**2025年河北省职业院校学生技能大赛**

**“数据安全技术与应用”赛项样题**

**样题一：**

1. **模块一数据安全风险评估与处置**
2. **项目描述**

A集团的信息系统遭受网络安全攻击，该系统的多台服务器被黑客入侵，系统的关键数据遭到破坏。您的团队需要帮助该公司追踪此事件的网络攻击来源，分析黑客的攻击行为，并制定相应的安全加固措施，避免服务器遭受进一步的攻击。

任务分为以下几个部分：

●网络安全事件响应

●数字调查取证

1. **任务书（竞赛时间 180 分钟，共 100 分）**

**任务一：网络安全应急响应**

本任务提供的素材文件类型为：Server服务器虚拟机，相关日志文件，相关流量文件。

A集团的WebServer服务器被黑客入侵，失陷的服务器资产涉及Linux和Windows操作系统，同时服务器的应用系统被上传恶意软件，重要数据库文件被加密，作为一个信息安全工程师需要针对企业发生的网络安全事件启动应急响应，根据企业提供的环境信息进行数据取证调查，调查服务器被黑客攻击的相关信息，发现被黑客放置在服务器上的恶意软件或后门程序，分析黑客如何入侵进服务器。

按答题卡的要求完成该部分的工作任务。

题目数量不少于15小题。

题目样例：

1. 攻击者的IP地址是？提交IP地址例如：1.1.1.1
2. 攻击者下载一个恶意的文件，提交该恶意的文件名称为？例如：abc.exe
3. 攻击者加密了数据库的内容，请分析攻击者的加密方法，解密被加密的文件，提交融清宁用户的卡号。例如：1220139936777。
4. ...

**任务二：数字调查取证**

本任务提供的素材文件类型：network.pcapng

A集团工作人员截获了含有攻击行为的网络数据包，请根据A集团提供的网络数据包文件，分析溯源攻击者的恶意行为。

题目数量不少于15小题。

题目样例：

1. 需要进行用户名密码验证的目录相对路径是？例如：/Resource/
2. 攻击者登陆成功所使用的账号密码是？例如：admin/Aa123456
3. 上传成功的后门文件名称为？例如：a.php
4. ......
5. **模块二创新创业演示与展示**

参赛选手需自拟命题选择具有创新性和现实意义的项目主题，并确保内容符合竞赛规范。

选手应提前准备项目展示材料，包括演示文稿和相关原型设计，演示文稿中不得包含学校或个人相关的信息及暗示，以保障评审的公平公正性。

选手应能够清晰有条理地展示项目，回应评委提出的问题，并展示出团队的专业性和项目的整体价值。

每只参赛队伍有10分钟进行项目宣讲，5分钟现场答辩，共计15分钟的展示时间。

**样题二：**

1. **模块一数据安全风险评估与处置**
2. **项目描述**

A集团的信息系统遭受网络安全攻击，该系统的多台服务器被黑客入侵，系统的关键数据遭到破坏。您的团队需要帮助该公司追踪此事件的网络攻击来源，分析黑客的攻击行为，并制定相应的安全加固措施，避免服务器遭受进一步的攻击。

任务分为以下几个部分：

●网络安全事件响应

●数字调查取证

1. **任务书（竞赛时间 180 分钟，共 100 分）**

**任务一：网络安全应急响应**

本任务提供的素材文件类型为：Server服务器虚拟机，相关日志文件，相关流量文件。

A集团的WebServer服务器被黑客入侵，失陷的服务器资产涉及Linux和Windows操作系统，同时服务器的应用系统被上传恶意软件，重要数据库文件被加密，作为一个信息安全工程师需要针对企业发生的网络安全事件启动应急响应，根据企业提供的环境信息进行数据取证调查，调查服务器被黑客攻击的相关信息，发现被黑客放置在服务器上的恶意软件或后门程序，分析黑客如何入侵进服务器。

按答题卡的要求完成该部分的工作任务。

题目数量不少于15小题。

题目样例：

1. 攻击者使用的MAC地址是？提交MAC地址，例如：00:1A:2B:3C:4D:5E
2. 攻击者利用了哪个漏洞进入系统？提交漏洞的CVE编号，例如：CVE-2023-1234
3. 攻击者在系统中创建的新用户名称是？例如：hacker
4. ...

