ONEPASS 第一章 网络信息安全概述重点案例

1. 网络安全基本属性

机密性、完整性、可用性、抗抵赖性、可控性（CIA+抵赖，可控）

1. 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

1. 网络安全管理流程（不作为重点）

确定管理对象、评估管理对象价值、识别管理对象威胁、识别管理对象脆弱性、确定管理对象风险级别、制定防范体系措施、落实防范措施、运维设备

1. 网络安全等级保护

定级、备案、整改、测评、监察运维

1. 网络信息安全管理工具

网络安全管理平台（SOC）、IT资产管理系统、网络安全台式感知系统、网络安全漏洞扫描器、网络安全协议分析器、上网行为管理

ONEPASS 第二章 网络攻击原理重点案例

1. DOS攻击步骤

探测扫描大量主机，寻找可攻击目标

攻击有安全漏洞的主机，并获取控制权

在攻击成功的主机安装客户端攻击程序

利用已攻击成功的主机继续扫描攻击其他主机

攻击客户端达到一定数量后，攻击者可以从主控端给被控端发布攻击指令攻击目标机器

1. 网络攻击过程

隐藏攻击源、收集攻击目标信息、挖掘漏洞信息、获取目标访问权限、隐蔽攻击行为、实施攻击、开辟后门、清除攻击痕迹

1. 网络攻击技术方法

端口扫描、口令破解、缓冲区溢出、恶意代码、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（此项作为了解，稍微背两个，不用全背）

1. 网络攻击四个危害行为

信息泄露、完整性破坏、拒绝服务、非法使用

ONEPASS 第三章 密码学基本理论重点案例

1. 密码系统的安全性依赖密码管理，密码管理的三个方面：密钥管理、密码管理政策、密码测评。
2. 密钥生命周期：生成、存储、分发、使用、更新、撤销、备份、恢复、销毁、审计。
3. DIFFIE-HELLMAN 看一下过程 交换协议
4. RSA 计算公式 掌握算法

P\*q=n (p-1)\*(q-1))=φ(n) ed=1modφ(n)

C=m^e mod n M=c^d mod n

大合数因子分解 公式里的D一般代表私钥，也是最后要求的

掌握乘法逆

10n 01a n为模数 假设57mod106 n为106 a为57

Q=x3/y3

T1=x1-q\*y1

T2=x2-q\*y2

T3=x3-q\*y3

最后求出x3=1的情况下 x2为逆元

X1 x2 x3 y1 y2 y3

1 0 n 0 1 a

掌握降幂

2^56次方mod 119

56化二进制，倒序写上来 只算1的 从上到下依次2mod119,2^2mod119... 最后算出来1的结果相乘MOD 119

1. 网络安全体系与网络安全模型重点案例

网络安全体系特征：整、协、过、全、适（整体性、协同性、过程性、全面性、适应性）

P2DR: 防护 检测 响应 策略

PDRR: 防护 检测 响应 恢复 = 纵深防御模型四道防线

PDCA: 计划 执行 检测 处理

WPDRRC: 预警 防护 检测 响应 恢复 反击 （智能交通）

NIST核心功能：识别 保护 检测 响应 恢复（PDRR基础上多识别）

网络安全基础设施：网络安全数字认证服务中心、网络安全测评认证中心、网络安全运营中心

密级：绝密、机密、秘密、公开

资产级别：公开 内部 机密 限制

数据安全能力成熟度模型：组织建设、制度流程、技术工具、人员能力

分层防护模型：用户层、应用层、系统层、网络层、物理层（用应系网物）

网络生存模型的3R策略：抵抗、识别、恢复（石灰地）

1. 物理与环境安全技术重点案例

容灾容错存储技术：磁盘阵列、双击在线备份、离线备份 保护存储数据及系统正常运行。

物理安全威胁：自然、人为

信息系统物理安全保护标准：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

灭火器四类：水、二氧化碳、固态化学品、卤代烷

供电安全3宝：专用供电线路、UPS、备用发电机

机房场地要求：环境安全、地址可靠、抗电磁干扰、避开强震源声源、避免在建筑物高层用水设备下层或隔壁

数据中心分类：10000以上大型 3000-10000中型 3000以下小型

IDC数据中心6大系统组成：基业资管网安（基础设施、业务系统、资源系统、管理系统、网络系统、安全系统）

CA机房至少5年进行一次屏蔽室检测 （读一遍就行）

网络通信线路防护：设备冗余、相互备份、多路通信

存储介质防护：安全管理、加密保存、容灾容错

设备实体防护：设备标记、设备电磁辐射防护、静电用电防护、磁场抗扰、环境安全保护、适用性可用性、

硬件木马检测：功耗分析法、反向分析法、侧信道分析法

存储系统威胁：管理失控、数据泄密、设备故障、数据非安全删除、恶意代码攻击

数据中心强制要求：所有金属设备必须接地、耐火等级不低于2级、数据中心墙耐火极限不低于2小时、楼板耐火极限不低于1.5小时、应由2组独立的火灾探测器（读一遍就行）

1. 认证技术原理与应用重点案例

Kerberos认证过程

1. 客户向AS服务器请求TGS票据
2. AS服务器发送TGT给客户
3. 客户发送TGT和应用服务票据申请给TGS服务器
4. TGS服务器发送应用票据给客户
5. 客户发送会话票据到应用服务器
6. 应用服务器确认请求

口令认证过程

1. A发送消息（Ua,Pa）到B
2. B收到消息后检查（Ua,Pa）正确性，若正确通过A的认证
3. B回复A验证结果消息

智能卡认证过程

1. 用户将自己ID发送给目标系统
2. 系统提示用户输入数字
3. 用户从智能卡上读取数字
4. 用户将数字发送给系统
5. 系统核对数字ID，并生成一个数字显示给用户，称为挑战
6. 用户将上面的挑战输入智能卡中
7. 智能卡根据输入的数字算出一个新的结果并显示，称为应答
8. 用户将应答输入系统
9. 系统验证是否正确，若正确则登录进入系统

三方认证过程：(ID为标识r为随机数)

1. A向三方P发送加密消息Kpa(IDb,Ra)
2. P收到消息后解密获得A消息，生成消息Kpa(Ra,Kab)和Kpb(IDa,Kab)发送给A
3. A发送Kpb(IDa,Kab)到B
4. B解密Kpb(IDa,Kab)生成Kab(IDa,Rb)发给A
5. A解密Kab(IDa,Rb)生成Kab(IDb,Rb)发送给B
6. B解密Kab(IDb,Rb)，检查Rb正确性，正确通过
7. B回复A验证结果消息

认证分类：单向认证、双向认证、三方认证

认证依据：所知道的秘密信息（口令验证码）、所拥有的实物凭证（智能卡U盾）、所具有的生物特征（指纹声音虹膜人脸）、所表现的行为特征(使用鼠标键盘习惯等)

一次性口令简称OTP

持续认证鉴定因素：认知因素、物理因素、上下文因素（事务、导航、设备、网络模式）

认证由标识、鉴别两部分组成

1. 访问控制技术原理与应用重点案例

主体、客体、授权三要素

访问控制目标：防止非法用户进系统 阻止合法用户对系统资源非法使用越权访问

访问控制参考模型：主体、客体、监视器、访问控制数据库、审计库

访问控制类型：自主访问控制（DAC）、强制访问控制（MAC）、基于角色访问控制（RBAC）、基于属性访问控制（ABAC）

角色访问控制：用户 角色 会话 权限（windowsNT windows2000 solaris）

自主访问控制分为：1.基于行自主访问控制（主体）2.基于列自主访问控制（客体）

访问能力表：从行到列

访问控制表：从列到行

访问控制矩阵：从主体和客体的行列关系出发

自主访问控制不足：主要依赖于用户的安全意识，不能满足高安全要求

军事->强制访问控制

访问控制规则：基于用户身份、时间、地址、服务数量、异常事件

访问控制管理5步：1.明确访问控制管理资产2.分析管理资产安全需求3.制定访问控制策略4.实现访问控制策略5.运维访问控制系统（确定资产、分析需求、制定策略、实现策略、运维）

访问控制安全管理三管原则：最小特权、用户访问、口令安全

3A：认证、授权、计账

4A（统一安全管理平台）：认证、授权、审计、账户（把计账拆开拆成审计和账户）

口令安全管理9原则：1.8字符以上大小写特殊符号 2.禁止账号密码一样3.更换系统默认口令4.限制账号登录次数5.禁止共享账户密码6.口令加密存放7.禁止以明文传输口令8.口令经常修改9.用破解工具检查是否存在弱口令

