题目1：Lisa正在试图防止她的网络成为IP欺骗攻击的目标，并防止她的网络成为这些攻击的源头。 以下哪些规则是Lisa应在其网络边界配置的最佳实践？（选择所有适用的选项）

Lisa is attempting to prevent her network from being targeted by IP spoofing attacks as well as preventing her network from being the source of those attacks. Which of the following rules are best practices that Lisa should configure at her network border? (Select all that apply.)

A：阻止具有内部源地址的数据包进入网络

Block packets with internal source addresses from entering the network.

B：阻止具有外部源地址的数据包离开网络

Block packets with external source addresses from leaving the network.

C：阻止具有公共IP地址的数据包进入网络

Block packets with public IP addresses from entering the network.

D：阻止带有私有IP地址的数据包离开网络

Block packets with private IP addresses from exiting the network.

答案:为了防止IP欺骗攻击，Lisa应该在她的网络边界配置以下规则：

A：阻止具有内部源地址的数据包进入网络

Block packets with internal source addresses from entering the network.

- 这个规则可以防止外部攻击者伪装成内部IP地址进行攻击。

D：阻止带有私有IP地址的数据包离开网络

Block packets with private IP addresses from exiting the network.

- 这个规则可以防止内部网络中的设备伪装成外部IP地址进行攻击，从而防止网络成为攻击的源头。

选项B和C不是最佳实践：

- B：阻止具有外部源地址的数据包离开网络

Block packets with external source addresses from leaving the network.

- 这个规则会阻止合法的外部通信，因此不是最佳实践。

- C：阻止具有公共IP地址的数据包进入网络

Block packets with public IP addresses from entering the network.

- 这个规则会阻止合法的外部通信，因此不是最佳实践。

因此，正确答案是A和D。

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

题目2：Ed负责确定一项服务，该项服务可为其雇主提供低延迟、高性能和高可用性的内容托管。他应该采用什么类型的解决方案，以确保雇主的全球客户能够快捷、可靠地访问内容？

Ed has been tasked with identifying a service that will provide a low-latency, highperformance, and high-availability way to host content for his employer. What type of solution should he seek out to ensure that his employer’s customers around the world can access their content quickly, easily, and reliably?

A：热站点

A hot site

B：CDN(内容分发网络)

A CDN

C：冗余服务器

Redundant servers

D：P2P CDN(对等的内容分发网络)

A P2P CDN

答案:题目2的正确答案是：

\*\*B：CDN(内容分发网络)\*\*

\*\*解释：\*\*

CDN（内容分发网络）是一种分布式服务器系统，旨在通过将内容缓存到全球多个地理位置的服务器上，来提供低延迟、高性能和高可用性的内容托管服务。CDN能够确保全球用户能够快速、可靠地访问内容，因为它将内容分发到离用户最近的服务器节点，从而减少延迟并提高访问速度。

其他选项的解释：

- \*\*A：热站点\*\*：热站点通常用于灾难恢复，而不是内容分发。

- \*\*C：冗余服务器\*\*：冗余服务器可以提高可用性，但不能解决全球用户访问的低延迟问题。

- \*\*D：P2P CDN\*\*：P2P CDN虽然也是一种内容分发方式，但通常用于特定的应用场景，不如传统CDN那样广泛适用。

因此，CDN是最适合Ed的需求的解决方案。

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

题目3：Fran正在构建一个取证分析工作站，并正在选择一个取证磁盘控制器将其包含在设置中。 以下哪些是取证磁盘控制器的功能？ （选择所有适用的选项。）

Fran is building a forensic analysis workstation and is selecting a forensic disk controller to include in the setup. Which of the following are functions of a forensic disk controller? (Select all that apply.)

A：防止修改存储设备上的数据

Preventing the modification of data on a storage device

B：将数据返回给请求设备

Returning data requested from the device

C：将设备报告的错误发送给取证主机

Reporting errors sent by the device to the forensic host

D：阻止发送到设备的读取命令

Blocking read commands sent to the device

答案:取证磁盘控制器是专门设计用于取证分析的硬件设备，其主要功能是确保在取证过程中数据的完整性和防止数据被篡改。根据题目描述，以下是取证磁盘控制器的功能：

A：防止修改存储设备上的数据

- 这是取证磁盘控制器的主要功能之一。它通过写保护机制确保在取证过程中数据不会被意外或恶意修改。

B：将数据返回给请求设备

- 这不是取证磁盘控制器的特定功能。任何磁盘控制器都可以将数据返回给请求设备。

C：将设备报告的错误发送给取证主机

- 这是取证磁盘控制器的功能之一。它可以帮助取证人员识别存储设备上的潜在问题或错误。

D：阻止发送到设备的读取命令

- 这不是取证磁盘控制器的功能。取证磁盘控制器通常不会阻止读取命令，因为取证分析需要读取数据。

因此，正确的选项是 \*\*A\*\* 和 \*\*C\*\*。

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

题目4：Mike正在构建容错服务器并想要实施RAID 1，实施此方案需要多少个物理磁盘？

Mike is building a fault-tolerant server and wants to implement RAID 1. How many physical disks are required to build this solution?

A：1

1

B：2

2

C：3

3

D：5

5

答案:RAID 1（镜像）是一种通过将数据复制到多个磁盘上来提供冗余的存储方案。在RAID 1中，数据会被完全复制到至少两个磁盘上。因此，实施RAID 1至少需要 \*\*2个物理磁盘\*\*。

正确答案是：\*\*B：2\*\*

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

题目5：Darren正在对其组织使用的Kerberized应用程序的身份验证问题进行故障排除。他认为问题在于会话密钥的生成。他应该首先调查什么Kerberos服务？

Darren is troubleshooting an authentication issue for a Kerberized application used by his organization. He believes the issue is with the generation of session keys. What Kerberos service should he investigate first?

A：KDC(密钥分发中心)

KDC

B：TGT(票据授予票据)

TGT

C：AS(身份验证服务)

AS

D：TGS(票据授予服务)

TGS

答案:在Kerberos身份验证协议中，会话密钥的生成与多个组件相关，但最关键的服务是\*\*KDC（密钥分发中心）\*\*。KDC负责生成和管理会话密钥，并分发TGT（票据授予票据）和服务票据。因此，如果Darren怀疑会话密钥生成有问题，他应该首先调查\*\*KDC\*\*。

\*\*正确答案：A. KDC（密钥分发中心）\*\*

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

题目6：Evelyn认为她所在组织的一个供应商违反了保护敏感数据的合同义务，并希望对这种情况进行调查。根据调查结果，Evelyn的组织很可能会起诉供应商违约。什么术语最能描述Evelyn正在进行的调查类型？

Evelyn believes that one of her organization's vendors has breached a contractual obligation to protect sensitive data and would like to conduct an investigation into the circumstances. Based upon the results of the investigation, it is likely that Evelyn's organization will sue the vendor for breach of contract. What term best describes the type of investigation that Evelyn is conducting?

A：行政调查

Administrative investigation

B：刑事调查

Criminal investigation

C：民事调查

Civil investigation

D：监管调查

Regulatory investigation

答案:Evelyn正在进行的调查是为了确定供应商是否违反了合同义务，特别是关于保护敏感数据的条款。这种调查的目的是为了收集证据，以便在必要时提起民事诉讼，要求赔偿或其他法律救济。因此，这种调查属于民事调查。

A选项“行政调查”通常是由政府机构进行的，目的是为了执行法律法规或政策，而不是为了民事诉讼。

B选项“刑事调查”涉及犯罪行为，通常由执法机构进行，目的是为了起诉犯罪行为。

D选项“监管调查”通常是由监管机构进行的，目的是为了确保遵守特定的行业规定或标准。

因此，最合适的答案是：

C：民事调查

Civil investigation

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

题目7：Ivan正在安装一个运动探测器，来保护敏感的工作区域，该区域使用高频微波信号传输来识别潜在的入侵者。他安装的是什么类型的探测器？

Ivan is installing a motion detector to protect a sensitive work area that uses high-frequency microwave signal transmissions to identify potential intruders. What type of detector is he installing?

A：红外

Infrared

B：热基

Heat-based

C：波形

Wave pattern

D：电容

Capacitance

答案:Ivan安装的运动探测器使用的是高频微波信号传输来识别潜在的入侵者。这种类型的探测器通常被称为微波探测器或雷达探测器。它们通过发射微波信号并检测反射回来的信号来检测移动的物体。

选项分析：

A：红外（Infrared） - 红外探测器通过检测红外辐射来识别移动的物体，通常用于检测人体的热辐射。

B：热基（Heat-based） - 热基探测器通过检测温度变化来识别移动的物体，通常用于检测人体的热辐射。

C：波形（Wave pattern） - 这个选项描述的是通过分析波形来检测移动的物体，通常指的是微波或超声波探测器。

D：电容（Capacitance） - 电容探测器通过检测电容变化来识别移动的物体，通常用于触摸屏或接近传感器。

根据题目描述，Ivan使用的是高频微波信号传输，因此最符合的选项是C：波形（Wave pattern）。

正确答案是：C：波形（Wave pattern）。

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

题目8：Susan 建立了一个防火墙，用于跟踪两个系统之间的通信状态，并允许远程系统在本地系统开始通信后响应本地系统。Susan 使用的是什么类型的防火墙？

Susan sets up a firewall that keeps track of the status of the communication between two systems and allows a remote system to respond to a local system only after the local system starts communication. What type of firewall is Susan using?

A：静态包过滤防火墙

A static packet filtering firewall

B：应用级网关防火墙

An application-level gateway firewall

C：状态包检测防火墙

A stateful packet inspection firewall

D：电路级网关防火墙

A circuit-level gateway firewall

答案:Susan 使用的防火墙类型是 \*\*状态包检测防火墙\*\*（Stateful Packet Inspection Firewall）。

\*\*解释：\*\*

- \*\*状态包检测防火墙\*\* 不仅检查单个数据包的内容，还会跟踪通信会话的状态。它能够记住先前通过防火墙的数据包，并根据这些信息来决定是否允许后续的数据包通过。这种防火墙可以确保远程系统只有在本地系统发起通信后才能响应，从而提供更高的安全性。

其他选项的解释：

- \*\*静态包过滤防火墙\*\*（A）：仅根据预定义的规则（如源地址、目标地址、端口等）来过滤数据包，不跟踪通信状态。

- \*\*应用级网关防火墙\*\*（B）：工作在应用层，能够深入检查应用层协议的数据，但不一定跟踪通信状态。

- \*\*电路级网关防火墙\*\*（D）：工作在会话层，主要验证会话的合法性，但不深入检查数据包内容。

因此，正确答案是 \*\*C：状态包检测防火墙\*\*。

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

题目9-1：根据以下情景，回答3个问题：

Ben 拥有一家咖啡馆，他希望为客户提供无线上网服务。Ben 的网络很简单，按照商业电缆数据合同，将无线路由器和有线调制解调器连接起来。使用Ben 的网络信息，回答以下问题。

For questions , please refer to the following scenario:

Ben owns a coffeehouse and wants to provide wireless internet service for his customers. Ben's network is simple and uses a single consumer-grade wireless router and a cable modem connected via a commercial cable data contract.

Ben 如何为客户提供访问控制，而不必在连接之前配置用户ID，同时还可以收集到有用的客户联系信息？

How can Ben provide access control for his customers without having to provision user IDs before they connect while also gathering useful contact information for his business purposes?

A：WPA2 PSK

WPA2 PSK

B：强制门户

A captive portal

C：要求客户使用公开发布的密码，如BensCoffee

Require customers to use a publicly posted password like"BensCoffee"

D：WPA3 SAE

WPA3 SAE

答案:正确答案是 \*\*B：强制门户 (A captive portal)\*\*。

### 解释：

- \*\*强制门户 (Captive Portal)\*\* 是一种常见的访问控制机制，通常用于公共场所（如咖啡馆、酒店、机场等）的无线网络。当用户连接到网络时，会被重定向到一个网页（即强制门户），要求他们输入某些信息（如电子邮件地址、姓名等）或接受使用条款后才能访问互联网。这种方式不需要预先配置用户ID，同时可以收集到有用的客户联系信息。

- \*\*WPA2 PSK\*\* 和 \*\*WPA3 SAE\*\* 是无线网络加密协议，主要用于保护网络的安全性，但它们不提供访问控制或客户信息收集的功能。

- \*\*要求客户使用公开发布的密码\*\* 虽然简单，但无法收集客户信息，且安全性较低，容易被滥用。

因此，\*\*强制门户\*\* 是最适合Ben的需求的解决方案。

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

题目9-2：根据以下情景，回答3个问题：

Ben 拥有一家咖啡馆，他希望为客户提供无线上网服务。Ben 的网络很简单，按照商业电缆数据合同，将无线路由器和有线调制解调器连接起来。使用Ben 的网络信息，回答以下问题。

For questions , please refer to the following scenario:

Ben owns a coffeehouse and wants to provide wireless internet service for his customers. Ben's network is simple and uses a single consumer-grade wireless router and a cable modem connected via a commercial cable data contract.

Ben打算运行一个开放(未加密)的无线网络，请问他应该如何将商业设备连接到此无线网络中去？

Ben intends to run an open (unencrypted) wireless network. How should he connect his business devices?

A：在同一SSID上运行WPA3

Run WPA3 on the same SSID.

B：使用WPA3设置单独的SSID

Set up a separate SSID using WPA3.

C：在企业模式下运行开放网络

Run the open network in Enterprise mode.

D：使用WEP设置单独的无线网络

Set up a separate wireless network using WEP.

答案:Ben 打算运行一个开放（未加密）的无线网络，这意味着任何人都可以连接到这个网络，而不需要输入密码。然而，开放网络存在安全风险，因此 Ben 应该确保他的商业设备不会暴露在这个开放网络中。

为了确保商业设备的安全，Ben 应该为商业设备设置一个单独的、加密的无线网络。这样，商业设备和客户设备可以分别连接到不同的网络，从而避免潜在的安全问题。

因此，正确的做法是：

\*\*B：使用WPA3设置单独的SSID\*\*

通过这种方式，Ben 可以为客户提供一个开放的无线网络，同时为商业设备设置一个加密的、安全的网络（使用 WPA3 加密），以确保商业数据的安全。

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

题目9-3：根据以下情景，回答3个问题：

Ben 拥有一家咖啡馆，他希望为客户提供无线上网服务。Ben 的网络很简单，按照商业电缆数据合同，将无线路由器和有线调制解调器连接起来。使用Ben 的网络信息，回答以下问题。

For questions , please refer to the following scenario:

Ben owns a coffeehouse and wants to provide wireless internet service for his customers. Ben's network is simple and uses a single consumer-grade wireless router and a cable modem connected via a commercial cable data contract.

为客户提供了访问控制后，Ben收到一个投诉，有人在他的咖啡馆窃听其他客户的网络流量，包括用户名和密码。这是如何做到的？

After implementing the solution from the first question, Ben receives a complaint about users in his cafe hijacking other customers'web traffic, including using their usernames and passwords. How is this possible?

A：密码由所有用户共享，使得网络流量易受攻击

The password is shared by all users, making traffic vulnerable.

B：恶意用户在路由器上安装了木马

A malicious user has installed a Trojan on the router.

C：用户使用ARP欺骗了路由器，使所有流量广播到所有用户

A user has ARP spoofed the router, making all traffic broadcast to all users.

D：开放网络未加密，使得网络流量很容易被嗅探

Open networks are unencrypted, making traffic easily sniffable.

答案:根据题目描述，Ben 的咖啡馆提供了无线上网服务，但有人窃听了其他客户的网络流量，包括用户名和密码。这种情况通常发生在网络流量未加密的情况下，使得攻击者可以通过网络嗅探工具轻松捕获数据包。

选项分析：

- \*\*A\*\*：密码由所有用户共享，使得网络流量易受攻击。这个选项描述的是密码共享的问题，但题目中提到的是网络流量被窃听，而不是密码被共享。

- \*\*B\*\*：恶意用户在路由器上安装了木马。虽然木马可以导致安全问题，但题目中描述的是网络流量被窃听，而不是路由器被感染。

- \*\*C\*\*：用户使用ARP欺骗了路由器，使所有流量广播到所有用户。ARP欺骗是一种常见的攻击手段，可以使攻击者捕获网络流量，但题目中描述的是网络流量被窃听，而不是ARP欺骗。

- \*\*D\*\*：开放网络未加密，使得网络流量很容易被嗅探。这个选项最符合题目描述的情况，开放网络未加密意味着网络流量可以被任何人捕获和分析，包括用户名和密码。

因此，最合适的答案是 \*\*D\*\*。

\*\*答案：D\*\*

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

题目10：Kevin正在审查和更新其组织使用的安全文档。他想记录他的团队在过去一年中开发的一些用于保护物联网设备的最佳实践。这些实践的本质是概括性的，不涵盖特定设备。哪种类型的文件最适合此目的？

Kevin is reviewing and updating the security documentation used by his organization. He would like to document some best practices for securing IoT devices that his team has developed over the past year. The practices are generalized in nature and do not cover specific devices. What type of document would be best for this purpose?

A：方针

Policy

B：标准

Standard

C：指南

Guideline

D：程序

Procedure

答案:在Kevin的情况下，他想要记录的是关于保护物联网设备的最佳实践，这些实践是概括性的，不针对特定设备。这种情况下，最适合的文件类型是：

C：指南 (Guideline)

\*\*指南\*\*通常提供建议和最佳实践，帮助组织或团队在特定领域（如物联网设备安全）中做出决策和实施措施。它们不像\*\*标准\*\*那样具有强制性，也不像\*\*程序\*\*那样详细描述具体的操作步骤。\*\*方针\*\*通常是高层次的，描述组织的总体方向和原则，而\*\*标准\*\*则更具体，规定了必须遵守的要求。因此，\*\*指南\*\*是最适合记录概括性最佳实践的文件类型。

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

题目11：Tom正在调整安全监控工具，以减少管理员收到的警报数量，同时要求不能因此丢失重要的安全事件。他决定将系统配置为只报告以下这种情况：在一小时内访问同一账户有五次登录失败。什么术语最好地描述了Tom使用的技术？

Tom is tuning his security monitoring tools in an attempt to reduce the number of alerts received by administrators without missing important security events. He decides to configure the system to only report failed login attempts if there are five failed attempts to access the same account within a one-hour period of time. What term best describes the technique that Tom is using?

A：域值

ThresholdingA

B：抽样

Sampling

C：账户锁定

Account lockout

D：阈值

Clipping

答案:Tom正在调整安全监控工具，以减少管理员收到的警报数量，同时确保不丢失重要的安全事件。他决定将系统配置为只报告在一小时内访问同一账户有五次登录失败的情况。这种技术是通过设置一个特定的条件或标准来触发警报，以减少不必要的警报数量，同时确保重要的安全事件不会被忽略。

在给定的选项中，最符合这种技术的术语是：

A：域值

Thresholding

Thresholding（阈值设定）是一种通过设置一个特定的阈值来触发警报或采取其他行动的技术。在这个例子中，Tom设置了一个阈值，即在一小时内五次登录失败，只有当达到或超过这个阈值时，系统才会报告这个事件。这样可以有效减少不必要的警报，同时确保重要的安全事件不会被忽略。

因此，正确答案是：

A：域值

Thresholding

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

题目12：Sally负责为其组织中的无线网络服务部署身份验证、授权和记账服务器，而且要避免使用专有技术。她应该选择什么技术？

Sally has been tasked with deploying an authentication, authorization, and accounting server for wireless network services in her organization and needs to avoid using proprietary technology. What technology should she select?

A：OAuth

OAuth

B：RADIUS

RADIUS

C：XTACACS

XTACACS

D：TACACS +

TACACS +

答案:Sally 应该选择 \*\*B：RADIUS\*\*。

\*\*RADIUS\*\*（Remote Authentication Dial-In User Service）是一种开放标准的协议，广泛用于网络访问的身份验证、授权和记账（AAA）。它支持多种认证方法，并且可以与各种设备和系统集成。RADIUS 是一个非专有技术，符合 Sally 的需求。

其他选项的解释：

- \*\*A：OAuth\*\*：OAuth 主要用于授权，而不是完整的 AAA 服务。

- \*\*C：XTACACS\*\* 和 \*\*D：TACACS+\*\*：这两种技术都是专有的，不符合 Sally 避免使用专有技术的要求。

因此，RADIUS 是最合适的选择。

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

题目13：Christopher拥有一家奶酪蛋糕店，他的会计员无法查看员工个人的薪水信息，但会计员想知道新员工的薪水。会计员在新人被雇用之前提取了工资支付期间的总工资支出，然后在下一个工资支付期内也提取了总工资支出。他通过计算这两个金额之间的差额来确定新员工的薪水。发生了什么类型的攻击？

An accounting clerk for Christopher's Cheesecakes does not have access to the salary information for individual employees but wanted to know the salary of a new hire. He pulled total payroll expenses for the pay period before the new person was hired and then pulled the same expenses for the following pay period. He computed the difference between those two amounts to determine the individual's salary. What type of attack occurred?

A：Salami切片

Salami slicing

B：数据填充

C：推理

Inference

D：社会工程

Social engineering

答案:题目描述的情况中，会计员通过合法的手段获取了两个工资支付期间的总工资支出，并通过计算这两个金额之间的差额来推断出新员工的薪水。这种方法并没有直接访问或篡改任何敏感数据，而是通过合法获取的数据进行推理，从而得出了原本无法直接访问的信息。

因此，这种情况属于\*\*推理攻击（Inference）\*\*。

\*\*正确答案：C：推理（Inference）\*\*

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

题目14：Alice想获得一个对象的读取权限，并且她知道Bob已经拥有这些权限，她希望Bob能将这些权限提供给自己。如果Alice和Bob之间存在关系，Take-Grant保护模型中的哪个规则将允许她完成此操作？

Alice would like to have read permissions on an object and knows that Bob already has those rights and would like to give them to herself. Which one of the rules in the Take-Grant protection model would allow her to complete this operation if the relationship exists between Alice and Bob?

