****

**网络安全**

**——十二章题目**

**学 院：大数据与信息工程学院**

**专 业：数据科学与大数据技术**

**班 级：大数据181**

**指导教师：卢晓寰**

**组 长：俞开斌1817000030**

**组 员：贡鑫铭1817000018**

**何祥建1817000054**

**李晶1817000088**

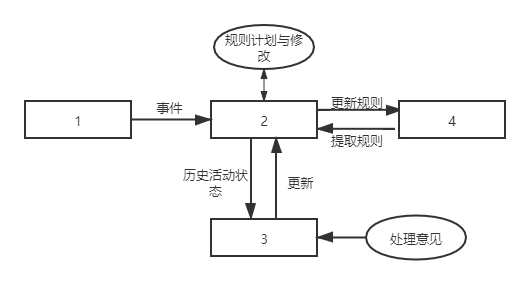
**李林睿1817000042**

**2021年 5月 22日**

**入侵检测系统**

选择题

一、下图中1和4分别是()和()。 P338 结构图

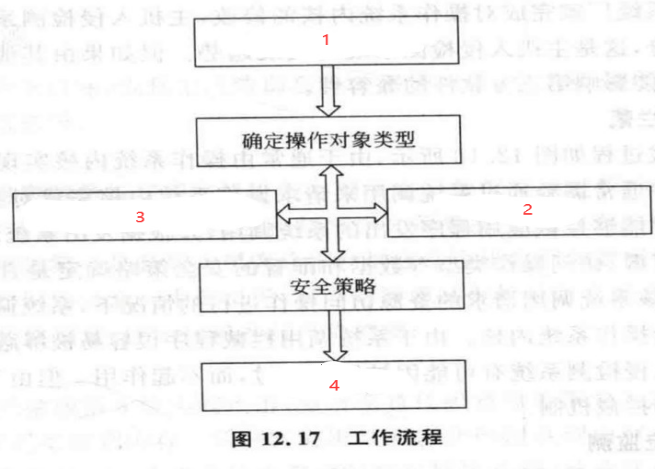


A:事件发生器 B:事件分析器 C:相应单元 D:时间数据库

记住通用框架结构

图中数字对应答案为：1A,2B,3C,4D

二、主机入侵检测系统工作流程中1，4分别是()和() P367 工作流程图



A:拦截操作请求 B:系统状态 C:采集和操作相关信息 D:操作决策

对应答案：1A,2B,3C,4D

填空(可归到选择)

网络入侵检测机制主要分为三类，分别是：攻击特征检测，协议译码和异常检测

P350 12.2.3

判断题

一、入侵检测系统评价指标分别是：入侵检测系统减少误报、入侵检测系统减少漏报。 P346 12.1.9

答案：错，还有捕获和检测信息流的能力。

三个指标分别是正确性，全面性和性能，但是可以进一步精确解释这三个指标是什么。

二、目前，用于拦截操作请求的机制有修改系统内核，系统调用拦截和网络信息流检测等。 P361 12.3.4拦截机制

答案：对

三、主机资源是攻击目标，也是主机防御系统的保护对象，它主要包括网络，内存，进程，文件和系统配置信息等。 P363 12.3.5主机资源

答案：对

名词解释

一、入侵检测系统概念中的在线方式和杂凑方式 P339 12.1.4

入侵检测系统的两种应用方式。

在线方式下，流经关键链路的信息必须经过入侵检测系统，因此，入侵检测系统能 实时阻断入侵信息的传输过程。

杂凑方式下，入侵检测系统对信息经过关键链路的传输过程没有影响，只能被动捕 获经过关键链路传输的信息，因此，无法实时阻断入侵信息的传输过程。

二、网络入侵检测系统中的协议译码 P357 第一段

一是对IP分组格式，TCP报文格式进行检测

二是根据TCP报文或IP报文的协议字段值确定报文净荷对应的应用层协议，通过协议来检测净荷各项内容，如发现当前净荷内容和协议要求不一致，则该信息可能是攻击信息。

三、网络入侵检测机制的安全策略 P356 12.2.4

主要用于指定一下信息：一是指定需要检测的信息流，二是指定检测机制和检测内 容，三是指定对入侵信息的反制动作。

简答题

一、入侵检测系统的需要具有的功能： P338 上面

入侵检测系统是在网络中传输的信息流中，或者输入输出主机系统的信息流中检测 出用于实施入侵的异常信息，并对异常信息予以反制。

所以需要：

1：获取流经某个网段的信息或拦截发送给操作系统内核的操作请求的能力。

2：检测获取的信息流或拦截到的操作请求是否具有攻击性的能力。

3：对多个点上的检测结果进行综合性分析和关联的能力。

4：记录入侵过程，提供审计和调查取证需要的信息能力

二、简述主机入侵检测系统和网络入侵检测系统不能互相替代的原因 P340,341

对于主机入侵检测系统来说：1、只能保护单台主机免遭攻击，2、有些攻击是主机 入侵检测系统无法检测的，如黑客进行的主机扫描等操作

对于网络入侵检测系统来说：实现对主机的保护是困难的。

简单来说，主机入侵检测系统主要保护主机，网络入侵检测系统监控网络，二者相辅相成。

第二题点太多，需要总结。