**1.入侵检测的概念以及检测的内容？**

**参考答案：**

入侵是指任何试图破坏或危及信息系统资源的完整性、机密性和可用性的行为。一旦信息系统与网络连接，其被攻击者入侵的危险就可能存在。入侵检测就是对入侵行为的发现，是一种试图通过观察行为、安全日志或审计数据来检测入侵的技术。

入侵检测的内容包括试图闯入，成功闯入，冒充其他用户，违反安全策略，合法用户的泄露，独占以及恶意使用资源等。

**2.入侵检测系统应该具有的功能和作用？**

**要点：（1）监控系统的异常操作，审计操作系统日志；（2）扫描系统漏洞；（3）保护文件系统完整性；（4）入侵行为的实时响应与统计分析；（5）可扩展性。**

**参考答案：**

进行入侵检测的软件与硬件组合就是入侵检测系统（IDS），它不同于防火墙、访问控制系统和漏洞扫描系统，其作用和功能如下：

（1）监控、分析用户和系统的活动，查找非法用户和合法用户的越权操作。

（2）审计系统的配置和弱点，提示管理员修补漏洞。

（3）评估关键系统和数据文件的完整性，如：计算和比较文件的校验和。

（4）识别攻击的活动模式并向系统安全管理员报警，能够对检测到的入侵行为进行实时响应。

（5）对异常活动进行统计分析，发现入侵行为的规律。

（6）对操作系统进行审计跟踪管理，识别用户违反安全策略的行为。

一个成功的入侵检测系统能够根据网络威胁、系统构造和安全需求的改变而改变其规模。

**3. 入侵检测系统的优、缺点是什么？分析这些优、缺点给信息系统安全设计所带来的影响。**

**参考答案：**

入侵检测的优点包括：提高信息安全体系中其他部分的完整性，提高系统的监控能力，能够从入口点到出口点跟踪用户的活动，能够识别和汇报文件的变化，能够侦测系统配置错误并纠正，能够识别特殊攻击类型并向系统安全管理员汇报，进行自动防御。

但入侵检测也存在缺点，即：它无法弥补差的认证机制；不能弥补网络协议的弱点；不能弥补系统服务质量或完整性的缺陷；如果没有人的干预，不能管理攻击调查；不能指导安全策略的内容；不能分析一个堵塞的网络；不能处理有关 package-level攻击。

**4.根据分析方法分类的入侵检测有哪些？它们的特点各有哪些不同？**

**要点：（1）异常IDS，基于主体活动的特征选择和阈值的判定，在主体的活动过程中进行是否为入侵行为的判断；（2）特征IDS，根据攻击方的行为特征建立模型，并将日常检测获得的特征与之比对；（3）协议分析IDS，根据网络协议规则是否被破坏进行入侵检测。**

**参考答案：**

根据入侵检测的分析方法不同，可以将入侵检测系统分为以下三类：

（1）异常入侵检测系统。它是通过比较入侵行为、异常活动与正常主体活动的差异，建立“主体活动简档”。当主体活动违反其统计规律时，判断为“入侵”行为。在这种入侵检测系统中，对异常阈值与特征的选择是关键。但这类入侵检测系统的局限是并非所有的入侵都表现为异常，而且主体的活动轨迹难于计算和更新。

（2）特征入侵检测系统。它是根据攻击者的入侵行为特征建立模型，然后将观察的对象与其进行比较，如果符合该模型，则判断为入侵行为。

（3）协议分析入侵检测系统。它是利用网络协议的高度规则性快速判断入侵行为。

**5.如何检测攻击者的入侵行为？**

**要点：（1）说明入侵信息收集的来源；（2）利用模式匹配、统计分析、完整性分析判断获取的信息是否异常；（3）在攻击行为被检测到后，根据攻击行为进行响应。**

**参考答案：**

入侵检测过程分为三个阶段，即：入侵信息收集，入侵信息分析和入侵检测响应。

入侵信息收集是指从系统、网络中收集数据和用户活动的状态和行为，为此，需要在计算机网络系统中的若干不同关键点（不同网段和不同主机）收集信息。信息收集的来源主要有以下四个方面：（1）系统和网络日志。（2）目录和文件中的异常改变。（3）程序执行中的异常行为。（4）物理形式的入侵信息。

