

信息安全工程师

历年真题汇总

本资料汇总2023、2024、2025三个下半年信息安全工程师（软考中级）考试真题，涵盖综合知识与应用技术两科，含答案解析与难度说明，供备考练习参考。

目 录

2023年下半年 • 综合知识真题

2023年下半年 • 应用技术案例

2024年下半年 • 综合知识真题

2024年下半年 • 应用技术案例

2025年下半年 • 综合知识真题

2025年下半年 • 应用技术案例

附录 • 考试说明与备考提示

合计：综合知识 171 题 + 应用技术案例 17 个

2023年下半年（11月） · 综合知识真题（共71题）

1. 《中华人民共和国网络安全法》第五十八条明确规定，因维护国家和社会公共秩序、处置重大突发社会安全事件的需要，经决定或者批准，可以在特定区域临时限制网络通信。

- A. 国务院
- B. 国家网信部门
- C. 省级以上人民政府
- D. 网络服务商

答案：A 难度：易

解析：

法条规定全网/大范围临时通信限制权限仅归国务院。

2. 2023年ISO发布ISO/IEC 10118-3正式纳入我国SM3哈希算法标准，SM3哈希输出长度为

- A. 8字节
- B. 16字节
- C. 32字节
- D. 64字节

答案：C 难度：中

解析：

SM3输出256比特=32字节；MD5为128bit=16字节。

3. BS7799/ISO27001信息安全管理体系以下描述错误的是

- A. 强化全员安全意识、规范安全行为
- B. 持续监控资产安全风险状态
- C. 推动管理层落实安全体系长效运行
- D. 通过认证后即可永久满足合规要求

答案：D 难度：中

解析：

ISO27001证书三年换证、每年监督审核，认证仅代表当期合规，无法永久有效。

4. 网络攻击分为主动、被动两类，下列属于被动攻击的是

- A. 拒绝服务攻击
- B. 重放攻击
- C. 身份假冒
- D. 流量分析

答案：D 难度：易

解析：

流量分析仅监听流量特征，不篡改、中断数据；其余均为主动干预通信。

5. 下列不属于对称加密算法的是

- A. IDEA
- B. DES
- C. RC4
- D. RSA

答案：D 难度：易

解析：

RSA是非对称公钥算法，IDEA、DES、RC4均为对称密码。

6. WAPI无线局域网国密标准采用的密钥协商算法是

- A. DH
- B. ECDSA
- C. ECDH
- D. CPK

答案：C 难度：中

解析：

ECDH椭圆曲线密钥协商；ECDSA仅用于数字签名。

7. 政务、网银场景通用高可靠身份认证技术是

- A. 数据库口令认证
- B. 摘要认证
- C. PKI数字证书认证
- D. 单一口令认证

答案：C 难度：易

解析：

PKI依托CA证书实现双向可信身份鉴别，安全性远高于单纯口令。

8. 持续消耗服务器CPU、连接队列等资源导致合法用户无法访问的攻击是

- A. 重放攻击
- B. DoS拒绝服务
- C. 反射攻击
- D. 服务劫持

答案：B 难度：易

解析：

DoS/DDoS核心目标耗尽系统资源，阻断正常业务访问。

9. 浏览器划分可信/不可信站点安全区域主要防护目标是

- A. 隔离网页恶意脚本执行权限
- B. 服务器证书加密传输
- C. IPSec内网隧道防护
- D. 全站SSL加密

答案：A 难度：易

解析：

安全区域管控JS、ActiveX等恶意脚本运行权限。

10. 关于网络攻击分类描述错误的是

- A. 服务攻击针对应用层业务程序
- B. 木马、陷阱属于渗透类威胁
- C. 非服务攻击针对底层网络协议
- D. 在线业务风险评估可执行高破坏性测试

答案：D 难度：中

解析：

业务渗透遵循最小影响原则，禁止中断业务的破坏性测试。

11. 无对外互联网访问的独立军用涉密系统等保定级最低为

- A. 二级
- B. 三级
- C. 四级
- D. 无级

答案：C 难度：中

解析：

四级结构化保护级适配军工、核心涉密关键信息基础设施。

12. 电子邮件传播恶意代码最主要载体是

- A. 邮件附件
- B. 邮件主题
- C. 纯文本正文
- D. 邮件头部

答案：A 难度：易

解析：

.exe、压缩包、宏文档等附件是病毒、木马主要传播载体。

13. Windows系统内置文件透明加密组件是

- A. TCFS
- B. CFS
- C. NTFS
- D. EFS

答案：D 难度：易

解析：

EFS依托NTFS分区实现文件透明加密保护。

14. 数字水印相关描述错误的是

- A. 隐形水印可追溯文件泄露源头
- B. 水印嵌入容量与鲁棒性相互制约
- C. 盲水印验证必须提供原始载体文件
- D. 视频水印需满足实时解码性能要求

答案：C 难度：中

解析：

盲水印无需原始载体即可从载体提取水印信息。

15. 大量主机植入bot程序由攻击者统一远程操控的网络集群称为

- A. 木马程序
- B. 僵尸网络Botnet
- C. ARP欺骗
- D. 网络钓鱼

答案：B 难度：易

解析：

僵尸网络用于批量发起DDoS、数据窃取、挖矿攻击。

16. 计算机取证操作描述错误的是

- A. 取证前后做哈希校验固定证据完整性
- B. 取证介质设置只读禁止写入数据
- C. 取证前对原磁盘制作镜像副本
- D. 取证完成可直接删除原始证据介质

