信息安全工程师第2版课程考前冲刺

目录

CONTENTS

领域划分

类型	具体章节
基础类	1~4章（网络信息安全概述、网络攻击原理与常用方法、密码学基本理论、网络安全体系与网络安全模型）
传统技术类	5~10章（物理与环境安全、认证、访问控制、防火墙、VPN、入侵检测技术）
网络防护类	11~18章（物理隔离、审计、恶意代码防护、漏洞防护、主动防御、风险评估、应急响应、安全测评）
系统及设备	19~21章（操作系统、数据库、网络设备）
新技术新方法	22~26（网站安全、云计算、工控、移动应用、大数据）

1.1 基础类-网络信息安全概述

主要内容	关键点
基本属性	机密性、完整性、可用性、抗抵赖性、可控性、真实性、时效性、合规性、隐私性等 ● **机密性（C）：网络信息不泄露给非授权的用户、实体或程序，能够防止非授权者获取信息。** ● **完整性（I）：网络信息或系统未经授权不能进行更改的特性。** ● **可用性（A）：合法许可的用户能够及时获取网络信息或服务的特性。** ● **抗抵赖性：防止网络信息系统相关用户否认其活动行为的特性。** ● **可控性：责任主体对其具有管理、支配能力的属性，能够根据授权规则对系统进行有效掌握和控制。**
信息安全管理	●**定义**：对网络资产采取合适的安全措施，以确保网络资产的可用性、完整性、可控制性和抗抵赖性等。 ●**管理对象**：**所有支持网络系统运行的软、硬件总和；** ●**管理方法**：风险管理、等级保护、纵深防御、层次化保护、应急响应以及**PDCA。** ●**管理要素：管理对象、威胁、脆弱性、风险、保护措施。** **风险控制方法：避免风险、转移风险、减少威胁、消除脆弱点、减少威胁的影响、风险监测。** **管理流程：确定对象、评估价值、识别威胁、识别脆弱性、确定风险级别、制定及实施防范措施、运行及维护。**
法律法规及政策	**《中华人民共和国网络安全法》：2017年6月1日起实施，是国家网络空间安全管理的基本法律；** **《中华人民共和国密码法》：2020年1月1日起实施。** **网络安全等级保护制度：主要工作（定级、备案、建设整改、等级测评、运营维护）。** **互联网域名安全管理：不得放置在境外。**

1.2 基础类-攻击原理与常用方法

主要内容	关键点
网络攻击概念	由**攻击者**发起，应用**攻击工具**（包括攻击策略与方法），对目标网络系统进行（合法与非法的）**攻击操作**，达到**攻击效果**，实现**攻击意图**。
攻击模型	（1）**攻击树模型：源于故障树分析方法**，用 **AND-OR形式的树结构**对目标对象进行网络安全威胁分析； **优点**：采取专家**头脑风暴**法，能够进行**费效分析**或者**概率分析**； **缺点**：**不能用来建模多重尝试攻击、时间依赖及访问控制、循环事件**等场景；对于**大规模网络处理起来将会特别复杂。** （2）**MITRE ATT&CK模型：抽象攻击活动**，如初始访问、执行、持久化、特权提升、躲避防御、凭据访问等，应用场景：网络红蓝对抗模拟、网络安全渗透测试、网络防御差距评估、网络威胁情报收集。 （3）**网络杀伤链（Kill Chain）模型：**7个阶段（目标侦察、武器构造、载荷投送、漏洞利用、安装植入、指挥和控制、目标行动）。
攻击过程	**隐藏攻击源、收集目标信息、挖掘漏洞、获取目标访问权限、隐藏攻击行为、实施攻击、开辟后门、清除痕迹。**
攻击方法	**端口扫描：完全连接、半连接、SYN扫描、FIN扫描、ACK扫描、NULL扫描等。** **缓冲区溢出：特意构造的攻击代码植入有缓冲区溢出漏洞的程序**之中，**改变漏洞程序的执行过程。** **拒绝服务**：最本质的特征是**延长服务等待时间，特点（难确认、隐蔽、资源有限、软件复杂）、类型（同步包风暴、UDP洪水、Smurf攻击、垃圾邮件、DDoS、死亡之ping、泪滴攻击）。** 口令破解、恶意代码、网络钓鱼、网络窃听、SQL注入、社交工程、电子监听、会话劫持、漏洞扫描、数据加密、代理技术等。
攻击常用工具	**扫描器（nmap、nessus、SuperScan）、 远程监控（冰河、Netcat）、** **密码破解（John the Ripper(LINUX)、LOphtCrack(WINDOWS)）、 网络嗅探器（Tcpdump、Wireshark、Dsniff）** **安全渗透工具箱（Metasploit）。**

1.3 基础类-密码学理论

主要内容	关键点
基本情况	**发展**：传统密码学（换位、置换），现代密码学（以**Diffie--Hellman及RSA**算法为代表开创**公钥密码学**）。 **定义**：研究信息安全保护的科学，以实现信息的保密性、完整性、可用性及抗抵赖性。 **分类**：**密码编码学、密码分析学** **密码分析的类型（唯密文攻击**（对攻击者最不利）**、已知明文攻击、选择明文攻击、密文验证攻击、选择密文攻击（常用于攻击数字签名））。**
密码体制	**（1）私钥密码体制（对称密码体制）：加解密密钥相同、速度快、但是存在密码分配和管理问题，常见算法如DES、IDEA、AES。** **（2）公钥密码体制（非对称密码体制）：密钥分发方便、支持数字签名，但是加解密速度慢，常见算法如RSA、ELGamal、椭圆曲线密码体制。** **（3）混合密码体制：利用公钥密码体制分配私钥密码体制的密钥，如数字信封。**
密码算法	**（1）对称密码算法** **DES：分组加密算法，分组长度64比特，密钥长度56比特，**延伸算法**3DES。** **IDEA：分组加密算法，分组长度64比特，密钥长度128比特** **AES**：分组长度至少128 比特，密钥长度至少为128、192和256比特。 **（2）非对称算法：** **RSA：基于大整数因子分解的困难性，素数p和q足够大，n长度至少应为1024比特，RSA算法过程很重要。** **（3）国密算法：** **SM1 分组密码算法（分组长度128bit）、SM2椭圆曲线公钥密码算法、SM3密码杂凑算法（杂凑长度256bit）、SM4分组算法（分组长度128bit）、SM9标识密码算法。**

1.3 基础类-密码学理论

主要内容	关键点
Hash函数	**定义：将任意长度的信息转换成固定长度的哈希值；** **条件：**输入是任意长度， 输出为固定位数，给定M计算hash很容易，给定M1和M2，hash值相同在计算上不可行。 **作用：保护消息完整性，也能用作密码信息的安全存储。** **算法：MD5（hash值128bit）、SHA(hash值256bit)、SM3(国密， 分组长度512bit， hash值256bit)。**
数字签名	**定义：签名者使用私钥对待签名数据的杂凑值做密码运算，结果只能用签名者的公钥进行验证。** **条件：不可否认、真实性、可鉴别。** **组成：签名算法（保密）、验签算法（公开）** **对比加密：相同之处（非对称密钥进行加解密）、不同之处（加密保障机密性、签名保障完整性和真实性）。**
数字证书	**定义：也称公钥证书，**是**由证书认证机构（CA）签名**的包含**公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息**的一种数据结构。 **基本信息：版本号、序列号、签名算法、颁发者、有效期、主体及主体公钥信息、颁发者及主体的密钥标识符。**
安全协议	**密钥交换协议：Differ-Hellman，基于求解离散对数问题的困难性。** **SSH协议：基于公钥的安全应用协议**，由**SSH传输层协议、SSH用户认证协议**和**SSH连接协议**组成，实现加密、认证、完整性检查等服务，服务端口：22。
应用	**身份鉴别：数字证书（用户实体与密码绑定）、双向身份鉴别、密码安全认证对登录设备用户进行身份鉴别等。** **加密技术：保护敏感信息、SSH和SSL建立设备远程管理安全通道，保证机密性和完整性。** **完整性保护：hash函数及数字签名保证完整性。** **口令管理：MD5对口令进行hash计算。　　远程安全访问：SSH替换Telnet。** **MD5-HMAC进行路由器路由信息认证；　　电子邮件安全加密：PGP。**

1.4 基础类-网络安全体系及模型

主要内容	关键点
体系特征	整体性、协同性、过程性、全面性、适应性。
安全模型	**BLP机密性模型：防止非授权信息的扩散。** **简单安全特性**（主体的安全级别不小于客体的安全级别，主体的范畴集合包含客体的全部范畴，**主体只能向下读，不能向上读**） ***特性**（客体的保密级别不小于主体的保密级别，客体的范畴集合包含主体的全部范畴，**主体只能向上写，不能向下写**）。 **安全级：公开<秘密<机密<绝密；　范畴集**：包含、被包含或无关。 **在一个访问类中，仅有单一的安全级，而范畴可以包含多个。**
	BiBa完整性模型：防止非授权修改系统信息。 **简单安全特性**（主体的完整性级别不小于客体的完整性级别，主体的范畴集合包含客体的全部范畴，即**主体不能向下读。**） ***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。**） **调用特性**（主体的完整性级别小于另一个主体的完整性级别，不能调用另一个主体。）
	信息流模型：根据两个客体的安全属性控制从一个客体到另一个客体的信息传输，用于分析系统的隐蔽通道，防止敏感信息通过隐蔽通道泄露。
	信息保障模型：PDRR（保护、检测、恢复、响应）； **P2DR（策略、防护、检测、响应）；WPDRRC（预警、保护、检测、响应、恢复、反击）。**
	能力成熟度模型（CMM）： **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），级别越大，能力成熟度越高。** 主要有SSE-CMM(系统安全工程能力成熟度模型)、数据安全能力成熟度模型、软件安全能力成熟度模型。
	其他模型：纵深防御模型（四道防线：安全保护、安全监测、实时响应、恢复）、**分层防护模型**（以OSI为参考，层次化保护）、 **等级保护模型**（根据网络信息系统重要程度划分不同安全等级）、**网络生存模型**（3R策略：抵抗、识别、恢复）。

1.4 基础类-网络安全体系及模型

主要内容	关键点
网络安全原则	**系统性和动态性原则（木桶原则）；纵深防护与协作性原则；网络安全风险和分级保护原则；标准化与一致性原则；技术与管理相结合原则；安全第一，预防为主原则；安全与发展同步，业务与安全等同；人机物融合和产业发展原则。**
网络安全策略	应包含的内容：涉及范围、有效期、所有者、责任、参考文件、策略主体内容、复查、违规处理。
网络安全体系	网络安全法律法规、网络安全策略、网络安全组织、网络安全管理、网络安全基础设施及网络安全服务、网络安全技术、网络信息科技与产业生态、网络安全教育与培训、网络安全标准与规范、网络安全运营与应急响应、网络安全投入与建设。 **网络安全组织：领导层、管理层**（安全负责人和中层管理人员）、**执行层**（业务人员、技术人员、系统管理员）**以及外部协作层**（组织外的安全专家或合作伙伴）。 **网络安全管理：**管理目标、管理手段、管理主体、管理依据、管理资源， 人员工作安排应遵循的原则：**多人负责原则、任期有限原则、职责分离原则。** **网络安全基础设施：**包括**网络安全数字认证服务中心、网络安全运营中心、网络安全测评认证中心。** **网络安全技术：**核心目标是**自主可控、安全可信，网络安全技术类型：保护类技术、监测类技术、恢复类技术、响应类技术。** **网络安全机构：ISO**、NIST、**OWASP**、PCI、MITRE； **网络安全标准规范：RFC、DES、MD5、AES、OWASP TOP10、PCI-DSS、CVE、CVSS。**
等保2.0	**五个阶段：定级、备案、建设整改、等级测评、监督检查。** **五个等级：第一级（用户自主保护级）、第二级（系统保护审计级）、第三级（安全标记保护级）、第四级（结构化保护级）、第五级（访问验证保护级）。** **主要变化：扩大了对象范围（云计算、移动互联、物联网、工业控制系统）、三重防护体系架构、可信计算技术使用的要求。**

