
CTF基础

CTF概念

Nantian

什么是CTF?

CTF（Capture The Flag）中文一般译作夺旗赛，在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。

其大致流程是，参赛团队之间通过进行攻防对抗、程序分析等形式，率先从主办方给出的比赛环境中得到一串具有一定格式的字符串或其他内容（也称为flag），并将其提交给主办方，从而夺得分数。

CTF模式

Nantian

1、解题模式（传统CTF）

在解题模式CTF赛制中，参赛队伍可以通过互联网或者现场网络参与，解出主办方设置的题目来获取分值；

2、攻防模式（AWD-Attack With Defense）

在攻防模式CTF赛制中，参赛队伍在网络空间互相进行攻击和防守，挖掘网络服务漏洞并攻击对手服务来得分，修补自身服务漏洞进行防御来避免丢分。

3、混合模式

结合了解题模式与攻防模式的CTF赛制，比如参赛队伍通过解题可以获取一些初始分数，然后通过攻防对抗进行得分增减的零和游戏，最终以得分高低分出胜负。

4、综合渗透

主办方给出综合网络场景，不同网络层面上部署具有不同漏洞的应用或系统，攻击者需要层层突破，搭建网络隧道，才能获取更高的分。

CTF赛制

Nantian

1、选拔赛传统CTF，半决赛或决赛AWD;

2、团队赛、个人赛或二者结合，如报名以团队方式报名，比赛时个人作战，团队分数为个人分数总合;

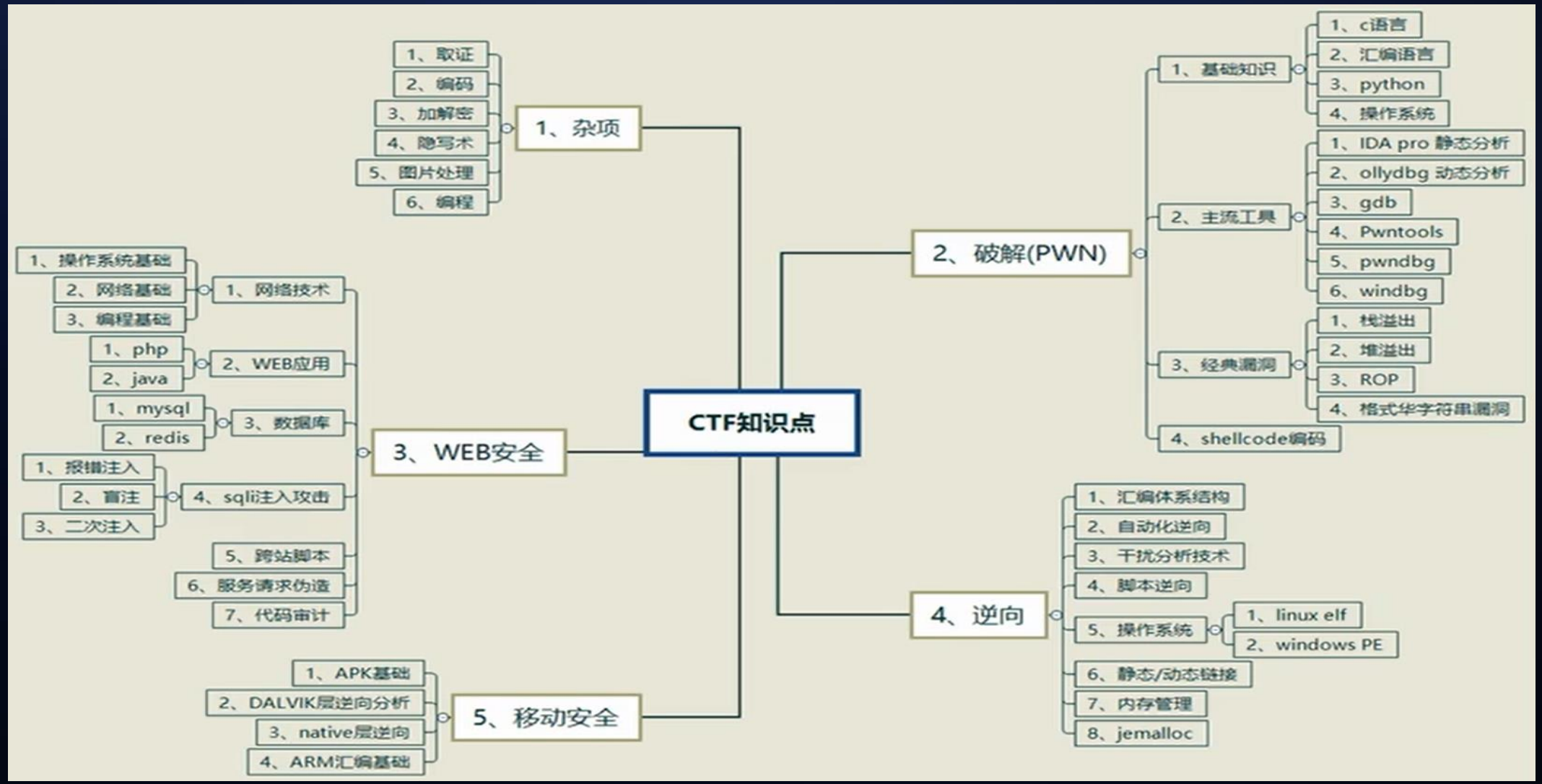
结合了解题模式与攻防模式的CTF赛制，比如参赛队伍通过解题可以获取一些初始分数，然后通过攻防对抗进行得分增减的游戏，最终以得分高低分出胜负。