用户访问管理流程9步：1.身份登记2.访问权限分配3.访问权限审查4.访问权限批准5.用户责任确认签字6.按权提供服务7.审计用户访问操作8.检查异常操作并提示或阻止

Web访问控制1请求4允许：1.HTTP访问请求2.客户IP或DNS是否允许3.WEB用户是否允许4.文件系统权限是否允许5.数据库系统权限是否允许（HTTP请求，ip web 文件数据库是否允许）

apache案例限制规则

<directory “允许授权访问的文件夹路径”>

Options all

Allowoverride none

Order deny,allow

Deny from all

Allow from 192.168.0.1/255.255.255.0

</directory>

1. 防火墙技术原理与应用重点案例

防火墙体系结构：双重宿主主机体系 屏蔽主机体系结构 屏蔽子网体系结构

防火墙结构体系特点：双宿主机->以双宿主机作为防火墙主体，分离内外网。 屏蔽主机->1个单独的路由器和内部堡垒机构成防火墙，实现内外网隔离。 屏蔽子网->由两个路由包围起来的周边网络，把容易受攻击的堡垒机放入周边网络中，主要由周边网络、内外部路由器、堡垒机组成。

防火墙工作原理：由软硬件组成的网络访问控制器，根据一定的安全规则控制流过防火墙的网络包，从而起到网络安全屏障的作用。

防火墙可以实现的功能：过滤非安全网路访问、限制网络访问、网络访问审计、网络带宽控制、协同防御

防火墙风险：网络安全旁路、功能缺陷、安全机制形成单点故障和特权威胁、内部威胁、受限于安全规则

白名单默认禁止，黑名单默认允许

包过滤防火墙在网络层

防火墙代理服务器在应用层

屏蔽端口命令：access-list 101 deny tcp any any eq 端口号

In->外部访问内部 进

Out->内部访问外部 出

包过滤防火墙优点：低负载、高通过率、对用户透明

包过滤防火墙缺点：无法在用户级别过滤、不能识别不同用户、无法防止IP盗用

代理服务器分类：ftp代理、telnet代理、http代理、socket代理、邮件代理

状态防火墙处理包过滤步骤：1.接收数据包2.检查数据包的有效性，若无效则抛弃数据包并审计3.查找会话表，若找到，则进一步检查数据包序列号和会话状态，如有效则地址转换和路由转发该数据包，无效，则丢弃数据包并审计4.会话表中没有新数据包信息时，找策略表，符合策略表则增加会话条目到会话表，地址转换和路由转发该数据包，不符合则丢弃数据包并审计

应用服务代理优点：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.可分析数据包内部应用命令4.可提供详细审计记录

应用服务代理缺点:1.速度比包过滤慢2.对用户不透明3.代理服务器不能支持所有的网络协议

网络地址转换三种方式：静态nat、nat池、端口nat

Web应用防火墙能抵御的攻击：sql注入、XSS跨站脚本攻击、web应用扫描、webshell、cookie注入攻击、csrf攻击(熟悉)

Web应用防火墙：modsecurity、webknight、shadow、daemon（熟悉）

web应用防火墙工作原理：预先定义过滤规则和安全防护规则，对所有访问web服务器的http请求进行http协议过滤，从而对web服务器和应用提供安全防护功能。

数据库防火墙工作原理：基于数据通信协议深度分析和虚拟补丁，根据安全规则对数据库访问操作及通信进行安全访问控制，防止数据库系统受到威胁。

工控防火墙工作原理：通过工控协议深度分析，对访问工控设备请求响应进行监控，防止恶意攻击工控设备，实现工控网络安全隔离和工控现场操作安全保护

防火墙共性技术：1.深度包检测2.操作系统3.网络协议分析

目前防火墙产品类型：1.网络防火墙2.web应用防火墙3.数据库防火墙4.主机防火墙5.工控防火墙6.下一代防火墙7.家庭防火墙

防火墙的三种体系结构中屏蔽子网体系结构最为安全，其优点是安全级别最高，其缺点是成本高，配置复杂

防火墙如何部署：1.根据公司安全策略要求，讲网络划分若干安全区域2.在安全区域之间设置针对网络通信的访问控制点3.针对不同访问点的需求，制定相应的边界安全策略4.依据控制点的边界安全策略，采用合适的防火墙技术和防范结构5.在防火墙上配置实现对应的网络安全策略6.测试验证边界安全策略是否正常执行7.运维防火墙

防火墙4个层面访问控制：服务控制、方向控制、用户控制、行为控制

三种防火墙：包过滤（网络层和传输层）、应用层网关（应用层）、电路层网关（传输层）

防火墙处理方式：允许、拒绝、抛弃 accept reject drop

下一代防火墙：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分类过滤6.带宽管理QOS优化7.加密通信分析（背）

