linux攻防比赛_CTF线下赛-AWD 参赛指南

原创

傅一一 于 2021-01-13 11:44:23 发布 1928 收藏 7
文章标签： linux攻防比赛

本文链接：https://blog.csdn.net/weixin_42317626/article/details/112883528

AWD参赛指南：

01. 赛制流程：攻防模式(AWD)常见于线下攻防。

一般比赛的具体环境会在开赛前半个小时由比赛主办方给出，前半个小时应熟悉配置环境。准备网线、网线转接口。

最好的防御就是攻击，不做好安全加固就会被吊打。

02. 赛前准备：

常用工具：(整理适合自己的)Burpsuite

sqlmap

nmap、masscan

nc

Chrome、Firefox各类插件

一句话木马：php

asp

aspx

jsp

内存马

py库、脚本：pwntools

requests

软waf

日志分析

Exp

SSH客户端：PuTTY

XShell

编辑器：Sublime

VS Code

Notepad++

Vim

个人知识库

常见应用源码库

Writeup集合

基础知识：语言运用：编写自动化脚本等……

WEB安全：熟悉常见漏洞类型、常见框架……

pwn型：需要较好的底层基础、懂汇编等，需要理解各种堆栈溢出的原理、基础密码学……

中间件：apache、nginx、tomcat、jboss、weblogic

语言基础：php、java、python

常见web应用：phpmyadmin、dedecms、phpcms、帝国cms、Discuz

linux命令：netstat -tulpn 、ps -ef

Gamebox:系统：ubuntu、centos

中间件、版本：apache \ nginx

php \ php-fpm

tomcat \ jboss \ weblogic

web程序

数据库：MySQL \ MariaDB \ Oracle

Redis \ MongoDB

03. 常见加固方式：

加固流程：修改网站管理员密码

备份网站源码tar -zcf /tmp/name.tar.gz /path/web

tar -zcf /tmp/name.tar.gz /var/www/html

备份数据库mysqldump -u 用户名 -p 数据库名 > 导出的文件名

mysqldump -u user -p database > /tmp/database.sql

修改ssh密码(即修改当前用户密码)

修改MySQL密码set password for 用户名@localhost = password('新密码');

set password for user@localhost = password('123');

修改MongoDB密码(27017端口)

修改Redis密码(6379端口)

修改网站源码中的数据库连接配置

部署waf(视情况而定)准备一个软waf

如何使用phpwaf.php找到CMS/框架通用配置文件进行包含：PHPCMS V9：\phpcms\base.php

PHPWIND8.7：\data\sql_config.php

DEDECMS5.7：\data\common.inc.php

DiscuzX2：\config\config_global.php

WordPress：\wp-config.php

Metinfo：\include\head.php

修改php.ini文件后重启(高权限):禁用敏感函数：

disable_functions =
system,exec,shell_exec,passthru,proc_open,proc_close,proc_get_status,checkdnsrr,getmxrr,getservbyname,ge
syslog,popen,show_source,highlight_file,dl,socket_listen,socket_create,socket_bind,socket_accept,
socket_connect, stream_socket_server, stream_socket_accept,stream_socket_client,ftp_connect,
ftp_login,ftp_pasv,ftp_get,sys_getloadavg,disk_total_space,
disk_free_space,posix_ctermid,posix_get_last_error,posix_getcwd, posix_getegid,posix_geteuid,posix_getgid,
posix_getgrgid,posix_getgrnam,posix_getgroups,posix_getlogin,posix_getpgid,posix_getpgrp,posix_getpid,posi
posix_getrlimit, posix_getsid,posix_getuid,posix_isatty,
posix_kill,posix_mkfifo,posix_setegid,posix_seteuid,posix_setgid,
posix_setpgid,posix_setsid,posix_setuid,posix_strerror,posix_times,posix_ttyname,posix_uname

自动包含waf：

auto_prepend_file = safe.php路径;

分析日志文件

文件监控准备一个脚本，监控并删除所有新增文件。

发现内存马，直接重启php。

若监控脚本无法使用，使用命令定期查看新增与修改文件。

find web路径 -ctime -1 (查看最近一日新增的文件，是否可疑)

修改目录权限：(可能会违规)chmod -R 644 www

04.攻防演练：

如何获得flag?

在实际比赛中，一般有两种方式获取flag，一种是先获取webshell权限，然后去读flag文件，另一种则是直接通过漏洞读取flag文件。Getshell：官方后门、文件上传

文件写入、文件包含

命令注入、反序列化

Redis写shell

Mysql写shell

直接读文件：SSRF

任意文件读取

XXE

文件包含

Sqli

1. web后门：

在任意APP的某个文件的源码中加上一句话后门。@eval($_POST['XXX']);

@assert($_POST['XXX']);

system($_REQUEST['CMD']);

对于这种类型的漏洞，只要用正则遍历匹配就能找到

grep -r "eval\(\$_"

或者还有一些复杂变异的后门，这种情况就可以选择使用D盾Webshell查杀或者SafeDog之类的工具对源码进行扫描。只要删掉就可以解决。

2. 系统后门NC后门

SSH后门

suid后门

3. webshell：内存马：不断生成shell文件

Webshell密码：给Webshell增加密码，增加一个password参数MD5

4. 文件上传：一般上传：各种绕过方式一定要熟悉

常见改包、解析漏洞、图片渲染、逻辑文件(双文件上传)、条件竞争

防护方式——白名单、禁止上传目录执行权限、上传于Web目录外

5. 文件写入：缓存：存在缓存机制，后缀名为php，直接代码执行。

-配置文件：单引号内：输入单引号，尝试逃逸。如'+@phpinfo()+'

双引号内：输入会被解析的符号。如${@phpinfo()}

模板文件：模板被包含，getshell。

创建新文件时无校验后缀名。

日志：日志以php后缀保存，X-Forwarded-For来伪造ip植入木马。

6. 命令注入/反序列化：

PHP中使用unserialize函数对数据进行反序列化，反序列化过程类的__wakeup方法与__destruct方法会被调用。

7. 文件读取：SSRF：存在服务器请求伪造漏洞时，可使用file协议读取本地文件。

http://127.0.0.1/read.php?url=file:///flag

SQL注入：目标存在SQL注入时，可尝试直接读取flag。

常规注入、盲注、二次注入、insert注入、http头注入

读取

select load_file()

写入

select outfile()

select dumpfile()

8. 困难漏洞：

有时候出题者会直接丢一个0day，现场审计。

找不到漏洞没关系，上Waf保平安，时刻关注你的日志记录，NPC也会打出攻击流量。

找到别人写在自己服务器上的shell，一般其他服务器也会有，可以去留后门。

Collected by 此名如此彪悍

相关