CTF相关知识

转载

无晴_ 于 2020-12-20 18:42:21 发布 212 收藏
分类专栏： ctfhub
原文链接：https://www.ctfhub.com/#/skilltree

CTF简介

CTF（Capture The Flag，夺旗赛）CTF 的前身是传统黑客之间的网络技术比拼游戏，起源于 1996 年第四届 DEFCON，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。 CTF是一种流行的信息安全竞赛形式，其英文名可直译为“夺得Flag”，也可意译为“夺旗赛”。其大致流程是，参赛团队之间通过进行攻防对抗、程序分析等形式，率先从主办方给出的比赛环境中得到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，从而夺得分数。为了方便称呼，我们把这样的内容称之为“Flag”。 flag所表示的为目标服务器上存储的一些敏感机密的信息, 这些信息正常情况下是不能对外暴露的。选手利用目标的一些漏洞，获取到flag，其表示的即为在真实的黑客攻击中窃取到的机密信息。 一般情况下flag拥有固定格式为`flag{xxxxx}`，有些比赛会把flag关键词替换，例如我们CTFHub平台的flag为`ctfhub{xxxxx}`，利用固定格式来反推flag也是一种常见的解题思路 通常来说CTF是以团队为单位进行参赛。每个团队3-5人(具体根据主办方要求决定)，在整个比赛过程中既要每个选手拥有某个方向的漏洞挖掘能力，也要同队选手之间的相互配合。

竞赛模式

理论知识

理论题多见于国内比赛，通常为选择题。包含单选及多选，选手需要根据自己所学的相关理论知识进行作答。最终得出分数。理论部分通常多见于初赛或是初赛之前的海选

Jeopardy-解题

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。

不同的是这个解题模式一般会设置 一血(First Blood) 、 二血(Second Blood) 、 三血(Third Blood) ，也即最先完成的前三支队伍会获得额外分值，所以这不仅是对首先解出题目的队伍的分值鼓励，也是一种团队能力的间接体现。

当然还有一种流行的计分规则是设置每道题目的初始分数后，根据该题的成功解答队伍数，来逐渐降低该题的分值，也就是说如果解答这道题的人数越多，那么这道题的分值就越低。最后会下降到一个保底分值后便不再下降。一般称之为动态积分

题目类型主要包含 Web 网络攻防 、 RE 逆向工程 、 Pwn 二进制漏洞利用 、 Crypto 密码攻击以及 Misc 安全杂项 这五个类别，个别比赛会根据题目类型进行扩展。

AwD-攻防模式

Attack **w**ith **D**efense(AwD)全称攻防模式，在攻防模式CTF赛制中，参赛队伍连接到同一个网络空间。主办方会预先为每个参赛队分配要防守的主机，该主机称之为`GameBox`，每个队伍之间的GameBox配置及漏洞是完全一致的，选手需要防护自己的GameBox不被攻击的同时挖掘漏洞并攻击对手服务来得分。在AwD中主办方会运行一个名为`Checker`的程序定时检测选手的GameBox的运行状态。若检测到状态不对则判定该GameBox宕机，按照规则扣除一定分数。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24至48小时左右），同时也比团队之间的分工配合与合作。 AwD通常仅包含`Web`及`Pwn`两种类型的题目。每个队伍可能会分到多个GameBox，随着比赛的进行，最早的GameBox可能会下线，同时会上线新的GameBox。

RHG-自动化[AI自动化]

Robo **H**acking **G**ame(RHG)该利用人工智能或是AI或是自动化攻击程序来全自动的挖掘并利用漏洞，考验选手对于漏洞理解以及工程化能力。比赛开始前(一般为1-4周左右)主办方会给出测试环境以及相关接口文档。选手需要编写自动化程序来请求接口获取题目相关信息，该类程序通常称之为`bot`，在程序中全自动访问并挖掘目标漏洞，完成利用漏洞攻击并获取flag的过程。获取到的flag也由程序自动化提交。RHG因为是由bot全自动进行工作，所以比赛开始即可视为结束。剩下的一切全看参赛选手编写的自动化bot的工作情况。 比赛过程中不允许选手对bot进行任何的操作(包括debug/patch等等)。选手仅能看到自己的bot完成了哪些题。目前的得分情况等等。