防火墙要在进口出口上都进行包过滤，进口防止被攻击，出口防止成为攻击源头跳板

双宿主机优点：网络结构简单、内外网数据没有直接交互、通过代理提供高程度网络控制

双宿主机缺点：用户访问外部资源复杂、用户机制存在安全隐患、一旦双宿主机被入侵，整个内网不安全

1. VPN技术原理与应用重点案例

VPN安全服务：保密性、完整性、认证服务

VPN技术风险：代码缺陷、算法缺陷、管理不当

VPN类型：传网恋（传输层、网络层、链路层）

二层PPTP、L2TP 点对点 认证压缩加密都在2层

三层IPSEC

VPN里 密码算法是核心，由密码算法、秘钥管理、认证访问控制、IPSEC、SSL、PPTP、L2TP组成实现的一门技术

IPSEC（网络层）：AH认证、ESP封装、IKE分发秘钥 （传输、隧道两种模式，隧道既为网络关联）支持ipv4/ipv6

SSL（应用层和传输层间）：具有握手协议（身份鉴别）、记录协议（分片、压缩加密、MAC消息摘要）

IPSEC提供的服务：数据源验证、无连接数据完整性、数据机密性、抗重播（了解）

SSL提供的服务：认证、加密、完整性（了解）

★IPSEC和SSL 2种VPN区别★：前者隧道传输模式、后者CS模式（既客户端-服务端模式）、网关-网关模式

数字信封：先用对称秘钥加密消息、再用对方公钥加密对称秘钥，对方先用私钥解密得到对称秘钥、再解密得消息

VPN三种应用场景：远程、内部、扩展

密码分类：核心密码、普通密码、商业密码

IPSEC(这种VPN的功能)：随密封身NAT（随机数、秘钥协商、安全报文封装、身份鉴别、nat穿越）

SSL（这种VPN的功能）：随密封身基础上+查访更（客户端主机检查、访问控制、秘钥更新）

VPN四种技术保证安全：隧道技术、加密技术、身份认证技术、秘钥管理技术、访问控制

具有最安全、最好的扩展性的vpn是mpls

 第十章 入侵检测技术原理与应用重点案例  
入侵检测是网络安全态势感知的核心关键技术。  
入侵检测框架模型（CIDF）：事件产生器、事件分析器、响应单元、事件数据库  
入侵检测目的：通过检测进行预防，而不是直接阻止入侵发生。  
入侵检测作用：发现、检验、分析、阻止、提供、取证（发现受保护系统的入侵异常行为、检验安全保护措施有效性、分析受保护系统所面临的威胁、阻止安全事件扩大及时报警、可为网络安全策略制定提供指导、报警信息可作为犯罪取证）  
入侵检测技术分两种：误用、异常（前者基于规则库，基于知识，依赖模式攻击库，后者基于行为，拿不正常和正常对比，保存正常特征）  
误用检测优点：具有很强的可分割性、独立性、针对性，有能力提供模糊入侵检测引擎  
误用检测缺点：可测量性和数据库体系结构有关、可扩展性差、不具备自学能力、攻击行为难以模式化  
异常检测四类行为：行不、行却、行既不也不、行且（行为是入侵，不表现异常 、行为是入侵，却表现异常、行为既不是入侵，也不表现异常、行为是入侵，且表现异常）  
异常检测优点：符合数据异常变化理论、检查算法普适化、有能力检测新攻击  
异常检测缺点：数据假设可能不合理、对突发正常事件容易误判、对长期稳定的攻击方法灵敏度低  
误用检测和异常检测的技术分类对比：前者：概率、状态迁移、键盘监控、规则（SNORT），后者：统计、模式预测、文本分类、贝叶斯  
入侵检测系统组成（IDS体系结构）：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  
入侵检测系统分类：基于主机（HIDS）、基于网络（NIDS）、分布式入侵检测系统（HDIDS、NDIDS）  
★万能公式：系统日志、系统调用、应用程序使用、系统资源、网络通信、用户使用★  
基于网络入侵检测硬件：有探测器、管理控制器  
入侵检测的几种系统：主机入侵检测系统、网络入侵检测系统、统一威胁管理、高级持续威胁检测APT  
入侵检测指标：三可时准安（可靠可用可扩展，时效准确安全）  
★IDS部署★1.确定保护的网段2.在保护网段装IDS探测器3.制定检测策略4.选用合适的IDS结构5.在IDS上配置入侵检测规则6.测试IDS安全策略是否正常7.运维IDS  
Snort特点：性能、简单、灵活   有三个子系统（网络包解析器、检测引擎、日志报警系统并内置一套插件作为扩展） 具备嗅探、包记录、入侵检测功能，可作为sniffer嗅探工具，基于模式特征库，典型误用检测工具  
入侵检测模型P2DR：防护、检测、响应、策略  
基于snort硬件配置规则达到过滤效果：关键字（msg“报警信息”，content“规则”）  
★一般在和计算机相连的主设备上装探测器★

第十一章 网络物理隔离技术重点案例

采用物理隔离依然面临的威胁：1.网络非法外联2.U盘摆渡攻击3.网络物理隔离产品安全隐患4.针对物理隔离的新方法（声波、热量等）

网络物理隔离类型按对象分：单点隔离、区域隔离

网络物理隔离类型按信息传递方向分：双向隔离、单向隔离

★网络物理隔离技术★1.专用计算机上网2.多PC（一个上外网一个上内网）3.外网代理4.内外网线路切换器5.单硬盘内外分区6.双硬盘7.网闸8.协议隔离9.单向传输10.信息摆渡11.物理断开

两个独立主机系统与网闸的连接是互斥的（熟悉）

网闸设计目标：1.最大限度规避泄密风险，保证内外网物理断开2.所有信息纯文本交换，并对内容进行审查3.通过密级标识管理，过滤向外传送的文件

单硬盘和双硬盘的区分：双硬盘就是双操作系统

1. 网络安全审计技术

审计都在事后

网络安全审计：对网络信息安全系统的活动信息进行获取、记录、存储、分析、利用的工作

常见安全审计功能：安全事件采集、存储查询

5个等级审计：主席爱街坊

审计日志不少于6个月

审计系统组成：1.审计信息获取2、审计信息存储3.审计信息分析4.审计信息展示利用5.系统管理

审计系统分类：大的方面 2个系统（综合审计系统、单个审计系统）

审计系统分类：小的方面 9个系统（操作系统、数据库、网络通信、应用系统、网络安全设备、工控、移动安全、互联网、代码）

网络安全审计机制：1.基于主机2.基于网络3.基于应用

系统日志采集方式：syslog、snmptrap

网络流量获取技术：1.共享网络监听2.交换机端口镜像3.网络分流器

数据采集软件libcap工作流程：1.设置网络接口2.设置过滤规则3.运行，开始接收符合过滤规则的数据包

网络审计数据分析技术：1.字符串匹配2.全文搜索3.数据关联4.统计报表5.可视化分析

网络审计数据存储技术：1.系统自己分散存储2.集中采集各种系统审计数据

网络审计数据保护技术：1.系统用户分权管理2.审计数据强制访问3.审计数据加密4.审计数据隐私保护5.审计数据完整性保护

主机监控和审计产品：它们都是通过代理程序对主机行为进行信息采集

数据库审计方式：1.网络监听审计2.自带审计3.数据库agent

网络安全审计产品的功能：1.网络流量采集2.网络流量数据挖掘分析

网络安全审计产品功能往细了分的功能：1.字符会话审计2.图形操作审计3.数据库运维审计4.文件传输审计5.合规审计

IT系统运维的威胁：1.内部2.三方外包

网络电子取证：借助日志分析技术提取证据

第十三章 网络安全漏洞防护技术原理与应用重点案例  
网络安全漏洞：又称脆弱性，简称漏洞  
★攻击者基于漏洞对网络安全构成的威胁：信息泄露、非授权访问、身份假冒、拒绝服务（利用漏洞可以干的事）  
漏洞来源：技术性的和非技术性的   
技术性的：1.设计错误2.输入验证错误3.缓冲区溢出4.意外情况处置错误5.访问验证错误6.配置错误7.竞争条件8.环境错误  
非技术性的：1.网络安全责任主体不明确2.网络安全策略不完备3.网络安全操作技能不足4.网络安全监督缺失5.网络安全特权控制不完备  
常见的几种漏洞分类：CVE、CVSS、cnnvd（中国信息安全测评中心）、cnvd、owasp  
★漏洞发布形式：网站、电子邮件、安全论坛、（一般主要由软硬件开发商、安全组织和黑客或者用户发布）  
漏洞信息来源：1.网络安全应急响应机构2.网络安全厂商3.IT产品系统提供商4.网络安全组织（CERT是第一个应急响应组织1988年成立）  
★网络安全漏洞管理过程：1.网络信息系统资产确认2.网络安全漏洞信息采集3.网络安全漏洞评估4.网络安全漏洞消除和控制5.网络安全漏洞变化和跟踪  
★漏洞扫描器模块组成：1.用户界面2.扫描引擎3.漏洞扫描结果分析4.漏洞信息、配置参数库  
★漏洞扫描器分三种：1.主机漏洞扫描器2.网络漏洞扫描器、专用漏洞扫描器  
★常见漏洞扫描器：nmap、nessus、x-scan  
漏洞发现技术：文本搜索、此法分析、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  
漏洞发现工具：splint、wireshark、metasploit、grep、ollydbg  
★补丁管理环节：现状分析、补丁跟踪、验证、安装、应急处理、补丁检查  
★网络安全漏洞防范技术：1.地址空间随机化2.数据执行阻止3.SEHOP 4.堆栈保护5.虚拟补丁  
网络安全漏洞服务平台：漏洞盒子、补天漏洞响应平台、网络威胁服务  
网络安全漏洞防护网关：IPS、waf、utm(统一威胁管理)

第十四章 恶意代码防范技术原理重点案例

恶意代码分主动传播（病毒、木马、间谍软件）被动传播（蠕虫、其他）

★恶意代码攻击过程：1.侵入系统2.维持、提升权限3.隐蔽4.潜伏5.破坏6.重复前5步（此项为重点，考的概率极大）

恶意代码生存技术：1.反跟踪2.加密3.模糊变换4.自动生产5.变形6.三线程7.进程注入8.通信隐藏9.内核级隐藏

★恶意代码攻击技术:1.进程注入2.超级管理3.端口反向链接4.缓冲区溢出

恶意代码分析技术由动态分析技术和静态分析技术构成

★恶意代码防范策略：1.组织管理上加强恶意代码安全防范意识2.通过技术手段实现恶意代码防御 （细分：安全意识、安全操作、安全管理组织、制度、流程、岗位、-----恶意代码检测预警、恶意代码预防、检测恶意代码、恶意代码应急响应）

计算机病毒：具备自我复制、传播能力的程序代码

★凡是计算机病毒都有的特点：1.隐蔽性2.传染性3.潜伏性4.破坏性（无传染性的程序不属于病毒）

病毒组成：1.复制传染部件2.隐藏部件3.破坏部件  
病毒生命周期：1.复制传播阶段2.病毒激活阶段

病毒类型：引导性、宏病毒、多态病毒、隐蔽病毒

★病毒防范策略：1.查找病毒源2.阻断病毒传播途径3.查杀病毒4.应急响应、灾备

★病毒防护分类：1.基于单机计算机病毒防护2.基于网络计算机病毒防护3.基于网络分级病毒防护4.基于邮件网关病毒防护5.基于网关防护

★特洛伊木马：所有木马都不具备传播能力，只是远控工具的一种

★特洛伊木马运行过程：1.寻找攻击目标2.收集目标信息3.将木马植入系统4.木马隐藏5.实施攻击 ★特洛伊木马感染的系统文件主要有：system.ini、config.sys、autostart、startup、explore