2.1 技术类-物理与环境安全

主要内容	关键点
物理安全概念	**威胁：自然（地震、洪水、火灾、鼠害）、人为（盗窃、爆炸、破坏、硬件攻击**（隐蔽、危害性、主动、非临近。 方法：木马、恶意代码、漏洞、环境）**）。** **措施：设备**（防电磁泄露干扰、电源保护、供应链安全、智能设备软件可信性）**、环境**（场地、屏蔽、防火等）**、系统**（存储介质安全、灾备、物理设备访问）**。** **规范：**《计算机场地通用规范》、《计算机场地安全要求》、**《信息系统物理安全技术要求（GB/T21052—2007）》等。**
具体防护措施	**防火**（消除隐患、设置报警、灭火设备（**水、二氧化碳、固态化学品和卤代烷 1211或1301**）、加强管理）； **防水、防震、防盗、防虫害、防雷、防电磁、防静电、安全供电**（专用线路、不间断供电UPS、备用发电机）。
机房安全	**机房功能区：主要工作房间**（主机房）**、第一类辅助**（配电/空调室/监控）**、第二类辅助**（资料室/维修室/办公室）**、第三类辅助**（储藏室/缓冲间/休息室）。 **机房安全等级：A级**（中断后有**严重损害、有严格的要求及完善的措施**）**、B级**（有**较大损害**、有**较严格要求、较完善的措施**）**、C级（有基本的要求和措施）。** **场地选择：环境安全、地质可靠、抗电磁干扰、避开强振动源和噪声源、避免设在高层以及用水设备的下层或隔壁（专用建筑物、二层为宜）。**
	数据中心：为实现对数据信息的集中处理、存储、传输、交换、管理以及为相关电子信息设备运行提供运行环境的建筑场所。 **要求：**所有设备的金属外壳、管道、线槽必须**等电位联结并接地等电位联结并接地。** **超大型：机架数>10000， 因素（气候环境、能源供给、灾备）、 选址（气候寒冷、能源充足的一类地区建设或**气候适宜，能源充足的**二类地区建设）。** **大型：机架数 [3000，10000）、因素（气候环境、能源供给）、选址（优先一类及二类，或者气候适宜、靠近能源富集**地区的**三类地区**建设 **）。** **中小型：机架数＜3000，因素（市场需求、能源供给，实时应用为主），选址（靠近用户所在地、能源获取便利**的地区建设，依市场需求灵活部署）。
	互联网数据中心（IDC）：向用户提供资源出租基本业务和有关附加业务、在线提供IT应用平台能力租用服务和应用软件租用服务的数据中心。 **组成：机房基础设施、网络系统、资源系统、业务系统、管理系统**和**安全系统。** **分级：R1(基础设施和网络系统的主要部分具备冗余能力,可用性不小于99.5%)、R2(冗余能力、可用性不小于99.9%)、R3(具备容错能力，不小于99.99%)。** **要求：**抗震设防烈度7度以上（含7度）地区IDC工程中使用的主要电信设备必须经电信设备抗震性能检测合格。
	CA机房：具备屏蔽、消防、物理访问控制、入侵检测报警等措施，**每五年进行一次屏蔽室检测**； **人员佩戴身份证明、人员进出留记录、人员访问制度、设备处理前检测敏感数据，并**对敏感数据应物理销毁或进行安全覆盖

2.1 技术类-物理与环境安全

主要内容	关键点
通信线路及设备安全	**网络通信线路安全防护：** **威胁：线路被切断、电磁干扰及泄露；** **措施：设备冗余**（备份）、**多路通信**（DDN专线/电话线）。
	设备硬件防护：硬件木马监测、硬件漏洞处理。 **硬件木马监测：反向分析**（使用逆向及分析软件重构电路图，与原始设计比较）、**功耗分析**（提取芯片功耗特征，进行比较）、**侧信道分析**（对比物理特性和旁路信息，技术原理是任何硬件电路的改变都会反映在一些电路参数上，如功率、时序、电磁、热等）。 **硬件漏洞处理：硬件漏洞的修补具有不可逆性，通常方法破坏漏洞利用条件。**
	存储介质安全： **威胁：**管理失控、数据泄密、设备故障、数据非安全删除、恶意代码。 **措施：强化存储安全管理**（专门区域存放、专人保管、借用审批、分类存放、删除敏感数据）、**数据存储加密保存**（加密文件系统）、**容错容灾存储技术**（磁盘阵列、双机热备、离线备份）。

2.2 技术类-认证

主要内容	关键点
基本知识	**概念：一个实体向另外一个实体证明其所声称的身份的过程。 包含声称者和验证者。** **组成：标识(确保实体唯一性和可辨识性，名称和标识符ID表示)、鉴别（利用凭证进行验证，如口令、电子签名、数字证书、令牌、生物特征、行为表现等）。** **依据：秘密信息（口令、验证码）、实物凭证**（智能卡、U盾）、**生物特征**（指纹、人脸、虹膜、声音）、**行为特征**（鼠标使用习惯、键盘敲击力度）。 **分类**：按凭据数量（**单因素、双因素、多因素**）、按时间长度（**一次性口令OTP、持续认证**）。 **相关法律**：电子签名法、网络安全法。
认证过程	**单向认证：验证者对声称者进行单方面的鉴别。** **方法一：基于共享密钥：A向B发送共享密钥及标识，B进行验证； 方法二：基于挑战响应， 挑战响应的认证步骤。** **双向认证：参与认证的实体双方互为验证者。** **第三方认证：通过可信的第三方TTP实现， 挑战响应认证步骤。**
认证技术	**1. 口令认证：优点（简单、易于实现）、缺点（容易受到攻击）、条件（口令安全加密存储、安全传输、口令协议、避免弱口令、口令设置符合安全规则）。**
	2. 智能卡技术：根据用户拥有的实物进行认证。 利用智能卡认证的挑战响应过程。
	3. 生物特征认证：指纹（采集、处理、登记、比对）、**人脸**（采集、处理、存储、识别）、**虹膜**（图像采集、处理分析、虹膜登记等）、**声音。**
	4. Kerberos认证： **原理（利用对称密码技术，使用可信的第三方来为应用服务器提供认证服务，并在用户和服务器之间建立安全信道）** **组成（客户机、AS、TGS、应用服务器）、流程、优点（减少用户密钥的密文的暴露次数、具有单点登录优点 ）、缺点（节点时间同步、抵御Dos）。**
	5. 其他：快速在线认证（FIDO，使用标准公钥加密技术来提供强身份验证，私钥保留在用户端设备中，只将公钥注册到在线服务。） **PKI（CA-证书授权机构，进行证书颁发、废止和更新，认证机构负责签发、管理和撤销一组终端用户的证书。RA、终端实体、客户端、服务器）；** **单点登录（SSO， 访问使用不同的系统时，只需要进行一次身份认证， 解决了登录不同系统都需要输口令的问题）。** **人机识别：利用计算机求解问题的困难性以区分计算机和人的操作， 主要技术：CAPTCHA技术** **基于行为的身份鉴别：根据用户行为和风险大小判断；** **多因素认证：多种鉴别信息进行组合，以提升认证的安全强度。**

2.2 技术类-认证

主要内容	关键点
主要产品	**系统安全增强（**多因素认证：口令+U盾、生物+口令等**）；生物认证（**人脸识别门禁、指纹U盘**）；电子认证（**数字证书、可信网络身份、SSL证书等**）；**网络准入控制（**VPN**）、身份认证网关（**单点登录、安全审计、数字证书、数据同步等**）。**
技术指标	**密码算法支持、 认证准确性、用户支持数量、安全保障级别。**
应用场景	**场景：用户身份识别、信息来源证实、信息安全保护。** 校园信任体系：统一认证平台； 网络路由认证：用户认证、路由器邻居认证（消息摘要认证） 人脸识别门禁； 网络身份电子标识（eID） HTTP认证：账号口令等。

2.3 技术类-访问控制

主要内容	关键点
基本知识	**概念：对资源对象的访问者授权、控制的方法及运行机制。** **目标：防止非法用户进入系统，禁止合法用户的越权访问。** **组成：主体、客体、参考监视器、访问控制数据库、审计库。**
访问控制类型	**1. 自主访问控制DAC**：客体的所有者按照自己的安全策略授予系统中的其他用户对其的访问权。 **分类：基于行的自主访问控制**（能力表、前缀表、口令）**、基于列的自主访问控制**（保护位、**访问控制表ACL**）**。** **特点：自行设置访问控制权限，简单、灵活，但依赖于用户的安全意识和技能，不能满足高安全等级的安全要求。**
	2. 强制访问控制MAC：系统根据主体和客体的安全属性，以强制方式控制主体对客体的访问。 **举例**：当且仅当进程的安全级别不小于客体的安全级别，并且进程的范畴包含文件的范畴时，进程才能访问客体，否则就拒绝。 **特点：常用于政府部门、军事和金融等领域，将系统中的资源划分安全等级和不同类别，然后进行安全管理。**
	3. 基于角色的访问控制RBAC：根据完成某些职责任务所需要的访问权限来进行授权和管理。 **组成：用户（U）、角色（R）、会话（S）、权限（P）。**一个角色可有多个权限，而一个权限也可赋予多个角色；一个用户可以扮演多个角色，一个角色也可以由多个用户承担。 **方法：权限赋予相应的角色，然后把角色映射到承担不同工作职责的用户身上。** **特点：强大、灵活**，适用于许多类型的用户需求。
	4. 基于属性的访问控制ABAC：根据主体的属性、客体的属性、环境的条件以及**访问策略对主体的请求操作**进行授权许可或拒绝。
安全管理	**访问控制过程**：明确资产、分析安全需求、制定访问控制策略、实现策略、运行及维护。 **最小特权管理：系统中每一个主体只能拥有完成任务所必要的权限集，按需使用（Need to Use），防止特权乱用。** **用户访问管理**：用户登记、用户权限分配、访问记录、权限监测、权限取消、撤销用户。 **口令安全管理：至少在8个字符以上**，应选用**大小写字母、数字、特殊字符组合；限制账号登录次数，建议为3次；口令文件加密存放**，并**只有超级用户才能读取；**禁止以明文形式在网络上传递口令；口令应有时效性；禁止共享账号和口令等。

2.3 技术类-访问控制

主要内容	关键点
产品及指标	**主要产品：4A系统（认证（Authentication）、授权（Authorization）、账号（Account）、审计（Audit））、安全网关、系统安全增强。** **技术指标：**策略规则类型、规则最大数量、规则检查速度、自身安全和质量保障级别。
技术应用	**应用场景：物理访问控制**（证件、门禁）、**网络**（接入控制、通信连接、区域划分、路由控制）、**操作系统**（文件读写、进程、内存控制）、**数据库**（表创建、生成及分发）、**应用系统**（业务执行的操作、业务文件读取）。
	UNIX/Linux系统：9比特位模式， owner、group、other； 读、写、执行。
	Windows系统：自主访问控制列表（DACL），标明谁有权访问； **系统访问控制列表（SACL）**，标明哪些主体的访问需要被记录。
	IIS FTP服务器：用户账号认证、匿名访问控制以及 **IP地址限制。**
	Web服务：多种控制环节（路由器、防火墙、口令认证、操作系统、数据库、服务器基于限定IP地址/网段/域名）。

2.4 技术类-防火墙

主要内容	关键点
基本知识	**概念：** 防火墙一般安装在不同安全区域（公共区域、内联网、外联网、**DMZ**）边界处，用于网络通信安全控制，由专用硬件或软件系统组成。 **工作原理：常部署于内外部之间，安全策略采用白名单或黑名单策略。** **主要功能：**过滤非安全网络访问、审计、带宽控制、协同防御。 **风险：旁路问题、功能缺陷（**不能完全防止感染病毒的软件、文件传输、后门**）、单点故障、无法有效防范内部威胁、受限于安全规则。**
实现技术	**1. 包过滤技术：IP层实现技术，**根据**包的源IP地址、目的IP地址、源端口、目的端口及包传递方向**等包头信息判断是否允许包通过。 **过滤规则：规则号、匹配条件（源IP地址、目的IP地址、源端口号、目的端口号、协议类型（UDP等）、通信方向、规则运算符）、匹配操作（拒绝、允许、审计）** **特点：**低负载、高通过率、对用户透明，但不能在用户级别进行过滤。
	2.状态检查：利用 TCP会话和UDP"伪"会话的状态信息进行网络访问机制，符合条件及关联性才可通过。
	3.应用服务代理：受保护网络的内部网主机和外部网主机的网络通信连接"**中间人**"的角色。 **分类：FTP代理、Telnet代理、Http代理、Socket代理、邮件代理等。** **组成：**按应用分类的代理服务程序和身份验证服务程序。 **特点：不允许**外部主机**直接访问内部主机；**多种认证方案；可分析数据包内部命令；提供详细的审计记录，但**速度慢、不透明，不支持所有协议。**
	4.网络地址转换NAT：解决公开地址不足问题，透明地对所有内部地址作转换，使外部网络无法了解内部网络的内部结构。 **原理：具有合法的公共IP地址集，当内部某一用户访问外网时，防火墙动态地从地址集中选一个未分配的地址分配给该用户。** **实现方式：静态NAT**（StaticNAT）、**NAT池**（pooledNAT）和**端口NAT**（PAT）。
	5. Web防火墙技术：根据预先定义的过滤规则和安全防护规则，对所有访问Web服务器的HTTP请求和服务器响应，进行HTTP协议和内容过滤。 **可抵御的攻击：**SQL注入攻击、XSS跨站脚本攻击、Web应用扫描、Webshell、Cookie 注入攻击、CSRF攻击。 **主要产品：**ModSecrity、WebKnight、ShadowDaemon。
	6. 数据库防火墙：数据库通信协议深度分析（源地址、目标地址、源端口、目标端口、SQL语句等**）、虚拟补丁**（安全屏障层，阻止可疑会话）。 **7. 工控防火墙：侧重于分析工控协议。** **8. 下一代防火墙：**应用识别和控制、可应对安全威胁演变、检测隐藏的网络活动、动态快速响应攻击、支持统一安全策略部署、智能化安全管理等新功能。 **9. 深度包检测DPI：运用模式（特征）匹配、协议异常检测等方法对包的数据内容进行分析。**

2.4 技术类-防火墙

主要内容	关键点
技术指标	**安全功能要求、性能要求**（最大吞吐量、最大连接速率、最大规则数、并发数）、**安全保障要求、环境适应性要求**
防御体系结构	**1. 基于双宿主主机防火墙：至少具有两个网络接口卡的主机系统， 内外连接不同网卡。**
	2. 基于代理型防火墙：一台主机同外部网连接，该**主机代理内部网和外部网的通信，由代理服务器和过滤路由器组成，代理主机位于内部。**
	3. 基于屏蔽子网的防火墙：代理型结构中**增加一层周边网络的安全机制，使内部网络和外部网络有两层隔离带。**应用代理位于被屏蔽子网中。 **特点：安全级别最高，但成本高、配置复杂。**
应用	**应用场景：**上网、网站保护、数据保护、网络边界保护等。 **部署**：划分安全区域、设置控制点、制定边界策略、采用合适的防火墙结构、配置策略、测试验证、运行维护。 **iptables：Linux系统自带的防火墙**，支持数据包过滤、数据包转发、地址转换、基于MAC 地址的过滤、基于状态的过滤、包速率限制等功能。 **Web应用防火墙：WAF。**

