CTF PWN

简介与前景

二进制安全初步介绍

PWN 简介

首先我们要了解软件安全。定义如下：

软件安全：软件安全专注于研究软件的设计和实现的安全。

- 研究对象：代码（源码、字节码、汇编等）。
- 研究目标：发掘漏洞、利用漏洞、修补漏洞。
- 研究技术：逆向工程、漏洞挖掘与利用、漏洞防御技术。

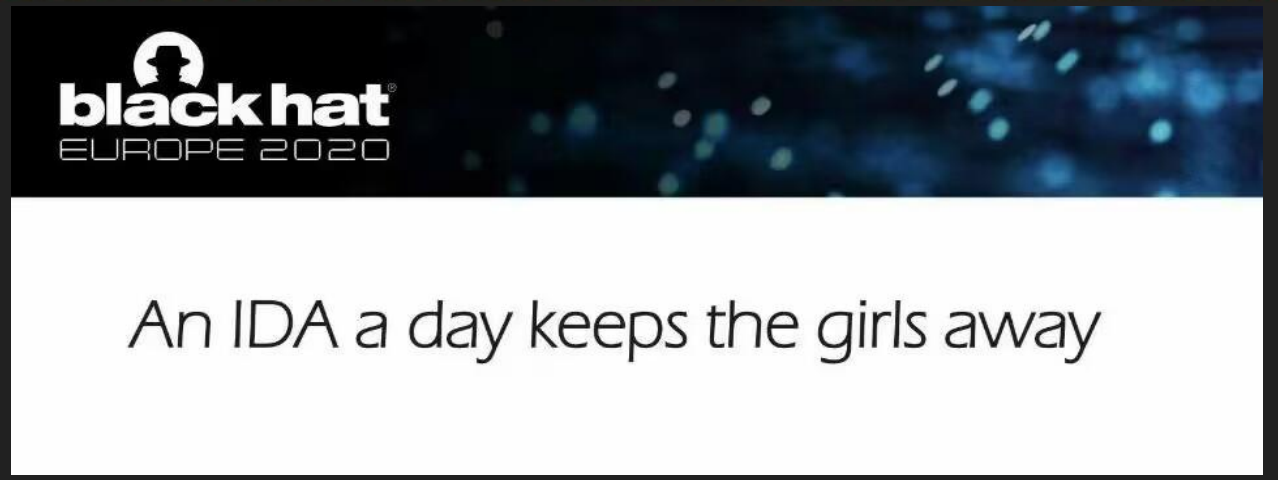
CTF PWN：

- 软件安全研究的一个缩影。
- 研究对象：可执行文件，主要是ELF文件（linux下）
- 研究目标：拿到flag/shell

PWN 简介

工　具

- 静态分析：IDA pro
- 动态分析：gdb、windbg、ollydbg
- 漏洞利用：pwntools、pwncli



前 置 技 能

- 汇编语言、程序执行、函数栈帧、函数调用等
- 编译、链接、装载、执行
- ELF文件结构
- 基础linux命令
- 基础python语句

PWN 简介

一次PWN攻击的基本流程

一、逆向分析可执行文件，往往是ELF文件
二、找到漏洞，从所学的知识思考如何利用
三、编写exp，本地调试
四、攻击远程服务器上的elf文件，执行你的指令

往往都是执行system('/bin/sh')从而获取一个shell解释器

PWN 简介

痛苦

- 刚入门的PWN选手，最基础的PWN题目可能会让你想不明白 -> 放弃
- 刚入门的PWN选手，做进阶的PWN题目可能会让你眩晕头疼 -> 放弃
- 有一定水平的PWN选手，比较难的PWN题目需要大量的耐心 -> 放弃

因此，学PWN需要耐心

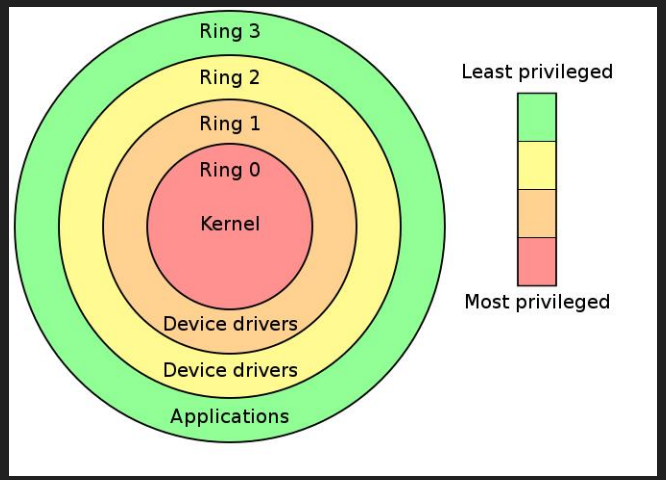
PWN
前景-不只是比赛

PWN

前景-不只是比赛

虚拟化

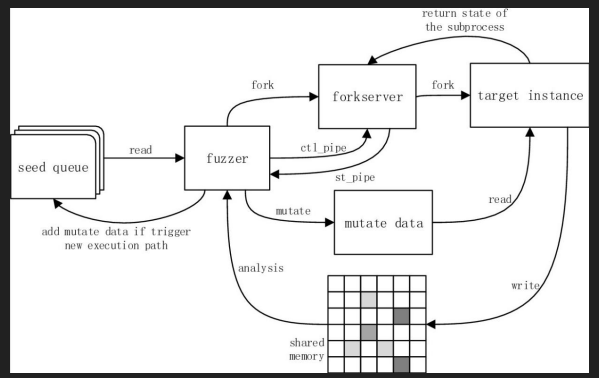
内核提权



浏览器

Date reported: 2021-11-17
Date fixed: 2022-01-06
Edge version: 95.0.1020.53 (Official build) (64-bit)
CVE: CVE-2022-21954
Reward: 30,000 USD 三万美刀

模糊测试引擎



IOT设备

ETC.....

PWN 前景

- PWN2Own 浏览器黑客竞赛，Apple Safari遭秒杀
  - 浏览器成今年Pwn2Own黑客竞赛焦点，南韩黑客破纪录，独自抱走22.5w美金
    - 世界黑客大赛中国队11秒攻破Chrome

- 世界黑客大赛Pwn2Own，Tesla提供一台Model3邀请黑客攻破
  - 找出漏洞！2青年成功 [黑走] 一辆Model 3及千万奖金

PWN
前景-就业

二进制安全工程师

二进制安全研究员

安全开发工程师（模糊测试方向）

ETC.....

结语