法律法规

点 名称：相关法律法规时间

考 试 频 次：14

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号		68	1、5	1、10、58	1、3、5、58	4、5、7、9

知识点 内容：

《中华人民共和国网络安全法》施行时间是2017年6月1日。

《中华人民共和国密码法》于2019年10月26日通过，自2020年1月1日起施行。

《中华人民共和国数据安全法》于2021年6月10日通过，自2021年9月1日起施行。

《网络安全审查办法》于2020年4月27日正式发布，自2020年6月1日起实施。其依据是《中华人民共和国国家安全法》《中华人民共和国网络安全法》。

根据我国《密码法》规定，密码分为核心密码、普通密码和商用密码。

2021年7月30日，国务院签署国务院令，公布《关键信息基础设施安全保护条例》，规定受到治安管理处罚的人员，**5**年内不得从事网络安全管理和网络运营关健岗位的工作，受到刑事处罚的人员，终身不得从事网络安企管理和网络运营关健岗位的工作。

推荐性国家标准的代号为"GB/T"，强制性国家标准的代号为"GB"。

《中华人民共和国网络安全法》第五十八条明确规定，因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经（国务院）决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

《网络安全法》明确了国家落实网络安全工作的职能部门和职责，其中明确规定由（国家网信部门）负责统筹协调网络安全工作和相关监督管理工作。

信息安全产品通用评测标准ISO/IEC 15408一1999《信息技术、安全技术、信息技术安全性评估准则》(简称CC)，该标准分为三个部分：第1部分“简介和一般模型”、第2部分“安全功能需求”和第3部分“安全保证要求”。其中：**评估保证级**别属于第3部分“安全保证要求”；**基本原理、保护轮廓**属于第1部分“简介和一般模型”；**技术要求**属于第2部分“安全功能需求”。

知识点 名称：法律法规>>《计算机信息系统安全保护等级划分准则》

考 试 频 次：7

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	24	2、46	3		46、48	61

知识点 内容：

《计算机信息系统安全保护等级划分准则》（ CGB17859-1999）规定了计算机系统安全保护能力的五个等级，即：用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级、访问验证保护级。

（1）第一级 用户自主保护级：通过隔离用户与数据，使用户具备自主安全保护的能力。

（2）第二级 系统审计保护级：与用户自主保护级相比，实施了粒度更细的自主访问控制，它通过登录规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责。

（3）第三级 安全标记保护级：具有系统审计保护级所有功能。此外，还提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述；具有准确地标记输出信息的能力；消除通过测试发现的任何错误。

（4）第四级 结构化保护级：建立于一个明确定义的形式化安全策略模型之上，它要求将第三级系统中的自主和强制访问控制**扩展到所有主体与客体**。

（5）第五级 访问验证保护级：满足访问监控器需求。访问监控器仲裁主体对客体的全部访问。访问监控器本身是抗篡改的；必须足够小，能够分析和测试。为了满足访问监控器需求，计算机信息系统可信计算基在构造时，排除那些对实施安全策略来说并非必要的代码；在设计和实现时，从系统工程角度将其复杂性降低到最小程度。支持安全管理员职能；扩充审计机制，当发生与安全相关的事件时发出信号；**提供系统恢复机制**。

第一级为用户自主保护级，该级适用于普通内联网用户;

第二级为系统审计保护级，该级适用于通过内联网或国际网进行商务活动，需要保密的非重要单位;

第三级为安全标记保护级，该级适用于地方各级国家机关、金融机构、邮电通信、能源与水源供给部门、交通运输、大型工商与信息技术企业、重点工程建设等单位;

第四级为结构化保护级，该级适用于中央级国家机关、广播电视部门、重要物资储备单位、社会应急服务部门、尖端科技企业集团、国家重点科研机构和国防建设等部门;

第五级为访问验证保护级，该级适用于国防关键部门和依法需要对计算机信息系统实施特殊隔离的单位。

军用不对外公开的信息系统至少应该属于：三级及三级以上。

计算机系统的安全级别分为四级：D、C（C1、C2）、B（B1、B2、B3）和 A。其中被称为选择保护级的是 C1。

计算机系统安全的主要目标是监督保障系统运行的安全性,保障系统自身的安全性,标识系统中的用户,进行身份认证,依据系统安全策略对用户的操作行为进行监控计算机系统的安全级别就是计算机系统的安全等级,分为四组七个等级:D、C(C1、C2)、B(B1、B2、B3)和 A。

D 级别是最低的安全级别,对系统提供最小的安全防护。

C 级别有 C1 级和 C2 级两个子系统。**C1 级称为选择性保护级**,可以实现自主安全防护,对用户和数据的分离,保护或限制用户权限的传播。C2 级具有访问控制环境的权利,比 C1 的访问控制划分的更为详细,能够实现受控安全保护、个人账户管理、审计和资源隔离。这个级别的系统包括 UNIX、 Linux 和 Windows NT 系统。

C 级别属于自由选择性安全保护,在设计上有自我保护和审计功能,可对主体行为进行审计与约束。

B 级别包括 B1、B2 和 B3 三个级别,B 级别能够提供强制性安全保护和多级安全。强制防护是指定义及保持标记的完整性,信息资源的拥有者不具有更改自身的权限,系统数据完全处于访问控制管理的监督下

B1 级称为标识安全保护。B2 级称为结构保护级别,要求访问控制的所有对象都有安全标签以实现低级别的用户不能访问敏感信息,对于设备、端口等也应标注安全级别。B3 级别称为安全域保护级别,这个级别使用安装硬件的方式来加强域的安全,比如用内存管理硬件来防止无授权访问。

A 级别称为验证设计级(Verity Design),是目前最高的安全级别。在 A 级别中,安全的设计必须给出形式化设计说明和验证,需要有严格的数学推导过程,同时应该包含秘密信道和可信分布的分析。

电子商务

知识点 名称：电子商务、安全电子交易协议 SET

考 试 频 次：4

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	10、59		59	59		

知识点 内容：

电子商务的安全需求：可认证性、保密性、完整性、不可抵赖性。

SET 协议确保了网上交易所要求的保密性、数据的完整性、交易的不可否认性和交 易的身份认证。

SET 协议主要使用的技术包括:对称密钥加密、公钥如密、 Hash 算法、 数字签名、数字信封以及数字证书等技术。

SET 通过使用公钥和对称密铠方式加密，以保证数据的保密性：通过使用数字签名、Hash 算法和数字证书实现交易各方的身份认证、 数据的完整性和交易的不可否认性。

网络安全

知识点 名称：网络安全>>网络安全目标

考 试 频 次：2

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号						3、63

知识点 内容：

要实现网络信息安全基本目标，网络应具备防御、监测、应急和恢复等基本功能。

网络信息安全风险是指特定的威胁利用网络管理对象所存在的脆弱性，导致网络管理对

象的价值受到损害或丢失的可能性。简单地说，网络风险就是网络威胁发生的概率和所造成影响的乘积。网络安全管理实际上是对网络系统中网管对象的风险进行控制，其方法如下：

- 避免风险。例如，通过物理隔离设备将内部网和外部网分开，避免受到外部网的攻击。
- 转移风险。例如，购买商业保险计划或安全外包。
- 减少威胁。例如，安装防病毒软件包，防止病毒攻击。
- 消除脆弱点。例如，给操作系统打补丁或强化工作人员的安全意识。
- 减少威胁的影响。例如，采取多条通信线路进行备份或制定应急预案。
- 风险监测。例如，定期对网络系统中的安全状况进行风险分析，监测潜在的威胁行为。

知识点 名称：网络安全>>网络安全等级保护

考 试 频 次：5

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号				5	43、67	6、26

知识点 内容：

根据网络安全等级保护 2.0 的要求，对云计算实施安全分级保护。围绕“一个中心，三重防护”的原则，构建云计算安全等级保护框架。其中一个中心是指安全管理中心，三重防护包括：计算环境安全、区域边界安全和通信网络安全。

“安全管理中心”主要包括系统管理、审计管理、安全管理和集中管控四个控制点。

等级保护 2.0 中的第四级，要求所有计算节点都应基于可信根实现开机到操作系统启动，再到应用程序启动的可信验证，并在应用程序的所有执行环节对其执行环境进行可信验证，主动抵御病毒入侵行为，同时验证结果，进行动态关联感知，形成实时的态势。

网络安全模型

知识点 名称：网络安全模型

考 试 频 次：1

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号				15		

知识点 内容：

安全模型也被称为策略表达模型，是一种对安全需求与安全策略的抽象概念模型。

安全策略表达模型一般分为两大类，即自主访问控制 CDAC) 和强制访问控制 CMAC) 。

自主访问控制模型的典型代表有 HRU 模型（Harrison Ruzzo 、Ullman 访问控制矩阵模型）、 Jones 取予模塑（Take-Grant 模型）、动作一一-实体模型等。

强制访问控制的典型代表有 BLP 模型（Bell-La Padula 模型）、基于角色的存取控制模型、Clark-Wilson 模型、 BN 模型（Brewer Nash Chinese Wall 模型）等。。

知识点 名称：网络安全模型>>BLP 机密性模型

考 试 频 次：2

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号			58		36	

知识点 内容：

BLP 模型有两个安全特性：简单安全特性、*特性。

简单安全特性：只能向下读，不能向上读。

*特性：只能向上写、不能向下写。

BLP 是安全访问控制的一种模型，是基于自主访问控制和强制访问控制两种方式实现的。它是一种严格的形式化描述，控制信息只能由低向高流动。它反映了多级安全策略的安全特性。

知识点 名称：网络安全模型>>Biba 模型

考 试 频 次：1

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号						23

知识点 内容：

BiBa 具有 3 个安全特性：简单安全特性、＊特性、调用特性。

*特性：主体的完整性级别小于客体的完整性级别，不能修改客体，即主体不能向上写。

知识点 名称：网络安全模型>> 动态安全模型 P2DR

考 试 频 次：2

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号				36		24

知识点 内容：

入侵检测的基本模型是 PDR 模型，其思想是防护时间大于检测时间和响应时间。 针对静态的系统安全模型提出了"动态安全模型 CP2DR)"。

P2DR 模型包含 4 个主要部分：Policy （安全策略）、 Protection（防护）、 Detection（检测）和 Response（响应）。

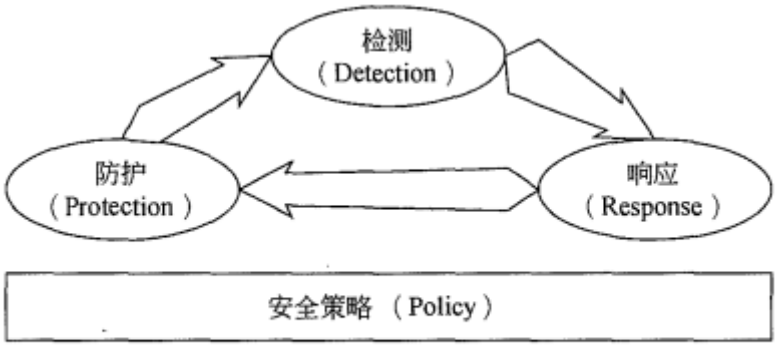


图 3-57 P2DR 模型

Protection（防护）：主要内容有加密机制,数字签名机制,访问控制机制,认证机制,信息隐藏,防火墙技术等.

Detection（检测）：主要内容有入侵检测,系统脆弱性检测,数据完整性检测,攻击性检测等.

Recovery（恢复）：主要内容有数据备份,数据恢复,系统恢复等.

Reaction（响应）：主要内容有应急策略,应急机制,应急手段,入侵过程分析,安全状态评估等.

