内网学习基础

要点

- SAM
- Hash
- Active Directory
- Kerberos
- SMB
- IPC
- NetBIOS
- LLMNR
- WMI
- Windows网络认证
- Windows本地认证流程
- 内网渗透流程
- 内网渗透常用工具

SAM

SAM(安全账户管理器)，SAM是用来存储Windows操作系统密码的数据库文件，为了避免明文密码泄漏，SAM文件中保存的是明文密码经过一系列算法处理过的Hash值，被保存的Hash分为LM Hash、NTLMHash。在用户在本地或远程登陆系统时，会将Hash值与SAM文件中保存的Hash值进行对比。在后期的Windows系统中，SAM文件中被保存的密码Hash都被密钥SYSKEY加密。
SAM文件在磁盘中的位置在C:\windows\system32\config\sam SAM文件在Windows系统启动后被系统锁定，无法进行移动和复制

Hash

Windows系统为了保证用户明文密码不会被泄漏，将明文密码转换为Hash值进行身份验证，被保存在SAM或ntds.dit中。

Hash背景

1.LM Hash，在早期的Windows操作系统中将明文密码转换为LM Hash保存在SAM文件中，因为LM Hash使用DES加密，密钥为硬编码，算法又存在缺陷，所以被废弃，为了保证系统兼容性可以自行开启。
2.NTLM Hash，在LM Hash算法被弃用时，NTLM Hash被用来进行Windows本地及远程身份验证的凭据，长度为32bit、由数字和字母组成。

