初识信息安全

原创

上官大大 于 2021-10-12 20:30:11 发布 9 收藏

分类专栏： ctf 文章标签： 安全

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/haoshangguan/article/details/115279446

版权

ctf 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

信息安全

语言环境的安装：

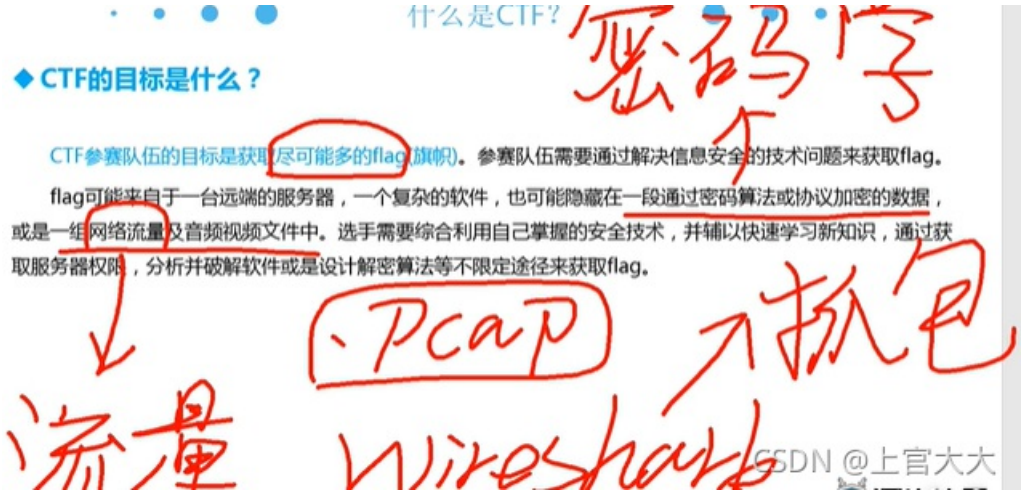
Java,Python,PHP。

常用工具：

vmware，Burpsuite。

CTF:全称：Capture The Flag,直译“夺旗赛“，信息安全技术竞赛。

flag:



CTF比赛形式：

1. 解题模式：通常为在线比赛，目前大多数国内外CTF比赛的主流形式 ，选手自由组队参赛（在线比赛人数一般不做限制）。题目通常在比赛过程中陆续放出。解出一道题目后，提交题目对应的flag即可得分，比赛结束时分高者胜。

2. 攻防模式：通常为现场比赛，多数CTF决赛的比赛形式，选手自由组队参赛，但通常队伍人数会受到限制（3~8人不等）。相比于解题模式，时间更短，比赛中更注重临场反应和解题速度，需要能够快速攻击目标主机并获取主机的权限，考察团队多方面的综合安全能力。

解体模式的题目类型：

1. web安全：通过浏览器访问题目服务器上的网站，寻找网站漏洞（sql注入，xss,文件上传，包含漏洞，xxe，ssrf，命令执行，代码审计等），利用网站漏洞获得服务器的部分或全部权限，拿到flag，通常包含分值最大的web渗透题；

2. 逆向工程（Reverse）：题目就是一个软件，但通常没有软件的源代码；需要利用工具对软件进行反编译甚至反汇编，从而理解软件内部逻辑和原理，找出与flag计算相关的算法并破解这个算法，获取flag；

3. 漏洞挖掘与漏洞利用（PWN,EXPLOIT）：访问一个本地或远程的二进制服务程序，通过逆向工程找出程序中存在的漏洞，并利用程序中的漏洞获取远程服务器的部分或全部权限，拿到flag；

CSDN @上官大大

sql:数据库查询。

xss:跨站脚本。

4. 密码学（Crypto）：分析题目中的密码算法与协议，利用算法或协议的弱点来计算密钥或对密文进行解密，从而获取flag。

5. 调查取证（Misc）：利用隐写术等保护技术将信息隐藏在图像、音频、视频，压缩包中，或者信息就在一段内存镜像或网络流量中，尝试将隐藏的信息恢复出来即可获得flag。

6. 移动安全（Mobile）：对安卓和IOS系统的理解，逆向工程等知识。

4.编码：base64。加密:凯撒。摘要：MD5,SHA1,SHA2.

