国家信息安全水平考试

知识体系大纲

NISP 一级（渗透测试员）

NISP 运营中心
版本：1.0

目 录

第 1 章 国家信息安全水平考试（一级）知识体系概述 4
1.1 NISP 一级（渗透测试员）简介 4
1.2 NISP 一级（渗透测试员）知识体系框架结构 5
1.3 授课模式 6
第 2 章 知识体：信息安全基础 7
2.1 知识域：信息安全概述 7
2.2 知识域：信息安全管理 8
2.3 知识域：信息安全法律法规 8
第 3 章 知识体：信息安全基础技术 9
3.1 知识域：信息安全基础技术 9
3.2 知识域：网络安全防护技术 10
3.3 知识域：操作系统安全防护技术 11
3.4 知识域：Web 应用与数据安全 12
3.5 知识域：新技术新应用安全防护 13
第 4 章 知识体：渗透测试与修复防护 14
4.1 知识域：渗透测试基础 14
4.2 知识域：操作系统安全防护 14
4.3 知识域：Web 漏洞防护方法 15
4.4 知识域：网络安全防护方法 15

前言

随着互联网的发展和信息技术的普及，网络和信息技术已经进入到日常生活和工作中。然而，社会信息化和信息网络化的同时，信息安全问题成为影响国家 安全、经济发展、社会稳定、公民利益的重要问题。2014 年 2 月 27 日，中央网络安全和信息化领导小组宣告成立，既表明了网络信息安全目前面临的形势任务复杂和所处地位的重要，也标志着中国已把信息化和网络信息安全列入了国家发展 的最高战略方向之一。

我国信息安全保障体系建设，需要完善信息安全立法，做好信息安全顶层设 计，强化信息基础设施建设，特别地，需要加强信息安全人才培养与管理。国家信息化领导小组关于加强信息安全保障工作的意见中也明确规定把信息安全人才培养作为加强国家信息安全保障工作的一项重要任务。

2017 年 6 月 1 日，《网络安全法》正式实施，其中第二十条规定：“国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流”。为此，中国信息安全测评中心推出了国家信息安全水平考试（National Information Security Test Program，简称 NISP）。NISP 考试采用理论与实践相结合的教学模式，是评定考生应用信息安全基础知识与防护技能的全国性信息安全水平考试体系。

本大纲从个人在工作、学习和生活中面临的信息安全问题出发，结合我国网络基础设施和信息系统安全保障的实际需求，以知识体系的基础性和实用性为原则，明确规定国家信息安全水平考试（一级）应当掌握的知识点，是 NISP（一级）教材编制、讲师授课、学生学习以及考试命题的重要依据。

第 1 章 国家信息安全水平考试（一级）知识体系概述

1.1 NISP 一级（渗透测试员）简介

国家信息安全水平考试（National Information Security Test Program，简称NISP）分为不同级别，分别定位于不同层次的目标群体。

NISP一级主要面向各行业信息系统使用人员及高校大学生，普及信息安全知识，增强信息安全意识，提高安全防范技能，为国家信息安全保障工作的顺利实施奠定基础。

NISP 一级（渗透测试员）以常识性、普及性知识为主，能力目标如下：

[1] 了解信息安全、信息安全保障和信息系统安全保障的基本含义和作用

[2] 了解信息安全相关法律法规

[3] 了解信息安全管理和信息安全风险管理的含义和作用

[4] 了解信息安全应急响应和灾难备份的概念与方法

[5] 理解信息安全基础技术，含密码学、身份认证、访问控制及安全审计

[6] 掌握网络、操作系统、智能终端和云计算的安全威胁和安全防护技术

[7] 掌握浏览器安全、网上金融交易安全、电子邮件安全、数据安全和账户口令安全的防护方法

[8] 掌握信息收集方法、扫描工具使用及渗透测试平台搭建方法

[9] 掌握主机漏洞与防护方法、常见 Web 漏洞与防护方法、常见网络安全防护方法

学员应掌握的预备知识：

- 计算机和网络基础知识
- 计算机操作系统基础知识

1.2 NISP 一级（渗透测试员）知识体系框架结构

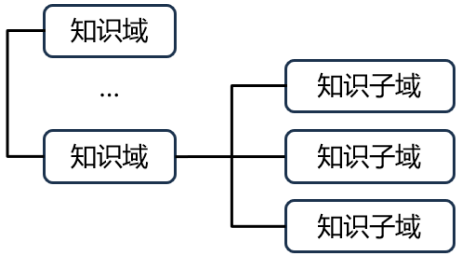

图 1-1：NISP 一级（渗透测试员）知识体系的组件模块结构

本大纲规定了知识子域中每一个知识要点的内容和深度要求，分为 3 个级别，分别是了解、理解和掌握。

- 了解：最低深度要求，学生需要正确认识该知识要点的基本概念和原理；
- 理解：中等深度要求，学生需要在正确认识该知识要点的基本概念和原理的基础上，深入理解其内容，并可以进一步的判断和推理；
- 掌握：最高深度要求，学生需要正确认识该知识要点的概念、原理，并在深入理解的基础上灵活运用。

