×00

好久好久没写东西了 中间其实想发两篇省赛的 writeup 的 可是环境没开 要等之后再次开放我会补上两篇 大概 9 月的时候

这次是去了西电去参加的电赛 和 h3ll0m4n 还有 whitesilt 一起去动态演示 也就是搞站 还有琪琪去做软件 一起去玩耍

比赛是持续了 24 个小时 从早上 9 点到次日 9 点 关在小黑屋里 全封闭的模式 还有手机屏蔽的装置 手机也没法用 比赛很接近于实战 都是拿靶机的形式 比赛限制了外网 只有几台机子有外网 需要外网时 要计时 超时要扣分 flag 分为几种 100 200 500 提交 flag 还要写上报告

0×01 寻找靶机

比赛一开始就没有进展 一开始 9 点的时候 只是宣布了比赛开始 然后也没有指定靶机什么的 需要我们自己去寻找靶机目标 接入网络之后 自动分配的网段是在 169.254 的网段，然后我们的思路 自然就是寻找存活的靶机 可是 用 nmap 扫了整个网段也没法发现什么 就发现了 4 台机器 3 台是我们的自己的 还有一台也没发现什么 估计是网关之类的

还去扫描的一些内网的网段 比如 10.10 还有 192.168 等 但是也没有什么发现 就这样子一个小时多已经过去了 10 点多 除了杭电的大神 大家还是没有什么进展 这时候竞赛组公布了一个新的提示 提示说要靠嗅探寻找靶机 既然说要嗅探 我就开了 cain 试了一下 发现没有什么效果 就用 wireshark 来抓了一会包观察了一下 因为中间还有我们自己还在扫描 有些噪声 后来把那些 nmap 停了之后 再去 wireshark 抓包 就比较好观察了

抓包发现了 有一个 10.10.0.102 的地址 在发 10.10.0.254 的 ARP 包 然后我们就发现了这个奇怪的 ip 10.10.0.102 和 10.10.0.254 直接访问上去 发现没有什么 然后改了同一段的 ip 设置好掩码 h3ll0m4n 发现 ip 冲突了 这说明这个 ip 是之前有人占用着的 就是这个了 需要修改自己的本地网段 然后去访问。

发现了 10.10.0.101 存在了一个 80 端口 上面有一个 resourcespace 的 cms 这时也就是 11 点多的时候 主办方放出了靶机的 ip 的 base64 的加密的密文 是 10.10.0.100 到 10.10.0.103 这 4 台机子 总算是寻找到了目标 已经花去了两个小时

0×02 iis+oracle

10.10.0.100 这一台机子 上面的配置是 iis6.0 还有开放了 Oracle 的端口 80 端口并没有什么页面 只是一个建设中的提示 然后 oracle 的 我之前在省赛中遇到过这次又跪了 砸过 oracle 的漏洞 还去尝试爆破弱口令 没有尝试出来 比赛结束也没有从这台机子上得分 只有 kingdom 做出来了 最后比赛完 交流了一下 他告诉我 发现是 ms08067 的漏洞 还有 oracle 是 authkey 漏洞 我们一开始也砸过在 msf 里有 可能是参数没有弄对 或者是需要自己修改代码 最后没搞出来

0×03 resourcespace upload

10.10.0.101 这个机子比较好搞 上去不到一个小时 就拿下来了 他开放了 80 端口 上去我就到处翻翻文件 发现了有列目录的漏洞 可以列出来目录 然后就寻找那些敏感的网页 来尝试 发现了一个上传的页面：

http://10.10.0.101/pages/alternative_files.php 然后尝试上传了个 jpg 和 php 的 webshell 发现都没有回显 然后我就走了 又去到处翻翻 翻到

http://10.10.0.101/filestore/这个目录的时候 突然发现了我之前上传的那种图片 还有一个 php 文件 也就是之前上传的 webshell 得来全不费工夫 就这样子拿到的 webshell 在相同的目录下 有出题人原先放置的 flag 提交了一个 100 分
flag1：15e5c558baf869eaf90ba58a389e86f388b567c5

然后又去拿到 http://10.10.0.101/include/config.php 里面有数据库的密码

```
1 $mysql_server = 'localhost';
2 $mysql_username = 'root';
3 $mysql_password = 'toor@vm2';
4 $mysql_db = 'resourcespace';
```