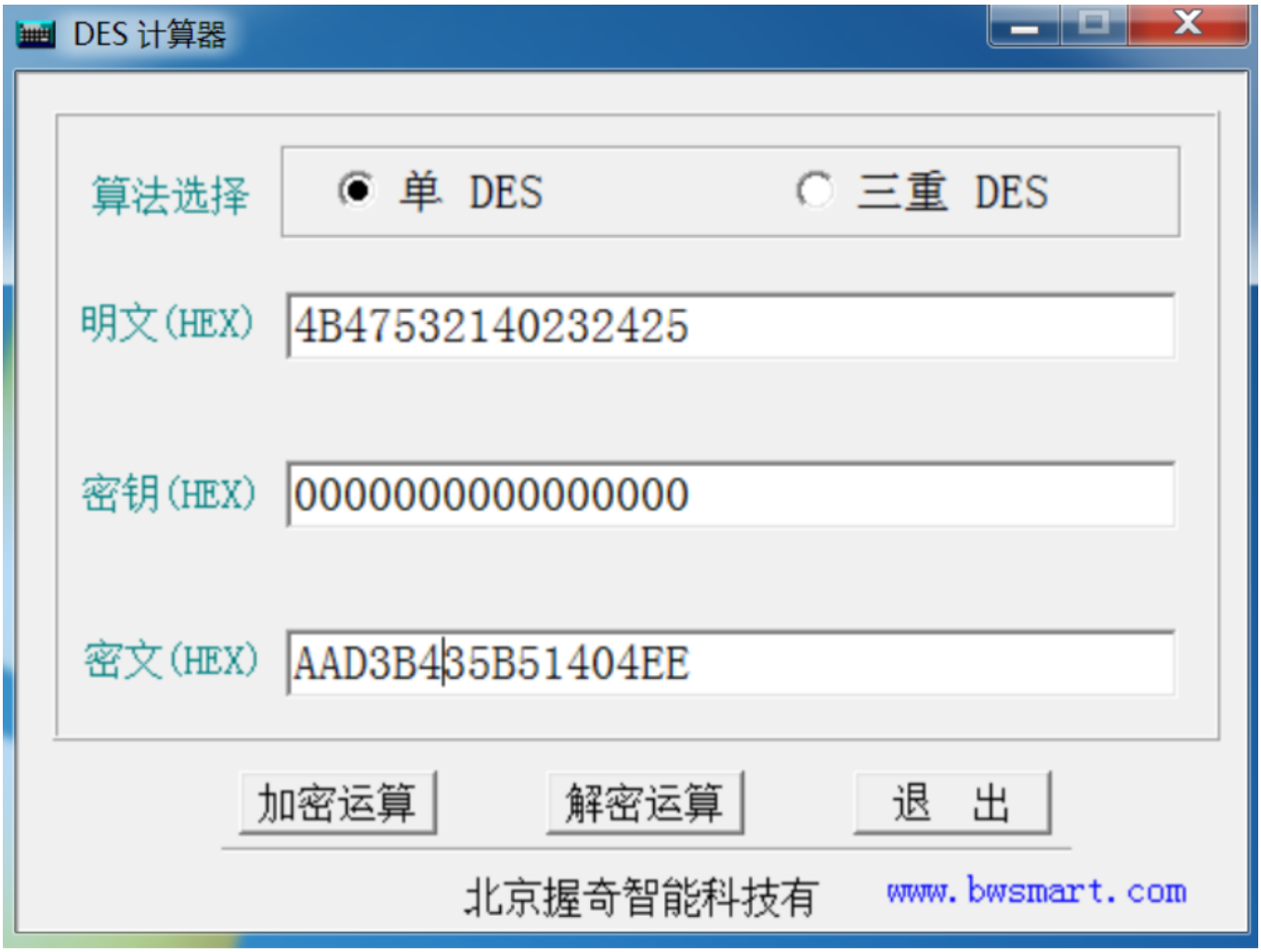
Hash示例

冒号前半段为LM Hash，冒号后半段为NTLM Hash
aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42 net-NTLM Hash：
admin::N46iSNekpT:08ca45b7d7ea58ee:88dcbe4446168966a153a0064958dac6:5c7830315c7830310000000000000b45c67103d07d7b95acd12ffa11230e0000000052920b85f78d013c31cdb3b92f5d765c783030

Hash产生：

1.LM Hash：

```
admin1-ADMIN1(将密码转换为大写字母  )
ADMIN1-41444d494e31(16进制转换)
41444d494e31-41444d494e3100000000000000000(密码未到7位，在末尾补0，填充为14个字符，补16个0)
41444d494e3100  00000000000000(分为两组，各转换为2进制)
10000010100010001001101010010010100111000110001000000000(长度不足56bit，左侧补0)
01000001010001000100110101001001010011100011000100000000(再分为7bit一组，后加0)
0100000 0
1010001 0
0001001 0
1010100 0
1001010 0
0111000 0
1100010 0
0000000 0
01000000101000100001001010101000100101000111000011000100000000000-40A212A89470C400（转换为16进制）
0000000000000000
将上面两组数字des加密
KGS!@#$%-4b47532140232425(KGS!@#$%为LM Hash加密时DES加密的硬编码，转换为16进制)
6C734076E7B827BFAAD3B435B51404EE(将两组des加密后的密文组合，得到LM Hash)
```



注：如果密码不超过7字节，后面的一半是固定的，都为0，安全性降低，所以被弃用。

2.NTLM Hash：
1.hex(16进制编码)
2.Unicode编码 3.md4加密

```
admin1-61646d696e31(将明文转换为16进制编码)
61646d696e31-610064006d0069006e003100(ASCII转Unicode)
610064006d0069006e003100-74561893ea1e32f1fab1691c56f6c7a5(md4加密得到NTLM Hash)
```

获取**Hash**方法

1.使用卷影副本将SAM文件导出，配合SYSKEY利用mimikatz等工具获得NTLM Hash 2.使用mimikatz等工具读取lsass.exe进程，获取Hash 3.配合其他漏洞和手法获取net-NTLM Hash 4.net-NTLM Hash可以使用Responder或Inveigh等工具获取