特洛伊木马的植入方法：1.文件捆绑2.邮件附件3.WEB网页

特洛伊木马隐藏技术：1.本地活动行为隐藏（文件、进程、通信链接隐藏）2.网络通信过程隐藏（通信内容加密、通信端口复用、网络隐蔽通道）

特洛伊木马防范技术：1.基于查看开放端口检测2.基于重要系统文件检测3.基于系统注册表检测4.rookit检测有隐藏能力的特洛伊木马5.基于网络检测6.基于网络阻断7.清楚特洛伊木马技术（★手工清除、软件清除 原理：删除受害机器的木马文件，进制木马的网络通信，恢复木马修改过的系统文件和注册表）

蠕虫：具备传播、自我复制、独立运行

★蠕虫的组成：1.探测模块2.传播模块3.引擎模块4.负载模块

★蠕虫感染过程：1.搜索发现易感染目标2.传送蠕虫代码到目标主机3.执行蠕虫代码感染目标主机

网络蠕虫传播方法分类：1.随机扫描2.顺序扫描3.选择性扫描

网络蠕虫快速有效传播的方法：减少扫描未用的地址空间、在主机漏洞高的地址空间发现易感染主机、增强感染源

小莫里斯蠕虫病毒利用了unix的脆弱性传播

网络蠕虫防范技术：1.监测预警2.传播抑制3.漏洞检测系统加固3.免疫技术5.阻断隔离6.清除技术

僵尸网络（botnet）:主要以挂马形式构造僵尸网络

僵尸网络防范：1.网络威胁监测2.网络检测3.主动遏制4.程序查杀

细菌：具有自我复制功能的独立程序

陷门：软件系统里的一段代码，允许用户避开系统安全机制访问系统

逻辑炸弹过程：1.程序运行2.判断触发条件3.条件满足激活逻辑炸弹否则控制权转给正常程序

★APT部署：APT检测系统主要布置在核心交换机外，防火墙内

★APT攻击步骤：1.情报收集2.防线突破3.通道建立4.横向渗透5.信息收集

★APT具备的防御功能：1.恶意代码检测2.主机应用保护3.网络入侵分析4.大数据分析检测

APT特性：持续性、组织性、隐蔽性、针对性、旁路

-------------------------------------------------------------------

设备配置防御过滤规则：

Snort入侵检测系统配置规则：

Etc文件夹/Snort.conf为配置文件，rules文件夹为规则库

配置过滤规则时应写入规则库rules文件夹下面的后缀为.rules文件里

1. Alert tcp any any -> 192.168.0.24 111(content:”|00 01 86 a5|”;msg:”mounted access”;)
2. Alert tcp any any -> 192.168.0.24 22(22可替换成any)(msg:”nmap ping sweep scan”;sid:10000005;rev:2;)
3. Alert tcp any any -> any 80(msg:”error based sql injection detected”;content:”%27”;sid100000011;)

Msg:报警信息 content:匹配过滤规则 %27代表单引号

Ospf：authentication-mode md5 1 cipher 123（华为协议认证配置 约定一个数字123用MD5加密）

Iptable防火墙自带过滤规则：

Iptables -A input -P TCP -S 192.168.0.2 -destination -port 23 -jDENY

A:在规则链尾部加新规则（忽略）input 进 -P协议 -S源地址 -d=destination(目标地址) port 端口 jdeny默认拒绝

Tcpdump（协议分析监听）过滤规则：

Tcpdump tcp port 23 and host 192.168.137.128（监听分析192.168.137.128主机的23端口）

Apache过滤规则：

etc/httpd/conf/httpd.conf(路径)

<directory “etc/httpd/www/admin”>

Options all

Allowoverride none

Order deny,allow

Deny from all

Allow from 192.168.0.1/255.255.255.0

</directory>

思科设备过滤端口规则：

Access-list 101 deny tcp any any eq 端口号

1. 网络安全主动防御技术与应用

为什么要用IPS：因为防火墙基于静态访问控制规则，IDS又只能识别记录，不能阻止攻击，只有IPS才是具多功能的安全系统，才能解决当前需求。

★IPS工作原理：根据网络包特性及上下文进行攻击行为判断来控制包转发，工作机制类似路由器或防火墙。

Ips能阻断入侵行为，并对攻击行为进行检测。（SPS旁路监测网络流量，通过旁路注入报文，阻断攻击流量）。

★IPS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

白名单审查流程：初审、复审、终审

软件白名单通过白名单技术限制非授权安装软件包。

★恶意代码防护：基于黑名单（病毒特征库）匹配来防范恶意代码，或者利用白名单技术，只允许可信软件安装执行，可以组织恶意软件安装到目标主机，同时阻断其运行。

白环境保护：只有可信任的设备才能接入控制网络。

★流量清洗技术（防止DDOS攻击）：1.畸形数据报文过滤2.抗拒绝服务攻击3.WEB应用保护4.DDOS高防IP服务

★流量清洗技术原理：通过异常流量检测，将原本发送给目标系统的流量牵引到流量清洗中心，当异常流量清洗完毕后，再把清洗后的正常流量转发给目标系统。

★流量清洗步骤：1流量检测2.流量牵引清洗3.流量回注

流量检测是基于深度数据包检测技术（DPI）

★可信计算：20世纪70年代（jame.p.anderson） 1999年10月（可信计算平台联盟TCPA） 2003年TCPA->TCG 安全芯片（tpm）

★可信计算原理：1.构造一个信任根2.再建一条信任链3.从信任根到硬件平台，操作系统，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可信。

★可信计算包含的基本属性：CIA+可控性

★可信计算能解决的问题：完整性度量 数据安全 身份认证 唯一标识

TPM是可信计算平台的信任根，是可信计算的关键部件。

可信计算技术应用于：计算平台、网络通信连接、应用程序、恶意代码防护

等保2.0以可信计算为基础。

★数字水印特性：（鲁棒性、安全性、透明性）

★数字水印算法组成：（水印、编码器、解码器、比较器）

★数字水印应用领域：版权保护、信息隐藏、信息溯源、访问控制、加指纹、标题注释、篡改提示、使用控制

数字水印嵌入方法（空间域、变换域）

网络攻击陷阱技术：1.蜜罐主机2.陷阱网络

网络攻击陷阱：属于主动攻击，具有恶意代码监测、增强抗攻击能力、网络态势感知等特点。

入侵容忍技术：1.分布式共识2.主动恢复3.门限密码4.多样性设计

★区块链：一个去中心化的分布式数据库。

★域名风险：1.域名信息篡改2.域名解析配置错误3.域名劫持4.域名软件安全漏洞

★域名安全保护措施：1.使用安全账户登记域名2.使用安全系数高的密码3.启用双因素身份认证4.保护电子邮件地址5.谨慎黑客陷阱

域名安全一套系统：有机统一的分布式系统

域名安全两类服务：权威域名服务、递归域名服务

域名安全三个层面：数据管理、域名服务、域名应用

域名安全四个环节：根域名服务、顶级域名服务、其他级域名服务、递归域名服务

yum

1. 网络安全风险评估技术原理与应用重点

网络安全风险评估：对网络系统的保密性、完整性、可控性、可用性等安全属性进行科学评价的过程。

评估要素：资产、威胁、脆弱性、风险、安全措施

风险值=风险概率X影响

风险评估模式：自评估、检查评估、委托评估

★网络风险评估过程：1.风险评估准备2.资产识别3.威胁识别4.脆弱性识别5.已有安全措施确认6.风险计算7.是否接受风险（如果接受保持已有安全措施，如果不接受）8.制定实施风险处理，计划并评估残余风险（是否接受残余风险，不接受返回上一步，接受）9.实施风险管理

威胁识别从几个方面进行：来源、途径、能力、效果、意图、频率

口令威胁：1.网络监听2.口令文件失窃3.口令猜测4.系统非法访问

威胁达到的效果：非法访问、拒绝服务、欺骗

最早的拒绝服务是电子邮件炸弹

脆弱性评估分类：技术脆弱性评估、管理脆弱性评估

★网络安全风险分析步骤：1.资产识别2.威胁识别3.脆弱性识别4.根据威胁、脆弱性判断安全事件发生的可能5.根据脆弱性严重程度计算安全事件的损失

6.计算网络安全风险值

★风险分析方法：定性、定量、定性定量相结合

★网络安全风险管理措施：1.制定安全策略2.建立安全组织3.实施网络资产分类控制4.加强人员安全管理5.保证物理环境安全6.加强安全通信运行7.采取访问控制机制8.进行安全系统开发、运维9.保持业务持续运行10.遵循法律法规，安全目标一致性检查