入侵信号分析：对收集到的上述信息进行分析，从海量信息中找出表征入侵行为的异常信息，它是入侵检测系统的核心环节。一般采用三种手段进行分析：模式匹配，统计分析和完整性分析。前两种方法用于实时入侵检测，而完整性分析则用于事后分析。

当一个攻击企图或事件被检测到以后，入侵检测系统就应该根据攻击或事件的类型或性质，做出相应的处理，即：通知系统安全管理员，系统正在遭受不良行为的入侵（被动响应），或采取一定的措施阻止入侵行为的继续（主动响应）：如断开网络连接，增加安全日志，杀死可疑程序，甚至对攻击系统实施反击。

**6.分析包捕获的工作原理。**

**要点：（1）包捕获机制分为三个部分：底层是包采集机制，中间层是包过滤机制，顶层是用户程序；（2）包捕获部件是在数据链路层的旁路处理器，不影响网络协议栈对数据包的处理；（3）旁路获取的数据包发送到过滤部件，根据条件过滤数据包；（4）过滤后的数据包经过缓存发送到应用程序**

**参考答案：**

包捕获机制是依赖于操作系统的。从广义的角度看，一个包捕获机制包含三个主要部分：最底层是针对特定操作系统的包捕获机制，中间层是包过滤机制，最高层是针对用户程序的接口。

数据包常规的传输路径依次为：网卡，设备驱动层，数据链路层，网络层，传输层，应用层。而包捕获机制是在数据链路层增加一个旁路处理器，对发送和接收的数据包进行缓冲和过滤等处理，最后直接送到应用程序。在这个过程中，包捕获机制并不影响网络协议栈对数据包的处理，它只是对所捕获的数据包根据用户的要求进行筛选，最终把满足过滤条件的数据包传递给用户程序。

包过滤机制实际上是针对数据包的布尔值操作函数，如果函数最终返回 true，则通过过滤，反之则被丢弃。形式上，包过滤由一个或多个谓词判断的“与（AND）”操作和“或（OR）”操作构成，每一个谓词判断基本上对应了数据包的协议类型或某个特定值。如：Sniffer 工具中，过滤的数据包为 TCP 类型且端口为 110 或 ARP 类型。包过滤机制在具体实现上与数据包的协议类型并无多少关系，它只是把数据包简单地看成一个字节数组，而谓词判断会根据具体的协议映射到数组特定位置的值。如：判断 ARP 类型的数据包，只需要判断数组中第 13、14 字节是否为 0x0806。

**7.分析包捕获机制的作用和局限性。**

**要点：**作用：（1）包捕获机制是从数据链路层旁路数据包，不影响数据包的正常处理；（2）数据包捕获机制对于用户和应用程序是透明的；（3）可以根据用户的需要对数据包头和协议进行过滤。

局限性：（1）所有的程序都是针对操作系统开发，可移植性差；（2）如果在内核空间执行所有操作，速度快，但程序开发复杂；如果在内核空间采集数据，用户空间处理数据，则浪费CPU周期。

**参考答案：**

作用：（1）包捕获为数据包捕获软件的设计提供了工作机制，作为sniffer、winpcap、wireshark、tcpdump等工具的底层原理提出。（2）建立在目标系统上，帮助实现网络数据包的实时获取、管理和控制。

BPF数据包捕获机制的局限性：虽然过滤一部分数据包在一定的程度上降低了系统的开销，提高了效率。但它的捕获和过滤都是在linux内核中完成。这样一来只要linux内核一更新，它也需要更新，降低了它的可移植性和通用性。