NISP 一级（渗透测试员）知识体系结构共包含 2 个模块，分别为：

- 通用知识模块：包含信息安全基础和网络安全知识两个知识体。信息安全基础介绍了信息安全概念和基本属性、信息安全的发展阶段与形势、信息安全保障和信息系统安全保障的含义和模型，以及信息安全相关法律法规和政策；网络安全知识介绍了密码学基础知识、身份认证、访问控制及安全审计的概念，重点阐释网络安全攻防知识，操作系统安全威胁和防护，WEB 安全知识、数据安全知识等，它是 NISP 一级需要掌握的主要专业基础知识。
- 专业技能模块：包含渗透测试基础、主机漏洞与防护、Web 漏洞与防护和网络安全与防护四个知识体。需要掌握信息收集的方法及工具使用方法，扫描状态确认方法，渗透测试环境搭建和工具使用方法，常见漏洞原理、漏洞验证及漏洞修复方法等。

NISP 一级（渗透测试员）知识体系结构框架如图 1-2 所述。

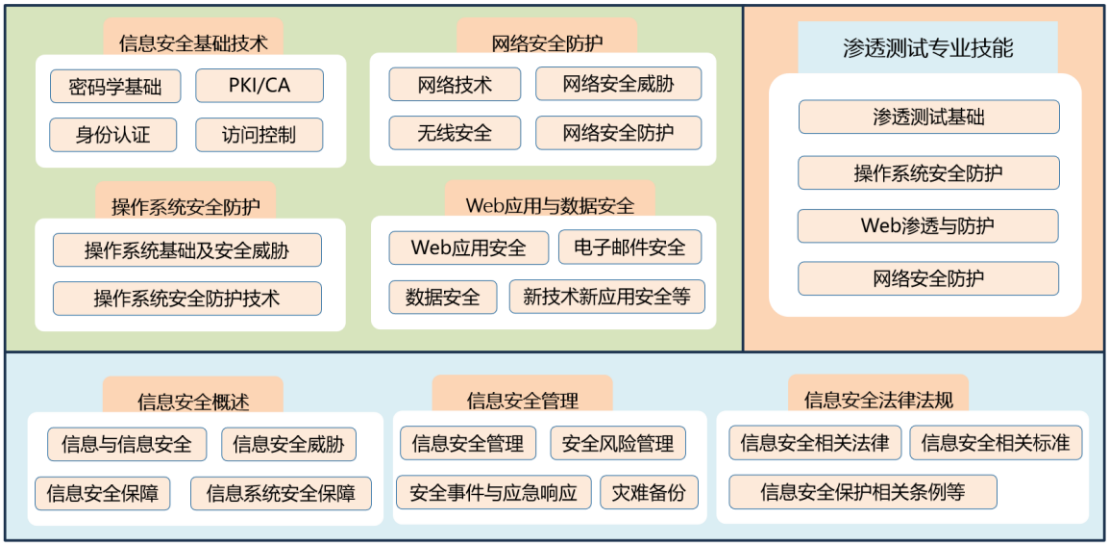

图 1-2：NISP 一级（渗透测试员）知识体系结构框架

1.3 授课模式

NISP 一级（渗透测试员）培训采用视频学习的模式，培训课时为 48 学时，表 1-1 中描述了各知识域的建议课程时间安排。

表 1-1：NISP 一级（渗透测试员）课程时间安排

知识体	组成部分	课时
信息安全基础知识	第一部分 信息安全概述	2 课时
	第二部分 信息安全管理	2 课时
	第三部分 信息安全法律法规	2 课时
信息安全专业技术知识	第四部分 信息安全基础技术	4 课时
	第五部分 网络安全防护技术	4 课时
	第六部分 操作系统安全防护技术	4 课时
	第七部分 Web 应用与数据安全	8 课时
	第八部分 新技术新应用安全	4 课时
渗透测试与修复防护	第九部分 渗透测试基础	2 课时
	第十部分 操作系统安全防护	4 课时
	第十一部分 Web 渗透与防护	6 课时
	第十二部分 网络安全防护	4 课时
合计：48 课时		