3、综合渗透

常出现在行业内比赛中，如工控场景中，高分题目为网络最内层的生产系统等。

CTF知识点

Nantian



CTF题型

Nantian

1、解题模式（传统CTF）

题目主要包含逆向、漏洞挖掘与利用、Web渗透、密码、取证、隐写、安全编程等类别

Misc（杂项，包括流量分析取证、隐写术、压缩包处理、文件提取、社会工程学、脑洞等）

Crypto（密码学，有些古典密码或者编码类型的题会在misc题里结合着考）

古典密码学：摩斯密码、栅栏密码、凯撒密码、猪圈秘密、棋盘密码、培根密码、维吉尼亚密码等

现代密码学：对称加密算法和非对称加密算法，常考的对称加密算法：DES，常考的非对称加密算法：RSA

编码类型的题：url、base家族等

Reverse（逆向，脱壳、花指令处理，破解程序的算法获取flag等）

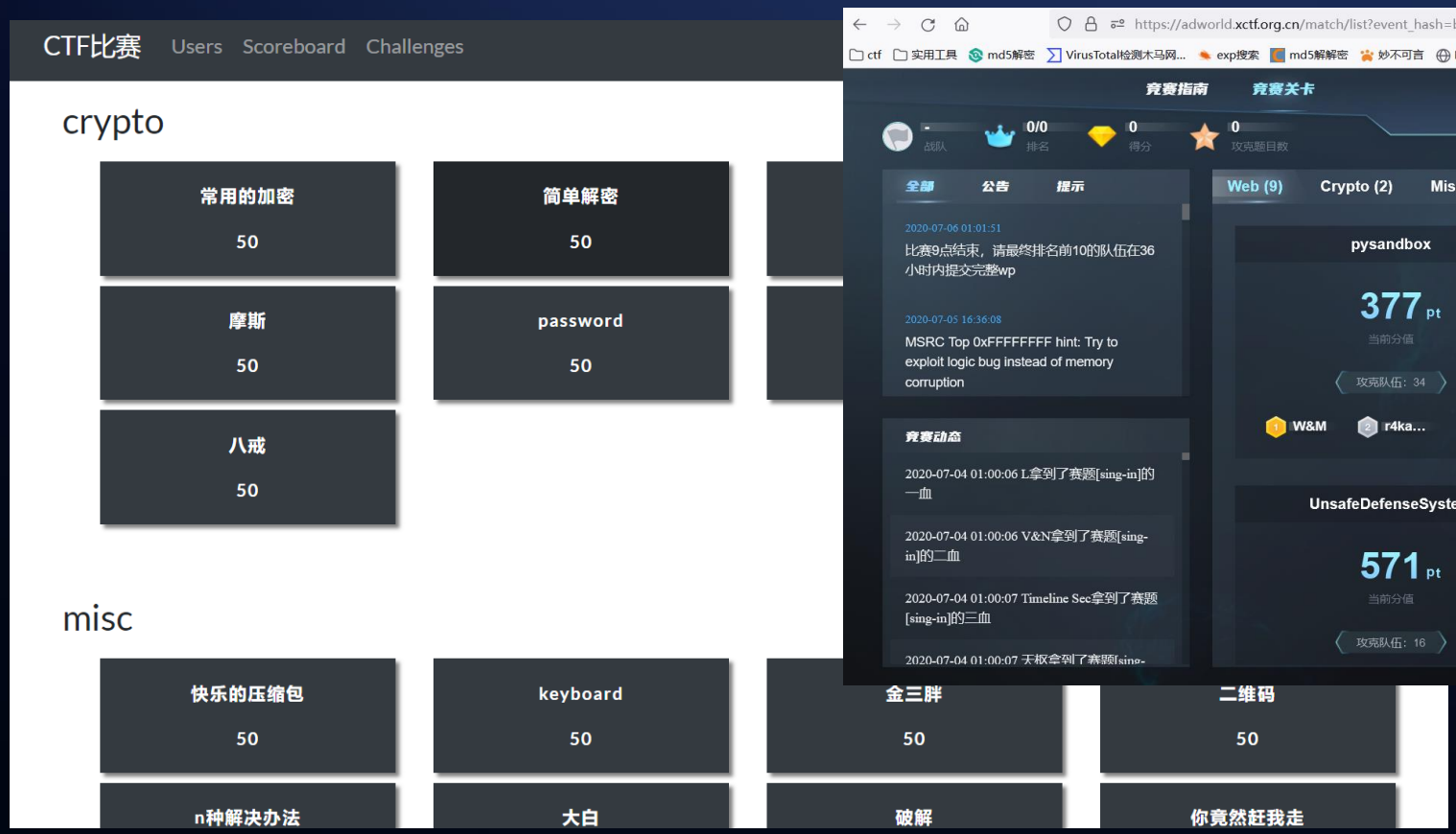
PWN（基于二进制的漏洞挖掘和利用、攻击远程服务器的服务）

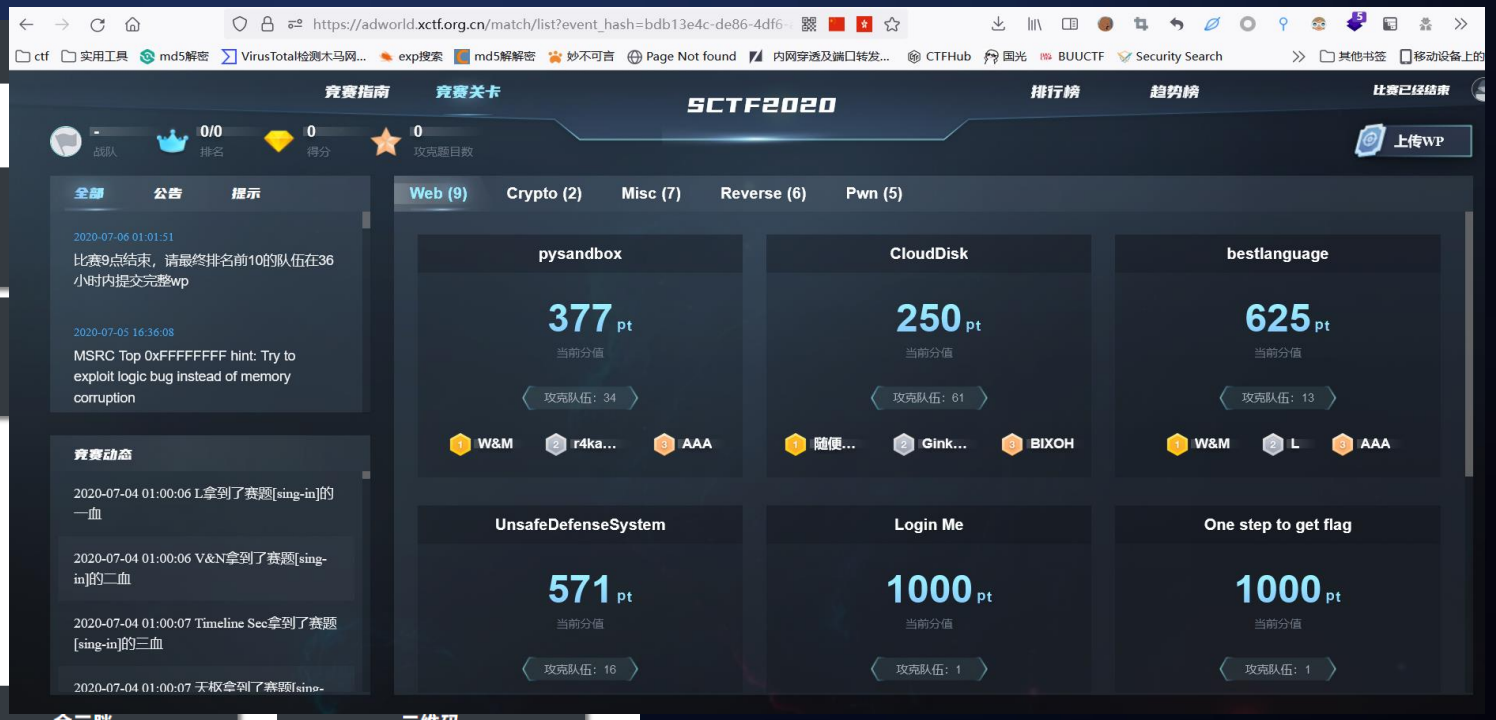
Web（sql注入、xss、文件上传、文件包含、命令执行、代码审计等）

传统CTF出题方式

Nantian

