2023级D.I.E战队CTF学习路线

写在前面

CTF对于计算机知识不充分的大一CTFer来说，知识面较为广泛，需要耐心的学习；同时相对应的，如果能在大一掌握不少知识，那么已经走在了许多人的前面。知识的获取需要文章的阅读和活用搜索引擎，因此，推荐你独立完成以下事项。

- 配置好你的设备，并让他们能够科学地上网。– https://98ka.men/#/register?code=AU275fUA
- 了解linux命令行基础 – https://linuxjourney.com/ 链接:https://pan.baidu.com/s/172gSpFilN-_KWapRiNWfcA 密码:sm75
- 利用Vmware配置你的虚拟机
- 了解github，使用gitpages+hexo搭建自己的博客。（选做项目，看个人分享欲和记录习惯）– https://cloud.tencent.com/developer/article/1591970

一些资料:

CTF特训营pdf版（不推荐作为入门学习书籍） 链接：https://pan.baidu.com/s/1NLX16SQxu4la83qKpfjFjw 提取码：1895

安恒信息《渗透攻击红队百科全书》上中下 链接：https://pan.baidu.com/s/1H2LbYGM-8oyZ-PcmXrejKQ 提取码：1895

想要知识广，路径少不了。以下是整理的一些网站和公众号，供大家学习（按需选取即可，不必全部关注）。

另外如果对某一特定方向感兴趣的话，欢迎大家联系群内对应方向的学长学姐聊天 =）

网站

CTFWiki – https://ctf-wiki.github.io/ctf-wiki/（帮助你快速了解CTF是什么以及各个方向大概都有什么内容，推荐简单了解后尝试确定个人兴趣点再具体学习）

CTFHUB – https://www.ctfhub.com/#/index

CTF Time – https://ctftime.org/

攻防世界 – https://adworld.xctf.org.cn/

BugkuCTF – https://ctf.bugku.com/

BUUCTF – https://buuoj.cn/resources

TryHackMe – https://tryhackme.com/

Hack the box – https://www.hackthebox.eu/

Hacker101 CTF – https://ctf.hacker101.com/

Websec – https://websec.fr/

CTF 101 – https://ctf101.org/

vulnhub（靶场） – https://www.vulnhub.com/

内网渗透 – https://lab.pentestit.ru/signup

工控安全 – https://game.fengtaisec.com

智能合约 – https://ethernaut.openzeppelin.com/

杨东山老师的csdn专栏 –https://blog.csdn.net/eastmount/category_9183790.html

公众号

DIE 战队

重生信息安全

Gamma实验室

腾讯安全应急响应中心

天驿安全

看雪学苑

Timeline Sec

SecPluse安全脉搏

ChaMd5安全团队

天億网络安全

Tide安全团队

Nu1L Team

玄魂工作室

渗透云笔记

边界骇客

虚拟框架

零时科技

星盟安全

宽字节安全 --------渗透测试,漏洞分析

鸿鹄实验室 --------red team,工具开发

奇安信威胁情报中心------APT分析

酒仙桥六号部队 --------渗透测试,red team

Web

首先基础知识很重要，不管你要精通 web 渗透,还是只想当一个脚本小子,都建议学习:

TCP/IP网络协议(计算机网络)

基础

在后续的 web 测试开始前,你要了解:

- 常见的 TCP 协议,udp 协议;
- ip,端口,域名的含义,我们见到的 web 页面是如何展示出来的
- http 的 get 与 post的区别 ;
- 如何用 wireshark 对 http流量进行分析,如何用浏览器控制台分析 http 流量;
- cookie 和 session是怎样进行身份认证的;
- https 是什么,它与 http 有什么不同;
- 网站数据存在哪里,网站是如何传输并存储数据的;
- 网页的动作控制依靠的是什么,形状和布局依靠的又是什么;
- 如何解密网站页面中密码处的*号;
- 怎样通过工具对网站的账户密码进行爆破;
- smtp 协议是什么,如何在发邮件时伪造发件人;
- 服务器是什么,如何操作

