

CISP-IRE

热门考试试题

注册信息安全应急响应工程师 精选100题

题型：一、单选题 二、多选题 三、判断题

每道题均含：正确答案 + 详细解析 + 难度说明

整理日期：2026年06月25日

本资料仅供学习参考，不构成考试承诺

目 录

- 一、单选题（共 58 题） （第 1~58 题）
- 二、多选题（共 37 题） （第 59~95 题）
- 三、判断题（共 5 题） （第 96~100 题）

一、单选题（共 58 题）

1. CISP-IRE中的'IRE'代表的含义是？

- A. 信息安全研究工程师
- B. 信息安全应急响应工程师
- C. 信息安全风险评估工程师
- D. 信息安全审计工程师

答案：B 易

解析：

CISP-IRE（Certified Information Security Professional - Incident Response Engineer）即注册信息安全应急响应工程师，专注于安全事件的应急响应与处置能力。

2. 信息安全应急响应的主要目标不包括以下哪一项？

- A. 快速遏制安全事件
- B. 彻底消除攻击根因
- C. 完全避免所有攻击再次发生
- D. 恢复业务正常运行

答案：C 易

解析：

应急响应无法保证完全避免所有攻击再次发生，其目标是快速响应、遏制、根除、恢复，并通过总结改进持续提升安全能力。

3. 应急响应工作遵循的核心原则是？

- A. 先恢复业务，再调查取证
- B. 先遏制扩散，再根除根因
- C. 先追责定责，再恢复系统
- D. 先发布公告，再内部处置

答案：B 易

解析：

应急响应强调'先止血再治病'：优先遏制事件影响范围，防止进一步扩散，随后再进行根因分析与根除。

4. PDCERF应急响应模型中，'P'代表的阶段是？

- A. 准备（Preparation）
- B. 检测（Detection）
- C. 保护（Protection）
- D. 策略（Policy）

答案：A 易

解析：

PDCERF模型包括：Preparation（准备）、Detection（检测）、Containment（遏制）、Eradication（根除）、Recovery（恢复）、Follow-up（跟踪总结）。

5. 应急响应过程中，‘遏制’阶段的首要任务是？

- A. 彻底删除所有恶意代码
- B. 防止事件影响范围进一步扩大
- C. 恢复受损的业务系统
- D. 撰写事件报告并对外披露

答案：B 中

解析：

遏制阶段的核心是限制损害扩散，如隔离受影响主机、阻断恶意通信等，而非直接恢复或根除。

6. 在应急响应中，‘RTO’指标的含义是？

- A. 恢复点目标
- B. 恢复时间目标
- C. 最大可容忍中断时间
- D. 数据丢失量指标

答案：B 中

解析：

RTO（Recovery Time Objective）指恢复时间目标，即业务中断后必须恢复的最长时间；RPO（Recovery Point Objective）是恢复点目标。

7. 应急响应中‘RPO’指标主要用于衡量？

- A. 业务系统恢复所需时间
- B. 灾难发生时可接受的数据丢失量
- C. 应急响应团队响应速度
- D. 系统可用性百分比

答案：B 中

解析：

RPO衡量的是在灾难发生时，组织能够承受的数据丢失量，通常由备份策略和恢复点决定。

8. 网络安全事件根据影响程度通常分为特别重大、重大、较大和一般四级，其划分依据不包括？

- A. 影响范围
- B. 危害程度
- C. 攻击者国籍
- D. 社会影响

答案：C 中

解析：

事件分级依据影响范围、危害程度、社会影响等客观因素，而非攻击者国籍。

9. 应急响应预案制定的第一步通常是？

- A. 编写具体处置流程
- B. 明确应急组织架构和职责分工

- C. 采购安全设备
- D. 开展攻防演练

答案: B 易

解析:

预案制定首先应明确组织架构、职责分工和沟通机制, 确保事件发生时有人决策、有人执行。

10. 应急响应工具包中, 不属于取证工具的是?

- A. FTK Imager
- B. Wireshark
- C. Volatility
- D. Nmap

答案: D 中

解析:

Nmap主要用于网络扫描和资产发现, 而FTK

Imager用于磁盘镜像, Wireshark用于流量分析, Volatility用于内存取证。

11. 应急响应演练的主要目的是?

