断剑重铸009

转载

avqfei90342 于 2019-09-22 23:13:00 发布 120 收藏
原文链接：http://www.cnblogs.com/sec875/p/11569909.html
版权

CTF黑客大赛导引

目的 已赛为练（多关注有趣的东西，来练习以前学过的知识）

- 介绍CTF比赛
- CTF比赛需要的基础知识
- CTF比赛神器 很多都是镜像，不要安装物理机。
- CTF比赛的意义 C，python，web，java 挑起你的求知欲，拔高你的知识面
- CTF比赛的经验 凡事都有套路

介绍CTF比赛

圈子内两家厉害的CTF培训：南京的赛宁网安，i春秋（e春秋） 它们提供CTF的环境和培训。
线下，需要在北京住几天，报名费2-3万。4-5天的课程。

夺旗大赛 flag 黑客的目的是黑进别人网络里面拿到他想要的东西。 CTF已黑客的角度看待，加强网络的安全。
1.核心的能力就是挖漏洞，利用漏洞进入对方电脑，拿到关键文件flag
约定成俗，大家都把把关键文件放到一个地方，如果你拿到了，就证明你黑进了我的电脑
/home/www/flag
/home/ctf/flag
flag文件一般是MD5的值
挖掘漏洞，写漏洞利用工具，拿到关键文件 靠C语言和web去挖掘漏洞

二进制要靠C语言去挖，web的漏洞要靠web和java的去挖
漏洞利用基本是靠python，非常少的情况会结合点C语言

C语言，java肯定是硬核，不用说也是要默认会的，其次python和web是很实用的。
可以从CTF的意义中进一步来定位自己想学什么语言就容易做选择了。

比赛历时与背景

比赛勾起兴趣，兴趣促进学习，知识用于加强网络安全的建设。
中国的CTF比赛 最主流的就这两个，其他的不是很专业
XCTF 强网杯
tctf 腾讯引起的
最著名的decon CTF比赛 CTF中的世界杯 蓝莲花战队，中国第一支CTF比赛拿到了前5，教练是诸葛建伟，清华大学的教授。
中国队一直拿不到冠军，中国人太多了，三个和尚没水喝的故事。招募队员的时候，一定要寻找无私的人，用人不疑，疑人不用。
PPP战队已经三连冠了。 台湾的橘子战队拿过一次冠军。 AAA浙江大学的队伍，也是中国的。

中国最好的战绩，拿到了第二。前十中，中国有三支（AAA，OOPS上海交大，腾讯的科恩实验室战队）。但是，韩国就一个队伍，拿了第一。
如果中国的三支战队组起来，早就拿到世界冠军了。 赞助商不同，导致这三支战队不可能结合，剪不清理还乱，干脆分家搞。

蓝莲花核心成员：张曹，web类挖掘 杨坤，web类挖掘 清华大学fish教授 清华大学李康教授

CTF线上赛：给你一个东西让你去破解。
web，二进制，杂项（图片隐写，暴力破解等） CTF线上赛训练平台 大把的资源
线上赛牵扯的东西太多了，玩起来的东西不是那么核心，主要关注线下赛

CTF线下赛：打攻防。
web漏洞挖掘与利用占10% pwn漏洞挖掘与利用占90%
web的题容易被人复现，马上就出现答案，很少去出题。
在中国比赛中还是很喜欢出web的题。
赛程：32小时连续奋战
每个队的资源：5-6个服务器（gamebox） 虚拟机 linux IP ssh登陆进行管理 端口与漏洞都是一样的
防御：写补丁程序
攻击：5分钟刷新一次，漏洞如果没有补上来，又被打了，又要扣分。

