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

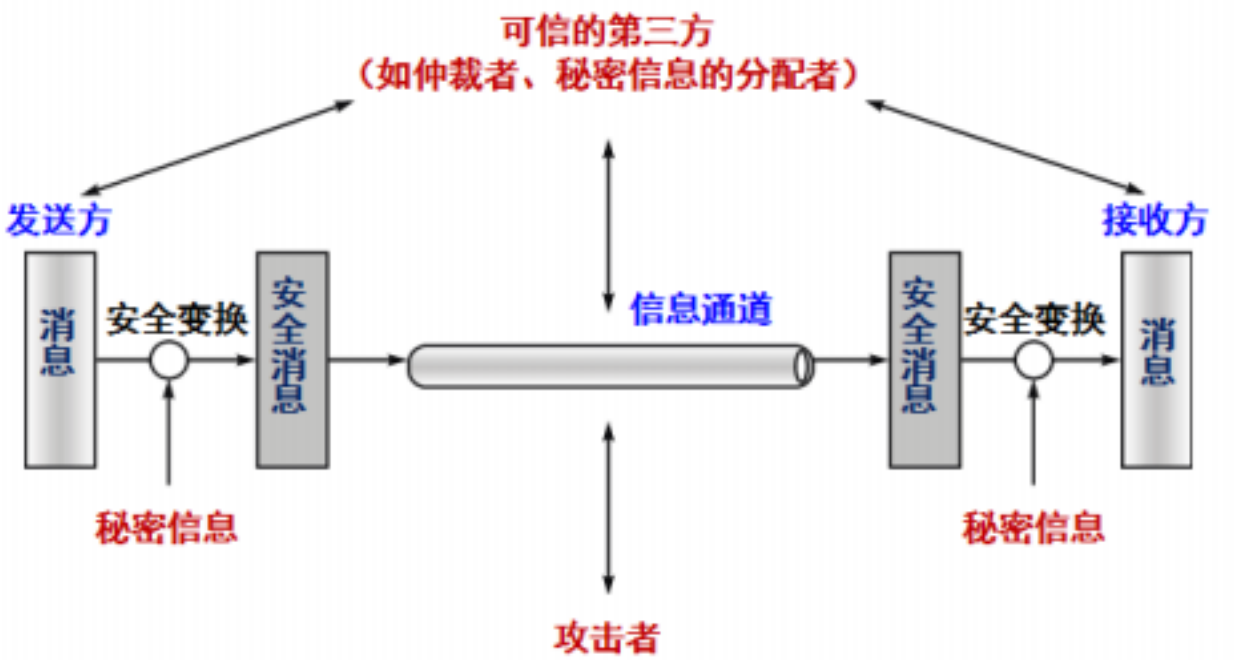
的保密性。主动攻击则意在篡改或者伪造信息、也可以是改变系统的状态和操作，因此主动攻击主要威胁信息的完整性、可用性和真实性。

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 **32**b，主机的 MAC 地址长度为 **48**b。IPv6 的地址长度为 **128**b。

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？

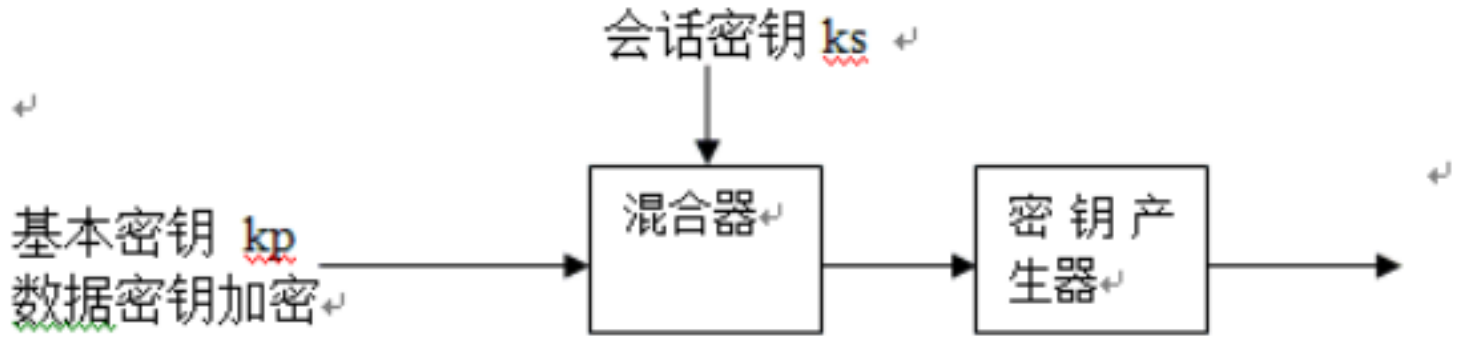
答：种类：1、基本密钥或称初始密钥其用途是与会话密钥一起去启动和控制某种算法所构造的密钥产生器，产生用于加密数据的密钥流。