第 2 章 知识体：信息安全基础

信息安全基础介绍了信息安全概念和基本属性、我国面临的信息安全威胁、信息安全问题产生根源、信息安全的发展阶段与形势、信息安全保障和信息系统安全保障的含义和模型，以及信息安全相关法律法规和政策，它是信息安全人才首先需要掌握的基础知识。

2.1 知识域：信息安全概述

- 知识子域：信息与信息安全
  - 了解信息、信息技术、信息安全的基本概念
  - 了解信息技术的发展阶段及各阶段的主要特点
  - 了解信息安全的基本属性和特征
- 知识子域：信息安全威胁
  - 了解我国面临的三类信息安全威胁，及其主要表现形式
  - 理解信息安全问题产生的根源
- 知识子域：信息安全发展阶段与形势
  - 了解信息安全发展的四个阶段及各阶段的特点
  - 了解我国信息安全的形势
- 知识子域：信息安全保障
  - 了解信息安全保障的基本概念、作用及模型
  - 理解信息安全保障与传统信息安全的区别
- 知识子域：信息系统安全保障
  - 了解信息系统的基本概念
  - 了解信息系统安全保障的基本概念和含义
  - 了解信息系统安全保障中风险、保障和使命的关系
  - 理解信息系统安全保障模型，以及保障要素、生命周期和安全特征的内容和含义

2.2 知识域：信息安全管理

- 知识子域：信息安全管理概述
  - ◆ 了解信息安全管理的概念和内容
  - ◆ 理解成功实施信息安全管理的关键因素
- 知识子域：信息安全风险管理
  - ◆ 了解风险、信息安全风险的概念，以及威胁、脆弱性、影响和资产的含义和关系
  - ◆ 了解风险管理、风险评估的基本概念和作用，以及信息安全管理体系的概念
  - ◆ 了解信息安全风险管理的基本步骤
- 知识子域：信息安全事件与应急响应
  - ◆ 了解信息安全事件的概念和分类，以及影响信息安全事件分级的主要考虑的三个要素
  - ◆ 了解信息安全应急响应的概念和作用；理解信息安全应急响应管理过程
- 知识子域：灾难备份
  - ◆ 了解灾难、灾难恢复和灾难备份的概念与作用，理解灾难备份的方法
  - ◆ 了解表示灾难恢复系统能力的业务参数
  - ◆ 了解本地备份与异地备份、数据级灾备和系统级灾备、完全备份和不完全备份的概念
  - ◆ 了解制定特定备份策略时的策略设置方法

2.3 知识域：信息安全法律法规

- 知识子域：信息保护相关法律法规
  - ◆ 了解国家秘密的概念、分级、基本范围和保密期限
  - ◆ 了解危害国家秘密安全的行为及犯罪行为
  - ◆ 了解《网络安全法》、《数据安全法》、《刑法》中保护国家秘密的条款和规定

◆ 了解商业秘密的概念及侵犯商业秘密的行为

◆ 了解《反不正当竞争法》、《合同法》、《劳动合同法》中保护商业秘密的主要条款

◆ 了解个人信息的概念及侵犯个人信息的行为

◆ 了解《宪法》、《居民身份证法》、《侵权责任法》中保护个人信息的主要条款

- 知识子域：打击网络违法犯罪相关法律法规

◆ 了解网络违法犯罪的基本概念及五大类网络违法犯罪行为

◆ 了解《关于维护互联网安全的决定》、《治安管理处罚法》中打击网络违法犯罪的主要条款

- 知识子域：信息安全管理相关法律法规

◆ 了解《电子签名法》、《保守国家秘密法》中关于信息安全管理的主要条款

第 3 章 知识体：信息安全基础技术

信息安全技术介绍了密码技术、身份认证、访问控制及审计技术的概念，重点阐释网络安全威胁和防护技术，操作系统安全威胁和防护技术，Web 应用安全，以及移动智能终端安全威胁和防护技术，是学生需要掌握的主体知识内容。