然后用菜刀配置一下 连接上去看看 发现了 flag 数据库

里面有 flag2：4a91c640e55fadfa9a98ab4b67b71345021d22e4
再提交一个 200 分 这个题一共拿下了 300 分 这个题比较简单 基本都做出来了 可是他不能作为跳板 进入内网

0×04 openssh 5.3
10.10.0.102 这个 nmap 扫了一发 只开发了 22 端口 看了一下版本是 openssh5.3 的 然后就先测试了弱口令 还有 溢出之类的漏洞 网上找到了一个 openssh<=5.3 的远程溢出 没有利用成功 还有一直在尝试着爆破 没有成功

0×05 passwd
10.10.0.103 这个题做出来很莫名其妙的感觉 是一个 apache 的 web 容器 有一个 index.php 是空白的 我怀疑是个 webshell 就用 webshell 去爆破一下 没发现什么。然后就和其他的机器差不多 是一个 linux 的 开放了 22 的 openssh 服务 然后我们就去用 dirb 去扫目录 扫出来的结果是有一个文件的 test 的文件 上面只有 test 还有一个 passwd 的文件 上面一开始空白的 什么都没有 到了吃晚饭的时候 突然发现着上面居然有 linux root 密码 搞得我怀疑是别人溢出成功之后 没有及时删除留下来的 root password:pwn_skill_get

然后登上去后机智的吧 root 密码改了

可是后来才发现 原来是一个队伍一套环境 弄得我很尴尬 原来一直都在搞自己 啥都不说了 登陆上去之后 先找 flag 之类的文件 然后在 web 目录下面发现了一个 webshell 还有一个 exe 在/root/目录下 ls 看到了 flaginroot 文件 提示如下 pwn_pwn_pwn_done 提交之后获得 100 分

在 www 目录下发现了一个 flag 文件 reverse_win_32_done 也是 100 分 一共获得 500 分

尴尬的是 我们发现了那个 exe 之后 就让队伍里的逆向 whitesilt 去做 他做了好久 终于做出来了 才发现 居然是那个 webshell 的 url 能得到那个 url 这才是第一步吗 结果我们一开始就拿到了 root 密码 把中间的都跳过了 这时间也浪费了

[下载 alaaladingding.exe]