2.5 技术类-VPN

主要内容	关键点
基本知识	**概念：** 在公共的物理网络上**通过逻辑方式构造出来的安全网络，把需要经过公共网传递的报文（packet）加密处理后，再由公共网络发送到目的地，在不可信任的公共网络上构建一条专用的安全通道，经过VPN 传输的数据在公共网上具有保密性。** **功能：保密性、完整性、认证。** **类型：链路层VPN、网络层VPN、传输层VPN。**
实现技术	**1. 密码算法：支持国际及国产密码算法。** **2. 密钥管理：手工配置、密钥交换协议自动分发（密钥交换管理标准SKIP和ISAKMP/Oakley）。** **3. 认证：用户身份认证、数据完整性和合法性认证。**
	4. IPSec：包含认证头（简称AH）、封装安全有效负荷（简称 ESP）以及密钥交换协议。 **AH：保证IP包的完整性和提供数据源认证，为IP数据报文提供无连接的完整性、数据源鉴别和抗重放攻击服务。** **ESP：保证IP包的保密性。** **工作模式：透明模式（只保护IP包中的数据域）、隧道模式（创建新的IP包头，并把旧的IP包作为新的IP包数据，从而保护IP包的包头和数据域）。**
	5. SSL：介于应用层和TCP层之间的安全通信协议。其主要目的在于两个应用层之间相互通信时，使被传送的信息具有保密性及可靠性。 **组成：握手协议、密码规格变更协议、报警协议和记录层协议。** **分层：SSL协议是一个分层协议，最底层协议为SSL 记录协议，位于传输层（如TCP）之上；另一层协议为SSL握手协议，**由3种协议组合而成。 **功能及服务：保密性通信、点对点身份认证、可靠性服务。**
	6. PPTP：点到点安全隧道协议，给电话上网的用户提供VPN安全服务，它是是PPP协议的一种扩展。 **7. L2TP：**用于保护设置L2TP-enabled的客户端和服务器的通信，采用**专用隧道协议，运行在**UDP的1701 端口。
产品及应用	**主要产品：商业（IPSec VPN、SSL VPN，或者集成 IPSec、SSL 安全功能的防火墙和路由器）、开源（StrongSwan、OpenSwan、OpenSSL）** **技术指标：**密码算法、功能、性能。 **应用场景：远程访问虚拟网（Access VPN，**解决远程用户安全办公问题）、 **企业内部虚拟网（IntranetVPN，**把分散在不同地理区域的企业办公点的局域网安全互联起来，实现内部安全共享和企业办公自动化）、 **企业扩展虚拟网（Extranet VPN，**把合作伙伴的网络或主机安全接到企业内部网，以方便企业与合作伙伴共享信息和服务）。

2.6 技术类-入侵检测IDS

主要内容	关键点
基本知识	**概念：** 通过收集操作系统、系统程序、应用程序、网络包等信息，**发现系统中违背安全策略或危及系统安全的行为。** **模型：CIDF，**由**事件产生器、事件分析器、响应单元**和**事件数据库**组成。
技术	**1. 基于误用的入侵检测技术（**又叫基于特征的入侵检测方法**）：根据已知的入侵模式检测入侵行为，误用入侵检测依赖于攻击模式库。** **前提条件：**入侵行为能够按某种方式进行特征编码，检测过程实际上就是模式匹配的过程。 **常用方法：基于条件概率、基于状态转移、基于键盘监控、基于规则（Snort）。**
	2. 基于异常的入侵检测技术：建立系统正常行为"轨迹"，定义正常情况的数值，然后**将系统运行时的数值与"正常"情况相比较**，得出是否有被攻击迹象。 **常用方法：基于统计的异常检测、基于模式预测、基于文本分类、基于贝叶斯推理。**
	3. 其他技术：基于规范、生物免疫、攻击诱骗、入侵报警、沙箱动态分析、大数据分析的入侵检测方法
组成及分类	**组成：数据采集模块、入侵分析引擎模块、应急处理模块、管理配置模块**和相关的**辅助模块。** **分类：基于主机的入侵检测系统（简称HIDS）、基于网络的入侵检测系统（简称 NIDS）、分布式入侵检测系统（简称 DIDS）。**
	1. 基于主机的入侵检测系统HIDS：收集主机系统的日志文件、系统调用、应用程序使用等信息，分析是否包含攻击特征或异常，来判断是否受到入侵。 **常用软件：SWATCH（监视日志）、Tripwire（文件目录完整性检测）、网页防篡改系统。** **优缺点：**可以运行在应用加密系统的网络上及交换网络中，但每个主机都需安全和维护，占用主机资源和性能，不能有效检测所有网络扫描。
	2. 基于网络的入侵检测系统（简称 NIDS）：通过**侦听网络系统，捕获网络数据包**，并依据网络包是否包含攻击特征，或网络通信流是否异常来识别入侵。 **常用软件：开源的网络入侵检测系统 Snort（**轻量型的NIDS，通过 libpcap软件包监听，基于规则的审计分析，进行包的数据内容搜索/匹配**）** **优缺点：**对网络影响小，属于被动型设备，但针对加密的网络流量，无法有效检测。
	3. 分布式入侵检测系统（简称 DIDS）：能够将基于主机和网络的系统结构结合起来，检测所用到的数据源丰富，可以克服前两者的弱点。 **基于主机检测的分布式入侵检测系统HDIDS：由主机探测器和入侵管理控制器组成，多以安全代理（Agent）形式直接安装在主机系统上。** **基于网络的分布式入侵检测系统NDIDS：由网络探测器**和**管理控制器组成，**适用于大规模网络或者是地理区域分散的网络。

2.6 技术类-入侵检测IDS

主要内容	关键点
主要产品及指标	**产品：主机入侵检测系统、网络入侵检测系统**以及**统一威胁管理**（UTM，部署在内部网络与外部网络的边界）、**高级持续威胁检测系统**（基于静态/动态分析检测可疑恶意电子文件及关联分析网络安全大数据）。 **指标：可靠性、可用性、可扩展性、时效性、准确性**和**安全性。**
应用	**应用场景：**上网保护、入侵检测、阻断、监测、应急响应、等级保护。
	部署：确定对象和网段、安装IDS探测器、制定策略、IDS选型、配置规则、测试验证、运行维护。
	基于HIDS的主机检测：一般用于检测针对单台主机的入侵行为 **基于 NIDS的内网检测：将网络IDS的探测器接在内部网的广播式Hub或交换机的Probe端口。** **基于 NIDS的网络边界检测：探测器接在网络边界处，采集与内部网进行通信的数据包，然后分析来自外部的入侵行为。** **网络安全态势感知：汇聚IDS报警信息、系统日志，然后利用大数据分析技术对网络系统的安全状况进行分析。**

3.1 网络防护类-物理隔离

主要内容	关键点
基本知识	**概念：** **避免两台计算机之间直接的信息交换以及物理上的连通，以阻断两台计算机之间的直接在线网络攻击。** **风险：** **U盘摆渡、网站非法外联。** **类型：** 按隔离对象，**单点物理隔离、区域物理隔离；** 按信息传递方向，**双向网络物理隔离系统、单向网络物理隔离系统。**
实现技术	**专用计算机、多PC、外网代理、内外网线路切换器、单硬盘内外分区、双硬盘** **网闸：** **利用一种GAP技术**，使两个或者两个以上的网络在不连通的情况下，实现它们之间的安全数据交换和共享。 **网闸原理：** 使用一个具有控制功能的开关读写存储安全设备，**通过开关的设置来连接或切断两个独立主机系统的数据交换。** **协议隔离：通过协议转换的手段保证受保护信息在逻辑上是隔离的，只有被系统要求传输的、内容受限的信息可以通过。** **单向传输部件：由一对独立的发送和接收部件构成，发送和接收部件只能以单工方式工作。** **信息摆渡：在任何时刻，中间缓存区域只与一端安全域相连。** **物理断开：处于不同安全域的网络之间不能以直接或间接的方式相连接，通常由电子开关实现。**
主要产品	**终端隔离产品（电子开关、隔离卡等）、** **网络隔离产品（2+1，两台主机+专用隔离部件，采用协议隔离/信息摆渡技术）、** **网络单向导入产品（双机方式+单向传输部件）：**
应用	**工作机安全上网：采用物理隔离卡，** 适合小规模上网用户。 **电子政务中网闸应用：**切断网络之间的通用协议连接，将数据包进行分解或重组为静态数据，然后进行安全审查、网络协议检查和代码扫描等，通过身份认证机制获取所需数据。

3.2 网络防护类-安全审计

主要内容	关键点
基本知识	**概念：** 对网络信息系统的安全相关活动信息进行**获取、记录、存储、分析**和**利用**的工作。 **作用：** **安全事件的采集、存储和查询，属于"事后"安全保障措施。重要的信息系统需部署独立的网络安全审计系统。** **标准及政策：国际**TCSEC、**国内**《计算机信息系统安全保护等级划分准则》，**留存相关的网络日志不少于六个月** **组成：审计信息获取、审计信息存储、审计信息分析、审计信息展示及利用、系统管理。** **类型：**按审计对象（**操作系统、数据库、网络通信、应用系统安全审计**）；按审计范围（**综合审计系统、单个审计系统**）。 **机制：基于主机、基于网络通信、基于应用的审计机制。**
实现技术	**1.系统日志数据采集：**事件信息汇聚到统一的服务器存储，以便于查询分析与管理，**常见方式：SysLog、SNMPTrap；** **2.网络流量数据获取：共享网络监听（**集线器**）、交换机端口镜像、网络分流器、网络流量采集设备（Linux（**Libpcap、 Tcpdump**）、Windows（**Winpcap、 Windump**）、Wireshark）。** **3. 网络审计数据安全分析：字符串匹配（grep）、全文搜索(Elasticsearch)、数据关联、统计报表、可视化分析；** **4. 网络审计数据存储及保护：分散存储（**存储于不同系统中**）、集中存储（**专用存储设备**）。** **系统用户分权管理、审计数据强制访问、加密、隐私保护、完整性保护。**
主要产品	**1. 日志安全审计产品：**利用Syslog、Snmptrap、NetFlow、Telnet、SSH、FTP等技术，**对分散设备的异构系统日志进行分布采集、集中存储、统计分析、集中管理；** **2. 主机监控与审计产品：**通过**代理程序**对主机的行为信息进行采集。 **3. 数据库审计产品：**通过网络流量监听、系统调用监控、数据库代理等对所有访问数据库系统的行为信息进行采集。**实现方式：网络监听审计、自带审计、数据库Agent。** **4. 网络安全审计产品：**通过网络流量信息采集及数据包深度内容分析，**主要功能：网络流量采集、网络流量数据挖掘分析。** **5. 工控系统审计产品：**利用网络流量采集及协议识别技术，对工业控制协议进行还原，形成工业控制系统的操作信息记录。**实现方式：一体化集中产品、采集端+分析端。** **6. 运维安全审计产品：**通过网络流量信息采集或服务代理等技术方式，记录Telnet、FTP、SSH等操作。**功能：字符会话、图形操作、数据库运维、文件传输、合规审计。**
应用	**安全运维保障、数据访问监测、网络入侵检测、网络电子取证。**

3.3 网络防护类-漏洞防护

主要内容	关键点
基本知识	**概念：** 漏洞一般是致使网络信息系统安全策略相冲突的缺陷。 **分类：** **普通漏洞（**漏洞信息已经广泛公开，安全厂商已经有了解决修补方案**）、零日漏洞（**系统或软件中新发现的、尚未提供补丁的漏洞，常被用来实施定向攻击**）。** **威胁：**威胁主体利用漏洞（脆弱性）实现攻击，主要威胁有：**敏感信息泄露、非授权访问、身份假冒、拒绝服务。** **标准及规范：国际（CVE、CVSS、NVD）、国内（CNNVD、CNVD）。** **CVE：美国，**通用漏洞披露，用来统一规范漏洞命名 **CVSS：通用漏洞计分系统，**分数组成**（基本度量计分、时序度量计分、环境度量计分）。** **CNNVD：国家信息安全漏洞库；　CNVD：国家信息安全漏洞共享平台。** **OWASP TOP 10：**Web 应用程序的前十种安全漏洞。 **来源：非技术性漏洞（**组织结构、管理制度、管理流程、人员等**）、技术性漏洞（**网络结构、通信协议、设备、软件产品、系统配置、应用系统**）。**
基本环节	**1. 漏洞发布：发布者（**软硬件开发商、安全组织、黑客或用户**）、发布方式（**网站/邮件/论坛**）、公布内容（漏洞编号、发布日期、安全危害级别、漏洞名称、漏洞影响平台、漏洞解决建议）。** **2. 漏洞信息获取：**网络安全应急响应机构（CERT）；网络安全厂商；IT产品或系统提供商；网络安全组织。 **3. 漏洞管理过程：**系统资产确认、漏洞信息采集、评估、消除和控制、变化跟踪。 **4. 漏洞扫描器：**检测系统中漏洞的技术。 **组成：用户界面、扫描引擎、漏洞扫描结果分析、漏洞信息及配置参数库。** **分类：主机漏洞扫描器（不需要通过建立网络连接就可以进行，只能单机检测，工具：COPS(UNIX)、Tiger(UNIX)、MBSA（windows）。** **网络漏洞扫描器（远程连接后，远程联网检查，工具：Nmap**（端口扫描）、**Nessus**（漏洞扫描）、**X-scan**（windows漏洞扫描））。 **专用漏洞扫描器：**数据库、网络设备、Web、工控。
应用及处置	**应用：常用于网络信息系统安全检查和风险评估。** **漏洞处置：网络安全漏洞发现技术（**人工安全性分析、工具自动化检测及人工智能辅助分析**）、网络安全漏洞修补技术（**现状分析、补丁跟踪、补丁验证、补丁安装、应急处理和补丁检查**）、网络安全漏洞利用防范技术（**地址空间随机化技术、数据执行阻止、SEHOP、堆栈保护、虚拟补丁**）。**
主要产品	**1. 漏洞扫描器：**利用已公开的漏洞信息及特征，通过程序对目标系统进行自动化分析，以确认目标系统是否存在相应的安全漏洞。商业（IBMRationalAppScan、Qualys、Shadow Security Scanner）、开源（**Nessus、OpenVAS、Nmap**）。 **技术指标（主机数量/并发数/扫描速度及能力、口令检查）。** **2. 网络安全漏洞服务平台：漏洞盒子、补天漏洞响应平台等；** **3. 网络安全漏洞防护网关：从网络流量中提取和识别漏洞利用特征模式，如IPS、 WAF、UTM。**