A：获取规则

Take rule

B：授予规则

Grant rule

C：创建规则

Create rule

D：远程规则

Remote rule

答案:在Take-Grant保护模型中，Alice想要从Bob那里获取对某个对象的读取权限，可以使用“获取规则”（Take rule）。这个规则允许一个主体（Alice）从另一个主体（Bob）那里获取权限，前提是Alice和Bob之间存在适当的关系（例如，Bob是Alice的“朋友”或“上级”）。

因此，正确答案是：

A：获取规则 (Take rule)

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

题目15：在日志审查期间，Danielle 发现了一系列显示登录失败的日志：

Jan 31 11:39:12 ip-10-0-0-2 sshd[29092]: Invalid user admin from remotehost passwd=aaaaaaaa

Jan 31 11:39:20 ip-10-0-0-2 sshd[29098]: Invalid user admin from remotehost passwd=aaaaaaab

Jan 31 11:39:23 ip-10-0-0-2 sshd[29100]: Invalid user admin from remotehost passwd=aaaaaaac

Jan 31 11:39:31 ip-10-0-0-2 sshd[29106]: Invalid user admin from remotehost passwd=aaaaaaad

Jan 31 20:40:53 ip-10-0-0-254 sshd[30520]: Invalid user admin from remotehost passwd=aaaaaaad

Danielle发现了什么类型的攻击？

During a log review, Danielle discovers a series of logs that show login failures:

Jan 31 11:39:12 ip-10-0-0-2 sshd[29092]: Invalid user admin from remotehost passwd=aaaaaaaa

Jan 31 11:39:20 ip-10-0-0-2 sshd[29098]: Invalid user admin from remotehost passwd=aaaaaaab

Jan 31 11:39:23 ip-10-0-0-2 sshd[29100]: Invalid user admin from remotehost passwd=aaaaaaac

Jan 31 11:39:31 ip-10-0-0-2 sshd[29106]: Invalid user admin from remotehost passwd=aaaaaaad

Jan 31 20:40:53 ip-10-0-0-254 sshd[30520]:Invalid user admin from remotehost passwd=aaaaaaae

What type of attack has Danielle discovered?

A：传递散列攻击

A pass-the-hash attack

B：暴力攻击

A brute-force attack

C：中间人攻击

A man-in-the-middle attack

D：字典攻击

A dictionary attack

答案:Danielle 发现的日志显示了一系列的登录失败尝试，每次尝试都使用了不同的密码（如 "aaaaaaaa"、"aaaaaaab"、"aaaaaaac" 等）。这种模式表明攻击者正在尝试通过系统地尝试不同的密码来猜测正确的密码。

这种攻击方式被称为 \*\*暴力攻击（Brute-force attack）\*\*，即攻击者通过尝试所有可能的密码组合来破解账户。

因此，正确答案是：

\*\*B：暴力攻击\*\*

A brute-force attack

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

题目16：Ben正在设计一个数据库驱动的应用程序，并希望通过将中间结果存储在数据库中，来确保两个正在执行的事务不会相互影响。他要强制执行什么特性？

Ben is designing a database-driven application and would like to ensure that two executing transactions do not affect each other by storing interim results in the database. What property is he seeking to enforce?

A：原子性

Atomicity

B：隔离性

Isolation

C：一致性

Consistency

D：持久性

Durability

答案:Ben希望通过将中间结果存储在数据库中，来确保两个正在执行的事务不会相互影响。这涉及到数据库事务的隔离性（Isolation）。

\*\*隔离性（Isolation）\*\* 是数据库事务的四个基本特性（ACID）之一，它确保并发执行的事务不会相互干扰。具体来说，隔离性要求一个事务的执行不能被其他事务看到，直到该事务提交。这样可以防止事务之间的数据不一致性。

因此，正确答案是：

\*\*B：隔离性 (Isolation)\*\*

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

题目17：Kim是一家遇到安全问题的小型企业网络的系统管理员。晚上她在办公室解决这个问题，没有其他人在那里。在她观看的过程中，她可以看到办公室另一侧以前运行正常的系统，现在一个接一个地显示出感染迹象。Kim可能会处理什么类型的恶意软件？

Kim is the system administrator for a small business network that is experiencing security problems. She is in the office in the evening working on the problem, and nobody else is there. As she is watching, she can see that systems on the other side of the office that were previously behaving normally are now exhibiting signs of infection one after the other. What type of malware is Kim likely dealing with?

A：病毒

Virus

B：蠕虫

Worm

C：木马

Trojan horse

D：逻辑炸弹

Logic bomb

答案:Kim 所描述的情况中，系统一个接一个地显示出感染迹象，这表明恶意软件正在通过网络传播并感染其他系统。这种行为最符合蠕虫（Worm）的特征。蠕虫是一种能够自我复制并通过网络传播的恶意软件，它不需要依附于其他程序或文件，而是独立运行并利用网络漏洞或弱密码等方式传播。

因此，Kim 可能正在处理的恶意软件类型是：

\*\*B：蠕虫 (Worm)\*\*

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

题目18：Barb正在审查她的组织面临的合规义务以及每个人可能承担的责任类型。违反下列哪项法律法规可能涉及刑事处罚？（选择所有适用的选项）

Barb is reviewing the compliance obligations facing her organization and the types of liability that each one might incur. Which of the following laws and regulations may involve criminal penalties if violated? (Select all that apply.)

A：FERPA

FERPA

B：HIPAA

HIPAA

C：SOX

SOX

D：PCI DSS

PCI DSS

答案:在审查合规义务时，了解哪些法律法规的违反可能导致刑事处罚是非常重要的。以下是每个选项的简要分析：

A. \*\*FERPA\*\*（家庭教育权利和隐私法案）：FERPA主要涉及学生教育记录的隐私保护。违反FERPA通常不会导致刑事处罚，而是可能导致联邦资金的损失或其他行政制裁。

B. \*\*HIPAA\*\*（健康保险可携性和责任法案）：HIPAA涉及个人健康信息的隐私和安全。违反HIPAA可能导致刑事处罚，特别是在故意或恶意泄露患者信息的情况下。

C. \*\*SOX\*\*（萨班斯-奥克斯利法案）：SOX涉及公司财务报告的准确性和透明度。违反SOX可能导致刑事处罚，特别是在故意篡改财务记录或进行欺诈的情况下。

D. \*\*PCI DSS\*\*（支付卡行业数据安全标准）：PCI DSS涉及支付卡数据的安全。违反PCI DSS通常不会直接导致刑事处罚，但可能导致罚款或其他商业制裁。然而，如果违反PCI DSS的行为涉及欺诈或其他犯罪行为，可能会引发刑事处罚。

因此，可能涉及刑事处罚的选项是：

\*\*B. HIPAA\*\* 和 \*\*C. SOX\*\*。

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

题目19：Quentin正在分析他使用Wireshark在TCP/IP网络上收集的网络流量。他想确定在他的流量收集期间建立的所有新连接。如果他正在寻找构成用于建立新连接的TCP三次握手的三个数据包，那么前三个数据包应该设置什么标志？

Quentin is analyzing network traffic that he collected with Wireshark on a TCP/IP network. He would like to identify all new connections that were set up during his traffic collection. If he is looking for the three packets that constitute the TCP three-way handshake used to establish a new connection, what flags should be set on the first three packets?

A：SYN, ACK, SYN/ACK

SYN, ACK, SYN/ACK

B：PSH, RST, ACK

PSH, RST, ACK

C：SYN, SYN/ACK, ACK

SYN, SYN/ACK, ACK

D：SYN, RST, FIN

SYN, RST, FIN

答案:在TCP/IP网络中，建立新连接的过程称为TCP三次握手。这个过程涉及三个数据包，每个数据包都有特定的标志位设置。以下是三次握手的步骤及其对应的标志位：

1. \*\*第一次握手\*\*：客户端向服务器发送一个SYN（同步）包，请求建立连接。这个包的标志位设置为SYN。

2. \*\*第二次握手\*\*：服务器响应客户端的SYN包，发送一个SYN-ACK（同步-确认）包，表示同意建立连接。这个包的标志位设置为SYN和ACK。

3. \*\*第三次握手\*\*：客户端向服务器发送一个ACK（确认）包，确认连接已建立。这个包的标志位设置为ACK。

因此，构成TCP三次握手的三个数据包的标志位设置分别是：

- 第一个数据包：SYN

- 第二个数据包：SYN/ACK

- 第三个数据包：ACK

所以，正确答案是：

\*\*C：SYN, SYN/ACK, ACK\*\*

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

题目20：Daniel正在为其组织选择一个新的移动设备管理（MDM）解决方案，并正在编写RFP。在将组织的安全需求与MDM平台的功能保持一致后，他正试图决定应包含某个功能作为需求。以下哪些是MDM解决方案的典型功能？（选择所有符合条件的）

Daniel is selecting a new mobile device management (MDM) solution for his organization and is writing the RFP. He is trying to decide what features he should include as requirements after aligning his organization's security needs with an MDM platform's capabilities. Which of the following are typical capabilities of MDM solutions? (Select all that apply.)

A：远程擦除移动设备的内容

Remotely wiping the contents of a mobile device

B：控制未注册的BYOD移动设备

Assuming control of a nonregistered BYOD mobile device

C：强制使用设备加密

Enforcing the use of device encryption

D：管理设备备份

Managing device backups

答案:在编写移动设备管理（MDM）解决方案的RFP时，Daniel需要考虑哪些功能是MDM解决方案的典型功能。以下是每个选项的分析：

A：远程擦除移动设备的内容

- 这是MDM解决方案的典型功能之一。远程擦除功能允许管理员在设备丢失或被盗时，远程删除设备上的所有数据，以保护敏感信息。

B：控制未注册的BYOD移动设备

- 这个选项不太准确。MDM解决方案通常不会控制未注册的BYOD（自带设备）移动设备。MDM解决方案通常要求设备注册后才能进行管理。

C：强制使用设备加密

- 这是MDM解决方案的典型功能之一。强制使用设备加密可以确保设备上的数据在存储和传输过程中得到保护，符合组织的安全需求。

D：管理设备备份

- 这个选项不太准确。MDM解决方案通常不直接管理设备备份。设备备份通常由其他解决方案或服务（如云存储服务）来处理。

因此，正确的选项是：

A：远程擦除移动设备的内容

C：强制使用设备加密

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

题目21：Jim正在为他的组织实施IDaaS解决方案。他使用了什么类型的技术？

Jim is implementing an IDaaS solution for his organization. What type of technology is he putting in place?

A：身份即服务

Identity as a service

B：员工ID 作为服务

Employee ID as a service

C：基于云的RADIUS

Intrusion detection as a service

D：OAuth

OAuth

答案:正确答案是 A：身份即服务 (Identity as a service)。

IDaaS 是 "Identity as a Service" 的缩写，中文称为“身份即服务”。它是一种基于云的身份和访问管理解决方案，允许组织通过云服务来管理用户的身份验证和授权。IDaaS 通常包括单点登录（SSO）、多因素认证（MFA）、用户生命周期管理等功能，帮助企业更高效地管理用户身份和访问权限。

其他选项的解释：

- B：员工ID 作为服务 (Employee ID as a service) 并不是一个常见的术语或技术。

- C：基于云的RADIUS (Intrusion detection as a service) 与身份管理无关，RADIUS 是一种用于网络访问控制的协议，而入侵检测是另一种安全技术。

- D：OAuth 是一种授权框架，用于允许第三方应用程序访问用户资源，但它本身并不是一种身份即服务解决方案。

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

题目22：Gina最近参加了CISSP认证考试，然后写了一篇博客文章，其中包含有关考题的一些内容。这种情况下，她直接违反(ISC)2道德规范的哪个方面？

Gina recently took the CISSP certification exam and then wrote a blog post that included the text of many of the exam questions that she experienced. What aspect of the (ISC)2 Code of Ethics is most directly violated in this situation?

A：推进和保护专业

Advance and protect the profession.

B：正直、诚实、公正、负责任和合法地行事

Act honorably, honestly, justly, responsibly, and legally.

C：保护社会公共利益和维持必要的公众信任

Protect society, the common good, necessary public trust and confidence, and the infrastructure.

D：为负责人提供高效优质的服务

Provide diligent and competent service to principals.

答案:在Gina的情况下，她直接违反了(ISC)2道德规范的B选项：正直、诚实、公正、负责任和合法地行事（Act honorably, honestly, justly, responsibly, and legally）。

CISSP考试是由(ISC)2组织管理的，该组织对考试内容有严格的保密要求。Gina在博客中公开了考试题目，这违反了考试的保密协议，损害了考试的公正性和有效性。这种行为不仅不诚实，也不负责任，因为它可能影响其他考生的公平竞争环境，同时也可能损害(ISC)2的声誉和考试的严肃性。

因此，Gina的行为直接违反了(ISC)2道德规范中关于正直、诚实、公正、负责任和合法行事的要求。

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

题目23：Gordon正在为其组织进行风险评估，并确定每年洪水预计对其设施造成的损害程度。Gordon 确定的是什么指标？

Gordon is conducting a risk assessment for his organization and determined the amount of damage that flooding is expected to cause to his facilities each year. What metric has Gordon identified?

A：ALE 年度 损失 期望

ALE

B：ARO 年度 发生率

ARO

C：SLE 单一 损失 期望

SLE

D：EF 暴露 因子

EF

答案:Gordon 确定的是 \*\*A：ALE 年度损失期望\*\*。

\*\*ALE (Annualized Loss Expectancy)\*\* 是指每年由于特定风险事件（如洪水）预计造成的损失金额。它是通过将单一损失期望（SLE）与年度发生率（ARO）相乘得出的。ALE 是风险评估中常用的指标，用于量化风险的潜在财务影响。

- \*\*SLE (Single Loss Expectancy)\*\* 是指每次风险事件发生时预计的损失金额。

- \*\*ARO (Annualized Rate of Occurrence)\*\* 是指每年风险事件发生的预期次数。

- \*\*EF (Exposure Factor)\*\* 是指资产在风险事件发生时可能受到影响的百分比。

因此，Gordon 确定的是 ALE。

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

题目24：Greg希望在他的组织中实施应用控制技术。他希望用户只在系统上安装已批准的软件。这种情况下采用什么类型的应用控制技术是恰当的？

Greg would like to implement application control technology in his organization. He would like to limit users to installing only approved software on their systems. What type of application control would be appropriate in this situation?

A：黑名单

Blacklisting

B：灰名单

Graylisting

C：白名单

Whitelisting

D：蓝名单

Bluelisting

答案:在这种情况下，Greg希望限制用户只能安装已批准的软件。这意味着他需要一种能够明确允许特定软件运行的技术，而阻止所有其他软件的安装和运行。这种控制技术被称为“白名单”（Whitelisting）。

\*\*白名单\*\*（Whitelisting）是一种安全策略，它只允许预先批准的应用程序在系统上运行。所有不在白名单上的应用程序都会被阻止。这种方法可以有效防止未经授权的软件安装和运行，从而提高系统的安全性。

其他选项的解释：

- \*\*黑名单\*\*（Blacklisting）：阻止已知的不良软件运行，但允许所有其他软件运行。这种方法不如白名单安全，因为新的或未知的恶意软件可能不在黑名单上。

- \*\*灰名单\*\*（Graylisting）：通常用于电子邮件过滤，与应用程序控制无关。

- \*\*蓝名单\*\*（Bluelisting）：这不是一个常见的术语，通常不用于描述应用程序控制技术。

因此，最合适的选项是 \*\*C：白名单\*\*（Whitelisting）。

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

题目25：Frank负责管理一台Web服务器的安全，该服务器向世界各地的人们提供新闻和信息。他的服务器收到了异常高的流量，以至于无法处理，于是服务器不得不拒绝请求。Frank追溯流量的来源，最后查出是僵尸网络。请问他的服务器受到了什么类型的攻击？

Frank is the security administrator for a web server that provides news and information to people located around the world. His server received an unusually high volume of traffic that it could not handle and was forced to reject requests. Frank traced the source of the traffic back to a botnet. What type of attack took place?

A：拒绝服务

Denial-of-service

B：侦察

Reconnaissance

C：损害

Compromise

D：恶意内部人员

Malicious insider

答案:Frank的服务器受到的攻击类型是 \*\*A：拒绝服务（Denial-of-service）\*\*。

解释：

- \*\*拒绝服务攻击（DoS）\*\* 是指攻击者通过发送大量请求或流量，使服务器资源耗尽，无法正常处理合法用户的请求，从而导致服务中断或拒绝服务。

- 在这个案例中，僵尸网络（botnet）被用来发起大规模的流量攻击，导致服务器无法处理正常的请求，因此这是一种 \*\*分布式拒绝服务攻击（DDoS）\*\*，属于拒绝服务攻击的一种。

其他选项：

- \*\*B：侦察（Reconnaissance）\*\*：通常是攻击前的信息收集行为，而不是直接导致服务中断。

- \*\*C：损害（Compromise）\*\*：通常指系统被入侵或数据被篡改，与流量攻击无关。

- \*\*D：恶意内部人员（Malicious insider）\*\*：指内部人员故意破坏系统，与僵尸网络无关。

因此，正确答案是 \*\*A：拒绝服务（Denial-of-service）\*\*。

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

题目26：在这里显示的数据库表中，哪一列将是主键的最佳候选？

In the database table shown here, which column would be the best candidate for a primary key?

<div style="text-align:center"><img alt="" height="91" src="/file/100000/m/20210823/b1d1bd1e2124411bb1cf2b2924f801f8.png" width="701" /></div>

A：公司ID

Company ID

B：公司名称

Company Name

C：邮政编码

ZIP Code

D：销售代表

Sales Rep

答案:在数据库设计中，主键（Primary Key）是用于唯一标识表中每一行记录的列或列组合。主键必须满足以下条件：

1. \*\*唯一性\*\*：每一行的主键值必须是唯一的，不能重复。

2. \*\*非空性\*\*：主键值不能为NULL。

3. \*\*稳定性\*\*：主键值一旦确定，通常不应更改。

根据这些条件，我们来分析题目中给出的选项：

- \*\*A：公司ID（Company ID）\*\*：通常，公司ID是唯一标识每个公司的编号，具有唯一性和非空性，且通常不会更改。因此，公司ID是主键的最佳候选。

- \*\*B：公司名称（Company Name）\*\*：虽然公司名称通常是唯一的，但有可能存在名称相同的情况（尤其是在不同地区或国家），并且公司名称可能会更改，因此不适合作为主键。

- \*\*C：邮政编码（ZIP Code）\*\*：邮政编码通常用于标识地理区域，而不是唯一的公司标识符。多个公司可能共享同一个邮政编码，因此不适合作为主键。

- \*\*D：销售代表（Sales Rep）\*\*：销售代表通常是一个人名或员工ID，可能对应多个公司，因此不具备唯一性，不适合作为主键。

综上所述，\*\*A：公司ID（Company ID）\*\* 是主键的最佳候选。

\*\*答案：A：公司ID（Company ID）\*\*

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

题目27：Gwen是一家金融服务公司的网络安全专家，该公司负责维护客户记录。这些记录包括每个客户的个人信息，包括客户的姓名、社会安全号码、出生日期和地点以及母亲的婚前姓氏。 哪项类别最能描述这些记录？

Gwen is a cybersecurity professional for a financial services firm that maintains records of their customers. These records include personal information about each customer, including the customer's name, Social Security number, date and place of birth, and mother's maiden name. What category best describes these records?

A：PHI

PHI

B：专有数据

Proprietary data

C：PII

PII

D：EDI

EDI

答案:题目中提到的客户记录包括客户的姓名、社会安全号码、出生日期和地点以及母亲的婚前姓氏。这些信息都属于个人身份信息（Personally Identifiable Information, PII），因为它们可以用来直接或间接地识别特定的个人。

- \*\*PHI（Protected Health Information）\*\*：受保护的健康信息，通常与医疗记录相关，题目中没有提到健康信息。

- \*\*专有数据（Proprietary data）\*\*：通常指公司内部的商业机密或知识产权，与个人身份信息无关。

- \*\*PII（Personally Identifiable Information）\*\*：个人身份信息，包括可以用来识别个人的信息，如姓名、社会安全号码等。

- \*\*EDI（Electronic Data Interchange）\*\*：电子数据交换，通常指企业之间的电子文档交换，与个人身份信息无关。

因此，最能描述这些记录的类别是 \*\*C：PII\*\*。

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

题目28：Bob正在其网络上配置出口过滤，检查发往Internet的流量。他的组织使用公共地址范围12.8.195.0/24。Bob应该允许带有以下哪个目标地址的数据包离开网络？

Bob is configuring egress filtering on his network, examining traffic destined for the internet. His organization uses the public address range 12.8.195.0/24. Packets with which one of the following destination addresses should Bob permit to leave the network?

