【渗透实战】记一次艰难的内网漫游之旅_拿下472台主机shell！

作者：Kali_MG1937

原文链接：https://mp.weixin.qq.com/s/kgVk52DzXYBCKW3XTjd91g

0x000

对这几周的渗透成果进行总结，为了这次的渗透能够顺利，我做了近两周的准备。

0x001

第一步：信息收集

1）在筹划期间我做了很多种方案但最后还是打算先渗透机房电脑比较直接

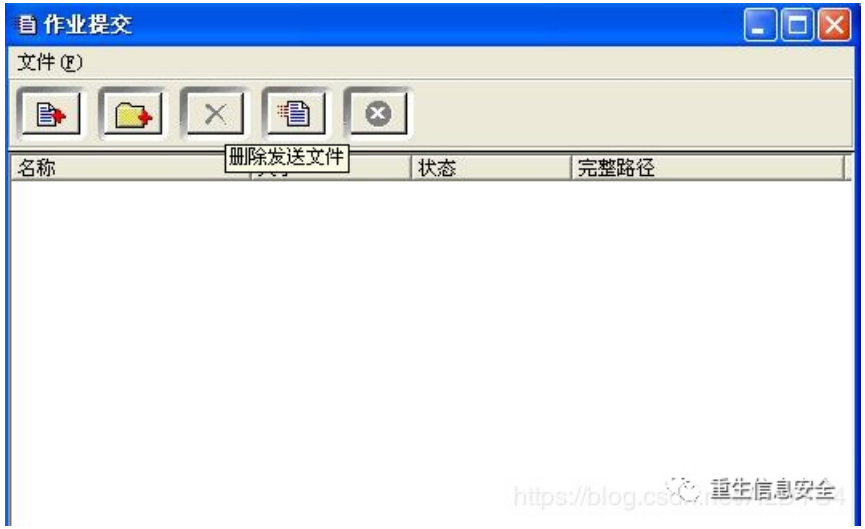
2）可是没机会给电脑上装payload

3） 机房内的用机是安装有控制软件的。。本文就从这里开始好了

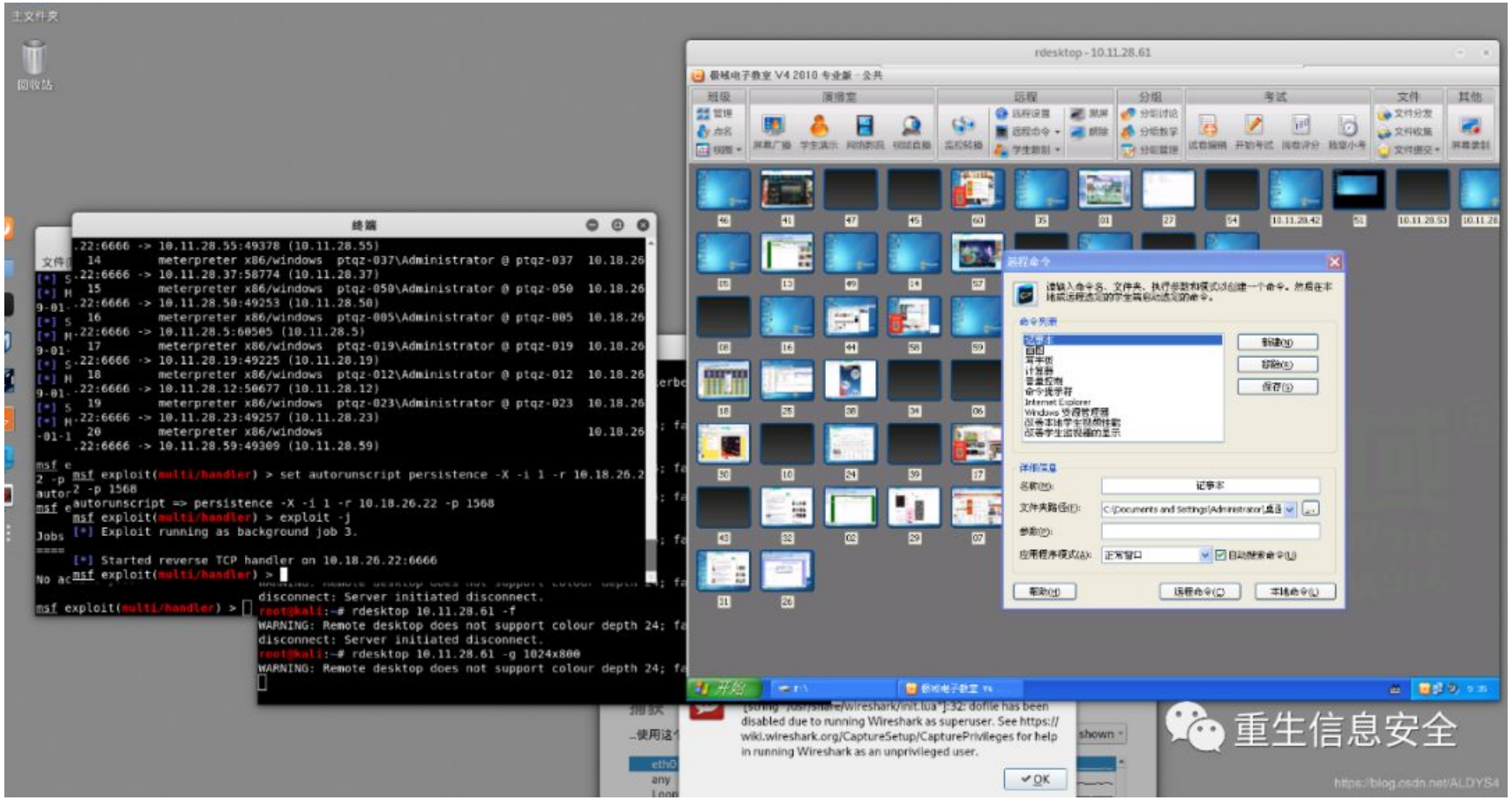
0x002

第二步：渗透机房

控制软件有一个功能,就是上传作业,很幸运的是教师机和学生机一样,全部使用windows默认设置: 不显示已知文件的后缀
提交作业时的标准是提交doc或xls文件,对msf的载荷名进行修改
例如:“作业.doc.exe”



提交完成,过了一阵子,meterpreter收到了反弹的shell
教师机权限到手
做好权限维持,以备在其他地方能够访问傀儡机



0x003

第三步：查看教师硬盘

1）浏览了一阵老师的电脑，发现了一些关于学校服务器的报告，其中包含了服务器地址，服务器地址:10.11.26.65。

0x004

第四步：ban服务器

1）看了下服务器地址，确认是办公楼的地址段

2）nmap粗略扫描后发现80端口开启

3）打开网页，试试看有没有注入漏洞

-
-

```
username='or'1'='1password='or'1'='1
```

发送post后服务器的确发生了302跳转，可最后看到的不是完整的学生信息，而是500错误，sqlma

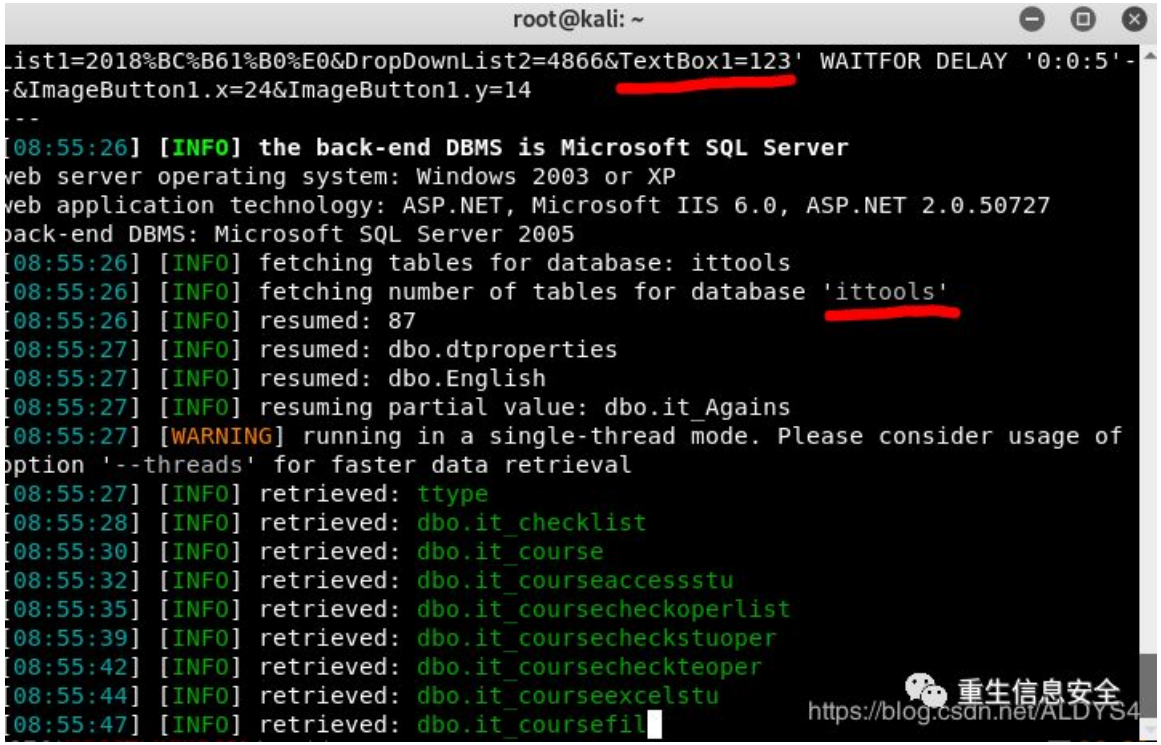
p扫描后也判断并没有注入点。

4）我返回去查看教师电脑上服务器文件的介绍，上面规定每个用户名的默认密码是123

-
-

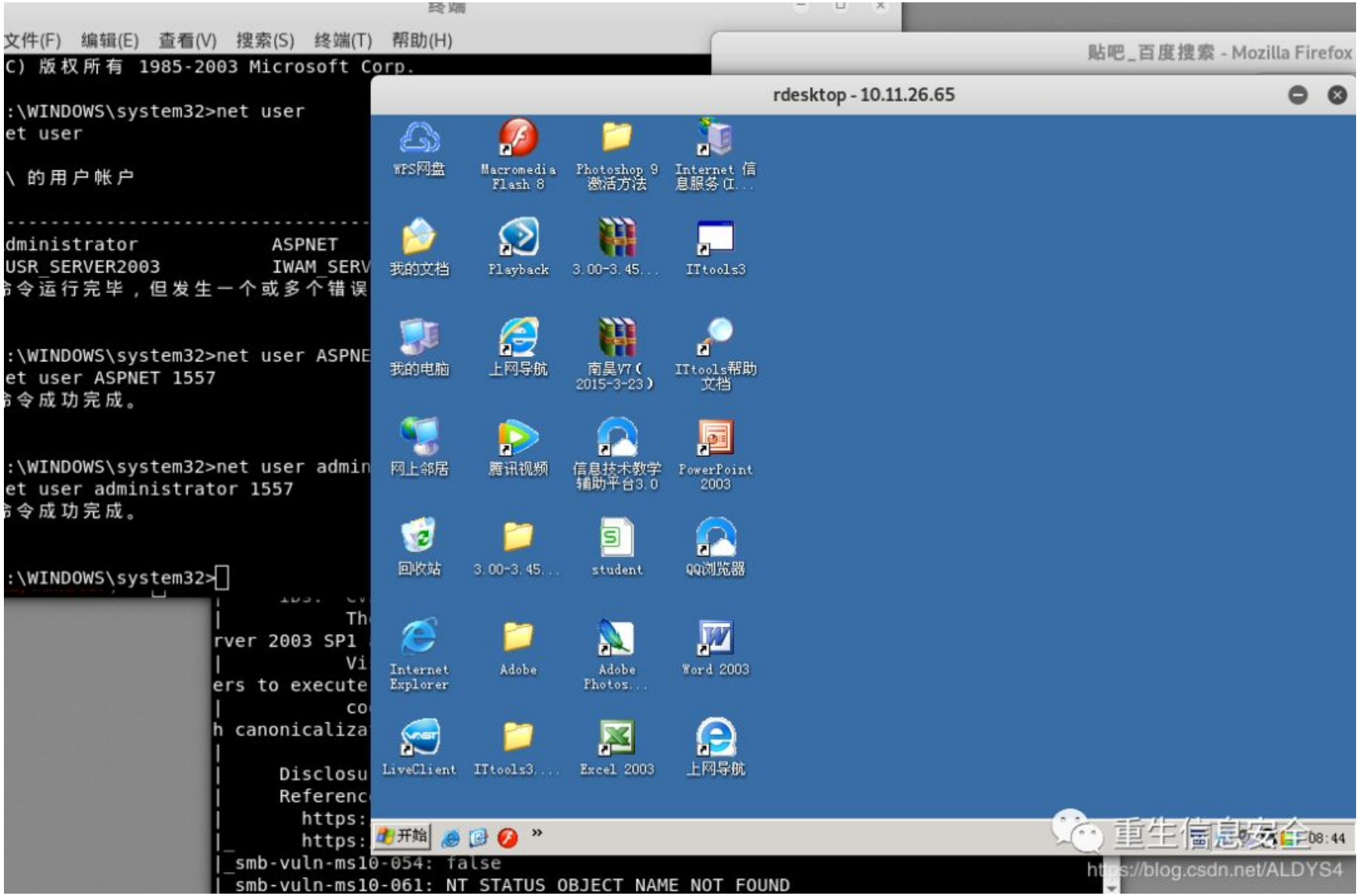
```
username=用户名’and’1’='1password=123
```