破解Hash

- LM Hash
  1.john --format=lm hash.txt
  2.hashcat -m 3000 -a 3 hash.txt
- NTLM Hash
  1.john --format=nt hash.txt
  2.hashcat -m 1000 -a 3 hash.txt
- Net-NTLMv1
  1.john --format=netntlm hash.txt
  2.hashcat -m 5500 -a 3 hash.txt

- Net-NTLMv2
  1.john --format=netntlmv2 hash.txt
  2.hashcat -m 5600 -a 3 hash.txt

Active Directory(活动目录)

简介

Active Directory，活动目录简称AD，是一个基于DNS并以树状的数据结构来组成网络服务存储了有关网络对象的信息，并以此作为基础对目录信息进行合乎逻辑的分层组织，让管理员和用户能够轻松地查找和使用这些信息。常网域都只有一个，在中型或大型的网络中，网域可能会有很多个，或是和其他公司或组织的AD相互链接。

活动目录功能

- 服务器及客户端计算机管理
- 用户服务
- 资源管理
- 桌面配置
- 应用系统支撑

存储方式

ntds.dit是AD中的数据库文件，它被保存在域控制器c:\windows\system32\ntds\NTDS.DIT位置。活动目录的数据库文件（ntds.dit）包含有关活动目录域中所有对象的所有信息，其中包含所有域用户和计算机帐户的密码哈希值。该文件在所有域控制器之间自动同步，它只能被域管理员访问和修改。

攻击活动目录

- 利用常规Web渗透进行横向渗透
- 常规Dump Hash后进行PTH，循环操作，直到获取Domain Admins
- 利用SYSVOL和组策略首选项(GPP)
- MS14-068
- 利用VSS卷影副本拷贝ntds.dit
- 利用Responder等工具进行ARP
- Netbios和LLMNR命名投毒
- kerberoast(破解Ticket)
- MS17-010

Kerberos

Kerberos是一种网络认证协议，对个人通信以安全的手段进行身份认证。其设计目标是通过密钥系统为客户机/服务器应用程序提供强大的认证服务。 它允许某实体在非安全网络环境下通信，向另一个实体以一种安全的方式证明自己的身份。该认证过程的实现不依赖于主机操作系统的认证，无需基于主机地址的信任，不要求网络上所有主机的物理安全，并假定网络上传送的数据包可以被任意地读取、修改和插入数据。在以上情况下， Kerberos 作为一 种可信任的第三方认证服务，是通过传统的密码技术(如:共享密钥)执行认证服务的。

协议内容

- AS：认证服务器
- KDC：密钥分发中心
- TGT：票据授权票据，票据的票据
- TGS：票据授权服务器

认证流程

认证流程包含三种角色：
1.Client（客户端）
2.Server(服务端) 3.KDC(也就是参与认证的域控制器) 4.AD(存储所有 client的白名单，只有存在于白名单的Client才能顺利申请到TGT) 5.AS(为Client生成TGT的服务) 6.TGS(为Client生成某个服务的 ticket) 7.Session Key(会话密钥，只有Client和TGS知道，在Kerberos认证中至关重要)

```
一、Client向KDC申请TGT
1.Client以明文方式将用户名、IP地址发送给AS请求TGT
2.KDC在ntds.dit中查找该账户
3.如果找到，KDC随机生成一个Session Key，此时AS向Client发送两条消息
(1)TGT(使用krbtgt NTLM Hash加密)，内容包含：
User Name
Domain Name
组成员资格
TGS Name
时间戳
IP地址
TGT的生命周期
Session Key
(2)另一条消息(使用Client申请TGT时使用的用户名对应的NTLM Hash加密)，内容包含:
TGS Name
时间戳
TGT的生命周期
Session Key
二.Client通过获得TGT向KDC申请用于访问Server的Ticket
1.Client向TGS发送三条消息
(1)Authenticator(使用Session Key加密)，内容包含:
User Name
时间戳
需要访问的服务名称
(2)TGT
2.KDC使用Ktbtgt NTLM Hash对TGT解密，获取Client信息和Session Key
3.使用Session Key对Client发来对Authenticator信息解密，对比Client信息，相同则认证通过
4.TGS向Client发送两条消息
(1)TGS生成Client需要访问服务的Ticket发送给Client，Ticket使用目标服务帐户的NTLM Hash加密。
(2)使用Session Key加密的Server Session Key，内容包含:
Server Name
时间戳
Server Session Key
5.Client收到消息后，使用Session Key解密获得Server Session Key
三.Client最终向为了Server对自己的认证向其提交Ticket
1.使用Server Session Key加密向Server发送Authenticator信息和TGS颁发的Server Ticket，内容包含:
User Name
时间戳
2.Server使用密钥解密Ticket，获得Server Session Key，使用Server Session Key解密Authenticator信息，对比Authenticator信息中的Client信息和Ticket中的Client信息对比，将Authenticator信息的时间戳和Ticket的时间戳是否相同(误差2min)
3.Server使用Server Session Key加密Authenticator信息，内容包含:
ID
时间戳
4.Client使用缓存中的用Server Session Key解密Authenticator信息，得到访问该访问需要携带的ID和时间戳。
5.认证完成，只需要使用申请的Service Ticket就可以正常访问服务。
```