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。

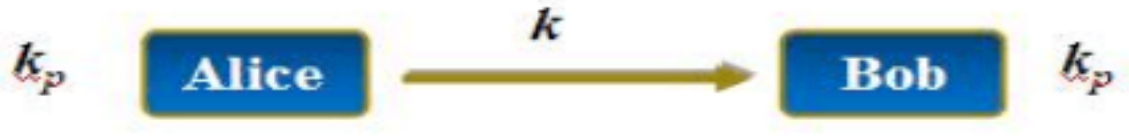
4、主机主密钥作用是对密钥加密密钥进行加密的密钥，存储于主机处理器中。

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、网络流量的跟踪与分析功能
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。

蜜网的作用： 1、蜜网在确保不被入侵者发现诱骗的前提下，尽可能多地捕获攻击行为信息， 2、 Honeynet 向 Internet 发起的连接进行跟踪，一旦 Honeynet 达到了规定的向外的连接数，防火墙将阻断任何后续的连接，并且及时向系统管理员发出警告信息 3、IDS 在数据链路层对蜜网中的网络数据流进行监控，分析和抓取以便将来能够重现攻击行为，同时在发现可疑举动时报警。
蜜罐和蜜网能从现存的各种威胁中提取有用的信息，发现新型的攻击工具，确定攻击模式并研究攻击者的攻击动机，从而确定更好的对策。

第 **14** 章 **VPN** 技术

一、填空题

1、根据访问方法的不同， VPN 可以分为 远程访问 **VPN** 和网关**-**网关 **VPN** 两种类型。

2、 VNP 的关键技术包括 隧道技术 、 加**/**解密技术 、 密钥管理技术 、 身份认证技术 和 访问控制 等。

3、第 2 层隧道协议主要有 **PPTP**、**L2F** 和 **L2TP** 3 个协议。

4、第 3 层隧道协议主要有 **IPSec** 、**GRE** 和 **MPLS** 3 个协议。

5、 IPSec的主要功能是实现加密、 认证和密钥交换，这 3 个功能分别由 **AH** 、**ESP** 和 **IKE** 3 个协议来实现

6、 IPSec VPN 主要由 管理模块 、密钥分配和生成模块 、身份认证模块 、数据加**/**解密模块 和 数据分组封装 **/**分解模块 5 个模块组成。

7、 IPSec在 OSI 参考模型的 C 层提供安全性。

A.应用 B.传输 C.网络 D.数据链路

8、 ISAKMP/Oakley 与 D 相关。

A.SSL B.SET C.SHTTP D.IPSec

9、 IPSec中的加密是由 D 完成的。

A.AH B.TCP/IP C.IKE D.ESP

10、在 A 情况下， IP 头才需要加密。

A.信道模式 B.传输模式 C.信道模式和传输模式 D、无模式

第一章 引言

1、网络安全的基本目标 ：保密性、完整性、可用性、合法使用

2、计算机病毒的发展态势： 1)、计算机病毒层出不穷 2)、黑客攻势逐年攀升 3)、系统存在安全漏洞 4)、各国军方加紧信息战研究

3、典型的安全威胁：假冒攻击 **/**冒充攻击、截获、窃听、篡改、消息重发 **/**重放攻击、拒绝服务攻击 **DOS**、**DDOS**（各定义详见课本）

