AWD（Attack With Defence）模式比赛技巧

第1课 AWD比赛模式概述

CTF中的线下赛又被称为AWD(Attack With Defence)。AWD对于选手的攻击能力，防御能力以及团队合作能力都有着很高的考验。比赛中有多支队伍，每个队伍维护多台服务器，服务器中存在多个漏洞，利用漏洞攻击其他队伍的服务器可以进行得分，修补漏洞可以避免被其他队伍攻击失分。

参赛人数多，规模大，更考验速度(解题+实现攻击)和团队协作(赛前分工+赛中分工)。战略有时候也很重要

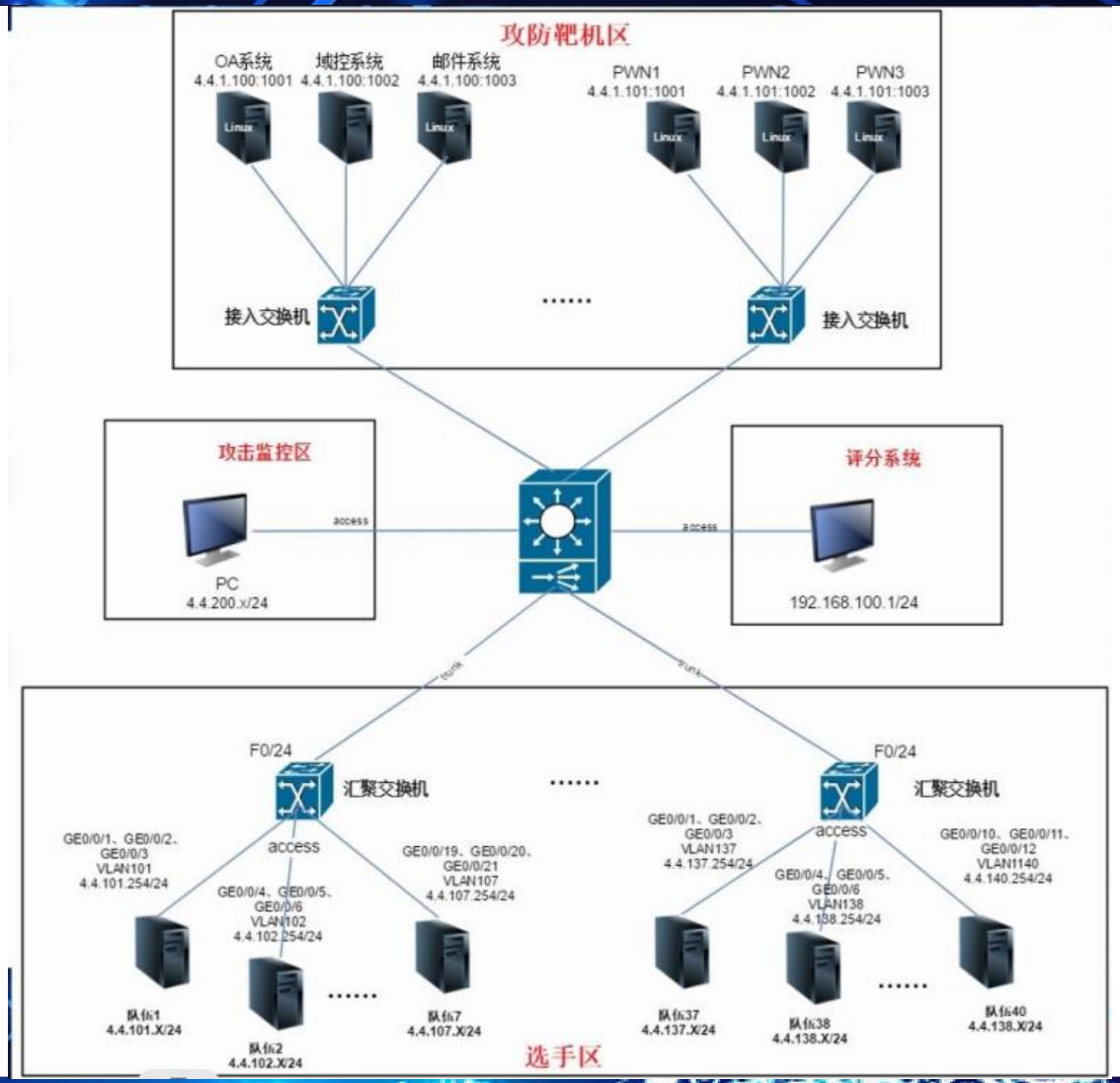
赛前起手式

情报搜集和分析

趁手的工具准备

情报搜集和分析——比赛网络拓扑

某场AWD线下赛的选手向网络拓扑图：



比赛时需要运维的服务器的ssh

用户名和密码

```
class SSH:

    def __init__(self, host, port, user, passwd):
        self.host = host
        self.port = int(port)
        self.user = user
        self.passwd = passwd
        self.ssh = None

    def startup(self):
        try:
            ssh = paramiko.SSHClient()
            ssh.set_missing_host_key_policy(paramiko.AutoAddPolicy())
            ssh.connect(self.host, self.port, self.user, self.passwd)
            t = paramiko.Transport((self.host, self.port))
            t.connect(username=self.user, password=self.passwd)
            self.ssh = ssh
            print("[+] Connect successfully")
            return True
        except BaseException as e:
            print("[-] Connect ERROR!! {}".format(e))
            return False

    def command_exec(self, command):
        try:
            std_in, std_out, std_err = self.ssh.exec_command(command)
            out = std_out.read()
            err = std_err.read()
            if out != b'':
                print(out.decode().rstrip("\n"))
                return out.decode().rstrip("\n")
            if err != b'':
                print(err.decode().rstrip("\n"))
        except BaseException as e:
            print("[-] Could not exec command! {}".format(e))
        return 0
```