知识点 名称：网络安全模型>>能力成熟度模型 CMM

考 试 频 次：1

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号						25

知识点 内容：

能力成熟度模型（简称 CMM) 是对一个组织机构的能力进行成熟度评估的模型。成熟度级别一般分成五级： 1 级－非正式执行、 2 级－计划跟踪、 3 级－充分定义、 4 级－量化控制、 5 级－ 持续优化。其中，级别越大，表示能力成熟度越高，各级别定义如下：

- 1 级－非正式执行：具备随机、无序、被动的过程；
- 2 级－计划跟踪：具备主动、非体系化的过程；
- 3 级－充分定义：具备正式的、规范的过程；
- 4 级－晕化控制：具备可量化的过程；
- 5 级持续优化：具备可待续优化的过程。

软件安全能力成熟度模型分成五级，各级别的主要过程如下：

- CMM1 级—补丁修补；
- CMM2 级——渗透测试、安全代码评审；
- CMM3 漏洞评估、代码分析、安全编码标准；
- CMM4 软件安全风险识别、 SDLC 实施不同安全检查点；
- CMM5 改进软件安全风险覆盖率 评估安全差

网络安全原则

知识点 名称：网络安全原则

考 试 频 次：5

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	12	12	9、12	4		

知识点 内容：

木桶原则：对信息进行均衡、全面的防护，提高整个系统“安全最低点”的安全性能。

整体原则：在网络被攻击、破坏事件的情况下，必须尽可能快地恢复网络的服务，减少损失。

分权制衡原则：为了达到信息安全的目标，各种信息安全技术的使用必须遵守一些基本原则，其中在信息系统中，应该对所有权限进行适当地划分，使每个授权主体只能拥有其中的一部分权限，使它们之间相互制约、相互监督，共同保证信息系统安全。

纵深防御原则：要求网络安全防护系统是一个多层安全系统，避免成为网络中的“单失效点”，要部署有多重防御系统。

网络安全威胁

知识点名称：网络安全威胁

考试频次：3

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	23、38		38			

知识点内容：

目前网络存在的威胁包括两类：渗入威胁和植入威胁。其中主要的渗入威胁有：假冒、旁路控制、授权侵犯。主要的植入威胁有：特洛伊木马、陷门。

知识点名称：网络安全威胁>>网络监听

考试频次：1

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号					10	

知识点内容：

一台连接在以太网内的计算机为了能跟其他主机进行通信，需要有网卡支持。网卡有几种接收数据帧的状态，如 unicast，broadcast，multicast，promiscuous 等，

unicast 指网卡在工作时接收目的地址是本机硬件地址的数据帧。

Broadcast 是指接收所有类型为广播报文的数据帧。

Mu1ticast 是指接收特定的组播报文。

Promiscuous 即混杂模式，是指对报文中的吕的硬件地址不加任何检查，全部接收的工作模式。

知识点名称：网络安全威胁>>网络安全漏洞

考试频次：1

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号						48

知识点内容：

网络信息系统的漏洞主要来自两个方面： 一方面是非技术性安全漏洞，涉及管理组织结构、 管理制度、管理流程、人员管理等；另一方面是技术性安全漏洞，主要涉及网络结构、通信协议、设备、软件产品、系统配置、应用系统等。

网络安全取证

知识点 名称：网络安全取证、计算机取证

考 试 频 次：6

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	18	8	18	22	22	58

知识点 内容：

计算机取证包括对以磁介质编码信息方式存储的计算机证据的保护、确认、提取和归档。

计算机取证主要是围绕电子证据进行的，具有高科技性、无形性和易破坏性等。

计算机取证的通常步骤包括：保护目标计算机系统、确定电子证据、收集电子证据、保全电子证据。

计算机取证分析工作中常用到包括密码破译、文件特征分析技术、数据恢复与残留数据分析、日志记录文件分析、相关性分析等技术，其中文件特征包括文件系统特征、文件操作特征、文件格式特征、代码或数据特征等。某单位网站被黑客非法入侵并上传了 Webshell，作为安全运维人员应首先从（Web 服务日志）入手。

网络安全取证步骤如下：①取证现场保护；②证据识别；③传输证据；④保存证据；⑤分析证据；⑥提交证据。

网络安全风险评估

知识点 名称：网络安全风险评估

考 试 频 次：3

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号		43	43	43		

知识点 内容：

风险评估是组织确定信息安全需求的过程,包括风险评估准备、风险因素识别、风险程度分析和风险等级评价。

风险评估实施划分为评估准备、风险要素识别、风险分析与风险处置四个阶段。

信息安全风险评估中需要识别的对象包括资产识别、威胁识别、脆弱性识别。

网络安全主动防御技术

知识点 名称：网络安全主动防御技术>>蜜罐技术

考 试 频 次：6

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	9	63	13	25	25	42

知识点 内容：

蜜罐 (Honeypot) 技术是)种主动助御技术，是入侵检测技术的一个重要发展方向。

蜜罐系统是一个包含漏洞的诱骗系统，它通过模拟一个或者多个易受攻击的主机和服务，给攻击者提供一个容易攻击的目标。

使用蜜罐技术，可以使目标系统得以保护，便于研究入侵者的攻击行为。

蜜罐有四种不同的配置方式：诱骗服务(DeceptionService) 、弱化系统(WeakenedSystem)、强化系统(HardenedSystem)、用户模式服务器(UserModeServer)。

诱骗服务是指在特定服务端口上进行侦昕，并像其他应用程序那样对各种网络请求进行应答的应用程序。

弱化系统是一个配置有己知攻击弱点的操作系统，比如，系统安装有己知的易受远程攻击的 RPC、Sadmind 和 mountd 等。

强化系统是对弱化系统配置的改进。

用户模式服务器是一个用户进程，它运行在主机上，并模拟成一个功能健全的操作系统，类似用户通常使用的操作系统。

蜜罐为了实现一台计算机绑定多个 IP 地址，可以使用（ARP）协议来实现。

知识点 名称：网络安全主动防御技术>>入侵防御技术

考 试 频 次：1

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号						52

知识点 内容：

入侵防御系统，简称 IPS (Intrusion Prevention System) ，工作基本原理是根据网络包的特性及上下文进行攻击行为判断来控制包转发，其工作机制类似于路由器或防火墙，但是 IPS 能够进行攻击行为检测，并能阻断入侵行为。

IPS/SPS 的主要安全功能如下：

- 屏蔽指定 IP 地址；
- 屏蔽指定网络端口；
- 屏蔽指定域名；
- 封锁指定 URL 、阻断特定攻击类型；
- 为零日漏洞 (Zero-day Vulnerab ties) 提供热补丁。

信息系统安全评测方法

知识点名称：信息系统安全评测方法>>渗透测试

考试频次：2

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号		10				60

知识点内容：

安全渗透测试通过模拟攻击者对测评对象进行安全攻击，以验证安全防护机制的有效性。根据对测评对象掌握的信息状况，安全渗透测试可以分为三种类型。

黑盒模型：只需要提供测试目标地址，授权测试团队从指定的测试点进行测试。

白盒模型：需要提供**尽可能详细**的测试对象信息，测试团队根据所获取的信息，制订特殊的渗透方案， 对系统进行高级别的安全测试。该方式适合高级持续威胁者模拟。

灰盒模型：需要提供**部分**测试对象信息，测试团队根据所获取的信息，模拟不同级别的威胁者进行渗透。该方式适合手机银行和代码安全测试。

安全渗透测试常用的工具有 Metasplo 止字典生成器、 GDB Backtrack4 Burpsu OllyDbg IDA Pro 等。

模糊测试（Fuzzing) 是一种黑盒测试技术，它将大量的畸形数据输入到目标程序中， 通过监测程序的异常来发现被蹦程序中可能存在的安全漏洞。

模糊测试是一种基于缺陷注入的自动化测试技术。

模糊测试是一种自动化的动态漏洞挖据技术，不存在误报，也不需要人工进行大量的逆向分析工作。

知识点名称：信息系统安全评测方法>>代码审计

考试频次：1

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号		64				

知识点内容：

代码静态分析采用的方法主要有：模式匹配、定理证明、模型检测等。

密码学

知识点 名称：密码学

考 试 频 次：3

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	32	53	68			

知识点 内容：

密码分析学是研究密码破译的科学，在密码分析过程中，破译密文的关键是：截获密文，获得密钥并了解解密算法。

密码分析的目的是：发现密钥或者密文对应的明文。

密码分析者针对加解密算法的数学基础和某些密码学特性，根据数学方法破译密码的攻击方式称为：数学分析攻击。

如果破解密码算法所需的代价或者时间超过一定限度,表示密码实际是安全的。

衡量密码体制安全性的基本准则有以下几种：

（1） 计算安全的：如果破译加密算法所需要的计算能力和计算时间是现实条件所不具备的，那么就认为相应的密码体制是满足计算安全性的。这意味着强力破解证明是安全的，即实际安全。

（2） 可证明安全的：如果对一个密码体制的破译依赖于对某一个经过深入研究的数学难题的解决，就认为相应的密码体制是满足可证明安全性的。这意味着理论保证是安全的。

（3） 无条件安全的：如果假设攻击者在用于无限计算能力和计算时间的前提下，也无法破译加密算法，就认为相应的密码体制是无条件安全性的。这意味着在极限状态上是安全的。

知识点 名称：密码学>>密码学安全目标

考 试 频 次：9

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	14	6	14、23	14	14、52、66	1

知识点 内容：

密码学作为信息安全的关键技术，其安全目标主要包括三个非常重要的方面:保密性（confidentiality）、完整性（integrity） 和可用性（availability）。

保密性是确保信息仅被合法用户访问，而不被泄露给非授权的用户、实体或过程， 或供其利用的特性。

完整性是指所有资源只能由授权方或以授权的方式进行修改,即信息未经授权不能进行改变的特性。

可用性是指所有资源在适当的时候可以由授权方访问,即信息可被授权实体访问并按需求使用的特性。

知识点 名称：密码学>>密码体制分类

考 试 频 次：25

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	4、6、15、29、33、35、50、65、70	4、56	15、35、50、66、70	35、48、68	18、35、68	15、18、20

知识点 内容：

根据密钥的特点，密码体制分为：私钥和公钥密码体制两种。而介入私钥和公钥之间的密码体制称为混合密码体制。

私钥密码体制又称为对称密码体制，加密和解密使用相同的密钥，典型算法有：DES、IDEA、AES 等。

AES 的密钥长度可以为 16、24 或者 32 字节,也就是 128、192、256 位。

AES 结构由 4 个不同的模块组成：字节代换、行移位、列混淆、轮密钥加，其中（字节代换 S 盒）是非线性模块。

DES 的分组长度为 64 位，秘钥长度为 56 位，子秘钥长度是 48 位。

DES 算法中，64 位密钥经过置换选择 1、循环左移、置换选择 2 等变换，产生 16 个 48 位长的子密钥

3DES 是 DES 加密算法的 1 种模式，它使用 3 条 64 位的钥对数据进行三次加密，本质上就相当于用个长为 168 位的密钥进行加密。若数据对安全性要求不那么高，K1 可以等于 K3，在这种情况下，密钥的有效长度为 112 位。

公钥密码体制又称为非对称密码体制，其基本原理是在加密和解密的过程中使用不同的密钥处理方式，其中，加密密钥可以公开，而只需要把解密密钥安全存放即可。在安全性方面，密码算法即使公开，由加密密钥推知解密密钥也是计算不可行的。不适合大数据、明文加密。

根据明密文的划分和密钥的使用不同，密码系统可以分为：分组密码系统和序列密码系统。

基于公开密钥的数字签名算法对消息进行签名和验证时，正确的签名和验证方式是：发送方用自己的私有密钥签名，接收方用发送方的公开密钥验证。

利用公开密钥算法进行数据加密时,采用的方式是：发送方用公开密钥加密,接收方用私有密钥解密。

如果对一个密码体制的破译依赖于对某一个经过深入研究的数学难题的解决，就认为相应的密码体制是（ 可证明安全）的。

雪崩效应(avalanche effect)，指加密算法(尤其是块密码和加密散列函数)的一种理想属性。雪崩效应是指当输入发生最微小的改变(例如，反转一个二进制位)时，也会导致输出的剧变(如，输出中一半的二进制位发生反转)。在高品质的块密码中，无论密钥或明文的任何细微变化都应当引起密文的剧烈改变。

Hash 算法是指产生哈希值或杂凑值的计算方法。MD5 算法是由 Rivest 设计的 Hash 算法，该算法以 512 比特数据块为单位处理输入，产生（128）的哈希值。

