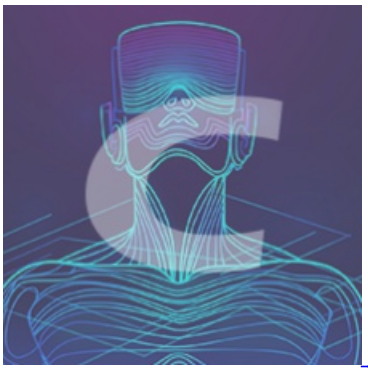
2021-07-04 CTF夺旗赛 CTF 黑客大赛导引

原创

愚公搬代码 于 2021-07-04 14:54:17 发布 27651 收藏

分类专栏： CTF成长之路 文章标签： 信息安全

本文链接：https://blog.csdn.net/aa2528877987/article/details/118462096



CTF 黑客大赛导引

目的

- 介绍CTF比赛
- CTF比赛需要的知识储备
- CTF比赛的神器
- CTF比赛的作用
- CTF比赛的经验

一：CTF比赛

“夺旗大赛”

比赛形式

1.挖掘漏洞，利用漏洞进入对方电脑，拿到关键文件
/home/www/flag
/home/ctf/flag

比赛历史与背景

1. 种类

```
cft
xcft--->强网杯
tcft
defcon ctf
```

2.形式

```
1.ctf线上赛
web 二进制 杂项
2.ctf线下赛
web漏洞挖掘与利用---10%
pwn漏洞与利用----90%
```

3.赛程：32小时连续奋战
打攻防
资源：5个服务器(gamebox) ip ssh登陆进行管理
防止自己的机器不被攻击—打补丁
攻击别人拿下别人的flag—

CTF比赛需要的知识储备

漏洞利用
二进制代码—木马 shellcode powershell
python pwn tools
web的机制 php js html

web漏洞挖掘能力
代码审计
调试环境

pwn漏洞挖掘
逆向分析
Linux系统知识

漏洞利用脚本编写
远程触发漏洞

服务器安全运维人员
shell
python
Linux运维的知识

流量分析能力
协议分析

CTF比赛的神器

kali系统 2018.02 kali
nmap 端口扫描
139 443 445 514 912
searchsploit 漏洞查询
metaspolit 攻击框架 use exploit/windows/smb/ms17_010_eternalblue

sqlmap sql注入的批量扫描
hydra ssh暴力破解
burpsuite sql注入的批量扫描

python的pwntools

ida pro ----kpathch插件

gdb 以及插件 gef peda-gdb gdbserver (apt-get install gdbserver)

notepad++

ue winhex

wireshark

pcap python lib

秘密武器

文件监控武器

权限检索武器

木马查杀武器

批量攻击框架

tly

菜刀