https://buuoj.cn/challenges





AWD

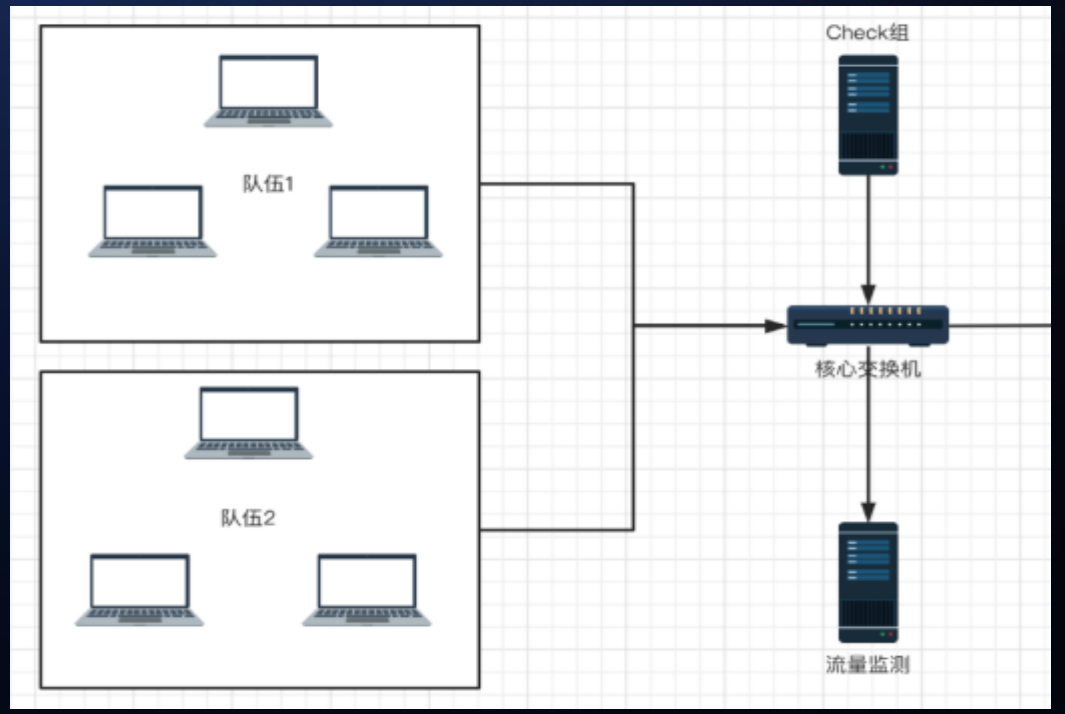
Nantian

赛制：一般为团队赛，考核团队攻击、防御技术能力

每个战队都拥有相同的起始分数，挖掘网络服务漏洞并攻击对手服务取得flag获得积分，被攻击方扣减相应分数；

一般比赛会将加固环节和攻击环节分开，先统一加固后再进行攻击。

所有队伍会在同一个网络环境下，一般会有Check脚本或程序，实时查询各队伍服务是否正常，如服务被关闭或check脚本无法检测到正常状态，那队伍会持续掉分，直至服务恢复正常



