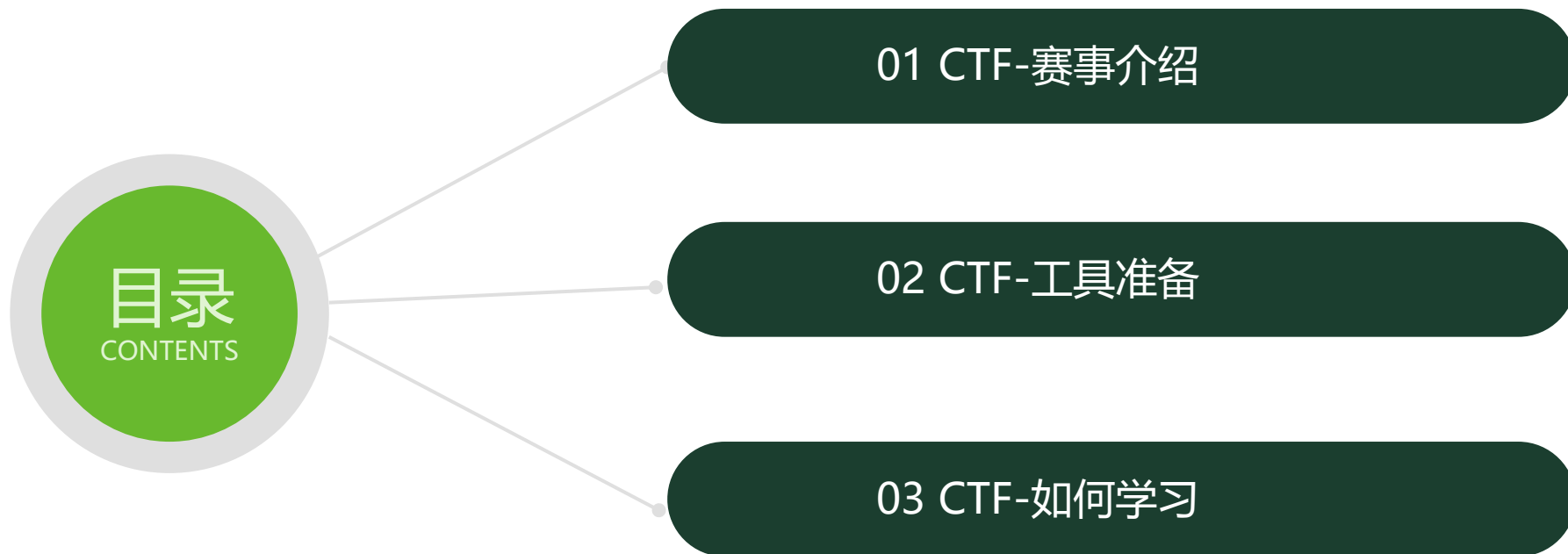


CTF 竞赛简(ke)介(pu)

—— 一次没有什么深度的科普,甚至可能有点枯燥.....



北京大学
PEKING UNIVERSITY



01

CTF-赛事介绍

CTF是什么?

CTF题目类型

CTF赛制

CTF是什么?

