CNS 详细知识点中文总结（Week 1–14）

2026 年 2 月 17 日

目录

1 使用说明与复习策略

1.1 资料范围

本文基于你目录中的全部课件文本（Week 1, 2, 3–4, 5–6, 7, 8–9, 10–11, 12, 13–14）整理，覆盖课程主线与高频考点。

1.2 建议复习顺序

1. 先建立主框架：安全目标、机制、威胁与分层。
2. 再攻克认证与访问控制：PAP/CHAP、BLP/Biba、RBAC。
3. 再学网络协议与架构：Kerberos、IPSec、SSL/TLS、防火墙与 DMZ。
4. 最后做综合设计题：规则设计、分区部署、加固与检测响应联动。

2 课程总框架（Week 1–2 主干）

2.1 安全服务与目标

课程主线围绕以下安全目标展开：

- **Confidentiality（机密性）**：防止未授权读取。
- **Integrity（完整性）**：防止未授权篡改。
- **Availability（可用性）**：系统按需可访问。
- **Authentication（认证）**：证明实体身份。
- **Access Control（访问控制）**：限制谁能访问什么。
- **Non-repudiation（不可否认性）**：行为不可抵赖。

2.2 服务与机制映射（必背）

- 机密性 → 加密（对称/非对称）。
- 实体认证 → 认证协议（挑战应答、证书、票据机制）。
- 完整性与数据来源认证 → MAC 或数字签名。
- 不可否认性 → 数字签名（通常需证书体系支撑）。

2.3 安全工程三分法：AAA + PDR

- AAA：Authentication, Authorization, Auditing。
- PDR：Prevention, Detection, Response。
- 典型认识：预防最理想但成本高；检测更易落地；响应决定恢复效率与损失控制。

2.4 分层思维

- 网络架构分层（OSI/TCP-IP）意味着：**下层漏洞会被上层继承**。
- 安全设计要按层识别攻击面，不要只靠单点工具。

3 密码学与认证基础（Week 1, 3–4）

3.1 密码学原语体系

- 对称加密：效率高，密钥分发难。
- 非对称加密：分发友好，计算开销大。
- 哈希函数：单向摘要，常用于完整性校验与口令存储。
- MAC：用共享密钥做消息认证，提供完整性与来源认证。
- 数字签名：提供完整性、来源认证与不可否认性。
- 证书与 PKI：把“身份”与“公钥”绑定，建立可验证信任链。

3.2 身份认证方法全景

- 知识因子：口令、PIN。
- 持有因子：令牌、智能卡。
- 生物因子：指纹、人脸、虹膜、行为特征。
- 实务建议：敏感系统优先多因子，不应只依赖口令。

3.3 口令安全与常见攻击

- 风险来源：弱口令、重用口令、可预测规则、错误提示泄露、口令传输被嗅探。
- 攻击方式：字典/暴力破解、离线哈希碰撞、账号枚举（account harvesting）。
- 防护思路：强策略、限速与锁定、统一错误信息、口令哈希加盐、审计告警。

3.4 PAP 与 CHAP（高频对比）

- PAP：口令或口令哈希可被重放，整体偏弱。
- CHAP：挑战应答机制，挑战值每次变化，抗重放显著更好。
- CHAP 流程：ID → Challenge → Response → 验证通过/拒绝。

3.5 SSO 与一次性口令

- SSO 优点是体验好；核心风险是单点账号被盗后横向影响大。
- OTP（如 RSA SecurID、S/Key）可抵抗窃听后的重放，但通常不能单独解决会话劫持等问题。

3.6 证书认证与私钥保护

- 证书认证强度很大程度取决于**私钥保护**。
- 智能卡/硬件令牌价值：把私钥从通用主机环境中隔离出来。

3.7 生物特征认证（理解型考点）

- 优点：不可遗忘、使用便捷、可提升认证强度。
- 难点：误识率权衡、隐私风险、模板泄露不可撤销、伪造攻击（fake biometrics）。
- 结论：生物特征适合做增强因子，不宜被神化为“万能认证”。

4 访问控制模型（Week 5–6）

4.1 访问控制结构

- 访问控制矩阵：行可看作主体能力（Capabilities），列可看作对象 ACL。
- ACL 管理的痛点：规模变大后维护复杂，容易引入误配。
- 组与角色可降低权限管理复杂度。

4.2 DAC/MAC/RBAC

- DAC：资源拥有者可自主授权，灵活但容易扩散。
- MAC：按安全级别强制控制，规则严格。
- RBAC：按岗位角色分配权限，工程可维护性通常最好。

4.3 Bell-LaPadula（保密性模型）

- 目标：防止敏感信息向低级别泄露。
- 核心规则：`No Read Up`，`No Write Down`。
- 常见考试点：读写方向不要记反。

4.4 Biba（完整性模型）

- 目标：防止低完整性数据污染高完整性对象。
- 核心规则：`No Read Down`，`No Write Up`（执行也避免“向上污染”）。
- 与 `BLP` 关系：方向几乎完全相反。