Diffie-Hellman 密钥交换体制要解决的是完成通信双方的对称秘钥交换，利用的原理是基于**离散对数问题**之上的公开秘钥密码体制。

知识点 名称：密码学>>分组密码工作模式

考 试 频 次：2

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号			53	65		

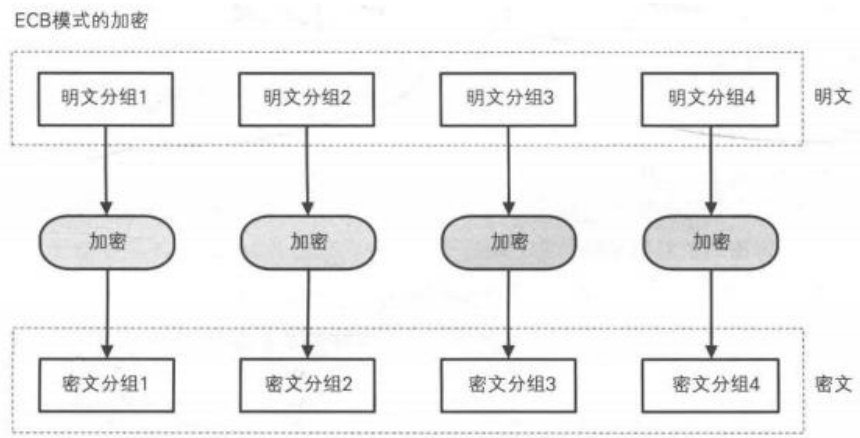
知识点 内容：

几种有代表性的近代分组密码：DES、AES 算法。

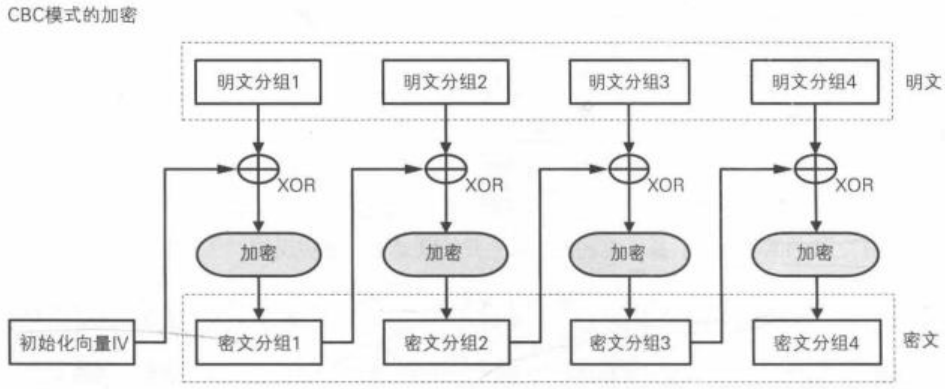
分组密码常用的工作模式包括:电码本模式（(Electric Code Book，ECB 模式）、密码反馈模式（CFB 模式）,密码分组链接模式（CBC 模式）,输出反馈模式（OFB 模式）。

电码本方式是分组密码的基本工作模式。

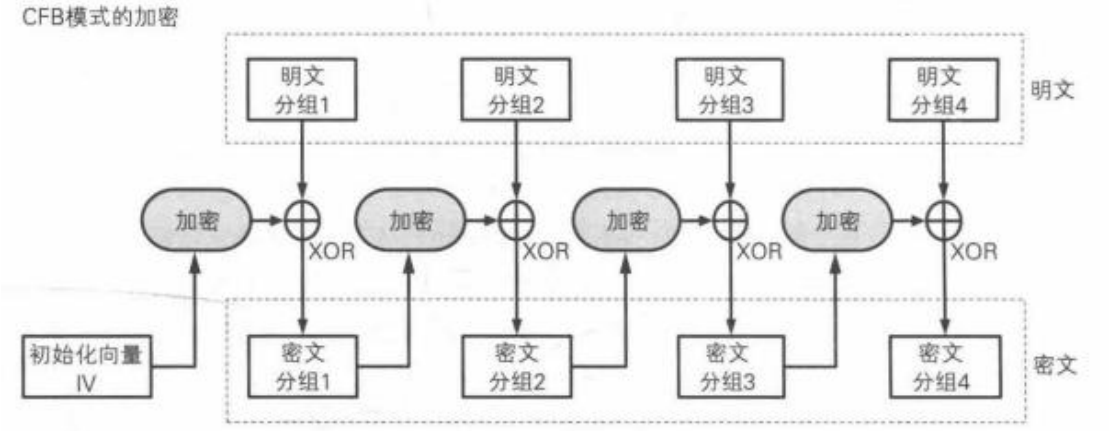
ECB（电子密码本）模式是一种最直接，最简单的消息加密方式。在 ECB 模式中，明文加密之后将直接得到密文，同样的密文解密之后，也直接得到明文。



CBC 模式的全称是 Cipher Block Chaining 模式（分组密码链接模式），在 CBC 模式中，首先将明文分组与上一个分组的密文进行“异或”运算，然后再进行加密操作。

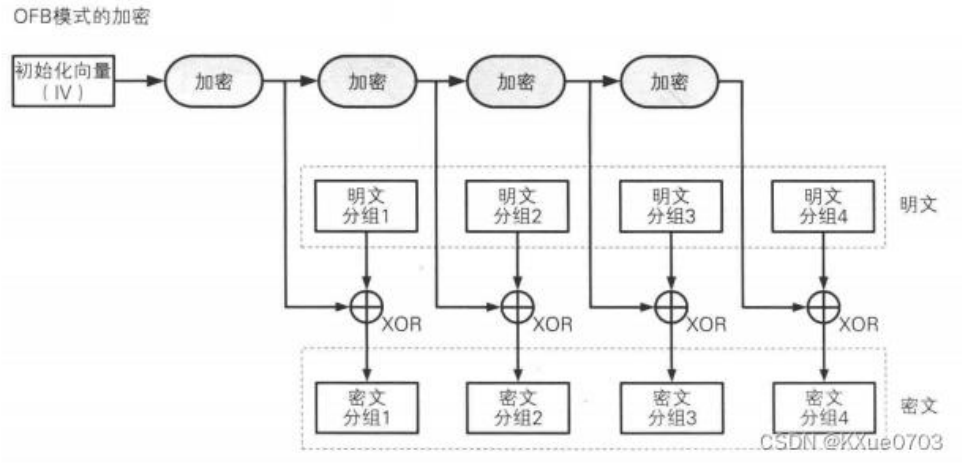


CFB 模式的全称是 Cipher FeedBack(密文反馈模式)。在 CFB 模式中，前一个密文分组会被送回到密码算法的输入端。所谓的反馈就是返回到输入端的意思。与 ECB、CBC 模式不同的是 CFB 加密的并不是明文，而是加密“上一分组的密文”，加密完“上一分组密文”之后在与当前分组的明文进行“异或”得到当前分组的密文。



OFB 模式的全称是 Output-FeedBack 模式（输出反馈模式）。在 OFB 模式中密码算法的输出会反馈到密码算法的输入中。OFB 模式并不是通过密码算法对明文直接进行加密

的，而是将“明文分组”与“密码算法的输出”进行 XOR 运算产生“密文分组”的。在这一点上，OFB 模式与 CFB 模式是非常相似的。



知识点 名称：密码学>>四种攻击密码类型

考 试 频 次：3

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号		1		6	6	

知识点 内容：

根据密码分析者可利用的数据资源来分类，可将攻击密码的类型分为以下四种：

（1） **仅知密文攻击** (Ciphertext-onlya attack) 。所谓仅知密文攻击是指密码分析者仅根据截获的密文来破译密码。因为密码分析者所能利用的数据资源仅为密文，因此这是对密码分析者最不利的情况。

（2） **已知明文攻击**(Known-plaintext attack) 。所谓已知明文攻击是指密码分析者根据已经知道的某些明文-密文对来破译密码。

（3） **选择明文攻击**(Chosen-plaintext attack) 。所谓选择明文攻击是指密码分析者能够选择明文并获得相应的密文。例如， Windows 环境下的数据库 SuperBase 的密码就被作者用选择明文方法破译。如果分析者能够选择明文并获得密文，那么他将会特意选择那些最有可能恢复出密钥的明文。

（4） **选择密文攻击** (Chosen ciphertext attack) 。所谓选择密文攻击是指密码分析者能够选择密文并获得相应的明文。这也是对密码分析者十分有利的情况。这种攻击主要

攻击公开密钥密码体制，特别是攻击其数字签名。

知识点 名称：密码学>>DES 算法>>S 盒

考 试 频 次：5

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	26		26	26	26	16

知识点 内容：

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_1

以 S_1 为例，设输入为 101011，第 1 位和第 6 位数字组成的二进制数为 $11=(3)_{10}$，表示选中 S_1 的行号为 3 的那一行，其余 4 位数字所组成的二进制数为 $0101=(5)_{10}$，表示选中 S_1 的列号为 5 的那一列。交点处的数字是 9，则 S_1 的输出为 1001。

知识点 名称：密码学>>商用密码算法

考 试 频 次：13

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	2、67	35、65	2、32、67	2、32	2、32、70	17

知识点 内容：

算法名称	算法特性描述
SM1	对称加密，分组长度和秘钥长度都是 128 位
SM2	非对称加密
SM3	摘要/杂凑算法， SM3 的杂凑长度为 32 字节（256 位）， SM3 的分组长度位 512 位，
SM4	对称加密，分组长度和秘钥长度都是 128 位

	我国无线局域网密码算法
SM7	对称加密，应用于非接触式 IC 卡
SM9	标识密码算法（IBE），应用于端对端离线安全通讯

国家密码管理局于 2006 年 1 月 6 日发布公告，公布了《无线局域网产品须使用的系列密码算法》，包括：对称密码算法：SMS4；签名算法：ECDSA；密钥协商算法：ECDH；杂凑算法：SHA-56；随机数生成算法：自行选择。其中，ECDSA 和 ECDH 密码算法须采用国家密码管理局指定的椭圆曲线和参数。

随着密码技术和计算机技术的发展，目前常用的 1024 位 RSA 算法面临严重的安全威胁，我们国家密码管理部门经过研究，决定采用 SM2 椭圆曲线算法替换 RSA 算法。

2017 年 11 月,在德国柏林召开的第 55 次 ISO/IEC 信息安全分技术委员会(SC27)会议上,我国专家组提出的（ SM9 与 SM2 ）算法一致通过成为国际标准

知识点 名称：密码学>>RSA 公钥密码算法

考 试 频 次：6

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	66、69	66	62、65、69			

知识点 内容：

余数运算：a mod b = c 表示整数 a 除以整数 b 所得余数为 c。

同余运算：两个整数 a，b，若它们除以整数 m 所得的余数相等，则称 a，b 对于模 m 同余，记作 a = b (mod m) 读作 a 同余于 b 模 m，或读作 a 与 b 关于模 m 同余。比如 26 ≡ 14 (mod 12)。

2.5.2.1 基本的 RSA 密码体制：参数、加密算法、解密算法

① 随机地选择两个大素数 p 和 q，而且保密；
② 计算 $n=pq$，将 n 公开；
③ 计算 $\varphi(n)=(p-1)(q-1)$，对 $\varphi(n)$保密；
④ 随机地选取一个正整数 e，$1<e<\varphi(n)$且（e，$\varphi(n)$）=1，将 e 公开；
⑤ 根据 $ed=1 \mod \varphi(n)$，求出 d，并对 d 保密；

例：设在 RSA 的公钥密码体制中，公钥为（c，n）=（13，35），则私钥为?

解：取 p=5,q=7, ψ (n)=4*6=24。13*d=1mod24,求得 d=13。

例：67mod119 的逆元是（）乘法逆元

解：67*x mod 119=1,得 x=16。

知识点 名称：密码学>>凯撒密码（移位密码）

考 试 频 次：3

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号		5		69	69	

知识点 内容：

移位密码中，当取密钥 key=3 时,得到的移位密码称为凯撒密码。按 key 值在 26 个英文字母中移位。

知识点 名称：密码学>>祖冲之算法

考 试 频 次：1

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号			54			

知识点 内容：

ZUC 算法，即祖冲之算法，是移动通信 3GPP 机密性算法 EEA3 和完整性算法 EIA3 的核心，是中国自主设计的加密算法。

ZUC 算法的 LFSR 设计首次采用素域 GF($2^{31}-1$) 的 m 序列。该类序列周期长、统计特性好，且在特征为 2 的有限域上是非线性的，其具有线性结构弱、比特关系符合率低等优点。

ZUC 算法具有天然的强抵抗二元域上密码攻击方法的能力，譬如二元域上的代数攻击、区分分析和相关攻击等。

知识点 名称：密码学>>数字签名

考 试 频 次：15

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	11、16、40	16、49、54、67	11、16	11、34、70	11、34	19

知识点 内容：

数字签名技术是将摘要用发送者的私钥加密，与原文一起传送给接收者。接收者只有用发送者的公钥才能解密得到被加密的摘要。

数字签名技术可以保证接收者不能伪造对报文的签名、接收者能够核实发送者对报文的签名、发送者事后不能抵赖对报文的签名。同时，接收者可以用 Hash 函数对收到的原文再产生一个摘要，与收到的摘要对比，如果二者相同，则说明收到的信息是完整的，从而保证信息传输的完整性。