3.1 知识域：信息安全基础技术

- 知识子域：密码学基础

◆ 了解明文、密文、密钥、加密和解密等密码学基本概念和术语；

◆ 了解对称密码算法、非对称密码算法的概念和典型算法及混合加密模式的工作原理；理解对称密码、非对称密码体制的优缺点；掌握 典型密码体制的应用举例

◆ 了解数字签名的概念和典型算法；理解数字签名的工作原理和主要应用；掌握数字签名的应用举例

◆ 了解哈希函数的概念和典型算法；理解哈希函数的特点；掌握哈希

函数的应用

- 知识子域：数字证书与公钥基础设施
  - 了解数字证书的作用、概念、组成部分和类型
  - 了解公钥基础设施的概念和组成及认证权威机构的概念和主要功能
- 知识子域：身份认证
  - 了解身份认证的概念和基本方法
  - 了解静态口令认证、短信口令认证、动态口令认证、USB Key 认证、生物认证、双因素认证
- 知识子域：访问控制
  - 了解访问控制的基本概念和主要任务及其三要素
  - 了解自主访问控制、强制访问控制和基于角色的访问控制方法
- 知识子域：安全审计
  - 了解被动式审计、主动式审计两种安全审计方法
  - 了解审计、安全审计和日志的基本概念及安全审计的作用与功能
  - 掌握系统日志安全审计的操作

3.2 知识域：网络安全防护技术

- 知识子域：网络技术基础知识
  - 了解万维网（WWW）、统一资源定位符（URL）、超文本标记语言（HTML）、传输控制协议/因特网互联协议（TCP/IP）、超文本 传输协议（HTTP）、端口、域名系统（DNS）等网络基本概念
- 知识子域：网络安全威胁
  - 理解网络嗅探的安全威胁
  - 理解网络钓鱼攻击的安全威胁
  - 理解拒绝服务攻击的安全威胁
  - 理解远程控制攻击的安全威胁
  - 理解社会工程学概念和社会工程学攻击威胁
- 知识子域：网络安全防护与实践
  - 了解虚拟专用网的概念和特点；理解虚拟专用网的主要应用

◆ 了解 Internet 协议安全性（IPSec）协议、安全套接层协议（SSL）的概念和功能；理解 Internet 协议安全性（IPSec）协议的工作模式

◆ 了解防火墙的概念和功能

- 知识子域：无线局域网安全防护

◆ 了解无线局域网的概念、特点和安全威胁

◆ 了解无线接入点的概念；理解无线接入点安全管理方法

◆ 掌握无线路由器的安全设置

3.3 知识域：操作系统安全防护技术

- 知识子域：操作系统概述

◆ 了解操作系统的基本概念及主要功能：CPU 管理、存储管理、设备管理、文件管理、网络与通信管理和用户接口资源管理

- 知识子域：操作系统的安全威胁

◆ 了解漏洞的概念和安全威胁；理解漏洞产生的原因；了解漏洞扫描的概念和实现手段

◆ 了解恶意代码的概念和安全威胁，以及计算机病毒的概念和对操作系统的危害

◆ 了解木马、蠕虫的概念和特点，木马的传播方式及危害以及防范蠕虫病毒的安全建议

◆ 了解端口扫描的概念、安全威胁和隐蔽手段

- 知识子域：操作系统安全防护

◆ 理解个人操作系统安全防护策略：关闭不必要服务和端口，开启审核策略和密码策略等的安全防护策略方法；掌握 Windows 操作系统 安全使用方法

◆ 了解个人防火墙的概念；掌握个人防火墙配置

◆ 理解补丁的概念和作用

◆ 掌握终端安全防护软件的功能和作用

3.4 知识域：Web 应用与数据安全

- 知识子域：Web 应用安全基础
  - ◆ 了解 Web 常见结构
  - ◆ 了解 Web 请求流程，HTTP 请求格式、HTTP 请求方法和状态码
  - ◆ 掌握 Web 漏洞扫描工具使用方法
- 知识子域：浏览器安全
  - ◆ 了解客户端与服务器端的概念，以及客户端/服务器结构和浏览器/服务器结构
  - ◆ 理解常见的浏览器安全措施；掌握浏览器安全设置和安全使用方法
- 知识子域：网上金融交易安全
  - ◆ 了解网上金融交易的概念
  - ◆ 了解网上金融交易常用的安全防护措施
- 知识子域：电子邮件安全
  - ◆ 了解电子邮件的概念、电子邮件系统结构；理解电子邮件工作流程
  - ◆ 理解邮箱地址欺骗、垃圾邮件、邮件病毒、邮件炸弹等主要安全威胁，以及电子邮件安全防护技术
  - ◆ 掌握电子邮件客户端安全设置和安全使用方法
- 知识子域：数据安全
  - ◆ 了解数据备份的概念；理解数据备份的重要性和常见手段
  - ◆ 了解数据恢复的概念和常用数据恢复工具；掌握数据恢复操作方法和要点
  - ◆ 了解常用数据加密和签名的重要性；掌握数据加密和签名的常见手段
  - ◆ 了解数据删除技术
- 知识子域：账户口令安全
  - ◆ 了解账号口令的安全威胁和口令设置的基本原则

