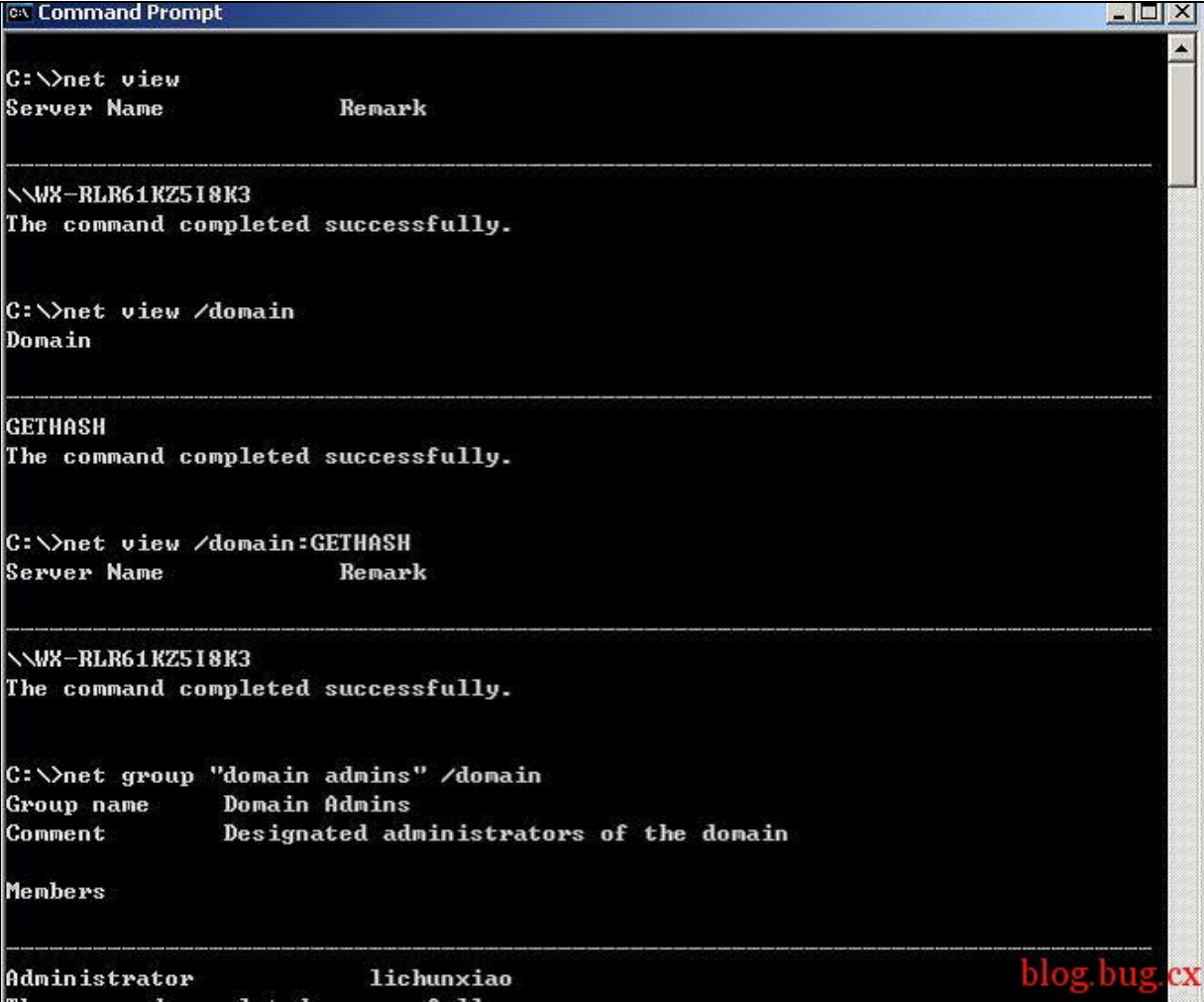
这期的专栏是我设定的题目,看够了**注入**,是不是想了解一下**内网**的**入侵**手法呢?做为出题人,自然要写一篇了。在各式各样大小不同的**内网**中,最常见的就是域内网了。其实域**内网**的**入侵**和我们平常的入侵手法在总体上来讲的逻辑也是一样,也是信息的收集、分析,找出薄弱点,然后击破,再综合归纳整理,最终拿到域管理员的密码,算是大功告成。有了内网的第一台机器的**权限**后,如何收集信息,这是很关键的一步,这篇文章讲的就是域内网信息的收集的第一步。