- A. 考核员工绩效
- B. 检验预案可行性和团队协作能力
- C. 展示安全设备功能
- D. 完成合规检查

答案: B 易

解析:

演练旨在检验预案的可操作性、团队协作能力和资源调配能力, 并发现改进点。

12. 在制定应急响应计划时, 以下哪项不是关键考虑因素?

- A. 业务影响分析
- B. 关键资产清单
- C. 攻击者攻击手法的详细分析
- D. 可用资源和恢复优先级

答案: C 中

解析:

应急响应计划的核心是保障业务连续性。制定时应以业务影响分析(BIA)为基础, 识别关键资产、恢复优先级和可用资源。攻击手法属于威胁情报输入, 可在预案附件或处置SOP中补充, 而非计划制定的首要考虑。

13. 应急响应通讯录中应优先包含哪些人员?

- A. 仅安全团队负责人
- B. 安全团队、IT运维、业务负责人、法务及公关联系人
- C. 仅一线运维人员
- D. 仅外部安全厂商

答案: B 易

解析:

应急响应需多部门协同, 通讯录应包含安全、运维、业务、法务、公关及外部支持人员。

14. IDS与IPS的主要区别是?

- A. IDS能检测入侵, IPS不能
- B. IPS能主动阻断攻击, IDS通常只检测告警
- C. IDS部署在内网, IPS部署在外网
- D. IPS只用于防火墙功能

答案: B 易

解析:

IDS (入侵检测系统) 主要检测并告警; IPS (入侵防御系统) 可实时阻断恶意流量。

15. SIEM的核心作用是?

- A. 直接阻断网络攻击
- B. 收集、关联和分析多源安全日志
- C. 提供VPN服务
- D. 替代防火墙

答案: B 中

解析:

SIEM (安全信息与事件管理) 聚合日志、关联事件、提供告警和可视化, 辅助检测与调查。

16. 威胁情报中的'IOC' 是指?

- A. 入侵检测系统
- B. 入侵指标
- C. 安全运营中心
- D. 漏洞扫描工具

答案: B 中

解析:

IOC (Indicator of Compromise) 即入侵指标, 如恶意IP、域名、文件哈希、URL等。

17. 下列哪项最可能是APT攻击初期的典型特征?

- A. 大量公开漏洞扫描
- B. 针对特定目标的鱼叉式钓鱼邮件
- C. 明显的勒索提示
- D. 大规模DDoS流量

答案: B 中

解析:

APT攻击通常具有针对性和隐蔽性, 鱼叉式钓鱼是常见初始入侵手段。

18. 网络流量分析的常见切入点不包括？

- A. 异常通信时间
- B. 未知外联IP
- C. 员工打卡记录
- D. 大流量异常传输

答案：C 中

解析：

员工打卡记录属于行政数据，不是网络流量分析的切入点。

19. 在日志分析中，'基线'的作用是？

- A. 记录所有攻击行为
- B. 提供正常行为的参照标准，便于发现异常
- C. 存储密码信息
- D. 替代备份系统

答案：B 中

解析：

基线代表正常行为模式，偏离基线的行为可能意味着异常或攻击。

20. 蜜罐技术的主要价值在于？

- A. 直接保护核心业务系统
- B. 诱捕攻击者并收集攻击行为数据
- C. 提升网络带宽
- D. 替代防火墙

答案：B 中

解析：

蜜罐通过模拟易受攻击目标吸引攻击者，用于捕获攻击行为、研究威胁和延缓攻击。

21. 当发现服务器被植入WebShell时，首选的遏制措施是？

- A. 直接删除WebShell文件
- B. 先隔离受影响主机，保留证据
- C. 立即重启服务器
- D. 通知所有用户修改密码

答案：B 中

解析：

应先隔离主机防止继续被利用，同时保留现场和证据用于后续分析，而非直接删除或重启。

22. 在勒索软件事件中，以下做法错误的是？

- A. 立即隔离受影响主机
- B. 从已知干净的备份恢复数据
- C. 优先支付赎金以快速恢复

D. 分析加密行为以阻止传播

答案: C 中

解析:

支付赎金不保证数据恢复, 且可能助长犯罪。应优先隔离、遏制、从备份恢复。

23. 横向移动的典型攻击特征不包括?

- A. 同一攻击者使用多个不同账户访问多台主机
- B. 使用Pass-the-Hash或票据传递
- C. 大量对内部网络的扫描
- D. 仅访问外部公开网站

答案: D 中

解析:

横向移动发生在内网, 表现为攻击者在多个内网主机间移动, 不会只是访问外部网站。

24. 发现内部主机大量对外发起异常连接, 最合理的初步处置是?

