HW8

PB17111614 王嵘晟

1,2.

1、①服务控制：决定哪些 Internet 服务可以被访问

②方向控制：决定哪些特定的方向上服务请求可以被发起并通过防火墙

③用户控制：根据用户正在试图访问的服务器来控制其访问

④行为控制：控制一个具体的服务怎样被实现

2、①事件分析器：输入原始数据源

②事件转换器：输出原始或低级事件高级中断事件

③事件数据库：负责存放各种原始数据或已加工过的数据

④响应单元：针对分析组件产生的分析结果根据响应策略采用相应行为，发出命令响应攻击

⑤目录服务器：用于各组件定位其他组件

3,4,5.

3、异常检测基于行为，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。

误用检测称为特征检测，建立在对过去各种已知网络入侵方法和系统缺陷知识的积累之上。

4、一种对攻击方进行欺骗的技术，诱使攻击方对它们实施攻击，从而对攻击行为进行捕获分析，了解攻击方使用的工具与方法，判断攻击意图和动机，让防御方了解他们所面对的安全威胁，进而增强安全防护能力。

5、应急响应是对国内外发生的有关计算机安全的事件进行实时响应与分析，提出解决方案和应急对策，保证计算机信息系统和网络免遭破坏功能，为在出现安全问题时对采取应急响应措施，以防计算机信息系统和网络被破坏。