Questions in `Cybersecurity Fundamentals`

93672. 经典的冯·诺依曼体系结构包括（ ）、（ ）、存储器、输入设备、输出设备等组成部件。

Options

A. 中央处理器
B. 运算器
C. 控制器
D. 计算器

Answers

B. 运算器
C. 控制器

93673. 支撑 WEB 的三种基础技术包括（）

Options

A. HTTP
B. URL
C. DNS
D. HTML

Answers

A. HTTP
B. URL
D. HTML

93674. 说出 3 种刻画复杂网络的常用特征参数及其定义。

Answers

(1)度分布:网络中某个节点拥有相邻节点的数目，即节点关联边的数目为该节点的度。度分布 P (k) 表示网络中度为 k 的节点出现的概率。(2)平均路径长度：（在网络中任意选择两个节点，连通这两个节点的最短路径就是这两个节点之间的路径长度。）网络中所有任意两个节点之间路径长度的平均值就是网络的平均路径长度。(3)聚合系数:节点的聚合系数定义为某节点的所有相邻节点之间连边的数目占可能的最大连边数目的比例。(4)介数：点介数即为网络中经过某个节点的最短路径的数目占网络中所有最短路径数的比例。边介数即为网络中经过某条边的最短路径的数目占网络中所有最短路径数的比例。【任意三点即可】

93675. 简述小世界特性和无标度特性

Answers

小世界特性，也称为六度空间理论或者是六度分割理论(Six degrees of separation)。小世界特性指出，社交网络中的任何一个成员和任何一个陌生人之间所间隔的人不会超过六个。小世界特性的关键在于:由成千上万节点组成的大型网络，实际上是“小世界”，绝大部分节点之间只需要经过很短的路径就可以到达。
无标度特性，网络中节点的度分布符合幂律分布，这一特性被称为网络的无标度特性(Scale-free)。无标度特性实际上反映了复杂网络整体上具有严重的分布不均匀性。

93676. 设完全图K_n有 n 个节点（n≥2），m 条边，当（ ）时，K_n中一定存在欧拉回路。

Options

A. m 为奇数
B. n 为偶数
C. n 为奇数
D. m 为偶数

Answers

C. n 为奇数

Explain

完全图每个节点的度为 n-1，n-1 为偶数，n 为奇数

93677. 设图 G 有 n 个节点，m 条边，且 G 中每个结点的度数不是 k，就是 k+1，则 G 中度数为 k 的节点数是（ ）。

Options

A. n/2
B. n(n+1)
C. nk-2m
D. n(k+1)-2m

Answers

D. n(k+1)-2m

93678. 设有 33 盏灯，拟公用一个电源，则至少需有 5 插头的接线板数（ ）。

Options

A. 7
B. 8
C. 9
D. 14

Answers

B. 8

Explain

类似哈夫曼编码问题：1 个 1 级，2 个 2 级，5 个 3 级。

93679. 1948 年，（ ）发表了著作《控制论》，标志着控制论的诞生。

Options

A. 瓦格纳
B. 维纳
C. 牛顿
D. 拉斯韦尔

Answers

B. 维纳

93680. 控制论的核心问题是（ ）。

Options

A. 消息的传递
B. 系统的调节
C. 信息传播和信息处理
D. 资源的管理

Answers

C. 信息传播和信息处理

93681. “神农尝百草”属于控制论中的（ ）。

Options

A. 随机控制
B. 共轭控制
C. 负反馈调节
D. 正反馈调节

Answers

A. 随机控制

93682. 下列关于占优策略均衡和纳什均衡的描述正确的是？（ ）

Options

A. 占有策略均衡肯定是纳什均衡
B. 纳什均衡都是占优策略均衡
C. 纳什均衡是特殊的占优策略均衡
D. 以上三种情况都有可能

Answers

A. 占有策略均衡肯定是纳什均衡

93683. 、囚徒困境说明（ ）。

Options

A. 双方都独立依照自己的利益行事，则双方不一定能得到整体最好的结果
B. 如果没有某种约束，局中人也可在（抵赖，抵赖）的基础上达到均衡
C. 双方都依照自己的利益行事，结果会是一方赢，一方输
D. 每个局中人在做决策时，不需要考虑对手的反应

Answers

A. 双方都独立依照自己的利益行事，则双方不一定能得到整体最好的结果

93684. 、对博弈中的每一个博弈者而言，无论对手作何选择，其总是拥有唯一最佳行为，此时的博弈具有（ ）。

Options

A. 囚徒困境式的均衡
B. 一报还一报的均衡
C. 占优策略均衡
D. 激发战略均衡

Answers

C. 占优策略均衡

93685. 线性规划的可行域的形状主要取决于（ ）

Options

A. 目标函数
B. 约束条件的个数
C. 约束条件的系数
D. 约束条件的个数以及约束条件的系数

Answers

D. 约束条件的个数以及约束条件的系数

93686. $f(x)$，$g(x)$均为凸函数，则$h(x)=max(f(x),g(x))$是（ ）

Options

A. 凸函数
B. 凹函数
C. 既不是凹函数也不是凸函数
D. 无法判断

Answers

A. 凸函数

93687. 给定问题，则下列各点属于 K-T 点的是（ ）。

$$\begin{cases} \min f=(x_1-2)^2+x_2^2 \\ s.t.\ -x_1+x_2^2\le 0 \\ x_1-x_2\le 0 \end{cases}$$

Options

A. $（0，0）^T$
B. $（1，1）^T$

C. $（\frac{1}{2}，\frac{\sqrt{2}}{2}）^T$
D. $（\frac{1}{2}，\frac{1}{2}）^T$
Answers
B. $（1，1）^T$

93688. 单纯形法所求线性规划的最优解（ ）是可行域的顶点。
Options
A. 一定
B. 一定不
C. 不一定
D. 无法判断
Answers
A. 一定

93689. 市场上某商品来自与两个不同的工厂，它们的市场占有率分别为 **60%**和 **40%**，有两个人各自买了一件。则两人买到的商品来自不同工厂的概率为（ ）。
Options
A. 0.5
B. 0.24
C. 0.48
D. 0.3
Answers
C. 0.48

93690. 甲、乙两人的射击命中率分别为 **1/3** 和 **1/2**。此二人同时向某目标各射击一次，已知目标被击中，则它由甲命中的概率为（ ）。
Options
A. 1/3
B. 1/2
C. 2/5
D. 2/3
Answers
B. 1/2

93691. 若当事件 **A**、**B** 同时发生时，事件 **C** 必然发生，则（ ）。
Options
A. P(C)≤P(A)+P(B)-1
B. P(C)≥P(A)+P(B)-1
C. P(C)=P(A∪B)
D. P(C)=P(AB)
Answers
B. P(C)≥P(A)+P(B)-1

93692. 设 **A，B，C** 为三个随机事件，且 **P（A）＝P（B）＝P（C）＝1/4，P（AB）＝0，P（AC）＝P（BC）＝1/12**，则 **A，B，C** 中恰有一个事件发生的概率为（ ）。
Options
A. 3/4
B. 2/3
C. 1/2
D. 5/12
Answers
D. 5/12

93693. 设随机变量 **X** 与 **Y** 相互独立，且都服从正态分布 **N（μ，σ^2）**，则 **P{|X－Y|＜1}**（ ）。
Options
A. 与 μ 有关，而与σ^2无关
B. 与 μ 无关，而与σ^2有关
C. 与 μ 和σ^2都有关
D. 与 μ 和σ^2都无关
Answers
B. 与 μ 无关，而与σ^2有关

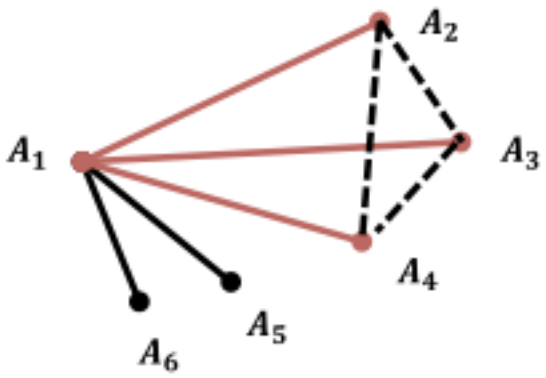
93694. 一个连通的无向图 **G**，如果它的所有节点的度数都是偶数，那么它一定具有一条（ ）。
Options
A. 哈密顿回路
B. 欧拉回路
C. 哈密顿通路
D. 欧拉通路
Answers
B. 欧拉回路
D. 欧拉通路

93695. 下面文字中，能用一笔画不重复写成的字有哪些？**( )**
Options
A. 口
B. 日
C. 田
D. 回
Answers
A. 口
B. 日

93696. 证明在一次 n（n≥6）个人的聚会中，任意 6 个人中必有 3 个人互相认识或者互相不认识，并举例说明将 6 个人改成 5 个人，结论不一定成立。

Answers

图解法：将问题抽象为右图的图论分析问题



，

在图中任取一个节点，假设为 A1。由于认识的人和不认识的人互为补集，图中 A1 至少认识 3 个人或者至少不认识 3 个人，以认识 3 个人为例（不认识的情况类似），将认识的人用红色的边连接起来，假设为 A2、A3、A4，不认识的人用黑色的边连接起来。观察 A2、A3、A4，若三者由黑色的边相连，则图中存在一个黑色的三角形，即 3 个人互不认识；若三条边中有任意一条为红色，则图中存在一个红色的三角形，即 3 个人互相认识。且这两种情况互为补集，由此，得证。

例：当 5 个人的认识（或不认识）关系构成一个环时，图中不存在 3 个相互认识（或不认识）的人。

93697. 设 G 为 9 个节点的无向图，每个节点的度数不是 5 就是 6，试证明 G 中至少有 5 个度为 6 的节点或者 6 个度为 5 的节点。

Answers

所有节点的度数之和是边的两倍，由此可知度数之和为偶数，从而度为 5 的节点一定有偶数个，可以写出所有度为 5 和 6 的节点的个数分布情况：{0，9}，{2，7}，{4，5}，{6，3}，{8，1}，可以看到，所有的情况中，前三种至少有 5 个度为 6 的节点，后两种情况至少有 6 个度为 5 的节点，得证。

93698. A、B 两企业利用广告进行竞争。若 A、B 两企业都做广告，在未来销售中，A 企业可以获得 20 万元利润，B 企业可获得 8 万元利润；若 A 企业做广告，B 企业不做广告，A 企业可获得 25 万元利润，B 企业可获得 2 万元利润；若 A 企业不做广告，B 企业做广告，A 企业可获得 10 万元利润，B 企业可获得 12 万元利润；若 A、B 两企业都不做广告，A 企业可获得 30 万元利润，B 企业可获得 6 万元利润。（1）画出 A、B 两企业的损益矩阵。（2）求纯策略纳什均衡

Answers

（1）

	B 企业		
A 企业		做广告	不做广告
	做广告	20，8	25，2
	不做广告	10，12	30，6

（2）对于 B 企业来说，做广告属于占优策略，因此 B 会选择做广告；A 知道 B 的占优策略，因此 A 会在 B 的占优策略中进行决策，选择做广告。因而（做广告，做广告）是一个纯策略纳什均衡。

93700.

设 S 是$\mathbf{R}^n$中的非空凸集，f是定义在 S 上的实函数。若对任意的

$\in (0,1)$，均有$f(\lambda x_1+(1-\lambda)x_2)\le \max\{f(x_1),\ f(x_2)\}$，则称$f$是凸集 S 上的准凸函数，$x^*$是$f(x)$在 S 上的严格局部极小点，则体极小点。

Answers

反证法。假设x^*不是严格整体极小点，则存在$x'\in$S为严格整体极

S因此对于实数$\lambda\in(0,1)$，有$\lambda x^*+(1-\lambda)x'\in$S，由于$x'$为严格整

从而有$f(\lambda x^*+(1-\lambda)x')\le\max\{f(x^*),\ f(x')\}<f(x^*)$。任取δ>

$\lambda\to1$，使得$\lambda x^*+(1-\lambda)x'\in\dot{U}(x^*,\delta)$。可知，在$x^*$的任意去心

点，与x^*为严格局部极小点矛盾。故x^*为严格整个极小点。

93701. 可信计算中，TPM 指的是（ ）。

Options

A. Technological Protection Measures
B. Third Party Manufacturer
C. Technical Project Manager
D. Trusted Platform Module

Answers

D. Trusted Platform Module

93702. 下面属于 2000 年以后提出的安全机制有（ ）。

Options

A. 移动目标防御
B. 沙箱
C. 拟态防御
D. 零信任网络

Answers

A. 移动目标防御
C. 拟态防御
D. 零信任网络

93703. 下面属于 2000 年以前提出的安全机制有（ ）。

Options

A. 拟态防御
B. 入侵容忍
C. 沙箱
D. 零信任网络

Answers

B. 入侵容忍
C. 沙箱

93704. 下面关于沙箱的描述中，正确的有（ ）。

Options

A. 沙箱的安全目标主要是防范恶意程序对系统环境的破坏
B. 沙箱的核心思想是“隔离”
C. 从访问控制的角度看，沙箱的本质是面向程序的访问控制
D. 沙箱是一项新兴的安全机制，目前还未得到广泛应用

Answers

A. 沙箱的安全目标主要是防范恶意程序对系统环境的破坏
B. 沙箱的核心思想是“隔离”
C. 从访问控制的角度看，沙箱的本质是面向程序的访问控制

93705. 下面关于入侵容忍的描述中，正确的有（ ）。

Options

A. 入侵容忍的安全目标主要是在攻击可能存在的前提下使系统的机密性、完整性和可用性能够得到一定程度的保证
B. 入侵容忍试图阻止每一次单个入侵的发生，从而使系统不会遭受攻击的影响
C. 入侵容忍是一种使系统维持生存性的技术
D. 入侵容忍和入侵检测是完全一样的安全机制

Answers

A. 入侵容忍的安全目标主要是在攻击可能存在的前提下使系统的机密性、完整性和可用性能够得到一定程度的保证
C. 入侵容忍是一种使系统维持生存性的技术

93706. 在攻击漏洞入侵混合错误模型中，系统从遭受攻击到最终失效涉及的环节包括（ ）。

Options

A. 攻击者（入侵者）攻击
B. 安全漏洞利用
C. 错误发生
D. 系统失效

Answers

A. 攻击者（入侵者）攻击
B. 安全漏洞利用
C. 错误发生
D. 系统失效

93707. 下面关于可信计算的描述中，正确的有（ ）。

Options

A. 可信计算最早是在国内诞生，而后发展到国外
B. 可信计算需要有一个可信根作为信任基点
C. 可信计算主要涉及到软件安全，不涉及硬件安全
D. 可信计算通过信任链来确保每一个环节的身份可信

Answers

B. 可信计算需要有一个可信根作为信任基点
D. 可信计算通过信任链来确保每一个环节的身份可信

93708. 以恶意代码检测为例对生物免疫和类免疫防御进行类比，下面类比正确的有（ ）。

Options

A. 生物免疫中的抗原相当于类免疫防御中的恶意代码文件

B. 生物免疫中的抗体相当于类免疫防御中的恶意代码特征
C. 生物免疫中的疫苗注射相当于类免疫防御中的恶意代码特征库更新
D. 生物免疫中的抗原清除相当于类免疫防御中的恶意代码清除

Answers

A. 生物免疫中的抗原相当于类免疫防御中的恶意代码文件
B. 生物免疫中的抗体相当于类免疫防御中的恶意代码特征
C. 生物免疫中的疫苗注射相当于类免疫防御中的恶意代码特征库更新
D. 生物免疫中的抗原清除相当于类免疫防御中的恶意代码清除

93709. 下面属于移动目标防御的原理要点的是（ ）。

Options

A. 系统动态变化
B. 系统组成异构
C. 系统工作模式不确定
D. 系统功能冗余

Answers

A. 系统动态变化
B. 系统组成异构
C. 系统工作模式不确定

93710. 下面属于移动目标防御动态变化层次的有（ ）。

Options

A. 动态网络
B. 动态操作系统平台
C. 动态运行环境
D. 动态存储

Answers

A. 动态网络
B. 动态操作系统平台
C. 动态运行环境

93711. 下面表述符合拟态防御思想的有（ ）。

Options

A. 在功能等价的条件下，以提供目标环境的动态性、异构性、冗余可靠为目的
B. 通过网络、平台、环境、软件、数据等结构的主动跳变或快速迁移来实现动态变化、弹性可靠的拟态环境
C. 扰乱攻击链的构造，使攻击的代价倍增、难以生效
D. 通过隔离程序的运行环境、限制程序执行不安全的操作，防止恶意程序对系统可能造成的破坏

