[CTF从0到1学习] 一、CTF 概述

原创

南岸青栀* 于 2021-11-13 23:13:02 发布 3347 收藏

分类专栏： CTF wp 文章标签： 安全 web安全 网络

本文链接：https://blog.csdn.net/qq_43710889/article/details/121251926

[CTF从0到1学习] 一、CTF 概述

> 哈哈，在学校图书馆借到的一本比较好的讲CTF的书籍，因为有配套资料。感觉不错，准备研读一波。先做一个引言吧"

首先大家能搜到这篇文章，也一定对CTF有一定了解，亦或是对网络安全感兴趣。这篇文章会分享CTF的起源，模式，所需要的基本技能的一个概述。

文章目录

CTF起源

CTF起源与1996年的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。其实早在1993-1996年，黑客们就通过比拼网汽车里装的人数多少进行竞赛。在1996-2991，比赛的重心有回归到黑客技术上，但这个阶段模式比较混乱。由于没有明确的竞赛规则与专业的裁判和竞赛环境，因此带来的争议较多，同时比赛的观赏性也不高。

从2002年开始，DEFCOM CTF由专业团队搭设比赛平台、命题采用自动化评分。2013年全球巨变了五十多场国际性CTF，2016年国内有记录的CTF多达百场。DEFCON CTF是目前全球最高水平和影响力的CTF。

国内最早的CTF是BCTF，由清华的白莲花战队组织，是国内首个国际CTF（ rank=40）

CTF模式

1.解题模式：

参赛队伍通过互联网或现场网络参与。这种竞赛模式与ACM、信息学奥赛比较类似，按照解决网络安全技术挑战题目的分支和时间排名。题目包含Web渗透，密码学，信息隐写，安全编程，杂项，逆向工程，漏洞挖掘与利用等类别。

2.攻防模式

AWD模式的CTF，参赛队伍在网络空间中互相进行攻击和防御，通过挖掘网络服务漏洞并攻击对手服务得分，同时通过修补自身服务漏洞进行防御避免丢分。这种赛制中，不仅比拼参赛队员的智力和技术，也比拼体力（通常会持续48小时以上），同时体现团队内部的分工与协作。

3.混合模式

结合题解迷失和攻防模式，例如参赛队伍通过解题获取一些分数后，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。

CTF必备的基础技能

1.网络

CTF选手首先要对网络有一个基本的了解，也别是一些网络相关的关键术语和设备名称，如TCP/IP、网关、协议、网线、集线器、路由器、交换机、防火墙等。

2.操作系统

操作系统是管理和控制计算机硬件与软件资源的计算机程序，是直接运行在'裸机'上的最基本的系统软件。CTF考试环境基于windows、unix、Linux这几种环境搭建，必须对操作系统的常用命令、快捷键和设置了如指掌，对每一种操作系统环境下的常见文件格式、种类和使用方法有一定掌握。

CTF选手来说，手写学习基本的操作系统理论，了解操作系统的发展历史、组成结构和基本功能，**其次重点掌握linux操作系统，特别是结构、各类常用命令、文件类型等知识点**。应该重点掌握centOS，Ubuntu和Fedora。

3.编程

在CTF做题环节中，经常需要实现数据计算、文本分析、软件逆向等操作，通过编程，我们可实现解题思路，将自己的想法变为具体实现。建议学习python，php，c，c++，java等编程语言的知识。

4.数据库

数据库是数据安全最核心的部分，所有数据信息都存储在各种数据库中，。献血定一种数据库深入学习原理和运行机制，待了解基本的知识框架后再进行安全特性学习。建议学习的数据库有SQL Server，MySQL，Redis,Oracle，MongDB

CTFd环境搭建

CTFd是目前最流行的开源CTF框架之一，是一个由python开发的框架。

我是用的是debian11+ctfd最新版+docker

debian11安装

docker安装

https://www.bilibili.com/read/cv13641063

安装docker-compose

```
1.安装docker-compose
curl -L https://get.daocloud.io/docker/compose/releases/download/1.25.5/docker-compose-`uname -s`-`uname -m` > /
usr/local/bin/docker-compose
2.更改权限
chmod +x /usr/local/bin/docker-compose
3.查看版本
docker-compose --version
```

下载CTFD

```
git clone https://github.com/CTFd/CTFd.git
chmod -R 755 /CTFd
```

安装CTFd

CTFd安装有两种方式:
docker安装方式 在这里我推荐使用docker安装方式

docker方式安装

```
cd CTFd/

docker-compose up -d
```

接下来就是等待安装完成，安装完成之后可以用http://ip:8000进行访问

> 参考 CTF安全竞赛入门 主编启明星辰网络空间安全学院