Gpp

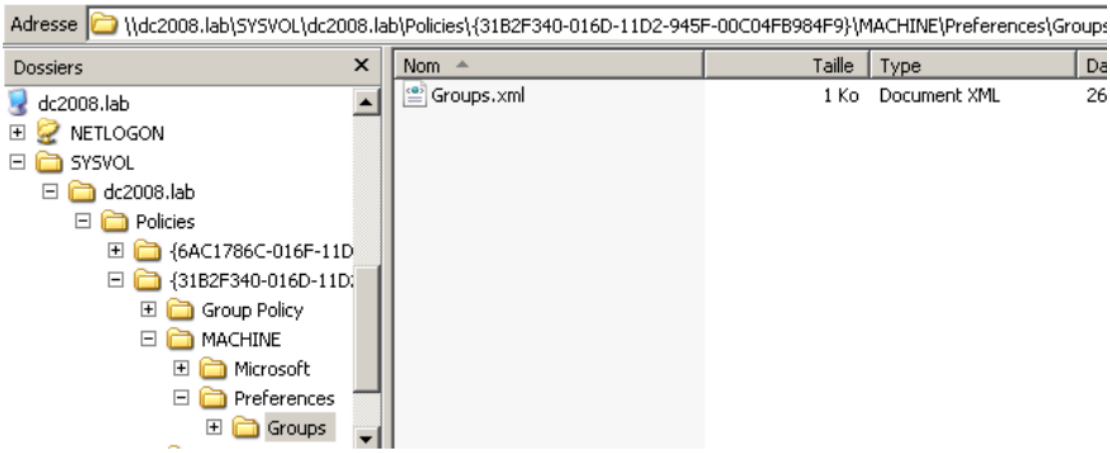
补丁：MS14-025

Windows Sever 2008　的组策略选项（GPP）是一个新引入的插件

GPP 最常用的一项基本功能——远程创建本地账户

这个功能允许域管理员在域控制端远程向域内主机添加本地账户以方便管理.

而 DC 端添加用户成功，需要域成员更新组策略，才可以添加用户"gpupdate && net",其实更新策略的时候是请求 DC 端下载了一个 sysvol 目录 Groups.xml 的文件，而 sysvol 目录对于任何域成员机器是可读的，并且密码是可逆的，相当于我们拿到了一个本地的账户跟密码。(这里面还有其他的功能 远程创建本地账户只是一种)



http://drops.wooyun.org/papers/576 (这个渗透文章用到了 Gpp)

http://www.carnal0wnage.com/papers/LARES-GPP.pdf

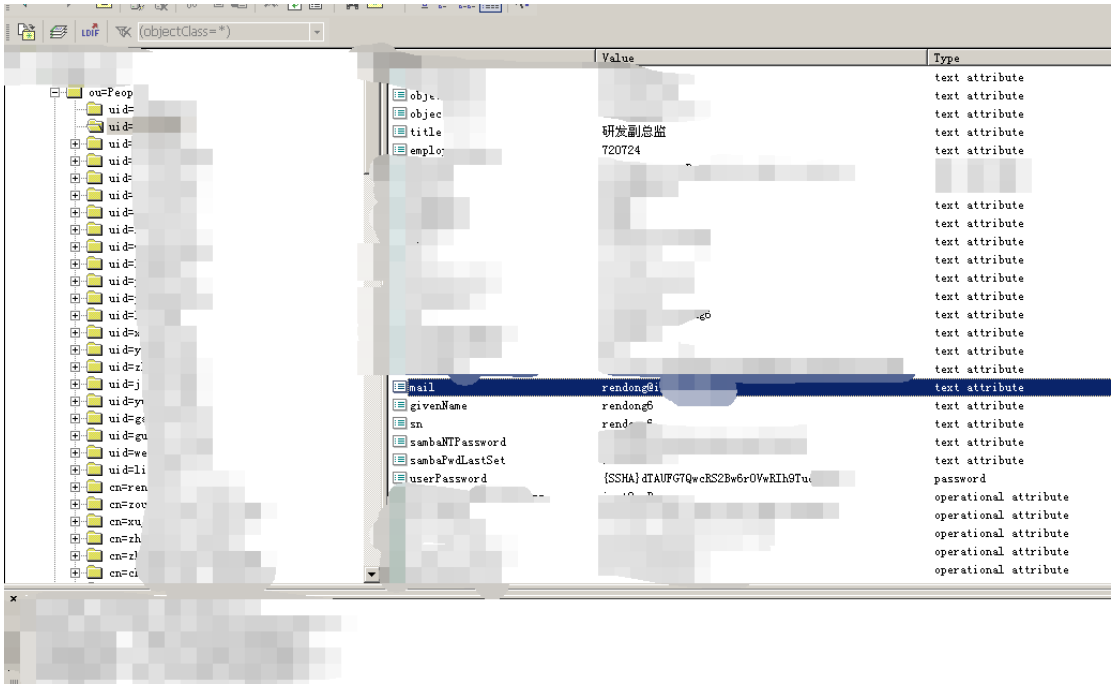
http://blogs.technet.com/b/grouppolicy/archive/2009/04/22/passwords-in-group-policy-preferences-updated.aspx

