
160
140
120
100
80
60
40
20
0
113,67
83,4843
102,4293
143,4768
79,8216
124,6581
140,8245
29,049
123,3951
Information technology
Telecommunications
Wood
Steel industry
Oil and Gas
Finance
Electronic commerce
Securities
Nuclear energy industry 2,30%
Industrials 11,15%
Chemical production 9,87%
Air transport 6,32%
Electronic commerce 6,73%
Securities 9,77%
Information technology 9,00%

CTF概述

CTF概述

- CTF概述
  - 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。CTF起源于1996年DEFCON全球黑客大会，以代替之前黑客们通过互相发起真实攻击进行技术比拼的方式。发展至今，已经成为全球范围网络安全圈流行的竞赛形式，2013年全球举办了超过五十场国际性CTF赛事。而DEFCON作为CTF赛制的发源地，DEFCON CTF也成为了目前全球最高技术水平和影响力的CTF竞赛，类似于CTF赛场中的“世界杯” 。
- CTF类型
  - CTF夺旗赛
  - AWD攻防对抗
  - 靶场渗透
  - BBFS战争分享

CTF夺旗赛

CTF夺旗赛模式（Jeopardy）常见于线上选拔比赛。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，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，类似于 ACM 编程竞赛、信息学奥林匹克赛，根据总分和时间来进行排名。解题赛考核的知识包括了杂项、加解密、逆向分析、Web安全、二进制安全等



CTF夺旗赛

夺旗赛常见规则

- 分值奖励：一血：5%、二血：3%、三血：1%
- 分值共享：题目分值与答对人数成反比
- 防作弊：
  - 附件型：多个附件对应多个flag，随机分发
  - 靶机型：随机flag

CTF夺旗赛

Crypto	Reverse	Web	Pwn	Mobile	Misc
密码学，题目考察各种加解密技术，包括古典加密技术、现代加密技术甚至出题者自创加密技术；	逆向主要指对软件的结构，流程，算法，代码等进行逆向拆解和分析。	涉及到常见的Web漏洞，诸如注入、文件上传、文件包含、代码执行、SSRF、XXE、反序列化、SSTI等漏洞；	二进制安全，包含栈溢出、堆溢出、格式化溢出、整数溢出等主要是通过程序本身的漏洞，编写利用脚本破解程序拿到主机的权限	移动端安全，通常题目会提供一个APK文件，用于逆向，也可能是漏洞利用；	安全杂项，信息隐藏、流量分析、电子取证、数据分析等；

