**作业类型——已实习对工作的理解**

17级信息安全3班 20175405 孟繁镇

**一、目前实习经历**

第一段 20190907-20200725知道创宇研发实习生

第二段 20200910-至今 启明星辰安全服务实习生（学校实习）

1. **最终结论**

计划毕业以后就不主力搞安全，我在实习期间和自己内心对比认为自己对于安全技术不够热爱。没有足够兴趣让我有那种废寝忘食学习研究的冲动，在启明星辰干到12月确保顺利拿到学分准备就撤退，以后自会多偏向代码研发一些

对于毕业如果没有目标，我推荐进入互联网行业，除非有一个工作同时满足钱多事少离家近中的两条时才优先考虑这份工作

1. **实习感悟与经历**

首先要感谢学校与各个任课老师给了我实习机会，我自己是对找工作不太上心的人，两段实习经历以及现在手里有的offer都分别是通过学校宣讲会，学校实习平台，学长内推得到的机会，这是在天津理工这个平台带给我的福利

通过一年有余的实习改变了一些我原本对于工作的看法，之前我可能非常渴望加班，希望通过加班来获得成倍速度的技术成长，在实习初期中也确实是这么实践的，但是随着实践推移，我发现因为大量的时间奉献给了实习岗位，因此缺失了一些事情。没有潜心修炼内功，计算机网络，操作系统，计算机组成，设计模式这些底层知识我在大学打下的基础个人不是很满意，其实还有很大提升的空间

对于毕业以后，应届生一穷二白肯定无脑想加班，因为在出租屋里也没有什么事情可以干(除了打游戏)自然对加班毫不抗拒。但是我已经不太想加班了，当一个人想要在业余时间多学习一些底层基础知识的时候，就会发现过度的加班挤占了很多个人成长时间

所以我现在先拿到了渤海银行的校招offer，如果11约外交部国考和2转年春招没有更好的机会的话，我觉得这里还是一个不错的选择。

12月-2月我觉得自己再补充一下专业知识可以再冲一次BAT，今天秋招腾讯字节捞了我10次我都挂了，所以还是比较艰难，基础知识只有数据结构算法算得上天衣无缝，其他知识还有所欠缺需要提升

具体实习经历如下

1 知道创宇

在知道创宇经历了超过一年的实习，经过了各种项目的洗礼

期间写过爬虫，爬取ipwhois全球数据，bgp，pop等数据，

并且学习并使用ETL开发，Hbase查询、Spark大数据开发

学习并使用Golang语言开发了TCP代理Proxy，爬虫等小工具，学习了Golang基本用法

可以说在这里我从一个小白成长了很多，不仅仅提升了自己的编程水平，还学会了很多软技能，Linux很多操作指令在潜移默化中便熟记于心，从需求调研，代码实现，项目测试，环境搭建的一整套流程我都做过，还在各种跨部门对接，日常工作中学到了一些待人接物的技巧

但未来职业发展和我预期有一些偏差，研发中心未来会向天津迁移，转正可能只能在天津转正，薪资相比北京会接近腰斩只有7000上下，知道创宇给的薪资处于较低水平，在疫情期间资金链曾严重出现问题，每年转正名额都有卡人，这与我期望的工作发展和信息待遇相差甚远，

考虑到职业稳定性和长期发展，毕业之后并不想在这家公司继续工作，所以先辞职回家自行学习了

2启明星辰

通过学校的校内实习平台找的实习，已于9月入职。现在参与了2020年9-10月的护网行动，在金融行业服务部门做一些资产扫描渗透的工作，第一次正式进入安全领域的工作，结合和以前学长的沟通，缺失安全服务其实是一件很麻烦的乙方工作，工作时间也没有保障，护网时期还需要职夜班。实际体验后并不喜欢这种工作环境氛围

肉眼可见我其实对安全技术研究的热爱不如代码开发来的多，所以后期如果有机会我还是想转会研发岗位的

在我看来如果没能在大学毕业前进入安全研究或安全实验室工作的话，渗透测试和安全服务是一件性价比很低的事情，还不如从事研发或甲方工作

1. **实习以来的提升**

这年一年多以来，学习了很多Linux系统环境下操作，学习部署环境，需求分析调研，设计文档编写，编写代码不要过分热衷于造轮子，及时上网以及寻求外界帮助，主动寻求沟通，保证任务进度

