王若愚

关于我

王若愚是广州大学的研二研究生，专业是网络空间安全，ctf pwn 手，他对网络安全攻防充满热情，对待工作认真，重视实践操作。技术栈为二进制攻防、编程语言相关技术，熟悉 iot 的漏洞利用，对 Android、Windows 下的攻防有过实践操作，自学能力强。

联系方式

Phone (86) 13388281278
Email cynault@163.com

技能

- **C/C++**
- **Python**
- **Linux**
- **windows**
- **Android**
- **gdb**
- **IDA Pro**
- **qemu**
- **pwntools**
- **Git**
- **BurpSuite**
- **ARM**
- **X86/64**

教育背景

广州大学

网络空间安全 2021.09.01 - 至今

相关课程: 安全协议；网络安全综合实验；密码学。

沈阳工业大学

智能科学与技术 2016.09.01 - 2020.06.01

相关课程: 神经网络；机器学习；自动控制原理。

项目经历

物联网设备漏洞检测 **2023.2 - 2023.4**

- 物联网所内项目，对存在漏洞设备进行攻击利用。
- 对 cisco 设备 (RV110、RV340)、小米设备 (R3P) 的漏洞进行分析评估。
- 对现有的 poc 进行分析学习复现 (RV110、R3P)。
- 对已公布漏洞，但未有系统形成命令执行 EXP 的设备，进行分析，对其多个漏洞进行系统梳理，构造最终命令执行 python 脚本 (RV340)。

基于管道进程迁移项目 **2023.1 - 2023.2**

- 白帽社区红队持久化权限维持工具。
- 目标是实现进程注入后，目标进程挂掉后能进行迁移，自动进行注入。
- 基于 C++ 语言，进程注入技术，以及管道技术。
- 涉及进程通信，设计一套进程间主服务端灵活转换的方案。

蜜罐项目 **2022.12**

- datacon 的网络流量检测项目
- 使用 C# 语言，asp.net core 框架，规则匹配，实现了对漏扫工具扫描结果的混淆。
- 抓取漏扫工具的攻击流量，分析出大部分流量来自于 xray。
- 对 poc 进行分析，其验证漏洞的方式，如命令执行验证，关键字验证，存储型验证。

小米设备协议安全评估 **2022.4 - 2022.6**

- 安全协议实验项目
- 发现小米设备存在协议漏洞。
- 小米 S1 台灯作为目标设备，BurpSuite 抓包，分析手机 APP 米家、台灯以及云服务器的通信过程。
- 认证过程存在缺陷，设备 id 泄露后，攻击者拥有控制权。

获奖情况

三等奖 第一届中国研究生网络安全创新大赛 2022.11
二等奖 第十五届全国大学生信息安全竞赛华南赛区 2022.9
三等奖 CICV 智能网联汽车漏洞挖掘赛（线上、线下） 2022.5 、2022.8

教学服务

讲师 ctf-pwn 攻与防，无锡税务局 2022.8
助教 计算机网络，广州大学 2022.3 - 2022.7