3.4 网络防护类-恶意代码防范

主要内容	关键点
基本知识	**概念：** 违背目标系统安全策略的程序代码，会造成目标系统信息泄露、资源滥用，破坏系统的完整性及可用性。 **分类：** **被动传播（计算机病毒、木马、间谍软件、逻辑炸弹）、主动传播（蠕虫、其他）。** **攻击过程：侵入、提权、隐蔽、潜伏、破坏。** **生存技术：反跟踪、加密、模糊变换、自动生产、变形等。** **攻击方式：进程注入、超级管理、端口反向连接、缓冲区溢出。** **分析方法：静态（**反恶意代码软件的检测和分析、字符串、脚本、反编译、静态反汇编分析**）、动态（**文件、进程、网络、注册表监测、动态反汇编分析**）。**
详细类型	**1. 计算机病毒：** **定义（自我复制、传播能力的程序代码）、特征（隐蔽性、传染性、潜伏性、破坏性）、组成（复制传染部件、隐藏部件、破坏部件）。** **运行机制（2个阶段，复制传播阶段、激活阶段）、 常见类型（引导性病毒、宏病毒、多态病毒、隐蔽病毒）。** **防范技术（查找病毒源、阻断途径、主动查杀、应急响应和灾备）、防护方案（单机、网络、网络分级、邮件网关）。**
	2. 特洛伊木马：具有**伪装能力、隐蔽执行**非法功能的恶意程序，伪装成合法程序或文件，植入系统。 **分类：本地特洛伊木马（**只运行在本地单台主机**）、网络特洛伊木马（远程木马控制管理、木马代理）。** **运行机制：寻找目标、收集信息、植入、隐藏、攻击。** **植入方法：被动植入（**需人工干预**）、主动植入（**程序自动执行**）。** **隐藏方法：本地活动隐藏、远程通信过程隐藏。** **防范方法：查看开放端口、重要文件检测、网络监测、网络阻断。**
	3. 蠕虫：自我复制和传播能力、可独立自动运行的恶意程序。 **组成：探测模块、传播模块、蠕虫引擎模块、负载模块。** **运行机制：3个阶段（**易感染主机在网络上搜索易感染目标主机、把蠕虫代码传送到易感染目标主机上、执行代码**）** **蠕虫扫描方法：随机扫描、顺序扫描、选择性扫描。** **防范：监测预警、抑制传播、免疫、阻断隔离、清除。**
	4. 僵尸网络：利用入侵手段将僵尸程序（bot or zombie）植入目标计算机上，进而操纵受害机执行恶意活动的网络。 **运行机制：僵尸程序的传播、 命令操作组成网络、发送命令执行攻击。** **5. 其他：逻辑炸弹、陷门、细菌、间谍软件。**
产品及指标	**主要产品：终端防护、安全网关、恶意代码监测等；　技术指标：恶意代码检测能力、恶意代码检测准确性、恶意代码阻断能力。**

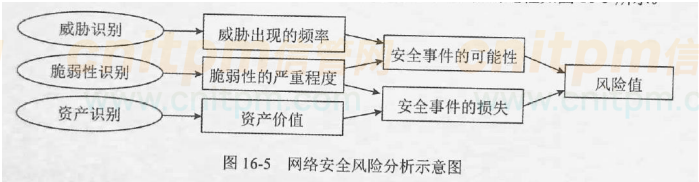
3.5 网络防护类-主动防御

主要内容	关键点
入侵阻断	**概念：** 入侵防御系统IPS，**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。** **实现方法： 1.基于ASIC 来实现 IPS。 2. 基于旁路阻断（SPS）来实现。** **作用：**过滤掉有害的网络信息流，阻断入侵者对目标的攻击行为。
软件白名单	**概念：限制非授权安装软件包，阻止系统非授权修改，避免恶意代码植入目标对象。** **原理：设置可信任的软件名单列表，以阻止恶意的软件在相关的网络信息系统运行。** **应用：构建可信网络生态、恶意代码防护、白环境保护（只有可信任的设备才能接入控制网络；只有可信任的消息才能在网络上传输；只有可信任的软件才允许被执行）。**
网络流量清洗	**概念：将原本发送给目标设备系统的流量牵引到流量清洗中心，**当**异常流量清洗完毕后，**再**把清洗后留存的正常流量转送到目标设备系统。** **方法：流量检测、流量牵引和清洗（**牵引方法：BGP、DNS**）、流量回注。** **应用：畸形数据报文过滤、抗DDOS、 Web应用保护、DDOS高防IP服务。**
可信计算技术	**原理：构建一个信任根，再建立一条信任链，从信任根开始到硬件平台，到操作系统，再到应用，一级认证一级，一级信任一级，把这种信任扩展到整个计算机系统，从而确保整个计算机系统的可信。** **组成：可信根（**TPM，包含三个根：可信度量根RTM、可信存储根RTS、可信报告根RTR**）、可信硬件平台、可信操作系统、可信应用系统。** **可信计算密码支撑平台：**以T**CM为核心**的自主可信计算标准体系，由**可信密码模块（TCM）**和**TCM服务模块（TSM）组成。** **应用：计算平台安全保护、可信网络连接、可信验证。**
数字水印技术	**概念：通过数字信号处理方法，在数字化的媒体文件中嵌入特定的标记。** **分类：可感知、不易感知。** **组成：水印嵌入**（嵌入方法：空间域、变换域）**、水印提取。** **应用：版权保护、信息隐藏、信息溯源、访问控制。**

3.5 网络防护类-主动防御

主要内容	关键点
攻击陷阱	**概念：** 网络诱骗技术，改变保护目标对象的信息，欺骗网络攻击者，从而改变网络安全防守方的被动性。 **主要技术：**蜜罐主机（空系统、镜像系统、虚拟系统）、 陷阱网络（多个蜜罐主机、路由器、防火墙、IDS、审计系统共同组成）。 **陷阱网络发展：第一代**（数据包都经过防火墙和路由器）、**第二代**（实现数据控制系统、数据捕获系统的集成系统）、**第三代**（虚拟陷阱网络，所需要的功能集中到一个物理设备中运行）。
入侵容忍与系统生存	**概念：**假定在遭受入侵的情况下，保障网络信息系统仍能按用户要求完成任务。 **方法：3R（抵抗（Resistance）、识别（Recognition）和恢复（Recovery））。** **分类：分布式共识、主动恢复、门限密码、多样性设计。** **应用：弹性CA、 区块链。**
隐私保护	**隐私分类：**身份隐私、属性隐私、社交关系隐私、位置轨迹隐私。 **保护方法：k-匿名方法（匿名化处理）、差分隐私（添加随机噪声）。**
其他	**网络威胁情报：**网络安全威胁信息共享平台。 **同态加密：一种加密函数，对明文的加法和乘法运算再加密，与加密后对密文进行相应的运算，结果是等价的。** **全同态加密体制：在不解密的条件下对加密数据进行任何可以在明文上进行的运算，从而使得对加密信息仍能进行深入和无限的分析，而不会影响其保密性。**

3.5 网络防护类-风险评估

主要内容	关键点
基本知识	**概念：** **评估威胁者利用网络资产的脆弱性，造成网络资产损失的严重程度。** **计算方法：**R=f（Ep，Ev）。其中，R表示风险值，Ep表示安全事件发生的可能性大小，Ev表示安全事件发生后的损失，即安全影响。 **评估要素：**资产、威胁、脆弱性、安全措施、风险等。 **评估模式：自评估、检查评估、委托评估。**
评估过程	**风险评估准备、资产识别、威胁识别、脆弱性识别、已有的网络安全措施分析、网络安全风险分析、网络安全风险处置与管理** **1. 评估准备：主要是确定评估对象和范围；** **2. 资产识别：网络资产鉴定、网络资产价值估算（价值估算不是资产的物理实际经济价值，而是相对价值，一般以保密性、完整性、可用性衡量，价值由资产安全属性未满足时，对资产自身及与其关联业务的影响大小来决定的）；** **3. 威胁识别：**威胁来源（自然、人为）、威胁途径、威胁意图、威胁效果（非法访问、欺骗、拒绝服务）、威胁频率； **4. 脆弱性识别：以资产为核心， 对不同环境中的相同弱点，其脆弱性的严重程度是不同的， 分为技术脆弱性评估和管理脆弱性评估。**
分析与处置	**步骤：资产识别、威胁识别、脆弱性识别、判断可能性及损失，计算风险值。** **方法：定性计算方法、定量计算方法、定性和定量综合计算方法。** **风险值计算方法：相乘法（f（x，y）=√xy）、矩阵法。** **风险处置： 为确保安全措施的有效性，一般要进行再评估，以判断实施安全措施后的风险是否已经降低到可接受的水平**  图 16-5 网络安全风险分析示意图
工具	**资产信息搜集、网络拓扑发现、漏洞扫描（**端口扫描工具，如Nmap（开源）。 通用漏洞扫描工具，如 X-Scan（开源）、绿盟极光（商用）、Nessus（开源）等。 数据库扫描，如 SQLMap（开源）、Pangolin（开源）等。Web漏洞扫描，如AppScan（商用）、Acunetix Web VulnerabiliyScanner（商用）等。 **）、渗透测试、问卷调查等。**

3.6 网络防护类-应急响应

主要内容	关键点
基本知识	**概念：** 为应对网络安全事件，相关人员或组织机构对网络安全事件进行监测、预警、分析、响应和恢复等工作。 **机构：国际（1988年，美国，**计算机安全应急组织**CERT），国内（2002年，**国家互联网应急中心CNCERT，**是中央网络安全和信息化委员会办公室领导下的国家级网络安全应急机构，主要职责：**按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展中国互联网上网络安全事件的预防、发现、预警和协调处置等工作）。 **应急响应组织：应急领导组、应急技术支撑组。** **应急响应组织类型：公益性应急响应组、内部应急响应组、商业性应急响应组、厂商应急响应组。**
网络安全事件	**分为4级：特别重大网络安全事件、重大网络安全事件、较大网络安全事件**和**一般网络安全事件.**
应急处理	**应急预案类型：国家级、区域级、行业级、部门级。管理层级高的预案偏向指导，**而**层级较低的预案侧重于网络安全事件的处置操作规程。** **处理流程：安全事件报警、安全事件确认、启动应急预案、安全事件处理、撰写安全事件报告、应急工作总结。** **应急演练：**对假定的网络安全事件出现情况进行模拟响应，分为（按组织形式：**桌面应急演练**和**实战应急演练；** 按内容：**单项应急演练和综合应急演练** 按目的：**检验性应急演练、示范性应急演练和研究性应急演练**
应急响应技术	**1. 访问控制：网络访问控制、主机访问控制、数据库访问控制、应用服务访问控制，通过防火墙、代理服务器等实现；** **2. 网络安全评估：**方法有**恶意代码检测、漏洞扫描、文件完整性检查、配置文件检查、日志审计等。** **3. 系统恢复：系统紧急启动、漏洞修补、容灾备份、文件删除恢复。** **4. 入侵取证：可作为证据的信息（**日志、文件、系统进程、用户、系统状态、网络通信连接记录、磁盘介质） **步骤：现场保护、识别证据、传输证据、保存、分析、提交。** **工具：证据获取（**ipconfig、ifconfig、netstat、lsof、date等）**、证据安全保护（**md5sum、Tripwire）**、证据分析（**grep、find、GDB）**。**