答案：D 难度：中

解析：

原始证据介质必须长期封存，不得销毁、删除。

17. 《密码法》法定三类密码不包含

- A. 核心密码
- B. 普通密码
- C. 商用密码
- D. 国际密码

答案：D 难度：易

解析：

法定分类：核心密码、普通密码、商用密码。

18. BLP机密模型*特性（星规则）描述正确的是

- A. 主体只能向上写
- B. 主体只能向下写
- C. 主体只能向下读
- D. 主体只能向上读

答案：A 难度：难

解析：

星规则：高安全级主体不能向低密文件写入，仅向上写；简单安全规则只能向下读。

19. Biba完整性模型核心规则是

- A. 不下写、不上读
- B. 不上写、不下读
- C. 仅向上读写
- D. 无读写限制

答案：A 难度：难

解析：

防止低完整性数据写入污染高完整性业务数据。

20. 等保2.0云安全“一个安全管理中心”不包含

- A. 安全审计
- B. 集中管控
- C. 可信验证
- D. 防火墙策略下发

答案：D 难度：中

解析：

安全管理中心三组件：审计、集中管控、可信验证；防火墙属于边界三重防护。

21. 依据GB/T 2887机房规范，第二类辅助房间是

- A. 监控室
- B. 资料储藏室
- C. 主机房
- D. 终端室

答案：B 难度：难

解析：

一类辅助监控，二类资料储藏，三类备件储藏。

22. 身份认证三要素（所知/所有/本身）不包含

- A. 指纹（本身）
- B. UKey（所有）
- C. 内网IP
- D. 登录口令（所知）

答案：C 难度：易

解析：

IP可伪造、多人共用，无法作为唯一身份凭证。

23. Kerberos体系KDC（密钥分发中心）由哪两部分组成

- A. AS认证服务器、TGS票据服务器
- B. 客户端、应用服务
- C. 证书库、RA注册机构
- D. 日志审计服务器

答案：A 难度：中

解析：

KDC由AS(认证服务器)和TGS(票据授予服务器)组成。

24. PKI体系中仅审核用户注册资料、不签发证书的组件

- A. CA
- B. RA
- C. CRL服务器
- D. 终端实体

答案：B 难度：易

解析：

CA负责签发、吊销证书，RA仅收集核验用户信息。

25. 自主访问控制中基于列（客体）的实现方式是

- A. ACL访问控制表
- B. 能力表
- C. 口令列表
- D. 用户组表

答案：A 难度：中

解析：

ACL绑定客体（列），能力表绑定主体（行）。

26. 登录连续多次密码错误自动锁定账户属于

- A. 基于角色访问控制
- B. 基于异常事件控制
- C. 基于时间控制
- D. 基于地址控制

答案：B 难度：易

解析：

多次登录失败属于安全异常事件触发防护策略。

27. 防火墙白名单策略含义是

- A. 匹配规则放行，其余全部拒绝
- B. 匹配规则拒绝，其余全部放行
- C. 所有流量默认放行
- D. 所有流量默认阻断

答案：A 难度：易

解析：

白名单仅允许列表流量；黑名单仅拦截匹配流量，默认放行。

28. PAT端口复用属于哪一类NAT

- A. 静态NAT
- B. 动态地址池
- C. 端口NAT
- D. 双向NAT

答案：C 难度：易

解析：

PAT(Port Address Translation)属于端口NAT（NAPT）。

29. IDS部署在防火墙内侧主要优势

- A. 扩大全网监控范围
- B. 过滤外网噪声降低误报
- C. 提升抓包速度
- D. 直接阻断外网攻击

答案：B 难度：中

解析：

防火墙过滤海量扫描垃圾流量，减少IDS无效告警。

30. IPSec协议中仅提供完整性、无加密功能的是

- A. ESP
- B. AH
- C. IKE
- D. SSL

答案：B 难度：中

解析：

AH仅提供完整性、数据源认证；ESP支持加密+完整性双重能力。

31. Snort入侵检测属于哪一类误用检测

- A. 基于规则字符串匹配
- B. 概率模型
- C. 状态机
- D. 键盘监控

答案：A 难度：易

解析：

Snort依靠自定义规则匹配攻击载荷特征。

32. 下列不属于主机入侵检测工具的是

- A. Tripwire
- B. SWATCH
- C. WAF网页防火墙
- D. 系统审计工具

答案：C 难度：易

解析：

WAF是Web边界防护设备，不属于主机检测。

33. Snort规则中msg（报警信息）属于

- A. 规则头
- B. 规则选项
- C. 协议字段
- D. 地址段

答案：B 难度：中

解析：

规则头含协议、源/目的IP端口；msg、content、sid属于规则选项。

34. 网闸核心隔离原理是

- A. 两套系统物理断开、单向数据摆渡
- B. 双网卡路由转发
- C. 逻辑VLAN隔离
- D. VPN加密隔离

答案：A 难度：易

解析：

网闸通过物理断开+摆渡交换实现隔离，与防火墙逻辑隔离不同。

35. 《GB 17859》一级自主保护级不强制审计的操作是

- A. 删除操作
- B. 登录行为
- C. 权限变更
- D. 管理员操作

答案：A 难度：中

解析：

一级审计要求最低，无需记录客体删除操作。

36. Windows系统中仅管理员可访问日志类型

- A. 系统日志
- B. 应用日志
- C. 安全日志
- D. 性能日志

答案：C 难度：易

解析：

安全日志默认仅管理员可访问。

37. 以下操作不能保护审计日志安全的是

- A. 分权管控审计员
- B. 日志加密存储
- C. 日志强制访问控制
- D. 日志压缩备份

答案：D 难度：易

解析：

压缩仅节省存储空间，无安全防护能力。

38. 入侵检测系统IDS无法直接发现

- A. 蠕虫攻击行为
- B. 漏洞本身
- C. 暴力登录
- D. 异常外联

答案：B 难度：中

解析：

IDS检测漏洞利用行为；漏洞扫描工具才能发现系统漏洞本身。

39. 冲击波Blaster蠕虫利用的系统漏洞为

- A. RPC DCOM漏洞
- B. SMB漏洞
- C. SQL漏洞
- D. Sendmail漏洞

答案：A 难度：中

解析：

Blaster利用RPC DCOM；WannaCry利用SMB；Slammer利用SQL漏洞。

40. 属于管理类非技术性安全漏洞的是

- A. 缓冲区溢出
- B. 安全策略不完善
- C. 输入过滤缺失
- D. 配置错误

答案：B 难度：易

解析：

制度、策略缺陷属于非技术漏洞；代码/配置错误为技术漏洞。

41. Wireshark工具核心功能是

- A. 源代码审计
- B. 网络抓包流量分析
- C. 漏洞扫描
- D. 密码爆破

答案：B 难度：易

解析：

Wireshark核心为抓包与协议分析。

42. 具备主动全网扫描、自主传播能力的恶意代码

- A. 逻辑炸弹
- B. 木马
- C. 网络蠕虫
- D. 普通病毒

答案：C 难度：易

解析：

蠕虫无需人为触发，主动扫描主机漏洞扩散。

43. 文件型病毒无法感染的文件类型

- A. EXE
- B. COM
- C. HTML网页
- D. SYS驱动

答案：C 难度：易

解析：

文件病毒感染可执行程序，HTML为纯脚本文本。

44. Blaster蠕虫采用哪种IP扫描策略

- A. 随机扫描
- B. 顺序扫描
- C. 选择性扫描
- D. 本地网段扫描

答案：B 难度：中

解析：

Blaster采用顺序扫描。

45. 攻击者批量控制肉鸡集群发起攻击的网络是

- A. 僵尸网络
- B. ARP欺骗
- C. 钓鱼
- D. 中间人

答案：A 难度：易

解析：

僵尸网络由大量被控主机组成，用于批量攻击。

46. SYN洪水攻击利用TCP握手缺陷原理

- A. 发送海量SYN耗尽半连接队列
- B. 伪造ACK报文
- C. 分片偏移异常
- D. ICMP重定向

答案：A 难度：中

解析：

SYN Flood发送大量SYN占用半连接队列，耗尽资源。

47. 姓名“王*”、年龄“20-30”脱敏方式属于

- A. 泛化
- B. 抑制
- C. 扰动
- D. 置换

答案：A 难度：中

解析：

泛化将精确值替换为模糊区间；抑制直接删除字段。

48. 识别资产、威胁、脆弱点并赋值属于风险评估哪个阶段

- A. 准备
- B. 风险要素识别
- C. 风险分析
- D. 风险处置

答案：B 难度：易

解析：

风险要素识别阶段识别资产/威胁/脆弱性并赋值。

49. 电子证据肉眼不可见必须借助工具查看，该特性为

- A. 易破坏性
- B. 无形性
- C. 高科技性
- D. 时效性

答案：B 难度：中

解析：

无形性指电子证据肉眼不可见，需借助设备查看。

50. 等保安全功能检测国标是

- A. GB/T 25070
- B. GB/T 22239
- C. GB 17859
- D. GB/T 35273

答案：A 难度：中

解析：

GB/T 25070为网络安全等级保护安全设计技术要求；GB/T 22239为基础要求。

51. 渗透测试确认方案、模拟攻击属于哪个阶段

- A. 准备
- B. 实施
- C. 评估
- D. 结题

答案：B 难度：易

解析：

实施阶段执行确认方案与模拟攻击。

52. syslog标准日志四元组格式

- A. 时间、主机、程序、消息
- B. 主机、用户、时间、内容
- C. 级别、进程、时间、消息
- D. 时间、IP、用户、日志

答案：A 难度：中

解析：

syslog标准格式为：时间 主机 程序 消息。

53. 不属于Windows账户策略配置项

- A. 密码复杂度
- B. 账户锁定阈值
- C. 日志审计
- D. 锁定计数器

答案：C 难度：易

解析：

日志审计属于本地安全审计策略，非账户策略。

54. 攻击者伪装合法账号登录数据库属于

- A. 伪装攻击
- B. 旁路
- C. 隐蔽信道
- D. 口令嗅探

答案：A 难度：中

解析：

伪装合法账号登录属伪装攻击。

55. Oracle默认存储账号密码配置文件

- A. listener.ora
- B. strXXX.cmd
- C. key.ora
- D. tnsnames.ora

答案：B 难度：难

解析：

56. 负责数据库角色、权限整体管控的安全机制

- A. 访问控制
- B. 安全管理
- C. 安全审计
- D. 数据加密

答案：B 难度：中

解析：

安全管理机制负责角色与权限整体管控。

57. 二层识别MAC、基于MAC转发交换机属于第几代

- A. 一代
- B. 二代
- C. 三代
- D. 四代

答案：B 难度：难

解析：

基于MAC地址转发的交换机为第二代（一代为集线器/共享介质）。

58. 不属于SNMP安全管控手段

- A. IP访问限制
- B. 团体字认证
- C. 权限分级
- D. 关闭服务

答案：A 难度：中

解析：

59. 交换机Web管理无认证远程执行命令漏洞类型

- A. 代码执行漏洞
- B. DoS漏洞
- C. 内存破坏
- D. 旁路泄露

答案：A 难度：中

解析：

无认证远程执行命令属代码执行/命令执行漏洞。

60. NIST安全框架五大功能，访问控制属于

- A. 识别
- B. 保护
- C. 检测
- D. 响应

答案：B 难度：中

解析：

NIST CSF：识别、保护、检测、响应、恢复；访问控制属保护(Protect)。

61. 3DES加密标准流程（E加密 D解密）

- A. $E(k1) \rightarrow D(k2) \rightarrow E(k3)$
- B. $D(k1) \rightarrow E(k2) \rightarrow D(k3)$
- C. 三次E加密
- D. 三次D解密

答案：A 难度：中

解析：

三重DES标准流程为加密-解密-加密。

62. PGP邮件明文默认对称加密算法

- A. DES
- B. IDEA
- C. AES
- D. RSA

答案：B 难度：中

解析：

RSA仅加密会话密钥，邮件正文使用IDEA。

63. SSL负责分段、压缩、加解密的子协议

- A. 握手协议
- B. 记录协议
- C. 告警协议
- D. 密码变更协议

答案：B 难度：中

解析：

SSL记录协议负责分段、压缩、加密/解密。

64. 屏蔽子网防火墙第一道边界设备

- A. 外网边界防火墙/路由器
- B. 内网防火墙
- C. DMZ堡垒机
- D. 核心交换机

答案：A 难度：中

解析：

屏蔽子网（Screened Subnet）最外侧为外网边界防火墙/路由器。

65. 最小特权管理含义是

- A. 用户仅拥有完成工作必需权限
- B. 管理员权限拆分互不干涉
- C. 多人共管核心系统
- D. 权限定期回收

答案：A 难度：易

解析：

最小特权原则：用户仅拥有完成工作必需的权限。

66. CIDE模型生成原始流量事件组件

- A. 事件产生器
- B. 分析器
- C. 响应单元
- D. 事件库

答案：A 难度：难

解析：

CIDE中事件产生器(Generator)生成原始事件。

67. DNS隧道攻击主要破坏安全目标

- A. 保密性数据外泄
- B. 完整性
- C. 可用性
- D. 不可否认

答案：A 难度：中

解析：

内网敏感数据通过DNS隧道向外泄露，破坏保密性。

68. R2级IDC机房业务可用性标准

- A. 99%
- B. 99.5%
- C. 99.9%
- D. 99.99%

答案：C 难度：难

解析：

R2级对应99.9%可用性。

69. 《互联网域名管理办法》安全事件上报时限

- A. 12h
- B. 24h
- C. 48h
- D. 72h

答案：B 难度：中

解析：

域名安全事件上报时限为24小时。

70. 访问控制三核心要素不包含

- A. 主体
- B. 客体
- C. 访问规则
- D. 审计日志

答案：D 难度：易

解析：

访问控制三要素：主体、客体、访问规则（访问策略）。

71. (71-75英文完形填空合并) Perhaps the most obvious difference between private-key and public-key encryption is that the former assumes complete secrecy of all cryptographic keys, whereas the latter requires secrecy for only the private key. Although this may seem like a minor distinction, the ramifications are huge: in the private-key setting the communicating parties must somehow be able to share the (71) key without allowing any third party to learn it, whereas in the public-key setting the (72) key can be sent from one party to the other over a public channel without compromising security. ... private-key encryption schemes use the (73) key for both encryption and decryption, whereas public-key encryption schemes use (74) keys for each operation. ... a single instance of a (75) encryption scheme enables multiple senders to communicate privately with a single receiver...

- 71. A. main B. same C. public D. secret
- 72. A. stream B. different C. public D. secret
- 73. A. different B. same C. public D. private
- 74. A. different B. same C. public D. private
- 75. A. private-key B. public-key C. stream D. Hash

答案：71.D 72.C 73.B 74.A 75.B 难度：难

解析：

71 secret key：对称加密双方共享秘密密钥； 72 public key：公钥可在公网明文传输； 73
same：对称加密加解密使用同一密钥； 74 different：非对称加密公私两组不同密钥； 75
public-key：公钥加密支持多发送者向单一接收者单向私密通信。

2023年下半年（11月） • 应用技术案例（共6个）

【案例1】试题一 密码学DES算法（S盒与填充）

已知DES算法S盒第0盒（S1）表格（行/列编号0-15），部分数据空缺需补全

使用DES对明文字符串“12345”加密需进行分组填充

给定密钥 \x01\x01\x01\x01\x01\x01\x01\x01 对明文加密

【问题】问题1(4分)补全S盒空缺数据(1)(2)(3)(4)；问题2(2分)S盒输入110011，计算二进制输出；问题3(3分)“12345”填充后数据长度多少比特，给出填充后字符串；问题4(3分)使用全01密钥加密出现什么安全问题；问题5(2分)替代和置换对应香农论文中哪两种密码技术；另含问题6。

【参考答案】

(1) 补全S盒空缺：参考答案为 3、13、15、0

(2) S盒输入110011 → 二进制输出 0110（第1、6位=11→行3；中间4位1001→列9；查第3行第9列=6→0110）

(3) 填充后长度64比特（8字节），填充后字符串：12345\x03\x03\x03（PKCS#5，缺3字节各填0x03）

(4)

该密钥为DES弱密钥（全相同字节），加密与解密操作完全相同（ $E_k(P)=D_k(P)$ ），攻击者一次加密即可破解，安全性失效

(5) 替代（Substitution，代换）与置换（Permutation/换位），对应香农《保密系统的通信理论》中混淆与扩散思想的基础操作

【解析】

本题考查DES核心机制：S盒查表、分组填充(PKCS#5)、弱密钥概念，以及香农密码学两大基本操作（代换与置换）。S盒填空因差异需以考场原表为准。

【案例2】试题二 网络扫描检测与iptables防护

某网络受到扫描攻击，使用Wireshark抓包分析，截图显示大量来自源IP 192.168.85.129的SYN数据包

目标端口21、80、443收到SYN后均回复SYN/ACK，部分端口回复RST/ACK

需使用iptables对扫描流量进行过滤

【问题】问题1(2分)写出扫描源地址；问题2(2分)写出产生如图流量包视图的Wireshark过滤规则；问题3(2分)此流量包属于什么类型扫描；问题4(2分)21/80/443端口收到SYN后回复SYN/ACK说明什么；问题5(2分)RST/ACK分组的TCP标志位值是多少；问题6(2分)iptables filter表应使用哪条链；问题7(2分)写出一条基于源地址过滤的iptables规则。

【参考答案】

(1) 扫描源地址：192.168.85.129

(2) Wireshark过滤规则：ip.src == 192.168.85.129（或 tcp.flags.syn==1 && tcp.flags.ack==0）

(3) SYN半连接扫描（隐蔽扫描 / Stealth SYN scan）

(4) 目标端口处于开放（open）状态

(5) RST/ACK的TCP标志位值：0x14（RST=0x04 + ACK=0x10）

(6) 应使用INPUT链（目标为本机流量的过滤）

```
(7) iptables -A INPUT -s 192.168.85.129 -j DROP
```

【解析】

本题综合考查Wireshark抓包分析与iptables防火墙规则编写。SYN扫描通过只发SYN、根据回应判断端口状态实现隐蔽探测；RST/ACK标志位=0x14；防护用INPUT链DROP源IP。

【案例3】 试题三 Web安全 命令注入漏洞

某PHP代码使用shell exec执行ping功能，未对用户输入(ip参数)做校验

代码片段: `if($ POST['submit']){ $target=$ REQUEST['ip']; ... shell exec('ping ' . $target); }`

【问题】问题1(2分)这段代码存在什么漏洞；问题2(3分)有几个参数，哪个存在安全漏洞；问题3(2分)HTTP请求类型是什么；问题4(2分)输入8.8.8.8点击submit，服务端执行什么命令；问题5(2分)输入127.0.0.1；

whoami (或8.8.8.8) && ls

-1) 执行了什么命令；问题6(2分)该提交编码类型；问题7(2分)文件属主所在用户组；问题8(5分)至少给出4种修复方案。

【参考答案】

(1) 操作系统命令注入漏洞 (OS Command Injection)

(2) 共2个参数：submit按钮、ip输入字段；存在漏洞的是ip（\$ REQUEST['ip']未校验）

(3) POST (提交数据; \$ REQUEST兼容GET, 主请求类型为POST)

(4) Windows: ping 8.8.8.8; Linux/Unix: ping -c 4 8.8.8.8

(5) 127.0.0.1; whoami → 执行 ping -c 3 127.0.0.1 与 whoami; 或 8.8.8.8 && ls -l

(6) D (application/x-www-form-urlencoded)

(7) www-data

(8)

修复方案：①使用`escapeshellarg()`/`escapeshellcmd()`对参数转义；②正则白名单严格校验IPv4/IPv6格式；③禁止调用`shell_exec`等系统命令函数，改用语言内置网络函数实现ping；④过滤；|&\$等命令分隔/危险字符；⑤部署WAF拦截命令注入特征载荷

【解析】

本题考查命令注入漏洞的识别与防护。核心是用户输入未经校验直接拼接到系统命令导致任意命令执行；修复应从输入校验、危险函数禁用、字符过滤、WAF多层防御。

【案例4】试题四 Android移动安全

Android应用存在组件安全风险，需进行安全分析

Android权限机制分为不同保护等级

ContentProvider等组件存在数据泄露风险

【问题】问题1(2分)Android应用安装包(APK)能否修改后缀为.zip解压；问题2(3分)Android权限三大类别；问题3(2分)应用权限声明保存在哪个文件；问题4(3分)ContentProvider组件主要风险漏洞；问题5(5分)移动APP安全加固手段。

【参考答案】

(1) APK可以修改后缀为.zip进行解压查看资源

(2)

权限三大类别：Normal（普通权限）、Signature（签名权限）、Dangerous（危险权限）（另有signatureOrSystem为第四类）

(3) AndroidManifest.xml

(4) ContentProvider主要风险：SQL注入、越权数据访问（外部应用无授权读写私有数据）

(5)

加固手段：代码混淆、防调试/防附加调试器、防二次打包、签名校验、so库加密、敏感数据本地加密存储、HTTPS证书校验防中间人劫持

【解析】

本题考查Android安全：APK包结构、权限保护等级、四大组件风险（ContentProvider易致SQL注入与越权）、APP安全加固方法。注意题序在不同中为试题四或试题五。

【案例5】试题五 信息安全管理（访问控制与审计，/）

企业信息系统需要设计身份认证、权限管理、安全审计体系

【问题】问题1(4分)简述三类访问控制模型；问题2(4分)双因素认证(2FA)两种常见因子举例；问题3(3分)安全审计日志至少需要包含哪些字段；问题4(4分)企业防范内部数据泄露管理措施。

【参考答案】

(1)

三类访问控制模型：DAC自主访问控制（资源所有者自主分配权限，灵活性高、安全性弱）；MAC强制访问控制（系统统一强制标记安全级别，用户无法自主更改，多用于涉密）；RBAC基于角色访问控制（权限绑定角色，用户分配角色，企业系统最常用）

(2) 双因素认证两种因子：something you know（密码）；something you have（短信验证码、硬件令牌、手机APP令牌）；something you are（指纹、人脸）

(3) 审计日志至少包含：主体账号、操作时间、源地址、操作类型、访问对象、操作结果

(4)

防内部泄露措施：最小权限原则分配账号、敏感操作审计、终端DLP数据防泄漏、离职人员账号及时回收、定期安全意识培训、禁止私自外传敏感文档

【解析】

本题考查信息安全管理体系设计：访问控制模型（DAC/MAC/RBAC）、双因素认证、安全审计日志要素、内部数据防泄露管理。

【案例6】试题四 Windows隐藏用户与克隆

Windows系统中通过net命令创建带\$的隐藏用户

需查看/克隆隐藏用户，并借助注册表实现权限提升

【问题】问题1(1分)查看用户的net命令；问题2(2分)用net命令创建test\$用户口令123456；问题3(1分)net命令能否查看刚建的test\$用户；问题4(2分)查看隐藏用户的方法；问题5(2分)用户账户保存在注册表路径；问题6(2分)管理员用户对应注册表Users目录下项；问题7(2分)将test\$克隆为管理员账户的方法。

【参考答案】

(1) net user

(2) net user test\$ 123456 /add; net localgroup administrators test\$ /add（提升为管理员）