在专业技能和技术认知上都有了较大提升，通过业余时间专门学习了数据结构算法，语言具体实现，底层等知识

学习成果感觉比较基础通用的知识还是需要自己私下学习比较好，在工作中学到的偏向于经验型知识，随着工作需要而被动学习得到的知识只是知道了怎么使用，并没有深入理解，这种水过地皮湿的学习方法在完成工作后很难存续，就很难受

1. **不足与反思**

在实习期间因为一些原因(大创),心理压力比较大导致所有进度反而被自己都搁置了，所以技术上的提升并没有非常大，只能说中规中矩，很多技术的底层原理都没有去深度挖掘

我认为在工作(实习)前需要让自己心态端正，带着不健康的心态投入到工作中本身就是一种错误的行为。我们作为大学生一定要心态放平和，快乐起来，带着这种心态投入到工作中，而不是被工作压力推动着走

1. **自己的爱好与日程规划**

每天坚持训练leetcode起步，每天都要写50行代码起步

关于信息安全领域以及代码开发主要还是要依靠自己自学，俗话说师傅领进门，修行靠个人。

只有自己通过良好学习生活习惯的培养，每天不断进取，坚持各个方向的学习，才能在日后有机会取得长久的进展

越发觉得咖啡和茶是提神界的瑰宝，但是在我国茶的价格太不透明了，还是买咖啡经济实惠一些。。。

1. **未来展望**

对自己目前的后端技术还是非常有信心，最近再踏实一下Golang语言基础，学习更加深入一些，数据库再深入了解一下，算法每天三道题的速度刷

我在3月份发现了极客时间这个学习平台，里面有很多课程比外面一些课程都讲的不错，我在上面学习了好几门课程，也看了很多盗版(省钱万岁)

向他人请教学习非常有效率，比自己学习可以省力很多

最后毕业的话，现在经历过一年多实习的我希望可以少加班，达到一个

1. **对这个学期的意见**

1 专业实习

大四的专业实习出发点不错，但是实际执行上有问题我认为

很多想要考研的同学都会被这个专业实习很大程度影响复习节奏，有的同学复习节奏会被完全打乱，被迫放弃考研。

辅导员为了就业率各种旁敲侧击不希望大家考研，而是都去就要以完成自己指标。

而且现在企业已经不是原来955的工作制度了，很多企业悄然向着更长的工作时间转化，在这种时代变化很快的时代，我认为专业实习有很大走出改变的空间

当然我可能站在视角思考问题格局太小了，还有很多老师们思量的问题没有考虑到才会得出这样可以结论

2 这门期中作业有点长

大学生在其他课程从来不写超过400字文章的前提下要求10页宋体A5的感想有点过于多了，很多同学为了完成作业而通过堆叠知识点以达到10页以上的作业标准，而没有认真完成作业

我觉得自己把真情实感全部写出来页超不过4页，所以至少后6页我也会开始”报菜名”，枚举自己大学课上课下学到的全部专业知识

1. **知识列举**

**一个授权网站的渗透测试思路，具体渗透流程**

　　1）信息收集

　　a.服务器的相关信息（真实ip，系统类型，版本，开放端口，WAF等）

　　b.网站指纹识别（包括，cms，cdn，证书等），dns记录

　　c.whois信息，姓名，备案，邮箱，电话反查（邮箱丢社工库，社工准备等）

　　d.子域名收集，旁站查询(有授权可渗透)，C段等

　　e.googlehacking针对化搜索，pdf文件，中间件版本，弱口令扫描等

　　f.扫描网站目录结构，爆后台，网站banner，测试文件，备份等敏感文件泄漏等

　　i.传输协议，通用**漏洞**，exp，github源码等

　　2）漏洞挖掘

　　1>浏览网站，看看网站规模，功能，特点等

　　2>端口，弱口令，目录等扫描

　　3>XSS，**SQL**注入，命令注入，CSRF，cookie安全检测，敏感信息，通信数据传输，暴力破解，任意文件上传，越权访问，未授权访问，目录遍历，文件包含，短信轰炸，服务器漏洞检测，最后使用漏扫工具等

