网络安全每周白话学习手册（零基础版）

2026 年 2 月 17 日

目录

1 怎么用这份手册

- 这份文档按 Week 1 到 Week 14 排好，适合没学过网络安全的人。
- 每周固定三部分：**本周要学会什么**、**术语白话 + 例子**、**本周学习任务**。
- 你不需要一次看完。建议 1 周看 1 章，先理解，再记术语。

2 Week 1：先知道“安全到底保护什么”

2.1 本周要学会什么

- 网络安全不只是“防黑客”，而是保护信息系统能可靠运行。
- 核心目标有 6 个：机密性、完整性、可用性、认证、授权、不可否认。

2.2 术语白话 + 例子

1. **Confidentiality（机密性）**：不该看的人看不到。例子：工资表只给 HR 看。
2. **Integrity（完整性）**：内容不能被偷偷改。例子：转账 1000 不能被改成 10000。
3. **Availability（可用性）**：该用的时候能用。例子：挂号系统不能总宕机。
4. **Authentication（认证）**：证明“你是谁”。例子：密码 + 手机验证码登录。
5. **Authorization（授权）**：登录后“你能做什么”。例子：你能看报表但不能删数据。
6. **Non-repudiation（不可否认）**：做过就不能赖。例子：数字签名后的合同不能否认签过。

2.3 本周学习任务

- 用自己的话解释这 6 个目标（每个一句话）。
- 试着给每个目标再举 1 个生活中的例子。

3 Week 2：先学“怎么防”，再学“防哪里”

3.1 本周要学会什么

- 安全工作有三步：预防、检测、响应（PDR）。
- 管理上有 AAA：认证、授权、审计。
- 网络是分层的，攻击也会按层出现。

3.2 术语白话 + 例子

1. **Prevention**：事前阻断。例子：防火墙先把高危端口封掉。
2. **Detection**：发现异常。例子：IDS 检测到可疑扫描并告警。
3. **Response**：出事后处置。例子：中毒主机隔离、重装、恢复备份。
4. **AAA**：认证身份、授予权限、记录日志。例子：VPN 登录全流程。
5. **OSI/TCP-IP 分层**：不同层有不同风险。例子：DNS 欺骗属于应用层风险。

3.3 本周学习任务

- 把你常用一个系统（如网盘）用 PDR 思路拆解一次。
- 想一想它的 AAA 分别在哪里体现。

4 Week 3：账号口令安全（第一部分）

4.1 本周要学会什么

- 密码为什么会被破解。
- 为什么不能明文存密码，为什么要哈希与加盐。
- 如何减少账号枚举（account harvesting）风险。

4.2 术语白话 + 例子

1. **Password Cracking**：猜密码。例子：先跑弱口令字典，再暴力枚举。
2. **Hash**：单向摘要。例子：文件改一个字符，哈希值就大变。
3. **Salt**：给密码加随机“调料”再哈希。例子：同样是 123456，数据库里哈希也不同。
4. **Account Harvesting**：探测哪些账号存在。例子：登录页提示“用户不存在”泄露信息。

4.3 本周学习任务

- 写出 5 条强密码规则（长度、复杂度、唯一性等）。
- 解释“为什么只哈希不加盐也不够”。

5 Week 4：账号口令安全（第二部分）与高级认证

5.1 本周要学会什么

- 认证协议基础：PAP vs CHAP。
- SSO、OTP、证书认证、生物认证各自优缺点。

5.2 术语白话 + 例子

1. **PAP**：认证材料可重放，安全性弱。例子：抓到包后可能直接复用。
2. **CHAP**：挑战应答，每次挑战不同。例子：门卫每次问不同口令。
3. **SSO**：一次登录多个系统。例子：公司门户一登，OA 和邮箱都可用。
4. **OTP**：一次性密码。例子：动态验证码每 60 秒变一次。
5. **Certificate Authentication**：用证书证明身份。例子：VPN 只允许企业证书设备接入。
6. **Biometrics**：生物特征认证。例子：指纹或人脸解锁。

