网络安全期末复习

题型：1、选择、判断、简答（45% ）

2、分析题（55% ）

注：如有发现错误，希望能够提出来。

第一章 引言

一、填空题

1、信息安全的 3 个基本目标是：保密性、完整性和可用性。此外，还有一个不可忽视的目标是：合法使用。

2、网络中存在的 4 种基本安全威胁有：信息泄漏、完整性破坏、拒绝服务和非法使用。

3、访问控制策略可以划分为：强制性访问控制策略和自主性访问控制策略。

4、安全性攻击可以划分为：被动攻击和主动攻击。

5、X.800 定义的 5 类安全服务是：认证、访问控制、数据保密性、数据完整性、不可否认性。

6、X.800 定义的 8 种特定的安全机制是：加密、数字签名、访问控制、数据完整性、认证交换、流量填充、路由控制和公证。

7、X.800 定义的 5 种普遍的安全机制是：可信功能度、安全标志、事件检测、安全审计跟踪和安全恢复。

二、思考题

2、基本的安全威胁有哪些？主要的渗入类型威胁是什么？主要的植入类型威胁时什么？请列出几种最主要的威胁。

答：基本的安全威胁有：信息泄露、完整性破坏、拒绝服务、非法使用。

主要的渗入类型威胁有：假冒、旁路、授权侵犯。

主要的植入威胁有：特洛伊木马 、陷门

最主要安全威胁：（1）授权侵犯（2）假冒攻击（3）旁路控制（4）特洛伊木马或陷阱（5）媒体废弃物（出现的频率有高到低）

4.什么是安全策略？安全策略有几个不同的等级？

答：安全策略：是指在某个安全区域内，施加给所有与安全相关活动的一套规则。

安全策略的等级：1 安全策略目标；2 机构安全策略；3 系统安全策略。

6. 主动攻击和被动攻击的区别是什么？请举例说明。

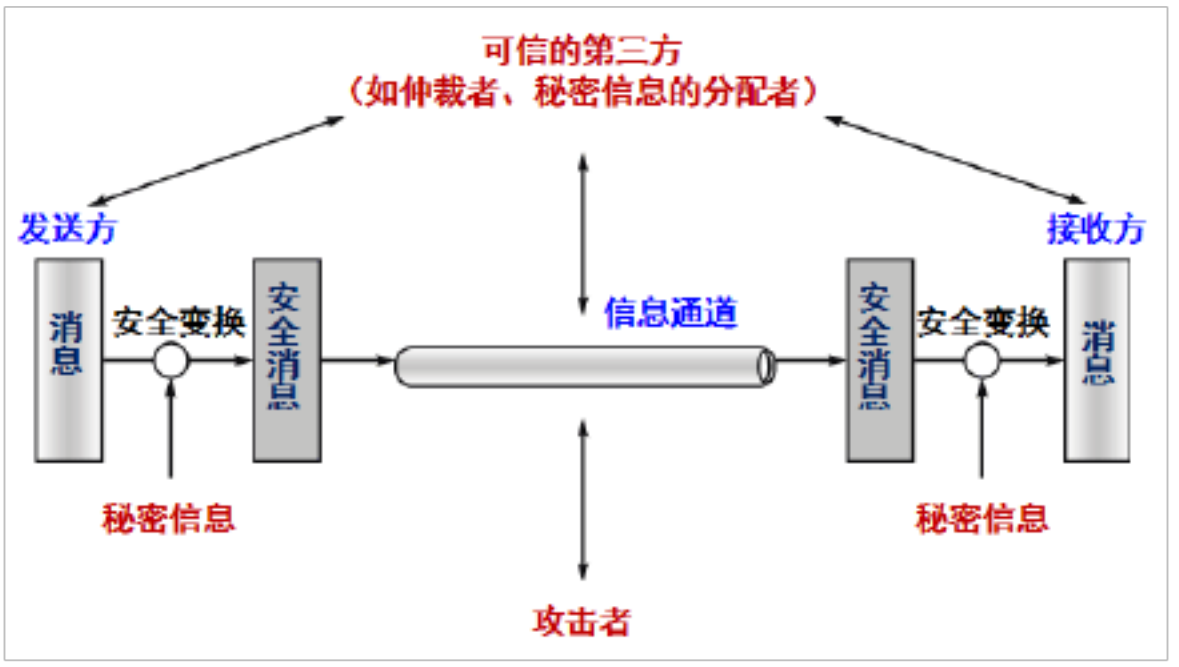
答：区别：被动攻击时系统的操作和状态不会改变，因此被动攻击主要威胁信息的保密性。主动攻击则意在篡改或者伪造信息、也可以是改变系统的状态和操作，因此主动攻击主要威胁信息的完整性、可用性和真实性。