4、防止重放攻击的方法： 时间戳、序号、提问与应答。

5、防范口令攻击的方法、暴力破解、字典攻击： 阻止选择低级口令；对口令文件严格保

护。要彻底解决口令机制的弊端是使用基于令牌的机制，转而使用基于令牌的机制。如果暂时不能做到，起码要使用一次性口令方案。

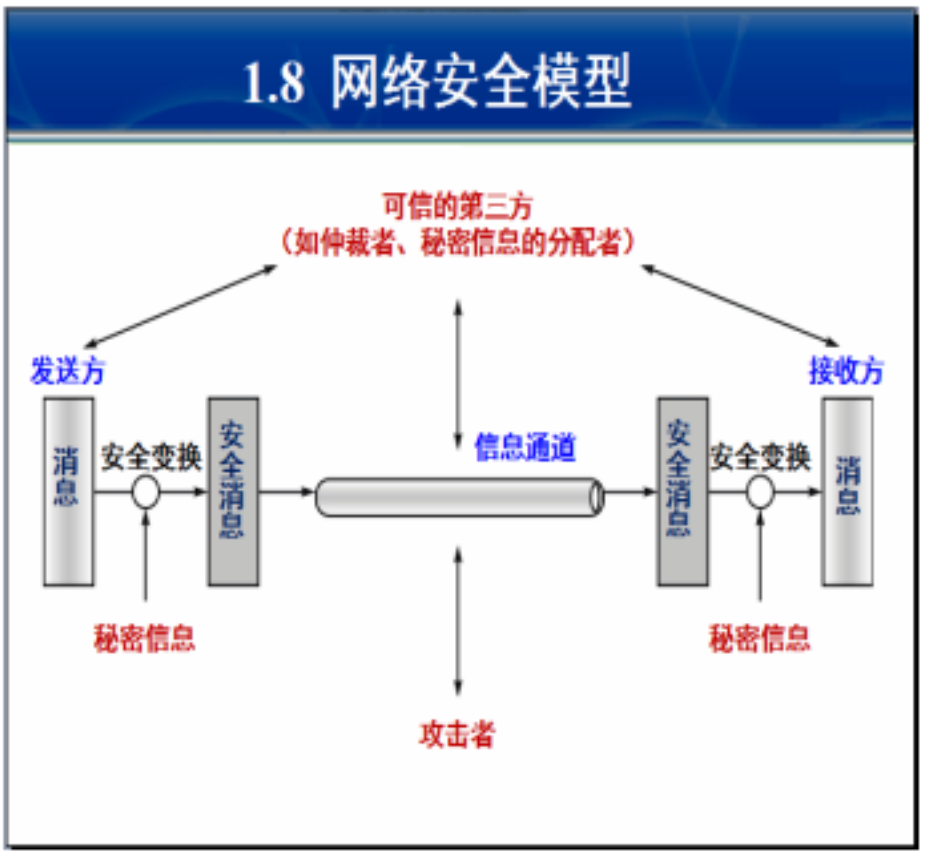
7、认证： 认证服务与保证通信的真实性有关 .在单条消息下 ,如一条警告或报警信号认证服务是向接收方保证信息来自所声称的发送方 .对于正在进行的交互 ,如终端和主机连接 ,就设计两个方面的问题 :首先 ,在连接的初始化阶段 ,认证服务保证两个实体是可信的 ,也就是说 ,每个实体都是它们所声称的实体 ;其次 ,认证服务必须保证该连接不受第三方的干扰 ,例如 ,第三方能够伪装成两个合法实体中的一方 ,进行非授权的传输或接收 .两个特殊的认证服务 :同等实体认证、数据源认证 .

认证机制的失效易导致服务器被攻击者欺骗。

被破坏的主机不会进行安全加密，因此对源主机采用密码认证的方式无用。

通过修改认证方案消除其缺陷，完全可以挫败这种类型的攻击。

8、网络安全的模型及说明（详见课本）



第二章 底层协议的安全性

9、 **IP** 协议的安全缺陷： 1） IP 协议不能保证数据就是从数据包中给定的源地址发出的，你绝对不能靠对源地址的有效性检验来判断数据包的好坏；

2）攻击者可以发送含有伪造返回地址的数据包，这种攻击叫做 IP 欺骗攻击；

3）当路由器遇到大数据流量的情况下，可能在没有任何提示的情况下丢掉一些数据包；

4）大数据包可能在中间节点上被分拆成小数据包。通过向包过滤器注入大量病态的小数据包，可以对包过滤器造成破坏；

10、 **ARP** 功能： 以太网发送的是 48 位以太地址的数据包； IP 驱动程序必须将 32 位 IP 目标地址转换成 48 位地址；两类地址存在静态或算法上的影射； ARP 用来确定两者之间的影射关系。

ARP 欺骗： 一台不可信赖的计算机会发出假冒的 ARP 查询或应答信息，并将所有流向它的数据流转移。这样，它就可以伪装成某台机器，或修改数据流。这种攻击叫做 ARP 欺骗攻击