whitesilt 的代码

```
01 //10.10.0.103 逆向 alaaladingding.exe
02 #include <stdio.h>
03 #include <windows.h>
04
05 int main(void)
06 {
07          char key[] = {0x55, 0x8B, 0xEC, 0x83, 0xEC, 0x58, 0x53, 0x56, 0x57};
        char toxor[] =
{0x6B, 0x4C, 0xD2, 0xE8, 0x8E, 0x16, 0xBB, 0xC9, 0x1A, 0xF5, 0x25, 0x9D, 0xD4, 0x
93, 0x86, 0xD4, 0xEE, 0xBE, 0x50, 0xEB, 0x63, 0x44, 0xF4, 0x43, 0x16, 0x68, 0x70,
0x6A, 0xD8, 0x3D, 0xB3, 0x75, 0x05, 0xAD, 0x2F, 0xE7, 0x70, 0x79, 0x37, 0x1A, 0x4
1, 0x5D, 0x49, 0x31, 0xBB, 0xB1, 0x91, 0xF1, 0xBD, 0x20, 0x57, 0x7F, 0xE6, 0x70, 0
x5F, 0x47, 0xD2, 0x35, 0x82, 0x2C, 0x17, 0x4C, 0x90, 0x91, 0xD6, 0xB9, 0xC1, 0x23
, 0x7B, 0x88, 0x29, 0x01, 0x98, 0x0E, 0xA8, 0x5C, 0xCE, 0x58, 0xFC, 0xFA, 0x92, 0x
D5, 0xA6, 0x6E, 0xD6, 0x08, 0x41, 0xE7, 0x36, 0xA0, 0xB9, 0xDE, 0x85, 0xB3, 0xA1,
0x34, 0xF7, 0x02, 0x41, 0xE2, 0xEC, 0x95, 0x3A, 0x06, 0xB7, 0x0C, 0xE3, 0xA1, 0xB
E, 0x64, 0xF1, 0x71, 0xAE, 0x78, 0x9C, 0x26, 0x18, 0xAD, 0x85, 0x5E, 0x7B, 0x11, 0
x98, 0xF3, 0xCB, 0x23, 0x58, 0xA8, 0x9B, 0x2D, 0x19, 0xB5, 0x45, 0x9F, 0xAD, 0x90
, 0x63, 0xE4, 0x62, 0x33, 0x6F, 0xF7, 0x16, 0x62, 0x5D, 0x62, 0xEE, 0x74, 0x1F, 0x
E8, 0x09, 0x33, 0x86, 0xD4, 0xE9, 0x94, 0x29, 0x10, 0x69, 0x14, 0x67, 0x0D, 0x1A,
0x96, 0xAE, 0xF2, 0x14, 0x99, 0x90, 0x4D, 0x67, 0x0C, 0x52, 0xED, 0x4A, 0xED, 0x8
A, 0x6D, 0xC9, 0x7D, 0xE3, 0xD3, 0xF8, 0xFC, 0xE0, 0xC2, 0xEA, 0xD9, 0x88, 0x2F, 0
x23, 0x16, 0xAA, 0xD1, 0x09, 0x16, 0x0C, 0x5C, 0xB2, 0x0A, 0x2A, 0x85, 0x58, 0x53
, 0x8C, 0x3B, 0x62, 0x7C, 0xBB, 0xC5, 0x13, 0xC6, 0x34, 0xC2, 0x57, 0x77, 0x04, 0x
89, 0x5D, 0x2E, 0x13, 0x9E, 0x4C, 0xF4, 0xE7, 0x0A, 0x6D, 0x7B, 0x39, 0xBC, 0x94,
0x50, 0xF5, 0x0B, 0x30, 0xCF, 0xAC, 0xE2, 0xAA, 0xD1, 0x19, 0x7C, 0x42, 0xD0, 0xF
B, 0x31, 0x35, 0xB5, 0xE4, 0x7F, 0xCE, 0x81, 0x94, 0xA7, 0xD7, 0xCC};
        char nochange[] =
{0x20, 0x33, 0x00, 0xF8, 0x0C, 0xF8, 0xF8, 0x8B, 0x17, 0xF8, 0x01, 0x00, 0x45, 0x
41, 0xEB, 0x53, 0xC2, 0x30, 0x45, 0x8A, 0xB9, 0x00, 0xF4, 0x41, 0x83, 0x16, 0x00,
0x53, 0x33, 0x83, 0x00, 0xCC, 0x83, 0x01, 0x09, 0x83, 0xC7, 0x83, 0x88, 0x7D, 0x8
```

D,0xFC,0x00,0x00,0x8B,0xF8,0x83,0xDC,0x41,0x45,0xC7,0xCC,0x15,0x7D,0x40,0x45,0x00,0x08,0x30,0x00,0x01,0x89,0xC4,0x00,0x8B,0x20,0x50,0xF8,0xCC,0x68,0x8B,0x05,0x45,0x45,0x55,0x74,0x99,0x30,0x88,0x00,0x91,0xF4,0x55,0xEC,0x58,0x09,0x1A,0x7D,0xF8,0xF8,0x4D,0xC0,0x00,0x89,0x8B,0x8B,0x00,0xE8,0x80,0x8B,0x55,0x20,0xD2,0x8B,0x33,0xDA,0x4D,0x45,0xFC,0x00,0x00,0xF3,0x90,0x00,0x41,0x89,0xC1,0x33,0x20,0x50,0x42,0x4D,0x00,0x45,0x07,0x91,0xF5,0x3B,0x19,0xC0,0xF8,0x8A,0xC0,0x88,0x00,0xE8,0x8A,0x15,0x00,0xC2,0x55,0x64,0xF8,0x58,0xCC,0x56,0x8B,0xC7,0x00,0x44,0x88,0x4D,0xF8,0x03,0x33,0xD4,0xF8,0xC7,0xEC,0x8B,0x00,0xEB,0x83,0x00,0xEB,0x44,0x89,0x08,0xD2,0xF0,0xA8,0x01,0xF8,0xC7,0x55,0xE8,0x09,0x57,0x03,0xB8,0xF0,0x03,0xEB,0x00,0xF8,0xC1,0xC0,0xD8,0x30,0xF8,0x7D,0xEB,0x8B,0x8B,0x54,0x4D,0xF8,0x8B,0x83,0x00,0x45,0xEA,0xEB,0x00,0x45,0x00,0x00,0x00,0xFC,0xFC,0x08,0x89,0x4B,0xC0,0x58,0x00,0xF8,0xD6,0x04,0xEB,0x83,0xF8,0xF0,0x0D,0x45,0x00,0x8B,0xAB,0x33,0x83,0x01,0x45,0x00,0x00,0x41,0xE2,0x8B,0x45,0xC2,0x5B,0x7D,0x45,0xFB,0xF8,0xE8,0x45,0x8A,0x7D,0xF4,0xFC,0x83,0x68,0x00,0x41,0xC7,0x45};

```
10          int i, j, m;
11          for(i=0; i<sizeof(key); i++)
12          {
13                  for(j=0; j<sizeof(nochange); j++)
14                  {
15                          if (nochange[j] == key[i])
16                          {
17                                  m = toxor[j]^i;
18                                  if ((m>='0'&&m<='9') || (m>='A'&&m<='Z') || (m>='a'&&m<='z'))
19                                  {
20                                          printf("key[%d]=%c,", j%8, m);
21                                  }
22                          }
23                  }
24                  printf("\n--------------------\n");
25          }
26          system("pause");
27 }
28 </windows.h></stdio.h>
```

