**2026年河北省职业院校学生技能大赛**

**“数据安全技术与应用”赛项样题一**

**样题一：**

1. **模块一数据安全理论知识考核**
2. **赛项描述**

题目类型为单选题和多选题。

1. **题目样例**

1.参照《GB/T 20988-2007信息安全技术 信息系统灾难恢复规范》，灾难恢复能力分为( )级。

1. 4
2. 5
3. 6
4. 7

正确答案：C

2.数据分级原则主要有( )。

1. 合法合规原则
2. 分类多维原则
3. 静态定义原理
4. 就高从严原则

正确答案：ABD

1. **模块一数据安全风险评估与处置**
2. **赛项描述**

该赛项考察内容为网络安全事件响应和数字调查取证两个部分。

1. **任务书**

**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，相关日志文件，相关流量文件。

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企业溯源追踪此事件的网络攻击来源，分析黑客的攻击行为，调查服务器被黑客攻击的相关行为，避免服务器遭受进一步的攻击。

按答题卡的要求完成该部分的工作任务。

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. 攻击者上传Webshell文件，提交该Webshell文件的完整路径。例如：/app/shell.php。
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。

题目样例：

1. 攻击者对多少端口号进行密码爆破？例如：445
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. ......

**样题二：**

1. **模块一数据安全理论知识考核**
2. **赛项描述**

题目类型为单选题和多选题。

1. **题目样例**

1.以下属于哈希算法的是( )。

1. DES
2. MD5
3. SHA
4. SM3

正确答案：B

2.在评估数据安全风险时，针对数据脱敏，应当重点评估( )方面。

1. 数据脱敏规则、脱敏方法和脱敏数据的使用限制情况
2. 需要进行数据脱敏处理的应用场景
3. 静态数据脱敏技术能力建设情况
4. 动态数据脱敏技术能力建设情况

正确答案：ABCD

1. **模块一数据安全风险评估与处置**
2. **赛项描述**

该赛项考察内容为网络安全事件响应和数字调查取证两个部分。

1. **任务书**

**任务一：网络安全应急响应**

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

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企业溯源追踪此事件的网络攻击来源，分析黑客的攻击行为，调查服务器被黑客攻击的相关行为，避免服务器遭受进一步的攻击。

按答题卡的要求完成该部分的工作任务。

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. ......

**样题三：**

1. **模块一数据安全理论知识考核**
2. **项目描述**

题目类型为单选题和多选题。

1. **题目样例**

1．Linux下使用( )命令可以查看二进制文件中的字符串。

1. cat
2. more
3. string
4. tail

正确答案：C

2.在应急响应的检测和分析阶段，分析主要为了( )。

A.确定事件性质

B.将事件分级分类

C.找到攻击源头

D.确定事件原因

正确答案：ABD

1. **模块一数据安全风险评估与处置**
2. **项目描述**

该赛项考察内容为网络安全事件响应和数字调查取证两个部分。

1. **任务书**

**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，相关日志文件，相关流量文件。

A集团WebServer服务器遭受黑客入侵，涉及多台Linux主机。攻击者在服务器上植入恶意软件，对服务器进行持续监听。作为信息安全工程师，需立即启动网络安全应急响应，依据现有环境信息开展取证调查，追溯服务器被攻击过程，定位恶意软件或后门程序，并分析黑客入侵路径与攻击手段。

按答题卡的要求完成该部分的工作任务。

题目样例：

1. 攻击者利用Web应用漏洞获取了执行权限，提交其最初用于验证漏洞存在的关键请求参数名称。例如：ifconfig
2. 攻击者通过漏洞写入了一个Webshell，提交该Webshell在服务器上的绝对路径。例如：/var/www/html/upload/shell.php
3. 攻击者通过Webshell执行了系统命令以获取服务器基本信息，提交其查看系统内核版本所使用的命令。例如：uname -a
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。