11、ICMP 泛洪攻击： 黑客能够用 ICMP 对消息进行重定向。只要黑客能够篡改你到达目的地的正确路由， 他就有可能攻破你的计算机。 一般来说， 重定向消息应该仅由主机执行，而不是由路由器来执行。仅当消息直接来自路由器时，才由路由器执行重定向。然而，有时网管员有可能使用 ICMP 创建通往目的地的新路由。这种非常不谨慎的行为最终会导致非常严重的网络安全问题。

12、TCP 连接的三次握手过程：

用三次握手建立 TCP 连接， 如图所示： A 的 TCP 向 B 发出连接请求报文段，其首部中的同步位 SYN = 1 ，并选择序号 seq = x ，表明传送数据时的第一个数据字节的序号是 x 。B 的 TCP 收到连接请求报文段后，如同意，则发回确认。 B 在确认报文段中应使 SYN = 1 ，使 ACK = 1 ，其确认号 ack = x+1 ，自己选择的序号 seq = y 。A 收到此报文段后向 B 给出确认， 其 ACK = 1 ，确认号 ack == y+1 。 A 的 TCP 通知上层应用进程， 连接已经建立。 B 的 TCP 收到主机 A 的确认后，也通知其上层应用进程： TCP 连接已经建立。

13、TCP SYN 洪泛攻击： 攻击者利用 TCP 连接的半开放状态发动攻击。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，从而无法完成 3 步握手协议。

14、DHCP 、DNS 服务器功能： 域名 DHCP 用来分配 IP 地址，并提供启动计算机（或唤醒一个新网络） 的其他信息， 它是 BOOTP 的扩展。 域名系统 DNS 是一个分布式数据库系统，用来实现“ 域名— IP 地址 ”，或“ IP 地址—域名 ”的影射。

15、网络地址转换 **NAT** ：NAT 的主要作用是解决当前 IPv4 地址空间缺乏的问题。从概念上讲， NAT 非常简单：它们监听使用了所谓专用地址空间的内部接口，并对外出的数据包重写其源地址和端口号。外出数据包的源地址使用了 ISP 为外部接口分配的 Internet 静态 IP 地址。对于返回的数据包，它们执行相反的操作。 NAT 存在的价值在于 IPv4 的短缺。协议的复杂性使 NAT 变得很不可靠。在这种情况下，我们在网络中必须使用真正意义的防火墙，并希望 IPv6 的应用尽快得到普及。

第二部分 密码学

16、密码体制构成的五个要素： 明文空间 M、密文空间 C、密钥空间 K、加密算法 E、解密算法 D。

17、双钥密码体制的基本概念及各自的密钥的功能和作用： 基本概念是公钥密码技术又称非对称密码技术或双钥密码技术，其加密和解密数据使用不同的密钥。公开密钥

(public-key)，可以被任何人知道，用于加密或验证签名。私钥 (private-key)，只能被消息的接收者或签名者知道，用于解密或签名。

18、数字签名的基本概念： 收方能够确认或证实发方的签名，但不能伪造，简记为 R1-条件；发方发出签名的消息给收方后，就不能再否认他所签发的消息，简记为 S-条件；收方对已收到的签名消息不能否认，即有收报认证，简记为 R2-条件；第三者可以确认收发双方之间的消息传送，但不能伪造这一过程，简记为 T-条件。

第九章 公钥基础设施

19、**PKI** 定义及主要任务

1）定义： PKI 公钥基础设施， 是一种遵循标准的利用公钥理论和技术建立的提供安全服务的基础设施。 其目的是解决网上身份认证、 电子信息的完整性和不可抵赖性等安全问题，为网络应用提供可靠的安全服务。

2）主要任务： 确立可信任的数字身份。

20、**PKI** 体系组成部分： 证书机构、 注册机构、证书发布库、 密钥备份与恢复、证书撤销、PKI 应用接口

21、**CA** 系统功能： 证书生成、 证书颁布、 证书撤销、 证书更新、 证书归档、 CA 自身管理、日志审计、密钥恢复。

22、 **RA** 系统功能： 填写用户注册信息、提交用户注册信息、审核、发送生成证书申请、发放证书、登记黑名单、证书撤销列表管理、日志审计、自身安全保证 .

