2014-2015

1.一个典型的企业 internet 网，内部用户通过统一认证平台访问内部各业务系统，内部终端既有通过 RJ45 网线连接的工作站、也有通过 wifi 连接的 ipad，均对外共享一个 x网公共 IP 地址出口通过 NAT、应用代理服务器和一个 IP 过滤刑防火墙接入互联网。试用IATF“三保卫一支撑”分解其深度保护区域并用简单网络拓扑图标注，对应“边界和接入区域列出其对应的基本信息资产。(20分)

2.对应一个公共 Ipv4 广域网，分析保密性 C在OSI 7 层各层实施的可行性，分别对应七层明确给出:

(1)结论

(2)对不可实现的层，给出理由

(3)对可行的层，给出可能的实现方法(15 分)

1. 基本的安全机制有哪些?当面临可能的身份冒用威胁时，分析在应用层抗重防攻击可以采取的安全机制(15 分)
2. 分析强制访问控制与自主访问控制之间的主要异同(15 分)
3. 安全风险评估时采用客观扫描工具除了网络扫描类以外，还有哪些类?实施扫描评估前要先评估扫描对目标系统可能产生的影响并做好适当的预防措施，这些影响一般有哪些?简述其主要部分。( 15分)
4. 阐述信息安全保障的 CIA 三角之C的主要两层含义。以一个学生成绩远程查询系统为例，具体分析其查询持续服务能力(a)可能面临的安全威胁和安全风险，并为此设计一个安全体系结构，请具体给出主要过程如深度保护区划分和信息资产识别、威胁-脆弱性安全风险分析、安全需求定义、安全策略设计、设计-组织和运行管理体系设计等。(20 分)

2025 回忆版

1. 三个课程作业的内容、创新点和可改进的地方
2. 简要描述零信任架构、IATF和等级保护2.0的核心思想。从访问控制、保护目标的角度分析三者的异同。
3. 简要描述微服务架构和单体架构。举例一些常见应用说明两者的特点。同时从身份鉴别、数据安全的角度分析两种架构的优劣势。
4. AWS是一个著名的云计算服务系统，按照IATF架构画出它的网络边界拓扑图，描述各安全域的主要信息资产。
5. 以一个容器上的应用服务为例，描述剩余信息保护的含义。并从容器销毁/重建的角度分析在代码或系统配置上实现缓存、日志和临时文件的剩余信息保护的具体方法。
6. 对于一个移动+边缘+云计算的系统，........ ，设计安全体系结构蓝图和总结攻击面管理方法论。（这道题涉及的各种术语太多，80%不是书上的，我估计是ai出的题，不要太放在心上）