3.7 网络防护类-安全测评

主要内容	关键点
基本知识	**概念：** 参照一定的标准规范要求，通过一系列的技术和管理方法，获取评估对象的网络安全状况信息，对其给出相应的网络安全情况综合判定。
测评类型	**按测评目标：网络信息系统安全等级测评（非涉及国家秘密）、网络信息系统安全验收测评、网络信息系统安全风险测评。** **按测评内容：技术安全测评**和**管理安全测评。** **按实施方式：安全功能检测、安全管理检测、代码安全审查、渗透测试、攻击测试。** **按保密性质：涉密信息系统测评、非涉密信息系统测评。**
流程及内容	**网络信息系统安全等级测评过程：测评准备活动、方案编制活动、现场测评活动**和**报告编制活动。** **渗透测试测评过程：委托受理、准备、实施、综合评估**和**结题。**
技术及工具	**漏洞扫描：网络（**Nmap、Nessus、OpenVAS**）、主机、数据库（**THC-Hydra、SQLMap**）、Web（**w3af、Nikto、AppScan、Acunetix WVS**）。** **渗透测试：黑盒测试、白盒测试、灰盒测试， 工具：Metasploit，**字典生成器、**GDB**、Backtrack4、**Burpsuit**、OllyDbg、IDAPro等。 **代码安全审查：工具-**HPFortify、IBMRationalAppScan Source Edition 、Checkmarx、FindBugs、PMD、360代码卫士等。 **协议分析：检测协议安全性，工具- TCPDump（命令行、支持正则表达式、包含类型关键字**（host、net、port）**、传输方向关键字**（src、dst）**、协议关键字**（IP、TCP、UDP、ARP等）**。）**、Wireshark。 **性能测试：**性能监测工具（操作系统自带）、Apache JMeter（开源）、LoadRunner （商业产品）、SmartBits（商业产品）等。
管理及标准	**中国合格评定国家认可委员会（简称CNAS）**负责对认证机构、实验室和检查机构等相关单位的认可工作。 信息系统安全等级保护测评标准、产品测评标准、风险评估标准、密码应用安全、工业控制系统信息安全防护能力评估

4.1 系统及设备类-操作系统安全

主要内容	关键点
基本知识	等级：五个安全等级，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。 安全机制：硬件安全、标识与鉴别、访问控制、最小特权管理（操作系统不分配用户超过执行任务所需的权限，防止权限滥用，减少系统的安全风险）、可信路径、安全审计、系统安全增强。
Windows	系统架构：三层（硬件抽象层、内核层、由一系列实现基本系统服务的模块组成的上层）； Windows2000安全子系统组成：本地安全授权（LSA）、安全账户管理（SAM）和安全参考监视器（SRM）。 安全机制：认证机制（本地、网络）、访问控制（用户ID，DACL，SACL）、审计/日志（系统日志SysEvent.evt、应用程序日志AppEvent.evt和安全日志SecEvent.evt，在目录system32config下）、协议过滤/防火墙、文件加密系统EFS、抗攻击机制。 增强方法：安全漏洞打补丁（Patch）、停止服务和卸载软件、升级或更换程序、修改配置或权限、去除特洛伊等恶意程序、安装专用的安全工具软件。 系统启动安全增强（CMOS设置为COnly，仅允许从C盘启动）、账号口令安全（停掉 guest账号；限制不必要的用户数量；把系统Administrator账号改名；创建一个陷阱账号；设置安全复杂的口令；设置屏幕保护口令；不让系统显示上次登录的用户名；开启口令安全策略；开启账号策略。）、安装补丁等。 典型工具：远程安全登录（OpenSSH）、系统身份认证（Kerberos）、恶意代码查杀工具、系统安全检查工具（NMAP）、系统安全监测工具（Netstat）
UNIX/ Linux	系统架构：三层（硬件层、系统内核和应用层）。 安全机制：认证（口令、终端、主机、第三方）、访问控制（ACL、9bit规则）、审计（日志文件及内容，lastlog-最近成功登录时间等）。 安全分析：口令安全（口令信息保存在passwd和shadow文件中，所在的目录是/etc）；可信主机（系统提供两个文件$HOME/rhost 或/etc/hosts.equiv来配置实现可信主机的添加。）。 增强方法：打补丁、升级、改配置、安装专用工具。 增强流程：确定安全目标、安装最小化UNIXLinux系统、配置策略、第三方软件包来增强系统安全（SSH替换telnet）、测试及运行。 增强技术：安装补丁（可以用MD5Sum检查工具来判断补丁软件包的完整性）、最小化系统网络服务、开机保护口令、弱口令检查（John the Ripper）、禁用默认账号、SSH增强、tcp_wrapper 增强访问控制、构筑防火墙、使用Tripwire 或 MD5Sum 完整性检测工具、检测LKM后门、系统安全监测。

4.1 系统及设备类-操作系统安全

主要内容	关键点
Linux安全增强参考	禁止访问重要文件、禁止不必要的SUID程序、为LILO增加开机口令、设置口令最小长度和最短使用时间（文件/etc/login.defs中的参数 PASS_MINLEN\PASS_MIN_DAYS）、限制远程访问（etc/hostsallow和/etc/hosts.deny ）、用户超时注销。
Unix/Linux典型工具	• 远程安全登录管理开源工具OpenSSH； • 系统身份认证增强开源工具Kerberos； • 系统访问控制增强开源工具SELinux、iptables、TCPWrappers等； • 恶意代码查杀工具ClamAV、Chkrootkit、Rotkit Hunter等； • 系统安全检查工具Nmap、John the Ripper、OpenVAS等； • 系统安全监测工具 lsof、Netstat、Snort等。
国产操作系统	安全风险：Linux 内核安全、自主研发系统组件安全、依赖第三方系统组件的安全、安全配置、硬件安全。 安全措施：管理员分权、最小特权、结合角色的基于类型的访问控制、细粒度的自主访问控制、多级安全。 主要厂商：中科方德、中标麒麟、北京凝思科技、普华、深度Linux 、华为鸿蒙操作系统、阿里飞天云操作系统。

4.2 系统及设备类-数据库安全

主要内容	关键点
基本知识	**概念：数据库的机密性、完整性、可用性能够得到保障。** **主流系统：MS SQL、MySQL、Oracle、DB2。** **安全隐患：账号密码隐患、扩展存储、软件漏洞、权限分配、内容传递、安全意识。**
安全机制	**安全机制：标识与鉴别、访问控制、安全审计、备份恢复、数据加密、资源限制、安全加固及管理。** **1. 数据加密：传输加密（SSL）、存储加密（库内加密、库外加密）。 常用技术：基于文件、基于记录、基于字段。** **2. 数据库防火墙：**通过SQL协议分析，根据预定义的禁止和许可策略让合法的SQL操作通过，阻断非法违规操作。 **3. 数据脱敏：**将数据库中的数据进行变换处理，匿名化，放置敏感数据泄露。**技术方法（屏蔽、变形、替换、随机、加密）。**
Oracle数据库	**概念：基于SQL标准的关系型数据库。** **安全机制：用户认证、访问控制、保险库DV（**设置安全域（Realm）和命令规则（Command Rules）对特权进行控制**）、安全审计、数据库防火墙。** **实践：增强操作系统安全（**最小化服务、补丁等**）、最小化安装Oracle、安装最新补丁、删除或修改默认的用户名和密码、启用认证机制、设置好的口令密码策略、最小化权限、传输加密、审计、灾备。**
MS SQL	**概念：**基于WindowsNT结构的大型关系型数据库管理系统。 **安全措施：身份认证、访问控制、数据加密、备份恢复（4种备份、3种恢复）、安全审计。** **实践：设置策略、加强扩展存储过程管理、数据加密传输（SSL）、修改默认端口、IP访问限制、审计、灾备。**
MySql	**概念：**网络化的关系型数据库系统。 **安全措施：身份认证、访问授权、安全审计。** **实践：建立 MySQL Chrooting 运行环境、关闭远程连接、禁止 MySQL导入本地文件、修改 MySQL的 root 用户 ID和密码、更改MySQL的 root 用户名、建立应用程序独立使用数据库和用户账号。**
国产数据库	中科院信息安全国家重点实验室基于开源数据库系统PostgreSQL，研制了安全数据库管理系统LOIS SDBMS。 **LOIS SDBMS是国内第一个采用核心化体系结构的安全数据库管理系统，强制访问控制粒度达到记录级。**

4.3 系统及设备类-网络设备安全

主要内容	关键点
交换机威胁	发展：第一代（集线器，工作于物理层）、第二代（以太网交换机，工作于数据链路层）、第三代（三层交换机，工作于网络层）、第四代（新增业务功能，如防火墙、负载均衡、IPS）、第五代（支持软件定义网络（SDN），具有强大的QoS能力）。 威胁：ARP欺骗、口令威胁、MAC地址泛洪等。
路由器威胁	漏洞利用、口令安全、路由协议安全、DOS。
机制与技术	1. 认证机制：TACACS+认证（提供用户名+口令认证）、RADIUS认证（过程简单）。 2. 访问控制：分类（带外访问-不依赖其他网络、带内访问）、访问方法（控制端口（Console Port）、辅助端口（AUXPort）、VTY、HTTP、TFTP、SNMP）； 3. 信息加密：启用service password-encryption配置后，对口令明文信息进行加密保护。 4. 安全通信：SSH、 IPSecVPN。 5. 日志审计：一般是建立专用的日志服务器，并开启网络设备的Syslog 服务。 6. 安全增强：关闭非安全的网络服务及功能、信息过滤、协议认证。 7. 物理安全。
安全增强方法	交换机：1. 配置交换机访问口令和 ACL，限制安全登录； 2.利用镜像技术监测网络流量； 3. MAC地址控制技术； 路由器：1.系统升级打补丁； 2.关闭不需要的网络服务； 3. 禁止不使用的端口；4. 禁止 IP直接广播和源路由；5.传输加密；6.口令安全。
常见漏洞及解决方法	常见漏洞：DOS、CSRF、XSS、旁路、代码执行、溢出破坏。 解决方法：及时获取网络设备漏洞信息；网络设备漏洞扫描；网络设备漏洞修补。

5.1 新技术新方法-网站安全

主要内容	关键点
基本知识	**网站概念：** 基于**B/S技术架构**的综合信息服务平台，主要提供**网页信息及业务后台对外接口**服务 。 **网站安全：**有关网站的**机密性、完整性、可用性及可控性。** **威胁：非授权访问、网页篡改、数据泄露、恶意代码、网站假冒、拒绝服务、后台管理安全（**管理员身份及密码安全、网页漏洞、内部管理权限分配）。
Apache	**概念：**搭建Web服务器的开源软件。 **主要配置文件：httpd.conf（设定端口Listen、属性、身份、权限等）、conf/srm.conf(索引)、conf/access.conf（访问控制）、conf/mime.conf。** **威胁：**软件程序、软件配置、安全机制、应用程序、服务通信、服务内容、服务器拒绝服务。 **安全机制：本地文件安全**-设置的文件属主和权限（chown、 chmod）； **模块管理**（--enable-module、--disable-module）； **认证机制（修改httpd.conf(order allow, deny)或创建.htaccess）；** **连接耗尽（access-log大量408错误信息，** 应对方法：**减少Apache超时（Timeout）设置、增大MaxClients 设置；限制同一IP最大连接数；多线程下载保护）** **访问控制（order deny allow，deny from all， allow from xxx）；** **日志审计（access.log 记录对Web站点的每个进入请求；error.log记录产生错误状态的请求）；** **服务器防范（**Apache DoS Evasive Maneuvers Module，快速拒绝重复请求）。 **增强方法：安装补丁、.htaccess文件保护网页、设置专门的用户和组、隐藏版本号（**ServerSignature Off， ServerTokens ProductOnly) **目录访问安全增强（禁用索引**-Options -Indexes FollowSymLinks；**设置默认访问**-Order allow, deny相关；**禁止用户重载**-AllowOverride None ） **文件目录保护（属主、属组、权限管理。 chown、 chmod）、 删除默认目录和非必要文件、第三方增强（沙箱chroot、open ssl、TCP Wrapper）**
IIS	**概念：**Web（网页）服务组件，用提供网页浏览、文件传输、新闻服务和邮件发送等服务。 **组件：协议侦听器（http.sys）、Word Wide Web Publishing Service(W3SVC**，负责HTTP请求的监听任务)、**WAS**（负责HTTP和非HTTP请求的应用程序池和工作进程）、**存储区配置文件ApplicationHost.config。** **处理HTTPS请求的步骤。** **安全威胁（非授权服务器、蠕虫、网页篡改、DOS）、安全机制（认证、访问控制、审计）、** **增强措施（安装补丁、动态IP限制、 URLScan、 WAF、 SSL）**

5.1 新技术新方法-网站安全

主要内容	关键点
Web漏洞及防护	**1. 注入漏洞：SQL注入（利用Web 应用程序中未对程序变量进行安全过滤处理，故意构造特殊的SQL语句，让后台的数据库执行非法指令** **举例：** `SELECT * FROM product WHERE Category='food' or 1=1--'` **防范：安全过滤（黑白名单）、最小化权限、屏蔽应用程序错误提示信息、对开源Web应用程序做安全适应性改造。** **2. 文件上传漏洞：**对用户提交的文件**未进行严格的分析和检查**，攻击者可以执行上传文件，从而获取网站控制权限。 **防范： 上传目录设置为不可执行；检查文件的安全性。** **3. 跨站脚本攻击：**利用网站漏洞，URL中注入恶意脚本。
网络安全保护机制	1. **身份鉴别：**用户名口令、U盾、人脸识别、证书等； 2. **访问控制：**防火墙、数据加密、操作系统、数据库的访问控制能力等； 3. **网站内容安全**：文字、网页、图片、敏感词检查和过滤； 4. **网站数据安全**：数据隔离、加密、SSL、数据备份、隐私保护； 5. **网站安全防护**：暴力破解防护、抗Ddos等； 6. **安全审计与监控**：Syslog日志审计、Web流量截取、入侵检测、电子取证； 7. **网站应急响应**：网页防篡改、域名服务灾备、流量清洗、等保测评； 8. **网站合规管理**：网站备案、防伪标识、网站等保测评； 9. **网站安全测评：**漏洞扫描、渗透测试、代码审核、风险分析； 10. **网站安全管理机制：**网站建设、运维、应急预案等安全管理制度。 11. **网站安全加固：**参考CIS标准规范，操作系统、数据库、Web服务器软件、应用程序、网站域名服务等安全加固。
具体技术及应用	**常用技术： 防火墙、漏洞扫描、网页防篡改（**利用**操作系统文件调用事件/** 密码学**单向函数**检测**）、流量清洗、网站安全监测。** **应用：电子政务（**政府网站的信息**安全等级原则上不应低于二级。三级网站每年应测评一次，二级网站每两年应测评一次）**

