一步步成为你的全网管理员（上） - SecPulse.COM | 安全脉搏

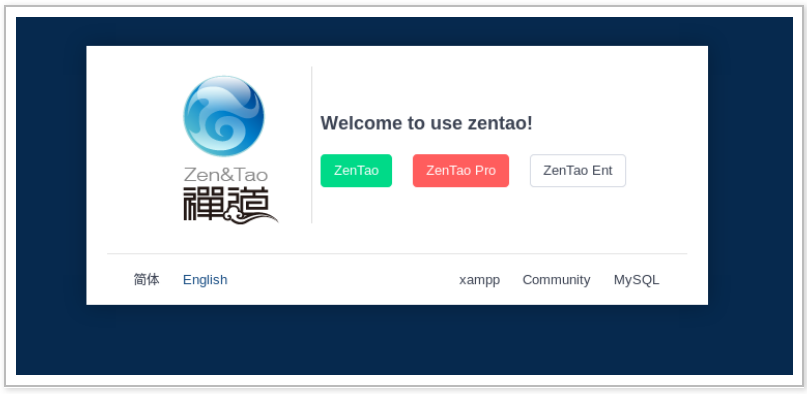
> 这是 酒仙桥六号部队 的第 113 篇文章。

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

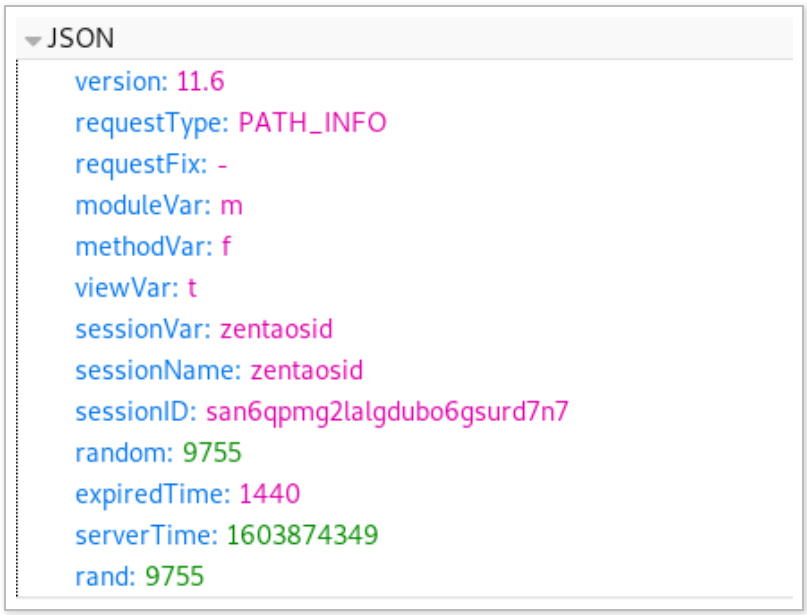
首先对目标进行资产收集，发现目标对外只开放了一个 WEB 服务，经过查看，发现运行的是禅道。



既然没有其他的选择，那就从这里入手，首先查看当前版

本，发现是 11.6。

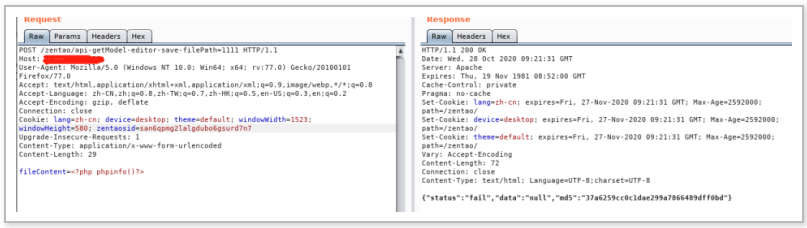
http://xxxxx/zentao/index.php?mode=getconfig