(3) 不能（带\$为隐藏账户，命令行看不到，但图形界面/注册表可见）

(4) WIN+R输入 lusrmgr.msc 打开本地用户和组查看；或 regedit 打开注册表查看

(5) HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users

(6) Administrator 或 000001F4

(7) 在注册表中将test\$的F值（用户权限数据）复制/替换为Administrator(000001F4)的F值，实现账户克隆

【解析】

本题考查Windows本地账户与隐藏用户（带\$）、注册表用户存储结构及账户克隆原理。注意：本案例主要见于；在/中对应试题四为Android、试题五为安全管理，试题四/五的题序与内容在不同间存在差异，请以实际考卷为准。

2024年下半年（11月10日） • 综合知识真题（共30题）

1. 我国的国家标准《计算机信息系统安全保护等级划分准则》（GB 17859）》将计算机信息系统安全保护等级分为五级，规定从开始要求提供审计安全机制。

- A. 第一级
B. 第二级
C. 第四级
D. 第三级

答案: B 难度: 易

解析:

GB 17859 第二级为“系统审计保护级”，从第二级起开始要求提供审计安全机制，故正确答案为B。

2. 《信息安全技术 信息安全风险评估方法（GB/T 20984-2022）》给出了一种基于表现形式的威胁分类方法。其中数据外泄属于。

- A. 越权或滥用
B. 网络流量不可控
C. 软硬件故障
D. 隐私保护不当

答案: B 难度: 中

解析:

GB/T 20984-2022 基于表现形式的威胁分类中，数据外泄归于“网络流量不可控”类。

3. 计算机病毒通常附加在正常软件或文档中，一旦触发执行，就会潜入受害用户的计算机。以下计算机病毒以Word文档为隐蔽载体的是。

- A. 熊猫病毒
B. NIMDA病毒
C. Melissa
D. 求职信病毒

答案: C 难度: 易

解析:

Melissa 是一种以 Word 文档为传播载体的宏病毒。

4. Kerberos是一个网络认证协议，其目标是使用密钥加密为客户端/服务器应用程序提供强身份认证。一个Kerberos系统涉及四个基本实体：Kerberos客户机、AS、TGS和应用服务器，通常统称为KDC。

- A. AS和TGS
B. 客户机、AS和TGS
C. TGS和应用服务器
D. 客户机和AS

答案: A 难度: 中

解析:

Kerberos 中 AS（认证服务器）与 TGS（票据授权服务器）合称 KDC（密钥分发中心）。

5. 网络安全等级保护2.0标准强化了可信计算技术使用的要求，各级增加了“可信验证”控制点。其中要求对设备的系统引导程序、系统程序等进行可信验证。

- A. 第三级
- B. 第四级
- C. 第一级
- D. 第二级

答案：C 难度：中

解析：

等保2.0 第一级即要求对设备的系统引导程序、系统程序等进行可信验证。

6. 《信息安全技术 36637-2018）》规定了ICT供应链的安全风险管理过程和控制措施，旨在提高网络运营者ICT供应链安全管理水平。其中给出的ICT供应链安全目标不包括。

- A. 抗抵赖性
- B. 保密性
- C. 完整性
- D. 可用性

答案：A 难度：中

解析：

ICT 供应链安全目标包括保密性、完整性、可用性，不包括抗抵赖性。

7. 中标麒麟可信操作系统支持TCM/TPCM和TPM2.0可信计算技术规范。中标麒麟可信操作系统结构包括管理子系统、安全子系统、可信子系统和应用开发环境四个部分，其中身份鉴别属于。

- A. 管理子系统
- B. 应用开发环境
- C. 可信子系统
- D. 安全子系统

答案：D 难度：中

解析：

中标麒麟可信操作系统的身份鉴别功能属于安全子系统。

8. 防火墙的网络地址转换（NAT）技术主要是为了解决公网地址不足而出现的，当内部某一个用户访问外网时，防火墙动态地从地址集中选择一个未分配的地址分配给该用户，该用户即可使用这个合法地址进行通信。在实现NAT的方式中，把内部地址映射到外部网络的一个IP地址的不同端口上的方式属于。

- A. pooled NAT
- B. Static NAT
- C. CAT
- D. PAT

答案：D 难度：中

解析：

将内部地址映射到外部一个IP的不同端口，为 PAT（端口地址转换/NAPT）。

9. 网络信息系统漏洞的存在是网络攻击成功的必要条件之一。网络安全重大事件几乎都会利用安全漏洞，

造成重大的网络安全危机。以下网络安全事件，利用了微软操作系统DCOM RPC缓冲区溢出漏洞的是。

- A. 分布式拒绝服务攻击
- B. 震网病毒
- C. 冲击波蠕虫
- D. 红色代码蠕虫

答案：C 难度：易

解析：

冲击波（Blaster）蠕虫利用 Windows DCOM RPC 缓冲区溢出漏洞传播。

10. 网闸通过利用一种GAP技术，使两个或者两个以上的网络在不连通的情况下，实现它们之间的安全数据交换与共享。以下有关网闸的表述，错误的是。

- A. 两个独立主机系统与网闸的连接是互斥的
- B. 网闸允许以数据文件形式进行应用数据交换
- C. 网闸可以有效抵御恶意数据驱动攻击
- D. 主机对网闸的操作只有“读”和“写”

答案：C 难度：中

解析：

网闸设计重点在于数据摆渡与协议剥离，不能有效抵御恶意数据驱动攻击，该项表述错误。

11. 隐私保护技术是针对个人信息安全保护的重要措施，常见的隐私保护技术有泛化、抑制、置换、裁剪、扰动等。其中改变数据属主的方式被称为。

- A. 置换
- B. 裁剪
- C. 抑制
- D. 泛化

答案：A 难度：易

解析：

隐私保护技术中，置换是改变数据属主（位置/归属）的方式。

12. 密码破解是安全渗透的常见方式，常见的口令破解方式包括口令猜测、穷举搜索、撞库等。以下工具软件中，常用于破解Windows系统口令的是。

- A. John the Ripper
- B. Tcpdump
- C. L0phtCrack
- D. WireShark

答案：C 难度：易

解析：

L0phtCrack 是常用于破解 Windows 口令的工具。

13. 运维安全审计产品是有关网络设备及服务器操作的审计系统。运维安全审计产品的主要功能有字符会话审计、图形操作审计、数据库运维审计、文件传输审计和合规审计等。其中审计SSH协议操作行为属于。

- A. 字符会话审计
- B. 数据库运维审计
- C. 文件传输审计

D. 合规审计

答案：A 难度：易

解析：

审计 SSH 协议操作属于字符会话审计。

14. 根据数字签名工作的基本流程，假设Alice需要签名发送一份电子合同文件给Bob，在签名过程中，Alice首先使用Hash函数将电子合同文件生成一个消息摘要，接下来需要用到对消息摘要进行数字签名。

A. Bob的私钥

B. Bob的公钥

C. Alice的私钥

D. Alice的公钥

答案：C 难度：中

解析：

数字签名由签名者用自身私钥对摘要签名，Alice 用 Alice 的私钥。

15. 恶意代码是一种违背目标系统安全策略的程序代码，会造成目标系统信息泄露、资源滥用，破坏系统的完整性和可用性。在恶意代码生存技术中，端口复用技术利用系统网络打开的端口传送数据，实现恶意代码的隐藏通信。以下木马复用25端口的是。

A. WinPC

B. WinCrash

C. Doly Trojan

D. FTP Trojan

答案：A 难度：中

解析：

WinPC 木马复用 25 端口（SMTP）进行隐藏通信。

16. 按照VPN在TCP/IP协议层的实现方式，可以将其分为链路层VPN、网络层VPN和传输层VPN。以下VPN实现方式，属于传输层VPN的是。

A. MPLS

B. SSL

C. 隧道技术

D. ATM

答案：B 难度：中

解析：

传输层 VPN 的典型实现是 SSL/TLS（VPN）。

17. 发动网络攻击之前，攻击者一般要先确定攻击目标并收集目标系统的相关信息，攻击者收集目标系统的信息类型包括目标系统一般信息、目标系统配置信息、目标系统安全漏洞信息、目标系统安全措施信息、目标系统用户信息等。其中社交网络账号属于。

A. 目标系统配置信息

B. 目标系统安全措施信息

C. 目标系统用户信息

D. 目标系统安全漏洞信息

答案：C 难度：易

解析:

社交网络账号属于目标系统用户信息。

18. W32.Blaster.Worm是一种利用DCOM
RPC漏洞进行传播的网络蠕虫，感染该蠕虫的计算机系统运行不稳定，系统会不断重启。以下有关W32.Blaster.Worm的表述，正确的是。

- A. 该蠕虫对windowsupdate.com进行拒绝服务攻击使得受害用户不能及时得到漏洞的补丁
- B. 该蠕虫对有DCOM RPC漏洞的机器发起TCP128端口的连接进行感染
- C. 该蠕虫在UDP port82端口进行监听
- D. 该蠕虫在TCP1344端口绑定一个cmd.exe后门

答案: A 难度: 中

解析:

Blaster 蠕虫对 windowsupdate.com 发起 DoS，以阻止受害用户及时获得补丁。

19. 以下关于防火墙的说法，错误的是。

- A. 防火墙的安全策略包括白名单策略、灰名单策略和黑名单策略
- B. 防火墙不能防止基于数据驱动式的攻击
- C. 防火墙是外部网络和受保护网络之间的唯一网络通道
- D. 防火墙能够屏蔽被保护网络内部的信息、拓扑结构和运行状况

答案: A 难度: 易

解析:

防火墙安全策略通常只有白名单与黑名单，不存在“灰名单策略”的通用说法，该项错误。

20. 在UNIX/Linux操作系统中，口令信息保存在passwd和shadow文件中，这两个文件所在的目录是。

- A. /bin
- B. /lib
- C. /etc
- D. /home

答案: C 难度: 易

解析:

UNIX/Linux 的 passwd 与 shadow 文件位于 /etc 目录。

21. 口令是保护路由器安全的有效方法，路由器口令的保存应是密文。在路由器配置时，使用命令保存口令密文。

- A. Blind
- B. Enable secret
- C. Encryption
- D. Secpwd

答案: B 难度: 易

解析:

Cisco 路由器使用 enable secret 命令以密文保存特权口令。

22. 操作系统审计一般是对操作系统用户和系统服务进行记录，主要包括用户登录和注销、系统服务启动和关闭、安全事件等。Linux操作系统自带审计功能，其中日志文件wtmp是。

- A. 当前用户登录日志

- B. 用户登录和退出日志
- C. 用户命令操作日志
- D. 最近登录日志

答案：B 难度：中

解析：

Linux 的 wtmp 日志记录用户登录与退出事件。

23. 国产商用密码算法是由国家密码研究相关机构自主研发，具有相关知识产权的商用密码算法。目前已经公布的国产密码算法主要有SM1、SM2、SM3、SM4和SM9等。以下属于椭圆曲线公钥密码算法的是。

- A. SM3
- B. SM1
- C. SM2
- D. SM4

答案：C 难度：易

解析：

SM2 为椭圆曲线公钥密码算法。

24. 网络安全漏洞利用防范技术针对漏洞触发利用的条件进行干扰或拦截，以防止攻击者成功利用漏洞。常见的网络安全漏洞利用防范技术包括，地址空间随机化技术ASLR、数据执行阻止技术DEP、堆栈保护技术、结构化异常处理覆盖保护技术SEHOP、虚拟补丁等。以下可以降低缓冲区溢出攻击成功率的是。

- A. SEHOP
- B. DEP
- C. ASLR
- D. 虚拟补丁

答案：C 难度：中

解析：

ASLR（地址空间随机化）可显著降低缓冲区溢出攻击成功率。

25. 对于客体File1，主体ID1、ID2、ID3，访问权限读r、写w和运行x。如果主体对客体的访问权限表示如下：File1: (ID1: rx) (ID2: rw) (ID3: rwx)。以上这种表示访问控制的方式被称为。

- A. 前缀表
- B. 访问控制表
- C. 能力表
- D. 后缀表

答案：B 难度：中

解析：

以客体为中心列出主体及其权限的访问控制表（ACL）属于访问控制表。

26. Windows用户登录到系统的过程中，用户进程访问客体对象时，通过子系统向核心请求访问服务。

- A. WSA
- B. WSL
- C. WIN32
- D. POSIX

答案：C 难度：中

解析：

Windows 用户进程通过 WIN32 子系统向核心请求访问服务。

27. 文件完整性检查的目的是发现受害系统中被篡改的文件或者操作系统的内核是否被替换。对于UNIX系统，网络管理员可以使用命令直接把系统中的二进制文件和原始发布介质上对应的文件进行比较。

- A. rmdir
- B. scp
- C. cmp
- D. pwd

答案：C 难度：易

解析：

UNIX 下可用 cmp 命令逐字节比较文件。

28. 按照交换机功能变化可以将其分为第一代交换机、第二代交换机、第三代交换机、第四代交换机和第五代交换机。其中第二代交换机识别数据中的MAC地址，并根据MAC地址选择转发端口。第二代交换机工作于OSI模型的。

- A. 应用层
- B. 数据链路层
- C. 传输层
- D. 网络层

答案：B 难度：易

解析：

第二代交换机基于 MAC 地址转发，工作于数据链路层。

29. 认证是一个实体向另外一个实体证明其所声称的身份的过程，一般由标识和鉴别两部分组成。标识是用来代表实体对象的身份标志，标识不仅要与实体存在强关联，同时要确保实体的。