**任务二：数字调查取证**

本任务提供的素材文件类型：network.pcapng

A集团工作人员截获了含有攻击行为的网络数据包，请根据A集团提供的网络数据包文件，分析溯源攻击者的恶意行为。

题目数量不少于15小题。

题目样例：

1. 攻击者下载的ZIP压缩文件名称是？例如：data.zip
2. 攻击者使用的SQL注入Payload是？例如：' OR '1'='1
3. 攻击者用于上传后门的完整URL是？例如：<http://example.com/upload.php>
4. ......
5. **模块二创新创业演示与展示**

参赛选手需自拟命题选择具有创新性和现实意义的项目主题，并确保内容符合竞赛规范。

选手应提前准备项目展示材料，包括演示文稿和相关原型设计，演示文稿中不得包含学校或个人相关的信息及暗示，以保障评审的公平公正性。

选手应能够清晰有条理地展示项目，回应评委提出的问题，并展示出团队的专业性和项目的整体价值。

每只参赛队伍有10分钟进行项目宣讲，5分钟现场答辩，共计15分钟的展示时间。

**样题三：**

1. **模块一数据安全风险评估与处置**
2. **项目描述**

A集团的信息系统遭受网络安全攻击，该系统的多台服务器被黑客入侵，系统的关键数据遭到破坏。您的团队需要帮助该公司追踪此事件的网络攻击来源，分析黑客的攻击行为，并制定相应的安全加固措施，避免服务器遭受进一步的攻击。

任务分为以下几个部分：

●网络安全事件响应

●数字调查取证

1. **任务书（竞赛时间 180 分钟，共 100 分）**

**任务一：网络安全应急响应**

本任务提供的素材文件类型为：Server服务器虚拟机，相关日志文件，相关流量文件。

A集团的WebServer服务器被黑客入侵，失陷的服务器资产涉及Linux和Windows操作系统，同时服务器的应用系统被上传恶意软件，重要数据库文件被加密，作为一个信息安全工程师需要针对企业发生的网络安全事件启动应急响应，根据企业提供的环境信息进行数据取证调查，调查服务器被黑客攻击的相关信息，发现被黑客放置在服务器上的恶意软件或后门程序，分析黑客如何入侵进服务器。

按答题卡的要求完成该部分的工作任务。

题目数量不少于15小题。

题目样例：

1. 攻击者上传的恶意脚本路径是？例如：/var/www/html/shell.php
2. 攻击者建立反向连接使用的端口号是？例如：4444
3. 攻击者创建的计划任务名称是？例如：malicious\_task
4. ...

**任务二：数字调查取证**

本任务提供的素材文件类型：network.pcapng

A集团工作人员截获了含有攻击行为的网络数据包，请根据A集团提供的网络数据包文件，分析溯源攻击者的恶意行为。

题目数量不少于15小题。

题目样例：

1. 攻击者用于发送钓鱼邮件的邮箱地址是？例如：attacker@evil.com
2. 攻击者使用了哪个工具嗅探网络流量？例如：tcpdump
3. 攻击者通过FTP认证使用的密码是？例如：P@ssw0rd!
4. ...
5. **模块二创新创业演示与展示**

参赛选手需自拟命题选择具有创新性和现实意义的项目主题，并确保内容符合竞赛规范。

选手应提前准备项目展示材料，包括演示文稿和相关原型设计，演示文稿中不得包含学校或个人相关的信息及暗示，以保障评审的公平公正性。

选手应能够清晰有条理地展示项目，回应评委提出的问题，并展示出团队的专业性和项目的整体价值。

每只参赛队伍有10分钟进行项目宣讲，5分钟现场答辩，共计15分钟的展示时间。

**样题四：**

1. **模块一数据安全风险评估与处置**
2. **项目描述**

A集团的信息系统遭受网络安全攻击，该系统的多台服务器被黑客入侵，系统的关键数据遭到破坏。您的团队需要帮助该公司追踪此事件的网络攻击来源，分析黑客的攻击行为，并制定相应的安全加固措施，避免服务器遭受进一步的攻击。

任务分为以下几个部分：

●网络安全事件响应

●数字调查取证

1. **任务书（竞赛时间 180 分钟，共 100 分）**

**任务一：网络安全应急响应**

本任务提供的素材文件类型为：Server服务器虚拟机，相关日志文件，相关流量文件。

A集团的WebServer服务器被黑客入侵，失陷的服务器资产涉及Linux和Windows操作系统，同时服务器的应用系统被上传恶意软件，重要数据库文件被加密，作为一个信息安全工程师需要针对企业发生的网络安全事件启动应急响应，根据企业提供的环境信息进行数据取证调查，调查服务器被黑客攻击的相关信息，发现被黑客放置在服务器上的恶意软件或后门程序，分析黑客如何入侵进服务器。