4.5 部分序与分类分区（categories）

- 安全级别不仅有等级（如 Secret/Top Secret），还可叠加分类分区。
- 通过“级别 + 分区集合”做支配关系比较，用于更细粒度策略表达。

4.6 Chinese Wall 模型

- 面向利益冲突场景（咨询、金融、审计）。
- 关注点是“防跨冲突域信息流动”，强调动态冲突约束。

5 恶意代码体系（Week 7）

5.1 主要类型与特征

- Virus：依附宿主传播。
- Worm：利用网络漏洞自传播。
- Trojan：伪装诱导执行，通常不自传播。
- Spyware/Keylogger：窃取行为与敏感输入。
- Rootkit：隐藏攻击痕迹与恶意能力。
- Backdoor/Botnet：持久控制与批量远程操控。
- Logic Bomb：条件触发恶意逻辑。

5.2 防护与检测思路

- 特征库查杀：对已知样本有效，对变种和未知样本有限。
- 行为检测：可提升未知威胁发现率，但误报控制难。
- 工程策略：最小权限、补丁、端点防护、流量监控、备份恢复、应急预案。

6 认证协议理论与实例（Week 8–11）

6.1 实体认证核心概念

- 单向认证：只证明一方身份。
- 双向认证：双方互证身份。
- 认证是时点行为，若要持续安全，需要后续会话密钥保护。

6.2 认证协议通用要求（高频）

课件模型强调至少关注：

1. 消息来源真实性（确由对方发出）。
2. 消息新鲜性（非旧报文重放）。
3. 消息目标绑定（确实发给本方）。
4. 消息时序绑定（响应与请求强关联，不可被“调包”）。

6.3 新鲜性机制：时间戳 vs Nonce

- 时间戳优点：消息轮次少，适合客户端-服务端模式。
- 时间戳缺点：依赖时钟同步，且需要处理消息关联问题。
- Nonce 优点：不依赖全局时钟，抗重放清晰。
- Nonce 要求：随机且不可预测，否则协议安全性下降。

6.4 消息关联（Linking Messages）

- 防止攻击者在并发请求中“错配响应”。
- 常见做法：引入事务标识（transaction ID）或挑战值绑定。

6.5 Kerberos（重点流程）

- 核心角色：AS、TGS、客户端 C、服务端 S。
- 核心思想：用票据与短期会话密钥减少长期密钥暴露。
- 典型流程：
  1. C -> AS：获取 TGT 与相关密钥材料。
  2. C -> TGS：凭 TGT 申请某服务票据。
  3. C -> S：携票据访问服务并完成会话建立。

6.6 证书与密钥分发

- 证书是“身份 + 公钥 + 有效期 + 签名”绑定体。
- 不同信任域之间依赖交叉证书与证书链验证。
- 认证协议常用于会话密钥分发或协商，是后续机密通信基础。

7 网络设备加固与安全架构（Week 12）

7.1 设备与管理面加固

- 及时打补丁。
- 交换机端口安全（MAC 绑定/限制）。
- 路由 ACL 先行过滤，降低边界防火墙压力。
- 管理协议优先 SNMPv3（认证、隐私、访问控制）。

7.2 安全网络设计原则

- 先有安全策略，再落地架构与控制。
- 在设计阶段内建安全，而不是后贴补丁。
- 平衡三角：性能、可用性、安全。
- 减少单点故障：防火墙/路由/链路冗余。

7.3 边界与内部并重

- 仅靠外部边界防护不够，要防内部发起攻击。
- 关键实践：DMZ 分区、主机加固、出站过滤、远程接入端点治理。
- VPN 终端受感染会带来“加密隧道穿透边界”的风险。

8 边界防护、VPN 与检测响应（Week 13–14）

8.1 防火墙基础与策略设计

- 防火墙本质：默认拒绝，按策略放行并审计。
- 常见判定维度：源/目的地址、端口服务、连接状态、应用内容。
- 常见动作：`Accept`、`Drop`、`Reject`、`Authenticate`。

8.2 防火墙类型

- 包过滤（网络/传输层）：
  - 优点：高性能、部署广。
  - 局限：深层应用语义可见性弱。
- 应用层代理防火墙：
  - 优点：协议理解更深，策略更细。
  - 局限：性能开销更高。
- 混合型：工程上最常见，按业务组合能力。

8.3 架构与规则（设计题高频）

- 单防火墙架构：部署简单，隔离能力有限。
- 双防火墙架构：外层守公网，内层守内网，`DMZ` 位于中间，隔离更强。
- 规则顺序遵循首条匹配（first match）：**具体规则在上，泛化规则在下，最后兜底拒绝**。