5.2 新技术新方法-云计算

主要内容	关键点
基本知识	**概念：通过虚拟化及网络通信技术，提供一种按需服务、弹性化的IT资源池服务平台** **特征：IT资源以服务的形式提供、多租户共享IT资源、按需定制及按使用付费、伸缩性部署。** **服务形式：IaaS(Infrastructure-as-a-service)-基础设施服务； PaaS(Platform-as-a-service)-平台服务； SaaS(Software-as-a-service)-软件服务**，从基础设施到平台到软件，资源供应形式的抽象程度越来越高，使用者需要关注的底层设施越来越少。 **部署形式：公有云、私有云、社区云、混合云。**
云计算安全威胁	**端（终端设备或用户端）、管（网络）、云（云计算服务平台）：** **端侧威胁：**弱口令设置导致账号被劫持；黑客假冒用户攻击终端平台；终端设备存在漏洞； **管道威胁：**网络监听、网络数据泄露、中间人攻击、拒绝服务等，从而导致云计算平台出现安全问题。 云计算平台威胁： ●**物理安全威胁**：物理环境安全、硬件失效问题； ●**服务安全威胁**：云服务安全漏洞导致客户信息泄露、虚拟机安全不可信、虚拟机逃逸、镜像污染、侧信道攻击； ●**资源滥用安全威胁**：黑客入侵虚拟主机，构造僵尸网络发动拒绝服务攻击； ●**运维及内部安全威胁**：内部人员违反安全规定或误操作，导致数据丢失和泄露、平台服务非正常关闭等； ●**数据残留**：存储空间回收后未清除剩余信息； ●**过度依赖** ●**利用共享技术漏洞攻击；滥用云服务；云服务终端；利用不安全接口的攻击；数据丢失、篡改或泄露。**
安全要求及防护	**安全要求：多租户安全隔离、虚拟资源安全、云服务安全合规、数据可信托管、安全运维及业务连续性保障、隐私保护。** **等级保护：保证云计算基础设施位于中国境内， 原则（一个中心是指安全管理中心； 三重防护包括安全计算环境、安全区域边界和安全通信网络。）** **防护机制：身份鉴别认证机制（**口令、多因子、Kerberos**）、数字签名、访问控制（**MAC、RBAC**）、入侵防范（**IPS、IDS、DMZ**）、安全审计。** **安全管理：策略、制度、机构、人员、对象。** **安全运维措施：风险评估、内部安全防护、网络安全监测、应急响应、容灾备份（两地三中心：** 同域、异地；生产中心、同城容灾中心、异地容灾中心**）** **隐私保护： 云计算服务提供方的个人隐私保护措施（**个人信息备份及保管、 严格的管理制度和流程、安全合规及认证、强化身份认证和访问控制、限制存储地理位置、个人信息留存管理**）、用户个人隐私保护措施、个人信息安全事件应急响应措施。**

5.3 新技术新方法-工控

主要内容	关键点
基本知识	**概念：简称ICS，是由各种控制组件、监测组件、数据处理与展示组件共同构成的对工业生产过程进行控制和监控的业务流程管控系统。** **组成： SCADA 系统（监控作用）；** **分布式控制系统（DCS，现场控制级、系统控制级和管理级）；** **过程控制系统（PCS，常采用反馈控制（闭环控制）方式）；** **可编程逻辑控制器（PLC）、远程终端（RTU）、数控机床及数控系统。**
威胁	**自然灾害及环境、内部安全威胁、设备功能安全故障、恶意代码、网络攻击。**
隐患	**工控协议安全、技术产品安全漏洞、基础软件安全漏洞、算法安全漏洞、设备固件漏洞、开放接入漏洞、供应链安全。**
安全需求	工控系统的安全保护需求不同于普通 IT系统，**要根据工控业务的重要性和生产安全，划分安全区域、确定安全防护等级，然后持续提升工控设备、工控网络和工控数据的安全保护能力。** **需求顺序（可用性——完整性——保密性"）、安全要求（技术、管理）、标准（IEC62443）。**
保护机制	**物理与环境安全（**核心工业控制软硬件所在区域采取访问控制、视频监控、专人值守； 拆除或封闭工业主机上不必要的USB、光驱、无线等接口**）** **安全边界保护（**开发/测试/生产环境独立； 划分安全区域；部署防护设备-工控防火墙等**）、身份认证及访问控制（**多因素认证；最小特权；口令问题**）** **远程访问安全（**通常禁止HTTP、FTP、Telnet，确需访问的，采用数据单向访问控制、并控制访问时限。 或采用VPN**）** **安全加固、安全审计、恶意代码防范、工控安全管理（**供应链管理-优先考虑具备工控安全防护经验的企事业单位，做好保密工作**）** **工控数据安全（工控数据-**研发、生产、运维、管理、外部； **分级分类管理-** 定期备份机保护**）** **安全监测与应急响应（**部署安全监测设备；部署具备工业协议深度包检测功能的防护设备；制定预案；应急演练；设备冗余配置**）**
产品及应用	**防护类（**工控防火墙、工控加密、身份认证等**）、物理隔离类（**网闸、正反向隔离装置**）、审计与监测、** **检测类（**漏扫、漏洞挖掘、基线**）、运维及风控（**工控堡垒机**）。** **电力监测系统：安全分区、网络专用、横向隔离、纵向认证。** **工控安全防护方案：**InTrust工控可信计算安全平台、Guard工业防火墙、中央管理平台CMP、安全管理平台SMP。

5.4 新技术新方法-移动应用

主要内容	关键点
基本知识	**组成：移动应用（App）、通信网络、应用服务端。** **威胁：移动操作系统漏洞、无线网络攻击、恶意代码、逆向工程、非法篡改。**
Android	**组成：Linux 内核层（Linux Kernel）**：硬件的驱动程序、网络、电源、系统安全、内存管理、进程管理等； **系统运行库层（Libraries 和 Android Runtime）**：标准的C函数库Libc、OpenSSL等； **应用程序框架层（Application Framework）**：开发人员主要是使用该层封装好的API进行快速开发； **应用程序层（Applications）**：核心应用程序包。 **安全机制：权限声明**（normal权限、dangerous权限、signature权限、signatureOrSystem权限， 权限分配由Manifest 文件确定）、 **应用程序签名（APK，**数字证书）；**沙箱（唯一且固定的User ID，**运行在独立的Linux进程空间，不与其他应用程序交叉，实现完全隔离）、 **网络通信加密**(ssl/tls)、**内核安全机制**（分区、ACL权限控制机制）。
IOS	**封闭的生态系统。** **组成：核心操作系统层（**Core OSLayer，本地认证、安全等）、**核心服务层（**Core Services Layer，基础的系统服务，如账户、数据存储、网络连接、地理位置、运动框架）、**媒体层（**Media Layer，应用中视听方面的技术，如图形图像、声音、视频）和可触摸层（**Cocoa Touch Layer，负责用户在 iOS 设备上的触摸交互操作）。 **安全架构：硬件/固件层（**证书、引擎、内核）、 **软件层（**文件系统、操作系统分区、用户分区、应用沙盒及数据保护）。 **安全机制：安全启动链（**每个步骤包含的组件都经 Apple 加密签名以确保其完整性，验证后才能继续）、**数据保护、数据加密（所有用户数据强制加密，**AES硬件级加解密）、**地址空间布局随机化ASLR、代码签名、沙箱。**
加固及检测	**加固：防反编译**（加密、代码混淆）、**防调试、防篡改、防窃取。** **检测：身份认证、会话、敏感信息、日志、防篡改、防SQL等。** **工具：进程注入工具Inject、数据抓包工具Tcpdump/Wireshark、基于代理实现的抓包和分析工具Burpsuite等。** **个人信息安全：服务类型的最小必要权限**

5.5 新技术新方法-大数据安全

主要内容	关键点
基本知识	**大数据特征：海量的数据规模、快速的数据流转、多样的数据类型和价值密度低。** **分类：结构化**（数据库中的表结构，如企业用的人事系统、财务系统、ERP系统）、**半结构化**（邮件、日志文件、网页、新闻）、**非结构化数据**（传感器、移动终端、社交网络数据、声音图像等）。 **安全威胁：**安全边界模糊、敏感数据泄露风险、数据失真及污染、业务连续性、隐私保护、大数据滥用。 **法律法规：关键词-境内。**（数据来源于中华人民共和国境内的，数据中心的物理位置应当位于境内；境内收集的个人金融信息的储存、处理和分析应当在中国境内进行等）
保护机制	**自身安全保护**（数字签名-真实性； hash-完整性；加密-保密性）、**大数据平台安全保护**（安全分区、防火墙、系统安全加固、数据防泄露）、**业务安全保护**（授权、逻辑安全、合规检查）、**隐私安全保护**（数据身份匿名、数据差分隐私、数据脱敏、数据加密、数据访问控制）、**运营安全保护、大数据安全标准规范**（大数据安全标准特别工作组）。
应用实践	阿里：业务、数据、生态三层安全保护。 京东：区块链助力确权溯源。 上海交易中心：交易规则设置及技术保护 华为：网络安全、主机安全、用户安全、数据安全。
管理规范	《科学数据管理办法》：**国务院办公厅印发。** **科学数据，不得对外开放共享，确需对外开放的，需严格审核及控制知悉范围；** **对外交往与合作中需要提供涉及国家秘密的科学数据，法人单位提申请，按照保密管理规定程序报主管部门批准。** 建立**应急管理**和**容灾备份**机制，按照要求建立应急管理系统，对**重要的科学数据**进行**异地备份。** 支付卡行业标准：**PCI—DSS， 分为4个等级。 保障银行卡用户在线交易的安全。**

目录

CONTENTS

大纲例题解析

1.攻击者利用John the Rpper工具对目标服务器进行攻击，则此攻击者所利用的方法是()。

A.会话劫持　　B.口令破解　　C.端口扫描　　D.拒绝服务

2.VPN产品的安全实现技术主要是()。

A.RFC、IPSec　　B.XML、BGP　　C.SSL、IPSec　　D. BGP、OSPF

3.网络中的明文传输容易造成信息泄露，为了抵御网络监听，常用的技术方法是()。

A.SSL、OSPF　　B.IPSec、SNMP　　C.SSL、IPSec　　D.OSPF、SNMP

大纲例题解析

1.攻击者利用John the Rpper工具对目标服务器进行攻击，则此攻击者所利用的方法是()。

A.会话劫持　　B.口令破解　　C.端口扫描　　D.拒绝服务

答案：B

2.VPN产品的安全实现技术主要是()。

A.RFC、IPSec　　B.XML、BGP　　C.SSL、IPSec　　D. BGP、OSPF

答案：C

3.网络中的明文传输容易造成信息泄露，为了抵御网络监听，常用的技术方法是()。

A.SSL、OSPF　　B.IPSec、SNMP　　C.SSL、IPSec　　D.OSPF、SNMP

答案：C

大纲例题解析

1. 某公司网站应用架构采用 LAMP模式，其操作系统为Linux，Web服务器采用Apache HTP，数据库是MySQL，应用编程则为PHP，试解决网站应用中的安全问题。

(1)已知管理员使用Telnet和HTTP远程管理网站服务器，而国家信息安全等级安全保护要求为：(5分)

●当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听。

●应为操作系统和数据库的不同用户分配不同的用户名，确保用户名具有唯一性。

请问：采取什么安全措施可以符合等级保护要求?如何获取网站操作系统和数据库的用户信息?

(2)网站安全策略要求网站的默认服务端口改成8081，远程计算机的IP地址192.168.0.2，若要其可以访问网站服务器/www/admin资源。如何配置Apache相关文件以符合安全策略要求?(5分)

大纲例题解析

1. 某公司网站应用架构采用 LAMP模式，其操作系统为Linux，Web服务器采用Apache HTP，数据库是MySQL，应用编程则为PHP，试解决网站应用中的安全问题。

(1)已知管理员使用Telnet和HTTP远程管理网站服务器，而国家信息安全等级安全保护要求为：(5分)

●当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听。

●应为操作系统和数据库的不同用户分配不同的用户名，确保用户名具有唯一性。

请问：采取什么安全措施可以符合等级保护要求?如何获取网站操作系统和数据库的用户信息?