但是，数字签名技术不是加密技术，它**不能防止数据在传输过程中被窃取**。

一个完整的数字签名方案由三部分组成：密钥生成算法、签名算法和验证算法。

数字签名可以利用公钥密码体制、对称密码体制或公证系统来实现。最常见的实现方法是建立在公钥密码体制和单向安全散列函数算法的组合基础之上。

数字签名具有与手写签名一样的特点，是可信的、不可伪造的、不可重用的、不可抵赖的以及不可修改的。

基于公开密钥的数字签名算法对消息进行签名和验证时，正确的签名和验证方式是：发送方用自己的私有密钥签名，接收方用发送方的公开密钥验证。

利用公开密钥算法进行数据加密时,采用的方式是：发送方用公开密钥加密,接收方用私有密钥解密。

DSS 数字签名标准的核心是数字签名算法 DSA，该签名算法中杂凑函数采用的是 SHA1

一个数字签名体制通常包括两个部分：施加签名和验证签名。

数字签名**不是**十六进制的字符串。

知识点 名称：密码学>>数字水印

考 试 频 次：7

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	20	9	20、33	20	20、53	

知识点 内容：

数字水印技术通过在数字作品中加入一个不可察觉的标识信息(版权标识或序列号等),需要时可以通过算法提出标识信息来进行验证,作为指证非法复制的证据,从而实现对数字产品的版权保护。其安全需求包括:安全性、隐蔽性、鲁棒性,但并**不要求具有可见性**。

数字水印的主要应用领域包括：原始数据的真伪鉴别、证据篡改鉴定、数据侦测和跟踪、数字产品版权保护等。

在数字水印技术中,水印的数据量和鲁棒性构成了一对基本矛盾；视频水印算法必须满足实时性的要求；隐形数字水印主要应用领域有原始数据的真伪鉴别、数据侦测与跟踪、数字产品版权保护。根据输入输出的种类及其组合可分为三种：**①秘密水印(非盲化水印)**，该类系统至少需要原始的数据；②半秘密水印(半盲化水印)；**③公开水印(盲化或健忘水印)**。盲水印的检测不需要任何原始数据和辅助信息。

数字水印的解释攻击是以阻止版权所有者对所有权的断言为攻击目的。解决方案主要有三种：

第一种方法是引入时戳机制，从而确定两个水印被嵌入的先后顺序；

第二种方法是作者在注册水印序列的同时对原始作品加以注册，以便于增加对原始图像的检测；

第三种方法是利用单向水印方案消除水印嵌入过程中的可逆性。其中前两种都是对水印的使用环境加以限制；

最后一种则是对解释攻击的条件加以破坏。

典型水印攻击方式可以分为鲁棒性攻击、表达攻击、解释攻击和法律攻击。

鲁棒性攻击以减少或消除数字水印的存在为目的，包括像素值失真攻击、敏感性分析攻击和梯度下降攻击等。

表达攻击是让图像水印变形而使水印存在性检测失败，包括置乱攻击、同步攻击等。

解释攻击包括拷贝攻击、可逆攻击等，它使数字水印的版权保护受到了挑战。

知识点 名称：密码学>>数字证书

考 试 频 次：4

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021

题目序号	31	61	31	33		

知识点 内容：

X.509 数字证书内容包括：版本号、序列号、签名算法标识、发行者名称、有效期、主体名称、主体公钥信息、发行者唯一标识符、主体唯一识别符、扩展项等，**不包括加密算法标识**。

知识点 名称：密码学>>数字信封技术

考 试 频 次：2

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	34		34			

知识点 内容：

数字信封是一种综合利用了对称加密技术和非对称加密技术两者优点进行信息**安全传输**的一种技术。

恶意代码

知识点 名称：恶意代码>>恶意代码前缀

考 试 频 次：4

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号		28		24	24、62	

知识点 内容：

恶意代码：Malicious Code。恶意代码前缀是指一个恶意代码的种类，具体有：

恶意代码	**前缀**	**恶意代码**	**前缀**
系统病毒	Win32、PE、Win95、W32、W95 等	木马病毒	Trojan
网络蠕虫	Worm	脚本病毒	Script
宏病毒	Macro	后门程序	Backdoor
玩笑病毒	Joke	病毒种植程序病毒	Dropper
捆绑机病毒	Binder	破坏性程序病毒	Harm

知识点 名称：恶意代码>>计算机病毒

考 试 频 次：4

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	49	41	41			50

知识点 内容：

一个计算机病毒程序的整个生命周期一般由如下 4 个阶段组成：潜伏阶段、传播阶段、传播阶段、发作阶段。

常见的计算机病毒类型包括引导型病毒、病毒、多态病毒、隐蔽病毒等。

引导区病毒是通过感染磁盘引导扇区进行传播的病毒。常见的引导区病毒有**磁盘杀手**、AntiExe 病毒等。

病毒的引导过程包括：驻留内存、窃取系统控制权（使有关部分取代或扩充系统的原有功能，并窃取系统的控制权）、恢复系统功能。

知识点 名称：恶意代码>>网络蠕虫

考 试 频 次：3

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号				62	41	51

知识点 内容：

勒索软件属于蠕虫。

震荡波蠕虫的家族名是 "Sasser"，冲击波蠕虫的家族名是 "MSBlaster"

网络蠕虫又可分为：漏溺利用类蠕虫、口令破解类蠕虫、电子邮件类蠕虫、即时通信工具类蠕虫、 IRC 类蠕虫、 P2P 类蠕虫，以及本地蠕虫(如利用本地复制及可移动存储设备进行传播)等。

网络蠕虫由四个功能模块构成：探测（probe）、传播（transport）、蠕虫引擎（worm engine）、负载（payload）。

①探测模块——探测目标主机的脆弱性，确定攻击、渗透方式；

②传播模块——复制并传播蠕虫；

③蠕虫引擎模块——扫描并收集目标网络信息，如 IP 地址、拓扑结构、操作系统版本等；

④负载模块——实现蠕虫内部功能的伪代码。

知识点 名称：恶意代码>>特洛伊木马

考 试 频 次：3

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号			10	41	38	

知识点 内容：

特洛伊木马，简称木马，英文名为 Trojan horse。

按照木马的行为和功能特征，特洛伊木马又可以分为多种，如远程控制型木马、信 息窃取型木马、破坏型木马等。

远程控制型木马一般都有客户端和服务端两个执行程序，其中客户端程序用于攻击 者远程控制己植入木马的计算机，或者获取来自被植入木马主机的数据，服务端程序就 是在用户计算机中的木马程序。

典型的远程控制型木马有冰河、网络神偷、广外女生、网络公牛、黑洞、上兴、彩虹桥、Posion-îvy、PCShare、灰鸽子等。

目前安卓平台恶意软件主要有（远程控制木马、话费吸取类、隐私窃取类和系统破坏类）四种类型。

知识点 名称：恶意代码>>电子邮件

考 试 频 次：1

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	25					

知识点 内容：

电子邮件是传播恶意代码的重要途径，为了防止电子邮件中的恶意代码的攻击，用（纯文本）方式阅读电子邮件。

网络协议

知识点名称：网络协议>>网络层协议 IPv4

考试频次：

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	27、42		42	12		

知识点内容：

IP 地址分为全球地址和专用地址。专用地址是:

A 类：10.0.0.0~10.255.255.255(或记为 10/8);

B 类：172.16.0.0~172.31.255.255(或记为 172.16/12)

C 类：192.168.0.0~192.168.255.255(或记为 192.168/16)

在 IPv4 的数据报格式中，字段（标识）最适合于携带隐藏信息

知识点名称：网络协议>>Internet 路由协议

考试频次：2

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号				27	12	

知识点内容：

由于 Intemet 规模太大，所以常把它划分成许多较小的自治系统(Autonomous System, AS) 。通常把自治系统内部的路由协议称为内部网关协议，自治系统之间的协议称为外部网关她议。常见的内部网关协议有 RIP 协议和 OSPF 协议;外部网关协议有 BGP 协议。

路由信息协议 RIP (Routing Information Protocol) 是一种分布式的基于距离向量的路由选择协议，它位于应用层。

开放最短路径优先协议 OSPF (Open Shortest Path First) 是分布式的链路状态路由协议。

外部网关协议 BGP (Border Gateway Protocol) 是不同自治系统的路由器之间交换路由信息的协议。BGP-4 共使用四种报文:

（1）**打开(Open)报文：**用来与相邻的另一个 BGP 发言人建立关系。

（2）**更新(Update)报文：**用来发送某一路由的信息，以及列出要撤销的多条路由。

（3）**保活(Keepalive)报文：**用来确认打开报文和周期性地证实邻站关系。

（4）**通知(Notification)报文：**用来发送检测到的差错。

知识点名称：网络协议>>电子邮件协议

考试频次：2

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号				28	28	

知识点内容：

邮件协议有发送协议 SMTP (Simple Mail Transfer Protocol) 、接收协议 POP3/IMAP4 (Post Office Protocol - Version 3/ Intemet Message Access Protocol 4。

SMTP 命令集：

HELO 发送身份标识
MAIL 识别邮件发起方
RCPT 识别邮件接收方
DATA 传送报文文本
RSET 放弃当前邮件事物
NOOP 无操作
QUIT 关闭 TCP 连接
SEND 向终端发送邮件
SOML 若可能向终端发送邮件，否则发往信箱
SAML 向终端和信箱发送邮件
VRFY 证实用户名
EXPN 返回邮件发送清单的成员
HELP 发送帮助文档
TURN 颠倒发送方和接收方的角色

客户端用“DATA”命令对报文的传送进行初始化，若服务器回应“354"，表示可以进行邮件输入。

知识点名称：网络协议>>文件传输协议 FTP（File Transfer Protocol）

考试频次：2

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号					40	47

知识点内容：

FTP 的工作过程：FTP 是一个交互会话的系统，在进行文件传输时， FTP 的客户和服务器之间需要建立两个 TCP 连接，一个控制连接，一个数据连接。

网络攻击

知识点 名称：网络攻击>>主动攻击和被动攻击

考 试 频 次：7

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	3	14	29	13、66	57	10

知识点 内容：

常见的**主动攻击**包括：利用缓冲区溢出 (Buffer Overflow, BOF) 漏洞执行代码，协议、软件、系统故障和后门，插入和利用恶意代码(如:特洛伊木马、后门、病毒等) ，伪装（假冒），盗取合法建立的会话，非授权访问，越权访问，重放所截获的数据，修改数据，插入数据， 拒绝服务攻击等。

常见的**被动攻击**包括：侦察、嗅探、监听、流量分析、口令截获等。

加密用以确保数据的保密性，阻止对手的被动攻击，如截取，窃听等，而对于各类主动攻击，如篡改、冒充、重播等却是无能为力的。

知识点 名称：网络攻击>>拒绝服务攻击

考 试 频 次：5

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	21		21	67		12、55

知识点 内容：

拒绝服务攻击有：SYN Flood 攻击、UDP 洪水攻击、Smurf 攻击、垃圾邮件、消耗 CPU 和内存资源的拒绝服务攻击、Ping 洪流攻击、Teardrop 泪滴攻击、分布式拒绝服务攻击。

知识点 名称：网络攻击>>重放攻击

考 试 频 次：6

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	7	7	7	7、29	50	

知识点 内容：

预防重放攻击的方式包括时间戳、 nonce、序号等，明文填充方式不能抵御重放攻击。

知识点 名称：网络攻击>>SQL 注入

考 试 频 次：1

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	19					

知识点 内容：

注入语句：http：//xxx.xxx.xxx/abc.asp?p=YY and user>0 不仅可以判断服务器的后台数据库是否为 SQL-SERVER，还可以得到：当前连接数据库的用户名。

知识点 名称：网络攻击>>网络钓鱼

考 试 频 次：4

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	57	11	57	57		

知识点 内容：

网络钓鱼（phishing）是一种通过假冒可信方（知名银行、在线零售商和信用卡公司等可信的品牌）提供网上服务，以欺骗手段获取敏感个人信息（如口令、信用卡详细信息等）的攻击方式。目前，网络钓鱼综合利用社会工程攻击技巧和现代多种网络攻击手段，以达到欺骗意图。最典型的网络钓鱼方法是，网络钓鱼者利用欺骗性的电子邮件和伪造的网站来进行诈骗活动，诱骗访问者提供一些个人信息，如信用卡号、账户和口令、社保编号等内容，以谋求不正当利益。例如，网络钓鱼攻击者构造一封所谓“安全提醒”邮件发给客户，然后让客户点击虚假网站，填写敏感的个人信息，这样网络钓鱼攻击者就能获取受害者的个人信息，并非法利用。

