题目1：什么类型的访问控制旨在事件发生后提供信息来发现不需要的或未授权的活动？

What type of access control is intended to discover unwanted or unauthorized activity by providing information after the event has occurred?

A：预防

Preventive

B：纠正

Corrective

C：检测

Detective

D：指令

Directive

答案:题目1的正确答案是：

C：检测

Detective

检测类型的访问控制旨在在事件发生后提供信息，以便发现不需要的或未授权的活动。这种控制通常包括日志记录、监控和审计，以便在安全事件发生后进行分析和调查。

-------------------

题目2：下列哪一个提供了攻击者在企图入侵期间探索的最复杂诱饵环境？

Which one of the following presents the most complex decoy environment for an attacker to explore during an intrusion attempt?

A：蜜罐

Honeypot

B：暗网

Darknet

C：蜜网

Honeynet

D：伪缺陷

Pseudoflaw

答案:在企图入侵期间，攻击者探索的最复杂诱饵环境是 \*\*C：蜜网（Honeynet）\*\*。

### 解析：

- \*\*蜜罐（Honeypot）\*\*：是一个单一的诱饵系统，通常模拟一个易受攻击的服务或系统，用于吸引攻击者并记录其行为。蜜罐相对简单，通常只模拟一个系统或服务。

- \*\*暗网（Darknet）\*\*：通常指的是未被使用的IP地址空间，用于监测和检测网络扫描和攻击行为。它并不是一个复杂的诱饵环境，而是一个被动的监测工具。

- \*\*蜜网（Honeynet）\*\*：是由多个蜜罐组成的网络，模拟一个完整的网络环境，包括多个系统、服务和网络设备。蜜网提供了更复杂的诱饵环境，攻击者可以在其中进行更深入的探索和攻击，因此蜜网是最复杂的诱饵环境。

- \*\*伪缺陷（Pseudoflaw）\*\*：是指系统中故意设置的漏洞或缺陷，用于诱使攻击者暴露其攻击手法。伪缺陷通常用于单个系统或服务，而不是一个复杂的网络环境。

因此，\*\*蜜网（Honeynet）\*\* 提供了最复杂的诱饵环境，适合用于深入研究和分析攻击者的行为。

-------------------

题目3-1：Ben的组织正在为他们的高安全性建筑物的访问控制系统采用生物识别身份验证。使用此图表，回答关于他们采用该技术的3个问题。

<div style="text-align:center"><img alt="" height="236" src="/file/100000/m/20210906/66ad20a28f6642f9abbfc0d26d70ea77.png" width="341" /></div>

Ben’s organization is adopting biometric authentication for their high-security building’s access control system. Using this chart, answer questions about their adoption of the technology.

<div style="text-align:center"><img alt="" height="237" src="/file/100000/m/20210906/a47f9df4f70a46b5b05dd71c74ea814f.png" width="392" /></div>

Ben的公司正在考虑将其系统配置为在图上的点A所示的水平上工作。他们设置的灵敏度应该是多少？

Ben’s company is considering configuring their systems to work at the level shown by point A on the diagram. What level are they setting the sensitivity to?

A：FRR交叉点

The FRR crossover

B：FAR点

The FAR point

C：CER

The CER

D：CFR

The CFR

答案:根据题目描述，Ben的公司正在考虑将其系统配置为在图上的点A所示的水平上工作。点A通常表示的是FRR（False Rejection Rate，错误拒绝率）和FAR（False Acceptance Rate，错误接受率）的交叉点，也就是CER（Crossover Error Rate，交叉错误率）。CER是生物识别系统中一个重要的性能指标，表示FRR和FAR相等时的错误率。

因此，正确答案是：

\*\*C：CER\*\*

The CER

-------------------

题目3-1：Ben的组织正在为他们的高安全性建筑物的访问控制系统采用生物识别身份验证。使用此图表，回答关于他们采用该技术的3个问题。

<div style="text-align:center"><img alt="" height="236" src="/file/100000/m/20210906/66ad20a28f6642f9abbfc0d26d70ea77.png" width="341" /></div>

Ben’s organization is adopting biometric authentication for their high-security building’s access control system. Using this chart, answer questions about their adoption of the technology.

<div style="text-align:center"><img alt="" height="237" src="/file/100000/m/20210906/a47f9df4f70a46b5b05dd71c74ea814f.png" width="392" /></div>

在B点，可能发生什么问题？

At point B, what problem is likely to occur?

A：错误接受率将非常高

False acceptance will be very high.

B：错误拒绝率将非常高

False rejection will be very high.

C：错误拒绝率将非常低

False rejection will be very low.

D：错误接受率将非常低

False acceptance will be very low.

答案:在生物识别系统中，错误接受率（False Acceptance Rate, FAR）和错误拒绝率（False Rejection Rate, FRR）是两个关键的指标。错误接受率是指系统错误地将未授权用户识别为授权用户的概率，而错误拒绝率是指系统错误地将授权用户识别为未授权用户的概率。

在图表中，B点通常表示系统的阈值设置较高，这意味着系统对匹配的要求非常严格。在这种情况下，系统可能会错误地拒绝许多授权用户，从而导致错误拒绝率（FRR）非常高。因此，正确答案是：

\*\*B：错误拒绝率将非常高\*\*

False rejection will be very high.

-------------------

题目3-1：Ben的组织正在为他们的高安全性建筑物的访问控制系统采用生物识别身份验证。使用此图表，回答关于他们采用该技术的3个问题。

<div style="text-align:center"><img alt="" height="236" src="/file/100000/m/20210906/66ad20a28f6642f9abbfc0d26d70ea77.png" width="341" /></div>

Ben’s organization is adopting biometric authentication for their high-security building’s access control system. Using this chart, answer questions about their adoption of the technology.

<div style="text-align:center"><img alt="" height="237" src="/file/100000/m/20210906/a47f9df4f70a46b5b05dd71c74ea814f.png" width="392" /></div>

如果本图中显示的FAR和FRR没有为其组织的需求提供可接受的绩效水平，Ben应该怎么办？

What should Ben do if the FAR and FRR shown in this diagram do not provide an acceptable performance level for his organization’s needs?

A：调整生物识别装置的灵敏度

Adjust the sensitivity of the biometric devices.

B：评估其他生物特征系统以进行比较

Assess other biometric systems to compare them.

C：调整CER

Move the CER.

D：在软件中调整FRR设置

Adjust the FRR settings in software.

答案:根据题目描述，Ben的组织正在为高安全性建筑物的访问控制系统采用生物识别身份验证技术。题目中提到，如果图中的FAR（False Acceptance Rate，错误接受率）和FRR（False Rejection Rate，错误拒绝率）没有达到组织需求的可接受水平，Ben应该采取什么措施。

选项分析：

- \*\*A：调整生物识别装置的灵敏度\*\*

调整生物识别设备的灵敏度可以影响FAR和FRR的表现。通常，提高灵敏度会降低FAR（减少错误接受），但可能会增加FRR（增加错误拒绝）。反之亦然。因此，这是一个可行的解决方案。

- \*\*B：评估其他生物特征系统以进行比较\*\*

如果当前的生物识别系统无法满足需求，评估其他生物特征系统（如指纹、虹膜、面部识别等）也是一种合理的做法。通过比较，可以选择更适合组织需求的系统。

- \*\*C：调整CER\*\*

CER（Crossover Error Rate，交叉错误率）是FAR和FRR相等时的错误率，通常用于衡量生物识别系统的性能。CER本身是一个指标，无法直接调整，因此这个选项不正确。

- \*\*D：在软件中调整FRR设置\*\*

FRR是系统性能的一个结果，而不是可以直接调整的参数。通常需要通过调整设备的灵敏度或其他硬件/软件参数来间接影响FRR。因此，这个选项也不正确。

\*\*正确答案：A 和 B\*\*

- 如果FAR和FRR不满足需求，Ben可以通过调整生物识别设备的灵敏度（A）来优化性能，或者评估其他生物特征系统（B）以找到更适合的解决方案。

-------------------

题目4：Ed的任务是保护其组织的客户的信息，包括他们的姓名、社会安全号码、出生日期和出生地点，以及各种其他信息。这个信息是什么？

Ed is tasked with protecting information about his organization’s customers, including their name, Social Security number, birthdate, and place of birth, as well as a variety of other information. What is this information known as?

A：PHI

PHI

B：PII

PII

C：个人保护数据

Personal protected data

D：PID

PID

答案:正确答案是 B：PII。

PII 是 "Personally Identifiable Information" 的缩写，指的是可以用来识别、联系或定位某个个体的信息。在题目中提到的信息，如姓名、社会安全号码、出生日期和出生地点等，都是典型的 PII 例子。这些信息如果被泄露，可能会导致个人隐私的侵犯或身份盗窃等问题。因此，保护 PII 是组织在信息安全方面的重要任务。

-------------------

题目5：下图显示了什么软件的开发生命周期模型？

<div style="text-align:center"><img alt="" height="548" src="/file/100000/m/20210906/4dedd543254b41fc88914b090c3f45c8.png" width="687" /></div>

What software development lifecycle model is shown in the following illustration?

<div style="text-align:center"><img alt="" height="496" src="/file/100000/m/20210906/f4217dc260c147579c1c312bec44b4f7.png" width="652" /></div>

A：螺旋

Spiral

B：敏捷

Agile

C：Boehm

Boehm

D：瀑布

Waterfall

答案:题目5的答案是 \*\*D：瀑布 (Waterfall)\*\*。

瀑布模型是一种线性的软件开发生命周期模型，通常包括需求分析、设计、实现、测试、部署和维护等阶段。每个阶段在前一个阶段完成后才开始，且通常不会返回到之前的阶段。这种模型适用于需求明确且变化较少的项目。

-------------------

题目6：封装是实现什么类型协议的核心概念？

Encapsulation is the core concept that enables what type of protocol?

A：桥接

Bridging

B：多层

Multilayer

C：散列

Hashing

D：存储

Storage

答案:题目6的正确答案是：

B：多层

Multilayer

封装（Encapsulation）是实现多层协议（Multilayer Protocol）的核心概念。在网络通信中，数据通常会在不同的协议层之间传递，每一层都会对数据进行封装，添加相应的头部或尾部信息，以便在接收端能够正确地解析和处理数据。这种多层封装的结构使得网络协议能够分层设计，每一层专注于特定的功能，从而实现复杂网络通信的高效管理。

-------------------

题目7：Amanda想要使用现有Gmail账户中的联系人，她的应用程序的新用户已经拥有这些联系人。以下选项中的哪个协议用于为许多云提供商的此类使用，提供安全的委托访问？

Amanda wants to use contacts from the existing Gmail accounts that new users for her application already have. What protocol from the following options is used to provide secure delegated access for this type of use by many cloud providers?

A：Open ID

OpenID

B：Kerberos

Kerberos

C：OAuth

OAuth

D：SAML

SAML

答案:正确答案是 \*\*C：OAuth\*\*。

### 解析：

- \*\*OAuth\*\* 是一种用于授权的开放标准协议，允许用户在不共享其密码的情况下，授权第三方应用程序访问其资源（如联系人、邮件等）。OAuth 通常用于云服务提供商之间的安全委托访问，例如允许应用程序访问用户的 Gmail 联系人。

- \*\*OpenID\*\* 主要用于身份验证（Authentication），而不是授权（Authorization），因此不适用于此场景。

- \*\*Kerberos\*\* 是一种网络身份验证协议，主要用于局域网环境中的身份验证，不适用于云服务之间的委托访问。

- \*\*SAML\*\* 是一种用于单点登录（SSO）的协议，主要用于身份验证和跨域的身份信息交换，而不是资源授权。

因此，OAuth 是最适合用于 Amanda 的场景的协议。

-------------------

题目8：在业务连续性计划中，以下哪项指标描述了在服务停止后恢复正常服务所需的时间量？

Which one of the following metrics specifies the amount of time that business continuity planners find acceptable for the restoration of service after a disaster?

A：MTD

MTD

B：RTO

RTO

C：RPO

RPO

D：MTO

MTO

答案:在业务连续性计划中，描述在服务停止后恢复正常服务所需的时间量的指标是 \*\*RTO（Recovery Time Objective）\*\*。

\*\*RTO\*\* 是指从灾难发生到业务恢复正常运作所需的时间目标。它定义了业务可以容忍的中断时间长度，是业务连续性计划中的一个关键指标。

其他选项的解释：

- \*\*MTD（Maximum Tolerable Downtime）\*\*：最大可容忍停机时间，是指业务可以承受的最长停机时间。

- \*\*RPO（Recovery Point Objective）\*\*：恢复点目标，是指业务可以接受的数据丢失量，通常以时间表示。

- \*\*MTO（Maximum Tolerable Outage）\*\*：最大可容忍中断时间，与MTD类似，表示业务可以承受的最长中断时间。

因此，正确答案是 \*\*B：RTO\*\*。

-------------------

题目9：Jill正在为她的组织采购新的网络硬件。她找到了一家从国外以更低价格进口硬件的灰色市场供应商。以这种方式获得的硬件最重要的安全问题是什么？

Jill is working to procure new network hardware for her organization. She finds a gray market supplier that is importing the hardware from outside the country at a much lower price. What security concern is the most significant for hardware acquired this way?

A：硬件和固件的安全性

The security of the hardware and firmware

B：硬件和软件支持的可用性

Availability of support for the hardware and software

C：硬件是否为实际供应商的合法产品

Whether the hardware is a legitimate product of the actual vendor

D：硬件的年龄

The age of the hardware

答案:题目9的正确答案是：

C：硬件是否为实际供应商的合法产品

Whether the hardware is a legitimate product of the actual vendor

解析：

从灰色市场供应商处采购硬件时，最大的安全问题是硬件的合法性和真实性。灰色市场的硬件可能不是由官方供应商直接提供的，因此可能存在假冒、篡改或未经授权的产品。这些硬件可能包含恶意软件、后门或其他安全漏洞，从而对组织的网络安全构成严重威胁。因此，确保硬件是实际供应商的合法产品是最重要的安全问题。

-------------------

题目10：通常使用什么流程来确保正在从服务中删除，但将被转售或以其他方式重用的工作站的数据安全？

What process is typically used to ensure data security for workstations that are being removed from service but that will be resold or otherwise reused?

A：销毁

Destruction

B：擦除

Erasing

C：净化

Sanitization

D：Clearing

清理

答案:正确答案是 C：净化（Sanitization）。

\*\*解释：\*\*

- \*\*销毁（Destruction）\*\*：销毁是指物理上破坏存储介质，使其无法再使用。这种方法适用于不需要保留设备的情况。

- \*\*擦除（Erasing）\*\*：擦除是指删除数据，但这种方法可能无法完全确保数据无法恢复。

- \*\*净化（Sanitization）\*\*：净化是指通过一系列技术手段确保数据无法被恢复，通常包括多次覆盖数据或使用专门的软件工具。这种方法适用于设备将被转售或重用的场景。

- \*\*清理（Clearing）\*\*：清理通常是指删除数据，但可能不如净化彻底。

因此，\*\*净化（Sanitization）\*\* 是确保数据安全的最佳选择，尤其是在设备将被转售或重用时。

-------------------

题目11：Colleen正在进行一个软件测试，评估安全缺陷和可用性问题的代码。最终她从用户的角度使用应用程序，并在使用产品时引用源代码。Colleen进行什么类型的测试？

Colleen is conducting a software test that is evaluating code for both security flaws and usability issues. She is working with the application from an end-user perspective and referencing the source code as she works her way through the product. What type of testing is Colleen conducting?

A：白盒测试

White box

B：蓝盒测试

Blue box

C：灰盒测试

Gray box

D：黑盒测试

Black box

答案:Colleen 正在进行的测试类型是 \*\*灰盒测试（Gray box testing）\*\*。

\*\*解释：\*\*

- \*\*白盒测试（White box testing）\*\*：测试人员完全了解内部代码结构和实现细节，测试是基于代码的内部逻辑进行的。

- \*\*黑盒测试（Black box testing）\*\*：测试人员不了解内部代码结构，仅从用户的角度测试应用程序的功能和可用性。

- \*\*灰盒测试（Gray box testing）\*\*：测试人员部分了解内部代码结构，结合了白盒和黑盒测试的特点。Colleen 从用户的角度使用应用程序，同时参考源代码，这符合灰盒测试的定义。

因此，正确答案是：

\*\*C：灰盒测试（Gray box）\*\*

-------------------

题目12：Harold正在寻找一种软件开发方法，这将有助于处理组织中发现的一个重要问题。目前，开发人员和操作人员不能一起工作，一旦出现问题，各团队经常推卸责任。什么技术管理方法可以减轻这个问题？

Harold is looking for a software development methodology that will help with a major issue he is seeing in his organization. Currently, developers and operations staff do not work together and are often seen as taking problems and “throwing them over the fence” to the other team. What technology management approach is designed to alleviate this problem?

A：ITIL

ITIL

B：精益

Lean

C：ITSM

ITSM

D：DevOps

DevOps

答案:正确答案是 D：DevOps。

DevOps 是一种旨在促进开发（Development）和运维（Operations）团队之间协作与沟通的技术管理方法。它通过自动化工具、持续集成和持续交付（CI/CD）等实践，帮助团队更高效地合作，减少推卸责任的现象，并加速软件交付过程。DevOps 的核心目标是打破开发和运维之间的壁垒，促进跨职能团队的协作，从而更快地响应问题和交付高质量的软件。

其他选项的解释：

- A：ITIL（信息技术基础设施库）是一种IT服务管理框架，主要用于标准化IT服务管理流程，但它并不直接解决开发和运维之间的协作问题。

- B：精益（Lean）是一种旨在减少浪费、提高效率的管理方法，虽然它可以应用于软件开发，但它并不专门针对开发和运维之间的协作问题。

- C：ITSM（IT服务管理）是一种管理IT服务的框架，类似于ITIL，但它也不直接解决开发和运维之间的协作问题。

-------------------

题目13：NIST特别出版物800-92 “计算机安全日志管理指南” 描述了日志管理的四种常见挑战：

大量日志源

不一致的日志内容

不一致的时间戳

不一致的日志格式。

以下哪项解决方案最适合解决这些问题？

NIST Special Publication 800-92, the Guide to Computer Security Log Management, describes four types of common challenges to log management:

■Many log sources

■Inconsistent log content

■Inconsistent timestamps

■Inconsistent log formats

Which of the following solutions is best suited to solving these issues?

A：为所有日志记录设备实施SNMP

Implement SNMP for all logging devices.

B：实施SIEM

Implement a SIEM.

C：对所有设备的Windows事件日志格式进行标准化，并使用NTP

Standardize on the Windows event log format for all devices and use NTP.

D：确保在所有端点上使用其本机日志格式启用日志记录，并正确设置其本地时间

Ensure that logging is enabled on all endpoints using their native logging formats and set their local time correctly.

答案:NIST特别出版物800-92中描述的日志管理挑战包括大量日志源、不一致的日志内容、不一致的时间戳和不一致的日志格式。要解决这些问题，需要一个能够集中管理和分析来自不同源的日志数据的系统。

选项分析：

- \*\*A：为所有日志记录设备实施SNMP\*\*

SNMP（简单网络管理协议）主要用于网络设备的管理和监控，而不是日志管理。它不能解决日志内容、时间戳和格式不一致的问题。

- \*\*B：实施SIEM\*\*

SIEM（安全信息和事件管理系统）是专门设计用于集中收集、分析和关联来自不同源的日志数据的工具。它可以解决大量日志源、不一致的日志内容、时间戳和格式的问题。SIEM系统通常具有日志标准化、时间同步和格式转换的功能。

- \*\*C：对所有设备的Windows事件日志格式进行标准化，并使用NTP\*\*

这种方法只能解决时间戳不一致的问题，并且仅适用于Windows系统。它无法解决大量日志源和不同设备之间的日志格式不一致的问题。

- \*\*D：确保在所有端点上使用其本机日志格式启用日志记录，并正确设置其本地时间\*\*

这种方法虽然可以确保日志记录和时间同步，但无法解决日志内容、格式不一致的问题，也无法集中管理和分析日志数据。

因此，\*\*B：实施SIEM\*\* 是最适合解决这些问题的解决方案。

-------------------

题目14：Mike有一张他想要重复使用的闪存卡。该卡包含敏感信息。他可以使用什么技术从卡上安全地删除数据并允许其重用？

Mike has a flash memory card that he would like to reuse. The card contains sensitive information. What technique can he use to securely remove data from the card and allow its reuse?

A：消磁

Degaussing

B：物理破坏

Physical destruction

C：加密粉碎

Cryptoshredding

D：重新格式化

Reformatting

答案:题目14的正确答案是：

\*\*C：加密粉碎 (Cryptoshredding)\*\*

解释：

- \*\*加密粉碎\*\*是一种通过删除或销毁加密密钥来使数据无法恢复的技术。即使数据仍然存在于闪存卡上，由于密钥已被销毁，数据将无法被解密和访问，从而达到安全删除数据的目的。

- \*\*消磁 (Degaussing)\*\* 适用于磁性存储介质（如硬盘），但不适用于闪存卡。

- \*\*物理破坏 (Physical destruction)\*\* 虽然可以确保数据无法恢复，但会破坏闪存卡，无法重复使用。

- \*\*重新格式化 (Reformatting)\*\* 并不能完全安全地删除数据，因为数据可能仍然可以通过特殊工具恢复。

因此，\*\*加密粉碎\*\*是既安全又允许闪存卡重复使用的最佳方法。

-------------------

题目15：Carlos正在调查其组织中的敏感信息。他认为攻击者设法从数据库检索所有员工的信息，并在基于Web的人员管理系统的日志条目中查找以下用户提供的输入：

Collins’＆1 = 1; --

这发生了什么类型的攻击，以及如何预防？

Carlos is investigating the compromise of sensitive information in his organization. He believes that attackers managed to retrieve personnel information on all employees from the database and finds the following user-supplied input in a log entry for a web-based personnel management system:

Collins’&1=1;&ndash;&ndash;

What type of attack took place, and how could it be prevented?

