一篇文章带你入门CTF（含工具与资源）

转载

anquanniu牛油果 于 2019-06-21 16:28:35 发布 4386 收藏 92

文章标签： ctf CTF比赛 信息安全

CTF（夺旗赛）有助提升安全技术，可为公司企业和组织机构发现安全人才。运用这些工具和框架设计并举行自己的CTF活动吧！

知己知彼百战不殆。想要阻止网络攻击者，就得像网络攻击者那样思考。这是一种需要实践的技术，为了得到这种实践，业界创办了各种CTF比赛，同台竞技，比拼谁能更快更好地拿下服务器，赢取黑客技术名声。

不久以前，这种活动的名声和合法性还令人质疑。如今，即便参赛者多以化名参加，且扮演反派入侵者的角色，CTF也是全然公开而备受推崇的了。

企业安全人员参加CTF是一场白帽子的双赢活动。安全人员在CTF中学习新技术，实践困难情况处理，并与安全界其他大牛把酒言欢建立联系。而且，CTF的作用还不仅止于此。

相当数量的企业实际上将CTF当成了自身社区推广和招聘策略的一部分。CTF能使人对网络安全产生兴趣，尤其是学生；还能帮助企业识别有前途的非传统潜力股人才。

网页一搜就能搜出很多CTF资源列表，其中很多都托管在GitHub上。有些资源是用于构建CTF的，有些则是辅助参赛者的，还有些二者兼而有之，比如awesome-ctf、AnarchoTechNYC和zardus。

最大的资源集是黑客资源。所有黑客资源，无论防御性的还是攻击性的，都是CTF资源：源代码和二进制静态分析、数据包捕获、调试器、反编译器、堆可视化工具、散列值破解器、图像编辑器和网络扫描器等等。每个安全专家都有自己的最爱工具集，但CTF可能会要求他们去寻找新的工具。

Didier Stevens 和他编写的工具非常有用。Didier最初专精PDF、微软Office文档和其他复杂数据文件分析工具，这些工具中很多都能用来实施攻击。如今他的工具集涵盖甚广，对检查和创建恶意文件帮助很大。他的所有工具都托管在GitHub代码库中。

CTF分类

CTF分两派：攻防战模式和解题模式。

攻防战模式
此类CTF中，参赛者分成两队，每队都分配有一个计算环境——可能仅仅是一台服务器。两队任务相同：攻击对方系统，并防御己方系统。每方系统中都含有一些信息性旗标供攻击者找出并夺取。这就是“夺旗赛”这一名称的由来。

攻防模式下，防御者需尽其所能地保护自身服务器：修复所有软件漏洞，甚至模糊不明的那些；防火墙只允许必要的服务出入；确保所有口令都是强口令，账户只具备必要的最小权限……

至于攻击者，需运用渗透技术获取防守方服务器的访问权。诚然，如果攻击者能拿到root权限，竞赛便会很快结束，但根据所涉及的应用和服务，更有限的攻击便已足够。

解题模式
解题锦标赛模式中，多支队伍竞相解决题板上不同分值的难题。解出题目找到旗标的队伍便可将之提交到计分系统，获得相应分数，并继续迎战下一个难题。计时结束之时，得分最高的团队胜出。

因为便于组织和管理，解题模式CTF远比攻防模式更为盛行。

山王模式
山王模式中，每支队伍努力夺下并守住服务器控制权。计时结束之时掌控服务器最久的团队获胜。这种模式是攻防CTF的一个变种。

几种模式各有千秋。解题模式有利于构筑问题解决技术集，山王模式CTF是很好的事件响应、规划和协作的训练场。总之，只要能让安全人员走出舒适区，无论哪种类型的训练都能有所收益。

CTF竞赛哪里寻？
开放竞赛全球各地一直都有。此类活动的一个主要举办地是在CTFtime网站。大部分的活动都是解题模式，比如说，2018年的152项活动中，只有16项是攻防模式，占绝大多数的135项都是解题模式。

若说CTFtime是CTF界的ESPN，那么CTF界的超级碗当属DefCon——拉斯维加斯举办的年度黑客盛会。2018年第26届DefCon的CTF胜出者是DEFKOR00T团队。DefCon CTF 的所有过往记录和完整资料都保存在他们的服务器上。另一项著名CTF随年度NorthSec安全大会而生，在蒙特利尔举办。

DefCon这种大会总有个举办地，但大多数CTF是线上赛。国家网络联盟(NCL)组织面向高中生和大学生的解题模式CTF，有明确的赛季和赛程。

CTFTime上的大多数比赛都是小型安全爱好者团体组织的，但也有例外。2018年末就见证了趋势科技的 CTF 2018，决赛在东京举办，其中囊括了山王模式竞赛。另一方面，2019年4月20，托马斯·杰斐逊科技高中的计算机安全俱乐部将在弗吉尼亚州费尔法克斯举行为期6天的比赛。没错，这确实是个高中举办的CTF。美国空军为初高中学生举行网络爱国者(CyberPatriot)竞赛。

DefCon这种主流安全大会上的CTF确实引人注目，因此很多企业也开展了自己的CTF项目。这种活动是很好的学习途径，还能让安全人员从琐碎的企业日常安全工作中切换出来，换换脑子，充盈下身心。