Libpcap数据包捕获机制的局限性：数据包经过了linux得内核网络协议栈，从网卡到用户空间的传递过程，存在多次的拷贝和中断相应，消耗大量得cpu时间片，降低系统整体的数据分析能力。

**8.共享网络和交换网络的数据捕获方式有什么不同？分析说明。**

**要点：（1）数据捕获在共享网络中需要配置本地的网卡工作模式，接受目的地址不是自身的数据包。（2）在交换网络中，无法侦听到其他端口和网段的数据包，可采用在网络中捕获、端口映射、改变网络结构、ARP欺骗等方法。**

**参考答案：**

共享网络的数据传输是通过广播的方式实现的。在通常情况下，主机上的通信网络程序只能响应与自己硬件地址匹配的或以广播形式发出的数据帧，对于到达网络接口但不是发给此地址的数据帧，网络接口直接丢弃，不做任何响应，即应用程序无法收到与自己无关的数据包。要想捕获流经网卡的所有数据包，包括不属于自己主机的数据包，就必须绕开系统正常工作的处理机制，直接访问数据链路层。为此，首先需要将网卡的工作模式设置为混杂模式，使其能够接收目标地址不是自己的 MAC 地址的数据包，然后直接访问数据链路层，获取数据并由应用程序进行过滤处理。

在使用交换机的交换网络中，处于侦听状态下的程序或设备只能捕获到它所连接端口上的数据，而无法侦听其他端口和其他网段的数据。因此，实现交换网络的数据捕获需要采用以下特殊的方法。（1）将数据包捕获程序安装在网络或代理服务器上，从而捕获到整个局域网的数据包。（2）对交换机实行端口映射，将所有端口的数据包全部映射到某个连接监控设备的端口上。3）在交换机和路由器之间连接一个 Hub，将数据以广播的方式发送。（4）采用 ARP 欺骗，在负责数据包捕获的设备上实现整个网络的数据包转发，这将降低局域网的效率。

**9.利用 C＋＋程序分别实现 BF 算法、KMP 算法、BM 算法和 AC 算法。**

**略**

**10.在数据预处理中，数据集成的难点是什么？**

**要点：（1）数据语义的不同降低数据预处理的有效性；（2）字段结构的差异降低数据集成的效率；（3）字段冗余和重复，影响数据集成的效率。（4）可能出现数据不一致的情况，需要进行取舍。**

**参考答案：**

数据集成是一个数据整合的工程，是将来自不同数据源的结果或附加信息进行合并处理，解决不同结构和不同属性的数据的差异性。该部分内容主要涉及数据选择、语义差异、结构差异、字段间的关联关系，以及数据的冗余重复等问题。在网络入侵检测系统中，可能需要接收来自不同数据源的数据，因此需要为这些不同的数据源提供统一的数据接口，以使高层应用能够汇总来自不同数据源的结果及其附加判断信息。数据集成不是简单合并，而是把数据进行统一化和规范化处理。

（1）由于数据来源的不同带来语义的差异。网络入侵检测中可能需要应对不同种类的异常检测，在针对每一种类型的入侵检测做数据集成时，需要考虑到数据对问题解决的有效性，进行数据的取舍与数据格式的重整。

（2）字段结构的不同，包括字段名称、数据类型、数据格式、单位、取值范围的差异。这些差异会影响数据集成的效率。

（3）字段的冗余一般源自于字段之间存在强相关性或者几个字段间可以相互推导得到。通过检测字段的相关性，可以侦察到数据冗余。相似的还有数据重复带来的问题。

（4）数据冲突就是两个数据源，同样的数据，但是取值记录的不一样。对待这种问题，就需要对实际的业务知识有一定的理解。同时，对数据进行调研，尽量明确造成冲突的原因。如果数据的冲突实在无法避免，就要考虑冲突数据是否都要保留、是否要进行取舍，如何取舍等问题。