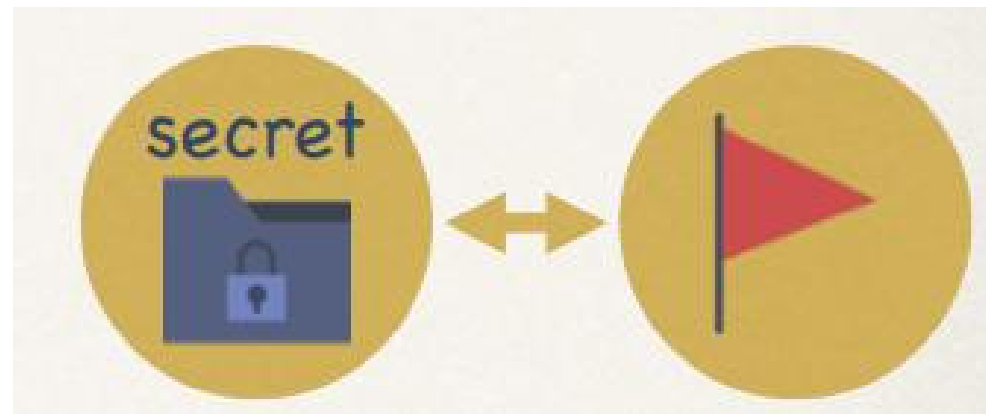


Capture The Flag

学习安全攻防的竞赛

利用执行在目标WEB服务或服务器的漏洞取得 Flag

解密藏在文件或程序中的 Flag



▶▶ CTF题目类型

Misc Crypto Web

Reverse Engineering Pwn Android ICS



Msic

- ❑ Recon (信息搜集)
- ❑ Encode (编码转换)
- ❑ Forensic && Stego (数字取证 && 隐写分析)
- ❑ 各类信息技术 (区块链?)
- ❑ 隐写取证是 Misc 中最为重要的一块，包括文件分析、隐写、内存镜像分析和流量抓包分析等等，涉及巧妙的编码、隐藏数据、层层嵌套的文件中的文件，灵活利用搜索引擎获取所需要的信息等等。