要有批量攻击的手段，20支队伍参赛，一个漏洞要打19支队伍。
打下来以后要批量拿flag，批量提交，定时执行。每5分钟执行一次。
写完这个批量脚本就可以睡觉了，一直涨分。
被打的要分析被打的漏洞，用二进制和web的方法去写补丁程序，更新服务。
每支队伍1万分。如果这个漏洞只有你一个人打，一个人拿10分，如果有10个人打，每个人拿1分。
删除服务器，宕机状态也会扣分。没有宕机的平分分数。又被打又宕机，扣双倍的分。
有的队伍不仅要打你，还要宕你的机。DOS攻击。
挖漏洞大概一个小时，写利用大概半个小时。两个小时大概就会出现第一波攻击。大概名列前茅。

挖不出漏洞，就抄袭。主要靠的是python。

CTF比赛需要的基础知识

漏洞利用-成功利用漏洞并突破安全防御机制
代码缺陷：堆溢出 栈溢出等 web漏洞
后果：控制流劫持（shell），敏感信息泄露（flag），可用性破坏等（打宕机，ddos）。
控制流劫持并执行shellcode，获得shell或读flag到socket。
破坏服务可用性：服务漏洞利用造成服务状态异常。
安全防御机制：NX（DEP），PIE，ASLR，stack canary.....
漏洞利用技术：ROP，结合地址泄露漏洞等/brute forcing，SEH Exploit

shell：用控制台操作你的电脑（访问权限）
漏洞利用，二进制代码：高级木马，shellcode，powershell

能够访问别人的机器 6个端口分到6个gamebox上面
端口扫描：nmap 22 21 23 80 443 3306.。。 意味着在这个端口上有监听程序。
怎么进去，就需要知道那些端口上的进程是什么，谁在监听，它们的漏洞是什么。
不用默认端口号，把进程的端口号改成别的也行。
nmap通过协议指纹也知道你改的端口号，后面的进程是干什么的，你改了也掩饰不了。别人一样知道端口后面是远程，是web，还是数据库。
你把80端口关了，正常的也进不去了，你的公司还开不开了。直接把路由器拔掉更好。
python 写漏洞利用的脚本（都是通过pwn tools这个库写的）

web的机制 php js html asp已经绝迹了（CTF中）
二进制的漏洞，全部要用到内核的知识。挖漏洞，只能从内核的角度去挖。

4-6人队伍：
121
231
131
前锋：打别人的，拿到漏洞就开始用python写批量脚本
中场：逆向分析人员，代码审计人员去发现漏洞（一个人负责web）
后卫：服务器安全运维人员

- web漏洞挖掘技巧
  PHP有源码 JavaScript一出就是难题，要结合多角度分析。出题来看最多是PHP的，JSP一出的话非常难。
  iis服务器都很少了，asp就更少了。学的价值不大。300块钱，非常好的站，淘宝就有。

最重要的能力，代码审计：学习资源，www.freebuf.com/vuls/169415.html
基于：html，php，JavaScript去审计的
代码审计太慢了，用调试提高效率。xdebug，phpstudy
python一般不做web，做真正的站的时候，python也很少做web。

调试环境搭建：PHPstudy+Xdebug+PHPstorm10
对PHP进行断点调试
查调用栈，对流量进行快速分析

- pwn漏洞挖掘
  逆向分析：java和C语言的人员上场，得到一个PE文件，二进制文件。
  要分析它的漏洞，没有源码，只能通过读汇编，C/C++/Java的伪代码，把它逆向出来分析。
  通过汇编，伪代码去分析环境中是否存在这样的漏洞。

一个业务的过程要清楚，正向，逆向都要清楚。
正向：输入账号密码，函数接收账号密码验证
逆向：账号密码输入到哪了，怎么传给后台验证服务程序的，后台服务程序怎么验证的

linux系统（内核）知识，配合逆向一起，漏洞挖掘与系统之间的利用过程搞清楚以后，就可以把心得传给前锋去进攻了。

- 漏洞利用脚本编写（python）
  远程触发漏洞 其他语言都可以写漏洞利用，但是太麻烦，python用的最多
  这就是为什么python更容易当黑客的原因