发送post请求，成功登入，带入sqlmap扫描，dump出注入点，拿到dba权限！



5）上传shell

6）通过dump出的服务器信息猜测，服务器一定是Windows XP sp1-2左右的版本，那么果断用nmap扫描445端口，发现ms17010漏洞！



0x005

第五步：渗透交换机与路由器

1）办公楼的地址段是10.11.*.*

2）查看被渗透服务器的ip信息，发现网关是10.11.254.254

3）打开http://10.11.254.254，是H3C交换机，很幸运的是账号密码都是默认的

-
-

```
adminadmin
```

4）这个弱口令没什么好讲的，纯属是学校的安全没做好，重要的是路由器

5）通过nmap扫描10.11.254.254以及其地址段下的ip

6）发现请求无一例外都跳向了192.168.11.1，nmap扫描192.168.11.1，发现根本没有结果。

-

```
1000 port all down
```

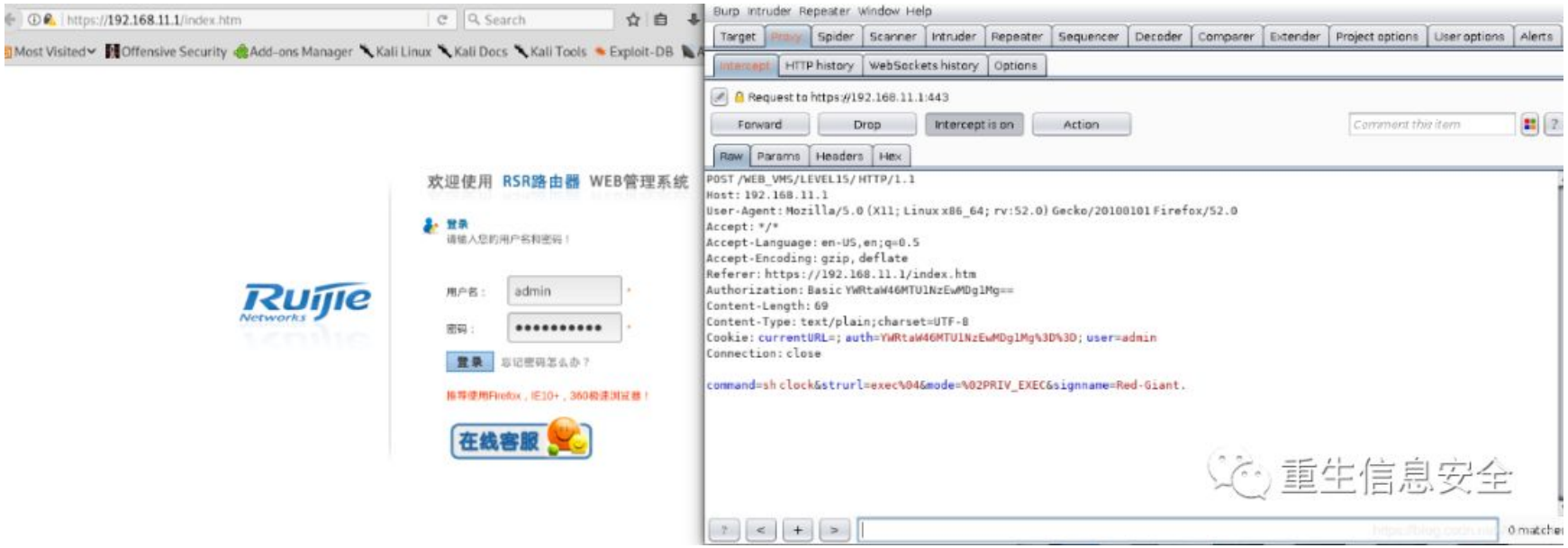
7）但奇怪的是nmap在扫描这个ip时总跳出一个提示：

-

```
Do the 443 port really open?
```