AWD

Nantian

出题方式：一般给定一个网段，以及队伍自己的服务器账号密码

攻击队伍需在网段自行进行资产探测和信息收集。

答案一般通过拿到其他参赛队伍服务器权限后，通过命令行curl或访问flag服务器获取。

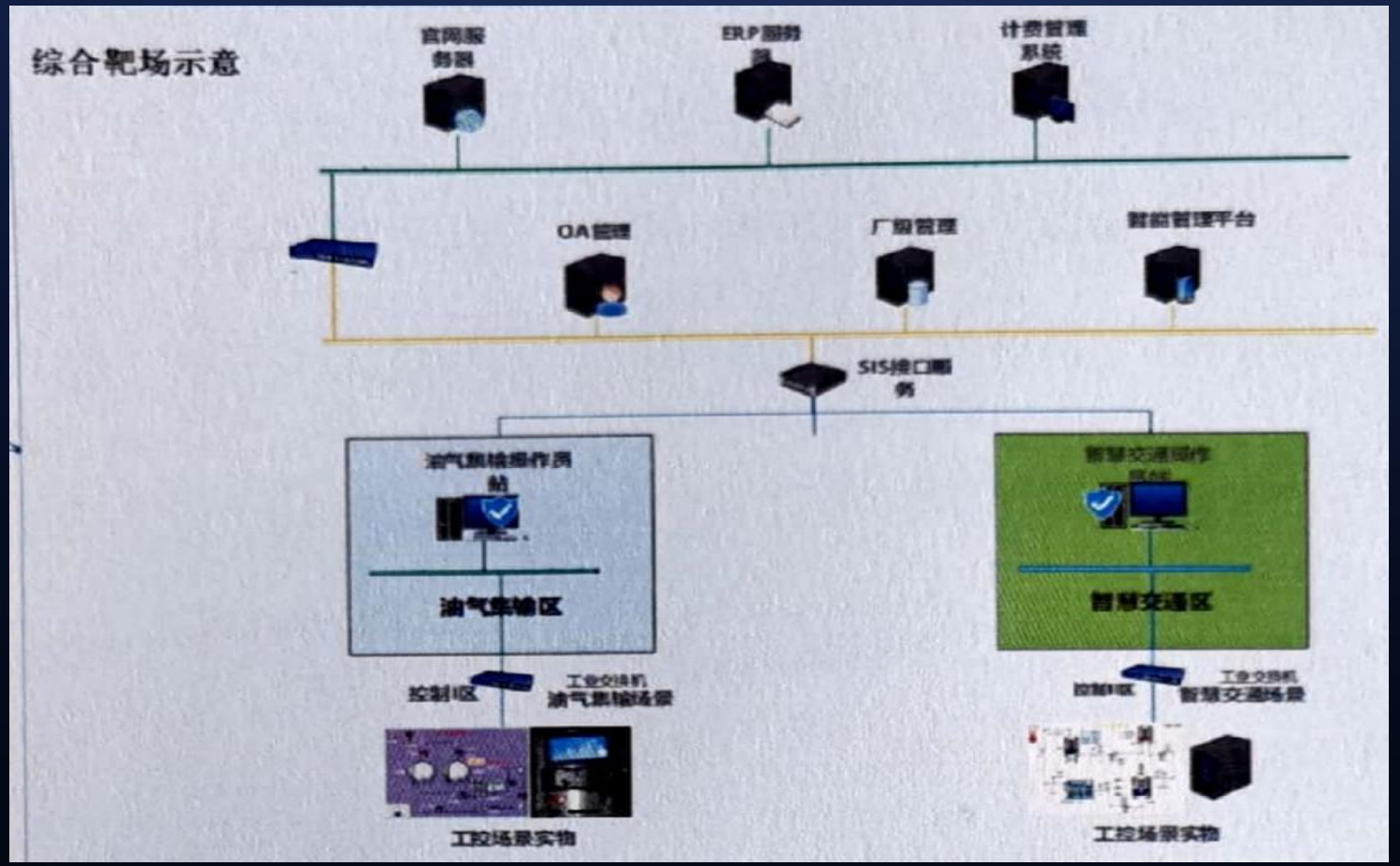
有轮次的说法，一般为10分钟一轮次，一轮次后，各队伍答案会改变，check脚本也根据轮次来工作。