23、证书发布库的作用： 用于集中存放 CA 颁发证书和证书撤销列表；支持分布式存放，以提高查询效率； LDAP 目录服务支持分布式存放，是大规模 PKI 系统成功实施的关键，也是创建高效的认证机构的关键技术

24、**PKI** 提供的主要服务： 认证服务、 数据完整性服务、 数据保密性服务、 不可否认服务、 、公证服务。

25、数字证书的典型内容： 证书拥有者的姓名、证书拥有者的公钥、公钥的有限期、颁发数字证书的单位、颁发数字证书单位的数字签名、数字证书的序列号

26、 **SSL** 工作层次、协议构成及功能： （详见课件“ **PKI** 补充材料 **.PPT** ”）

1）工作层次：介于 TCP/IP 模型应用层与传输层之间

2）协议分成两部分：

SSL 握手协议 :通信双方互相验证身份、以及安全协商会话密钥

SSL 记录协议 :定义了传输的格式 ,对上层传来的数据加密后传输 .

3）功能：

a 鉴别机制：确保网站的合法性； b 保护隐私：采用加密机制； c 信息完整性：确保传输的信息不被篡改 .

27、数字证书的验证方法

RA 验证用户材料，以明确是否接受用户注册。

检查私钥的拥有证明（ POP, Proof of possession)。

RA 要求用户采用私钥对证书签名请求进行数字签名。

RA 生成随机数挑战信息，用该用户公钥加密，并将加密后的挑战值发送给用户。若用

户能用其私钥解密，则验证通过。

RA 将数字证书采用用户公钥加密后，发送给用户。用户需要用与公钥匹配的私钥解密方可取得明文证书。

28、数字证书撤销的原因及方法

1）原因： a）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）；b）CA 发现签发数字证书时出错； c）证书持有者离职，而证书为其在职期间签发的。

2）方法：发生第一种情形需由证书持有者进行证书撤销申请；发生第二种情形时，CA 启动证书撤销；发生第三种情形时需由组织提出证书撤销申请。

29、**PMI** 的定义、 **PMI** 与 **PKI** 的关系

定义：权限管理基础设施或授权管理基础设施，是属性证书、属性权威、属性证书框架等部件的集合体，用来实现权限和证书的产生、管理、存储、分发和撤销等功能。

PMI与PKI的关系

内 容	PKI实体	PMI实体
证书	PKC公钥证书	AC属性证书
证书颁发者	证书机构	属性机构
证书接收者	证书主体	证书持有者
证书的绑定	主体的名字绑定到公钥上	证书持有者绑定到一个或多个特权属性上
证书撤销	证书撤销列表（CRL）	属性证书撤销列表（ACRL）
信任的根	根CA或信任锚	权威源SOA
子机构	子CA	AA
验证者	可信方	特权验证者

第十章 网络加密与密钥管理

30、网络加密方式及特点

1）链路加密： a ）不同结点对之间的密码机和密钥不一定相同； b ）在每个中间节点上，消息先解密，后加密； c ）报文和报头可同时进行加密； d ）在结点内部，消息以明文的方式存在； e ）在链路加密中，密钥分配存在困难； f ）随着结点增多，保密机的需求数量很大。

2）节点加密： a) 在中间节点先对消息进行解密，然后进行加密吧 b) 在通信链路上所传输的消息为密文； c) 加密过程对用户是透明； d) 消息在节点以明文形式存在； e) 加解密过程在结点上的一个安全模块中进行； f) 要求报头和路由信息以明文形式传送。

3）端到端加密： a ）对两个终端之间的整个通信线路进行加密； b ）只需要 2 台加密机， 1 台在发端， 1 台在收端； c ）从发端到收端的传输过程中，报文始终以密文存在； d ）消息报头（源 /目的地址）不能加密，以明文传送； e ）只需要 2 台加密机， 1 台在发端， 1 台在收端； f ）从发端到收端的传输过程中，报文始终以密文存在； g ）比链路和节点加密更安全可靠，更容易设计和维护。

4）混合加密 **：** 链路加密 +端到端加密

31、软件加密和硬件的特点：

1）硬件加密的特点 :加密速度快、硬件安全性好、硬件易于安装。

2）软件加密的特点 :速度慢、灵活、轻便、可安装于多种机器上、可将几个软件组合成一个系统 .。

32、文件删除方法： 真正从存储器中消除所存储的内容需用物理上的重复写入方法。

33、密钥管理的功能及目的：

A）密钥管理是处理密钥从产生到最终销毁的整个过程中的有关问题，包括系统的初始化及密钥的产生、存储、备份 /恢复、装入、分配、保护、更新、控制、丢失、撤销和销毁等内容。