从图1中我们可以看到子网掩码、本机IP、网关和dns服务器是多少。你可以用这些数据结合Advanced IP Address Calculator这个工具来在脑子里画出一个大体结构，看看有几个子网呀，每个子网可能有多大等等，我认为不重要，略过。多数内网当中，很有可能DNS服务器也就是其中的一台域服务器。另一个重要的命令就是net命令了，net view是可以看到本机所在的域约有多少台机器，net view /domain，可以看到有几个域，"net view /domain: 域名" 是看每个域中有多少台机器，net group "domain admins" /domain，是可以看到域管理员的名字，运气好的情况下是直接可以看到域服务器是哪一台，如图2所示。net group是看看把用户分了多少个组。在英文机器中，我们要看域管理员密码用的是

```
net group "domain admins" /domain
```

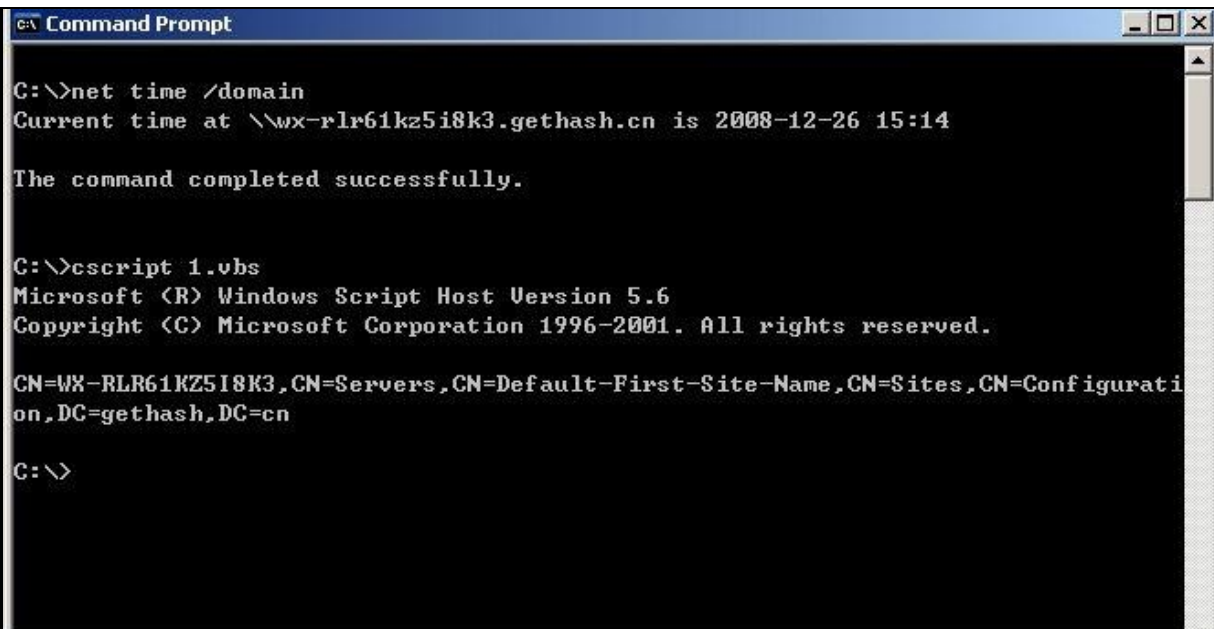
在非英文英器上你可能要把domain admins这个名字来换一下了，就要先用net group来看看哪一个可能是域管理员的组。



以上关键探测的步骤是探测出域管理员的名字和域服务器的名字。探测域服务器是哪一台还有另几个办法，除了dns的名字和net group "domain admins" /domain这个命令外，另一个办法是net time /domain，因为域服务器一般也做时间服务器。不过除了用系统命令外，结合工具也是不错的办法。微软对域提供了专门的adsi（Active Directory）活动目录服务模型，其中在域用到的就是ADSI的接口之一LDAP提供者，用来管理域的。我们可以写一个很简短的vbs程序来探测出域服务器是哪一台，1.vbs代码如下：

```
★
set obj=GetObject("LDAP://rootDSE")
wscript.echo obj.servername
```