- A. 机密性和可辨识性
- B. 机密性和可用性
- C. 唯一性和可用性
- D. 唯一性和可辨识性

答案：D 难度：易

解析：

标识须与实体强关联，并确保唯一性与可辨识性。

30. Oracle数据库建立数据库保险库（DV）机制，该机制用于保护敏感数据，具有防止数据系统未授权变更、多因素可信授权、职责隔离、最小化特权的功能。DV机制通过设置对特权进行控制。

- A. 透明数据加密和数据屏蔽
- B. 多级认证和数据库管理员
- C. 强认证和网络认证
- D. 安全域和命令规则

答案：D 难度：中

解析：

Oracle DV 通过“安全域”和“命令规则”对特权进行控制。

2024年下半年（11月10日）

• 应用技术案例（共2个）

【案例1】网络安全与数据安全（滴滴处罚与隐私保护案例）

网络安全侧重于防护网络和信息化的基础设施，特别重视重要系统和设施、关键信息基础设施以及新产业、新业务和新模式的有序和安全。

数据安全侧重于保障数据在开放、利用、流转等处理环节的安全以及个人信息隐私保护；网络安全与数据安全紧密相连、相辅相成。

数据安全要实现数据资源异常访问行为分析，高度依赖网络安全日志的完整性。

随着《网络安全法》和《数据安全法》的落地，数据安全已经进入法制化时代。

【问题】 【问题1，6分】2022年7月21日国家互联网信息办公室公布对滴滴全球股份有限公司依法做出网络安全审查相关行政处罚的决定，开出80.26亿罚单，请分析滴滴违反了哪些网络安全法律法规？ 【问题2，2分】根据《数据安全法》，数据分类分级中一般员工个人信息属于几级数据？ 【问题3，2分】员工薪水属于哪一类隐私？ 【问题4，2分】月薪8750元脱敏显示为5k-10k，属于哪种隐私保护技术措施？ 【问题5，5分】用RSA对用户名“admin”加密， $p=47$ 、 $q=71$ 、 $e=3$ ，求私钥、admin的十六进制整数、直接用公钥加密是否可行及原因、加密计算公式。

【参考答案】

- (1) 【问题1】滴滴违反了《网络安全法》《数据安全法》《个人信息保护法》及网络安全审查相关法规（未依法合规开展数据处理活动、未履行个人信息保护义务、危害国家数据安全等）。
- (2) 【问题2】一般员工个人信息属于三级秘密数据。
- (3) 【问题3】员工薪水属于属性隐私。
- (4) 【问题4】月薪8750显示为5k-10k属于泛化技术（将精确值映射为区间/范围）。
- (5) 【问题5】 $n=p \times q=47 \times 71=3337$ ， $\phi(n)=(47-1)(71-1)=3220$ ，公钥 $e=3$ ，私钥 $d=e^{-1} \bmod 3220=2147$ （因 $3 \times 2147=6441 \equiv 1 \bmod 3220$ ）；“admin”的十六进制整数为0x61646D696E；直接用公钥加密不可行，因明文整数远大于模数 $n=3337$ （明文须小于模数）；加密计算公式为 $C = M^e \bmod n = M^3 \bmod 3337$ 。

【解析】

本案例综合考查数据安全法律法规、隐私分类与隐私保护技术、以及RSA公钥密码的应用。以上答案为依据题干与公开法规的参考作答

【案例2】企业网络安全事件应急响应

某制造企业2024年8月15日10:00发现生产管理系统（三级等保系统）无法访问。

网络管理员检查发现：核心交换机CPU利用率达98%，上联链路带宽占满（1Gbps）。

防火墙日志显示大量源IP为/24的ICMP请求（每个IP发送5000包/秒）。

生产管理服务器（Windows Server 2022）进程中存在异常程序“sysupdate.exe”，占用大量内存。

服务器日志显示凌晨2:00有未知用户“admin2”登录成功，并执行了“net user admin2 /add”命令。

【问题】 【问题1，8分】请判断该事件的类型，并分析攻击路径。 【问题2，10分】请列出应急响应的关键步骤，并说明每一步的具体操作。 【问题3，7分】为防止类似事件再次发生，应采取哪些长期加固措施。

【参考答案】

(1) **【问题1】**事件类型为混合攻击：①内网DDoS攻击（ICMP洪泛）——源IP为内网地址，通过大量ICMP请求耗尽带宽和设备资源；②服务器恶意程序植入与权限提升——攻击者通过暴力破解或弱口令登录服务器，添加“admin2”用户，植入“sysupdate.exe”（可能为远控木马或勒索软件）。

(2) **【问题2】**应急响应关键步骤（参考）：①遏制——隔离受感染服务器与交换机、封禁可疑源IP、断开恶意外联；②根除——终止异常进程、删除恶意文件、清除后门账号admin2、修补弱口令；③恢复——从干净备份恢复系统、重置凭据、验证业务可用性；④溯源与加固——分析日志定位入口、部署监测；⑤总结上报——形成事件报告。

(3) **【问题3】**长期加固措施（参考）：①强制口令策略与多因素认证，杜绝弱口令；②完善日志审计与终端检测（EDR），记录终端信息（MAC/设备指纹）；③部署流量监测与抗DDoS设备，限制ICMP速率；④及时打补丁、最小权限原则、定期漏洞扫描；⑤建立应急响应预案并演练。

【解析】

本案例考查网络安全事件应急响应（DDoS+恶意代码+权限提升）的研判、处置与加固。注：本案例答案均为参考作答，官方答案未公开。

2025年下半年（11月） • 综合知识真题（共70题）

1. 以下关于中标麒麟操作系统的描述中，错误的是。

- A. 提供细粒度的自主访问控制
- B. 结合角色的基于类型的访问控制
- C. 通过了国家标准《信息安全技术 操作系统安全技术要求》(GB/T 20272-2019)规定的第五级要求
- D. 在自主可控、安全方面对开源Linux系统进行了安全增强

答案：C 难度：中

解析：

中标麒麟安全操作系统达到并通过的是GB/T

20272中的第四级（结构化保护级）要求，第五级（访问验证保护级）为国内操作系统尚未达到的最高级，故C错误。

2. 只完成TCP三次握手的前两次连接、不建立完整连接的扫描方式是。

- A. 隐蔽扫描
- B. 半连接扫描
- C. SYN扫描
- D. 完全连接扫描

答案：B 难度：易

解析：

半连接扫描（又称SYN扫描）只发送SYN并接收SYN/ACK，不发送最后的ACK，因此不建立完整TCP连接。本题B与C实质同义，给出的答案为B（教材以“半连接扫描”为标准表述）。

3. 陷阱网络（蜜网）中的数据捕获设备是。

- A. 路由器
- B. 蜜罐主机
- C. 防火墙
- D. IDS

答案：D 难度：中

解析：

教材P311-312：陷阱网络一般需实现蜜罐系统、数据控制系统、数据捕获系统、数据记录、数据分析、数据管理等功能，其中数据捕获设备是IDS；蜜罐只负责诱骗，数据控制设备是防火墙。

4. 以下不属于访问控制策略要素的是。

- A. 访问控制规则
- B. 访问控制过程
- C. 用户权限
- D. 控制对象

答案：B 难度：中

解析：

访问控制策略描述“谁能以什么方式访问什么对象”，包含控制对象、用户权限、访问控制规则等要素；“访问控制过程

”属于机制实现层面，不属于策略要素。

5. 根据《密码法》，以下属于国家秘密的是。

- A. 量子加密和解密算法
- B. 核心密码和普通密码
- C. 对称加密和非对称加密算法
- D. 分组密码和序列密码

答案：B 难度：易

解析：

《密码法》将密码分为核心密码、普通密码和商用密码。核心密码、普通密码用于保护国家秘密信息，其本身属于国家秘密；商用密码不属于国家秘密。

6. SSL VPN工作在OSI参考模型的哪一层？

- A. 物理层
- B. 网络层
- C. 传输层
- D. 数据链路层

答案：C 难度：易

解析：

SSL/TLS位于传输层之上、应用层之下，软考教材按“传输层VPN”归类；IPSec VPN为网络层，PPTP/L2TP为数据链路层。

7. 在零信任架构中，以下不能作为持续验证依据的是。

- A. 位置信息获取
- B. 短信验证码
- C. 使用的设备型号
- D. 网络访问轨迹

答案：B 难度：中

解析：

持续验证依赖可持续采集的环境与行为属性（位置、设备指纹/型号、访问轨迹等）；短信验证码是一次性的身份鉴别手段，属于“一次认证”，无法支撑持续性信任评估。

8. Alice给Bob发送文件并进行数字签名，应使用。

- A. Bob的私钥
- B. Alice的私钥
- C. Alice的公钥
- D. Bob的公钥

答案：B 难度：易

解析：

数字签名用签名者（发送方Alice）的私钥对消息摘要加密，接收方用Alice的公钥验签，从而实现身份认证与不可否认性。

9. 在Kerberos协议中，负责向用户颁发（服务）授予票据的组件是。

- A. AS（认证服务器）
- B. TGS（票据授予服务器）
- C. KDC（密钥分发中心）

D. SS（业务服务器）

答案：B 难度：中

解析：

AS负责初始身份认证并发放TGT（票据授予票据），TGS凭TGT向用户发放访问具体服务的服务票据（ST）。注：仅还原出A、B两个选项，C、D为按教材补齐的常见干扰项。

10. 操作系统中将内存特定区域标注为“非执行”，从而阻止代码在数据区执行的技术是。

A. 堆栈保护（Stack Guard）

B. 数据执行阻止（DEP）

C. 地址空间布局随机化（ASLR）

D. 沙箱隔离

答案：B 难度：易

解析：

DEP（Data Execution Prevention）把数据页标记为不可执行，缓冲区溢出注入的shellcode无法运行；ASLR是随机化地址布局，堆栈保护是插入canary值。注：仅还原出A、B、C三个选项，D为补齐项。

11. Snort规则中用于显示（输出）报警信息的关键字是。

A. syslog

B. content

C. msg

D. pass

答案：C 难度：中

解析：

msg用于指定报警时输出的提示信息；content用于匹配报文载荷内容；syslog是输出插件；pass是规则动作。注：第四个选项未还原，D为补齐项。

12. IPSec认证头（AH）协议无法实现的功能是。

A. 数据源鉴别

B. 提供保密通信（加密）

C. 数据完整性验证

D. 无连接完整性

答案：B 难度：易

解析：

AH只提供数据源认证、无连接完整性和抗重放，不提供机密性（不加密）；加密需由ESP提供。

13. 防火墙的“路由支持”属于以下哪类技术指标？

A. 性能指标

B. 安全功能指标

C. 安全保障指标

D. 环境适应性指标

答案：B 难度：中

解析：

教材P172：防火墙安全功能指标包括网络接口、协议支持、路由支持、NAT、VPN支持等；性能指标指吞吐量、时延、并发连接数等。

14. BLP（Bell-LaPadula）安全模型的特性是。

- A. 不能上写，可以下写
- B. 不能下写，可以上写
- C. 不能上读，可以下读
- D. 不能下读，可以上写

答案：B 难度：难

解析：

BLP的两条规则：简单安全特性“不上读”（no read up）、*特性“不下写”（no write down），即可以上写、可以下读。注意本题B与C均为BLP的正确表述，给出答案B；若考场原题四选一仅一个正确，则选项文字应有细节差异，此处。

15. 信息安全能力成熟度模型中，“漏洞分析/漏洞评估”属于CMM的哪一级？

- A. CMM1
- B. CMM3
- C. CMM2
- D. CMM4

答案：B 难度：中

解析：

教材P69 网络安全能力成熟度等级：CMM3（充分定义级）要求具备漏洞分析、渗透测试等充分定义的过程能力。

16. 防火墙的访问控制功能不能作用于以下哪一层？

- A. 传输层
- B. 物理层
- C. 网络层
- D. 应用层

答案：B 难度：难

解析：

防火墙可在网络层（包过滤）、传输层（状态检测）、应用层（应用代理/WAF）实施访问控制，无法作用于物理层，故按原理应选B。标注为D并自注“此题你怎么看？”，存在分歧，建议以B为准。

17. Linux系统中记录每个用户使用过的命令的文件是。

- A. lastlog
- B. acct（pacct）
- C. sulog
- D. utmp

答案：B 难度：中

解析：

教材P229：acct/pacct记录每个用户使用过的命令；lastlog记录最近登录时间；utmp记录当前登录用户；solog记录su命令使用情况。

18. SSL协议中，负责进行算法协商和密钥交换的子协议是。

- A. SSL连接协议
- B. SSL握手协议
- C. SSL记录协议
- D. SSL用户认证协议

答案：B 难度：难

解析：

SSL中算法协商与密钥交换由握手协议（Handshake

Protocol）完成。此处记录的选项为“连接协议/SSL传输层协议/用户认证协议”，与第32题的SSH子协议题高度重合，疑为回忆混淆（SSH对应答案为“SSH传输层协议”）。本条按SSL标准知识点给出选项与答案。

19. 以下不属于特洛伊木马“被动植入”方式的是。

- A. 社会工程学诱骗
- B. 网络蠕虫传播
- C. 邮件附件
- D. Web网页挂马

答案：B 难度：中

解析：

被动植入需要受害者参与（点击附件、浏览挂马网页、被诱骗执行）；网络蠕虫利用漏洞自动传播、无需用户参与，属于主动植入。对本题自注，但按教材定义B为正确答案。

20. 国产密码算法是由国家密码相关研究机构自主研发、具有相关知识产权的商用密码算法。目前已经公布的国产密码算法主要有SM1、SM2、SM3杂凑算法、SM4、SM9标识密码算法和ZUC算法等。其中SM1是一种对称的分组密码算法，其分组长度和密钥长度分别是。

- A. 256比特和128比特
- B. 64比特和128比特
- C. 256比特和256比特
- D. 128比特和128比特

答案：D 难度：易

解析：

SM1为分组密码算法，分组长度128比特、密钥长度128比特（算法不公开，仅以IP核形式提供）。

21. 以下WAF（Web应用防火墙）不能过滤的是。

- A. URL地址
- B. IP地址
- C. 文件后缀名
- D. 允许/禁止的HTTP方法

答案：B 难度：难

解析：

答案为B，理由是WAF聚焦HTTP/HTTPS应用层内容（URL、参数、后缀、HTTP方法），IP层过滤属传统防火墙职责。但实际主流WAF普遍支持IP黑白名单，此题争议较大。

22. FTP型特洛伊木马通常使用的端口是。

- A. 80
- B. 21
- C. 443
- D. 1080

答案：B 难度：易

解析：

FTP型木马在受害主机上开放21端口（FTP控制端口）等待攻击者连接上传下载文件。

23. 运维安全审计中，“字符会话审计”包含以下哪种协议？

- A. SFTP
- B. SSH
- C. FTP
- D. PostgreSQL

答案：B 难度：中

解析：

字符会话审计针对命令行终端类协议（SSH、Telnet、Rlogin）；SFTP/FTP属于文件传输审计；PostgreSQL属于数据库审计。

24. 以下不是网络嗅探（抓包）工具的是。

- A. tcpdump
- B. nmap
- C. wireshark
- D. dsniff

答案：B 难度：易

解析：

nmap是端口/漏洞扫描器，属于主动探测工具；tcpdump、wireshark、dsniff均为被动嗅探工具。

25. 我国的“国家信息安全漏洞共享平台”的英文缩写是。

- A. CNNVD
- B. CNVD
- C. CVSS
- D. CVE

答案：B 难度：易

解析：

CNVD（China National Vulnerability Database）为国家信息安全漏洞共享平台，由CNCERT牵头；CNNVD为国家信息安全漏洞库（中国信息安全测评中心）；CVE是漏洞编号标准，CVSS是漏洞评分系统。