5.调查取证（Misc):就是杂项。

6.window:.exe，安卓：.APK,Mac:.dmg。

难度排序：Misc < Crypto < Web < Reverse < PWN。

wp (writeup): 答案。

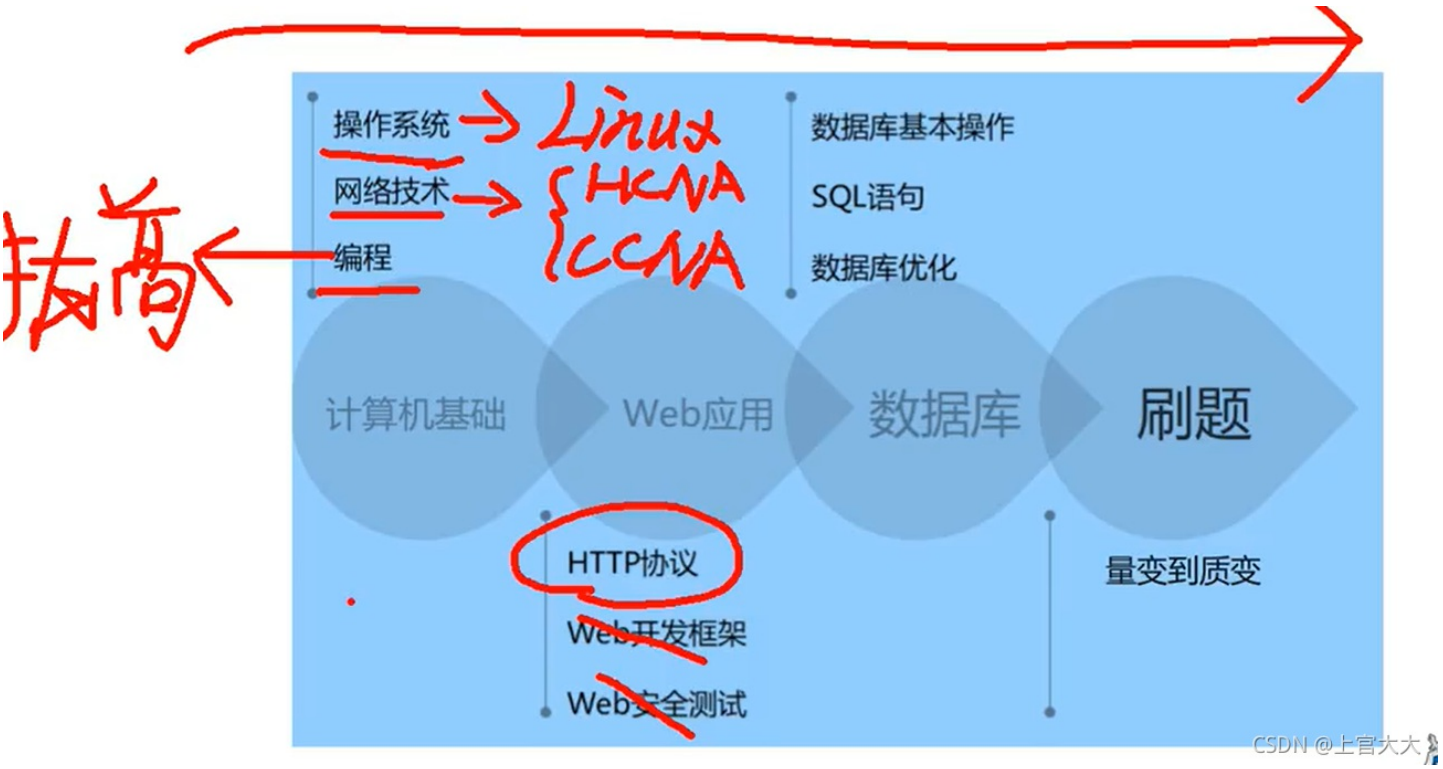
学习方向	需掌握的技能	
基础知识	Linux基础，计算机组成原理，操作系统原理，网络协议分析	
A方向	PWN+Reverse+Crypto	IDA工具（f5插件），逆向工程，密码学，缓冲区溢出
B方向	Web+Misc	网络安全，内网渗透，数据库安全，信息收集能力

CSDN @上官大大

基础：Linux与网路协议分析要重点掌握。

A > B.

Web方向：



http在谷歌浏览器上显示不安全

https则是安全，https = http + TLS(套接层)。

刷题网站：

CTF真题演练场

hackingLab实验室：http://hackinglab.cn
实验吧：http://www.shiyanbar.com/ctf/practice
i春秋CTF大本营：https://www.ichunqiu.com/competition
合天实验室：www.hetianlab.com
USSLab Jarvis OJ Platform ：https://www.jarvisoj.com
XCTF实训平台：http://oj.xctf.org.cn
Capture the Flag：http://captf.com
CTF Time：https://ctftime.org
BugkuCTF：http://ctf.bugku.com/login

Hackgame

SQL注入练习：http://redtiger.labs.overthewire.org
xss game：http://prompt.ml/0
XSS Challenges：http://xss-quiz.int21h.jp/
白帽学院CTF挑战赛：http://www.baimaoxueyuan.com/ctf
红客闯关游戏：http://hkyx.myhack58.com
梦之光芒hack游戏：http://monyer.com/game

CTF-Writeup

实验吧Writeup：
http://hebin.me
360播报：
http://bobao.360.cn/ctf
安全脉搏：
https://www.secpulse.com/archives/catego
github上的writeup：
https://github.com/ctfs
https://github.com/VulnHub/ctf-write

CSDN @上官大大

新手：**实验吧与bugku**