- A. 直接关闭该主机
- B. 在防火墙上限制该主机外联并隔离分析
- C. 通知用户继续使用
- D. 重新安装系统

答案: B 中

解析:

应限制外联并隔离分析, 既阻止进一步危害, 又保留证据, 避免直接关闭丢失内存数据。

25. 在处置过程中, 对受影响系统的'内存转储'应在何时进行?

- A. 系统恢复后
- B. 系统关闭或重启后
- C. 系统仍在运行时尽早进行
- D. 证据分析完成后

答案: C 中

解析:

内存数据易失, 应在系统运行时尽早进行内存转储, 以保留进程、网络连接等关键证据。

26. 根除阶段的核心任务是?

- A. 恢复业务系统
- B. 彻底消除攻击根因和后门
- C. 通知相关方
- D. 总结经验教训

答案: B 中

解析:

根除阶段需清理恶意代码、关闭漏洞、移除后门、修复配置, 确保攻击根因被消除。

27. 恢复系统时，'从已知干净备份恢复'的优势是？

- A. 可以保留所有最新数据
- B. 避免将恶意代码或后门一同恢复
- C. 恢复速度最快
- D. 不需要验证备份完整性

答案: B 中

解析:

从已知干净备份恢复可避免重新引入恶意代码或后门，恢复前仍需验证备份完整性。

28. 在根除阶段，'漏洞修复'应优先处理哪类漏洞？

- A. 所有已知漏洞同时修复
- B. 被攻击者利用或最可能被利用的高危漏洞
- C. 历史最久的漏洞
- D. 仅修复操作系统漏洞

答案: B 中

解析:

应优先修复被利用或可能被利用的高危漏洞，以阻断再次入侵路径。

29. 恢复阶段应优先恢复哪些业务？

- A. 所有业务同时恢复
- B. 关键业务和依赖关系最简的业务
- C. 最容易恢复的业务
- D. 最后受损的业务

答案: B 中

解析:

应优先恢复关键业务，并考虑业务依赖关系，确保恢复过程可控。

30. 数据恢复后，为验证数据完整性，应优先？

- A. 对比备份哈希值
- B. 直接打开业务系统
- C. 删除备份以节省空间
- D. 通知用户验证

答案: A 中

解析:

对比备份哈希值可验证数据未被篡改，是恢复后完整性验证的重要手段。

31. 以下哪项不属于恶意代码的常见类型？

- A. 病毒
- B. 蠕虫
- C. 木马

D. 防火墙

答案: D 易

解析:

防火墙是安全设备，不属于恶意代码类型。病毒、蠕虫、木马是常见恶意代码。

32. 勒索软件的主要危害是？

- A. 窃取用户账号密码
- B. 加密文件并要求赎金
- C. 发起DDoS攻击
- D. 传播垃圾邮件

答案: B 中

解析:

勒索软件通过加密文件、数据库等要求受害者支付赎金以获取解密密钥。

33. 静态分析是指？

- A. 直接运行恶意代码观察行为
- B. 不运行代码，通过反编译、字符串提取等方式分析
- C. 分析网络流量
- D. 分析用户行为

答案: B 中

解析:

静态分析在不执行代码的情况下，通过反编译、字符串、导入表、PE结构等手段分析。

34. 在动态分析中，'沙箱'的作用是？

- A. 提高恶意代码运行速度
- B. 在隔离环境中观察恶意代码行为
- C. 直接清除恶意代码
- D. 加密分析样本

答案: B 中

解析:

沙箱提供隔离环境，安全地运行恶意代码并观察其行为、网络通信、文件操作等。

35. 木马程序的常见通信方式不包括？

- A. HTTP/HTTPS回连
- B. DNS隧道通信
- C. ICMP隧道通信
- D. 本地文件系统写入

答案: D 中

解析:

本地文件系统写入是本地行为，不是通信方式。HTTP/HTTPS、DNS隧道、ICMP隧道都是常见隐蔽通信方式。

36.