打造自己的CTF
如何组织自己的CTF？作为企业，惯于改进和支持专业产品的你可能会对自己的发现倍感失望。并没有太多现成的CTF供你选择，但你可以收集无数细节，将它们组织成自身独特和颇具挑战性的竞赛。

与CTF靶场最为接近的东西可能是 OWASP Juice Shop (开放网页应用安全计划果汁商店项目)。OWASP是设计工具和指南以帮助开发者及其他IT人员打造安全应用的安全专家组织。

Juice Shop 是虚构的网店，售卖果汁、T恤等东西，不用在意细节，你只需要知道该网站满载各种已知漏洞就行了。该网站是可定制的，你可以根据自己的意愿更换品牌标志，或将产品更改为自己希望的样子。OWASP的 Juice Shop 有多种形式，包括一个Docker镜像，且运行在单一服务器实例上。

Juice Shop 还含有举办比赛所需的记分牌和账户管理功能。

CTF框架
有些CTF框架相当流行，有些则略默默无闻。CTFd是被安全供应商、大型和黑客组织广泛使用的CTF平台，包含比赛所需的记分牌和其他基础设施，只需添加实际的题目和相应的得分供用户赚取即可。

其他主流框架还有：

Facebook CTF 框架
加州大学圣巴巴拉分校计算机安全实验室iCTF
HackTheArch
Mellivora
NightShade
LibreCTF
picoCTF
CTF工具
谷歌举办一些重大CTF，虽然没有释出其整个框架，但记分牌代码和大部分竞赛题是已经发布了的。

有用工具的列表很长，此处仅举几例抛砖引玉：

> 安全场景生成器(SecGen)：生成半随机的带漏洞虚拟机。
>
> mkctf：以预定义格式创建可输入到框架中的挑战题目。
>
> DVWA：用于展示已知及未知漏洞的开源PHP/MySQL网页应用。用户可选择漏洞(如SQL注入)，并用UI激活之。DVWA没有 Juice Shop 那种有意思的前端，但有时候简单才是最好的。

CTF报告哪里找？
大部分最佳资源，尤其是解题模式CTF的，都是过往CTF的参与者撰写的报告，描述具体问题和解题方法。报告读得够多，自然也就掌握了一些套路。你可以在 GitHub CTF 页面上找到大量报告存档，以及撰写报告的工具。

这些报告描述足够详细，可以据此改变其中一些变量生成你自己的CTF挑战问题。但主要问题是，很多报道存档都只是“待解”问题列表，而且很多作者的写作水平并不高。

在公共云上举办CTF活动
因为CTF的短期特性，我们可以在公共云上举办——分配资源与事后释放资源都很方便，只需为所用到的东西付费。只要你足够谨慎并且按规则行事，你就可以这么做。

AWS有自己的渗透测试规则，因此你得提交一份申请表，而且只能针对一组固定的服务进行测试，不能使用低配实例。因为亚马逊会查找用户在CTF中展现的那类行为并封禁之，所以，请遵守规则并耐心等待批准。

微软对在Azure上的渗透测试有着严格的规则，但不要求事前核准授权。

谷歌也不要求预先授权，只要遵从谷歌云平台可接受使用政策和谷歌云平台服务条款即可。

CTF或许比传统培训更受员工欢迎，效果也更好。安全职位亟待填补的时代，CTF可能会成为很有价值的招聘工具，帮你以客观的方式找出技术水平最高的未来员工人选。将CTF作为最大化团队技术力量的工具，其中有趣的那部分享受纯属免费附赠。

以下是免费资料：

CTF从入门到提升
https://edu.aqniu.com/course/8954

Awesome-ctf：

https://github.com/apsdehal/awesome-ctf

AnarchoTechNYC：

https://github.com/AnarchoTechNYC/meta/wiki/InfoSec#hacking-challenges

zardus：

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

Didier Stevens 的工具库：

https://github.com/DidierStevens/DidierStevensSuite

CTFtime：

https://ctftime.org/

DefCon历届CTF活动完整存档：

https://media.defcon.org/

NorthSec大会：

https://nsec.io/competition/

国家网络联盟(NCL)：

https://www.nationalcyberleague.org/

OWASP Juice Shop：

https://www.owasp.org/index.php/OWASP_Juice_Shop_Project

CTFd平台：

https://ctfd.io/

Facebook CTF框架：

https://github.com/facebook/fbctf

加州大学圣巴巴拉分校计算机安全实验室iCTF：

https://github.com/ucsb-seclab/ictf-framework

HackTheArch：

http://hta.mcpa-stl.org/

Mellivora：

https://github.com/Nakiami/mellivora

NightShade：

https://github.com/UnrealAkama/NightShade

LibreCTF：

https://github.com/easyctf/librectf

picoCTF：

https://github.com/picoCTF/picoCTF-Platform-2

谷歌CTF：

https://github.com/google/google-ctf

谷歌CTF计分板代码：

https://github.com/google/ctfscoreboard

SecGen：

https://github.com/cliffe/SecGen

mkctf：

https://github.com/koromodako/mkctf

Damn Vulnerable Web Application：

http://www.dvwa.co.uk/

CTF报告及撰写工具：

https://github.com/ctfs

AWS渗透测试规则：

https://aws.amazon.com/security/penetration-testing/

Azure渗透测试规则：

https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement

谷歌云平台可接受使用政策及服务条款：

https://cloud.google.com/terms/aup