https://labs.portcullis.co.uk/blog/are-you-considering-using-microsoft-group-policy-preferences-think-again/#imageclose-2242

Ldap

很多企业会使用 ldap 做 sso,为了账户统一管理。

Ldap 配置不当会存在匿名用户访问 泄漏用户名 密码，有了员工的账户密码，登录邮箱，oa 等。



LDAP 配置为 secret 的时候 密码是明文

LDAP 加密方式有： CRYPT、MD5、SMD5、SHA 和 SSHA。刚好我遇到的就是 SSHA 可以看上图{SSHA},由于时间的关系，当时没去看 SSHA 到底怎么样加密的。要是知道 SSHA 加密方式的，可以告诉我，免去暴力破解密码的时间。

Sudo

sudo 命令用来以其他身份来执行命令。

visudo /etc/sudoers

sanr ALL=/bin/more (这里可以是 all)

sanr 可以切换到 root 下执行 more 来查看文件

[sanr@localhost ~]$ sudo more /etc/shadow

在我们渗透的过程中，不妨用 sudo 试试，可能会有意外的发现。

Ssh 信任

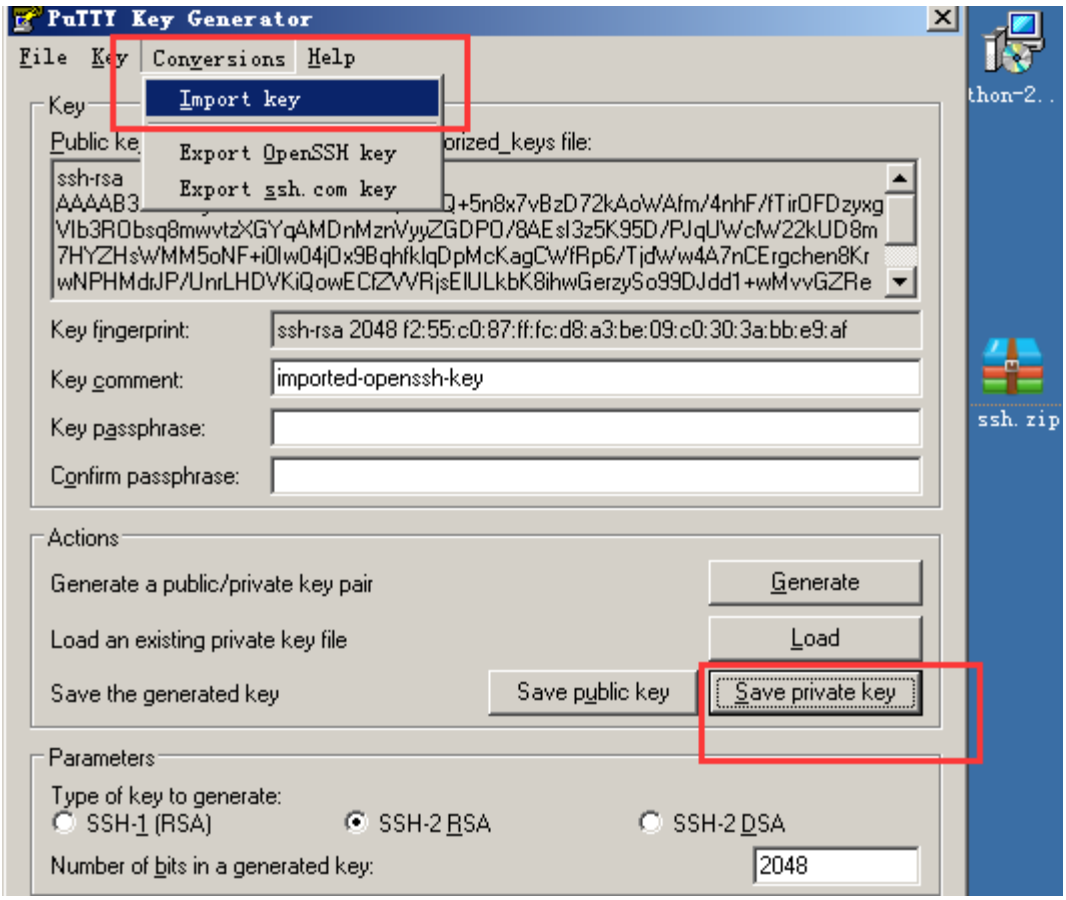
很多企业运维为了方便管理，或者自动化运维之类的,会为了两台主机不用输入密码.使用证书登录这种，如果你运气好，在/home/用户/.ssh 目录.找到 id_rsa(私钥) known_hosts(连接过的历史记录 会知道连接那个用户连接用户的)