8）接着第二次扫描时就再也没有结果，在停止扫描十几分钟后才能再次ping通地址

9）直觉告诉我这是学校的防火墙拦截了nmap扫描因为可能开着443端口，先打开https://192.168.11.1



10）上网查找锐捷路由器的弱口令，admin回车！登入失败！

11）可惜不是弱口令，那么用burpsuite抓个包看看有没有漏洞，发现有个command参数：

-

```
sh clock
```

12）上网查找了锐捷路由器的资料后发现这是用来测试用户是否有路由器权限的

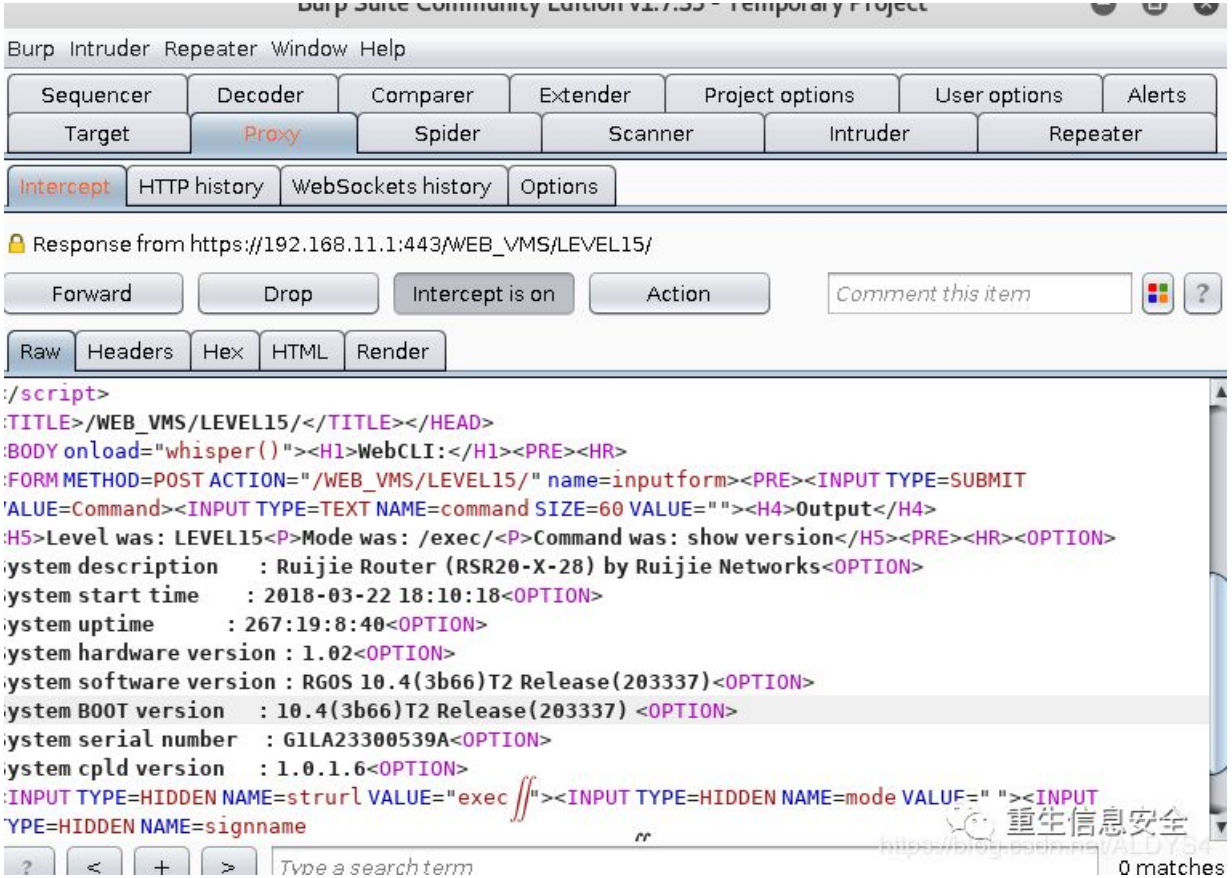
如果账号密码错误，

-

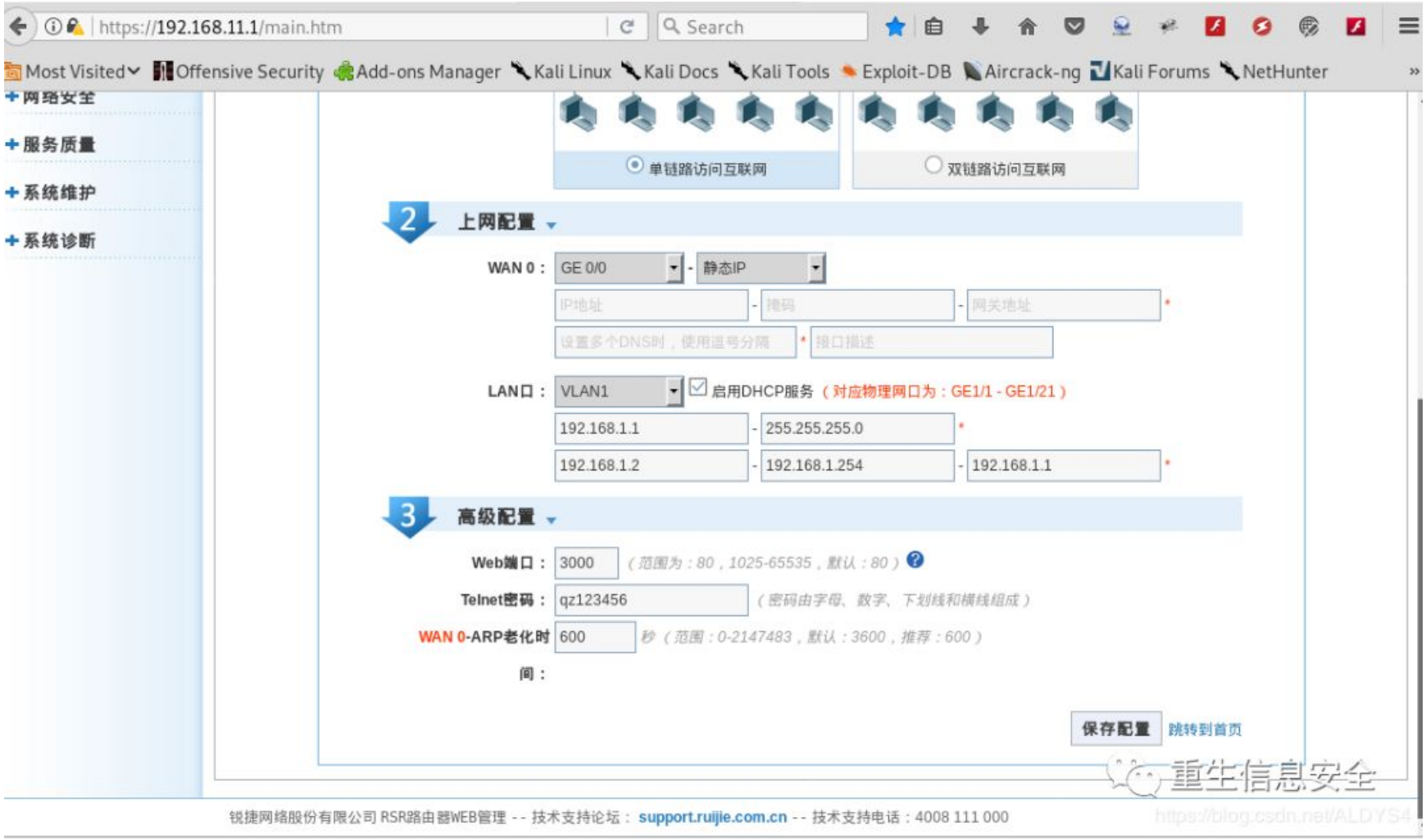
```
response则是401 Unauthorized
```

13）继续查找资料，发现show version这个命令是不用权限就能执行的

你懂得，改sh clock为show version，发送post

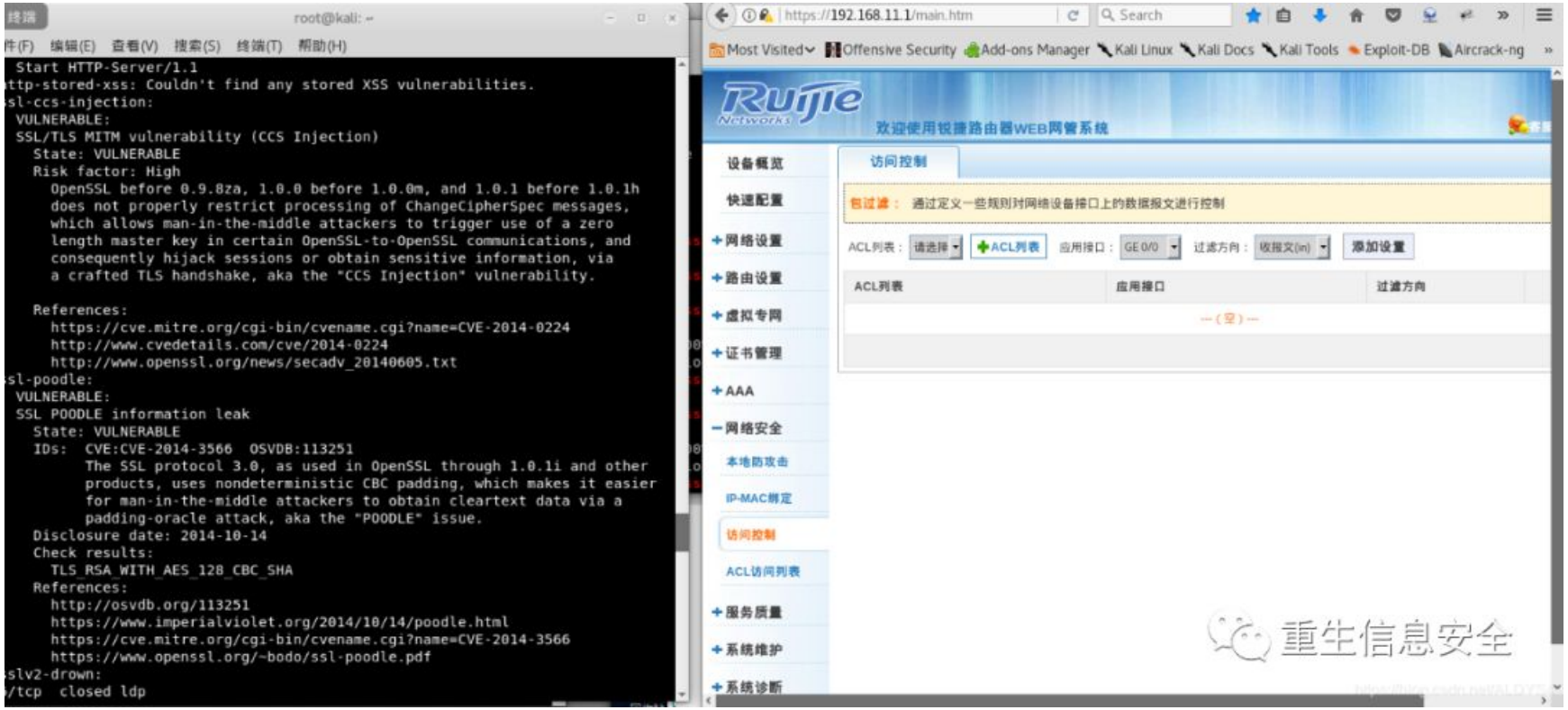


14）成功爆出服务器信息，并且返回值为302而不是401！成功进入路由器后台，查看路由器配置

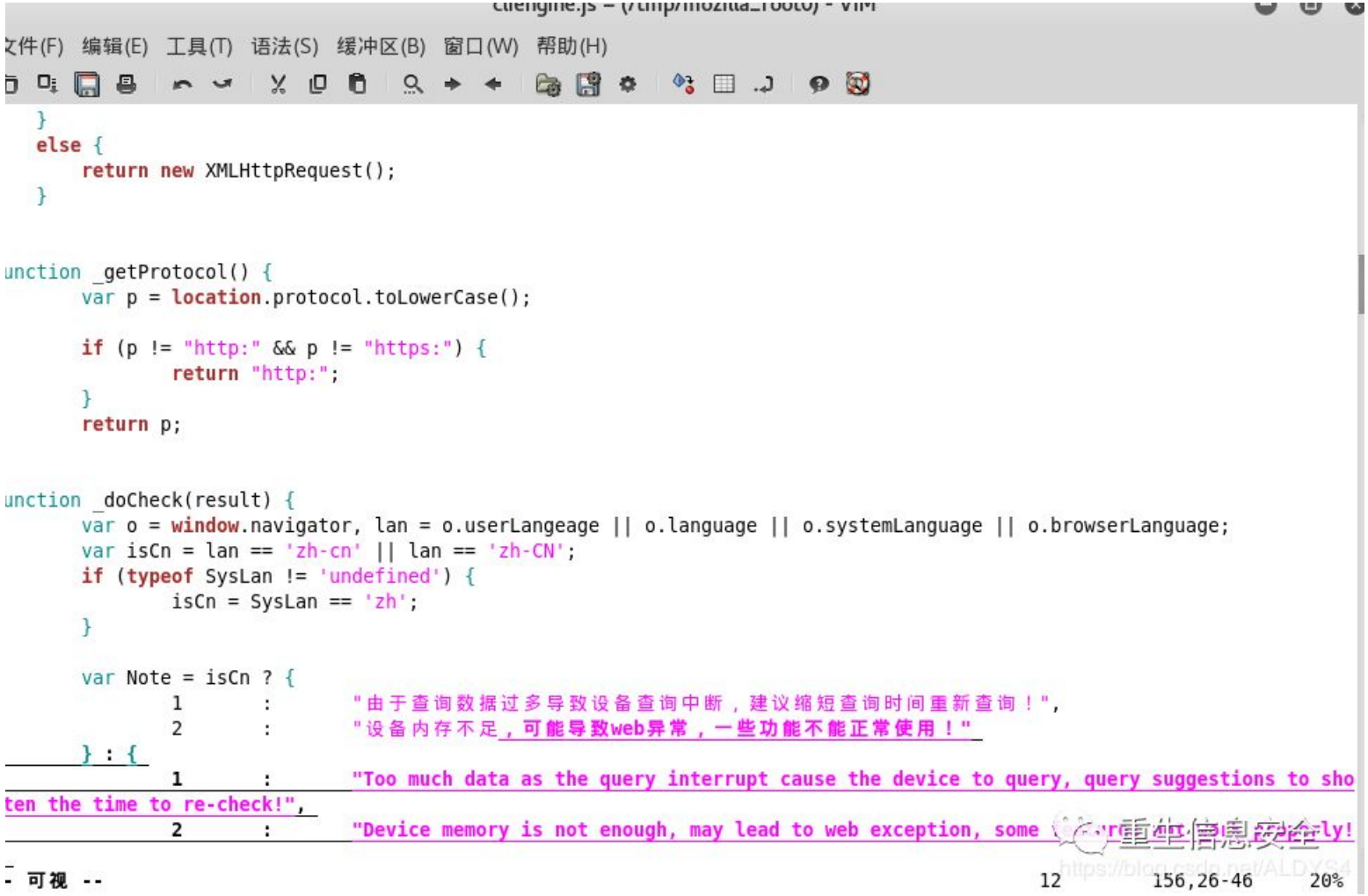


15）发现Telnet密码为qz123456，当然qz是我们学校的缩写啦，关闭路由器防dos措施和arp欺骗过滤。

16）再次使用nmap扫描，发现了心脏出血漏洞，css注入漏洞，apache畸形请求导致反射攻击的漏洞也出来了。



17）我甚至还利用openssl漏洞dump到了内部js文件



不过拿到权限后就没什么用了

0x006

第六步：继续挖掘_渗透学校防火墙

1）只获得这么一点点小成就的我怎么可能满足！

2）回头查看nmap扫描结果时发现请求再次被不断发送到了192.168.100.253

3）根据之前的经验，192.168.100.253一定做了防护措施，先不进行nmap扫描，避免打草惊蛇

4）直接打开https://192.168.100.253，果不其然！！

5）是SANGFOR防火墙！而且还是2016年的版本！我企图用之前渗透路由器的蠢办法绕过验证，可惜不行，尝试sql注入 仍然不行！总之就是用尽了各种方法都无济于事 😔 。