Answers

A. 在功能等价的条件下，以提供目标环境的动态性、异构性、冗余可靠为目的
B. 通过网络、平台、环境、软件、数据等结构的主动跳变或快速迁移来实现动态变化、弹性可靠的拟态环境
C. 扰乱攻击链的构造，使攻击的代价倍增、难以生效

93712. 下面表述符合零信任网络思想的有（ ）。

Options

A. 内网是安全的、可靠的，应当把主要的资源集中用于防御来自外网的威胁
B. 所有的通信必须以最安全的方式进行，与网络位置无关，网络位置并不意味着信任
C. 所有资源的身份认证和授权都是动态的，并且在允许访问之前严格执行
D. 企业尽可能收集有关资产、网络基础架构和通信现状的信息，并利用这些信息改善其安全态势

Answers

B. 所有的通信必须以最安全的方式进行，与网络位置无关，网络位置并不意味着信任
C. 所有资源的身份认证和授权都是动态的，并且在允许访问之前严格执行
D. 企业尽可能收集有关资产、网络基础架构和通信现状的信息，并利用这些信息改善其安全态势

93713. 沙箱是如何发挥作用的？请谈谈你对沙箱工作原理的理解。

Answers

沙箱的核心思想是“隔离”，即通过隔离程序的运行环境、限制程序执行不安全的操作，防止恶意程序对系统可能造成的破坏。沙箱内部环境可以是某种受限的、与外部隔离的虚拟操作系统，沙箱内部运行的是可信性无法保证的程序 X，与沙箱外部的程序不同，程序 X 只能对沙箱内部的资源进行自由访问，不能访问或只能根据安全规则有限制地访问沙箱外部的资源；程序 X 的启动控制、安全规则配置可以由沙箱外部的某个程序 A 来实现。在沙箱模式下，可信性无法保证的程序 X 能够使用的资源集（如内存空间，文件系统空间、网络等资源）可以得到有效控制，使程序 X 无法像正常程序那样对网络进行未授权访问，也无法随意检查主机状态或从输入设备读取数据，从而有效限制程序 X 的行为能力，使程序 X 无法对沙箱外部资源环境造成威胁。

93714. 入侵容忍通过哪些关键机制防止系统失效？

Answers

主要有两类机制：基于入侵检测和响应的机制；基于冗余的错误容忍机制。基于入侵检测和响应的机制首先要有一个入侵检测系统能够及时准确地检测到各种入侵行为失效的发生。当检测到系统可能遭受攻击时或发现系统局部失效时，通过重新分配资源、调整系统配置等手段进行快速响应，使系统能够继续工作。基于冗余的错误容忍机制，主要是借鉴容错技术的思想，即在设计和部署系统时就做好了足够的冗余，从而保证部分系统失效的时候，整个系统仍然能够正常工作。

93715. 请简要谈谈你对可信计算基本思想的理解。

Answers

可信计算的基本思想是：（1）建立一个可信根。可信根的可信性由物理安全、技术安全与管理安全共同保证。（2）基于可信根建立一条信任链，从可信根开始到硬件平台、操作系统、应用系统逐级传递信任关系，将信任扩展到整个系统，从而确保系统整体可信。可信计算强调从可信根出发解决系统结构中的安全问题，其最本质的问题是信任问题，即通过信任链确保每一个环节的身份可信，从而保证从起点的可信根到后续的可信应用的信任关系是可靠的，为计算机系统安全提供一体化的安全保证。

93716. 零信任网络的核心思想是什么？这种安全机制有哪些基本的假定？

Answers

零信任网络的核心思想是“从来不信任，始终在校验”（Never Trust, Always Verify）。在《零信任网络：在不可信网络中构建安全系统》一书中，埃文等人将零信任网络建立在 5 个基本假定之上：（1）网络无时无刻不处于危险的环境中；（2）网络中自始至终存在外部或内部威胁；（3）网络的位置不足以决定网络的可信程度；（4）所有的设备、用户和网络流量都应当经过认证和授权；（5）安全策略必须是动态的，并基于尽可能多的数据源计算而来。

数据加密

93717. 一个密码系统至少由明文、密文、加密算法、解密算法和密钥 5 部分组成，而其安全性是由（）决定的。

Options

A. 加密算法;
B. 解密算法;
C. 加解密算法;
D. 密钥;

Answers

D. 密钥;

93718. 置换密码本质上是通过下述哪种操作实现对明文的加密（）。

Options

A. 将明文中字符的位置次序重新排列;
B. 将明文中字符替换为其他字符;
C. 在明文字符中增加其他字符;
D. 在明文字符中减少其他字符;

~~**Answers**~~

~~B. 将明文中字符替换为其他字符;~~

~~**Explain**~~

~~置换密码是将明文中的每个字符替换成密文中的另外一个字符，替换后的各字符保持原来的位置，再对密文进行替换即可恢复出明文。~~

93719. 密码学在信息安全领域中的应用是多样的，以下（）不属于密码学的具体应用。

Options

A. 保证分组传输可靠;
B. 消息完整性校验;
C. 信息加密;
D. 身份认证;

Answers

A. 保证分组传输可靠;

Explain

密码学是研究如何隐密地传递信息的学科，而分组的可靠传输并不涉及信息的隐密传输。因此，保证分组传输可靠部署于密码学的具体应用。

93720. 使用密钥 k=5 的恺撒密码对明文 university 进行加密，则加密后的密文为（）。

Options

A. zsnajwxqye;
B. zsnajwxgrs;
C. zsnajwxqyd;
D. zsnajwxqxc;

Answers

C. zsnajwxqyd;

Explain

由 k=5 可得恺撒密码表：
明文 abcdefghijklmnopqrstuvwxyz

密文 fghijklmnopqrstuvwxyzabcde

根据明文与密文的对应关系，可得密文为 zsnajwxqyd。

93721. 密码学包括哪两个相互对立的分支（）。

Options

A. 对称密码和公钥密码;
B. 密码编码学和密码分析学;
C. 序列密码与分组密码;
D. DES 和 RSA;

Answers

B. 密码编码学和密码分析学;

93722. 一次完整的 DES 密码加密需要经过（）次迭代运算。

Options

A. 8;
B. 16;
C. 20;
D. 32;

Answers

B. 16;

93723. 下列描述中，哪一项是 ECB 模式下分组密码的缺点（）。

Options

A. 不利于并行计算，目前没有已知的并行运算算法;
B. 不能隐藏明文的模式，若明文重复，则对应的密文也会重复;
C. 存在误差传送，一个加密单元的损坏，会影响多个加密单元;
D. 需要初始化向量;

Answers
B. 不能隐藏明文的模式，若明文重复，则对应的密文也会重复;
Explain

在电子密码本模式中，通常对明文分组后，使用密钥对每一组明文进行加密来获得密文分组，再将密文分组连接获得密文。因此，在该种模式中明文分组与密文分组是一一对应的关系，且每个明文分组各自独立地进行加密和解密。这也就意味着，如果明文中存在多个相同的明文分组，则对这些明文分别进行加密得到的密文也相同。这样，恶意攻击者只需要观察密文就可以推知明文中存在怎样的重复组合，并以此为线索破译密码，因此电子密码本模式存在明显的风险。

93724. 在 DES 加密的过程中，非线性的结构变换发生在下列哪一部件中（）。

Options
A. E 盒;
B. S 盒;
C. P 盒;
D. N 盒;
Answers
B. S 盒;
Explain

S 盒作为 DES 算法中唯一的非线性部件，具有抵抗差分密码分析和线性密码分析的能力。因此，S 盒密码性质的好坏会直接影响到 DES 算法的安全性。

93725. 公钥密码学的思想最早由（）提出。

Options
A. 香农（Claude Elwood Shannon）;
B. 迪菲（Whitefield Diffie）和赫尔曼（Martin Hellman）;
C. 李维斯特（Ron Rivest）、萨莫尔（Adi Shamir）和阿德曼（Leonard Adleman）;
D. 图灵（Alan Mathison Turing）;
Answers
B. 迪菲（Whitefield Diffie）和赫尔曼（Martin Hellman）;

93726. 若 Alice 给 Bob 发送一封邮件，并想让 Bob 确信邮件是 Alice 发出的，则 Alice 应该选用哪种密钥对邮件加密（）

Options
A. Alice 的公钥;
B. Alice 的私钥;
C. Bob 的公钥;
D. Bob 的私钥;
Answers
B. Alice 的私钥;
Explain

消息发送者使用自身私钥对消息进行加密可以起到数字签名的作用，消息接收者使用消息发送者的公钥即可验证消息发送者身份。

93727. 在 RSA 算法中，取 p=3，q=11，E=3，则 D 为（）

Options
A. 5;
B. 20;
C. 14;
D. 7;
Answers
D. 7;
Explain

N=p*q=33，L=lcm(3-1，11-1)=10。则 1<D<10，且 3*D mod 10 = 1，则 D=7。

93728. RSA 密码体制的安全性是基于（）

Options
A. 大整数分解问题;
B. 离散对数问题;
C. 背包问题;
D. 格困难问题;
Answers
A. 大整数分解问题;

93729. 关于散列函数，下列叙述中不正确的是（）

Options
A. 输入任意大小的消息，输出是一个长度固定的摘要;
B. 输入消息中的任何变动都会对输出摘要产生影响;
C. 输入消息中的细微变动不会对输出摘要产生影响;
D. 可以防止消息被篡改;

Answers
C. 输入消息中的细微变动不会对输出摘要产生影响;

93730. 关于数字签名，下列叙述中正确的是：（）

Options
A. 数字签名是在所传输的数据后附加一段与传输数据毫无关系的数字信息;
B. 数字签名可以保证数据的安全传输;
C. 数字签名一般采用对称加密机制;
D. 数字签名可以用于验证消息发送方的身份;

Answers
D. 数字签名可以用于验证消息发送方的身份;

93731. 根据密码分析者所掌握的知识条件，可将密码分析分为唯密文攻击、已知明文攻击、选择明文攻击、选择密文攻击和（）

Options
A. 选择文本攻击;
B. 已知密文攻击;
C. 已知文本攻击;
D. 唯明文攻击;

Answers
A. 选择文本攻击;

Explain

按照攻击者掌握的知识条件，密码分析可分为唯密文攻击、已知明文攻击、选择明文攻击、选择密文攻击和选择文本攻击五类。

93732. 密码分析者欲对某一密码体制发起唯密文攻击时需要掌握的信息是（）

Options
A. 使用同一密钥加密的多个消息的密文;
B. 消息的部分明文及其对应的密文;
C. 交易发送方的身份信息;
D. 消息的摘要;

Answers
A. 使用同一密钥加密的多个消息的密文;

Explain

唯密文攻击（Ciphertext-Only Attack）：密码分析者已知一些用同一密钥加密的多个消息的密文，其任务是尽可能恢复足够多的明文或者推算出加密消息的密钥。

93733. 下列算法中既可以用于消息加密，也可以用于数字签名的是：（）

Options
A. RSA;
B. DES;
C. Caesar;
D. SHA-256;

Answers
A. RSA;

93734. 密码学的发展历史主要包括以下哪几个阶段（）。

Options
A. 古典密码阶段;
B. 近代密码阶段;
C. 商用密码阶段;
D. 现代密码阶段;

Answers
A. 古典密码阶段;
B. 近代密码阶段;
D. 现代密码阶段;

Explain

密码学发展历史古典密码阶段一般指 1949 年之前的时期，其基本特点是手工加密和解密；近代密码阶段一般指 1949 年~1975 年的时期，其主要特点是采用机械或机电密码机进行加密和解密；现代密码阶段一般指 1975 年至今的时期，其主要特点是采用计算机进行加密和解密。

93735. 导致 OTP 密码实用性差的原因包括：（）

Options
A. 密钥的同步问题;
B. 密钥保存问题;
C. 密钥的重用问题;
D. 安全性差，易被破解;

Answers
A. 密钥的同步问题;
B. 密钥保存问题;
C. 密钥的重用问题;

Explain

密钥的同步问题：由于一次性密码本的密钥长度至少要与明文长度等同，那么当明文很长时，一次性密码本也会跟着变长。如果明文是一个大小为 10GB 的文件，则密钥的大小至少也需要 10GB；而且在通信过程中，发送方和接收方的密钥的比特序列不允许任何错位，否则错位的比特后的所有信息将无法被解密。

B.密钥保存问题：如果有办法安全保存与明文一样长的密钥，那不是也可以用同样的办法安全保存明文本身吗？如果真有这样的方法，我们根本就不需要密码了。
C.密钥的重用问题：作为密钥的比特序列一旦被泄密，过去所有的机密通信内容将全部被解密，因此在一次性密码本中绝对不能重用随机比特序列。

93736. 下列密码算法中，属于分组密码的算法是（ ）

Options

A. DES;
B. TDES;
C. RC4;
D. OTP;

Answers

A. DES;
B. TDES;

93737. 简要说明计算机密码学发展的三个时期。

Answers

古典密码阶段一般指 1949 年之前的时期，其基本特点是手工加密和解密；近代密码阶段一般指 1949 年~1975 年的时期，其主要特点是采用机械或机电密码机进行加密和解密；现代密码阶段一般指 1975 年至今的时期，其主要特点是采用计算机进行加密和解密。

93738. 请简述散列函数所具备的性质。

Answers

（1）根据任意长度的消息计算出固定长度的消息摘要：不论散列函数的输入消息长度有多长，所输出的摘要都应该是固定长度的。
（2）能够快速计算出摘要：由于散列函数常常被用来检验消息的完整性，若生成摘要所需计算时间过长，甚至超过了检验消息本身所需要花费的时间，那么摘要的计算将毫无意义。
（3）单向性：单向性指散列函数可以很容易地根据消息计算其摘要，但无法通过摘要反向计算出消息本身
（4）抗碰撞性：由两个不同的消息计算得到相同摘要的情况称为碰撞。难以发现碰撞的性质则称为抗碰撞性。

93739. 请简述分组密码与流密码的不同之处。

Answers

分组密码（Block Cipher）是每次只能处理特定长度的一块数据的一类密码算法，当需要加密的明文长度超过分组密码的分组长度时，需要对分组密码算法进行迭代。流密码对数据进行处理时并不需要按长度对数据进行分组，而是直接对数据流进行连续处理，因此需要保持内部状态。

93740. 与对称密码相比，公钥密码具有哪些优点和不足？

Answers

优点：
（1）通讯网络中的每个用户只需保管自己的私钥，密钥数量相对较少；
（2）密钥分发简单，安全性高
（3）可以实现数字签名
缺点：与对称密码相比，公钥密码的加密和解密处理速度较慢

93741. 请简要介绍 SHA-256 算法生成摘要的流程。

Answers

SHA-256 是 SHA-2 标准下细分出的一种散列函数。SHA-256 算法以长度为 $1 \sim 2^{64} - 1$ 位的信息作为输入，以 256 位的摘要作为输出。在该算法中，输入信息会被分成一个或者多个长为 512 位的信息块，并逐块进行处理。为此，算法的输入信息首先要进行比特填充，直到信息长度为 512 的倍数。紧接着，从第一个信息块开始，每个信息块都与一个 256 位的状态块一并被映射函数处理为一个 256 位的临时摘要，而该临时摘要将作为处理下一个信息块所需的状态块。最终输出的是最后一个信息块的摘要。