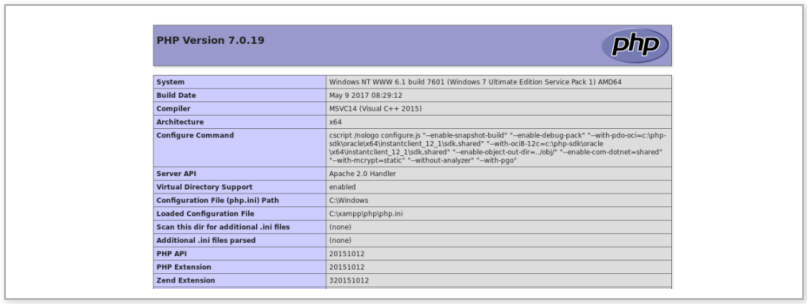


经过搜索发现此版本存在多个漏洞，但是受限于需要先进行登录，于是使用常用用户名对登录接口进行弱口令爆破，成功发现一个可登录账号：lihua/qwe!@#456。

使用爆破出的账号登录进入系统。

检查漏洞是否被修复，发现 RCE 漏洞未修复。





接下来自然就是愉快的写马 Getshell，由于路径问题，需要覆盖 www 目录下的原有 php 文件才可以被解析，这里选择覆盖 x.php 文件。成功写入一句话木马，并用蚁剑成功连接，获取到目标服务器权限。