A：SQL注入，使用存储过程

SQL injection, use of stored procedures

B：缓冲区溢出，自动扩展缓冲区

Buffer overflow, automatic buffer expansion

C：跨站脚本，开启Web服务器的XSS防护

Cross-site scripting, turning on XSS prevention on the web server

D：跨站请求伪造，需要已签名的请求

Cross-site request forgery, requiring signed requests

答案:这个问题的正确答案是：

A：SQL注入，使用存储过程

SQL injection, use of stored procedures

解释：

- \*\*SQL注入攻击\*\*：攻击者通过在输入字段中插入恶意SQL代码来操纵数据库查询。在这个例子中，`Collins’&1=1;&ndash;&ndash;` 是一个典型的SQL注入尝试。`1=1` 是一个永远为真的条件，`--` 是SQL中的注释符号，用于忽略后续的查询部分。这种攻击可能导致数据库泄露敏感信息。

- \*\*预防措施\*\*：

- \*\*使用存储过程\*\*：存储过程可以预编译SQL语句，减少SQL注入的风险。

- \*\*参数化查询\*\*：使用参数化查询可以防止用户输入被解释为SQL代码。

- \*\*输入验证\*\*：对用户输入进行严格的验证和过滤，确保输入符合预期的格式和类型。

- \*\*最小权限原则\*\*：数据库用户应仅具有执行其任务所需的最小权限，以减少攻击的影响范围。

其他选项的解释：

- \*\*B：缓冲区溢出\*\*：与SQL注入无关，通常涉及内存操作。

- \*\*C：跨站脚本（XSS）\*\*：涉及在网页中注入恶意脚本，与SQL注入不同。

- \*\*D：跨站请求伪造（CSRF）\*\*：涉及伪造用户请求，与SQL注入不同。

因此，正确答案是A。

-------------------

题目16：以下哪一项是详细的分步骤文件，描述个人必须完成的确切行动？

Which one of the following is a detailed, step-by-step document that describes the exact actions that individuals must complete?

A：策略

Policy

B：标准

Standard

C：准则

Guideline

D：程序

Procedure

答案:正确答案是 D：程序 (Procedure)。

解释：

- \*\*策略 (Policy)\*\*：是高层级的指导原则，通常不涉及具体的操作步骤。

- \*\*标准 (Standard)\*\*：是具体的规范或要求，通常用于确保一致性，但不一定详细描述每一步操作。

- \*\*准则 (Guideline)\*\*：是建议性的指导，通常提供灵活性，不强制要求严格执行。

- \*\*程序 (Procedure)\*\*：是详细的分步骤文件，明确描述个人必须完成的确切行动，通常用于确保任务的一致性和可重复性。

因此，程序是最符合题目描述的选项。

-------------------

题目17：CIS基准在组织中经常用于什么目的？

What purpose are the CIS benchmarks frequently used for in organizations?

A：安全编码标准

Secure coding standards

B：性能测试

Performance testing

C：基线

Baselining

D：监控度量

Monitoring metrics

答案:CIS基准（Center for Internet Security Benchmarks）是一组最佳实践和配置指南，旨在帮助组织提高其信息系统的安全性。这些基准通常用于以下目的：

C：基线（Baselining）

CIS基准用于建立安全配置的基线，确保系统按照最佳实践进行配置，从而减少潜在的安全风险。通过遵循这些基准，组织可以确保其系统配置符合行业标准，并能够抵御常见的安全威胁。因此，CIS基准在组织中主要用于基线配置和安全加固。

-------------------

题目18：Bryan有一套他希望避免公开披露的敏感文件。他想要使用一个控制，如果文档出现在公共论坛中，可用于跟踪最初泄露文档副本的人。什么安全控制将最好地实现这一目的？

Bryan has a set of sensitive documents that he would like to protect from public disclosure. He would like to use a control that, if the documents appear in a public forum, may be used to trace the leak back to the person who was originally given the document copy. What security control would best fulfill this purpose?

A：数字签名

Digital signature

B：文件染色

Document staining

C：散列

Hashing

D：水印

Watermarking

答案:Bryan 希望使用一种安全控制，能够在敏感文件被泄露到公共论坛时，追踪到最初泄露文档副本的人。这种控制需要能够在文档被公开时识别出特定的副本来源。

让我们逐一分析选项：

A. \*\*数字签名 (Digital signature)\*\*

数字签名主要用于验证文档的完整性和真实性，确保文档未被篡改，并且可以确认文档的来源。然而，数字签名并不能帮助追踪到具体的副本泄露者。

B. \*\*文件染色 (Document staining)\*\*

文件染色是一种技术，通过在文档中嵌入独特的标识符（如用户ID、时间戳等），使得每个副本都具有唯一的标记。如果文档被泄露，可以通过这些标识符追踪到具体的副本来源。这正符合Bryan的需求。

C. \*\*散列 (Hashing)\*\*

散列是一种用于验证数据完整性的技术，通常用于检测文件是否被篡改。散列并不能用于追踪具体的副本来源。

D. \*\*水印 (Watermarking)\*\*

水印是一种在文档中嵌入可见或不可见标识的技术，通常用于版权保护或防止未经授权的复制。虽然水印可以用于追踪文档的来源，但它通常不如文件染色那样精确地追踪到具体的副本泄露者。

综上所述，\*\*文件染色 (Document staining)\*\* 是最适合Bryan需求的安全控制，因为它可以在文档泄露时追踪到具体的副本来源。

\*\*正确答案：D.\*

-------------------

题目19：Carlos正在规划一个将在一个新的四层公司总部内建造的数据中心。该建筑由地下室和三个地面楼层组成。数据中心的最佳位置是什么？

Carlos is planning a design for a data center that will be constructed within a new fourstory corporate headquarters. The building consists of a basement and three above-ground floors. What is the best location for the data center?

A：地下室

Basement

B：一楼

First floor

C：二楼

Second floor

D：三楼

Third floor

答案:在设计数据中心时，选择最佳位置需要考虑多个因素，包括安全性、环境控制、物理访问、电力供应和网络连接等。对于Carlos正在规划的四层公司总部，以下是各楼层的优缺点分析：

1. \*\*地下室（Basement）\*\*：

- \*\*优点\*\*：地下室通常较为隐蔽，安全性较高，不易受到外部物理攻击。此外，地下室通常温度较低，有助于数据中心的冷却。

- \*\*缺点\*\*：地下室可能存在洪水风险，尤其是在降雨量大的地区。此外，地下室的通风和排水系统需要特别注意。

2. \*\*一楼（First floor）\*\*：

- \*\*优点\*\*：一楼通常便于物理访问，适合需要频繁维护的设备。此外，一楼的电力供应和网络连接通常较为稳定。

- \*\*缺点\*\*：一楼可能更容易受到外部物理攻击，安全性较低。此外，一楼的环境控制（如温度和湿度）可能不如地下室稳定。

3. \*\*二楼（Second floor）\*\*：

- \*\*优点\*\*：二楼相对于一楼来说，安全性较高，且环境控制较为稳定。此外，二楼通常不会受到洪水的影响。

- \*\*缺点\*\*：二楼的物理访问可能不如一楼方便，尤其是在需要搬运大型设备时。

4. \*\*三楼（Third floor）\*\*：

- \*\*优点\*\*：三楼的安全性最高，几乎不受外部物理攻击的影响。此外，三楼的环境控制通常非常稳定。

- \*\*缺点\*\*：三楼的物理访问最为不便，尤其是在需要频繁维护或搬运大型设备时。此外，三楼的电力供应和网络连接可能需要额外的考虑。

\*\*综合考虑\*\*，\*\*地下室\*\*通常是数据中心的最佳选择，因为它提供了较高的安全性和较低的环境温度，有助于数据中心的冷却。然而，必须确保地下室的防洪措施和通风系统设计得当，以应对潜在的风险。

因此，最佳答案是：

\*\*二楼

-------------------

题目20：Chris是一家大公司的信息安全专家，当他走进大楼时，他注意到一个安全区域的大门已经开了。物理安全不属于他的责任，但他立即采取行动，关闭门，并通知物理安全团队。Chris的行动体现了什么原则？

Chris is an information security professional for a major corporation, and as he is walking into the building, he notices that the door to a secure area has been left ajar. Physical security does not fall under his responsibility, but he takes immediate action by closing the door and informing the physical security team of his action. What principle is Chris demonstrating?

A：应尽关注

Due care

B：通过环境设计预防犯罪

Crime prevention through environmental design

C：职责分离

Separation of duties

D：知情同意

Informed consent

答案:Chris的行动体现了“应尽关注”（Due care）的原则。应尽关注是指在特定情况下，一个人应当采取合理的措施来防止可能发生的损害或风险。尽管物理安全不是Chris的直接职责，但他注意到了潜在的安全风险，并采取了适当的行动来减轻这种风险，这显示了他对公司的整体安全负有责任感和关注。

其他选项的解释如下：

- \*\*通过环境设计预防犯罪（Crime prevention through environmental design）\*\*：这是一种通过设计和环境管理来减少犯罪机会的策略，与Chris的行为不直接相关。

- \*\*职责分离（Separation of duties）\*\*：这是一种内部控制机制，旨在通过将关键任务分配给不同的人员来防止欺诈和错误，与Chris的行为无关。

- \*\*知情同意（Informed consent）\*\*：这通常涉及在收集、使用或披露个人信息之前获得个人的明确同意，与Chris的行为无关。

因此，正确答案是 \*\*A：应尽关注（Due care）\*\*。

-------------------

题目21：以下哪种调查类型总是使用超出合理怀疑的证据标准？

Which one of the following investigation types always uses the beyond-a-reasonable-doubt standard of proof?

A：民事调查

Civil investigation

B：刑事调查

Criminal investigation

C：业务调查

Operational investigation

D：监管调查

Regulatory investigation

答案:正确答案是 B：刑事调查 (Criminal investigation)。

在刑事调查中，证据标准通常是“超出合理怀疑”（beyond a reasonable doubt），这是最高的证据标准，要求证据必须非常充分，以至于没有任何合理的怀疑可以存在。这种标准用于确保只有在证据非常确凿的情况下，才能对被告定罪。

其他选项的说明：

- A：民事调查 (Civil investigation) 通常使用“优势证据”（preponderance of the evidence）标准，即证据更有可能支持一方的主张。

- C：业务调查 (Operational investigation) 和 D：监管调查 (Regulatory investigation) 通常使用较低的证据标准，如“合理怀疑”（reasonable suspicion）或“合理依据”（probable cause），具体取决于调查的性质和目的。

因此，B 是唯一一个总是使用“超出合理怀疑”证据标准的调查类型。

-------------------

题目22：Kristen想要使用多个站点来处理她的数据，但不想为一个完整的数据中心付费。如果她希望能够将部分自定义应用程序环境快速迁移到多个国家/地区的设施，而无需等待发货或购买硬件，那么你会推荐以下哪选作为她的最佳选择？

Kristen wants to use multiple processing sites for her data, but does not want to pay for a full data center. Which of the following options would you recommend as her best option if she wants to be able to quickly migrate portions of her custom application environment to facilities in multiple countries without having to wait to ship or acquire hardware?

A：云PaaS供应商

A cloud PaaS vendor

B：托管数据中心提供商

A hosted data center provider

C：云IaaS供应商

A cloud IaaS vendor

D：提供机架、电源和远程操作服务的数据中心供应商

A data center vendor that provides rack, power, and remote hands services

答案:Kristen 的需求是能够快速迁移部分自定义应用程序环境到多个国家/地区的设施，而不需要等待发货或购买硬件。这意味着她需要一个灵活、可扩展且无需管理物理硬件的解决方案。

- \*\*A：云PaaS供应商\*\*

PaaS（平台即服务）提供应用程序开发和部署的平台，但通常限制了用户对底层基础设施的控制。虽然PaaS可以快速部署应用程序，但它可能不适合需要高度自定义环境的需求。

- \*\*B：托管数据中心提供商\*\*

托管数据中心提供商通常提供物理服务器和基础设施的租赁服务。虽然这可以满足部分需求，但它仍然需要物理硬件的部署和管理，无法满足快速迁移和无需购买硬件的需求。

- \*\*C：云IaaS供应商\*\*

IaaS（基础设施即服务）提供了虚拟化的计算资源，允许用户快速创建、迁移和管理虚拟机。IaaS提供了高度的灵活性和可扩展性，能够满足Kristen快速迁移应用程序环境到多个国家/地区的需求，且无需购买或管理物理硬件。

- \*\*D：提供机架、电源和远程操作服务的数据中心供应商\*\*

这种服务仍然依赖于物理硬件，无法满足快速迁移和无需购买硬件的需求。

因此，\*\*C：云IaaS供应商\*\* 是最佳选择，因为它提供了灵活的基础设施，能够快速迁移应用程序环境到多个国家/地区，且无需购买或管理物理硬件。

-------------------

题目23：什么类型的备用处理设施包含恢复操作所需的硬件，但没有当前的数据副本？

What type of alternate processing facility contains the hardware necessary to restore operations but does not have a current copy of data?

A：热站点

Hot site

B：温站点

Warm site

C：冷站点

Cold site

D：移动网站

Mobile site

答案:题目问的是哪种备用处理设施包含恢复操作所需的硬件，但没有当前的数据副本。根据选项：

A. 热站点（Hot site）通常包含所有必要的硬件和最新的数据副本，可以立即恢复操作。

B. 温站点（Warm site）包含恢复操作所需的硬件，但数据可能不是最新的，需要从备份中恢复。

C. 冷站点（Cold site）只包含基本的硬件设施，没有数据副本，需要较长时间来恢复操作。

D. 移动网站（Mobile site）通常是指可以移动的设施，可能包含硬件和数据，但具体配置取决于具体情况。

根据题目描述，温站点（Warm site）最符合“包含恢复操作所需的硬件，但没有当前的数据副本”这一条件。

所以，正确答案是：

B：温站点

Warm site

-------------------

题目24：下列哪个术语描述了一段短暂的高电压过程？

Which one of the following terms describes a period of momentary high voltage?

A：下降

Sag

B：断电

Brownout

C：尖峰

Spike

D：浪涌

Surge

答案:正确答案是：

C：尖峰 (Spike)

解释：

- \*\*尖峰 (Spike)\*\*：描述了一段非常短暂的高电压过程，通常持续几毫秒到几微秒。

- \*\*下降 (Sag)\*\*：指的是电压的短暂下降。

- \*\*断电 (Brownout)\*\*：指的是电压的持续降低，通常持续几秒到几分钟。

- \*\*浪涌 (Surge)\*\*：指的是电压的持续升高，通常持续几毫秒到几秒。

因此，描述一段短暂的高电压过程的术语是 \*\*尖峰 (Spike)\*\*。

-------------------

题目25：Greg需要标记用于其公司医疗保险索赔数据库的驱动器。以下选项中的哪个数据标签与他正在处理的数据类型最匹配？

Greg needs to label drives used for his company’s medical insurance claims database. What data label from the following list best matches the type of data he is dealing with?

A：PII

PII

B：秘密

Secret

C：商业机密

Business confidential

D：PHI

PHI

答案:题目25的正确答案是：

D：PHI

解释：

PHI（Protected Health Information）是指受保护的健康信息，包括与个人健康相关的任何信息，如医疗记录、保险索赔等。由于Greg正在处理的是医疗保险索赔数据库，这些数据属于PHI的范畴。PII（Personally Identifiable Information）虽然也涉及个人身份信息，但PHI更具体地涵盖了与健康相关的信息。秘密（Secret）和商业机密（Business confidential）虽然也是数据分类的标签，但它们不专门针对健康信息。因此，PHI是最匹配的标签。

-------------------

题目26：开放最短路径优先(OSPF)协议是路由协议，保持所有连接的远程网络的映射，并使用该映射选择到远程目的地的最短路径。什么类型的路由协议是OSPF？

The Open Shortest Path First (OSPF) protocol is a routing protocol that keeps a map of all connected remote networks and uses that map to select the shortest path to a remote destination. What type of routing protocol is OSPF?

A：链路状态

Link state

B：最短路径优先

Shortest path first

C：链接映射

Link mapping

D：距离矢量

Distance vector

答案:OSPF（开放最短路径优先）协议是一种链路状态路由协议。链路状态路由协议通过收集网络中所有路由器的链路状态信息来构建网络的完整拓扑图，并使用该拓扑图来计算最短路径。因此，正确答案是：

A：链路状态

Link state

-------------------

题目27：Selah希望确保车辆不会撞到她公司的入口和前厅，同时仍可供行人、轮椅或其他可移动装置进入。什么最适合这个目的？

Selah wants to ensure that vehicles cannot crash through into her company’s entryway and front lobby while still remaining accessible to pedestrians and wheelchairs or other mobility devices. What c best suited to this purpose?

A：围栏

Fences

B：护柱

Bollards

C：墙壁

Walls

D：楼梯

Stairs

答案:题目要求Selah确保车辆不会撞到公司的入口和前厅，同时仍可供行人、轮椅或其他可移动装置进入。我们需要选择一个既能阻挡车辆，又不会妨碍行人通行的选项。

A：围栏（Fences）通常用于划定边界，但可能无法有效阻挡车辆，尤其是高速行驶的车辆。

B：护柱（Bollards）是一种坚固的柱子，通常用于阻挡车辆进入特定区域，同时允许行人通过。护柱可以有效防止车辆撞击，同时不会妨碍行人、轮椅或其他可移动装置的通行。

C：墙壁（Walls）虽然可以阻挡车辆，但通常会完全封闭空间，可能不适合需要保持行人通行的情况。

D：楼梯（Stairs）显然不适合，因为楼梯不仅不能阻挡车辆，还会妨碍轮椅和其他移动装置的通行。

因此，最适合的选项是 \*\*B：护柱（Bollards）\*\*。

-------------------

题目28-1：参考以下场景，回答5个问题：

Concho Controls是一家专注于楼宇自动化系统的中型企业。它在其内部部署数据中心内托管一组本地文件服务器，用于存储客户建议、构建计划、产品信息以及对其业务运营至关重要的其他数据。

Tara在Concho Controls IT部门工作，负责设计和实施组织的备份策略以及其他任务。她目前在每个星期日晚上8点进行完全备份，星期一至星期五中午进行差异备份。

Concho的服务器在星期三下午3点发生故障。Tara重建服务器，并希望从备份中恢复数据。

For questions , please refer to the following scenario:

Concho Controls is a midsize business focusing on building automation systems. It hosts a set of local file servers in its on-premises data center that store customer proposals, building plans, product information, and other data that is critical to their business operations.

Tara works in the Concho Controls IT department and is responsible for designing and implementing the organization’s backup strategy, among other tasks. She currently conducts full backups every Sunday evening at 8 p.m. and differential backups on Monday through Friday at noon.

Concho experiences a server failure at 3 p.m. on Wednesday. Tara rebuilds the server and wants to restore data from the backups.

Tara首先应该将哪些备份应用于服务器？

What backup should Tara apply to the server first?

A：星期天的完全备份

Sunday’s full backup

B：星期一的差异备份

Monday’s differential backup

C：星期二的差异备份

Tuesday’s differential backup

D：星期三的差异备份

Wednesday’s differential backup

答案:Tara首先应该将星期天的完全备份应用于服务器。这是因为完全备份包含了所有数据的完整副本，是恢复数据的基础。在应用完全备份之后，Tara可以继续应用星期三的差异备份，以恢复自完全备份以来所做的更改。

因此，正确答案是：

A：星期天的完全备份

Sunday's full backup

-------------------

题目28-1：参考以下场景，回答5个问题：

Concho Controls是一家专注于楼宇自动化系统的中型企业。它在其内部部署数据中心内托管一组本地文件服务器，用于存储客户建议、构建计划、产品信息以及对其业务运营至关重要的其他数据。

Tara在Concho Controls IT部门工作，负责设计和实施组织的备份策略以及其他任务。她目前在每个星期日晚上8点进行完全备份，星期一至星期五中午进行差异备份。

Concho的服务器在星期三下午3点发生故障。Tara重建服务器，并希望从备份中恢复数据。

For questions , please refer to the following scenario:

Concho Controls is a midsize business focusing on building automation systems. It hosts a set of local file servers in its on-premises data center that store customer proposals, building plans, product information, and other data that is critical to their business operations.

Tara works in the Concho Controls IT department and is responsible for designing and implementing the organization’s backup strategy, among other tasks. She currently conducts full backups every Sunday evening at 8 p.m. and differential backups on Monday through Friday at noon.

Concho experiences a server failure at 3 p.m. on Wednesday. Tara rebuilds the server and wants to restore data from the backups.

Tara必须将总共多少备份应用到系统，以使其包含的数据尽可能是最新的？

How many backups in total must Tara apply to the system to make the data it contains as current as possible?

A：1

1

B：2

2

C：3

3

D：4

4

答案:为了将数据恢复到尽可能最新的状态，Tara需要应用以下备份：

1. \*\*完全备份\*\*：这是在上周日晚上8点进行的备份，包含了所有数据的完整副本。

2. \*\*差异备份\*\*：差异备份会备份自上次完全备份以来所有发生变化的数据。Tara在周一、周二和周三中午都进行了差异备份。

由于服务器在周三下午3点发生故障，Tara需要应用以下备份：

- 上周日的完全备份

- 周三中午的差异备份（因为周三的差异备份包含了自周日完全备份以来所有的变化）

因此，Tara总共需要应用 \*\*2个备份\*\*（完全备份 + 周三的差异备份）来使数据尽可能最新。

正确答案是：\*\*B：2\*\*

-------------------

题目28-1：参考以下场景，回答5个问题：

Concho Controls是一家专注于楼宇自动化系统的中型企业。它在其内部部署数据中心内托管一组本地文件服务器，用于存储客户建议、构建计划、产品信息以及对其业务运营至关重要的其他数据。

Tara在Concho Controls IT部门工作，负责设计和实施组织的备份策略以及其他任务。她目前在每个星期日晚上8点进行完全备份，星期一至星期五中午进行差异备份。

Concho的服务器在星期三下午3点发生故障。Tara重建服务器，并希望从备份中恢复数据。

For questions , please refer to the following scenario:

Concho Controls is a midsize business focusing on building automation systems. It hosts a set of local file servers in its on-premises data center that store customer proposals, building plans, product information, and other data that is critical to their business operations.

