Notes about ebpf learning

Mayrain

2023 年 11 月 29 日

1 Introduction

主要是参照 b 站上的某个视频，看他们介绍 ebpf 的功能。
ebpf 是 cbpf 的后续。
1. risc 指令集：11 个 64 位寄存器，以及一些指令集用于操控。我已经在图中标定。
2. helpers 函数。利用这个函数访问内核数据。（提供内核交互。）
3. maps，一个全局变量数组。

使用方式和概念
4. object pinning，一个概念，利用特定工具和接口将程序或者 map 加载到内核中。一般适用于持久性使用。
5. 尾调用优化，一种编译器优化技术，可以减少函数调用的开销。它的实现方式是，将函数调用的返回地址设置为被调用函数的返回地址。这样就可以避免在被调用函数返回后，再返回到调用函数的返回地址。这样就减少了一次函数调用的开销。

6. jit: just in time，即时编译。一种编译方式，将源代码编译成机器码的过程放在运行时进行。这样可以减少编译时间，但是会增加运行时的开销。另外它还可以根据不同环境生成不同机器码，提升了泛用度。
7. hardening: 保护 bpf 程序。

> tcpdump：命令行的网络流量分析工具。一般用来抓 TCP 包。应该和 wireshark 类似。