某场比赛的比赛规则：

在攻防对抗混战比赛中，选手需要加固自己防守的靶机，同时攻击对方的靶机。比赛初始分值为 1000，攻陷对方一台靶机并获得 KEY 值提交得 10 分，被对方攻破丢失 10 分。比赛 KEY 值每 1 分钟变换一次。每阶段每队只能提交一次 flag，多次提交无效；攻击方式只能以拿到 flag 为目的，不可对网站正常运营产生影响。

不仅要做的快，提交策略也很重要

•比赛工位的位置安排

·shell管理工具

·putty(https://www.chiark.greenend.org.uk/~sgtatham/putty/)

·mobaxterm (https://mobaxterm.mobatek.net/)

·xftp (https://www.netsarang.com/zh/xftp/)

·xshell (https://xshell.en.softonic.com/)

- web源码自动审计工具
- seay
- rips
- cobra

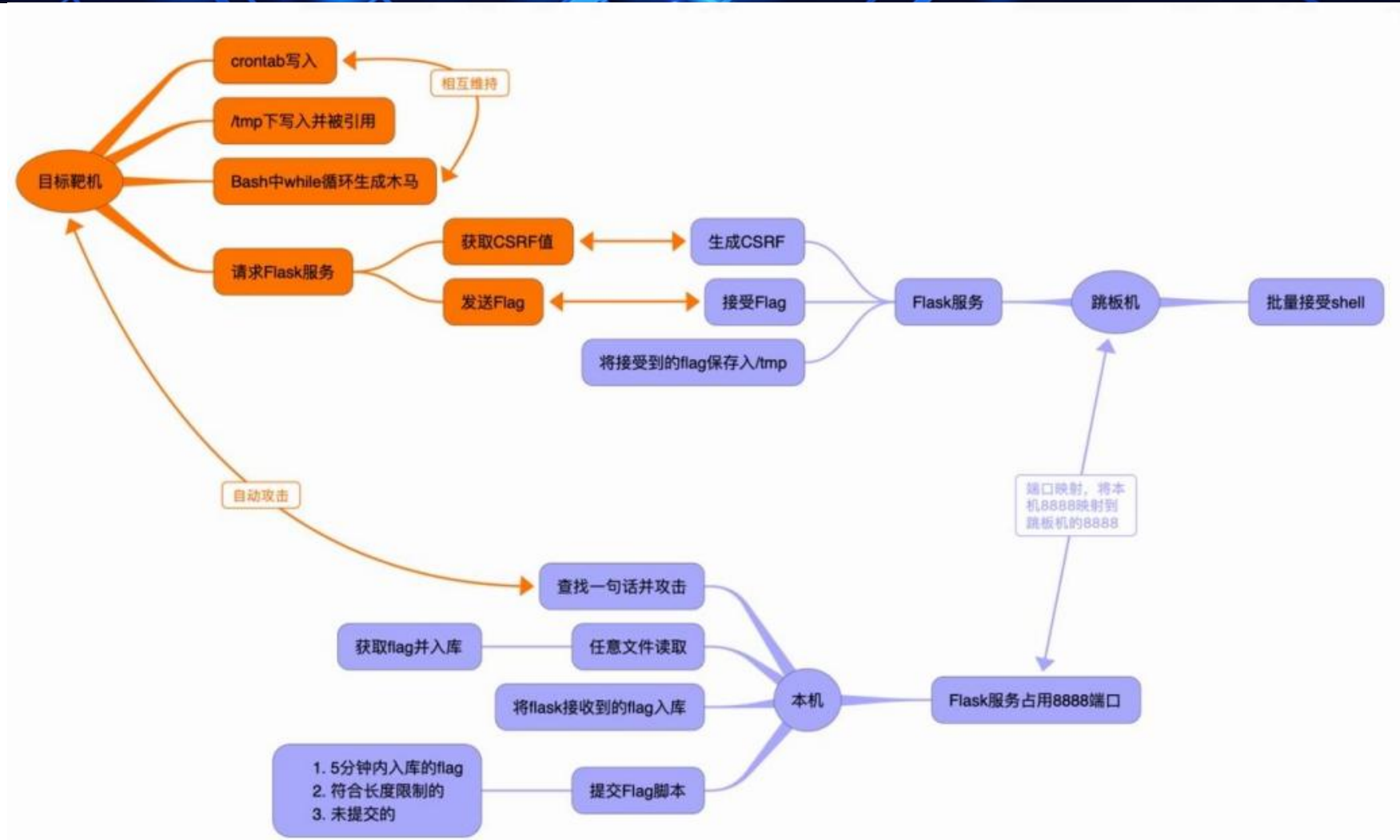
以防万一，准备一手信息嗅探

扫描工具：nmap、zenmap、masscan……

识别工具：whatweb、常见的一些cms识别脚本……

路径探测：dirsearch、御剑……

常规的AWD思路体系图



谢谢观赏