1. 网络空间安全概述——两个出题点，只看书
2. 物理安全——只看书
3. 第三章网络安全——书上内容结合补充知识

书上有写得不太准确的地方：

1. 身份认证技术——在计算机网络中为确认操作者身份而采取的有效解决方法。
2. 访问控制技术——为防止对任何资源进行未授权的访问，使计算机系统在合法的范围内使用的技术。意指用户身份及其所归属的某项定义组来限制用户对某些信息项的访问，或限制对某些控制功能的使用的一种技术。

书上需要补充的地方

1. 误用检测技术与异常检测技术的主要区别是什么，这两种技术各有什么优点
2. 蜜罐技术的定义——蜜罐技术本质上是一种对攻击方进行欺骗的技术，通过布置一些作为诱饵的主机、网络服务或者信息，诱使攻击方对它们实施攻击，从而可以对攻击行为进行捕获和分析，了解攻击方所使用的工具与方法，推测攻击意图和动机，能够让防御方清晰地了解他们所面对的安全威胁，并通过技术和管理手段来增强实际系统的安全防护能力。
3. DOS（Denial of Service）拒绝服务攻击

DDOS(Distributed Denial of Service) 分布式拒绝服务攻击

1. 系统安全——只看书

* 虚拟机逃逸：虚拟机逃逸是指利用虚拟机软件或者虚拟机中运行的软件的漏洞进行攻击，以达到攻击或控制虚拟机宿主操作系统的目的

1. 应用安全——知识点都在书上，讲义上会有部分的解释
2. 数据安全——书结合讲义

讲义部分：

什么是本地备份，本地备份的不足

什么是网络备份，网络备份的优点

1. 大数据背景下的先进计算安全问题——只看书
2. 舆情分析——只看书
3. 隐私保护——内容涵盖在其他各章节
4. 密码学及应用——只看讲义

10.1 Kerckhoffs准则

10.2 加密置换矩阵和解密置换矩阵

10.3 矩阵加密置换的方法（做几道题）

10.4 分组密码设计过程中，混乱和扩散的解释

10.5DES是安全的么？DES加密过程中S盒的使用

10.6 单向陷门函数

10.7对称密钥和非对称密钥的区别（对称密钥加解密使用的同一个密钥，或者能从加密密钥很容易推出解密密钥；而非对称密钥算法加解密使用的不同密钥，其中一个很难推出另一个密钥）

10.8 数字签名的过程（可以结合图示）

10.9 数字签名的特性

10.10 PKI的中英文解释和用途

第十二章 网络空间安全治理——全看讲义

12.1 网络空间安全的目标

进不来、拿不走、看不懂、改不了、逃不掉、打不垮分别通过什么技术实现

12.2 主动攻击与被动攻击的解释与举例

12.3 APPDRR模型的六个关键环节，每个环节的作用和地位

12.4 网络安全保障的三大支柱(背)，每一个支柱的意义和作用（理解）

12.5 计算机犯罪（刑法）

计算机犯罪的定义

计算机犯罪的常用方法

12.6 信息系统安全保护法律规范

构成：命令性规范、禁止性规范

我国对信息系统安全的保护主要通过三大体系予以保障，这三大体系是什么？

强制性技术标准体系中代表性标准，容易出选择题

信息系统安全保护法律规范的基本原则

第十三章 补充内容

13.1 木桶原理

13.2 信息安全管理涉及的方面（容易出判断）

13.3信息安全风险评估的要素（要会简单解释）