隐私保护

93742. 2018 年 5 月 25 日，欧盟的（ ）正式生效，这是目前在隐私保护领域应用范围最广以及最受关注的一部法律。该法律将会对违反其法律条款的企业进行罚款，罚款最高可达到两千万欧元或者企业全年全球营业总额的 4%。

Options

A.《联邦数据保护法》；
B.《隐私权法》；
C.《数据保护法》；
D.《通用数据保护条例》；

Answers

D.《通用数据保护条例》；

Explain

欧盟在 2018 年 5 月 25 日生效的《通用数据保护条例》（General Data Protection Regulation，GDPR）受到了各界人士的广泛关注。该法律保护了欧洲公民的个人数据，只要处理的数据涉及欧洲公民的个人数据，企业一旦违反其法律条款，将会受到最高达两千万欧元或者企业全年全球营业总额的 4%的罚款。所以正确答案是 D。

93743. 以下选项中描述匿名化思想的是（ ）。

Options

A. 通过利用多种密码学工具实现保护隐私的多方协同合作框架来保护隐私;
B. 通过隐藏用户身份和数据的对应关系来保护隐私;
C. 通过对数据进行加密并直接处理密文来保护隐私;
D. 通过在统计结果中加入噪声使某些输出难以区分来保护隐私;

Answers

B. 通过隐藏用户身份和数据的对应关系来保护隐私;

Explain

匿名化的思想是通过隐藏用户身份和数据的对应关系来保护隐私，为了实现匿名化，抵御连接攻击，研究人员提出了一系列匿名化隐私保护模型。所以正确答案是 B。

93744. 数据表中的准标识符是指（ ）。

Options

A. 唯一标识个体身份的属性或者属性的集合;
B. 可以与其他数据表进行链接以标识个体身份的属性或属性组合;
C. 发布时需要保密的属性;
D. 以上答案全部错误;

Answers

B. 可以与其他数据表进行链接以标识个体身份的属性或属性组合;

Explain

准标识符是指与其他数据表进行链接以标识个体身份的属性或属性组合，如性别、出生日期、邮政编码等，准标识符的选择由进行链接的外部数据表决定。所以正确答案是 B。

93745. 若攻击者通过将选民信息表中某条记录的性别、年龄、出生日期和邮政编码信息（即准标识符）与匿名病患信息表中某条记录的性别、年龄、出生日期和邮政编码信息匹配成功，从而推断出张三患有糖尿病，那么攻击者执行的攻击为（ ）。

Options

A. 差分攻击;
B. 链接攻击;
C. 同质性攻击;
D. 背景知识攻击;

Answers

B. 链接攻击;

Explain

准标识符可能被攻击者用来与其他能够获得的公共数据集联系起来，获得隐私信息，这种攻击被称为链接攻击。如果攻击者掌握的两个数据集中有重叠的属性，就有可能通过链接攻击推断出用户的信息。所以正确答案是 B。

93746. 若攻击者在已掌握选民信息表的基础上对某个已经删去标识符的匿名病患数据表进行链接攻击时发现，匿名病患数据表中具有相同准标识符的记录最少有 x 条，即某选民的准标识符最少与匿名病患数据表中 x 条记录的准标识符相匹配，那么该匿名病患数据表符合（ ）隐私保护模型的要求。

Options

A. k-anonymity;
B. l-diversity;
C. t-closeness;
D. 以上答案全部错误;

Answers

A. k-anonymity;

Explain

如果将数据表中具有相同准标识符的记录放在一起，并将其称为一个等价类，k- anonymity 隐私保护模型要求对于每一条记录来说，等价类中至少包含 k-1 个与该记录无法区分的记录来降低数据的识别度，从而抵御链接攻击。所以正确答案是 A。

93747. 若攻击者在已掌握选民信息表的基础上对某个已经删去标识符的匿名病患数据表进行链接攻击时发现，选民张三在选民信息表中的准标识符与匿名病患数据表中的 x 条记录的准标识符相匹配，虽然攻击者不确定具体哪条记录属于张三，但是由于这 x 条记录的疾病属性值均为糖尿病，因此攻击者推断张三患有糖尿病。该攻击属于（ ）。

Options

A. 差分攻击;
B. 链接攻击;
C. 同质性攻击;
D. 背景知识攻击;

Answers

C. 同质性攻击;

Explain

在对数据进行匿名化时，如果不对敏感属性的属性值进行约束，当同一个等价类中的记录的敏感属性值取值单一甚至全部相同时，只要攻击者定位到该等价类，即使不知道对应的记录具体是哪条，攻击者根据等价类中单一的敏感属性值也能推断出用户隐私，此种攻击被称为同质性攻击。所以正确答案是 C。

93748. 以下选项中描述的是差分隐私思想的是（ ）。

Options

A. 通过利用多种密码学工具实现保护隐私的多方协同合作框架来保护隐私;
B. 通过隐藏用户身份和数据的对应关系来保护隐私;
C. 通过对数据进行加密并直接处理密文来保护隐私;
D. 通过在统计结果中加入噪声使得同一个体在或不在数据集中时查询得到的结果没有显著变化来保护隐私;

Answers

D. 通过在统计结果中加入噪声使得同一个体在或不在数据集中时查询得到的结果没有显著变化来保护隐私;

Explain

差分隐私是一种安全发布数据的隐私保护机制，它通过在查询结果中添加噪声，使得同一个体在或不在数据集中时查询得到的结果没有显著变化来保护个体隐私。所以正确答案是 D。

93749. 差分隐私是一种安全发布数据的隐私保护机制，它可以抵抗（ ），保护数据集中每个个体的隐私。

Options

A. 差分攻击;
B. 同质性攻击;
C. 链接攻击;
D. 背景知识攻击;

Answers

A. 差分攻击;

Explain

差分隐私是一种安全发布数据的隐私保护机制，它可以抵抗差分攻击，保护数据集中每个个体的隐私。它通过在查询结果中添加噪声，使得同一个体在或不在数据集中时查询得到的结果没有显著变化来保护个体隐私。所以正确答案是 A。

93750. 当差分隐私中的隐私保护预算降低时，差分隐私提供的隐私保护能力（ ）。

Options

A. 减弱;
B. 不发生变化;
C. 增强;
D. 以上答案全部错误;

Answers

C. 增强;

Explain

差分隐私中的差分隐私预算越小，作用在一对邻近数据集上的差分隐私算法返回的查询结果的概率分布越相似，攻击者越难区分邻近数据集，因此提供的隐私保护能力越强。所以正确答案是 C。

93751. 对于诸如疾病种类之类的非数值型数据，一般采用（ ）来实现差分隐私保护。

Options

A. 拉普拉斯机制;
B. 高斯机制;
C. 指数机制;
D. 以上答案全部错误;

Answers

C. 指数机制;

Explain

差分隐私处理的数据主要有数值型数据和非数值型数据，对于数值型数据，一般采用拉普拉斯机制和高斯机制来实现差分隐私保护，对于非数值型数据，一般采用指数机制来实现差分隐私保护。所以正确答案是 C。

93752. 以下选项中描述的是同态加密思想的是（ ）。

Options

A. 通过利用多种密码学工具实现保护隐私的多方协同合作框架来保护隐私;
B. 通过隐藏用户身份和数据的对应关系来保护隐私;
C. 通过对数据进行加密并直接处理密文来保护隐私;
D. 通过在统计结果中加入噪声使某些输出难以区分来保护隐私;

Answers

C. 通过对数据进行加密并直接处理密文来保护隐私;

Explain

同态加密通过对数据进行加密来保护数据的机密性，通过直接对加密数据进行操作来保证数据的流通和合作。所以正确答案是 C。

93753. 第一个全同态加密方案的构造者克雷格·金特里（Craig Gentry）曾经说过“A way to delegate processing of your data, without giving a way access to it”即“一种无需授予对数据的访问权就可以委托他人对数据进行处理的方法”，这是对（ ）的描述。

Options

A. 匿名化;
B. 差分隐私;
C. 同态加密;
D. 安全多方计算;

Answers

C. 同态加密;

Explain

第一个全同态加密方案的构造者克雷格·金特里（Craig Gentry）认为同态加密可以被定义为“A way to delegate processing of your data, without giving a way access to it”，即“一种无需授予对数据的访问权就可以委托他人对数据进行处理的方法”。所以正确答案是 C。

93754. 帕斯卡·佩利尔（Pascal Paillier）1999 年提出的 Paillier 加密算法是典型的（ ）加密算法。

Options

A. 全同态;
B. 乘法同态;
C. 浅同态;
D. 加法同态;

Answers

D. 加法同态;

Explain

Paillier 算法是第一种也是应用最广泛的具有加法同态性质的加密算法，该算法由帕斯卡·佩利尔（Pascal Paillier）于 1999 年提出。所以正确答案是 D。

93755. 现在有两个明文 7 和 2，若使用 Paillier 加密算法生成一对公私钥并分别对这两个明文进行加密，那么两密文相乘所得值的解密值为（ ）。

Options

A. 5;
B. 9;
C. 14;
D. 3;

Answers

B. 9;

Explain

Paillier 算法是第一种也是应用最广泛的具有加法同态性质的加密算法，该算法由帕斯卡·佩利尔（Pascal Paillier）于 1999 年提出。使用 Paillier 加密算法对明文加密得到密文后，密文相乘再解密的结果与明文相加的结果相同。所以正确答案是 B。

93756. RSA 公钥加密算法是典型的（ ）加密算法。

Options

A. 全同态;
B. 乘法同态;
C. 浅同态;
D. 加法同态;

Answers

B. 乘法同态;

Explain

RSA 公钥加密算法是最早的具有乘法同态性质的加密方案，该算法由罗纳德·李维斯特（Ronald Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman）于 1977 年共同提出。所以正确答案是 B。

93757. 全同态加密是（ ）的同态加密方案。

Options

A. 同时满足加法同态和乘法同态并且可以进行任意多次加和乘运算;
B. 支持加法同态;
C. 支持乘法同态;
D. 同时满足加法同态和乘法同态但只能进行有限次的加和乘运算;

Answers

A. 同时满足加法同态和乘法同态并且可以进行任意多次加和乘运算;

Explain

同态加密包括仅支持加法同态（或乘法同态）的半同态加密，同时满足加法同态和乘法同态但只能进行有限次的加和乘运算的浅同态加密以及同时满足加法同态和乘法同态并且可以进行任意多次加和乘运算的全同态加密。所以正确答案是 A。

93758. 以下选项中描述的是安全多方计算思想的是（ ）。

Options

A. 通过利用多种密码学工具实现保护隐私的多方协同合作框架来保护隐私;
B. 通过隐藏用户身份和数据的对应关系来保护隐私;
C. 通过对数据进行加密并直接处理密文来保护隐私;
D. 通过在统计结果中加入噪声使某些输出难以区分来保护隐私;

Answers

A. 通过利用多种密码学工具实现保护隐私的多方协同合作框架来保护隐私;

Explain

安全多方计算是为解决一类方法提出的隐私保护框架，它能够实现互不信任的参与方之间保护隐私的协同计算，它的实现需要多种密码学工具的支持，例如秘密共享，混淆电路，同态加密等。所以正确答案是 A。

93759. 图灵奖获得者姚期智教授在 1982 年提出的“百万富翁问题”让想要比较谁更富有的两个百万富翁能够在无需提供真实财富值的情况下比较两个人财富的多少，该问题的提出标志着（ ）的诞生。

Options

A. 混淆电路协议;
B. 不经意传输协议;
C. 秘密共享协议;
D. 安全多方计算;

Answers

D. 安全多方计算;

Explain

1982 年，姚期智教授在论文“Protocols for secure computations”中提出的百万富翁问题是第一个安全两方计算问题，该问题的提出标志着安全多方计算的诞生。之后，姚期智教授又提出了安全两方计算的通用解决方案，为该领域的发展做出了开创性贡献。所以正确答案是 D。

93760. 下面属于隐私信息的包括（ ）。

Options

A. 个人账号信息;
B. 网页浏览记录;
C. 电子邮件内容;
D. 开源软件代码;

Answers

A. 个人账号信息;
B. 网页浏览记录;
C. 电子邮件内容;

Explain

隐私是个体或集体不希望被他人知晓的信息，网络空间中的隐私信息主要包括个人数据，例如个人注册的账号信息；网络行为数据即使用网络服务时产生的数据，例如用户浏览网页时产生的浏览记录；

通信内容数据，例如用户使用邮件进行通信时的通信内容。所以正确答案是 ABC。

93761. 网络空间中的数据携带着网民们的隐私信息，这些信息一旦被泄露，势必会为网民的人身财产安全带来危害，为了保护人们在使用网络服务时的隐私权，我国近些年相继颁布了（ ）等法律法规。

Options

A.《网络安全法》；
B.《个人信息安全规范》；
C.《数据安全法》；
D.《个人信息保护法》；

Answers

A.《网络安全法》；
B.《个人信息安全规范》；
C.《数据安全法》；
D.《个人信息保护法》；

Explain

为了保护人们在使用网络服务时的隐私权，我国在 2017 年颁布了《网络安全法》，在 2020 年发布了新版《个人信息安全规范》，在 2021 年表决通过了《数据安全法》，在 2021 年施行了《个人信息保护法》。所以正确答案是 ABCD。

93762. 请思考，若想要将某数据表发布出去，简单地删除或者替换表中容易推测出用户身份信息的属性是否足够安全。如果不够安全，请简述应当如何处理数据。

Answers

已有研究者证明可以通过对选举注册数据和医院出院数据执行链接攻击推测出选举人的住院信息。因此，只是简单地删除或者替换表中容易推测出用户信息的属性是不安全的，将该表发布出去有可能会泄露用户隐私。数据发布方可以对数据进行处理，使其满足隐私保护模型的要求来保护用户隐私。具体来说，数据发布方可以对已删除了标识符的数据表中的准标识符进行分类，将具有相同准标识符的记录放入同一个等价类中，保证对于任意一条记录，可以在它所在的等价类中找到至少 k-1 条具有相同等价类的记录，此时该数据表就满足了 k-anonymity 隐私保护模型的要求。当攻击者执行链接攻击定位到某一个等价类中时，由于等价类中的记录不可区分，因此降低了数据的识别度，从而在一定程度上保护了用户隐私。考虑到同质性攻击等攻击的存在，数据发布方也可以考虑对数据进行处理，使其满足 l-diversity 等隐私保护模型的要求进一步增强对用户隐私的保护。

93763. 简述什么是差分攻击以及差分隐私技术是如何抵御差分攻击的。

Answers

假设有一个医疗数据记录数据集，其中的每一条记录代表对应的用户是否患病，当攻击者通过查询得知前三行有两人患病，通过查询又得知前四行有三人患病时，他可以通过两次查询结果的差值推断出第四行记录代表的用户患病。

这种在没有**具体查询特定某个用户信息的情况下就能够获得其隐私数据的攻击被称为差分攻击**。

为了抵御差分攻击，差分隐私通过向查询结果中添加噪声，保证对于两个只有一条记录不同的数据集来说，在这两个数据集上进行同一查询得到相同结果的比值接近于 1。这样就使添加一条记录对数据集造成的隐私泄露风险被控制住了，使攻击者无法通过两次查询结果推测出有关个体的隐私信息，从而达到了防御差分攻击、保护隐私的目的。

93764. 简要分析适用于非数值型差分隐私的指数机制是如何实现隐私保护的。

Answers

指数机制的思想是为每一种可能输出的非数值型结果打分来确定每一种查询结果的输出概率，通过将确定的输出转换为具有一定概率的输出来实现隐私保护。

指数机制利用**可用性函数**来评估输出值的优劣程度，随着隐私预算的增大，可用性最高的选项被输出的概率不断增大；而当隐私预算降低时，各选项在可用性上的差异被抑制，被输出的概率趋于相同，隐私保护水平升高。