**11.评估入侵检测系统性能的指标有哪些？它们的作用？**

**参考答案：**

评价入侵检测系统主要有以下 5 个指标：

（1）准确性（Accuracy）：指入侵检测系统能正确地检测出系统的入侵活动，从各种行为中正确地识别入侵的能力。当一个入侵检测系统的检测不准确时，就有可能把系统中的合法活动当作入侵行为并标识为异常，即虚警现象。

（2）处理性能（Performance）：指入侵检测系统处理源数据的速度。当入侵检测系统的处理性能较差时，它就不可能实现实时的入侵检测，并有可能成为整个系统的瓶颈，进

而严重影响整个系统的性能。

（3）完备性（Completeness）：指入侵检测系统能够检测出所有攻击行为的能力。如果存在一个攻击行为无法被入侵检测系统检测出来，那么该入侵检测系统就不具有检测完备性。也就是说，它把对系统的入侵活动当作正常行为，出现漏报现象。由于在一般情况下，攻击型、攻击手段的变化很快，我们很难得到关于攻击行为的所有知识，所以关于入侵检测系统的检测完备性的评估相对比较困难。

（4）容错性（Fault Tolerance）：入侵检测系统自身必须能够抵御对它的攻击，特别是拒绝服务攻击。由于大多数入侵检测系统运行在极易遭受攻击的系统和硬件平台上，从而使得入侵检测系统的容错性显得特别重要。

（5）及时性（Timeliness）：及时性要求入侵检测系统必须尽快地分析数据并将分析结果传递出去，以使系统安全管理员能够在入侵攻击尚未造成更大伤害之前做出反应，阻止攻击者修改审计系统甚至入侵检测系统的企图。

**12.入侵检测系统的测试评估方法是什么？**

**参考答案：**

（1）功能性测试。功能性测试出来的数据能够反映出入侵检测系统的攻击检测、报告、审计、报警等能力。

攻击识别。以 TCP/IP 为例，识别攻击可以分为以下几种：协议包头攻击分析的能力：入侵检测系统是否能够识别与 IP 包头相关的攻击；重装攻击分析的能力，入侵检测系统能够重装多个 IP 包的分段并从中发现攻击的能力；数据驱动攻击分析能力。入侵检测系统具有分析 IP 包的具体内容的能力。

抗攻击性。入侵检测系统可以抵御拒绝服务攻击。对于某一时间段内的重复攻击，入侵检测系统能够识别并能抑制不必要的报警。

过滤。入侵检测系统中的过滤器可以方便设置规则，以便根据需要过滤掉不需要的原始数据信息，如：网络上的数据包和审计日志文件等。一般要求入侵检测系统的过滤器具有：修改或调整能力；创建简单字符规则的能力；使用脚本工具创建复杂规则的能力。

报警。报警机制是入侵检测系统的必需功能，一旦发现入侵行为，即刻向系统安全管理员发送报警信号。

日志。入侵检测系统应具有保存日志数据的能力。按照特定需求说明，日志内容可以选取。

报告。入侵检测系统能够产生入侵行为报告，提供查询报告，以及创建和保存报告。

（2）性能测试。性能测试是在各种不同的环境下，检验入侵检测系统的承受能力。其主要的指标有以下几点：

入侵检测系统引擎的吞吐量。入侵检测系统在预先不加载攻击标签的情况下，处理原始检测数据的性能。

包的重装性能。测试目的是评估入侵检测系统的包重装能力。如：通过 Ping of Death 攻击，入侵检测系统的入侵签名库只有单一的 Ping of Death 标签，这时来测试入侵检测系统的响应情况。

过滤的效率。测试的目标是评估入侵检测系统在遭受攻击的情况下过滤器接收、处理和报警的效率。这种测试可以利用 LAND 攻击的基本包头为引导，这种包的特征是源地址等于目的地址。

（3）产品可用性测试评估入侵检测系统用户界面的可用性、完整性和扩充性，能支持多种操作系统，容易使用且稳定。