联系方式

- 手机：18855999143
- Email：njcx86@gmail.com
- QQ：1666276469
- 微信号: cxwin512

个人信息

- 刘少华/男/1995
- 本科/黄山学院计算机系
- 工作年限：1.5年
- 技术博客：：https://www.njcx.bid
- Github：http://github.com/njcx
- 知乎： https://www.zhihu.com/people/njcxs
- 知乎专栏：https://zhuanlan.zhihu.com/pythons
- 期望职位：安全开发工程师
- 期望薪资：税前月薪20k~25k
- 期望城市：上海

自我简介

在点融网安全应急响应中心工作1.5年，收获颇丰，熟悉甲方的安全建设流程，熟悉企业安全建设，日常工作主要负责安全运维工作、安全工具维护、安全工具开发、渗透测试、应急响应，日常喜欢关注安全事件、威胁情报，业余偶尔挖挖SRC，对网络安全充满热爱，熟悉项目开发流程和团队协同工作，有很好的团队合作意识，能很好利用baidu、google解决问题，有良好的逻辑思维能力，喜好新事物，对新技术比较敏感，兴趣面和技术面比较广泛，希望能在日后通过继续学习更进一步

技术能力

- 熟悉主流WEB安全技术，如SQL注入、XSS、CSRF、文件包含、命令执行、文件上传等，以及简单的漏洞修补建议
- 熟悉常见的业务逻辑漏洞，如水平越权、纵向越权、业务绕过等
- 熟悉常用安全渗透测试工具的使用，比如Burp Suite、AWVS、SQLMAP、Nmap、MSF等

- 熟悉常用安全开发组件的使用，比如Kafak、ELK、Bro、Snort、Suricata等
- 熟悉Python WEB开发、爬虫编写，了解JavaScript、CSS、HTML，可以进行简单的前端开发
- 熟悉常用Python标准库和常用的第三方库的使用，比如requests等
- 熟悉常见的Linux发行版本，了解shell编程,了解常见服务搭建与故障排除，能以Linux为开发环境正常工作
- 熟悉Linux分布式生产环境部署，了解常见Web架构，了解Web分布式生产环境搭建
- 熟悉TCP/IP、HTTP协议
- 熟悉git版本控制系统的使用， 在Github、Coding、开源中国(码云）上有开源项目
- 熟悉Linux环境常用工具使用，比如Docker的使用等
- 熟悉常用数据库的使用，熟悉MySQL、NoSQL(Redis、MongoDB)的使用
- 了解安卓的逆向，可以进行简单的安卓逆向
- 了解大数据平台，可以进行简单的使用、数据存储

工作经历

上海点融网安全应急响应中心 （ 2018年7月 ~ 至今）

代码依赖异常审计项目

- 简介：目前很多代码项目没有对依赖的包进行检查，导致很多依赖的包存在cve和exp，存在巨大的风险，危及到上线的项目的安全，所以，安全部门建立该项目，进行项目包依赖检查，该项目把大量风险扼杀在摇篮之中
- 主要工作
    - 担任主要开发、管理、运维工作，项目与自动集成工具联动，从kafka中获取项目发布信息，拉取repo，使用DependencyCheck 检测对应repo，然后把检测报告放到nginx下面，并把对应的url 通过email发送出来，供对应的人员参考查阅，并修复升级相关的依赖包，主要编程语言是Python，主要使用DependencyCheck模块，生成html格式的异常检测报告

企业内部蜜罐的平台的建设

- 简介：由于我们的NIDS是通过镜像交换机流量建设而成，无法检测网段间的内部异常，一旦来内网段间内部攻击，就无法通过NIDS检测到，所以我们在各个生产环境的网段部署了蜜罐的agent，我们采用了开源的蜜罐做了简单二次开发，部署网段超过100个，蜜罐工作期间检测到大量的异常
- 主要工作
    - 项目是基于开源的蜜罐做了简单二次开发而成，我在此项目负责了主要的开发工作，包括，前端和后端、以及一些组件，项目采用了Docker容器化部署，大量的agent节点分布在各个网段，在安全异常事件收集过程中，起到了较好的作用

NIDS的自研项目

- 简介：公司内部的NIDS是自主研发的，主要镜像核心交换流量,采用PacketBeat、Bro工具解析流量，通

过kafka做传输管道，然后进行后续规则引擎分析,分析的维度包括:主机的异常连接行为、异常流量等

- 主要工作
    - 我在此项目负责了规则添加、规则编写、自定义组件的开发，添加了比如防爬虫规则、挖矿检测、扫描器检测等，在目前力严重依赖前置WAF的前提下,需要有一定的入侵感知能力,给内部环境一定的安全感知能力,可以做到及时感知及时处理

