刘向乐

求职意向：Linux C/C++服务端

23岁 | 本科 | 北京 | 15562922282 | liuxiangle_yy@163.com

学校：临沂大学　　专业：计算机科学与技术　　时间：2018.9 —— 2022.7

专业技能

- 熟悉LinuxC/C++开发调试、了解python、shell；掌握基本数据结构
- 熟悉Linux网络编程：常用协议，Reactor并发模型、5种IO模型、同步异步
- 熟悉Linux多线程：　线程同步，线程安全；进程通信
- 服务端：　阅读过部分nginx-http模块源码、muduo网络库；会使用mysql、redis、docker；了解些分布式系统
- 网络安全：了解边界安全-零信任架构体系；了解Linux下的远控、ELF/shellcode注入隐藏

工作经历

2022.07--至今　　360 数字安全科技集团　　漏洞研究院

1. Linux远程控制工具(独自负责)　　https://github.com/liu-9969/TSH

简介：基于 c++11 多线程+多进程、原生socket 编写的 linux 后门程序 (包括 C2C、agent两端)。功能如下

- [多会话管理]：支持控制多台目标、session列表、多任务并行；多个目标间一键快速切换
- [交互式shell]：基于linux伪终端设备文件，模拟真实bash 达到交互式的效果
- [　文件传输　]：支持异步、同步两种传输模式、大文件分片、断点续传、进度条
- [　Http协议　]：封装了一个Http状态解析机、状态弹性Buffer
- [　健康检查　]：agent端保活机制

2. web武器库::靶场搭建(负责后台)

简介：负责武器库中靶场模块的后台搭建，具备几套经典漏洞环境，基于django、libvirtAPI、qemu

1) 通过动态生成XML配置文件，来使 libvirtd 创建不同平台、不同配置的虚拟机

2) 以快照方式启动、暂停、销毁 ，支持BIOS、UEFI两种固件的镜像

3) 服务部署：nginx + uwsgi +django

3. 研究性

1）研究基于Ptrace的内存读写、寄存器读写技术，并用c++封装了此inject注入器。

2）研究了开源elf to shellcode工具源码 、shellcode分段技术egg-hunter

2021.11--2022.3(校招实习)　　北京 天融信科技集团　　安全接入产线

1. 期间，主要看部门项目文档，学习 **零信任体系下身份检控** 的业务逻辑，完成导师安排的demo任务。
2. 阅读了部分Nginx-http模块源码，梳理 http框架初始化的11个阶段，并调试了ACCESS_PASS阶段异步拿包体的bug。
3. 参与（**可信接入检控后台管理系统**）：nginx令牌校验模块 、HA双机热备、系统流量控制功能需求。
   1）双机热备：该项目放在下页单独说明了
   2）令牌校验：主要涉及http模块和upstream模块，参考导师的代码，完成请求的检验和转发功能

服务端项目经历

Health- Checking For HA

简介：这是我实习期间学习并debug的一个项目，项目采用shell script编写。
基于开源软件Keepalived和数据库自带sync功能，采用主从架构，来为资源 提供高可用解决方案。

功能：实现了存储(mysql、redis）、服务(nginx)的高可用，支持检控系统的双机热备。

原理：1. keepalived的核心协议vrrp工作在ip层，能够在单点故障后进行vip漂移。

2. 我们只需要将健康检查脚本挂到keepalived上，发生单点故障后kill掉keepalived进程，从而快速触发切换

3. 切换后master、slaved分别执行各自的切换脚本、数据互备脚本

Debug：redis发生故障切换后，master有机会不执行主降备逻辑，造成双主，从而数据不在继续同步。

解决：通过在keepalived里额外添加定时任务来检查双主的情况，并降备。

C++ 11 轻量级 WebServer

简 介： 这是我学校期间的写的项目， https://github.com/liu-9969/WebServer
通过看 muduo网络库对Linux原生socket、原始API的封装来入门C++ 多线程网络编程技术。
这是一个静态httpServer ， 支持 长连接、get静态文件、两个查询数据库接口。

并发模型： 单Reactor多线程， 即（主线程: epoll反应堆+ 回调入队） + （ IO线程池： 回调执行 ）
并发量 ： get 10K的文件 QPS10000+； 访问数据库 QPS2000+
组件 ：

- (epoll注册反应中心) 负责提前注册事件 ， 监听所有Fd ， 分发就绪事件
- (有锁任务队列 ） 有锁任务队列
- (IO线程池) 负责消费任务队列的 事件 ， 线程同步用到了互 斥锁和条件变量
- （mysql连接池）事先初始化server和my sql 的tcp 链接
- (计时 器）计时器是为了支持http长连接 ， 小根堆管理
- (异步日志 ） IO线程将日志 消息转发给后台Log 线程进行磁盘写 + 日志 消息缓存策略优化。
- (http状态解析机 ）定义了几种状态 ， 负责tcp 分包
- (弹性Buffer) muduo里的应用层Buffer ， 有状态的 ， 可扩容的 ， 只能扩大不能缩小。

个人评价

心态积极！ 永远年轻！