　　3）漏洞利用|权限提升

　　a)mysql提权，serv-u提权，**linux**内核版本提权等

　　4）清除测试数据|输出报告

　　i日志、测试数据的清理

　　ii总结，输出渗透测试报告，附修复方案

　　5)复测

　　验证并发现是否有新漏洞，输出报告，归档

**APP的逆向分析思路与流程**

　　1.代码保护检测；

　　2.数据存储安全；

　　3.加密算法；

　　4.四大组件安全；

　　5.应用规范等

**Kali-Linux基础使用**

　　whatweb指纹识别

　　dirb目录扫描

　　whoiswhois查询

　　字典生成套件

　　爆破工具

　　kali系统中的工具清单-官方介绍

**OWASP-Top10-2017介绍**

　　A1注入，A2失效的身份认证，A3敏感信息泄露，A4XML外部实体(XXE)，A5失效的访问控制，A6安全配置错误，A7跨站脚本(XSS)，A8不安全的反序列化，A9使用含有已知漏洞的组件，A10不足的日志**记录**和监控

　　OWASP\_Top\_10\_2017\_中文版v1.2.pdf

**网络安全事件应急响应（如，一业务主站被挂黑页的处理流程及应对方法）**

　　1.取证，登录服务器，备份，检查服务器敏感目录，查毒（搜索后门文件-注意文件的时间，用户，后缀等属性），调取日志（系统日志，中间件日志，WAF日志等）；

　　2.处理，恢复备份（快照回滚，最近一次），确定入侵方法（漏洞检测，并进行修复）

　　3.溯源，查入侵IP，入侵手法的确定等

　　4.记录，归档--------预防-事件检测-抑制-根除-恢复-跟踪-记录

通用漏洞的应对等其他安全应急事件

1.拿到一个待检测的站，你觉得应该先做什么？

1)信息收集

1，获取域名的whois信息,获取注册者邮箱姓名电话等。

2，查询服务器旁站以及子域名站点，因为主站一般比较难，所以先看看旁站有没有通用性的cms或者其他漏洞。

3，查看服务器操作系统版本，web中间件，看看是否存在已知的漏洞，比如IIS，APACHE,NGINX的解析漏洞

4，查看IP，进行IP地址端口扫描，对响应的端口进行漏洞探测，比如 rsync,心脏出血，mysql,ftp,ssh弱口令等。

5，扫描网站目录结构，看看是否可以遍历目录，或者敏感文件泄漏，比如php探针

6，google hack 进一步探测网站的信息，后台，敏感文件

2）漏洞扫描

开始检测漏洞，如XSS,XSRF,sql注入，代码执行，命令执行，越权访问，目录读取，任意文件读取，下载，文件包含，

远程命令执行，弱口令，上传，编辑器漏洞，暴力破解等

3）漏洞利用

利用以上的方式拿到webshell，或者其他权限

4）权限提升

提权服务器，比如windows下mysql的udf提权，serv-u提权，windows低版本的漏洞，如iis6,pr,巴西烤肉，linux脏牛漏洞，linux内核版本漏洞提权，linux下的mysql system提权以及oracle低权限提权

5) 日志清理

6）总结报告及修复方案

2.判断出网站的CMS对渗透有什么意义？

查找网上已曝光的程序漏洞。

如果开源，还能下载相对应的源码进行代码审计。

3.一个成熟并且相对安全的CMS，渗透时扫目录的意义？

敏感文件、二级目录扫描

站长的误操作比如：网站备份的压缩文件、说明.txt、二级目录可能存放着其他站点

4.常见的网站服务器容器。

IIS、Apache、nginx、Lighttpd、Tomcat

5.mysql注入点，用工具对目标站直接写入一句话，需要哪些条件？

root权限以及网站的绝对路径。

6.目前已知哪些版本的容器有解析漏洞，具体举例。

IIS 6.0

/xx.asp/xx.jpg "xx.asp"是文件夹名

IIS 7.0/7.5

默认Fast-CGI开启，直接在url中图片地址后面输入/1.php，会把正常图片当成php解析

Nginx

版本小于等于0.8.37，利用方法和IIS 7.0/7.5一样，Fast-CGI关闭情况下也可利用。

空字节代码 xxx.jpg.php

Apache

上传的文件命名为：test.php.x1.x2.x3，Apache是从右往左判断后缀

lighttpd

xx.jpg/xx.php，不全,请小伙伴们在评论处不吝补充，谢谢！

7.如何手工快速判断目标站是windows还是linux服务器？

linux大小写敏感,windows大小写不敏感。

8.为何一个mysql数据库的站，只有一个80端口开放？

更改了端口，没有扫描出来。

站库分离。

3306端口不对外开放

9、3389无法连接的几种情况

没开放3389 端口

端口被修改

防护拦截

处于内网(需进行端口转发)