93765. 简述同态加密技术可以应用于哪些领域？。

Answers

同态加密可被应用于云计算、匿名电子投票等领域。在云计算领域，没有存储和计算能力的用户可将同态加密后的数据发送给云服务提供商并委托其进行相应的计算，云服务商利用同态加密的性质可直接对密文进行相应的处理，随后再把处理过的密文返还给用户，用户解密后即得到了做了相应处理后的明文结果。在此过程中，数据在机密性得到保证的情况下实现了流通。

在匿名电子投票领域，投票方可将同态加密后的投票结果发送给计票方，计票方只负责密文上的票数

统计，随后将统计的密文结果汇总给发布方，发布方则只能对计算好的密文进行解密从而得到投票结果。在此过程中，计票方无法知晓每一个投票结果且不能修改票面信息，无法从中作梗，公布方也无法得到单独每张票的内容，利用同态加密实现匿名电子投票既保证了投票者的隐私安全，又保证了投票结果的公证。

93766. 简述安全多方计算可能应用的场景。

Answers

安全多方计算适用于解决互不信任的参与方之间保护隐私的协同计算问题。
例如，当多家医院想要合作使用医疗数据进行科学研究、分析预测病人患病情况，但为了保护患者隐私，不能直接共享数据的场景，或者多个商家想要合作促销，统计共同的用户画像，但又不想让对方知道自己掌握的信息的场景。

系统硬件安全

93767. 在缓存侧信道攻击中需要不断探测目标数据是否被缓存，以下哪些攻击方法在探测时中无需内存读取即可判断目标数据是否被缓存（ ）。

Options

A. Prime-Probe;
B. Flush-Reload;
C. Evict-Reload;
D. Flush-Flush;

Answers

D. Flush-Flush;

Explain

Flush-Flush 攻击是基于 clflush 指令执行时间的长短来实施攻击的。如果数据没在 Cache 中则 clflush 指令执行时间会比较短，反之若有数据在 cache 中则执行时间会比较长，整个过程中不涉及内存数据的读取操作。

93768. 下面属于故障注入分析的是（ ）。

Options

A. 监视密码模块能量消耗的变化以发现指令的能量消耗模式;
B. 密码模块的执行时间与密码算法的特殊数学操作之间的关系;
C. 对微波、电压等的控制引发密码模块内部运行错误，进而进行错误、模式分析;
D. 对正在运行的密码模块和辅助设备发出的电磁信号进行远程或外部探测和接收;

Answers

C. 对微波、电压等的控制引发密码模块内部运行错误，进而进行错误、模式分析;

93769. CPU 不能直接访问的存储器是（ ）。

Options

A. ROM;
B. RAM;
C. CACHE;
D. 光盘;

Answers

D. 光盘;

93770. 计算机硬件的五大基本构件包括:运算器、存储器、输入设备、输出设备和（ ）。

Options

A. 显示器;
B. 控制器;
C. 磁盘驱动器;
D. 鼠标;

Answers

B. 控制器;

93771. 在微型计算机中，内存器编址的基本单位是（ ）。

Options

A. 二进制;
B. 字节;
C. 字;
D. 位;

Answers

B. 字节;

93772. 硬件木马的组成部分有（ ）。

Options

A. 触发器;
B. 有效负载;
C. 启动器;
D. 接收器;

Answers

A. 触发器;
B. 有效负载;

93773. 集成电路芯片的主要材料是（ ）和（ ）。

Options

A. N 型半导体;
B. P 型半导体;
C. R 型半导体;
D. S 型半导体;

Answers

A. N 型半导体;
B. P 型半导体;

93774. 在 CLKscrew 和 VoltJockey 攻击中，是分别通过（ ）和（ ）向处理器注入故障的。

Options

A. 提高处理器频率;
B. 降低处理器频率;
C. 提高处理器电压;
D. 降低处理器电压;

Answers
A. 提高处理器频率;
D. 降低处理器电压;

93775. 故障注入攻击的影响因素有（ ）。

Options
A. 故障注入的开始时间;
B. 故障注入的作用强度;
C. 故障注入的持续时间;
D. 故障注入的空间位置;

Answers
A. 故障注入的开始时间;
B. 故障注入的作用强度;
C. 故障注入的持续时间;
D. 故障注入的空间位置;

93776. 功耗侧信道攻击可以分为（ ）。

Options
A. 简单功耗分析;
B. 差分功耗分析;
C. 相关功耗分析;
D. 混合功耗分析;

Answers
A. 简单功耗分析;
B. 差分功耗分析;
C. 相关功耗分析;

93777. 在存储器隔离技术中使用（ ）和（ ）限制设备能够访问的存储器。

Options
A. 重定位寄存器;
B. 目的寄存器;
C. 界地址寄存器;
D. 数据寄存器;

Answers
A. 重定位寄存器;
C. 界地址寄存器;

93778. 常用的侧信道防护技术有（ ）。

Options
A. 旁路信道隐藏;
B. 掩码技术;
C. 设计分区;
D. 物理空间拒绝接近和访问;

Answers
A. 旁路信道隐藏;
B. 掩码技术;
C. 设计分区;
D. 物理空间拒绝接近和访问;

93779. 处理器的安全模型有（ ）。

Options
A. 特权安全模型;
B. 隔离安全模型;
C. 可信安全模型;
D. 冗余安全模型;

Answers
A. 特权安全模型;
B. 隔离安全模型;

93780. 常见的系统硬件攻击手段有（ ）。

Options
A. 漏洞攻击;
B. 硬件木马;
C. 故障注入攻击;
D. 侧信道攻击;

Answers
A. 漏洞攻击;
B. 硬件木马;
C. 故障注入攻击;
D. 侧信道攻击;

93781. 现代处理中一级缓存的组成部分有（ ）。

Options
A. 指令缓存;
B. 数据缓存;
C. 内容缓存;
D. 操作缓存;

Answers
A. 指令缓存;
B. 数据缓存;

93782. 以下哪些旁路信道可以被攻击者利用发起攻击（ ）。

Options
A. 代码运行时间;
B. 芯片运行功耗;
C. 设备产生的电磁辐射;
D. 设备产生的声波;

Answers
A. 代码运行时间;
B. 芯片运行功耗;
C. 设备产生的电磁辐射;
D. 设备产生的声波;

93783. 常见的硬件故障注入攻击方式有（ ）。

Options

A. 基于激光的故障注入攻击;
B. 基于电磁的故障注入攻击;
C. 基于处理器电压的故障注入攻击;
D. 基于处理器频率的故障注入攻击;

Answers

A. 基于激光的故障注入攻击;
B. 基于电磁的故障注入攻击;
C. 基于处理器电压的故障注入攻击;
D. 基于处理器频率的故障注入攻击;

93784. 硬件木马的检测方法有（ ）。

Options

A. 基于逻辑测试检测硬件木马;
B. 基于芯片的旁路信道参数检测硬件木马;
C. 基于逆向工程检测硬件木马;
D. 基于恶意代码扫描检测硬件木马;

Answers

A. 基于逻辑测试检测硬件木马;
B. 基于芯片的旁路信道参数检测硬件木马;
C. 基于逆向工程检测硬件木马;

93785. 物理不可克隆函数（Physical Unclonable Function, PUF）按照实现方法可分为（ ）。

Options

A. 非电子 PUF;
B. 模拟电路 PUF;
C. 数字电路 PUF;
D. 软件 PUF;

Answers

A. 非电子 PUF;
B. 模拟电路 PUF;
C. 数字电路 PUF;

93786. 隔离技术一般可分为（ ）。

Options

A. 软件隔离技术;
B. 硬件隔离技术;
C. 系统级隔离技术;
D. 代码隔离技术;

Answers

A. 软件隔离技术;
B. 硬件隔离技术;
C. 系统级隔离技术;

93787. 什么是芯片的 Setup 和 Hold 时间？

Answers

建立时间（Setup Time）是指触发器的时钟信号上升沿到来以前，数据能够保持稳定不变的时间。输入数据信号应在时钟上升沿（假设上升沿有效）T 时间前到达芯片，这个 T 就是通常所说的 Setup Time。如不满足 Setup Time，这个数据就不能被载入触发器，只有在下一个时钟上升沿到来时，数据才能被载入触发器。保持时间（Hold Time）是指触发器的时钟信号上升沿到来以后，数据保持稳定不变的时间。如果 Hold Time 不够，数据同样不能被载入触发器。

93788. 什么是电路的竞争与冒险现象？

Answers

在组合逻辑电路中，某个输入变量通过两条或两条以上的途径传到输出端，由于门电路的输入信号经过的通路不尽相同，所产生的延时也就会不同，从而导致到达输出门的时间不一致，我们把这种现象叫做竞争。由于竞争而在电路输出端可能产生尖峰脉冲或毛刺的现象叫冒险。

93789. 请结合 VoltJockey 漏洞简要描述集成时序电路的时间约束。

Answers

一个时序电路通常包括多个电子元件，这些电子元件在统一的时钟脉冲控制下运行，为了使电子元件稳定运行，每个电子元件需要在输入信号稳定后再开始处理输入数据，电子元件的输入信号需要先于时钟脉冲信号到达，并且持续一段时间。VoltJockey 攻击通过操作电压频率管理器，将受害者进程所处的处理器内核设置为合适的低电压，使得受害者内核的输入信号晚于时钟脉冲信号到达，进而造成错误的输出。

93790. 请简要描述 Prime-Probe 缓存探测的攻击过程。

Answers

Prime-Probe 缓存探测过程分为三个步骤。1）攻击者用预先准备的数据填充多个特定的 cache 组；2）等待目标进程响应服务请求，将 cache 数据更新；3）重新读取 Prime 阶段填充的数据，测量并记录各个 cache 组的读取时间。

93791. 请结合 Meltdown 漏洞简要分析乱序执行。

Answers

处理器获取指令后，将指令解码存访在执行缓冲区（保留站）中，指令将在执行缓冲区中等待，直到它的数据运算对象是可以获取的；乱寻执行技术允许后序指令先于前面指令离开缓冲区，指令离开缓冲区后会被分配给一个合适的功能单元并由之执行，然后处理器将指令的执行结果重新排序并进行安全检查（如地址访问的权限检查等），最后将检查后的结果提交给寄存器。

在 Meltdown 漏洞攻击中，一个用户级特权的攻击者首先使用缓存探测技术构造缓存监控区，然后使用越权指令尝试读取内核数据，并将处理器的读取结果映射在缓存监控区域。根据乱序执行技术，处理器会执行读取内核数据的指令，然后在安全检查之后丢弃该指令的执行结果，但处理器并不会更新缓存区状态。因此攻击者可以使用缓存探测技术窃取内核中的敏感数据。

操作系统安全

93792. 下列哪些内存区段具备可执行权限（ ）。

Options

A. 堆区（Heap）
B. 栈区（Stack）
C. 文本段（Text Segment）
D. BSS 段（BSS Segment）

Answers

C. 文本段（Text Segment）

Explain

本题考查内存段的权限。

93793. 下列哪些内存区段不具备写权限（ ）。

Options

A. 文本段（Text Segment）
B. 数据段（Data Segment）
C. 栈区（Stack）
D. 堆区（Heap）

Answers

A. 文本段（Text Segment）

Explain

本题考查内存段的权限。

93794. 莫里斯蠕虫病毒是第一个蠕虫病毒，它具体利用了哪种类型的漏洞（ ）。

Options

A. 堆区溢出
B. 微处理器架构侧信道
C. 栈区溢出
D. 网络协议漏洞

Answers

C. 栈区溢出

Explain

莫里斯蠕虫病毒采用 gets 函数构造栈溢出。

93795. 下列内存区段增长方是向低地址方向的有（ ）。

Options

A. 文本段
B. 数据段
C. 堆区
D. 栈区

Answers

D. 栈区

Explain

本题考查内存段的布局特征。

93796. 使操作系统下受害进程产生攻击者期望的异常行为的攻击效果被称为（ ）。

Options

A. 进程的控制流劫持
B. 权限提升
C. 数据窃取
D. 拒绝服务

Answers

A. 进程的控制流劫持

Explain

本题考查控制流劫持的定义。

93797. 在函数调用的过程当中，EBP 寄存器被用于保存（ ）。

Options

A. 主调函数的栈帧基地址
B. 被调函数的栈帧基地址
C. 返回地址
D. 局部变量起始地址

Answers

A. 主调函数的栈帧基地址

Explain

本题考查函数调用历程。

93798. 在函数调用历程当中，EAX 寄存被用于保存（ ）。

Options

A. 函数返回地址
B. 主调函数的栈帧基地址
C. 被调函数的栈帧基地址
D. 函数返回值

Answers

D. 函数返回值

Explain

本题考查函数调用历程。

93799. 著名的 OpenSSL 心脏滴血漏洞属于哪一类堆区漏洞（ ）。

Options

A. Heap-Overread
B. Heap-Overflow
C. Double-Free
D. Use-After-Free

Answers

A. Heap-Overread

Explain

心脏滴血漏洞通过越界读取窃取信息。

93800. W^X 内存保护方案指的是（ ）两种权限不可同时获得。

Options

A. 管理员和用户
B. 读取和写入
C. 读取和执行
D. 写入和执行

Answers

D. 写入和执行

Explain

W 是 Write 的缩写，X 是 eXecute 的缩写。

93801. Stack Canary 防御机制是通过在栈上保存的（ ）之后插入随机化内容来实现防御的。

Options

A. 栈帧基地址
B. 返回地址
C. 局部变量
D. 函数参数

Answers

A. 栈帧基地址

Explain

本题考查 Stack Canary 的原理。

93802. SMAP 和 SMEP 解决的安全问题是（ ）。

Options

A. 隐私保护
B. 内存隔离
C. 身份认证
D. 完整性校验

Answers

B. 内存隔离

Explain

SMAP 和 SMEP 是内存隔离方案。

93803. 面向返回地址编程当中的 Gadget 是以（ ）指令结尾的代码段。

Options

A. ret
B. pop
C. store
D. load

Answers

A. ret

Explain

ROP Gadget 以 ret 结尾。

93804. 下列防御方案中能在防御以栈溢出为基础的 ROP 中起到作用的是（ ）。

Options

A. NX
B. ASLR
C. SMAP
D. Stack Canary

Answers

D. Stack Canary

Explain

Stack Canary 可以防御栈溢出。

93805. GOT Hijacking 当中的全局偏置表位于（ ）。

Options

A. Text Segment
B. Data Segment
C. BSS Segment
D. Map Segment

Answers

B. Data Segment

Explain

全局偏置表位于数据段。

93806. 指向全局偏置表（GOT）的程序链接表（PLT）位于（ ）。

Options

A. Text Segment

B. Data Segment
C. BSS Segment
D. Map Segment

Answers

A. Text Segment

Explain

PLT 位于文本段。

93807. 控制流完整性保护需要借助（ ）实现保护能力。

Options

A. 程序依赖图
B. 控制流图
C. 数据流图
D. 抽象语法树

Answers

B. 控制流图

Explain

本题考查 CFI 的原理。

93808. 信息流控制解决的根本问题是：（ ）。

Options

A. 身份验证
B. 信息完整性保护
C. 访问权限控制
D. 资源管理

Answers

C. 访问权限控制

Explain

IFC 解决访问控制问题。

93809. 信息流控制的三要素是（ ）。

Options

A. 约束
B. 权限
C. 属性
D. 标识

Answers

A. 约束
B. 权限
C. 属性

Explain

本题考查 IFC 的原理。

93810. 下列漏洞是因为操作系统的 I/O 管理模块设计或实现不当而产生的是（ ）。

Options

A. BadUSB
B. BlueBrone
C. BleedingBit
D. TLS Padding Oracle

Answers

A. BadUSB
B. BlueBrone
C. BleedingBit

Explain

本题考查 I/O 子系统安全问题。

93811. ASLR 随机化的内存区段有（ ）。

Options

A. 堆区（Heap）
B. 栈区（Stack）
C. 数据段（Data Segment）
D. 内存映射段（Map Segment）

Answers

A. 堆区（Heap）
B. 栈区（Stack）
C. 数据段（Data Segment）

Explain

本题考查 ASLR 的原理。

93812. 请简述堆区的 UAF 漏洞的产生的原因。

Answers

在某一堆块被释放后使用该堆块。

Explain

本题考查 UAF 的定义。

93813. 请简述面向返回地址编程（ROP）的原理，以及 ASLR、W^X、Stack Canary 在阻碍攻击者设计实施 ROP 时起到的作用。

Answers

ROP 采用位于代码段的一系列 Gadget（以 ret 结尾的代码片段）拼凑出恶意程序，ASLR 不随机化代码段，无法起作用；代码段上必有执行权限，W^X 不起作用，Stack Canary 可以检测 ROP 修改了函数返回地址，因而可以起到作用。