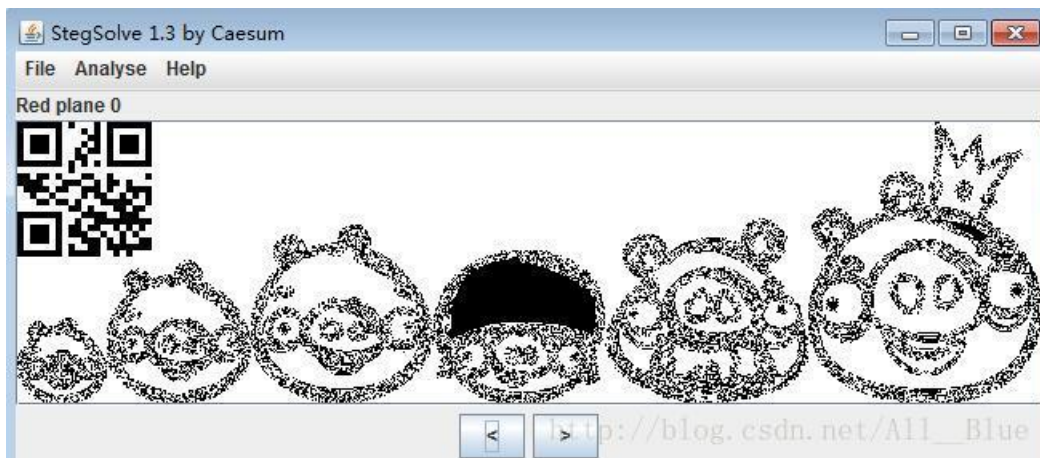


Msic

□ 图片隐写



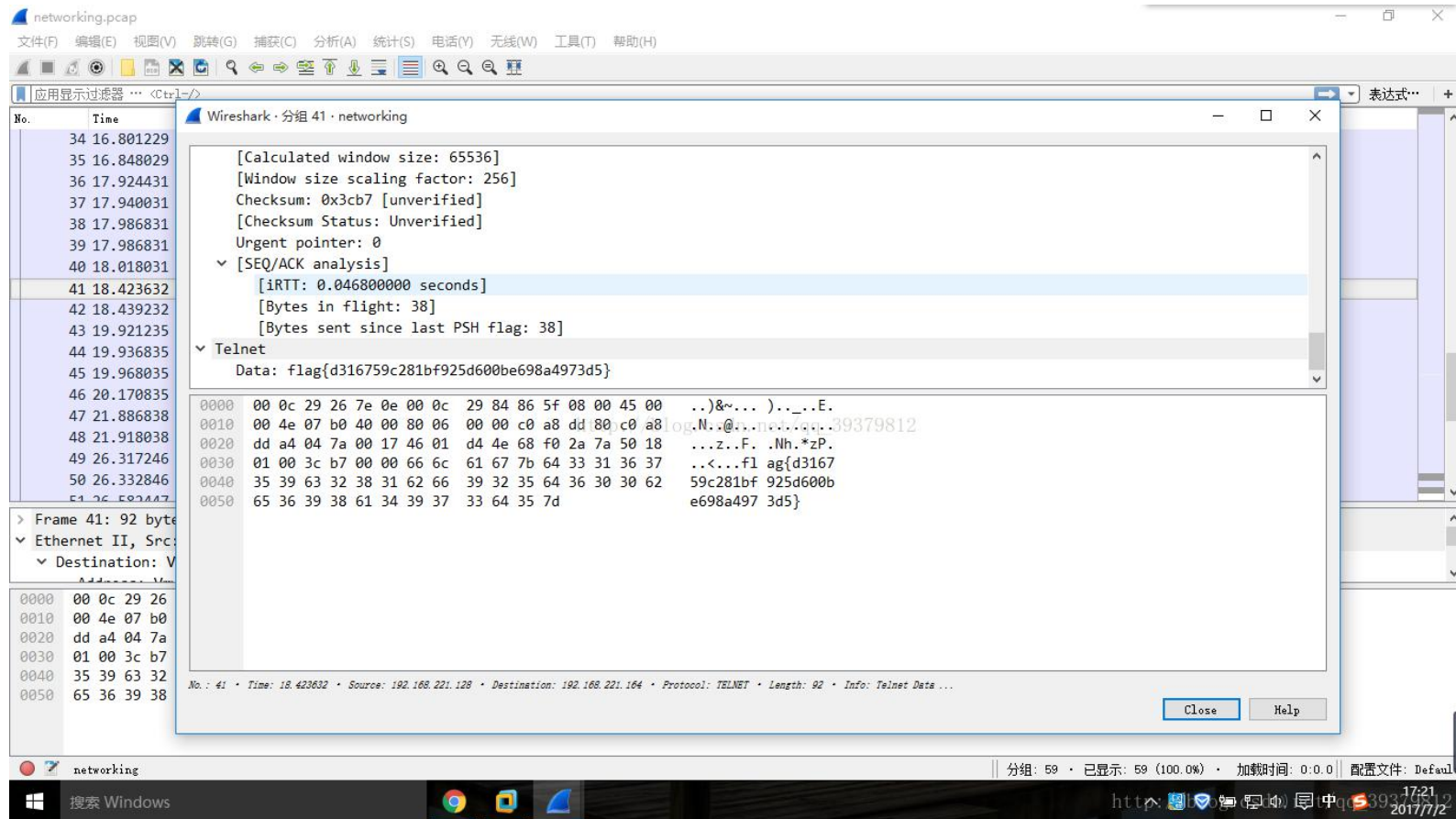
用stegsolve在红色0通道可以发现一个二维码，
扫描二维码就能得到flag





Msic

- 网络流量(.pcap)分析
- 分析包内的摘要及详细内容
- 常用工具: Wireshark





Crypto

- 一般来说，我们都会假设攻击者已知待破解的密码体制，而攻击类型通常分为以下四种：

攻击类型	说明
唯密文攻击	只拥有密文
已知明文攻击	拥有密文与对应的明文
选择明文攻击	拥有加密权限，能够对明文加密后获得相应密文
选择密文攻击	拥有解密权限，能够对密文解密后获得相应明文



Web

- 在 CTF 竞赛中，WEB 是占比重较大的一个方向之一，WEB 类的题目种类繁多，知识点细碎，时效性强，能紧跟时下热点漏洞，贴近实战。
- WEB 类的题目包括但不限于：
 - SQL 注入
 - XSS 跨站脚本
 - CSRF 跨站请求伪造
 - CRLF注入
 - XXE
 - 文件上传
 - SSRF 服务端请求伪造攻击
 - 文件包含
 - 框架安全
 - PHP 常见漏洞
 - 代码审计等



Web

□ 基础套路：

- 1. 爆破，包括包括md5、爆破随机数、验证码识别等
- 2. 绕WAF，包括花式绕sql、绕文件读取关键词检测之类拦截
- 3. 花式玩弄PHP特性，包括弱类型， strpos和===， 反序列化 destruct、\0截断
- 4. 各种找源码技巧，包括git、svn、xxx.php.swp、*www*.(zip|tar.gz|rar|7z)、xxx.php.bak、
- 5. 文件上传，包括花式文件后缀 .php345 .inc .phtml .phpt .phps、各种文件内容检测<?php <?<% <script language=php>、花式解析漏洞
- 6. Mysql类型差异，包括和PHP弱类型类似的特性,0x、0b、1e之类， varchar和integer相互转换
- 7. open_basedir、 disable_functions花式绕过技巧，包括dl、mail、imagick、bash漏洞、DirectoryIterator及各种二进制选手插足的方法