参考答案：

安全措施（1）使用SSH替换telnet， 使用HTTPS（SSL技术）替换http访问。

（2） Linux下及Mysql中为不同用户创建独立的账号，并采用身份认证及访问控制机制保证安全性。

获取用户信息：（1）操作系统用户信息获取方法：管理员登录后，查看/etc/passwd文件内容。

（2） 数据库获取用户信息方法：管理员登录后sql语句查询，select user, host, password from mysql.user。

(2)网站安全策略要求网站的默认服务端口改成8081，远程计算机的IP地址192.168.0.2，若要其可以访问网站服务器/www/admin资源。如何配置Apache相关文件以符合安全策略要求?(5分)

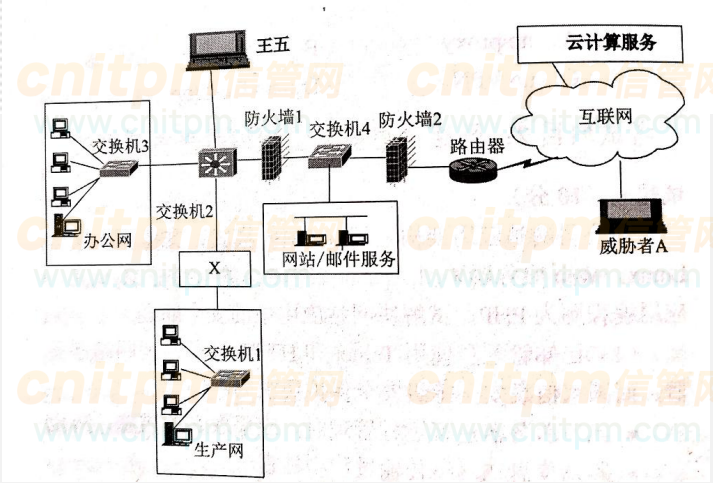
参考答案：1. 修改默认服务端口：配置文件httpd.conf中Listen字段值设置为8081。

2. 访问资源限制：www/admin目录下创建.htaccess文件，并做如下控制：

```
Order deny, allow
deny from all
allow from 192.168.0.2
```

大纲例题解析

2. 已知甲公司网络环境结构如右图所示



【问题1】公司为了防止生产网受到外部的网络安全威胁，安全策略要求生产网和外部网之间部署安全隔离装置，隔离强度达到接近物理隔离。请问：X最有可能代表的安全设备是什么?简要描述该设备的工作原理。(6分)

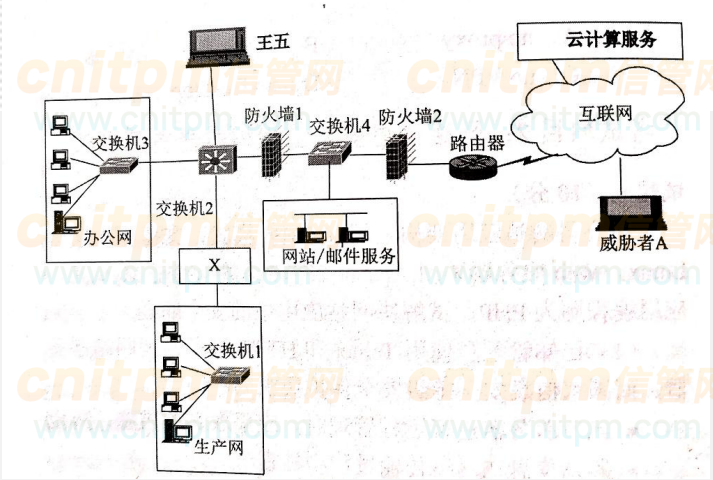
【问题2】公司拟购买云计算服务，并租用虚拟主机，请列举云计算的服务安全风险类型。(5分)

【问题3】公司的防火墙是否能有效地保护虚拟主机安全?为什么?(4分)

【问题4】高级持续威胁(简称APT)常常利用电子邮件，开展有针对性的目标攻击，威胁者A发送带有恶意Word附件的电子邮件到公司邮件服务器，等待邮件接收者执行电子邮件附件，触发恶意程序运行，从而渗透到甲公司内部网络，请给出威胁者A的攻击流量经过的网络设备。针对APT，可以部署什么安全设备来自动检测?该设备的主要技术方法是什么?(10分)

大纲例题解析

2. 已知甲公司网络环境结构如右图所示



【问题1】公司为了防止生产网受到外部的网络安全威胁，安全策略要求生产网和外部网之间部署安全隔离装置，隔离强度达到接近物理隔离。请问：X最有可能代表的安全设备是什么?简要描述该设备的工作原理。(6分)

参考答案：网闸。 工作原理：使用一个具有控制功能的开关读写存储设备，通过开关的设置来连接/切断两个独立系统的数据交换，将数据包进行分解或重组为静态数据，然后进行安全审查、网络协议检查和代码扫描等，通过身份认证机制获取所需数据。

【问题2】公司拟购买云计算服务，并租用虚拟主机，请列举云计算的服务安全风险类型。(5分)

参考答案：“端-管-云”三个方面存在风险。端（弱口令设置导致账号被劫持；黑客假冒用户攻击终端平台；终端设备存在漏洞等**）**

管（网络监听、网络数据泄露、中间人攻击、拒绝服务**）、云计算平台（**物理安全、服务安全、资源滥用、数据残留等**）。**

【问题3】公司的防火墙是否能有效地保护虚拟主机安全?为什么?(4分)

参考答案：不能，防火墙受限于安全规则，不能完全防止感染病毒的软件/文件传输；不能完全防止后门攻击；不能有效防范内部威胁。

【问题4】高级持续威胁(简称APT)常常利用电子邮件，开展有针对性的目标攻击，威胁者A发送带有恶意Word附件的电子邮件到公司邮件服务器，等待邮件接收者执行电子邮件附件，触发恶意程序运行，从而渗透到甲公司内部网络，请给出威胁者A的攻击流量经过的网络设备。针对APT，可以部署什么安全设备来自动检测?该设备的主要技术方法是什么?(10分)

参考答案：流经的网络设备： 1. 发恶意邮件阶段： 路由器->防火墙2->交换机4->邮件服务。

2. 触发恶意程序阶段： 邮件服务->交换机4->防火墙1->交换机2->交换机3 ）。

部署入侵检测系统IDS/高级持续威胁检测系统。 主要技术方法： 基于误用/异常方法进行检测， 或基于静态/动态分析检测可疑恶意电子文件及关联分析网络安全大数据。

案例分析考点推断

考点推断	具体涉及的内容
网络安全风险评估	风险评估过程、 风险分析步骤、方法、**风险计算方法**
操作系统安全	Windows安全增强方法及流程， Linux访问控制及安全加固的方法。
数据库安全	数据库的安全机制 Oracle、MS SQL、MySQL数据库安全加固实践方法。 MySQL数据库常用安全配置命令（创建、查询、修改用户名及密码等）；
防火墙、VPN及IDS	防火墙：安全策略、安全问题、**包过滤防火墙规则配置、体系结构类型**、iptables。 VPN：安全服务、类型、**IPSec、SSL** IDS：入侵检测技术分类、入侵检测系统分类、Snort。
Web网站安全	网站安全定义、**Apache安全增强、IIS安全增强、SQL注入及防范**、网站整体安全防护。
密码学基本理论	密码分析攻击种类、密码体制、**数字信封、RSA计算方法**

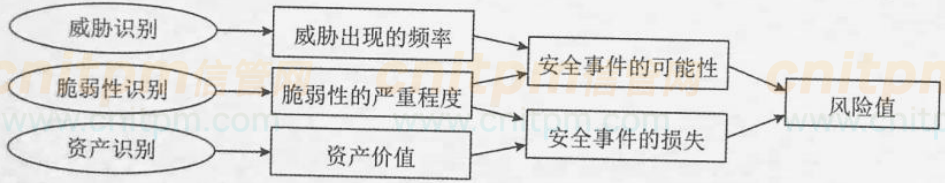
考前冲刺例题-风险评估

【问题1】请简述风险评估的各环节。

参考答案：风险评估准备、资产识别、威胁识别、脆弱性识别、已有的网络安全措施分析、网络安全风险分析、风险处置、风险管理。

【问题2】风险分析是风险评估的主要环节，请简述风险分析步骤

参考答案： 1.资产识别，对资产价值进行赋值； 2. 威胁识别，对威胁频率赋值； 3. 脆弱性识别，对脆弱性严重程度赋值； 4.根据威胁及脆弱性严重程度判断安全事件的可能性； 5.根据脆弱性严重程度和资产价值计算安全事件的损失； 6.根据安全事件的可能性及损失计算风险值。



【问题3】网络安全风险值的计算方法主要有哪几个类型?

参考答案：定性计算方法、定量计算方法、综合计算方法

【问题4】假设某资产A的资产价值为4， 威胁频率为1， 脆弱性严重程度为3， 根据相乘法求A的风险值。

参考答案：1. 安全事件的可能性=√威胁频率*脆弱性严重程度=√1*3 =√3，

2. 安全事件的损失=√脆弱性严重程度*√资产价值= √3*4 = 2√3，

3.风险值=√3* 2√3= 6。

考前冲刺例题-windows系统

【问题1】请简述Windows安全增强的方法。

参考答案：1.安全漏洞打补丁； 2. 停止服务和卸载软件； 3. 升级或更换程序； 4. 修改配置或权限； 5. 去除恶意程序； 6. 安全专用安全工具。

【问题2】简述Windows安全增强基本步骤。

参考答案： 1.确认系统安全目标和业务用途； 2. 安装最小化的操作系统； 3. 安装最新系统补丁； 4. 配置安全的系统服务； 5. 配置安全策略； 6. 禁用NetBIOS; 7. 账户安全配置； 8. 文件系统安全配置； 9.配置TCP/IP； 10. 禁用光盘/软盘启动； 11.使用屏幕保护口令； 12. 设置应用软件安全。 13. 安装第三方防护软件。

【问题3】列举windows的日志类型及文件名， 通常存放在哪个目录下?

参考答案： 系统日志（SysEvent.evt）、应用程序日志（AppEvent.evt）、安全日志（SecEvent.evt），在system32\config目录下。

【问题4】针对账号和口令，如何增强安全措施?

参考答案：1. 停掉guest账号； 2.限制不必要的用户数量； 3.修改系统账号名； 4.创建一个陷阱账号； 5.设置安全复杂的口令； 6.设置屏幕保护口令； 7. 不让系统显示上次登录的用户名； 8. 开启口令安全策略；9.开启账号策略。

【问题5】windows系统下，如何保障远程登录安全和身份安全认证?

参考答案：1.采用OpenSSH进行远程安全登录管理； 2. 采用Kerberos进行系统身份认证增强。

考前冲刺例题-UNIX/Linux

【问题1】账号和口令是入侵者最为重要的攻击对象，Unix/Linux系统中，口令信息保存在哪两个文件中?

参考答案：/etc/passwd和/etc/shadow中。

【问题2】UNIX/Linux通常通过ACL实现访问控制，也就是9bit位来实现，（1）请简述如下9bit表达的含义，（2）请将9bit转化为数字权限表示。

-rwxr-xr-- 1 test test 11月1日 11:00 sample.txt

参考答案：（1）用户test对sample.txt访问权限有“读、写、执行”；test所在组的其他用户具有“读，执行”的权限，除此之外的其他用户只有”读权限。”

（2）转化为数字权限表示为754。

【问题3】最小化配置服务是在满足业务前提下，尽量关闭不需要的服务和网络端口，请说明UNIX/LINUX网络服务最小化的安全要求有哪些？并说明如何通过命令进行配置?

参考答案：inet.conf文件权限为600，属主为root;

命令为 chmod 600 /etc/inet.conf；chown root:root /etc/inet.conf；chattr +i /etc/inet.conf。

services文件权限为644，属主为root;

在inet.conf中注销不必要的服务，只开放与系统业务相关的网络通信端口。

【问题4】简述UNIX/Linux系统安全增强方法

参考答案：1.给安全漏洞打补丁；2.停止不必要的服务；3.升级或更换软件包；4.修改系统配置；5. 安装专用的安全工具软件。

考前冲刺例题-数据库安全

【问题1】数据库是一个复杂性高的基础性软件，请列举其安全机制。

参考答案：标识与鉴别、访问控制、安全审计、备份与恢复、数据加密、资源限制、安全加固、安全管理等。

【问题2】数据库存储加密方式是哪两种？ 存储加密常用技术方法有哪些？

参考答案： （1）库内加密、 库外加密； （2）基于文件的加密、基于记录的加密、基于字段的加密。

【问题3】MySQL是常见的数据库，广泛用于互联网中，请列举MySQL的安全增强措施。

参考答案： 1. MySQL安装时建立单独启动的用户和组； 2. 建立Chrooting运行环境； 3. 关闭远程连接； 4.禁止MySQL导入本地文件；
5.修改MySQL的 root用户ID和密码； 6. 删除MySQL的默认用户和db； 7. 更改root用户名，防止暴力破解；
8. 建立应用程序独立使用的数据库和用户账号； 9.安全监测； 10. 安全备份。

【问题4】将MySQL的root用户名改为roottest， 请写出命令。

参考答案： update user set user=” roottest” where user = “root” ;
flush privileges。

常见mysql命令有：

创建用户： CREATE USER 'username'@'host' IDENTIFIED BY 'password';
修改密码：SET PASSWORD FOR username@host=PASSWORD('new password');
查询语句：SELECT 要查询的列名 FROM 表名字 WHERE 限制条件;

考前冲刺例题-防火墙

【问题1】防火墙安全策略有几种类型，各自的内容是什么。

参考答案：1.白名单策略：只允许符合安全规则的包通过，其他通信包禁止。

2.黑名单策略：禁止与安全规则相冲突的包通过防火墙，其他通信包都允许

【问题2】如右图过滤规则，描述其作用：

规则编号	通信方向	协议类型	源 IP	目标 IP	源端口	目标端口	操作
A	in	TCP	外部	内部	≥1024	25	允许
B	out	TCP	内部	外部	25	≥1024	允许
C	out	TCP	内部	外部	≥1024	25	允许
D	in	TCP	外部	内部	25	≥1024	允许
E	either	any	any	any	any	any	拒绝