按答题卡的要求完成该部分的工作任务。

题目数量不少于15小题。

题目样例：

1. 攻击者修改了哪个配置文件以维持权限？例如：.bashrc
2. 发现的恶意文件的MD5哈希值是？例如：d41d8cd98f00b204e9800998ecf8427e
3. 攻击者执行了哪个命令来提升权限？例如：sudo exploit
4. ...

**任务二：数字调查取证**

本任务提供的素材文件类型：network.pcapng

A集团工作人员截获了含有攻击行为的网络数据包，请根据A集团提供的网络数据包文件，分析溯源攻击者的恶意行为。

题目数量不少于15小题。

题目样例：

1. 攻击者用于列出目录内容的命令是？例如：ls -la
2. 攻击者使用了哪个HTTP方法上传文件？例如：PUT
3. 攻击者设置的Cookie值是？例如：sessionid=abc123...
4. ...
5. **模块二创新创业演示与展示**

参赛选手需自拟命题选择具有创新性和现实意义的项目主题，并确保内容符合竞赛规范。

选手应提前准备项目展示材料，包括演示文稿和相关原型设计，演示文稿中不得包含学校或个人相关的信息及暗示，以保障评审的公平公正性。

选手应能够清晰有条理地展示项目，回应评委提出的问题，并展示出团队的专业性和项目的整体价值。

每只参赛队伍有10分钟进行项目宣讲，5分钟现场答辩，共计15分钟的展示时间。

**样题五：**

1. **模块一数据安全风险评估与处置**
2. **项目描述**

A集团的信息系统遭受网络安全攻击，该系统的多台服务器被黑客入侵，系统的关键数据遭到破坏。您的团队需要帮助该公司追踪此事件的网络攻击来源，分析黑客的攻击行为，并制定相应的安全加固措施，避免服务器遭受进一步的攻击。

任务分为以下几个部分：

●网络安全事件响应

●数字调查取证

1. **任务书（竞赛时间 180 分钟，共 100 分）**

**任务一：网络安全应急响应**

本任务提供的素材文件类型为：Server服务器虚拟机，相关日志文件，相关流量文件。

A集团的WebServer服务器被黑客入侵，失陷的服务器资产涉及Linux和Windows操作系统，同时服务器的应用系统被上传恶意软件，重要数据库文件被加密，作为一个信息安全工程师需要针对企业发生的网络安全事件启动应急响应，根据企业提供的环境信息进行数据取证调查，调查服务器被黑客攻击的相关信息，发现被黑客放置在服务器上的恶意软件或后门程序，分析黑客如何入侵进服务器。

按答题卡的要求完成该部分的工作任务。

题目数量不少于15小题。

题目样例：

1. 攻击者连接的指挥控制服务器IP地址是？例如：203.0.113.5
2. 与恶意进程相关的进程ID（PID）是？例如：1234
3. 攻击者利用了哪个服务获得初始访问权限？例如：SSH
4. ...

**任务二：数字调查取证**

本任务提供的素材文件类型：network.pcapng

A集团工作人员截获了含有攻击行为的网络数据包，请根据A集团提供的网络数据包文件，分析溯源攻击者的恶意行为。

题目数量不少于15小题。

题目样例：

1. 攻击者搭建的钓鱼网站URL是？例如：http://fakebank.com/login
2. 攻击者修改的注册表键值路径是？例如：HKEY\_LOCAL\_MACHINE\Software\Malware
3. 攻击者用于加密文件的加密算法是？例如：AES-256..
4. ...
5. **模块二创新创业演示与展示**

参赛选手需自拟命题选择具有创新性和现实意义的项目主题，并确保内容符合竞赛规范。

选手应提前准备项目展示材料，包括演示文稿和相关原型设计，演示文稿中不得包含学校或个人相关的信息及暗示，以保障评审的公平公正性。

选手应能够清晰有条理地展示项目，回应评委提出的问题，并展示出团队的专业性和项目的整体价值。

每只参赛队伍有10分钟进行项目宣讲，5分钟现场答辩，共计15分钟的展示时间。