然后我就放弃了当天的渗透测试

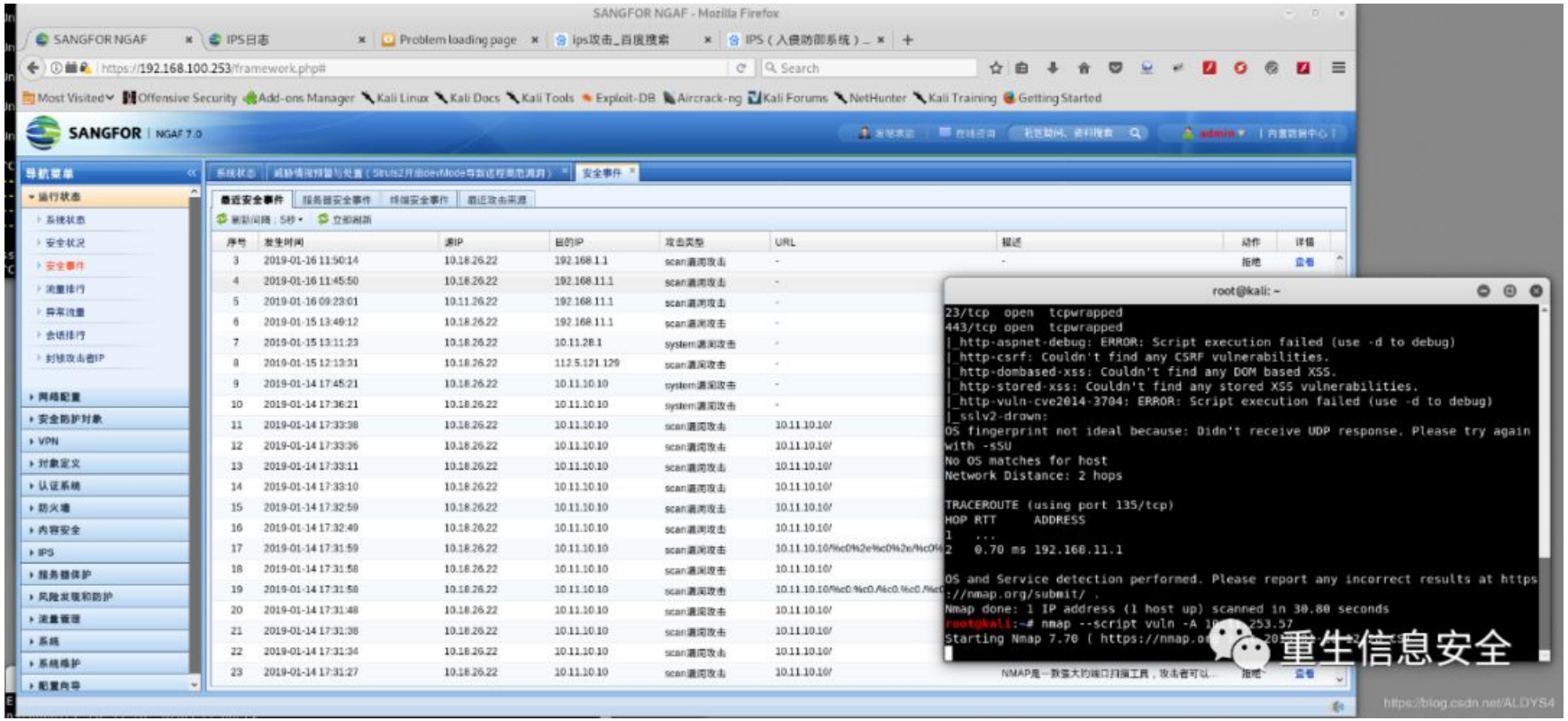
回宿舍睡觉时翻来覆去就是睡不着

果然不拿到权限就是心痒痒！ ！

6)如果渗透不成，就猜密码！刚要睡着，发现之前渗透路由器的时候

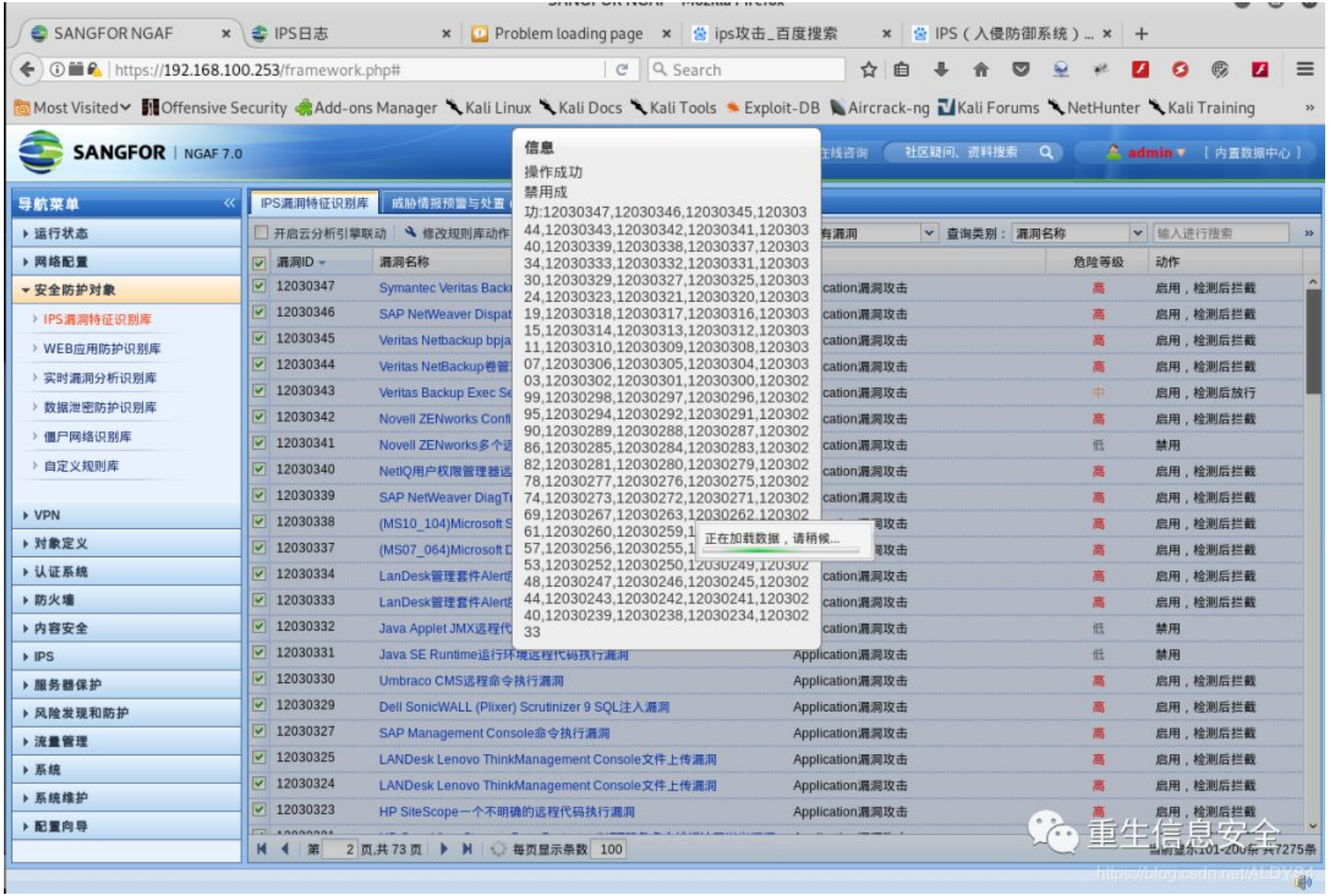
看到Telnet的密码是qz123456.