C和JAVA想要在别人那里运行，需要环境。
目标机器的环境你左右不了，别人电脑装的东西是别人决定的。
但是python不需要目标有环境，就算需要，可执行的环境也非常多。

- 服务器安全运维人员
  一般新人负责，更容易上手。
  shell脚本编写或python脚本一个，二选一就可以了
  linux运维的知识
  要防止别人打进来，要防止别人种植木马，要分析流量，备份数据库、服务器
  一个好的运维，让你无从攻击，没有办法下手。有了漏洞你也不好利用，一利用马上就知道有人在攻击。
  一上木马就能杀掉。

有的队伍，2个进攻，2个逆向，没有安全运维人员。输得非常惨，不停的被别人进攻。
站被人删了，服务器被人搞了，数据库被人瞎写了半天也被人删除了。各种各样的东西被人种了木马。
在你服务器里面写了一个木马，让你自己每5分钟一次定期提交自己的flag。
这就是没有运维的后果，木马不能及时杀掉。

- 流量分析能力
  我们队伍的逆向能力偏弱，发现不了多少漏洞，但是前锋的进攻性非常好。咋办呢？被动挨打来抄袭。
  等着别人来进攻，web怎么访问呢？肯定要构造一个特殊的URL来触发你web的漏洞。或者http/https请求来触发的。
  你想要通过web来攻击我，只能用URL来和我交互。用别人打我的招式，去打别人。
  怎么知道别人打你的招式？抓取服务器上面的流量，分析流量，找到进攻性的流量。把这个流量给漏洞利用人员去复现。

这样就可以抄袭成功。

在真正的比赛中，充满了垃圾流量
0day漏洞，未公开漏洞，核心秘密武器。不到万不得已的时候是不会去用的。
网上存在着大量的蜜罐。十几万美元的0day漏洞只是非常小的漏洞。大的漏洞几个亿。
拿到这个东西可以控制全球的机器。
如果你这个0day漏洞被别人抓包复现了，心都在滴血。

一般不会把漏洞利用直接发过去进攻，会先发大量无用的流量，几十兆，1个G等，再打出几个KB的流量。
这样的话，对于流量分析人员来说，就相当的考验能力了。
python有个库专门自动分析流量的
协议分析能力（就是流量分析能力）会交给运维人员去做。市场也非常吃香，分析的好，找个2-3万的工作一点问题都没有。
运维网络安全，最重要的就是靠流量分析，看别人打没打你。

CTF比赛神器（个人常用）

kali系统
nmap 端口扫描
searchsploit 漏洞查询（工作上用）

```
searchsploit smb                /      microsoft-ds
```

出来大量漏洞和漏洞利用（exp）的模块路径，用python写漏洞利用

metasploit 攻击框架
sqlmap sql注入的批量扫描
hydra ssh暴力破解
burpsuite sql注入的批量扫描
linux装软件很容易 apt-get install gdbserver就完事了。其他搜一下，很容易。

python的pwntools库（进攻人员） 用kali装，不要用别的装

逆向分析人员 ida pro----kpathch插件，专用于防御，打补丁 notepad++ ue winhex
逆向分析人员 gdb 以及插件：gef peda-gdb gdbserver ODdub不需要（很少有windows的逆向调试）

流量分析人员 wireshark
流量分析人员 pcap python lib 库
流量分析人员 秘密武器 个人经验收集的

运维人员 python或shell 文件监控武器（python写的）监控到底别人在你的可写文件夹里面传入了东西没有
文件监控武器，是个人自己写的，一般找人要或者自己找
运维人员 权限检索武器 木马查杀武器 这些都是要自己收集的

进攻人员 批量攻击框架 所有中文写的都是个人经验收集的，需要自己去找
进攻人员 特洛伊木马 菜刀（管理webshell）

参考资料：
网络漏洞挖掘 Pwn/二进制安全 CTF大赛培训班（完）：https://www.bilibili.com/video/av62214776?from=search&seid=4848688354162141552

转载于:https://www.cnblogs.com/sec875/p/11569909.html