等等等等..... 推荐书籍 <计算机网络(谢希仁)>

不建议上来就啃两三个月《计算机网络（自顶向下方法）》

工具

工欲善其事,必先利其器.学好 web 安全,工具必不可少.以下是常见工具,请查收:

工具名	用途
kali	操作系统.内含多种测试工具
burpsuite	神器.http,https 抓包改包爆破
fiddler	同上,常用于 Android 渗透
hackbar	火狐浏览器插件,改包
中国菜刀	神器.webshell 管理软件
蚁剑	同上,webshell 管理软件
sqlmap	神器.sql 注入自动化测试工具
nmap	端口扫描工具
metasploit	神器.自动化漏洞利用工具
awvs	漏洞扫描工具

另外,手头宽裕的同学建议在腾讯云/阿里云上购买一台vps (有学生优惠)以备后用.

常见漏洞

web 开发的语言有很多,目前常见包括 Java PHP Python Go 等.

请注意: 每种语言都会有漏洞,所以每种语言都必须有了解.相对于二进制的深度,web 方向的学习在初级阶段**更具广度**

需要了解简单的php语言和SQL语句，正则表达式等，然后去学习漏洞的类型，明白原理和学会复现漏洞的利用

基本了解的漏洞类型需要有：

- SQL注入: 显错注入，盲注，宽字节注入，堆叠注入，（DNS注入和反弹注入作为小trick可了解），cookie注入，偏移注入等.
- xss: 反射型xss,存储型xss，（dom Based xss ）
- 请求伪造:
  - CSRF(客户端请求伪造)
  - SSRF(服务器端请求伪造)
- 文件上传,解析漏洞：
- 逻辑漏洞：
  - 验证码绕过
  - 密码爆破
  - 平行越权
  - 垂直越权
  - 支付漏洞
  - 顺序执行缺陷
- XXE（外部实体注入攻击）
  - https://xz.aliyun.com/t/3357
- SSTI (模板注入)
  - https://xz.aliyun.com/t/6885

除了上述常见的漏洞外,我们还会遇到代码审计的题目,目的是找出代码中的 "安全性 bug"

白盒审计常见漏洞挖掘：sql 注入，文件上传绕过，变量覆盖，本地包含和远程包含，反序列化

以上为外网需要掌握的知识

其他

上面了解的差不多了以后，可以去各种论坛上面看一些最新的文章进行自我学习和提高：

常见论坛推荐：

t00ls:https://www.t00ls.net/ （需要投稿或邀请码）

先知社区：https://xz.aliyun.com/（不需要投稿或邀请码）

freebuf:https://www.freebuf.com/ （不需要投稿或邀请码）

安全客：https://www.anquanke.com/（不需要投稿或邀请码）

sec圈子：https://www.secquan.org/（需要投稿或邀请码）

嘶吼社区：https://www.4hou.com/（不需要投稿或邀请码）

安全维基：https://www.sec-wiki.com/（不需要投稿或邀请码）

安全脉搏：https://www.secpulse.com/（不需要投稿或邀请码）

可以在 bugku、攻防世界、buuctf 进行练习（刷题）

题目难度大致排列（从低到高，推荐0基础按这个顺序刷题）：

入门：攻防世界web新手练习区 https://adworld.xctf.org.cn/challenges/problem-set-index?id=25

熟悉：bugku平台web题 https://ctf.bugku.com/challenges/index/gid/1/tid/1.html

练习：buuctf（常见基础靶场及各大赛事真题）https://buuoj.cn/challenges

同时非常推荐积极参加各类大小赛事，以赛代练，赛后分析学习WP，成长很快

Pentest（实战渗透,萌新勿入）

行业前景

先贴几张图让各位了解下当前行业所需的技能栈:

4.Web安全工程师

工作地点：上海

岗位职责：

- 负责核心能力研发、维护，将前沿攻防经验沉淀为产品模块；
- 参与攻防实战项目；
- 研究并跟进最新的安全漏洞与安全动态；

岗位需求：

- 熟悉开发测试流程，熟练掌握Go/Python，具备扎实的开发技能基础，熟悉常用的开发协作流程；
- 有过作为一线技术成员深度参与攻防赛事的经验，熟悉当下攻防流行的各类漏洞的原理及利用；
- 熟悉Java漏洞挖掘及利用，挖掘过国内外常见的Java项目；
- 具有自我思考和理解能力，能够独立分析问题及提出解决方案；
- 善于跨团队沟通和协调，具备良好的团队意识和自驱力；

高级渗透测试工程师（红队方向）

人数及地点

5人 , 坐标北京、武汉、重庆

岗位职责

负责对企业网络进行安全评估（拿权限、拿数据，不限制攻击手段）
前沿攻击技术的研究，攻击小工具的研发

任职要求

熟练掌握各种渗透测试工具并且对其原理有深入了解（不仅限于 Burpsuite、sqlmap、appscan、AWVS、nmap、MSF，cobalt strike 等等）
至少掌握一门开发语言，操作语言不限 C/C++、Golang、Python、Java 都可，要求至少能上手写代码
熟练掌握常见的攻防技术以及对相关漏洞（ web 或二进制）的原理有深入的理解
具有丰富的实战经验可独立完成渗透测试工作
能从防御者或者运维人员的角度思考攻防问题，对后渗透有深入了解者更佳
对安全有浓厚的兴趣和较强的独立钻研能力，有良好的团队精神

加分项

具备渗透大型目标的经验
熟悉常见 Windows,Linux 安全机制，具备一定的安全开发能力以及problem solving能力

安全研究员（JAVA漏洞分析/挖掘方向）

人数及地点

2人 , 坐标北京

岗位职责

跟踪和分析业界最新安全漏洞
JAVA方向漏洞挖掘工作

任职要求

对JAVA编程有深入了解，熟悉JAVA主流框架（Spring、Struts2等），具备较强的Java代码审计能力
独立分析过公开漏洞，能快速输出漏洞利用EXP
深入理解常见安全漏洞产生原理及防范方法
对安全有浓厚的兴趣和较强的独立钻研能力，有良好的团队精神

加分项

独立挖掘过java等开源程序0day漏洞

安全开发工程师

薪资：25k~50k

岗位职责

1. 参与高防产品需求讨论、架构方案设计、开发、调试工作
2. 分析系统瓶颈，解决各种问题
3. 优化系统架构，规范开发、上线等流程

岗位要求

1. 本科及以上学历、计算机相关专业，3年及以上工作经验
2. 精通nginx、PHP、Mysql、Linux编程开发环境，对PHP源码有一定了解
3. 熟悉TCP/IP、HTTP等常见网络协议
4. 了解数据库基本原理，了解MySQL、ES、MQ、Redis等存储系统
5. 喜欢钻研技术，对技术有执着追求，对代码有洁癖，具有良好的团队合作精神

加分项

1. 了解常见的网络攻击及防护方法，对抗DDOS、抗CC有一定了解优先
2. 有技术博客或开源项目代码贡献者优先

所需技能

（刚刚列举的漏洞类型除外）：

信息搜集

nmap端口扫描工具（记住常见的端口漏洞，学会使用命令行）

目录扫描：御剑，disbuster sublist3r（子域名扫描）

CMSeek:识别CMS

WAFw00f：识别WAF

xcdn:寻找目标真实的IP地址

xray AWVS：项目上面可能用的到的漏洞扫描工具

等很多工具

无明确目标时谷歌语法（若不会科学上网的话找一下谷歌镜像站，直接百度谷歌镜像就可以）谷歌语法如下：

site+关键词：可寻找网址中带关键词的网址,例：site:edu.cn 寻找网址中带edu.cn的网址

inurl：当我们用inurl进行查询的时候，Google会返回那些在URL（网址）里边包含了我们查询关键词的网页。例：inurl:edu.cn 寻找带edu.cn的网址