A：12.8.195.15

12.8.195.15

B：10.8.15.9

10.8.15.9

C：192.168.109.55

192.168.109.55

D：129.53.44.124

129.53.44.124

答案:Bob 正在配置出口过滤，目的是检查发往 Internet 的流量。他的组织使用的公共地址范围是 \*\*12.8.195.0/24\*\*。这意味着该组织的公共 IP 地址范围是从 \*\*12.8.195.0\*\* 到 \*\*12.8.195.255\*\*。

在出口过滤中，Bob 应该允许发往 Internet 的流量通过，同时阻止发往内部私有地址范围的流量。私有地址范围包括：

- \*\*10.0.0.0/8\*\*（10.0.0.0 到 10.255.255.255）

- \*\*172.16.0.0/12\*\*（172.16.0.0 到 172.31.255.255）

- \*\*192.168.0.0/16\*\*（192.168.0.0 到 192.168.255.255）

根据这些信息，我们来分析选项：

- \*\*A：12.8.195.15\*\*

这个地址属于 Bob 组织的公共地址范围（12.8.195.0/24），因此应该允许通过。

- \*\*B：10.8.15.9\*\*

这个地址属于私有地址范围（10.0.0.0/8），不应该允许通过。

- \*\*C：192.168.109.55\*\*

这个地址属于私有地址范围（192.168.0.0/16），不应该允许通过。

- \*\*D：129.53.44.124\*\*

这个地址是一个公共地址，不属于私有地址范围，因此应该允许通过。

### 正确答案：

\*\*A：12.8.195.15\*\* 和 \*\*D：129.53.44.124\*\* 都应该被允许通过。

如果只能选择一个最符合题意的答案，那么 \*\*A：12.8.195.15\*\* 是最合适的，因为它明确属于 Bob 组织的公共地址范围。

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

题目29：Brian正在考虑增加其组织使用的加密密钥长度。如果他将8位添加到加密密钥中，那么将有多少可能的密钥添加到算法的密钥空间中？

Brian is considering increasing the length of the cryptographic keys used by his organization. If he adds 8 bits to the encryption key, how many more possible keys will be added to the keyspace for the algorithm?

A：密钥空间的大小将增加一倍

The size of the keyspace will double.

B：密钥空间的大小将增加8倍

The size of the keyspace will increase by a factor of 8.

C：密钥空间的大小将增加64倍

The size of the keyspace will increase by a factor of 64.

D：密钥空间的大小将增加256倍

The size of the keyspace will increase by a factor of 256.

答案:在加密技术中，密钥空间的大小是由密钥的位数决定的。每增加一位，密钥空间的大小就会翻倍。这是因为每一位可以是0或1，所以每增加一位，可能的组合数就乘以2。

如果Brian将加密密钥的长度增加8位，那么密钥空间的大小将增加2^8倍，即256倍。这是因为每一位的增加都会使可能的组合数翻倍，8位就是2的8次方，即256。

因此，正确答案是：

D：密钥空间的大小将增加256倍

The size of the keyspace will increase by a factor of 256.

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

题目30：使用粉碎可以安全有效地处理以下哪些数据资产？（选择所有符合条件的）

Which of the following data assets may be safely and effectively disposed of using shredding? (Select all that apply.)

A：纸质记录

Paper records

B：信用卡

Credit cards

C：可移动介质

Removable media

D：SSD硬盘

SSD hard drives

答案:使用粉碎可以安全有效地处理以下数据资产：

A：纸质记录 (Paper records)

B：信用卡 (Credit cards)

C：可移动介质 (Removable media)

解释：

- \*\*纸质记录\*\*：可以通过碎纸机进行物理粉碎，确保信息无法恢复。

- \*\*信用卡\*\*：通常包含敏感信息，可以通过粉碎机或专门的信用卡切割设备进行销毁。

- \*\*可移动介质\*\*：如CD、DVD、USB驱动器等，可以通过物理粉碎或专门的销毁设备进行处理。

\*\*D：SSD硬盘 (SSD hard drives)\*\* 不适合通过粉碎处理，因为SSD硬盘通常需要使用专门的电子设备进行数据擦除或物理破坏，以确保数据无法恢复。

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

题目31：GAD Systems关注的是黑客可能窃取存储在文件服务器上的敏感信息。这些系统会选择采取风险缓解策略。下列哪种做法符合该策略？

GAD Systems is concerned about the risk of hackers stealing sensitive information stored on a file server. They choose to pursue a risk mitigation strategy. Which one of the following actions would support that strategy?

A：加密文件

Encrypting the files

B：删除文件

Deleting the files

C：购买网络安全保险

Purchasing cyber-liability insurance

D：不采取行动

Taking no action

答案:GAD Systems关注的是黑客可能窃取存储在文件服务器上的敏感信息，并选择采取风险缓解策略。风险缓解策略的目的是减少潜在风险的影响或可能性。在给定的选项中，最符合风险缓解策略的做法是：

A：加密文件

Encrypting the files

加密文件可以确保即使黑客成功窃取了文件，也无法轻易读取或使用其中的敏感信息。这种做法直接减少了信息泄露的风险，因此是最符合风险缓解策略的选择。

其他选项的解释：

- B：删除文件 - 虽然删除文件可以消除信息泄露的风险，但这可能不符合业务需求，因为文件可能仍然需要被访问和使用。

- C：购买网络安全保险 - 这属于风险转移策略，而不是风险缓解策略。保险可以在发生损失时提供经济补偿，但并不能减少信息泄露的风险。

- D：不采取行动 - 这显然不符合任何风险缓解策略，因为它不会减少风险。

因此，正确答案是 A：加密文件。

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

题目32：Viola正在对用户帐户进行审计，以确定帐户是否具有适当级别的权限，以及所有权限是否已通过正式流程获得批准。该组织拥有大约50,000个用户帐户，员工年流动率为24%。在选择记录进行人工审核时，以下哪种抽样方法对于她的时间利用率最有效？

Viola is conducting a user account audit to determine whether accounts have the appropriate level of permissions and that all permissions were approved through a formal process. The organization has approximately 50,000 user accounts and an annual employee turnover rate of 24 percent. Which one of the following sampling approaches would be the most effective use of her time when choosing records for manual review?

A：选择上个月内已修改的所有记录

Select all records that have been modified during the past month.

B：要求访问管理员确定最有可能出现问题的帐户，并对其进行审计

Ask access administrators to identify the accounts most likely to have issues and audit those.

C：从整个总体或审计期间发生变化的总体记录中，随机选择记录样本

Select a random sample of records, either from the entire population or from the population of records that have changed during the audit period.

D：抽样在这种情况下是无效的，所有帐户都应该被审计

Sampling is not effective in this situation, and all accounts should be audited.

答案:在Viola进行用户帐户审计的情况下，她需要确定帐户是否具有适当级别的权限，并且所有权限是否已通过正式流程获得批准。考虑到组织有大约50,000个用户帐户和24%的年员工流动率，选择一个有效的抽样方法对于她的时间利用率至关重要。

让我们逐一分析每个选项：

A：选择上个月内已修改的所有记录

- 这种方法可能会捕捉到最近变动的帐户，但可能忽略了那些权限设置不当但近期未修改的帐户。此外，如果上个月内的修改量很大，这种方法可能仍然需要审查大量记录。

B：要求访问管理员确定最有可能出现问题的帐户，并对其进行审计

- 这种方法依赖于访问管理员的判断，可能会引入偏见。此外，访问管理员可能无法准确识别所有有问题的帐户，导致某些问题被忽略。

C：从整个总体或审计期间发生变化的总体记录中，随机选择记录样本

- 随机抽样是一种统计上有效的方法，可以确保样本具有代表性。通过随机选择记录，Viola可以覆盖整个用户帐户群体，而不仅仅是那些近期修改过的帐户。这种方法在时间和资源上都是高效的，并且可以提供可靠的审计结果。

D：抽样在这种情况下是无效的，所有帐户都应该被审计

- 审计所有50,000个帐户将非常耗时且资源密集，对于Viola来说可能不切实际。抽样方法在大多数情况下是有效的，尤其是在资源有限的情况下。

综上所述，选项C（从整个总体或审计期间发生变化的总体记录中，随机选择记录样本）是最有效的时间利用方法。这种方法不仅能够提供具有代表性的样本，还能在合理的时间内完成审计任务。

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

题目33：Lila正在审查其组织不利的离职流程。在这个过程中，什么时候撤销用户对数字系统的访问权限最合适？

Lila is reviewing her organization's adverse termination process. In that process, when would be the most appropriate time to revoke a user's access privileges to digital systems?

A：在通知用户离职时

At the time the user is informed of the termination

B：在雇佣的最后一天结束时

At the end of the last day of employment

C：在作出决定时

At the time the decision is made

D：雇佣最后一天后的几天

Several days after the last day of employment

答案:在审查组织的不利离职流程时，撤销用户对数字系统的访问权限的时间点是一个关键的安全问题。最合适的做法是在通知用户离职时立即撤销其访问权限（选项A）。这样做可以防止用户在得知即将离职后，可能出于报复或其他不良动机，对系统进行破坏或窃取敏感信息。

其他选项的考虑：

- 选项B（在雇佣的最后一天结束时）可能会给用户留下时间窗口，在这段时间内他们可能滥用系统访问权限。

- 选项C（在作出决定时）可能过早，因为此时用户还未被正式通知，过早撤销访问权限可能会引起不必要的注意或恐慌。

- 选项D（雇佣最后一天后的几天）则明显过晚，增加了安全风险。

因此，为了最大限度地保护组织的数字资产和数据安全，最佳实践是在通知用户离职时立即撤销其访问权限。

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

题目34：William正在审查存储在系统上的日志文件，这些文件里包含了可能受到的攻击。他找到了图中的日志文件。这是什么类型的日志文件？

William is reviewing log files that were stored on a system with a suspected compromise. He finds the log file shown here. What type of logfile is this?

<div style="text-align:center"><img alt="" height="363" src="/file/100000/m/20210823/b11d8a0746a34972ad82d3d2d9a96114.png" width="697" /></div>

A：防火墙日志

Firewall log

B：变更日志

Change log

C：应用程序日志

Application log

D：系统日志

System log

答案:根据题目描述，William正在审查可能受到攻击的系统日志文件。虽然题目中提到了一个图片，但由于无法查看图片内容，我们可以根据常见的日志类型来推测。

- \*\*防火墙日志（Firewall log）\*\*：通常记录网络流量、连接尝试、被阻止的IP地址等信息，用于监控和防御网络攻击。

- \*\*变更日志（Change log）\*\*：记录系统或应用程序的配置更改、文件修改等操作。

- \*\*应用程序日志（Application log）\*\*：记录应用程序的运行状态、错误信息、用户操作等。

- \*\*系统日志（System log）\*\*：记录操作系统的事件，如启动、关机、硬件错误、服务状态等。

由于题目中提到的是“可能受到的攻击”，防火墙日志是最有可能的，因为防火墙日志通常用于检测和防御网络攻击。因此，最合适的答案是：

\*\*A：防火墙日志（Firewall log）\*\*

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

题目35：Roger正在审查其组织中的安全漏洞列表，并根据其严重性对其进行评级。以下哪种模型对他的工作最有用？

Roger is reviewing a list of security vulnerabilities in his organization and rating them based upon their severity. Which one of the following models would be most useful to his work?

A：CVSS

CVSS

B：STRIDE

STRIDE

C：PASTA

PASTA

D：ATT&CK

ATT&CK

答案:题目35的正确答案是：

A：CVSS

\*\*解释：\*\*

CVSS（Common Vulnerability Scoring System，通用漏洞评分系统）是一种用于评估和评分安全漏洞严重性的标准化方法。它通过考虑多个因素（如攻击向量、攻击复杂性、影响范围等）来为漏洞分配一个分数，帮助组织确定哪些漏洞需要优先修复。因此，CVSS 是 Roger 在审查和评级安全漏洞严重性时最有用的模型。

其他选项的解释：

- \*\*STRIDE\*\*：是一种威胁建模方法，用于识别和分类系统中的潜在威胁。

- \*\*PASTA\*\*：是一种风险分析框架，用于将业务目标与安全需求对齐。

- \*\*ATT&CK\*\*：是一个描述攻击者行为和技术的框架，主要用于防御和检测攻击。

这些模型虽然与安全相关，但不直接用于漏洞的严重性评级。

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

题目36：攻击者最近致电组织的服务台，并说服他们重置另一个用户的帐户密码。哪项术语最恰当的描述了这种攻击？

An attacker recently called an organization's help desk and persuaded them to reset a password for another user's account. What term best describes this attack?

A：人类木马

A human Trojan

B：社会工程学

Social engineering

C：网络钓鱼

Phishing

D：捕鲸

Whaling

答案:正确答案是：

B：社会工程学

Social engineering

解释：社会工程学是一种通过操纵人类心理来获取信息或访问权限的攻击方式。在这个例子中，攻击者通过电话说服服务台重置另一个用户的密码，这是一种典型的社会工程学攻击。

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

题目37：Greg正在评估一家新供应商，这家供应商将为其组织提供网络设备。由于其组织的工作性质，Greg担心攻击者可能会尝试利用供应链进行攻击。假设Greg的组织和供应商都在合理的安全程序下运行，以下哪项活动可能对设备造成最大的供应链风险？

Greg is evaluating a new vendor that will be supplying networking gear to his organization. Due to the nature of his organization's work, Greg is concerned that an attacker might attempt a supply chain exploit. Assuming that both Greg's organization and the vendor operate under reasonable security procedures, which one of the following activities likely poses the greatest supply chain risk to the equipment?

A：在供应商现场被未经授权的第三方篡改

Tampering by an unauthorized third party at the vendor's site

B：拦截传输中的设备

Interception of devices in transit

C：安装后管理员配置错误

Misconfiguration by an administrator after installation

D：在Greg的网站上被未经授权的第三方篡改

Tampering by an unauthorized third party at Greg’s site

答案:在评估供应链风险时，我们需要考虑攻击者可能利用的各个环节。根据题目描述，Greg的组织和供应商都在合理的安全程序下运行，因此我们需要找出哪个环节可能成为最薄弱的环节。

A. \*\*在供应商现场被未经授权的第三方篡改\*\*

供应商现场的安全措施可能不如Greg的组织严格，攻击者可能利用这一点在设备出厂前进行篡改，植入恶意软件或硬件后门。这种篡改可能在设备交付后很长时间内不被发现，因此具有较高的风险。

B. \*\*拦截传输中的设备\*\*

虽然拦截传输中的设备是一种潜在的风险，但通常运输过程中会有一定的安全措施，如加密通信、跟踪设备等。此外，设备在运输过程中被拦截的风险相对较低，因为攻击者需要具备较高的技术能力和资源。

C. \*\*安装后管理员配置错误\*\*

配置错误虽然可能导致安全漏洞，但这属于内部管理问题，而不是供应链攻击。供应链攻击通常指的是在设备或软件进入组织之前被篡改或植入恶意代码。

D. \*\*在Greg的网站上被未经授权的第三方篡改\*\*

这种篡改发生在设备已经交付并安装后，属于内部安全管理的范畴，而不是供应链攻击。供应链攻击通常发生在设备或软件进入组织之前。

综上所述，\*\*A选项\*\*（在供应商现场被未经授权的第三方篡改）是最有可能对设备造成最大供应链风险的活动，因为这种篡改可能在设备交付前就已经发生，并且可能在很长一段时间内不被发现。

\*\*最终答案：A\*\*

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

题目38：Kevin在单一级别的安全环境中运行，并试图根据信息系统处理的信息类型对信息系统进行分类。他分配资产分类的最佳方式是什么？

Kevin is operating in a single-level security environment and is seeking to classify information systems according to the type of information that they process. What procedure would be the best way for him to assign asset classifications?

A：为系统分配它们通常处理的信息分类

Assign systems the classification of information that they most commonly process.

B：为系统分配期望它们经常处理的最高级别信息的分类

Assign systems the classification of the highest level of information that they are expected to process regularly.

C：为系统分配期望它们处理的最高级别信息的分类

Assign systems the classification of the highest level of information that they are ever expected to process.

D：为所有系统分配相同的分类级别

Assign all systems the same classification level.

答案:在单一级别的安全环境中，信息系统的分类通常基于它们处理的信息的最高安全级别。这是因为即使系统通常处理较低级别的信息，如果它们有可能处理更高级别的信息，那么系统本身也需要具备相应的安全措施来保护这些信息。因此，最佳的做法是为系统分配它们期望处理的最高级别信息的分类。

选项分析：

- \*\*A\*\*：为系统分配它们通常处理的信息分类。这种方法可能不足以保护偶尔处理的高级别信息。

- \*\*B\*\*：为系统分配期望它们经常处理的最高级别信息的分类。这种方法比A更安全，但仍然可能不足以保护偶尔处理的高级别信息。

- \*\*C\*\*：为系统分配期望它们处理的最高级别信息的分类。这是最安全的方法，确保系统能够处理所有可能的信息级别。

- \*\*D\*\*：为所有系统分配相同的分类级别。这种方法可能过于严格或不切实际，特别是在系统处理不同级别信息的情况下。

因此，最佳答案是 \*\*C\*\*：为系统分配期望它们处理的最高级别信息的分类。

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

题目39-1：根据以下情景回答3个问题：

Ben所在的组织有一个传统的现场Active Directory环境，该公司有350名员工，每增加一名员工都需要进行手动配置。随着公司采用新技术，他们越来越多地使用软件即服务应用程序来替换其内部开发的软件堆栈。

Ben的任务是设计一个身份管理系统，该系统允许公司使用云服务，同时应该支持现有的系统。使用给出的逻辑图，回答关于以下问题。

<div style="text-align:center"><img alt="" height="304" src="/file/100000/m/20210823/f7343b5290534372a5461057ccb550f5.png" width="481" /></div>

For questions , please refer to the following scenario:

The organization that Ben works for has a traditional onsite Active Directory environment that uses a manual provisioning process for each addition to their 350-employee company. As the company adopts new technologies, they are increasingly using software as a service applications to replace their internally developed software stack.

Ben has been tasked with designing an identity management implementation that will allow his company to use cloud services while supporting their existing systems. Using the logical diagram shown here, answer the following questions about the identity recommendations Ben should make.

<div style="text-align:center"><img alt="" height="392" src="/file/100000/m/20210823/9e47803fecc642a3b8fb137cc7829a73.png" width="593" /></div>

如果组织最关心的是身份验证服务的可用性，那么Ben应该使用什么类型的身份验证平台？

If availability of authentication services is the organization’s biggest priority, what type of identity platform should Ben recommend?

A：在线

Onsite

B：基于云的

Cloud-based

C：混合

Hybrid

D：外包

Outsourced

答案:如果组织最关心的是身份验证服务的可用性，Ben应该推荐使用基于云的身份验证平台（选项B：Cloud-based）。

### 理由：

1. \*\*高可用性\*\*：云服务提供商通常提供高可用性和冗余机制，确保身份验证服务在大多数情况下都能正常运行。即使某个数据中心出现问题，云服务提供商通常会有多个数据中心来保证服务的连续性。

2. \*\*自动扩展\*\*：云平台可以根据需求自动扩展资源，确保在高负载情况下仍能提供稳定的服务。

3. \*\*全球覆盖\*\*：云服务通常在全球范围内都有数据中心，能够为分布在不同地理位置的用户提供低延迟的身份验证服务。

4. \*\*减少单点故障\*\*：与传统的本地部署相比，云服务通常具有更好的容错能力，减少了单点故障的风险。

5. \*\*维护和更新\*\*：云服务提供商负责维护和更新身份验证平台，确保其始终处于最新状态，减少了组织内部的维护负担。

因此，基于云的身份验证平台能够更好地满足组织对身份验证服务可用性的高要求。

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

题目39-1：根据以下情景回答3个问题：

Ben所在的组织有一个传统的现场Active Directory环境，该公司有350名员工，每增加一名员工都需要进行手动配置。随着公司采用新技术，他们越来越多地使用软件即服务应用程序来替换其内部开发的软件堆栈。

Ben的任务是设计一个身份管理系统，该系统允许公司使用云服务，同时应该支持现有的系统。使用给出的逻辑图，回答关于以下问题。

<div style="text-align:center"><img alt="" height="304" src="/file/100000/m/20210823/f7343b5290534372a5461057ccb550f5.png" width="481" /></div>

For questions , please refer to the following scenario:

The organization that Ben works for has a traditional onsite Active Directory environment that uses a manual provisioning process for each addition to their 350-employee company. As the company adopts new technologies, they are increasingly using software as a service applications to replace their internally developed software stack.

Ben has been tasked with designing an identity management implementation that will allow his company to use cloud services while supporting their existing systems. Using the logical diagram shown here, answer the following questions about the identity recommendations Ben should make.

<div style="text-align:center"><img alt="" height="392" src="/file/100000/m/20210823/9e47803fecc642a3b8fb137cc7829a73.png" width="593" /></div>

如果Ben 需要与上述业务伙伴共享身份信息，他应该调查什么？

If Ben needs to share identity information with the business partner shown, what should he investigate?

A：单点登录

Single sign-on

B：多因素验证

Multifactor authentication

C：联邦

Federation

D：IDaaS

IDaaS

答案:如果Ben需要与业务伙伴共享身份信息，他应该调查的是 \*\*C：联邦（Federation）\*\*。

联邦身份管理（Federation）允许不同组织之间共享身份信息，使得用户可以使用一个组织的身份凭证来访问另一个组织的资源。这种方式通常通过标准协议（如SAML、OAuth、OpenID Connect等）实现，确保身份信息的安全传输和验证。

其他选项的解释：

- \*\*A：单点登录（Single Sign-On, SSO）\*\*：允许用户使用一组凭证登录多个系统，但不涉及跨组织的身份共享。

- \*\*B：多因素验证（Multifactor Authentication, MFA）\*\*：增加身份验证的安全性，但不直接涉及身份信息的共享。

- \*\*D：IDaaS（Identity as a Service）\*\*：提供基于云的身份管理服务，但不专门解决跨组织的身份共享问题。

因此，\*\*C：联邦（Federation）\*\*是最合适的选项。

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

题目39-1：根据以下情景回答3个问题：

Ben所在的组织有一个传统的现场Active Directory环境，该公司有350名员工，每增加一名员工都需要进行手动配置。随着公司采用新技术，他们越来越多地使用软件即服务应用程序来替换其内部开发的软件堆栈。

Ben的任务是设计一个身份管理系统，该系统允许公司使用云服务，同时应该支持现有的系统。使用给出的逻辑图，回答关于以下问题。

<div style="text-align:center"><img alt="" height="304" src="/file/100000/m/20210823/f7343b5290534372a5461057ccb550f5.png" width="481" /></div>

For questions , please refer to the following scenario:

The organization that Ben works for has a traditional onsite Active Directory environment that uses a manual provisioning process for each addition to their 350-employee company. As the company adopts new technologies, they are increasingly using software as a service applications to replace their internally developed software stack.