分析一个可疑文件时，发现其大量使用了VirtualAllocEx、WriteProcessMemory、CreateRemoteThread API，最可能的行为是？

- A. 正常的数据库操作
- B. 进程注入或DLL注入
- C. 正常的日志记录
- D. 网络代理转发

答案：B 难

解析：

VirtualAllocEx、WriteProcessMemory、CreateRemoteThread是进程/DLL注入的典型API组合。

37. Wireshark主要用于？

- A. 网络流量捕获与分析
- B. 漏洞扫描
- C. 密码破解
- D. 网站开发

答案：A 易

解析：

Wireshark是著名的网络协议分析工具，用于捕获和分析网络流量。

38. TCP三次握手过程中，SYN Flood攻击发生在哪个阶段？

- A. 第一次握手（SYN）
- B. 第二次握手（SYN+ACK）
- C. 第三次握手（ACK）
- D. 连接建立后的数据传输

答案：A 中

解析：

SYN Flood攻击通过发送大量SYN包但不完成第三次握手，耗尽服务器半连接资源。

39. DNS隧道攻击通常用于？

- A. 提升域名解析速度
- B. 绕过网络防火墙进行数据外传或C2通信
- C. 防止DNS劫持
- D. 加速网络访问

答案：B 中

解析：

DNS隧道利用DNS协议传输数据，常用于绕过网络限制进行隐蔽通信或数据外传。

40. 在网络流量中发现大量目标端口为3389的连接，可能意味着？

- A. 正常的Web访问

- B. 针对远程桌面（RDP）的暴力破解或滥用
- C. 邮件服务异常
- D. DNS查询异常

答案: B 中

解析:

3389是RDP默认端口，大量连接可能意味着暴力破解或RDP被滥用。

41. 下列哪种协议最常被用于隐蔽数据传输？

- A. HTTP明文
- B. DNS
- C. ICMP
- D. 以上都可能

答案: D 中

解析:

HTTP、DNS、ICMP等协议都可能被用于隐蔽数据传输，DNS和ICMP因常被放行而尤其常见。

42. 流量分析中，‘协议解码’的作用是？

- A. 加密流量
- B. 将二进制数据包解析为可读的应用层信息
- C. 阻断攻击
- D. 生成随机流量

答案: B 中

解析:

协议解码将原始数据包按协议层次解析，提取可读的应用层信息供分析。

43. Windows系统中，登录成功事件通常记录在安全日志的事件ID为？

- A. 4624
- B. 4625
- C. 4634
- D. 4648

答案: A 易

解析:

Windows事件ID 4624表示成功登录，4625表示登录失败，4634表示注销，4648表示显式凭据登录。

44. Linux系统中，用户登录日志通常记录在？

- A. /var/log/auth.log 或 /var/log/secure
- B. /var/log/apache2/access.log
- C. /var/log/syslog
- D. /var/log/dmesg

答案: A 中

解析:

Debian/Ubuntu使用/var/log/auth.log, RHEL/CentOS使用/var/log/secure记录认证登录日志。

45. 分析Windows安全日志时, 大量4625事件可能表示?

- A. 用户频繁成功登录
- B. 存在暴力破解攻击
- C. 系统正常注销
- D. 用户权限提升

答案: B 中

解析:

4625是登录失败事件, 大量出现通常意味着暴力破解或密码喷射攻击。

46. 在日志分析中, 以下哪种情况最可疑?

- A. 工作时间内正常业务访问
- B. 非工作时间来自海外的管理员登录
- C. 定期系统备份任务
- D. 用户正常修改密码

答案: B 中

解析:

非工作时间、异常地理位置、高权限账户登录属于典型异常, 需重点排查。

47. 为确保日志的法律效力, 以下哪项最重要?

- A. 日志存储在本地
- B. 日志具有完整性保护和可信时间戳
- C. 日志只保存7天
- D. 日志不加密

答案: B 中

解析:

日志作为证据需保证完整性、不可篡改性和可信时间, 才能具备法律效力。

48. 日志保留策略应考虑的主要因素不包括?

- A. 合规要求
- B. 存储成本
- C. 攻击者国籍
- D. 业务调查需求

答案: C 中

解析:

