国家信息安全水平考试

知识体系大纲

（渗透测试专项）

NISP 专项证书管理中心

2020 年 12 月 30 日

目 录

一、概述

信息安全作为我国信息化建设健康发展的重要因素，关系到贯彻落实科学发展观、全面建设小康社会、构建社会主义和谐社会和建设创新型社会等国家战略举措的实施，是国家安全的重要组成部分。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。在信息系统安全保障工作中，人是最核心、也是最活跃的因素，人员的信息安全意识、知识与技能已经成为保障信息系统安全稳定运行的重要基本要素之一，近年来，我国网络安全人才培养取得一定进展，但专业人才缺口仍然较大。

为培养更多优秀的实践型网络安全人才，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，是评定考生掌握信息安全知识、技能和本领的全国性信息安全水平考试体系。NISP 水平考试共分三级，一级、二级为通用证书，分别定位于不同层次的目标群体。三级为专项证书，面向特定技术领域的人才进行培养和颁发。

NISP 一级主要面向各行业信息系统使用人员及高校非信息安全专业学生，普及信息安全知识，增强信息安全意识，提高安全防范技能，为今后工作中能安全的使用信息系统。

NISP 二级主要面向从事信息安全相关行业人员及高校信息安全相关专业学生，构建信息安全知识框架，帮助学员形成信息安全保障的总体概念，为国家信息安全保障工作的顺利实施打下坚实的理论基础。

NISP 三级（专项）主要面向有志于从事信息安全相关行业的从业人员，在理解信息安全基础知识基础上，掌握信息系统安全运营知识、渗透测试、信息系统审计、数据隐私保护、工业控制系统安全等特定信息安全领域的知识和技能，为国家培养跨领域的信息安全专项人才。

1.1 适用范围

本大纲从我国国情和企事业单位渗透测试人才的需求出发，结合我国网络基础设施和重要信息系统安全保障的实际需求，兼顾知识体系的全面性、实用性和实践性。本大纲明确 NISP 渗透测试专业人员应当掌握的知识要点，是 NISP 渗透测试专项（NISP-PT）课程教材编制、讲师授课、学员学习以及考试命题的重要依据。

1.2 大纲框架结构

NISP 渗透测试专项知识体系使用组件模块化的结构，包括知识域和知识子域两个层次。

知识域：是属于同一技术领域的知识内容构成的相对独立的知识集合；

知识子域：是构成知识域的基本模块，对知识域进一步分解细化形成的完整的知识组件。每个知识子域包含了一个或多个知识要点。

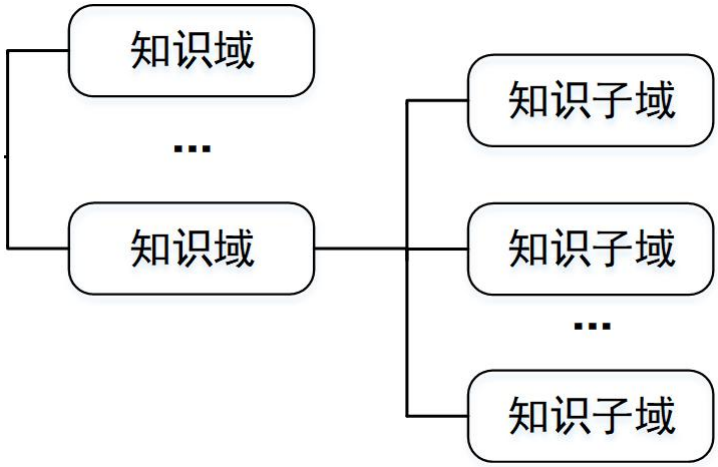

图 1：知识体系组件模块结构

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“了解”、“理解”和“掌握”三类。

了解：是最低深度要求，学员需要正确认识该知识点的基本概念和原理；

理解：是中等深度要求，学员需要在正确认识该知识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：是最高深度要求，学员需要正确认识该知识点的概念、原理，并在深入理解的基础上灵活运用。

1.3 知识体系构成及考试

NISP 渗透测试专项知识体系包括综合理论、专项基础和专项能力三个模块。

综合理论模块为所有 NISP 专项课程通用，采用 NISP 二级课程体系。

专项基础模块划分为八个知识域，是渗透测试能力课程的基础，在培训时可根据学员基础水平安排适当课程。该模块中的知识在理论考试中均可作为考点。

专项能力模块包括六个知识域，在理论考试和实操考试中会将此模块中的知识点作为考点。

图 2　NISP-PT 知识体系结构

NISP 渗透测试专项考试题型为选择题与实操题,总分共 100 分，其中理论题（单项选择题）40 分，实操题 60 分，得到 70 分以上（含 70 分）为通过。

