目录

第十五届“新华三杯”全国大学生数字技术大赛复赛考试大纲（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”）-安全赛道复赛考试的大纲，用于指导参赛人员复习备考。

大赛复赛为理论笔试，全国统一开赛。

1.2 复赛考试说明

考试对象

安全赛道所有进入复赛的参赛人员。

考试内容

考试内容	百分比	备注
安全攻防技能知识	50%	以考试知识点中六大模块的内容为主。
构建安全网络架构	25%	以《构建安全网络架构》 教材中的内容为主。
部署内容安全系统	25%	以《部署内容安全系统》 教材中的内容为主。

考试时长及分数

考试时长	考试总分
120 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	200

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 认证安全技术高级工程师（H3CSE- Security）培训	《构建安全网络架构》	5
H3C 认证安全技术高级工程师（H3CSE- Security）培训	《部署内容安全系统》	3

参考资料路径：

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

***安全攻防技能知识建议根据考试知识点自行查阅资料复习备考。**

2 复赛考试知识点分布

2.1 安全攻防技能知识

2.1.1 Web 模块知识

- **Web 基础核心：**掌握 HTTP/HTTPS 协议原理、请求方法（GET/POST 等）、状态码含义、Cookie 与 Session 机制，熟练掌握 Web 基础理论。
- **常见 Web 漏洞原理：**掌握 SQL 注入、XSS 跨站脚本、CSRF 跨站请求伪造、文件上传/包含漏洞、命令执行、路径遍历、常见的 php 特性等漏洞的理论知识，明确各漏洞的形成原因、触发条件及核心利用逻辑。
- **Web 安全防护机制：**掌握 WAF（Web 应用防火墙）工作原理、常见绕过思路，以及输入验证、输出编码、权限控制等基础防护手段的理论知识。
- **框架与中间件安全：**掌握常见 Web 框架（如 PHP 的 ThinkPHP、Python 的 Django）、Web 服务器（Apache、Nginx）的默认配置、常见漏洞及特性等理论知识，明确框架层面的安全隐患)。

2.1.2 MISC 模块知识

- **隐写术基础：**掌握图像隐写（PNG/JPG/BMP 格式隐写原理）、音频隐写、视频隐写、文本隐写的核心理论知识，熟练掌握各类隐写方式的核心逻辑与识别方法。
- **编码与加密基础：**掌握 Base 系列编码、URL 编码、ASCII/Unicode 编码、摩尔斯电码等常见编码方式的理论知识，以及凯撒密码、栅栏密码等简单古典加密的原理与解密逻辑。
- **数据恢复与流量分析：**掌握文件碎片恢复、误删文件恢复的基础理论知识，熟练掌握 Wireshark 等工具的使用逻辑，能基于理论知识分析 TCP/UDP 流量包中的隐藏信息、异常数据。
- **杂项工具与场景应用：**掌握压缩包加密（ZIP/RAR）的破解思路、图片/音频文件格式分析、日志文件解读等理论知识，熟悉 MISC 赛事中常见杂项场景的解题核心理论与逻辑。

2.1.3 CRYPTO（密码学）模块知识

- **古典密码学：**掌握置换密码、代换密码（凯撒、维吉尼亚、仿射密码等）的理论知识，熟练掌握各类古典密码的加密规则、解密方法，以及频率分析等破解技巧的核心理论。
- **现代密码学基础：**掌握对称加密（AES、DES）、非对称加密（RSA、ECC）的核心原理、密钥生成逻辑、加密解密流程等理论知识，明确对称与非对称加密的区别及适用场景的理论依据。

- **密码学常见攻击方式：**掌握 RSA 的共模攻击、低加密指数攻击、差分攻击、中间人攻击等常见密码学攻击方式的理论知识，明确各类攻击的适用场景、原理及防御思路。

2.1.4 PWN 模块知识

- **计算机底层基础：**掌握 CPU 架构（x86/x64）、寄存器功能、栈/堆/全局变量的内存布局等底层理论知识，理解进程、线程的基本概念，夯实漏洞利用的底层理论基础。
- **常见内存漏洞原理：**掌握栈溢出、堆溢出、格式化字符串漏洞、UAF（使用后释放）、Double Free（双重释放）等常见内存漏洞的理论知识，明确各漏洞的形成原因、内存破坏逻辑及利用思路。
- **漏洞利用技术：**掌握 ROP（返回导向编程）、ret2libc、ret2shellcode、栈迁移等漏洞利用技术的核心理论知识，熟练掌握函数调用栈的工作机制、返回地址覆盖的核心逻辑。
- **防护机制与绕过：**掌握 ASLR（地址空间布局随机化）、PIE（位置无关执行）、Stack Canary（栈保护）、NX（不可执行）等防护机制的理论知识，以及对应的绕过方法的核心理论。