26. 计算机信息系统安全保护等级划分中，“安全标记保护级”对应第几级？

- A. 二级
- B. 三级
- C. 一级
- D. 四级

答案：B 难度：易

解析：

GB

17859五级划分：一级用户自主保护级、二级系统审计保护级、三级安全标记保护级、四级结构化保护级、五级访问验证保护级。

27. 数字签名在PDRR模型中属于哪个环节？

- A. 检测（Detection）
- B. 保护（Protection）
- C. 响应（Response）

D. 恢复（Recovery）

答案：B 难度：易

解析：

PDRR=保护、检测、响应、恢复。数字签名属于事前的主动防护技术手段，归入保护环节。

28. CNCERT的中文全称是。

- A. 国家信息安全漏洞库
- B. 国家计算机网络应急技术处理协调中心
- C. 国家密码管理中心
- D. 国家信息安全测评中心

答案：B 难度：易

解析：

CNCERT/CC即国家计算机网络应急技术处理协调中心，是我国非政府性网络安全应急技术协调组织。

29. 计算机病毒的结构一般由三部分组成，即。

- A. 扫描模块、隐藏模块、破坏模块
- B. 复制传染模块、隐藏模块、感染模块
- C. 扫描模块、隐藏模块、感染模块
- D. 复制传染（引导）模块、隐藏（触发）模块、破坏（表现）模块

答案：D 难度：中

解析：

教材P272：计算机病毒一般由潜伏（隐藏/触发）机制、传染（复制）机制、表现（破坏）机制三部分构成。

30. 以下不属于分布式拒绝服务（DDoS）攻击工具/方式的是。

- A. TFN2k
- B. HashDoS
- C. Trino
- D. TFN

答案：C 难度：中

解析：

TFN、TFN2k为经典DDoS攻击工具（支持SYN Flood、UDP Flood等）；HashDoS利用哈希碰撞耗尽CPU，属应用层DoS；Trino（原PrestoSQL）是开源分布式SQL查询引擎，与攻击无关。注：教材中DDoS工具有“Trinoo”，本题以“Trino”作为干扰项。

31. 《网络安全法》第二十一条规定，国家实行网络安全等级保护制度。网络安全等级保护的主要工作中，等级保护测评机构依据相应等级要求，对定级的保护对象进行测评，并出具相应的等级保护测评证书的过程被称为。

- A. 备案
- B. 定级
- C. 等级测评
- D. 运营维护

答案：C 难度：易

解析：

等级保护五个环节：定级、备案、建设整改、等级测评、监督检查。由测评机构测评并出具测评报告/证书的环节即“等级测评”。

32. SSH协议是基于公钥的安全应用协议，可以实现加密、认证、完整性检查等多种安全服务。在SSH协议的子协议中，提供算法协商和密钥交换，并实现服务器认证，形成一个加密的安全连接，提供完整性、保密性和压缩选项服务。

- A. SSH传输层协议
- B. SSH连接协议
- C. SSH端口转发技术
- D. SSH用户认证协议

答案：A 难度：易

解析：

教材P58：SSH由传输层协议、用户认证协议、连接协议三个子协议组成。SSH传输层协议负责算法协商、密钥交换和服务器认证，建立加密安全通道。

33. 访问控制是指对资源对象的访问者授权、控制的方法及运行机制。以下属于“控制”的是。

- A. 接收邮件
- B. 读写
- C. 删除
- D. 禁止访问

答案：D 难度：中

解析：

访问控制中“授权”表现为允许读、写、删除、接收等操作许可；“控制”表现为对访问的限制与拒绝，即“禁止访问”。

34. 防火墙和网闸都是保障内网安全的网络安全技术。以下关于防火墙和网闸的说法中，错误的是。

- A. 防火墙依赖规则库防御已知威胁
- B. 网闸对外提供开放端口
- C. 网闸可实现协议层面的完全隔离
- D. 防火墙支持双向通信与会话保持

答案：B 难度：中

解析：

网闸（安全隔离与信息交换系统）通过“摆渡”方式剥离协议、断开链路，不对外提供开放端口、不存在网络连接，故B错误。

35. 信息安全领域中，MAC（Mandatory Access Control）属于。

- A. 强制访问控制
- B. 自主访问控制
- C. 基于角色的访问控制
- D. 基于属性的访问控制

答案：A 难度：易

解析：

MAC=强制访问控制，由系统按安全标记强制实施；DAC为自主访问控制，RBAC为基于角色，ABAC为基于属性。注：仅记录题干与答案关键词，选项为按教材补齐。

36. APT（高级持续性威胁）攻击的显著特点是。

- A. 持久性地控制目标系统
- B. 一次性大流量冲击

- C. 随机选择攻击目标
- D. 仅利用公开已知漏洞

答案：A 难度：易

解析：

APT具有目标明确、手段高级、长期潜伏并持久控制目标系统的特点。注：仅记录题干与答案关键词，选项为按教材补齐。

37. 以下安全模型中，从攻击者角度描述攻击行为的模型是。

- A. PDRR
- B. PPDR
- C. CFS（能力成熟度框架）
- D. ATT&CK

答案：D 难度：中

解析：

ATT&CK（Adversarial Tactics, Techniques and Common Knowledge）从攻击者视角对战术、技术进行知识化建模；PDRR、PPDR均为防御方视角的安全模型。

38. 信息安全CIA三元组中的“I”对应。

- A. 机密性（Confidentiality）
- B. 完整性（Integrity）
- C. 可用性（Availability）
- D. 不可否认性（Non-repudiation）

答案：B 难度：易

解析：

CIA=Confidentiality（机密性）、Integrity（完整性）、Availability（可用性）。不可否认性属于扩展属性。

39. 以下工具中适用于端口扫描的是。

- A. Nessus
- B. Nmap
- C. X-scan
- D. Wireshark

答案：B 难度：中

解析：

Nmap是最典型的端口扫描器。若本题为多项选择题，则A、B、C（Nessus、Nmap、X-scan）均具备端口扫描能力，Wireshark仅为抓包分析工具、不能扫描；记录不清，按单选取B。

40. 一串数字如3254355487665，对外公布显示为3254XXXXX665，这属于哪种数据脱敏（去标识化）方式？

- A. 替换
- B. 屏蔽（掩码）
- C. 泛化
- D. 变形

答案：A 难度：难

解析：

给出答案A（替换，用X替换原字符）；教材P434数据脱敏技术中，用固定符号遮盖部分字段的做法通常归为“屏蔽/掩码”，故不少考生认为应选B。两种理解并存，建议以教材原文表述为准。

41. CA使用一个来管理、分发和发布所颁发的数字证书。

- A. RA（注册机构）
- B. 目录服务器
- C. 客户端
- D. 实体终端

答案：B 难度：中

解析：

PKI中由目录服务器（通常基于LDAP/X.500）集中存储、发布和分发证书及CRL；RA只负责用户身份审核与注册申请。

42. tcpdump中用于指定抓包网卡（网络接口）的参数是。

- A. -i
- B. -a
- C. -c
- D. -d

答案：A 难度：易

解析：

tcpdump -i eth0 指定监听接口；-c 指定抓包数量；-w 写入文件；-d 以人可读方式输出编译后的匹配码。

43. grep命令中，仅匹配完整单词的参数是。

- A. -i
- B. -w
- C. -c
- D. -n

答案：B 难度：易

解析：

教材P234：-w（word-regexp）只匹配整个单词；-i忽略大小写；-c统计匹配行数；-n显示行号。

44. 以下不属于设备物理安全防护技术特性的是。

- A. 防电磁信息泄漏
- B. 设备标记标识
- C. 抗电磁干扰
- D. 存储介质安全

答案：D 难度：中

解析：

教材P99设备物理安全的技术特性包括设备标志和标记、防止电磁信息泄漏、抗电磁干扰、电源保护、设备振动/碰撞/冲击适应性等；存储介质安全属于介质安全范畴，故答案为D。

45. 根据ISO/OSI模型，SSL VPN属于哪一层的VPN？

- A. 网络层
- B. 应用层
- C. 传输层
- D. 数据链路层

答案：C 难度：易

解析：

与第6题为同一考点。SSL/TLS按软考教材归类为传输层VPN。

46. MySQL数据库进行逻辑备份（导出SQL脚本）的命令是。

- A. mysqldump
- B. mysql
- C. mysqladmin
- D. mysqlbinlog

答案：A 难度：易

解析：

mysqldump用于逻辑备份导出；mysql为客户端（可用于恢复导入）；mysqladmin为管理工具；mysqlbinlog用于解析二进制日志做增量恢复。注：仅记录答案关键词mysqldump，选项为补齐。

47. 以下关于攻击树（Attack Tree）方法的描述中，错误的是。

- A. 不能用来对循环事件建模
- B. 可以进行费效分析和概率分析
- C. 对于任意大规模的复杂场景不适用
- D. 可以图形化表示攻击者达成目标的多条路径

答案：B 难度：难

解析：

教材列出攻击树的缺点为：不能用来发现未知漏洞、不能对循环事件建模、对于大规模复杂系统不适用；而“能够进行费效分析和概率分析”通常被列为攻击树的优点，因此选B为“错误描述”存在争议。给出的答案为B，按收录并。

48. X.509数字证书中的Validity字段表示的信息是。

- A. 有效日期（起止时间）
- B. 序列号
- C. 版本号
- D. 颁发者

答案：A 难度：易

解析：

Validity包含Not Before和Not After，即证书有效期起止时间。注：注明“选项排序已乱”。

49. 网络设备上配置TACACS+服务器共享密钥的命令是。

- A. tacacs-server key
- B. tacacs-server ticket
- C. tacacs-server pw
- D. tacacs-server host

答案：A 难度：中

解析：

tacacs-server key <密钥> 用于配置设备与TACACS+服务器之间的共享密钥；tacacs-server host用于指定服务器地址。

50. 在交换机上配置可以对登录用户进行过滤。

- A. MAC地址表
- B. IP源地址封装
- C. 端口号
- D. ACL（访问控制列表）

答案：D 难度：中

解析：

在交换机VTY线路上应用ACL，可限制哪些源地址允许远程登录管理设备。

51. Windows系统中用于管理（查询、导出、清除）事件日志的命令行工具是。

- A. auditutil
- B. auditpol
- C. wevtutil
- D. aureport

答案：C 难度：中

解析：

wevtutil用于查询/导出/清空Windows事件日志；auditpol用于配置审核策略；aureport是Linux auditd的报表工具。

52. 在PDRR模型中，数字签名属于哪个环节？

- A. 保护
- B. 检测
- C. 恢复
- D. 响应

答案：A 难度：易

解析：

与第27题为同一考点，数字签名属于保护（Protection）环节。

53. HMAC消息认证码在国密体系中通常采用算法作为其杂凑函数。

- A. SM2
- B. SM3
- C. SM4
- D. SM9

答案：B 难度：易

解析：

HMAC需要一个杂凑（散列）函数，国密体系中的杂凑算法是SM3；SM2/SM9为非对称算法，SM4为对称分组算法。

54. 网络安全组织体系中，负责日常安全运维工作的是。

- A. 领导层
- B. 管理层
- C. 执行层
- D. 外部协作层

答案：C 难度：易

解析：

网络安全管理组织通常分为领导层（决策）、管理层（规划与制度）、执行层（日常运维与操作）、外部协作层（第三方支撑）。

55. GB 17859中，计算机信息系统安全保护等级的第三级名称是。

- A. 系统审计保护级
- B. 安全标记保护级
- C. 结构化保护级
- D. 访问验证保护级

答案：B 难度：易

解析:

与第26题为同一考点。第三级为安全标记保护级。

56. 代理服务器中,FTP代理使用的端口是。

- A. 21
- B. 1080
- C. 80
- D. 443

答案: A 难度: 中

解析:

答案为A(21,与FTP服务端口一致);但SOCKS代理常用1080端口,部分考生认为应选B。按教材“代理服务技术”中FTP代理端口21收录。

57. Windows系统中用于安全检测/查看修改注册表的工具是。

- A. Tripwire
- B. regedit
- C. wevtutil
- D. lusrmgr.msc

答案: B 难度: 易

解析:

regedit为Windows注册表编辑器;Tripwire是Unix/Linux文件完整性检查工具。注:仅还原出A、B两个选项,C、D为补齐项。

58. W32.Blaster.Worm是一种利用DCOM RPC漏洞进行传播的网络蠕虫,其传播能力很强。感染蠕虫的计算机系统运行不稳定,系统会不断重启。并且该蠕虫还将对windowsupdate.com进行,使得受害用户不能及时地得到这个漏洞的补丁。

- A. 拒绝服务攻击
- B. SQL注入攻击
- C. DNS投毒攻击
- D. 中间人攻击

答案: A 难度: 中

解析:

教材P41:冲击波蠕虫(Blaster)会对windowsupdate.com发起SYN Flood拒绝服务攻击,阻断用户获取补丁。注:仅记录答案关键词,B/C/D为补齐的干扰项。

59. 红色代码(Code Red)蠕虫病毒利用微软Web服务器IIS 4.0或5.0中服务的安全缺陷,通过自动扫描感染方式传播蠕虫。

- A. index(索引服务idq.dll)
- B. print(打印服务)
- C. webdav
- D. asp.dll

答案: A 难度: 中

解析:

教材P33:红色代码利用IIS索引服务(Index Server,idq.dll)的缓冲区溢出漏洞传播。注:仅记录答案关键词index,其余为补齐的干扰项。

60. 网络杀伤链（Kill

Chain）模型将网络攻击活动分成目标侦察、武器构造、载荷投送、漏洞利用、安装植入、指挥和控制、目标行动等七个阶段。在受害目标系统上安装远程访问的特洛伊木马或后门程序，以持久性地控制目标系统，属于哪个阶段？

- A. 安装植入（Installation）
- B. 载荷投送（Delivery）
- C. 漏洞利用（Exploitation）
- D. 指挥和控制（Command and Control）