RW-真实世界

Real **W**orld(RW) 首次于2018年长亭科技主办的RealWorldCTF中出现，该赛制着重考察选手在面对真实的环境下的漏洞挖掘与利用能力。通常RW模式出题也会围绕着能够应用于真实渗透攻击当中的漏洞，一般来说RW常见题型为VM/Docker逃逸、针对浏览器的攻击、针对IoT/Car等设备的攻击，Web类攻击等等 在RW赛制中会有一个`Show Time`，当选手认为自己已经可以完成题目时，选手可以在比赛平台上提交展示申请，由工作人员根据申请先后顺序进行展示排期。选手展示之前需要上台并连接相关网络，同时现场大屏会切换至目标的正常页面。选手确认连接并测试OK之后开始计时。一般情况下上台攻击的时间为`5`分钟，选手一旦完成攻击现场大屏幕会实时看到攻击的效果，此时裁判会根据效果是否符合题目要求来判定该题是否完成。如5在攻击时间内依然未能看到展示效果则认为本次攻击失败。现如今为了防止选手恶意排期。通常会有一个队伍总展示次数(例如在2019年数字经济云安全公测大赛中每个队伍只允许上台展示30次)，选手也需要尽可能保证上台之后攻击的成功率 举个例子。题目要求需要攻击位于比赛网络中的某个网站并将首页替换为包含队伍名称的页面。题目给出该网站的一些信息(源代码/数据库等等)，选手经过本地挖掘漏洞之后，提交展示申请，排期到了之后进行上台展示。注意，因为RW模式是以展示效果来作为题目是否完成的准则，所以在RW模式中并不存在`Flag`。

KoH-抢占山头

King **o**f **H**ill(KoH)是近些年新衍生的一种赛制。该赛制有点类似于AwD，但是又和AwD有些不一样。选手面对的是一个黑盒的目标，需要先挖掘漏洞并利用漏洞控制目标。将自己的队伍标识(队伍名称或是`Token`之类)写入到指定文件。随后在该主机上进行加固等操作防止其他队伍攻击，主办方会定期去检查标识文件，根据文件中的队伍标识来判定本回合分数给予哪个队伍。可以看出KoH也是一种对抗极为激烈的赛制，同时考察选手的渗透能力及防御加固能力。

Mix[混合]

混合模式结合了以上多种模式，现如今单一的赛制已经无法满足比赛及选手的参赛需求，所以大部分比赛会同时以多个模式进行比赛。例如参赛队伍通过解题(Jeopardy)可以获取一些初始分数，然后通过攻防对抗(AwD)进行得分增减的零和游戏，最终以得分高低分出胜负。

比赛形式

CTF比赛一般分为线上赛和线下赛。通常来说，线上赛多为初赛, 线下赛多为决赛, 但是也不排除直接进行

线上

选手通过主办方搭建的比赛平台在线注册，在线做题并提交flag，线上比赛多为解题模式，攻防模式较为少见。通常来说对于长时间未解出的题目，主办方会酌情给出提示(`Hint`)来帮助选手做题。

线下

选手前往比赛所在地，现场接入比赛网络进行比赛，线下多为AWD模式，近年来随着比赛赛制的不断革新，线下赛也会出现多种模式混合进行，例如结合**解题+AWD**，**解题+RW** 等等

题目类型

在CTF中主要包含以下5个大类的题目，有些比赛会根据自己的侧重点单独添加某个分类，例如移动设备(`Mobile`), 电子取证(`Forensics`)等，近年来也会出来混合类型的题目，例如在Web中存在一个二进制程序，需要选手先利用Web的漏洞获取到二进制程序，之后通过逆向或是Pwn等方式获得最终flag

---

Web

Web类题目大部分情况下和网、Web、HTTP等相关技能有关。主要考察选手对于Web攻防的一些知识技巧。诸如`SQL`注入、`XSS`、代码执行、代码审计等等都是很常见的考点。
一般情况下Web题目只会给出一个能够访问的URL。部分题目会给出附件

Pwn

Pwn类题目重点考察选手对于二进制漏洞的挖掘和利用能力，其考点也通常在堆栈溢出、格式化漏洞、`UAF`、`Double Free`等常见二进制漏洞上。选手需要根据题目中给出的二进制可执行文件进行逆向分析，找出其中的漏洞并进行利用，编写对应的漏洞攻击脚本(`Exploit`)，进而对主办方给出的远程服务器进行攻击并获取flag
通常来说Pwn类题目给出的远程服务器信息为`nc IP_ADDRESS PORT`，例如`nc 1.2.3.4 4567`这种形式，表示在`1.2.3.4`这个IP的`4567`端口上运行了该题目

Reverse

Re类题目考察选手逆向工程能力。题目会给出一个可执行二进制文件，有些时候也可能是Android的APK安装包。选手需要逆向给出的程序，分析其程序工作原理。最终根据程序行为等获得flag

---

Crypto

Crypto类题目考察选手对密码学相关知识的了解程度，诸如`RSA`、`AES`、`DES`等都是密码学题目的常客。
有些时候也会给出一个加密脚本和密文，根据加密流程逆推出明文。

Misc

Misc意为杂项，即不包含在以上分类的题目都会放到这个分类。题目会给出一个附件。选手下载该附件进行分析，最终得出flag
常见的题型有图片隐写、视频隐写、文档隐写、流量分析、协议分析、游戏、IoT相关等等。五花八门，种类繁多。