知识点 名称：网络攻击>>网络监听

考 试 频 次：1

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号		50				

知识点 内容：

网络监听是一种监视网络状态、数据流程以及网络上信息传输的管理工具,它可以将网络界面设定成监听模式,并且可以截获网络上所传输的信息。为了防御网络监听，最常用的方法是**信息加密**。

知识点 名称：网络攻击>>跨站攻击

考 试 频 次：1

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号		42				

知识点 内容：

跨站攻击 (CrossSiteScriptExecution XSS) 是指攻击者利用网站程序对用户输入过滤不足，输入可以显示在页面上对其他用户造成影响的 HTML 代码，从而盗取用户资料、 利用用户身份进行某种动作或者对访问者进仔病毒侵害的一种攻击方式。

跨站攻击是指入侵者在远程 WEB 页面的 HTML 代码中插入具有恶意目的的数据，用户认为该页面是可信赖的，但是当浏览器下载该页面， 嵌入其中的脚本将被解释执行。

造成 XSS 攻击的原因是网站程序对用户的输入过滤不足，不修改任何数据，属于**被动攻击**。

知识点 名称：网络攻击>IP 地址欺骗

考 试 频 次：1

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号		47				

知识点 内容：

IP 地址欺骗是冒充身份通过认证来骗取信任的攻击方式，是使一台主机信任另外台主机的复杂技术。IP 地址欺骗是指行动产生的 IP 数据包为伪造的源 IP 地址,以便冒充其他系统或发件人的身份。IP 地址欺骗的基本流程是：确定要攻击的主机 A；发现和它有信任关系的

主机 B；将 B 利用某种方法攻击瘫痪；猜测序列号；成功连接，留下后门。

知识点 名称：网络攻击>中间人攻击

考 试 频 次：1

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号				50		

知识点 内容：

中间人攻击(Man-in-the-Middle Attack MITM)是指 A 和 B 通信的同时，有第三方 C 处于信道的中间，可以完全听到 A 与 B 通信的消息，并可拦截、替换和添加这些消息。

例如 SMB 会话劫持、DNS 欺骗等攻击，都是典型的 MITM 攻击。

知识点 名称：网络攻击>APT 攻击

考 试 频 次：1

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号				51		

知识点 内容：

高级持续性威胁 (Advanced Persistent Threat, APT) 是指隐匿而持久的电脑入侵过程，通常由某些人员精心策划，针对特定目标。

一般 APT 攻击过程可概括为 3 个阶段：攻击前准备阶段、攻击入侵阶段和持续攻击阶段，又可细分为 5 个步骤：情报收集、防线突破、通道建立、横向渗透、信息收集及外传。

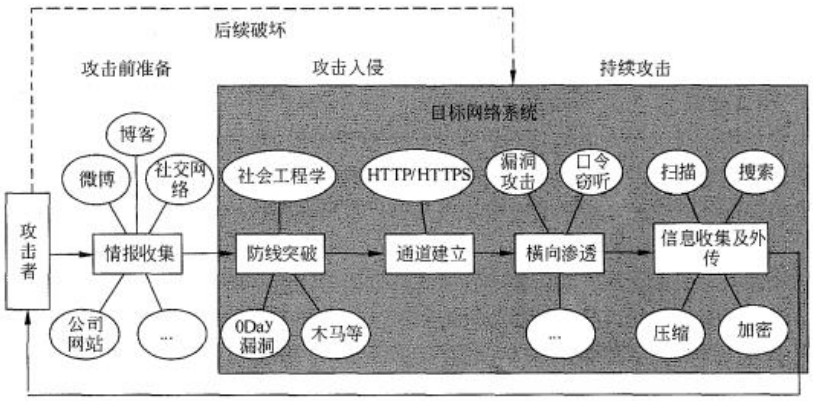


图 3-30　APT 攻击过程

情报收集：在实施攻击之前，攻击者会针对特定组织的网络系统和相关员工展开大量的信息搜集。

防线突破：攻击者在完成情报收集和技术准备后，开始采用木马/恶意代码攻击特定员工的个人电脑。

通道建立：攻击者在突破防线并控制员工电脑后，在员工电脑与入侵服务器之间开始建立命令控制通道。

横向渗透：攻击者会采用口令窃听、漏洞攻击等多种渗透方法尝试进一步入侵组织内部更多的个人电脑和服务器，同时不断地提升自己的权限，以求控制更多的电脑和服务器，直至获得核心电脑和服务器的控制权。

信息收集及外传：攻击者常常长期潜伏，并不断实行网络内部横向渗透，通过端口扫描等方式获取服务器或设备上有价值的信息，针对个人电脑通过列表命令等方式获取文档列表信息等。

知识点 名称：网络攻击>缓冲区溢出攻击

考 试 频 次：1

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号						8

知识点 内容：

缓冲区溢出攻击是一种通过往程序的缓冲区写超出其长度的内容，造成缓冲区溢出，从而破坏程序的堆枝，使程序转而执行其他预设指令，以达到攻击目的的攻击方法。

金丝雀（Canary）这一名称来源于早先英国的探测技术。英国矿工下井前会带一只金丝雀，金丝雀对毒气敏感，如果井下有有毒气体，则会停止鸣叫甚至死亡，从而矿工们很到预

警。

Canary 技术属于**缓解缓冲区溢出**的有效手段，该技术在堆栈溢出发生的高危区域的低地址部分插入一个值，通过检测该值是否改变，来判断堆栈或者缓冲区是否出现溢出。这种方式，增加了堆栈溢出攻击的难度，而且几乎不消耗资源，属于**堆栈保护**的常用手段。

知识点 名称：网络攻击>>网络攻击工具

考 试 频 次：4

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	62	22	47			13

知识点 内容：

网络攻击者经常采用的工具主要包括：扫描器、远程监控、密码破解、网络嗅探器、安全渗透工具箱等。

扫描器工具：NMap（Network Map，网络地图）、Nessus、SuperScan；

远程监控工具：冰河、网络精灵、Netcat；

密码破解工具：John the Ripper(检查 Unix/Linux 系统的弱口令)、LophtCrack(破解 Windows 系统口令)。常见的密码破解方式有：口令猜测、穷举搜索、撞库等。

网络嗅探器工具：Tcpdump/Wireshark、Dsniff；

安全渗透工具箱：Metasploit、BackTrack5

扫描技术主要用于获取目标的各种信息,这些信息既可以用于后续的进一步攻击渗透,也可以作为防守使用。

攻击者通过对目标主机进行端口扫描，可以直接获得：目标主机开放了那些端口服务。

网络流量监控和协议分析

知识点 名称：网络流量监控和协议分析

考 试 频 次：3

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	64		64	64		

知识点 内容：

流量监测中所监测的流量通常采集自主机节点、服务器、路自器的接口、链路和路径等。

数据采集探针是专门用于获取网络链路流量数据的硬件设备。

网络流量监控分析的基础是协议行为解析技术，主要包含协议描述和协议行为解析两个环节。

网络流量状况是网络中的重要信息，利用流量监测获得的数据，可以实现以下目标：①负载监测②性能分析③网络纠错④网络优化⑤业务质量监视⑥用户流量计费⑦入侵检测⑧协议调测。

知识点 名称：网络流量监控和协议分析>> 深度流检测技术(DFI)

考 试 频 次：2

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	46		44			

知识点 内容：

深度流检测技术主要分为三部分：流特征选择、流特征提取、分类器。

知识点 名称：网络流量监控和协议分析>> 网络协议分析工具

考 试 频 次：

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号						

知识点 内容：

Sniffer ，也可以称为嗅探器，它是一种基于"被动侦听"原理的网络分析方式，能 够快速定位网络故障，并能捕获网络故障数据包，帮助网管人员分析和处理故障数据包， 有效提高

网络管理水平。

Wireshark (前称 Ethereal) 是一款免费开源的协议解析器，是目前世界范围内应用最广泛的网络协议解析软件之一。

无线网络安全

知识点 名称：无线网络安全>>无线公开秘钥体系 WPKI

考 试 频 次：

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号						

知识点 内容：

WPKI 即"无线公开密钥体系"它是将互联网电子商务中 PKI （PublicKeyInfrastructure) 安全机制引入到无线网络环境中的一套遵循既定标准的密钥及证书管理平台体系，用它来管理在移动向络环境中使用的公开秘钥和数字证书，有效建立安全和值得信赖的无线网络环境。基本的 WPKI 组件包括端实体应用（EE)、注册中心（RA))、认证中（CA)、PKI 目录。

知识点 名称：无线网络安全>>有线等效保密协议(WEP)

考 试 频 次：2

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号		37			29	

知识点 内容：

有线等效保密协议（Wired Equivalent Privacy，WEP）是 1999 年 9 月通过的 IEEE802.11 标准的一部分，使用 **RC4 (RivestCipher) 串流加密技术**达到机密性，并使用 CRC-32 验和达到资料正确性。

标准 **64** 比特 WEP 使用 **40** 比特的钥匙接上 **24** 比特的初向量(Initialization Vector, IV) 成为 RC4 用的钥匙。

知识点 名称：无线网络安全>> Wi-Fi 网络安全接入（WPA/WPA2）

考 试 频 次：3

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	37		37		55	

知识点 内容：

WPA 全名为 Wi-Fi Protected Access，有 WPA 和 WPA2 两个标准，是一种保护无线电脑网络（Wi-Fi）安全的系统，它是应研究者在前一代的系统有线等效加密(WEP)中找到的几个严重的弱点而产生的。WPA 适用于 IEEE802.11 标准的大部分，是在 802.11i 完备之前替代 WEP 的过渡方案。

WPA 加密方式目前有四种认证方式 WPA、WPA-PSK、WPA2、WPA2-PSK。采用的加密算法有二种：AES（Advanced Encryption Standard 高级加密算法）和 TKIP（Temporal Key Integrity Protocol 临时密钥完整性协议）。

知识点 名称：无线网络安全>>无线局域网鉴别与保密体系 WAPI

考 试 频 次：4

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号		27	48、52	52		

知识点 内容：

无线局域网鉴别和保密体系(WirelessLAN Authentication and Privacy Infrastructure WAPI)，是一种安全协议，同时也是中国无线局域网安全强制性标准。

与 WIFI 的单向加密认证不同，WAPI 双向均认证，从而保证传输的安全性。

WAPI 安全系统采用公钥密码技术，鉴权服务器 AS 负责证书的颁发、验证与吊销等，无线客户端与无线接入点 AP 上都安装有 AS 颁发的公钥证书，作为自己的数字身份凭证。

WAPI 鉴别及密钥管理的方式有两种，即基于证书和基于预共享密钥 PSK。

WPKI 并不是一个全新的 PKI 标准,它是传统的 PKI 技术应用于无线环境的优化扩展。它采用了优化的 ECC 椭圆曲线加密和压缩的 x.509 数字证书。

WAPI 从应用模式上分为单点式和集中式。（**不包含分布式**）

WAPI 包括两部分：WAI（WLAN Authentication Infrastructure）WPI（WLAN PrivacyIn frastructure）。WAI 和 WPI 分别实现对用户身份的鉴别和对传输的业务数据加密，其中 WAI 采用公开密钥密码体制，利用公钥证书来对 WLAN 系统中的 STA 和 AP 进行认证；WPI 则采用对称密码算法实现对 MAC 层 MSDU 的加、解密操作。

知识点 名称：无线网络安全>>无线传感器网络 (WirelessSensorNetworks WSN)

考 试 频 次：2

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号		57		37		

知识点 内容：

无线传感器网络容易受到各种恶意攻击，例如干扰服务、节点捕获等。**可以采用被干扰区内节点切换通信频率的方式抵御干扰**，并解决了干扰区节点和干扰区外节点通信 频率协调问题。针对传感器被敌方获取、解密甚至篡改程序后将对无线传感器网络的运行和数据的正确性带来很大的威胁，**无线传感器节点可以通过向独立多路径发送验证数据来发现异常节点**。在时间同步过程中，系统可以**利用安全并具有弹性的时间同步协议，对抗外部攻击和被俘获节点的影响**。另外，每个节点在多属性上监视其邻居节点的网络行为，通过异常数据值检测技术和投票方式来发现恶意节点，同时，通过无线信道监听可以追踪恶意数据包来源节点，采用转发节点以一定概率进行嵌套签名的策略实现对恶意数据包的准确追踪。

现有的 WSN 标准有 Zigbee ISA100.1 1a, WirelessHART, WIA 等。其中 Zigbee 标准是民用标准。

无线传感器网络中现有的**基于公开密钥**的机制包括基于椭圆曲线的加密机制和基于阻技术的加密协议 TinyPK。但是由于采用公开密钥的管理机制在节点进行认证或获取密钥时，网络通信开销和节点计算开销大，容易招致拒绝服务攻击，**目前尚未形成主流**。