题目样例：

1. 攻击者已控制一台内网机器，其首先扫描了内网网段，提交其扫描的/24网段地址。例如：192.168.10.0
2. 攻击者发现了一台开启SMB服务的机器，提交该目标主机的IP地址。例如：192.168.10.25
3. 攻击者利用永恒之蓝（MS17-010）漏洞进行攻击，提交其使用的Metasploit模块名称。例如：exploit/windows/smb/ms17\_010\_eternalblue
4. 攻击者横向移动成功后，在新机器上创建了一个计划任务作为后门，提交该计划任务的名称。例如：WindowsUpdateTask

**样题四：**

1. **模块一数据安全理论知识考核**
2. **项目描述**

题目类型为单选题和多选题。

1. **题目样例**

1.在Linux系统中，（ ）命令常用于查看实时日志文件。

A.echo logfile.log

B. head logfile.log

C. cat logfile.log

D. tail -f logfile.log

正确答案：D

2**.**在应急响应的准备阶段，需要完成的事项有（ ）。

1. 风险评估
2. 业务影响分析
3. 系统恢复能力等级设定
4. 恢复目标确定

正确答案：ABCD

1. **模块一数据安全风险评估与处置**
2. **项目描述**

该赛项考察内容为网络安全事件响应和数字调查取证两个部分。

1. **任务书**

**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，相关日志文件，相关流量文件。

A集团WebServer服务器遭受黑客入侵，涉及多台Linux主机。攻击者在服务器上植入恶意软件，对服务器进行持续监听。作为信息安全工程师，需立即启动网络安全应急响应，依据现有环境信息开展取证调查，追溯服务器被攻击过程，定位恶意软件或后门程序，并分析黑客入侵路径与攻击手段。

按答题卡的要求完成该部分的工作任务。

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. ...

**样题五：**

1. **模块一数据安全理论知识考核**
2. **项目描述**

题目类型为单选题和多选题。

1. **题目样例**

1**.**关于数据模型，其内容不包含下面哪项（ ）。

1. 数据实体
2. 实体间关系
3. 实体属性
4. 实体的访问控制权限

正确答案：D

2.参照《网络安全标准实践指南—网络数据分类分级指引》，常见的数据分类维度包含( )。

A.公民个人维度

B.公共管理维度

C.组织经营维度

D.行业领域维度

正确答案：ABCD

1. **模块一数据安全风险评估与处置**
2. **项目描述**

该赛项考察内容为网络安全事件响应和数字调查取证两个部分。

1. **任务书**

**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，相关日志文件，相关流量文件。

A集团WebServer服务器遭受黑客入侵，涉及多台Linux主机。攻击者在服务器上植入恶意软件，对服务器进行持续监听。作为信息安全工程师，需立即启动网络安全应急响应，依据现有环境信息开展取证调查，追溯服务器被攻击过程，定位恶意软件或后门程序，并分析黑客入侵路径与攻击手段。

按答题卡的要求完成该部分的工作任务。

题目样例：

1. 攻击者在Linux服务器上添加了一个SSH公钥以维持访问，提交该后门公钥文件（authorized\_keys）中的邮箱标识部分。例如：hacker@backdoor
2. 攻击者修改了系统定时任务（crontab）以定期回连，提交其添加的定时任务执行周期（前5个字段）。例如：\*/5 \* \* \* \*
3. 攻击者创建了一个隐藏的恶意系统服务，提交该服务的名称。例如：systemd-networkd-helper
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。

题目样例：

1. 攻击者入侵系统后首先查看了当前的登录会话，提交其使用的命令。例如：who
2. 攻击者为隐藏行踪，清除了当前用户的所有命令历史记录，提交其执行的命令。例如：history -c
3. 攻击者删除（或清空）了一个关键的应用日志文件以掩盖攻击行为，提交该日志文件的完整路径。例如：/opt/app/logs/access.log
4. ......