1. 网络信息按概述

安全基本属性：机密性、完整性、可用性、抗抵赖性、可控性

CIA：机密性：网络信息不泄露给非授权用户、实体或程序、能够防止非授权者获取信息

完整性：网络信息或系统未经授权不能进行更改的特性

可用性：指合法许可的用户能够及时获取网络信息或服务的特性

网络信息访问控制目的： 1）限制非法用户获取或使用网络资源 2）防止合法用户滥用权限、越权访问网络资源

网络信息安全管理要素：网络管理对象、网络威胁、网络脆弱性、网络风险、网络保护措施组成。 基本过程：通过对网络管理对象的威胁和脆弱性进行分析，确定网络管理对象的价值，网络管理对象威胁发生的可能性、网络管理对象的脆弱程度，从而确定网络管理对象的风险等级，然后据此选取合适的安全保护措施，降低网络管理对象的风险。

网络信息安全管理流程： 确定对象-评估价值-识别威胁-识别脆弱性-确定风险级别-制定防范措施-实施防范措施-运行/维护

网络信息安全术语：

* **基础技术类**：加密encryption、解密decryption、非对称加密算法asymetric cryptographic algorithm、公钥加密算算法public key cryptographic algonrithm、公钥public key
* **风险评估技术类**： 拒绝服务Denial of Service、分布式拒绝服务Distributed Denial of Service、网页篡改Website Distortion、网页仿冒Phishing、网页挂马Website Malicious Code、域名劫持DNS Hijack、路由劫持Routing Hijack、垃圾邮件Spam、恶意代码Malicious Code、特洛伊木马Trojan Horse、网络蠕虫Network Worm、僵尸网络Bot Net
* **防护技术类：**访问控制Access Control、防火墙Firewall、入侵防御系统Intrusion Prevention System
* **检查技术类：**入侵检测Intrusion Detection、漏洞扫描Vulnerability Scanning
* **响应/恢复技术类：**应急响应Emergency Response、灾难恢复Disaster Recovery、备份Backup
* **测评技术类：**黑盒测试Black Box Testing、白盒测试White Box Testing、灰盒测试Gray Box Testing、渗透测试Penetration Testing 、模糊测试Fuzz Testing

态势感知：结合防毒软件、防火墙、入侵检测系统、安全审计对整个网络情况进行评估，预测未来的变化趋势

四个部分：数据采集、特征提取、态势评估、安全预警

内容：1、感知网络资产 2、感知资产脆弱性 3、感知安全事件 4、感知网络威胁 5、感知网络攻击 6、感知安全风险

1. 网络攻击原理与常用方法

**危害行为**： 1）信息泄露攻击 2）完整性破坏攻击 3）拒绝服务攻击 4）非法使用攻击

**网络攻击过程**：1）隐藏攻击源 2）收集攻击目标信息 3）挖掘漏洞信息 4）获取目标访问权限5）隐藏攻击行为 6）实施攻击 7）开辟后门 8）清除攻击痕迹

**实施攻击的目标**：1、攻击其他被信任的主机和网络 2、修改或删除重要数据 3、窃听敏感数据 4、停止网络服务 5、下载敏感数据 6、删除数据账号 7、修改数据记录

**开辟后门方法**：1、放宽文件许可权 2、重新开放不安全的服务 3、修改系统配置 4、替换系统本身的共享库文件 5、修改系统的源代码 6、安装嗅探器 7、建立隐蔽信道

**清除攻击痕迹方法**：1、篡改日志文件中的审计信息 2、改变系统时间造成日志文件数据紊乱以迷惑系统管理员 3、删除或停止审计服务进程 4、干扰入侵检测系统的正常运行 5、修改完整性检测标签

**网络攻击常见技术方法**

* **端口扫描 –** 找出目标系统上提供的服务列表

完全连接扫描 – 三次握手，成功：端口开放，失败：端口关闭

半连接扫描 – 只完成两次握手，目的：不留扫描痕迹

SYN扫描 – 发送连接请求，返回响应进行断开，返回ACK:端口开放 返回RESET:端口关闭

ID头信息扫描：SYN|ACK：端口开放 RST|ACK:端口关闭

隐蔽扫描:绕过IDS、防火墙

SYN|ACK扫描：发送SYN|ACK数据包，返回RST，端口关闭 不返回信息，端口开放

FIN扫描：发送FIN数据包，返回RESET,端口关闭，不返回信息,端口开放

ACK扫描：发送FIN数据包，返回TTL<64或WIN>0，端口开放 返回TTL>64或WIN=0端口关闭

NULL扫描：发送空数据，不返回，端口开放。返回RET，端口关闭

XMAS扫描：发送1，不返回，端口开放。返回RET，端口关闭

* 口令破解、缓冲区溢出
* 恶意代码- 计算机病毒、网络蠕虫、特洛伊木马、后门、逻辑炸弹、僵尸网络
* 拒绝服务、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、代理技术、数据加密