对称密钥加密算法由于加密处理简单，加解密速度'快，密钥较短等特点，非常适合资源受限的传感器网络部署使用。

知识点 名称：无线网络安全>>无线网络安全威胁

考 试 频 次：1

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号			51			

知识点 内容：

无线网络由于自身特点，面临着比有线网络更多更严重的安全威胁，主要可划分为对无线接口的攻击、对无线设备的攻击以及对无线网络本身的攻击。

对无线接口的攻击可以分为物理攻击和密码学攻击，包括窃听、篡改、重放、干扰和欺诈等等。

攻击无线网络是指针对网络基础设施进行攻击，也包括内部人员破坏和泄密。

针对无线设备的攻击包括克隆、盗窃等等。

网站安全

知识点 名称：网站安全

考 试 频 次：2

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号						37、69

知识点 内容：

Apache Httpd 是一个用于搭建 Web 服务器的开源软件，目前应用非常广泛。Apache Httpd 配置文件如下：

httpd.conf Apache 的主配置文件， httpd 程序启动时会先读取 httpd.conf。

conf/srm.conf 是数据配置文件，在这个文件中主要设置 WWWServer 读取文件的目录、目 录索引时的画面、 CGI 执行时的目录等。

access.conf 负责基本的读取文件控制，限制目录所能执行的功能及访问目录的权限，设置 access.conf 不是必需的，可以在 httpd.conf 里设定。

mime.conf 设定 Apache 所能辨别的 MIME 格式，一般而言，无须动此文件。若要增加

MIME 格式，可参考 snn.conf AddType 的语法说明。

防火墙是网站安全的第一道技术屏障，主要用于限制来自某些特定 IP 地址的网站连接请求，阻止常见的 Web 应用攻击及 Web Services 攻击。目前，可以使用的防火墙技术主要有包过滤防火墙、Web 应用防火墙。其中，**包过滤防火墙只能基于 IP 层过滤网站恶意包，Web 应用防火墙针对 80、443 端口、Web Services 攻击**。

网站防篡改的实现技术主要有两类：一是利用操作系统的文件调用事件来检测网页文件的完整性变化，以此防止网站被非授权修改；二是利用密码学的单向函数检测网站中的文件是否发生了改变。若检测到网页受到非法修改，则启动网页恢复机制，自动地用正常的页面文件替换已破坏的页面。

网络流量清洗是指通过基于网络流量的异常监测技术手段，将对目标网络攻击的 DoS DDoS 等恶意网络流量过滤掉，同时把正常的流量转发到目标网络中。

防火墙

知识点名称：防火墙

考试频次：5

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	8	24、51		63		35

知识点内容：

防火墙是一种位于内部网络与外部网络之间的网络安全系统，内外网络通信时，依照特定的规则，允许或是限制传输的数据通过。它**不能防范内部威胁及病毒威胁**。

应用代理防火墙也被称为代理服务器，它针对特定的网络应用服务协议使用指定的数据过滤逻辑，并在过滤的同时，对数据包进行必要的分析、登记和统计，形成报告。

应用代理防火墙的优点是安全性较高,可以针对应用层进行侦测和扫描,安全控制更细化、更灵活。

防火墙的规则处理方式如下：

Accept：允许数据包或信息通过；

Reject：拒绝数据包或信息通过，并且通知信息源该信息被禁止；

Drop：直接将数据包或信息丢弃，并且不通知信息源。

防火墙的功能主要有以下几个方面：过滤非安全网络访问、限制网络访问、网络访问审计、网络带宽控制、协同防御。

知识点名称：防火墙>>包过滤技术

考试频次：4

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号		52	63	42		36

知识点内容：

防火墙在过滤数据包时，一般不关心数据包的内容。

当防火墙在网络层实现信息过滤与控制时，主要是针对 TCP/IP 协议中的 IP 数据包头部制定规则的匹配条件并实施过滤，其规则的匹配条件包括以下内容：IP 源地址，IP 数据包的发送主机地址；IP 目的地址，IP 数据包的接收主机地址；协议，IP 数据包中封装的协议类型，包括 TCP、UDP 或 ICMP 包等。**不包括源端口**。

包过滤型防火墙对用户透明，合法用户在进出网络时，感觉不到它的存在，使用起来很方 便。在实际网络安全管理中，包过滤技术经常用来进行网络访问控制。标准 IP 访问控制规则的格式如下：

```
access-list list-number{deny|permit}source[source-wildcard][log]
```

而扩展 IP 访问控制规则的格式是：

```
access-list list-number{deny|permit}protocol
    source source-wildcard source-qualifiers
   destination destination-wildcard destination-qualifiers[log|log-input]
```

其中：

- 标准 IP 访问控制规则的 list-number 规定为 1～99，而扩展 IP 访问控制规则的 list-number 规定为 100～199；
- deny 表示若经过 Cisco IOS 过滤器的包条件不匹配，则禁止该包通过；
- permit 表示若经过 Cisco IOS 过滤器的包条件匹配，则允许该包通过；
- source 表示来源的 IP 地址；
- source-wildcard 表示发送数据包的主机 IP 地址的通配符掩码，其中 1 代表“忽略”，0 代表“需要匹配”，any 代表任何来源的 IP 包；
- destination 表示目的 IP 地址；
- destination-wildcard 表示接收数据包的主机 IP 地址的通配符掩码；
- protocol 表示协议选项，如 IP、ICMP、UDP、TCP 等；
- log 表示记录符合规则条件的网络包。

知识点名称：防火墙>>防火墙体系结构

考试频次：2

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号		45			42	

知识点内容：

防火墙的经典体系结构主要有三种形式：双重宿主主机体系结构、被屏蔽主机体系结构和被屏蔽子网体系结构。

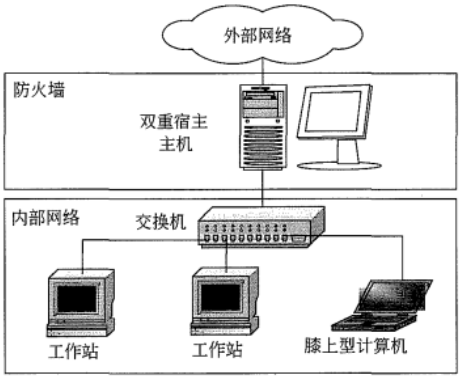


图 3-51　双重宿主主机体系结构

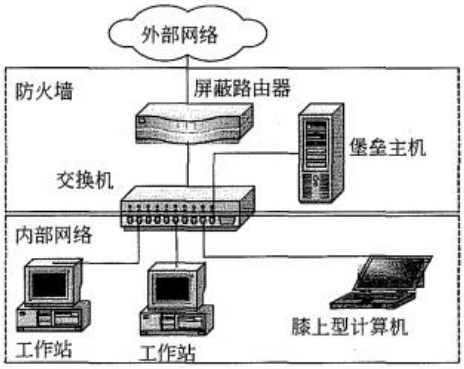


图 3-52　被屏蔽主机体系结构

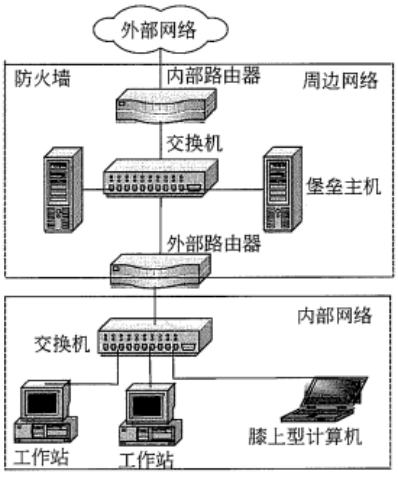


图 3-53　被屏蔽子网体系结构

外部路由器的主要作用在于保护周边网络和内部网络，是屏蔽子网体系结构的第一道屏障。

VPN

知识点名称：VPN 技术

考试频次：16

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	55、58、61	33、58、62	55、61	17、40、55、61	17	38、39、40

知识点内容：

VPN 连接中一般包括两种形式的认证：用户身份认证、数据完整性和合法性认证。

VPN 主要的安全服务有以下 3 种：

- 保密性服务 (Confidentiality) ：防止传输的信息被监听；
- 完整性服务 (Integrity) ：防止传输的信息被修改；
- 认证服务 (Authentication) ：提供用户和设备的访问认证，防止非法接入。

目前 VPN 主要采用如下四项技术保证安全：隧道技术、加解密技术、密钥管理技术、使用者与设备身份认证技术。

隧道技术是 VPN 的基本技术，类似于点对点连接技术，它在公用建立一条数据通道（隧道），让数据包通过这条隧道传输。隧道是由隧道协议形成的，分为第二、三层隧道协议。第二层隧道协议是先把各种网络协议封装到 PPP 中，再把整个数据包装入隧道协议中，这种双层封装方法形成的数据包靠第二层协议进行传输。**第二层隧道协议有 L2F、PPTP、L2TP 等**；第三层隧道协议是把各种网络协议直接装入隧道协议中，形成的数据包依靠第三层协议进行传输。**第三层隧道协议有 VTP、IPSec 等**。

IPSec 提供了两种安全机制：认证（采用 ipsec 的 **AH**）和加密（采用 ipsec 的 **ESP**）。

IPSec 属于**网络层**的安全解决方案。

VPN 的隧道协议主要有 PPTP、L2TP 和 IPSec 三种，其中 PPTP 和 L2TP 协议工作在 OSI 模型的第二层，又称为第二层隧道协议；IPSec 是第三层隧道协议。PPTP 通常可以搭配 PAP、CHAP、MS-CHAPv1/v2 或 EAP-TLS 来进行身份验证。

VPN 有多种实现技术，按照 VPN TCP/IP 协议层的实现方式，可以将其分为链路层 VPN

网络层 VPN 、传输层 VPN 。**链路层 VPN** 的实现方式有 ATM、Frame Relay、多协议标签交换 MPLS; **网络层 VPN** 的实现方式有受控路由过滤、隧道技术；**传输层 VPN** 则通过 SSL 来实现。

知识点名称：VPN 技术>>SSL

考试频次：6

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	52	13、32	40	54	54	

知识点内容：

SSL 是一种应用于传输层的安全协议。（传输层和应用层之间）

SSL 安全套接层是为网络通信提供安全及数据完整性的一种安全协议。其提供的安全服务包括：1、认证用户和服务器，确保数据发送到正确的客户机和服务器；2、加密数据以防止数据中途被窃取；3、维护数据的完整性，确保数据在传输过程中不被改变。**不能提供可用性**。

认证技术

知识点 名称：认证技术

考 试 频 次：8

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	5、11、28		28	16	7、61	29

知识点 内容：

认证一般由标识 (Identification) 和鉴别 (Authentication) 两部分组成。

身份认证是证实客户的真实身份与其所声称的身份是否相符的验证过程。常见的身份认证协议包括 S/Key 口令协议、 Kerberos 协议、X.509 协议等。

面向身份信息的认证应用中最常用的认证方式是基于账户名/口令认证。

Kerberos 是标准网络身份认证协议，它采用（DES）加密算法进行加密。

Kerberos 是一种网络认证协议，其设计目标是通过密钥系统为客户机 / 服务器应用程序提供强大的认证服务。该认证过程的实现不依赖于主机操作系统的认证，无需基于的信任，不要求网络上所有主机的物理安全，并假定网络上传送的数据包可以被任意地读取、修改和插入数据。在以上情况下， Kerberos 作为一种可信任的第三方认证服务，是通过传统的密码技术（如：共享密钥）执行认证服务的。

一个 Kerberos 系统涉及四个基本实体：：

(1) Kerberos 客户机，用户用来访问服务器设备；

(2) AS (Authentication Server, 认证服务器)，识别用户身份并提供 TGS 会话密钥；

(3) TGS (Ticket Granting Server, 票据发放服务器)，为申请服务的用户授予票据 (Ticket);

(4) 应用服务器 (Application Server) ，为用户提供服务的设备或系统。

其中，通常将 AS 和 TGS 统称为 KDC (Key Distribution Center) 。

知识点 名称：认证技术>>基于生物特征认证技术

考 试 频 次：5

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	17	17	17	45	45	

知识点 内容：

目前，指纹、人脸、视网膜、语音等生物特征信息可用来做身份认证。

能用于身份认证的生物特征必须具有唯一性和稳定性。

知识点 名称：认证技术>>公钥基础设施（PKI）技术

考 试 频 次：12

考 题 类 型：选择题

相 关 真 题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	36、60	31、55、60	36、60	31、60	31、33	30