主动攻击的例子：伪装攻击、重放攻击、消息篡改、拒绝服务。

被动攻击的例子：消息泄漏、流量分析。

9、请画出一个通用的网络安全模式，并说明每个功能实体的作用。

网络安全模式如下：



网络安全模型由六个功能实体组成：消息的发送方（信源）、消息的接收方（信宿）、安全变换、信息通道、可信的第三方和攻击者。

第二章 低层协议的安全性

一、填空题

1、主机的 IPv4 的长度为 32b，主机的 MAC 地址长度为 48b。IPv6 的地址长度为 128b。

2、ARP 的主要功能是将 IP 地址转换成为物理地址

3、NAT 的主要功能是实现 网络地址和 IP 地址之间的转换，它解决了 IPv4 地址短缺的问题。

4、DNS 服务使用 53 号端口，它用来实现域名到 IP 地址或 IP 地址到域名的映射。

二、思考题

1、简述以太网上一次 TCP 会话所经历的步骤和涉及的协议。

答：步骤：开放 TCP 连接是一个 3 步握手过程：在服务器收到初始的 SYN 数据包后，该

连接处于半开放状态。此后，服务器返回自己的序号，并等待确认。最后，客户机发送第 3 个数据包使 TCP 连接开放，在客户机和服务器之间建立连接。

协议:路由协议、Internet 协议、 TCP/IP 协议

2、在 TCP 连接建立的 3 步握手阶段，攻击者为什么可以成功实施 SYN Flood 攻击？在实际中，如何防范此类攻击？

答：当 TCP 处于半开放状态时，攻击者可以成功利用 SYN Flood 对服务器发动攻击。攻击者使用第一个数据包对服务器进行大流量冲击，使服务器一直处于半开放连接状态，导致服务器无法实现 3 步握手协议。

防范 SYN Flood 攻击，一类是通过防火墙、路由器等过滤网关防护；另一类是通过加固 TCP/IP 协议栈防范。

4、为什么 UDP 比 BGP 的主要区别。

答：由于 UDP 自身缺少流控制特性，所以采用 UDP 进行大流量的数据传输时，就可能造成堵塞主机或路由器，并导致大量的数据包丢失；UDP 没有电路概念，所以发往给定端口的数据包都被发送给同一个进程，而忽略了源地址和源端口号；UDP 没有交换握手信息和序号的过程，所以采用 UDP 欺骗要比使用 TCP 更容易。

9、通过 DNS 劫持会对目标系统产生什么样的影响？如何避免？

答：通过劫持了 DNS 服务器，通过某些手段取得某域名的解析记录控制权，进而修改此域名的解析结果，导致对该域名的访问由原 IP 地址转入到修改后的指定 IP，其结果就是对特定的网址不能访问或访问的是假网址。

避免 DNS 劫持:暴露的主机不要采用基于名称的认证；不要把秘密的信息放在主机名中；进行数字签名

14、判断下列情况是否可能存在？为什么？

（1）通过 ICMP 数据包封装数据，与远程主机进行类似 UDP 的通信。

（2）通过特意构造的 TCP 数据包，中断两台机器之间指定的一个 TCP 会话。

答:（1）不存在。TCP/UDP 是传输层（四层）的协议，只能为其上层提供服务，而 ICMP 是网络互联层（三层）的协议，怎么可能反过来用四层协议来为比它还低层的数据包来服务呢。