**DDOS攻击的步骤**：1、扫描大量主机，寻找可攻击目标 2、攻击有安全漏洞主机，获取控制权 3、安装攻击程序 4、利用主机继续扫描和攻击 5、遥控所有攻击客户端进行目标攻击

1. 密码学基本理论

**DES** 分组64位，密钥长度56位，每轮子密钥48位

**IDEA** 分组64位，密钥长度128位

**AES** 分组128位，密钥长度128、192、256

**RSA** 非对称算法

**国产密码**： SM1：对称加密，分组、密钥长度128位 SM2:非对称加密 SM3:杂凑算法，分组512，杂凑值长度256 SM4：对称加密，分组、密钥长度128 SM9：标识密码

**Hash算法**：MD5(512位数据块，产生128位的哈希值)、SHA（512位数据块，产生160位的哈希值）、SM3（512位数据块，产生256位的哈希值）

**数字签名**： 满足三个条件：非否认、真实性、可鉴别性

**密钥管理**：三个方面：密钥管理、密钥管理政策、密码评测

**密钥管理周期**：生成-存储-分发-使用-更新-撤销-备份-恢复-销毁-审计

第4章 网络安全体系与网络安全模型

**网络体系的主要特征**：整体性、协同性、过程性、全面性、适应性、

**BLP模型**：机密性 下读上写

**BiBa模型**：完整性 上读下写

**PDRR模型**：保护Protection、检测Detection、恢复Recovery、响应Response

**P2DR模型**：策略Policy、保护Protection、检测Detection、响应Response

**WPDRRC模型**：预警、保护、检测、响应、恢复和反击构成

**纵深防御模型**：4道防线：安全保护、安全监测、实时响应、恢复网络

**网络生存模型3R策略**：抵抗Resistance、识别Recognition、恢复Recovery

**网络安全建设的主要内容**：1、网络安全策略及标准规范制定和实施 2、网络安全组织管理机构的设置和岗位人员配件 3、网络安全项目规划、设计、实施 4、网络安全方案设计和部署 5、网络安全工程项目验收评测和交付使用

**网络安全等级保护工作**：定级、备案、建设整改、等级测评、监督检查

第5章 物理与环境安全技术

机房等级要求：A级：中断后，对国家安全、社会秩序、公共利益造成**严重损害**

B级：中断后，对国家安全、社会秩序、公共利益造成**较大损害**

C级：不属于A和B

数据中心建设：超大型数据中心-大于等于10000个标准机架

大型数据中心—大于等于3000个 小于10000个标准机架

中小型数据中心—小于3000个标准机架

IDC机房要求：R1级 一定冗余能力，可用性不应小于99.5%

R2级 具备冗余能力，可用性不应小于99.9%

R3级 具备容错能力，可用性不应小于99.99%

硬件木马检测：反向分析法、功耗分析法、侧信道分析法

容错容灾存储技术：磁盘阵列、双机在线备份、离线备份

第6章 认证技术原理与应用

认证：标识和鉴别组成

认证分类：单向认证、双向认证、第三方认证

认证技术方法：口令认证技术、智能卡技术、基于生物特征认证技术、kerberos认证技术

PKI安全服务：身份认证、完整性保护、数字签名、会话加密、密钥恢复

CA:证书颁发、废止、更新、签发、管理、测写

RA：辅助CA（前台）

第7章 访问控制技术原理与应用

主体：访问者 客体：资源对象 授权：访问者对资源对象的访问方式

目标：防止非法用户进入系统 阻止合法用户越权访问

访问控制参考模型组成：主体、参考监视器、客体、访问控制数据库、审计库

访问控制模型发展

* 自主访问控制模型 Discretionary Access Control DAC ,客体的所有者按照自己的安全策略授予系统中其他用户对其的访问权

基于行的自主访问控制：能力表（读写执行）、前缀表（权限）、口令表（口令）

基于列的自主访问控制：保护位、访问控制表（ACL,从客体出发）

* 强制访问控制模型 Mandatory Access Control MAC 主体和客体的安全属性，用于军事，划分安全等级和不同类别
* 基于角色的访问控制模型 RBAC由用户、角色、会话、权限组成
* 基于使用的访问控制模型
* 基于地理为主的访问控制模型
* 基于属性的访问控制模型 Attribute Based Access Control ABAC 根据主体的属性、客户的属性、环境的条件及方位策略对主体的请求操作进行授权许可或拒绝
* 基于行为的访问控制模型
* 基于时态的访问控制模型

访问控制规则

* 基于用户身份的访问控制规则 -- 账号口令
* 基于角色的访问控制规则 – 角色权限
* 基于地址的访问控制规则 – IP、域名、物理地址
* 基于时间的访问控制规则 – 下班时间
* 基于异常事件的访问控制规则 – 登录3次失败，冻结
* 基于服务数量的访问控制规则 – 服务能力的某个阀值