Tara works in the Concho Controls IT department and is responsible for designing and implementing the organization’s backup strategy, among other tasks. She currently conducts full backups every Sunday evening at 8 p.m. and differential backups on Monday through Friday at noon.

Concho experiences a server failure at 3 p.m. on Wednesday. Tara rebuilds the server and wants to restore data from the backups.

在这种备份方法中，可能会不可恢复地丢失一些数据。所做的任何更改将会丢失的时间段有多长？

In this backup approach, some data may be irretrievably lost. How long is the time period where any changes made will have been lost?

A：3 小时

3 hours.

B：5 小时

5 hours.

C：8 小时

8 hours.

D：数据不会丢失

No data will be lost.

答案:在这种备份方法中，Tara在星期三中午进行了差异备份，而服务器在下午3点发生故障。因此，从中午12点到下午3点之间的数据更改将不会被备份，这意味着这些更改可能会丢失。

所以，可能会丢失的数据更改的时间段是3小时。

正确答案是：

A：3 小时

3 hours.

-------------------

题目28-1：参考以下场景，回答5个问题：

Concho Controls是一家专注于楼宇自动化系统的中型企业。它在其内部部署数据中心内托管一组本地文件服务器，用于存储客户建议、构建计划、产品信息以及对其业务运营至关重要的其他数据。

Tara在Concho Controls IT部门工作，负责设计和实施组织的备份策略以及其他任务。她目前在每个星期日晚上8点进行完全备份，星期一至星期五中午进行差异备份。

Concho的服务器在星期三下午3点发生故障。Tara重建服务器，并希望从备份中恢复数据。

For questions , please refer to the following scenario:

Concho Controls is a midsize business focusing on building automation systems. It hosts a set of local file servers in its on-premises data center that store customer proposals, building plans, product information, and other data that is critical to their business operations.

Tara works in the Concho Controls IT department and is responsible for designing and implementing the organization’s backup strategy, among other tasks. She currently conducts full backups every Sunday evening at 8 p.m. and differential backups on Monday through Friday at noon.

Concho experiences a server failure at 3 p.m. on Wednesday. Tara rebuilds the server and wants to restore data from the backups.

如果Tara遵循相同的计划，但将差异备份切换为增量备份，则她需要将多少备份应用到系统，以使其包含的数据尽可能是最新的？

If Tara followed the same schedule but switched the differential backups to incremental backups, how many backups in total would she need to apply to the system to make the data it contains as current as possible?

A：1

1

B：2

2

C：3

3

D：4

4

答案:在Tara的备份策略中，如果她将差异备份切换为增量备份，那么在服务器发生故障后恢复数据时，她需要应用的备份数量会有所不同。

1. \*\*完全备份\*\*：每周日晚上8点进行完全备份，这是所有数据的基础备份。

2. \*\*增量备份\*\*：从周一到周五中午进行增量备份，每次增量备份只备份自上次备份以来发生变化的数据。

在服务器发生故障时（星期三下午3点），Tara需要恢复的数据包括：

- 上周日的完全备份（包含所有数据）。

- 周一中午的增量备份（包含自周日以来变化的数据）。

- 周二中午的增量备份（包含自周一以来变化的数据）。

- 周三中午的增量备份（包含自周二以来变化的数据）。

因此，Tara需要应用以下备份来恢复数据：

1. 上周日的完全备份。

2. 周一中午的增量备份。

3. 周二中午的增量备份。

4. 周三中午的增量备份。

总共需要应用 \*\*4\*\* 个备份。

所以，正确答案是：

\*\*D：4\*\*

-------------------

题目28-1：参考以下场景，回答5个问题：

Concho Controls是一家专注于楼宇自动化系统的中型企业。它在其内部部署数据中心内托管一组本地文件服务器，用于存储客户建议、构建计划、产品信息以及对其业务运营至关重要的其他数据。

Tara在Concho Controls IT部门工作，负责设计和实施组织的备份策略以及其他任务。她目前在每个星期日晚上8点进行完全备份，星期一至星期五中午进行差异备份。

Concho的服务器在星期三下午3点发生故障。Tara重建服务器，并希望从备份中恢复数据。

For questions , please refer to the following scenario:

Concho Controls is a midsize business focusing on building automation systems. It hosts a set of local file servers in its on-premises data center that store customer proposals, building plans, product information, and other data that is critical to their business operations.

Tara works in the Concho Controls IT department and is responsible for designing and implementing the organization’s backup strategy, among other tasks. She currently conducts full backups every Sunday evening at 8 p.m. and differential backups on Monday through Friday at noon.

Concho experiences a server failure at 3 p.m. on Wednesday. Tara rebuilds the server and wants to restore data from the backups.

如果Tara做出了从差异备份到增量备份的更改，我们假设每天都有相同的信息变化，下列哪个文件将是最大的？

If Tara made the change from differential to incremental backups and we assume that the same amount of information changes each day, which one of the following files would be the largest?

A：星期一的增量备份

Monday’s incremental backup.

B：星期二的增量备份

Tuesday’s incremental backup.

C：星期三的增量备份

Wednesday’s incremental backup.

D：所有三个将是相同的大小

All three will be the same size.

答案:在增量备份策略中，每次备份只包含自上次备份以来发生变化的数据。因此，如果每天都有相同的信息变化，那么每天的增量备份文件大小应该是相同的。

因此，正确答案是：

D：所有三个将是相同的大小

All three will be the same size.

-------------------

题目29：下图显示了一个攻击示例，攻击者Mal将流量从用户系统重定向到他们自己的系统，从而能让他们读取到TLS加密流量。以下什么术语最能描述这种攻击？

The following figure shows an example of an attack where Mal, the attacker, has redirected traffic from a user’s system to their own, allowing them to read TLS encrypted traffic. Which of the following terms best describes this attack?

<div style="text-align:center"><img alt="" height="236" src="/file/100000/m/20210906/5c5082099cb4435fa286b9e1098e48c3.png" width="484" /></div>

A：DNS劫持攻击

A DNS hijacking attack

B：ARP欺骗攻击

An ARP spoofing attack

C：中间人攻击

A man-in-the-middle attack

D：SQL注入攻击

A SQL injection attack

答案:这个攻击示例中，攻击者Mal将流量从用户系统重定向到他们自己的系统，从而能够读取到TLS加密流量。这种攻击方式最符合“中间人攻击”（Man-in-the-Middle Attack）的描述。

中间人攻击是指攻击者在通信双方之间插入自己，使得双方都以为自己在直接与对方通信，而实际上通信内容被攻击者截获、篡改或伪造。在这个例子中，攻击者Mal通过重定向流量，使得用户的加密流量经过自己的系统，从而能够解密和读取这些流量。

因此，正确答案是：

C：中间人攻击

A man-in-the-middle attack

-------------------

题目30：Bob负责编写一份策略，描述应保存多长时间的数据以及何时应清除数据。这体现了以下哪个概念？

Bob has been tasked with writing a policy that describes how long data should be kept and when it should be purged. What concept does this policy deal with?

A：数据剩余

Data remanence

B：记录保留

Record retention

C：数据编辑

Data redaction

D：审计日志

Audit logging

答案:题目30的正确答案是：

B：记录保留

Record retention

解析：

Bob负责编写的策略描述了数据应保存多长时间以及何时应清除数据，这直接涉及到“记录保留”（Record retention）的概念。记录保留是指组织根据法律、法规或业务需求，制定数据保存和销毁的政策和程序。这包括确定不同类型数据的保存期限以及在达到保存期限后如何安全地销毁数据。

其他选项的解释：

A：数据剩余（Data remanence）指的是数据在存储介质上被删除后仍然残留的现象。

C：数据编辑（Data redaction）是指从文档或数据中删除敏感信息的过程。

D：审计日志（Audit logging）是指记录系统活动和事件的日志，用于监控和审查系统的使用情况。

-------------------

题目31：IPSec的哪个组件提供身份验证、完整性和不可否认性？

Which component of IPsec provides authentication, integrity, and nonrepudiation?

A：L2TP

L2TP

B：封装安全有效载荷

Encapsulating Security Payload

C：加密安全头

Encryption Security Header

D：身份验证头

Authentication Header

答案:正确答案是 D：身份验证头 (Authentication Header, AH)。

IPSec（Internet Protocol Security）是一种用于保护IP通信的协议套件，它提供了身份验证、数据完整性保护和不可否认性等功能。IPSec主要由两个组件组成：

1. \*\*身份验证头 (Authentication Header, AH)\*\*：提供数据完整性、身份验证和防止重放攻击。AH通过使用哈希函数（如MD5或SHA-1）来生成一个消息认证码（MAC），确保数据在传输过程中没有被篡改，并且可以验证发送方的身份。

2. \*\*封装安全有效载荷 (Encapsulating Security Payload, ESP)\*\*：提供数据加密、数据完整性、身份验证和防止重放攻击。ESP不仅可以加密数据，还可以提供与AH类似的身份验证和完整性保护功能。

选项A的L2TP（Layer 2 Tunneling Protocol）是一种用于创建虚拟专用网络（VPN）的协议，但它本身并不提供身份验证、完整性和不可否认性。

选项C的“加密安全头”并不是IPSec的标准组件。

因此，正确答案是 D：身份验证头 (Authentication Header)。

-------------------

题目32：Renee注意到她的网络上的一个系统最近在短时间内从单个系统接收了所有65536个TCP端口的连接尝试。Renee最可能遇到什么类型的攻击？

Renee notices that a system on her network recently received connection attempts on all 65,536 TCP ports from a single system during a short period of time. What type of attack did Renee most likely experience?

A：拒绝服务

Denial-of-service

B：侦察

Reconnaissance

C：恶意内部人

Malicious insider

D：破坏

Compromise

答案:Renee最可能遇到的攻击类型是 \*\*B：侦察（Reconnaissance）\*\*。

### 解释：

- \*\*侦察攻击\*\* 通常是指攻击者试图收集目标系统的信息，以便为后续的攻击做准备。在这种情况下，攻击者通过扫描目标系统的所有65536个TCP端口，试图找出哪些端口是开放的、哪些服务正在运行，以及可能存在的漏洞。这种扫描行为是典型的侦察活动。

- \*\*拒绝服务（Denial-of-service）\*\* 通常是指攻击者试图通过大量请求或流量使目标系统无法正常提供服务。虽然端口扫描可能会对系统造成一定的负载，但它的主要目的并不是使系统瘫痪，而是收集信息。

- \*\*恶意内部人（Malicious insider）\*\* 和 \*\*破坏（Compromise）\*\* 通常涉及已经获得系统访问权限的攻击者，而题目中描述的行为更像是外部攻击者进行的初步侦察。

因此，最合适的答案是 \*\*B：侦察（Reconnaissance）\*\*。

-------------------

题目33：下列哪项Windows的审计记录包含操作系统关机或业务停止等事件？

What type of Windows audit record describes events like an OS shutdown or a service being stopped?

A：应用日志

An application log

B：安全日志

A security log

C：系统日志

A system log

D：配置日志

A setup log

答案:正确答案是 C：系统日志 (A system log)。

系统日志记录了与操作系统相关的事件，包括系统启动、关机、服务启动或停止等。这些事件对于系统管理员来说非常重要，因为它们可以帮助诊断系统问题和监控系统状态。安全日志（B）主要记录与安全相关的事件，如登录尝试和权限更改；应用日志（A）记录由应用程序生成的事件；配置日志（D）通常记录与系统配置更改相关的事件。

-------------------

题目34：Melissa负责其组织的安全合规性工作，并被告知该组织在补丁发布一个月后才会安装 Windows补丁，除非存在零日漏洞正被积极利用。为什么公司会像这样延迟修补补丁？

Melissa is in charge of her organization security compliance efforts and has been told that the organization does not install Windows patches until a month has passed since the patch has been released unless there is a zero-day exploit that is being actively exploited. Why would the company delay patching like this?

A：为了尽量减少安装对业务的影响

To minimize business impact of the installation

B：为了识别补丁的任何缺陷

To allow any flaws with the patch to be identified

C：为了防止补丁中的恶意软件在被识别之前被安装

To prevent malware in the patches from being installed before it is identified

D：为了将补丁分发到所有系统

To allow the patch to be distributed to all systems

答案:题目34的正确答案是：

A：为了尽量减少安装对业务的影响

To minimize business impact of the installation

B：为了识别补丁的任何缺陷

To allow any flaws with the patch to be identified

解释：

- 选项A正确，因为延迟安装补丁可以减少对业务运营的潜在影响。立即安装补丁可能会导致系统不稳定或兼容性问题，从而影响业务连续性。

- 选项B也正确，因为延迟安装补丁可以让公司有时间观察补丁是否会导致任何问题或缺陷。这样可以避免在补丁发布后立即安装可能带来的风险。

- 选项C不正确，因为补丁通常是由可信的供应商（如微软）发布的，不太可能包含恶意软件。

- 选项D不正确，因为补丁的分发通常可以在较短时间内完成，不需要延迟一个月。

因此，最合适的答案是A和B。

-------------------

题目35：什么级别的RAID也被称为磁盘条带化？

What level of RAID is also known as disk striping?

A：RAID 0

RAID 0

B：RAID 1

RAID 1

C：RAID 5

RAID 5

D：RAID 10

RAID 10

答案:正确答案是：A：RAID 0

RAID 0 也被称为磁盘条带化（disk striping）。在RAID 0中，数据被分割成多个块，并分别存储在不同的磁盘上，这样可以提高读写性能，但没有冗余功能，因此不提供数据保护。

-------------------

题目36：Jacob通过访问账户有权访问的文件指针，使用有效但权限低的用户账户对系统执行攻击。在访问检查后，但在文件打开之前，他快速切换文件指针，使其指向用户账户无权访问的文件。这是什么类型的攻击？

Jacob executes an attack against a system using a valid but low-privilege user account by accessing a file pointer that the account has access to. After the access check, but before the file is opened, he quickly switches the file pointer to point to a file that the user account does not have access to. What type of attack is this?

A：TOC/TOU

TOC/TOU

B：特权蠕变

Permissions creep

C：假冒

Impersonation

D：链接交换

Link swap

答案:这个题目描述的攻击类型是 \*\*TOC/TOU\*\*（Time-of-Check to Time-of-Use，检查时间到使用时间的攻击）。

### 解释：

- \*\*TOC/TOU\*\* 是一种利用系统在检查资源权限和使用资源之间的时间差进行攻击的技术。攻击者在系统检查权限后，但在实际使用资源之前，快速更改资源的状态或指向，从而绕过权限检查。

- 在题目中，Jacob 在系统检查文件权限后，但在文件实际打开之前，快速切换文件指针，使其指向一个用户无权访问的文件，这正是 TOC/TOU 攻击的典型特征。

### 其他选项的解释：

- \*\*B：特权蠕变（Permissions creep）\*\*：通常指用户或进程逐渐积累更多权限的过程，与题目描述的攻击方式不符。

- \*\*C：假冒（Impersonation）\*\*：指攻击者冒充其他用户或进程的身份进行操作，与题目描述的攻击方式不符。

- \*\*D：链接交换（Link swap）\*\*：通常指攻击者通过更改符号链接或硬链接来指向不同的文件，虽然与文件指针有关，但不完全符合题目描述的 TOC/TOU 攻击。

因此，正确答案是 \*\*A：TOC/TOU\*\*。

-------------------

题目37：实现RAID级别0所需的最少磁盘数是多少？

What is the minimum number of disks required to implement RAID level 0?

A：1

1

B：2

2

C：3

3

D：5

5

答案:RAID级别0（RAID 0）是一种磁盘阵列技术，它通过将数据分块并分布在多个磁盘上来提高性能。RAID 0 不提供冗余，因此它不提供数据保护，但它的主要优势是提高了读写速度。

要实现RAID 0，至少需要 \*\*2个磁盘\*\*。这是因为RAID 0的工作原理是将数据分成块并交替存储在两个或多个磁盘上。如果只有一个磁盘，就无法实现数据的分块和分布，因此无法实现RAID 0。

所以，正确答案是：

\*\*B：2\*\*

-------------------

题目38：Fred的公司希望确保通过其中央电子邮件服务器发送的电子邮件的完整性。如果消息的机密性不重要，Fred应该建议什么解决方案？

Fred’s company wants to ensure the integrity of email messages sent via its central email servers. If the confidentiality of the messages is not critical, what solution should Fred suggest?

A：数字签名和加密所有消息，以确保完整性

Digitally sign and encrypt all messages to ensure integrity.

B：数字签名，但不加密所有消息

Digitally sign but don’t encrypt all messages.

C：使用TLS保护消息，确保其完整性

Use TLS to protect messages, ensuring their integrity.

D：使用散列算法在每个消息中提供散列，以证明它没有改变

Use a hashing algorithm to provide a hash in each message to prove that it hasn’t changed.

答案:题目38的正确答案是：

\*\*B：数字签名，但不加密所有消息\*\*

\*\*Digitally sign but don’t encrypt all messages.\*\*

### 解析：

- \*\*数字签名\*\*可以确保电子邮件的完整性，因为它允许接收方验证消息在传输过程中是否被篡改。数字签名通过使用发送方的私钥对消息进行签名，接收方可以使用发送方的公钥验证签名的有效性。

- \*\*加密\*\*主要用于确保消息的机密性，防止未经授权的人读取消息内容。由于题目中提到机密性不重要，因此不需要加密。

- \*\*TLS（传输层安全协议）\*\*主要用于保护数据在传输过程中的安全性，但它并不直接提供消息的完整性验证。

- \*\*散列算法\*\*可以用于验证消息的完整性，但它通常需要与数字签名结合使用，以确保散列值本身没有被篡改。单独使用散列算法并不能完全保证消息的完整性。

因此，\*\*数字签名但不加密\*\*是最合适的解决方案，因为它可以确保消息的完整性，同时不需要额外的加密开销。

-------------------

题目39：领导层要求Susan实施一个访问控制系统，该系统可以支持规则声明，例如”只允许在上午8点到下午6点之间从无线网络上的受管设备访问销售人员数据”，请问什么类型的访问控制系统是Susan的最佳选择？

The leadership at Susan’s company has asked her to implement an access control system that can support rule declarations like “Only allow access to salespeople from managed devices on the wireless network between 8 a.m. and 6 p.m.” What type of access control system would be Susan’s best choice?

A：ABAC

ABAC

B：RBAC

RBAC

C：DAC

DAC

D：MAC

MAC

答案:题目中提到的访问控制系统需要支持基于特定条件的规则声明，例如时间、设备类型和网络类型等。这种类型的访问控制通常被称为基于属性的访问控制（Attribute-Based Access Control, ABAC）。

ABAC 允许根据用户、资源、环境等多种属性来定义访问控制策略。例如，可以根据用户的角色、设备的状态、时间、位置等属性来决定是否允许访问。这与题目中描述的需求非常吻合。

其他选项的解释如下：

- \*\*RBAC（Role-Based Access Control）\*\*：基于角色的访问控制，主要根据用户的角色来决定访问权限，而不考虑其他属性（如时间、设备等）。

- \*\*DAC（Discretionary Access Control）\*\*：自主访问控制，允许资源的所有者自主决定谁可以访问资源，通常不涉及复杂的规则声明。

- \*\*MAC（Mandatory Access Control）\*\*：强制访问控制，通常用于高安全性环境，访问权限由系统管理员强制设定，用户无法更改。

因此，\*\*A：ABAC\*\* 是 Susan 的最佳选择。

-------------------

题目40：Nora的公司运行的服务器的生命周期为五年。根据该流程，当它们达到使用寿命时，服务器将被送到电子垃圾回收站。以下哪项是Nora可以实施的最有效控制措施，以确保不会因剩余数据而发生数据泄露？

Nora’s company operates servers on a five-year lifecycle. When they reach their end of life according to that process, the servers are sent to an e-waste recycler. Which of the following is the most effective control that Nora could implement to ensure that a data breach does not occur due to remanent data?

A：在服务器离开组织之前对驱动器进行零擦除

Zero wipe the drives before the servers leave the organization.

B：卸下驱动器并将其切碎

Remove the drives and shred them.

C：在将服务器发送给电子垃圾回收站之前重新格式化驱动器

Reformat the drives before the servers are sent to the e-waste company.

D：需要电子垃圾回收站出具处置证书

Require certificates of disposal from the e-waste company.

答案:在Nora的公司中，确保服务器在达到使用寿命并被送往电子垃圾回收站时不会因剩余数据而发生数据泄露，是一个重要的数据安全管理问题。我们来分析一下每个选项的有效性：

A：在服务器离开组织之前对驱动器进行零擦除

- 零擦除是一种数据销毁方法，通过将驱动器上的所有数据位设置为零来确保数据无法恢复。这是一种非常有效的数据销毁方法，可以防止数据泄露。

B：卸下驱动器并将其切碎

- 物理销毁驱动器（如切碎）是一种非常彻底的数据销毁方法，可以确保数据无法恢复。这种方法非常有效，但可能成本较高，且需要专门的设备。

C：在将服务器发送给电子垃圾回收站之前重新格式化驱动器

- 重新格式化驱动器并不能彻底销毁数据，因为数据仍然可以通过专业工具恢复。因此，这种方法不如零擦除或物理销毁有效。

D：需要电子垃圾回收站出具处置证书

- 虽然要求电子垃圾回收站出具处置证书可以确保驱动器被正确处理，但这并不能保证数据在离开组织之前已经被彻底销毁。因此，这种方法本身不足以防止数据泄露。

综上所述，最有效的控制措施是 \*\*A：在服务器离开组织之前对驱动器进行零擦除\*\*。这种方法既能有效销毁数据，又相对成本较低，易于实施。

\*\*最终答案：A：在服务器离开组织之前对驱动器进行零擦除\*\*

-------------------

题目41：Chris正在两个建筑物之间部署使用6类电缆的千兆位以太网。根据第6类标准可以运行电缆的最大距离是多少？

Chris is deploying a gigabit Ethernet network using Category 6 cable between two buildings. What is the maximum distance he can run the cable according to the Category 6 standard?