2.1.5 Reverse 模块知识

- **逆向基础核心：**掌握汇编语言基础（x86/x64 汇编指令、寄存器操作、指令执行流程）、反编译原理等理论知识，熟练掌握逆向分析的基本思路，为解读二进制程序逻辑提供理论支撑。。
- **常见逆向工具与技巧：**掌握 IDA Pro、GDB、OllyDbg 等逆向工具的使用逻辑相关理论知识，熟练掌握反编译、动态调试、静态分析的核心技巧，能基于理论知识还原程序执行流程与核心功能。
- **软件保护与脱壳：**掌握 UPX、ASPack 等常见软件加壳技术的理论知识，熟练掌握脱壳的基本思路与方法，理解代码混淆、反调试、反跟踪等保护机制及绕过技巧的核心理论。

2.1.6 其他模块知识

- **移动开发基础：**掌握 Android/iOS 开发基础、APP 打包与签名机制、移动操作系统（Android/iOS）核心架构等理论知识，明确移动应用的运行原理与安全隐患的理论依据。
- **移动应用逆向与篡改：**掌握 Android APK 反编译（Apktool、Jadx）、iOS IPA 逆向的基本方法相关理论知识，熟悉 Smali 代码解读、Java 层/原生层逆向理论，理解 APP 篡改、重打包的核心逻辑。
- **移动应用常见漏洞：**掌握组件暴露、权限滥用、数据泄露、本地存储加密漏洞、API 接口漏洞等移动应用常见漏洞的理论知识，明确各漏洞的形成原因、触发条件及利用思路。
- **工控安全：**掌握工控系统（ICS）的核心架构、组成部件（PLC、SCADA、DCS、HMI）的

理论知识，理解工控系统与传统 IT 系统的区别，掌握工控网络的基本拓扑与通信模式，掌握工控系统常见漏洞（PLC 程序漏洞、SCADA 系统漏洞、协议漏洞）的理论知识，明确漏洞形成原因、触发条件，掌握工控系统安全防护的核心理论与防御思路。

- **IoT 安全：**掌握 IoT 领域常见通信协议（MQTT、CoAP、LoRa、BLE）的理论知识、通信流程，熟悉各协议的安全缺陷、加密机制及常见攻击方式的核心原理，熟悉 IoT 设备常见漏洞（固件漏洞、权限漏洞、硬件漏洞）的理论依据与利用思路。

2.2 构建安全网络架构

- **构建安全网络架构概述：**安全部署综述、虚拟化技术、高可靠 HA、高级 NAT 技术等概述。
- **虚拟化技术：**SCF 技术的产生背景，技术优势，技术实现，技术原理，MAD 检测原理，典型配置；SOP 技术的产生背景，context 优点，context 资源分配配置，context 典型场景配置。
- **双机热备（RBM）技术：**RBM 技术背景、工作原理、基本配置、典型组网。
- **负载均衡技术：**负载均衡技术基本原理，四层服务器负载均衡原理及配置，Outbound 链路负载均衡原理及配置，Inbound 链路负载均衡原理及配置，七层服务器负载均衡原理及配置。
- **高可靠性：**链路聚合、接口组联动、链路质量监测之 NQA/BFD/TRACK、设备冗余备份部署方式、设备的可靠性之 bypass。
- **高级 NAT 技术：**NAT 技术背景、双向 NAT 技术、两次 NAT 技术、NAT hairpin 技术、IPv6 演进下的高级 NAT 技术、NAT 会话日志。
- **综合排错：**通用信息收集方法、故障排查常用工具、典型故障排查。

2.3 部署内容安全系统

- **部署内容安全系统概述：**部署内容安全系统概述、内容安全风险、内容安全需求。
- **运维审计系统：**运维审计系统的基本工作原理、部署方式、用户验证方式、设备运维、会话审计、自动运维。
- **Web 应用防火墙：**Web 安全概述、WAF 产品介绍、WAF 设备管理、WAF 功能特性及部署介绍、WAF 典型配置举例。
- **异常流量清洗系统：**什么是 DDOS 攻击、常见的 DDOS 攻击及攻击原理简介、AFC 与 AFD 系统概述、AFC 与 AFD 部署方案、AFC 与 AFD 防御原理、AFC 与 AFD 配置。
- **数据库审计系统：**数据库审计概述、数据库审计原理、数据库审计系统部署。
- **漏洞扫描系统：**漏洞扫描系统概述、漏洞扫描系统的技术实现、漏洞扫描系统的原理介绍、漏洞扫描系统的功能配置、漏洞扫描系统的设备维护。

- **安全隔离与信息交换系统：**网络隔离现状、安全隔离与信息交换系统概述、网闸的系统结构、网闸的主要功能、网闸的功能配置、网闸的维护。