Ssh 信任,你生成的公钥跟私钥，你把生成的公钥放在别人的机器/home/用户/.ssh 目录，有别人问过我，那你直接连接过去是什么权限，这个完全取决于,你的证书存放在对方机器那个用户目录，是 root 那么你用证书登录过去就是 root，是其他用户则是其他用户。

Window 的利用方法:

如果你通过文件读取或者其他方法获取到 id_rsa 了，但是你怎么样利用呢,例如 putty

Puttu 直接导入不了,openssh 生成的私钥的,需要转换成 ppk 格式。(xshell 不需要转换)



缓存密码

缓存密码这个有太多了，我挑我常用的几个说下把。取决于你入侵的场景是什么，假如你搞的这个机器没有 wincsp、svn 这些，但是有 navicat 也是可以的获取，不管什么软件要是有保存密码。那么他肯定会缓存密码的，有的可能是加密的，需要解密。

1.浏览器

2..winscp

2.svn

Hash 注入

拿到某 hash 破解不了怎么办

wce.exe -s administrator:ip:LM-HASH:NT-HASH

直接 ipc 命令操作对方的机器就可以了

自从 win7 之后，默认不存储 lmhash 了，因为 lmhash 不支持 14 位以上密码，都使用 nthash，当你发现 LM Hash 的部分全是 0 或者 aad3b435b51404eeaad3b435b51404ee 的话，就证明没有 lmhash。虽然只有 nthash，只是增加了破解的难度， 并不是绝对不可破，很多人用的密码还是弱口令,还是可以破解的。

如：

LM-HASH: aad3b435b51404eeaad3b435b51404ee

NT-HASH　　1e63d8bc5c29d353d59819b20a4ca8a8

lmhash 是空的,nthash 算出来的明文是 j35015

没有 lmhash 还可以 hash 注入吗？是可以的

用 32 个 0 代替

wce -s　administrator:ip:00000000000000000000000000000000:NThash

域缓存 hash

域缓存是个什么鬼？要是你追究你加入域之后，为何回家了电脑还可以使用域用户登录进去，你就知道为何了。

计算机加入域后，Windows 系统默认会在注册表内缓存最近 10 个在机器上登录的域账号与密码信息。这是为了方便当计算机联系不到域控制器时，还能使用曾经登陆过的域账号继续登录。

提取域缓存 hash

reg save hklm\sam c:\sam.hive & reg save hklm\system c:\system.hive & reg save hklm\security c:\security.hive

