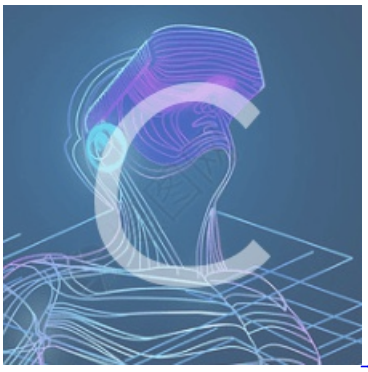
初识CTF

原创

gclome 于 2019-11-09 16:20:58 发布 261 收藏 1

分类专栏： # CTF

本文链接：https://blog.csdn.net/qq_44108455/article/details/102988235



CTF 专栏收录该内容

20 篇文章 0 订阅

订阅专栏

一、夺旗赛(Capture The Flag)

一般线上初选采用传统的夺旗赛模式，也就是在题目中设置一些标识，解题的目的就是为了找到标识并提交。通常包含的题目类型包括MISC、CRYPTO、PWN、REVERSE、WEB、STEGA等。

二、分类

1、MISC(Miscellaneous)类型，即安全杂项，题目或涉及流量分析、电子取证、人肉搜索、数据分析等等。

2、 CRYPTO(Cryptography)类型，即密码学，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。

3、 PWN类型，PWN在黑客俚语中代表着攻破、取得权限，多为溢出类题目。

4、 REVERSE类型，即逆向工程，题目涉及到软件逆向、破解技术。

5、 STEGA(Steganography)类型，即隐写术，题目的Flag会隐藏到图片、音频、视频等各类数据载体中供参赛者获取。

6、 WEB类型，即题目会涉及到常见的Web漏洞，诸如注入、XSS、文件包含、代码执行等漏洞。

三、攻防对抗赛

目前线下决赛普遍采用比较新的对抗模式，也叫AWD模式（Attack withDefence），强调攻防对抗。相比传统的夺旗模式，AWD模式难度更大，对选手综合能力要求也更高。比赛中考察到的知识面更广，除了攻击技术以外，防御技术涉及到漏洞修补、流量分析、系统维护等多方面。

一般的比赛模式是这样的：每支队伍分配虚拟网络，在虚拟网络的边界上会放虚拟的防火墙，一台防守机、一台Flag机。其中防守机上放十几个服务。在攻防对战中，防守的一方要保护自己防守机的上的业务能够正常打开。攻击时则要通过各种攻击手段夺取对手Flag机上的权限。

两种竞赛模式相比，传统的CTF比赛类似于“应试教育”，主要强调攻击和破解。为了训练安全从业人员的防护能力，AWD模式还是非常贴近实战的。更多的了解可参考文章

http://bobao.360.cn/ctf/detail/169.html。

四、练习的推荐：

1：ctf题目练习题库：

https://blog.csdn.net/qq_43679873/article/details/84033547

2：网络安全技术CTF竞赛模式与训练平台

https://mp.weixin.qq.com/s?__biz=MzAwMTMzMDUwNg==&mid=2650879027&idx=1&sn=cb17a302cc6b755c2084b253c3402679&chksm=812ec816b6594100a56a77afcfc1ab456313bbe2bce062e487258021f4998a63a9724dce68ee&mpshare=1&scene=23&srcid=0722SaawVx8zWfyS14TF7sYv#rd

3：CTF训练平台：

i春秋 http://www.ichunqiu.com/

合天智汇 http://www.hetianlab.com/

实验吧 http://www.shiyanbar.com/

胖哈勃 https://pwnhub.cn/index

安全客CTF训练营 http://bobao.360.cn/ctf/index

XCTF实训平台 http://oj.xctf.org.cn/

五、Misc从入门到进阶

https://mp.weixin.qq.com/s?__biz=MjM5MTYxNjQxOA==&mid=2652843368&idx=1&sn=ad346be520aea30e61beb6820bfdafde&chksm=bd5951a58a2ed8b358c6cb991abfa5b64d752bd7618464be08bcc5cb51fdc931d0f44e209be7&mpshare=1&scene=23&srcid=0722YYi3doz4Cx4ZMsjCtA3H#rd

如何判断密文的加密方式：

1、如果密文是十进制，字符范围是“0-9”，可以猜测是ASCII编码；

2、如果密文由“a-z”、“A-Z”和“=”构成，特别是末尾有“=”，那么判断可能是Base64编码；

3、如果密文有“%”，形式为“%xx”和“%uxxxx”，字符范围又是十六进制的“0-F”,判断是escape()函数编码，用unescape()解码；

4、如果密文由“[],(),{},+,!”字符组成的编码通常就是通过Jother解码，可以使用Chrome浏览器对其进行解码，直接将需要解密的内容丢到 Console 回车就OK！

判断出可能的编码方式就可以使用程序或者工具进行解码

六、CTF线下攻防赛总结

https://mp.weixin.qq.com/s?__biz=MzIzNTcyNTI0Mg==&mid=2247485371&idx=1&sn=efc9bdeda63007d261b0dee839dd9c51&chksm=e8e38f6edf9406780c3f83b5d49106b3cae3de773c6e6221e162ba46b6d319199c1c8ffe82bc&mpshare=1&scene=23&srcid=0722iuXQG3XJTF4ZDDXUqAXK#rd