二、专项基础模块

2.1 知识域：网络与网络安全设备

2.1.1 知识子域：网络与网络设备

了解网络拓扑、网络结构等计算机网络基础知识；

了解路由器、交换机等网络设备的工作原理及作用；

了解 IP 地址规划、Vlan 等网络设计规划相关概念。

2.1.2 知识子域：防火墙

了解防火墙产品的基本概念、工作原理及应用场景；

了解包过滤、代理、NAT、状态检测等防火墙应用技术；

了解防火墙部署的方式及防火墙应用中的优缺点。

2.1.3 知识子域：边界安全设备

了解网闸的工作原理及应用场景；

了解 IPS、UTM 等边界安全防护设备的工作原理及应用场景；

了解防病毒网关、上网行为管理等防护设备的工作原理及应用场景。

2.1.4 知识子域：入侵检测与网络审计

了解入侵检测系统的基本概念、工作原理及应用场景；

了解入侵检测系统的数据采集、入侵检测实现原理；

了解入侵检测产品的类型、部署方式及优缺点；

了解网络审计、数据库审计等审计类产品的工作原理、部署方式及应用场景。

2.1.5 知识子域：虚拟专网（VPN）

了解虚拟专网（VPN）的概念，作用及应用场景；

了解 VPN 实现的技术原理及隧道模式、传输模式的区别；

了解 IPSec、SSL 两种不同 VPN 协议的区别。

2.2 知识域：TCP/IP 协议安全

2.2.1 知识子域：OSI 七层模型与 TCP/IP 协议

了解 OSI 七层模型的构成、分层作用；

了解 OSI 七层模型中每一层的作用；

了解 OSI 七层模型中数据发送和接收的过程（数据封装和数据分用）；

了解 TCP/IP 协议四层架构。

2.2.2 知识子域：网络接口层

了解网络接口层的作用和主要的协议；

了解 ARP、RARP 协议的作用；

了解 ARP 协议的工作原理及实现。

2.2.3 知识子域：互联网络层协议

了解互联网网络层的作用及主要协议；

理解 IP 协议包头的结构及各字段的作用；

理解 IP 协议工作机制及无连接、不可靠的特点；

了解 ICMP 协议的作用及工作机制；

了解 IGMP 协议的作用。

2.2.4 知识子域：传输层协议

了解传输层协议的作用；

理解 TCP 协议包头的结构及各字段的作用；

理解 TCP 协议工作机制及连接、可靠的实现方式；

了解 TCP 协议建立连接三次握手、断开连接四次挥手协议处理方式；

了解 TCP 协议流量控制等机制的实现方式；

理解 UDP 协议包头的结构及各字段的作用；

理解 TCP、UDP 协议不同的应用场景。

2.2.5 知识子域：应用层协议

了解 FTP 协议的工作机制、安全风险及相关命令；

了解 Telnet 协议工作机制、安全风险及解决方案；

了解 DNS 协议的工作机制及安全风险；

了解电子邮件协议（smpt/pop3）工作机制、安全风险及解决方案。

2.3 知识域：Window 系统安全基础

2.3.1 知识子域：windows 终端安全

了解 windows 终端安全安装的基本要求；

了解 Windows 终端安全配置等相关要求。

2.3.2 知识子域：windows server 安全设置

了解 windows server 安全安装的基本概念要求；

掌握 windows Server 安全策略设置；

掌握 windows 系统常用命令的使用。

2.3.3 知识子域：windows 系统服务配置

掌握 Windows server 上各类服务的部署及安全设置；

了解 Windows Server 上 VPN、远程终端等远程管理服务的部署及安全设置。

2.4 知识域：Linux 系统服务及安全管理

2.4.1 知识子域：Linux 系统终端安全

了解 Linux 系统终端安装过程；

掌握 Linux 系统常用命令的使用；

了解 Linux 系统的日常使用及安全策略设置。

2.4.2 知识子域：Linux 系统服务安全部署

了解 Linux 系统服务器安装过程；

掌握 Linux 系统上 FTP、DNS、Openssh 等常用应用的安全部署。

2.5 知识域：Web 应用安全基础

2.5.1 知识子域：Web 浏览器安全

了解 Web 应用体系的结构及相关问题；

理解 Web 客户端（浏览器）常用的安全机制及安全风险；

理解浏览器端面临的网页挂马、网络钓鱼等攻击的技术原理并掌握浏览器安全设置方法。

了解 XML、HMTL 等 Web 应用中常用开发语言。

2.5.2 知识子域：HTTP 协议

理解 HTTP 协议的请求、响应工作机制；