7)第二天中午时我打开电脑，尝试输入这个密码,回车！



8)登入成功！发现我之前的扫描记录和system攻击全部被记录在防火墙里了！

9)所有的安全策略全部禁用,并且允许445端口开放



0x007

第七步：进一步挖掘_拿到302台主机shell

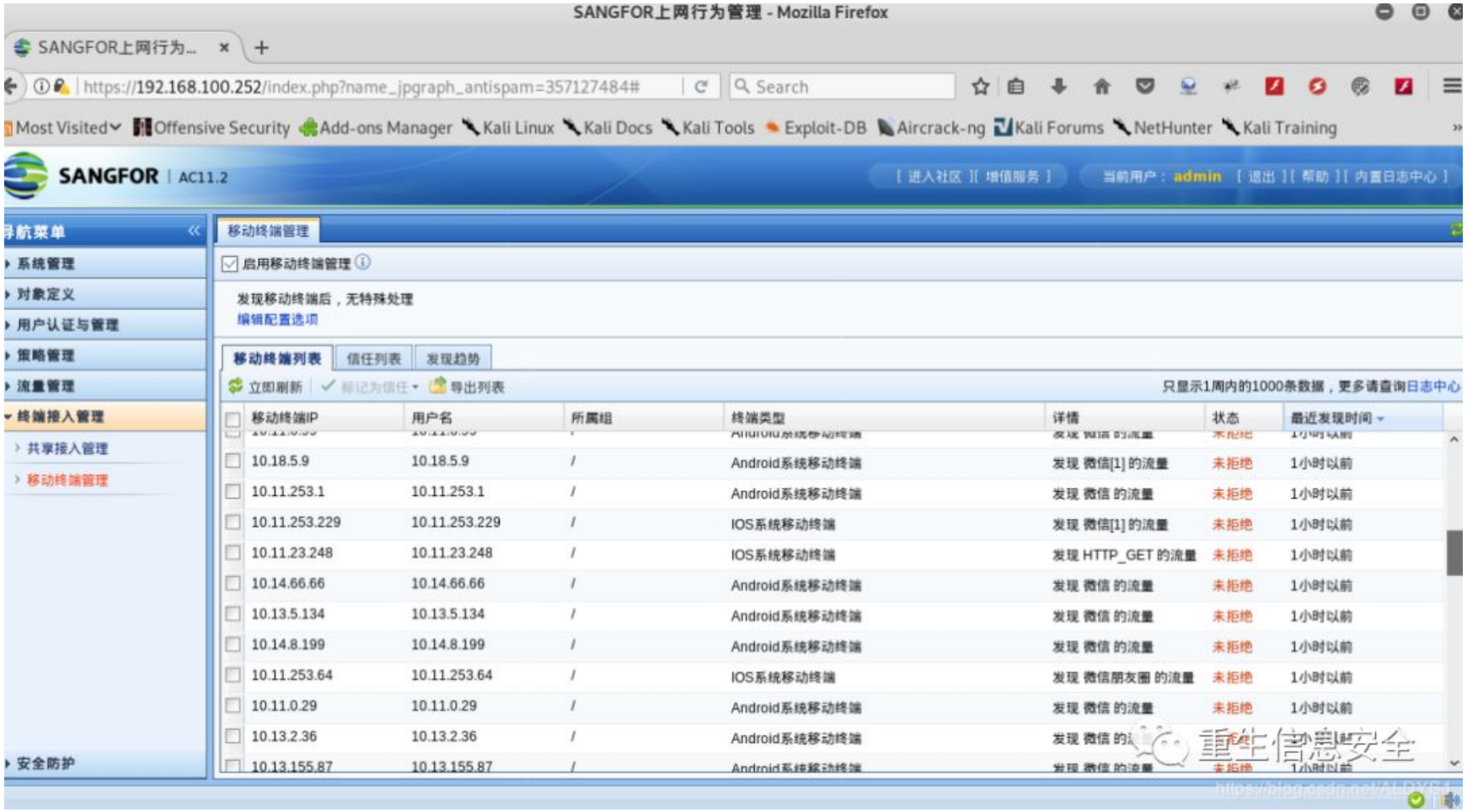
1)按照学校安排服务器地址的习惯,应该有其他类似防火墙的主机

2)我尝试了https://192.168.100.252,结果真的打开了，是行为控制模块

密码仍然是

-

qz123456



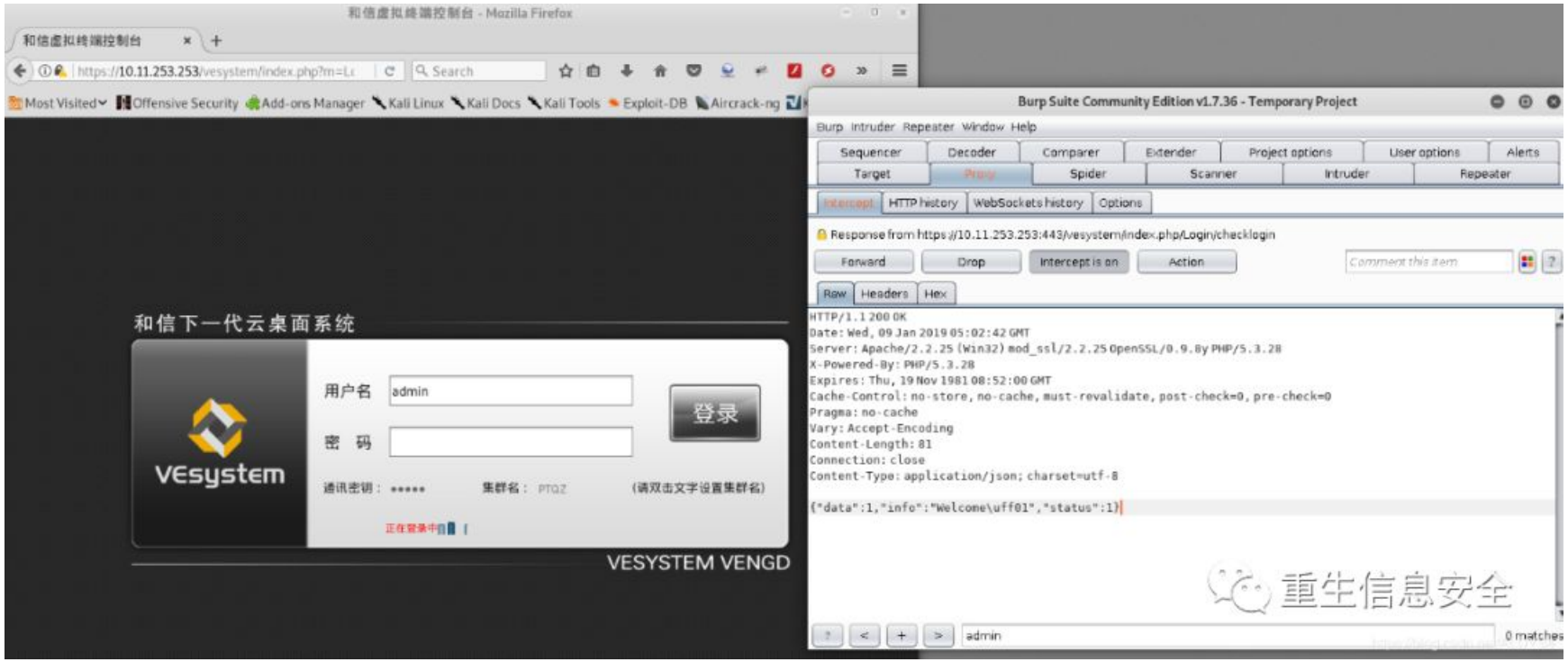
3)按照这个规律,那么之前发现的H3C交换器地址是10.11.254.254

猜测应该会有服务器在10.11.254.254之前

-
-
-
-

ping 10.11.254.253超时ping 10.11.253.253ping通了！

4)尝试打开https://10.11.253.253



5)是和信虚拟终端控制系统

-
-
-

首先尝试弱口令admin，不行！尝试了qz123456这个密码，不行！试着改response绕过验证，也不行！

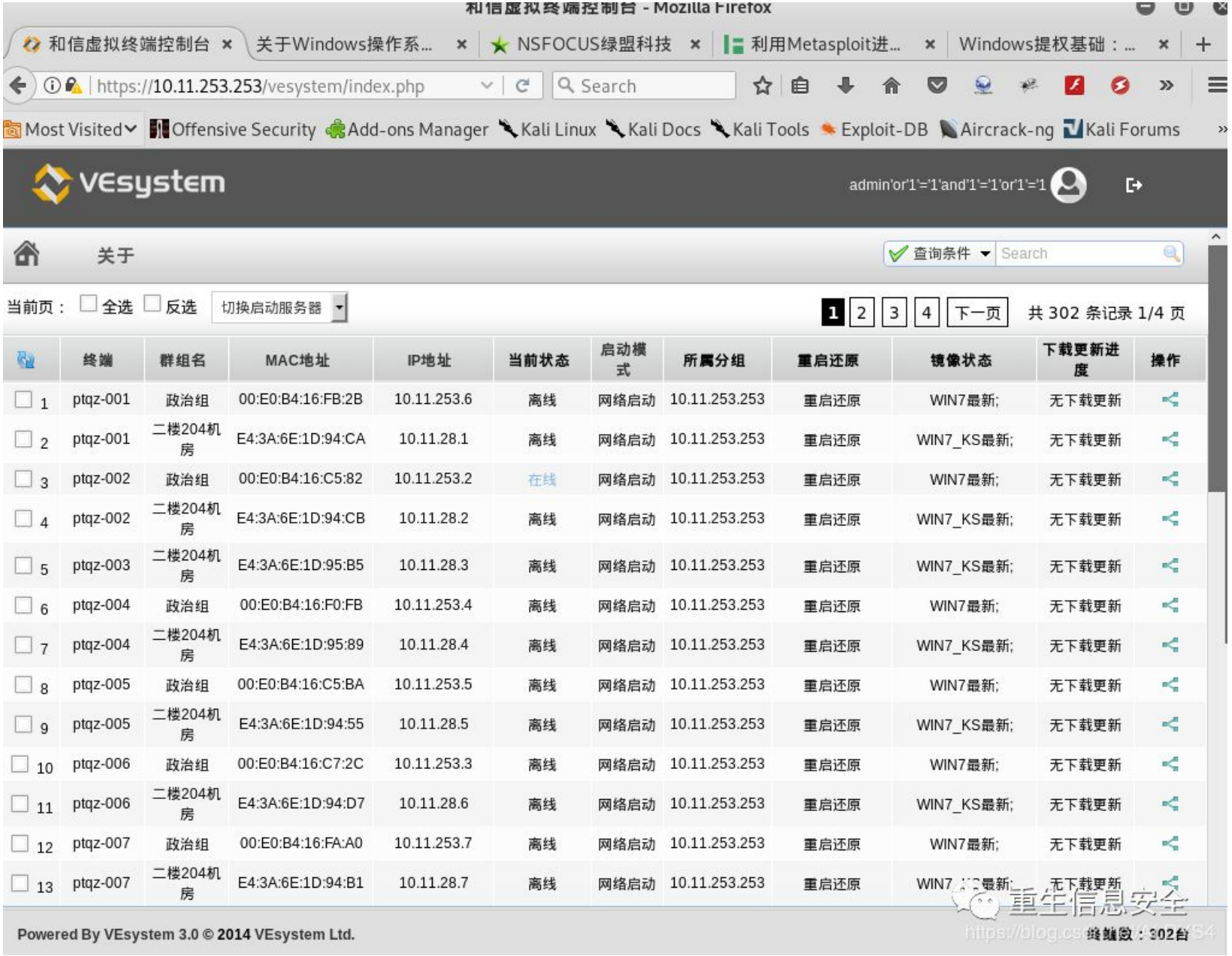
6)百般无奈之际，手欠的我不小心多写了一个单引号'回车！报错！

7)我的直觉告诉我有sql注入点！

-

username=admin'or'1'='1'and'1'='1'or'1'='1

8)利用or语句的优先级绕过password的判断



	终端	群组名	MAC地址	IP地址	当前状态	启动模式	所属分组	重启还原	镜像状态	下载更新进度	操作
1	ptqz-001	政治组	00:E0:B4:16:FB:2B	10.11.253.6	离线	网络启动	10.11.253.253	重启还原	WIN7最新;	无下载更新	
2	ptqz-001	二楼204机房	E4:3A:6E:1D:94:CA	10.11.28.1	离线	网络启动	10.11.253.253	重启还原	WIN7_KS最新;	无下载更新	
3	ptqz-002	政治组	00:E0:B4:16:C5:82	10.11.253.2	在线	网络启动	10.11.253.253	重启还原	WIN7最新;	无下载更新	
4	ptqz-002	二楼204机房	E4:3A:6E:1D:94:CB	10.11.28.2	离线	网络启动	10.11.253.253	重启还原	WIN7_KS最新;	无下载更新	
5	ptqz-003	二楼204机房	E4:3A:6E:1D:95:B5	10.11.28.3	离线	网络启动	10.11.253.253	重启还原	WIN7_KS最新;	无下载更新	
6	ptqz-004	政治组	00:E0:B4:16:F0:FB	10.11.253.4	离线	网络启动	10.11.253.253	重启还原	WIN7最新;	无下载更新	
7	ptqz-004	二楼204机房	E4:3A:6E:1D:95:89	10.11.28.4	离线	网络启动	10.11.253.253	重启还原	WIN7_KS最新;	无下载更新	
8	ptqz-005	政治组	00:E0:B4:16:C5:BA	10.11.253.5	离线	网络启动	10.11.253.253	重启还原	WIN7最新;	无下载更新	
9	ptqz-005	二楼204机房	E4:3A:6E:1D:94:55	10.11.28.5	离线	网络启动	10.11.253.253	重启还原	WIN7_KS最新;	无下载更新	
10	ptqz-006	政治组	00:E0:B4:16:C7:2C	10.11.253.3	离线	网络启动	10.11.253.253	重启还原	WIN7最新;	无下载更新	
11	ptqz-006	二楼204机房	E4:3A:6E:1D:94:D7	10.11.28.6	离线	网络启动	10.11.253.253	重启还原	WIN7_KS最新;	无下载更新	
12	ptqz-007	政治组	00:E0:B4:16:FA:A0	10.11.253.7	离线	网络启动	10.11.253.253	重启还原	WIN7最新;	无下载更新	
13	ptqz-007	二楼204机房	E4:3A:6E:1D:94:B1	10.11.28.7	离线	网络启动	10.11.253.253	重启还原	WIN7_KS最新;	无下载更新	