intext: 当我们用intext进行查询的时候，Google会返回那些在文本正文里边包含了我们查询关键词的网页。

filetype: 指定文件类型 例：filetype:.xls 寻找可下载表格文件的网址

bypass（绕过防火墙）

现有网站的主流防火墙大概有安全狗，D盾，创宇盾，云盾，云锁，阿里云盾，宝塔等

bypass手段有很多，可以去搜一下，搜不到的话可以在群里询问（SQL和文件上传可能现在还会一点，别的可能得通过本地测试得到，注意本地测试时断网）

内网

- 代理
    - ew

    - nps/npc
    - venom
    - frp
- 未授权访问漏洞总结(直接用工具利用):
    - https://www.freebuf.com/articles/web/207877.html
- java 常见的漏洞:
    - struct2漏洞
    - JBoss 反序列化漏洞
    - weblogic 反序列化漏洞
    - fastjson 反序列化漏洞
    - shiro 反序列化漏洞
- 域渗透: https://xz.aliyun.com/t/237

以上漏洞在内网渗透中非常常见.

提权

- linux: 内核漏洞，定时任务，suid，sudo，NFS，第三方服务 等
- windows:烂土豆 等

权限维持

Google镜像：

https://g.365deyu.cn/ （不能用就去百度一个，很多的）

github有Google专项 里面应有尽有

web攻防不拘泥于理论，更依赖实践（但请注意不要未授权攻击），欢迎感兴趣的同学来参与战队各类渗透项目（“合法攻击”）。

Reverse

工具

- 逆向使用工具：链接:https://pan.baidu.com/s/1Qokrn5qfw2FXJUL162y7Ug 密码:q9pn
- win7破解机下载：https://www.52pojie.cn/forum.php?mod=viewthread&tid=677163&page=1
- linux系统推荐ubuntu或者kali-geekeyes版本

方法学习

从攻防世界的题目入手，了解简单的工具使用方法（通过搜索质量高的题解），了解简单的汇编和ollydbg调试方法。

能够学懂ida的使用方法后（不是只有F5）其实学的就差不多了。= =（指入门）

然后可以自学一些架构比如x86 x32 mips arm等等（了解即可）

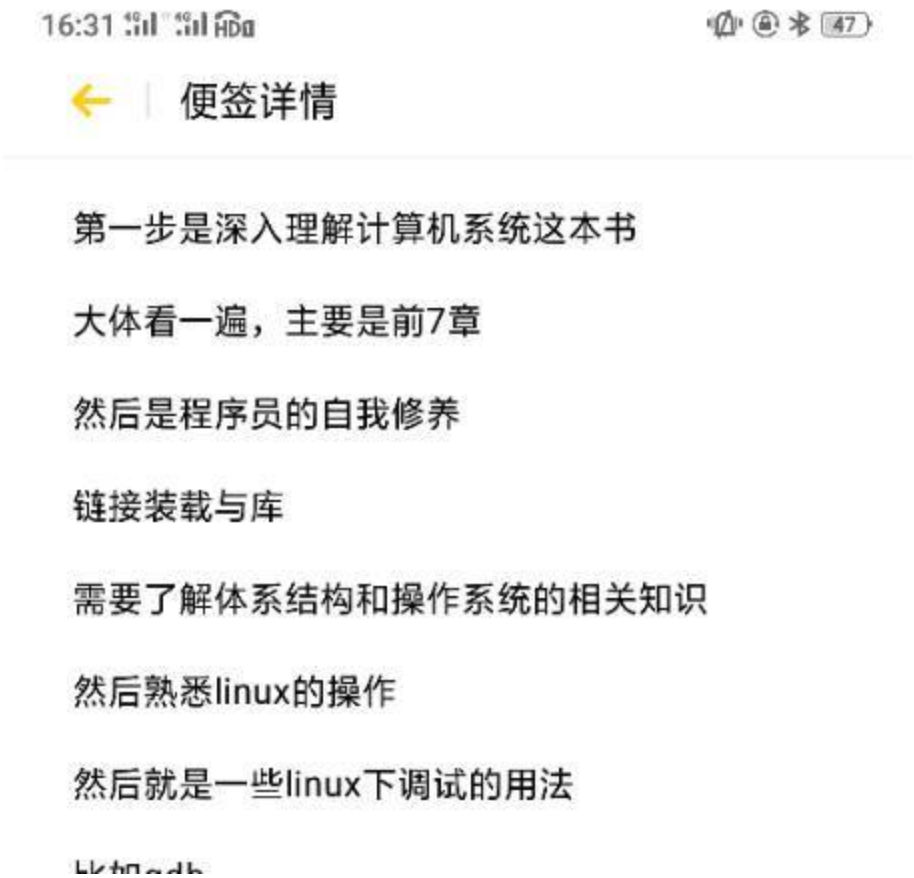
基本两种题 exe 就是ida静态观察ollydbg动态调试，elf就是linux下gdb或者ida动态调试