了解 URL、请求方法（Post、get 等）、响应状态码等基本概念；

了解 cookie、session 等机制及存在的安全风险。

2.6 知识域：数据库安全

2.6.1 知识子域：数据库安全基础

了解 SQL 的基本概念并掌握 Select、update、delete 等常用的 SQL 命令的使用；

了解数据库用户、权限管理机制及安全策略；

了解存储过程、视图等数据库机制对安全的作用；

掌握数据库漏洞扫描软件的使用；

理解针对数据库的攻击方法并掌握如何构建安全的数据库防御体系。

2.6.2 知识子域：数据库安全配置及管理

掌握 SQL server 安全配置、安全管理的方法与工具；

掌握 Mysql 安全配置、安全管理的方法与工具；

掌握 Oracle 安全配置、安全管理的方法与工具。

2.7 知识域：Web 服务软件安全

2.7.1 知识子域：IIS 服务配置及安全管理

掌握 IIS 服务网站配置的方法；

掌握 IIS 安全配置及安全管理的方法；

掌握 IIS 中 Https 的配置方法；

掌握 IIS 日志安全配置及管理相关要求。

2.7.2 知识子域：Web 服务配置及安全管理

掌握基于 Apache 配置 Web 网站的方法及安全管理要求；

掌握基于 Nginx 配置 Web 网站的方法及安全管理要求；

了解 Tomcat、weblogic 等其他 Linux 系统常用 Web 服务软件的配置和管理要求。

2.8 知识域：渗透测试工具

2.8.1 知识子域：渗透测试集成工具

了解 kali Linux 等渗透测试集成工具包；

掌握 Kali Linux 在虚拟机及实体计算机上安装及配置。

2.8.2 知识子域：渗透测试模拟环境

了解 virtualbox、kvm 等虚拟机环境的搭建；

掌握在虚拟机中导入虚拟系统的方法。

2.8.3 知识子域：python 语言基础

掌握 Python 语言环境的部署；

了解 Python 脚本在渗透测试中的应用。

三、专项能力模块

3.1 知识域：渗透测试基础

3.1.1 知识子域：渗透测试方法与流程

了解渗透测试的概念、特点及优缺点；

了解白盒、黑盒、灰盒等渗透测试方法在渗透测试中的应用；

了解渗透测试项目启动、测试准备、测试实施、测试汇报各阶段的工作内容；

了解渗透测试常用的工具类型；

了解渗透测试中风险规避的原则及常用措施；

了解渗透测试方案、报告等材料编写要点。

3.1.2 知识子域：信息收集及数据分析

了解信息收集的概念、作用及信息收集的工作内容；

掌握公开信息收集的方法与技巧；

理解端口扫描的作用并掌握 nmap 等端口扫描常用工具使用；

了解漏洞扫描的作用并掌握典型的系统漏洞扫描、Web 漏洞扫描、数据库漏洞扫描工具使用；

了解 kali Linux 等综合渗透测试工具集；

了解漏洞关联信息收集的方法及渠道。

3.2 知识域：网络通信安全与渗透

3.2.1 知识子域：电子欺骗攻击

理解 ARP 欺骗的技术实现原理及防御措施；

了解 IP 欺骗的技术原理及防御措施；

了解 DNS 欺骗的技术原理及防御措施。

3.2.2 知识子域：拒绝服务攻击

理解 SYN Flood 攻击的实现原理及防御措施；

理解 UDP Flood 攻击的实现原理及防御措施；

了解 Teardrop（碎片攻击）的实现原理及防御措施；

了解 ping of death 的实现原理及防御措施；

了解 Smurf、Land 等其他利用协议设计缺陷及系统实现缺陷进行拒绝服务攻击的原理；

了解分布式拒绝服务攻击的实现方式及实现工具。

3.2.3 知识子域：无线局域网安全

了解无线局域网体系及安全机制、安全问题；

了解 AP 伪造攻击的威胁并掌握伪 AP 创建方法及攻击利用；

了解密码破解、拒绝服务等无线局域网攻击技术原理；

了解无线局域网安全协议 WEP、WPA2 加密网络的破解方法。

3.3 知识域：Windows 系统安全

3.3.1 知识子域：账户安全

理解 windows 系统用户信息安全管理的机制；

了解 windows 口令散列码的获取及破解方法并掌握相关工具的使用；

掌握 windows 系统中及 Powershell 中账户管理相关命令的使用；

掌握 Windows 口令安全策略的设置。

3.3.2 知识子域：进程与文件系统安全

理解 Windows 系统中访问控制、完整性保护等文件保护机制；

了解 bitlocker 等文件加密机制并掌握对文件进行加密保护的方法；

掌握文件删除、粉碎及数恢复的方法及工具。

理解 Windows 系统进程、服务的权限管理的机制；