9)成功登入！一看，乖乖，这个vesystem系统掌管着302台主机！

10)而且可以查看每台机子的详细信息，甚至可以监控画面，上传文件！

0x008

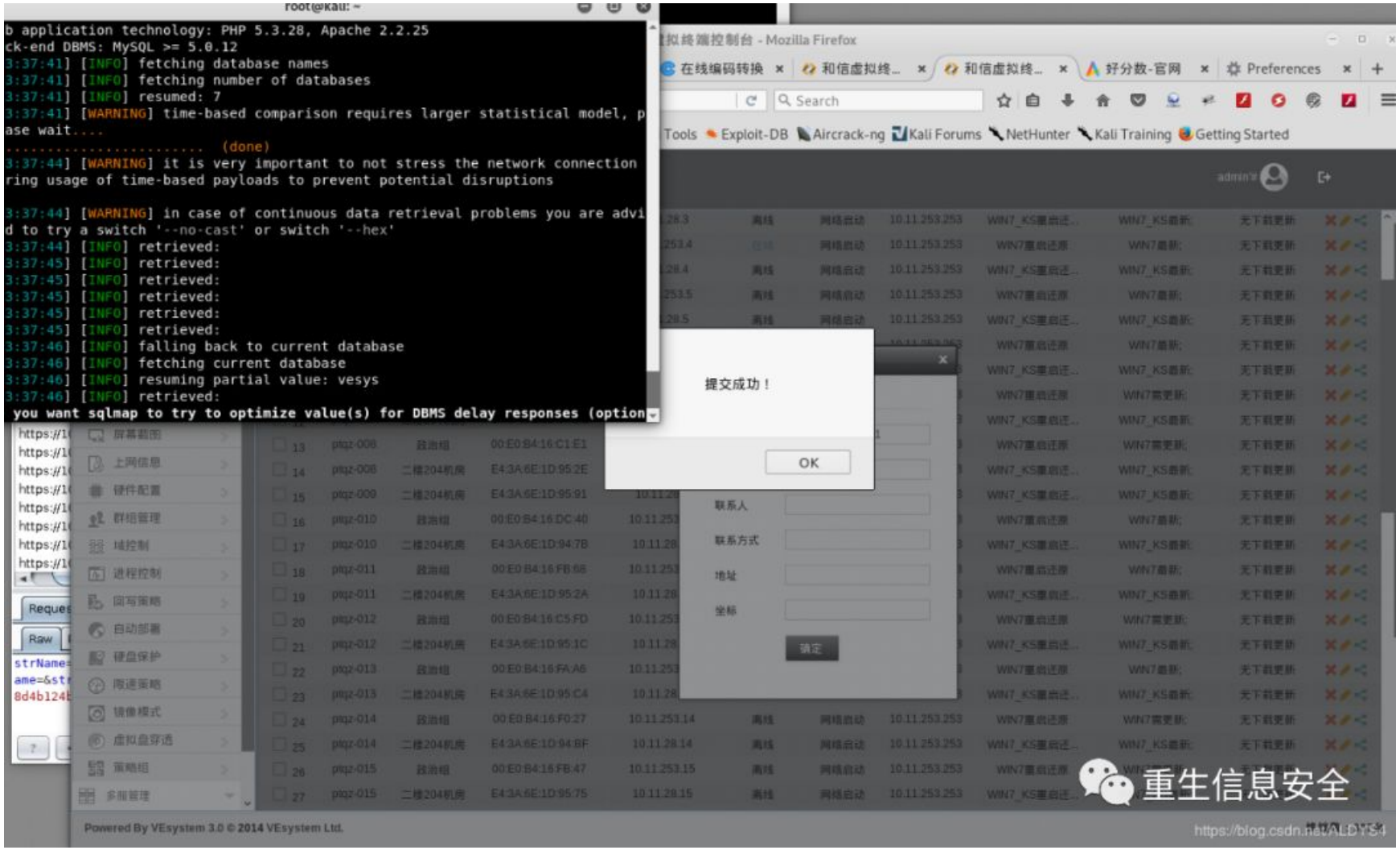
第八步：挖掘和信系统的注入漏洞

1)在不断测试的过程中，我发现和信系统在修改服务器信息时存在sql注射漏洞

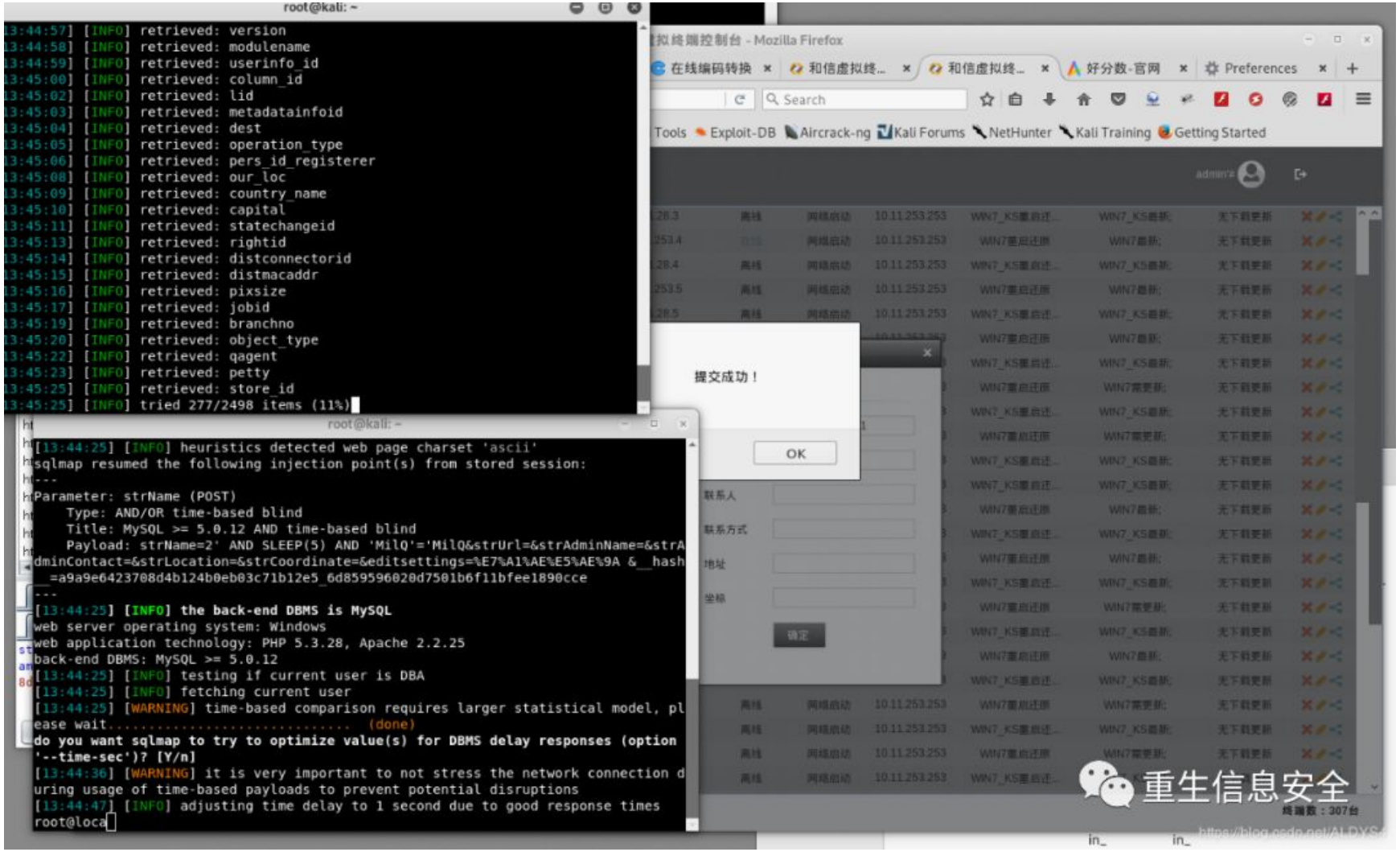
-
-
-
-

-
-

strName=1回车，成功修改strName=1’修改失败，无疑是因为单引号引起的闭合错误strName=1’and’1’='1修改成功!



2)果断丢sqlmap里，并带上–no-cast参数，因为我通过注入发现某些表是16进制的格式



3)爆出数据，查看password列

-

qz1234567

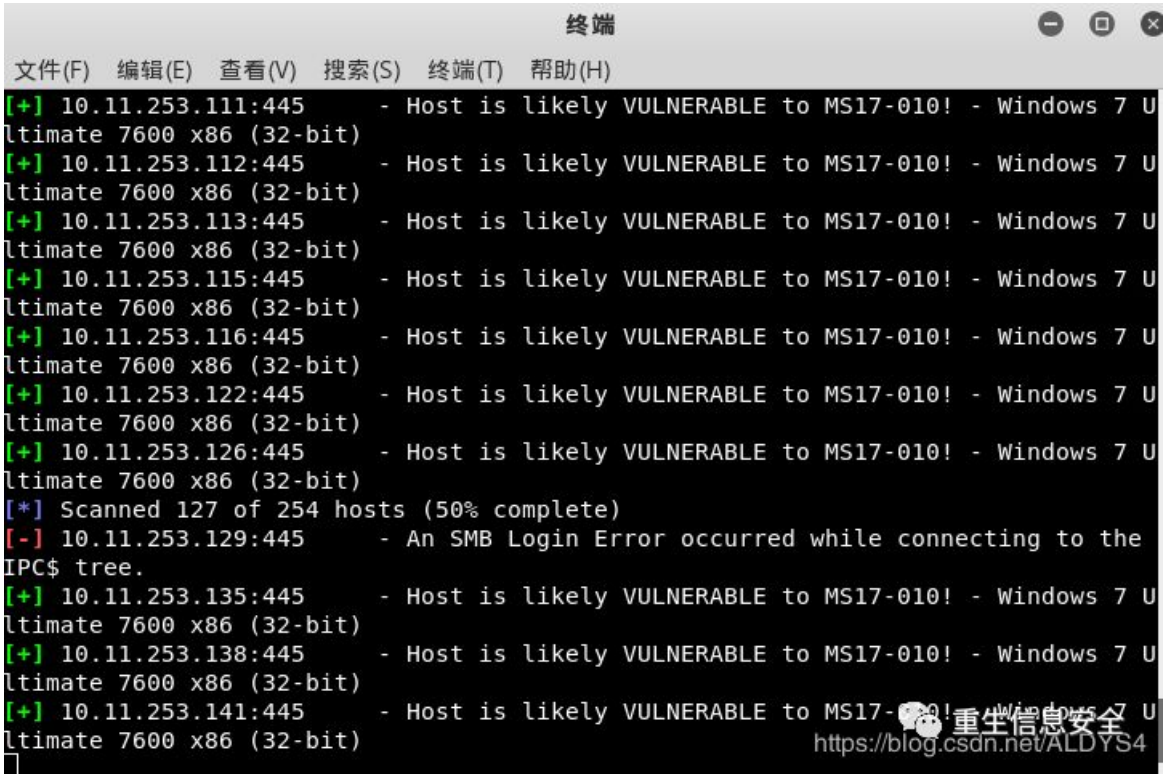
比之前的密码多了个7我tm。。。

0x009

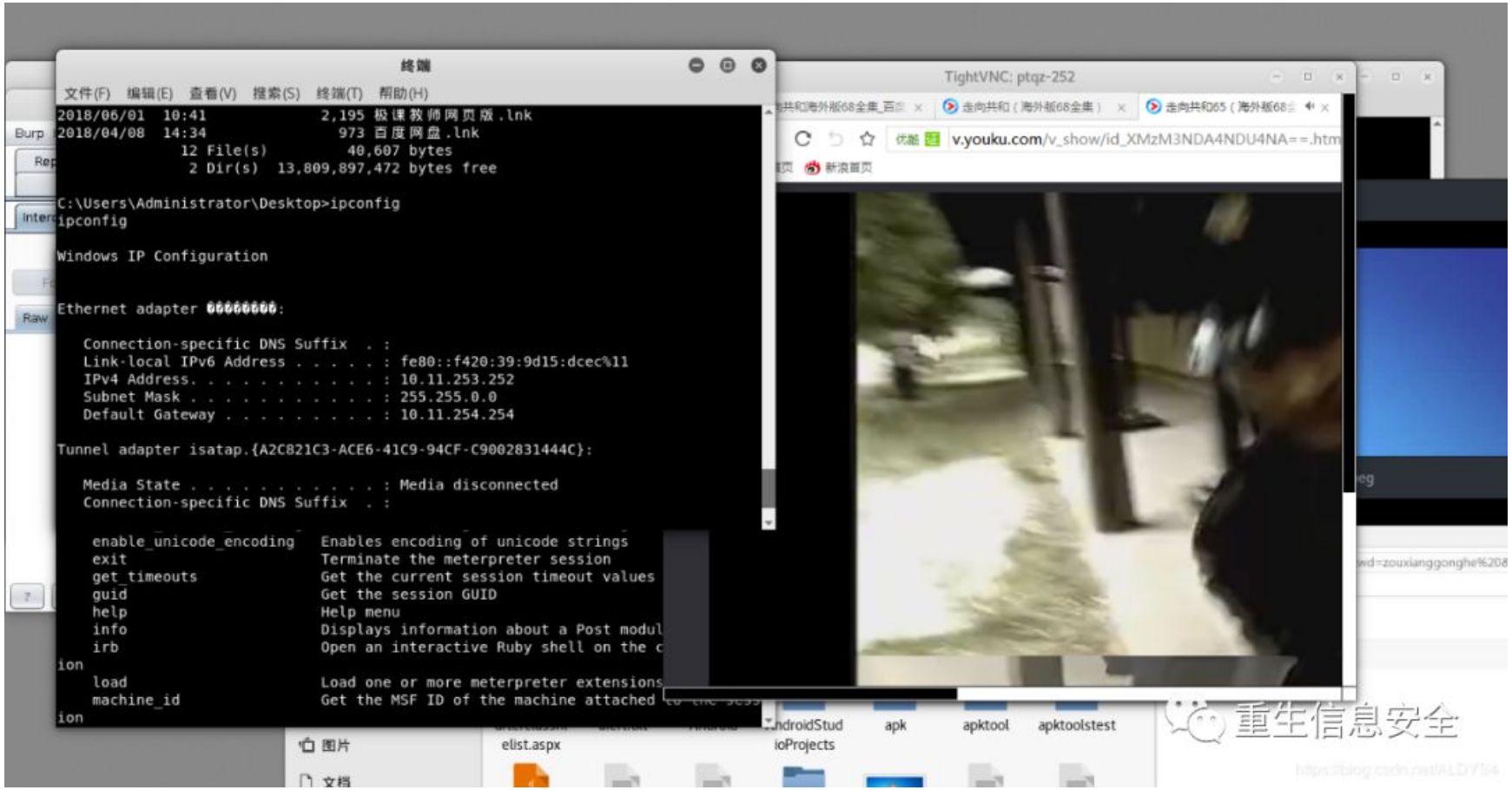
第九步：挖掘傀儡机信息

1)因为在之前的渗透中关闭了防火墙，禁用所有对smb之类的安全策略,拿到了和信服务器,渗透过程更加轻松了

2)nmap扫描在和信系统里发现的终端



3)我的天！这是挖到金矿了吗？！我找到我们班主任的电脑ms17010,boom!