打开终端查看权限发现是 system 权限，那就可以省了提权。

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
# 查看网络连接情况
```

```
# 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
```

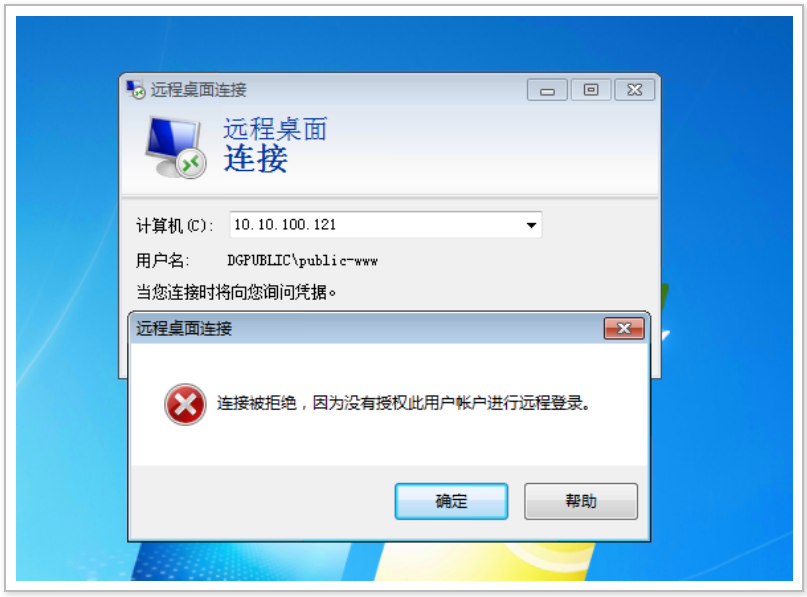
通过对主机信息进行收集发现此主机不可出网，并且处于域环境（dgpublic）中，且主机同段存在其它域主机。

发现的部分主机：

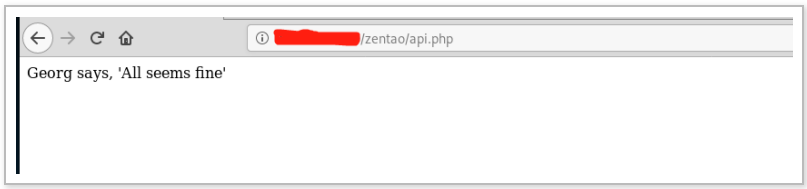
根据主机名和域账户名对比发现部分对照关系，比如 john 员工的主机名为 IT-SUPPORT-JOHN，根据主机名和 john 在域管组中的信息，猜测 john 为目标内部网络管理员，通过查看 john 账户状态发现其账号处于活跃状态，此账户的情况可以在后续横向移动中重点关注。

在禅道系统主机上获取到域账号 public-www/P@ssw0rd!@#$，但由于权限较低，无法登录其他

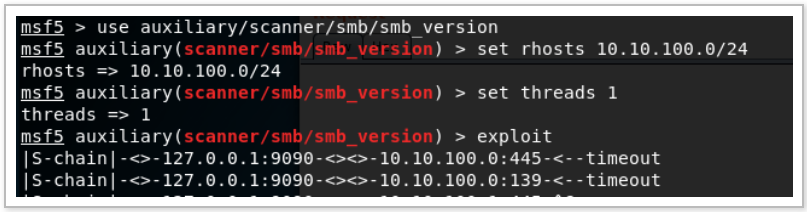
主机，仅可在当前主机进行登录。

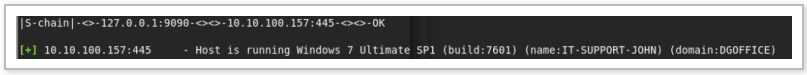


接下来把自己流量代理进去，上传 reGeorg 流量代理工具，成功把流量代理进去。



通过 proxychains 将 msf 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。

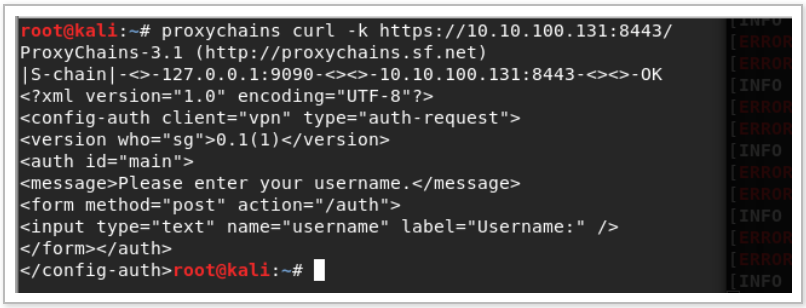




在扫描结果中发现 IT-SUPPORT-JOHN 主机，其 IP 就是 10.10.100.157，并且其所属域已经更改，已经不在当前域中（dgpublic），但域中主机信息未删除，所以前面进行解析时没有接触出其 IP 地址，现在位于 dgoffice 域，根据所在域的名字判断其为目标办公域。

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。



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。

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。

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

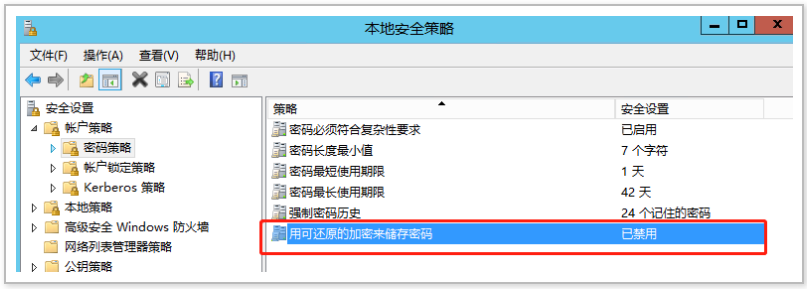
改密码后，就可以通过在域控上提取域快照直接获取其修改后的明文密码。为了防止其修改密码后我们无法再使用 john 账户登录，所以在域控上先留下后门备用。设置完成后，只需要进行等待，等待其下一次登录。

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：



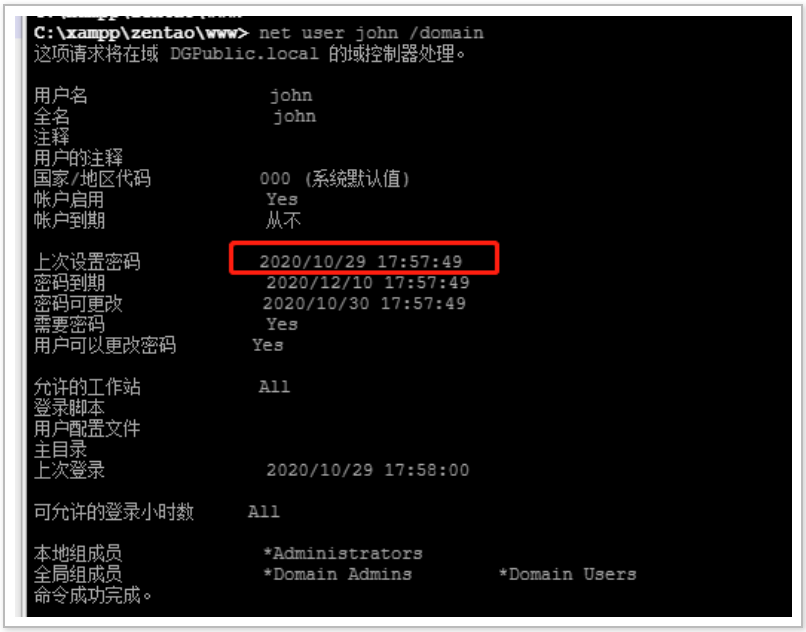
可以使用如下命令获取域中设置了可逆加密标志的用户列表：

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

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

name                 samaccountname       useraccountcontrol
----                 --------------       ------------------
john                 john                                640
```