综合渗透

Nantian

赛制：一般为团队赛；

出题方式：给定综合靶场，层层渗透得，每个主机一个flag。



技战法

传统CTF

先易后难

比赛时间长，脑子最清醒的时候一定要做最擅长的题。

Misc→web→Crypto→ Reverse→pwn

注意读题目，一般题目会给一定的提示，简单题目通过读题就能做出来。

例如： URLBASEBASEROT等

学会利用工具：

Mics：binwalk、foremost、 Stegsolve、 CTFCrackTools

Crypto：rsa解密脚本

Reverse：IDA

Pwn：pwntools（https://github.com/Gallopsled/pwntools）

工具+靶场

Nantian

CTF工具包

国外：https://ctftime.org/（各类资讯、考点都比较新）

国内：

Buuctf靶场：https://buuoj.cn

Xctf攻防世界：https://adworld.xctf.org.cn/

i春秋、墨者学院等

技战法

AWD

比赛准备：

1、提前把各种可以复制粘贴的东西都放到记事本里（平台地址 各种账号密码）；

2、Ssh sftp等各种软件提前准备好学会利用工具；

3、提前准备好awd的攻击框架 打开D盾 等webshell查杀工具，直接扫后门；

4、 根据后门的路径、参数等，简单写一下攻击框架的代码，开始批量利用；

攻击：

1、打首轮

2、马上就要备份（源码为主 数据库一般不会有事 但推荐也备份 只是不在首轮去做数据库的备份）

3、打完首轮后，立马进行权限维持，注入不死马等

技战法

Nantian

AWD

防护：

1、抓流量，部署抓流量脚本

1）知道别人怎么打的你，知道你自己哪里有漏洞，然后抄作业；

2）判断ip地址 1个地址和其他地址明显不一样 判断出check都检查了哪些页面，维持这些页面的正常即可， 其他的页面都可以删了;

2、通用防御

1）上waf等

搅浑水：

1）删别人文件;

2）修改别人的网站配置文件，让别人找不出问题在哪;

3）去找交换机或防火墙设备等，修改访问控制策略，不然别的队伍打你;

工具+靶场

Nantian

AWD工具包

AWDl练习靶场：https://github.com/zhl2008/awd-platform

技战法

综合渗透

赛前准备：

准备好隧道搭建工具，综合靶场中的网络可能会有三层代理，学会使用工具：Venom等；

准备好提权工具等；

准备好内网共享工具或方法；

比赛开始：

信息收集，先把第一层网络中的资产收集到位；

做好分工和配合，层层突破，循序渐进；

技战法

Nantian

综合渗透

拿下系统应用+数据库+服务器

渗透方案&思路：

1：分析框架+组件（通过框架和组件漏洞获取服务器权限，通过服务器获取数据库权限、从数据库中获取应用账号密码，登录应用系统获取权限）

2：通过应用系统获取服务器+数据库权限（登入系统后通过文件上传、命令执行等获取服务器+数据库权限）

1）任意用户注册、忘记密码等是否存在逻辑漏洞，如注册系统管理员账号、重置管理员密码等；

2）收集信息，生成字典后，通过暴破登入系统；

3）未授权漏洞，无需登录直接获取系统权限；越权漏洞：越权获取应用系统管理员权限

3：通过数据库获取应用系统+服务器权限（sql注入漏洞）

1）数据库用户为dba权限，尝试直接写码或反弹服务器权限；

2）数据库用户不是dba用户，获取应用系统账号密码，通过应用系统获取服务器权限；

4：其他方式（旁站、开放端口、中间件等）

工具+靶场

Nantian

综合渗透：红日靶场等

书籍：https://book.nu1l.com/《从0到1：CTFer成长之路》


谢谢