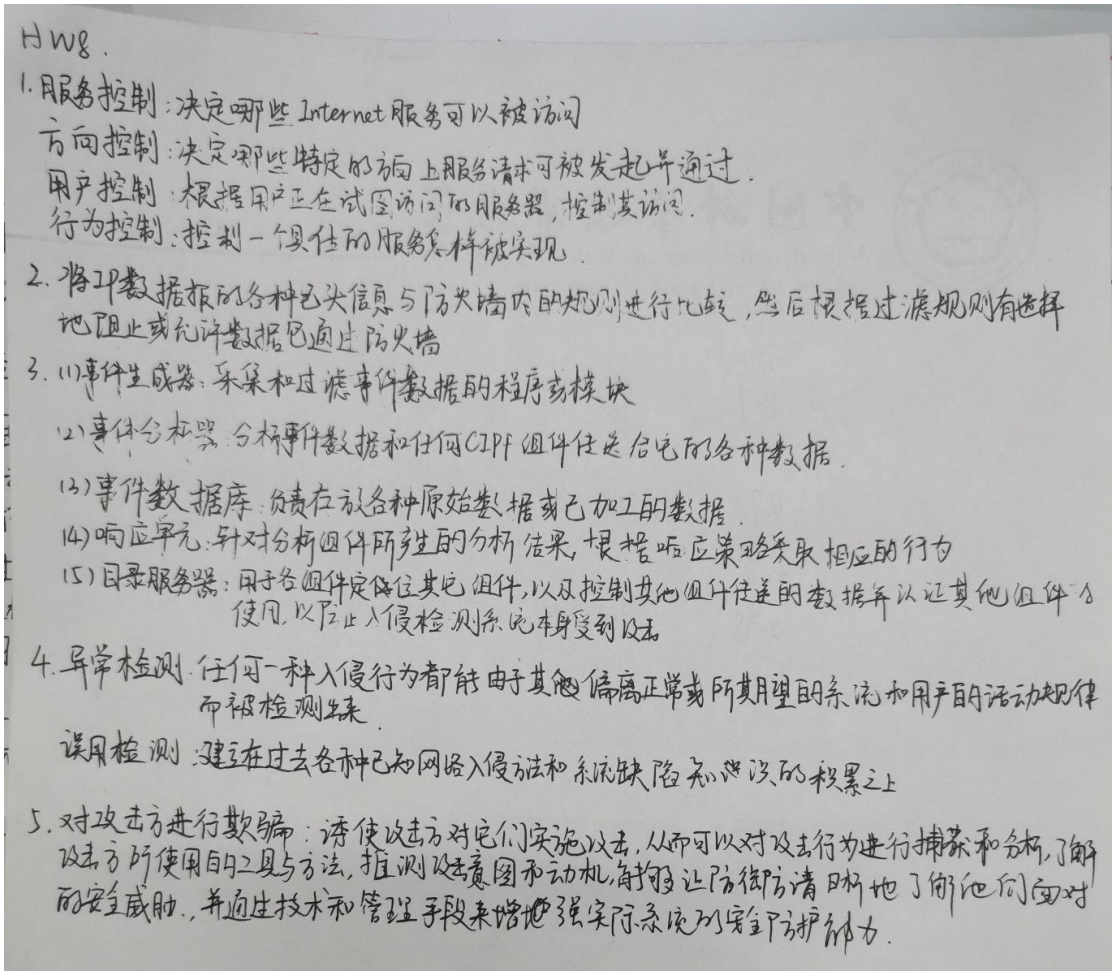
第八次作业

PB19111708 杨云皓



HW8.

1. 服务控制：决定哪些Internet服务可以被访问
   方向控制：决定哪些特定的方向上服务请求可被发起并通过.
   用户控制：根据用户正在试图访问的服务器，控制其访问.
   行为控制：控制一个具体的服务怎样被实现.
2. 将IP数据报的各种包头信息与防火墙内的规则进行比较，然后根据过滤规则有选择地阻止或允许数据包通过防火墙
3. (1)事件生成器：采集和过滤事件数据的程序或模块
   (2)事件分析器：分析事件数据和任何CIPF组件送给它的各种数据.
   (3)事件数据库：负责存放各种原始数据或已加工的数据.
   (4)响应单元：针对分析组件所产生的分析结果，根据响应策略采取相应的行为
   (5)目录服务器：用于各组件定位其它组件，以及控制其他组件送到的数据并认证其他组件的使用，以防止入侵检测系统本身受到攻击
4. 异常检测：任何一种入侵行为都能由于其偏离正常或所期望的系统和用户的活动规律而被检测出来.
   误用检测：建立在过去各种已知网络入侵方法和系统缺陷知识的积累之上
5. 对攻击方进行欺骗：诱使攻击方对它们实施攻击，从而可以对攻击行为进行捕获和分析，了解攻击方所使用的工具与方法，推测攻击意图和动机，能够让防御方清晰地了解他们面对的安全威胁，并通过技术和管理手段来增强实际系统的安全防护能力.