参考答案： A和B表明，外部可以访问内部邮件系统； C和D表明，内部可以访问外部邮件系统； E表明其他通信包都禁止。

所以，作用是，只允许内外网的邮件访问。

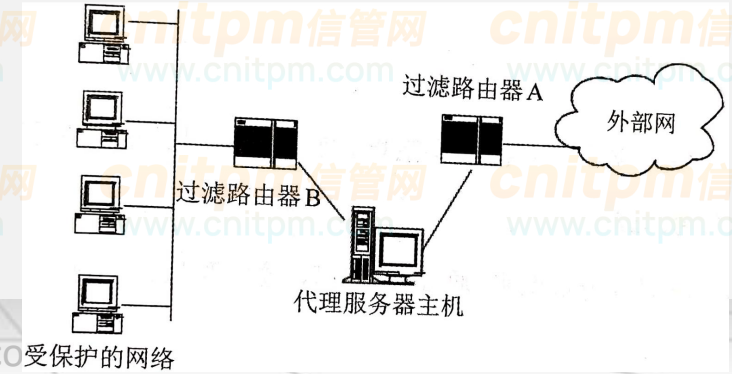
【问题3】如下是某防火墙部署结构，请说明是哪一种防火墙体系，并描述其特点？ 过滤路由器A和B的作用是什么？

参考答案： 1. 屏蔽子网防火墙， 因由两个过滤路由器和一个代理服务器主机组成。

特点：安全级别最高，但是成本高，配置复杂。

2. 路由器A用于过滤外网对被屏蔽子网的访问；

路由器B用于过滤被屏蔽子网到内网的访问。



考前冲刺例题-iptables简述

iptables的结构：iptables -> Tables -> Chains -> Rules. 简单地讲，tables由chains组成，而chains又由rules组。
rules就是防火墙的一条一条的规则
iptables规则：rules包括一个条件和一个目标(target), 如果满足条件，就执行目标(target)中的规则或者特定值。如果不满足条件，就判断下一条Rules。

iptables的一些命令说明：
INPUT链 – 处理来自外部的数据。
OUTPUT链 – 处理向外发送的数据。
FORWARD链 – 将数据转发到本机的其他网卡设备上。
ACCEPT – 允许防火墙接收数据包
DROP – 防火墙丢弃包

语法：iptables -A chain firewall-rule
-A chain – 指定要追加规则的链
firewall-rule – 具体的规则参数

-p 协议（protocol）；
-s 源地址（source）；
-d 目的地址（destination）；
-j 执行目标（jump to target）；
-i 输入接口（input interface）；
-o 输出（out interface）

–sport 源端口（source port）
--dport 目的端口（destination port）

举例：仅允许SSH数据包通过本地

```
# 1.清空所有iptables规则
iptables -F

# 2.接收目标端口为22的数据包
iptables -A INPUT -i eth0 -p tcp --dport 22 -j ACCEPT

# 3.拒绝所有其他数据包
iptables -A INPUT -j DROP
```

考前冲刺例题-VPN&IDS

【问题1】VPN的主要产品有哪两种?

参考答案： IPSec VPN， SSL VPN

【问题2】IPSec VPN中 AH协议、 ESP协议各自的作用是什么?

参考答案： AH：认证头协议，保证IP包的完整性和提供数据源认证。

ESP：封装安全有效负荷，保证IP包的保密性。

【问题3】远程用户安全办公问题应通过什么VPN技术实现? 分布在不同区域的企业办公点安全互联，应通过什么VPN技术实现?

参考答案： 1. 远程安全办公采用 Access VPN实现； 2. 不同区域的企业办公点互联采用Intranet VPN 实现。

【问题4】基于误用的入侵检测与基于异常的入侵检测方法的各自定义和区别是什么?

参考答案： 1. 基于误用的入侵检测：根据已知的入侵模式检测入侵行为，其原理是基于模式匹配进行，依赖于攻击模式库。

2. 基于异常的入侵检测：建立系统正常行为轨迹，将系统运行时的数值与正常情况比较，判断是否有攻击。

【问题5】入侵检测系统有哪些分类?

参考答案： 基于主机的入侵检测系统HIDS、 基于网络的入侵检测系统NIDS、分布式入侵检测系统。

考前冲刺例题-Snort简述

Snort是常见的开源入侵检测系统。

技术原理：通过获取网络数据包，基于安全规则进行检测，最后形成报警信息。

Snort规则组成：规则头、规则选项。

规则头包括：规则动作、协议、源IP地址，源端口，方向，目的IP，目的端口。

规则选项：以；隔开每组关键词。

```
alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 111 (content: "|00 01 86 a5|"; msg: "external mountd access";)
```

规则动作：

1、Alert-使用选择的报警方法生成一个警报，然后记录（log）这个包。
2、Log-记录这个包。
3、Pass-丢弃（忽略）这个包。
4、activate-报警并且激活另一条dynamic规则。
5、dynamic-保持空闲直到被一条activate规则激活，被激活后就作为一条log规则执行。

规则选项：

msg - 在报警和包日志中打印一个消息。
dsize - 检查包的净荷尺寸的值 。
sid - snort规则id。
rev - 规则版本号。
content - 在包的净荷中搜索指定的样式。
depth - content选项的修饰符，设定搜索的最大深度。
nocase - 指定对content字符串大小写不敏感。
session - 记录指定会话的应用层信息的内容。
rpc - 监视特定应用/进程调用的RPC服务。
resp - 主动反应（切断连接等）。
react - 响应动作（阻塞web站点）。
reference - 外部攻击参考ids

考前冲刺例题-网站安全

【问题1】网站安全主要是有关网站的机密性、完整性、可用性及可控性，请阐述具体内容

参考答案：

网站的机密性是指网站信息及相关数据不被授权查看或泄露。

网站的完整性是指网站的信息及数据不能非授权修改，网站服务不被劫持。

网站的可用性是指网站可以持续为相关用户提供不中断的服务的能力，满足用户的正常请求服务。

网站的可控性是指网站的责任主体及运营者对网站的管理及控制的能力，网站不能被恶意利用。

Apache Web： 关键配置文件：httpd.conf

安全机制：

本地文件： chmod 修改权限、chown 修改属主属组

模块管理：enable， --disable-module

认证机制：对目录进行访问控制

httpd.conf中增加控制：

```
<Directory “目录”>
 Options Indexes FollowSymlinks MultiViews     #可以显示目录列表
 AllowOverride AuthConfig    #启用身份验证
 Order allow, deny      #先allow后deny
  Allow from all
</Directory>
```

Apache Web安全增强：

禁止目录访问： Options -Indexes FollowSymlinks

禁止用户修改配置文件：AllowOverride None

及时安装补丁

按照最小特权原则，为服务软件设置专门的用户和组

隐藏版本号：ServerSignature Off， ServerTokens Prod

文件目录保护： chmod、 chown

删除默认目录及不必要的权限。

考前冲刺例题-网站安全

【问题1】IIS的安全增强方式有哪些?

参考答案:

1. 及时安装补丁;

2.启动动态IP限制;

3.启用URLScan;

4.启用WAF;

5.启用SSL服务

【问题2】请问下面SQL语句属于何种攻击?应当如何防范此类攻击?

SELECT * FROM product WHERE Category= 'food' or 1=1--

参考答案:

1. 属于SQL注入攻击，可以获取到所有种类的产品信息;

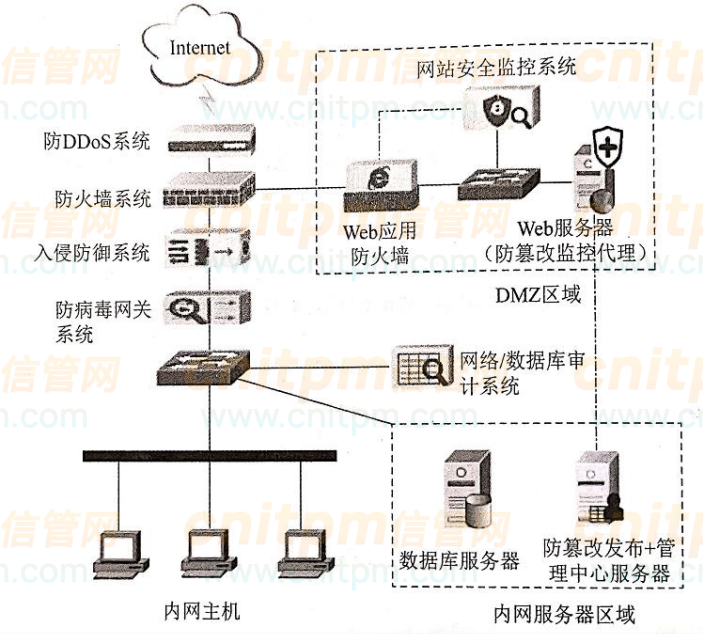
2. 防范方法:

对应用程序输入进行安全过滤;

设置应用程序最小化权限;

屏蔽应用程序错误提示信息;

对开源Web应用程序做安全适应性改造。



（1）DDoS防御。用于防护来自互联网的拒绝服务攻击。

（2）网络访问控制。防止不必要的服务进入网站系统，减少被攻击的可能性。

（3）网页防篡改。在Web服务器上部署网页防篡改系统，针对Web应用网页和文件进行防护。

（4）网站应用防护。通过Web 应用防火墙代理互联网客户端对Web 服务器的所有请求，清洗异常流量，有效控制各类安全威胁。

（5）入侵防御和病毒防护。通过入侵防御系统和防病毒网关系统实现对非法入侵行为和网络病毒的有效检测和阻断。

（6）网络/数据库审计。通过网络/数据库审计系统实现对网站访问行为和网站后台数据库的访问行为进行监控、记录和审计。

（7）网站安全监控。通过网站安全监控系统实现漏洞扫描、网页木马监测、网页篡改监测、网页敏感信息监测等功能，同时系统与Web应用防火墙进行联动，进一步提升防护能力。

考前冲刺例题-密码学基本理论

【问题1】请列举密码分析攻击的五种类型?

参考答案:

(1) 唯密文攻击。密码分析者只拥有一个或多个用同一个密钥加密的密文，没有其他可利用的信息。

(2) 已知明文攻击。密码分析者仅知道当前密钥下的一些明文及所对应的密文。

(3) 选择明文攻击。密码分析者能够得到当前密钥下自己选定的明文所对应的密文。

(4) 密文验证攻击。密码分析者对于任何选定的密文，能够得到该密文"是否合法"的判断。

(5) 选择密文攻击。除了挑战密文外，密码分析者能够得到任何选定的密文所对应的明文。

【问题2】数字信封属于何种密码体制下的技术？请简述该密码体制的原理。

参考答案:

1. 属于混合密码体制;

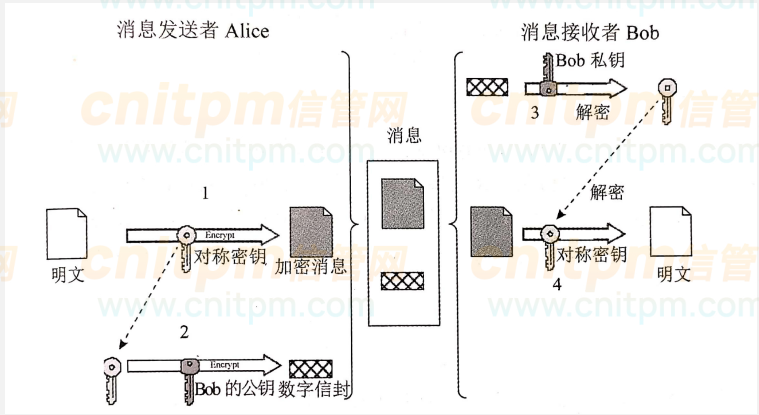
2. 原理:

第一步，消息发送者Alice用对称密钥把需要发送的消息加密。

第二步，Alice用Bob的公开密钥将对称密钥加密，形成数字信封。然后，一起把加密消息和数字信封传送给 Bob。

第三步，Bob收到Alice的加密消息和数字信封后，用自己的私钥将数字信封解密，获取Alice加密消息时的对称密钥。

第四步，Bob使用Alice加密的对称密钥把收到的加密消息解开。



考前冲刺例题-RSA计算方法

【问题1】设素数p=3, q=17, e=13，明文M=2 求密文C，

参考答案：C=32

1. n=p*q=3*17=51

2. φ(n)=(p-1)*(q-1)=2*16=32， 因$d=e^{-1} \bmod \varphi(n)$，所以d=(k φ(n)+1)/e， k是p-1和q-1的最大公约数，即k=2
得出，d=(2*32+1)/13=5

3. $C=M^e \bmod n = 2^{13} \bmod 51 = 32$

RSA 算法基于大整数因子分解的困难性，该算法的步骤如下：

第一步，生成两个大素数 p 和 q 。

第二步，计算这两个素数的乘积 $n=pq$。

第三步，计算小于 n 并且与 n 互素的整数的个数，即欧拉函数 $\varphi(n)=(p-1)(q-1)$ 。

第四步，选取一个随机数 e，且满足 $1<e<\varphi(n)$，并且 e 和 $\varphi(n)$ 互素，即 $\gcd(e,\varphi(n))=1$ 。

第五步，计算 $d=e^{-1} \bmod \varphi(n)$ 。

第六步，保密 d、p 和 q，而公开 n 和 e，即 d 作为私钥，而 n 和 e 作为公钥。

总结和期望

1. 拥抱变化，平和对待
2. 认真复习，不要放弃
3. 不忘初心，持续精进

谢　谢！