Ben has been tasked with designing an identity management implementation that will allow his company to use cloud services while supporting their existing systems. Using the logical diagram shown here, answer the following questions about the identity recommendations Ben should make.

<div style="text-align:center"><img alt="" height="392" src="/file/100000/m/20210823/9e47803fecc642a3b8fb137cc7829a73.png" width="593" /></div>

当Ben的组织向他们的电子商务云合作伙伴提供验证和授权时，可能会涉及哪些技术？

What technology is likely to be involved when Ben’s organization needs to provide authentication and authorization assertions to their cloud e-commerce application?

A：Active Directory

Active Directory

B：SAML

SAML

C：RADIUS

RADIUS

D：SPML

SPML

答案:在Ben的组织向他们的电子商务云合作伙伴提供验证和授权时，可能会涉及的技术是 \*\*B：SAML\*\*。

\*\*SAML（Security Assertion Markup Language）\*\* 是一种基于XML的标准，用于在不同的安全域之间交换认证和授权数据。它通常用于单点登录（SSO）场景，允许用户在多个系统之间无缝切换，而无需重复登录。SAML特别适用于云服务环境，因为它允许组织在本地身份管理系统（如Active Directory）和云服务之间建立信任关系。

其他选项的解释：

- \*\*A：Active Directory\*\* 是本地身份管理系统，虽然它可以与云服务集成，但它本身并不是用于向云服务提供验证和授权的标准协议。

- \*\*C：RADIUS\*\* 主要用于网络访问控制，通常用于VPN或Wi-Fi认证，而不是用于云服务的身份验证和授权。

- \*\*D：SPML（Service Provisioning Markup Language）\*\* 用于用户账户的自动化配置和管理，而不是用于身份验证和授权。

因此，SAML是最合适的选项。

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

题目40：Dave负责组织中的密码安全，并希望加强密码文件的安全性。他想保护组织以对抗彩虹表的攻击。以下哪种技术是专门设计用来阻止彩虹表的？

Dave is responsible for password security in his organization and would like to strengthen the security of password files. He would like to defend his organization against the use of rainbow tables. Which one of the following techniques is specifically designed to frustrate the use of rainbow tables?

A：密码到期策略

Password expiration policies

B：盐

Salting

C：用户培训

User education

D：密码复杂性策略

Password complexity policies

答案:正确答案是 \*\*B：盐 (Salting)\*\*。

### 解释：

- \*\*彩虹表攻击\*\* 是一种预先计算的哈希值表，用于快速破解密码哈希。彩虹表通过存储大量常见密码及其对应的哈希值，使得攻击者可以通过查找哈希值来快速恢复原始密码。

- \*\*盐 (Salting)\*\* 是一种专门设计用来对抗彩虹表攻击的技术。盐是一个随机生成的值，与密码结合后再进行哈希处理。由于每个用户的盐值不同，即使两个用户使用相同的密码，其哈希值也会不同。这使得彩虹表攻击变得无效，因为攻击者无法预先计算所有可能的盐值和密码组合。

- \*\*密码到期策略 (Password expiration policies)\*\* 和 \*\*密码复杂性策略 (Password complexity policies)\*\* 虽然可以增强密码的安全性，但它们并不能直接防止彩虹表攻击。

- \*\*用户培训 (User education)\*\* 虽然有助于提高用户的安全意识，但它也不是专门用来对抗彩虹表攻击的技术。

因此，\*\*盐 (Salting)\*\* 是专门设计用来阻止彩虹表攻击的技术。

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

题目41：Helen最近建立了一个新系统，作为其组织诱骗活动的一部分。该系统的配置方式使其容易受到攻击，并表明它可能包含高度敏感的信息。什么术语最能描述这个系统？

Helen recently built a new system as part of her organization's deception campaign. The system is configured in a manner that makes it vulnerable to attack and that conveys that it might contain highly sensitive information. What term best describes this system?

A：蜜网

Honeynet

B：暗网

Darknet

C：蜜罐

Honeypot

D：伪缺陷

Pseudoflaw

答案:这个系统被设计成容易受到攻击，并且看起来包含高度敏感的信息，目的是诱骗攻击者。这种系统通常被称为“蜜罐”（Honeypot）。

蜜罐是一种安全机制，用于检测、转移或研究攻击者的行为。它通过模拟一个易受攻击的系统或服务来吸引攻击者，从而让安全团队能够监控和分析攻击行为。

因此，正确答案是：

C：蜜罐

Honeypot

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

题目42：Nandi正在评估一组候选系统，以取代其组织中的生物身份验证机制。什么指标是比较不同系统有效性的最佳方式？

Nandi is evaluating a set of candidate systems to replace a biometric authentication mechanism in her organization. What metric would be the best way to compare the effectiveness of the different systems?

A：FAR

FAR

B：FRR

FRR

C：CER

CER

D：FDR

FDR

答案:在评估生物身份验证系统的有效性时，常用的指标包括：

- \*\*FAR（False Acceptance Rate，错误接受率）\*\*：表示系统错误地将未授权用户识别为授权用户的比率。FAR越低，系统的安全性越高。

- \*\*FRR（False Rejection Rate，错误拒绝率）\*\*：表示系统错误地将授权用户识别为未授权用户的比率。FRR越低，系统的用户体验越好。

- \*\*CER（Crossover Error Rate，交叉错误率）\*\*：是FAR和FRR相等时的错误率，通常用来衡量系统的整体性能。CER越低，系统的性能越好。

在这三个指标中，\*\*CER（Crossover Error Rate）\*\* 是最常用的综合指标，因为它同时考虑了FAR和FRR，能够更全面地反映系统的性能。

因此，最佳的比较不同系统有效性的指标是：

\*\*C：CER\*\*

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

题目43：Sean 怀疑公司有人泄露了秘密信息，尽管公司使用了数据丢失预防系统。他发现嫌疑人正将照片(包括题中显示的照片)发布到公共互联网留言板。该嫌疑人可使用什么类型的技术来隐藏此图像中的消息？

Sean suspects that an individual in his company is smuggling out secret information despite his company's careful use of data loss prevention systems. He discovers that the suspect is posting photos, including the one shown here, to public internet message boards. What type of technique may the individuals be using to hide messages inside this image?

<div style="text-align:center"><img alt="" height="349" src="/file/100000/m/20210823/1897266adcbe452ba9dabdc153c01bfb.png" width="697" /></div>

A：水印

Watermarking

B：VPN

VPN

C：隐写

Steganography

D：隐蔽时序通道

Covert timing channel

答案:正确答案是 C：隐写（Steganography）。

隐写是一种将信息隐藏在其他媒介（如图片、音频、视频等）中的技术。通过隐写技术，用户可以在不引起注意的情况下将秘密信息嵌入到看似普通的文件中。在这个例子中，嫌疑人可能使用隐写技术将秘密信息隐藏在发布的图片中，从而绕过公司的数据丢失预防系统。

其他选项的解释：

- A：水印（Watermarking）通常用于版权保护或标识来源，而不是隐藏信息。

- B：VPN（虚拟专用网络）用于加密和隐藏网络流量，而不是隐藏信息在图片中。

- D：隐蔽时序通道（Covert timing channel）是一种通过调整数据传输的时间来隐藏信息的技术，通常不用于图片中隐藏信息。

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

题目44：Roger担心第三方公司开发的应用程序会有后门。然而，开发人员拥有知识产权，并且仅将最终软件提供给Roger的组织。以下哪种语言由于可以提供便于人们阅读的代码，因而对这种后门类型的攻击最不敏感？

Roger is concerned that a third-party firm hired to develop code for an internal application will embed a backdoor in the code. The developer retains rights to the intellectual property and will only deliver the software in its final form. Which one of the following languages would be least susceptible to this type of attack because it would provide Roger with code that is human-readable in its final form?

A：JavaScript

JavaScript

B：C

C

C：C++

C++

D：Java

Java

答案:题目中提到的关键点是Roger担心第三方开发的应用程序可能包含后门，并且开发人员只提供最终软件，而不提供源代码。因此，Roger希望使用一种语言，使得最终软件中的代码是易于人类阅读的，从而减少后门攻击的风险。

选项分析：

- \*\*A：JavaScript\*\*

JavaScript 是一种解释型语言，通常以源代码形式分发。即使经过压缩或混淆，JavaScript 代码仍然可以通过工具进行反混淆，使其相对易于阅读。因此，JavaScript 代码在最终形式中仍然可以被人类阅读，从而更容易检测潜在的后门。

- \*\*B：C\*\*

C 是一种编译型语言，通常以二进制形式分发。编译后的代码对人类来说是不可读的，因此很难通过阅读代码来检测后门。

- \*\*C：C++\*\*

C++ 也是一种编译型语言，通常以二进制形式分发。与 C 类似，编译后的代码对人类来说是不可读的，因此很难通过阅读代码来检测后门。

- \*\*D：Java\*\*

Java 是一种编译型语言，但它编译为字节码，而不是机器码。字节码可以通过反编译工具转换为相对可读的源代码。因此，Java 代码在最终形式中仍然可以被人类阅读，从而更容易检测潜在的后门。

综上所述，\*\*JavaScript\*\* 和 \*\*Java\*\* 的代码在最终形式中相对易于阅读，但 JavaScript 通常以源代码形式分发，因此更容易被人类阅读。因此，\*\*JavaScript\*\* 是最不敏感于这种后门攻击的语言。

\*\*正确答案：A：JavaScript\*\*

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

题目45：Jesse正在查看系统上的/etc/passwd文件，该系统配置了阴影密码。她应该会在此文件的密码字段中看到什么？

Jesse is looking at the /etc/passwd file on a system configured to use shadowed passwords. What should she expect to see in the password field of this file?

A：明文密码

Plaintext passwords

B：加密的密码

Encrypted passwords

C：散列化的密码

Hashed passwords

D：x

x

答案:在配置了阴影密码（shadowed passwords）的系统中，`/etc/passwd` 文件中的密码字段通常不会包含实际的密码信息。相反，密码字段会被替换为一个占位符，通常是字母 `x`。实际的密码信息存储在 `/etc/shadow` 文件中，这个文件只有特权用户（如 root）才能访问。

因此，Jesse 在 `/etc/passwd` 文件的密码字段中应该会看到的是 `x`。

正确答案是：

D：x

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

题目46：Rob最近收到来自供应商的通知，说他的组织中使用的防火墙平台的EOL日期即将到来。 Rob应该采取什么行动？

Rob recently received a notice from a vendor that the EOL date is approaching for a firewall platform that is used in his organization. What action should Rob take?

A：准备尽快停止使用该平台

Prepare to discontinue use of the platform as soon as possible.

B：立即停止使用该设备

Immediately discontinue use of the device.

C：作为组织正常计划周期的一部分，准备停止使用该设备

Prepare to discontinue use of the device as part of the organization’s normal planning cycle.

D：无需采取任何行动

No action is necessary.

答案:当供应商通知某个产品的EOL（End of Life，生命周期结束）日期即将到来时，这意味着供应商将不再为该产品提供支持、更新或安全补丁。这可能会导致安全漏洞和合规性问题。因此，Rob应该采取行动来确保组织的网络安全。

选项分析：

- \*\*A：准备尽快停止使用该平台\*\*

这是一个合理的行动，但“尽快”可能意味着在没有充分准备的情况下停止使用，这可能会导致业务中断或其他问题。

- \*\*B：立即停止使用该设备\*\*

立即停止使用可能会导致业务中断，尤其是在没有替代方案的情况下。这不是一个理想的选择。

- \*\*C：作为组织正常计划周期的一部分，准备停止使用该设备\*\*

这是最合理的选项。Rob应该将停止使用该设备纳入组织的正常计划周期中，确保有足够的时间来评估替代方案、进行迁移并确保业务连续性。

- \*\*D：无需采取任何行动\*\*

这是不合适的，因为EOL意味着设备将不再获得支持，可能会带来安全风险。

\*\*正确答案：C\*\*

Rob应该作为组织正常计划周期的一部分，准备停止使用该设备。

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

题目47：什么原则要求一个人应该尽力准确和及时地履行他的职责？

What principle states that an individual should make every effort to complete his or her responsibilities in an accurate and timely manner?

A：最小特权

Least privilege

B：职责分离

Separation of duties

C：应尽关注

Due care

D：应尽职责

Due diligence

答案:题目47询问的是关于一个人应该尽力准确和及时地履行他的职责的原则。选项A“最小特权”是指用户或程序只能获得完成其任务所需的最小权限，这与题目无关。选项B“职责分离”是指将任务和责任分配给不同的人以减少错误和欺诈的风险，这也与题目无关。选项C“应尽关注”是指个人或组织在履行职责时应采取合理的关注和谨慎，这与题目描述的原则相符。选项D“应尽职责”通常指的是在投资或商业决策中进行的详细和系统的评估，这与题目描述的原则不完全相符。因此，正确答案是C“应尽关注”。

正确答案是：C：应尽关注

Due care

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

题目48：Tony正在为他的组织开发一个数据分类系统。在确定每一类信息的分类级别时，他应该使用什么因素作为主要驱动因素？

Tony is developing a data classification system for his organization. What factor should he use as the primary driver when determining the classification level of each category of information?

A：敏感性

Sensitivity

B：来源

Source

C：被盗的可能性

Likelihood of theft

D：数据丢失的可能性

Likelihood of data loss

答案:在确定每一类信息的分类级别时，Tony应该使用\*\*敏感性\*\*作为主要驱动因素。这是因为数据的敏感性直接关系到数据的重要性、保护需求以及泄露后可能带来的影响。高敏感性的数据通常需要更高级别的保护措施，而低敏感性的数据则可能需要较少的保护。

因此，正确答案是：

\*\*A：敏感性\*\*

\*\*Sensitivity\*\*

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

题目49：Perry正在为其组织建立信息处理要求。他发现该组织经常需要通过互联网向供应商发送敏感信息，并担心这些信息会被截获。什么处理要求最能防止这种风险？

Perry is establishing information handling requirements for his organization. He discovers that the organization often needs to send sensitive information over the internet to a supplier and is concerned about it being intercepted. What handling requirement would best protect against this risk?

A：要求使用传输加密

Require the use of transport encryption.

B：需要适当的分类和标签

Require proper classification and labeling.

C：要求使用数据防泄漏技术

Require the use of data loss prevention technology.

D：要求使用存储加密

Require the use of storage encryption.

答案:题目49的正确答案是：

A：要求使用传输加密

Require the use of transport encryption.

解析：

Perry担心敏感信息在通过互联网传输时被截获，因此最有效的处理要求是使用传输加密。传输加密可以确保数据在传输过程中被加密，即使被截获，也无法被解读。其他选项如分类和标签、数据防泄漏技术和存储加密虽然也有助于信息安全，但它们主要针对数据在存储或使用过程中的保护，而不是在传输过程中的保护。因此，A选项是最能防止信息在传输过程中被截获的风险的。

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

题目50：John正在为他的组织开发有形资产清单。以下哪些项目最有可能包含在此清单中？（选择所有符合条件的）

John is developing a tangible asset inventory for his organization. Which of the following items would most likely be included in this inventory? (Select all that apply.)

A：知识产权

Intellectual property

B：服务器硬件

Server hardware

C：存储在服务器上的文件

Files stored on servers

D：移动设备

Mobile devices

答案:有形资产清单通常包括那些具有物理形态、可以被触摸和计量的资产。根据这个定义，以下选项最有可能包含在John的有形资产清单中：

B：服务器硬件 - 服务器硬件是物理设备，具有明确的物理形态，因此属于有形资产。

D：移动设备 - 移动设备如手机、平板电脑等也是物理设备，属于有形资产。

A：知识产权 - 知识产权是无形的，因为它涉及的是思想、发明、设计等，不具有物理形态，因此不属于有形资产。

C：存储在服务器上的文件 - 这些文件虽然是数字形式，但它们存储在物理设备上。然而，文件本身是数据，不具有物理形态，因此通常不被视为有形资产。

因此，最有可能包含在John的有形资产清单中的是：

B：服务器硬件

D：移动设备

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

题目51：Maria正在分析一起安全事件，她认为攻击者获得了光纤电缆的访问权限，并在该电缆上安装了一个分接头。这种攻击发生在OSI模型的哪一层？

Maria is analyzing a security incident where she believes that an attacker gained access to a fiber-optic cable and installed a tap on that cable. What layer of the OSI model did this attack occur at?

A：传输层

Transport

B：网络层

Network

C：数据链路层

Data Link

D：物理层

Physical

答案:这种攻击发生在OSI模型的\*\*物理层\*\*。

\*\*解释\*\*：

- \*\*物理层（Physical Layer）\*\*是OSI模型的最底层，负责在物理介质上传输原始比特流。攻击者通过访问光纤电缆并安装分接头，实际上是在物理介质上进行窃听或干扰，这属于物理层的攻击。

因此，正确答案是：

\*\*D：物理层\*\*

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

题目52：Bert正在考虑使用基础架构即服务(IaaS)的云计算环境来充当虚拟服务器。这种情况下，以下哪一项属于供应商的责任？

Bert is considering the use of an infrastructure as a service cloud computing partner to provide virtual servers. Which one of the following would be a vendor responsibility in this scenario?

A：维护管理程序

Maintaining the hypervisor

B：管理操作系统安全设置

Managing operating system security settings

C：维护主机防火墙

Maintaining the host firewall

D：配置服务器访问控制

Configuring server access control

答案:在基础架构即服务（IaaS）的云计算环境中，供应商和客户之间的责任划分是明确的。供应商通常负责底层的基础设施，而客户则负责操作系统及以上的管理。

选项分析：

A：维护管理程序（Maintaining the hypervisor）

- 这是供应商的责任。管理程序（hypervisor）是虚拟化技术的核心，负责管理虚拟机的创建、运行和资源分配。供应商需要确保管理程序的正常运行和安全性。

B：管理操作系统安全设置（Managing operating system security settings）

- 这是客户的责任。在IaaS模型中，客户负责管理操作系统及其安全设置，包括补丁更新、用户权限管理等。

C：维护主机防火墙（Maintaining the host firewall）

- 这是供应商的责任。主机防火墙通常由供应商管理，以确保底层基础设施的安全。

D：配置服务器访问控制（Configuring server access control）

- 这是客户的责任。客户需要根据自身需求配置服务器的访问控制策略，例如用户权限、网络访问控制等。

因此，正确答案是 \*\*A：维护管理程序（Maintaining the hypervisor）\*\*。

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

题目53：Ben事先记录数据，然后在测试网站上重播它，通过真实的生产负荷来验证这些数据是如何工作的，他进行什么类型的性能监控？

When Ben records data and then replays it against his test website to verify how it performs based on a real production workload, what type of performance monitoring is he undertaking?

A：被动

Passive

B：主动

Proactive

C：反应

Reactive

D：重放

Replay

答案:题目中描述的是Ben通过记录数据并在测试网站上重播这些数据，以验证网站在真实生产负荷下的性能。这种方法是通过模拟真实的生产环境来主动测试和监控系统的性能，因此属于主动性能监控。

正确答案是：

B：主动

Proactive

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

题目54：Kailey正在审查她的组织维护的一组旧记录，并希望安全地处理它们。她不确定该组织应将记录保留多长时间，因为它们涉及税务数据。Kailey如何确定是否可以处置这些记录

Kailey is reviewing a set of old records maintained by her organization and wants to dispose of them securely. She is unsure how long the organization should keep the records because they involve tax data. How can Kailey determine whether the records may be disposed?

A：咨询组织的记录保留策略

Consult the organization's records retention policy.

B：咨询IRS的要求

Consult IRS requirements.

C：保留记录至少七年

Retain the records for at least seven years.

D：永久保留记录

Retain the records permanently.

答案:Kailey 需要确定她的组织是否可以安全地处理涉及税务数据的旧记录。为了做出这个决定，她应该考虑以下几点：

A. 咨询组织的记录保留策略：组织的内部政策通常会规定不同类型记录的保留期限。这些政策通常是根据法律要求和行业最佳实践制定的。

B. 咨询IRS的要求：美国国税局（IRS）对税务记录的保留有具体的要求。根据IRS的规定，通常建议保留税务记录至少七年，以便在审计或税务争议时提供支持。

C. 保留记录至少七年：这是一个常见的建议，因为IRS通常有七年的时间限制来审计税务记录。然而，具体的保留期限可能因情况而异。

D. 永久保留记录：虽然某些记录可能需要永久保留，但这通常不适用于所有税务记录。永久保留可能会增加存储成本和管理复杂性。

综合考虑，Kailey 应该首先 \*\*咨询组织的记录保留策略\*\*（选项A），因为这通常会考虑到法律要求和组织的具体需求。如果组织的政策不明确或没有涵盖税务记录，她应该 \*\*咨询IRS的要求\*\*（选项B），以确保符合法律规定。

因此，最佳答案是 \*\*A：咨询组织的记录保留策略\*\* 和 \*\*B：咨询IRS的要求\*\*。

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

题目55：Alan正在考虑在其组织中使用新的身份证，用于物理访问控制。他看到一种样品卡，但不确定该卡使用的技术。因此他打开卡片，看到了以下内部结构。这是什么类型的卡？

Alan is considering the use of new identification cards in his organization that will be used for physical access control. He comes across a sample card and is unsure of the technology. He breaks it open and sees the following internal construction. What type of card is this?