答案：A 难度：中

解析：

教材P25：在目标系统上安装后门/木马以维持持久访问，对应Kill Chain的“安装植入”阶段。注：仅记录答案关键词，其余为补齐的干扰项。

61. 以下哪些属于对称加密算法？

- A. SM1
- B. SM4
- C. SM7
- D. SM9

答案：A、B、C 难度：中

解析：

SM1、SM4、SM7均为对称分组密码算法；SM9为标识（非对称）密码算法。

62. 关于DNSSEC，下列说法正确的是？

- A. 使用RRSIG记录进行签名
- B. 支持DS记录建立信任链
- C. 采用EDNS0扩展
- D. 提供数据机密性

答案：A、B、C 难度：难

解析：

DNSSEC通过RRSIG/DNSKEY/DS等记录提供来源认证与完整性保护，依赖EDNS0扩展承载大报文；DNSSEC不提供机密性（不加密DNS报文）。

63. 在Linux能力（capability）机制中，可允许普通用户执行低端口（<1024）绑定的能力包括？

- A. CAP_NET_ADMIN
- B. CAP_NET_BIND_SERVICE
- C. CAP_SYS_RAWIO
- D. CAP_DAC_OVERRIDE

答案：B 难度：难

解析：

仅CAP_NET_BIND_SERVICE允许绑定1024以下特权端口。

64. 以下哪些攻击可导致容器逃逸？

- A. 脏牛（Dirty COW）
- B. runC容器逃逸漏洞（CVE-2019-5736）
- C. Kubernetes API Server未授权访问

D. docker cp 竞态条件（CVE-2021-41089）

答案：B、D 难度：难

解析：

CVE-2019-5736（runC）与CVE-2021-41089（docker cp）均为典型容器逃逸漏洞；Dirty COW需依赖老内核本地提权，K8s API未授权属横向移动而非逃逸。

65. 在零信任参考架构中，可作为策略执行点（PEP）的组件有？

- A. SDP网关
- B. API网关
- C. 微隔离代理
- D. 传统VPN集中器

答案：A、B、C 难度：中

解析：

PEP需支持动态、细粒度授权决策的实时执行；传统VPN集中器只做一次性接入认证，不具备持续动态授权能力。

66. 以下属于NIST SP 800-61事件响应生命周期阶段的有？

- A. 检测与分析
- B. 遏制与根除
- C. 恢复
- D. 事后经验教训

答案：A、B、C、D 难度：中

解析：

NIST SP 800-61生命周期为：准备；检测与分析；遏制、根除与恢复；事后活动（经验教训）。

67. 在Android应用逆向中，可用于检测Root状态的方法有？

- A. 检查su二进制文件是否存在
- B. 检查ro.debuggable/ro.secure属性
- C. 调用Google SafetyNet API
- D. 检查应用签名证书

答案：A、B、C 难度：中

解析：

签名证书校验用于判断应用是否被重打包篡改，与设备是否Root无关。

68. 关于日志审计合规要求，下列明确要求留存期限不少于6个月的有？

- A. 《网络安全法》
- B. 《电子商务法》
- C. 《个人信息保护法》
- D. GB/T 22239-2019 第三级

答案：A、B、D 难度：难

解析：

《网络安全法》第二十一条明确网络日志留存不少于六个月；等保2.0三级要求审计记录留存不少于6个月；《个人信息保护法》未明确规定6个月期限。

69. 在防火墙双机热备（HA）中，可实现会话（状态）同步的协议/技术有？

- A. VRRP

- B. HRP (Huawei Redundancy Protocol)
- C. FGCP (FortiGate Clustering Protocol)
- D. CARP

答案：B、C、D 难度：难

解析：

HRP、FGCP、CARP可同步会话表等状态信息；VRRP仅提供网关/路由冗余，不同步会话状态。

70. **【第71~75题**

英语题（阅读/完形填空）• 未还原】综合知识科目最后5题为英文试题（通常为一段信息安全主题英文短文，考查5个空的词汇/搭配选择）。

- A. （未还原）
 - B. （未还原）
 - C. （未还原）
 - D. （未还原）
-

2025年下半年（11月）

• 应用技术案例（共9个）

【案例1】案例一：Android APK 逆向分析与权限安全

题目给出一个Android应用的APK文件结构截图（压缩包内含 META-INF/、classes.dex、AndroidManifest.xml、resources.arsc 等条目）。并给出一段 AndroidManifest.xml 代码片段，其中包含 <permission> 自定义权限声明及 protectionLevel 属性，同时声明了多个应用组件。

要求考生结合APK包结构、权限保护级别和Android四大组件安全，回答相关问题。

- 【问题】问题1：安卓APK实际上是什么类型的文件？（A. 文件型 B. 压缩型 C. 执行型 D. 图片型）
- 问题2：APK压缩包中负责存放数字签名信息的是哪个目录/文件？
- 问题3：APK的字节码（Dalvik字节码）存放在哪个文件中？
- 问题4：应用的参数与组件配置声明在哪个文件中？
- 问题5：（结合给出的AndroidManifest.xml代码）该自定义权限定义所使用的保护级别参数是什么？
- 问题6：图中 protectionLevel 的取值属于哪一类权限？
- 问题7：除代码中声明的权限保护级别外，还有 dangerous、signature、signatureOrSystem 三种，其中与题干所示级别一样“不安全”的是哪个？
- 问题8：图中的AndroidManifest.xml用到了哪些Android组件？
- 问题9：Android四大组件中最容易遭受界面（页面）劫持攻击的组件是哪个？

【参考答案】

- 问题1：选 B（压缩型）。APK本质是一个ZIP压缩包，可用解压工具查看其内部结构；但直接修改ZIP内容会破坏签名导致无法安装。
- 问题2：META-INF 目录（其中的 MANIFEST.MF、CERT.SF、CERT.RSA 保存摘要与数字签名信息）。
- 问题3：classes.dex（Dalvik/ART 可执行字节码文件，多dex时还有 classes2.dex 等）。
- 问题4：AndroidManifest.xml。
- 问题5：protectionLevel="normal"（普通级权限，安装时系统自动授予，无需用户确认）。
- 问题6：normal 级权限（低风险权限，自动授予）。
- 问题7：dangerous（危险级权限，需在运行时向用户申请；与 normal 同属“可被普通第三方应用申请到”的相对不安全级别，而 signature / signatureOrSystem 需签名或系统级匹配，安全性更高）。
- 问题8：activity、service、content provider（内容提供者）、broadcast receiver（广播接收者）——即Android四大组件。
- 问题9：activity（Activity负责界面展示，攻击者可通过启动伪造Activity覆盖在正常界面之上实施界面/页面劫持与钓鱼）。

【解析】

本案例考查Android应用安全基础：APK包结构（ZIP + META-INF签名 + classes.dex字节码 + AndroidManifest.xml清单）、权限保护级别四分类（normal/dangerous/signature/signatureOrSystem）及其风险差异、四大组件及其典型攻击面（Activity—界面劫持；Content Provider—数据泄露/SQL注入；Broadcast Receiver—广播伪造；Service—未授权调用）。提到同类考点还问到“地图导航类应用的最小必要权限（位置、存储）”。

”以及“SQL注入由Content

Provider组件引起”、“移动应用加固应包含防反编译/防调试/防篡改/防窃取”，可作为补充。

【案例2】案例二：SSH 远程安全访问与服务加固配置

某单位需要对Linux服务器进行远程运维管理，要求使用加密的远程登录协议，并采用公钥认证方式替代口令登录。

题目给出一份SSH服务端配置文件的部分内容截图，其中若干安全相关配置项被留空，要求考生补全。

同时给出客户端生成密钥、上传公钥、设置文件权限的操作场景。

【问题】问题1：远程安全运维应使用什么协议？

问题2：SSH使用的是哪种密码体制？

问题3：在Linux中生成SSH的RSA密钥对使用什么命令？

问题4：SSH服务的默认端口是多少？

问题5：图中给出的是哪个配置文件？

问题6：使用公钥认证时，应把哪个文件上传到SSH服务器端？

问题7：为防止其他用户篡改 authorized_keys，应把该文件权限设置为多少（用数字表示）？

问题8：请把以下SSH服务安全配置补充完整：PasswordAuthentication ____ / PermitRootLogin ____ / PubkeyAuthentication ____

【参考答案】

问题1：SSH（Secure Shell）协议。它对传输的数据加密，可替代明文的Telnet、rlogin、rsh。

问题2：公钥密码体制（即非对称密码体制，答“非对称密码体制”同样正确）。教材P46密码体制分类中，公钥密码体制又称非对称密码体制。

问题3：ssh-keygen。完整写法如 ssh-keygen -t rsa -f ./id_rsa -N ''（-t 指定算法，-f 指定输出文件，-N 指定私钥口令为空）；只写 ssh-keygen 亦可得分。

问题4：22（TCP 22端口）。

问题5：SSH服务端主配置文件 /etc/ssh/sshd_config（注意必须带字母d；/etc/ssh/ssh_config 是客户端配置文件，写错不得分）。

问题6：公钥文件 id_rsa.pub（上传后追加写入服务器端用户家目录下的 ~/.ssh/authorized_keys；也可用 ssh-copy-id 自动完成）。

问题7：600（即 -rw-----，仅属主可读写；.ssh 目录本身应为 700。若权限过松，sshd 会拒绝使用该公钥）。

问题8：PasswordAuthentication no# 禁止口令登录（仅允许公钥登录）；PermitRootLogin no# 禁止root直接远程登录；PubkeyAuthentication yes# 启用公钥认证。若按另一的三项：PermitRootLogin no、PermitEmptyPasswords no（不允许空口令登录）、PasswordAuthentication no（关闭口令验证，改用密钥）。

【解析】

本案例为SSH安全加固送分题，核心是“公钥认证 + 禁口令 + 禁root直登 + 严格文件权限”四件套。注意两份对问题8的填空项记录不一致（一份为 PasswordAuthentication/PermitRootLogin/PubkeyAuthentication，另一份为 PermitRootLogin/PermitEmptyPasswords/PasswordAuthentication），且第二份还把 PasswordAuthentication 填为 YES，与安全加固目标矛盾，此处以“关闭口令认证、启用公钥认证”的标准加固答案为准，填空项组合。

【案例3】案例三：流量分析与命令注入漏洞取证

某安全设备抓取到如下流量（题目给出Wireshark抓包截图及包详情，此处为文字概要）：

192.168.133.1 -> 192.168.133.130 /vulnerability/exec/HTTP/1.1（POST请求）

192.168.133.130 -> 8.8.8.8 ICMP request

8.8.8.8 -> 192.168.133.130 ICMP reply

8.8.8.8 -> 192.168.133.130 ICMP reply

192.168.133.130 -> 8.8.8.8 ICMP request

8.8.8.8 -> 192.168.133.130 ICMP reply

192.168.133.130 -> 192.168.133.1 HTTP/1.1 200 OK

题目另给出一段PHP源码截图（对用户提交的ip参数未做过滤，直接拼接进执行ping命令），以及Snort/告警规则片段。

shell_exec/system

【问题】问题1：这是什么安全设备抓取到的流量？

问题2：受害者（被攻击主机）的IP是什么？

问题3：要过滤出图中数据包，Wireshark过滤规则怎么写？

问题4：用iptables写一条规则禁止该攻击IP访问。

问题5：该攻击的类型是什么？

问题6：结合PHP代码，判断服务端操作系统上被执行了哪些命令？（多选：ping / netstat / ifconfig / whoami / id / ls）

问题7：漏洞（告警）所在的文件目录路径是什么？

问题8：受害主机的操作系统是Linux还是Windows？

问题9：Snort规则中用于显示告警信息的选项是哪个？（A.msg B.pass C.log D.content）

【参考答案】

问题1：IDS（入侵检测系统）。教材P311-312明确“陷阱网络的数据捕获设备是IDS”，蜜罐只负责诱骗、不负责数据捕获。若按第一份的四个选项（NTA/SIEM/Firewall/Honeypot）作答，则应选

A. NTA（网络流量分析），因为NTA才是以全流量镜像采集为职责的设备；两份选项不同、答案分歧，考场原题以给出的选项为准。

问题2：192.168.133.130（Web服务器，被注入命令后主动向8.8.8.8发起ICMP请求，是受害者）。攻击者为192.168.133.1。

问题3：ip.addr == 192.168.133.130（所有相关报文均含该地址，一条规则即可过滤出全部；也可写ip.addr==192.168.133.1 && ip.addr==192.168.133.130 只看攻击会话）。

问题4：iptables -I INPUT -s 192.168.133.1 -j DROP（在受害主机本机上拦截）。若判断中间还有一台设备做转发/受害主机为Windows不支持iptables，则应写在中间设备上并使用FORWARD链、且用 -I 插到最前：iptables -I FORWARD -s 192.168.133.1 -d 192.168.133.130 -p tcp --dport 80 -j DROP。注意用 -I 而非 -A，避免被前面已存在的放行规则抢先匹配。

问题5：命令注入（操作系统命令注入漏洞）。安全从业者常备 RCE（远程命令执行）；按教材P248 CNNVD漏洞分类框架，标准表述为“操作系统命令注入漏洞”，两种答法均可。

问题6：ping 和 whoami（从流量中可见对 8.8.8.8 的ICMP请求，说明执行了ping；从HTTP响应内容/代码可见执行了whoami回显当前用户）。

问题7：/vulnerability/exec/（直接照抄抓包首行URL中的路径即可）。

问题8：Linux。第一份答Linux；第二份考生答Windows并自评“应该是做错了，ping结果跟Linux是一样的”，说明现场判断依据（ping参数-c、命令回显格式、www-data属主等）不明确。若代码中用到 ping -c 或文件属主为www-data，则应判为Linux。

问题9：A（msg）。msg用于指定告警时输出的描述信息；pass/log是规则动作，content是载荷匹配选项。

【解析】

本案例为典型的“流量取证 + 代码审计 + 处置加固”综合题，答题主线：从抓包时序判断谁是受害者（谁主动外联）→ 写Wireshark过滤表达式 → 结合PHP代码定位命令注入 → 判断被执行的系统命令 → 用iptables封堵源IP。加固措施应答：对用户输入做白名单校验与转义、避免使用system/shell_exec拼接、使用参数化API、以最低权限账号（如www-data）运行Web服务、部署WAF。注：中同类命令注入案例还问到“HTTP请求方法为POST”、