Explain

本题考查 ROP 的流程和常见内存保护方案的原理。

93814. 请简述全局偏执表劫持攻击（GOT Hijacking）的流程，并分析 ASLR 和 W^X 能否防御这种攻击。

Answers

全局偏执表劫持攻击通过修改全局偏置表篡改被调函数代码的地址，ASLR 无法防御该攻击，因为索引 GOT 的 PLT 位于代码段，ASLR 不随机化代码段基地址。W^X 也无法防御该攻击，因为共享库必有可执行权限。

Explain

本题考查全局偏置表劫持攻击的流程和常见内存保护方案的原理。

93815. 请简述 CFI 在防御控制流劫持攻击时的两个关键阶段。

Answers

1.获得程序的控制流图 2.根据控制流图判断控制流转移的合法性

Explain

本题考查 CFI 的原理和流程。

93816. 请描述 IFC 防御非法访问的流程，并讨论为什么 IFC 难以被部署。

Answers

判断进程的权限满足约束对其中全部属性的要求。IFC 当中的属性、权限、约束均依赖人工设计，配置开销过大。

Explain

本题考查 IFC 的原理和运行流程，并探讨 IFC 的可部署性。

TCP/IP 协议栈安全

93817. 第 8 章 TCP/IP 协议栈安全的研究范畴不包括（ ）？

Options

A. 协议栈的安全漏洞
B. 侧信道
C. 协议栈不当实现
D. 掉电、硬盘损坏等随机故障

Answers

D. 掉电、硬盘损坏等随机故障

93818. 以太网网卡的默认 MTU 大小为（ ）字节。

Options

A. 1000
B. 1500
C. 2000
D. 3000

Answers

B. 1500

93819. ping flooding 是一种基于（ ）协议的 DDoS 攻击，攻击者伪装成受害主机，广播发送大量的 ping 请求，然后短时间内受害主机就会收到大量的回复，消耗主机资源，主机资源耗尽后就会瘫痪或者无法提供其他服务。

Options

A. IP
B. TCP
C. UDP
D. ICMP

Answers

D. ICMP

93820. TCP 源端口的范围是[0，（ ）]。

Options

A. 1023
B. 4095
C. 32767
D. 65535

Answers

D. 65535

93821. 常见的 Web 威胁不包括（ ）？

Options

A. 跨站脚本攻击 XSS
B. SQL 注入
C. 跨站请求伪造
D. ARP 污染

Answers

D. ARP 污染

93822. 一个旁路的攻击者，如果要对一个目标 TCP 连接进行恶意劫持，需要推断出 TCP 连接的四元组，通常情况下，这四元组中唯一需要猜测的是（ ）？

Options

A. 源 IP 地址
B. 目的 IP 地址
C. 源端口号
D. 目的端口号

Answers

C. 源端口号

93823. 在以太网环境下，攻击者要想暴力的猜测出序列号和应答号，需要一次性发送大约（ ）个伪造报文。

Options

A. 3 万
B. 30 万
C. 3 亿
D. 30 亿

Answers

C. 3 亿

93824. 攻击者成功实施 TCP 连接劫持攻击通常需要具备两种能力：其中之一是攻击者可以进行推理猜测，成功构造出可被接收端接受的数据报文，这些报文能够通过接收端的合法性检查。该能力的前提是（ ）？

Options

A. 攻击者可以进行身份欺骗
B. 攻击者可以劫持信息
C. 攻击者可以篡改消息
D. 攻击者可以阻断连接

Answers

A. 攻击者可以进行身份欺骗

93825. 在 IPSec 的（ ）模式下，用户的整个 IP 数据包被用来计算 AH 或 ESP 头，AH 或 ESP 头以及 ESP 加密的用户数据被封装在一个新的 IP 数据包中。

Options

A. 传输
B. 隧道
C. 秘密
D. 安全

Answers

B. 隧道

93826. 攻击者可以利用（ ）攻击，绕过 TCP 对源端口号、序列号、应答号等的检查，注入伪造消息。

Options

A. IP 分片误用
B. ICMP 误用
C. IPID 侧信道
D. IP Spoofing

Answers

A. IP 分片误用

93827. 针对 ARP 污染攻击，目前已有的成熟的防御方案包括（ ）？

Options

A. MAC 地址和 IP 地址的绑定
B. unsolicited ARP reply discarding
C. IPSec
D. TLS

Answers

A. MAC 地址和 IP 地址的绑定
B. unsolicited ARP reply discarding

93828. 常见的 IPID 分配算法主要包括（ ）？

Options

A. 基于全局计数器的 IPID 分配
B. 单连接的 IPID 分配
C. 随机的 IPID 分配
D. 基于哈希值的 IPID 分配
E. 单目标的 IPID 分配

Answers

A. 基于全局计数器的 IPID 分配
B. 单连接的 IPID 分配
C. 随机的 IPID 分配
D. 基于哈希值的 IPID 分配
E. 单目标的 IPID 分配

93829. 一个旁路的攻击者，如果要对一个目标 TCP 连接进行恶意劫持，除了源端口号之外，攻击者还需要猜测 TCP 连接报文中的（ ）字段。

Options

A. 校验和
B. 序列号
C. 应答号
D. IPID

Answers

B. 序列号
C. 应答号

93830. 在 SYN Flooding 攻击中，发送大量伪造的 TCP 连接请求可能会导致目标服务器（ ）？

Options

A. 资源耗尽
B. CPU 满负荷
C. 内存不足
D. 性能提升

Answers

A. 资源耗尽
B. CPU 满负荷
C. 内存不足

93831. 在网络通信中，每一个通信参与者都会有自己确定的身份标识，比如（ ）等。

Options

A. 链路层的 MAC 地址
B. IP 层的 IP 地址
C. 传输层的端口号
D. 通信用户的身份证

Answers

A. 链路层的 MAC 地址
B. IP 层的 IP 地址
C. 传输层的端口号

93832. 协议栈安全的基本防御手段包括（ ）？

Options

A. 基于真实源地址的网络安全防御
B. 增强协议栈随机化属性
C. 安全加密机制 IPSec
D. 安全加密机制 TLS

Answers

A. 基于真实源地址的网络安全防御
B. 增强协议栈随机化属性
C. 安全加密机制 IPSec

D. 安全加密机制 TLS

93833. 在具体研究和实践层面，移动目标防御技术的层次或维度包括（ ）？

Options

A. 系统指令随机化
B. 网络特征随机化
C. 动态编译
D. 无法判断

Answers

A. 系统指令随机化
B. 网络特征随机化
C. 动态编译

93834. IPSec 提供的安全机制包括（ ）？

Options

A. 身份认证
B. 入侵监测
C. 传输加密
D. 病毒检测

Answers

A. 身份认证
C. 传输加密

93835. TLS 协议通常在 TCP 等传输层协议之上运行，其提供的基本安全功能包括（ ）？

Options

A. 通过加密阻止第三方对传输数据的窃听
B. 身份验证，确保交换信息的各方是它们声称的身份
C. 完整性保护，验证数据是否被伪造或被篡改
D. 无法判断

Answers

A. 通过加密阻止第三方对传输数据的窃听
B. 身份验证，确保交换信息的各方是它们声称的身份
C. 完整性保护，验证数据是否被伪造或被篡改

93836. 网络安全防御系统的设计与实现，通常遵循的原则包括（ ）？

Options

A. 最小权限原则
B. 纵深防御原则
C. 防御多样性原则
D. 安全性与代价平衡原则

Answers

A. 最小权限原则
B. 纵深防御原则
C. 防御多样性原则
D. 安全性与代价平衡原则

93837. ARP poisoning 攻击是否可以跨局域网，为什么？

Answers

不行，因为 ARP 协议运行于局域网中。

93838. 对比说明，IPv6 协议相比 IPv4 协议，在哪些方面进行了安全性增强？

Answers

a、可溯源和防攻击：IPv6 终端之间可以直接建立点到点的连接，无需地址转换，因此容易溯源。IPv6 地址分为 64 位的网络前缀和 64 位的接口地址，使得网络扫描的难度和代价都大大增加，进一步防范了攻击。
b、支持 IPSec 安全加密机制：IPv6 协议中默认集成了 IPSec 安全功能，通过扩展认证报头(AH)和封装安全载荷报头(ESP)实现加密和验证功能。
c、NDP 和 SEND 的安全增强：IPv6 协议采用邻居发现协议（NDP）取代现有 IPv4 中的 ARP 及部分 ICMP 控制功能。NDP 协议通过在节点之间交换 ICMPv6 信息报文和差错报文实现链路层地址及路由发现、地址自动配置等功能。IPv6 的安全邻居发现协议（SEND）协议是 NDP 的一个安全扩展，通过独立于 IPSec 的另一种加密方式保护 NDP，保证了传输的安全性。
d、保护终端用户隐私：IPv6 协议具有一些通过隐藏接口标识符(IID)来保护用户隐私的特定方法。

93839. 针对 TCP DoS 攻击，操作系统内核层面有哪些主要的安全防御方法？

Answers

操作系统内核中设置了 SYN Cookie 等安全防御方法。

93840. 请分析说明，流量加密是否一定能阻止中间人攻击？

Answers

不一定，如 HTTPS 会话中，如果攻击者利用侧信道等推断出 TCP 首部的如序列号、源端口号等字段，可以发送一个 TCP RST 报文阻断连接。

93841. 除第 8 章：TCP/IP 协议栈安全总结的 2 个协议栈根本缺陷之外，你认为协议栈还有哪些共性的安全漏洞或缺陷？

Answers

如协议栈底层加密保护做得不够，需要上层协议不断增加加密措施（如 HTTPS、TCP 中的 MD5 选项等）以提升安全性。

DNS 安全

93842. DNSSEC 基于 DNS 区域层次结构提供信任链，DoH 与 DoT 的信任基础是（ ）。

Options

A. PKI
B. HTTPS
C. RPKI
D. TLS

Answers

A. PKI

93843. 下列关于认证 DNSSEC 报文流程和 DNS 解析流程的说法错误的是（ ）。

Options

A. 认证 DNSSEC 报文的流程和 DNS 解析流程刚好是相反的
B. 完整的 DNS 解析流程是从根服务器依次往下，先从根服务器查询
C. DNSSEC 的认证流程是从权威域名服务器依次往上，直到到达根服务器
D. 完整的 DNS 解析流程是从权威域名服务器依次往上，直到到达根服务器

Answers

D. 完整的 DNS 解析流程是从权威域名服务器依次往上，直到到达根服务器

93844. DNS 应答报文中，A 记录是指（ ）。

Options

A. 域名对应主机的 IPv6 地址
B. 域名对应主机的 IPv4 地址
C. 域名对应权威服务器的域名
D. 域名指向的别名记录

Answers

B. 域名对应主机的 IPv4 地址

93845. DNS 远程缓存中毒攻击中，如果攻击者针对一个查询的回复部分进行伪造，则影响面为：（ ）。

Options

A. 本地 DNS 服务器接受并缓存的该查询对应的主机名
B. 本地 DNS 服务器缓存的所有主机名
C. 向本地 DNS 服务器发起查询的部分域的所有主机名
D. 向本地 DNS 服务器发起查询的所有域的所有主机名

Answers

A. 本地 DNS 服务器接受并缓存的该查询对应的主机名

93846. 根域名服务器采用了（ ），能够有效防御 DDoS 攻击。

Options

A. 加密机制
B. 分布式部署机制
C. 私钥签名机制
D. 层次化结构

Answers

B. 分布式部署机制

93847. 理论上，DNS 层次化域名空间分配最多可有（ ）层。

Options

A. 127
B. 128
C. 255
D. 256

Answers

A. 127

93848. 下列关于 DNS 本地缓存中毒攻击的说法正确的是（ ）。

Options

A. 得到 DNS 查询请求包的源端口号和事务 ID，攻击者就可以伪造应答包
B. 攻击者与本地 DNS 服务器处于同一局域网，无需事务 ID 即可成功伪造应答包
C. 攻击者通过伪造 URL 欺骗用户
D. 攻击者对回复部分进行伪造，可以随意欺骗整个目标域的主机名

Answers

A. 得到 DNS 查询请求包的源端口号和事务 ID，攻击者就可以伪造应答包

93849. DNSSEC 通过（ ）的方式建立信任链。

Options

A. 上级权威域名服务器为下级权威域名服务器提供公钥验证
B. 权威域名服务器通过网状方式互相提供公钥验证
C. 根域名服务器为每个权威域名服务器提供公钥验证
D. 权威域名服务器自己的私钥签名

Answers
A. 上级权威域名服务器为下级权威域名服务器提供公钥验证

93850. DNS 查询使用 DoT 后，通过（ ）提升安全性能。

Options
A. 通过从根域名到权威域名服务器的证书信任链
B. 让域名 IP 地址对应的服务器提供根域名服务器签名的公钥证书
C. 在得到域名 IP 地址后，客户端询问 IP 地址的所有者，让其提供域名所有权的证明
D. 采用 HTTPS 传输域名协议数据

Answers
C. 在得到域名 IP 地址后，客户端询问 IP 地址的所有者，让其提供域名所有权的证明

93851. DNS 缓存中毒是指利用（ ），使得受害者将被篡改的虚假信息缓存，达到持续造成危害的目的。

Options
A. 权威域名服务器的漏洞
B. 根域名服务器的缓存机制
C. DNS 查询客户端的缓存机制
D. 本地 DNS 服务器的缓存机制

Answers
D. 本地 DNS 服务器的缓存机制

93852. DNSSEC 通过上级权威域名服务器为下级权威域名服务器提供公钥验证的方式建立信任链，信任链的顶端以（ ）作为信任锚。

Options
A. 多个权威域名服务器公钥
B. 根服务器公钥
C. 根服务器私钥
D. 本地 DNS 服务器公钥

Answers
B. 根服务器公钥

93853. Kaminsky 攻击促使本地 DNS 服务器缓存失效的方法是（ ）。

Options
A. 发送 DNS 请求给目标本地 DNS 服务器
B. 局域网嗅探得到每次 DNS 查询的事务 ID
C. 不断查询随机化的域名并有针对性的伪造授权记录
D. 直接伪造应答包回复记录通知本地 DNS 服务器更新

Answers
C. 不断查询随机化的域名并有针对性的伪造授权记录

93854. 下列关于本地 DNS 服务器和权威 DNS 服务器的说法正确的是（ ）

Options
A. 本地 DNS 服务器与客户端位于同一局域网
B. 缓存中毒攻击主要针对权威 DNS 服务器
C. 本地 DNS 服务器对客户端查询采用递归解析
D. 权威 DNS 服务器可以采用分布式部署方式缓解 DDoS 攻击