<div style="text-align:center"><img alt="" height="479" src="/file/100000/m/20210823/74d528e84057422a8750f89a26c22f9d.png" width="593" /></div>

A：智能卡

Smart card

B：感应卡

Proximity card

C：磁条

Magnetic stripe

D：相二卡

Phase-two card

答案:根据题目描述和图片，Alan打开的卡片内部结构显示了一个线圈和一个小芯片。这种结构是感应卡（Proximity Card）的典型特征。感应卡通常用于物理访问控制，通过无线电频率识别（RFID）技术进行通信。

因此，正确答案是：

B：感应卡

Proximity card

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

题目56：Mark计划为他的组织进行灾难恢复测试。他想对灾难恢复设施进行实时测试，但不想干扰主要设施的运行。Mark 应该选择什么类型的测试？

Mark is planning a disaster recovery test for his organization. He would like to perform a live test of the disaster recovery facility but does not want to disrupt operations at the primary facility. What type of test should Mark choose?

A：全中断测试

Full interruption test

B：清单审查

Checklist review

C：并行测试

Parallel test

D：桌面练习

Tabletop exercise

答案:Mark 应该选择 \*\*C：并行测试\*\*。

并行测试（Parallel test）是一种灾难恢复测试方法，在这种测试中，灾难恢复设施和主要设施同时运行。通过这种方式，Mark 可以在不影响主要设施正常运行的情况下，验证灾难恢复设施的功能和性能。并行测试允许组织在实际环境中测试恢复流程，而不会对日常业务造成干扰。

其他选项的解释：

- \*\*A：全中断测试\*\*（Full interruption test）会中断主要设施的运行，这可能会对业务造成影响，因此不符合Mark的需求。

- \*\*B：清单审查\*\*（Checklist review）是一种文档化的审查过程，不涉及实际操作，无法验证灾难恢复设施的实际功能。

- \*\*D：桌面练习\*\*（Tabletop exercise）是一种模拟演练，通常不涉及实际操作，主要用于讨论和验证恢复计划，无法进行实时测试。

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

题目57：下列哪一项不是软件开发的敏捷方法原则？

Which one of the following is not a principle of the Agile approach to software development?

A：最好的架构、要求和设计源于自组织团队

The best architecture, requirements, and designs emerge from self-organizing teams.

B：不经常提供工作软件，强调的是在跨度更大的时间段创建准确的代码

Deliver working software infrequently, with an emphasis on creating accurate code over longer timelines.

C：欢迎不断变化的需求，甚至在开发过程的后期

Welcome changing requirements, even late in the development process.

D：简单是至关重要的

Simplicity is essential.

答案:题目57的正确答案是：

B：不经常提供工作软件，强调的是在跨度更大的时间段创建准确的代码

Deliver working software infrequently, with an emphasis on creating accurate code over longer timelines.

解释：

敏捷开发方法强调频繁地交付工作软件，通常以较短的迭代周期（如2-4周）进行。这与选项B中描述的“不经常提供工作软件”相矛盾。敏捷方法的核心原则之一是持续交付可用的软件，以便快速获得反馈并进行调整。因此，选项B不符合敏捷开发的原则。

其他选项（A、C、D）都是敏捷开发方法的核心原则：

- A：自组织团队能够产生最好的架构、需求和设计。

- C：敏捷方法欢迎需求的变化，即使在开发后期。

- D：简单性是敏捷开发的重要原则之一。

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

题目58：在安全审计期间，Susan发现组织正使用手形几何扫描仪作为其安全数据中心的访问控制机制。Susan应该对手形几何扫描仪的使用提出什么建议？

During a security audit, Susan discovers that the organization is using hand geometry scanners as the access control mechanism for their secure data center. What recommendation should Susan make about the use of hand geometry scanners?

A：该项技术的FRR比较高，应该换成其他技术

They have a high FRR and should be replaced.

B：应该添加第二个因素，因为该项技术不能可靠地区分个体

A second factor should be added because they are not a good way to reliably distinguish individuals.

C：手形几何扫描仪为数据中心提供适当的安全性，应考虑用于其他高安全性领域

The hand geometry scanners provide appropriate security for the data center and should be considered for other high-security areas.

D：可能产生安全访问问题，应考虑备用的生物识别系统

They may create accessibility concerns, and an alternate biometric system should be considered.

答案:在安全审计期间，Susan发现组织使用手形几何扫描仪作为安全数据中心的访问控制机制。手形几何扫描仪是一种生物识别技术，它通过扫描和记录手形特征来验证个人身份。然而，这种技术可能不是最可靠或最安全的访问控制方法，特别是在高安全性的环境中。

选项分析：

A：该项技术的FRR（False Rejection Rate，错误拒绝率）比较高，应该换成其他技术。这个选项指出手形几何扫描仪的FRR较高，可能导致合法用户被错误拒绝访问。这是一个合理的考虑，因为高FRR会影响用户体验和操作效率。

B：应该添加第二个因素，因为该项技术不能可靠地区分个体。这个选项建议增加第二个认证因素（如密码、智能卡等），以提高安全性。多因素认证（MFA）是提高安全性的有效方法，特别是在生物识别技术可能不够可靠的情况下。

C：手形几何扫描仪为数据中心提供适当的安全性，应考虑用于其他高安全性领域。这个选项认为手形几何扫描仪已经提供了足够的安全性，并建议在其他高安全性领域也使用这种技术。然而，这可能忽略了手形几何扫描仪的潜在局限性。

D：可能产生安全访问问题，应考虑备用的生物识别系统。这个选项指出手形几何扫描仪可能存在访问问题，并建议考虑其他生物识别系统。这也是一个合理的建议，因为不同的生物识别技术有不同的优缺点，选择最适合的技术可以提高安全性。

综合考虑，选项B是最合适的建议。增加第二个认证因素可以显著提高安全性，特别是在手形几何扫描仪可能不够可靠的情况下。多因素认证是当前安全实践中的一种常见做法，可以有效降低未经授权访问的风险。

最终答案：B：应该添加第二个因素，因为该项技术不能可靠地区分个体。

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

题目59：Colleen正为组织进行业务影响评估。哪个指标描述了组织在服务崩溃的情况下不造成巨大损害的最长时间？

Colleen is conducting a business impact assessment for her organization. What metric provides important information about the amount of time that the organization may be without a service before causing irreparable harm?

A：MTD 最大 容忍 宕机事件

MTD

B：ALE 年度 损失 期望

ALE

C：RPO 恢复 目标 点

RPO

D：RTO 恢复 时间 点

RTO

答案:在业务影响评估中，描述组织在服务崩溃的情况下不造成巨大损害的最长时间的指标是 \*\*MTD（最大容忍宕机时间，Maximum Tolerable Downtime）\*\*。

- \*\*MTD\*\* 是指组织在服务中断的情况下，能够容忍的最长时间，超过这个时间可能会导致不可挽回的损害。

- \*\*ALE（年度损失期望，Annualized Loss Expectancy）\*\* 是用于风险评估的指标，表示每年可能因特定风险事件而导致的预期损失。

- \*\*RPO（恢复点目标，Recovery Point Objective）\*\* 是指组织在灾难恢复中能够接受的数据丢失的最大时间点。

- \*\*RTO（恢复时间目标，Recovery Time Objective）\*\* 是指组织在灾难发生后，恢复到正常运营所需的时间。

因此，正确答案是：

\*\*A：MTD 最大容忍宕机事件\*\*

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

题目60：Bailey担心她组织中的用户正在云服务中使用各种敏感信息，并希望在这些服务中一致地实施安全策略。什么安全控制最适合她的需要？

Bailey is concerned that users around her organization are using sensitive information in a variety of cloud services and would like to enforce security policies consistently across those services. What security control would be best suited for her needs?

A：DRM

DRM

B：IPS

IPS

C：CASB

CASB

D：DLP

DLP

答案:题目60的正确答案是：

C：CASB

CASB（Cloud Access Security Broker，云访问安全代理）是一种安全控制工具，专门用于管理和保护组织在云服务中的数据和应用程序。CASB可以帮助Bailey在多个云服务中一致地实施安全策略，监控用户活动，防止数据泄露，并确保敏感信息的安全。它提供了对云服务的可见性、数据保护、威胁防护和合规性管理等功能，非常适合Bailey的需求。

其他选项的解释：

- A：DRM（数字版权管理）主要用于保护数字内容的版权，不适用于云服务中的安全策略实施。

- B：IPS（入侵防御系统）主要用于检测和阻止网络攻击，不直接涉及云服务中的安全策略管理。

- D：DLP（数据丢失防护）主要用于防止敏感数据泄露，虽然与数据保护相关，但不具备CASB在多个云服务中统一实施安全策略的能力。

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

题目61：Matt正在为他的组织设计一套信息处理需求，并希望借鉴常见的行业实践。Matt应该实施以下哪些实践？（选择所有符合条件的）

Matt is designing a set of information handling requirements for his organization and would like to draw upon common industry practices. Which of the following practices should Matt implement? (Select all that apply.)

A：用分类级别标记纸质和电子文档

Labeling both paper and electronic documents with their classification level

B：自动授予高级管理人员对所有机密信息的完全访问权限

Automatically granting senior executives full access to all classified information

C：自动授予访问者访问敏感度最低级别信息的权限

Automatically granting visitors access to information classified at the lowest level of sensitivity

D：加密存储和静止的敏感信息

Encrypting sensitive information in storage and at rest

答案:在设计信息处理需求时，Matt应该考虑实施以下实践：

A：用分类级别标记纸质和电子文档

- 这是一个常见的行业实践，有助于确保信息的安全性和适当的访问控制。通过标记文档的分类级别，可以帮助员工了解信息的敏感程度，并采取相应的保护措施。

D：加密存储和静止的敏感信息

- 加密是保护敏感信息的重要手段，尤其是在信息存储和静止状态下。加密可以防止未经授权的访问，确保即使数据被窃取，也无法轻易解读。

B和C选项不建议实施：

- B：自动授予高级管理人员对所有机密信息的完全访问权限

- 这种做法可能会导致信息泄露的风险增加，因为即使是高级管理人员，也不一定需要访问所有机密信息。访问权限应根据工作需要来分配，而不是自动授予。

- C：自动授予访问者访问敏感度最低级别信息的权限

- 即使是敏感度最低的信息，也不应自动授予访问者访问权限。访问者应经过适当的身份验证和授权程序，以确保他们有权访问这些信息。

因此，Matt应选择A和D作为实施的信息处理实践。

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

题目62：Jerry正在调查一次攻击，攻击者从用户的Web会话中窃取身份验证令牌，并使用它来冒充网站上的用户。哪项术语最能描述这种攻击？

Jerry is investigating an attack where the attacker stole an authentication token from a use's web session and used it to impersonate the user on the site. What term best describes this attack?

A：伪装

Masquerading

B：重放

Replay

C：欺骗

Spoofing

D：篡改

Modification

答案:这种攻击最合适的术语是 \*\*B：重放 (Replay)\*\*。

\*\*重放攻击 (Replay Attack)\*\* 是指攻击者截获并重复使用有效的身份验证令牌或会话信息，以冒充合法用户。在这种情况下，攻击者窃取了用户的身份验证令牌，并在后续的请求中使用该令牌来冒充用户，从而获得对系统的访问权限。

其他选项的解释：

- \*\*A：伪装 (Masquerading)\*\*：通常指攻击者伪装成另一个用户或系统，但不特指通过重放令牌的方式。

- \*\*C：欺骗 (Spoofing)\*\*：通常指伪造数据包或身份信息，但不特指重放攻击。

- \*\*D：篡改 (Modification)\*\*：指对数据进行修改，与重放攻击无关。

因此，\*\*B：重放 (Replay)\*\* 是最准确的描述。

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

题目63：Lisa需要与一家采用OAuth 2.0的云身份认证提供商进行对接，且需要选择一套合适的认证框架。下列哪项最符合她的需求？

Lisa wants to integrate with a cloud identity provider that uses OAuth 2.0, and she wants to select an appropriate authentication framework. Which of the following best suits her needs?

A：OpenID Connect

OpenID Connect

B：SAML

SAML

C：RADIUS

RADIUS

D：Kerberos

Kerberos

答案:题目要求Lisa选择一个适合与使用OAuth 2.0的云身份认证提供商对接的认证框架。我们需要分析每个选项的适用性：

A. \*\*OpenID Connect\*\*

OpenID Connect是基于OAuth 2.0的身份认证协议，专门用于身份验证和用户信息交换。它与OAuth 2.0兼容，并且是云身份认证提供商的常见选择。因此，OpenID Connect是最符合Lisa需求的选项。

B. \*\*SAML\*\*

SAML（安全断言标记语言）是一种基于XML的协议，主要用于单点登录（SSO）。虽然SAML也可以用于身份认证，但它与OAuth 2.0不直接兼容，因此不是最佳选择。

C. \*\*RADIUS\*\*

RADIUS（远程认证拨号用户服务）是一种用于网络访问控制的协议，通常用于VPN或Wi-Fi认证。它与OAuth 2.0不兼容，因此不适合Lisa的需求。

D. \*\*Kerberos\*\*

Kerberos是一种基于票据的身份认证协议，主要用于企业内部网络的身份验证。它与OAuth 2.0不兼容，因此也不适合Lisa的需求。

\*\*正确答案是A：OpenID Connect\*\*。

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

题目64：Owen最近设计了一种安全访问控制结构，防止单个用户同时拥有创建新供应商所需的角色和执行检查所需的角色。Owen执行什么原则？

Owen recently designed a security access control structure that prevents a single user from simultaneously holding the role required to create a new vendor and the role required to issue a check. What principle is Owen enforcing?

A：两人控制

Two-person control

B：最小特权

Least privilege

C：职责分离

Separation of duties

D：工作轮换

Job rotation

答案:Owen设计的访问控制结构防止单个用户同时拥有创建新供应商和执行检查所需的角色，这体现了职责分离的原则。职责分离（Separation of Duties, SoD）是一种安全控制措施，旨在通过将关键任务和权限分配给不同的个体或角色，以减少欺诈、错误和滥用的风险。通过确保没有单个用户能够控制整个流程的关键部分，可以增加系统的安全性和完整性。

因此，正确答案是：

C：职责分离

Separation of duties

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

题目65：Denise 正为公司和软件供应商之间的合同纠纷审判做准备。供应商声称Denise凭借一份口头协议，修改了他们的书面合同。Denise 在辩护中应该提出了什么证据规则？

Denise is preparing for a trial relating to a contract dispute between her company and a software vendor. The vendor is claiming that Denise made a verbal agreement that amended their written contract. What rule of evidence should Denise raise in her defense?

A：真实证据规则

Real evidence rule

B：最佳证据规则

Best evidence rule

C：口头证据规则

Parol evidence rule

D：证词证据规则

Testimonial evidence rule

答案:在合同纠纷中，如果一方声称存在口头协议修改了书面合同，另一方可以引用“口头证据规则”（Parol Evidence Rule）来辩护。口头证据规则是一项法律原则，旨在防止当事人在书面合同之外引入口头或书面证据来修改或解释书面合同的条款，除非这些证据用于澄清合同的模糊之处、证明合同无效或存在欺诈、错误等情况。

因此，Denise 在辩护中应该提出“口头证据规则”（Parol Evidence Rule）来阻止供应商引入口头协议作为修改书面合同的证据。

正确答案是：

C：口头证据规则

Parol evidence rule

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

题目66：当Lauren在监控网络连接的两端流量时，她发现公共IP地址的入站流量出现在生产网络中。 它流向具有RFC 1918保留目标地址的内部主机。她应该希望在网络边界使用什么技术？

While Lauren is monitoring traffic on two ends of a network connection, she sees traffic that is inbound to a public IP address show up inside the production network. It is headedfor an internal host with an RFC 1918 reserved destinationaddress. What technology should she expect is in use at the network border?

A：NAT

NAT

B：VLAN

VLAN

C：S/NAT

S/NAT

D：BGP

BGP

答案:当Lauren在监控网络连接的两端流量时，她发现公共IP地址的入站流量出现在生产网络中，并且这些流量流向具有RFC 1918保留目标地址的内部主机。这种情况表明网络边界可能使用了网络地址转换（NAT）技术。

NAT（Network Address Translation）是一种将私有IP地址转换为公共IP地址的技术，通常用于允许内部网络中的设备使用私有IP地址访问外部网络（如互联网）。RFC 1918定义了私有IP地址范围，这些地址在互联网上是不可路由的，因此需要通过NAT进行转换。

因此，Lauren应该期望在网络边界使用的是NAT技术。

正确答案是：

A：NAT

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

题目67：以下哪些关于SSAE-18的陈述是正确的？（选择所有适用的选项）

Which of the following statements about SSAE-18 are correct? (Select all that apply.)

A：它规定了一个特定的控制集

It mandates a specific control set.

B：它是一个证明标准

It is an attestation standard.

C：它用于外部审计

It is used for external audits.

D：它使用一个包括SOC 1、SOC 2和SOC 3报告的框架

It uses a framework, including SOC 1, SOC 2, and SOC 3 reports.

答案:关于SSAE-18（Statement on Standards for Attestation Engagements No. 18）的正确陈述是：

B：它是一个证明标准

It is an attestation standard.

C：它用于外部审计

It is used for external audits.

D：它使用一个包括SOC 1、SOC 2和SOC 3报告的框架

It uses a framework, including SOC 1, SOC 2, and SOC 3 reports.

解释：

- SSAE-18 是一个由美国注册会计师协会（AICPA）制定的证明标准，用于指导注册会计师在提供证明服务时的行为。因此，选项B是正确的。

- SSAE-18 通常用于外部审计，特别是当服务组织需要向用户组织提供关于其控制环境的保证时。因此，选项C是正确的。

- SSAE-18 使用一个框架，包括SOC 1、SOC 2和SOC 3报告，这些报告用于不同的目的和不同的用户群体。因此，选项D是正确的。

选项A是不正确的，因为SSAE-18并不规定一个特定的控制集。它提供了一个框架，用于评估和报告服务组织的控制环境，但具体的控制集取决于组织的特定需求和环境。

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

题目68：Elliott正在使用非对称密码系统，并希望为消息中添加数字签名。他应该使用什么密钥来加密消息摘要？

Elliott is using an asymmetric cryptosystem and would like to add a digital signature to a message. What key should he use to encrypt the message digest?

A：Elliott的私钥

Elliott's private key

B：Elliott的公钥

Elliott's public key

C：接收者的私钥

Recipient's private key

D：接收者的公钥

Recipient's public key

答案:在非对称密码系统中，数字签名用于验证消息的完整性和真实性。数字签名的生成过程通常包括以下步骤：

1. \*\*生成消息摘要\*\*：首先，Elliott会对消息进行哈希处理，生成一个消息摘要（也称为哈希值）。

2. \*\*加密消息摘要\*\*：然后，Elliott会使用自己的私钥对这个消息摘要进行加密，生成数字签名。

3. \*\*发送消息和签名\*\*：Elliott将原始消息和数字签名一起发送给接收者。

接收者在收到消息和签名后，可以使用Elliott的公钥来解密数字签名，得到消息摘要。然后，接收者会对原始消息进行哈希处理，生成一个新的消息摘要，并将其与解密得到的消息摘要进行比较。如果两者一致，说明消息确实来自Elliott，并且在传输过程中没有被篡改。

因此，Elliott应该使用自己的私钥来加密消息摘要，以生成数字签名。

正确答案是：

\*\*A：Elliott的私钥\*\*

Elliott's private key

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

题目69：Greg正为组织制定灾难恢复计划，并希望确定在中断后恢复特定IT服务所需的时间。Greg计算的是什么变量？

Greg is building a disaster recovery plan for his organization and would like to determine the amount of time that it should take to restore a particular IT service after an outage. What variable is Greg calculating?

A：MTD 最大 容忍 宕机事件

MTD

B：RTO 恢复 时间 目标

RTO

C：RPO 恢复 点 目标

RPO

D：SLA 水平服务协议

SLA

答案:Greg正在计算的变量是 \*\*B：RTO 恢复时间目标\*\*。

\*\*RTO（Recovery Time Objective）\*\* 是指在灾难或中断发生后，恢复到正常运营所需的时间目标。Greg希望确定在中断后恢复特定IT服务所需的时间，这正是RTO的定义。

其他选项的解释：

- \*\*A：MTD（Maximum Tolerable Downtime）\*\* 是指系统或服务可以容忍的最大停机时间。

- \*\*C：RPO（Recovery Point Objective）\*\* 是指在灾难恢复过程中，数据可以恢复到的时间点，即数据丢失的最大容忍量。

- \*\*D：SLA（Service Level Agreement）\*\* 是服务提供商和客户之间的协议，规定了服务的质量标准和责任。

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

题目70：在对系统进行修改之前，哪项业务流程通常需要管理员签字同意？

What business process typically requires sign-off from a manager before modifications are made to a system?

A：SDN

SDN

B：发布管理

Release management

C：变更管理

Change management

D：版本控制

Versioning

答案:正确答案是 C：变更管理 (Change management)。

变更管理是一个正式的过程，用于控制对系统、应用程序或基础设施的修改。在变更管理过程中，通常需要管理员或相关负责人的签字同意，以确保变更的必要性、风险评估以及变更后的影响得到充分评估和控制。这样可以减少变更带来的潜在风险，并确保系统的稳定性和可靠性。

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

题目71：Jen正在为其组织的数据中心选择灭火系统，并希望缩小候选名单的范围。以下哪种抑制系统最不适合使用？

Jen is selecting a fire suppression system for her organization's data center and would like to narrow down the list of candidates. Which one of the following suppression systems would be LEAST appropriate for use?