HIDS 的自研项目

- 简介：公司内部的HIDS是自主研发的，主要通过加载LKM模块的方式进入Ring0层，通过修改寄存器CR0中保护控制位中的WP位来达到可修改Linux原本syscall地址的方式来Hook主要操作,主要支持安全基线、系统完整性检测、反弹shell、webshell检测等
- 主要工作
    - 我在此项目负责了HIDS的规则添加，比如，日志删除检测、bash history删除检测、异常下载检测，以及安全基线规则添加等，HIDS和NIDS联动，可以提高异常的关联度，方便异常发生的溯源

ELK 平台的建设和维护

- 简介：ELK 平台共用了8个CentOS7节点，容量为40T，主要服务对象是安全部门，用于流量收集、日志存放检索、NIDS的告警收集、HIDS的告警收集等
- 主要工作
    - 项目是基于ELK组件搭建，我在此项目负责了主要的ELK搭建和管理工作，包括，日志和流量的收集存储展示，用于历史事件的检索和溯源，并充当安全部门的SOC使用，主要受众是安全部门全体人员

上海点融网安全应急响应中心（ 2017年7月 ~ 2018年7月 ）

点融网安全应急响应中心平台项目

- 简介：点融网安全应急响应中心平台是一个对外提供服务的项目，主要是收录白帽子提交的漏洞，以及提供漏洞审核、奖品发放的项目
- 主要工作
    - 项目是基于Django开发而成，我在此项目负责了主要的开发工作，包括，前端和后端，项目采用了Docker容器化部署，项目在对外漏洞收集过程中起到重要的作用，服务白帽子超过1000人

等级保护与ISO27001安全合规审计平台项目

简介：等级保护与iso27001安全合规审计平台是为安全部门提供一个直观显示并能轻松管理的公司安全合规审计平台,用于执行安全检查，风险评估等需求

- 主要工作
    - 项目是基于Django开发而成，我在此项目负责了主要的开发工作，包括，前端和后端，前端采用了H+框架，项目采用了Docker容器化部署，该平台系统主要服务于安全合规审计人员使用

堡垒机日志机器学习审计项目

简介：基于K-means算法训练的机器学习算法模型，基于时间、设备、IP、在线时长等为特征，把相关异常记录在数据库，并通知到对应的Devops人员

- 主要工作
  - 我在此项目负责了主要的开发工作，包括前端和后端以及数据分析工作，在项目中用到了pandas、numpy、scikit-learn以及 kafka等

Github 代码泄露扫描项目

简介：Github 代码泄露扫描项目是一个爬虫项目，会按预定时间频率爬取Github，匹配相关的关键字，检测是否有公司的相关的代码以及敏感信息泄露

- 主要工作
  - 我在此项目负责了主要的开发工作和维护工作，该项目包含两个子项目：代理获取模块和爬虫模块，主要开发语言是Python，该项目上线以后，查找到大量的源代码泄露和敏感信息泄露

开源项目

- pocsuite*poc*collect：https://github.com/njcx/pocsuite*poc*collect

  收集的POC

- peppa_gitscan: https://github.com/njcx/peppa_gitscan.git

  Github 扫描器

- Linux Basics for Hackers: https://github.com/OpenCyberTranslationProject/TP1

  参与翻译的书，Linux Basics for Hackers，第5、6、7章节

技术文章

- 反弹shell总结
- 抓包和nids规则编写
- rootkit的检测工具使用介绍
- ossec 搭建与简单用法
- 机器学习简介
- K-means算法简介
- 使用PyPy性能调优
- kafka 集群搭建实践笔记

技能列表

以下均为我用过或正在使用的编程语言、工具或者库：

- 编程语言：C/Python/JAVA/Golang/Bash/Lua/JavaScript
- Web框架：Django/Flask
- 数据库相关：MySQL/Redis
- 系统平台： Centos7.3/Debian 9.0/Ubuntu Server 18.04/KALI Linux2.0
- Http服务器：Nginx/Apache/uwsgi
- 常用组件： ELK/Kafka/Zookeeper/Splunk/Syslog
- 常用工具：Burp Suite/AWVS/Nessus/Bro/OSSEC/Snort/Suricata/Wireshark

漏洞挖掘经验

- 某在线借贷平台的ssrf 引起的xss打cookie
- 某OA 任意文件上传拿webshell
- 某OA 平台存在字符型SQL注入
- 某在线视频的json挟持
- 某在线视频的vip限制绕过
- 某在线教育平台发短信验证绕过
- 某在线商城的扣一次金币多次订单提交
- 某在线商城的任意订单查询
- 某在线教育平台发短信验证绕过

.....

参考技能关键字

- Linux运维
- 前端开发
- web后端开发
- 渗透测试
- 安全开发
- 数据分析

致谢

感谢您花时间阅读我的简历，期待能有机会和您共事。