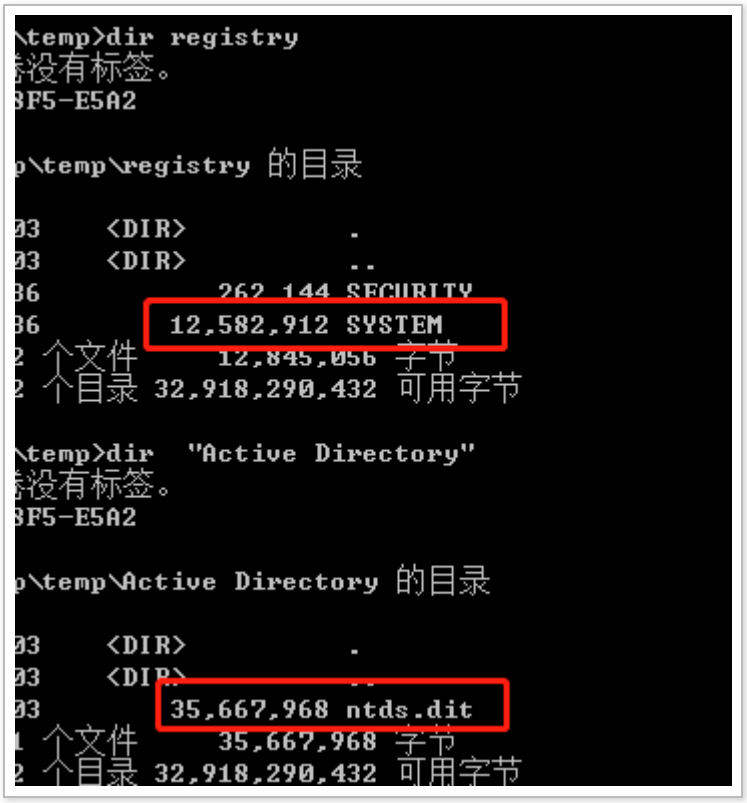
功夫不负有心人，在又等待了一段时间后，查看到 john 账户在域中再次被使用过，并修改了密码，但并不知道在哪台主机上使用的。



这样就直接远程域控，通过提取域快照获取其新密码。

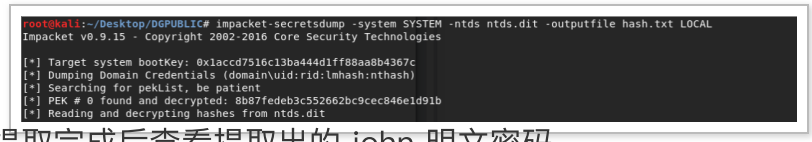
```
ntdsutil "ac i ntds" "ifm" "create full c:windowstemp
```