B）目的：是维持系统中各实体之间的密钥关系，以抗击各种可能的威胁，如： 1）密钥的泄露 2）密钥或公开钥的确证性的丧失，确证性包括共享或关于一个密钥的实体身份的知识或可证性。 3）密钥或公开钥未经授权使用，如使用失效的密钥或违例使用密钥。

34、密钥的种类及各类密钥的有效期

1）基本密钥 ：是由用户选定或由系统分配给他的、可在较长时间）内由一对用户所专用的秘密钥。记为 kp

2）会话密钥： 两个通信终端用户在一次通话或交换数据时所用的密钥。记为 ks

3）密钥加密密钥： 用于对所传送的会话或文件密钥进行加密的密钥，也称次主密钥。记为 ke

4）主机密钥： 它是对密钥加密钥进行加密的密钥，存储于主机处理器中。记为 km

5）数据加密密钥： 也称为工作密钥。

6）在双钥体制下 **,**有公钥和私钥、签名密钥和证实密钥之分

35、密钥的分级保护管理法：

如图所示，从图中可以清楚看出各类密钥的作用和相互关系。由此可见，大量数据可以通过少量动态产生的数据加密密钥（初级密钥）进行保护；而数据加密密钥又可由少量的、相对不变（使用期较长）的密钥（二级）或主机主密钥 0 来保护；其他主机主密钥（ 1 和 2）用来保护三级密钥。这样，只有极少数密钥以明文形式存储在有严密物理保护的主机密码器件中，其他密钥则以加密后的密文形式存于密码器之外的存储器中，因而大大简化了密钥管理，并改了密钥的安全性。

图 10-15 密钥的分级保护

为了保证密钥的安全，在密码设备中都有防窜扰装置。当密封的关键密码器件被撬开时，其基本密钥和主密钥等会自动从存储器件中清除，或启动装置自动引爆。

对于密钥丢失的处理也是安全管理中的一项重要工作。在密码管理中要有一套管理程序和控制方法，最大限度地降低密钥丢失率。对于事先产生的密钥加密密钥的副本应存放在可靠的地方作为备份。一旦密钥丢失时，可派信使或通过系统送新的密钥，以便迅速恢复正常业务。由于硬件和软件故障以及人为操作上的错误都会造成密钥丢失或出错，采用报文鉴别程序可以检测系统是否采用了正确的密钥进行密码操作。

表 10-4　密钥分级结构

密钥种类	密 钥 名	用　途	保护对象
密钥加密密钥	主机主密钥 $0=k_{m0}$	对现用密钥或存储在主机内的密钥加密	初级密钥
	主机主密钥 $1=k_{m1}$		二级密钥
	主机主密钥 $2=k_{m2}$		二级密钥
	终端主密钥 k_t（或二级通信密钥）	对主机外的密钥加密	初级通信密钥
	文件主密钥 k_v（或二级文件密钥）		初级文件密钥
数据加密密钥	会话（或初级）密钥 k_s	对数据加密	传送的数据
	文件（或初级）密钥 k_f		存储的数据

36、将密钥按类型分成不同的等级。

1）大量的数据通过少量的动态产生的初级密钥来保护。

2）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。

3）二级密钥用主机主密钥　　KM1,KM2　来保护。

4）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。　　（实际上保护一个密钥，因为　KM1,KM2　是由　KM0　派生而来。）

37、实现秘密信息共享的　　**3** 个基本方法

1)利用安全信道实现密钥传递　　2）利用双钥体制建立安全信息传递　　3）利用特定物理现象实现密钥传递。

38、密钥生存期的　**4** 个阶段

1）预运行阶段　,此时密钥尚不能正常使用

2）运行阶段　,密钥正常使用

3）后运行阶段　,密钥不再提供正常使用　,但为了特殊目的可以在脱机下接入

4）报废阶段　,将有关被吊销密钥从所有记录中山区　　,这类密钥不可能再用

第十二章　防火墙技术

39、防火墙工作原理：　防火墙是由软件和硬件组成的系统，它处于安全的网络和不安全的网络之间，根据由系统管理员设置的访问控制规则，对数据流进行过滤。

40、防火墙对数据流的　**3** 种处理方式：　a 允许数据流通过；　b 拒绝数据流通过，并向发送者回复一条消息，提示发送者该数据流已被拒；　　c 将数据流丢弃，不对这些数据包进行任