★网络安全风险评估技术方法：1.资产信息收集2.网络拓扑发现3.漏洞扫描4.人工检查5.安全渗透测试

端口扫描：nmap

漏洞扫描：x-scan、Nessus

数据库扫描：sqlmap

Web扫描：appscan

渗透:metasploit、backtracks、cobaltstnike

审计工具:grep、logparser

网络协议分析器：tcpdump、wireshark

★owasp(web安全组织)风险评估方法：1.确定风险类别2.评估可能性因素3.评估影响因素4.确定风险严重程度5.决定修复内容6.定制合适的风险评价模型

★网络安全风险处理措施：1.管理安全2.物理环境安全3.网络安全4.应用安全5.主机安全

入侵检测可分为：1.主机入侵检测2.网络入侵检测3.应用入侵检测

ICT供应链风险管理目标：CIA+可控

1. 网络安全应急响应技术原理与应用重点案例

第一个计算机安全应急组织CERT.国家互联网应急中心CNCERT或CNCERT/CC

CNCERT职责：积极预防、及时发现、快速响应、力保恢复

网络安全事件类型与分级：事件类型主要有1.恶意程序2.网络攻击3.信息破坏4.信息内容安全5.设备设施故障6.灾害性事件7.其他信息安全事件

事件分级：特别重大、重大、较大、一般

★网络应急预案的内容：1.系统晋级情况类型、处理措施2.事件处理工作流程3.应急处理步骤4.执行应急预案相关人员联系方式

★网络安全应急处理流程：1.安全事件报警2.安全事件确认3.启动应急预案4.安全事件处理5.撰写安全事件报告6.应急工作总结

应急响应技术类型：访问控制、网络安全评估、系统恢复、网络安全监测、入侵取证

★网络安全评估方法：1.恶意代码检测2.漏洞扫描3.文件完整性检查4.系统配置文件检查5.网卡混杂模式检查6.文件系统检查7.日志文件审查

网络安全监测方法：1.网络流量检测2.系统自身监测（natstat、ps命令监测进程，losf工具查端口进程,arp-a命令地址缓存表）

★系统恢复方法：1.系统紧急启动2.恶意代码清除3.系统漏洞修补4.文件删除恢复5.系统备份容灾（备份分6级）

★入侵取证可以作为证据信息的：1.日志2.文件3.系统进程4.用户系统状态5.网络通信链接记录6.磁盘介质

★网络安全取证步骤：1.取证现场保护2.识别证据3.传输证据4.保存证据5.分析证据6.提交证据

阿里云应急响应服务流程：1.购买服务2.分配合作伙伴3.事件确认4.事件抑制5.事件处理6.入侵原因分析7.提交报告8.结束

IBM应急响应流程：1.漏洞信息报告接收登记2.漏洞分析3.漏洞确认判定4.漏洞补丁开发安全防护措施研究5.发布漏洞修补措施6.避免出现类似漏洞

★永恒之蓝（感染端口445，利用windows的SMB漏洞）紧急处理方式：1.主机被感染，直接拔网线，有备份则恢复备份2.主机未被感染预防措施有:安装免疫补丁、漏洞修补、系统加固、阻断445端口网络通信

华为阻断445端口命令：rule deny tcp destination-port eq 445

思科阻断445端口命令：deny tcp any any eq 445

锐捷阻断445端口命令：deny tcp any any eq 445

概括命令：Access-list 101 deny tcp any any eq 445

页面篡改处置规程：启动处置、记录特征、攻击确认、上报部门负责人、上报应急领导小组、确认进行应急响应、分析处置、控制追踪、清除恢复、网站恢复、上报分管领导、上报应急小组组长、攻击分析和风险检测、完成事件报告

1. 网络安全测评技术与标准重点案例

可信计算机系统评估准则（TCSEC 1983）

信息技术安全评估准则（ITSEC 1993）

1998 CC2.0->保护轮廓（功能、保证）

信息系统安全保护能力5级（主席爱街坊）

信息技术、安全技术、信息技术安全性评估准则《GB/T18336-2001》 三部分

网络安全测评按目标分类：1.等级测评2.验收测评3.风险测评

网络安全测评按内容分类：1.技术安全测评2.物理安全测评

★网络安全测评按实施方式分类：1.安全功能检测2.安全管理检测3.代码安全审查4.安全渗透5.信息系统攻击测试

网络安全等级保护测评内容基本要求：1.技术要求（安全物理环境、通信网络、区域边界、计算环境、管理中心）2.管理要求（安全管理制度、管理机构、管理人员、建设管理、运维管理）

★等保2.0测评过程：1.测评准备2.方案编制3.现场测评4.报告编制

★网络安全渗透测试过程：1.受理2.准备3.实施4.综合评估5.结题

网络安全测评工具：web(apscan、nikto、dirb、w3af、wvs、) 端口（nmap、nessus）

数据库（sqlmap）

安全渗透测试：黑白灰三种盒模型 灰盒测试（适合手机银行、代码测试）

安全渗透测试常用工具：metasploit、ollydbg、gdb、backtrack4、burpsuit、idapro

模糊测试的优点：1.无需源码2.复用性高3.不受限于被测系统

★代码安全缺陷：1.缓冲区溢出2.代码注入3.跨站脚本4.输入验证5.API误用6.密码管理7.配置错误8.危险函数

性能测试工具：load ruuner、apache jmeter、smartbits

性能监测工具:win任务管理器 ping命令 tracert命令

★信息安全等级保护是基本制度、基本国策（3级以上包含3级涉及国家属于重要，5级特别重要）

公安部等级保护规定：自主、指导、监督、强制、专控

等级保护涉及到主体、客体、授权

1994.2.18->计算机信息系统安全保护条例

2019.9.7->加强信息安全保障工作

2019.9.15->信息安全等级保护实施意见

2019.6.22->信息安全等级保护管理办法

2019.7.16->开展信息安全等保定级工作

等保建设目标基本要求：1.技术要求（物理安全、网络安全、主机安全、应用安全、数据安全）2.管理要求（安全管理机构、安全管理制度、人员安全管理、系统建设管理、运维管理）

补：

数字签名需满足的条件：非否认、真实性、鉴别性

几种DDOS判定:1.ping of death死亡攻击（数据包>65535）2.teardrop泪滴分段攻击（多个分片IP包）3.winnuke带外传输攻击(涉及端口)4.land攻击（源地址目标地址都是一个地址）5.smurf攻击(涉及ICMP，将回复地址设置成受害网络的[广播地址](https://baike.baidu.com/item/%E5%B9%BF%E6%92%AD%E5%9C%B0%E5%9D%80" \t "https://baike.baidu.com/item/Smurf%E6%94%BB%E5%87%BB/_blank)的ICMP应答请求数据包)

网络信息安全基本技术需求：1.物理环境安全2.网络信息安全认证3.访问控制4.安全保密5.漏洞扫描6.恶意代码防护7.网络信息内容安全8.安全监测预警9.应急响应

