CTF — 入门

原创

Harvey丶北极熊 于 2019-10-29 23:12:39 发布 1591 收藏 45

分类专栏： CTF 文章标签： CTF

本文链接：https://blog.csdn.net/qq_38867330/article/details/102809795

CTF摘要

CTF（夺旗赛）

CTF（Capture The Flag）中文一般译作夺旗赛，在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。CTF起源于1996年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。发展至今，已经成为全球范围网络安全圈流行的竞赛形式，2013年全球举办了超过五十场国际性CTF赛事。而DEFCON作为CTF赛制的发源地，DEFCON CTF也成为了目前全球最高技术水平和影响力的CTF竞赛，类似于CTF赛场中的“世界杯”。

赛事介绍

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”。

竞赛模式

CTF竞赛模式具体分为以下三类：

一、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。

二、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。

三、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iCTF国际CTF竞赛。

CTF — 入门

一、CTF对于我们的意义

1、CTF类似于奥数
2、能力提升：思维能力、快速学习能力、技术能力
3、学校荣誉

二、如何入门

所需基础：
1：编程语言[C/C++、PHP、python、go、汇编语言、脚本语言]
2：数学基础[算法、密码学]
3：脑洞大开[天马行空的想象、推理解密]
4：体力脑力[熬夜突破某个技术]

如何学
1：恶补基础知识[有基础的可以跳过此步]
2：尝试从脑洞开始{Hackgame}
3：持续刷题，从基础题目出发
4：学习信息安全专业知识
5：锻炼体力耐力[学习某个技术通宵，利用好周六周天]
6：练习编写文案能力

分析赛题情况
WEB（网络安全）：
•WEB是CTF竞赛的主要题型，题目涉及到许多常见的WEB漏洞，诸如XSS、文件包含、代码执行、上传漏洞、SQL注入。也有一些简单的关于网络基础知识的考察，例如返回包、TCP-IP、数据包内容和构造。可以说题目环境比较接近真实环境。
•所需知识：PHP、python、TCP-IP、SQL

MISC（安全杂项）：
•MISC即安全杂项，题目涉及隐写术、流量分析、电子取证、人肉搜索、数据分析、大数据统计等等，覆盖面比较广，主要考查参赛选手的各种基础综合知识。
•所需知识：常见隐写术工具、wireshark等流量审查工具、编码知识。

Crypto（密码学）：
•题目考察各种加解密技术，包括古典加密技术、现代加密技术甚至出题者自创加密技术，以及一些常见编码解码，主要考查参赛选手密码学相关知识点。通常也会和其他题目相结合。
•所需知识：矩阵、数论、古典密码学

Reverse（逆向工程）：
•题目涉及到软件逆向、破解技术等，要求有较强的反汇编、反编译扎实功底。主要考查参赛选手的逆向分析能力。
•所需知识：汇编语言、加密与解密、常见反编译工具

PPC（编程类题目）：
•题目涉及到程序编写、编程算法实现，当然PPC相比ACM来说，还是较为容易的。至于编程语言嘛，推荐使用Python来尝试。题目较少，一般与其他类型相结合。
•所需知识：基本编程思路、C,C++,Python,php皆可。

PWN（二进制安全）：
PWN在黑客俚语中代表着攻破，取得权限，在CTF比赛中它代表着溢出类的题目，其中常见类型溢出漏洞有栈溢出、堆溢出。主要考察参数选手对漏洞的利用能力。
所需知识：C，OD+IDA，数据结构，操作系统。

>>>常规发展方向：

A:Pwn+Reverse+Crypto+ppc[偏底层]

B:Web+Misc[发散思维]

Suggestion：先从一个方向做起。

都需要学习的内容

Linux基础
计算机组成原理
网络协议分析
网络安全基础

熟练使用以下工具：

1.burpsuite
2.sqlmap
3.nmap
4.AWVS
5.metasploit
6.cobaltstrike

推荐书籍

A方向

IDA工具使用（F5插件） 逆向工程神器
RE For Beginners(逆向工程入门)
IDA Pro 权威指南
揭秘家庭路由器0day漏洞挖掘技术
自己动手写操作系统
黑客技术宝典

B方向

Web应用安全权威指南(宏观角度让你了解信息安全)
Web前段黑客技术揭秘
黑客秘籍-渗透测试实用指南
黑客攻防技术宝典 Web实战篇
代码审计：企业级Web代码安全架构

怎么学习CTF

从基础题出发

CTF练习

idf实验室：http：//ctf.idf.cn {题目非常基础}
移动安全：http：//canyouhack.it{容易入门}
酷炫化：http://microcorruption.com/login{pwn、Crypto}
题库网站：http://oj.xctf.org.cn/xctf
国外ctf题库：http：//www.wechall.net/challs{国内选手成长摇篮}
http：//smashthestack.org
XCTF实训平台

A方向

Wargame : Http://exploit-exercises.com
Pwn类题目的游乐场： Http：//pwnable.kr/paly.php

B方向

米安的漏洞靶场：

http://moonsos.com/pentest/index.php

国外的XSS测试：

http：//prompt.ml/o

国外的SQL注入的挑战网站

http://redtiger.labs.overthewire.org

工具

burp、IDA

CTF 工具集

https://github.com/thruongkma/ctf-tools

https://github.com/Plakachu/volt

https://github.com/zardus/ctf-tools

https://github.com/TUCTF/Tools

参加比赛锻炼自己的能力

选择一场已存在Writeup的比赛，自己养成写Writeup的习惯

国际比赛：https://ctftime.org

国内比赛：http://www.xctf.org.cn

组建团队

强力成员

1：思维活跃、灵活性、不会钻墙角

2：专注 遇到问题不放弃直到解决

3：耐力 可以一天一夜不睡觉的研究技术

4：团队精神： 责任 凝聚 分享

如何组队

1：新人招募：如何评判新人潜力

2：队员培养：如何快速培养队伍能力[个人能力的成长]

3：梯队有序：如何建立阶层梯队

4：纪律严格：如何拒绝无团队精神的对员{军人的素质，责任感}

忠告：

渗透千万条 安全第一条

无授权 不渗透

```
                    — — Harvey、北极熊
```