4)在看电视剧。。。不管了，先查看硬盘,发现一份关于心理健康查询的网站

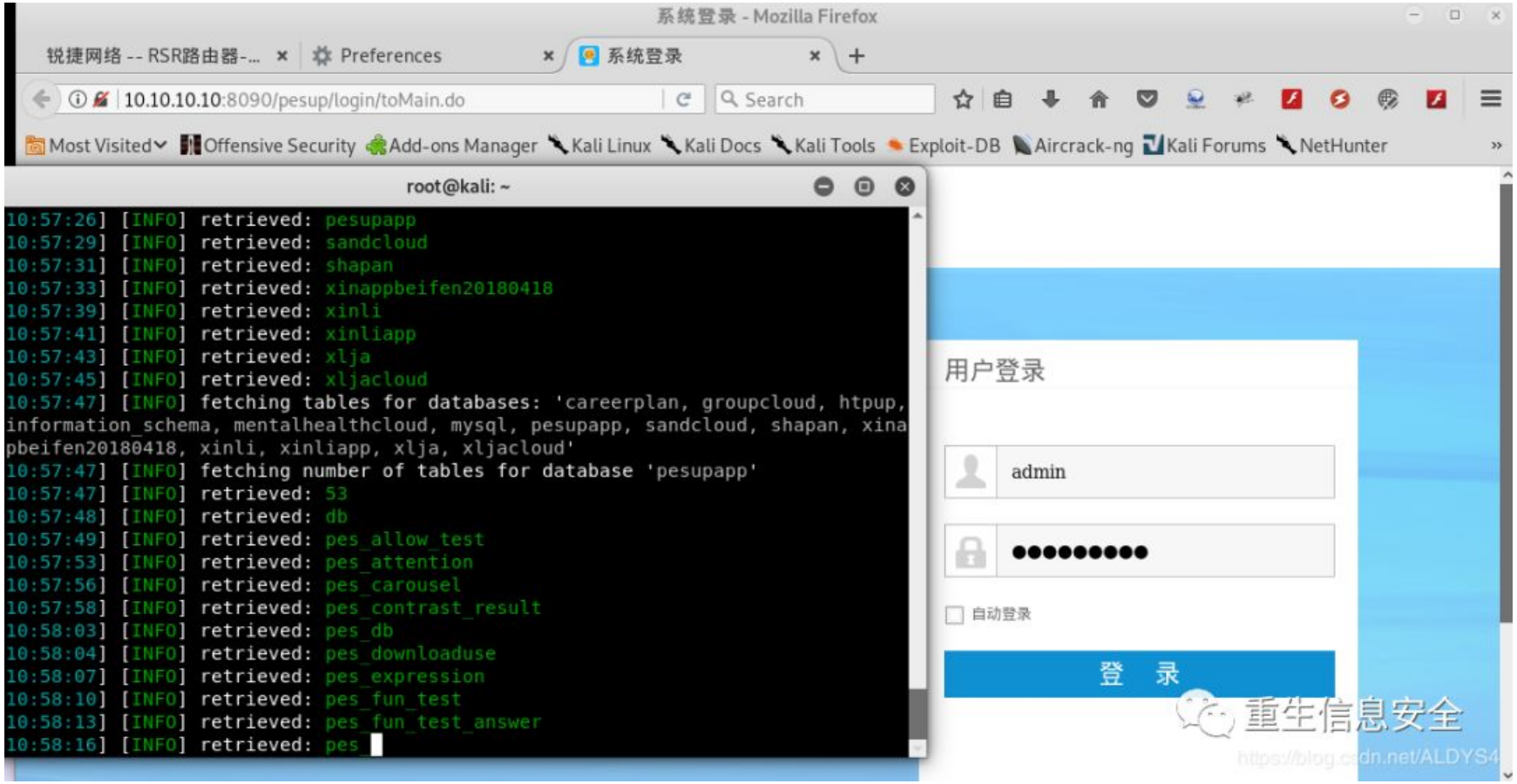
一看

-

内网10.10.10.10

5)我还寻思着着不就是上次被我绕waf给xss注入了的网站么。。因为没什么利用价值所以这里就不讲了

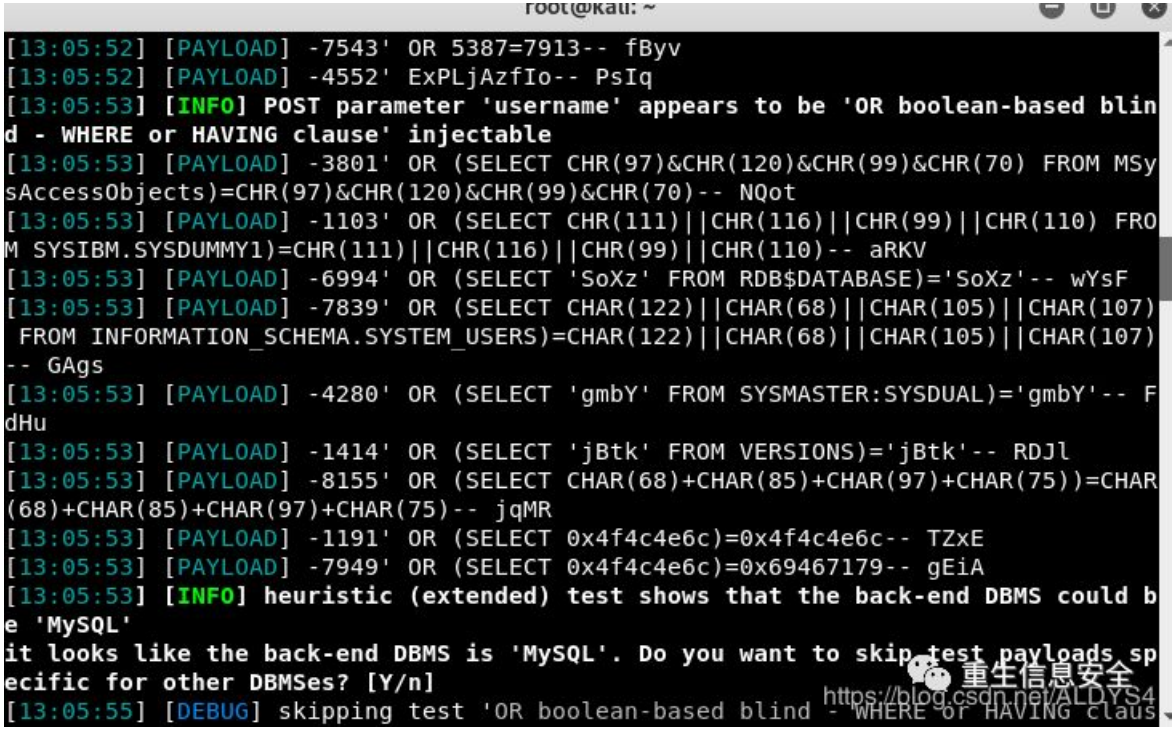
6)重点是这个地址的8090端口才是进行心理健康查询的



7)这个网站进行了一些过滤,经过测试,过滤了%#&'"/等等字符串,且对大小写敏感,所以payload:

-

```
username=admin’AnD '1’Like '1
```