A：50米

50 meters

B：100米

100 meters

C：200米

200 meters

D：300米

300 meters

答案:根据第6类（Category 6）电缆的标准，千兆位以太网（Gigabit Ethernet）的最大传输距离是100米。因此，Chris在两个建筑物之间部署6类电缆时，电缆的最大长度不应超过100米。

正确答案是：

B：100米

100 meters

-------------------

题目42：Howard是一名安全分析师，与一位经验丰富的计算机取证调查员合作。调查员要求他检索取证驱动器控制器，但Howard无法在具有此名称的存储室中找到设备。什么是取证驱动器控制器的另一个名称？

Howard is a security analyst working with an experienced computer forensics investigator. The investigator asks him to retrieve a forensic drive controller, but Howard cannot locate a device in the storage room with this name. What is another name for a forensic drive controller?

A：RAID控制器

RAID controller

B：写阻塞器

Write blocker

C：SCSI终结器

SCSI terminator

D：取证装置分析仪

Forensic device analyzer

答案:正确答案是 B：写阻塞器（Write blocker）。

\*\*解释：\*\*

取证驱动器控制器（forensic drive controller）的另一个常见名称是写阻塞器（write blocker）。写阻塞器是一种硬件设备，用于在计算机取证过程中防止对原始存储设备（如硬盘驱动器）进行写操作。这样可以确保在取证过程中不会意外修改或损坏原始数据，从而保持数据的完整性和可采信性。

其他选项的解释：

- \*\*A：RAID控制器\*\* - RAID控制器用于管理和控制RAID阵列，与取证驱动器控制器的功能不同。

- \*\*C：SCSI终结器\*\* - SCSI终结器用于终止SCSI链路的信号，防止信号反射，与取证驱动器控制器的功能无关。

- \*\*D：取证装置分析仪\*\* - 这个选项并不是一个常见的术语，也不特指写阻塞器。

因此，正确答案是 B：写阻塞器（Write blocker）。

-------------------

题目43：Saria的开发团队正在开发的Web应用程序需要提供安全的会话管理，以防止使用应用程序所依赖的cookie来劫持会话。她最适合推荐以下哪种技术来防止这种情况？

The web application that Saria’s development team is working on needs to provide secure session management that can prevent hijacking of sessions using the cookies that the application relies on. Which of the following techniques would be the best for her to recommend to prevent this?

A：设置cookie的安全属性，从而强制TLS

Set the Secure attribute for the cookies, thus forcing TLS.

B：将域cookie属性设置为example.com，以限制对同一域中的服务器的cookie访问

Set the Domain cookie attribute to example.com to limit cookie access to servers in the same domain.

C：将Expires cookie属性设置为不到一周

Set the Expires cookie attribute to less than a week.

D：将HTTP-Only属性设置为仅需要未加密的会话

Set the HTTP-Only attribute to require only unencrypted sessions.

答案:为了提供安全的会话管理并防止会话劫持，Saria的开发团队应该采取以下措施：

\*\*A：设置cookie的安全属性，从而强制TLS\*\*

这是正确的选择。通过设置 `Secure` 属性，可以确保cookie只能通过HTTPS（即TLS加密的连接）传输，防止在未加密的HTTP连接中传输cookie，从而减少会话劫持的风险。

\*\*B：将域cookie属性设置为example.com，以限制对同一域中的服务器的cookie访问\*\*

虽然设置 `Domain` 属性可以限制cookie的访问范围，但它并不能直接防止会话劫持。它主要用于控制cookie在哪些子域中可用。

\*\*C：将Expires cookie属性设置为不到一周\*\*

设置 `Expires` 属性可以控制cookie的过期时间，但这并不能直接防止会话劫持。较短的过期时间可以减少cookie被滥用的时间窗口，但并不是防止会话劫持的主要手段。

\*\*D：将HTTP-Only属性设置为仅需要未加密的会话\*\*

这个选项的描述有误。`HTTP-Only` 属性的作用是防止客户端脚本（如JavaScript）访问cookie，从而减少跨站脚本攻击（XSS）的风险。它并不能强制使用未加密的会话，实际上，`HTTP-Only` 属性与加密无关。

\*\*最佳答案：A\*\*

设置 `Secure` 属性并强制使用TLS是最有效的防止会话劫持的方法之一。

-------------------

题目44：近期Ben公司的多功能打印机报废了。信息安全团队担心打印机的硬盘驱动器可能残留着一些数据，以下哪项技术术语用于描述该问题？

Ben’s company has recently retired its fleet of multifunction printers. The information security team has expressed concerns that the printers contain hard drives and that they may still have data from scans and print jobs. What is the technical term for this issue?

A：数据池

Data pooling

B：清除失败

Failed clearing

C：数据持久性

Data permanence

D：数据残留

Data remanence

答案:正确答案是 D：数据残留（Data remanence）。

数据残留（Data remanence）是指数据在存储介质（如硬盘驱动器）上被删除或覆盖后，仍然可能以某种形式残留的现象。在这种情况下，信息安全团队担心打印机的硬盘驱动器上可能仍然存有之前扫描和打印作业的数据，因此需要采取适当的措施来确保这些数据被彻底清除，以防止敏感信息泄露。

-------------------

题目45：以下哪种访问控制方案使用标签，在主体和客体上做标记，只有当主体和客体匹配成功时，才允许主体访问客体？

What access control scheme labels subjects and objects and allows subjects to access objects when the labels match?

A：DAC

DAC

B：MAC

MAC

C：基于规则的访问控制

Rule-based access control (RBAC)

D：基于角色的访问控制

Role-based access control (RBAC)

答案:正确答案是 B：MAC（Mandatory Access Control，强制访问控制）。

MAC 是一种访问控制方案，它在主体（如用户或进程）和客体（如文件或资源）上使用标签（通常是安全标签或安全级别）。只有当主体的标签与客体的标签匹配时，才允许主体访问客体。这种访问控制方式通常用于高安全级别的环境中，如军事或政府系统。

其他选项的解释：

- A：DAC（Discretionary Access Control，自主访问控制）允许资源的所有者决定谁可以访问资源，而不是基于标签匹配。

- C：基于规则的访问控制（Rule-based access control）是基于预定义的规则来决定访问权限，而不是基于标签匹配。

- D：基于角色的访问控制（Role-based access control, RBAC）是基于用户的角色来决定访问权限，而不是基于标签匹配。

-------------------

题目46：哪项基于云的服务提供以下功能：账户配置、管理、身份验证、授权、报告和监视？

A cloud-based service that provides account provisioning, management, authentication, authorization, reporting, and monitoring capabilities is known as what type of service?

A：PaaS

PaaS

B：IDaaS

IDaaS

C：IaaS

IaaS

D：SaaS

SaaS

答案:正确答案是 \*\*B：IDaaS\*\*。

\*\*IDaaS\*\*（Identity as a Service，身份即服务）是一种基于云的服务，提供账户配置、管理、身份验证、授权、报告和监视等功能。它主要用于管理用户的身份和访问权限，确保安全性和合规性。

其他选项的解释：

- \*\*PaaS\*\*（Platform as a Service，平台即服务）：提供开发和部署应用程序的平台。

- \*\*IaaS\*\*（Infrastructure as a Service，基础设施即服务）：提供虚拟化的计算资源，如服务器、存储和网络。

- \*\*SaaS\*\*（Software as a Service，软件即服务）：提供通过互联网访问的应用程序。

-------------------

题目47：Sally想提高组织的VOIP系统的安全性，请问她不需要担心以下哪种攻击？

Sally wants to secure her organization’s VoIP systems. Which of the following attacks is one that she shouldn’t have to worry about?

A：窃听

Eavesdropping

B：拒绝服务

Denial-of-service

C：黑箱

Blackboxing

D：来电显示欺骗

Caller ID spoofing

答案:在提高组织的VOIP系统安全性时，Sally需要考虑多种潜在的攻击类型。让我们逐一分析每个选项：

A：窃听（Eavesdropping） - 这是一种常见的攻击方式，攻击者可以截获并监听VOIP通话内容。因此，Sally需要采取措施来防止窃听。

B：拒绝服务（Denial-of-service） - 这种攻击旨在通过大量请求或恶意流量使VOIP系统无法正常工作，导致服务中断。Sally需要防范这种攻击以确保系统的可用性。

C：黑箱（Blackboxing） - 这个术语在信息安全领域并不常见，通常不用于描述VOIP系统的攻击类型。因此，Sally不需要特别担心这种攻击。

D：来电显示欺骗（Caller ID spoofing） - 这种攻击涉及伪造来电显示信息，使接收者误以为来电来自可信来源。Sally需要采取措施来防止这种欺骗行为。

综上所述，Sally不需要特别担心的是：

C：黑箱（Blackboxing）

-------------------

题目48：Marty发现：组织中的访问限制机制允许任何用户登录到任意一台工作站。请问该现象直接违反了哪种信息安全原则？

Marty discovers that the access restrictions in his organization allow any user to log into the workstation assigned to any other user, even if they are from completely different departments. This type of access most directly violates which information security principle?

A：职责分离

Separation of duties

B：双人控制

Two-person control

C：需知

Need to know

D：最小特权

Least privilege

答案:题目描述的现象是任何用户都可以登录到任意一台工作站，即使这些用户来自完全不同的部门。这种情况最直接违反了信息安全原则中的“最小特权”原则。

\*\*最小特权原则（Least Privilege）\*\* 是指用户或系统应该只拥有完成其工作所需的最小权限，而不应该拥有超出其工作范围的权限。这样可以减少潜在的安全风险，防止用户访问或操作他们不应该接触的资源。

在题目中，任何用户都可以登录到任意一台工作站，这意味着用户拥有超出其工作范围的权限，违反了最小特权原则。

因此，正确答案是：

\*\*D：最小特权\*\*

\*\*Least privilege\*\*

-------------------

题目49：Fred需要在两个服务器之间传输文件，但传输时的信道是不安全的。为此他考虑选择一个加密协议，以确保数据的安全性。请问他应该选择什么协议？

Fred needs to transfer files between two servers on an untrusted network. Since he knows the network isn’t trusted, he needs to select an encrypted protocol that can ensure that his data remains secure. What protocol should he choose?

A：SSH

SSH

B：TCP

TCP

C：SFTP

SFTP

D：IPsec

IPsec

答案:Fred 需要在两个服务器之间传输文件，并且信道是不安全的，因此他需要选择一个加密协议来确保数据的安全性。以下是各选项的分析：

- \*\*A: SSH\*\*

SSH（Secure Shell）是一种加密的网络协议，用于在不安全的网络中安全地传输数据。它提供了加密的通信通道，适合用于远程登录和文件传输。虽然SSH本身可以用于文件传输，但它通常用于远程命令执行和隧道传输。

- \*\*B: TCP\*\*

TCP（Transmission Control Protocol）是一种传输层协议，用于在网络中可靠地传输数据。然而，TCP本身并不提供加密功能，因此不适合用于在不安全的网络中传输敏感数据。

- \*\*C: SFTP\*\*

SFTP（SSH File Transfer Protocol）是基于SSH的文件传输协议，专门用于在不安全的网络中安全地传输文件。它提供了加密的文件传输功能，适合Fred的需求。

- \*\*D: IPsec\*\*

IPsec（Internet Protocol Security）是一种网络层协议，用于在网络层提供加密和认证。虽然IPsec可以用于保护数据传输，但它通常用于VPN等场景，而不是专门用于文件传输。

综合考虑，\*\*SFTP\*\* 是最适合Fred需求的协议，因为它专门用于在不安全的网络中安全地传输文件。

\*\*正确答案：C：SFTP\*\*

-------------------

题目50：Chris使用数据包嗅探器捕获来自TACACS +服务器的流量。他应该监控什么协议，可以监控到什么有用数据？

Chris uses a packet sniffer to capture traffic from a TACACS+ server. What protocol should he monitor, and what data should he expect to be readable?

A：UDP；没有任何有用的数据，因为TACACS +对整个会话加密

UDP; none&mdash;TACACS+ encrypts the full session.

B：TCP；没有任何有用的数据，因为TACACS +对整个会话加密

TCP; none&mdash;TACACS+ encrypts the full session.

C：UDP；除了用户名和密码之外的其他数据

UDP; all but the username and password, which are encrypted.

D：TCP；除了用户名和密码之外的其他数据

TCP; all but the username and password, which are encrypted.

答案:TACACS+（Terminal Access Controller Access-Control System Plus）是一种用于网络设备认证、授权和计费（AAA）的协议。它使用TCP协议进行通信，并且对整个会话进行加密，包括用户名和密码。

因此，Chris在使用数据包嗅探器捕获来自TACACS+服务器的流量时，应该监控TCP协议。由于TACACS+对整个会话进行加密，Chris将无法读取任何有用的数据，包括用户名和密码。

正确答案是：

B：TCP；没有任何有用的数据，因为TACACS +对整个会话加密

TCP; none—TACACS+ encrypts the full session.

-------------------

题目51-1：用有关 Kerberos身份验证和授权的知识以及下面的图来回答3个问题

Use your knowledge of Kerberos authentication and authorization as well as the following diagram to answer questions .

<div style="text-align:center"><img alt="" height="449" src="/file/100000/m/20210907/89c5582ad64c4dc696b2516ec6187b37.png" width="689" /></div>

如果客户端已经通过KDC的验证，当客户端工作站想要访问资源时，客户端工作站在A点应该向KDC发送什么？

If the client has already authenticated to the KDC, what does the client workstation send to the KDC at point A when it wants to access a resource?

A：重新发送密码

It resends the password

B：TGR

ATGR

C：客户端工作站的TGT

Its TGT

D：服务票证

A service ticket

答案:在Kerberos身份验证和授权过程中，当客户端已经通过KDC（Key Distribution Center）的验证并拥有TGT（Ticket Granting Ticket）后，客户端工作站想要访问某个资源时，它需要向KDC请求一个服务票证（Service Ticket）。这个服务票证是用于访问特定资源的凭证。

因此，在A点，客户端工作站应该向KDC发送它的TGT（Ticket Granting Ticket），以便KDC可以验证客户端的身份并颁发一个服务票证。

正确答案是：

C：客户端工作站的TGT

Its TGT

-------------------

题目51-1：用有关 Kerberos身份验证和授权的知识以及下面的图来回答3个问题

Use your knowledge of Kerberos authentication and authorization as well as the following diagram to answer questions .

<div style="text-align:center"><img alt="" height="449" src="/file/100000/m/20210907/89c5582ad64c4dc696b2516ec6187b37.png" width="689" /></div>

步骤A和B之间发生了什么？

What occurs between steps A and B?

A：KDC验证TGT的有效性，验证用户是否具有访问资源的合法权限

The KDC verifies the validity of the TGT and whether the user has the right privileges for the requested resource.

B：KDC根据TGT中的数据更新它的访问控制列表

The KDC updates its access control list based on the data in the TGT.

C：KDC检查它的服务列表，并根据服务请求准备好更新后的TGT

The KDC checks its service listing and prepares an updated TGT based on the service request.

D：KDC生成服务票证，接着将其发送给客户端

The KDC generates a service ticket to issue to the client.

答案:在Kerberos身份验证和授权过程中，步骤A和B之间发生的是KDC（密钥分发中心）生成服务票证并将其发送给客户端的过程。因此，正确答案是：

\*\*D：KDC生成服务票证，接着将其发送给客户端\*\*

The KDC generates a service ticket to issue to the client.

### 解释：

1. \*\*步骤A\*\*：客户端向KDC发送一个请求，请求访问某个服务。这个请求中包含了客户端的TGT（Ticket Granting Ticket）。

2. \*\*步骤B\*\*：KDC验证TGT的有效性，并生成一个服务票证（Service Ticket），这个票证包含了客户端访问该服务的权限信息。

3. \*\*步骤C\*\*：KDC将生成的服务票证发送给客户端。

因此，步骤A和B之间发生的是KDC生成服务票证并将其发送给客户端的过程。

-------------------

题目51-1：用有关 Kerberos身份验证和授权的知识以及下面的图来回答3个问题

Use your knowledge of Kerberos authentication and authorization as well as the following diagram to answer questions .

<div style="text-align:center"><img alt="" height="449" src="/file/100000/m/20210907/89c5582ad64c4dc696b2516ec6187b37.png" width="689" /></div>

如果一项服务正在被访问，请问该服务会使用什么来验证票证？

What system or systems does the service that is being accessed use to validate the ticket?

A：KDC

The KDC.

B：客户端工作站和KDC

The client workstation and the KDC.

C：客户端工作站会以”客户端到服务器”形式来提供票证。

The client workstation supplies it in the form of a client-to-server ticket and an authenticator.

D：KVS

The KVS.

答案:在Kerberos身份验证和授权过程中，当一项服务被访问时，服务会使用 \*\*KDC（Key Distribution Center）\*\* 来验证票证。具体来说，服务会检查客户端提供的票证（Ticket）和认证器（Authenticator），并使用KDC提供的会话密钥来验证这些信息的有效性。

因此，正确答案是：

\*\*A：KDC\*\*

The KDC.

-------------------

题目52：服务票证(ST)在Kerberos身份验证中的作用是什么？

What does a service ticket (ST) provide in Kerberos authentication?

A：它充当身份验证主机

It serves as the authentication host.

B：它可以证明主体对客体的访问是合法的

It provides proof that the subject is authorized to access an object.

C：它可以证明主体已通过KDC身份验证，该主体可以请求票证从而访问特定的客体

It provides proof that a subject has authenticated through a KDC and can request tickets to access other objects.

D：它提供票证授予服务

It provides ticket granting services.

答案:在Kerberos身份验证中，服务票证（Service Ticket, ST）的作用是允许用户（主体）访问特定的服务（客体）。服务票证是由Kerberos密钥分发中心（KDC）签发的，它证明了用户已经通过了KDC的身份验证，并且有权访问特定的服务。

因此，正确的选项是：

C：它可以证明主体已通过KDC身份验证，该主体可以请求票证从而访问特定的客体

It provides proof that a subject has authenticated through a KDC and can request tickets to access other objects.

这个选项准确地描述了服务票证在Kerberos身份验证中的作用。

-------------------

题目53：Judy正准备进行业务影响分析。在这个过程中，她的第一步应该是什么？

Judy is preparing to conduct a business impact analysis. What should her first step be in the process?

A：识别业务面临的威胁

Identify threats to the business.

B：识别组织面临的风险

Identify risks to the organization.

C：确定业务优先级

Identify business priorities.

D：进行可能性分析

Conduct likelihood analysis.

答案:在业务影响分析（Business Impact Analysis, BIA）的过程中，第一步通常是确定业务的优先级。这是因为在了解哪些业务功能对组织的持续运营最为关键之前，评估威胁、风险或进行可能性分析可能会缺乏针对性。通过确定业务优先级，Judy可以确保后续的分析和资源分配能够集中在最关键的业务功能上，从而更有效地保护组织的利益。

因此，正确答案是：

C：确定业务优先级

Identify business priorities.

-------------------

题目54：手机热点给商业网络带来的最常见风险是什么？

What is the most common risk that cellular phone hotspots create for business networks?

A：它们可以为攻击者提供进入你的网络的不安全网络路径

They can provide attackers with a non-secured network path into your network.

B：它们可以像恶意接入点一样用于中间人攻击

They can be used like rogue access points for man-in-the-middle attacks.

C：它们会拦截无线数据

They allow wireless data to be intercepted.

D：它们是未加密的，很容易被嗅探

They are unencrypted and can be easily sniffed.

答案:题目54的正确答案是：

A：它们可以为攻击者提供进入你的网络的不安全网络路径

They can provide attackers with a non-secured network path into your network.

解析：手机热点通常不像企业级网络那样具有严格的安全措施。当员工使用手机热点连接到公司网络时，可能会为攻击者提供一个不安全的网络路径，从而增加网络被入侵的风险。虽然其他选项（如中间人攻击、数据拦截和未加密通信）也是潜在的风险，但最常见的问题是手机热点提供了一个不安全的网络路径，使得攻击者更容易进入企业网络。

-------------------

题目55：以下哪种灭火系统的意外风险最大，可能会损坏数据中心的设备？

Which one of the following fire suppression systems poses the greatest risk of accidental discharge that damages equipment in a data center?

A：湿管

Wet pipe

B：干管

Dry pipe

C：喷水

Deluge

D：预处理系统

Preaction

答案:题目55的正确答案是：

C：喷水

Deluge

喷水灭火系统（Deluge System）在启动时会大量喷水，虽然能有效灭火，但在数据中心等环境中，意外启动可能会对电子设备造成严重损害。因此，喷水灭火系统的意外风险最大，可能会损坏数据中心的设备。

-------------------

题目56：Amanda的医疗保健提供者将她的医疗数据保存起来，这些数据涉及她的健康、治疗和医疗费用。请问上述数据是什么类型的数据？

Amanda’s healthcare provider maintains such data as details about her health, treatments, and medical billing. What type of data is this?

