NUAA_CTF All In One

CTF比赛模式

解题模式 - Jeopardy

参赛队伍可以通过互联网或者现场网络参与，参数队伍通过与在线环境交互或文件离线分析，解决网络安全技术挑战获取相应分值，根据总分和时间来进行排名。

解题模式一般会设置 一血 、 二血 、 三血 ，也即最先完成的前三支队伍会获得额外分值。

还有一种计分规则是设置每道题目的初始分数后，根据该题的成功解答队伍数，来逐渐降低该题的分值。最后会下降到一个保底分值后便不再下降。

攻防模式 - Attack & Defense

初始时刻，所有参赛队伍拥有相同的系统环境（包含若干服务，可能位于不同的机器上），常称为 gamebox，参赛队伍挖掘网络服务漏洞并攻击对手服务获取 flag 来得分，修补自身服务漏洞进行防御从而防止扣分（一般来说防御只能避免丢分，当然有的比赛在防御上可以得分）。

在这种赛制中，不仅仅是比参赛队员的智力和技术，也比体力（因为比赛一般都会持续 48 小时），同时也比团队之间的分工配合与合作。

战争分享模式 - Belluminar

由受邀参赛队伍相互出题挑战，并在比赛结束后分享赛题的出题思路，学习过程以及解题思路等。战队评分依据出题得分，解题得分和分享得分，进行综合评价并得出最终的排名。

赛制中将 Challenge 的出题方交由受邀战队，让战队能尽自己所能互相出题，比赛难度和范围不会被主办方水平限制，同时也能提高 Challenge 的质量，每个战队都能有不一样的体验与提升。在 "分享" 环节，对本队题目进行讲解的同时也在提高自己的能力水平，在讨论回答的过程更是一种思维互动的环节。

CTF Contest content

Web - 网络攻防： Web 安全中常见的漏洞，如 SQL 注入、XSS、CSRF、文件包含、文件上传、代码审计、PHP 弱类型等。

Reverse Engineering - 逆向工程： 逆向工程中的工具平台、解题思路，进阶部分为逆向工程中常见的软件保护、反编译、反调试、加壳脱壳技术。

Pwn - 二进制漏洞利用： 主要考察二进制漏洞的发掘和利用，需要对计算机操作系统底层有一定的了解。CTF 竞赛中主要出现在 Linux 平台上。

Crypto - 密码攻击： 包括古典密码学和现代密码学两部分内容，古典密码学趣味性强，种类繁多，现代密码学安全性高，对算法理解的要求较高。

Mobile - 移动安全： 主要考察安卓逆向中的常用工具和主要问题类型，需要一定的安卓开发知识，iOS 逆向题目在 CTF 竞赛中较少出现。

Misc - 安全杂项： 内容主要包括信息搜集、编码分析、取证分析、隐写分析等。

全国大学生信息安全竞赛 - 竞赛内容

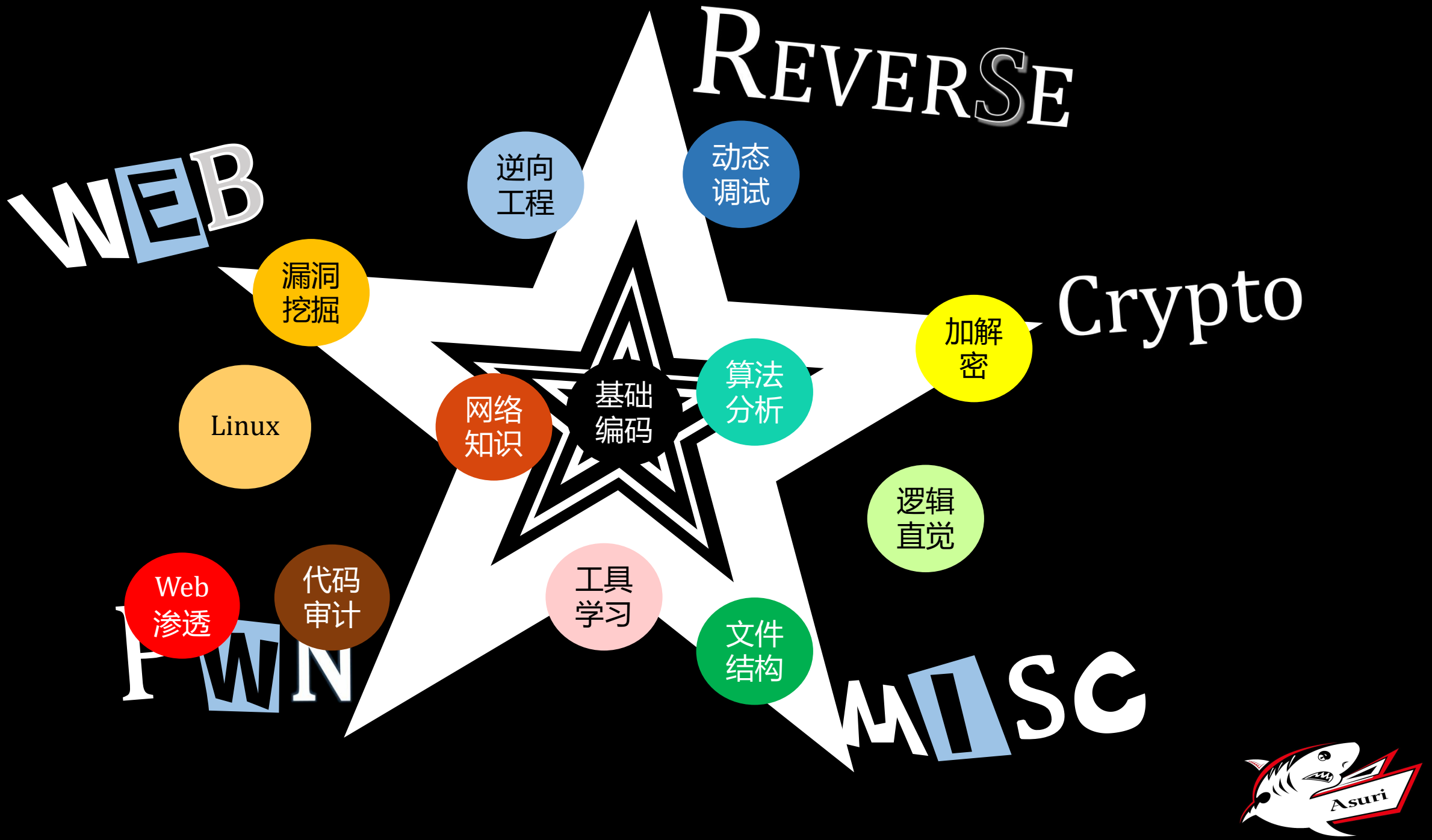
系统安全。涉及操作系统和 Web 系统安全，包括 Web 网站多种语言源代码审计分析（特别是 PHP）、数据库管理和 SQL 操作、Web 漏洞挖掘和利用（如 SQL 注入和 XSS）、服务器提权、编写代码补丁并修复网站漏洞等安全技能。