Answers
C. 本地 DNS 服务器对客户端查询采用递归解析
D. 权威 DNS 服务器可以采用分布式部署方式缓解 DDoS 攻击

93855. 下列可能属于 DNS 解析过程中薄弱环节的是：（ ）

Options
A. 明文传输
B. 不进行身份认证
C. 复杂的解析依赖和管理者存在的拼写配置错误
D. 根域名服务器的分布式部署机制

Answers
A. 明文传输
B. 不进行身份认证
C. 复杂的解析依赖和管理者存在的拼写配置错误

93856. 下列关于 DNSSEC 的描述正确的是（ ）。

Options
A. DNSSEC 提供了可认证的授权记录
B. DNSSEC 部署成本高，难以快速推进
C. DNSSEC 对交互数据进行加密，提升了安全性
D. DNSSEC 实现和配置过程可能引入新的错误，导致区域文件中子域名信息泄露

Answers
A. DNSSEC 提供了可认证的授权记录
B. DNSSEC 部署成本高，难以快速推进
D. DNSSEC 实现和配置过程可能引入新的错误，导致区域文件中子域名信息泄露

93857. 下列属于加密 DNS 协议的是（ ）。

Options
A. DoT
B. LDNS

C. DoH
D. DNSKEY

Answers

A. DoT
C. DoH

93858. 恶意权威服务器可以在附加部分直接指定域名对应的 IP 地址，比如，attack.com 权威域名服务器，在针对查询 www.attack.com 的应答报文附加部分加上另一个域名 www.thucsnet.com 的 IP 地址，此时正确的做法是：（ ）。

Options

A. 对不在查询域内的附加字段，本地 DNS 服务器可以丢弃这些信息
B. 对不在查询域内的附加字段，本地 DNS 服务器可以接受这些信息
C. 对在查询域内的附加字段，本地 DNS 服务器直接接受这些信息
D. 对在查询域内的附加字段，本地 DNS 服务器有必要对每个附加部分的域名再进行一次查询

Answers

A. 对不在查询域内的附加字段，本地 DNS 服务器可以丢弃这些信息
D. 对在查询域内的附加字段，本地 DNS 服务器有必要对每个附加部分的域名再进行一次查询

93859. 下列说法正确的是（ ）。

Options

A. 如果攻击者通过某种方式直接控制了权威域名服务器，对 DNS 查询生成恶意应答，就能达到劫持终端用户访问流量的目的
B. 攻击者如果发现拼写或配置错误的授权记录，就可以申请这个错误记录对应的域名，进而实现劫持特定权威域名服务器的目的
C. 对基于 IP 地址过滤的防火墙，恶意域名服务器可以在反向查找时回复伪造域名信息逃避
D. 当授权记录和问题记录能够对应起来时，本地 DNS 服务器可采信附加记录中域名对应的 IP 地址，不会带来安全问题

Answers

A. 如果攻击者通过某种方式直接控制了权威域名服务器，对 DNS 查询生成恶意应答，就能达到劫持终端用户访问流量的目的
B. 攻击者如果发现拼写或配置错误的授权记录，就可以申请这个错误记录对应的域名，进而实现劫持特定权威域名服务器的目的

93860. 下列可以缓解或阻断远程缓存中毒攻击的方法是（ ）。

Options

A. DNS 请求和应答方交互一些侧信道攻击者不知道的秘密信息
B. UDP 源端口随机化策略
C. DNSSEC 实现安全认证
D. 降低 DNS 事务 ID 号位数

Answers

A. DNS 请求和应答方交互一些侧信道攻击者不知道的秘密信息
B. UDP 源端口随机化策略
C. DNSSEC 实现安全认证

93861. 下列关于 DNS 的描述正确的是（ ）。

Options

A. 从逻辑上，DNS 域通过层次化授权过程形成了树形结构的域名空间
B. DNS 区域以网状形式组织
C. DNS 域和区域是一一对应的
D. 权威域名服务器以区域为单位将域名与 IP 的映射关系存储在区域文件

Answers

A. 从逻辑上，DNS 域通过层次化授权过程形成了树形结构的域名空间
D. 权威域名服务器以区域为单位将域名与 IP 的映射关系存储在区域文件

93862. 请描述一下 DNS 基础设施中，Authoritative Name Server，Recursive Name Server，Iterative Name Server，Root Name Server 之间的关系和区别。

Answers

Name Server 即域名服务器，是进行域名和与之相对应的 IP 地址转换的服务器。
Authoritative Name Server 是指权威域名服务器，是在特定的一个区域内具有唯一性，本身负责维护着这个范围内域名和 IP 地址之间对应关系的域名服务器，其回复的解析结果被称为权威应答；
Recursive Name Server 是指递归域名服务器，递归的意思是客户端向其请求的结果，它将会负责向其他域名服务器进行请求查询，并获得到最终的结果转发给客户端；
Iterative Name Server 是指迭代域名服务器，迭代的意思是其他域名服务器向其请求的结果，如果它本身不知道请求的结果，它会将下一步应该请求的域名服务器的地址转发给发来请求的服务器，并要求其向该服务器进行查询操作；

Root Name Server 是指根域名服务器，所有本地域名服务器自身不知道的结果（本地无设置或缓存结果）都会直接向最高级的 Root Name Server 进行迭代查询，Root Name Server 会将符合查询要求的下一个域名服务器（顶级域名服务器 TLD Name Server）的地址发送给本地域名服务器。
ChatGPT:
DNS，即域名系统，是用于将网站的 URL 地址（例如，www.google.com）转化为它们实际的 IP 地址（例如，192.0.2.44）的系统。以下是 DNS 基础设施中各部分的描述：

1. Stub Resolver：也被称为 DNS 客户端，是位于用户设备（如电脑、手机等）上的软件。它发送 DNS 查询，接收 DNS 响应，但不执行查询过程。通常，它将查询发送给公共 DNS 服务器。

2. Public Resolver：这是公开的 DNS 服务器，如 Google Public DNS 或 Cloudflare 的 1.1.1.1。这些服务器接收来自 Stub Resolver 的查询，然后通过自身的递归查询过程解析查询。

3. Open Resolver：这是一种任何人都可以查询的公共 DNS 服务器。它们可以被用于进行 DDoS 攻击，并因此有可能带来安全风险。

4. Authoritative Name Server：这是为特定域（如 openai.com）提供“权威”答案的服务器。它们存储有关它们负责的特定域的所有 DNS 记录。如果 Public Resolver 或 Recursive Resolver 对某个域的 DNS 记录有疑问，它们会向 Authoritative Name Server 查询。

5. Recursive Name Server：它会执行查询过程，直到找到答案为止。例如，如果 Stub Resolver 询问 Public Resolver 地址 "www.google.com" 的 IP，而 Public Resolver 也不知道答案，那么 Public Resolver 会成为 Recursive Resolver，通过向 Authoritative Name Servers 或其他 Recursive Name Servers 查询，直到找到答案。

6. Iterative Name Server：它在收到查询时，会将查询者重定向到可能知道答案的其他 DNS 服务器，而不是尝试自己寻找答案。这是递归查询和迭代查询之间的关键区别。

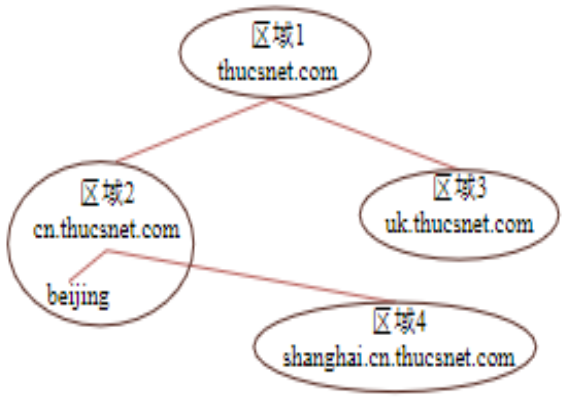
7. Root Name Server：这是位于 DNS 层次结构顶部的服务器，是整个 DNS 查询开始的地方。如果其他 DNS 服务器不知道某个地址，它们会向 Root Name Server 查询。Root Name Server 不会存储全部域名的信息，但它知道如何将查询定向到下一级的 Top Level Domain (TLD) Name Servers（例如 .com, .org 等）。这些 TLD 服务器然后可以将查询定向到更下一级的 Authoritative Name Server。

在 DNS 查询中，上述这些不同类型的服务器通常会协同工作，从用户发起查询开始，经过一系列的迭代或递归查询，最终找到并返回请求的 DNS 记录。

93863. 简述 DNS 域与 DNS 区域的区别与联系。

Answers

在逻辑上 DNS 由域（Domain）组成；在物理上则由区域（Zone）组成。
从逻辑上，DNS 域通过层次化授权过程形成了树形结构的域名空间，每个域成为域名空间的一个子树。域作为逻辑概念，不会真正存储数据文件供用户查询，但它很形象地体现出 DNS 的组织形式。通过域的结构可以清楚地了解 DNS 的层次化划分。
而解析所需的文件，则以区域为单位存储在服务器上。DNS 区域是一个物理概念，DNS 区域真正存储域名和 IP 地址的映射关系。每个 DNS 区域至少有一个权威域名服务器发布该区域的文件。
大多数情况下，域和区域是一一对应的。但也有例外情况，一个区域可以包含多个域，如下图中 cn.thucsnet.com 作为一个域时，包含两个子域，beijing 和 shanghai；cn.thucsnet.com 作为一个区域时，包含两个区域，一个区域包含 cn 和 beijing 域名，另一个区域包含 shanghai 域名。



93864. 以一个实际域名访问过程为例，简述 DNS 解析的步骤。

Answers

以访问 www.thucsnet.com 为例，实际的 DNS 域名解析过程包括：
1）在客户端上执行解析功能的解析器查询本机缓存及 hosts 文件，如果找到该域名 IP 地址，直接使用该地址。
2）如本机记录里不存在该域名，客户端向本地 DNS

服务器发出请求，很多时候我们直接称本地 DNS 服务器为递归解析服务器，或直接称为解析器。
3）本地 DNS 服务器查找本地 DNS 服务器缓存，有结果直接返回。
4）如没有结果，则查找根服务器，如根服务器查找无结果，则会告知本地 DNS 服务器去.com 顶级域权威服务器查询。
5）本地服务器去.com 顶级域查找，.com 顶级域查找无结果，则告知本地 DNS 服务器无记录，并给出 thucsnet.com 权威服务器的 IP 地址。
6）本地 DNS 服务器向 thucsnet.com 权威服务器获取结果，并向客户端返回查询结果。此时可在本地 DNS 服务器缓存一份结果，方便再次查询时直接使用。

93865. 简述 DNS 缓存策略对性能的提升和可能引入的安全威胁。

Answers

实际请求过程中，由于有了缓存，并不是每一次域名解析都要完成整个查询流程，在本机和本地 DNS 服务器都会缓存一些可直接使用的记录，用户自己还可以在 hosts 文件中手动配置一些记录，从而降低了查询的时延和开销。
缓存策略大大提高了查询性能，减少了大量重复的查询，但也引入了安全风险，因为只要攻击者修改了缓存，所有使用该本地 DNS 服务器的客户可能得到的都是攻击者篡改后的 IP 地址，这被称为 DNS 污染。

93866. 简述一种实现远程 DNS 缓存中毒攻击的步骤，并提出至少一种缓解策略。

Answers

步骤：第 1 步攻击者请求一个随机域名的 IP 地址。由于该域名不在本地 DNS 服务器缓存中，本地 DNS 服务器在第 2 步向权威域名服务器发出请求，在第 3 步，伪造回复如果比真实回复先到达本地 DNS 服务器并被接受，攻击就会成功。
缓解策略：1）通过 DNSSEC 确保每个回复都能得到验证。2）UDP 源端口随机化策略，可以将 16 位源端口号中约 64 000 个端口随机使用（实际使用端口号为 1024 以上），使攻击者猜测成功的难度从 16 位增加到 32 位，有效降低攻击成功率。

真实源地址验证

93867. 下面哪种技术不属于数据包签名技术（ ）。

Options

A. SPM;
B. uRPF;
C. Passport;
D. StackPi;

Answers

B. uRPF;

93868. 下面哪种技术不属于出流量源地址检测技术（ ）。

Options

A. Ingress Filtering;
B. uRPF;
C. SAVE;
D. SPM;

Answers

D. SPM;

93869. SAV 表是（ ）的对应关系。

Options

A. <源前缀，出端口>;
B. <目的前缀，入端口>;
C. <目的前缀，出端口>;
D. <源前缀，入端口>;

Answers

D. <源前缀，入端口>;

93870. 下面哪项不是 **SAVA-X** 边界路由器的职责（ ）。

Options

A. 传输加密;
B. 标签验证;
C. 标签替换;
D. 标签移除;

Answers

A. 传输加密;

93871. 网络内路由器数量为 **N, SAVA-P** 中每台路由器处理的协议报文数量约为（ ）。

Options

A. O(N);
B. O(logN);
C. $O(N^2)$;
D. $O((\log N)^2)$;

Answers

A. O(N);

93872. SAVA-X 目前支持（ ）层分层结构。

Options

A. 3;
B. 4;
C. 5;
D. 6;

Answers

C. 5;

93873. 下列哪个 **RFC** 提出了基于真实 **IPv6** 源地址的网络寻址体系结构（ ）。

Options

A. RFC 5210;
B. RFC 5120;
C. RFC 7513;
D. RFC 7856;

Answers

A. RFC 5210;

93874. 当前互联网体系结构的安全隐患包括（ ）。

Options

A. 地址易被伪造;
B. 隐私信息易被泄露;
C. 数据转发过程易受攻击;
D. 链路容易发生故障;

Answers

A. 地址易被伪造;
B. 隐私信息易被泄露;
C. 数据转发过程易受攻击;

93875. 当前 **IP** 地址的脆弱性体现在（ ）。

Options

A. 数据包是同质的;
B. 数据包中没有签名;
C. IP 数据包中源 IP 地址可以任意指定;
D. 网关等设备不会对出流量数据包源地址进行检查;

Answers

A. 数据包是同质的;
B. 数据包中没有签名;
C. IP 数据包中源 IP 地址可以任意指定;
D. 网关等设备不会对出流量数据包源地址进行检查;

93876. 真实源地址的三重含义是（ ）。

Options

A. 经授权的;
B. 唯一的;
C. 已验证的;
D. 可追溯的;

Answers

A. 经授权的;
B. 唯一的;
D. 可追溯的;

93877. 真实源地址验证体系结构 SAVA 由（ ）组成。

Options

A. 地址域间真实源地址验证;
B. 地址域内真实源地址验证;
C. 子网内真实源地址验证;
D. 终端真实源地址验证;

Answers

A. 地址域间真实源地址验证;
B. 地址域内真实源地址验证;
C. 子网内真实源地址验证;

93878. 真实源地址验证 SAVA 体系结构设计原则包括（ ）。

Options

A. 革新性;
B. 可扩展性;
C. 兼容性;
D. 安全性;

Answers

B. 可扩展性;
C. 兼容性;
D. 安全性;

93879. 面向地址域的 SAVA 源地址验证体系结构将源地址验证划分为（ ）粒度。

Options

A. 前缀;
B. 子网;
C. 主机;
D. 地址域;

Answers

A. 前缀;
C. 主机;
D. 地址域;

93880. 下面哪种可以用作 SAVI 技术绑定锚（ ）。

Options

A. 交换机端口;
B. MAC 地址;
C. 无线链路上主机和基站之间的安全关联;
D. IP 地址;

Answers

A. 交换机端口;
B. MAC 地址;
C. 无线链路上主机和基站之间的安全关联;

93881. 下面属于域内源地址验证技术的包括（ ）。

Options

A. uRPF;
B. SAVE;
C. O-CPF;
D. SAVA-P;

Answers

A. uRPF;
B. SAVE;
C. O-CPF;
D. SAVA-P;

93882. SAVA-X 中成员域内控制服务器 ACS 负责（ ）。

Options

A. 维护成员列表;
B. 交换地址前缀列表;
C. 协商状态机;
D. 配置边界路由器 AER;

Answers

A. 维护成员列表;
B. 交换地址前缀列表;
C. 协商状态机;
D. 配置边界路由器 AER;

93883. 支持嵌入真实身份的已有解决方案有（ ）。

Options

A. HIP;
B. SSL;
C. Web 认证;
D. NBIoT/5G;

Answers

A. HIP;
B. SSL;
C. Web 认证;
D. NBIoT/5G;

93884. SAVA-X 中的数据包签名由（ ）这几部分计算得到。

Options

A. 原始 SMA 标签;
B. 源地址;
C. 目的地址;
D. 载荷前 n 位;

Answers

A. 原始 SMA 标签;
B. 源地址;
C. 目的地址;
D. 载荷前 n 位;

93885. 基于区块链的域间信任联盟中区块链存储（ ）。

Options

A. 节点 ID;
B. 节点 IP 前缀;
C. 节点公钥;
D. 节点私钥;

Answers

A. 节点 ID;
B. 节点 IP 前缀;
C. 节点公钥;

93886. 接入网的异构多样性体现在（ ）。

Options

A. 终端多样性;
B. IP 分配方式多样性;
C. 地域多样性;
D. 接入方式多样性;

Answers

A. 终端多样性;
B. IP 分配方式多样性;
D. 接入方式多样性;

93887. 当前互联网体系结构中网络攻击频发的原因是什么？

Answers

当前互联网体系结构缺乏可信基础。互联网体系结构设计之初，没有考虑到网络规模的爆炸式增长以及网络应用的日趋多元化，更没有进行基本的安全属性设计，导致其难以胜任从彼此信任的单一网络环境到信任缺失的复杂网络空间的转变。