Web

□ 基础套路：

- 8. 社工，包括花式查社工库、whois等
- 9. 服务器特性，包括短文件名、IIS解析漏洞、冒号截断等
- 10. XSS，各种浏览器auditor绕过、富文本过滤黑白名单绕过、flash xss
- 11. XXE，各种XML存在地方（rss/word/流媒体）、各种XXE利用方法（SSRF、文件读取）
- 12. HTTP协议，花式IP伪造 X-Forwarded-For/X-Client-IP/X-Real-IP/CDN-Src-IP、花式改UA，花式藏FLAG、花式分析数据包
- 13. 条件竞争
- 14. 近几年爆出的各类漏洞复现



Web

□ 引用某师傅的话：

- web 也是一个逆向的过程，猜测web服务的代码逻辑
- 做题和出题都是一种学习
- 理解机制，有理可循

```
$what=$_POST['what'];  
echo $what;  
if($what=='flag')  
    echo 'flag{****}';
```

```
$md51 = md5('QNKCDZO');  
$a = @$_GET['a'];  
$md52 = @md5($a);  
if(isset($a)){  
    if ($a != 'QNKCDZO' && $md51 == $md52) {  
        echo "flag{*}";  
    } else {  
        echo "false!!!";  
    }  
}  
else{echo "please input a";}
```



Reverse

```
#include <stdio.h>
#include <string.h>

int main()
{
    char szKey[20];
    printf("Input Key");
    scanf("%16s",szKey);
    if (strcmp(szKey,"Thi5_is_T0o_E4sy",16) == 0)
    {
        printf("flag is your key! \r\n");
    }else{
        printf("please reverse me!\r\n");
    }
    return 0;
}
```

```
char secret[] = "QjRzZTYOX2k1X2MwbW1vbG==";
int main()
{
    char szKey[20] = {0}, szBase64[40] = {0};
    unsigned int i = 0;
    printf("Input Key");
    scanf("%16s",szKey);
    Base64encode(szBase64,szKey,strlen(szKey));
    if (memcmp(szBase64,secret,sizeof(secret)) == 0)
    {
        printf("flag is your key! \r\n");
    }else{
        printf("please reverse me!\r\n");
    }
    return 0;
}
```

- ❑ 参赛者会得到一个程序(binary), 需在没有完整原始码的情况下分析程序,找到隐藏的信息或者改变程序运行流程
- ❑ 静态分析(Static Analysis)
- ❑ 不执行程序, 单纯从反编译的程序代码、组合语言、
- ❑ 程式流程图、Global & Static data 等进行分析