A：受保护的健康信息

Protected health information

B：个人身份信息

Personally identifiable information

C：受保护的健康保险

Protected health insurance

D：个人保护数据

Individual protected data

答案:正确答案是 \*\*A：受保护的健康信息\*\*（Protected health information）。

\*\*解释：\*\*

Amanda的医疗数据涉及她的健康、治疗和医疗费用，这些信息属于受保护的健康信息（Protected Health Information, PHI）。PHI 是指与个人的健康状况、医疗护理或医疗费用相关的信息，通常受到隐私保护法规（如美国的HIPAA）的保护。

其他选项的解释：

- \*\*B：个人身份信息\*\*（Personally identifiable information）是指可以用来识别个人身份的信息，如姓名、地址、社会安全号码等，虽然PHI可能包含这些信息，但题目中描述的内容更具体地指向健康信息。

- \*\*C：受保护的健康保险\*\*（Protected health insurance）和 \*\*D：个人保护数据\*\*（Individual protected data）并不是常见的术语，也不符合题目描述的内容。

因此，最合适的答案是 \*\*A：受保护的健康信息\*\*。

-------------------

题目57：什么类型的代码审查最适合识别业务逻辑缺陷？

What type of code review is best suited to identifying business logic flaws?

A：突变Fuzzing

Mutational fuzzing

B：手动测试

Manual

C：分代Fuzzing

Generational fuzzing

D：接口测试

Interface testing

答案:题目57的正确答案是：

B：手动测试

Manual

解析：手动测试最适合识别业务逻辑缺陷。业务逻辑缺陷通常涉及代码中的逻辑错误或不符合业务需求的情况，这些缺陷往往需要人工审查和理解业务需求才能发现。手动测试允许测试人员深入理解业务逻辑，并通过模拟用户操作或手动检查代码来发现潜在的问题。

其他选项的解析：

- A：突变Fuzzing（Mutational fuzzing）和 C：分代Fuzzing（Generational fuzzing）通常用于发现安全漏洞或输入验证问题，而不是业务逻辑缺陷。

- D：接口测试（Interface testing）主要用于验证不同模块或系统之间的接口是否正确工作，而不是直接识别业务逻辑缺陷。

因此，手动测试是最适合识别业务逻辑缺陷的代码审查类型。

-------------------

题目58：”你知道什么”属于什么类型的身份验证因素？

Something you know is an example of what type of authentication factor?

A：类型1

Type 1

B：类型2

Type 2

C：类型3

Type3

D：类型4

Type 4

答案:“你知道什么”（Something you know）属于身份验证因素中的类型1（Type 1）。身份验证因素通常分为以下几类：

1. \*\*类型1：你知道什么（Something you know）\*\*

例如：密码、PIN码、安全问题答案等。

2. \*\*类型2：你拥有什么（Something you have）\*\*

例如：智能卡、手机、硬件令牌等。

3. \*\*类型3：你是什么（Something you are）\*\*

例如：指纹、面部识别、虹膜扫描等生物特征。

因此，正确答案是：

\*\*A：类型1（Type 1）\*\*

-------------------

题目59：Saria是一家医疗保健机构的系统所有者，对于系统中的数据，她负有什么责任？

Saria is the system owner for a healthcare organization. What responsibilities does she have related to the data that resides on or is processed by the systems she owns?

A：她必须对数据进行分类

She has to classify the data.

B：她必须确保实施适当的安全控制来保护数据

She has to make sure that appropriate security controls are in place to protect the data.

C：她必须授予全体员工适当的系统访问权限

She has to grant appropriate access to personnel.

D：她对数据安全性负全部责任，数据包括静止中的数据、传输中的数据、使用中的数据

She bears sole responsibility for ensuring that data is protected at rest, in transit, and in use.

答案:

B：她必须确保实施适当的安全控制来保护数据。这包括物理安全措施、技术安全措施和行政安全措施，以防止数据泄露、篡改或丢失。

-------------------

题目60：在软件测试期间，Jack假设了一个场景：一个黑客想访问他正在审查的应用程序。Jack在考虑黑客可能会从哪里入手，然后他针对攻击者的可能行为对系统进行测试，请问Jack进行的是什么类型的测试？

During software testing, Jack diagrams how a hacker might approach the application he is reviewing and determines what requirements the hacker might have. He then tests how the system would respond to the attacker’s likely behavior. What type of testing is Jack conducting?

A：误用案例测试

Misuse case testing

B：用例测试

Use case testing

C：Hacker用例测试

Hacker use case testing

D：静态代码分析

Static code analysis

答案:题目描述的是Jack在软件测试期间，模拟黑客的行为来测试系统的安全性。他考虑黑客可能如何接近应用程序，并测试系统对攻击者可能行为的响应。这种测试方法是为了确保系统能够抵御潜在的安全威胁。

选项分析：

- A：误用案例测试（Misuse case testing）是一种测试方法，专门用来模拟和测试系统对恶意或非预期使用的反应。这与题目中描述的情景相符。

- B：用例测试（Use case testing）通常是指根据正常使用场景来测试系统，而不是针对恶意行为。

- C：Hacker用例测试（Hacker use case testing）并不是一个标准的测试术语。

- D：静态代码分析（Static code analysis）是通过分析源代码来发现潜在的错误和安全漏洞，而不是通过模拟攻击行为来测试系统。

因此，最符合题目描述的测试类型是误用案例测试（Misuse case testing）。

正确答案是：A：误用案例测试（Misuse case testing）。

-------------------

题目61：Rick对其公司Web应用程序的风险评估报告指出，它可能遭受SQL注入攻击。你会推荐Rick应用以下哪些缓解技术来帮助降低这些风险？（选择所有符合条件的）

Rick’s risk assessment for his company’s web application noted that it could suffer from SQL injection attacks. Which of the following mitigation techniques would you recommend Rick apply to help reduce this risk? (Select all that apply.)

A：存储过程

Stored procedures

B：转义所有用户提供的输入

Escaping all user-supplied input

C：参数化查询

Parameterized queries

D：输入验证

Input validation

答案:为了降低SQL注入攻击的风险，Rick可以采取以下几种缓解技术：

A：存储过程（Stored procedures）

- 存储过程可以将SQL逻辑封装在数据库中，减少直接在应用程序中拼接SQL语句的机会，从而降低SQL注入的风险。

B：转义所有用户提供的输入（Escaping all user-supplied input）

- 转义用户输入可以防止恶意输入被解释为SQL代码的一部分。这是一种有效的防御措施，但不如参数化查询和存储过程安全。

C：参数化查询（Parameterized queries）

- 参数化查询是防止SQL注入的最有效方法之一。通过使用参数化查询，用户输入被视为数据而不是可执行代码，从而避免了SQL注入的可能性。

D：输入验证（Input validation）

- 输入验证可以确保用户输入符合预期的格式和类型，从而减少恶意输入的可能性。虽然输入验证本身不能完全防止SQL注入，但它可以作为多层防御的一部分。

因此，推荐的缓解技术是：

- A：存储过程

- B：转义所有用户提供的输入

- C：参数化查询

- D：输入验证

所有选项都是有效的缓解措施，因此选择所有选项（A、B、C、D）是正确的。

-------------------

题目62：Chris的任务是扫描系统上所有可能的TCP和UDP端口。请问每种类型的端口必须扫描多少个端口才能完成任务？

Chris has been assigned to scan a system on all of its possible TCP and UDP ports. How many ports of each type must he scan to complete his assignment?

A：65,536个TCP端口和32,768个UDP端口

65,536 TCP ports and 32,768 UDP ports

B：1024个常用TCP端口和32,768个临时UDP端口

1,024 common TCP ports and 32,768 ephemeral UDP ports

C：65,536个TCP端口和65, 536个UDP端口

65,536 TCP and 65,536 UDP ports

D：16,384个TCP端口和16,384个UDP端口

16,384 TCP ports, and 16,384 UDP ports

答案:正确答案是 \*\*C：65,536个TCP端口和65,536个UDP端口\*\*。

### 解析：

在计算机网络中，端口号是一个16位的数字，范围从0到65,535（即2^16）。因此，无论是TCP还是UDP协议，理论上都有65,536个可能的端口号。

- \*\*TCP端口\*\*：TCP协议使用端口号来标识不同的服务或应用程序，端口号范围是0到65,535。

- \*\*UDP端口\*\*：UDP协议同样使用端口号来标识不同的服务或应用程序，端口号范围也是0到65,535。

因此，Chris需要扫描 \*\*65,536个TCP端口\*\* 和 \*\*65,536个UDP端口\*\* 才能完成任务。

其他选项的端口数量不符合实际情况：

- A选项中的UDP端口数量不正确。

- B选项中的TCP端口数量仅涵盖了常用端口，而不是所有端口。

- D选项中的端口数量远低于实际可能的端口数量。

所以，正确答案是 \*\*C\*\*。

-------------------

题目63：CVE和NVD都提供了什么信息？

CVE and the NVD both provide information about what?

A：漏洞

Vulnerabilities

B：标记语言

Markup languages

C：漏洞评估工具

Vulnerability assessment tools

D：渗透测试方法

Penetration testing methodologies

答案:正确答案是 A：漏洞 (Vulnerabilities)。

CVE（Common Vulnerabilities and Exposures）和 NVD（National Vulnerability Database）都提供了关于漏洞的信息。CVE 是一个公开的漏洞列表，每个漏洞都有一个唯一的标识符（CVE ID）。NVD 是由美国国家标准与技术研究院（NIST）维护的数据库，它包含了详细的漏洞信息，包括漏洞的描述、严重性评分、受影响的软件和补丁信息等。两者都是信息安全领域的重要资源，帮助安全专业人员识别和管理漏洞。

-------------------

题目64：Michelle希望确保她的公司日志保存的时间不会超过他们需要的时间。她应该制定和实施什么类型的策略来确保这一点？

Michelle wants to ensure that her company does not keep logs for longer than they need to. What type of policy should she write and implement to ensure this?

A：EOL策略

An EOL policy

B：数据分类策略

A data classification policy

C：EOS策略

An EOS policy

D：记录保留策略

A record retention policy

答案:Michelle希望确保她的公司日志保存的时间不会超过他们需要的时间。她应该制定和实施什么类型的策略来确保这一点？

答案是 D：记录保留策略 (A record retention policy)

记录保留策略（Record Retention Policy）是一种规定组织如何管理和保留其记录（包括日志）的正式政策。这种策略通常会规定不同类型记录的保留期限，以及何时和如何安全地销毁不再需要的记录。通过实施记录保留策略，Michelle可以确保公司日志不会保留超过必要的时间，从而减少数据泄露的风险，并遵守相关的法律法规。

-------------------

题目65：在什么类型的可信恢复过程中，系统针对一个或多个故障类型进行恢复，而不需要管理员的干预，同时可以防止数据丢失？

In what type of trusted recovery process does the system recover against one or more failure types without administrator intervention while protecting itself against data loss?

A：自动恢复

Automated recovery

B：手动恢复

Manual recovery

C：功能恢复

Function recovery

D：无不当数据丢失的

Automated recovery without undue data loss

答案:题目65的正确答案是：

D：无不当数据丢失的自动恢复

Automated recovery without undue data loss

解析：

题目描述的系统恢复过程需要满足以下条件：

1. 针对一个或多个故障类型进行恢复

2. 不需要管理员的干预（即自动恢复）

3. 可以防止数据丢失

选项D"无不当数据丢失的自动恢复"完全符合以上所有条件。它既强调了自动恢复的特性，又特别指出了在恢复过程中不会造成不当的数据丢失，这与题目要求的"防止数据丢失"相吻合。

其他选项分析：

A. 自动恢复：虽然符合不需要管理员干预的要求，但没有提及数据保护

B. 手动恢复：与题目要求的"不需要管理员干预"相矛盾

C. 功能恢复：没有明确说明恢复的自动性和数据保护特性

因此，D选项是最符合题目要求的正确答案。

-------------------

题目66：如果你试图控制无线网络的信号强度和可用性，应考虑哪三个重要方面？

What three important items should be considered if you are attempting to control the strength of signal for a wireless network as well as where it is accessible?

A：天线放置、天线类型、天线功率

Antenna placement, antenna type, antenna power levels

B：天线设计、天线功率、强制门户

Antenna design, power levels, use of a captive portal

C：天线放置、天线设计、强制门户

Antenna placement, antenna design, use of a captive portal

D：天线功率、天线放置、FCC最低强度要求

Power levels, antenna placement, FCC minimum strength requirements

答案:正确答案是 \*\*A：天线放置、天线类型、天线功率\*\*（Antenna placement, antenna type, antenna power levels）。

### 解析：

1. \*\*天线放置（Antenna placement）\*\*：天线的位置对无线信号的强度和覆盖范围有直接影响。合理的天线放置可以优化信号覆盖，减少干扰。

2. \*\*天线类型（Antenna type）\*\*：不同类型的天线（如全向天线、定向天线等）具有不同的信号覆盖特性。选择合适的天线类型可以帮助控制信号的强度和方向。

3. \*\*天线功率（Antenna power levels）\*\*：天线的发射功率直接影响信号的强度和覆盖范围。通过调整功率，可以控制信号的传播距离和强度。

其他选项中的“强制门户”（captive portal）主要用于用户认证和访问控制，与信号强度和覆盖范围的控制关系不大。FCC最低强度要求是法规要求，而不是控制信号强度的直接手段。因此，选项A是最合适的答案。

-------------------

题目67：确保数据无法从SSD恢复的最佳方法是什么？

What is the best way to ensure that data is unrecoverable from an SSD?

A：使用内置的擦除命令

Use the built-in erase commands.

B：使用1或者0的随机模式来擦除SSD

Use a random pattern wipe of 1s and 0s.

C：物理毁坏驱动器

Physically destroy the drive.

D：消磁

Degauss the drive.

答案:确保数据无法从SSD（固态硬盘）恢复的最佳方法是：

\*\*C：物理毁坏驱动器 (Physically destroy the drive)\*\*

### 原因：

1. \*\*内置的擦除命令 (A)\*\*：虽然SSD有内置的擦除命令（如ATA Secure Erase），但这些命令并不总是能完全确保数据无法恢复。某些情况下，数据可能仍然可以通过特殊手段恢复。

2. \*\*使用1或者0的随机模式来擦除SSD (B)\*\*：对于SSD来说，由于其内部的磨损均衡技术和数据分布机制，简单的随机模式擦除可能无法覆盖所有数据块，因此不能保证数据完全不可恢复。

3. \*\*消磁 (D)\*\*：消磁是针对传统机械硬盘（HDD）的方法，对SSD无效，因为SSD使用的是闪存芯片，而不是磁性介质。

4. \*\*物理毁坏驱动器 (C)\*\*：物理毁坏SSD是最可靠的方法。通过粉碎、焚烧或其他物理破坏手段，可以确保数据无法恢复。这种方法彻底破坏了存储介质，使得任何数据恢复手段都无法奏效。

因此，\*\*物理毁坏驱动器\*\*是确保数据无法从SSD恢复的最佳方法。

-------------------

题目68：Alice向Bob发送消息，希望第三方的Mal在传输过程中无法读取消息的内容。Alice想实现加密的什么目标？

Alice sends a message to Bob and wants to ensure that Mal, a third party, does not read the contents of the message while in transit. What goal of cryptography is Alice attempting to achieve?

A：机密性

Confidentiality

B：完整性

Integrity

C：认证

Authentication

D：不可否认

Nonrepudiation

答案:Alice希望确保在消息传输过程中，第三方的Mal无法读取消息的内容。这涉及到保护消息的隐私，防止未经授权的访问。因此，Alice想要实现的是加密的\*\*机密性\*\*目标。

正确答案是：

\*\*A：机密性\*\*

\*\*Confidentiality\*\*

-------------------

题目69：对于图中显示的MITRE ATT&CK框架，请按照正确顺序放置每个阶段。请注意，侦察是流程的开始，维护是流程的结束。

Place the following stages in their proper order for the MITRE ATT&CK framework shown here. Note that Recon is the start of the process and Maintain is the end.

<div style="text-align:center"><img alt="" height="408" src="/file/100000/m/20210907/d8acb535edaa40878b80b2ff0e747250.png" width="703" /></div>

A：1侦察--2交付--3武器化&mdash;4利用--5控制--6执行--7维护

1 Recon-2 Deliver- 3 Weaponize-4 Exploit - 5 Control- 6 Execute-7 Maintain

B：1侦察--2武器化--3交付&mdash;4利用--5控制--6执行--7维护

1 Recon -2 Weaponize- 3 Deliver- 4 Exploit- 5 Control- 6 Execute- 7 Maintain

C：1侦察--2武器化--3交付&mdash;4利用--5执行--6控制--7维护

1 Recon -2 Weaponize - 3 Deliver - 4 Exploit- 5 Execute - 6 Control - 7 Maintain

D：1侦察--2武器化&mdash;3利用--4交付--5控制--6执行--7维护

1 Recon- 2 Weaponize- 3 Exploit - 4 Deliver- 5 Control -6 Execute -7 Maintain

答案:MITRE ATT&CK框架描述的是网络攻击者可能采取的一系列战术和技术。这些阶段通常按照攻击的流程顺序排列，从最初的侦察到最后的维护。根据标准的攻击流程，正确的顺序应该是：

1. 侦察 (Recon) - 攻击者收集关于目标的信息。

2. 武器化 (Weaponize) - 攻击者创建或获取用于攻击的工具或恶意软件。

3. 交付 (Deliver) - 攻击者将武器化的内容发送到目标系统。

4. 利用 (Exploit) - 攻击者利用目标系统的漏洞。

5. 控制 (Control) - 攻击者在目标系统上建立控制点。

6. 执行 (Execute) - 攻击者在目标系统上执行恶意代码或命令。

7. 维护 (Maintain) - 攻击者保持对目标系统的访问和控制。

因此，正确的选项是：

B：1侦察--2武器化--3交付—4利用--5控制--6执行--7维护

1 Recon -2 Weaponize- 3 Deliver- 4 Exploit- 5 Control- 6 Execute- 7 Maintain

-------------------

题目70：Gary工作的公司处理信用卡，并按照信用卡处理行业标准运营。他的公司需要遵守以下哪些标准？

The company that Gary works for processes credit cards and operates under an industry standard for credit card handling. Which of the following standards will his company need to comply with?

A：ISO 27001

ISO 27001

B：FIPS 140

FIPS 140

C：PCI-DSS

PCI-DSS

D：ISO 27002

ISO 27002

答案:Gary工作的公司处理信用卡，因此需要遵守与信用卡处理相关的行业标准。以下是各选项的简要说明：

A. \*\*ISO 27001\*\* - 这是一个信息安全管理体系（ISMS）的国际标准，适用于各种类型和规模的组织，帮助管理信息安全风险。虽然它与信息安全相关，但并不是专门针对信用卡处理的。

B. \*\*FIPS 140\*\* - 这是美国联邦信息处理标准，涉及加密模块的安全性。它主要用于确保加密技术的安全性，但并不是专门针对信用卡处理的。

C. \*\*PCI-DSS\*\* - 这是支付卡行业数据安全标准（Payment Card Industry Data Security Standard），专门针对处理信用卡数据的公司。它规定了保护持卡人数据的最低安全要求，是信用卡处理行业必须遵守的标准。

D. \*\*ISO 27002\*\* - 这是ISO 27001的补充标准，提供了信息安全控制的实施指南。虽然它与信息安全相关，但并不是专门针对信用卡处理的。

因此，Gary的公司需要遵守的标准是 \*\*C：PCI-DSS\*\*。

-------------------

题目71：James决定实施一个NAC解决方案，使用后准入原则来控制网络连接。后准入原则不能解决什么类型的问题？

James has opted to implement a NAC solution that uses a post-admission philosophy for its control of network connectivity. What type of issues can’t a strictly post-admission policy handle?

A：带外监控

Out-of-band monitoring

B：防止未连接的笔记本电脑在连接到网络后立即被利用

Preventing an unpatched laptop from being exploited immediately after connecting to the network

C：当用户行为与授权矩阵不匹配时，拒绝用户访问

Denying access when user behavior doesn’t match an authorization matrix

D：当用户行为满足基于授权的矩阵时，允许用户访问特定对象

Allowing a user access to a specific object when user behavior is allowed based on an authorization matrix

答案:后准入原则（Post-admission policy）是指在设备或用户已经连接到网络之后，再对其进行安全检查和控制的策略。这种策略主要关注的是在设备或用户已经进入网络后，如何监控和管理其行为，以确保网络安全。

选项分析：

A. 带外监控（Out-of-band monitoring）：带外监控通常指的是通过独立的网络或通道进行监控，而不是通过主网络。后准入原则主要关注的是网络连接后的行为，而带外监控可以在网络连接之前或之后进行，因此后准入原则并不直接影响带外监控。

B. 防止未连接的笔记本电脑在连接到网络后立即被利用（Preventing an unpatched laptop from being exploited immediately after connecting to the network）：后准入原则主要是在设备或用户已经连接到网络后进行控制，因此它无法在设备连接到网络之前就防止未打补丁的笔记本电脑被利用。这种问题需要在设备连接网络之前进行预防，例如通过预准入控制（Pre-admission control）来确保设备符合安全策略。

C. 当用户行为与授权矩阵不匹配时，拒绝用户访问（Denying access when user behavior doesn’t match an authorization matrix）：后准入原则可以在用户连接到网络后监控其行为，并根据授权矩阵来决定是否允许其继续访问。因此，后准入原则可以处理这种情况。

D. 当用户行为满足基于授权的矩阵时，允许用户访问特定对象（Allowing a user access to a specific object when user behavior is allowed based on an authorization matrix）：后准入原则可以根据用户的行为和授权矩阵来决定是否允许其访问特定资源。因此，后准入原则可以处理这种情况。

综上所述，后准入原则无法解决的是在设备连接到网络之前就防止未打补丁的笔记本电脑被利用的问题。因此，正确答案是：

B：防止未连接的笔记本电脑在连接到网络后立即被利用

Preventing an unpatched laptop from being exploited immediately after connecting to the network

-------------------

题目72：Ben建立了一个访问控制列表，列出了他的用户被允许访问的客体。当用户尝试访问某个客体但他们没有相应权限时，即使没有允许访问该客体的明确规则，这些用户也会被拒绝访问。这体现了什么访问控制原则？

Ben has built an access control list that lists the objects that his users are allowed to access. When users attempt to access an object that they don’t have rights to, they are denied access, even though there isn’t a specific rule that prevents it. What access control principle is key to this behavior?