访问控制过程：

1、明确访问控制管理的资产（路由器、WEB服务）

2、分析管理资产的安全需求（保密性、完整性、可用性要求）

3、制定访问控制策略，确定访问控制规则及用户权限分配

4、实现访问控制策略，建立用户访问身份认证系统并根据用户类型授权用户访问资产

5、运行和维护访问控制系统，及时调整访问策略

最小特权管理：按需使用

口令安全管理：

* 口令选择至少8个字符以上，选用大小写字母、数字、特殊字符组合
* 禁止使用与账号相同的口令
* 更换系统默认口令、避免使用默认口令
* 限制账号登录次数、建议为3次
* 禁止共享账号和口令
* 口令文件应加密存放，并只有超级用户才能读取
* 禁止以明文形式在网络传递口令
* 口令应有时效机制，经常更改，并且禁止重用口令
* 对所有账号运行口令破解工具，检查是否存在弱口令或没有口令的账号

Web服务访问控制由：网络通信、用户身份认证、操作系统、数据库

Apache httpd保护/secret，限定ip地址，子网或域名可以访问，则需在access.conf中加一个类似下面的目录控制段

<Directory /full/path/to/secret>

<Limit GET POST>

deny from all

allow from x.y.z XXX.XXX.XXX.cn

allow from a.b.c.d

</Limit>

</Directory>

第8章 防火墙技术原理与应用

安全区域：公共外部网络、内联网、外联网、军事缓冲区域DMZ

防火墙的访问控制可以作用于：网络接口层、网络层、传输层、应用层

访问墙的功能：过滤非安全的网络访问、限制网络访问、网络访问审计、网络带宽控制、协同防御

防火墙的风险：1）网络安全旁路 2）防火墙功能缺陷（1-不能防止感染病毒的软件或文件传输 2-不能防止基于数据驱动攻击 3-不能防止后门攻击） 3）防火墙安全机制形成单点故障和特权威胁 4）防火墙无法有效防范内部威胁 5）防火墙效用受限于安全规则

防火墙类型：包过滤防火墙、代理防火墙、下一代防火墙、Web应用防火墙、数据库防火墙、工控防火墙

防火墙实现技术：

* 包过滤 –根据ip地址、目的IP地址、源端口、目的端口、方向进行判断是否允许包通过



优点：低负载、高通过率、对用户透明

缺点：不能在用户级别过滤、不能识别不同的用户和防止IP地址的盗用

* 状态检测 步骤

1）接收数据包 2）检查数据包的有效性，若无效丢弃 3）有效，查找会话表，若找到，检查数据包的序列号和会话状态，若有效则进行地址转换和路由，转发该数据包，否择丢弃 4）当会话表中没有新到德数据包信息时，则查找策略表，如符合策略表，则怎加会话条目到会话表，并进行地址转换和路由，转发该数据包，否择，丢弃该数据包

* 应用服务代理 中间人角色 （应用代理服务器、身份验证服务程序构成）

优点：1、不允许外部主机直接访问内部主机 2、支持多种用户认证方案 3、可以分析数据包内部的应用程序 4、可以提供详细的审计记录

缺点：1、速度比包过滤慢 2、对用户不透明 3、不能支持所有网络协议

* 网络地址转换： 静态NAT(一对一)、NAT池（随机对应）、端口NAT（ip+端口）
* 协议分析
* 深度包检查

Web防火墙： 功能：允许/禁止HTTP请求类型、HTTP协议头各个字段的长度限制、后缀名过滤、URL内容关键字过滤、Web服务返回内容过滤

可抵御攻击：SQL注入、XSS跨站脚本攻击、Web应用扫描、webshell、Cookie注入攻击、CSRF攻击

数据库防火墙： 源地址、目标地址、源端口、目标端口、SQL语句，阻断违规SQL操作

下一代防火墙：功能：1、应用识别和管控 2、入侵防护（IPS） 3、数据防泄露 4、恶意代码防护 5、URL分类与过滤 6、带宽管理和Qos优化 7、加密通信分析

双宿主主机防火墙 两个网卡

代理型防火墙（屏蔽主机）: 位于内部网络

优点：代理型比双宿主主机结构提供更好的安全保护，操作简单

缺点：攻破了代理主机，就可以侦听到内部网络的所有信息

屏蔽子网防火墙：DMZ区

优点：安全级别更高 缺点：成本高、配置复杂

第9章 VPN技术原理和应用

主要安全服务：保密性服务（防止被监听）、完整性服务（防止被修改）、认证服务（防止非法接入）

VPN类型：链路层VPN、网络层VPN、传输层VPN

VPN实现技术：密码算法、密钥管理、认证访问控制、IPSec(网络层)、SSL（应用层和网络层之间）、PPTP、L2TP

VPN采用的多种安全机制：隧道技术、加密技术、身份认证技术、密钥管理技术、访问控制

隧道的实质是一种封装 第二层隧道：PPTP 第三层隧道：IPSec IP安全协议

IPSec工作模式：传输模式、隧道模式

SLL:传输层的安全协议，介于应用层和TCP层之间

PPTP:提供认证、压缩。它是点到点的安全隧道协议

IPSec VPN 功能：随机数生成、密钥协商、安全报文封装、NAT穿越、身份鉴别

SSL VPN功能：随机数生成、密钥协商、安全报文传输、身份鉴别、访问控制、密钥更新、客户端主机安全检查

VPN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（Intranet VPN）、企业扩展虚拟网（Extranet VPN）