（2）如果攻击者能够预测目标主机选择的起始序号，他就可能欺骗该目标主机，使目标主机相信自己正在与一台可信的主机会话。

第 4 章 单（私）钥加密体制

一、填空题

1、密码体制的语法定义由以下六部分构成：明文消息空间、密文消息空间、加密密钥空间、密钥生成算法、加密算法、解密算法。

2、单（私）钥加密体制的特点是：通信双方采用的密钥相同所以人们通常也称其为对称加密体制。

第 9 章 数字证书与公钥基础设施

一、选择题

1． 数字证书将用户与其 B 相联系。

A．私钥 B. 公钥 C. 护照 D. 驾照

2． 用户的 B 不能出现在数字证书中。

A. 公钥 B. 私钥 C. 组织名 D. 人名

3. A 可以签发数字证书。

A． CA B. 政府 C. 小店主 D. 银行

4． D 标准定义数字证书结构。

A. X.500 B. TCP/IP C. ASN.1 D. X.509

5．RA A 签发数字证书。

A. 可以 B.不必 C.必须 D. 不能

6．CA 使用 D 签名数字证书。

A. 用户的公钥 B. 用户的私钥 C. 自己的公钥 D.自己的私钥

7. 要解决信任问题，需使用 C 。

A. 公钥 B. 自签名证书 C. 数字证书 D. 数字签名

8. CRL 是 C 的。

A. 联机 B. 联机和脱机 C. 脱机 D. 未定义

9. OCSP 是 A 的。

A. 联机 B. 联机和脱机 C. 脱机 D. 未定义

10. 最高权威的 CA 称为 C 。

A. RCA B. RA C. SOA D. ARA

二、思考题

1、数字证书的典型内容什么？

答：数字证书的概念：一个用户的身份与其所持有的公钥的结合，由一个可信任的权威机构 CA来证实用户的身份,然后由该机构对该用户身份及对应公钥相结合的证书进行数字签名，以证明其证书的有效性。

一般包括：

（1）证书的版本信息；

（2）证书的序列号，每个证书都有一个唯一的证书序列号；

（3）证书所使用的签名算法；

（4）证书的发型机构名称；

（5）证书的有效期；
（6）证书所有人名称；
（7）证书所有人的公开密钥；
（8）证书发行者对证书的签名；

4、简述撤销数字证书的原因？
答：(1) 数字证书持有者报告该证书中指定公钥对应的私钥被破解（被盗）；
(2) CA 发现签发数字证书是出错；
(3) 证书持有者离职，而证书为其在职期间签发的。

10、攻击者 A 创建了一个证书，放置一个真实的组织名（假设为银行 B）及攻击者自己的公钥。你在不知道是攻击者在发送的情形下，得到了该证书，误认为该证书来自银行 B。请问如何防止该问题的产生？
答：

第 10 章 网络加密与密钥管理

一、填空题
1、网络加密方式有 4 种，它们分别是链路加密、节点加密、端到端加密和混合加密。
2、在通信网的数据加密中，密钥可分为基本密钥、会话密钥、密钥加密密钥、主机主密钥。
3、密钥分配的基本方法有利用安全信道实现密钥传输、利用双钥体制建立安全信道传递和利用特定的物理现象实现密钥传递等
4、在网络中，可信第三方 TTP 的角色可以由密钥服务器、密钥管理设备、密钥查阅服务和时戳代理 等来承担（请任意举出 4 个例子）
5、按照协议的功能分类，密码协议可以分为认证建立协议、密钥建立协议、认证的密钥建立协议。
6、Diffie-Hellman 密钥交换协议不能抵抗中间人的攻击
7、Kerberos 提供 A
A.加密 B.SSO C.远程登录 D.本地登陆
8、在 Kerberos 中，允许用户访问不同应用程序或服务器的服务器称为 A
A.AS B.TGT C.TGS D.文件服务器
9、在 Kerberos 中， C 与系统中的每个用户共享唯一一个口令。
A.AS B.TGT C.TGS D.文件服务器

