

第二期网络安全等级测评师能力评估（初级）

网络安全法哪年实施

- A.2016 年 6 月 1 日
- B.2017 年 6 月 1 日
- C.2016 年 12 月 30 日
- D.2017 年 12 月 30 日

答案：B

哪项不属于“安全事件处置”里面的内容

- A.应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等
- B.应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；
- C.应及时向安全管理部门报告所发现的安全弱点和可疑事件
- D.对造成系统中断和造成信息泄漏的重大安全事件应采用相同的处理程序和报告程序

答案：D

- A.水坑攻击
- B.钓鱼邮件攻击
- C.DNS 放大
- D.攻击目标用户经常访问的网站

答案：C

以下控制点属于安全管理机构的是哪些 不定项

- A.人员配备
- B.授权和审批
- C.岗位设置
- D.评审和修订

答案：ABC

通信线缆铺设在隐蔽处属于哪个控制点

- A.防火
- B.防静电
- C.防盗窃和防破坏

答案：C

下列说法错误的是

- A.hash 哈希算法实现机密性
- B.sm4 实现机密性
- C.SM3 实现完整性
- D.数字签名实现不可否认性

答案：A

确定测评对象需要遵循的原则不包括

- A.重要性
- B.全面性
- C.关联性
- D.安全性

答案：C

三级云计算拓展，安全计算环境不包括哪个控制点：

- A.访问控制
- B.身份鉴别
- C.入侵防范
- D.安全审计

答案：D

esp 协议不能提供（和那个 IPsecVPN 的 ah 协议很相似）

- A.数据机密性
- B.身份认证
- C.不可否认性
- D.数据完整性

答案：B

布尔盲注是下列哪个？

- A.数据库注入
- B.使用 1=1 和 1=2 进行测试
- C.输入 DELETE 测试

答案：B

生产活动在哪一层

- A.现场设备层
- B.现场控制层
- C.企业资源层
- D.生产管理层

答案：D

XSS 攻击最严重的类型是哪一种

- A.Dom 型
- B.存储型
- C.反射型

答案：B

重大风险隐患判定原则：

- A.严重性原则
- B.高发性原则
- C.相关性原则
- D.普遍性原则

答案：ABC

云计算安全运维管理那个测评项的测评对象是什么

- A.运维地点
- B.运维记录
- C.运维设备
- D.相关管理文档

答案：ABCD

物联网的逻辑层面有哪些 不定项

- A.物理层
- B.感知层
- C.网络传输层

D.处理应用层

答案：BCD

云计算拓展供应链选择的测评项

A.定监督、评审和审核服务供应商提供的服务,并对其变更服务内容加以控制

B.应确保供应商的选择符合国家有关规定

C.应将供应链安全事件信息或安全威胁信息及时传达到云服务客户;

D.应将供应商的重要变更及时传达到云服务客户,并评估变更带来的安全风险,采取措施对风险进行控制。

答案：BCD

测评实施过程常用的三种方式是什么

A.访谈

B.核查

C.调研

D.测试

答案：ABD

身份鉴别的实施内容

A.定期更换口令

B.身份标识唯一

C.口令具有复杂度

D.口令长度大于8位

答案：ABCD

变更管理测评实施内容

A.应明确变更需求,变更前根据变更需求制定变更方案,变更方案经过评审、审批后方可实施;

B.应建立变更的申报和审批控制程序,依据程序控制所有的变更,记录变更实施过程;

C.应建立中止变更并从失败变更中恢复的程序,明确过程控制方法和人员职责,必要时对恢复过程进行演练。

D.应识别需要定期备份的重要业务信息、系统数据及软件系统等;