第10章 入侵检测技术原理与应用

入侵检测的作用：

* 发现受保护系统中的入侵行为或异常行为
* 检验安全保护措施的有效性
* 分析受保护系统所面临的威胁
* 有利阻止安全事件扩大，及时报警出发网络安全应急响应
* 可以为网络爱不起策略的制定提供重要指导
* 报警信息可用作网络犯罪取证

入侵检测的技术

* 基于误用的入侵检测技术 -- 特征匹配

基于条件概率的误用检测方法、基于状态迁移的误用检测方法、基于键盘监控的误用检测方法、基于规则的误用检测方法

* 基于异常的入侵检测技术 --- 与正常的数值比，表现异常的

优点：1、符合数据异常变化理论，适合事务的发展规律

2、检测算法普适化，对变量跟踪不需要大量的内存

3、有能力检测与响应某些新的攻击

缺点：1、数据假设可能不合理，加权算法在统计意义上可能不准确

2、对突发事件容易引起误判

3、对长期、稳定的攻击方法的灵敏度低

基于统计的异常检测方法、基于模式预测的异常检测方法、基于文本分类的异常检测方法、基于贝叶斯推理的异常检测方法

入侵检测系统组成： 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、相关辅助模块

基于主机的入侵检测系统HIDS，收集日志文件，调用系统资源、网络通信、用户使用信息，分析是否包含攻击特征

入侵检测的指标：可靠性、可用性、可扩展性、时效性、准确性和安全性

入侵检测的部署：1、确定要监测的对象或网段 2、安装IDS探测器，采集网络入侵检测所需的信息 3、制定相应的检测策略 4、选用合适的IDS结构类型 5、配置入侵检测规则 6、测试验证是否正常执行 7、允许和维护IDS

第11章 网络物理隔离技术原理与应用

分类：单点隔离、区域分离

技术：专用计算上网、多PC、外网代理服务、内外网线切换器、单硬盘内外分区、双硬盘、网闸、协议隔离、单向传输、信息摆渡、物理断开

第12章 网络安全审计技术原理与应用

标准：TCSEC：C2级开始提出安全审计要求 B3级之后更高级别不再变化

国家标准GB17859 ：第二级开始要求提供审计安全机制

计算机系统安全保护能力等级：主席爱街坊

用户自主保护级、系统审计保护级（客体保护，阻止非授权）、安全标记保护级（读出标记）、结构化保护级（审计隐藏）、访问验证保护级（监控安全）

网络安全审计系统组成：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

网络安全审计系统类型： 按审计对象类型分类： 操作系统安全审计、数据库安全审计、网络通信安全审计、应用系统安全审计、网络安全设备审计、工控安全审计、移动安全审计、互联网安全审计、代码安全审计

Windows审计信息：注册登录事件、目录服务访问、审计账号管理、对象访问、审计策略变更、特权使用、进程跟踪、系统事件

Linux审计信息：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、用户当前登录日志utmp、用户退出日志wtmp、系统接收和发送邮件日志maillog、系统消息messages

数据库审计：读、写、查询、添加、删除、修改操作，对数据库操作进行回放

网络通信安全审计：IP源地址、IP目的地址、源端口号、目的端口号、协议类型、传输内容

网络审计数据安全分析技术：字符串匹配、全文搜索、数据关联、统计报表、可视化分析

网络审计数据保护技术：系统用户分权管理、审计数据强制访问、审计数据加密、审计数据隐私保护、审计数据完整性保护

日志安全审计：日志采集、日志存储、日志分析、日志查询、事件警告、统计报表、系统管理

第13章 网络安全漏洞防护技术原理与应用

基于漏洞的安全威胁：敏感信息泄露、非法授权访问、身份假冒、拒绝服务

网络安全漏洞的来源：非技术性安全漏洞- - 管理组织结构、管理制度、管理流程、人员管理 技术性安全漏洞 - - 网络结构、通信协议、设备、软件产品、系统配置、应用系统

非技术性安全漏洞的主要来源：

* 网络安全责任主体不明确
* 网络安全策略不完备
* 网络安全操作技能不足
* 网络安全监督缺失
* 网络安全特权控制不完备

技术安全漏洞的主要来源

* 设计错误
* 输入验证错误
* 缓冲区溢出
* 意外情况处置错误
* 访问验证错误
* 配置错误
* 竞争条件
* 环境错误

漏洞分类：注入、未验证的重定向和转发、失效的身份认证、XML外部实体（XXE）、敏感信息泄露、失效的访问控制、安全配置错误、跨站脚本（XSS）、不安全的反序列化、使用含有已知漏洞的组件、不足的日志记录和监控、非安全加密存储