软件逆向。涉及 Windows/Linux/Android 平台的多种编程技术，要求利用常用工具对源代码及二进制文件进行逆向分析，掌握 Android 移动应用 APK 文件的逆向分析，掌握加解密、内核编程、算法、反调试和代码混淆技术。

漏洞挖掘和利用。掌握 C/C++/Python/PHP/Java/Ruby / 汇编 等语言，挖掘 Windows/Linux（x86/x86 _ 64 平台）二进制程序漏洞，掌握缓冲区溢出和格式化字符串攻击，编写并利用 shellcode。

密码学原理及应用。掌握古典密码学和现代密码学，分析密码算法和协议，计算密钥和进行加解密操作。

其他内容。包括信息搜集能力，编程能力、移动安全、云端计算安全、可信计算、自主可控、隐写术和信息隐藏、计算机取证（Forensics）技术和文件恢复技能，计算机网络基础以及对网络流量的分析能力。


REVERSE
WEB
逆向
工程
动态
调试
漏洞
挖掘
Crypto
加解
密
Linux
网络
知识
基础
编码
算法
分析
逻辑
直觉
Web
渗透
代码
审计
工具
学习
文件
结构
PWN
MISC
Asuri

Pwn

pwn-基础知识

- C语言：推荐书籍 – C与指针
- 汇编语言：推荐书籍 – 汇编语言(王爽)，深入了解计算机系统2，3章
- 不同操作系统(Linux/Windows)二进制程序的运行机制与常用函数
- gdb动态调试与IDA静态调试
- 基础python脚本编写，pwntools库的使用：https://pwntools-docs-zh.readthedocs.io/zh_CN/dev/
- 看雪学院： https://www.kanxue.com/chm.htm

pwn-二进制漏洞挖掘与利用

- 二进制指环境：为机器代码。
- 漏洞：即超出程序作者考虑外的操作，一般为读写漏洞。
- 挖掘：也就是发现，现代一般通过fuzz(启发式穷举)。
- 利用：也是ctf比赛中pwn的主要考察方面，通过漏洞达到自己的目的，在比赛中通常为getshell。

pwn-研究方向

- 栈溢出
- IO/输入输出函数漏洞
- 堆漏洞
- 逻辑漏洞
- 内核漏洞
- 等其他读写漏洞

pwn-栈溢出

- 栈溢出大部分题型在ctfwiki上都有介绍，可自行搜索合适的例题。
- 这里例举以下主要技能：ret2stack，ROP，ret2resolve，brop，srop，栈迁移，canary绕过。

pwn-IO/输入输出函数漏洞

- 主要有格式化字符串漏洞和FSOP文件流定向编程。
- 前者网上有大量教程，且通俗易懂
- 后者需要对IO函数对FILE结构体的调用了解

pwn-堆漏洞

- 推荐首先阅读：glibc内存管理ptmalloc源代码分析.pdf
- 堆漏洞：https://github.com/shellphish/how2heap

pwn-题库

- ctfwiki对应例题：https://ctf-wiki.github.io/ctf-wiki/pwn/readme-zh/
- https://pwnable.xyz/ (难度较易)
- https://www.jarvisoj.com/login (中等难度)
- http://pwnable.kr/ (题型较老，经典)
- https://pwnable.tw/ (较难)
- 之后就是自己在网上寻找往期比赛的经典赛题