Reverse

□ 逆向一般流程：

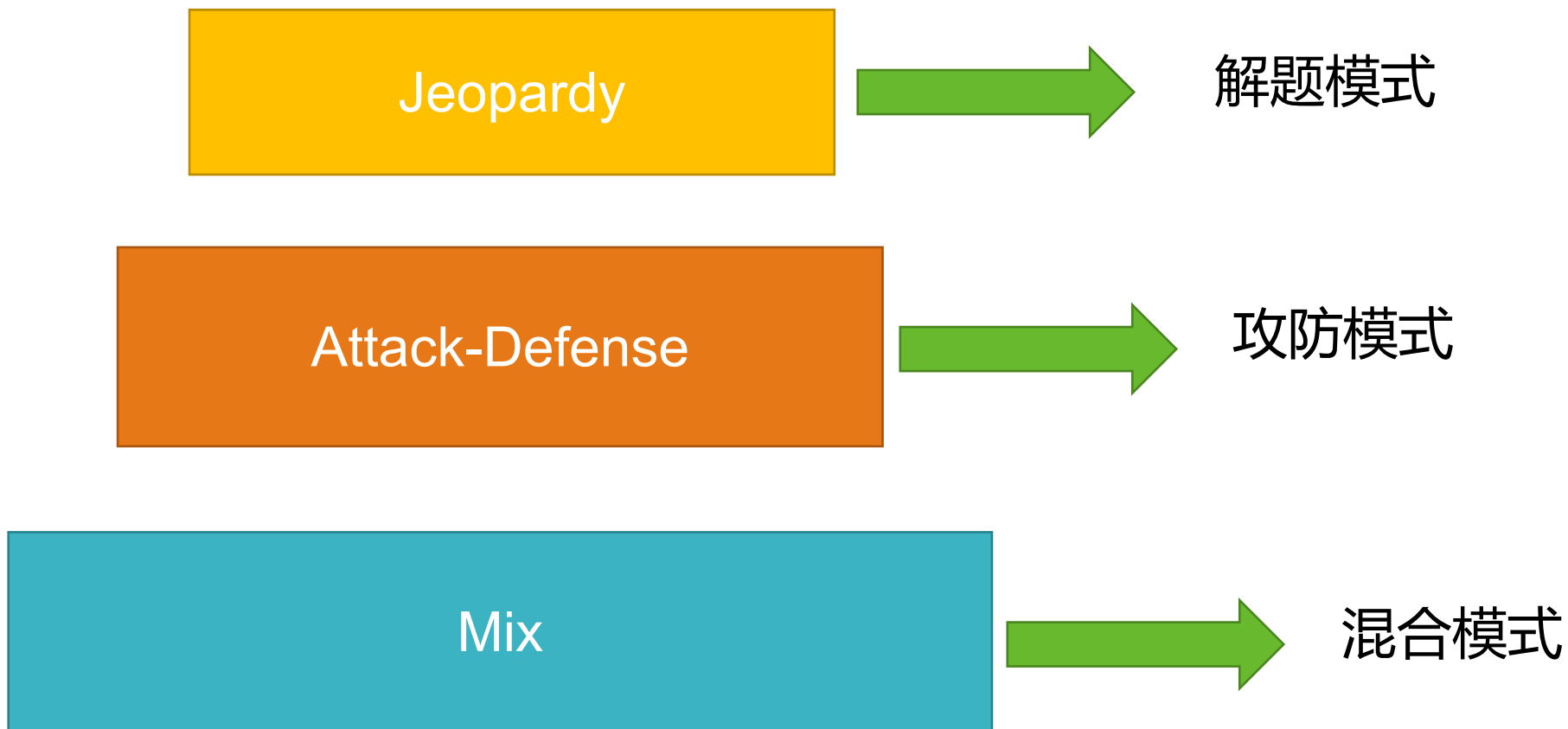
- 使用strings/file/binwalk/IDA等静态分析工具收集信息
- 研究程序的保护方法，如代码混淆，保护壳及反调试等技术，并设法破除或绕过保护
- 反汇编目标软件，快速定位到关键代码进行分析
- 结合动态调试，验证自己的初期猜想，在分析的过程中理清程序功能与运行流程
- 针对程序功能，写出对应脚本，破解程序，求解出 flag



Pwn

- 与Reverse 相似，参赛者也会得到一个 binary
- 但目标是要攻击执行在对方主机上的 binary，拿到对方主机控制权
 - 分析(analysis)→找寻漏洞(bug)→编写攻击程序(exploit)
 - bug
Buffer overflow, Use after free,...etc
 - exploit
利用程式漏洞从而获得主机控制权(get shell)

▶▶ CTF 赛制





Jeopardy

Jeopardy game interface showing categories and questions.

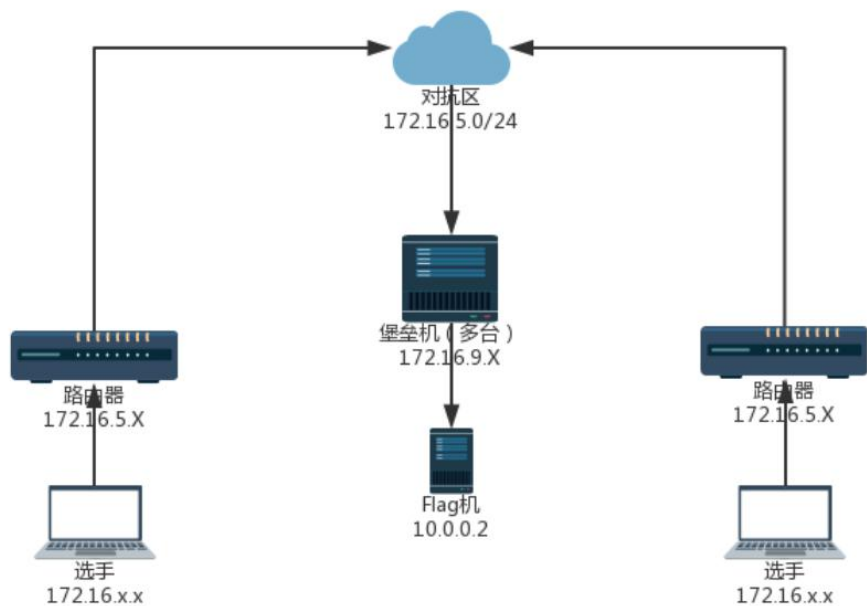
Categories: Crypto (0/4), Reverse (0/6), Misc (0/6), Pwn (0/6), Web (0/6).