SMB

SMB(Server Message Block)被称为服务器消息块，又叫网络文件共享系统(CIFS)。在Windows2000中，SMB除了基于NBT实现，还可以直接通过445端口实现。

主要功能

使网络上的机器能够共享计算机文件、打印机、串行端口和通讯等资源。

原理

CIFS消息一般使用NetBIOS或TCP协议发送，分别使用不同的端口139或445，当前倾向于使用445端口。

- 直接运行在 TCP 上 port 445
- 通过使用 NetBIOS API
    - 基于 UDP ports 137, 138 & TCP ports 137, 139
    - 基于一些传统协议，例如 NBF

历史版本

1.SMB 1.0 没有数字签名功能 2.SMB 2.0 3.SMB 2.1 4.SMB 3.0

IPC(进程间通信)

简介

指至少两个进程或线程间传送数据或信号的一些技术或方法。

作用

- 信息共享：Web服务器，通过网页浏览器使用进程间通信来共享web文件（网页等）和多媒体
- 加速：维基百科使用通过进程间通信进行交流的多服务器来满足用户的请求
- 模块化
- 私有权分离

功能

IPC$

简介

IPC$是共享“命名管道”的资源，为了让进程间通信而开放的命名管道，通过提供可信任的用户名和口令，连接双方可以建立安全的通道并以此通道进行加密数据的交换，从而实现对远程计算机的访问，从NT/2000开始使用。

IPC$在同一时间内，两个IP之间只允许建立一个连接。

NT/2000在提供了 ipc$ 功能的同时，在初次安装系统时还打开了默认共享，即所有的逻辑共享(c, d,e$.....)和系统目录winnt或管理员目录(admin$)共享。

IPC$主要使用

IPC空连接

对于NT，在默认安全设置下，借助空连接可以列举目标主机上的用户和共享，访问everyone权限的共享，访问小部分注册表等；在WIndows Server 2000及以后作用更小，因为在Windows 2000 和以后版本中默认只有管理员有权从网络访问到注册表。

常用命令

建立IPC$空连接：net use \\192.168.1.101\ipc$ "" /user:"domain\username"

建立IPC$非空连接：net use \\192.168.1.101\ipc$ "password" /user:"domain\username"