Web

Web-基础技能

- 查看源码
- 抓包工具+增删改查http请求头
- cookie和session的理解与利用
- Web(h5,css,js,php,java.....)代码审计
- 数据库相关知识-sql注入
- 基础Linux操作

Web-网络攻防

CTF中的Web题型，通常是给定一个Web网站，选手要根据题目所提示的信息，找到网站上的flag字符串。

做题的方法类似于渗透测试，但通常不会是一个完整的渗透测试，而是用到渗透测试中的某一个或某几个环节。可能涉及信息搜集、各类漏洞发现与利用、权限提升等等。

为了获取flag，可能需要拿到管理员权限，数据库权限，甚至获取网站所在服务器的权限。

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、文件上传、文件包含、框架安全、PHP 常见漏洞、代码审计等。

Web-研究方向

- SQL 注入
- XSS 跨站脚本攻击
- 命令执行
- 文件包含
- 文件上传
- CSRF 跨站请求伪造
- ……

Web-传送门

- 详细介绍：https://ctf-wiki.github.io/ctf-wiki/web/introduction-zh/
- 技能树：https://skills.bugbank.cn/
- sqli-labs:https://github.com/Kit4y/Sql-Injection (sql注入题库)
- xss-challenges: http://xss-quiz.int21h.jp (xss练习)
- web百宝箱：https://github.com/CHYbeta/Web-Security-Learning (非常全面)

Crypto

Crypto-密码学简介

密码学（Cryptography）一般可分为古典密码学和现代密码学

数学是密码学的基石，编码能力是解密的工具

Crypto-古典密码学

古典密码学，作为一种实用性艺术存在，其编码和破译通常依赖于设计者和敌手的创造力与技巧，并没有对密码学原件进行清晰的定义。古典密码学主要包含以下几个方面：

1、单表替换加密（Monoalphabetic Cipher）

2、多表替换加密（Polyalphabetic Cipher）

3、奇奇怪怪的加密方式

Crypto-现代密码学

现代密码学则起源于 20 世纪中后期出现的大量相关理论，1949 年香农（C. E. Shannon）发表了题为《保密系统的通信理论》的经典论文标志着现代密码学的开始。现代密码学主要包含以下几个方面：

1、对称加密（Symmetric Cryptography），以 DES，AES，RC4 为代表。

2、非对称加密（Asymmetric Cryptography），以 RSA，ElGamal，椭圆曲线加密为代表。

3、哈希函数（Hash Function），以 MD5，SHA-1，SHA-512 等为代表。

4、数字签名（Digital Signature），以 RSA 签名，ElGamal 签名，DSA 签名为代表。

Crypto-CTF常见古典密码

1、ASCII编码
2、凯撒密码
3、栅栏密码
4、摩斯密码
5、base全家桶
6、Brainfuck/Ook!编码
7、当铺密码
8、培根密码
9、猪圈密码
10、unicode编码
11、URL编码
12、ROT5/13/18/47编码
13、维吉尼亚加密
14、键盘密码
15、JSFuck
16、词频分析

Crypto-传送门

- 实验吧：http://www.shiyanbar.com/ctf 里面有基础密码题
- 解密工具大礼包: https://github.com/guyoung/CaptfEncoder (基本覆盖所有古典密码)
- RSA证明：https://kit4y.github.io/2018/12/31/RSA%E8%AF%81%E6%98%8E/
- 密码学练习：https://cryptopals.com （比较难）

Reverse

综合

论坛与学习网站

- 看雪论坛：https://bbs.pediy.com/。偏二进制（逆向和pwn）。
- Pwn环境搭建：https://www.hirworld.xyz/posts/c3943130/
- CTF wiki: https://ctf-wiki.github.io/ctf-wiki/introduction/resources-zh/
- 先知社区：https://xz.aliyun.com
- 看雪学院：https://www.kanxue.com/chm.htm
- XCTF平台: https://www.xctf.org.cn

综合入门题库

- 实验吧：http://www.shiyanbar.com/ctf　入门基础题
- Bugku:　https://ctf.bugku.com/　全面-wp多
- jarvios:　https://www.jarvisoj.com　真实

CTF工具链接

- 工具包：https://pan.baidu.com/s/1FswzHCnY3IYPIsR5S0eM6w/
- 在线工具： http://ctf.ssleye.com/
- 扫描工具：https://github.com/Kit4y/Some-Scanner/
- IDA7.0：https://pan.baidu.com/s/1M0CbuBQx1F_IcqmygQWatw
- 爱盘：https://down.52pojie.cn/Tools/
- CTFTools：https://ctftools.com/down
- 看雪工具：https://tools.pediy.com