网络安全管理方法：1.风险管理2.等级保护3.纵深防御4.层次化保护5.应急响应6.PDCA

APT特性：组织性、持续性、隐蔽性、旁路攻击

第十九章操作系统安全保护  
操作系统5个安全等级：主席爱街坊

Window安全机制：认证、访问控制、审计、协议过滤、文件加密、抗攻击

Linux 安全机制：认证、访问控制、审计机制  
操作系统安全可控目标分2个层面：1.用户实现对操作系统的可理解、可修改、可检测、可修复、可保护2.商业用户能够自己主导操作系统产品化，不受商业利益绑架  
★操作系统安全需求：1.标识鉴别2.访问控制3.系统资源安全4.网络安全5.抗攻击6.自身安全  
★操作系统安全机制：1.硬件安全2.标识鉴别3.访问控制4.最小特权管理5.安全审计6.可信路径7.系统安全增强  
★★★操作系统安全技术：1.容灾备份2.可信计算3.身份认证4.访问控制5.加密技术6.安全审计7.特权管理8.形式化分析9.安全渗透10.隐蔽信道分析11.安全补丁12.防火墙13.入侵检测14.沙箱15.攻击欺骗16.地址空间随机化17.系统恢复（此项背会，安全随意结合）  
Windows系统划分三层：1.抽象层2.内核层3.模块  
Win2000有专门的安全子系统：本地安全授权LSA 、账户安全管理SAM、安全参考监视器SRM  
Windows橘皮书->C2级 自主访问控制  
windows日志有：系统日志、应用程序日志、安全日志  
★windows系统安全分析（存在的威胁）：1.口令安全2.恶意代码3.应用软件漏洞4.系统程序漏洞5.注册表安全6.文件共享7.物理临近攻击  
★windows系统安全增强方法：1.安全漏洞补丁2.停止服务，卸载软件3.升级更换程序4.修改配置权限5.去除恶意程序6.安装专用安全工具软件  
★Windows200系统安全增强方法：1.系统启动安全增强2.账号口令管理安全增强3.安装最新系统补丁4.网络安全增强（禁止建立空链接将注册表lsa键值改1，关闭默认共享，关闭无必要的端口和服务）5.安装三方防护软件  
windows安全工具：openssh  kerberos  clamav   nmap   netstat   windump  
Linux操作系统划分三层：1.硬件层2.系统内核3.应用层  
★linux系统安全增强方法：1.给安全漏洞打补丁2.停止不必要的服务3.升级更换软件包4.修改系统配置5.安装专用安全工具软件  
★国产操作系统存在的安全风险隐患：1.linux内核2.自主研发的系统组件3.三方组件4.系统安全配置5.硬件安全  
★国产操作系统安全增强措施：1.管理员分权2.最小特权3.访问控制4.细粒度自主访问控制5.多级安全   
linux限制远程访问命令：hosts.deny文件添加内容->ALL:ALL@ALL(禁止所有外部主机访问)  
Hosts.allow文件添加内容->放行个别访问  FTP:IMG_256192.168.0.1   宋毅含的PC机名  （允许宋毅含的主机访问FTP服务）  
口令长度修改etc/login.defs文件下的PASS\_MIN\_LEN  修改时间->PASS\_MIN\_DAYS  
★禁用netbios命令：HKLM\SYSTEM\CurrentControlSet\Control\Lsa:restrictanonymouse=2  
Inetd.conf文件权限600，属ROOT  
Services文件权限644，属ROOT  
禁用不必要程序：chmod a-s  程序名  
SElinux服务器->混合安全策略，采取强制访问控制有利于减缓网络攻击影响

第二十章  数据库系统安全（CIA）重点案例  
★数据库面临的主要威胁：1.授权误用2.逻辑推断汇聚3.伪装4.旁路控制5.隐蔽信道6.SQL注入7.数据库口令密码破解8.硬件介质攻击  
★数据库安全隐患：1.账号密码2.扩展存储过程3.软件应用程序漏洞4.权限分配隐患5.用户安全意识薄弱6.网络通信内容明文传递7.安全机制不健全  
★数据库安全需求安全机制：1.标识鉴别2.访问控制3.安全审计4.备份恢复5.数据库加密6.资源限制7.安全加固8.安全管理  
数据库加密方式：1.库内加密2.库外加密  （库内加密就是数据库画在内部，库外加密数据库就画在外面）  
数据库加密类型：1.网上传输数据（通过SSL实现）  2.数据库存储数据（通过存储加密实现）  
★数据库漏洞防控：通过虚拟补丁包来解决  
★数据库防火墙的作用：1.屏蔽直接访问数据库的通道2.增强认证3.攻击检测4.防止漏洞利用5.防止内部高危操作6.防止敏感数据泄露7.数据库安全审计  
★数据库脱敏技术（对数据进行变换处理，避免敏感数据外泄）：1.屏蔽2.变形3.替换4.随机5.加密  
数据库漏洞扫描工具：xsecur-dbscam、ngssquirel for oracle  
Oracle(1979年)->安全机制：1.用户认证2.访问控制3.保险库4.安全审计、数据库防火墙5.高级安全功能  
oracle透明数据加密可阻止攻击者绕过数据库  
★数据库系统安全增强加固（通用版）：1.增强操作系统安全2.最小化安装数据库，删除不必要组件，关闭不必要的远程端口和服务3.删除修改默认用户密码端口号4.启用认证机制5.设置安全口令密码6.最小化权限7.安装最新补丁8.限制连接IP 9.传输加密10.启用审计11.定期查看漏洞发布信息，及时修补漏洞12.灾备  
★数据库备份方案：1.文件文件组备份2.事务日志备份3.完全备份4.差异备份  
★数据库恢复机制：1.简单恢复2.完全恢复3.批量日志记录恢复  
审计->c2级  
网站最佳配置：LAMP   linux+apache+mysql+php   
国产数据库：DM达梦、人大金仓  
修改数据库密码命令：set password for 用户名@localhost=password(‘新密码’);  
修改数据库账号命令：update user set user=”新建账户名” where user=”root”;  
刷新服务：flush privileges;  
★mysql主要漏洞：拒绝服务、代码执行、溢出、逃避、特权获批  
LOIS SDBMS数据库管理系统：是国内第一个核心化体系结构的系统，强制访问控制粒度达到记录级，达到3级要求，softbase也达到3级要求

第二十一章 网络设备安全重点案例

交换机共有5代：（集线器、以太网交换机、三层交换机、四代交换机IPS、5代交换机QOS）

★交换机面临的威胁：1.MAC地址洪泛2.ARP欺骗3.口令威胁4.漏洞利用

★路由面临的威胁：1.漏洞利用2.口令威胁3.路由协议4.DDOS 5.依赖性

路由交换机支持TACACS认证（TCP）、RADIUS认证（UDP）

网络设备访问分类：1.带外访问2.带内访问 （SNMP提供读、读写，可访问所有网络设备）

★从设备进行访问控制的几个方面：1.CON端口访问2.VTY访问控制3.HTTP访问控制4.SNMP访问控制5.设置管理专网6.特权分级

★安全通信的两种方式：1.SSH 2.VPN

★网络设备的审计方式：1.控制台日志审计2.缓冲区日志审计3.终端审计4.SNMPtraps 5.AAA审计 6.Syslog审计

★网络设备安全增强：1.关闭非安全网络服务功能2.信息过滤3.协议认证

★交换机安全增强技术：1.配置交换机访问口令和ACL进行限制2.利用镜像技术监测网络流量3.MAC地址控制技术4.安全增强

★路由器安全增强技术：1.升级操作系统打补丁2.关闭不需要的网络服务3.禁止不使用端口4.禁止IP直接广播5.增强路由VTY安全6.阻断恶意数据包7.路由口令安全8.传输加密9.增强路由SNMP安全

★网络设备漏洞解决方法：1.及时获取设备漏洞信息2.网络设备漏东扫描3.网络设备漏洞修补

★常见设备安全漏洞：1.拒绝服务2.跨站伪造（CSRF）3.格式化字符串4.XSS 5.旁路6.代码执行7.溢出8.内存破坏

网络设备漏洞扫描软件：1.端口扫描工具2.通用漏洞扫描器3.专用漏洞扫描器

网络设备漏洞处理方式：1.修改配置文件2.安全漏洞利用3.服务替换4.软件包升级

物理安全：环境、设备、系统

http状态码：200 请求成功 300 重定向 400 请求错误 500 服务器或者网关错误

1. 网站安全需求分析与安全保护工程 重点案例

★网站威胁：1.非授权访问2.网页篡改3.数据泄露4.恶意代码5.网站假冒6.拒绝服务7.网站后台管理安全威胁

★常见的网站后台管理问题：1.网站管理员身份密码被窃2.后台管理页面存在漏洞3.内部管理权限分配不合理

★网站安全需求：1.物理环境2.网络通信3.操作系统4.数据库5.应用服务器6.WEB服务软件7.WEB应用程序8.数据等安全威胁防护

★apache软件下面的几个配置文件:1.httpd.conf 主配置文件，最先读取2.conf/access.conf (基本的读取文件控制，限制目录的权限，此项设置不是必须的，可以在httpd.conf里设定)

Apache web威胁：1.配置威胁2.安全机制威胁3.应用程序威胁4.服务通信威胁5.服务内容威胁6.软件程序威胁7.拒绝服务威胁

Apache 本地用户较多修改默认配置文件：#chown -R root.root /usr/local/apache #chmod 511 /usr/local/apache/bin/httpd #chmod 600 /usr/local/apche/logs/\*log