删除IPC$连接：net use \\192.168.1.101\ipc$ /del

已经建立IPC$连接并且有权限，将目标C盘映射到本地Z盘：net use z: \\192.168.1.101\c$

删除映射：net use z: /del

关闭IPC默认共享：net use ipc$ /del

注：

1.现在绝大多数的Windows操作系统默认策略不允许来自远程网络验证的空密码，所以IPC空连接已经被废弃。

2.如果远程服务端未开启139、445端口，无法使用IPC$进行连接。

NETBIOS

简介

- NETBIOS(网络基本输入输出系统),严格讲不属于网络协议，NETBIOS是应用程序接口(API),早期使用NetBIOS Frames(NBF)协议进行运作,是一种非路由网络协议，位于传输层；后期NetBIOS over TCP/IP（缩写为NBT、NetBT）出现，使之可以连接到TCP/IP，是一种网络协议，位于会话层。基于NETBIOS协议广播获得计算机名称——解析为相应IP地址，WindowsNT以后的所有操作系统上均可用，不支持IPV6

类型

NETBIOS提供三种服务

- NetBIOS-NS（名称服务）：为了启动会话和分发数据报，程序需要使用Name Server注册NETBIOS名称，可以告诉其他应用程序提供什么服务，默认监听UDP137端口，也可以使用TCP 137端口。
- Datagram distribution service（数据报分发服务）：无连接，负责错误检测和恢复，默认在UDP 138端口。
- Session Server（会话服务）：允许两台计算机建立连接，默认在TCP 139端口。

利用NETBIOS发现主机

1.nbtstat(Windows自带命令)
获取目标主机MAC地址
nbtstat -A 192.168.100.200

```
C:\Users\Administrator>nbtstat -A 192.168.100.200

Local Area Connection:
Node IpAddress: [192.168.100.205] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    COMPUTER1      <20>  UNIQUE      Registered
    COMPUTER1      <00>  UNIQUE      Registered
    PENTEST        <00>  GROUP       Registered

    MAC Address = 00-0C-29-E9-A4-31
```

2.nbtscan

扫描指定网段的主机名和网络开放共享

nbtscan.exe 192.168.100.1/24

```
C:\Users\Dm\Desktop>nbtscan.exe 192.168.100.1/24
192.168.100.200 PENTEST\COMPUTER1               SHARING
192.168.100.205 PENTEST\DC                      SHARING DC
```

SHARING表示开放，DC 表示可能是域控

LLMNR

简介

- LLMNR是链路本地多播名称解析，当局域网中的DNS服务器不可用时，可以使用LLMNR解析本地网段上机器名称，只有WindowsVista和更高版本才支持LLMNR，支持IPV6

工作流程

- 通过UDP发送到组播地址224.0.0.252:5355，查询主机名对应的IP，使用的是DNS格式数据包，数据包会被限制在本地子网中。
- 本地子网中所有支持LLMNR的主机在受到查询请求时，会对比自己的主机名是否相同，不同就丢弃，相同就发送包含自己IP的单播信息给查询主机。

1. 主机在内部名称缓存中查询名称
2. 在主DNS查询名称
3. 在备用DNS查询名称
4. 使用LLMNR查询名称

WMI

WMI(Windows管理规范)，由一系列对Windows Driver Model的扩展组成，它通过仪器组件提供信息和通知，提供了一个操作系统的接口。在渗透测试过程中，攻击者往往使用脚本通过WMI接口完成对Windows操作系统的操作，远程WMI连接通过DCOM进行。例如：WMIC、Invoke-WmiCommand、Invoke-WMIMethod等。另一种方法是使用Windows远程管理（WinRM）。

Windows网络认证

1.工作组

简介

工作组是指数台计算机在同一个内网中，在逻辑上都属于工作组，但是在工作组中的机器之间相互没有信任关系，每台机器的账号密码只是保存在自己的SAM文件中。那就意味着如果需要共享资源只能新建一个账号并指定相关资源授予该账号权限才可以完成共享。早期利用SMB协议在内网中传输明文口令，后为了安全出现LM Challenge/Response 验证机制，再之后LM Challenge/Response 验证机制因为安全性问题，从Windows Vista / Server 2008开始LM就被弃用，改用Windows NT挑战/响应验证机制，常被人称为NTLM，现在被更新到NTLMv2