二、思考题

1、网络加密有哪几种方式？请比较它们的优缺点。

答：网络加密的方式有 4 种分别是链路加密、节点加密、端到端加密、混合加密。

链路加密的优点：(1) 加密对用户是透明的，通过链路发送的任何信 息在发送前都先被加密。

(2) 每个链路只需要一对密钥。

(3) 提供了信号流安全机制。

缺点：数据在中间结点以明文形式出现，维护结点安全性的代价较高。

节点加密的优点：（1）消息的加、解密在安全模块中进行，这使消息内容不会被泄密

（2）加密对用户透明

缺点：（1）某些信息（如报头和路由信息）必须以明文形式传输

（2）因为所有节点都必须有密钥，密钥分发和管理变的困难

端到端加密的优点：①对两个终端之间的整个通信线路进行加密

②只需要 2 台加密机，1 台在发端，1 台在收端

③从发端到收端的传输过程中，报文始终以密文存在

④消息报头（源/目的地址）不能加密，以明文传送

⑤只需要 2 台加密机，1 台在发端，1 台在收端

⑥从发端到收端的传输过程中，报文始终以密文存在

⑦比链路和节点加密更安全可靠，更容易设计和维护

缺点：不能防止业务流分析攻击。

混合加密的是链路和端到端混合加密组成。

优点：从成本、灵活性和安全性来看，一般端到端加密方式较有吸引力。对于某些远程机构，链路加密可能更为合适。缺点信息的安全设计较复杂。

4、密钥有哪些种类？它们各自的用途是什么？请简述它们之间的关系？

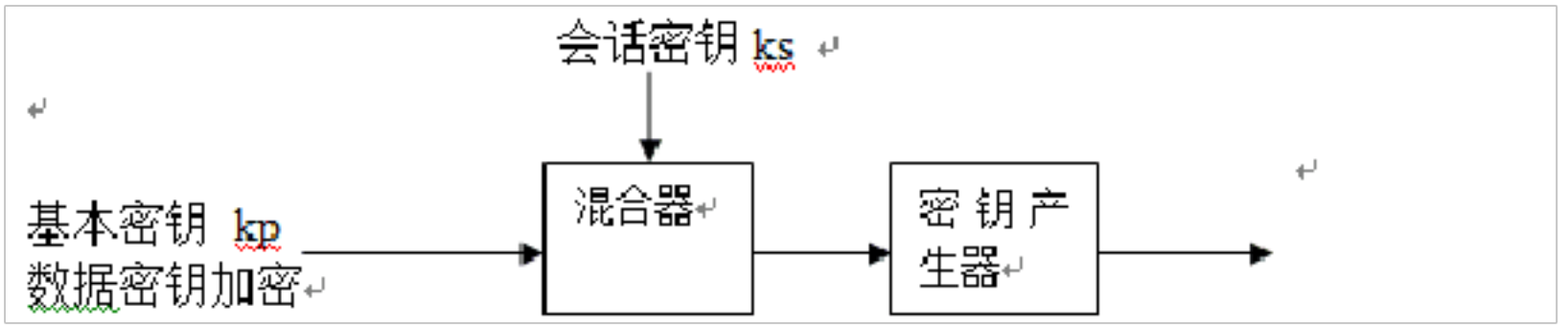
答：种类：1、基本密钥或称初始密钥其用途是与会话密钥一起去启动和控制某种算法所构造的密钥产生器，产生用于加密数据的密钥流。

