CTF 介绍及杂项

转载

weixin_30478619 于 2019-04-23 20:54:00 发布 1226 收藏 15
文章标签： git 网络 开发工具
原文链接：http://www.cnblogs.com/Hydraxx/p/10758888.html

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”

CTF竞赛模式

单兵作战：理论，杂项，web，pwn，逆向等各种题目

综合靶场：团队形式，攻击相同环境的靶机，只需攻击，不需防御，针对同一个环境，越早拿到flag越好

混战模式：参赛团队即是攻击者，也是防御者

CTF知识点

web：sql注入，xss，文件上传，包含漏洞，xxe，ssrf，命令执行，代码审计等

pwd：攻击远程服务器的服务，会提供服务程序的二进制文件，分析漏洞并编写exp，栈溢出,堆溢出，绕过保护机制（ASLR，NX等）

reverse：逆向，破解程序的算法来得到程序中的flag，对抗反调试，代码混淆等

mobile：主要考察选手对安卓和ios系统的理解

misc：杂项，取证，编解码，加解密，隐写，图片处理，压缩包，编程.....

杂项：

隐写术（steganography）：将信息隐藏在其他载体中，不让计划的接收者之外的人获取到信息

常见载体：

图片：细微颜色差别，GIF图多帧隐藏，exif信息隐藏，图片修复等 ----解题工具 Stegsolve

音频：信息隐藏在声音里(逆序)，信息隐藏在数据里(分析音频数据) ----解题工具 Audition，Matlab

视频：信息隐藏在视频的某个或多个帧里 ---解题工具 Premiere

文件隐写：把多个文件拼接成一个 ---解题工具 binwalk

密码学及编码：

凯撒密码(caeser)：是一种最简单且最广为人知的加密技术。它是一种替换加密的技术，明文中的所有字母都在字母表上向后（或向前）按照一个固定数目进行偏移后被替换成密文。例如，当偏移量是3的时候，所有的字母A将被替换成D，B变成E，以此类推

加解密方法---

在线工具

python的pycipher模块

pip install pycipher

```
>>> from pycipher import Caesar
>>> Caesar(key=5).encipher("XXSEC")
'CCXJH'
>>> Caesar(key=5).decipher("CCXJH")
'XXSEC'
>>>
```

ROT13(Rotate By 13 Places)：可以理解为一种特殊的凯撒密码，套用ROT13到一段文字上仅仅只需要检查字元字母顺序并取代它在13位之后的对应字母，有需要超过时则重新绕回26英文字母开头即可。A换成N、B换成O、依此类推到M换成Z，然后序列反转：N换成A、O换成B、最后Z换成M。只有这些出现在英文字母里头的字元受影响；数字、符号、空白字元以及所有其他字元都不变。因为只有在英文字母表里头只有26个，并且26=2×13，ROT13函数是它自己的逆反

加解密方法---

在线工具

栅栏密码(Rail Fence Cipher)：把要加密的信息分成N组，依次取各组的1，2，3....位

例：

明文：XSECHITMAN

分组：XSEC

HITMAN

密文：XHECITMAN（2栏）

加解密方法---

在线工具

弗吉尼亚密码(Vigenere Cipher)：维吉尼亚密码是在凯撒密码基础上产生的一种加密方法，它将凯撒密码的全部25种位移排序为一张表，与原字母序列共同组成26行及26列的字母表。另外，维吉尼亚密码必须有一个密钥，这个密钥由字母组成，最少一个，最多可与明文字母数量相等