网络安全漏洞管理过程：

* 网络信息系统**资产确认**
* 网络安全漏洞**信息采集**
* 网络安全**漏洞评估**
* 网络安全**漏洞消除和控制**
* 网络安全**漏洞变化跟踪**

漏洞发现方法：人工安全性分析、工具自动化检测、人工智能辅助分析

漏洞发现技术：文本搜索、词法分析、范围检查、状态机检查、错误注入、模糊测试、动态污点分析、形式化验证

网络安全漏洞利用防范技术

* 地址空间随机化技术 - - 通过对程序加载到内存地址进行随机化处理，使得攻击者不能事先确定程序的返回地址
* 数据执行阻止 - - 操作系统通过对特定的内存区域标注为执行，使得代码不能在指定的内存区域运行
* SEHOP – 防止攻击者利用SHE重写
* 堆栈保护 - - -设置堆栈完整性标记以检查函数调用返回地址是否被篡改，从而阻止攻击者利用缓冲区漏洞
* 虚拟补丁

第14章 恶意代码防范技术原理

恶意代码：计算机病毒Computer Virus 、蠕虫Worms、特洛伊木马Trojan Horse、逻辑炸弹Logic Bombs、细菌Bacteria、恶意脚本Malicious Scripts、恶意ActiveX控件、间谍软件Spyware

恶意代码攻击技术：进程注入技术、超级管理技术、端口反向链接技术、缓冲区溢出攻击技术

恶意代码分析方法：静态分析法（反恶意软件检查、字符串分析、静态反编译分析）、动态分析法（文件监测、进程监测、注册表监测、动态反汇编分析）

特洛伊木马防范技术：

* 基于**查看开放端口**检测特洛伊木马技术
* 基于**重要系统文件**检测特洛伊木马技术
* 基于**注册表**检测特洛伊木马技术
* 检测具有隐藏能力的特洛伊木马技术
* 基于网络检测特洛伊木马技术
* 基于网络阻断特洛伊木马技术
* 清除特洛伊木马技术

网络蠕虫防范技术

* 网络蠕虫监测与预警技术 -- 安装探测器
* 网络蠕虫传播抑制技术 -- 蜜罐
* 网络系统漏洞检测与系统加固技术
* 网络蠕虫免疫技术 – 欺骗
* 网络蠕虫阻断与隔离技术 -- 路由器、防火墙
* 网络蠕虫清除技术 –删除文件、注册表、进程

僵尸网络，构建方式：远程漏攻击、弱口令扫描入侵、邮件附件、恶意文档、文件共享、网页挂马

步骤：1、僵尸程序传播 2、操作受害机组成网络 3、执行攻击

僵尸网络防范技术：威胁监测、监测、主动遏制、查杀

第15章 网络安全主动防御技术与应用

原理：通过对目标对象的网络攻击行为进行阻断、从而达到保护目标对象的目的

IPS/SPS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

IPS/SPS安全功能：1、屏蔽指定IP地址 2、屏蔽指定网络端口 3、屏蔽指定域名 4、封锁指定URL、阻断特定攻击类型 5、为零日漏洞提供热补丁

网络流量清洗技术：清除目标对象的恶意流量，以保障正常网络服务通信

网络流量清洗场景：畸形数据报文过滤、抗拒绝服务攻击、Web应用保护、DDos高防IP服务

网络流量清洗技术： 1、流量检测 2、流量牵引与清洗 3、流量回注

可信计算计算应用

* 计算平台安全保护 --完整性度量和检查，防止恶意代码篡改BIOS、操作系统和应用软件
* 可信网络连接 - - 身份认证、完整性认证
* 可信验证

数字水印应用场景：敏感信息增加保护、防范电子文件非授权扩散、知识产权保护、网络攻击活动溯源、敏感信息访问控制

数字水印技术应用：版权保护、信息隐藏、信息溯源、访问控制

网络攻击陷阱技术应用：恶意代码监测、增强抗攻击能力、网络态势感知

域名服务安全风险：域名信息篡改、域名解析配置错误、域名劫持、域名软件安全漏洞

第16章 网络安全风险评估技术原理与应用

网络安全风险评估过程：1、网络安全风险评估准备 2、资产识别 3、威胁识别 4、脆弱性识别 5、已有的网络安全措施封闭性 6、网络安全风险分析 7、网络安全风险处置与管理

脆弱性识别方法：漏洞扫描、人工扫描、问卷调查、安全访谈、渗透测试

网络安全风险分析步骤：

* 对资产进行识别，并对资产的价值进行赋值
* 对威胁进行识别，描述威胁的属性，并对威胁出现的频率赋值
* 对脆弱性进行识别，并对具体资产的脆弱性的严重程度赋值
* 根据威胁及威胁利用脆弱性的难易程度判断安全事件发生的可能性
* 根据脆弱性的严重程度及安全事件所作用的资产价值计算安全事件的损失
* 根据安全事件发生的可能性及安全事件出现后的损失，计算安全事件一旦发生对组织的影响。