下载地址：https://github.com/Neohapsis/creddump7

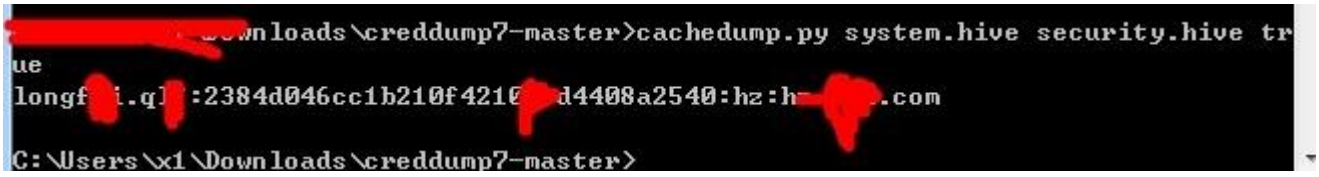
Example (Windows Vista/7):

./cachedump.py /path/to/System32/config/SYSTEM /path/to/System32/config/SECURITY true

Example (Windows XP):

./cachedump.py /path/to/System32/SYSTEM /path/to/System32/config/SECURITY false

需要注意你执行命令后面的 false 跟 true　因为 xp 跟 win7 的域缓存 hash 加密不一样，



利用监控跨网段

进入一个公司内网，知道目标机，可是访问不了怎么办？我常用的做法,看本地的机器存在不存在 zabbix 客户端 etc/zabbix/zabbix_agentd.conf，之后找到 server 的地址，去把 zabbix 搞定(CVE-2013-5743 弱口令)，利用 zabbix 跨网段，当然不仅仅是 zabbix cacti 等都可以， 取决于自己的内网存在什么东西，没有固定的思路。

快速寻找目标机

进内网了，怎么样知道内网拓扑，渗透之前通过收集子域名，有时候已经知道内网服务器环境的 IP 是多少，如果内网有自己的 dns，如存在 dns 域传送，直接可以列出来域名在内网解析的 IP。

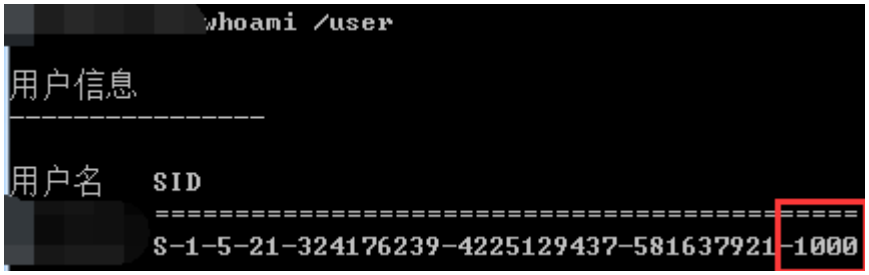
UAC 的问题

server2008 2012 由于开启了 UAC 了功能，ipc 时候只能是 Administrator (SID 500)帐号。

就算是管理员用户组的其他用户也不能进行远程连接

你添加账户在管理员组也不能 ipc，PSEXEC 不能使用

如果你是域管理员，不受 UAC 的影响



Linux 跨 window 渗透

不借助第三方打包文件

压缩一个文件：

makecab c:\ls.exe ls.zip

解压一个文件：

expand c:\ls.zip c:\ls.exe

不借助第三方 base64 编码

编码一个文件

certutil encode demo.tz 1.txt

解码一个文件

```
certutil  encode  1.txt c:\demo.tz
```

搞内网搞域,就自己去搭建域,自己去实践已知域中所存在的漏洞,基础知识也很重要,建议买本 Windows Server 2008 R2 Active Directory 配置指南。

有的人可能看了会说，就像 zabbix rce、dns 域传送漏洞可以使用嘛，搞内网主要看的还是耐心跟思路，跟追女朋友一样，先试这个思路，这个思路不行换其他的思路，别把国内的内网想的太高大上，我在内网还见过 ms08067 06040 的漏洞，一个公司存在很多部门，程序员也会自己搭建一些测试系统，很多企业都重力放在了边界安全，心中所想，黑客入侵不进来就可以了，往往忽略了内部的安全，就像那些出口流量审计的 waf 等设备，要是你从内部发起的攻击，无法拦截，国内基础安全都没做好，很多情况下就扯不上 apt 攻击。

2015 年 12 月 3 日 sanr