A：最小特权

Least privilege

B：隐式拒绝

Implicit deny

C：显式拒绝

Explicit deny

D：最终规则的通过

Final rule fall-through

答案:题目描述的情况是，当用户尝试访问某个客体时，如果没有明确的规则允许他们访问，系统会自动拒绝访问。这种行为体现了“隐式拒绝”（Implicit deny）的访问控制原则。

隐式拒绝原则意味着，除非有明确的规则允许访问，否则所有访问请求都会被默认拒绝。这与“显式拒绝”（Explicit deny）不同，显式拒绝是指有明确的规则禁止访问。

因此，正确答案是：

B：隐式拒绝

Implicit deny

-------------------

题目73：Mary是一家保险公司的安全风险分析师。她目前正在考虑一个情景，黑客可能使用SQL注入攻击来攻击公司的Web服务器，然而公司的Web应用程序中缺少相应的补丁程序。这种情况下，风险是什么？

Mary is a security risk analyst for an insurance company. She is currently examining a scenario where a hacker might use a SQL injection attack to deface a web server due to a missing patch in the company’s web application. In this scenario, what is the risk?

A：未打补丁的Web应用程序

Unpatched web application

B：网页崩溃

Web defacement

C：黑客

Hacker

D：操作系统

Operating system

答案:在这个情景中，Mary正在考虑的是由于公司Web应用程序缺少相应的补丁程序，黑客可能利用SQL注入攻击来破坏Web服务器。这种情况下，最直接的风险是黑客能够利用未打补丁的Web应用程序中的漏洞进行攻击，导致网页被篡改或其他形式的安全破坏。

因此，正确的答案是：

B

-------------------

题目74：检测入侵的平均时间是什么类型的安全指标？

The mean time to detect a compromise is what type of security measurement?

A：MTO

An MTO

B：技术控制目标

A technical control objective

C：合规目标

A compliance objective

D：KPI

A KPI

答案:题目问的是“检测入侵的平均时间是什么类型的安全指标？” 选项D中的KPI（关键绩效指标）是用于衡量组织在特定目标上的表现和效率的指标。检测入侵的平均时间（Mean Time to Detect, MTD）是衡量安全团队或系统在检测到潜在安全威胁或入侵事件方面的效率，因此它是一个关键绩效指标（KPI）。

所以，正确答案是：

D：KPI

A KPI

-------------------

题目75：Val正在尝试审查安全日志，但被其组织的中央日志存储库中保存的大量记录所覆盖。她可以使用什么技术来选择一组代表性记录进行进一步审查？

Val is attempting to review security logs but is overwhelmed by the sheer volume of records maintained in her organization’s central log repository. What technique can she use to select a representative set of records for further review?

A：统计抽样

Statistical sampling.

B：剪切

Clipping.

C：从每天选择前5%的记录

Choose the first 5 percent of records from each day.

D：从中间选择5%的记录

Choose 5 percent of records from the middle of the day.

答案:题目75的正确答案是：

A：统计抽样

Statistical sampling.

解析：

统计抽样是一种从大量数据中选择代表性样本的技术。通过这种方法，Val可以从整个日志数据集中随机或有策略地选择一部分记录进行详细审查，而不必处理所有数据。这种方法既节省时间，又能确保所选样本能够反映整个数据集的特征，从而有效地进行安全审查。

其他选项的解析：

B：剪切 - 这不是一个标准的统计或数据分析技术，无法确保所选记录的代表性。

C：从每天选择前5%的记录 - 这种方法可能会导致偏差，因为前5%的记录可能不具有代表性，特别是如果日志记录是按时间顺序排列的。

D：从中间选择5%的记录 - 同样，这种方法也可能导致偏差，因为中间部分的记录可能无法全面反映整个数据集的特征。

-------------------

题目76：Jen是工业生产设施的网络管理员，她的任务是确保网络不受生产车间上大型电机的电磁干扰影响。如果这个问题比成本和安装难度更重要，她应该选择什么类型的网络布线？

In Jen’s job as the network administrator for an industrial production facility, she is tasked with ensuring that the network is not susceptible to electromagnetic interference due to the large motors and other devices running on the production floor. What type of network cabling should she choose if this concern is more important than cost and difficulty of installation?

A：10Base2

10Base2

B：100BaseT

100BaseT

C：1000BaseT

1000BaseT

D：光纤

Fiber optic

答案:在工业生产环境中，大型电机和其他设备可能会产生强烈的电磁干扰（EMI），这可能会影响网络信号的传输。为了确保网络的稳定性和可靠性，选择一种能够抵抗电磁干扰的布线技术是非常重要的。

选项分析：

- \*\*10Base2\*\* 和 \*\*100BaseT\*\* 使用的是铜缆，容易受到电磁干扰的影响。

- \*\*1000BaseT\*\* 虽然使用的是更高级的铜缆技术，但仍然可能受到电磁干扰的影响。

- \*\*光纤\*\* 使用的是光信号传输，不受电磁干扰的影响，因此在电磁干扰严重的环境中是最佳选择。

因此，如果电磁干扰的防护比成本和安装难度更重要，Jen应该选择 \*\*光纤\*\* 作为网络布线。

正确答案是：\*\*D：光纤\*\* (Fiber optic)

-------------------

题目77-1：参考以下场景，回答4个问题：

Jasper Diamonds是一家珠宝制造商，通过他们的网站销售和定制珠宝。Bethany是Jasper软件开发组织的经理，她正在努力使公司符合行业标准实践。她正在为组织开发一个新的变更管理流程，并希望遵循普遍接受的方法。

For questions , please refer to the following scenario:

Jasper Diamonds is a jewelry manufacturer that markets and sells custom jewelry through its website. Bethany is the manager of Jasper’s software development organization, and she is working to bring the company into line with industry-standard practices. She is developing a new change management process for the organization and wants to follow commonly accepted approaches.

Bethany希望实施控制措施，为公司员工提供一个有组织的框架，从而为团队开发的新网站功能提出建议。什么变更管理流程有助于实现这一目标？

Bethany would like to put in place controls that provide an organized framework for company employees to suggest new website features that her team will develop. What change management process facilitates this?

A：配置控制

Configuration control

B：变更控制

Change control

C：发布控制

Release control

D：请求控制

Request control

答案:Bethany希望为公司员工提供一个有组织的框架，以便他们能够提出新的网站功能建议，并且这些建议能够被她的团队开发和实施。在这种情况下，最合适的变更管理流程是 \*\*请求控制（Request control）\*\*。

\*\*请求控制\*\* 是一种变更管理流程，它允许员工或利益相关者提出变更请求，并确保这些请求被系统地记录、评估和批准。通过请求控制，Bethany可以确保所有的建议都经过适当的审查和优先级排序，从而为团队提供一个有组织的框架来处理这些变更请求。

其他选项的解释：

- \*\*配置控制（Configuration control）\*\* 主要用于管理系统的配置项，确保系统的配置一致性和可追溯性。

- \*\*变更控制（Change control）\*\* 通常用于管理已经批准的变更的实施过程，确保变更按照计划进行。

- \*\*发布控制（Release control）\*\* 主要用于管理软件或系统的发布过程，确保发布的版本是经过测试和验证的。

因此，\*\*D：请求控制（Request control）\*\* 是最适合Bethany需求的变更管理流程。

-------------------

题目77-1：参考以下场景，回答4个问题：

Jasper Diamonds是一家珠宝制造商，通过他们的网站销售和定制珠宝。Bethany是Jasper软件开发组织的经理，她正在努力使公司符合行业标准实践。她正在为组织开发一个新的变更管理流程，并希望遵循普遍接受的方法。

For questions , please refer to the following scenario:

Jasper Diamonds is a jewelry manufacturer that markets and sells custom jewelry through its website. Bethany is the manager of Jasper’s software development organization, and she is working to bring the company into line with industry-standard practices. She is developing a new change management process for the organization and wants to follow commonly accepted approaches.

Bethany还希望创建一个过程，帮助多个开发人员同时处理代码。什么变更管理流程可以实现这一目标？

Bethany would also like to create a process that helps multiple developers work on code at the same time. What change management process facilitates this?

A：配置控制

Configuration control

B：变更控制

Change control

C：发布控制

Release control

D：请求控制

Request control

答案:Bethany希望创建一个过程，帮助多个开发人员同时处理代码。这种情况下，最合适的变更管理流程是 \*\*A：配置控制 (Configuration control)\*\*。

### 解释：

- \*\*配置控制 (Configuration control)\*\*：配置控制是管理代码库和系统配置的过程，确保多个开发人员可以同时工作而不会相互干扰。它通常包括版本控制系统（如Git），允许多个开发人员在同一个代码库上并行工作，同时跟踪和管理代码的变更。配置控制还涉及分支、合并和冲突解决等操作，以确保代码的一致性和完整性。

- \*\*变更控制 (Change control)\*\*：变更控制主要关注对系统或代码的变更进行审批和管理，确保变更经过适当的评估和批准。它更多关注变更的流程和审批，而不是直接支持多个开发人员同时工作。

- \*\*发布控制 (Release control)\*\*：发布控制涉及管理软件版本的发布过程，确保发布的版本是稳定和经过测试的。它不直接涉及多个开发人员同时处理代码的问题。

- \*\*请求控制 (Request control)\*\*：请求控制通常涉及管理用户或开发人员的变更请求，确保这些请求被记录、评估和批准。它也不直接支持多个开发人员同时处理代码。

因此，\*\*配置控制 (Configuration control)\*\* 是最适合帮助多个开发人员同时处理代码的变更管理流程。

-------------------

题目77-1：参考以下场景，回答4个问题：

Jasper Diamonds是一家珠宝制造商，通过他们的网站销售和定制珠宝。Bethany是Jasper软件开发组织的经理，她正在努力使公司符合行业标准实践。她正在为组织开发一个新的变更管理流程，并希望遵循普遍接受的方法。

For questions , please refer to the following scenario:

Jasper Diamonds is a jewelry manufacturer that markets and sells custom jewelry through its website. Bethany is the manager of Jasper’s software development organization, and she is working to bring the company into line with industry-standard practices. She is developing a new change management process for the organization and wants to follow commonly accepted approaches.

Bethany正在与她的同事一起进行用户验收测试。以下哪个变更管理流程包括这个任务？

Bethany is working with her colleagues to conduct user acceptance testing. What change management process includes this task?

A：配置控制

Configuration control

B：变更控制

Change control

C：发布控制

Release control

D：请求控制

Request control

答案:在变更管理流程中，用户验收测试（User Acceptance Testing, UAT）通常是在变更控制（Change Control）过程中进行的。变更控制是确保所有变更都经过适当审查、批准、测试和记录的过程，以确保变更不会对系统的稳定性和功能产生负面影响。用户验收测试是变更控制过程中的一个关键步骤，它确保变更满足用户需求和业务目标。

因此，正确答案是：

\*\*B：变更控制\*\*

\*\*Change control\*\*

-------------------

题目77-1：参考以下场景，回答4个问题：

Jasper Diamonds是一家珠宝制造商，通过他们的网站销售和定制珠宝。Bethany是Jasper软件开发组织的经理，她正在努力使公司符合行业标准实践。她正在为组织开发一个新的变更管理流程，并希望遵循普遍接受的方法。

For questions , please refer to the following scenario:

Jasper Diamonds is a jewelry manufacturer that markets and sells custom jewelry through its website. Bethany is the manager of Jasper’s software development organization, and she is working to bring the company into line with industry-standard practices. She is developing a new change management process for the organization and wants to follow commonly accepted approaches.

Bethany注意到，当系统管理员更新库而不通知开发人员时会出现一些问题。什么变更管理流程

可以帮助解决这个问题？

Bethany noticed that some problems arise when system administrators update libraries without informing developers. What change management process can assist with this problem?

A：配置控制

Configuration control

B：变更控制

Change control

C：发布控制

Release control

D：请求控制

Request control

答案:Bethany注意到的问题是由于系统管理员在更新库时没有通知开发人员，这导致了潜在的系统兼容性和功能性问题。为了解决这个问题，最合适的变更管理流程是：

\*\*B：变更控制 (Change control)\*\*

变更控制流程确保所有的变更，包括库的更新，都经过适当的审查、批准和沟通。这包括在变更实施前通知所有相关的利益相关者，如开发人员，以确保他们了解变更的内容和可能的影响，并可以相应地调整他们的工作。这样可以减少因未通知的变更而导致的问题，确保系统的稳定性和一致性。

-------------------

题目78：Ben已经为他正在建立的Web应用程序编写了密码散列系统。他的密码散列函数的一部分工作过程如下所示：

hash (password1 + 07C98BFE4CF67B0BFE2643B5B22E2D7D) = 10B222970537B97919DB36EC757370D2

hash (password2 + 07C98BFE4CF67B0BFE2643B5B22E2D7D) = F1F16683F3E0208131B46D37A79C8921

Ben在实现散列函数时，存在什么问题？

Ben has written the password hashing system for the web application he is building. His hashing code function for passwords results in the following process for a series of passwords:

Hash(password1+07C98BFE4CF67B0BFE2643B5B22E2D7D)= 10B222970537B97919DB36EC757370D2

hash(password2+07C98BFE4CF67B0BFE2643B5B22E2D7D)= F1F16683F3E0208131B46D37A79C8921

What flaw has Ben introduced with his hashing implementation?

A：明文的盐

Plaintext salting

B：盐的再利用

Salt reuse

C：盐的长度较短

Use of a short salt

D：盐的选择算法比较差

Poor salt algorithm selection

答案:Ben在实现密码散列函数时，使用了相同的盐值（07C98BFE4CF67B0BFE2643B5B22E2D7D）来散列不同的密码（password1和password2）。这种做法存在一个严重的安全问题，即盐的再利用（Salt reuse）。

盐的主要目的是确保即使两个用户使用相同的密码，他们的散列值也会不同。如果盐被重复使用，攻击者可以使用彩虹表等预计算攻击方法来破解密码，因为相同的盐值会导致相同的密码生成相同的散列值。因此，每个密码应该使用唯一的盐值。

选项A（明文的盐）不正确，因为盐通常是明文存储的，这是正常的做法。选项C（盐的长度较短）和选项D（盐的选择算法比较差）也不正确，因为盐的长度和选择算法在这个问题中并没有被提及或存在问题。

因此，正确答案是：

\*\*B：盐的再利用\*\*

\*\*Salt reuse\*\*

-------------------

题目79：下列哪一个是风险转移的例子？

Which one of the following is an example of risk transference?

A：建立一个警卫棚屋

Building a guard shack

B：购买保险

Purchasing insurance

C：架设栅栏

Erecting fences

D：搬迁设施

Relocating facilities

答案:风险转移是指将潜在的风险或损失从一方转移到另一方的行为。在给出的选项中，购买保险（B）是最典型的风险转移的例子。通过购买保险，个人或企业将可能发生的财务损失风险转移给保险公司。如果发生保险范围内的事件，保险公司将承担相应的经济损失。

其他选项：

- A：建立一个警卫棚屋，这是风险控制或风险减少的措施，通过增加安全措施来降低风险。

- C：架设栅栏，这也是风险控制的一种方式，通过物理屏障来防止潜在的风险。

- D：搬迁设施，这可能是风险避免的一种方式，通过改变位置来避免特定的风险。

因此，正确答案是 B：购买保险。

-------------------

题目80：什么协议取代证书撤销列表并添加实时状态验证？

What protocol takes the place of certificate revocation lists and adds real-time status verification?

A：RTCP

RTCP

B：RTVP

RTVP

C：OCSP

OCSP

D：CSRTP

CSRTP

答案:正确答案是 C：OCSP。

OCSP（Online Certificate Status Protocol，在线证书状态协议）是一种用于检查数字证书状态的协议。它取代了传统的证书撤销列表（CRL，Certificate Revocation List），并提供了实时的证书状态验证。通过OCSP，客户端可以向OCSP服务器查询某个证书是否已被撤销，而不需要下载整个CRL文件。

其他选项的解释：

- A：RTCP（Real-time Transport Control Protocol，实时传输控制协议）是用于控制RTP（Real-time Transport Protocol）流的协议，与证书撤销无关。

- B：RTVP 不是一个常见的协议名称。

- D：CSRTP 也不是一个常见的协议名称，可能与SRTP（Secure Real-time Transport Protocol）混淆，但SRTP用于加密实时传输数据，与证书撤销无关。

-------------------

题目81：Xavier的公司逐步在使用更多的云服务，他担心公司在现有数据中心实施的安全策略到了云中没有得到遵循。以下哪项解决方案最适合确保将策略应用于所有云服务中？

Xavier’s company has been using an increasing number of cloud services, and he is concerned that the security policies that the company has implemented in its existing data center are not being followed in the cloud. Which of the following solutions is best suited to ensuring that policies are applied to all cloud services?

A：CIPS

A CIPS

B：CASB

A CASB

C：CSG

A CSG

D：CDLP

A CDLP

答案:题目中提到的Xavier担心公司在现有数据中心实施的安全策略在云中没有得到遵循，这涉及到云服务的安全管理和策略执行。以下是对每个选项的简要分析：

A. CIPS (Critical Infrastructure Protection System) - 关键基础设施保护系统，通常用于保护国家或企业的关键基础设施，与云服务的安全策略管理关系不大。

B. CASB (Cloud Access Security Broker) - 云访问安全代理，是一种安全策略执行点，位于云服务消费者和云服务提供商之间，用于确保企业安全策略在云环境中得到遵循。CASB可以提供数据安全、威胁防护、合规性管理和活动监控等功能。

C. CSG (Cloud Security Gateway) - 云安全网关，通常指的是提供安全服务的网络设备或软件，用于保护云环境中的数据和应用。它可能包括防火墙、入侵检测系统等功能，但不一定专门用于策略执行。

D. CDLP (Cloud Data Loss Prevention) - 云数据丢失防护，主要关注防止敏感数据在云环境中泄露，虽然它涉及安全策略，但主要侧重于数据保护而非全面的策略执行。

综合考虑，CASB（选项B）是最适合确保将策略应用于所有云服务中的解决方案，因为它专门设计来在云环境中执行和监控安全策略。

正确答案是：B. CASB

-------------------

题目82：什么过程使TCP成为面向连接的协议？

What process makes TCP a connection-oriented protocol?

A：它通过网络连接工作

It works via network connections.

B：它使用握手协议

It uses a handshake.

C：它监视断开的连接

It monitors for dropped connections.

D：它使用一个复杂的头

It uses a complex header.

答案:正确答案是 \*\*B：它使用握手协议\*\* (It uses a handshake)。

TCP（传输控制协议）是一种面向连接的协议，因为它通过三次握手（three-way handshake）过程在通信双方之间建立连接。这个过程确保了双方在数据传输之前已经准备好进行通信，并且确认了彼此的可用性。握手过程包括以下步骤：

1. \*\*SYN\*\*：客户端向服务器发送一个SYN（同步）包，请求建立连接。

2. \*\*SYN-ACK\*\*：服务器收到SYN包后，回复一个SYN-ACK（同步-确认）包，表示同意建立连接。

3. \*\*ACK\*\*：客户端收到SYN-ACK包后，再发送一个ACK（确认）包，确认连接已建立。

这个过程确保了连接的可靠性和顺序性，因此TCP被称为面向连接的协议。

其他选项的解释：

- A：它通过网络连接工作（It works via network connections）—— 虽然TCP确实通过网络连接工作，但这并不是它成为面向连接协议的原因。

- C：它监视断开的连接（It monitors for dropped connections）—— TCP确实会检测和处理断开的连接，但这并不是它成为面向连接协议的主要原因。

- D：它使用一个复杂的头（It uses a complex header）—— TCP的头部确实比较复杂，但这与它是否是面向连接的协议无关。

-------------------

题目83：Susan想为她的组织建立一个安全意识计划，但她知道让员工参与是很困难的。以下哪项技术通常在评估过程中与积分和分数的使用有关？

Susan wants to build a security awareness program for her organization, but knows that keeping staff engaged is difficult. Which of the following techniques is often associated with the use of points and scores as part of the assessment process?

A：游戏化

Gamification

B：网络钓鱼测试

Phishing testing

C：安全捍卫者

Security champions

D：社会工程学评估

Social engineering evaluations

答案:题目问的是在评估过程中通常与积分和分数使用相关的技术。让我们逐一分析每个选项：

A：游戏化（Gamification）

游戏化是一种通过引入游戏元素（如积分、分数、排行榜等）来激励和吸引用户的技术。它常用于提高员工的参与度和积极性，尤其是在安全意识培训中，通过积分和分数来评估员工的表现。

B：网络钓鱼测试（Phishing testing）

网络钓鱼测试是一种模拟网络钓鱼攻击的测试，用于评估员工对钓鱼邮件的识别能力。虽然它可以帮助评估员工的安全意识，但它本身并不直接涉及积分和分数的使用。

C：安全捍卫者（Security champions）

安全捍卫者是指在组织中推广安全意识和最佳实践的个人或团队。他们通常负责教育和培训其他员工，但并不直接涉及积分和分数的使用。

D：社会工程学评估（Social engineering evaluations）

社会工程学评估是通过模拟社会工程攻击（如电话诈骗、假冒身份等）来测试员工的安全意识。虽然它可以评估员工的表现，但它本身并不直接涉及积分和分数的使用。

综上所述，\*\*游戏化（Gamification）\*\* 是通常与积分和分数使用相关的技术。

\*\*正确答案：A：游戏化（Gamification）\*\*

-------------------

题目84：假如你正在为组织进行定性风险评估。在风险分析中，最重要的两个重要风险因素是概率和\_\_\_\_\_。

You are conducting a qualitative risk assessment for your organization. The two important risk elements that should weigh most heavily in your analysis of risk are probability and\_\_\_\_\_\_\_.