“编码类型为 application/x-www-form-urlencoded”、“文件属主用户组为 www-data”，可作补充，但该文网段与本题不同，疑非同一套题。

【案例4】案例四：Windows 操作系统账户与日志安全

题目给出Windows系统安全子系统架构图（含 Winlogon、Lsass、Msv1_0.dll、Kerberos.dll、SAM服务器、LSA、Netlogon、活动目录等模块）并给出一张SAM文件（注册表项）的权限/访问控制列表截图，以及Windows事件日志相关截图。要求结合Windows身份认证与审计机制回答问题。

- 【问题】问题1：负责给用户提供Windows登录交互界面的组件是什么？
问题2：存储用户身份（账户与口令散列）信息的是什么？
问题3：应用日志、系统日志、安全日志分别对应哪些日志文件（名称）？
问题4：表示“登录失败”的Windows安全事件ID是多少？
问题5：访问控制列表（ACL）属于基于行还是基于列的访问控制策略？
问题6：根据图中SAM文件的权限信息，写出其访问控制列表。
问题7：打开系统“事件查看器”的命令是什么？
问题8：查看当前在线/本机用户的命令是什么？

【参考答案】

问题1：Winlogon（配合登录界面组件 LogonUI.exe / 早期的 GINA 动态库）负责提供交互式登录界面并把凭据交给 Lsass 校验。

问题2：SAM（Security Account Manager，安全账户管理器数据库，文件位于 %SystemRoot%\System32\config\SAM，对应注册表 HKEY_LOCAL_MACHINE\SAM）。域环境下为活动目录（AD）中的 NTDS.dit。

问题3：应用日志 → Application（AppEvent.Evt / Application.evtx）；系统日志 → System（SysEvent.Evt / System.evtx）；安全日志 → Security（SecEvent.Evt / Security.evtx）。

问题4：4625（登录失败）。对应的登录成功事件ID为4624；旧版（Windows 2003及以前）失败为529/一。

问题5：基于列（Column-based）的访问控制策略。ACL是“挂在客体（资源）上、列出各主体权限”的表示方式，属于访问控制矩阵按列存储；按行存储则是能力表（Capability List）。

问题6：按图中条日照写，典型形式为：SYSTEM—完全控制（Full Control）；Administrators—完全控制/读取；其他普通用户与组—无任何权限（SAM表默认只有SYSTEM可访问，连Administrator默认也无权直接读取，需提权或借助工具）。

问题7：eventvwr.msc（或 eventvwr）。

问题8：net user（查看本机所有账户）、whoami（查看当前登录身份）；查看当前登录会话可用 query user / quser。

【解析】

本案例考查Windows安全体系：Winlogon/LSASS/SAM

认证链路、三大事件日志与关键事件ID（4624成功/4625失败）、ACL的“基于列”本质、常用管理命令。还涉及“隐藏账户”：用 net user test\$ 123456 /add 创建以\$结尾的隐藏用户后，net user 无法列出，需用 lusrmgr.msc（本地用户和组）查看；账户克隆需在 HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users 下复制 Administrators 项的 F 值，可作为补充要点。

【案例5】案例五：网络安全体系结构与“进不来、拿不走、改不了”

题目围绕OSI安全体系结构（ISO 7498-2）的安全服务与安全机制对应关系设问并给出通俗的安全目标口诀“进不来、拿不走、改不了、看不懂、跑不了”，要求映射到具体安全服务/机制/设备。另给出一组安全产品分类（网络型、Web应用型、主机型/终端防护型、数据库型），要求判断iptables的归类。

【问题】问题1：保密性要求对应什么安全机制？

问题2：不可否认性对应什么安全机制？

问题3：“进不来”对应于什么设备/机制？

问题4：“拿不走”对应于什么安全要素？（四选一：授权、审计、身份认证、____）

问题5：给出网络型、Web应用型、主机型（终端防护、数据库型）等分类，iptables对应于哪些类型？（多选）

问题6：“改不了”对应于什么安全机制？

问题7：“改不了”所依赖的核心算法是什么？

问题8：在Ubuntu中计算文件MD5值的命令是什么？

【参考答案】

问题1：加密机制（Encipherment）。对应机密性/保密性安全服务。

问题2：数字签名机制（Digital Signature）。对应抗抵赖（不可否认）安全服务。

问题3：防火墙（对应访问控制机制/访问控制服务）——阻止未授权主体进入受保护网络。

问题4：授权（访问控制）。“拿不走”即通过授权与访问控制限制主体对客体的读取/导出权限（与之配套的还有数据防泄漏DLP）。

问题5：网络型

和

主机型（多选）。iptables是Linux内核netfilter的包过滤规则管理工具，既在网络层实施包过滤（网络型），又运行在主机之上保护本机（主机防火墙，主机型）。

问题6：（数据）完整性机制 / 完整性服务。

问题7：哈希（散列）算法，如MD5、SHA-1/SHA-256、SM3；用于生成消息摘要以校验数据是否被篡改。

问题8：md5sum（如 md5sum filename；SHA系列对应 shasum、sha256sum）。

【解析】

本案例是ISO

7498-2安全服务与安全机制对应关系的直接考查，属于必得分题。建议牢记五大安全服务与八大安全机制的映射：鉴别—鉴别交换/加密；访问控制—访问控制机制；数据机密性—加密/路由控制；数据完整性—数据完整性/数字签名；抗抵赖—数字签名/公证。口诀映射：看不懂→加密；进不来→防火墙/访问控制；拿不走→授权与访问控制；改不了→完整性（哈希）；跑不了→审计与追踪。

【案例6】案例六：DES算法 S盒计算与填充

阅读下列说明，回答问题1至问题6。

题目给出DES算法某个S盒的数据表，表中有4处数据空缺，标记为(1) (2) (3) (4)。

并给出DES算法整体结构图（含初始置换IP、16轮迭代、逆初始置换IP⁻¹等操作部件）。

【问题】问题1（4分）：已知DES算法S盒如下，请补全S盒空缺的数据(1) (2) (3) (4)。

问题2（2分）：已知S盒的输入为 110011，请计算经过S盒变换之后的二进制输出。

问题3（3分）：使用DES算法对明文字符串“12345”进行加密，应当对明文进行填充，请问填充后的数据长度是多少比特（位）？并给出填充后的明文字符串表示。

问题4（2分）：如果使用密钥“\x01\x01\x01\x01\x01\x01\x01\x01”对明文进行加密，会出现什么安全问题？

问题5（2分）：不论古典密码还是现代密码，其中最为核心的操作是替代和置换，对应于香农《保密系统的通信理论》论文中的哪两种密码技术？

问题6（2分）：在DES算法中，置换对应下图中哪个操作部件？

【参考答案】

问题1: (1)3(2)13(3)15(4)0。解法: DES的S盒每一行都是0~15的一个排列, 逐行检查缺哪个数字就填哪个。

问题2: 0110。解法: 输入6位 110011, 取首位和末位组成 11 → 十进制3, 作为行号; 取中间四位 1001 → 十进制9, 作为列号; 查该S盒第3行第9列(均从0开始计数)得到6, 转为4位二进制即 0110。

问题3: 填充后数据长度为 64 比特(8字节, 即DES的一个分组长度)。明文“12345”为5字节, 按PKCS#5/PKCS#7填充需补3字节、每字节值为0x03, 故填充后表示为“12345\\x03\\x03\\x03”。

问题4: 该密钥所有字节相同(全为0x01), 属于弱密钥/低熵密钥, 密钥空间极小, 极易被暴力破解或字典猜测; 且DES本身有效密钥仅56位(每字节最低位为奇偶校验位), 此类规律性密钥进一步降低安全性。应使用密码学安全随机数生成器产生密钥。

问题5: 混乱(Confusion, 对应替代/S盒)与扩散(Diffusion, 对应置换/P置换与移位)。

问题6: 初始置换(IP)与逆初始置换(IP⁻¹, 末置换); 轮函数内部还有扩展置换E与P置换。

【解析】

因此本条应视为高质量的DES算法练习题, 而非2025年真题。

【案例7】案例七: Wireshark 完全连接扫描分析与 iptables 防护

阅读下列说明, 回答问题1至问题7。

题目给出一张Wireshark抓包截图: 源主机 192.168.85.129 向目标主机 192.168.85.132 的大量端口发起TCP连接 其中绝大多数端口回复 RST/ACK, 只有80端口完成了完整的三次握手(SYN / SYN, ACK / ACK)。

【问题】问题1(2分): 根据Wireshark流量包写出扫描源地址。

问题2(2分): 要产生如图流量包视图, 请写出Wireshark过滤规则。

问题3(3分): 根据流量包分析目标系统开放了哪些端口, 并说明理由。

问题4(2分): 此流量包属于什么类型的扫描?

问题5(2分): 抓包截图中有很多RST/ACK分组, 写出RST/ACK分组的TCP标志位值(十六进制)是多少?

问题6(2分): 若使用iptables过滤该扫描, 需要用到filter表的哪条链?

问题7(2分): 写出一条基于源地址防止该扫描的iptables规则。

【参考答案】

问题1: 192.168.85.129(看第一个包的源地址及Info列即可确认)。

问题2: `ip.addr==192.168.85.129 && ip.addr==192.168.85.132`(只保留这两台主机之间的会话)。

问题3: 开放了80端口。理由: 只有80端口完成了完整的TCP三次握手(SYN → SYN, ACK → ACK); 其余端口目标主机直接回复 RST/ACK, 表明端口关闭。

问题4: 完全连接扫描(TCP Connect扫描)。因为扫描方对开放端口完成了完整三次握手(若只发SYN收到SYN/ACK后即发RST, 则为半连接/SYN扫描)。

问题5: 0x14。RST/ACK即 `ACK(0x10) + RST(0x04)`, 标志位字节为 `00010100b = 0x14`。

问题6: INPUT链(流量由外部进入本机, 属于filter表的INPUT链; 若本机为转发设备则用FORWARD链)。

问题7: `iptables -A INPUT -s 192.168.85.129 -d 192.168.85.132 -p tcp -j DROP`(更稳妥可用 `-I` 插入到规则链最前; 也可结合 `-m limit / recent` 模块做扫描频率限制而非全封)。

【解析】

技术要点仍然重要: 完全连接扫描 vs 半连接扫描的流量特征区分、TCP标志位十六进制换算(FIN=0x01, SYN=0x02, RST=0x04, PSH=0x08, ACK=0x10, URG=0x20)、iptables五链四表与规则插入顺序。

【案例8】案例八: 省级政务平台边界安全架构升级——STRIDE/防火墙ACL/IPS漏报/零信任/

DDoS

某省级政务服务平台2025年启动边界安全架构升级项目。当前平台覆盖省、市、县三级共127个政务部门业务系统，对外提供342项公共服务事项，对接公安、民政、人社等多个涉密/敏感政务子系统。

此前多次出现针对平台边界的SQL注入、流量型DDoS攻击。原有边界采用传统“防火墙+WAF”的两层防护架构，漏报率高达17%，不符合等保2.0三级的最新防护要求。

本次升级要求引入IPS、零信任访问控制组件、云抗D防护集群，构建“云-网-端”一体化的边界防护体系。

【问题】问题1（6分）：项目组采用STRIDE威胁模型对升级后的边界架构做威胁建模，请分别写出STRIDE六个字母对应代表的威胁类型名称，并指出其中哪两类威胁可以通过部署数字签名机制直接实现防护。

问题2（4分）：运维人员配置边界防火墙ACL规则时，先后设置了5条规则：①允许所有源地址访问目标端口80/443；②拒绝所有源地址访问目标端口22、3389；③允许政务内网段/8访问所有业务端口；④拒绝所有地址访问管理后台端口9090；⑤默认拒绝所有流量。上线后发现政务内网用户无法正常访问管理后台的运维端口，请指出规则配置的两处错误，并给出调整后的正确规则排序逻辑。

问题3（4分）：平台部署入侵防御系统（IPS）后，实测发现针对政务业务系统的变种SQL注入攻击存在11%的漏报率，请列出至少3项导致IPS漏报的核心技术原因，并给出对应的优化落地措施。

问题4（3分）：本次升级引入零信任访问控制架构替代传统的“基于网络位置信任”的边界防护逻辑，请结合该政务平台场景，说明零信任“持续验证、永不信任”原则的3项落地核心要求。

问题5（3分）：平台面临峰值带宽达500Gbps的流量型DDoS攻击风险，请说明“云清洗中心-本地抗D设备-服务器端流量清洗插件”三级DDoS防护体系的协同部署逻辑。

【参考答案】

问题1：STRIDE六类威胁为——S: Spoofing 身份假冒（仿冒）；T: Tampering 篡改；R: Repudiation 抵赖（否认）；I: Information Disclosure 信息泄露；D: Denial of Service 拒绝服务；E: Elevation of Privilege 权限提升。其中可通过部署数字签名机制直接防护的两类是 T（篡改）与 R（抵赖）：数字签名基于哈希摘要保证数据完整性，可发现任何篡改；基于签名者私钥的唯一性提供不可否认证据，防止抵赖。（注：数字签名同时也能辅助对抗S身份假冒，但直接对应的标准答案是T与R。）

问题2：两处错误——错误一：规则③“允许政务内网段访问所有业务端口”被排在规则②之后，而②已“拒绝所有源地址访问22、3389”，防火墙ACL按自上而下首次匹配即生效，内网运维流量先被②拒绝，③永远不生效；错误二：规则④“拒绝所有地址访问管理后台端口9090”未对政务内网做例外放行，且排在任何允许内网访问9090的规则之前，导致合法运维访问被一律阻断（同时规则①“允许所有源地址访问80/443”过于宽松，未做最小化限定）。正确排序逻辑：遵循“具体规则在前、通用规则在后；允许例外在前、拒绝在后；默认拒绝置于末尾”——①

允许政务内网段访问管理后台9090及22/3389运维端口（源地址最小化到运维网段/跳板机IP）；②

拒绝其他所有源地址访问9090、22、3389；③ 允许所有源地址访问对外服务端口80/443；④ 按需放行其他业务端口；⑤ 默认拒绝所有流量（deny any any）。

问题3：漏报核心原因与优化措施——（1）

特征库滞后：IPS依赖已知攻击特征签名，对变种/0day SQL注入（编码变形、注释拆分、大小写混淆、宽字节）无匹配规则。措施：建立特征库自动更新机制（≤24小时）、订阅威胁情报、补充正则化的泛化规则。（2）