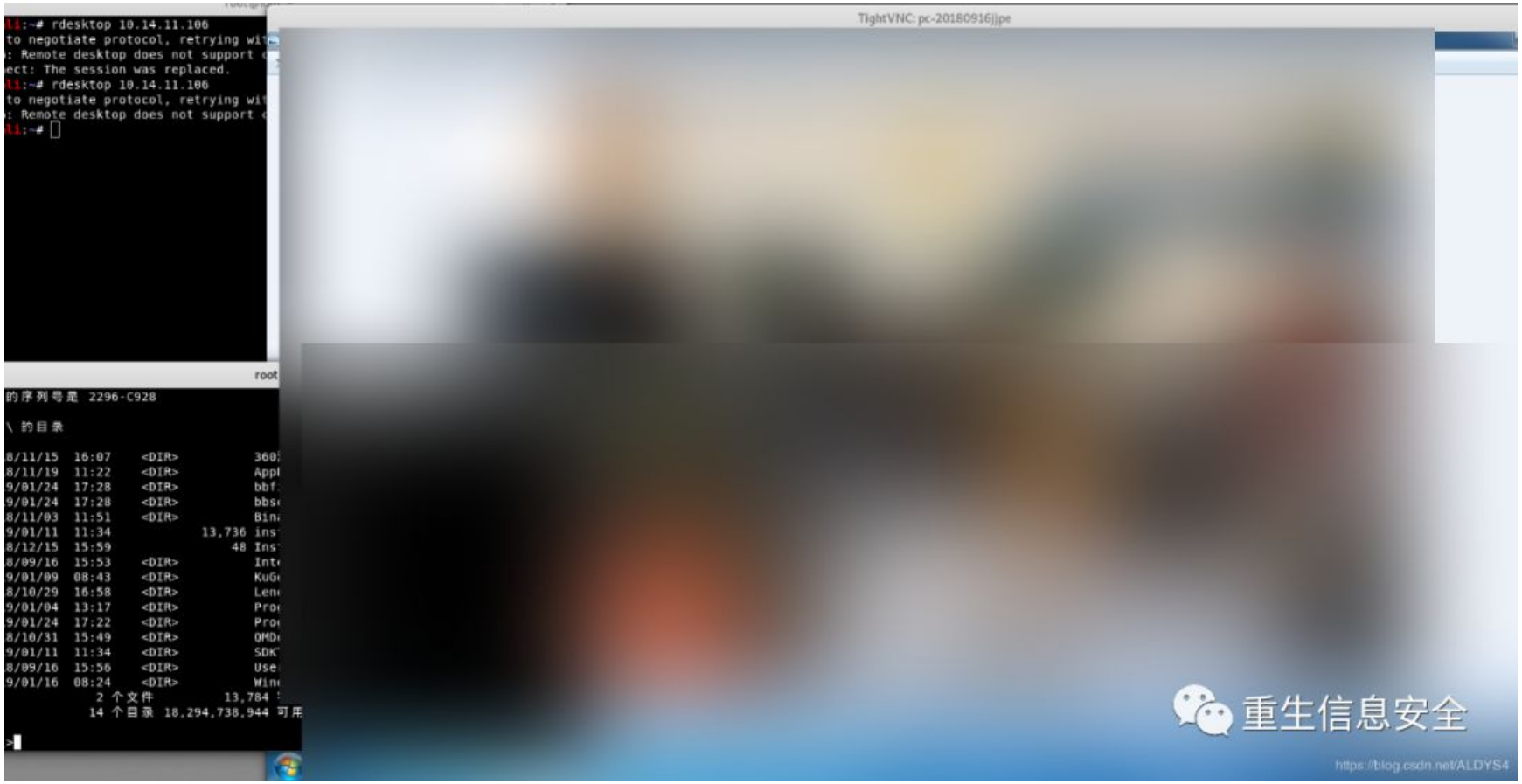


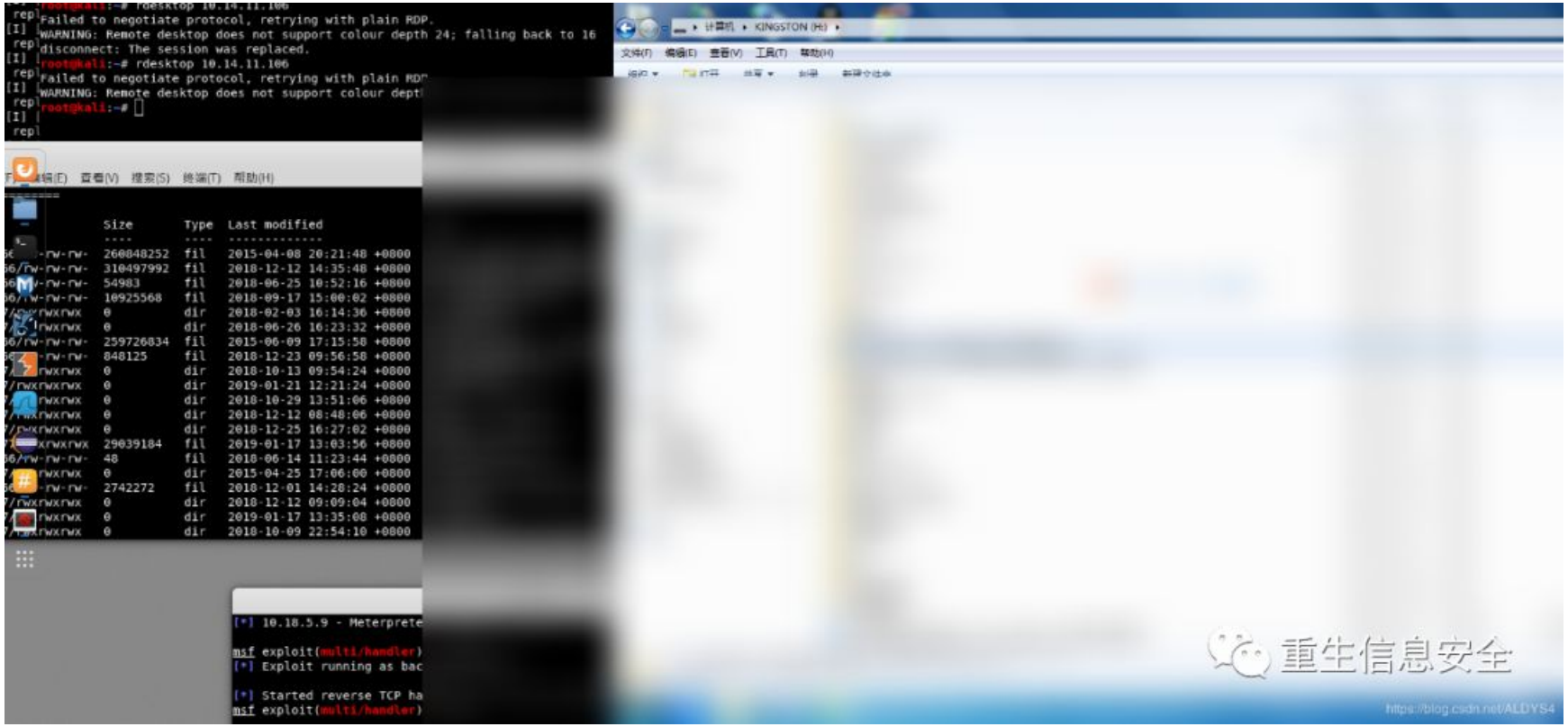
8)这里有意思的是,挖出的内容都是一些关于心理健康测试的题目和考试规范之类的

0x010

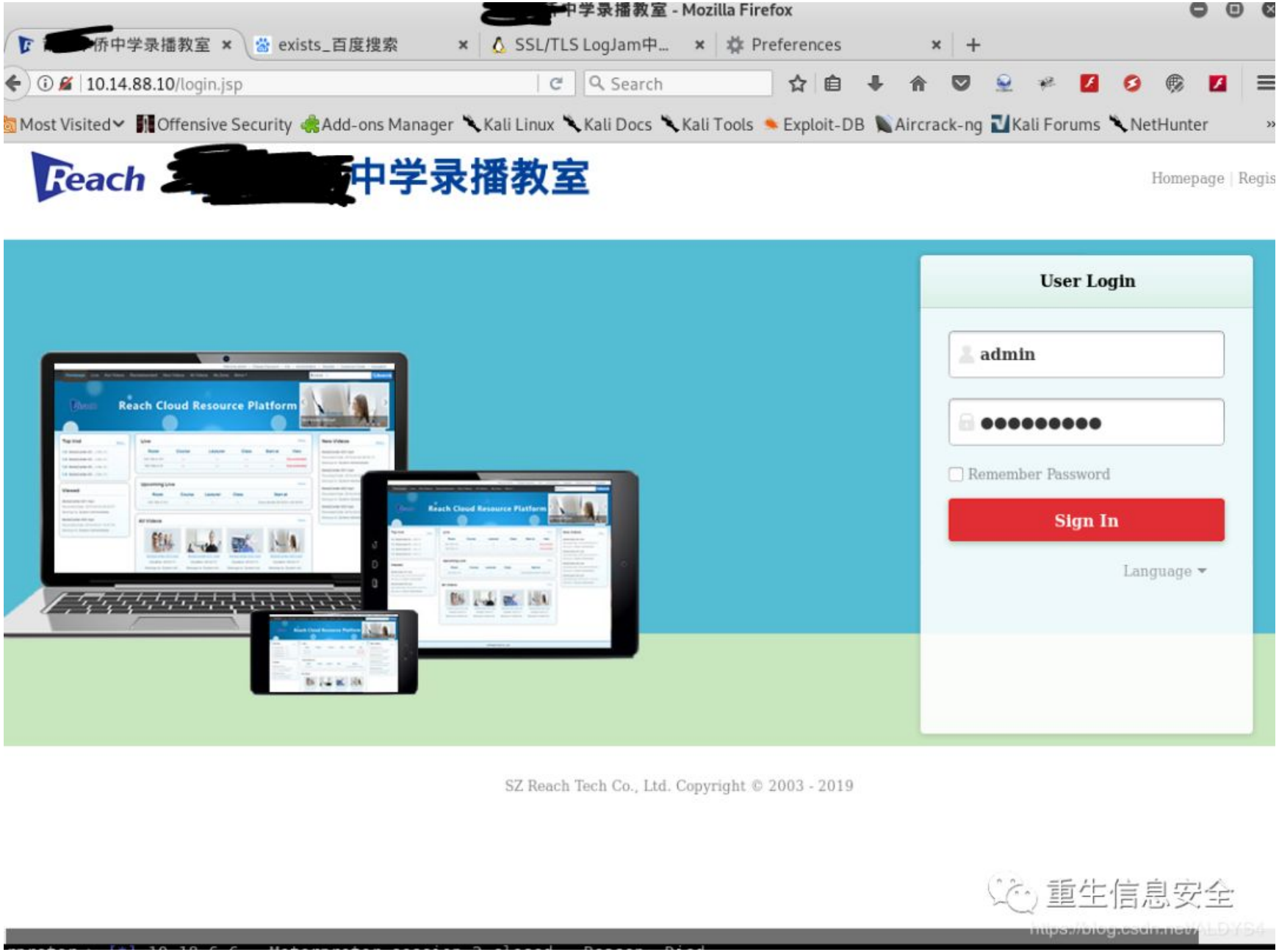
第十步：对一些傀儡机收集信息

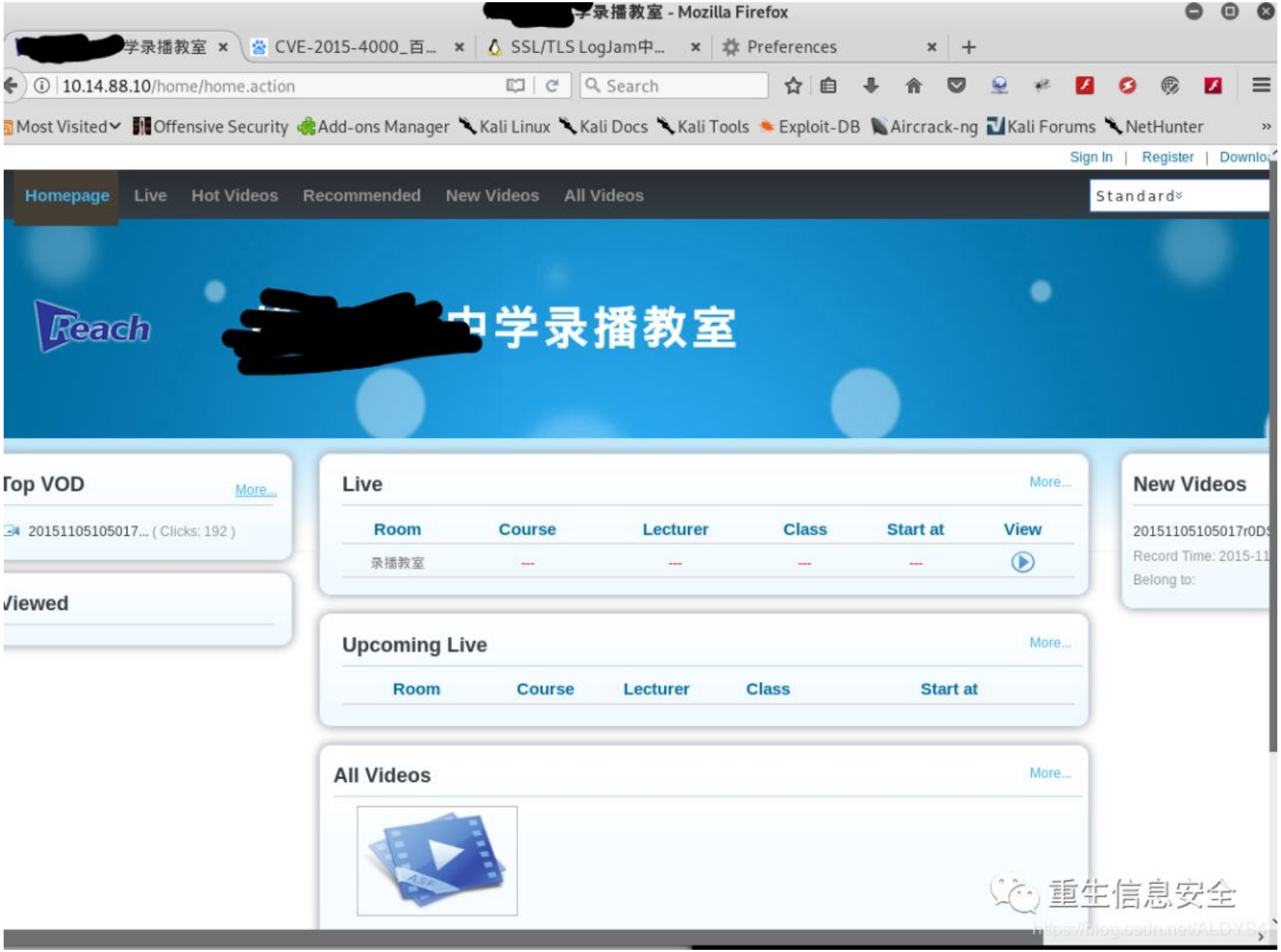
1) 这部分就可以略讲了
比如教师在登入某些设备时cookie被我抓到


TightVNC: pc-20180916jjpe
root
的序列号是 2296-C928
\ 的目录
重生信息安全
https://blog.csdn.net/ALDYS4



2)接着顺藤摸瓜把学校广播站日了,弱口令，没什么好讲的


中学录播教室 - Mozilla Firefox
exists_百度搜索
SSL/TLS LogJam中...
Preferences
10.14.88.10/login.jsp
Search
Most Visited
Offensive Security
Add-ons Manager
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Reach
中学录播教室
Homepage | Regis
Reach Cloud Resource Platform
User Login
admin
Remember Password
Sign In
Language
SZ Reach Tech Co., Ltd. Copyright © 2003 - 2019
重生信息安全



3)记录渗透成果,加上教学楼傀儡机和办公楼的主机,算了一下，472台权限 ps;好了不说了该总结总结报告给老师了 😁


长按识别二维码关注我们