A：干管

Dry pipe

B：湿管

Wet pipe

C：预作用

Pre-action

D：FM-200

FM-200

答案:在选择数据中心的灭火系统时，需要考虑多个因素，包括系统的可靠性、对设备的潜在损害、以及系统的响应速度等。对于数据中心来说，保护电子设备和数据不受损害是至关重要的。

A. 干管系统（Dry pipe）：这种系统在管道中充满压缩空气，当火灾发生时，空气被释放，水才会流入管道并喷出。这种系统适用于可能冻结的环境，但在数据中心中使用可能会因为延迟喷水而增加火灾损害。

B. 湿管系统（Wet pipe）：这种系统管道中始终充满水，一旦检测到火灾，水会立即喷出。虽然响应速度快，但在数据中心中使用可能会因为水损害电子设备而不适合。

C. 预作用系统（Pre-action）：这种系统结合了干管和湿管系统的特点，需要两个独立的触发条件才会释放水。这种系统在数据中心中较为常见，因为它减少了误操作的风险，并且只有在确认火灾后才会释放水，从而减少水损害的风险。

D. FM-200：这是一种气体灭火系统，使用化学气体来抑制火灾，不会留下残留物，对电子设备无害。这种系统非常适合数据中心，因为它可以快速灭火且不会损害敏感的电子设备。

综合考虑，湿管系统（B）最不适合数据中心使用，因为它可能会因为水损害电子设备。而FM-200（D）是最适合的选择，因为它可以快速有效地灭火且不会对设备造成损害。

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

题目72：Chris工作的公司在每道门上张贴通知，提醒员工要小心，要求他们不允许其他人进入。这是哪种类型的控制？

The company Chris works for has notifications posted at each door reminding employees to be careful to not allow people to enter when they do. Which type of control is this?

A：探测

Detective

B：物理

Physical

C：预防

Preventive

D：指示

Directive

答案:这道题目是关于不同类型的控制措施的分类。题目描述的情况是公司在每道门上张贴通知，提醒员工要小心，不允许其他人进入。这是一种通过指示或指导来防止未经授权的人员进入的控制措施。

选项分析如下：

A. 探测（Detective）：这种控制措施通常用于检测已经发生的事件或行为，例如监控摄像头或审计日志。题目中的情况并不涉及检测已发生的事件，因此不符合。

B. 物理（Physical）：这种控制措施涉及物理屏障或设备，例如锁、门禁系统等。题目中的通知并不是物理屏障，因此不符合。

C. 预防（Preventive）：这种控制措施旨在防止事件的发生，例如密码保护或防火墙。虽然通知的目的是防止未经授权的人员进入，但它并不是一种技术或物理上的预防措施。

D. 指示（Directive）：这种控制措施通过指示或指导来引导行为，例如政策、程序或通知。题目中的通知正是通过指示员工来防止未经授权的人员进入，因此符合。

因此，正确答案是 D：指示（Directive）。

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

题目73：Seth在为他的组织正在建造的新设施设计物理安全控制。他想尽可能地阻止攻击。以下哪些控制可以起到威慑作用？（选择所有符合条件的）

Seth is designing the physical security controls for a new facility being constructed by his organization. He would like to deter attacks to the extent possible. Which of the following controls serve as deterrents? (Select all that apply.)

A：运动探测器

Motion detectors

B：看门狗

Guard dogs

C：陷阱

Mantraps

D：照明

Lighting

答案:在物理安全控制中，威慑作用是指通过可见的措施或设备来阻止潜在的攻击者尝试入侵或破坏。以下选项分析：

A：运动探测器 - 运动探测器主要用于检测入侵者的活动并触发警报，但它们通常是隐蔽的，不会直接起到威慑作用。

B：看门狗 - 看门狗是一种非常有效的威慑手段，因为它们的存在和潜在的攻击性可以阻止潜在的攻击者接近设施。

C：陷阱 - 陷阱通常用于捕获或限制入侵者的行动，但它们通常是隐蔽的，不会直接起到威慑作用。

D：照明 - 良好的照明可以显著提高设施的可见性，使潜在的攻击者感到容易被发现，从而起到威慑作用。

因此，可以起到威慑作用的控制是：

B：看门狗

D：照明

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

题目74：Thomas最近签署了一项关于无服务器计算环境的协议，他所在组织的开发人员将能够在该环境中用Python编写函数，并将它们部署到云提供商的服务器上以供执行。云提供商将管理服务器。什么术语最能描述这个模型？

Thomas recently signed an agreement for a serverless computing environment where his organization's developers will be able to write functions in Python and deploy them on the cloud provider's servers for execution. The cloud provider will manage the servers. What term best describes this model?

A：SaaS

SaaS

B：PaaS

PaaS

C：IaaS

IaaS

D：容器化

Containerization

答案:这个模型最能描述的是 \*\*B：PaaS\*\*（Platform as a Service）。

\*\*解释：\*\*

- \*\*SaaS（Software as a Service）\*\* 是指通过互联网提供软件应用程序的服务，用户通常通过浏览器访问这些应用程序，而不需要管理底层的基础设施。

- \*\*PaaS（Platform as a Service）\*\* 提供了一个平台，允许开发者在云环境中编写、部署和管理应用程序，而无需管理底层的基础设施（如服务器、存储等）。开发者只需专注于编写代码，云提供商会处理服务器的管理和维护。

- \*\*IaaS（Infrastructure as a Service）\*\* 提供虚拟化的计算资源，如虚拟机、存储和网络，用户需要自己管理操作系统、应用程序等。

- \*\*容器化\*\* 是一种将应用程序及其依赖项打包在一起的技术，通常用于简化部署和管理，但它本身并不是一种服务模型。

在这个场景中，Thomas的开发者只需编写Python函数并部署到云提供商的服务器上，云提供商负责管理服务器，这符合PaaS的定义。

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

题目75：攻击者截获了大量使用相同算法和加密密钥的加密数据。在没有更多信息的情况下，以下哪些密码分析攻击是可能的？（选择所有符合条件的）

An attacker has intercepted a large amount of data that was all encrypted with the same algorithm and encryption key. With no further information, which of the following cryptanalytic attacks are possible? (Select all that apply.)

A：已知明文

Known plaintext

B：选择密文

Chosen ciphertext

C：频率分析

Frequency analysis

D：暴力破解

Brute-force

答案:在攻击者截获了大量使用相同算法和加密密钥的加密数据的情况下，以下密码分析攻击是可能的：

A：已知明文 (Known plaintext)

- 如果攻击者知道部分明文和对应的密文，他们可以利用这些信息来推断加密密钥或算法的工作原理。然而，题目中没有提到攻击者是否知道任何明文，因此这个选项不一定适用。

B：选择密文 (Chosen ciphertext)

- 这种攻击需要攻击者能够选择特定的密文并获取对应的明文。题目中没有提到攻击者能够选择密文或获取对应的明文，因此这个选项不适用。

C：频率分析 (Frequency analysis)

- 如果加密算法是某种经典加密算法（如替换密码或移位密码），攻击者可以通过分析密文中字符或模式的频率来推断明文。然而，现代加密算法（如AES）通常对频率分析具有抵抗力。题目中没有说明使用的是哪种加密算法，因此这个选项可能适用，但取决于具体的加密算法。

D：暴力破解 (Brute-force)

- 如果加密密钥的长度较短，攻击者可以通过尝试所有可能的密钥来破解加密数据。暴力破解是一种通用的攻击方法，适用于任何加密算法，但它的效率取决于密钥的长度和计算资源。

综上所述，最有可能适用的攻击是 \*\*C：频率分析\*\* 和 \*\*D：暴力破解\*\*。

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

题目76-1：请参考以下场景,回答3个问题：

Alex已经在大学工作10年以上。在那段时间，他一直是一个系统管理员和数据库管理员，在大学的服务台工作。他现在是运行大学Web应用程序的团队经理。使用此处显示的配置图，回答以下问题。

<div style="text-align:center"><img alt="" height="383" src="/file/100000/m/20210823/d3ec629547dd4093b920e28b1d1e990a.png" width="471" /></div>

For questions , please refer to the following scenario:

Alex has been with the university he works at for more than10 years. During that time, he has been a system administrator and a database administrator, and he has worked in the university's help desk. He is now a manager for the team that runs the university's web applications. Using the provisioning diagram shown here, answer the following questions.

<div style="text-align:center"><img alt="" height="513" src="/file/100000/m/20210823/842fe14377d14061a38a71099d6daf05.png" width="689" /></div>

如果Alex雇用一名新员工，并且HR根据Alex提供的一系列表单手动将信息输入配置系统，成功配置了该员工的账户，这里发生了哪种类型的配置？

If Alex hires a new employee and the employee's account is provisioned after HR manually inputs information into the provisioning system based on data Alex provides via a series of forms, what type of provisioning has occurred?

A：自主账户配置

Discretionary account provisioning

B：基于工作流的账户配置

Workflow-based account provisioning

C：自动账户配置

Automated account provisioning

D：自助账户配置

Self-service account provisioning

答案:在这个场景中，HR根据Alex提供的信息手动输入到配置系统中，然后成功配置了员工的账户。这个过程涉及到人工干预和手动操作，而不是完全自动化的过程。因此，这里发生的配置类型是：

\*\*B：基于工作流的账户配置 (Workflow-based account provisioning)\*\*

基于工作流的账户配置通常涉及多个步骤和人工干预，特别是在信息需要经过不同部门或人员的审核和输入时。在这个例子中，HR根据Alex提供的信息手动输入数据，这符合基于工作流的配置过程。

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

题目76-1：请参考以下场景,回答3个问题：

Alex已经在大学工作10年以上。在那段时间，他一直是一个系统管理员和数据库管理员，在大学的服务台工作。他现在是运行大学Web应用程序的团队经理。使用此处显示的配置图，回答以下问题。

<div style="text-align:center"><img alt="" height="383" src="/file/100000/m/20210823/d3ec629547dd4093b920e28b1d1e990a.png" width="471" /></div>

For questions , please refer to the following scenario:

Alex has been with the university he works at for more than10 years. During that time, he has been a system administrator and a database administrator, and he has worked in the university's help desk. He is now a manager for the team that runs the university's web applications. Using the provisioning diagram shown here, answer the following questions.

<div style="text-align:center"><img alt="" height="513" src="/file/100000/m/20210823/842fe14377d14061a38a71099d6daf05.png" width="689" /></div>

Alex可以访问图中的B、C和D。他应该向大学的身份管理团队提出什么问题？

Alex has access to B, C, and D in the diagram. What concern should he raise to the university's identity management team?

A：配置系统没有给他所需的权利

The provisioning process did not give him the rights he needs.

B：他有过多的特权

He has excessive privileges.

C：特权蠕变可能正在发生

Privilege creep may be taking place.

D：日志未正确启用

Logging is not properly enabled.

答案:根据题目描述，Alex已经在大学工作了10年以上，并且担任过系统管理员、数据库管理员以及服务台工作。现在他是运行大学Web应用程序的团队经理。根据配置图，Alex可以访问图中的B、C和D。

考虑到Alex的职责和权限，他应该关注的是他是否有过多的权限，或者是否存在权限逐渐增加的情况。这种情况被称为“特权蠕变”（Privilege Creep），即用户随着时间的推移逐渐积累了超出其工作职责所需的权限。这可能会导致安全风险，因为过多的权限可能会被滥用或导致系统漏洞。

因此，Alex应该向大学的身份管理团队提出的问题是：

\*\*C：特权蠕变可能正在发生\*\*

\*\*Privilege creep may be taking place.\*\*

这个选项最符合Alex的情况，因为他已经积累了多个角色的权限，并且现在担任管理职位，可能会继续获得更多的权限。

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

题目76-1：请参考以下场景,回答3个问题：

Alex已经在大学工作10年以上。在那段时间，他一直是一个系统管理员和数据库管理员，在大学的服务台工作。他现在是运行大学Web应用程序的团队经理。使用此处显示的配置图，回答以下问题。

<div style="text-align:center"><img alt="" height="383" src="/file/100000/m/20210823/d3ec629547dd4093b920e28b1d1e990a.png" width="471" /></div>

For questions , please refer to the following scenario:

Alex has been with the university he works at for more than10 years. During that time, he has been a system administrator and a database administrator, and he has worked in the university's help desk. He is now a manager for the team that runs the university's web applications. Using the provisioning diagram shown here, answer the following questions.

<div style="text-align:center"><img alt="" height="513" src="/file/100000/m/20210823/842fe14377d14061a38a71099d6daf05.png" width="689" /></div>

当Alex改变角色时，应该发生什么？

When Alex changes roles, what should occur?

A：他应该被取消配置，并创建一个新账户

He should be de-provisioned, and a new account should be created.

B：他应该将他的新权利添加到他现有账户

He should have his new rights added to his existing account.

C：他应该只能得到与他角色相匹配的权利

He should be provisioned for only the rights that match his role.

D：他的权利应该与他所替代的员工权利相匹配

He should have his rights set to match those of the person he is replacing.

答案:根据题目描述，Alex已经在大学工作了10年以上，并且他的角色发生了变化。他现在是运行大学Web应用程序的团队经理。在这种情况下，应该根据他的新角色来调整他的权限。

选项分析：

- \*\*A\*\*：他应该被取消配置，并创建一个新账户。这个选项不太合适，因为Alex已经在系统中有一个账户，没有必要创建一个新账户。

- \*\*B\*\*：他应该将他的新权利添加到他现有账户。这个选项也不太合适，因为仅仅添加新权利可能会导致他保留旧角色的权限，这可能会带来安全风险。

- \*\*C\*\*：他应该只能得到与他角色相匹配的权利。这个选项是最合适的，因为Alex的新角色是团队经理，他应该只拥有与这个角色相匹配的权限，以确保他只能访问和操作与他职责相关的内容。

- \*\*D\*\*：他的权利应该与他所替代的员工权利相匹配。这个选项不适用，因为题目中没有提到Alex是替代了某个员工。

因此，最合适的答案是 \*\*C\*\*：他应该只能得到与他角色相匹配的权利。

\*\*答案：C\*\*

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

题目77：Robert正在审查根据共同标准分配了EAL2评估保证级别的系统。他对系统的最高保证是什么？

Robert is reviewing a system that has been assigned the EAL2 evaluation assurance level under the Common Criteria. What is the highest level of assurance that he may have about the system?

A：它已经完成了功能测试

It has been functionally tested.

B：它已经完成了结构测试

It has been structurally tested.

C：它已经完成了正式的验证、设计和测试

It has been formally verified, designed, and tested.

D：它已经半正式地完成了设计和测试

It has been semiformally designed and tested.

答案:根据共同标准（Common Criteria），EAL2（评估保证级别2）是一个相对较低的保证级别。EAL2主要关注功能测试和结构测试，但并不涉及正式的验证或设计。因此，Robert对系统的最高保证是系统已经完成了功能测试和结构测试。

选项A和B都提到了功能测试和结构测试，但题目要求选择最高保证，因此需要选择涵盖这两者的选项。然而，选项C和D提到的正式验证和半正式设计测试超出了EAL2的范围。

因此，最合适的答案是：

\*\*A：它已经完成了功能测试\*\*

\*\*It has been functionally tested.\*\*

这个选项最符合EAL2的保证级别，因为它主要关注功能测试。

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

题目78：Adam正在处理对最终用户的访问请求。在授予访问权限之前，他还应该验证哪两项？

Adam is processing an access request for an end user. What two items should he verify before granting the access?

A：分离和需知

Separation and need to know

B：许可和认可

Clearance and endorsement

C：许可和需知

Clearance and need to know

D：第二因素和许可

Second factor and clearance

答案:在授予访问权限之前，Adam应该验证的两项是：

C：许可和需知

Clearance and need to know

解释：

- \*\*许可（Clearance）\*\*：确保用户具有适当的权限级别来访问特定的资源或信息。这通常涉及到用户的身份验证和权限级别检查。

- \*\*需知（Need to Know）\*\*：确保用户确实需要访问特定的信息或资源来完成其工作。即使一个用户有权限访问某些信息，但如果他们不需要这些信息来完成其工作，也不应该授予访问权限。

这两个原则是信息安全中的基本概念，旨在最小化信息泄露的风险。

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

题目79：在电子发现参考模型的哪个阶段，组织应当确保潜在的可发现信息受到保护，防止该信息遭到变更或删除？

During what phase of the electronic discovery reference model does an organization ensure that potentially discoverable information is protected against alteration or deletion?

A：识别

Identification

B：保存

Preservation

C：收集

Collection

D：处理

Processing

答案:在电子发现参考模型（Electronic Discovery Reference Model, EDRM）中，组织应当确保潜在的可发现信息受到保护，防止该信息遭到变更或删除的阶段是 \*\*B：保存（Preservation）\*\*。

在保存阶段，组织需要采取法律和技术措施，确保相关数据不会被修改、删除或以其他方式被破坏。这一步骤对于确保数据的完整性和可采信性至关重要，尤其是在法律诉讼或调查过程中。

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

题目80：Dana正在选择一个散列函数用于她的组织，并希望在密码学强散列的关注方面与算法的速度、效率之间取得平衡。以下哪个散列函数最能满足她的需求？

Dana is selecting a hash function for use in her organization and would like to balance a concern for a cryptographically strong hash with the speed and efficiency of the algorithm. Which one of the following hash functions would best meet her needs?

A：MD5

MD5

B：RIPEMD

RIPEMD

C：SHA-2

SHA-2

D：SHA-3

SHA-3

答案:Dana 在选择散列函数时，需要在密码学强度与算法的速度、效率之间取得平衡。以下是对每个选项的分析：

A. \*\*MD5\*\*：

- MD5 是一种广泛使用的散列函数，但由于其已知的安全漏洞（如碰撞攻击），它不再被认为是密码学安全的。因此，MD5 不适合用于需要高安全性的场景。

B. \*\*RIPEMD\*\*：

- RIPEMD 是另一种散列函数，虽然它比 MD5 更安全，但它的使用并不广泛，且在某些情况下也存在安全漏洞。因此，RIPEMD 也不是最佳选择。

C. \*\*SHA-2\*\*：

- SHA-2 系列（包括 SHA-256 和 SHA-512）是目前广泛使用的密码学散列函数，具有较高的安全性和良好的性能。它在密码学强度和速度之间提供了良好的平衡，因此是 Dana 的最佳选择。

D. \*\*SHA-3\*\*：

- SHA-3 是最新的散列函数标准，具有与 SHA-2 相当的安全性，但其设计结构与 SHA-2 不同。虽然 SHA-3 也是安全的，但其性能在某些情况下可能不如 SHA-2。因此，SHA-3 也是一个可行的选择，但在平衡安全性和效率方面，SHA-2 更为成熟和广泛使用。

综上所述，\*\*SHA-2\*\* 是最能满足 Dana 需求的散列函数。

\*\*正确答案：C. SHA-2\*\*

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

题目81：Harry想访问Sally拥有的存储在文件服务器上的文档。将主体/客体模型应用于此场景，请问什么是资源请求的客体？

Harry would like to access a document owned by Sally stored on a file server. Applying the subject/object model to this scenario, who or what is the object of the resource request?

A：Harry

Harry

B：Sally

Sally

C：文件服务器

File server

D：文档

Document

答案:在主体/客体模型中，主体是发起请求的实体，而客体是被请求的资源或对象。在这个场景中，Harry是主体，因为他想访问文档。文档是客体，因为它是被请求的资源。

因此，正确答案是：

D：文档

Document

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

题目82：当会话层删除掉传输层发来的数据头时，会发生什么过程？

What is the process that occurs when the Session layer removes the header from data sent by the Transport layer?

A：包封

Encapsulation

B：数据包解包

Packet unwrapping

C：解封装

De-encapsulation

D：负载

Payloading

答案:当会话层删除掉传输层发来的数据头时，发生的过程是解封装（De-encapsulation）。

解封装是指在不同网络层次之间传递数据时，每一层在接收到数据后会去除掉上一层添加的头部信息，以获取实际的数据内容。在这个例子中，会话层接收到传输层发来的数据后，会去除传输层添加的头部信息，以便进一步处理数据。

因此，正确答案是：

C：解封装

De-encapsulation

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

题目83：Rob正在使用环境设计预防犯罪（CPTED）框架审查其组织的校园物理安全。 以下哪项不是此框架中的策略？

Rob is reviewing his organization's campus for physical security using the Crime Prevention Through Environmental Design (CPTED) framework. Which one of the following is NOT a strategy in this framework?

A：自然入侵检测

Natural intrusion detection

B：自然访问控制

Natural access control

C：自然监视

Natural surveillance

D：自然区域加固

Natural territorial reinforcement

答案:环境设计预防犯罪（CPTED）框架主要包括以下几个策略：

1. \*\*自然访问控制（Natural Access Control）\*\*：通过设计引导人们进入和离开空间的方式，减少犯罪机会。例如，设置明确的入口和出口，使用围栏、大门等物理障碍物。

2. \*\*自然监视（Natural Surveillance）\*\*：通过设计增加空间的可见性，使得潜在犯罪者感到被监视，从而减少犯罪。例如，使用开放式设计、良好的照明和透明的材料。

3. \*\*自然区域加固（Natural Territorial Reinforcement）\*\*：通过设计明确公共和私人空间的界限，增强居民对空间的归属感和责任感，从而减少犯罪。例如，使用标志、围栏、景观设计等。

4. \*\*维护（Maintenance）\*\*：保持环境的整洁和良好维护，传达出该区域受到关注和管理的信息，从而减少犯罪。

\*\*自然入侵检测（Natural Intrusion Detection）\*\* 并不是CPTED框架中的策略。入侵检测通常是通过技术手段（如传感器、摄像头等）来实现的，而不是通过环境设计。

因此，正确答案是：

\*\*A：自然入侵检测\*\*

\*\*Natural intrusion detection\*\*

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

题目84：什么标记语言使用请求权限、供应服务点和供应服务目标的概念来处理其核心功能？

What markup language uses the concepts of a requesting authority, a provisioning service point, and a provisioning service target to handle its core functionality?