提取成功后，下载 SYSTEM 和 ntds.dit 文件到本地进行操作。

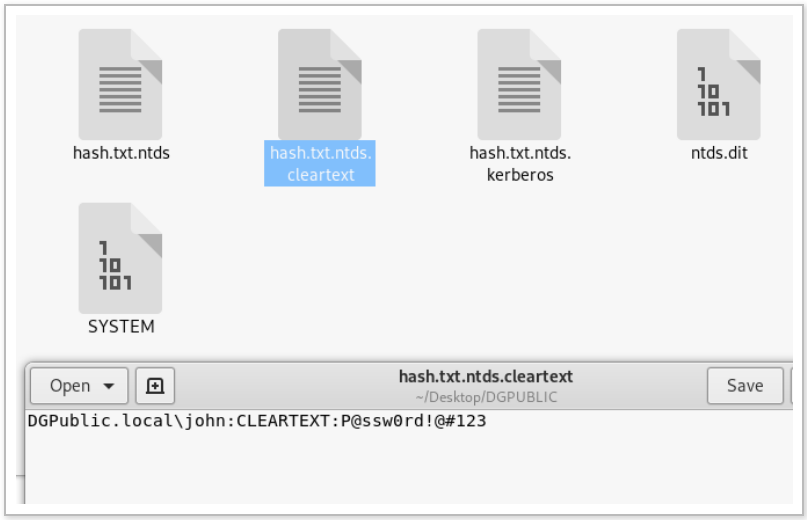


使用 impacket 中的 secretsdump 提取。

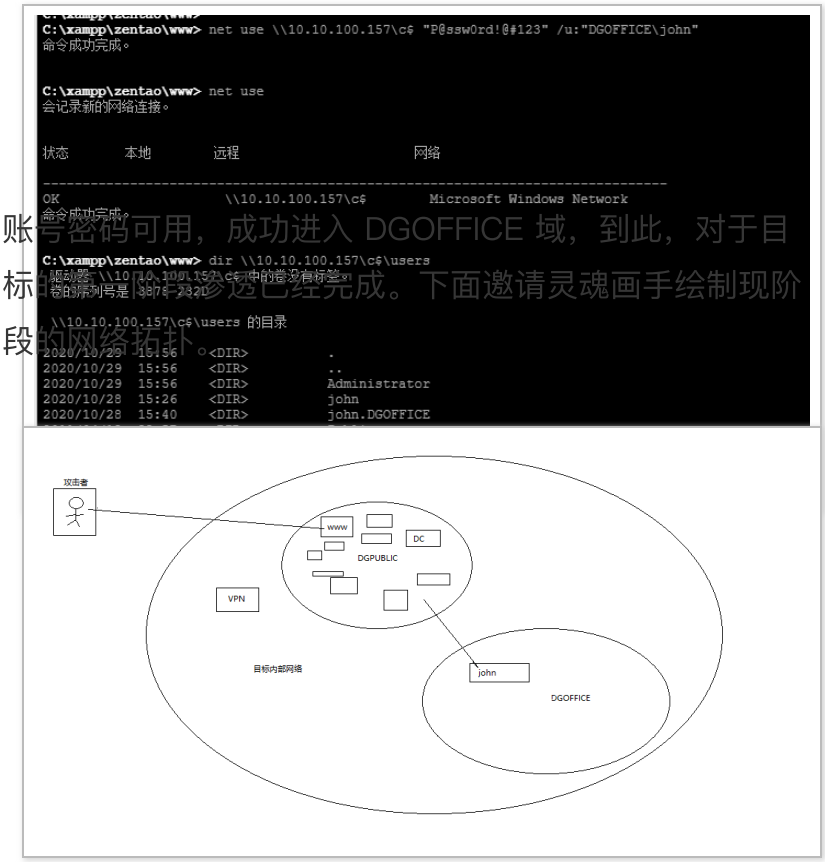
```
impacket-secretsdump -system SYSTEM -ntds ntds.dit -ou
```



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，对于目标的渗透已经完成。下面邀请灵魂画手绘制现阶段的网络拓扑。

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