Questions and Scores:

- bytecipher** (solved: 0): 1000 pt
- easy_rust** (solved: 2): 952 pt. Top teams: W&M, 苍海Wra1Nc.
- NaughtyBoy** (solved: 10): 689 pt. Top teams: Dawn, Lilac, GUET_Team.
- s390** (solved: 5): 833 pt. Top teams: Mini-Venom, GZCLAB, Metasequoia.
- 驱动逆向** (solved: 15): 588 pt. Top teams: L3H Sec, GUET_Team, Vidar-Team.
- Reverse** (solved: 0): 1000 pt



Attack-Defense



- ❑ 各队参赛者有自己的主机，主机上执行着各种有漏洞的服务
- ❑ 攻击他队的服务的同时，也要防御自己的服务
- ❑ 分析主机上的服务，找到漏洞利用方式
- ❑ 撰写攻击程序，攻击其他各队
- ❑ 修补自己有漏洞的程序
- ❑ 攻击成功（取得Flag）则得分，被他队取得Flag则扣分

02

CTF-工具准备



基础

- 至少一门编程语言！！！！
- 推荐Python
- 科学上网，搜索和学习能力

工具合集：<https://ctf-wiki.github.io/ctf-tools/>



Msic

□ 压缩包

- Ziperello
- zip 压缩包密码爆破。
- Advanced Rar Password Recovery
- Advanced Zip Password Recovery

□ GIF在线分解

- <https://ezgif.com/split>

□ 条形码、二维码

- <https://online-barcode-reader.inliteresearch.com/default.aspx>

□ 图片隐写

- Stegsolve
- Steghide
- Outguess amd64 deb
- PNGCheck
- JPHS win32
- OurSecret

□ 编辑器

- 010 Editor Windows x64

□ NTFS 文件流

- Alternate Stream View

□ 取证

- Elcomsoft Forensic Disk Decryptor

□ 破解工具音频隐写

- Audacity
- 在线拨号音识别

□ 无线密码

- Elcomsoft Wireless Security Auditor



Crypto

□ RSA

- yafu 大数分解
- factordb 在线大数分解
- RSATool
- wiener-attack
- rsatool

□ 古典密码

- CAP4
- JPK - 406
- RC4 在线加解密
- 栅栏密码加解密工具
- 摩斯密码在线加解密
- 维吉尼亚密码在线解密
- 厦大 ph0en1x 在线密码工具
- 密码机器—栅栏、凯撒、维吉尼亚、摩斯、置换等。
- quipquip—移位密码破解
- PYG 密码学综合工具

□ Hash

- CRC32 碰撞脚本

□ 其他

- Cisco 密码在线破解
- Base64 加解密



Web

- ❑ 基础工具：F12 + 好的浏览器
- ❑ 菜刀
- ❑ 注入—SQLMAP
- ❑ 抓包
 - Burp Suite
 - WireShark
 - PKAV HTTP FUZZER
- ❑ 目录扫描
 - 御剑后台扫描
 - dirfuzz
 - dirsearch
 - weakfilesan
- ❑ 源码泄露
 - Seay - SVN 源码泄露利用工具
 - Githack
- ❑ 日志分析--LogForensics
- ❑ 内网--Termite



Reverse

□ 反汇编

- IDA Pro
- dnSpy
- ILSpy

□ 调试

- 吾爱破解专用 Ollydbg

□ 脱壳

- UPX Unpacker

□ Python

- unpy2exe

□ Android

- AndroidResEdit
- JD - GUI
- Android Killer
- JEB

□ 动态插桩

- intel pin



Pwn

- ❑ 基础工具: Pwntool gdb nc
- ❑ 反汇编
 - IDA
- ❑ 调试
 - peda
- ❑ Patch
 - Fentanyl

03

CTF-如何学习

▶▶ CTF-如何学习

□ 学之前的思考：分析赛题情况，结合兴趣选择

PWN、Reverse	偏重对汇编、逆向的理解
Crypto	偏重对数学、算法的深入学习
Web	对技巧沉淀、快速搜索能力的挑战
Misc	更为复杂，所有与计算机安全挑战有关的都算在其中