历史版本。

NTLMv1：服务器通过发送一个8字节的随机数（挑战）来验证客户端，客户端返回两个24字节Hash进行计算并返回计算结果。
NTLMv2：它通过加强协议来抵御许多欺骗攻击，并增加服务器向客户端进行身份验证的能力，从而增强了NTLM的安全性。服务器通过发送一个16字节的HMAC - MD5随机数（挑战）来验证客户端。

工作流程

Client(客户端)、Server(服务端)

- [1] 协商
  Clint向Server发送消息，确定协议版本
- [2] 质询
  Client向Server发送用户名消息作为请求
  Server收到请求，验证是否存在Client发来的用户名，如果存在，生成16位的随机数(Challenge)发送给Cilent，并使用SAM中查询用户名对应的NTLM Hash加密Chanllenge，生成Net-NTLM Hash存放在内存中。
  Client使用发送的用户名对应的NTLM Hash加密Challenge，将结果(Response)发送给Server
- [3] 验证
  Server收到Client发送的Response，将接收的Response与Net-NTLM Hash进行比较，如果相同，则认证通过。
  注：每次生成的16字节的Challenge都不同，保证的安全性。

本地认证流程

- Windows Logon Process(即 winlogon.exe)，Winlogon 是负责处理安全相关的用户交互界面的组件。Winlogon的工作包括加载其他用户身份安全组件、提供图形化的登录界面，以及创建用户会话。
- LSASS(本地安全认证子系统服务)用于微软Windows系统的安全机制。它负责Windows系统安全策略。它负责用户在本地验证或远程登陆时验证用户身份，管理用户密码变更，并产生访问日志。

用户注销、重启、锁屏后，操作系统会让winlogon显示图形化登录界面，也就是输入框，接收域名、用户名、密码后交给lsass进程，将明文密码加密成NTLM Hash，对SAM数据库比较认证，相同则认证成功。

内网渗透常用端口

- 53
  DNS服务，在使用中需要用到TCP/UDP 53端口，AD域的核心就是DNS服务器，AD通过DNS服务器定位资源
- 88
  Kerberos服务，在使用中需要用到TCP/UDP 88端口，Kerberos密钥分发中心(KDC) 在该端口上侦听Ticket

请求

- 135
  135端口主要用于使用RPC协议并提供DCOM服务。
- 137
  NetBIOS-NS(名称服务)，在使用中需要用到TCP/UDP 137端口
- 139
  Session Server(会话服务),在使用中需要用到TCP/UDP 139端口，允许两台计算机建立连接
- 389
  LDAP服务(轻量级目录访问协议)，在使用中需要用到TCP/UDP 389端口，如果需要使用SSL，需要使用636端口，
- 445
  主要用于共享文件夹或共享打印，存在较多漏洞，如MS08-067、MS17-010
- 3268 Global Catalog(全局编录服务器)，如果需要使用SSL，需要用到3269端口，主要用于用户登录时，负责验证用户身份的域控制器需要通过防火墙，来向“全局编录”查询用户所隶属的通用组

内网渗透流程

Initial Access

- Webshell
- 个人机Beacon
- VPN

网络位置判断

- 网络区域
- 主机角色
- 连通性判断

信息收集

信息收集常分为工作组信息收集、域信息收集，管理员、非管理员。信息收集范围包括但不限于对权限信息，机器信息，进程端口，网络连接，共享、会话、敏感文件、密码文件、配置文件、浏览器记录、远程连接工具如xshell等工具记录等信息进行详细收集并加以合理运用，将已有信息最大程度利用，如某大佬所说，渗透的本质是信息收集。具体信息收集命令可以查阅参考链接，不再赘述。