A：SAML

SAML

B：SAMPL

SAMPL

C：SPML

SPML

D：XACML

XACML

答案:正确答案是：C：SPML

SPML（Service Provisioning Markup Language）是一种基于XML的标记语言，用于在系统之间交换用户、资源和服务配置信息。它使用请求权限（requesting authority）、供应服务点（provisioning service point）和供应服务目标（provisioning service target）等概念来处理其核心功能。这些概念帮助在系统中自动化地管理和配置用户和服务。

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

题目85：什么类型的风险评估使用了这里所示的工具？

<div style="text-align:center"><img alt="" height="218" src="/file/100000/m/20210823/3d59e93535ba4f8a80af2208e2efb301.png" width="362" /></div>

What type of risk assessment uses tools such as the one shown here?

<div style="text-align:center"><img alt="" height="310" src="/file/100000/m/20210823/ff479ff90053472599d4bb79f70dabb1.png" width="501" /></div>

A：定量

Quantitative

B：预期寿命

Loss expectancy

C：金融

Financial

D：定性

Qualitative

答案:根据题目描述和提供的图像，这里展示的工具可能是一个风险矩阵（Risk Matrix），这是一种常用的定性风险评估工具。风险矩阵通常用于评估风险的可能性和影响，并将风险分为不同的等级（如低、中、高）。因此，这里展示的工具最可能用于定性风险评估。

正确答案是：

D：定性

Qualitative

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

题目86：MAC模型使用三种类型的环境。以下哪项不是强制性访问控制设计？

MAC models use three types of environments. Which of the following is not a mandatory access control design?

A：分层

Hierarchical

B：包围

Bracketed

C：分区

Compartmentalized

D：混合

Hybrid

答案:在强制性访问控制（MAC）模型中，通常使用的环境类型包括分层（Hierarchical）、分区（Compartmentalized）和混合（Hybrid）。这些环境类型用于定义和管理不同级别的安全访问权限。

- \*\*分层（Hierarchical）\*\*：这种环境类型基于层次结构，通常用于军事或政府机构，其中信息按照不同的安全级别进行分类。

- \*\*分区（Compartmentalized）\*\*：这种环境类型将信息划分为不同的隔间或区域，每个区域有独立的访问控制策略。

- \*\*混合（Hybrid）\*\*：这种环境类型结合了分层和分区的特点，允许更复杂的访问控制策略。

选项 \*\*B：包围（Bracketed）\*\* 并不是MAC模型中常用的环境类型。因此，正确答案是：

\*\*B：包围（Bracketed）\*\*

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

题目87：Mandy是一个由6人组成的项目团队的助长。她希望为这些人提供私下交流的功能，这样任何一对人都可以交换不受任何其他人（团队成员或非团队成员）拦截的通信。她正在使用非对称加密算法。实现这些要求需要多少个密钥？

Mandy is the team leader for a project team that includes six people. She would like to pro- vide those people with the ability to communicate privately, such that any pair of people can exchange communications that are not subject to interception by anyone else (team member or nonteam member). She is using an asymmetric encryption algorithm. How many keys are required to implement these requirements?

A：6

6

B：12

12

C：15

15

D：36

36

答案:在非对称加密系统中，每个用户都有一个公钥和一个私钥。公钥可以公开分享，用于加密信息，而私钥则必须保密，用于解密信息。

对于Mandy的6人团队，如果希望任何一对人都能进行私密通信，那么每个人都需要有一个公钥和一个私钥。因此，每个人需要生成一对密钥（一个公钥和一个私钥）。

具体来说，6个人每个人需要一对密钥，所以总共需要的密钥对数是6对。每对包括一个公钥和一个私钥，因此总的密钥数量是6对 × 2 = 12个密钥。

所以，正确答案是 B：12。

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

题目88：Sally为千兆以太网网络接线。她应该做哪些布线选择，来确保她的用户可以使用1000 Mbps 的网络？

Sally is wiring a gigabit Ethernet network. What cabling choices should she make to ensure she can use her network at the full 1000 Mbps she wants to provide to her users?

A：Cat 5 和Cat 6

Cat 5 和Cat 6

B：Cat 5e 和Cat 6

Cat 5e 和Cat 6

C：Cat 4e 和Cat 5e

Cat 4e 和Cat 5e

D：Cat 6 和Cat 7

Cat 6 和Cat 7

答案:为了确保Sally的千兆以太网网络能够提供1000 Mbps的速度，她需要选择能够支持这种速度的电缆。以下是各选项的分析：

A：Cat 5 和Cat 6

- Cat 5电缆理论上可以支持1000 Mbps的速度，但在实际应用中，由于信号衰减和干扰问题，通常不推荐用于千兆以太网。

- Cat 6电缆设计用于支持1000 Mbps的速度，并且在实际应用中表现良好。

B：Cat 5e 和Cat 6

- Cat 5e电缆是Cat 5的增强版，专门设计用于支持1000 Mbps的速度，并且在实际应用中表现良好。

- Cat 6电缆同样支持1000 Mbps的速度，并且在更高频率下表现更好。

C：Cat 4e 和Cat 5e

- Cat 4e电缆不支持1000 Mbps的速度，通常用于较低速度的网络。

- Cat 5e电缆支持1000 Mbps的速度。

D：Cat 6 和Cat 7

- Cat 6电缆支持1000 Mbps的速度。

- Cat 7电缆支持更高的速度（10 Gbps），并且具有更好的屏蔽性能，但通常用于更高要求的网络环境。

综上所述，为了确保1000 Mbps的速度，Sally应该选择Cat 5e和Cat 6电缆。因此，正确答案是：

B：Cat 5e 和Cat 6

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

题目89：Ursula正在寻求扩大其组织网站的覆盖范围和可扩展性。她希望将她的数据副本放置在世界各地，并靠近网站访问者的位置，以减少加载时间和服务器负担。什么类型的云服务最能满足她的需求？

Ursula is seeking to expand the reach and scalability of her organization’s website. She would like to position copies of her data around the world in locations close to website visitors to reduce loading time and the burden on her servers. What type of cloud service would best meet her needs?

A：IaaS

IaaS

B：容器化

Containerization

C：CDN

CDN

D：SaaS

SaaS

答案:Ursula的需求是将数据副本放置在世界各地，靠近网站访问者的位置，以减少加载时间和服务器负担。这种需求最适合使用内容分发网络（Content Delivery Network, CDN）。

CDN 是一种分布式服务器系统，它通过将内容缓存到全球多个数据中心，使用户可以从离他们最近的服务器获取数据，从而减少延迟并提高加载速度。这对于需要快速加载时间的网站尤其重要，特别是当用户分布在全球各地时。

因此，正确答案是：

C：CDN

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

题目90：Robert是一家小型企业的网络管理员，最近安装了一个新的防火墙。在看到异常繁重的网络流量迹象后，他检查了入侵检测系统，报告说Smurf攻击正在进行。Robert可通过哪些防火墙配置更改来最有效地防止这种攻击？

Robert is the network administrator for a small business and recently installed a new firewall. After seeing signs of unusually heavy network traffic, he checked his intrusion detection system, which reported that a smurf attack was under way. What firewall configuration change can Robert make to most effectively prevent this attack?

A：阻止攻击的源IP地址

Block the source IP address of the attack.

B：阻止入站UDP流量

Block inbound UDP traffic.

C：阻止攻击的目的IP地址

Block the destination IP address of the attack.

D：阻止入站ICMP流量

Block inbound ICMP traffic.

答案:Smurf攻击是一种利用ICMP（Internet Control Message Protocol）协议的拒绝服务攻击。攻击者发送大量的ICMP回显请求（ping）到广播地址，这些请求会被广播到网络中的所有设备。这些设备会向源IP地址发送回显应答，导致目标系统被大量的ICMP流量淹没，从而无法正常处理其他网络请求。

为了防止Smurf攻击，最有效的防火墙配置更改是阻止入站ICMP流量。这样可以防止攻击者发送大量的ICMP回显请求到网络中的广播地址，从而避免网络设备被大量的ICMP流量淹没。

因此，正确答案是：

D：阻止入站ICMP流量

Block inbound ICMP traffic.

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

题目91：以下哪种类型的防火墙无法跟踪不同数据包之间的连接状态？

Which one of the following types of firewalls does not have the ability to track connection status between different packets?

A：状态检查

Stateful inspection

B：应用代理

Application proxy

C：数据包过滤器

Packet filter

D：下一代

Next generation

答案:题目问的是哪种类型的防火墙无法跟踪不同数据包之间的连接状态。我们来逐一分析选项：

A：状态检查（Stateful inspection）防火墙能够跟踪连接状态，因为它会监控每个连接的建立、维护和终止过程。

B：应用代理（Application proxy）防火墙也能够跟踪连接状态，因为它工作在应用层，能够理解应用协议并管理连接。

C：数据包过滤器（Packet filter）防火墙通常只检查数据包的头部信息，如源地址、目的地址、端口等，而不关心数据包之间的连接状态。因此，它无法跟踪连接状态。

D：下一代（Next generation）防火墙通常集成了多种功能，包括状态检查、深度包检测等，因此它们能够跟踪连接状态。

综上所述，无法跟踪不同数据包之间连接状态的防火墙类型是数据包过滤器（Packet filter）。

答案是：C：数据包过滤器（Packet filter）。

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

题目92：Frances担心她所在组织的服务器中的设备故障会导致这些服务器断电。以下哪项控制措施最能解决此风险？

Frances is concerned that equipment failures within her organization's servers will lead to a loss of power to those servers. Which one of the following controls would best address this risk?

A：冗余电源

Redundant power sources

B：备用发电机

Backup generators

C：双电源

Dual power supplies

D：不间断电源

Uninterruptible power supplies

答案:Frances担心的是服务器中的设备故障会导致断电，因此需要一种能够在设备故障时继续供电的解决方案。让我们逐一分析每个选项：

A：冗余电源（Redundant power sources） - 这意味着有多个电源供应系统，如果一个电源失效，另一个可以继续供电。这可以解决电源故障的问题，但题目中提到的是设备故障，而不是电源故障。

B：备用发电机（Backup generators） - 备用发电机通常用于在主电源失效时提供电力，但它们通常需要一定的时间来启动，并且主要用于长时间断电的情况。这并不能直接解决设备故障导致的断电问题。

C：双电源（Dual power supplies） - 双电源意味着服务器有两个独立的电源供应，如果一个电源失效，另一个可以继续供电。这可以解决电源故障的问题，但同样，题目中提到的是设备故障，而不是电源故障。

D：不间断电源（Uninterruptible power supplies, UPS） - UPS可以在主电源失效时立即提供电力，确保服务器不会断电。UPS通常用于短时间的电力中断，直到备用发电机启动或主电源恢复。UPS可以解决设备故障导致的断电问题，因为它可以在设备故障时立即提供电力。

综上所述，最合适的控制措施是 \*\*D：不间断电源（Uninterruptible power supplies）\*\*。

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

题目93：Peter正在审查其组织使用的远程访问技术，并希望消除使用任何不包括内置加密的技术。 他应该保留以下哪种方法？（选择所有符合条件的）

Peter is reviewing the remote access technologies used by his organization and would like to eliminate the use of any techniques that do not include built-in encryption. Which of the fol- lowing approaches should he retain? (Select all that apply.)

A：RDP

RDP

B：Telnet

Telnet

C：SSH

SSH

D：Dial-up

Dial-up

答案:在审查远程访问技术时，Peter希望保留那些包含内置加密的技术。以下是各个选项的分析：

A：RDP（远程桌面协议）

- RDP 是微软开发的一种协议，用于远程访问Windows系统。它支持加密，因此可以保留。

B：Telnet

- Telnet 是一种早期的远程访问协议，但它不提供加密功能，所有数据（包括密码）都是以明文形式传输的。因此，Telnet 不应该被保留。

C：SSH（安全外壳协议）

- SSH 是一种加密的网络协议，用于安全地访问远程计算机。它提供了强大的加密功能，因此应该被保留。

D：Dial-up（拨号连接）

- 拨号连接通常使用电话线进行数据传输，但它本身并不提供内置的加密功能。因此，拨号连接不应该被保留。

综上所述，Peter应该保留 \*\*A：RDP\*\* 和 \*\*C：SSH\*\*。

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

题目94：Matthew所在组织的网络发生了网络服务的质量问题。主要的症状是，数据包有时需要很长时间才能从源地址到达目的地。什么术语用来描述Matthew遇到的问题？

Matthew is experiencing issues with the quality of network service on his organization's network. The primary symptom is that packets are occasionally taking too long to travel from their source to their destination. The length of this delay changes for individual packets. What term describes the issue Matthew is facing?

A：延迟

Latency

B：抖动

Jitter

C：数据包丢失

Packet loss

D：干扰

Interference

答案:Matthew遇到的问题描述的是数据包从源地址到目的地的时间不一致，有时需要很长时间。这种现象被称为“抖动”（Jitter）。抖动是指数据包传输延迟的变化，即数据包到达时间的不一致性。因此，正确答案是：

B：抖动

Jitter

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

题目95：Gavin是一名内部审计师，负责评估其组织的网络安全状况。以下哪项是他从工作中生成报告的合适接收者？（选择所有符合条件的）

Gavin is an internal auditor working to assess his organization's cybersecurity posture. Which of the following would be appropriate recipients of the reports he generates from his work? (Select all that apply.)

A：经理

Managers

B：个人贡献者

Individual contributors

C：供应商

Suppliers

D：董事会成员

Board members

答案:在评估组织的网络安全状况时，Gavin作为内部审计师生成的报告应该提供给那些对组织的整体安全和风险管理有决策权和责任的人员。因此，合适的报告接收者包括：

A：经理（Managers） - 经理们需要了解网络安全状况，以便在日常运营中采取适当的措施来保护组织的资产和数据。

D：董事会成员（Board members） - 董事会成员对组织的整体战略方向和风险管理负有最终责任，因此他们需要了解网络安全状况，以便在战略层面做出决策。

个人贡献者（Individual contributors）和供应商（Suppliers）通常不需要直接接收这些报告，除非他们的工作直接涉及到网络安全的具体实施或管理。因此，选项B和C通常不是合适的接收者。

所以，正确答案是：

A：经理（Managers）

D：董事会成员（Board members）

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

题目96：Kim正在对其组织开发的Web应用程序进行测试，并希望确保所有常用的Web浏览器访问该Web应用程序。她应该进行什么类型的测试？

Kim is conducting testing of a web application developed by her organization and would like to ensure that it is accessible from all commonly used web browsers. What type of testing should she conduct?

A：回归测试

Regression testing

B：接口测试

Interface testing

C：模糊测试

Fuzzing

D：白盒测试

White-box testing

答案:Kim 希望确保所有常用的Web浏览器都能访问该Web应用程序，这意味着她需要测试应用程序在不同浏览器上的兼容性和功能表现。这种类型的测试被称为\*\*跨浏览器测试\*\*（Cross-browser testing）。

在给定的选项中，最接近的答案是 \*\*B：接口测试\*\*（Interface testing），因为跨浏览器测试通常涉及验证用户界面（UI）和功能在不同浏览器中的表现。然而，严格来说，跨浏览器测试并不完全等同于接口测试。

如果选项中有“跨浏览器测试”或“兼容性测试”，那将是最准确的答案。但在给定的选项中，\*\*B：接口测试\*\* 是最接近的。

所以，正确答案是：

\*\*B：接口测试\*\*

Interface testing

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

题目97：Kathleen正在为她的组织实施访问控制系统，并构建以下分组：

审阅者：更新文件，删除文件；

提交者：上传文件；

编辑：上传文件，更新文件

存档：删除文件，

Kathleen实施了哪种访问控制系统？

Kathleen is implementing an access control system for her organization and builds the following array:

Reviewers: update files, delete files

Submitters: upload files

Editors: upload files, update files

Archivists: delete files

What type of access control system has Kathleen implemented?

A：基于角色的访问控制

Role-based access control

B：基于任务的访问控制

Task-based access control

C：基于规则的访问控制

Rule-based access control

D：自主访问控制

Discretionary access control

答案:Kathleen实施的访问控制系统是基于角色的访问控制（Role-based access control, RBAC）。在这种系统中，访问权限是根据用户的角色来分配的，而不是基于用户个人或特定的任务。在这个例子中，Kathleen为不同的角色（如审阅者、提交者、编辑和存档者）分配了不同的权限，这是RBAC的典型特征。

因此，正确答案是：

A：基于角色的访问控制

Role-based access control

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

题目98：Alan正在安装一个灭火系统，该灭火系统会在火灾发生之后启动，并保护数据中心中的设备免受严重损坏。Alan试图降低什么指标？

Alan is installing a fire suppression system that will activateafter a fire breaks out and protect the equipment in the data center from extensive damage. What metric is Alan attempting to lower?

A：可能性

Likelihood

B：RTO 恢复 时间 目标

RTO

C：RPO 恢复 点 目标

RPO

D：影响

Impact

答案:Alan正在安装的灭火系统旨在在火灾发生后启动，以保护数据中心中的设备免受严重损坏。这种措施主要是为了减少火灾对数据中心设备和运营的影响。因此，Alan试图降低的指标是影响（Impact）。

正确答案是：

D：影响

Impact

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

题目99：Alan's Wrenches最近为其产品开发了一个新的制造工艺。他们计划在内部使用这项技术，而不是与他人共享。他们希望该技术得到尽可能长时间的保护。什么类型的知识产权保护最适合这种情况？

Alan's Wrenches recently developed a new manufacturing process for its product. They plan to use this technology internally and not share it with others. They would like it to remain protected for as long as possible. What type of intellectual property protection is best suited for this situation?

A：专利

Patent

B：版权

Copyright

C：商标

Trademark

D：商业秘密

Trade secret

答案:题目中描述的情况是Alan's Wrenches开发了一个新的制造工艺，并计划在内部使用而不与他人共享。他们希望这项技术得到尽可能长时间的保护。在这种情况下，最适合的知识产权保护类型是商业秘密（Trade secret）。

商业秘密是指不为公众所知悉、具有商业价值且被采取了合理保密措施的信息。与专利不同，商业秘密不需要公开，只要保密措施得当，理论上可以无限期地保护。因此，对于Alan's Wrenches来说，选择商业秘密保护可以确保他们的制造工艺在内部使用的同时，不会因为公开而失去保护。

其他选项：

- 专利（Patent）：虽然专利可以提供强有力的保护，但需要公开技术细节，且保护期限有限（通常为20年）。

- 版权（Copyright）：适用于保护文学、艺术和音乐作品等，不适用于制造工艺。

- 商标（Trademark）：用于保护品牌标识，如名称、标志等，不适用于技术或制造工艺。

因此，正确答案是：

D：商业秘密

Trade secret

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

题目100：Ben想使用标准化协议来连接国家漏洞数据库。他应该使用什么选项来确保他构建的工具与国家漏洞数据库中包含的数据能够配合使用？

Ben wants to interface with the National Vulnerability Database using a standardized protocol. What option should he use to ensure that the tools he builds work with the data contained in the NVD?

A：XACML 传递访问控制信息

XACML

B：SCML

SCML

C：VSML

VSML

D：SCAP

SCAP

答案:题目是关于Ben想要使用标准化协议来连接国家漏洞数据库（National Vulnerability Database, NVD），并确保他构建的工具能够与NVD中的数据配合使用。我们需要从给定的选项中选择最合适的协议。

选项分析：

- \*\*A：XACML\*\* - XACML（eXtensible Access Control Markup Language）是一种用于访问控制策略的语言，主要用于定义谁可以在什么条件下访问什么资源。它不直接与漏洞数据库的数据交互相关。

- \*\*B：SCML\*\* - SCML（Software Configuration Management Library）并不是一个广泛认可的标准化协议，与NVD的连接无关。

- \*\*C：VSML\*\* - VSML（Vulnerability State Modeling Language）并不是一个广泛认可的标准化协议，与NVD的连接无关。

- \*\*D：SCAP\*\* - SCAP（Security Content Automation Protocol）是一种用于自动化管理安全内容的协议，广泛用于漏洞管理和配置检查。SCAP包含多个标准，如CVE（Common Vulnerabilities and Exposures）、CPE（Common Platform Enumeration）等，这些标准与NVD中的数据格式和内容直接相关。

因此，\*\*D：SCAP\*\* 是确保工具与NVD数据配合使用的最佳选择。

最终答案是： D

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

题目101：Ron的组织没有资源来执行耗时的、人工的技术渗透测试，但他希望实现渗透测试的一些好处。他可以从事以下哪项技术，该技术需要最少的人工？

Ron's organization does not have the resources to conduct penetration testing that uses time-intensive manual techniques, but he would like to achieve some of the benefits of penetration testing. Which one of the following techniques could he engage in that requires the least manual effort?

A：白盒测试

White-box testing

B：黑盒测试

Black-box testing

C：灰盒测试

Gray-box testing

D：入侵和攻击模拟

Breach and attack simulation

答案:题目中提到的Ron的组织没有资源来执行耗时的、人工的技术渗透测试，但他希望实现渗透测试的一些好处。他需要选择一种需要最少人工的技术。

选项分析：

A：白盒测试 - 这种测试方法需要详细了解系统的内部结构和代码，通常需要较多的人工参与。

B：黑盒测试 - 这种测试方法不需要了解系统的内部结构，但通常需要较多的人工来设计和执行测试案例。

C：灰盒测试 - 这种测试方法介于白盒测试和黑盒测试之间，需要一定的人工参与。

D：入侵和攻击模拟 - 这种技术通常使用自动化工具来模拟攻击，需要的人工参与较少。

因此，Ron可以选择入侵和攻击模拟（Breach and attack simulation）这种技术，因为它需要最少的人工。

最终答案是：$\boxed{D}$。

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

题目102：在这里显示的图中，Harry要求读取数据文件的请求被阻止。Harry拥有“秘密”级别的文件访问许可，而数据文件的分类级别是“最高机密”。Bell-LaPadula模型的什么原则阻止了这个请求？

<div style="text-align:center"><img alt="" height="127" src="/file/100000/m/20210824/48755808f0f445dcaccd6a1fa7f22281.png" width="365" /></div>

In the figure shown here, Harry's request to read the data file is blocked. Harry has a Secret security clearance, and the data file has a Top Secret classification. What principle of the Bell-LaPadula model blocked this request?