那个我们根据那些提示 接着输入 第一个 flag 的提示是 分析 pwnme.demo 还有 pwnme.ok 可是我在那台 103 的机子上 find / -name pwnme 什么都没有找到 也没法分析这个文件 倒是那个内网的两台可以做

0×06 ctf

根据跳板机的提示 我们把那个 192.168.0 的网段用 iptables 转发了出来 然后就直接访问啊什么的 转发这一步还是比较成功的 3389 什么端口都转出来的 有的队伍没有转发完全 一开始想用 msf 转发的 可是用 msf 转发只能一个人做题了 用 iptables 的话 可是设置网关之类的 让大家一起看题 做题 爆破之类的

h3ll0m4n 给出的转发方法 让我涨姿势了
打开转发功能

```
1 sysctl   net.ipv4.ip_forward=1
```

设置 iptables 规则

```
1 iptables -t nat -A POSTROUTING -s 10.0.0.0/8 -o eth1 -j MASQUERADE
```

把从 10.0.0.0/8 网段的数据通过 eth1 网卡转发出去

然后访问了 80 端口 发现了是一个题目的页面 还可以有几种方式进行入侵

1 发现文件类型 这个分分钟啊 下载 dump.zip 下来
下载 dump.zip
解压后 拿到 linux file 看一下 发现是 mac 的 doc 文件 然后就加上 doc 的后缀 在 win 下用 word 打开，打开发现需要密码 在文件的信息里就看到有一串 base64 加密过的东西 解码一下 this_is_base64 发现这个就是密码了 用这个密码上去

```
1 The server’s passwd like as follow:
2 User: Administrator
3 Pass: 4 rows of keyboard
```

发现了这个东西 然后我们就猜测是 1qaz 这样子的密码 可是手工试了很久 还写了字典去爆破 都不行 不知道是要怎么猜 甚至还尝试了手机的键盘 都没正确 比赛最后一刻还在猜这个密码 真难猜 搞不懂意思

半夜我就在看那个抓包的 pcap 文件
下载 tips.zip
那个并不大 不到 1M 很好看懂逻辑 需要我们找到远程溢出的方式 来重放达到攻击的目的 首先就要先找到攻击的类型还有 shellcode 发现了一个特殊的 ip

192.168.18.7 把和这个 ip 相关的提取出来单独看看 ip.dst == 192.168.18.7 || ip.src == 192.168.18.7 发现了这里是一个 ftp 的协议 溢出点也是在 ftp 这里 shellcode 我找到了 交给了 whitesilt 可是这个时候问题来了 ftp 的 21 号端口 居然没有开放 叫来了工作人员 也发现和原题的设定不一样 最后也没法解决 后来我问了问 貌似大家的 21 端口都访问不了