内网穿透常见协议及利用

- TCP
- UDP
- Http
- Https
- SSH
- DNS
- Icmp
- FTP
- GRE

在内网渗透中常见方法:
1.将单一端口转发到公网VPS
2.反向sockets代理，可以将流量全局带入
常用文件类型:

exe/ps1/python

权限提升

1.EXP提权
利用已公开EXP进行溢出提权可参照windows-kernel-exploits，可以配合Windows-Exploit-Suggeste进行辅助提权。
2.利用AD特性提权
如MS14-068、GPP等
3.Windows非EXP提权
劫持类提权如DLL劫持、COM劫持、Unquoted Service Paths、利用第三方高权限服务提权
4.Bypass UAC
Windows系统中Administrators组非SID为500的用户必须Bypass Uac才可以获得特权令牌，具体方法可以使用Windows自带程序进行Bypass，可以参考UACME项目。

内网横向渗透方法

- ipc$+计划任务
- PTH
- Wmi
- WinRm
- 利用常规Web渗透横向
- sc
- ps1

在无法抓取用户明文密码的情况下可以使用Hash注入登陆系统或登陆服务

内网渗透持久化

1.利用活动目录

- Golden Ticket
- Silver Ticket
- DSRM
- SSP(Security Support Provider)
- Hook PasswordChangeNotify
- SID History

2.Windows常规持久化

- 常规Webshell
- 利用Windows注册表项
- Logon Scripts
- Dll劫持
- 计划任务
  (1)at
  (2)schtasks
- wmi事件
- COM劫持

MITI

1.Responder responder.py –A 分析模式 2.Impacket Relay attacks Tools，该工具可以进行SMB Relay、NTLM

Relay。 3.smb relay ntlmv2 使用Impacket中的ntlmrelayx.py和Responder中的MultiRelay.py配合使用。在SMB签名关闭的情况下将net-ntlm Hash中继进行攻击，SMB签名默认在非Windows Server系统中关闭。

日志清理

Windows EventLog、Application Log、Session、进程、物理存储中的二进制文件

内网渗透常用工具

1.渗透框架

- Cobalt Strike
- Empire
- NiShang
- Metasploit
- Powersploit

2.信息收集

- Netsess.exe
- Powerview
- Bloodhound

3.权限提升

- Powerup
- UACME

4.口令爆破

- Hydra
- John
- Hashcat

5.凭据窃取

- Mimikatz
- Procdump
- QuarksPwDump
- LaZagne.exe

6.横向渗透

- psexec
- wmi
  (1)wmic (2)wmiexec.vbs (3)Invoke-WMIMethod
- WinRM
- wce
- 组策略种马

7.MIMT

- Responde
- Impacket
- Invoke-Inveigh.ps1

- Cain

7.Bypass AV

- Invoke-Obfuscation
- Veil

参考资料：

https://blog.csdn.net/qq_36119192/article/details/83143354 https://payloads.online/archivers/2018-11-30/
https://github.com/l3m0n/pentest_study https://github.com/SecWiki/windows-kernel-exploits
https://blog.csdn.net/qq_29647709/article/details/84636049 https://zh.wikipedia.org/wiki/Active_Directory
https://zh.wikipedia.org/wiki/Kerberos
https://mp.weixin.qq.com/s?__biz=MzIxNTQxMjQyNg==&mid=2247484247&idx=1&sn=ca9f7fd6ca95000b2b41b13a0a356ede&chksm=9799f8f2a0ee71e44ca01c49c4f9d5a7e222e822608de9e27941272f445600e40e6c7406e94f&mpshare=1&scene=1&srcid=0125ruNezc26zLQykmh48YTO#rd https://blog.csdn.net/wulantian/article/details/42418231
https://www.roguelynn.com/words/explain-like-im-5-kerberos/
https://www.freebuf.com/articles/system/45631.html https://en.wikipedia.org/wiki/NT_LAN_Manager
https://docs.microsoft.com/en-us/windows/desktop/secauthn/microsoft-ntlm
https://wenku.baidu.com/view/8c342e95700abb68a982fba5.html