93888. 简述真实 IP 源地址的三重含义。

Answers

经授权的，即 IP 源地址必须是经互联网 IP 地址管理机构分配授权的，不能伪造；唯一，即 IP 源地址必须是全局唯一的；可追溯的，网络中转发的 IP 分组，可根据其 IP 源地址找到其所有者和位置。

93889. 简述“地址域”的概念及由来。

Answers

随着真实源地址验证技术的发展和应用的增量部署，出现了一个自治域中部分子网部署了真实源地址验证技术，而剩余子网尚未部署的情形，这样就导致 SAVA 部署与地址管理范围的失配。这时候继续以自治域为粒度进行真实源地址验证就不再合适。地址域被定义为可信任、可管理和可控制的一个或多个 IP 地址前缀的集合。以一个校园网为例，地址域可以是某一个院系下的某个课题组，也可以是某个所、某个院系，甚至可以是整个校园网。

93890. 简述 SAVI 工作的“三部曲”。

Answers

（1）监听控制类报文（如 ND、DHCPv6），即 CPS（Control Packet Snooping），获取地址分配信息以识别主机合法 IP 源地址；
（2）将合法的 IP 地址与主机网络附属的链路层属性（“绑定锚”）绑定；
（3）对数据包中的 IP 源地址与其绑定锚进行匹配，只有报文源地址与绑定锚匹配时才可以转发。

93891. 简述 SAVA-P 的基本工作原理。

Answers

SAVA-P 的基本思路是路由器通过发送探测报文，探测域内转发路径，沿途路由器根据收到的探测报文生成<源前缀和入接口>的对应关系，也就是 SAV 表。

公钥基础设施

93892. 在甲乙双方利用数字证书进行签名的场景下，甲方使用（ ）完成签名，乙方使用（ ）验证签名。

Options

A. 甲方的私钥、甲方的私钥
B. 甲方的私钥、甲方的公钥
C. 甲方的公钥、乙方的公钥
D. 乙方的公钥、乙方的私钥

Answers

B. 甲方的私钥、甲方的公钥

93893. PKI 中，CA 的核心功能是（ ）。

Options

A. 颁发及撤销数字证书
B. 提供面对面的证书业务服务
C. 完成申请者的身份审核
D. 记录用户信息

Answers

A. 颁发及撤销数字证书

93894. 下列关于以用户为中心的信任体系的说法错误的是（ ）。

Options

A. 每个用户都自签名一个证书
B. 每个证书中可通过证明列表包含其他用户的签名
C. 高度依赖于根 CA
D. 用户本身可以作为 CA

Answers

C. 高度依赖于根 CA

93895. 以 CA 为中心的 PKI 存在的一个严重问题是单点信任问题，其导致的最大威胁是（ ）。

Options

A. CA 之间的去中心化性能降低
B. 用户可以立即识别出该 CA 被攻击
C. 一旦 CA 的公钥公布后，攻击者能够利用 CA 的公钥发布恶意证书
D. 一旦 CA 的私钥被泄露，攻击者就能利用 CA 的私钥发布恶意证书

Answers

D. 一旦 CA 的私钥被泄露，攻击者就能利用 CA 的私钥发布恶意证书

93896. 客户端使用 HTTPS 协议时，为了提高双方建立 SSL 连接时的安全能力，可以为 HTTPS 客户端内置（ ），浏览器可以基于本地证书验证服务器证书，保证用户的安全登录及通信隐私。

Options

A. 浏览器公钥
B. 浏览器信任的 CA 颁发的证书
C. 浏览器信任的 CA 私钥
D. 浏览器厂商证书

Answers

B. 浏览器信任的 CA 颁发的证书

93897. RPKI 的主要思路是将每个 AS 号与其对应的 IP 地址块进行绑定，即完成（ ）。

Options

A. 路由源授权
B. 路径授权
C. 公私钥绑定
D. AS 所宣告路由（AS path）的验证

Answers

A. 路由源授权

93898. RPKI 部署非常缓慢最主要的原因是（ ）。

Options

A. 存在一定开销，且严格的路由源授权会导致 ISP 损失流量
B. RPKI 对路由源的认证能力存在不足
C. RPKI 没有采用加密传输数据
D. 数据面传输数据并不需要 RPKI 提供的路由源认证

Answers

A. 存在一定开销，且严格的路由源授权会导致 ISP 损失流量

93899. Web 信任模型以 Web 浏览器预置的（ ）为信任起点。

Options

A. 多个子 CA
B. 层次化信任传递路径
C. 单个根 CA
D. 多个根 CA

Answers

D. 多个根 CA

93900. 通过“数字信封”协商对称密钥时，发送方生成一个密钥作为对称密钥，用接收方的公钥加密该对称密钥，接收方用（ ）解密被封装的对称密钥。

Options

A. 接收方的公钥
B. 发送方的公钥
C. 接收方的私钥
D. 发送方的私钥

Answers

C. 接收方的私钥

93901. PKI 中，用户与安全服务的通信采取 SSL 等安全信道。以确保通信过程安全，因此，用户申请证书之前，需要获取（ ）。

Options

A. 安全服务器的证书
B. 安全服务器的私钥
C. CA 公钥
D. CA 证书

Answers

A. 安全服务器的证书

93902. PKI 中的 CA 制作与分发的数字证书主要包含（ ）。

Options

A. 用户公钥
B. 数字签名
C. CA 私钥
D. 用户私钥

Answers

A. 用户公钥
B. 数字签名

93903. X.509 证书格式主要包括（ ）。

Options

A. X.509 版本号、CA 编号、签名算法
B. 用户私钥、CA 公钥
C. 颁发者、有效期、主体名
D. 主体的公钥信息、拓展信息和签名

Answers

A. X.509 版本号、CA 编号、签名算法
C. 颁发者、有效期、主体名
D. 主体的公钥信息、拓展信息和签名

93904. 下列关于 PKI 中层次信任模型的描述正确的是（ ）。

Options

A. PKI 以中心化方式管理、掌握用户的身份数据
B. 是一个以主、从 CA 关系为基础建立的分级 PKI 结构
C. 也称为分级信任模型
D. 是一种 CA 间可以相互认证的网状信任模型

Answers

B. 是一个以主、从 CA 关系为基础建立的分级 PKI 结构
C. 也称为分级信任模型

93905. 甲方和乙方拥有对方数字证书的前提下，下列关于利用数字证书进行的操作描述正确的是（ ）。

Options

A. 甲方使用乙方的公钥进行加密，乙方使用自己的私钥完成解密，整个过程无需甲乙双方交互密钥信息
B. 甲方使用自己的私钥完成签名，乙方使用甲方证书中的公钥验证签名
C. 甲方使用自己的私钥进行签名，并使用乙方的公钥进行加密，乙方用自己的私钥解密密文，使用甲方证书中的公钥验证甲方的数字签名
D. 甲方使用自己的公钥进行加密，乙方使用自己的私钥完成解密，整个过程无需甲乙双方交互密钥信息

Answers

A. 甲方使用乙方的公钥进行加密，乙方使用自己的私钥完成解密，整个过程无需甲乙双方交互密钥信息
B. 甲方使用自己的私钥完成签名，乙方使用甲方证书中的公钥验证签名
C. 甲方使用自己的私钥进行签名，并使用乙方的公钥进行加密，乙方用自己的私钥解密密文，使用甲方证书中的公钥验证甲方的数字签名

93906. 下列属于 PKI 中 CA 的职能的是（ ）。

Options

A. 颁发证书
B. 注销证书
C. 存储证书和证书状态信息
D. 恢复及更新密钥

Answers

A. 颁发证书
B. 注销证书
D. 恢复及更新密钥

93907. 与基于 CA 信任体系的中心化 PKI 不同，以用户为中心的信任体系具有以下特点（ ）。

Options

A. 基于“信任网”（Web of Trust），是去中心化的
B. 不需要 CA 为用户颁发证书
C. 用户与用户之间形成一个网状的信任结构
D. 用户本身可以作为 CA 签署其他实体的公钥，签署后其余用户必须信任

Answers

A. 基于“信任网”（Web of Trust），是去中心化的
B. 不需要 CA 为用户颁发证书
C. 用户与用户之间形成一个网状的信任结构

93908. PKI 中，CA 在数字证书颁发过程中主要存在以下安全隐患：（ ）。

Options

A. 由于配置或操作失误，误发证书
B. 恶意颁发证书
C. 通过提高网站身份认证成本推广证书部署
D. 钓鱼网站通过仅验证域名的 DV SSL 证书欺骗用户

Answers

A. 由于配置或操作失误，误发证书
B. 恶意颁发证书
D. 钓鱼网站通过仅验证域名的 DV SSL 证书欺骗用户

93909. PKI 中，CA 需要处理的证书变更信息主要由以下原因导致（ ）。

Options

A. CA 公钥被盗
B. 用户私钥泄露
C. 用户需要更换密钥
D. 用户身份信息发生变化

Answers

B. 用户私钥泄露
C. 用户需要更换密钥
D. 用户身份信息发生变化

93910. 以 CA 为中心的 PKI 环境主要存在以下问题：（ ）。

Options

A. 单点信任问题
B. 证书状态管理机制存在开销、延时及用户信息泄露问题
C. 部分 CA 规模非常庞大，一旦对其证书撤销将会造成大范围的网站无法连接
D. 无法实现层次化的验证结构

Answers

A. 单点信任问题
B. 证书状态管理机制存在开销、延时及用户信息泄露问题
C. 部分 CA 规模非常庞大，一旦对其证书撤销将会造成大范围的网站无法连接

93911. 以用户为中心的 PKI 因为消除了对 CA 的依赖，每个用户都可以自签名证书并收集他人的签名来提升自己证书的可信性，从而避免了证书申请及后续维护所需要向 CA 缴纳的费用，但仍然存在以下问题：（ ）。

Options

A. 缺乏激励机制的情况下，新用户难以有效获取足够多的老用户签名信任
B. 用户的密钥丢失或撤销后，证书状态信息很难迅速传播出去
C. 与以 CA 为中心的中心化 PKI 中的单点信任问题基本一致
D. 用户维护证书状态成本远高于向 CA 缴纳的费用

Answers

A. 缺乏激励机制的情况下，新用户难以有效获取足够多的老用户签名信任
B. 用户的密钥丢失或撤销后，证书状态信息很难迅速传播出去

93912. 典型的 PKI 体系由哪几部分组成？试举例说明用户通过 PKI 申请证书的过程。

Answers

PKI 体系通常由用户、证书认证中心（CA）、证书注册机构（Registration Authority，RA） 和证书数据库四部分组成。如用户 example.org 申请数字证书，它首先向 RA 发送一个证书注册申请。RA 受理用户提出的证书注册申请，审核通过后向 CA 提出证书请求，CA 创建证书，并存储证书信息于数据库，方便后续的查询。

93913. 简述 PKI 体系中 CA 的职能，试举例说明在实际中 CA 如何实现其职能。

Answers

在 PKI 体系中公认的、值得信赖的且公正的第三方机构，即为负责颁发及撤销公钥证书的 CA。
颁发及撤销数字证书是 CA 的核心功能，具体来说，CA 的职能包括用户注册、颁发证书、注销证书、恢复及更新密钥等。
实际中，在 CA 收到用户申请数字证书的请求后，需要认证申请者的真实身份。为实现 CA 的职能，为

PKI 中管理的用户颁发证书，在验证用户身份的基础上，CA 用自己的私钥对证书内容签名，证书内容包括用户的公钥和其他信息，绑定在一起用于验证用户的身份。
除此之外，CA 还要负责用户证书有效期管理，即登记和发布证书所处的状态。比如，域名（example.org）向 CA 申请数字证书，CA 首先验证获得证书需要的域名（example.org）是否属于该用户。通过验证后，CA 把申请者的公钥、身份信息、数字证书的有效期等信息作为消息原文，生成哈希摘要，并用 CA 的私钥加密进行签名。

93914. 以 CA 为中心的 PKI 信任模型主要有哪几种？

Answers

PKI 信任模型是为不同用户群体的 CA 之间建立信任的机制，包括 CA 间信任关系的建立和完成证书验证的路径。以 CA 为中心的 PKI 信任模型主要包括以下几类：
（1）单 CA 信任模型。
（2）层次信任模型。
（3）分布式信任模型。
（4）桥 CA 信任模型。
（5）Web 信任模型。

93915. 以 CA 为中心的 PKI 可能存在哪些安全问题？

Answers

以 CA 为中心的 PKI 环境依然存在着以下问题：
（1）单点信任问题。
目前大部分的用户都只向少数几个服务器申请证书注册，证书注册信息过于集中，存在着单点信任问题。
（2）证书状态管理机制存在开销、延时及用户信息泄露问题。
证书撤销列表规模越来越大，对用户造成了很大的下载开销；通过服务器查询方式虽然避免了下载撤销列表的开销，但是却要向第三方查询，不仅会引入一轮响应等待延时，还会泄露用户站点访问信息。
（3）对大型 CA 难以形成有效的管理。
由于部分 CA 规模非常庞大，以至于一旦对其证书撤销将会造成大范围的网站无法连接；因此很难对这些 CA 的过失行为进行惩罚，致使部分 CA 自身的安全性存疑。

93916. 数字证书颁发过程中可能遇到哪些安全问题？

Answers

CA 在数字证书颁发过程中主要存在以下安全问题：
（1）误发证书。
由于配置或操作失误，CA 有可能向错误的用户颁发证书。由于用户对 CA 是完全信任的，这种信任使得用户不会怀疑证书的正确性，从而引起安全问题。
（2）恶意颁发证书。
CA 被操控或私钥被盗时，可能颁布虚假证书，产生巨大的危害。
（3）钓鱼网站证书。
由于网站身份认证成本较高，导致证书应用推广进程缓慢。DV SSL 证书对验证内容进行了简化，仅需验证域名，证书仅用于数据传输加密。但这种方式可以被不法分子利用，通过钓鱼网站仿冒真实网站来欺骗消费者。