日志保留策略依据合规要求、成本、调查需求制定, 与攻击者国籍无关。

49. 内存取证工具Volatility常用于分析？

- A. 网络流量
- B. 磁盘镜像
- C. 内存转储文件
- D. 数据库

答案：C 中

解析：

Volatility是开源内存取证框架，用于分析内存转储文件中的进程、网络、注册表等信息。

50. 在取证过程中，'证据链'（Chain of Custody）的主要作用是？

- A. 加速分析速度
- B. 证明证据从获取到呈现的全过程未被篡改
- C. 隐藏证据来源
- D. 减少存储空间

答案：B 中

解析：

证据链记录证据的获取、传递、存储、分析全过程，确保证据完整性和可采信。

51. 在Windows取证中，Prefetch文件主要用于分析？

- A. 网络连接历史
- B. 程序执行历史
- C. 浏览器访问历史
- D. 用户文档编辑历史

答案：B 中

解析：

Prefetch文件记录程序执行信息，包括执行时间、路径、次数等，用于分析程序执行历史。

52. 时间戳篡改（Timestamping）攻击的主要目的是？

- A. 加速文件访问
- B. 隐藏恶意文件的创建或修改时间
- C. 破坏文件系统
- D. 增加文件大小

答案：B 中

解析：

Timestamping通过修改文件时间戳，使恶意文件在取证分析中难以被识别为异常。

53. 在Linux取证中，'bash_history'文件可用于分析？

- A. 用户执行的命令历史
- B. 网络连接状态
- C. 系统启动时间

D. 硬件配置信息

答案: A 中

解析:

bash_history保存用户执行的命令历史, 可用于追踪攻击者执行的操作。

54. 应急响应的最后一个阶段通常是?

- A. 检测
- B. 恢复
- C. 跟踪总结与改进
- D. 遏制

答案: C 易

解析:

应急响应通常以总结改进收尾, 提炼经验教训, 优化预案、流程和安全措施。

55. 根据《网络安全法》, 网络运营者应当制定网络安全事件应急预案, 并定期进行?

- A. 采购设备
- B. 演练
- C. 裁员
- D. 系统重装

答案: B 中

解析:

《网络安全法》要求网络运营者制定应急预案并定期进行演练。

56. 关键信息基础设施运营者应多长时间至少组织一次网络安全应急演练?

- A. 每月
- B. 每季度
- C. 每年
- D. 每三年

答案: C 中

解析:

根据《关键信息基础设施安全保护条例》, 运营者应每年至少组织一次网络安全应急演练。

57. 在事件总结阶段, 'KPI' 通常用于衡量?

- A. 攻击者的攻击能力
- B. 应急响应团队的响应效率和质量
- C. 网络带宽大小
- D. 员工满意度

答案: B 中

解析:

KPI用于衡量响应团队的MTTD、MTTR、遏制时间、恢复时间等效率和质量指标。

58. 以下哪项最能体现应急响应‘持续改进’的理念？

- A. 事件结束后立即归档不再关注
- B. 每次事件后进行复盘并更新预案和防护措施
- C. 仅在遭受重大事件后才进行改进
- D. 将事件责任归咎于个人

答案：B 中

解析：

持续改进要求每次事件后进行复盘，将经验教训转化为预案更新、能力提升和防护措施优化。

二、多选题（共 37 题）

1. 应急响应团队的主要职责包括哪些？

- A. 事件监测与检测
- B. 事件分析、遏制与根除
- C. 系统恢复与业务连续性保障
- D. 事件总结与改进建议

答案：ABCD 中

解析：

应急响应团队覆盖事件全生命周期：监测检测、分析研判、遏制根除、恢复重建、总结改进。

2. 完善的应急响应预案应包含哪些内容？

- A. 事件分级与响应流程
- B. 应急联系人清单
- C. 各类事件的处置SOP
- D. 演练计划与持续改进机制

答案：ABCD 中

解析：

应急响应预案应涵盖组织架构、分级标准、处置流程、联系人、SOP、演练与改进机制。

3. 应急响应准备阶段应建立的安全基线包括哪些？

- A. 主机操作系统安全配置基线
- B. 网络设备安全配置基线
- C. 应用系统安全配置基线
- D. 数据库安全配置基线

答案：ABCD 中

解析：

安全基线覆盖主机、网络、应用、数据库等各层面，是事件检测与恢复的重要参照。

4. 应急响应沙箱环境应满足哪些要求？

- A. 与生产网络物理或逻辑隔离
- B. 能够模拟目标系统环境
- C. 具备恶意代码样本分析能力
- D. 与互联网完全开放以便下载工具

答案：ABC 中

解析：

沙箱环境必须隔离，避免污染生产网络；需能模拟目标环境并支持恶意样本分析，不应随意开放互联网。

5. 以下哪些属于应急响应常用资源储备？

- A. 备用网络设备和服务器
- B. 已知干净的系统镜像
- C. 取证工具 license
- D. 法律顾问联系方式

答案：ABCD 中

解析：

应急资源包括备用硬件、干净镜像、工具授权、外部专家和法务支持等。

6. 有效的安全事件监测数据来源包括？

- A. 防火墙日志
- B. 终端EDR告警
- C. 网络流量镜像
- D. 员工投诉和报告

答案：ABCD 中

解析：

事件监测需多源数据：网络日志、终端告警、流量镜像、员工报告及威胁情报。

7. 检测内存马（无文件落地Webshell）时，可重点关注哪些异常？

- A. 应用进程中出现可疑的类加载或字节码
- B. 异常的网络连接或端口监听
- C. 注册表或启动项变化
- D. 特定URL的异常访问频率

答案：ABD 难

解析：

内存马无文件落地，常表现为进程异常类加载、可疑网络连接、特定URL高频访问。注册表变化更多用于持久化检测。

8. 以下哪些属于有效的安全事件检测技术？

- A. 基于签名的检测
- B. 基于行为的异常检测
- C. 基于威胁情报的匹配
- D. 基于机器学习的异常识别

答案：ABCD 中

解析：

现代检测技术包括签名检测、行为分析、威胁情报匹配和机器学习异常识别。

9. 有效的网络遏制措施包括？

- A. 关闭受影响主机的网络连接
- B. 在边界防火墙阻断已知恶意IP
- C. 调整DNS解析使恶意域名指向黑洞

D. 增加网络带宽以稀释攻击

答案: ABC 中

解析:

遏制措施包括隔离主机、阻断恶意IP/DNS、限制横向移动等。增加带宽通常用于缓解DDoS，但不是根本遏制。

10. 处置Web应用入侵事件时，应优先检查哪些内容？

- A. 应用访问日志
- B. 数据库操作日志
- C. WebShell或可疑文件
- D. 用户权限和账户变更

答案: ABCD 中

解析:

Web应用入侵调查需综合日志、文件、数据库和账户权限等多方面证据。

11. 遏制阶段需要考虑哪些因素？

- A. 对业务连续性的影响
- B. 证据保全的完整性
- C. 攻击者的反制能力
- D. 事件影响范围

答案: ABCD 难

解析:

遏制需平衡业务影响、证据完整、攻击者可能的反制以及影响范围。

12. 事件通报机制应包括哪些要素？

- A. 通报对象和联系方式
- B. 通报内容和紧急程度分级
- C. 通报时间节点和责任人
- D. 对外口径和保密要求

答案: ABCD 中

解析:

通报机制需明确对象、内容、分级、时间、责任人以及对外口径和保密要求。

13. 根除恶意代码时，通常需要执行哪些操作？

- A. 删除恶意文件和启动项
- B. 修复被利用的漏洞
- C. 重置受影响账户密码和凭据
- D. 重新安装所有系统

答案: ABC 中

解析:

根除包括删除恶意文件、修复漏洞、重置凭据等。重新安装所有系统不是必须的，仅在必要时进行。

14. 系统恢复后的验证工作包括？

- A. 漏洞扫描和基线核查
- B. 恶意代码扫描
- C. 日志审计和异常监测
- D. 业务功能测试

答案：ABCD 中

解析：

恢复后需验证系统安全性、功能正常性和监测有效性，确保无残留威胁。

15. 对于已知存在后门的系统，以下哪些措施是必要的？

- A. 彻底清除后门和恶意文件
- B. 分析攻击路径并修复所有漏洞
- C. 重置所有相关凭据和密钥
- D. 持续监控并分析网络流量

答案：ABCD 难

解析：

处理后门需全面清理、修复漏洞、重置凭据、密钥，并持续监控防止复发。

16. 应急响应中‘根除’与‘恢复’的合理关系是？

- A. 先根除再恢复
- B. 根除不彻底可导致再次入侵
- C. 恢复和根除可部分并行
- D. 恢复必须在根除完全结束后才能开始

答案：ABC 中

解析：

通常先根除再恢复，但部分恢复工作可在根除过程中并行开展。根除不彻底会留下复发隐患。

17. 恶意代码分析可分为哪些类型？

- A. 静态分析
- B. 动态分析
- C. 社会工程学分析
- D. 网络流量分析

答案：AB 中

解析：

恶意代码分析主要包括静态分析（不运行样本）和动态分析（在受控环境运行样本）。

18. 判断一个PE文件是否可疑，可从哪些方面入手？

- A. 是否存在加壳或混淆
- B. 导入表中是否有可疑API调用
- C. 数字签名是否有效

D. 文件大小是否异常

答案：ABCD 难

解析：

可疑PE文件常表现为加壳、可疑API调用（如创建远程线程、注入）、签名无效、文件大小异常等。

19. 恶意代码持久化机制包括？

- A. 注册表启动项
- B. 计划任务
- C. 系统服务
- D. WMI事件订阅

答案：ABCD 中

解析：

恶意代码常通过注册表、计划任务、服务、WMI事件订阅等方式实现持久化。

20. 无文件恶意代码（Fileless Malware）的检测难点包括？

- A. 不写入传统可执行文件
- B. 依赖合法系统工具（如PowerShell、WMI）
- C. 行为与正常系统管理行为相似
- D. 仅通过文件哈希无法检测