精力有限先从一两个方向做起
其实Misc所有人可以做

不总结=白做题

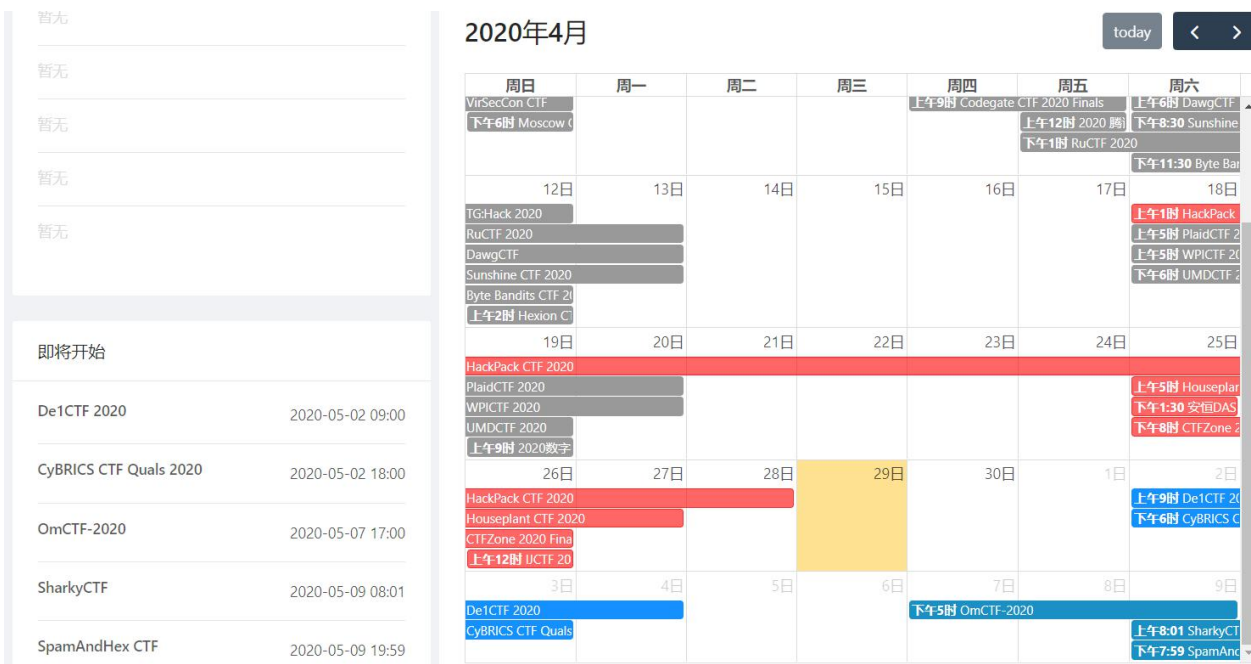
□ 补充基础知识&信息安全专业知识

linux、组原、OS、网络框架、网络协议
IDA工具使用、OD、逆向工程、密码学、缓冲区溢出

□ 刚刚入门建议打好基础，多思考，多总结，不用强求打多少比赛，总结和积累是最重要的

CTF-如何学习

- CTF wiki (<https://ctf-wiki.github.io/ctf-wiki/>)
- CTF hub (<https://www.ctfhub.com/>)
- CTF TIME (<https://ctftime.org/ctfs/>)
- XCTF 攻防世界 (<https://adworld.xctf.org.cn/>)
- BuuOJ (<https://buuoj.cn/>)
- CTF WP (<https://www.ctfwp.com/>)
- 大佬们的博客.....



Team rating


2018	2017	2016	2015	2014	2013	2012	2011
Place	Team	Country	Rating				
1	Dragon Sector		704.084				
2	Plaid Parliament of Pwning		583.287				
3	dcua		513.359				
4	TokyoWesterns		485.811				
5	p4		485.207				
6	LC#BC		435.130				
7	CyKOR		431.074				
8	Bushwhackers		411.255				
9	0days0ber		334.684				
10	RPISEC		322.138				

Full rating | Rating formula



Past events

With scoreboard


All

 **Hackcon 2018**




八月 16, 2018 18:30 UTC | On-line | [Weight voting in progress](#)

Place	Team	Country	Points
1	p4		48.660*
2	dcua		36.495
3	secuiseccf		27.501

459 teams total | [Tasks and writeups](#)

 **TJCTF 2018**

八月 12, 2018 23:00 UTC | On-line

Place	Team	Country	Points
1	WreckitRalph		48.580
2	pearl		
3	noraneco		



一起加油！



北京大學

PEKING UNIVERSITY