2、会话密钥其用途是使人们可以不必繁琐的更换基本密钥，有利于密钥的安全和管理。

3、密钥加密密钥用途是用于对传送的会话或文件密钥进行加密时采用的密钥，也成为次主密钥、辅助密钥或密钥传送密钥。

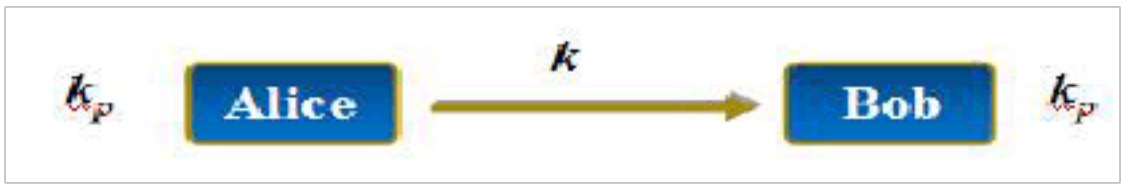
4、主机主密钥作用是对密钥加密密钥进行加密的密钥，存储于主机处理器中。

5、双钥体制下的公开钥和秘密钥、签名密钥、证实密钥。关系如图：

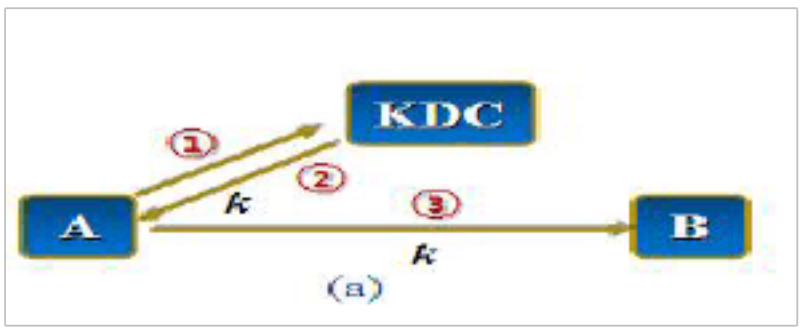


7、密钥分配的基本模式有哪些？

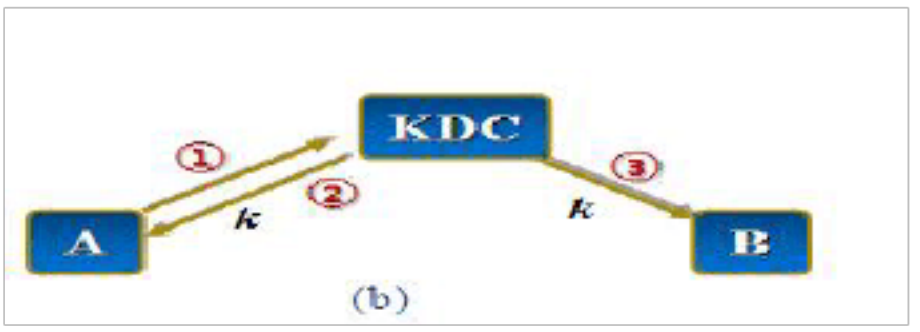
（a）点对点密钥分配：由 A 直接将密钥送给 B，利用 A 与 B 的共享基本密钥加密实现。



（b）密钥分配中心（KDC）：A 向 KDC 请求发送与 B 通信用的密钥，KDC 生成 k 传给 A,并通过 A 转递给 B,利用 A 与 KDC 和 B 与 KDC 的共享密钥实现。



（c）密钥传递中心（KTC）：A 与 KTC，B 与 KTC 有共享基本密钥。



11、在密码系统中，密钥是如何进行保护、存储和备份的？

密钥的保护：将密钥按类型分成不同的等级。大量的数据通过少量的动态产生的初级密钥来保护。初级密钥用更少量的、相对不变的二级密钥或主密钥 KM0 来保护。二级密钥用主机主密钥 KM1,KM2 来保护。少量的主密钥以明文形式存储在专用的密码装置中，其余的密钥以密文形式存储在专用密码装置以外。这样，就把保护大量数据的问题简化为保护和使用少量数据的问题。

密钥的存储：密钥在多数时间处于静态，因此对密钥的保存是密钥管理重要内容。密钥可以作为一个整体进行保存，也可化为部分进行保存。密钥的硬件存储；使用门限方案的密钥保存 ；公钥在公用媒体中存储。

密钥的备份：交给安全人员放在安全的地方保管；采用共享密钥协议。

第 12 章 防火墙技术

一、填空题

1、防火墙应位于__C__

A、公司网络内部　　B、公司网络外部

C、公司网络与外部网络　　D、都不对

2、应用网关的安全性__B__包过滤防火墙。

A、不如　　B、超过　　C、等于　　D、都不对

3、防火墙可以分为静态包过滤、动态包过滤、电路级网关、应用级网关、状态检查包过滤、切换代理和空气隙 7 种类型。

4、静态包过滤防火墙工作于 OSI 模型的网络层上，他对数据包的某些特定域进行检查，这些特定域包括：数据源地址、目的地址、应用或协议、源端口号、目的端口号。

5、动态包过滤防火墙工作于 OSI 模型的网络层上，他对数据包的某些特定域进行检查，这些特定域包括数据源地址、目的地址、应用或协议、源端口号、目的端口号。

6、电路级网关工作于 OSI 模型的会话层上，它检查数据包中的数据分别为源地址、目的地址、应用或协议、源端口号、目的端口号和握手信息及序列号。

7、应用级网关工作于 OSI 模型的应用层上，它可以对整个数据包进行检查，因此其安全性最高。

8、状态检测防火墙工作于 OSI 模型的网络层上，所以在理论上具有很高的安全性，但是现有的大多数状态检测防火墙只工作于网络层上，因此其安全性与包过滤防火墙相当。

9、切换代理在连接建立阶段工作于 OSI 模型的会话层上，当连接建立完成值后，再切换到动态包过滤模式，即工作于 OSI 模型的网络层上。

10、空气隙防火墙也称作安全网闸，它在外网和内网之间实现了真正的隔离。

二、思考题

1.防火墙一般有几个接口？什么是防火墙的非军事区（DMZ）？它的作用是什么？

答：防火墙一般有 3 个或 3 个以上的接口。网关所在的网络称为‘非军事区’（DZM）。网关的作用是提供中继服务，以补偿过滤器带来的影响。

2.为什么防火墙要具有 NAT 功能？在 NAT 中为什么要记录端口号？

答：使用 NAT 的防火墙具有另一个优点， 它可以隐藏内部网络的拓扑结构， 这在某种程度上提升了网络的安全性。 在 NAT 中记录端口号是因为在实现端口地址转换功能时，两次 NAT 的数据包通过端口号加以区分。