10.如何突破注入时字符被转义？

宽字符注入

hex编码绕过

11.在某后台新闻编辑界面看到编辑器，应该先做什么？

查看编辑器的名称版本,然后搜索公开的漏洞。

12.拿到一个webshell发现网站根目录下有.htaccess文件，我们能做什么？

能做的事情很多，用隐藏网马来举例子：

插入

<FilesMatch "xxx.jpg"> SetHandler application/x-httpd-php </FilesMatch>

.jpg文件会被解析成.php文件。

具体其他的事情，不好详说，建议大家自己去搜索语句来玩玩。

13.注入漏洞只能查账号密码？

只要权限广，拖库脱到老。

14.安全狗会追踪变量，从而发现出是一句话木马吗？

是根据特征码，所以很好绕过了，只要思路宽，绕狗绕到欢，但这应该不会是一成不变的。

15.access 扫出后缀为asp的数据库文件，访问乱码，如何实现到本地利用？

迅雷下载，直接改后缀为.mdb。

16.提权时选择可读写目录，为何尽量不用带空格的目录？

因为exp执行多半需要空格界定参数

17.某服务器有站点A,B 为何在A的后台添加test用户，访问B的后台。发现也添加上了test用户？

同数据库。

18.注入时可以不使用and 或or 或xor，直接order by 开始注入吗？

and/or/xor，前面的1=1、1=2步骤只是为了判断是否为注入点，如果已经确定是注入点那就可以省那步骤去。

19:某个防注入系统，在注入时会提示：

系统检测到你有非法注入的行为。

已记录您的ip xx.xx.xx.xx

时间:2016:01-23

提交页面:test.asp?id=15

提交内容:and 1=1

20、如何利用这个防注入系统拿shell？

在URL里面直接提交一句话，这样网站就把你的一句话也记录进数据库文件了 这个时候可以尝试寻找网站的配置文件 直接上菜刀链接。具体文章参见：http://ytxiao.lofter.com/post/40583a\_ab36540。

21.上传大马后访问乱码时，有哪些解决办法？

浏览器中改编码。

22.审查上传点的元素有什么意义？

有些站点的上传文件类型的限制是在前端实现的，这时只要增加上传类型就能突破限制了。

23.目标站禁止注册用户，找回密码处随便输入用户名提示：“此用户不存在”，你觉得这里怎样利用？

先爆破用户名，再利用被爆破出来的用户名爆破密码。

其实有些站点，在登陆处也会这样提示

所有和数据库有交互的地方都有可能有注入。

24.目标站发现某txt的下载地址为http://www.test.com/down/down.php?file=/upwdown/1.txt，你有什么思路？

这就是传说中的下载漏洞！在file=后面尝试输入index.php下载他的首页文件，然后在首页文件里继续查找其他网站的配置文件，可以找出网站的数据库密码和数据库的地址。

25.甲给你一个目标站，并且告诉你根目录下存在/abc/目录，并且此目录下存在编辑器和admin目录。请问你的想法是？

直接在网站二级目录/abc/下扫描敏感文件及目录。

26.在有shell的情况下，如何使用xss实现对目标站的长久控制？

后台登录处加一段记录登录账号密码的js，并且判断是否登录成功，如果登录成功，就把账号密码记录到一个生僻的路径的文件中或者直接发到自己的网站文件中。(此方法适合有价值并且需要深入控制权限的网络)。

在登录后才可以访问的文件中插入XSS脚本。

27.后台修改管理员密码处，原密码显示为\*。你觉得该怎样实现读出这个用户的密码？

审查元素 把密码处的password属性改成text就明文显示了

1. **最后的话**

大学时光转瞬即逝，眨眼间也已然要毕业。知识无限时间有限，势必会有遗憾。我们在大学里需要学习的不仅仅是知识，还有和学姐学长前辈、老师请教规划，自己规划未来道路的重要时机。

或许我们来到大学之前都在小学初中高中，学习着差不多的知识，但是从大学开始每个小朋友将会因为一次次的选择而走上截然不同的人生路径，或奋斗或沉沦，不论曲直，这是每个人专属的路，我们只是彼此路上的过客。

大家最后都走在自己的路上

最后衷心愿每个同学都可以快乐，活成自己想要的样子