5.3 本周学习任务

- 能口述 CHAP 四步流程。
- 解释为什么“方便的 SSO”也有“单点失守”风险。

6 Week 5：访问控制基础

6.1 本周要学会什么

- 什么是访问控制矩阵。
- ACL 与 Capability 的视角差异。
- DAC、MAC、RBAC 的区别。

6.2 术语白话 + 例子

1. **Access Control Matrix**：谁对什么资源有何权限的总表。
2. **ACL**：从“资源角度”看谁能访问我。
3. **Capability**：从“用户角度”看我能访问谁。
4. **DAC**：资源所有者自己授权。例子：你分享自己网盘文件。

5. **MAC（访问控制）**：按系统强制规则授权。例子：涉密系统按密级。
6. **RBAC**：按角色授权。例子：财务角色默认有报销审批权限。

6.3 本周学习任务

- 把“学校教务系统”画成一个小型权限矩阵。
- 说明为什么企业里 RBAC 常比直接 ACL 更好维护。

7 Week 6：经典安全模型

7.1 本周要学会什么

- BLP 与 Biba 的方向差异。
- 角色模型与利益冲突模型（Chinese Wall）。

7.2 术语白话 + 例子

1. **BLP**：防泄密。口诀：`No Read Up, No Write Down`。
2. **Biba**：防污染。口诀：`No Read Down, No Write Up`。
3. **Partial Ordering**：不是所有分类都能直接比较高低。
4. **Chinese Wall**：防利益冲突访问。例子：顾问看过 A 机密后不能看 B 竞品机密。

7.3 本周学习任务

- 用一句话区分 BLP 和 Biba 的“保护目标”。
- 每个模型各举 1 个业务场景。

8 Week 7：恶意软件（Malware）

8.1 本周要学会什么

- 病毒、蠕虫、木马、间谍软件、Rootkit、后门、僵尸网络的区别。
- 检测为什么不能只靠一种手段。

8.2 术语白话 + 例子

1. **Virus**：依附文件传播。例子：感染文档后继续感染别的文档。
2. **Worm**：可自动通过网络扩散。例子：一台中招后扫网段继续感染。

3. **Trojan**：伪装软件骗你安装。例子：破解工具里藏后门。
4. **Spyware/Keylogger**：偷行为数据和键盘输入。
5. **Rootkit**：隐藏恶意痕迹。例子：系统看不到它但它在运行。
6. **Botnet**：大量肉鸡被统一控制发起攻击。

8.3 本周学习任务

- 比较 Virus 和 Worm 的传播方式。
- 解释“为什么 Rootkit 更难查”。

9 Week 8：认证协议理论（上）

9.1 本周要学会什么

- 认证协议不只是“验证身份”，还要防重放和错配。
- 单向认证与双向认证差异。

9.2 术语白话 + 例子

1. **Entity Authentication**：确认通信实体身份。
2. **Unilateral Authentication**：只验证一方。
3. **Mutual Authentication**：双方互相验证。
4. **Protocol Requirements**：来源真实性、新鲜性、目标绑定、时序绑定。

9.3 本周学习任务

- 试说出“只做身份验证还不够”的原因。
- 举例说明为什么需要“消息目标绑定”。

10 Week 9：认证协议理论（下）

10.1 本周要学会什么

- 新鲜性机制：时间戳、序列号、Nonce。
- 链接请求与响应（linking messages）的意义。

10.2 术语白话 + 例子

1. **Replay Attack**：重放旧包骗系统。
2. **Time-stamp**：看时间是否过期。
3. **Sequence Number**：用递增序号防乱序与重放。
4. **Nonce**：一次性随机挑战值。
5. **Transaction ID**：把请求和响应一一绑定，防串包。