★apache 认证：<directory>背的那一段回看以前的代码</directory>

apache后台管理页面创建用户账户口令提高安全度：#/usr/local/apache/bin/htpasswd -c /usr/local/apache/conf/passwd testuser

Apache 模块管理机制里面记俩单词：enable disable

Apache链接耗尽应对：time out 30 MaxClients 256 限制同一IP最大链接数 多线程下载保护

★apache web 自带访问机制 access.conf里面配置 order deny,allow deny from all allow from pair 192.168.0.1/255.255.255.0

★apache安全增强方法：1.及时打补丁2.启用.htaccess文件保护网页3.为apache设置专门的用户和组4.隐藏apache版本号5.目录访问安全增强6.文件目录保护7.删除默认目录和不必要的文件8.使用三方软件增强apache服务

★★★万金油：见“用户二字”-> 最小特权

见“安全机制”->物理环境安全、网络通信安全、操作系统安全、数据库安全、WEB服务器安全、应用程序安全、域名安全、访问控制、防火墙、入侵检测、审计、保证CIA可控性

★IIS认证机制：1.匿名认证2.基本验证3.证书认证4.数字签名认证5.windows认证

★IIS访问控制流程：1.ip是否允许2.身份是否允许3.web权限是否允许4.文件权限是否允许5.通过按需提供访问

IIS访问控制措施：1.请求过滤2.授权控制3.IP限制4.文件授权

★IIS安全增强方法：1.安装补丁2.启动动态IP限制3.启用URLscan 4.启用应用防火墙5.启用SSL服务

Web安全漏洞主要分：1.技术安全漏洞2.业务逻辑安全漏洞

★AI注入漏洞三个场景代码wen会分辨：1.SQL注入2.NOSQL注入3.OS注入（最简单的判断sql注入看有无ID，判断OS注入看有无system，剩余的就是nosql）

★SQL注入防范：1.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

Sql注入的特点：普遍性、隐蔽性、危害性

Web应用的几种漏洞：1.SQL注入2.文件上传3.跨站脚本

★网站安全保护机制：1.物理环境安全2.身份鉴别3.访问控制4.内容安全5.数据安全6.安全防护7.安全审计监控8.应急响应灾备9.合规管理10.安全测评11.安全管理机制

★网站安全加固从以下几个方面下手：1.操作系统2.数据库3.WEB服务软件，应用程序4.网站域名服务5.网站后台管理

★网站合理部署规划：1.防火墙2.漏洞扫描3.网站防篡改4.网络流量清洗5.网站安全监测

★★政府网站防护方案：1.DDOS防御2.网络访问控制3.网页防篡改4.网站应用防护5.入侵防御，病毒防护6.网络数据库审计7.网络安全监控

★网上银行保护：1.安装证书组件2.开启安全通信方式3.使用验证码认证4.防暴力破解

政府网站系统安全技术措施从几个层面实施：1.网站层2.数据层3.主机层4.网络层5.物理层

------------------------------------------------------------------

★★★★★★：对比老头要点遗漏之处

防火墙功能指标：网络接口、协议支持、加密支持、认证支持、访问控制

防火墙性能指标：最大吞吐量、转发速率、最大规则数、并发连接数

脆弱性识别方法：漏洞扫描、任重检测、渗透测试、问卷调查、安全访谈

信息系统安全测评包括：1.信息系统安全风险评估2.信息系统安全等级保护测评3.信息系统安全验收测评4.信息系统安全渗透测试5.信息系统安全保障能力评估

1. 云计算安全需求分析与安全保护工程 重点案例

★什么是云计算：通过虚拟化及网络通信技术，提供按需服务，**弹性化的IT资源服务平台**

★云计算特征：1.IT资源以服务形式提供2.多租户共享IT资源3.IT资源按需定制4.IT资源可伸缩性部署

云计算四种部署模式：私有云、公有云、社区云、混合云

★云安全威胁主要有哪些：1.弱口令2.假冒3.网络监听4.数据泄露5.中间人6.拒绝服务7.物理安全8.平台服务9.滥用资源、服务10.内部威胁11.数据残留12.过度依赖13.共享技术漏洞14.不安全接口15.服务中断

云计算安全要求：1.物理2.环境3.通信4.设备5.数据应用6.多租户安全隔离7.虚拟资源8.云服务合规9.数据可信托管10.安全运维连续性保障

云计算服务需求：技术安全、安全合规、隐私保护

云计算技术安全需求：1.云端安全（身份鉴别、标识、资源访问控制）2.网络通信安全（身份认证、数据加密、防火墙、VPN）3.云计算平台安全（主机、操作系统、数据库、应用等的安全）

★云计算隐私保护需求：1.数据采集2.数据传输3.数据存储4.数据使用5.数据维护6.数据安全事件处置

★云计算技术措施等级保护要求：1.物理环境安全2.网络通信安全3.设备计算安全4.应用数据安全

★云计算安全组织管理保障措施等级保护要求：1.安全策略制度2.安全机构人员3.安全管理对象

★云计算服务安全运维保障要求：1环境资产2.漏洞、风险3.设备策略4.监管5.监测响应

★云计算运维安全措施：1.风险评估2.内部防护3.安全监测4.应急响应5.容灾备份

★云计算安全机制：身份鉴别、数据完整、访问控制、入侵防范、安全审计、云操作系统安全增强

华为云安全技术措施：1.芯片级可信计算安全加密2.平台安全3.系统安全4.应用安全5.数据安全6.开发安全7.生态安全8.隐私保护

★云计算安全国内管理标准规范：数据中心云计算服务平台要设在境内

★云服务网络安全管理意见：1.安全管理责任不变2.数据归属关系不变3.安全管理标准不变4.敏感信息不出境

★等保2.0一个中心三重防护原则：安全管理中心、安全计算环境、安全区域边界、安全通信网络

两地三中心-容灾机制：两地是同城或异地，三中心是生产中心、同城容灾中心、异地容灾中心

防御csrf跨站伪造攻击方法：referer防盗链、token验证、http头+hash验证

防御xss的方法：http-only 输入输出验证

容灾三种技术：数据容灾，应用容灾，系统容灾

第二十四章 工控安全需求分析与安全保护工程（此章只背三星内容） 重点分析

工控系统分两大类：1.离散制造类2.过程控制类

★工控系统威胁：1.自然灾害环境2.内部安全威胁3.设备功能故障4.恶意代码5.网络攻击

★工控系统安全隐患：1.工控协议2.产品漏洞3.软件漏洞4.算法漏洞5.固件漏洞6.硬件漏洞7.接入漏洞8.供应链

工控信息安全需求：CIA倒序

工控系统的网络信息安全主要有1：技术安全2.管理安全

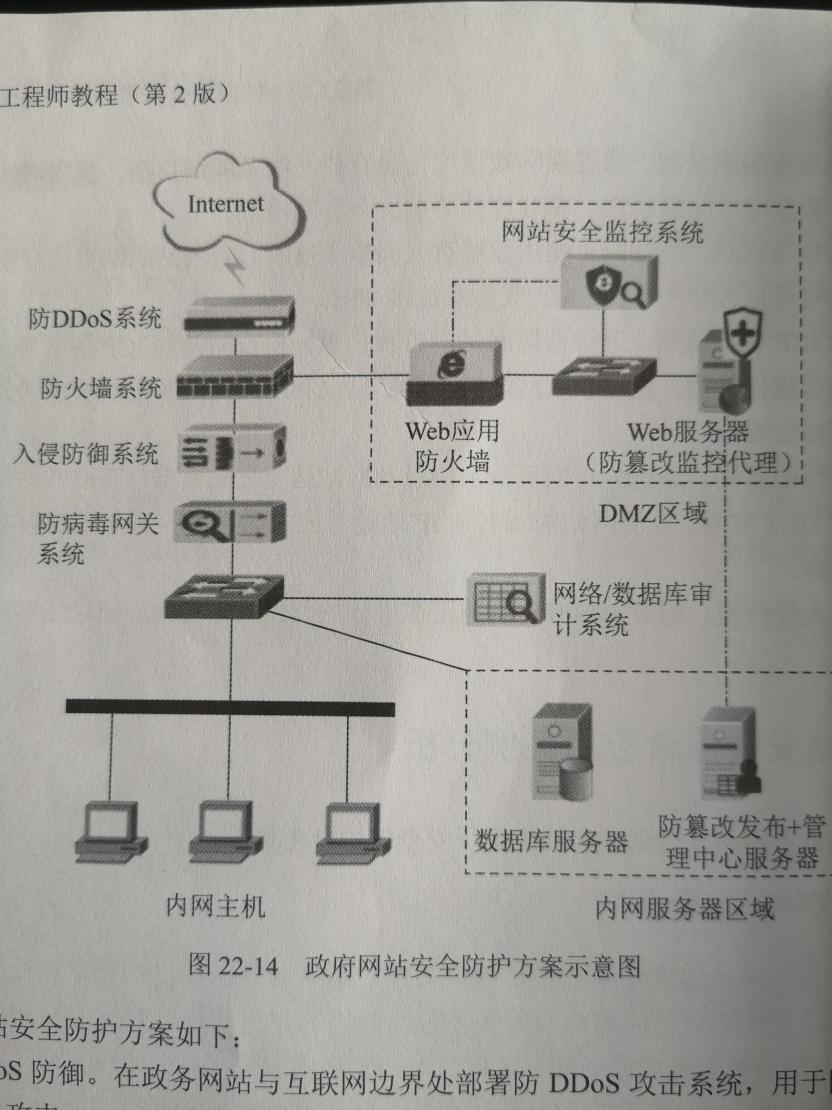
★工控保护机制：物理环境防护、安全分区边界保护、身份认证、访问控制、远程访问安全、恶意代码防范、数据安全、网络安全监测、应急响应、安全管理、