3.5 知识域：新技术新应用安全防护

- 知识子域：移动智能终端安全
  - ◆ 了解移动智能终端的基本概念、特点、分类和功能，以及常见智能终端操作系统
  - ◆ 了解伪基站的概念和伪基站攻击威胁
  - ◆ 了解二维码扫描的概念和二维码扫描威胁
  - ◆ 了解移动智能终端遗失和恶意扣费软件的安全威胁
  - ◆ 了解手机病毒的概念、危害和安全威胁
  - ◆ 了解移动智能终端的安全使用建议
  - ◆ 理解手机病毒、二维码扫描、移动智能终端遗失等的安全防范措施
  - ◆ 掌握手机终端防护软件的设置
- 知识子域：物联网安全
  - ◆ 了解物联网的概念、安全特征与架构
  - ◆ 了解工业互联网的典型架构
  - ◆ 了解工业互联网的安全需求及防护机制
- 知识子域：云计算安全
  - ◆ 了解云计算的概念，云主机的概念和云服务的类型；
  - ◆ 了解 IaaS 云服务架构，服务器虚拟化、存储虚拟化、网络虚拟化等核心架构安全威胁
  - ◆ 了解 PaaS 云服务架构，分布式文件系统、分布式计算、分布式数据库和分布式同步机制等安全威胁
  - ◆ 了解 SaaS 云服务模式，多租户、数据库、应用程序等安全威胁
- 知识子域：大数据安全
  - ◆ 了解大数据的特征、分类和价值
  - ◆ 了解典型行业大数据应用和风险
  - ◆ 了解大数据应用安全的防护措施

第 4 章 知识体：渗透测试与修复防护

渗透测试人员通过对目标网络及系统进行渗透测试，发现安全问题并提出改进建议。本章主要介绍信息收集的方法、渗透测试平台搭建及工具使用、系统安全防护的措施、常见 Web 漏洞的防护方法和常见网络安全的防护方法。

4.1 知识域：渗透测试基础

- 知识子域：信息收集方法
  - 理解信息收集的概念、作用及信息收集的工作内容
  - 掌握信息收集的方法
- 知识子域：扫描工具的安装与使用
  - 掌握端口扫描工具的安装与使用
  - 了解漏洞扫描的作用并掌握典型漏洞工具安装与使用
- 知识子域：渗透测试平台搭建
  - 掌握 kali linux 渗透平台的搭建流程
  - 了解渗透测试工具集

4.2 知识域：操作系统安全防护

- 知识子域：系统漏洞防护措施
  - 了解操作系统的功能，访问控制、文件加密等安全机制
  - 了解系统漏洞产生的原因
  - 理解操作系统安全防护的措施
- 知识子域：恶意代码防护措施
  - 了解恶意代码的概念及类型
  - 理解恶意代码的防护措施
- 知识子域：入侵威胁防护措施
  - 了解入侵威胁的原理

- 理解入侵威胁的防护措施

4.3 知识域：Web 漏洞防护方法

- 知识子域：SQL 注入漏洞与防护
  - 了解 SQL 注入漏洞的技术原理
  - 理解 SQL 注入漏洞的防护方法
- 知识子域：文件上传漏洞与防护
  - 了解文件上传漏洞的技术原理
  - 理解文件上传漏洞的防护方法
- 知识子域：XSS 和 CSRF 漏洞与防护
  - 了解 XSS 和 CSRF 漏洞的技术原理
  - 理解 XSS 和 CSRF 漏洞的防护方法
- 知识子域：远程代码执行漏洞与防护
  - 了解远程代码执行漏洞的技术原理
  - 理解远程代码执行漏洞的防护方法

4.4 知识域：网络安全防护方法

- 知识子域：ARP 欺骗防护方法
  - 了解 ARP 工作原理和 ARP 欺骗的原理
  - 理解 ARP 欺骗的防护方法
- 知识子域：网络欺骗防护方法
  - 了解网络欺骗的常见类型
  - 理解 IP 地址欺骗的原理和防护方法
- 知识子域：会话劫持防护方法
  - 了解会话劫持攻防的分类
  - 理解 DNS 欺骗的原理和防护方法
- 知识子域：DDoS 攻击防护方法

- 了解 DDoS 攻击实现方式
- 理解 DDoS 攻击的防护方法