何处理，也不会向发送者发送任何提示信息。

41、防火墙的要求及基本目标：　　所有进出网络的数据流都必须经过防火墙；只允许经过授权的数据流通过防火墙；防火墙自身对入侵是免疫的。

42、防火墙的　**OSI** 模型工作层次及特点

防火墙通常建立在　TCP/IP 模型基础上，　OSI 模型与　TCP/IP 模型之间并不存在一一对应的关系。

43、防火墙的　**NAT** 功能：　隐藏内部网络的拓扑结构，提升网络安全性。

44、静态包过滤防火墙、动态包过滤防火墙的主要区别

1）静态包过滤：　使用分组报头中存储的信息控制网络传输。当过滤设备接收到分组时，把报头中存储的数据属性与访问控制策略对比（称为访问控制表或　　ACL ），根据对比结果的不同，决定该传输是被丢弃还是允许通过。

2）动态包过滤：　通过包的属性和维护一份连接表来监视通信会话的状态而不是简单依靠标志的设置。针对传输层的，所以选择动态包过滤时，要保证防火墙可以维护用户将要使用的所有传输的状态，如　　TCP，UDP，ICMP 等。

45、状态检测防火墙的原理及安全性分析

1）状态检测防火墙的原理：

通信信息：防火墙的检测模块位于操作系统的内核，在网络层之下，能在数据包到达网关操作系统之前对它们进行分析；

通信状态：状态检测防火墙在状态表中保存以前的通信信息，记录从受保护网络发出的数

据包的状态信息；

应用状态：能够理解并学习各种协议和应用，以支持各种最新的应用；能从应用程序中收集状态信息并存入状态表中，以供其他应用或协议做检测策略；

操作信息：状态监测技术采用强大的面向对象的方法；

2）安全性分析：

优点：具备动态包过滤所有优点，同时具有更高的安全性；没有打破客户 /服务器模型；提供集成的动态包过滤功能；运行速度更快。

缺点：采用单线程进程，对防火墙性能产生很大影响；没有打破客户 /服务器结构，会产生不可接受的安全风险；不能满足对高并发连接数量的要求；仅能提供较低水平的安全性。

46、分布式防火墙系统组成： 网络防火墙；主机防火墙；中心管理。

47、防火墙未来的发展方向： 智能化 ；高速度；并行体系结构；多功能；专业化；防病毒。

48、防火墙的部署位置： 部署在内网与接进的外网之间。

49、防火墙的安全域和非安全域。 （详见课件“ 防火墙（一） **.PPT** ”）

另外：防火墙包过滤规则的设置（详见课件“ 防火墙（二） **.PPT** ”补充内容）

第十三章 入侵检测系统

50、入侵检测的概念、 **IDS** 工作原理： IDS 不间断的从计算机网络或计算机系统中的若干关键点上收集信息，进行集中或分布式的分析，判断来自网络和外部的入侵企图，并实时发出报警。

51、 **IDS** 信息收集的来源： 基于主机、基于网络、混合型。

52、信息分析： 模式匹配、统计分析

53、 **IDS** 的异常检测和误用检测： 异常检测：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。

误用检测： 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。

54、入侵检测的 **3** 个基本步骤： 入侵信息的收集、信号分析、入侵检测响应方式

55、 **NIDS** ：检测内容：包头信息和有效数据部分。

56、 **HIDS** ：检测内容：系统调用、端口调用、审计记录、系统日志、应用日志。

蜜罐技术：是一种被侦听、被攻击或已经被入侵的资源。

57、 **IPS** 的特点（详见课课本）

第十四章 虚拟专网

58、虚拟专网定义： 是指物理上分布在不同地点的网络通过公用网络连接成逻辑上的虚拟子网， 并采用认证、 访问控制、 保密性、 数据完整性等在公用网络上构建专用网络的技术，使得数据通过安全的“ 加密通道 ”在公用网络中传输。

59、 **VPN** 的引入的原因及特点： 费用低、安全保障、服务质量保证、可扩充性和灵活性、可管理性

60、**VPN** 的关键技术： 隧道技术、加 /解密技术、密钥管理技术、身份认证技术、访问控制、 Qos 技术

61、**VPN** 的隧道协议种类及各协议的功能、特点：

62、安全协议： 就是构建隧道的“ 隧道协议 ”