答案：ABCD 难

解析：

无文件恶意代码利用合法工具和内存执行，难以通过传统文件检测发现，需要行为分析和内存检测。

21. 分析可疑C2通信时，应关注哪些特征？

- A. 周期性心跳包
- B. 异常的DNS请求
- C. 已知恶意IP或域名
- D. 加密流量中的固定字节模式

答案：ABCD 中

解析：

C2通信常表现为心跳、异常DNS、已知恶意IOC、固定加密模式或User-Agent等特征。

22. HTTPS加密流量分析可采用的方法包括？

- A. 部署SSL/TLS解密设备
- B. 分析JA3/JA4指纹
- C. 关注SNI和证书信息
- D. 仅分析目的IP地址

答案：ABC 难

解析：

HTTPS流量分析可通过解密、JA3/JA4指纹、SNI和证书信息等方式，仅看目的IP信息量不足。

23. 网络流量取证中需要保存的信息包括？

- A. 完整的数据包捕获（PCAP）
- B. 捕获时间、端口和协议信息
- C. 相关告警和日志
- D. 分析人员的个人推测

答案：ABC 中

解析：

流量取证需保存原始PCAP、时间/端口/协议信息及相关日志，个人推测不属于证据。

24. 检测数据外泄（Data Exfiltration）时，可重点关注哪些异常？

- A. 非工作时间的大流量上传
- B. 内部主机与陌生外部IP建立长时间连接
- C. 压缩或加密后的大量数据外传
- D. 员工正常下载工作文档

答案：ABC 难

解析：

数据外泄常表现为异常时间的大流量、陌生外联、加密/压缩数据外传。正常下载不属于异常。

25. Web访问日志中可用于入侵分析的信息包括？

- A. 请求URL和HTTP方法
- B. 来源IP和用户代理
- C. 响应状态码和响应大小
- D. 请求时间戳

答案：ABCD 中

解析：

Web日志包含URL、方法、IP、UA、状态码、响应大小、时间戳等，是入侵分析的重要数据源。

26. 日志集中管理（日志审计）的优势包括？

- A. 便于跨系统关联分析
- B. 提高日志留存安全性
- C. 支持快速检索和告警
- D. 降低日志存储成本

答案：ABC 中

解析：

日志集中管理便于关联分析、安全留存、快速检索和告警，但不一定降低存储成本。

27. 日志分析中的‘关联分析’可以做什么？

- A. 将不同系统的日志关联起来识别攻击链
- B. 通过时间序列发现多步攻击
- C. 识别单一日志中无法体现的异常

D. 自动修复漏洞

答案：ABC 难

解析：

关联分析整合多源日志，还原攻击链、识别多步攻击和隐蔽异常，但不能自动修复漏洞。

28. 以下哪些日志属于关键安全日志？

- A. 操作系统认证日志
- B. 防火墙连接日志
- C. 数据库审计日志
- D. Web应用访问日志

答案：ABCD 中

解析：

关键安全日志包括操作系统、防火墙、数据库、Web应用、EDR、网络设备等多类日志。

29. 内存取证中可以提取的信息包括？

- A. 运行中的进程和线程
- B. 网络连接和端口
- C. 加载的DLL和驱动
- D. 已解密的数据和密钥

答案：ABCD 中

解析：

内存中可提取进程、线程、网络连接、加载模块、密钥、明文密码等易失性信息。

30. 创建磁盘镜像时，为保证证据完整性，应记录哪些信息？

- A. 原始介质的哈希值（MD5/SHA256）
- B. 镜像文件的哈希值
- C. 操作时间和操作人员
- D. 使用的工具和设备信息

答案：ABCD 难

解析：

取证镜像需记录原始哈希、镜像哈希、时间、人员、工具等信息，确保可追溯和可验证。

31. 文件系统取证时可关注的痕迹包括？

- A. 文件创建、修改、访问时间（MAC时间）
- B. 已删除文件和文件残留
- C. 隐藏文件和ADS（交替数据流）
- D. 文件签名和哈希

答案：ABCD 中

解析：

文件系统取证关注MAC时间、删除文件、隐藏文件、ADS、文件签名和哈希等。

32. 系统取证中，'Live Response'与'Dead Response'的区别包括？

- A. Live Response在系统运行时进行，可获取易失性数据
- B. Dead Response针对已关机或断电系统
- C. Live Response需要快速操作以保留内存数据
- D. Dead Response无法获取内存中的证据

答案：ABCD 难

解析：

Live Response针对运行系统获取内存、进程等易失数据；Dead Response针对已关机系统，内存数据会丢失。

33. 数字取证的基本原则包括？

- A. 原始证据不改变（或改变可记录）
- B. 所有操作有记录、可追溯
- C. 分析在可控环境中进行
- D. 结果可重现和验证

答案：ABCD 难

解析：

数字取证需遵循原始证据保护、操作可追溯、环境可控、结果可重现等原则。

34. 事件总结报告应包含哪些内容？

- A. 事件经过和时间线
- B. 影响范围和损失评估
- C. 处置过程和经验教训
- D. 改进建议和预防措施

答案：ABCD 中

解析：

总结报告需涵盖事件经过、时间线、影响、损失、处置过程、经验教训和改进建议。

35. 以下哪些属于我国网络安全应急响应相关法律法规？

- A. 《网络安全法》
- B. 《数据安全法》
- C. 《个人信息保护法》
- D. 《国家网络安全事件应急预案》

答案：ABCD 中

解析：

《网络安全法》《数据安全法》《个人信息保护法》及《国家网络安全事件应急预案》共同构成应急响应法律框架。

36. 持续改进应急响应能力的方法包括？

- A. 定期复盘和演练
- B. 更新威胁情报和IOC库

- C. 优化检测规则和工具
- D. 加强人员培训和技能考核

答案：ABCD 中

解析：

持续改进需复盘演练、更新情报、优化工具、加强培训和考核。

37. 网络安全事件应急预案的演练形式包括？

- A. 桌面演练
- B. 模拟演练
- C. 实战演练
- D. 红蓝对抗演练

答案：ABCD 中

解析：

演练形式包括桌面演练、模拟演练、实战演练、红蓝对抗等多种形式。

三、判断题（共 5 题）

1. 应急响应只发生在安全事件已经发生之后，事前准备并不重要。

答案：错误 易

解析：

应急响应强调‘平时准备、战时响应’。事前的预案编制、工具清单、人员培训和桌面/实战演练，直接决定了事件发生时能否快速定位、有效遏制和有序恢复。缺乏准备会导致响应混乱、证据丢失和损失扩大。

2. 应急响应预案一旦制定完成，就不需要再更新。

答案：错误 易

解析：

应急预案属于活文档，必须随着组织架构调整、业务系统变更、威胁情报更新以及演练复盘结果持续修订。建议至少每年评审一次，重大变更或演练发现缺陷后应及时更新，确保响应流程与当前环境匹配。

3. 事件处置中，证据保全应在遏制之后进行。

答案：错误 易

解析：

证据保全与遏制并非严格的先后关系，而应同步开展。在隔离受影响主机、阻断恶意流量的同时，需立即进行内存转储、磁盘镜像、日志封存和哈希校验，避免易失性证据丢失或被攻击者清理。

4. 恢复阶段完成后，应立即将系统重新上线投入生产。

答案：错误 易

解析：

恢复后上线前必须经过严格验证：运行漏洞扫描与恶意代码查杀、核查安全基线、进行业务功能测试、持续监控异常行为，并确认备份数据未被污染。过早上线可能导致二次入侵或业务数据再次受损。

5. 演练和事件总结是应急响应持续改进的重要手段。

答案：正确 易

解析：

PDCA

式的持续改进是应急响应体系建设的核心。演练可暴露预案缺陷和协同问题，真实事件复盘能提炼攻击手法、处置效率和沟通机制的改进点，两者结合推动检测、响应和恢复能力螺旋上升。