答案：ABC

资产重要程度赋值

A.一般

B.重要

C.非常重要

D.关键

答案：ABD

确定远程主机是否在线

A.Ping

B.nmap

C.ls

D.netcat

答案：ABD

蜜罐作用

A.提供仿真系统给测试者用于测试

B.监控网络流量

C.引诱黑客进行攻击

D.进行数据清洗

答案：C

通用计算机访问控制的实施内容包括：

A.应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

B.应对登录的用户分配账户和权限；

C.应重命名或删除默认账户，修改默认账户的默认口令；

D.应及时删除或停用多余的、过期的账户，避免共享账户的存在；

答案：BCD

通用计算机入侵防范的实施内容包括

A.应遵循最小安装的原则，仅安装需要的组件和应用程序；

B.应关闭不需要的系统服务、默认共享和高危端口；

C.应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；

D.应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；

答案：ABCD

安全管理人员控制点

A.人员录用

B.人员离岗

C.外部人员访问管理

D.安全意识教育和培训

答案：ABCD

在网络安全法中，当发生了网络攻击事件时，应启用应急预案，巴拉巴拉

A.全权处置

B.临时处置

C.监测和预警

D.分析和调查

答案：D

答案：ABCD

定级的测评点

A.应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；

B.应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；

C.应保证定级结果经过相关部门的批准；

D.应将备案材料报主管部门和相应公安机关备案。

答案：ABCD

渗透隐藏与伪装的技术有哪些

A.域名伪装

B.隧道

C.加密

D.社会工程

答案：ABCD

2025 版测评结论哪种仅能判定为符合

A.符合率 60%且无重大风险隐患

B.70%无隐患

C.80%无隐患

D.90%无隐患

答案：D

我国哪一部()法规首次明确提出“计算机信息系统实行安全等级保护”制度？

A.《中华人民共和国网络安全法》

B.《中华人民共和国计算机信息系统安全保护条例》

C.《中华人民共和国保密法》

D.《中华人民共和国数据安全法》

答案：B

安全管理机构控制点

A.岗位设置

B.人员配备

C.授权和审批

D.沟通和合作

答案：ABCD

移动互联部分由（ ）组成。

A.移动终端

B.移动应用

C.无线网络

D.无线协议

答案：ABC

物联网从架构上分为

A.感知层

B.网络传输层

C.处理应用层

D.物理层

答案：ABC

PASS 平台下,云服务客户的安全责任

A.软件平台

B.应用平台

C.物理机房

D.基础设施

答案：AB

云计算安全计算环境不涉及哪些控制点

A.访问控制

B.入侵防范

C.安全审计

D.身份鉴别

答案：C

2025 年之后重新备案

A.1 级

B.2 级

C.3 级

D.4 级

答案：B

IDS 不能够起到的作用

A.阻断

B.恢复

C.根据行为模式分析

D.对破坏数据进行修复

答案：ABD

端口扫描不可以得到哪个信息

A.用户名

B.系统版本

C.端口

D.服务器名称

答案：A

属于社会工程学的是：

A.钓鱼

B.暴力破解密码

C.sql 注入

D.尾随进入机房

答案：ABD

不属于自行软件开发

A.应在软件交付前检测其中可能存在的恶意代码；

B.应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；

C.应制定代码编写安全规范，要求开发人员参照规范编写代码；

D.应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；

答案：A

以下哪项措施不能实现安全事件的识别、报警和分析

A.工具测试

B.防火墙

C.扫描工具

D.态势感知

答案：B

三级系统“安全审计”是哪个层面的控制点

A.安全区域边界

B.安全计算环境

C.安全管理中心

D.安全运维管理

答案：AB

rw- r-- r--

A.644

B.640

C.755

答案：A

内存 巴拉巴拉

- A.缓冲区溢出
- B.不记得
- C.不记得
- D.不记得

答案：A

安全计算环境入侵防范的测评内容包括：

- A.是否不存在高危端口
- B.是否关闭不需要的系统服务
- C.是否安装不必要的组件
- D.是否应遵循最小安装原则

答案：ABCD

工具测试接入点规划时应该遵循以下那些原则？

- A.由低级别系统向高级别系统探测
- B.同一系统中同等重要程度的功能区域之间要相互探测
- C.由外联接口向系统内部探测
- D.由较低重要程度区域向较高重要程度区域探测

ABCD

IPSEC 协议中 ESP 不能保证什么

- A.完整性
- B.保密性
- C.不可否认性
- D.身份认证

答案：A

传输完整性的实施内容

- A.核查是否采用校验技术或密码技术保证重要数据在传输过程中的完整性
- B. 核查是否采用校验技术或密码技术保证重要数据在存储过程中的完整性
- C.测试验证检测到完整性受到破坏时能否恢复
- D.核查是否对重要程序的完整性进行保护，并在检测到完整性受到破坏时采取恢复措施

答案：AB

第三级网络在“安全通信网络”层面“通信传输”测评实施内容的是

- A.核查是否采用校验技术或密码技术保证通信过程中数据的完整性
- B.测试在通信过程中对敏感信息字段进行加密的有效性
- C.核查网络设备的管理员登录地址是否被限制
- D.核查是否采用密码技术保证通信过程中数据的保密性

答案：AD

端口扫描工具可以得到以下哪些信息？

- A.系统版本
- B.端口信息
- C.登录用户名
- D.开放的服务

答案：ABD

安全运维的控制点包括？

- A.安全事件处置
- B.漏洞和风险管理
- C.网络和系统安全管理
- D.恶意代码防范管理

ABCD

确定定级对象的原则包括哪几方面

- A.关联性
- B.重要性
- C.安全性
- D.全面性

答案：BCD

《f 基本要求》三级安全计算环境的安全管理制度的“安全管理制度”要求项，安全管理制度的管理制度测评项，选择两个测评项写实施内容

- a)应对安全管理活动中的各类管理内容建立安全管理制度；
- b)应对管理人员或操作人员执行的日常管理操作建立操作规程；
- c)应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。

三级“安全审计”d 要求项，发现业务应用软件系统没有日志安全审计，写出安全审计的测评项，说明未开日志安全审计会带来的风险