A：可能性

Likelihood

B：历史

History

C：影响

Impact

D：成本

Cost

答案:在定性风险评估中，最重要的两个风险因素是概率和影响。概率指的是风险事件发生的可能性，而影响则是指风险事件发生后对组织或项目造成的后果或损害程度。因此，正确答案是：

C：影响

Impact

所以完整的句子是：

You are conducting a qualitative risk assessment for your organization. The two important risk elements that should weigh most heavily in your analysis of risk are probability and impact.

-------------------

题目85：OSI模型中，数据链路层使用什么格式来格式化从堆栈接收的消息？

Using the OSI model, what format does the Data Link layer use to format messages received from higher up the stack?

A：数据流

A data stream

B：帧

A frame

C：段

A segment

D：数据报

A datagram

答案:在OSI模型中，数据链路层负责将网络层传递下来的数据包（数据报）格式化为帧（Frame），以便在物理介质上进行传输。帧是数据链路层的基本传输单位，包含了数据以及必要的控制信息，如帧头、帧尾和错误检测码等。

因此，正确答案是：

\*\*B：帧\*\*

\*\*A frame\*\*

-------------------

题目86：在考虑违反道德的行为时，(ISC)2同行评审委员会可能施加的最大惩罚是什么？

What is the maximum penalty that may be imposed by an (ISC)2 peer review board when considering a potential ethics violation?

A：撤销认证

Revocation of certification

B：终止雇用

Termination of employment

C：罚款

Financial penalty

D：暂停认证

Suspension of certification

答案:在考虑违反道德的行为时，(ISC)2同行评审委员会可能施加的最大惩罚是撤销认证。因此，正确答案是：

A：撤销认证

Revocation of certification

(ISC)2 是一个国际性的信息安全认证机构，负责管理 CISSP（Certified Information Systems Security Professional）等认证。当认证持有者违反道德准则时，(ISC)2 同行评审委员会有权采取多种措施，其中最严厉的惩罚是撤销其认证资格。这意味着该人将不再被认可为 (ISC)2 认证的专业人员。

-------------------

题目87：关于SDLC，以下哪个陈述是正确的？

Which one of the following statements about the SDLC is correct?

A：SDLC需要使用迭代方法来进行软件开发

The SDLC requires the use of an iterative approach to software development.

B：SDLC需要使用顺序方法来进行软件开发

The SDLC requires the use of a sequential approach to software development.

C：SDLC不包括为最终用户和支持人员提供的培训

The SDLC does not include training for end users and support staff.

D：瀑布方法与SDLC兼容

The waterfall methodology is compatible with the SDLC.

答案:D：瀑布方法与SDLC兼容

The waterfall methodology is compatible with the SDLC.

解释：

- A选项：SDLC（软件开发生命周期）并不强制要求使用迭代方法。虽然迭代开发是SDLC中的一种方法，但SDLC也可以使用其他方法，如瀑布模型。

- B选项：SDLC并不强制要求使用顺序方法。虽然瀑布模型是一种顺序方法，但SDLC也可以使用迭代或增量方法。

- C选项：SDLC通常包括为最终用户和支持人员提供的培训，这是确保软件成功部署和使用的重要步骤。

- D选项：瀑布方法是SDLC中的一种经典模型，因此它与SDLC是兼容的。瀑布模型是一种顺序的开发方法，适用于需求明确且变化较少的项目。

-------------------

题目88：如图所示，Harry在访问安全级别更高的文件时被拒绝，请问什么安全模型阻止此行为？

<div style="text-align:center"><img alt="" height="115" src="/file/100000/m/20210907/2b6f4ba44c6b45809fc02402075d21e7.png" width="355" /></div>

In the diagram shown here, Harry is prevented from reading a file at a higher classification level than his security clearance. What security model prevents this behavior?

<div style="text-align:center"><img alt="" height="121" src="/file/100000/m/20210907/ffcbb6c2ff19461ea28c782f5e32abf3.png" width="433" /></div>

A：Bell-LaPadula

Bell-LaPadula

B：Biba

Biba

C：Clark-Wilson

Clark-Wilson

D：Brewer-Nash

Brewer-Nash

答案:题目描述的是Harry在访问安全级别更高的文件时被拒绝，这种情况符合Bell-LaPadula模型的特点。Bell-LaPadula模型是一种多级安全模型，主要用于防止信息从高安全级别流向低安全级别。该模型有两个主要规则：

1. \*\*简单安全属性（Simple Security Property）\*\*：一个主体不能读取安全级别高于其许可级别的对象。

2. \*\*星属性（\*-Property）\*\*：一个主体不能写入安全级别低于其许可级别的对象。

因此，Harry被阻止访问安全级别更高的文件，正是Bell-LaPadula模型的简单安全属性在起作用。

所以正确答案是：

\*\*A：Bell-LaPadula\*\*

-------------------

题目89：Susan正在为当地咖啡馆建立网络，希望确保用户必须使用电子邮件地址进行身份验证，并在允许之前同意咖啡馆的使用政策。她应该使用什么技术来做到这一点？

Susan is setting up the network for a local coffee house and wants to ensure that users have to authenticate using an email address and agree to the coffee house’s acceptable use policy before being allowed on the network. What technology should she use to do this?

A：802.11

802.11

B：NAC

NAC

C：强制门户

A captive portal

D：无线网关

A wireless gateway

答案:题目89的正确答案是：

C：强制门户 (A captive portal)

解释：

强制门户（Captive Portal）是一种网络访问控制技术，通常用于公共Wi-Fi网络中。当用户尝试连接到网络时，强制门户会拦截用户的请求，并将用户重定向到一个特定的网页。在这个网页上，用户通常需要输入电子邮件地址进行身份验证，并同意网络的使用政策（如咖啡馆的“可接受使用政策”）。只有在用户完成这些步骤后，才会被允许访问网络。

其他选项的解释：

- \*\*802.11\*\*：这是无线局域网（WLAN）的标准，与身份验证和使用政策无关。

- \*\*NAC（网络访问控制）\*\*：NAC是一种更广泛的网络安全管理技术，用于控制设备访问网络的权限，但它不直接涉及强制门户的功能。

- \*\*无线网关\*\*：无线网关是连接无线网络和有线网络的设备，也不直接涉及强制门户的功能。

因此，强制门户是最适合Susan需求的解决方案。

-------------------

题目90：Travis关注于他的组织使用Microsoft的Bit-Locker为系统提供的安全性。如果系统配备了TPM并使用全盘加密，那么基于驱动器加密状态的系统，何时最安全的防止数据丢失？

Travis is concerned about the security that his organization’s use of Microsoft’s Bit-Locker provides for systems. When are the systems most secure from data loss based on the encryption state of the drive if the systems are equipped with TPM and use full disk encryption?

A：当系统启动并运行时，因为系统会监视驱动器访问

When they are booted up and running because the system monitors for drive access

B：当系统正在停机时，因为密码会从内存中删除

When the system is shutting down because keys are removed from memory

C：当系统正在启动时，因为TPM会检查安全启动过程

When they are booting up because the TPM checks for a secure boot process

D：当系统被关闭时，因为磁盘被全盘加密了

When they are off because the drive is fully encrypted

答案:正确答案是 D：当系统被关闭时，因为磁盘被全盘加密了。

解析：

- \*\*A选项\*\*：当系统启动并运行时，系统确实会监视驱动器访问，但这并不意味着数据最安全。在系统运行时，加密密钥通常存储在内存中，如果系统被攻击，攻击者可能能够访问这些密钥。

- \*\*B选项\*\*：当系统正在停机时，密码会从内存中删除，这确实增加了安全性，但系统仍然处于一个过渡状态，可能还未完全关闭。

- \*\*C选项\*\*：当系统正在启动时，TPM会检查安全启动过程，但这只是启动过程中的一个安全措施，并不能保证整个系统的数据安全。

- \*\*D选项\*\*：当系统被关闭时，磁盘被全盘加密，这意味着数据在没有正确密钥的情况下是无法访问的。因此，这是数据最安全的状态，因为即使物理磁盘被窃取，数据也无法被解密。

因此，D选项是最正确的答案。

-------------------

题目91：Andrea希望确保虚拟化环境之间的虚拟化网络安全。她在她所在州的多个位置使用虚拟机集群，并且在这些位置之间使用第三方互联网服务提供商。如果她在这些位置之间运行扁平化2层网络，以下哪项解决方案最适合保护她的流量？

Andrea wants to ensure that her virtualized networks are secure between virtual environments. She uses virtual machine clusters in multiple locations in her state with third-party internet service providers between those locations. Which of the following solutions is best suited to protecting her traffic if she runs a flattened layer 2 network between those locations?

A：TLS

TLS

B：BGP

BGP

C：IPsec

IPsec

D：AES

AES

答案:在Andrea的情况下，她需要在多个位置的虚拟机集群之间保护流量，并且这些位置之间使用的是第三方互联网服务提供商。她运行的是扁平化的2层网络。在这种情况下，最适合的解决方案是使用IPsec（Internet Protocol Security）。

IPsec是一种用于保护IP通信的协议套件，它提供了加密和认证服务，确保数据在传输过程中的机密性、完整性和真实性。IPsec可以在网络层（第3层）上运行，因此它适用于保护2层网络中的流量。

其他选项的解释如下：

- \*\*TLS（Transport Layer Security）\*\*：主要用于保护应用层（第7层）的通信，例如HTTPS。它不适合用于保护2层网络流量。

- \*\*BGP（Border Gateway Protocol）\*\*：是一种用于在互联网上交换路由信息的协议，它本身并不提供加密或安全保护。

- \*\*AES（Advanced Encryption Standard）\*\*：是一种加密算法，通常用于加密数据，但它本身不是一个完整的解决方案，通常需要与其他协议（如IPsec）结合使用。

因此，\*\*C：IPsec\*\* 是最适合保护Andrea流量的解决方案。

-------------------

题目92-1：根据如下场景，回答3个问题

Fred的公司在审查该公司发行的手机的安全性。他们发布支持Android和iOS系统的4G 智能手机，并使用移动设备管理解决方案将公司软件部署到手机。一旦手机丢失，公司可通过移动设备管理软件远程擦除电话。

For questions , please refer to the following scenario:

The company that Fred works for is reviewing the security of their company-issued cell phones. They issue 4G-capable smartphones running Android and iOS and use a mobile device management solution to deploy company software to the phones. The mobile device management software also allows the company to remotely wipe the phones if they are lost.

Fred 的公司在通过蜂窝网络发送敏感数据时需要考虑哪些安全问题？

What security considerations should Fred’s company require for sending sensitive data over the cellular network?

A：他们应该使用与任何公共网络上的数据相同的要求

They should use the same requirements as data over any public network.

B：蜂窝提供商网络是专用网络，不需要特别考虑

Cellular provider networks are private networks and should not require special consideration.

C：加密所有流量以确保机密性

Encrypt all traffic to ensure confidentiality.

D：对于从电话发送的所有数据，需要使用WAP

Require the use of WAP for all data sent from the phone.

答案:在通过蜂窝网络发送敏感数据时，Fred 的公司需要考虑以下几个安全问题：

1. \*\*数据加密\*\*：确保所有传输的数据都经过加密，以防止数据在传输过程中被拦截和窃取。加密可以保护数据的机密性和完整性。

2. \*\*网络安全性\*\*：虽然蜂窝网络相对较为安全，但它们仍然是公共网络的一部分，可能会受到攻击。因此，公司不应假设蜂窝网络是完全安全的，而应采取额外的安全措施。

3. \*\*身份验证和授权\*\*：确保只有经过授权的设备和用户才能访问公司网络和数据。使用强身份验证机制，如多因素认证（MFA），可以增加安全性。

4. \*\*远程擦除功能\*\*：如果设备丢失或被盗，公司应能够远程擦除设备上的数据，以防止敏感信息泄露。

5. \*\*定期更新和补丁管理\*\*：确保所有设备和软件都定期更新，以修补已知的安全漏洞。

根据这些考虑，最合适的选项是：

\*\*C：加密所有流量以确保机密性\*\*

这个选项直接涉及到数据加密，这是保护敏感数据在传输过程中不被窃取的关键措施。其他选项要么不够全面（如选项A），要么基于错误的假设（如选项B），或者不适用于所有情况（如选项D）。

-------------------

题目92-1：根据如下场景，回答3个问题

Fred的公司在审查该公司发行的手机的安全性。他们发布支持Android和iOS系统的4G 智能手机，并使用移动设备管理解决方案将公司软件部署到手机。一旦手机丢失，公司可通过移动设备管理软件远程擦除电话。

For questions , please refer to the following scenario:

The company that Fred works for is reviewing the security of their company-issued cell phones. They issue 4G-capable smartphones running Android and iOS and use a mobile device management solution to deploy company software to the phones. The mobile device management software also allows the company to remotely wipe the phones if they are lost.

Fred今年打算参加一个重要的黑客会议，他在会议期间需要连接到公司内网络。在会议期间连接到他的蜂窝提供商的4G 网络时应该怎么做？

Fred intends to attend a major hacker conference this year and needs to connect to his employer’s network during his time at the conference. What should he do when connecting to his cellular provider’s 4G network while at the conference?

A：继续正常使用

Continue normal usage.

B：停止所有使用；可能发生塔欺骗

Discontinue all usage; towers can be spoofed.

C：仅使用受信任的Wi-Fi网络

Only use trusted WiFi networks.

D：连接到他公司的加密VPN服务

Connect to his company’s encrypted VPN service.

答案:在Fred参加黑客会议期间，连接到蜂窝提供商的4G网络时，最安全的做法是连接到公司的加密VPN服务。这是因为：

1. \*\*安全性\*\*：VPN（虚拟私人网络）可以加密Fred的互联网连接，保护数据不被拦截或窃听。在黑客会议这样的高风险环境中，这一点尤为重要。

2. \*\*隐私保护\*\*：通过VPN，Fred的网络活动将通过加密的隧道传输，使得外部观察者难以追踪或分析他的网络行为。

3. \*\*访问控制\*\*：VPN还可以帮助Fred安全地访问公司内部资源，确保只有授权用户才能访问敏感信息。

选项A（继续正常使用）不够安全，因为在不加密的连接下，数据容易被拦截。选项B（停止所有使用；可能发生塔欺骗）虽然指出了塔欺骗的风险，但完全停止使用可能不切实际。选项C（仅使用受信任的Wi-Fi网络）虽然比公开Wi-Fi更安全，但在黑客会议这样的环境中，即使是受信任的Wi-Fi也可能存在风险。

因此，\*\*D：连接到他公司的加密VPN服务\*\* 是最佳选择。

-------------------

题目92-1：根据如下场景，回答3个问题

Fred的公司在审查该公司发行的手机的安全性。他们发布支持Android和iOS系统的4G 智能手机，并使用移动设备管理解决方案将公司软件部署到手机。一旦手机丢失，公司可通过移动设备管理软件远程擦除电话。

For questions , please refer to the following scenario:

The company that Fred works for is reviewing the security of their company-issued cell phones. They issue 4G-capable smartphones running Android and iOS and use a mobile device management solution to deploy company software to the phones. The mobile device management software also allows the company to remotely wipe the phones if they are lost.

哪种情况最可能导致移动电话的远程擦除失败？

What are the most likely circumstances that would cause a remote wipe of a mobile phone to fail?

A：手机上有密码

The phone has a passcode on it.

B：电话无法联系网络

The phone cannot contact a network.

C：提供商尚未解锁手机

The provider has not unlocked the phone.

D：电话正在使用中

The phone is in use.

答案:根据题目描述，Fred的公司使用移动设备管理（MDM）解决方案来远程擦除丢失的手机。远程擦除功能依赖于手机能够连接到网络，以便接收和执行来自MDM服务器的擦除指令。因此，如果手机无法连接到网络，远程擦除指令将无法传递到手机，从而导致擦除失败。

选项分析：

- \*\*A：手机上有密码\*\*

手机上有密码并不会影响远程擦除功能，因为远程擦除是通过MDM软件执行的，与手机是否解锁无关。

- \*\*B：电话无法联系网络\*\*

如果手机无法连接到网络（例如，处于飞行模式、没有信号或关闭了数据连接），MDM服务器将无法将擦除指令发送到手机，从而导致远程擦除失败。这是最可能导致远程擦除失败的情况。

- \*\*C：提供商尚未解锁手机\*\*

手机是否被提供商解锁与远程擦除功能无关，只要手机能够连接到网络，远程擦除指令就可以执行。

- \*\*D：电话正在使用中\*\*

手机是否正在使用并不会影响远程擦除功能，只要手机能够连接到网络，擦除指令就可以执行。

因此，最可能导致远程擦除失败的情况是 \*\*B：电话无法联系网络\*\*。

\*\*答案：B\*\*

-------------------

题目93：Elaine 正在为所在组织制定业务连续性计划。她应该尽量减少什么价值？

Elaine is developing a business continuity plan for her organization. What value should she seek to minimize?

A：AV

AV

B：SSL

SSL

C：RTO

RTO

D：MTO

MTO

答案:在制定业务连续性计划时，Elaine应该尽量减少的是 \*\*C：RTO（Recovery Time Objective，恢复时间目标）\*\*。

\*\*RTO\*\* 是指从灾难或中断发生到业务恢复正常运作所需的时间。减少RTO意味着组织能够更快地恢复业务运作，从而减少业务中断带来的损失和影响。因此，RTO是业务连续性计划中的一个关键指标，Elaine应该尽量优化和减少这个时间。

其他选项的解释：

- \*\*AV（Asset Value，资产价值）\*\*：这是指资产的价值，通常不是业务连续性计划中需要减少的指标。

- \*\*SSL（Secure Sockets Layer，安全套接层）\*\*：这是一种加密协议，与业务连续性计划的目标无关。

- \*\*MTO（Maximum Tolerable Outage，最大可容忍中断时间）\*\*：这是指业务可以容忍的最大中断时间，通常是一个固定的阈值，而不是需要减少的指标。

因此，正确答案是 \*\*C：RTO\*\*。

-------------------

题目94：Warren想要进行内部安全审计。他想使用一个广泛接受的审计框架，以便他可以更容易地将结果与其他组织进行比较。他应该选择以下哪项作为他的基本审计框架？

Warren wants to conduct an internal security audit. He wants to use a broadly accepted audit framework so that he can more easily compare the results to other organizations. Which of the following options should he select as his base audit framework?

A：ITSM

ITSM

B：ATT&CK

ATT&CK

C：COBIT

COBIT

D：CIS

CIS

答案:Warren 想要进行内部安全审计，并且希望使用一个广泛接受的审计框架，以便更容易地将结果与其他组织进行比较。在给定的选项中，最适合的选择是：

\*\*C：COBIT\*\*

\*\*解释：\*\*

- \*\*COBIT (Control Objectives for Information and Related Technologies)\*\* 是一个广泛接受的审计框架，专门用于IT治理和管理。它提供了一套全面的控制目标和最佳实践，帮助组织确保其IT系统与业务目标一致，并且能够有效地管理风险。

- \*\*ITSM (IT Service Management)\*\* 主要关注IT服务的管理和交付，而不是审计。

- \*\*ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)\*\* 是一个用于描述和分类网络攻击行为的框架，主要用于威胁情报和防御策略，而不是审计。

- \*\*CIS (Center for Internet Security)\*\* 提供了一些安全基准和最佳实践，但它不是一个全面的审计框架。

因此，\*\*COBIT\*\* 是最适合 Warren 进行内部安全审计的框架。

-------------------

题目95：将灾难恢复测试类型列表按其对业务的潜在影响的顺序列出，从影响最小到最有影响进行排序。

1. 通读测试

2. 平行测试

3. 桌面测试

4. 完全中断测试

Place the list of disaster recovery test types in order of their potential impact on the business, starting with the least impactful and progressing through the most impactful.

1. Checklist review

2. Parallel test

3. Tabletop exercise

4. Full interruption test

A：1, 2, 3, 4

1, 2, 3, 4

B：1, 3, 2, 4

1, 3, 2, 4

C：1, 3, 4, 2

1, 3, 4, 2

D：2, 1, 3, 4

2, 1, 3, 4

答案:正确答案是 \*\*B：1, 3, 2, 4\*\*。

解释如下：

1. \*\*Checklist review（通读测试）\*\*：这是对灾难恢复计划的简单审查，通常不涉及实际操作，对业务的影响最小。

2. \*\*Tabletop exercise（桌面测试）\*\*：这是一种模拟演练，团队成员讨论和模拟灾难恢复过程，但不涉及实际系统操作，对业务的影响较小。

3. \*\*Parallel test（平行测试）\*\*：在这种测试中，备用系统与实际生产系统同时运行，以验证备用系统的功能。虽然对业务有一定影响，但不会中断正常业务操作。

4. \*\*Full interruption test（完全中断测试）\*\*：这是最全面的测试类型，涉及实际中断生产系统并切换到备用系统。这种测试对业务的影响最大，因为它可能导致业务中断。

因此，按照对业务的潜在影响从小到大排序，正确的顺序是 \*\*1, 3, 2, 4\*\*。

-------------------

题目96：Jack的数据中心设计要求每台关键服务器都配备双电源。他通过这个设计可以解决CIA的哪一部分？

Jack’s data center design calls for dual-power supplies in every critical server. What part of the CIA triad is he addressing with this design decision?