网络安全风险分析方法：定性计算方法、定量计算方法、综合计算方法

网络安全风险评估技术：资产信息收集、网络拓扑发现、漏洞扫描、人工检查、安全渗透

人工智能安全风险：训练数据安全风险、算法安全风险、系统代码实现安全风险、技术滥用风险、高度自治智能系统导致社会安全风险

第17章 网络安全应急响应技术原理与应用

网络安全事件类型：恶意程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件、其他信息

安全事件分级：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、一般网络安全事件

网络安全应急处理流程： 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

第18章 网络安全评测技术与标准

1999年，我国颁布了《计算信息系统系统安全保护等级划分准则》

测评主要包括：安全功能检测、安全管理检测、代码安全审查、安全渗透、信息系统攻击测试

测评主要包括：技术安全测评、管理安全测评

技术安全测评：物理环境、通信网络、区域边界、计算环境、管理中心

管理安全测评：制度、机构、人员、建设、运维

网络安全渗透测试过程：

* 用户确认渗透性目标
* 签定授权书及撰写测试方案
* 确定渗透时间、执行渗透方案
* 汇总分析渗透数据，验证安全威胁场景及安全影响
* 撰写渗透分析报告及安全改进建议

第19章 操作系统安全保护

操作系统安全需求：标识与鉴别、访问控制、系统资源安全、网络安全、抗攻击、自身安全

操作系统安全机制：硬件安全、标识与鉴别、访问控制、最小特权管理、安全审计、可信路径、系统安全增强

Windows系统安全问题：口令、恶意代码、应用软件漏洞、系统程序漏洞、注册表安全、文件共享安全、物理临近攻击

安全增强方法：

* 安全漏洞打补丁
* 停止服务或卸载软件
* 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

安全增强步骤：

* 确认系统安全增加的目标和业务用途
* 安装最小化的操作系统
* 安装最新的系统补丁
* 配置安装的系统服务
* 配置安全策略 – 密码复杂度要求、用户锁定阀值、时间、计数器
* 禁用NetBIOS – 过滤135~139、445端口
* 账户安全配置 – 禁用默认账号、定期检测账户、尽早发现可疑账户、关闭Guest账户
* 文件系统安全配置 – 删除不必要文件、应用程序，启用加密文件系统，设置文件共享口令，修改系统默认的安装目录名
* 配置TCP/IP筛选和ICF -- 过滤不使用的端口、应用层网络服务、ICMP数据包
* 禁用光盘或软盘启动
* 使用屏幕保护口令
* 设置应用软件安全
* 安装第三方防护软件

账号与口令管理安全增强：1、停掉guest账号 2、限制不必要的用户数量 3、把系统administrator账号改名 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名 8、开启口令安全策略 9、开启账号策略

网络安全增强：1）紧张建立空连接 2）关闭默认共享 3）关闭不必要的网络服务和网络端口

Linux三层：硬件层、系统内核、应用层

Linux认证：1、基于口令的认证方式 2、终端认证 3、主机信任机制 4、第三方认证

Linux系统安全增强方法：

* 给安全漏洞打补丁
* 停止不必要的服务
* 升级或替换软件包
* 修改系统配置
* 安装专用的安全工具软件

Linux系统安全加固步骤

* 确定系统的安全目标
* 安装最小化Linux系统
* 利用Linux系统自身安全机制，配置安全策略
* 利用第三方软件包增强系统安全
* 检测Linux系统的安全策略的有效性或安全隐患
* 根据系统安全测试，重新调整安全策略或安全措施
* 安全检查通过，Linux系统开始正常运行

Linux系统安全增强技术

* 安装系统补丁软件包
* 最小化系统网络服务
* 设置系统开机保护口令
* 弱口令检查
* 禁用默认账号
* 用SSH增强网络服务安全
* 利用tcp\_wrapper增强访问控制
* 构筑Linux主机防火墙
* 使用Tripwire或MD5Sum完整性检测工具
* 检测LKM后门
* 系统安全监测

Linux安全增强措施

* 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
* 限制远程访问
* 用户超时注销
* 注销时删除命令记录

国产操作系统风险：Linux内核安全风险、自主研发系统组件的安全、依赖第三方系统组件的安全、系统安全配置的安全、硬件安全

第20章 数据库系统安全

数据库安全威胁：授权的误用、逻辑判断和汇聚、伪装、旁路控制、隐蔽信道、SQL注入攻击、数据库口令密码破解、硬件及介质攻击

数据库安全隐患：数据库用户账号和密码隐患、数据库系统扩展存储过程隐患、数据库系统软件和应用程序漏洞、数据库系统权限分配隐患、数据库系统用户安全意识薄弱、网络通信内容是明文传递、数据库系统安全机制不健全

