CTF入门介绍

原创

tuzkizki 于 2020-11-19 19:42:20 发布

文章标签： 安全 网络安全 web

本文链接：https://blog.csdn.net/tuzkizki/article/details/109822912

CTF入门介绍

前言

信息安全是一个极其庞大的领域，囊括了网络、web、系统、工控、无线、社会工程学等领域。广义上来说，只要信息存在，就会有安全问题。

目前人们对信息安全的普遍印象只停留在最表层的web安全，也可以说网站安全。

注：作者见识浅薄，很多地方的描述不太恰当，还请见谅。

行业前景

先聊一聊国内的安全就业前景，由于行业门槛较高，目前行业内中高端人才紧俏，低端人才过剩，薪酬两极分化较大，薪酬天花板高的同时，中低端人才的薪酬位于均值以下。国内安全人才主要聚集于互联网IT老牌大厂（腾讯、阿里、百度等）和专注于安全行业的公司（奇安信、深信服、天融信、绿盟等）中。

CTF

本文的重点是CTF中的Web安全，那什么是CTF呢？

CTF，Capture The Flag，中文译为夺旗赛。是黑客之间的安全技术竞赛，比赛内容包括但不限于Web安全、逆向工程、pwn等。

通常有以下三种模式：

- 解题模式（Jeopardy）

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，这种模式的CTF竞赛与ACM编程竞赛、信息学奥赛比较类似，以解决网络安全技术挑战题目的分值和时间来排名，通常用于在线选拔赛。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。

- 攻防模式（Attack-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。攻防模式CTF赛制可以实时通过得分反映出比赛情况，最终也以得分直接分出胜负，是一种竞争激烈，具有很强观赏性和高度透明性的网络安全赛制。在这种赛制中，不仅仅是比参赛队员的智力和技术，也比体力（因为比赛一般都会持续48小时及以上），同时也比团队之间的分工配合与合作。

- 混合模式（Mix）

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。采用混合模式CTF赛制的典型代表如CTF国际CTF竞赛。

这里介绍一下CTF常见的四大板块：

- Web安全：Web安全也可以称之为网站安全，是黑客最为常见的领域，黑客会使用各种手段进行信息搜集，挖掘出网站存在的漏洞（如SQL注入、文件包含、DDOS、跨站脚本攻击等），并对其进行利用，以获得数据库、上传恶意脚本对用户进行攻击等。

Web安全具有广而杂的学习特点，学习者需要具有编程基础（不一定要会，但要能大概看懂，会涉及到Python、HTML、CSS、JavaScript、数据库以及PHP，Python/PHP要有一门达到精通，以便后续编写脚本和工具），系统基础（包括Windows、Linux一些简单的命令行操作以及配置）、网络基础（入门级的HTTP协议知识，以及了解网站的组成和运作方式），掌握主流漏洞的原理以及攻击、利用手段。

行业发展方向有（按难度从大到小）：

安全研发工程师、渗透测试工程师、安全服务工程师、安全运维工程师、安全售前工程师等

- 逆向工程：逆向工程相较Web安全更加底层，黑客需要通过对软件的逆向得到其组织结构乃至部分源码，针对其存在的漏洞进行利用修改以攻破系统、破解软件。

其最为常见的应用是游戏外挂、软件破解，具有专而精，学习曲线陡峭且反馈较低的特点，漏洞的挖掘往往需要较长时间，需要学习者掌握汇编、C/C++的反汇编、CPU架构等知识。

行业发展方向有：逆向工程师（包括PC、移动端）、病毒分析工程师

PWN：PWN是CTF中的大爷，学习难度最高，行业内需要高精尖的人才，黑客通过对软件漏洞的挖掘和利用，可以在各种的场景（网站、软件、嵌入式设备等）达到入侵、操纵、破坏系统的目的。

杂项：CTF中最容易入门的模块，但也是最杂的模块，各种奇技淫巧都可以在这里发现，flag会隐藏在文本、图片乃至音频中，也会与以上模块结合

写在最后

如今，随着科技的发展，安全问题日益凸显，政府及各大厂商纷纷举行CTF竞赛，发布SRC漏洞响应平台（白帽子挖掘并提交漏洞赚钱，甚至可以收到offer），安全在走向更重要的位置的同时，行业创新也在不断推动，适合该行业的人具备以下条件：

1. 开放、敢于打破常规的思维
2. 自主学习、终身学习的意识及决心
3. 对网络安全行业的热爱
4. 喜欢瞎折腾

PS: 本文作者菜鸡一枚，写作目的仅为让爱好者对行业有大概的了解，还请路过的大佬见谅。