8.4 IPSec 总结

- 协议族：`AH`、`ESP`、`IKE`。
- 运行层：网络层，适合站点到站点与全流量保护。
- 模式：
  - 传输模式：保护上层负载，外层 IP 头保留。
  - 隧道模式：封装整个原始 IP 包，更适合 VPN。

8.5 AH vs ESP

- AH：认证、完整性、防重放；不加密；可保护 IP 头完整性。
- ESP：加密为主，也可提供完整性与认证；常见于 VPN。
- 两者可组合使用，按场景取舍。

8.6 安全关联与 IKE 两阶段

- SA（Security Association）是 IPSec 安全上下文核心。
- Phase 1：建立受保护信道，完成对等体认证与密钥交换（Main/Aggressive）。
- Phase 2：协商具体业务流 IPSec SA 参数并周期更新。

8.7 SSL/TLS 主线

- 位置：位于应用与 TCP 之间，保护应用层数据通道。
- 服务：服务器认证、加密、消息完整性（客户端认证可选）。
- 阶段：握手阶段协商算法与密钥，数据阶段进行加密传输。

8.8 SSL/TLS vs IPSec VPN

- SSL/TLS：更偏应用接入，按会话/应用保护。
- IPSec VPN：更偏网络层隧道，按链路/网段保护。
- 选型应基于业务范围、终端可控性、运维复杂度和合规要求。

8.9 IDS/IPS（检测与防御联动）

- HIDS：主机视角，适合关键资产深度检测。
- NIDS：网络视角，覆盖广，但对加密流量可见性受限。
- 检测模型：
  - 特征检测：已知威胁效果好。
  - 异常检测：可发现未知威胁，但误报率通常更高。
- 响应方式：被动（日志告警）与主动（断连、重配置、阻断）。
- NIDS 变 IPS（串联在线）要评估性能、可用性与误阻断风险。

9 综合题答题模板（可直接套用）

9.1 模板 A：防火墙/DMZ 设计题

1. 先说明安全域：Internet、DMZ、Intranet、管理区。
2. 写原则：默认拒绝、最小权限、纵深防御、审计留痕。
3. 列核心放行：公网到 DMZ 的必要服务、内网到外网的业务流、DMZ 到内网最小化通道。
4. 列拒绝策略：其余全拒绝，出站过滤，伪造源地址过滤。
5. 写高可用：双机热备、双链路、配置一致性与变更审计。

9.2 模板 B：认证协议分析题

1. 指出协议目标：单向/双向认证，是否附带会话密钥建立。
2. 检查四点：来源真实性、新鲜性、目标绑定、消息关联。
3. 标注攻击面：重放、反射、并发错配、中间人、时钟偏差。
4. 给修复建议：引入 Nonce/时间戳、事务 ID、双向绑定、密钥更新周期。

9.3 模板 C：IDS/IPS 部署题

1. 明确资产分级：互联网出口、边界防火墙后、敏感子网前、关键主机本地。
2. 按位置说明传感器：NIDS 与 HIDS 组合部署。
3. 给响应分层：先被动告警，关键场景再主动阻断。
4. 提醒代价：在线阻断会带来性能、误报与单点问题。

10 高频必背清单（考前 15 分钟）

1. `BLP: No Read Up, No Write Down; Biba: No Read Down, No Write Up`。
2. `PAP` 弱，`CHAP` 挑战应答抗重放。
3. 认证协议不只要“能验身份”，还要“防重放、能关联请求响应”。
4. 新鲜性三件套：时间戳、逻辑序号、Nonce。
5. Kerberos：`AS -> TGS -> Service` 票据链路。
6. `AH` 不加密、`ESP` 可加密；隧道模式保护更完整。

7. IKE Phase 1 建安全信道，Phase 2 建业务 SA。
8. SSL/TLS 偏应用层保护，IPSec VPN 偏网络层保护。
9. 防火墙规则：首条匹配，先具体后泛化，最后默认拒绝。
10. HIDS + NIDS 组合优于单点；异常检测强在未知威胁，弱在误报控制。

11 常见失分点

- 把 BLP/Biba 的读写方向写反。
- 说 CHAP 会传输口令本身。
- 误写 AH 提供加密，或误写 ESP 保护外层 IP 头完整性。
- 把 IKE 两阶段职责混淆。
- 防火墙题只写“部署防火墙”不写规则顺序、默认拒绝、日志和分区边界。
- 忽略加密流量环境下 NIDS 的可见性限制。

结语

这份总结可直接用于三类题型：

- 对比题：模型、协议、检测方法的差异与边界。
- 流程题：认证握手、票据交换、IKE 两阶段。
- 设计题：规则、分区、加固、检测与响应的整体方案。