目录

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

为明确实操赛的能力考核范围，依据常见竞赛方向及当前网络安全实战能力要求，制定本技能大纲。本大纲侧重参赛人员在靶场环境中的实际分析、工具使用、漏洞验证、脚本编写、综合利用和结果提交能力，不以单纯理论记忆作为主要评价依据。

1.2 决赛考试说明

考试对象：

安全赛道决赛的所有参赛人员。

考试时长及分数

考试时长	考试总分
180 分钟	1000 分

试题数量及类型

试题类型	试题数量
实操题	10~15 题

考试系统

网络安全实战竞赛平台，线下集中答题。

2 决赛考试知识点分布

2.1 Web 安全模块实操技能

- 掌握使用浏览器开发者工具、Burp Suite、Postman、curl 等工具，对 HTTP/HTTPS 请求、GET/POST 参数、Cookie、Session、Header、JWT、接口返回等内容进行抓包、重放、修改和分析，定位 Web 应用中的异常交互点等技能。
- 掌握在靶场环境中识别并利用 SQL 注入、XSS、CSRF、SSRF、文件上传、文件包含、目录遍历、命令执行、代码执行、反序列化、模板注入、XXE 等常见漏洞，完成漏洞验证、权限提升和 Flag 获取。
- 可分析登录认证、验证码、Token、Session、JWT、权限控制、水平越权、垂直越权等机制，发现身份认证缺陷，并通过参数篡改、接口重放、权限绕过等方式完成实操利用。
- 掌握针对 ThinkPHP、Laravel、Spring、Django、Flask、Node.js、Apache、Nginx、Tomcat、Redis、Fastjson 等框架及组件进行指纹识别、漏洞验证、配置缺陷利用和敏感信息获取。
- 根据题目环境完成从信息收集、漏洞发现、Payload 构造、漏洞利用、WebShell 获取、内网探测、敏感文件读取到最终 Flag 获取的完整流程。

2.2 MISC 模块实操技能

- 掌握对图片、音频、视频、压缩包、PDF、Office 文档等文件进行隐写检测和数据提取技能，并使用 binwalk、foremost、zsteg、steghide、Audacity、010 Editor 等工具获取隐藏信息。
- 熟练使用 Wireshark、tshark 等工具分析 TCP、UDP、HTTP、DNS、FTP、ICMP、USB、蓝牙等流量数据，提取账号密码、文件内容、通信特征和隐藏 Flag。
- 能够对磁盘镜像、内存镜像、日志文件、浏览器缓存、数据库文件等进行取证分析，恢复删除文件、提取敏感信息、分析攻击痕迹并定位 Flag。
- 掌握处理 ZIP、RAR、7z 等压缩包伪加密、爆破、CRC 修复、分卷恢复、文件头修复、文件尾补全等实操场景技能。
- 能够综合使用 CyberChef、010 Editor、Volatility、binwalk、strings、exiftool、hashcat、John the Ripper 等工具，对复杂附件进行多阶段分析和解题。

2.3 CRYPTO（密码学）模块实操技能

- 识别并处理 Base、Hex、URL、Unicode、ASCII、栅栏、凯撒、维吉尼亚、培根、仿射等常见编码与古典密码，使用工具或脚本完成解码和密文恢复。
- 针对 AES、DES、RC4、SM4 等对称加密题目，需掌握分析密钥、IV、模式、填充方式和

加解密流程，完成弱密钥、模式误用、已知明文等场景下的实操破解技能。

- 针对 RSA、ECC 等非对称密码题目，分析公钥参数、模数、指数、曲线参数等信息，完成共模攻击、低指数攻击、广播攻击、因数分解、私钥恢复等实操利用。
- 分析 MD5、SHA、HMAC、JWT 签名、长度扩展攻击、哈希碰撞、弱随机数等场景，构造有效伪造数据或绕过完整性校验。
- 能够使用 Python、SageMath、CyberChef、openssl 等工具完成加解密脚本编写、参数爆破、数学运算和 Flag 自动化恢复。

2.4 PWN 模块实操技能

- 能够使用 file、checksec、strings、ltrace、strace、IDA、Ghidra、pwndbg、gdb 等工具分析 ELF 程序结构、保护机制、函数逻辑和输入输出流程。
- 在靶场环境中识别并利用栈溢出、格式化字符串、整数溢出、数组越界、Off-by-one 等漏洞，完成控制程序执行流、泄露地址、构造 ROP 链和获取 Shell。
- 掌握分析 malloc/free 流程，识别并利用 UAF、Double Free、Heap Overflow、Tcache Poisoning、Fastbin Attack、Unsorted Bin Attack 等堆漏洞，完成任意地址读写或劫持控制流。
- 针对 NX、Canary、PIE、ASLR、RELRO 等防护机制，完成地址泄露、Canary 泄露、libc 基址计算、ret2libc、ret2csu、SROP 等利用操作。
- 能够使用 Python、pwntools 编写自动化利用脚本，完成本地调试、远程连接、Payload 发送、结果解析和 Flag 获取。

2.5 Reverse 模块知识

- 能够使用 IDA、Ghidra、Binary Ninja、JEB、dnSpy、jadx 等工具，对 Windows、Linux、Android 程序进行反汇编、反编译、字符串分析、函数定位和关键逻辑还原。
- 能够使用 gdb、x64dbg、OllyDbg、Frida、adb、lldb 等工具，对程序运行流程进行断点调试、寄存器分析、内存查看、函数 Hook 和关键数据提取。
- 能够分析程序中的加密、校验、混淆、编码转换、虚拟机保护等逻辑，使用 Python、C、C++ 还原核心算法，并生成正确输入或解密 Flag。
- 能够识别常见加壳、混淆、反调试、反虚拟机、字符串加密等保护方式，并通过脱壳、Patch、Hook、内存 Dump 等方式恢复程序真实逻辑。
- 能够对 APK、小程序、Unity 程序等进行反编译、资源提取、接口分析、签名校验绕过和动

态调试，获取隐藏逻辑、密钥或 Flag。

2.6 其他模块知识

- 能够识别并分析 Modbus、S7、OPC UA、DNP3、BACnet、MQTT 等常见工业控制协议，使用 Wireshark、Scapy、工控协议解析工具提取寄存器数据、设备信息和异常指令。
- 能够在靶场环境中识别 PLC、HMI、SCADA、工程师站、数据库服务器、网关设备等关键资产，分析设备开放端口、服务类型、通信关系和业务流程。
- 能够根据题目给出的生产流程、传感器数据、控制指令、报警日志等信息，判断异常控制逻辑，定位错误配置、越权操作或恶意指令。
- 能够针对 HMI 管理页面、SCADA Web 后台、设备管理接口等场景，完成弱口令登录、权限绕过、接口调用、配置文件读取、日志分析和敏感数据获取。
- 能够在模拟工业网络中完成信息收集、协议交互、配置分析、指令重放、数据篡改、异常状态恢复和 Flag 获取，具备工控场景下的综合实操能力。