知识点 内容：

CA 的功能主要有证书管理、证书签发、证书验证、证书撤销等，**不包括证书加密**。

RA 的主要功能如下：认证注册信息的合法性、批准或拒绝证书的申请、批准或控绝恢复密钥的申请、批准或拒绝撤销证书的申请。

当用户个人身份信息发生变化或私钥丢失、泄露、疑似泄露时，证书用户应及时地向 CA（证书的签发机构，是 PKI 的核心）提出证书撤销、废止、更新的请求。

PKI 的组成部分包括：证书主体、CA、RA、使用证书的应用和系统、证书权威机构等；自治系统 AS 在互联网中是一个有权自主地决定在本系统中应采用何种路由协议的小型单位，其不属于 PKI 的组成部分。

入侵检测技术

知识点名称：入侵检测技术

考试频次：7

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	53			44、53	44	13、41、43

知识点内容：

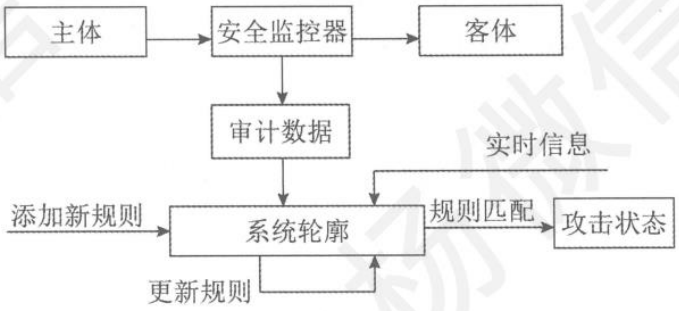


图 10-1　入侵检测模型

入侵检测系统主要包括：基于主机的入侵检测系统、基于网络的入侵检测系统和分布式入侵检测系统。

将入侵检测系统置于防火墙内部,使得很多对网络的攻击首先会被防火墙过滤,也就是防火墙是首当其冲的,从而也就减少了对内部入侵检测系统的干扰,提高入侵检测系统的准确率,但是其检测能力不会变化。

入侵检测技术包括异常入侵检测和误用入侵检测。

异常检测(也称基于行为的检测)是指把用户习惯行为特征存储在特征库中，然后将用户当前行为特征与特征数据库中的特征进行比较，若两者偏差较大，则认为有异常情况发生。

误用检测一般是由计算机安全专家首先对攻击情况和系统漏洞进行分析和分类，然后手工的编写相应的检测规则和特征模型。

Snort 是一款开源的网络入侵检测系统，它能够执行实时流量分析和协议网络的数据包记录。Snort 的配置有 3 个主要模式：嗅探(Sniffer)、包记录(PacketLogger)和网络入侵检测(NetworkIntrusionDetection)。

Sniffer 主要是捕获到达本机端口的报文。如果要想完成监听，即捕获网段上所有的报文，

前提条件是:①网络必须是共享以太网。②把本机上的网卡设置为混杂模式。

Sniffer 分为软件和硬件两种，软件的 Sniffer 如 NetXray、Packetboy、Netmonitor 等。硬件的 Sniffer 通常称为协议分析仪，一般都是商业性的，价格也出较贵。

入侵检测框架模型，简称为 CIDF（CommonIntrusionDetectionFramework）。该模型认为入侵检测系统由事件产生器 (event generators) 、事件分析器 (event analyzers) 、响应单元 (response units) 和事件数据库 (event databases) 组成。

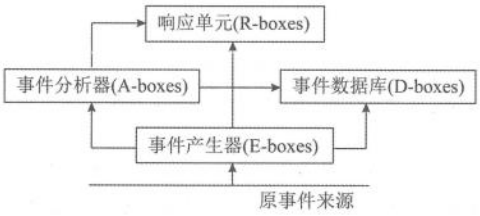


图 10-2 CIDF 各组件之间的关系图

事件产生器从整个计算环境中获得事件，并向系统的其他部分提供事件。

事件分析器分析所得到的数据，并产生分析结果。

响应单元对分析结果做出反应，如切断网络连接、改变文件属性、简单报警等应急响应。

事件数据库存放各种中间和最终数据，数据存放的形式既可以是复杂的数据库，也可以是简单的文本文件。

网络的入侵检测系统(NIDS)可以检测到的攻击有：同步风暴、分布式拒绝服务攻击、网络扫描、缓冲区溢出、协议攻击、流量异常、非法网络访问等。

基于主机的入侵检测系统(HIDS)可以检测：针对主机的端口和漏洞扫描、重复登录失败、拒绝服务、系统账号变动、重启、服务停止、注册表修改、文件和目录完整性变化等。

访问控制技术

知识点名称：访问控制技术

考试频次：7

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号		34、70		23	9	31、32、33

知识点内容：

信息系统访问控制的基本要素包括主体、客体和授权访问。

在计算机系统中，访问控制包括以下三个任务：授权，即确定可给予哪些主体存取客体的权力；确定存取权限(读、写、执行、删除、追加等存取方式的组合)实施存取权限。

常用的访问控制类型有：自主访问控制、强制访问控制、基于角色的访问控制、基于属性的访问控制。

自主访问控制（DiscretionaryAccessControl，DAC）的实现方法有两大类：基于行的自主访问控制、基于列的自主访问控制。

基于行的自主访问控制机制在每个主体上都附加一个该主体可访问的客体的明细表，根据表中信息的不同又可分成以下三种形式：访问能力表、前缀表、口令。

基于列的自主访问控制机制，在每个客体都附加一个可访问它的主体的明细表，它有两种形式，即保护位和访问控制表。

强制访问控制（MandatoryAccessControl，MAC）是一种不允许主体干涉的访问控制类型。它是基于安全标识和信息分级等信息敏感性的访问控制,通过比较资源的敏感性与主体的级别来确定是否允许访问。系统将所有主体和客体分成不同的安全等级,给予客体的安全等级能反映出客体本身的敏感程度;主体的安全等级标志着用户不会将信息透露给未经授权的用户。根据 MAC 的安全级别,用户与访问的信息的读写关系有四种类型,其中能保证数据完整性的读写组合方式是**上读下写**。

MAC 可通过使用敏感标签对所有用户和资源强制执行安全策略，即实行强制访问控制。安全级别一般有四级：绝密级（Top Secret），秘密级（Secret），机密级（Confidential）和无级别级（Unclassified），其中 T＞S＞C＞U。

则用户与访问的信息的读写关系将有 4 种，即：

下读（read down）：用户级别高于文件级别的读操作。

上写（write up）：用户级别低于文件级别的写操作。

下写（write down）：用户级别高于文件级别的写操作。

上读（read up）：用户级别低于文件级别的读操作。

基于角色的存取控制（Role-Based Access Control，RBAC）模型主要用于管理特权，

在基于权能的访问控制中实现职责隔离及极小特权原理。

操作系统访问控制是针对计算机系统资源而采取的访问安全措施。操作系统访问控制的具体措施有文件读写、进程、内存等访问控制。

隐私保护技术

知识点名称：隐私保护技术

考试频次：3

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号		69	8			53

知识点内容：

从数据挖掘的角度，目前的隐私保护技术主要可以分为三类：

（1）基于数据失真的隐私保护技术：它是使敏感数据失真但同时保持某些关键数据或者属性不变的隐私保护技术，例如，采用交换(Swapping)、添加噪声等技术对原始数据集进行处理，并且保证经过扰动处理后的数据仍然保持统计方面的性质，以便进行数据挖掘等操作。

（2）基于数据加密的隐私保护技术：它是采用各种加密技术在分布式环境下隐藏敏感数据的方法，如安全多方计算(SecureMultipartyComputation,SMC)、分布式匿名化、分布式关联规则挖掘和分布式聚类等。

（3）基于数据匿名化的隐私保护技术：它是根据具体情况有条件地发布数据，例如，不发布原始数据的某些值、数据泛化(Generalization)等。

消息认证技术

知识点名称：消息认证技术

考试频次：4

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	39	39	39		16	

知识点内容：

消息认证通过采用哈希算法实现数据的完整性。

信息通过网络进行传输的过程中,存在着被慕改的风险,为了解决这一安全隐患通常采用的安全防护技术是：消息认证技术。

产生认证码的方法有以下三种：①报文加密；②消息认证码(MAC) ③基于 hash 函数的消息认证码(HMAC)

漏洞扫描技术

知识点名称：漏洞扫描技术

考试频次：3

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号		44				11、59

知识点内容：

网络安全漏洞扫描技术的两大核心技术就是端口扫描技术与漏洞扫描技术。

TCP SYN 扫描。这种方法也叫"半打开扫描(Half-openScanning)"。这种扫描方法并没有建立完整的 TCP 连接。客户端首先向服务器发送 SYN 分组发起连接，如果收到一个来自服务器的 **SYN/ACK** 应答，那么可以推断该端口处于监听状态。如果收到一个 **RST/ACK** 分组则认为该端口不在监听。而客户端不管收到的是什么样的分组，都向服务器发送一个 RST/ACK 分组，这样并没有建立一个完整的 TCP 连接，但客户端能够知道服务器某个端口是否开放。该扫描不会在目标系统上产生日志。

ID 头信息扫描：这种扫描方法需要用一台第三方机器配合扫描，并且这台机器的网络通信量要非常少，即 dumb 主机。

数据加密存储技术

知识点名称：数据加密存储技术

考试频次：1

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号				19		

知识点内容：

文件加密就是将重要的文件以密文形式存储在媒介上，对文件进行加密是一种有效的数据加密存储技术。基于 Windows 系统的是（EFS）。

加密文件系统(Encrypting File System，EFS)可以说是微软为用户提供的一个内建在 Windows 产品中的方便快捷并且强大的加密系统 ，然而，微软设计了让其他操作系统也能读取 NTFS 的文件格式来使用户能够避开硬盘故障以及启动分区故障。因此，使用某些操作系统可以很容易地绕过 NTFS 安全机制，存取 NTFS 文件。

网络地址转换

知识点名称：网络地址转换 NAT

考试频次：2

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号		23				21

知识点内容：

NAT 有三种类型：静态 NAT、动态地址 NAT 、端口地址转换 PAT。

静态 NAT 设置起来最为简单和容易，内部网络中的每个主机都被永久映射成某个全球地址。

动态方式：以地址池的方式。地址池中有多个全球地址用来对内部地址进行映射， 但

不固定绑定。

端口地址转换 PAT：一个外网地址可以和多个内网地址(如一个网段)进行映射， 同时在该地址上加上一个由 NAT 设备指定的 TCP/UDP 的端口号来进行区分。

通过采用 DHCP 协议，DHCP 服务器可以为 DHCP 客户端动态分配 IP 地址。

DNS 协议可实现域名地址和 IP 地址之间的转换。

ARP 协议可以实现 MAC 地址和 IP 地址之间的转换。

IP 地址是 IP 协议提供的一种统一的地址格式，是分配给互联网主机的逻辑地址，属于网络层协议。而端口地址通常是指为 TCP 或者 UDP 协议通信提供服务的数字标记，属于传输层。所以 IP 地址和端口地址本质上属于不同的两类事物，是不能用 DHCP 协议进行转换的。

数据库系统安全

知识点名称：数据库系统安全>>数据库恢复技术

考试频次：1

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号					39	

知识点内容：

数据库恢复技术一般有四种策略：基于数据转储的恢复、基于日志的恢复、基于检测点的恢复和基于镜像数据库的恢复。

基于数据转储的恢复是指数据库管理员定期地将整个数据库复制到磁带或另一个磁盘上保存起来的过程，这些数据文本称为后备副本或后援副本。

基于日志的恢复是指，运行时将对数据库每一次更新操作，都应优先记录到日志文件中。

基于检测点的恢复是在日志文件中增加一类新的记录一一检查点记录，增加一个重新开始文件，并使恢复子系统在登录日志文件期间动态地维护日志。

数据库镜像就是在另一个磁盘上作数据库的实时副本。

知识点名称：数据库系统安全>>MySQL

考试频次：1

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号			19			

知识点内容：

MySQL 口令设置方法：

（1）使用 MySQL 自带的命令 mysqladmin 设置 root 口令；

% mysqladmin -u root password 'rootpassword'

（2）使用 setpassword 设置口令；

%mysql> SET password for root@localhos PASSWORD('rootpassword');

（3）登录数据库,修改数据库 mysql 下 user 表的字段内容设置口令

%mysql> UPDATE user SET password=PASSWORD('rootpassword') WHERE user='root';