掌握使用 Windows 系统命令及 powershell 对服务进行管理的方法；

了解 DLL 注入、加载设备驱动等系统后门设置的原理。

3.3.3 知识子域：安全配置与管理

了解 Windows 系统安全安装、部署的相关概念；

了解系统备份、还原点创建的方法；

了解 Windows 安全中心的作用并掌握安全中心配置管理的方法；

掌握服务安全、网络访问安全等策略的设置方法；

了解 Windows 日志系统并掌握如何对日志进行安全管理。

3.4 知识域：Linux 系统安全

3.4.1 知识子域：账户安全

理解 Linux 系统用户信息安全管理的机制；

了解 Linux 账户的口令散列码破解方法并掌握相关工具的使用；

掌握 Linux 系统中账户管理相关命令的使用；

掌握 Linux 口令安全策略的设置。

3.4.2 知识子域：进程与文件系统安全

理解 Linux 系统中访问控制、完整性保护等文件保护机制；

了解 Linux 下文件加密机制并掌握对文件进行加密保护的方法；

掌握 Linux 下文件删除、粉碎及数恢复的方法及工具。

理解 Linux 系统进程的权限管理的机制；

掌握对进程进行管理的 Linux 系统命令的使用。

3.4.3 知识子域：安全配置与管理

了解 Linux 安全部署相关要求；

了解 linux 远程管理的方法及安全防御措施；

了解 Linux 网络防火墙框架 iptables、firewalld 的应用；

了解 Linux 日志系统并掌握如何对日志进行安全管理。

3.5 知识域：Web 渗透

3.5.1 知识子域：SQL 注入攻击

理解 SQL 注入漏洞原理及危害；

理解 SQL 注入攻击实现方式及攻击过程；

掌握使用 Sqlmap 进行注入检测及攻击利用的方法；

了解 SQL 注入检测时注入绕过、盲注等注入攻击技巧；

掌握 SQL 注入漏洞修复和防御措施。

3.5.2 知识子域：其他注入漏洞

理解 XML 注入、Xpath 注入、命令注入等漏洞产生的原理；

掌握 XML 注入、Xpath 注入、命令注入等攻击利用方法及工具；

掌握 XML 注入、Xpath 注入、命令注入漏洞的防御措施。

3.5.3 知识子域：跨站脚本漏洞

了解跨站脚本漏洞的原理及危害；

理解存储式、反射式、DOM 等跨站脚本漏洞的检测、利用方法及防御措施；

了解服务端请求伪造（SSRF）漏洞的概念；

了解服务端请求伪造（SSRF）漏洞检测方法、工具及漏洞修复。

3.5.4 知识子域：跨站请求漏洞

了解跨站请求（CSRF）漏洞产生的原因及危害；

理解 CSRF 漏洞的利用和修复方方法。

3.5.5 知识子域：访问控制漏洞

了解文件上传漏洞产生的原因及危害；

了解服务端语言对上传文件类型限制方法；

掌握上传漏洞的检测思路和修复方法；

了解文件非法下载产生的原因及危害；

掌握通过文件下载漏洞读取服务端文件的方法；

掌握能够通过代码审计和测试找到文件下载漏洞；

掌握修复文件下载漏洞的方法。

了解横向越权、垂直越权漏洞的基本概念及形式；

了解横向越权、垂直越权漏洞的利用方法及工具；

了解横向越权、垂直越权漏洞的测试和修复方法。

3.5.6 知识子域：会话管理漏洞

了解会话劫持漏洞的原理及危害；

掌握会话劫持漏洞防御方法。

了解会话固定漏洞的原理及危害；

了解会话固定漏洞的检测及防御方法。

3.6 知识域：渗透测试通用技术

3.6.1 知识子域：口令攻击

了解口令嗅探、远程破解、重放攻击等针对口令的攻击方法；

理解口令远程暴力破解的原理及技术实现并掌握远程口令破解攻击的工具使用；

理解口令字典、彩虹表的概念及在口令破解中的应用；

掌握口令字典生成工具的使用及口令字典的构造方法。

3.6.2 知识子域：代码安全与溢出攻击

了解缓冲区溢出攻击的相关概念及基本原理；

理解缓冲区溢出攻击的实现及威胁；

了解 Metasploit 框架的部署及使用方法；

了解缓冲区溢出利用代码(exploit)的编译及攻击实现过程。

3.6.3 知识子域：社会工程学攻击

了解社会工程学攻击的概念；

理解社会工程学在信息安全中的重要性；

了解利用社会工程学直接攻击的方式方法；

了解社工库的概念及在网络攻击中的作用；

掌握社会工程学在口令破解中的利用方法；

理解应对社会工程学攻击的防御措施。

3.6.4 知识子域：恶意代码

了解恶意代码的概念及类型；

理解文件传播、网络传播、漏洞传播等恶意代码的传播方式的技术原理；

了解恶意代码的自我保护机制、隐藏等机制的技术原理。