然后就是 wordpress 还有 jakcms 这两个的入侵
wordpress 用 wpscan 扫了一发 扫了下用户啊什么的 root 我怀疑是插件的问题 wordpress 是比较安全的 但是 wp 插件就不是这样子了 常常出注入什么的漏洞 扫了扫插件就发现了一个 xss 漏洞 比较鸡肋 就没有去利用 后来看到 wordpress 的提示 说 是管理员的疏忽还有配置有问题 但是就在想有没有可能是弱口令什么的 就去爆了一发 可惜字典用错了 用了自己做的之前用来爆破 webshell 的字典 结果就悲剧了 15000+什么都没有拿到 比赛最后还是没有爆破出来 非常可惜 赛后和 cyrils 聊了聊 发现了 原来是 root:toor 这个弱口令 这个弱口令我用来爆过 ssh 的 就是没想到往 wp 上试 too young too simple 然后进去之后 还能发现一个 config.php.bak 的备份 然后可以来拿到 mysql 的 root 密码 udf 提权拿下这台机子 500 分 有 6 队做出来了

jakcms 的这个渗透 就比较悲催了 我们利用宝贵的外网时间 在网上找到了一个 exp 是一个上传的 exp 打上去没有用 我们就在那里修改 exp 的代码 改得头昏眼花 就没做出来 打了酱油 哎

0×07 getfile
这个题在比赛的时候 一开始以为是之前见到过的 rand()爆破 可惜是 linux 下的 就知道自己思路错了
这个题给了 user.txt 和 pass.txt 使用 getfile.php?filename=&accesscode=的方式来获取的 观察一下发现 accesscode 是 filename 的 md5 那个 pass.txt 是没法 access 的 就用 md5 的方法来获取 发现是 LMNT hash 给了好多个
再去 getfile.php 试试看 让这个题变成白盒的代码审计题 获取到了 getfile

```
01 <?php
02 $value = time();
03 $filename = $_GET["filename"];
04 $accesscode = $_GET["accesscode"];
05 if (md5($filename) == strtolower($accesscode)){
06         echo "Welcome to view $filename!<br><br>";
07         srand($value);
           if (in_array($filename, array('getfile.php', 'classes.php',
08 'index.html', 'robots.txt', 'key.txt', 'login.php', 'passwords.txt',
   'usernames.txt'))==TRUE){
```

```
09                  $data = file_get_contents($filename);
10                  if ($data !== FALSE) {
11                          if ($filename == "key.txt") {
12                                  $key = rand();
13                                  $cyphertext =
mcrypt_encrypt(MCRYPT_RIJNDAEL_128, $key, $data, MCRYPT_MODE_CBC);
14                                  echo   base64_encode($cyphertext);
15                          } else if ($filename == "robots.txt") {
16                                  $key = rand();
17                                  $cyphertext =
mcrypt_encrypt(MCRYPT_RIJNDAEL_128, $key, $data, MCRYPT_MODE_ECB);
18                                  echo   base64_encode($cyphertext);
19                          }
20                          else if ($filename == "getfile.php") {
21                                  echo base64_encode($data);
22                          }
23                          else{
24                                  echo nl2br($data);
25                          }
26
27                  }
28                  else{
29                          echo "File does not exist";
30                  }
31          }
32          else{
33                  echo "File does not exist";
34          }
35
36 }
37 else{
38          echo "You don't have permission to view this file";
39 }
40 ?>
```

赛后和 kingdom 聊 他说这个题是 defcon 的原题 当时眼泪就掉下来
当时没上网找啊 尴尬了
就是这个 google 第一条 用关键字去搜就能搜到
DEF CON CTF Qualifier 2013 3dub 4 Writeup

平时 defcon 的题目做少了 关键时候掉链子了
当时是 以为是 rand()的范围还是 32767 可惜 win 下的 32767 linux 下是 2^31-1
这个还只是这个题的前半办法 还要再做一半才能进去 需要拿到 shell 看到在 /var/flag 的 flag 文件

比赛做到这里才是第二层 还有第三层内网在等待着我们 实在是太难了 表示平时没有收集字典什么的可惜了 也没好好整理整理 然后就跪了
这里还有 h3ll0m4n 做的网络拓扑图

0×07 后记
最后比赛是第 9 名 混了个三等奖 中间等待的时候 就一直宅在旅馆里玩琪琪的 mc
Minecraft 真好玩 4 个人一直玩 出去大雁塔玩的时候 还说要把大雁塔做到我们的世界里去