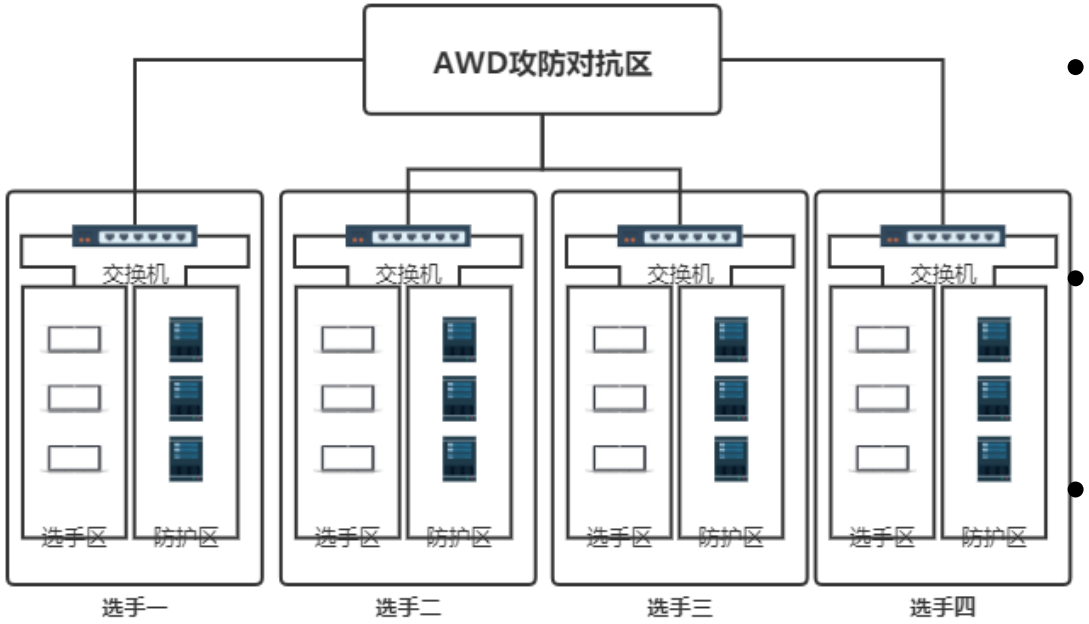
AWD攻防对抗

攻防对抗常见规则

- 防御
  - 防御时间：0-30分钟
  - 不定时check
- 攻击
  - Flag会定时变更
- 分值
  - 零和机制

AWD攻防对抗

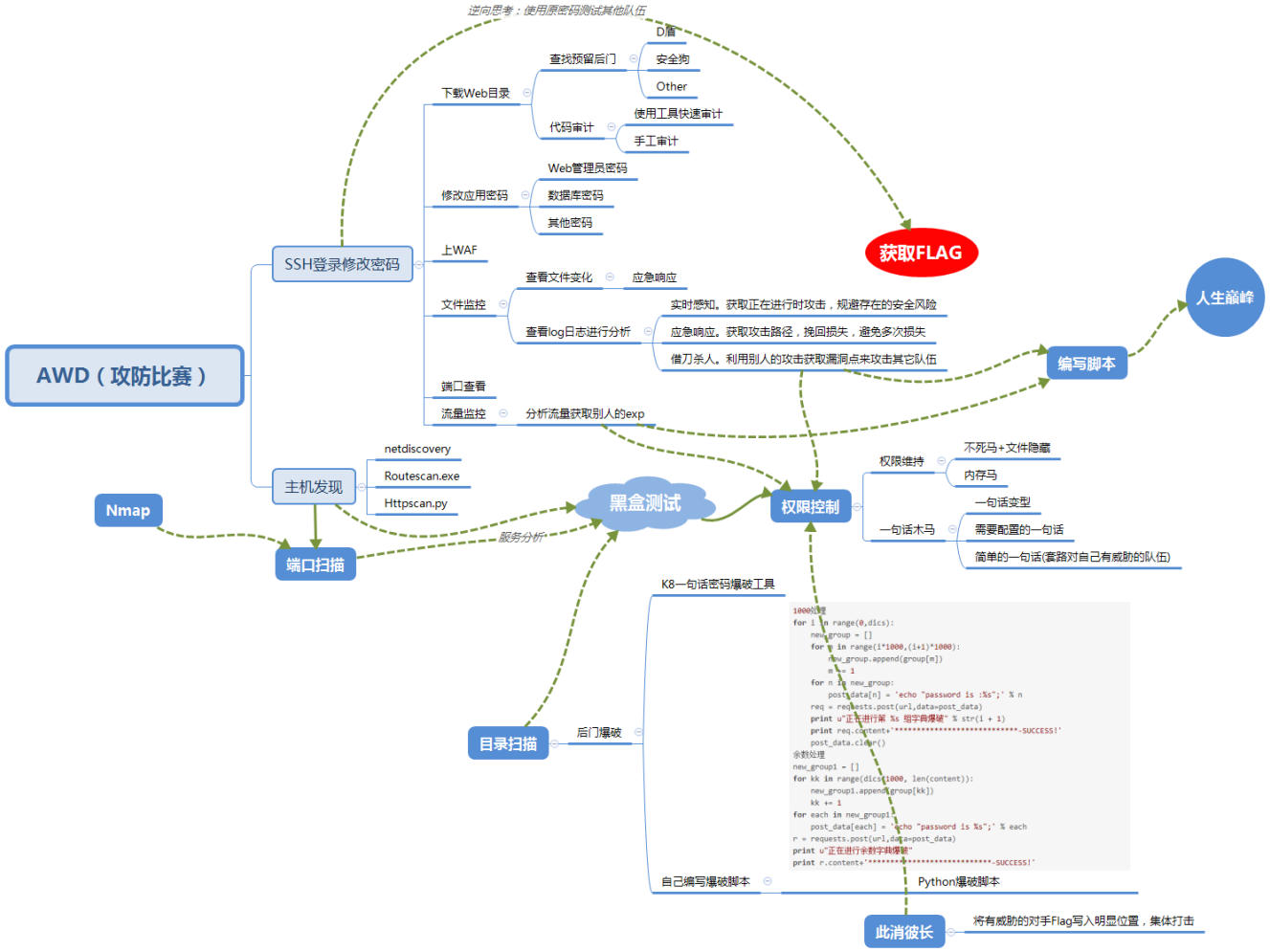
常规AWD



AWD Plus

- 1. 攻击：选手攻破某一赛题，获取flag提交到平台，证明具有对该题攻击能力
- 2. 防御：选手提交防御脚本，平台会运行exp和check，如果能check过且exp攻击失败则认为防御成功
- 3. *分钟一轮，平台会自动扣掉不具备某题防御能力的队伍分数然后平分给解题成功的队伍