例：

明文：XSEC

密钥：XX

密文：UPBZ

加解密方法---

在线工具

脚本

对称加密算法

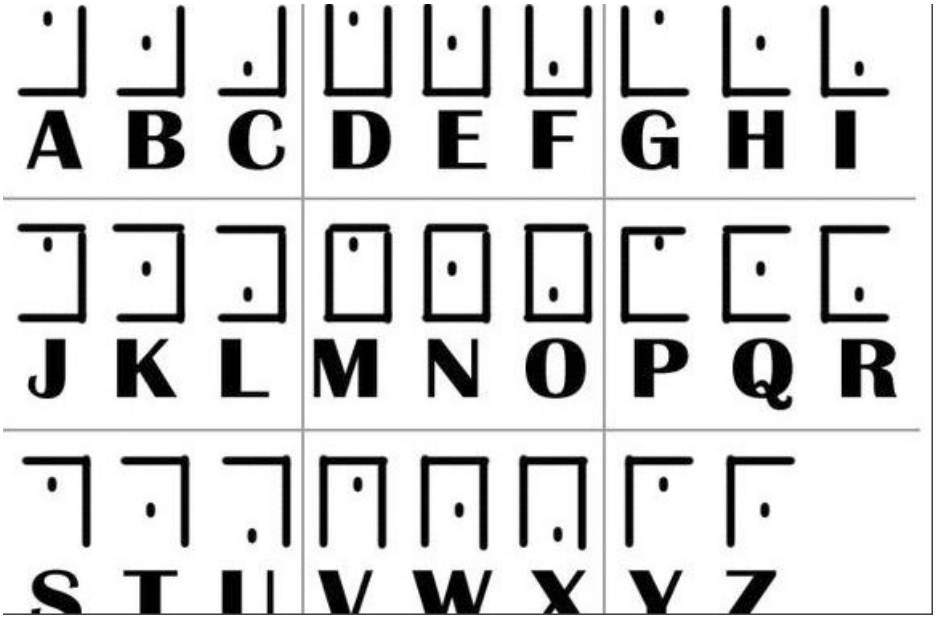
特点：使用加密用过的密钥及相同的逆算法对密文进行解密，才能使其恢复可读明文，即加密解密使用相同的密钥，

常见对称加密算法：DES：3DES，AES等

加解密方法---

在线工具

猪圈密码：**猪圈密码**（亦称**朱高密码**、**共济会暗号**、**共济会密码**或**共济会员密码**），是一种以格子为基础的简单替代式密码。即使使用符号，也不会影响密码分析，亦可用在其它替代式的方法



加解密方法---

在线工具

培根密码：加密时，明文中的每个字母都会转换成一组五个英文字母。其转换依靠下表

A/a	aaaaa	H/h	aabbb	O/o	abbba	V/v	babab
B/b	aaaab	I/i	abaaa	P/p	abbbb	W/w	babba
C/c	aaaba	J/j	abaab	Q/q	baaaa	X/x	babbb
D/d	aaabb	K/k	ababa	R/r	baaab	Y/y	bbaaa
E/e	aabaa	L/l	ababb	S/s	baaba	Z/z	bbaab
F/f	aabab	M/m	abbaa	T/t	baabb		
G/g	aabba	N/n	abbab	U/u	babaa		

加密者需使用两种不同字体，分别代表A和B。准备好一篇包含相同AB字数的假信息后，按照密文格式化假信息，即依密文中每个字母是A还是B分别套用两种字体。

解密时，将上述方法倒转。所有字体一转回A，字体二转回B，以后再按上表拼回字母。
法兰西斯·培根另外准备了一种方法，其将大小写分别看作A与B，可用于无法使用不同字体的场合（例如只能处理纯文本时）。但这样比起字体不同更容易被看出来，而且和语言对大小写的要求也不太兼容。
培根密码本质上是将二进制信息通过样式的区别，加在了正常书写之上。培根密码所包含的信息可以和用于承载其的文章完全无关。
加解密方法---

在线工具

编码和摘要

加密：加密传输信息，保证信息的安全性，通过密钥和密文可以还原原始信息

编码：将数据转换成某种固定的格式的编码信息，方便不同系统间的传输，通过编码信息可以得到原始信息

散列：也叫摘要或哈希，验证信息的完整性，不能通过哈希值还原原始信息

常见的编码：ASCII，Base64，URL，HTML，Unicode，UTF-8，莫斯电码，二维码

隐写术常用的工具

Stegsolve.jar：图片隐写术工具

010Editor/vim：查看16进制数

Photoshop：图片拼接查看

Audition：音频隐写工具

常见密码编码工具

在线加解密工具

python脚本

CTF解密框架（https://github.com/0Chencc/CTFCrackTools）

Burp的Decoder模块

取证技巧

流量分析：

wireshark：协议筛选，追踪流，文件导出

电子取证：

日至分析通过日志分析寻找隐藏在其中的信息

sql注入点的查找，webshell的查找，用户访问敏感路径的查找

杂项题目解题思路

前期准备：

工具，知识

解题过程：判断考点（单个考点？多个考点？）

形成思路（如何尝试？什么工具？）

距离答案只有一步之遥

友情链接 http://www.cnblogs.com/klionsec

http://www.cnblogs.com/l0cm

http://www.cnblogs.com/Anonyaptxxx

http://www.feiyusafe.cn

转载于:https://www.cnblogs.com/Hydraxx/p/10758888.html