通俗理解CTF网络安全比赛

原创

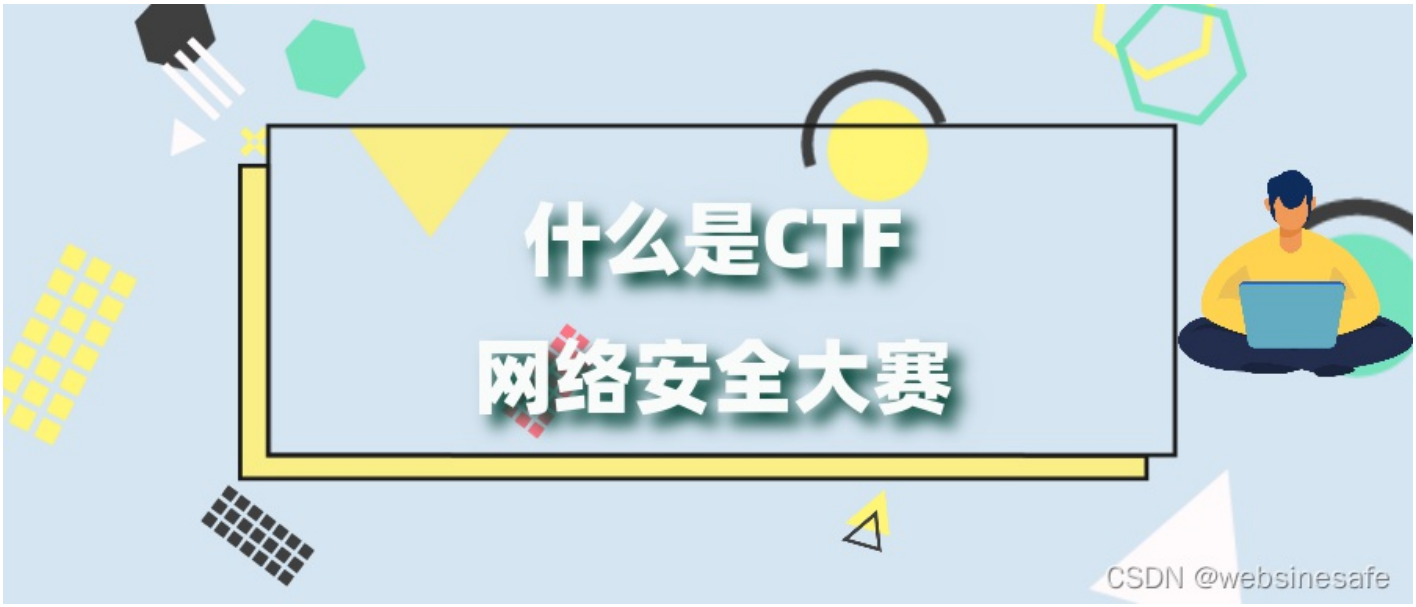
websinesafe 于 2022-03-02 15:17:12 发布 764 收藏 2
分类专栏： 渗透测试公司 网站漏洞修复 网站安全漏洞检测 文章标签： 安全 web安全 CTF比赛


渗透测试公司 同时被 3 个专栏收录
52 篇文章 6 订阅
订阅专栏


网站漏洞修复
43 篇文章 3 订阅
订阅专栏


网站安全漏洞检测
87 篇文章 10 订阅
订阅专栏

什么是CTF?下面我们对课程进行一个内容的讲解，在讲解之前我们首先来对ctf进行对应讲解，ctf是当前1种非常流行的信息安全竞赛形式，其英文名可翻译为夺得flag，也可翻译为夺旗赛。其大体流程是参赛团队之间通过攻防对抗程序分析等形式，首先从主办方给出的比赛环境中获得一串具有一定格式的字符串或其他内容，并将其提交给主办方，从而得的对应分数，为了方便称呼，我们把这样的内容称之为flag，当然在ctf比赛当中涉及内容非常繁杂，我们需要利用，所有可以利用的方，法获得对应的flag，以上就是咱们ctf这样一个比赛形式。



下面咱们介绍一下我们所用的实验环境，每节课当中都会提供对应的攻击机kali Linux和对应的靶场机器Linux，但是学员需要下载攻击机和靶场机器之后自行搭建测试环境，并对靶场机器进行对应的渗透测试，取得对应的flag值。那么咱们在拿到实验环境之后，大家需要做的是什么？大家需要搭建完成之后,抱有这样一个目的,要获取靶场机器上的flag值。咱本门课程面向的对象,定位在一个中等难度的程度上，需要咱们的学员具备一定基础，比如了解HTTP协议，以及会使用一些基本的，安全工具，其中就包括book、suit、circum，map以及metabolit这样一些基本安全工具,当然对于课程中内容无论是想要入门的ctf小白或者是具备一定经验的ctf选手以及网络爱好者，都是一门不错的学习资料。

咱们课程内容涉及了这样几个方面，首先课程当中涉及了外部安全当中的多种漏洞以及ssh，FTP等服务的，漏洞咱们通过获得靶场机器的shell，但是该shell并不是root权限，那我们这时候就需要涉及到各种提权方式，其中我们讲解了内核，出密码复用以及定时任务等方式，对靶场机器进行对应的提权。当然我们本门课程完全是以实战的方式，对靶场进行渗透测试获取对应的flag值，学员在掌握该课程当中的内容，切勿用于非法用途，否则后果自负。那么咱们就开启对应的ctf之旅。