数据库安全需求：标识与鉴别、访问控制、安全审计、备份与恢复、加密、资源限制、安全加固、安全管理

数据库防火墙的安全作用：

* 屏蔽直接访问数据库的通道
* 增强认证
* 攻击检测
* 防止漏洞利用
* 防止内部高危操作
* 防止敏感数据泄露
* 数据库安全审计

Oracle安全最佳实践：

* 增强oracle数据库服务器的操作系统安全
* 最小化安装oracle，删除不必要的组件
* 安装最新的安全补丁
* 删除或修改默认的用户和密码
* 启用认证机制
* 设置好的口令密码策略
* 设置最小化权限
* 限制连接oracle的IP地址
* 传输加密
* 启用oracle审计
* 定期查看oracle漏洞发布信息
* 实施Oracle灾备计划

Sql Server安全机制：用户身份认证、访问控制、数据库加密、备份恢复机制、安全审计

SQL Server安全最佳实践：

* 设置好的数据库密码安全策略
* 加强扩展存储过程，删除不必要的存储过程
* 网上数据加密传输
* 修改数据库默认的TCP/IP端口号
* 对SQL数据库访问的网络连接进行IP限制
* 启用SQL Server日志审计，记录所有的用户访问和分析安全事件日志
* 定期查看MS SQL Server漏洞发布信息，及时修补漏洞
* 保证MS SQL Server的操作系统安全
* MS SQL Server安全检测，制定安全容灾备份计划

My SQL 安全机制：用户身份认证、授权访问、安全审计

My SQL 安全最佳实践：

* MySQL 安装，单独启动MySQL 的用户和组
* 建立MySQL Chrooting运行环境，形式沙箱保护，增强系统抗渗透能力
* 关闭MySQL的远程连接
* 禁止MySQL导入本地文件
* 修改MySQL的root用户ID和密码
* 删除MySQL的默认用户和db
* 更改MySQL的用户名，防止口令暴力破解
* 建立应用程序独立使用数据库和用户账号
* 安全监测
* 安全备份

第21章 网络设备安全

交换机面临的网络安全威胁： MAC地址泛洪、ARP欺骗、口令威胁、漏洞利用

路由器面临的网络安全威胁：漏洞利用、口令安全威胁、路由协议安全威胁、Dos/DDos威胁、依赖性威胁

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

交换机安全增加的技术方法

* 配置交换机访问口令和ACL,限制安全登录
* 利用镜像技术监控网络流量
* MAC地址控制技术

1. 设置最多可学习到的MAC地址数
2. 设置系统MAC地址老化时间

* 安全增强

1. 关闭不需要的网络服务
2. 创建本地账号
3. 启用SSH服务
4. 限制安全远程访问
5. 限制控制台的访问
6. 启动登录安全检查
7. 安全审计
8. 限制SNMP访问
9. 安全保存交换机IOS软件镜像文件
10. 关闭不必要的端口
11. 关闭控制台及监测的审计
12. 警示信息

路由器安全增加技术方法

* 及时升级操作系统和补丁
* 关闭不需要的网络服务

1. 禁止CDP
2. 禁止其他的TCP\UDP Small服务
3. 禁止Finger服务

* 明确禁止不使用的端口
* 禁止IP直接广播和源路由
* 增强路由器CTX安全
* 阻断恶意数据包
* 路由器口令安全
* 传输加密
* 增强路由器SNMP的安全

第22章 网站安全需求分析与安全保护工程

网站安全：机密性、完整性、可用性、可控性

网站安全威胁：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、网站后台管理安全威胁

Apache Web配置：httpd.conf-主配置、conf/srm.conf-数据配置、conf/access.conf-读取文件控制、conf/access.conf-MIME格式

Apache Web安全威胁：软件程序威胁、软件配置威胁、安全机制威胁、应用程序威胁、服务通信威胁、服务内容威胁、拒绝服务威胁

Apache Web安全机制

* 本地文件安全
* 模块管理机制
* 认证机制
* 链接耗尽应对机制 – 应对拒绝服务攻击
* 自带分访问机制
* 审计和日志
* 防范Dos

Apache Web 安全增强

* 及时安装Apache Web补丁
* 启用.htaccess文件保护网页
* 为Apache Web服务软件设置专门的用户和组
* 隐蔽Apache Web 软件的版本号
* Apache Web 目录访问安全增强
* Apache Web 文件目录保护
* 删除Apache Web默认目录或不必要的文件
* 使用第三方软件安全增强Apache Web服务

IIS 安全威胁：非授权访问、网络蠕虫、网页篡改、拒绝服务、IIS软件漏洞

IIS安全增强：

* 及时安装IIS补丁
* 启用动态IP限制
* 启用URLScan
* 启用IIS web应用防火墙
* 启用SSL服务

漏洞排名TOP10

1. 注入漏洞 - -SQL、NoSQL、OS、LDAP注入漏洞
2. 遭受破坏的认证
3. 敏感数据暴露漏洞
4. XML-外部实体引用漏洞
5. 受损害的访问控制漏洞
6. 安全配置错误
7. 跨站脚本漏洞
8. 非安全反序列化漏洞
9. 使用含有已知漏洞的组件

