作业和实践(第6讲 入侵检测)

- 作业
  1. IDS有哪些主要功能?
  2. 简述误用检测和异常检测。
  3. 简述snort的5个组成部分及其作用。
  4. 简述网络安全态势感知系统。

- 上机实践(自己练习，不考核)
  1. 在Linux系统中部署和使用Snort。
  2. 参考SEED的实验，设计一个网络嗅探系统:
     - https://seedsecuritylabs.org/Labs_16.04/Networking/Sniffing_Spoofing/