目录

第十五届“新华三杯”全国大学生数字技术大赛预赛考试大纲（安全赛道）.....2

1 概述.....2

1.1 文件说明.....2

1.2 预赛考试说明.....2

1.3 建议参加的培训.....3

2 预赛考试知识点分布.....4

2.1 安全基础知识.....4

2.1.1 法律法规与政策合规.....4

2.1.2 网络安全基础与安全防护.....4

2.1.3 操作系统与安全管理.....5

2.1.4 应急响应与恢复.....5

2.1.5 数据安全与保护.....5

2.1.6 新技术应用安全.....5

2.2 构建中小企业安全网络.....6

第十五届“新华三杯”全国大学生数字技术大赛预赛考试大纲（安全赛道）

1 概述

1.1 文件说明

本文件是新华三技术有限公司在全国范围内举行的第十五届“新华三杯”全国大学生数字技术大赛（后简称“大赛”）-安全赛道预赛考试的大纲，用于指导参赛人员复习备考。

大赛预赛为理论笔试，全国统一开赛。

1.2 预赛考试说明

考试对象

安全赛道的所有参赛人员。

考试内容

考试内容	百分比	备注
安全基础知识	60%	以考试知识点中六大模块的内容为主。
构建中小企业安全网络	40%	以《构建中小企业安全网络 V1.0》教材中的内容为主。

考试时长及分数

考试时长	考试总分
90 分钟	1000 分

试题数量及类型

试题类型	试题数量
单选题 多选题	125

考试形式

使用考试系统，集中考试。

1.3 建议参加的培训

培训项目	培训课程	时长(天)
H3C 认证网络安全工程师（H3CNE-Security）培训	构建中小企业安全网络 V1.0	5

参考资料路径：

https://www.h3c.com/cn/BizPortal/TrainingPartner/TeachingMaterial/TeachingMaterialCertification.aspx

***安全基础知识建议根据考试知识点自行查阅资料复习备考。**

2 预赛考试知识点分布

2.1 安全基础知识

2.1.1 法律法规与政策合规

- **网络安全法：**了解《网络安全法》主要内容，包括：网络运行安全、关键信息基础设施安全、网络信息安全、监测预警与应急处置、明确网络数据收集、存储、传输、处理的合法合规等要求，了解责任主体义务、处罚条款（如运营者责任、个人信息保护要求）。
- **数据安全法：**了解《数据安全法》主要内容，包括：数据安全与发展，数据安全制度、数据安全保护义务、政务数据安全与开放、法律责任、数据分类分级保护制度(一般数据、重要数据、核心数据)、跨境传输规则等要求以及数据安全风险评估义务。了解《网络数据安全管理条例》主要内容，包括：网络数据安全管理、网络数据跨境安全管理、网络数据监督管理、供应链安全以及数据流转中的安全保护等要求。
- **个人信息保护法：**了解《个人信息保护法》主要内容，包括：个人信息处理规则、个人信息跨境提供的规则、个人在个人信息处理活动中的权利、个人信息处理者的义务以及敏感个人信息的特殊保护等要求。
- **密码法：**了解《密码法》主要内容，包括：核心密码、普通密码、商用密码、法律责任、密码安全的基本策略等要求以及商用密码在数据加密、数字签名中的强制应用场景（政务数据、金融数据）。
- **其他规范：**了解《通信网络安全防护管理办法》、《关键信息基础设施安全保护条例》、《工业和信息化领域数据安全管理办法》、等级保护制度、应急响应要求、安全管理职责等相关法规。

2.1.2 网络安全基础与安全防护

- 了解网络层的网络架构、传输方式、传输协议和控制措施；了解针对有线和无线的攻击方式和安全防护机制。熟悉常见的网络层攻击，包括：DoS 和 DDoS、窃听、假冒/伪装、重放攻击、篡改、针对 DNS 的工具(欺骗、投毒和动持)、ARP 攻击、DHCP 攻击等及相关防护手段。
- 了解 Web 应用安全架构，风险分析及常规防护思路。熟悉框架和组件漏洞、权限绕过、弱口令、注入、跨站、文件包含、非法上传、非法命令执行、任意文件读取和下载等常见安全问题。
- 掌握常见 Web 环境的安全配置方法和检测方法以及安全防护手段。

2.1.3 操作系统与安全管理

- 了解操作系统(Windows、Linux 等)的常规安全防护机制。熟悉系统日志、应用程序日志等溯源攻击途径。掌握系统账号、权限、文件系统、文件共享、网络参数、端口和服务、日志审计、漏洞补丁等项目的安全检测与安全加固方法。
- 掌握系统加密、系统防火墙、安全策略、杀毒软件的安装和配置方法。安全运维规范，如变更管理、资产清单、安全域划分。

2.1.4 应急响应与恢复

- 熟悉应急响应与恢复的基本方法和流程。掌握应急响应和恢复的调查、取证、恢复等相关技术，包括：入侵取证分析、日志审计分析、反取证技术、文件删除恢复等。

2.1.5 数据安全与保护

- 了解安全多方计算、联邦学习、差分隐私等隐私计算技术；熟悉容灾备份、持续数据保护等技术和应用方法。
- 熟悉数据安全的全流程管控、追溯技术，以及动态行为分析和数据安全加密保护技术；熟悉数据安全特性，了解数据全生命周期安全威胁类型及安全防护技术，了解数据安全技术体系，包括：数据防泄漏、数据溯源和审计以及数据匿名化等，了解数据安全生命周期防护、包含采集存储、传输、处理以及销毁等阶段的技术方法。

2.1.6 新技术应用安全

- 了解云计算的概念及特征。熟悉云计算常见的安全问题，包括：虚拟机安全、容器安全、应用程序安全、数据安全、网络隔离、微隔离、接口安全等。
- 了解大数据的概念及特征。熟悉利用大数据分析技术提升网络系统安全隐患发现和防护能力。
- 了解物联网的概念及相关基础技术，了解智能摄像头、ID/IC 卡、智能卡、智能家居、可穿戴智能设备等常见安全威胁。
- 了解 5G 技术的概念及特征。熟悉 5G 网络架构和关键技术，了解 5G 关键技术存在的安全风险以及安全框架等。
- 了解 AI 大模型数据安全相关基础技术，例如训练数据投诉攻击防御、模型输出隐私保护等。
- 了解人工智能的典型应用及安全风险，了解其可能导致的数据隐私泄露、深度伪造、智能钓鱼等安全风险以及安全措施。

2.2 构建中小企业安全网络

- **网络安全概述：**TCP/IP 协议基础、TCP/IP 协议安全、网络安全威胁方式。
- **防火墙基础技术：**防火墙的发展背景及技术演进、防火墙应具备的基本功能、防火墙性能衡量指标、防火墙的组网方式。
- **防火墙用户管理：**AAA 技术原理、防火墙用户分类、防火墙用户管理及应用。
- **防火墙安全策略：**包过滤技术、安全域、防火墙转发原理、防火墙安全策略。
- **网络地址转换技术：**NAT 概述、动态 NAT、内部服务器、静态 NAT、NAT ALG 功能。
- **VPN 原理及配置：**VPN 概述、GRE VPN、L2TP VPN、IPSec VPN、SSL VPN。
- **DPI 技术：**DPI 技术背景、DPI 技术原理、DPI 技术配置。
- **应用控制技术：**应用控制技术概述、应用过滤、带宽管理、日志报表、用户和认证。