63、**IP** 隧道协议： 使用 IP 协议作为封装协议的隧道协议

64、第二层隧道协议： 首先把各种网络协议封装到数据链路层的 PPP 帧中，再把整个 PPP 帧装入隧道中。这种双层缝制方法形成的数据包依靠第二层协议进行传输。

65、第三层隧道协议： 把各种网络协议直接装入隧道协议中， 封装的是网络层协议数据包。

66、**IPSec** 的主要协议： AH 、 ESP 和 IKE 三个协议来实现加密、认证和管理交换功能。

67、**IPsec** 的两种工作模式： 传输模式和隧道模式

68、**VPN** 的身份认证方法： CHAP 、 MS-CHAP 、 MS-CHAP v2 、 EAP

69、**IPSec** 的组成： 管理模块、数据加 /解密模块、密钥分配和生成技术、数据分组封装 / 分解模块、身份认证模块、加密函数模块

70、**SSL/TLS** 协议：TLS 协议主要用于 HTTPS 协议中；TLS 也可以作为构造 VPN 的技术；TLS VPN 的最大优点是用户不需要安装和配置客户端软件；只需要在客户端安装一个 IE 浏览器即可；由于 TLS 协议允许使用数字签名和证书，故它能提供强大的认证功能。

71、**TLS VPN** 实现的 **3** 中协议： TLS 握手协议、 TLS 密钥交换协议和 TLS 报警协议

补充：计算机病毒防范技术

72、蠕虫： 是一种通过网络传播的恶性计算机病毒，是使用危害的代码来攻击网上的受害主机，并在受害主机上自我复制， 再攻击其他的受害主机的计算机病毒。

蠕虫病毒的行为特征：自我繁殖 ；利用软件漏洞； 造成网络拥塞； 消耗系统资源； 留下安全隐患。

73、木马与病毒的区别： 木马不传染 ,病毒传染，木马主要是盗取的密码及其他资料，而病毒是不同程度不同范围的影响电脑的使用 ,木马的作用范围是所有使用这台有木马的人在使用电脑时的资料 ,但是不会传染到其他机器 ,但是病毒可以随着软盘， U 盘 ,邮件等传输方式或者媒介传染到其他机器。

74、计算机病毒特征： 寄生性、传染性、隐蔽性、潜伏性、可触发性、破坏性、

75、计算机病毒的危害性表现： 计算机经常性无缘无故地死机；操作系统无法正常启动；运行速度异常； 内存不足的错误； 打印、 通信及主机接口发生异常； 无意中要求对软盘 （移动存储设备） /U 盘等移动存储设备进行写操作； 以前能正常运行的应用程序经常发生死机或者非法错误；系统文件的时间、日期和大小发生变化；打开 Word 文档后，另存文件时只能以模板方式保存；磁盘空间迅速减少；网络驱动器卷或共享目录无法调用；陌生人发来的电子邮件；自动链接到一些陌生的网站；

76、中病毒和木马的典型表现： （1）自动打开陌生的网站； （2）非正常的对话框窗口的跳出；（3）Windows 系统配置被莫名其妙的更改； （4）硬盘灯非正常闪动、软驱或光驱自动运行、网络连接异常、鼠标异常等。

77、病毒的 **4** 个生命周期： 潜伏阶段；传染阶段；触发阶段；发作阶段。

78、计算机病毒的组成模块： 引导模块、感染模块、表现模块

79、计算机病毒的传播方式： 通过不可移动的计算机硬件设备进行传播；通过移动存储设备进行传播；通过计算机网络进行传播；通过点对点通讯系统和无线通道传播。

防杀病毒软件的功能及特点： (1)工具自身具有自诊断、自保护的能力 ：；(2)具有查毒、杀毒、实时监控多种功能； (3)兼容性好； (4)界面友好，报告内容醒目、明确，操作简单；(5)全面地与 Internet 结合，不仅有传统的手动查杀与文件监控，还必须对网络层、邮件客户端进行实时监控，防止计算机病毒入侵； (6)快速反应的计算机病毒检测网，在计算机病毒爆发的第一时间即能提供解决方案； (7)完善的在线升级服务， 使用户随时拥有最新的防计算机病毒能力； (8)对计算机病毒经常攻击的应用程序提供重点保护 (如 MS Office，Outlook， IE， ICQ/QQ 等）；(9)提供完整、即时的反计算机病毒咨询，提高用户的反计算机病毒意识与警觉性，尽快地让用户了解到新计算机病毒的特点和解决方案。

80、身份认证方式（知道有哪些就可以了） ：口令认证系统；个人生物特征的身份认证技术；一次性口令认证技术；基于证书的认证。