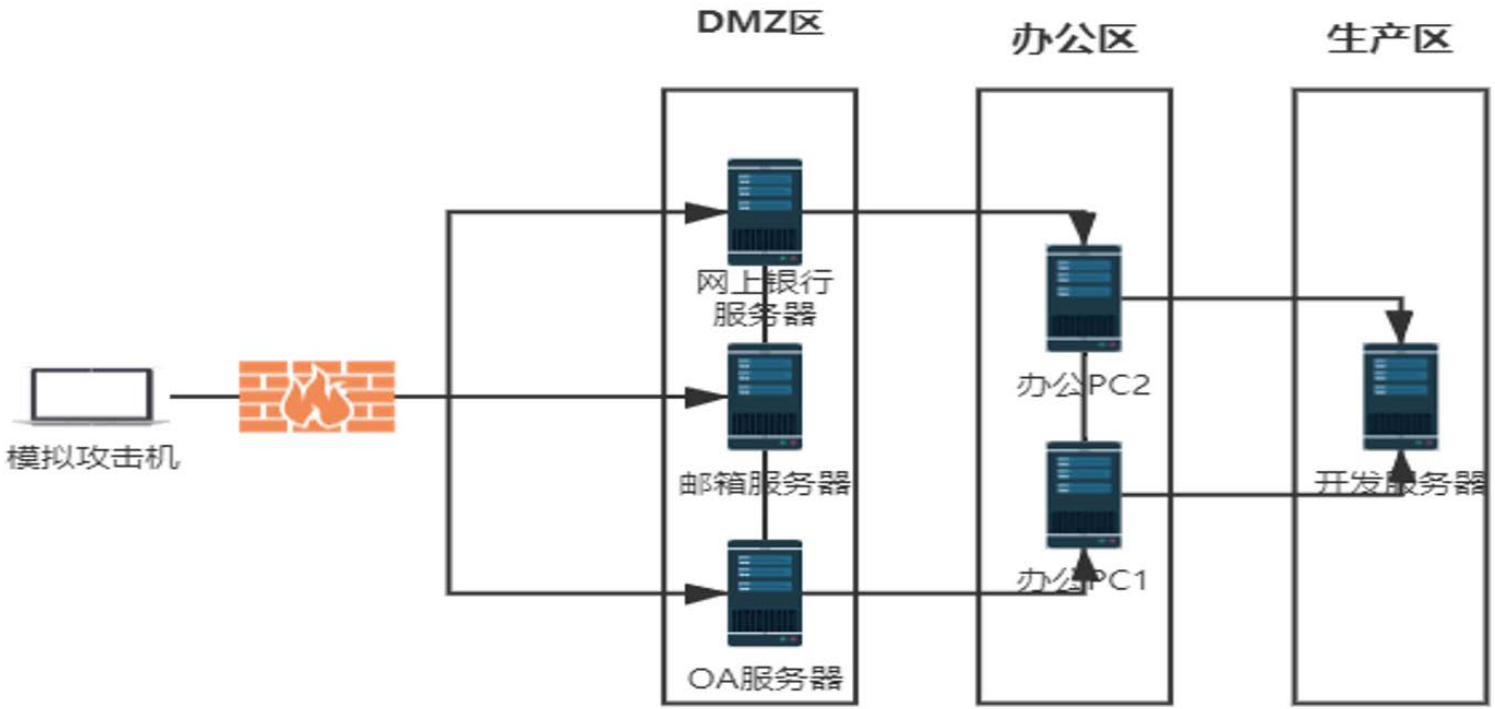
AWD攻防对抗


逆向思考：使用原密码测试其他队伍
AWD（攻防比赛）
SSH登录修改密码
下载Web目录
查找预留后门
D盾
安全狗
Other
代码审计
使用工具快速审计
手工审计
修改应用密码
Web管理员密码
数据库密码
其他密码
上WAF
文件监控
查看文件变化
应急响应
查看log日志进行分析
实时感知。获取正在进行时攻击，规避存在的安全风险
应急响应。获取攻击路径，挽回损失，避免多次损失
借刀杀人。利用别人的攻击获取漏洞点来攻击其它队伍
端口查看
流量监控
分析流量获取别人的exp
获取FLAG
编写脚本
人生巅峰
主机发现
netdiscovery
Routescan.exe
Httpscan.py
Nmap
端口扫描
服务分析
黑盒测试
权限控制
权限维持
不死马+文件隐藏
内存马
一句话木马
一句话变型
需要配置的一句话
简单的一句话(套路对自己有威胁的队伍)
目录扫描
后门爆破
K8一句话密码爆破工具
自己编写爆破脚本
Python爆破脚本
此消彼长
将有威胁的对手Flag写入明显位置，集体打击

靶场渗透

靶场渗透常见规则

- 多层网络
- 多个靶机
- 多个flag
- Flag位置
  - 管理员后台
  - 网站根目录
  - 服务器根目录
  - 数据库



竞赛准备

团队合作

- 团队角色
  - 领队、队长、队员
- 技术角色
  - Web师傅、二进制师傅、其他等

竞赛准备

攻击环境

- 常用的CTF工具
- 常用的框架
- 常用的脚本

学习途径

CTF练习平台

- https://ctftime.org/
- https://ctf.bugku.com/
- https://buuoj.cn/

学习途径

CTF学习平台

- https://ctf-wiki.github.io/ctf-wiki/