A：机密性

Confidentiality

B：完整性

Integrity

C：可用性

Availability

D：以上都不是

None of the above

答案:题目中提到的Jack的数据中心设计要求每台关键服务器都配备双电源。这个设计主要是为了解决服务器的电源故障问题，确保在一路电源出现故障时，另一路电源可以继续供电，从而保证服务器的持续运行。这直接关系到系统的可用性（Availability），即确保授权用户在需要时可以访问信息和资源。

因此，这个设计决策主要解决的是CIA三元组中的可用性部分。

正确答案是：

C：可用性

Availability

-------------------

题目97：图中显示的IR流程循环图中缺少哪一步骤？

What step is missing from the IR process cycle diagram shown here?

<div style="text-align:center"><img alt="" height="383" src="/file/100000/m/20210907/b0b2de11653b41259fd254de5afa988a.png" width="467" /></div>

A：取证

Forensics

B：惩罚

Retribution

C：恢复

Recovery

D：分析

Analysis

答案:在信息检索（IR）流程循环图中，通常包括以下几个关键步骤：需求分析、信息收集、信息处理、信息存储、信息检索、信息展示和反馈。根据题目描述，图中缺少的步骤是“恢复”（Recovery）。

因此，正确答案是：

C：恢复

Recovery

-------------------

题目98：Frank 试图保护他的Web 应用程序不受跨站点脚本攻击。用户不需要提供包含脚本的输入，因此他认定最有效的过滤方法是在监视<SCRIPT>标记的服务器上编写一个过滤器，并删除它。Frank 的方法有什么问题？

Frank is attempting to protect his web application against cross-site scripting attacks. Users do not need to provide input containing scripts, so he decided the most effective way to filter would be to write a filter on the server that watches for the &lt;SCRIPT&gt; tag and removes it. What is the issue with Frank’s approach?

A：验证应始终在客户端执行

Validation should always be performed on the client side.

B：攻击者可以使用XSS 过滤器逃避技术来抵抗这种方法

Attackers may use XSS filter evasion techniques against this approach.

C：服务器端验证需要删除所有HTML 标记，而不仅是&lt;SCRIPT&gt;标记

Server-side validation requires removing all HTML tags, not just the &lt;SCRIPT&gt; tag.

D：Frank 的做法没有问题

There is no problem with Frank’s approach.

答案:Frank 的方法存在一些问题，主要在于跨站点脚本攻击（XSS）的复杂性。XSS 攻击不仅仅依赖于 `<SCRIPT>` 标签，攻击者可以使用多种技术来绕过这种简单的过滤机制。例如，攻击者可以使用其他 HTML 标签、事件处理器、JavaScript 伪协议等方式来注入恶意脚本。

选项分析：

- \*\*A：验证应始终在客户端执行\*\*

这个选项是错误的。客户端验证虽然可以提高用户体验，但不能替代服务器端验证，因为客户端验证可以被绕过。服务器端验证是确保安全的关键。

- \*\*B：攻击者可以使用XSS 过滤器逃避技术来抵抗这种方法\*\*

这个选项是正确的。攻击者可以使用各种技术来绕过简单的 `<SCRIPT>` 标签过滤，例如使用 `<img>` 标签的 `onerror` 属性、`<a>` 标签的 `href` 属性中的 JavaScript 伪协议等。

- \*\*C：服务器端验证需要删除所有HTML 标记，而不仅是<SCRIPT>标记\*\*

这个选项部分正确，但并不完全准确。虽然删除所有 HTML 标记可以防止 XSS 攻击，但这并不是唯一的方法。更有效的方法是使用上下文相关的输出编码和输入验证。

- \*\*D：Frank 的做法没有问题\*\*

这个选项是错误的。Frank 的方法过于简单，无法有效防止 XSS 攻击。

因此，最合适的答案是 \*\*B：攻击者可以使用XSS 过滤器逃避技术来抵抗这种方法\*\*。

-------------------

题目99：Megan希望确保与她的公司签订合同的新软件即服务提供商，能够确保服务始终正常运行而不会中断。以下哪项通常是提供这种保证合同的一部分？

Megan wants to ensure that the new software as a service provider that her company is signing a contract with will make sure the service works all the time without disruptions. Which of the following is often part of contracts to provide that assurance?

A：SLA

An SLA

B：RPA

An RPA

C：NDA

An NDA

D：MOU

An MOU

答案:A：SLA

SLA（Service Level Agreement，服务级别协议）通常是合同中用于确保服务提供商能够保证服务正常运行而不会中断的部分。SLA 会明确规定服务的可用性、性能标准、响应时间等关键指标，并规定如果未能达到这些标准时的补救措施或赔偿条款。因此，SLA 是 Megan 所寻求的保证服务正常运行的关键合同组成部分。

-------------------

题目100：Uptown Records 的管理层最近与医院签订了一份合同，用于安全存储医疗记录。该医院是一家总部位于美国、受HIPAA保护的实体，这意味着它需要确保与其签约的组织能够满足安全实践要求。两个组织必须签署什么类型的协议才能遵守HIPAA？

Uptown Records Management recently entered into a contract with a hospital for the secure storage of medical records. The hospital is a U.S.-based, HIPAA-covered entity, which means it needs to ensure that organizations they contract with can meet security practice requirements. What type of agreement should the two organizations sign to meet this requirement?

A：NDA

NDA

B：NCA

NCA

C：BAA

BAA

D：SLA

SLA

答案:为了遵守HIPAA（健康保险可携性和责任法案）的要求，Uptown Records Management 和医院之间需要签署一份商业伙伴协议（Business Associate Agreement, BAA）。BAA 是 HIPAA 要求的一种法律协议，确保所有涉及处理受保护健康信息（PHI）的商业伙伴遵守 HIPAA 的隐私和安全规则。

选项解释：

A: NDA（Non-Disclosure Agreement，保密协议）通常用于保护商业秘密和敏感信息，但不是专门针对 HIPAA 要求的。

B: NCA（Non-Compete Agreement，非竞争协议）用于限制员工或合作伙伴在合同结束后与竞争对手合作，与 HIPAA 无关。

C: BAA（Business Associate Agreement，商业伙伴协议）是 HIPAA 要求的，确保商业伙伴遵守 HIPAA 规则。

D: SLA（Service Level Agreement，服务级别协议）定义了服务提供商和客户之间的服务标准和期望，但不是专门针对 HIPAA 的。

因此，正确答案是：

C：BAA

-------------------

题目101：Norm准备为其组织进行灾难恢复测试，并希望选择最彻底的测试类型，认识到它可能相当具有破坏性。Norm应该选择什么类型的测试？

Norm would like to conduct a disaster recovery test for his organization and wants to choose the most thorough type of test, recognizing that it may be quite disruptive. What type of test should Norm choose?

A：完全中断测试

Full interruption test

B：平行测试

Parallel test

C：桌面测试

Tabletop exercise

D：通读测试

Checklist review

答案:Norm准备为其组织进行灾难恢复测试，并希望选择最彻底的测试类型，认识到它可能相当具有破坏性。Norm应该选择什么类型的测试？

\*\*A：完全中断测试 (Full interruption test)\*\*

完全中断测试是最彻底的灾难恢复测试类型。在这种测试中，生产系统会被完全中断，所有操作都会转移到灾难恢复系统上。这种测试能够全面验证灾难恢复计划的有效性，但由于其破坏性较大，可能会对业务造成较大影响。因此，Norm在选择这种测试时需要谨慎考虑其对业务的影响。

其他选项：

- \*\*B：平行测试 (Parallel test)\*\*：在这种测试中，生产系统和灾难恢复系统同时运行，以验证灾难恢复系统的功能。这种测试的破坏性较小，但不如完全中断测试彻底。

- \*\*C：桌面测试 (Tabletop exercise)\*\*：这是一种模拟演练，团队成员通过讨论和模拟来验证灾难恢复计划。这种测试的破坏性最小，但无法全面验证系统的实际恢复能力。

- \*\*D：通读测试 (Checklist review)\*\*：这是一种简单的检查清单审查，确保所有步骤和程序都已准备就绪。这种测试的破坏性最小，但无法验证实际恢复过程。

因此，Norm应该选择\*\*A：完全中断测试 (Full interruption test)\*\*，以确保最彻底的测试效果。

-------------------

题目102：Ed 正在建设一个支持IPv6 但需要将其连接到IPv4 网络的网络。应该在网络之间放置什么类型的设备？

Ed is building a network that supports IPv6 but needs to connect it to an IPv4 network. What type of device should Ed place between the networks?

A：交换机

A switch

B：路由器

A router

C：桥

A bridge

D：网关

A gateway

答案:正确答案是 D：网关 (A gateway)。

IPv6 和 IPv4 是两种不同的网络协议，它们之间不能直接通信。为了在 IPv6 网络和 IPv4 网络之间进行通信，需要使用一种能够进行协议转换的设备，这种设备就是网关。网关可以在 IPv6 和 IPv4 之间进行数据包的转换和路由，使得两种不同协议的网络能够互相通信。

其他选项的解释：

- A：交换机 (A switch) - 交换机主要用于在同一网络内转发数据包，不能处理不同协议之间的通信。

- B：路由器 (A router) - 路由器主要用于在不同网络之间转发数据包，但通常需要网络使用相同的协议（如 IPv4 或 IPv6），不能直接处理 IPv6 和 IPv4 之间的通信。

- C：桥 (A bridge) - 桥用于连接同一协议的网络段，不能处理不同协议之间的通信。

因此，网关是最合适的设备。

-------------------

题目103：Henry的公司已经部署了广泛的物联网基础设施，用于楼宇监控，其中包括环境控制、占用传感器以及有助于管理楼宇的各种其他传感器和控制器。Henry在分析物联网部署时，应报告以下哪项安全问题最为关键？

Henry’s company has deployed an extensive IoT infrastructure for building monitoring that includes environmental controls, occupancy sensors, and a variety of other sensors and controllers that help manage the building. Which of the following security concerns should Henry report as the most critical in his analysis of the IoT deployment?

A：IoT设备常见的安全日志本地存储空间不足

The lack of local storage space for security logs that is common to IoT devices.

B：IoT设备可能没有单独的管理界面，允许同一网络上的任何人尝试登录，这使得暴力攻击成为可能

The IoT devices may not have a separate administrative interface, allowing anybody on the same network to attempt to log into them and making brute-force attacks possible.

C：IoT设备可能不支持强加密通信，将日志和传感器数据暴露在网络上被拦截

The IoT devices may not support strong encryption for communications, exposing the log and sensor data to interception on the network.

D：IoT设备的长期支持和修补模型可能会给组织带来安全和运营风险

The long-term support and patching model for the IoT devices may create security and operational risk for the organization.

答案:

\*\*D选项\*\*是最关键的安全问题。

-------------------

题目104：Isaac想要使用无连接协议来传输数据，因为他需要优化传输速度而不是可靠性。他应该选择哪种协议？

Isaac wants to use a connectionless protocol to transfer data because he needs to optimize speed of transmission over reliability. Which protocol should he select?

A：ICMP

ICMP

B：TCP

TCP

C：UDP

UDP

D：SNMP

SNMP

答案:Isaac应该选择 \*\*C：UDP\*\*。

UDP（用户数据报协议）是一种无连接协议，它不保证数据的可靠传输，但传输速度较快。UDP适用于那些对传输速度要求较高、但对数据可靠性要求较低的应用场景，例如实时视频流、在线游戏等。

其他选项的解释：

- \*\*A：ICMP\*\*（Internet控制消息协议）主要用于网络诊断和错误报告，不是用于数据传输的协议。

- \*\*B：TCP\*\*（传输控制协议）是一种面向连接的协议，提供可靠的数据传输，但速度相对较慢。

- \*\*D：SNMP\*\*（简单网络管理协议）用于网络设备的管理和监控，也不是用于数据传输的协议。

因此，UDP是最符合Isaac需求的选择。

-------------------

题目105：下列哪项动作不属于欧盟数据保护指令GDPR的要求？

Which one of the following actions is not required under the EU General Data Protection Regulation?

A：组织必须允许个人选择不进行信息共享

Organizations must allow individuals to opt out of information sharing.

B：组织必须向个人列出可获取信息的员工的名单

Organizations must provide individuals with lists of employees with access to information.

C：组织必须使用适当的机制保护数据免受未经授权的披露

Organizations must use proper mechanisms to protect data against unauthorized disclosure.

D：组织必须有针解决隐私问题纠纷的解决流程

Organizations must have a dispute resolution process for privacy issues.

答案:根据欧盟的《通用数据保护条例》（GDPR），组织必须遵守一系列数据保护要求。这些要求包括允许个人选择不进行信息共享（A选项），使用适当的机制保护数据免受未经授权的披露（C选项），以及有针解决隐私问题纠纷的解决流程（D选项）。然而，GDPR并没有要求组织必须向个人列出可获取信息的员工的名单（B选项）。因此，B选项是不属于GDPR要求的动作。

正确答案是：

B：组织必须向个人列出可获取信息的员工的名单

Organizations must provide individuals with lists of employees with access to information.

-------------------

题目106：Tammy为她的组织选择了一个灾难恢复设施。她想选择一个能够平衡恢复运营所需时间和所涉成本的设施。她应该选择什么类型的设施？

Tammy is selecting a disaster recovery facility for her organization. She would like to choose a facility that balances the time required to recover operations with the cost involved. What type of facility should she choose?

A：热站点

Hot site

B：温站点

Warm site

C：冷站点

Cold site

D：红站点

Red site

答案:Tammy 应该选择一个能够平衡恢复运营所需时间和所涉成本的设施。在这种情况下，最合适的选择是 \*\*B：温站点（Warm site）\*\*。

### 解释：

- \*\*热站点（Hot site）\*\*：热站点是完全配置好的设施，几乎可以立即恢复运营。虽然恢复时间非常短，但成本也非常高。

- \*\*温站点（Warm site）\*\*：温站点部分配置，需要一些时间来恢复运营，但成本比热站点低。它提供了一个平衡点，既不会像热站点那样昂贵，也不会像冷站点那样需要很长时间来恢复。

- \*\*冷站点（Cold site）\*\*：冷站点是一个空壳设施，几乎没有预先配置的设备或资源。虽然成本最低，但恢复时间最长。

- \*\*红站点（Red site）\*\*：这个选项通常不是一个标准的灾难恢复设施类型，可能是干扰项。

因此，\*\*温站点（Warm site）\*\* 是最符合 Tammy 需求的选项，因为它能够在恢复时间和成本之间提供一个合理的平衡。

-------------------

题目107：哪一层OSI模型与数据报相关联？

What layer of the OSI model is associated with datagrams?

A：会话层

Session

B：传输层

Transport

C：网络层

Network

D：数据链路层

Data Link

答案:正确答案是：C：网络层 (Network)

在OSI（开放系统互连）模型中，数据报（datagram）是与网络层（Network Layer）相关联的。网络层负责数据包的路由和转发，确保数据能够从源设备传输到目标设备。数据报是网络层的基本传输单元，通常包含源地址和目标地址信息，以便在网络中进行路由选择。

其他选项的解释：

- A：会话层（Session Layer）负责建立、管理和终止会话。

- B：传输层（Transport Layer）负责端到端的通信，确保数据的可靠传输。

- D：数据链路层（Data Link Layer）负责在物理链路上传输数据帧，并进行错误检测和纠正。

-------------------

题目108：以下哪一项不是高级加密标准的有效密钥长度？

Which one of the following is not a valid key length for the Advanced Encryption Standard?

A：128位

128 bits

B：192位

192 bits

C：256位

256 bits

D：384位

384 bits

答案:高级加密标准（AES）是一种广泛使用的对称加密算法。AES的有效密钥长度包括128位、192位和256位。因此，384位不是AES的有效密钥长度。

正确答案是：

D：384位

384 bits

-------------------

题目109：以下哪种技术提供了一个功能接口，允许开发人员在不知道该系统的实现细节的情况下直接与系统交互？

Which one of the following technologies provides a function interface that allows developers to directly interact with systems without knowing the implementation details of that system?

A：数据字典

Data dictionary

B：客体模型

Object model

C：源代码

Source code

D：API

API

答案:正确答案是 D：API。

API（Application Programming Interface，应用程序编程接口）提供了一个功能接口，允许开发人员在不知道系统内部实现细节的情况下直接与系统交互。API 定义了如何与系统进行通信的规则和协议，开发人员只需按照这些规则调用相应的函数或方法即可使用系统的功能，而无需关心系统内部的具体实现。

其他选项的解释：

- A：数据字典（Data dictionary）主要用于描述数据库中的数据结构，而不是提供功能接口。

- B：客体模型（Object model）是一种面向对象的编程模型，用于描述对象之间的关系和行为，但它本身不是一个功能接口。

- C：源代码（Source code）是系统的实现细节，开发人员需要了解源代码才能进行修改或扩展，因此不符合题目要求。

-------------------

题目110：Ian想要评估其公司新的SaaS提供商的安全性。以下哪项是他实际期望能够用来评估主要云提供商安全性的最有可能选项？

Ian wants to assess the security of his company’s new SaaS provider. Which of the following options is the most likely option that he can realistically expect to be able to use to assess a major cloud provider’s security?

A：针对提供商的外部服务运行漏洞扫描

Run a vulnerability scan against the provider’s external services.

B：要求提供SOC 2类型II报告

Request a SOC 2 Type II report.

C：针对提供商的内部系统运行漏洞扫描

Run a vulnerability scan against the provider’s internal systems.

D：要求提供SOC 1类型II报告

Request a SOC 1 Type II report.

答案:在评估SaaS提供商的安全性时，Ian最有可能使用的方法是要求提供SOC 2 Type II报告。SOC 2（Service Organization Control 2）报告是一种由独立第三方审计机构出具的报告，专门用于评估服务提供商在安全性、可用性、处理完整性、保密性和隐私性等方面的控制措施。SOC 2 Type II报告不仅描述了这些控制措施的设计，还评估了这些措施在一段时间内的有效性。

其他选项的分析如下：

- \*\*A：针对提供商的外部服务运行漏洞扫描\*\*：虽然漏洞扫描可以识别外部服务的潜在安全漏洞，但云服务提供商通常不会允许客户对其外部服务进行漏洞扫描，因为这可能会影响服务的稳定性和安全性。

- \*\*C：针对提供商的内部系统运行漏洞扫描\*\*：云服务提供商通常不会允许客户访问其内部系统，更不用说进行漏洞扫描了。这种做法不仅不现实，还可能违反服务协议。

- \*\*D：要求提供SOC 1 Type II报告\*\*：SOC 1报告主要关注与财务报告相关的控制措施，而不是安全性。因此，SOC 1报告对于评估SaaS提供商的安全性帮助不大。

因此，\*\*B：要求提供SOC 2 Type II报告\*\* 是最合适的选项。

-------------------

题目111：当Ben在Linux系统上列出文件时，他会如图中看到一组属性。字母rwx表示什么不同级别？

When Ben lists the files on a Linux system, he sees a set of attributes as shown here. The letters rwx indicate different levels of what?

<div style="text-align:center"><img alt="" height="138" src="/file/100000/m/20210907/476f7140a21b421a8363ce1b53a0b5fa.png" width="448" /></div>

A：身份

Identification

B：授权

Authorization

C：认证

Authentication

D：问责

Accountability

答案:在Linux系统中，文件或目录的权限通常由一组字母表示，这些字母包括 `r`、`w` 和 `x`。这些字母分别代表不同的权限级别：

- `r` 表示“读”（Read）权限，允许用户读取文件内容或列出目录中的文件。

- `w` 表示“写”（Write）权限，允许用户修改文件内容或在目录中创建、删除文件。

- `x` 表示“执行”（Execute）权限，允许用户执行文件或进入目录。

这些权限通常与文件的用户（User）、组（Group）和其他用户（Others）相关联，分别定义了不同用户对文件或目录的访问权限。

因此，字母 `rwx` 表示的是不同级别的 \*\*授权\*\*（Authorization），即哪些用户或组有权对文件或目录进行读、写或执行操作。

正确答案是：

\*\*B：授权\*\*

\*\*Authorization\*\*

-------------------

题目112：请为数字标记的协议，匹配与之对应的描述信息；每个选项仅匹配一次。

协议：

1. TCP

2. UDP

3. DNS

4. ARP

描述：

A. 执行MAC地址和IP地址之间的转换

B. 执行FQDN与IP地址之间的转换

C. 在网络中以连接的形式传输数据

D. 在网络中以无连接的形式传输数据

Match each one of the numbered protocols with the most accurate lettered description. Use each answer exactly once.

Protocol

1.TCP

2. UDP

3. DNS

4. ARP

Description

A.Performs translations between MAC addresses and IP addresses

B.Performs translations between FQDNs and IP addresses

C.Transports data over a network in a connection-oriented fashion

D.Transports data over a network in a connectionless fashion

A：看答案

B：不看答案

答案:根据题目要求，将每个协议与最准确的描述匹配如下：

1. \*\*TCP\*\* - \*\*C. 在网络中以连接的形式传输数据\*\*

TCP（传输控制协议）是一种面向连接的协议，确保数据在网络中可靠地传输。

2. \*\*UDP\*\* - \*\*D. 在网络中以无连接的形式传输数据\*\*

UDP（用户数据报协议）是一种无连接的协议，传输数据时不建立连接，速度较快但不保证可靠性。

3. \*\*DNS\*\* - \*\*B. 执行FQDN与IP地址之间的转换\*\*

DNS（域名系统）负责将完全限定域名（FQDN）转换为对应的IP地址。

4. \*\*ARP\*\* - \*\*A. 执行MAC地址和IP地址之间的转换\*\*

ARP（地址解析协议）用于将IP地址转换为对应的MAC地址。

因此，匹配结果为：

1. TCP - C

2. UDP - D

3. DNS - B

4. ARP - A

-------------------