<div style="text-align:center"><img alt="" height="150" src="/file/100000/m/20210824/c16c6e9032bb4aef87319d2054519f19.png" width="478" /></div>

A：简单安全属性

Simple Security Property

B：简单完整性属性

Simple Integrity Property

C：\*安全属性

\*-Security Property

D：自主安全属性

Discretionary Security Property

答案:在Bell-LaPadula模型中，阻止Harry读取数据文件的请求的原则是“简单安全属性”（Simple Security Property）。这个原则也被称为“无上读”（No Read Up）原则，它规定了一个主体（如用户）只能读取其安全级别等于或低于其许可级别的对象（如文件）。在这个例子中，Harry的安全许可级别是“秘密”（Secret），而数据文件的分类级别是“最高机密”（Top Secret），因此Harry的读取请求被阻止。

所以，正确答案是：

A：简单安全属性

Simple Security Property

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

题目103：Norm准备开始一个新的软件项目，与他合作的供应商使用SDLC方法开发。当他开始工作时，他收到一个文档，其中有一部分显示在这里。这是什么类型的规划文件？

<div style="text-align:center"><img alt="" height="238" src="/file/100000/m/20210824/68bdc8f9251748e595e5a3b64743689d.png" width="418" /></div>

Norm is starting a new software project with a vendor that uses an SDLC approach to development. When he arrives on the job, he receives a document that has the sections shown here. What type of planning document is this?

<div style="text-align:center"><img alt="" height="345" src="/file/100000/m/20210824/e59877d0e38545e79e3e597b0bec3489.png" width="616" /></div>

A：功能要求

Functional requirements

B：工作分解结构

Work breakdown structure

C：测试分析报告

Test analysis report

D：项目计划

Project plan

答案:根据题目描述和提供的图片内容，Norm收到的文档包含了项目的各个阶段和任务，这通常与工作分解结构（Work Breakdown Structure, WBS）相关。工作分解结构是一种将项目分解为更小、更易管理的部分的工具，它帮助项目团队理解项目的范围和任务。

因此，正确答案是：

B：工作分解结构

Work breakdown structure

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

题目104：Kolin正在寻找一种网络安全解决方案，该方案可帮助减少零日攻击，同时在系统连接到网络之前使用身份验证作为安全策略。Kolin想实现的是什么类型的解决方案？

Kolin is searching for a network security solution that will allow him to help reduce zero-day attacks while using identities to enforce a security policy on systems before they connect to the network. What type of solution should Kolin implement?

A：防火墙

A firewall

B：NAC(网络访问控制)系统

A NAC system

C：一种入侵检测系统

An intrusion detection system

D：端口安全

Port security

答案:Kolin正在寻找的网络安全解决方案需要能够在系统连接到网络之前使用身份验证来执行安全策略，并且能够帮助减少零日攻击。这种需求最适合的解决方案是网络访问控制（NAC）系统。

NAC系统的主要功能是确保只有经过身份验证和授权的设备才能接入网络。它可以在设备连接到网络之前对其进行安全检查，确保设备符合安全策略，如安装了最新的安全补丁、启用了防火墙等。这有助于减少零日攻击的风险，因为只有符合安全标准的设备才能接入网络。

其他选项的解释：

- \*\*防火墙\*\*：主要用于监控和控制进出网络的流量，但它不具备在设备连接网络之前进行身份验证和安全检查的功能。

- \*\*入侵检测系统（IDS）\*\*：主要用于检测网络中的异常行为或已知的攻击模式，但它不涉及设备连接网络之前的身份验证和安全策略执行。

- \*\*端口安全\*\*：主要用于限制特定端口上的设备接入，但它不具备全面的身份验证和安全策略执行功能。

因此，正确答案是：

\*\*B：NAC(网络访问控制)系统\*\*

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

题目105：Gwen发现了在Web服务器上的服务账户下运行的应用程序。服务账户对服务器具有完全的管理权限。这违反了什么信息安全原则？

Gwen comes across an application that is running under a service account on a web server. The service account has full administrative rights to the server. What principle of information security does this violate?

A：需知

Need to know

B：职责分离

Separation of duties

C：最小特权

Least privilege

D：工作轮换

Job rotation

答案:题目描述的情况是，一个应用程序在Web服务器上以服务账户的身份运行，并且这个服务账户拥有服务器的完全管理权限。这种情况违反了信息安全中的“最小特权”原则。

\*\*最小特权原则（Least Privilege）\*\* 是指用户或系统进程在执行任务时，应该只拥有完成任务所必需的最小权限，而不是拥有过多的权限。这样可以减少潜在的安全风险，因为即使账户被攻击或滥用，攻击者也只能访问有限的资源或执行有限的操作。

在这个例子中，服务账户拥有完全的管理权限，这意味着如果该账户被攻击或滥用，攻击者可以完全控制服务器，导致严重的安全问题。因此，服务账户应该只拥有运行应用程序所需的最小权限，而不是完全的管理权限。

所以，正确答案是：

\*\*C：最小特权

Least privilege\*\*

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

题目106：Ed正在为其组织的信息安全计划制定一套关键绩效和风险指标。以下哪项是常用的指标？ （选择所有符合条件的）

Ed is developing a set of key performance and risk indicators for his organization's information security program. Which of the following are commonly used indicators? (Select all that apply.)

A：定期审计次数

Number of scheduled audits

B：解决漏洞的时间

Time to resolve vulnerabilities

C：恶意站点访问尝试次数

Number of malicious site visit attempts

D：帐户泄露次数

Number of account compromises

答案:在制定信息安全计划的关键绩效和风险指标时，常用的指标通常包括以下几个方面：

A：定期审计次数

- 定期审计次数可以帮助评估组织是否按照计划进行安全审计，确保安全措施的有效性。

B：解决漏洞的时间

- 解决漏洞的时间是一个重要的指标，反映了组织对安全漏洞的响应速度和修复能力。

C：恶意站点访问尝试次数

- 这个指标可以帮助识别潜在的安全威胁，并评估组织的防御措施是否有效。

D：帐户泄露次数

- 帐户泄露次数是一个关键的风险指标，反映了组织在保护用户帐户方面的有效性。

因此，所有选项（A、B、C、D）都是常用的关键绩效和风险指标。

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

题目107：Kara正在记录漏洞扫描的结果。在审查调查结果后，她确定该漏洞确实存在。该团队随后实施了一项配置变更，以修复该问题。Kara应该如何在她的报告中对该漏洞进行分类？

Kara is documenting the results of a vulnerability scan. After reviewing one finding, she determined that the vulnerability did exist. The team then implemented a configuration change that corrected the issue. How should Kara classify this vulnerability in her report?

A：真阳性

True positive

B：真阴性

True negative

C：假阳性

False positive

D：假阴性

False negative

答案:在Kara的情况下，她通过审查确定漏洞确实存在，并且团队已经实施了配置变更来修复该问题。这意味着漏洞扫描工具正确地识别了一个实际存在的漏洞，因此这是一个“真阳性”（True Positive）的情况。

因此，Kara应该在她的报告中将该漏洞分类为：

\*\*A：真阳性 (True positive)\*\*

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

题目108-1：请参考以下情形，回答3个问题：

在 Web应用程序漏洞扫描测试期间，Steve针对他认为可能容易受到攻击的Web服务器运行Nikto。使用此处显示的Nikto输出，回答以下问题。

For questions , please refer to the following scenario:

During a web application vulnerability scanning test, Steve runs Nikto against a web server he believes may be vulnerable to attacks. Using the Nikto output shown here, answer the following questions.

<div style="text-align:center"><img alt="" src="/file/100000/m/20210824/5a7c3ff83cb2485aa79b7c42a628f70a.png" /></div>

Nikto为什么会标记 /test目录？

Why does Nikto flag the /test directory?

A：/test目录允许对PHP的管理访问

The /test directory allows administrative access to PHP.

B：它用于存储敏感数据

It is used to store sensitive data.

C：测试目录通常包含可被滥用的脚本

Test directories often contain scripts that can be misused.

D：它表示潜在的危害

It indicates a potential compromise.

答案:根据题目描述，Nikto 是一个用于扫描 Web 服务器漏洞的工具，它会检测常见的漏洞和潜在的安全问题。在 Web 应用程序中，`/test` 目录通常用于存放测试文件或脚本，这些文件可能包含未经验证的代码或配置错误，容易被攻击者利用。

选项分析：

- \*\*A\*\*：`/test` 目录允许对 PHP 的管理访问。这个选项没有直接关联到 Nikto 标记 `/test` 目录的原因。

- \*\*B\*\*：它用于存储敏感数据。Nikto 不会因为目录存储敏感数据而标记它，除非这些数据暴露在外部。

- \*\*C\*\*：测试目录通常包含可被滥用的脚本。这是 Nikto 标记 `/test` 目录的主要原因，因为测试目录中的脚本可能存在漏洞或被滥用。

- \*\*D\*\*：它表示潜在的危害。虽然 `/test` 目录可能暗示潜在的安全问题，但 Nikto 标记它的直接原因是它可能包含可被滥用的脚本。

因此，最合适的答案是：

\*\*C：测试目录通常包含可被滥用的脚本\*\*

\*\*Test directories often contain scripts that can be misused.\*\*

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

题目108-1：请参考以下情形，回答3个问题：

在 Web应用程序漏洞扫描测试期间，Steve针对他认为可能容易受到攻击的Web服务器运行Nikto。使用此处显示的Nikto输出，回答以下问题。

For questions , please refer to the following scenario:

During a web application vulnerability scanning test, Steve runs Nikto against a web server he believes may be vulnerable to attacks. Using the Nikto output shown here, answer the following questions.

<div style="text-align:center"><img alt="" src="/file/100000/m/20210824/5a7c3ff83cb2485aa79b7c42a628f70a.png" /></div>

为什么Nikto将目录索引标识为问题？

Why does Nikto identify directory indexing as an issue?

A：它列出目录中的文件

It lists files in a directory.

B：它可能允许XDRF

It may allow for XDRF.

C：目录索引可能导致拒绝服务攻击

Directory indexing can result in a denial-of-service attack.

D：目录索引默认情况下关闭，可能意味着潜在的损害

Directory indexing is off by default, potentially indicating compromise.

答案:Nikto将目录索引标识为问题的原因是：

\*\*A：它列出目录中的文件\*\*

解释：目录索引（Directory Indexing）是指当访问一个没有默认页面（如 `index.html` 或 `index.php`）的目录时，Web 服务器会自动列出该目录中的所有文件和子目录。这种行为可能会暴露敏感文件或目录结构，从而为攻击者提供有价值的信息，帮助他们进一步利用漏洞或发起攻击。因此，Nikto 将目录索引标识为一个潜在的安全问题。

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

题目108-1：请参考以下情形，回答3个问题：

在 Web应用程序漏洞扫描测试期间，Steve针对他认为可能容易受到攻击的Web服务器运行Nikto。使用此处显示的Nikto输出，回答以下问题。

For questions , please refer to the following scenario:

During a web application vulnerability scanning test, Steve runs Nikto against a web server he believes may be vulnerable to attacks. Using the Nikto output shown here, answer the following questions.

<div style="text-align:center"><img alt="" src="/file/100000/m/20210824/5a7c3ff83cb2485aa79b7c42a628f70a.png" /></div>

Nikto列出了OSVDB-877，指出系统可能容易受到XST攻击。这种类型的攻击允许攻击者做什么？

Nikto lists OSVDB-877, noting that the system may be vulnerable to XST. What would this type of attack allow an attacker to do?

A：使用跨站定位

Use cross-site targeting.

B：窃取用户的cookie

Steal a user's cookies.

C：计数器SQL跟踪

Counter SQL tracing.

D：修改用户的TRACE信息

Modify a user's TRACE information.

答案:XST（Cross-Site Tracing）攻击是一种利用HTTP TRACE或TRACK方法的漏洞。TRACE方法通常用于调试目的，允许客户端查看服务器接收到的请求内容。如果服务器配置不当，攻击者可以利用TRACE方法来窃取用户的敏感信息，例如用户的cookie。

具体来说，XST攻击允许攻击者通过TRACE方法获取用户的cookie信息，然后利用这些信息进行进一步的攻击，例如会话劫持或身份冒充。因此，XST攻击的主要目的是窃取用户的cookie。

所以，正确答案是：

\*\*B：窃取用户的cookie (Steal a user's cookies.)\*\*

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

题目109：谁是组织首席审计执行官（CAE）最合适的上级？

Who would be the most appropriate supervisor for an organization's chief audit executive (CAE)?

A：CIO

CIO

B：CISO

CISO

C：CEO

CEO

D：CFO

CFO

答案:在组织中，首席审计执行官（CAE）的职责是确保内部审计的独立性和客观性，以便有效地评估和改进组织的风险管理、控制和治理过程。因此，CAE的最合适的上级应该是能够支持其独立性和客观性的人。

选项分析：

- \*\*A：CIO（首席信息官）\*\* - CIO主要负责信息技术和系统，通常不涉及审计的独立性和客观性。

- \*\*B：CISO（首席信息安全官）\*\* - CISO主要负责信息安全，同样不涉及审计的独立性和客观性。

- \*\*C：CEO（首席执行官）\*\* - CEO是组织的最高管理者，能够支持CAE的独立性和客观性，确保审计工作不受其他部门的影响。

- \*\*D：CFO（首席财务官）\*\* - CFO主要负责财务管理和报告，如果CAE向CFO汇报，可能会影响审计的独立性和客观性，因为审计工作可能会涉及财务方面的内容。

因此，最合适的上级是 \*\*C：CEO\*\*。

\*\*最终答案：C：CEO\*\*

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

题目110：Ursula认为，她组织中的许多人都以不安全的方式将敏感信息存储在笔记本电脑上，并可能违反组织的安全政策。她可以使用什么控制方法来识别这些文件的存在？

Ursula believes that many individuals in her organization are storing sensitive information on their laptops in a manner that is unsafe and potentially violates the organization's security policy. What control can she use to identify the presence of these files?

A：网络DLP

Network DLP

B：网络IPS

Network IPS

C：端点DLP

Endpoint DLP

D：端点IPS

Endpoint IPS

答案:Ursula可以使用端点DLP（数据丢失防护）来识别这些文件的存在。端点DLP是一种安全技术，它安装在终端设备（如笔记本电脑）上，用于监控、检测和保护存储在设备上的敏感信息。通过端点DLP，Ursula可以扫描笔记本电脑上的文件，识别出包含敏感信息的文件，并确保这些文件按照组织的安全政策进行存储和处理。

因此，正确答案是：

C：端点DLP

Endpoint DLP

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

题目111：在什么云计算模型中，客户在自己的数据中心中构建云计算环境或在另一个数据中心中构建供客户专用的环境？

In what cloud computing model does the customer build a cloud computing environment in his or her own data center or build an environment in another data center that is for the customer's exclusive use?

A：公共云

Public cloud

B：私有云

Private cloud

C：混合云

Hybrid cloud

D：共享云

Shared cloud

答案:正确答案是 B：私有云 (Private cloud)。

私有云是指专门为一个客户或组织构建的云计算环境，可以位于客户自己的数据中心内，也可以位于第三方数据中心中，但仅供该客户或组织使用。这种模型提供了更高的安全性和控制能力，适合对数据隐私和安全性要求较高的企业。

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

题目112：以下哪种技术旨在防止由于Web服务器脱机，从而成为Web应用程序系统结构中的一个单点故障？

Which one of the following technologies is designed to prevent a web server going offline from becoming a single point of failure in a web application architecture?

A：负载平衡

Load balancing

B：双电源

Dual-power supplies

C：IPS

IPS

D：RAID

RAID

答案:题目112的正确答案是：

A：负载平衡

Load balancing

负载平衡技术旨在通过将流量分配到多个服务器上，防止任何一个服务器成为单点故障。如果其中一个Web服务器脱机，负载均衡器可以将流量重定向到其他正常运行的服务器，从而确保Web应用程序的持续可用性。其他选项如双电源、IPS和RAID虽然也有助于提高系统的可靠性和安全性，但它们并不直接解决Web服务器脱机导致的单点故障问题。

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

题目113：Alice想要向Bob发送一个信息，他希望Bob知道该消息在传输期间没有被改变。Alice想实现什么安全目的？

Alice wants to send Bob a message with the confidence that Bob will know the message was not altered while in transit. What security goal is Alice trying to achieve?

A：保密性

Confidentiality

B：不可否认

Nonrepudiation

C：身份验证

Authentication

D：完整性

Integrity

答案:Alice希望确保Bob知道消息在传输期间没有被改变，这意味着她关注的是消息的完整性。完整性确保数据在传输过程中没有被篡改或损坏。

因此，Alice想要实现的安全目的是 \*\*完整性\*\*。

正确答案是：

D：完整性

Integrity

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

题目114：这里显示了什么网络拓扑？

What network topology is shown here?

<div style="text-align:center"><img alt="" height="431" src="/file/100000/m/20210824/0bf89dbf97ef465a9815e8bd11e85a22.png" width="601" /></div>

A：环型

A ring

B：总线型

A bus

C：星型

A star

D：网状

A mesh

答案:根据题目描述和提供的图片，网络拓扑显示的是星型结构（A star）。在星型拓扑中，所有节点都连接到一个中心节点（通常是集线器或交换机）。这种结构的特点是易于管理和扩展，但如果中心节点出现故障，整个网络可能会受到影响。

因此，正确答案是：

C：星型

A star

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

题目115：Monica正在开发一个软件应用程序，计算个人的身体质量指数，用于医疗规划。她希望能了解医生测量出的体重值的一般区间，以确保在录入体重时能处于预期范围内。Monica使用什么类型的控制？

Monica is developing a software application that calculates an individual’s body mass index for use in medical planning. She would like to include a control on the field where the physician enters an individual’s weight to ensure that the weight falls within an expected range. What type of control should Monica use?

A：故障打开

Fail open

B：失败安全

Fail secure

C：限制检查

Limit check

D：缓冲区边界

Buffer bounds

答案:Monica 应该使用 \*\*C：限制检查（Limit check）\*\*。

限制检查是一种输入验证技术，用于确保输入的数据在预期的范围内。在这个场景中，Monica 希望确保医生输入的体重值在一个合理的范围内（例如，正常成年人的体重范围），以避免输入错误或异常值。通过限制检查，软件可以在用户输入数据时立即验证其是否在允许的范围内，从而防止无效数据的录入。

其他选项的解释：

- \*\*A：故障打开（Fail open）\*\*：这是一种安全机制，通常在系统故障时允许访问，而不是阻止访问。与输入验证无关。

- \*\*B：失败安全（Fail secure）\*\*：这是一种安全机制，系统在故障时会进入安全状态，阻止访问。与输入验证无关。

- \*\*D：缓冲区边界（Buffer bounds）\*\*：这是指防止缓冲区溢出攻击的安全措施，与输入范围验证无关。

因此，\*\*C：限制检查\*\* 是最合适的选项。

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

题目116：将下列数字标记的测试方法匹配到相应的字母标记的知识等级

测试方法：

1.黑盒

2. 白盒

3. 灰盒

知识等级：

A.全知识

B. 部分知识

C. 零知识

Match the following numbered types of testing methodologies with the lettered correct level of knowledge:

Testing methodologies

1.Black box

2. White box

3. Gray box

Level of knowledge

A.Full knowledge of the system

B.Partial or incomplete knowledge

C.No prior knowledge of the system

答案:将测试方法与知识等级匹配如下：

1. 黑盒 (Black box) - C. 零知识 (No prior knowledge of the system)

- 黑盒测试方法假设测试人员对系统的内部结构和工作原理一无所知，仅通过输入和输出来测试系统的功能。

2. 白盒 (White box) - A. 全知识 (Full knowledge of the system)

- 白盒测试方法要求测试人员对系统的内部结构、代码和逻辑有全面的了解，以便进行详细的测试。

3. 灰盒 (Gray box) - B. 部分知识 (Partial or incomplete knowledge)

- 灰盒测试方法介于黑盒和白盒之间，测试人员对系统的内部结构有一定的了解，但不如白盒测试那样全面。

因此，匹配结果为：

1 - C

2 - A

3 - B

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

题目117：将以下字母因素与编号类型进行匹配：

因素：

A. PIN

B. 令牌

C. 指纹

D. 密码

E.智能卡

F. 视网膜扫描

G. 安全问题/答案

类型：

1. 你知道什么

2. 你拥有什么

3. 你是什么

Match the following lettered factors to their numbered type:

Factors

A PIN

B. A token

C. A fingerprint

D. A password

E. A smart card

F. A retinal scan

G. A security question/answer

Types

1. Something you know

2. Something you have

3. Something you are

答案:根据题目要求，将字母因素与编号类型进行匹配如下：

1. 你知道什么 (Something you know):

- A. PIN

- D. 密码 (A password)

- G. 安全问题/答案 (A security question/answer)

2. 你拥有什么 (Something you have):

- B. 令牌 (A token)

- E. 智能卡 (A smart card)

3. 你是什么 (Something you are):

- C. 指纹 (A fingerprint)

- F. 视网膜扫描 (A retinal scan)

这些匹配基于每个因素所属的认证类型。PIN、密码和安全问题/答案属于“你知道什么”类型，因为它们是基于知识的认证方式。令牌和智能卡属于“你拥有什么”类型，因为它们是物理设备或物品。指纹和视网膜扫描属于“你是什么”类型，因为它们是基于生物特征的认证方式。

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