知识点名称：数据库系统安全>>Oracle

考试频次：1

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号						67

知识点内容：

Oracle 数据库提供认证、访问控制、特权管理、透明加密等多种安全机制和技术。

Oracle 数据库的认证方式采用“用户名＋口令”, 具有口令加密、账户锁定、口令生命期和过期、口令复杂度验证等安全功能。对于数据库管理员认证， Oracle 数据库要求进行特别认证，支持强认证、操作系统认证、口令文件认证。网络认证支持第三方认证、PKI 认证、远程认证等。

操作系统安全

知识点名称：操作系统安全>>Windows

考试频次：1

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号					15	

知识点内容：

Netstat 是 DOS 命令，是一个监控 TCP/IP 网络的非常有用的工具，可以了解网络的整体使用情况。它可以显示路由表、实际的网络连接以及每一个网络接口设备的状态信息，一般用于检验本机各端口的网络连接情况。

Ipconfig 是调试计算机网络的常用命令，通常大家使用它显示计算机中网络适配器的 IP 地址、子网掩码及默认网关。

Nslookup 命令用来判断域名系统(DNS)是否可用，可以显示域名系统的相关信息，用户可以通过该命令查看指定网站的 IP 地址。

Traceroute 命令能够遍历到数据包传输路径上的所有路由器。

在 Windows 系统下，可以使用 fport 工具对相关进程和端口号进行关联。

知识点名称：操作系统安全>>Linux

考试频次：3

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号			24			45、65

知识点内容：

Linux 系统将用户名存放在/etc/passwd 文件中，而将口令以加密的形式存放在/etc/shadow 文件中。

日志存储在/var/log 目录中。

Linux 操作系统的基本审计信息有系统开机自检日志 boot.log 、用户命令操作日志

acct/pacct 、最近登录日志 lastlog 、使用 SU 命令日志 sulog 、当前用户登录日志 utmp 用户登录和退出日志 wtmp 、系统接收和发送邮件日志 maillog 、系统消息 messages 等。

UNIX/Linux 系统中可用 lsof 工具检查进程使用的文件、tcp/udp 端口、用户等相关信息。

对于 UNIX 系统，网络管理员可使用 cmp 命令直接把系统中的二进制文件和原始发 布介质上对应的文件进行比较。或者利用 MD5 工具进行 Hash 值校验，其方法是向供应商获取 其发布的 进制文件的 Hash 值，然后使用 MD5 工具对可疑的二进制文件进行检查。

Inetd.conf 文件是 Linux 系统中的重要文件之一。它保存了系统提供 internet 服务的数据库。**service** 文件是某项服务对应的配置文件,可用于 systemd 管理和控制的服务的设置。

最小化配置服务是指在满足业务的前提条件下，尽量关闭不需要的服务和网络端口，以减 少系统潜在的安全危害。实现 UNIX/Linux 网络服务的最小化，具体安全要求如下：

- inetd.conf 的文件权限设置为 600;
- inetd.conf 的文件属主为 root;
- services 的文件权限设置为 644;
- services 的文件属主为 root;
- inetd.conf 中，注销不必要的服务，比如 finger echo chargen rsh rlogin tftp 服务；
- 只开放与系统业务运行有关的网络通信端口

知识点名称：操作系统安全>>Android

考试频次：4

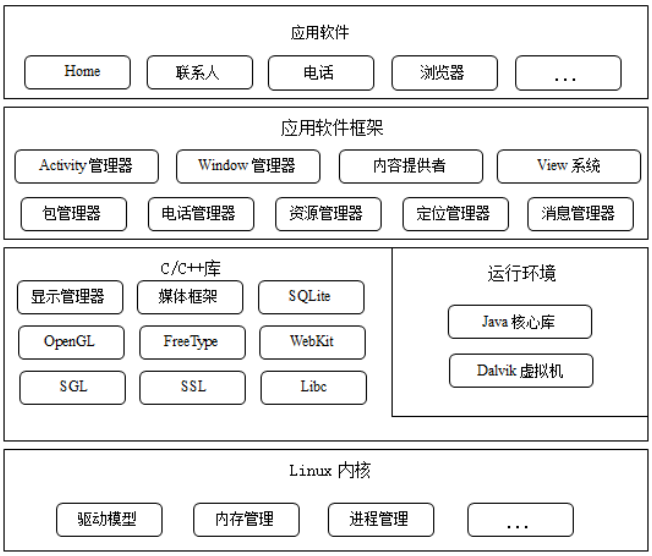
考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号		30		18	19	62

知识点内容：

安卓系统架构是指安卓系统的体系结构，是一个分层的架构，共分为四层，从上层到下层依次为：应用程序层、应用程序框架层、系统库和安卓运行时、Linux 内核。安卓的核心系统服务依赖于 Linux 内核，如安全性、内存管理、进程管理、网络协议栈和驱动模型等，其中**文件访问控制的安全服务**位于 **Linux 内核**。**显示驱动**位于 **Linux 内核。**



Android 平台进行数据存储的方式包括：(1)使用 Shared Preferences 存储数据；(2)文件存储数据：(3)SQLite 数据库存储数据；(4)使用 Content Provider 存储数据；(5)网络存储数据。

在移动应用 App 程序插入无关代码属于代码混淆技术，用于增加阅读代码的难度，是防反编译的一种手段。

知识点名称：操作系统安全>>安全机制

考试频次：1

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号					23	

知识点内容：

操作系统的安全机制就是指在操作系统中利用某种技术、某些软件来实施一个或多个安全服务的过程。主要包括：标识与鉴别机制，访问控制机制，最小特权管理机制，可信通路机制、安全审计机制，以及存储保护、运行保护和 I/O 保护机制。。

知识点名称：操作系统安全>>系统审计

考试频次：2

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号		40	45			

知识点内容：

操作系统的安全审计是指对系统中有关安全的活动进行记录、检查和审核的过程，现有的审计系统包括（收集及过滤功能模块、记录及查询功能模块、分析及响应报警功能模块）三大功能模块。

知识点名称：操作系统安全>>日志审计

考试频次：2

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号				38		64

知识点内容：

使用集中的日志审计工具和事件关联分析软件可以应对“**多组件事故**”。

Windows 日志有三种类型：系统日志、应用程序日志、安全日志。这些日志文件通常存放在操作系统的安装区域的 system32\config 目录下。默认文件大小 512KB，管理员都会改变这个默认大小。

Windows 系统日志、应用程序日志和安全日志，对应的文件名分别为 SysEvent.evt，AppEvent.evt，SecEvent.evt。

计算机机房安全

知识点名称：计算机机房安全

考试频次：1

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号						27

知识点内容：

按照《计算机场地通用规范 (GB/T 2887-2011)》的规定，计算机机房可选用下列房间（允许一室多用或酌情增减）：

---

(1) 主要工作房间：主机房、终端室等；

(2) 第一类辅助房间：低压配电间、不间断电源室、蓄电池室、空调机室、发电机室、气 体钢瓶室、监控室等；

(3) 第二类辅助房间：资料室、维修室、技术人员办公室；

(4) 第三类辅助房间：储藏室、缓冲间、技术人员休息室、盟洗室等。

OSI 参考模型

知识点名称：OSI 参考模型

考试频次：4

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	45	18				68、70

知识点内容：

OSI 安全体系结构中包含了安全服务(Security Service) 、安全机制 (Security Mechanism) 和安全管理(Security Managemer)。

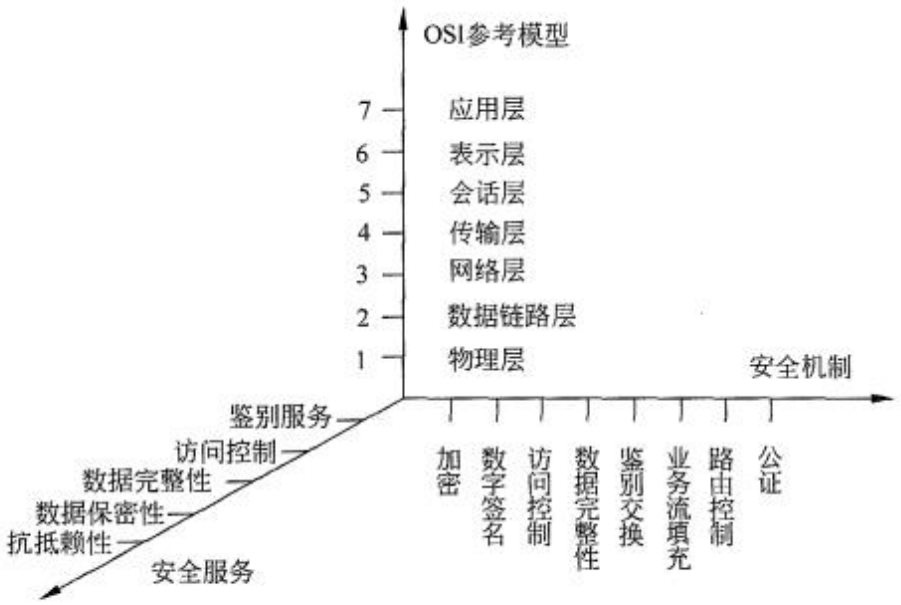


图 6-1 开放系统互连安全提携结构示意图

物理层：设计在物理通信道上传输原始比特，处理与物理传输介质有关机制的、电器过程的接口。在物理层上传输的单元是信号。

链路层：分为介质访问控制和逻辑链路控制两个子层。在链路层上传输的单元是比特。

网络层：负责将数据从物理连接的一端传递到另一端，即所谓的点到点通信。 它的主要功能是寻找路径，以及与之相关的流量控制和拥塞控制等。在网络层上传输的单元是网络数据包。

传输层：主要目的在于弥补网络服务与用户需求之间的差距。传输层通过向上提供一个标准、通用的界面，使上层与通信子网(下三层)的细节相隔离。传输层的主要任务是提供进程间通信机制和保证数据传输的可靠性。

应用层：向用户提供最常用旦适用的应用程序，包括电子邮件、文件传输、 网页浏览等。应用层描述了端对端之间的通信。

目前，工业界按照交换机的功能变化，将交换机分为第一代交换机、第二代交换机、第三代交换机、第四代交换机、第五代交换机。

其中，**集线器是第一代交换机**，工作于 OSI（开放系统互联参考模型）的物理层，主要功能是对接收到的信号进行再生整形放大，延长网络通信线路的传输距离，同时，把网络中的节点汇聚到集线器的一个中心节点上集线器会把收到的报文向所有端口转发。

第二代交换机又称为以太网交换机，工作于 OSI 的数据链路层，称为第二层交换机。 二层交换机识别数据中的 MAC 地址信息，并根据 MAC 地址选择转发端口。

第三代交换机通俗地称为三层交换机，针对 ARP/DHCP 等广播报文对终端和交换机的影响，三层交换机实现了虚拟网络 (VLAN) 技术来抑制广播风暴，将不同用户划分为不同的 VLAN, VLAN 之间的数据包转发通过交换机内置的硬件路由查找功能完成。三层交换机工作于 OSI 模型的网络层。

第四代交换机为满足业务的安全性、可靠性、 QoS 等需求，在第二、第三代交换机功能的基础上新增业务功能，如防火墙、负载均衡、IPS 这些功能通常由多核 CPU 实现。

第五代交换机通常支待软件定义网络 (SDN) ，具有强大的 QoS 能力。

在路由器配置时，使用（Enable Secret）命令保存口令密文。

智能卡

知识点名称：智能卡

考试频次：3

考题类型：选择题

相关真题：

真题年份	2016	2017	2018	2019	2020	2021
题目序号	54			30	30	

知识点内容：

智能卡是指粘贴或嵌有集成电路芯片的一种便携式卡片塑胶，智能卡的片内操作系统（COS）是智能卡芯片内的一个监控软件。

COS 一般由四部分组成:通讯管理模块和安全管理模块、应用管理模块和文件管理模块。

通讯管理模块是 COS 与外界的半双工通信通道，其按照 ISO7816 国际标准的 T=0 或 T=1 异步通讯协议，接受读写器命令；并对接收信息采取奇偶校验、累加和及分组长度检验等手段进行正确性判断。

安全管理模块是 COS 的极重要组成部分。COS 安全体系有三个基本概念：安全状态、安全属性、安全机制。

应用管理模块的主要任务是对接收命令进行可执行性判断，而智能卡的所有应用都 是以文件形式存在，应用管理的内涵已表现为对文件访问权限的安全控制，因此它常常融于安全管理和文件管理之中，而非一独立模块。

文件管理模块：所谓文件，是指卡中数据单元或记录的有组织的集合。COS 通过给每种应用建立对应文件的办法，实现它对各项应用的存储及管理。