9.应用级网关与电路级网关有何不同？简述应用级网关的优缺点。

答：与电路级网关不同的是应用级网关必须针对每个特定的服务运行一个特定的代理，它只能对特定服务所生成的数据包进行传递和过滤。
应用级网关的优点：1、在已有的安全模型中安全性较高
2、具有强大的认证功能
3、具有超强的日志功能
4、应用级网关防火墙的规则配置比较简单
缺点：1、灵活性差 2、配置复杂 3、性能不高

14.防火墙有什么局限性？
答：防火墙是 Internet 安全的最基本组成部分，但对于内部攻击以及绕过防火墙的连接却无能为力，另外，攻击者可能利用防火墙为某些业务提供的特殊通道对内部网络发起攻击，注入病毒或木马。

15.软件防火墙与硬件防火墙之间的区别是什么？
答：软件防火墙是利用 CPU 的运算能力进行数据处理，而硬件防火墙使用专用的芯片级处理机制。

第 13 章 入侵检测系统

一、填空题
1、根据数据源的来源不同，IDS 可分为 基于网络 NID3 、 基于主机 HIDS 和两种都有 DIDS 种类型。
2、一个通用的 IDS 模型主要由数据收集、 检测器、知识库和控制器 4 部分组成。
3、入侵检测分为 3 个步骤，分别为信息收集、 数据分析 和 响应 。
4、一个 NIDS 的功能结构上至少包含 事件提取、入侵分析、入侵响应和远程管理 4 部分功能
5、DIDS 通常由 数据采集构建 、通信传输构建、入侵检测分析、应急处理的构建和 用户管理构建 5 个构建组成。
6、IDS 控制台主要由 日志检索、探测器管理、规则管理、日志报表和用户管理 5 个功能模块构成。
7、HIDS 常安装于被保护的主机，NIDS 常安装于 网络 入口处。
8、潜在人侵者的可以通过检查蜜罐日志来获取。
9、吸引潜在攻击者陷阱为蜜罐。

二、思考题
2、入侵检测系统按照功能可分为哪几类,有哪些主要功能?
答：功能构成包含：事件提取、入侵分析、入侵响应、远程管理 4 个部分功能

1
2、已知攻击特征的识别功能
3、异常行为的分析、统计与响应功能
4、特征库的在线和离线升级功能
5、数据文件的完整性检查功能
6、自定义的响应功能
7、系统漏洞的预报警功能
8、IDS 探测器集中管理功能

3、一个好的 IDS 应该满足哪些基本特征？
答：1、可以使系统管理员时刻了解网络系统的任何变更
2、能给网络安全策略的制定提供依据
3、它应该管理、配置简单，即使非专业人员也非常容易使用
4、入侵检测的规模还应根据网络威胁、系统构造和安全需求的改变而改变
5、入侵检测系统在发现入侵后会及时做出响应，包括切断网络连接、记录事件和报警。

6、什么是异常检测，基于异常检测原理的入侵检测方法有哪些？
答：异常检测技术又称为基于行为的入侵检测技术，用来识别主机或网络中的异常行为。通过收集操作活动的历史数据，建立代表主机、用户或网络连接的正常行为描述，判断是否发生入侵。
1、统计异常检测方法
2、特征选择异常检测方法
3、基于贝叶斯网络异常检测方法
4、基于贝叶斯推理异常检测方法
5、基于模式预测异常检测方法

7、什么是误用检测，基于误用检测原理的入侵检测方法有哪些？
答：误用检测技术又称为基于知识的检测技术。它通过对已知的入侵行为和手段进行分析，提取检测特征，构建攻击模式或攻击签名，判断入侵行为。
1、基于条件的概率误用检测方法
2、基于专家系统误用检测方法
3、基于状态迁移分析误用检测方法
4、基于键盘监控误用检测方法
5、基于模型误用检测方法

10、蜜网和蜜罐的作用是什么，它们在检测入侵方面有什么优势？
蜜罐的作用:1、把潜在入侵者的注意力从关键系统移开 2、收集入侵者的动作信息 3、设法让攻击者停留一段时间，使管理员能检测到它并采取相应的措施。