检测机制单一，仅做单包特征匹配：攻击载荷被分片、分段传输或跨多个报文时无法还原。措施：启用协议还原与流重组、开启会话级深度检测（DPI/DFI）、启用URL/参数解码归一化（多重URL解码、Base64、Unicode解码）。（3）

加密流量不可见：HTTPS流量未解密，IPS无法检查载荷。措施：部署SSL/TLS卸载或解密代理，在解密后再送IPS检测。（4）

检测性能与策略配置问题：大流量下超过设备处理能力触发旁路（fail-open），或阈值/灵敏度设置过低、部分规则未开启阻断模式。措施：按峰值容量选型扩容、启用旁路告警、将高危规则由“告警”改为“阻断”、结合基线做异常行为检测与AI模型辅助。（5）单点检测缺乏纵深。措施：IPS与WAF、RASP、数据库审计联动，形成多层交叉检测。

问题4：零信任落地3项核心要求——（1）

以身份为中心的强身份认证与动态授权：所有政务部门用户、设备、应用均需唯一可信身份，统一身份认证（IAM/SSO）+

多因素认证（MFA），访问决策不再基于“是否在内网”，而基于身份、设备安全状态、访问上下文实时计算信任分并动态授权；(2)

最小权限与微隔离：按业务事项和岗位职责细粒度授权到“用户-应用-接口”级别，127个部门业务系统之间实施微隔离，涉密/敏感子系统单独隔离域，禁止横向自由访问，默认拒绝、按需放行；(3)

持续验证与全程审计：会话建立后仍持续采集设备指纹、地理位置、访问轨迹、行为基线等信号做周期性再评估，一旦信任分下降（异地登录、设备失陷、异常批量下载）立即降权、二次认证或阻断会话；全部访问行为集中日志审计、可溯源，日志留存≥6个月。

问题5：三级DDoS防护协同部署逻辑——(1)

云清洗中心（第一级，抗大流量）：部署在运营商/云厂商侧，具备T级清洗带宽。平时通过BGP路由/DNS调度将业务流量牵引监测，当检测到流量超过本地链路阈值（如超过本地带宽的70%或达数十Gbps）时，自动触发BGP引流把500Gbps级攻击流量牵引至云端清洗，清洗后的干净流量通过GRE隧道/专线回注给平台，从而避免攻击流量打满本地出口链路——这是应对500Gbps峰值的唯一有效手段。(2)

本地抗D设备（第二级，精细清洗）：部署在平台互联网出口内侧，负责清洗云端未拦净的中小流量攻击和协议层攻击（SYN Flood、ACK Flood、UDP反射、CC攻击），基于连接数/速率阈值、源认证（SYN Cookie）、指纹学习做精细过滤，并向云清洗中心上报攻击态势，联动触发引流。(3)

服务器端流量清洗插件（第三级，应用层兜底）：以Agent/模块形式部署在Web服务器与应用侧，针对慢速攻击（Slowloris）、HTTP

CC、业务接口滥刷等应用层攻击，做人机校验（验证码/JS挑战）、会话频率限制、URL级限流与业务优先级保障。(4)

协同机制：三级之间共享攻击特征与黑名单，统一由安全运营中心（SOC）做态势感知与策略联动，形成“云端抗量、本地抗协议、端侧抗业务”的分层递进防护，并预先编制引流演练与业务降级预案，保障大流量攻击下核心政务服务可用。

【解析】

其分值构成（案例一20分、案例四18分）与真考（4大题、每题约19分、合计75分）不符，场景数据（127个部门、342项事项、漏报率17%/11%、500Gbps）过于工整，且与三份记录的五大题完全不重合。技术要点（STRIDE六类、ACL首次匹配顺序、IPS漏报原因、零信任落地、DDoS三级防护）本身均为教材范围内的高价值考点，可作为练习使用，但不应作为2025年11月真题看待。

【案例9】案例九：高校选课系统冰蝎WebShell入侵应急响应与溯源

某省属本科高校在2025年全国网络安全攻防演练期间，蓝队运维人员通过EDR告警发现一台对外提供服务的选课系统Web服务器存在异常外联行为。

经初步排查，该服务器已被攻击者植入冰蝎（Behinder）WebShell，攻击者正在尝试通过该服务器横向渗透校内教务系统域控服务器。

最终排查发现攻击者已下载存储在该Web服务器上的12万条学生个人信息，事件被判定为一般网络安全事件。

【问题】问题1（4分）：按照《信息安全技术 信息安全事件处置指南》GB/T 20986-2023的要求，标准应急响应流程分为7个核心阶段，请写出7个阶段的完整名称，并说明在遏制阶段处置该Web服务器冰蝎WebShell入侵事件的3项核心操作要求。

问题2（4分）：攻击者拿到Web服务器权限后采用Pass-the-Hash（哈希传递）技术开展内网横向移动，请说明该攻击技术的实现原理，以及蓝队可部署的3项针对性检测措施。

问题3（5分）：蓝队完成攻击事件遏制之后开展溯源分析工作，请说明从Web访问日志到域控安全日志的完整攻击链溯源分析路径，以及最终输出的攻防演练事件溯源报告必须包含的5项核心要素。

问题4（5分）：按照《网络安全事件报告管理办法》要求，本次事件排查发现攻击者已下载12万条学生个人信息，判定为一般网络安全事件，请说明该事件的上报要求，以及事件闭环整改的核心工作流程。

【参考答案】

问题1：7个阶段为——准备阶段、检测阶段、遏制阶段、根除阶段、恢复阶段、跟踪（跟进）阶段、总结阶段。遏制阶段3项核心操作要求：(1)

立即断开该选课系统Web服务器的外部网络访问（或加入隔离VLAN），同时完整保留服务器运行状态与原始日志证据，禁

止直接重启或关机，避免内存中的恶意代码痕迹、网络连接与进程信息丢失（冰蝎为内存加密马时更需先做内存取证）；
(2) 临时将选课业务切换至备用/灾备环境，保障学生正常选课业务连续性；(3)
在边界防火墙上封禁已确认的全部攻击源IP及C2外联地址，阻断攻击者后续访问与数据外传通道，并立即修改该服务器及
域内相关账号口令、吊销可疑会话票据。

问题2：哈希传递（Pass-the-Hash）原理：攻击者获取Windows主权限后，从LSASS进程内存或SAM数据库中dump出账号
的NTLM哈希值；由于NTLM认证协议在质询-响应过程中直接使用口令哈希参与运算、并不校验明文口令，攻击者无需破解
出明文密码，即可携带该哈希向域内其他主机的SMB/WMI/RDP等服务发起认证，从而以该账号身份横向登录并执行命令（
若拿到域管哈希则可直接控制域控）。3项针对性检测措施：(1)

日志与行为检测：集中采集域控与主机的安全日志，重点监控事件ID

4624（登录成功）中登录类型为3（网络登录）且认证包为NTLM、LogonProcessName为NtLmSsp的异常记录，以及同一账号
在短时间内从多台主机异地登录、非管理终端发起的管理员登录等异常模式；(2)

终端侧检测：部署EDR监控对
lsass.exe 的可疑内存读取/句柄打开行为（mimikatz、procdump、comsvcs.dll 转储），检测可疑的
sekurlsa、DCSync、WMI/PsExec 远程执行行为；(3)

网络侧检测：在核心交换镜像流量上检测异常SMB/NTLM认证流量（同一源IP短时间对大量主机的445端口认证、认证失败
率突增），并结合微隔离限制工作站之间的445/135/3389横向互访。补充加固：启用Kerberos替代NTLM并禁用NTLMv1、部
署LSA

Protection（RunAsPPL）与Credential
Guard、限制本地管理员账号网络登录（LocalAccountTokenFilterPolicy）、使用LAPS随机化本地管理员口令、域管账号
仅在专用特权终端使用。

问题3：完整溯源路径——(1) 从Web访问日志（access.log /
IIS日志）入手，按告警时间窗口检索异常请求：定位WebShell文件的访问记录（固定URL、异常长POST体、无Referer、U
ser-Agent固定或异常）、确认冰蝎流量特征（AES加密载荷、Content-Type固定、Accept头特征），回溯首次成功访问该
文件的时间与源IP，确定攻击入口点；(2)

结合Web中间件错误日志、上传目录文件时间戳（mtime/ctime）与WAF日志，还原上传WebShell所利用的漏洞（文件上传
、反序列化、命令注入等）及利用时间线；(3)

分析Web服务器主机日志与EDR记录：进程树（web进程派生cmd/powershell）、可疑外联连接（C2地址与端口）、新增计
划任务/服务/账号、凭据dump工具落地痕迹，确认提权与凭据窃取行为；(4)

顺着被窃取的账号，在内网流量与主机日志中追踪横向移动路径：445/3389/WMI连接记录、跳板主机上的登录与命令执行
痕迹；(5) 在域控安全日志中检索该账号相关的

4624（登录成功，尤其登录类型3的NTLM登录）、4625（失败）、4768/4769（Kerberos票据申请）、4672（特权分配）、
4726/4720（账号变更）、DCSync相关的目录服务访问事件，确认攻击者是否成功登录域控、执行了哪些操作；(6)

结合数据库审计与文件访问审计，确认12万条学生个人信息的导出时间、导出方式与外传通道，形成从“入口—提权—横
移—域控—数据窃取—外传”的完整攻击链闭环。溯源报告必须包含的5项核心要素：①

事件基本情况（发现时间、发现方式、受影响资产范围、事件定级）；②

攻击者画像与攻击来源（源IP、归属地、C2域名/IP、使用的工具与TTPs、是否可关联到已知攻击组织）；③

完整攻击时间线与攻击路径（各阶段时间点、利用漏洞、横向移动路径图）；④

影响与损失评估（被控主机清单、泄露数据类型与数量12万条学生个人信息、业务中断时长、合规风险）；⑤

处置过程与整改建议（已采取的遏制/根除/恢复措施、残余风险、漏洞修复与加固方案、责任与后续改进计划）。另可含
证据清单与取证哈希，保证证据链完整可采信。

问题4：上报要求——(1)

时限与对象：一般网络安全事件应在发现后按《网络安全事件报告管理办法》规定的时限（一般事件为发现后24小时内，
较大及以上事件需1小时内）向属地网信部门及行业主管部门（教育主管部门）报告；因涉及12万条个人信息泄露，还应
同步向属地公安机关网安部门报告，并依据《个人信息保护法》第五十七条立即采取补救措施、及时通知履行个人信息保
护职责的部门和受影响的学生个人；(2)

报告内容：事件发现时间与经过、涉事系统与单位、事件初步定级与判定依据、已造成的危害（12万条学生个人信息被下
载）、已采取的处置措施与效果、事件原因初步分析、后续处置计划与联系人；(3)

续报与结报：处置过程中如事态升级（如确认域控失陷、数据被公开售卖）应立即续报并重新定级；处置完成后按要求提
交结案报告。闭环整改核心工作流程：①

根除与验证——彻底清除WebShell及所有后门（计划任务、服务、账号、内存马），修补被利用漏洞，重置全域相关账号口令与Kerberos krbtgt票据，并通过复扫与人工核查验证无残留；②
恢复与观察——从可信备份重建或加固后上线选课系统，恢复域内正常服务，设置观察期加强监控，确认无再次入侵迹象后转入常态运行；③
原因分析与责任认定——组织复盘，明确技术原因（漏洞管理缺失、日志与监测不足、内网未隔离、凭据保护缺失）与管理原因（上线未做安全测试、运维职责不清），认定责任；④
制定整改方案并跟踪落实——形成整改任务清单（漏洞修复、WAF/RASP部署、微隔离、EDR全覆盖、日志集中审计留存≥6个月、个人信息加密存储与脱敏、最小权限与特权账号管理、备份与容灾），明确责任人与完成时限，逐项验收销项；⑤
制度与能力建设——修订应急预案并开展应急演练与全员安全意识培训，将本次事件的IOC与检测规则沉淀入安全运营平台；⑥
总结归档与报告——编制事件总结报告与整改验收报告，报送主管部门，完成事件闭环。

【解析】

但其考点（GB/T

20986应急响应7阶段、冰蝎WebShell处置、Pass-the-Hash原理与检测、攻击链溯源、个人信息泄露事件上报与闭环整改）均为软考信息安全工程师下午题的高频方向，具备练习价值。注意：教材常考的应急响应模型还有PDCERF六阶段（准备、检测、抑制/遏制、根除、恢复、跟踪总结），作答时需看清题目引用的是哪个标准。

附录 考试说明与备考提示

一、科目与考试安排

信息安全工程师属于计算机技术与软件专业技术资格（水平）考试（软考）中级资格。

开考规律：该科目仅在每年下半年（11月）开考，上半年中级科目不含信息安全工程师。

考试科目：上午《基础知识》（综合知识，原75道单选题，含71-75英语完形）、下午《应用技术》（案例分析）。

合格标准：两科均为45分及以上（满分75，相对固定合格线为满分60%），须一次通过，成绩不保留。

考试形式：全国统一机考（分批次）。发证：人力资源和社会保障部、工业和信息化部。

二、真题性质与题量说明

本册真题为非官方公布的整理内容，答案经交叉核对，供练习参考。

题量差异说明：因各年真题完整性不同，综合知识收录题量不一（2023年71题、2024年30题、2025年70题）；案例分析以可确证内容为准。

2024下半年综合知识仅确证30题，题31-70及英语完形因各版本彼此冲突、混有旧大纲与模拟题，未采信，故未收录。

案例分析题无公开标准答案，本册答案为基于考点的参考作答，仅作参考。

三、备考提示

综合知识重点：密码学（SM系列国密算法、PKI/CA、对称与非对称）、网络安全（防火墙/IDS/IPS/VPN、DDoS、Web安全）、系统安全（Linux/Windows加固、访问控制模型BLP/Biba、可信计算）、应用安全（安卓/iOS、逆向、Web防护）、安全管理与法规（等保2.0、ISO27001、网络安全法、密码法）。

应用技术重点：STRIDE威胁建模、防火墙/ACL配置、入侵检测与防御（IPS漏报分析）、零信任架构、DDoS防护体系、密码应用（DES的S盒、密钥管理）、流量分析（Wireshark过滤与命令注入识别）、SSH安全配置、Android应用安全。

复习建议：以官方教程与历年真题为主，选择题抓考点记忆，案例题练「读题—建模—分点作答」的答题节奏，注意答题纸分栏对应。