★工控系统安全措施：1.安全监测2.应急响应

★★★工控系统安全需要涵盖一下几部分（方案）：1.工控可信计算平台2.工业防火墙3.中央管理平台4.安全管理平台

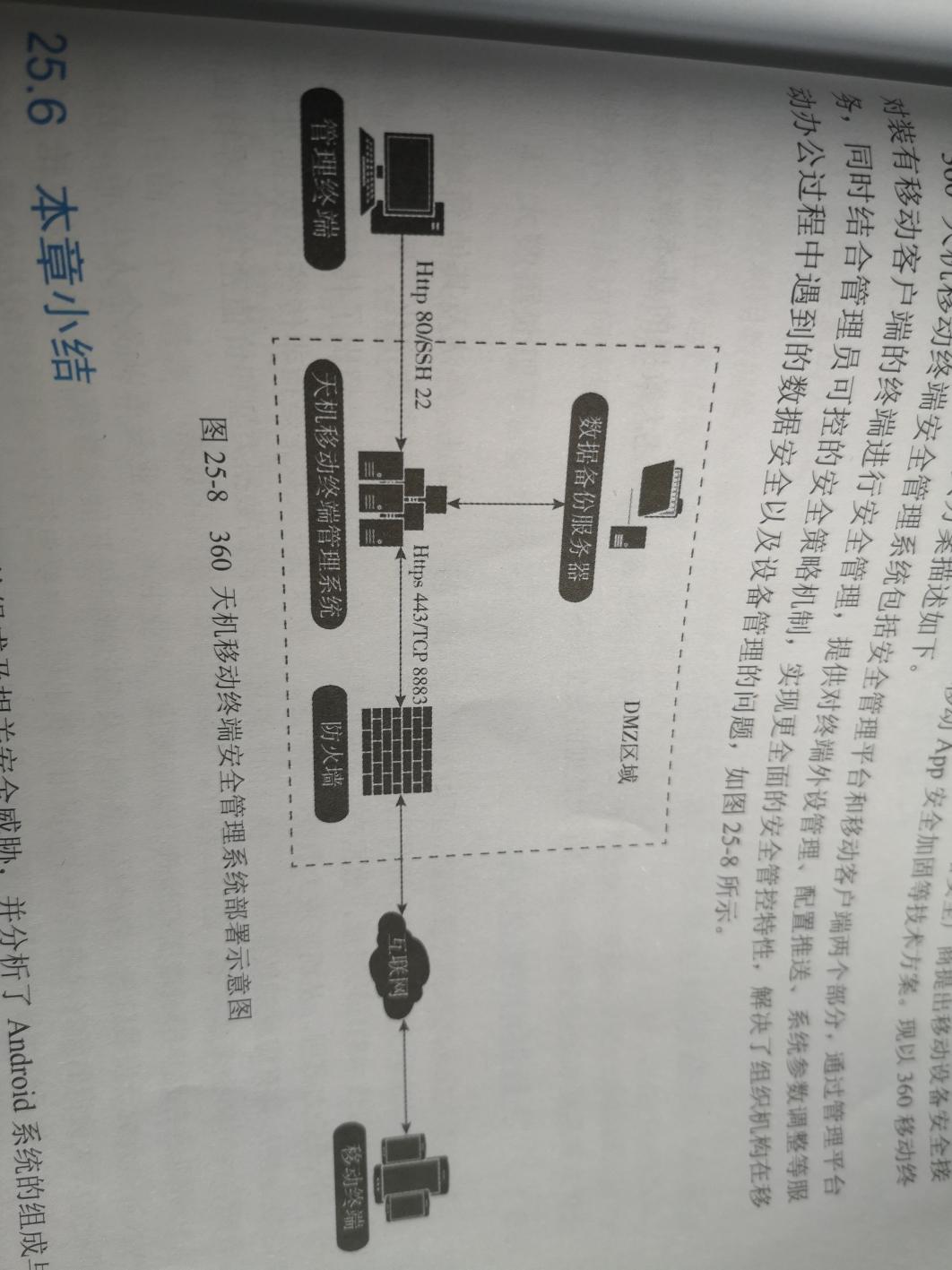
★★★电力监控系统的方案：1.安全分区2.网络专用3.横向隔离4.纵向认证

补：政府网站防护方案



第二十五章 移动应用安全需求分析与安全保护工程 重点分析

熟悉图（移动办公安全部署安全方案） 移动办公风险：设备丢失、信息泄露、恶意攻击、共享访问

移动运营商安全的主要威胁：1.账号密码窃取2.漏洞利用3.恶意代码4.数据窃取5.恶意刷单6.拒绝服务7.计费SDK破解8.钓鱼攻击9.社工库诈骗

移动运营商应用安全的防护方案：1.加固运营商APP 2.给APP提供木马、病毒、恶意代码查杀服务3.对运营商的通信协议、证书进行加密4.提供态势感知服务

移动应用系统组成：1.移动应用APP 2.通信网络 3.应用服务端

★移动应用安全威胁类型：1.操作系统平台2.无线网络攻击3.恶意代码4.应用代码逆向工程5.应用程序非法篡改

★Android组成：1.linux内核层2.系统运行库层3.应用程序框架层4.应用程序层

★Android安全机制：1.权限声明机制2.应用程序签名机制3.沙箱机制4.网络通信加密5.内核安全机制

IOS组成：1.核心操作系统层2.核心服务层3.媒体层4.可触摸层

IOS架构分：软硬件、固件

IOS安全机制：1.安全启动链2.数据保护3.数据加密4.地址空间随机化5.代码签名5.沙箱机制

移动APP安全加固：防反编译、调试、篡改、窃取

★APP安全保护方案：1.安全开发管理2.网络通信内容安全加密保护3.安全加固4.安全测评5.安全监测

第二十六章 大数据安全需求分析与安全保护工程 （这章要看一下） 重点分析

★★★大数据特征：海量数据规模、快速数据流转、多样数据类型、价值密度低

大数据种类：结构化、半结构化、非结构化

★大数据技术：1.大规模数据分析处理2.数据挖掘3.分布式文件系统4.分布式数据库5.云计算平台6.互联网7.存储系统

★大数据安全威胁：1.数据集安全边界日渐模糊，保护难度提升2.敏感数据泄露风险增大3.数据失真、大数据污染风险4.大数据处理平台业务连续性、拒绝服务5.个人数据分布多个平台，隐私保护难度大6.数据交易安全风险7.大数据滥用

★大数据安全需求：1.自身安全2.安全合规3.跨境安全4.隐私保护5.处理平台安全6.业务安全7.运营安全

★大数据安全保护机制：1.数据分类分级2.数据源认证3.数据追溯4.数据用户标识和鉴别5.数据资源访问控制6.数据隐私保护7.数据备份恢复8.数据安全审计监测9.数据安全管理

★华为大数据安全措施：1.网络安全2.主机安全3.用户安全4.数据安全