10.3 本周学习任务

- 比较时间戳和 Nonce 各自优缺点。
- 用一句话解释“加密本身不能自动防重放”。

11 Week 10：安全协议实例

11.1 本周要学会什么

- 理解典型认证协议消息来回设计思路。
- 明白“协议属性”如何被验证。

11.2 术语白话 + 例子

1. **Time-stamp Protocol**：轮次少，但依赖时钟同步。
2. **Nonce Protocol**：更灵活，但要有可靠随机数。
3. **Property Linking**：响应必须对应本次请求。

11.3 本周学习任务

- 画一个最小挑战应答流程图（3 4 步）。
- 指出流程里哪一步在防重放。

12 Week 11：Kerberos 与证书链

12.1 本周要学会什么

- Kerberos 的角色与三段式流程。
- 证书链如何建立跨域信任。

12.2 术语白话 + 例子

1. **Kerberos**：票据式认证系统。
2. **AS**：先验证你身份并给初始票据。
3. **TGS**：给你发访问具体服务的票据。
4. **TGT**：访问 TGS 的通行证。
5. **Session Key**：一次会话临时密钥。

12.3 本周学习任务

- 口述 Kerberos 三步：`C->AS`, `C->TGS`, `C->S`。
- 解释“为什么要用临时会话密钥而不是长期密钥一直用”。

13 Week 12：设备加固与网络架构设计

13.1 本周要学会什么

- 交换机/路由器加固、SNMPv3、边界和内部并重。
- 安全设计要考虑可用性，不要单点故障。

13.2 术语白话 + 例子

1. **Network Hardening**：收紧配置、打补丁、减少攻击面。
2. **Port Security**：限制交换机端口允许的设备。
3. **SNMPv3**：带认证和加密的网络管理协议。
4. **DMZ**：公网服务隔离区。
5. **Outbound Filtering**：限制内网向外发可疑流量。

13.3 本周学习任务

- 写一份 8 条网络加固清单（补丁、端口、账户、日志等）。
- 画一个“内网- DMZ -互联网”简图。

14 Week 13：防火墙、VPN、IPSec

14.1 本周要学会什么

- 防火墙规则如何设计（默认拒绝、最小权限、规则顺序）。
- IPSec 关键术语（AH/ESP、模式、SA、IKE）。

14.2 术语白话 + 例子

1. **Firewall**：按规则决定流量放行/拒绝。
2. **First Match**：规则从上到下，命中即停。
3. **AH**：认证/完整性/防重放，不加密。
4. **ESP**：可加密，VPN 常用。
5. **Transport vs Tunnel**：一个保上层负载，一个包整个原始 IP 包。
6. **SA/SPI**：安全参数集合及其编号。
7. **IKE Phase 1/2**：先建安全协商通道，再建业务 SA。

14.3 本周学习任务

- 给出一组最小防火墙策略（放 443，其他拒绝）。
- 解释 AH 和 ESP 的核心区别。

15 Week 14：SSL/TLS 与 IDS/IPS

15.1 本周要学会什么

- SSL/TLS 握手核心步骤与 VPN 的区别。
- IDS/IPS 的部署方式和取舍。

15.2 术语白话 + 例子

1. **TLS Handshake**：协商算法、验身份、建会话密钥。
2. **SSL/TLS vs IPSec VPN**：前者偏应用会话，后者偏网络隧道。
3. **HIDS**：主机侧检测。
4. **NIDS**：网络侧检测。
5. **Signature Detection**：抓已知攻击特征。

6. **Anomaly Detection**：抓“偏离正常”的行为。
7. **IPS**：在检测基础上可主动阻断。

15.3 本周学习任务

- 说出 HIDS 和 NIDS 的差别与适用场景。
- 解释“为什么异常检测会更容易误报”。

16 最后的学习建议（给零基础）

- 先会讲人话版本，再背术语，不要反过来。
- 每周做 3 件事：**看懂概念**、**会举例子**、**能画流程图**。
- 记忆优先级：BLP/Biba、PAP/CHAP、Kerberos、AH/ESP、IKE 两阶段、HIDS/NIDS。