★
运行后的结果如图3所示。



blog.bug.cx

收集的到这些信息够了吗？当然不足够，所以我们还要继续收集。<http://www.rlmuellet.net>这个网站是有很多专门针对域的vbs，我精选挑选了两个，还做了一下改动，让它更适应我们的入侵。第一个是DocumentProperties.vbs，代码太长我就不列了，直接来看运行示例。第一个是cscript DocumentProperties.vbs LDAP://dc=gethash,dc=cn，你会得太多的信息了，在图4、图5中我没有办法截全图，大家运行一下就清楚了。大家可能会想我为什么用LDAP://dc=gethash,dc=cn这个，这串从哪来的，其实就是在图3中我写的那两句小代码1.vbs来得到的。当然你也可以具体到看具体用户像LDAP://cn=TestUser,ou=Sales,dc=MyDomain,dc=com这样的一串，表示在MyDomain这个域中里边的Sales部门里的TestUser用户是什么样的具体信息。



我们再用DocumentProperties.vbs来举两例，用它也直接可以探测本机信息的。第一个是cscript DocumentProperties.vbs WinNT://./administrator，查看本机administrator的信息，看一下密码长度呀，多久过期等。如果你看到可能一两天就要过期了，表示它肯定要来修改密码了，这时你就想到要丢一下记录密码的东东上去了。再来一个是cscript DocumentProperties.vbs WinNT://./Themes,service，来查看Themes服务的相关信息，可以看到路径、启动方式，和帐号的启动方式等。分别示例如图6、图7。

```
C:\>cscript DocumentProperties.vbs
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

Error, required argument missing.
DocumentProperties.vbs
Program to list AD object properties
Syntax:
cscript DocumentProperties.vbs ADSPATH > output.txt
where ADSPATH is the full AdsPath of an AD object.
For example, ADSPATH could be:
WinNT://MyDomain/TestUser,user
LDAP://cn=TestUser,ou=Sales,dc=MyDomain,dc=com

C:\>cscript DocumentProperties.vbs WinNT://./administrator
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

<O> Description = Built-in account for administering the
<O> FullName =
<O> AccountExpirationDate =
<O> BadPasswordAttempts = 0
<O> HomeDirDrive =
<O> HomeDirectory =
<O> LastLogin = 2008-12-26 14:31:45
<O> LastLogoff =
<O> LoginHours = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
<O> LoginScript =
<O> LoginWorkstations =
<O> MaxLogins =
<O> MaxPasswordAge = 3710851
<O> MaxStorage = -1
<O> MinPasswordAge = 86400
<O> MinPasswordLength = 7
<O> objectSid = 0105000000000000515000000878CAAA066F94B
<O> Parameters =
<O> PasswordAge = 1551774
<O> PasswordExpired = 0
```

blog.bug.cx

```
C:\>cscript DocumentProperties.vbs WinNT://./Themes.service
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

<M> StartType = 4
<M> ServiceType = 32
<M> DisplayName = Themes
<M> Path = C:\WINDOWS\System32\svchost.exe -k net
<M> ErrorControl = 1
<O> HostComputer = WinNT://gethash.cn/.
<O> LoadOrderGroup = UIGroup
<O> ServiceAccountName = LocalSystem
<O> Dependencies =
<O> Name = Themes

C:\>
```

blog.bug.cx

这个DocumentProperties.vbs最大的好处是不需要太多的权限，普通域用户的权限就够了。还有一个vbs是Inventory2.vbs，这个我在内网中试过，好像需要域管理员权限。不过这个脚本虽然权限需要高一低，但是也有好处，直接运行就可以，不像上一个DocumentProperties.vbs需要你域知识有相关一些概念。由于这个脚本它原来的要调用excel组件，而且还会弹出ie对话框，我花了一点时间修改了一下，可以直接保存成html了，无声无息且方便用于入侵,也不需要提供什么excel组件了，系统默认都支持的。由于在程序中我用的是数组pc(65535,10)，如果内网过大(>65535?,呵呵)请小心使用。直接运行后，它的结果如图8所示，它会列出域中每一台机器的系统版本、充当什么重要角色，打的补丁号等等。



说实话，我虽然对域内网有过入侵经验，但毕竟没有亲自组过域内网，很多专业名词我也没有去查专业字典，只是凭自己理解写出来，所以写起来如果有不严谨的地方，希望读者指出，我们下一期再继续内网入侵之旅。

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 \(最全面的iftop教程\)](#)