之后比较难的就是花指令 反调试 加壳去壳 加混淆去混淆 也有硬磕字节码这种

mobile暂且不叙，如果学完有兴趣可以找我私聊。大体思路还是相通的。

Pwn

1. 先贴丁佬的图



比如gdb

装个插件，还有逆向的工具IDA

就可以按CTF WIKI

学一些利用技巧

然后做题

先是栈溢出，rop这些，然后是ptmalloc的原理

管理方法和利用技巧

这些完了之后基本可以打国内难度不高的比赛的

pwn

国际赛就需要补充全面知识了

1. 推荐是按这个来。

先看一下书，pwn入门可能比较吃基础

不清楚栈、汇编、ELF文件结构的话可能根本不知道程序是什么样的，干了什么

看书差不多了以后开始调题。(如果觉得学的好可以直接来调题，不过如果调自闭了就回去看书)

先装虚拟机。建议Ubuntu 14/16/18

自己调源，熟悉Linux命令。

毕竟pwn手主要还是在Linux环境下做题。

然后装工具。虚拟机有pwndbg、ROPgadget、onegadget 、python(建议装python2.然后pip 装pwntools 这个是pwn手最重要的框架之一 基本上wp里面的exp都用这个库)

而且得熟悉常见的工具指令。

如果觉得麻烦可以先只装pwndbg和pwntools、IDA

剩下的用到了再装。

栈按CTF WiKi上的顺序看就可以了。切记一定要调试!

不熟悉程序流程也好，exp打不通也好，都可以拿调试查错。core相关的也了解一下。

栈完了大概就是堆……前置知识也是一大堆。

个人不建议看wiki上面的堆入门，理论知识可能讲的很麻烦，容易自闭

资料可以看我发的那些。

先熟悉一下简单的double free 、uaf、unlink、堆溢出、off by one等等 先调已有的题，看懂exp，再自己找题写.

pwn需要一定逆向能力，不过主要是能看出来程序本身漏洞的能力，对算法要求不是太高

Crypto

基础：会python

基础加密算法：凯撒，猪圈，栅栏（普通，w），base64等；rsa，aes系列等等

密码学需要数论知识，也需要学

其实看ctf wiki就行

然后遇到给出源码的题基本都是自己编的加密算法，需要推导得到解密算法或者别的帮助解密的算法，然后自己写python脚本

Misc

基本上也是按Wiki来 已经比较全面了

但是还得看wp misc比较吃脑洞 看想法

IoT安全：http://www.ctfiot.com/ https://iotsec-zone.com/home

娱乐项目

学累了又想看点安全相关的/能帮助了解安全人日常的（？）娱乐节目怎么办：（部分推荐，有更好看的欢迎分享）

电影：WHOAMI

综艺：GeekPwn 燃烧吧天才程序员

电视剧：~~亲爱的热爱的~~ 你安全吗