10非充分的日志记录和监控

WEB 应用漏洞防护

* SQL注入漏洞分析与防护

1. 对应用程序输入进行安全过滤
2. 设置应用程序最小化权限
3. 屏蔽应用程序错误提示信息
4. 对开源web应用程序做安全适应性改造

* 文件上传漏洞分析与防护

1. 将上传目录设置为不可执行，避免上传文件远程触发执行
2. 检查上传文件的安全性，阻断恶意文件上传

* 跨站脚本攻击

网站安全保护机制：

* 身份鉴别 – 用户名/口令、U盾、人脸识别
* 访问控制 – 防止非授权的用户访问网站资源
* 网站内容安全 – 确保网站符合法律法规及政策要求。 措施：网站内容安全检查、网页防篡改、敏感词过滤
* 网站数据安全 – 措施：用户数据隔离、加密、SSL、备份、隐私保护
* 网站安全防护 – 增强抗攻击能力 支持DDOS清洗
* 网站安全审计与监控 – 措施：syslog、web流量截取、网页篡改或挂马检查、Web入侵检测、电子取证
* 网站应急响应 – 措施：网页防篡改、网站域名服务灾备、网络流量清洗、灾备中心、网络攻击取证
* 网站合规管理 -- 网站备案、防伪识别、等保测评
* 网站安全测评 – 措施：漏洞扫描、渗透测试、代码审核、风险分析
* 网站安全管理机制

第23章 云计算安全需求分析与安全保护工程

云计算概念：按需服务、弹性化的IT资源池服务平台

云计算的主要特征

* IT资源以服务形式提供 ： 基础设施即服务Iaas、平台即服务Paas、软件即服务SaaS、数据即服务DaaS、存储即服务STaaS
* 多用户共享IT资源 -- 功能、性能、故障隔离
* IT资源按需定制与按用付费
* IT资源可伸缩性部署 - - 私有云、社区云、公有云、混合云

云计算技术安全需求

* 云端安全需求分析 --确保云用户能够获取可信云服务

1. 云用户身份标识和鉴别
2. 云用户资源访问控制
3. 云用户数据安全存储
4. 云端设备及服务软件安全

* 网络安全通信安全需求分析 – 确保云用户及时访问云服务及网上数据的安全性

技术包括：身份认证、密钥分配、数据加密、信道加密、防火墙、VPN、抗拒绝服务

* 云计算平台安全需求分析 – 确保云服务的安全可信性和业务连续性

主要有：物理环境安全、主机服务器安全、操作系统安全、数据库安全、应用及数据安全、云操作系统安全、虚拟机安全、多租户安全隔离

第24章 工控安全需求分析与安全保护工程

工业工控系统安全威胁分析：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

工业控制系统安全隐患：工控协议安全、工控系统技术产品安全漏洞、工控系统基础软件安全漏洞、工控系统算法安全漏洞、工控系统设备固件漏洞、工控系统开放接入漏洞、工控系统供应链安全

工控系统安全保护机制与技术： 物理及环境安全防护、安全分区及边界保护、身份认证与访问控制、远程访问安全、恶意代码防范、数据安全、网络安全检测与应急响应、安全管理

第25章 移动应用安全需求分析与安全保护工程

移动应用安全分析：

* 移动操作系统平台安全威胁
* 无线网络攻击
* 恶意代码
* 移动应用代码逆向工程
* 移动应用程序非法篡改

Android系统安全机制

* 权限声明机制
* 应用程序签名机制
* 沙箱机制
* 网络通信加密
* 内核安全机制

IOS系统安全机制

* 安全启动链
* 数据保护
* 数据加密与保护机制
* 地址空间布局随机化
* 代码签名
* 沙箱机制

移动应用APP安全加固：防反编译、防调试、防篡改、防窃取

移动应用APP安全检测：身份认证机制检测、通信会话安全机制检测、敏感信息保护机制检测、日志安全策略检测、交易流程安全机制检测、服务端鉴权机制检测、访问控制机制检测、数据防篡改能力检测、防SQL注入能力检测、防钓鱼安全能力检测、APP安全漏洞检测

第26章 大数据集安全需求分析与安全保护工程

大数据安全威胁：

* “数据集”安全边界日渐模糊，安全保护难度提升
* 敏感数据泄露安全风险增大
* 数据失真与大数据污染安全风险
* 大数据处理平台业务连续性与拒绝服务
* 个人数据广泛分布于多个数据品后台，隐私保护难道加大
* 数据交易安全风险
* 大数据滥用

大数据安全需求分析：

* 大数据自身安全 -- 真实性、实时性、机密性、完整性、可用性、可追溯性
* 大数据安全合规 -- 满足数据安全政策法规
* 大数据跨境安全
* 大数据隐私保护
* 大数据处理平台安全
* 大数据业务安全
* 大数据运营安全