分布式系统安全

93917. 以下哪个协议可用于时钟同步（ ）。

Options

A. Paxos 协议
B. NTP 协议
C. Raft 协议
D. PBFT 协议

Answers

B. NTP 协议

93918. 、在解决拜占庭将军问题的口头消息协议中，若要容忍 6 个叛徒，则包括叛徒在内需要至少多少个将军？（ ）。

Options

A. 7
B. 13
C. 19
D. 31

Answers

C. 19

93919. 在解决拜占庭将军问题的签名消息协议中，若要容忍 4 个叛徒，并且要求共识在两回合交互之内完成，则包括叛徒在内需要至少多少个将军？（ ）？？？

Options

A. 7
B. 13
C. 19
D. 31

Answers

B. 13

~~**93920. 基于时间戳的重放攻击预防方案中，存在哪些特征（ ）。**~~

~~**Options**~~

~~A. 维护开销大~~
~~B. 要求精确时钟同步~~
~~C. 存在受攻击的时间窗口~~
~~D. 要求粗略的时钟同步~~

~~**Answers**~~

~~A. 维护开销大~~

93921. 如何确保分布式事务的一致性（ ）。

Options

A. 引入协调者
B. 分布式锁
C. 两阶段提交
D. 引入冗余备份

Answers

C. 两阶段提交

93922. 如何确保分布式事务的隔离性（ ）。

Options

A. 引入协调者
B. 分布式锁
C. 两阶段提交
D. 引入冗余备份

Answers

B. 分布式锁

93923. 分布式系统中的 CAP 定理包含（ ）。

Options

A. 一致性
B. 原子性
C. 可用性
D. 分区容错性

Answers

A. 一致性
C. 可用性
D. 分区容错性

93924. 以下哪些特性是 BASE 准则所要求的（ ）。

Options

A. 基本可用性
B. 稳定性
C. 最终一致性

Answers

A. 基本可用性
C. 最终一致性

Explain

基本可用性、软状态、最终一致性

93925. 以下哪些方案能防御重放攻击？( )

Options

A. TCP 协议
B. UDP 协议
C. 时间戳机制
D. 随机数机制

Answers

C. 时间戳机制
D. 随机数机制

93926. 以下哪些特性是 ACID 所要求的（ ）。

Options

A. 可用性
B. 原子性
C. 一致性
D. 隔离性

Answers

B. 原子性
C. 一致性
D. 隔离性

Explain

ACID 包含原子性、一致性、隔离性、持久性。

93927. 以下哪些角色是 Paxos 协议中所定义的（ ）。

Options

A. 提议者
B. 接受者
C. 协调者
D. 候选者

Answers

A. 提议者
B. 接受者

93928. 以下哪些角色是 Raft 协议中所定义的（ ）。

Options

A. 提议者
B. 接受者
C. 领导者
D. 候选者

Answers

C. 领导者
D. 候选者

93929. 以下哪些选项是基于角色的访问控制模型的组成部分（ ）。

Options

A. 用户
B. 角色
C. 权限
D. 被访问者

Answers

A. 用户
B. 角色
C. 权限

93930. 基于属性的访问控制模型中，引入了以下哪些要素？（ ）

Options

A. 策略实施点
B. 策略信息点
C. 策略储存点
D. 策略执行点

Answers

A. 策略实施点
B. 策略信息点
D. 策略执行点？？

93931. 、基于信任的访问控制模型中，信任根据获取渠道的不同可以分为（ ）。

Options

A. 基本信任
B. 直接信任
C. 间接信任
D. 推荐信任

Answers

A. 基本信任
B. 直接信任
D. 推荐信任

93932. 以下哪些阶段是 PBFT 协议中的（ ）

Options

A. 预准备阶段
B. 准备阶段
C. 预确认阶段
D. 确认阶段

Answers

A. 预准备阶段
B. 准备阶段
D. 确认阶段

93933. 在基于时间戳的重放攻击预防方案中，存在哪些特征（ ）。

Options

A. 维护开销大
B. 要求精确时钟同步
C. 存在受攻击的时间窗口
D. 要求粗略的时钟同步

Answers

B. 要求精确时钟同步
C. 存在受攻击的时间窗口

93934. P2P 网络的路由机制包含哪些形式（ ）。

Options

A. 有结构的路由表机制
B. 无结构的广播洪泛机制
C. 分布式的路由机制
D. 中心化的路由机制

Answers

A. 有结构的路由表机制
B. 无结构的广播洪泛机制

93935. 以下哪些方案有助于降低 P2P 网络被日蚀攻击的风险（ ）。

Options

A. 选择少部分权威节点作为邻居
B. 增加邻居节点的个数
C. 减少邻居节点个数
D. 采用分层的架构

Answers

A. 选择少部分权威节点作为邻居
B. 增加邻居节点的个数

93936. 以下哪些说明是网络时间协议 NTP 的特征（ ）。

Options

A. 任意两个节点间都需要相互进行一次时间同步
B. 采用分层的架构
C. 引入身份认证机制确保时间源的权威性
D. 不以单一时间服务器为基准

Answers

B. 采用分层的架构
C. 引入身份认证机制确保时间源的权威性

93937. 什么是重放攻击？请简要介绍一种重放攻击的防御方式。

Answers

重放攻击是指攻击者通过监听客户端发往服务端的数据，然后将其原封不 动重新发送给服务端，从而触发服务端多次执行同一条指令。防御重放攻击有以下三种方式：
时间戳机制：发送方在每次发送 请求消息时可以附带一个时间戳t_0；接收方在收到消息后通过对比时间戳与本地时间获得一个时间差，然后判断该时间差是否小于一个允许值 δ;若是则认为该消息合法，否则将其视作重放消息。
随机数机制：消息发送方维护一个随机数池，确保每次取出的随机数都不一样，并为每次发送的消息附带上一个新的随机数;接收方则维护一个随机数日志，存储每 个来自发送方消息的随机数;当接收方收到新的消息时，判断其中的随机数是 否已在日志中存储;若未存储则认为该消息合法，否则将其视作重放消息。
时间戳与随机数相结合：消息发送方维护一个随机数池，其中随机数的数量能够确保在任意时间窗口 δ' 内不重复;发送方为每次发送的 消息附带上本地时间戳以及一个随机数，当随机数用完时可以复用之前的随机 数;接收方则存储最近 δ 时间内来自发送方消息的随机数;当接收方收到消息 时，若其中的随机数未在日志中存储且本地时间与时间戳的差值不超过 δ，则 认为该消息合法，否则将其视作重放消息。

93938. 在 Quorum 机制中，设计法定人数 q 时需要满足安全性准则和有效性准则，请简述这两个准则。

Answers

一致性准则: 对于任意两个至少包含 q 个节点的集合，它们之间的交集 必须至少包含一个正确节点;
有效性准则: q 不能超过正确节点的数量。

93939. 简述 Cristian 时间同步算法的流程

Answers

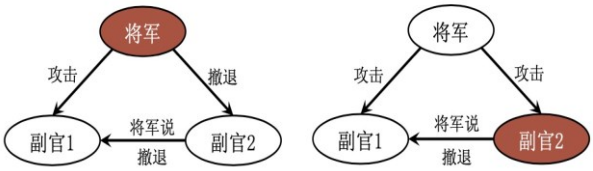
客户端发送一个时间同步的消息给时间服务器 S，并附带上本地时间t；时间服务器 S 收到该请求后将返回一个本地时间t‘；客户端收到回应后，通过此时的本地时间t’‘可以获得消息的往返延时 $t'' - t$，因此可以预测消息的传播延时为$(t'' - t)/2$，据此可以将本地时间设置为 $t' + (t'' - t)/2$，从而完成与时间服务器 S 的同步。

93940. 说明为什么口头消息协议中三将军问题无解

Answers

可以举例进行说明，以下图为例进行说明：
（1）当将军是叛徒时，副官 1 和副官 2 都是忠诚的，将军向副官 1 下达攻击命令但是 向副官 2 下达撤退命令，而副官 2 告诉副官 1 他收到的命令是撤退，该情况下，副官 1 收到了将军的攻击指令以及副官 2 的撤退指令;
（2）在图中的第二种情形下，副官 2 是叛徒，将军和副官 1 都是忠诚的，将军向副官 1 和副官 2 发 送的命令都是攻击，但是副官 2 却告诉副官 1 自己收到的命令是撤退，该情况 下，副官 1 收到了来自将军的攻击指令以及来自副官 2 的撤退指令。
从上面两种情况分析中可以看到，在 3 个将军其中有一个是叛徒的情况下，存在两种不同的情形(将军是叛徒和副官 2 是叛徒)使得副官 1 所接收到的指 令

形式完全一样，因此副官 1 无法判断自己身处何种情形。



93941. Raft 协议的 Leader 选举过程中，假设网络没有故障，所有发送的消息都顺利到达，什么情况下会导致 leader 选举失败？如何解决这个问题。

Answers

当多个节点同时参与 Leader 选举导致分票，任意节点都没拿到超过一半的投票时，此轮竞选失败；为了解决这个问题，每次竞选失败后，节点随机等待一个时间然后再参与下一轮竞选，从而避免多个节点同时竞选导致分票。

应用安全

93942. 应用安全，一般指涉及互联网应用的（ ）和（ ）的安全问题。

Options

A. 相关协议
B. 软件系统
C. 操作规范
D. 使用方法

Answers

A. 相关协议
B. 软件系统

93943. 以下哪条命令有可能造成 SQL 注入攻击：

Options

A. SELECT * FROM user WHERE username='admin' '– AND psw='password'
B. SELECT * FROM user WHERE username='admin' AND psw='password'
C. SELECT * FROM users WHERE user_id = $user_id
D. SELECT * FROM users WHERE user_id = 1234; DELETE FROM users

Answers

B. SELECT * FROM user WHERE username='admin' AND psw='password'
D. SELECT * FROM users WHERE user_id = 1234; DELETE FROM users

---

93944. 云计算是一种通过网络提供按需可动态伸缩的廉价计算服务。它具有大规模、虚拟化、高可用性和扩展性、按需服务和安全等特点。通常它的服务类型分为哪几类:

Options

A. 基础设施即服务(Infrastructure as a Service, IaaS)
B. 平台即服务(Platform as a Service, PaaS)
C. 软件即服务(Software as a Service, SaaS)
D. 数据即服务（Data as a Service, DaaS）

Answers

A. 基础设施即服务(Infrastructure as a Service, IaaS)
B. 平台即服务(Platform as a Service, PaaS)
C. 软件即服务(Software as a Service, SaaS)

93945. 网络应用的攻击主要目标有哪两个:

Options

A. 拒绝服务
B. 信息泄露
C. 网络瘫痪
D. 线路损坏

Answers

A. 拒绝服务
B. 信息泄露

93946. XSS 攻击有哪些:

Options

A. 反射型 XSS
B. 存储型 XSS
C. 跳跃型 XSS
D. 点击型 XSS

Answers

A. 反射型 XSS
B. 存储型 XSS

93947. 完成 CSRF 攻击必须要有三个条件（ ）

Options

A. 用户已经登录了信任网站 A，并在本地生成了 Cookie;
B. 在用户没有登出信任网站 A 的情况下(也就是 Cookie 生效的情况下)， 访问了恶意攻击者提供的引诱危险网站 B(危险 B 网站要求访问 A);
C. 网站 A 没有采用任何 CSRF 防御措施。
D. 网站 B 没有采用任何 CSRF 防御措施

Answers

A. 用户已经登录了信任网站 A，并在本地生成了 Cookie;
B. 在用户没有登出信任网站 A 的情况下(也就是 Cookie 生效的情况下)， 访问了恶意攻击者提供的引诱危险网站 B(危险 B 网站要求访问 A);
C. 网站 A 没有采用任何 CSRF 防御措施。

93948. 常见的社交网络安全问题包括（ ）

Options

A. 数字档案收集;
B. 运维数据收集;
C. 垃圾信息传播。
D. 女巫攻击(Sybil 攻击)

Answers

A. 数字档案收集;
B. 运维数据收集;
C. 垃圾信息传播。
D. 女巫攻击(Sybil 攻击)

93949. 云计算的特点（ ）

Options

A. 大规模、虚拟化;
B. 高可用性和扩展性;
C. 按需服务。

D. 网络安全

Answers

A. 大规模、虚拟化;
B. 高可用性和扩展性;
C. 按需服务。
D. 网络安全

93950. 云计算安全攻击有哪些（ ）

Options

A. 虚拟机逃逸;
B. 提权攻击;
C. 侧信道攻击。
D. XSS 攻击

Answers

A. 虚拟机逃逸;
B. 提权攻击;
C. 侧信道攻击。

93951. 应用安全的共性特征包括（ ）

Options

A. 资源有限;
B. 资源共享;
C. 系统漏洞。
D. 操作错误

Answers

A. 资源有限;
B. 资源共享;
C. 系统漏洞。

93952. 如何预防撞库攻击?（ ）

Options

A. 强制用户密码的强度
B. 定期强制用户更换密码
C. 在账户相关接口加强人机防控策略
D. 重要业务流程采用二次验证

Answers

A. 强制用户密码的强度
B. 定期强制用户更换密码
C. 在账户相关接口加强人机防控策略
D. 重要业务流程采用二次验证

93953. 以下关于网络钓鱼的说法中，正确的是?（ ）

Options

A. 网络钓鱼融合了伪装、欺骗等多种攻击方式
B. 网络钓鱼与 web 服务没有关系
C. 典型对网络钓鱼攻击都将被攻击者引诱到一个恶意的网站中
D. 网络钓鱼是“社会工程攻击”的一种形式

Answers

A. 网络钓鱼融合了伪装、欺骗等多种攻击方式
C. 典型对网络钓鱼攻击都将被攻击者引诱到一个恶意的网站中
D. 网络钓鱼是“社会工程攻击”的一种形式

93954. 以下关于物联网安全的说法中，正确的是?（ ）

Options

A. 安全体系结构复杂
B. 涵盖广泛的安全领域
C. 物联网安全机制已经成熟健全
D. 有别于传统的信息安全

Answers

A. 安全体系结构复杂
B. 涵盖广泛的安全领域
D. 有别于传统的信息安全

93955. 物联网感知层遇到的安全挑战有（ ）

Options

A. 网络节点被恶意控制
B. 感知信息被非法获取
C. 感知节点被标实
D. 被钓鱼攻击

Answers

A. 网络节点被恶意控制
B. 感知信息被非法获取
C. 感知节点被标实

93956. 移动应用安全分为哪几层（ ）

Options

A. 源代码层
B. 应用分发层
C. 数据链路层
D. 终端检测层

Answers

A. 源代码层
B. 应用分发层
D. 终端检测层

93957. 应用安全问题的本质原因有哪些?

Answers

（系统的 3 个共性特征？）

总体来说，攻击者想要实现的目标有两个:一是阻断网络应用提供正常服务;二 是攻击者从网络应用越权

获取不该得到的服务，前者表现为拒绝服务，使得应该提供服务的网络应用失去服务能力;后者则对应了形形色色的信息泄露，攻击者从网络应用获取了不应获取的服务。一是拒绝服务，二是信息泄露。达到这种目的需要利用当前网络应用技术 和设备存在的系统漏洞(网络协议栈、物理服务器等)。
言之有理即可。

93958. 应用安全基本防范原理有哪些？

Answers

1. 身份认证与信任管理；2. 隐私保护；3. 应用安全监控防御；

93959. 应用安全发展趋势有哪些？

Answers

人工智能(AI)使能的智能检测系统和海量应用场景下的用户隐私保护

93960. 常见的 Web 安全漏洞有哪些？简要说明它们的攻击原理。

Answers

XSS 攻击、CSRF 攻击、SQL 注入攻击

93961. CDN 的作用是什么？潜在的安全风险有哪些？

Answers

CDN 的全称是 Content Delivery Network，即内容分发网络。CDN 是由分布在不同地理位置的服务器集群组成的网络系统，目标是帮助其客户网站实现负载均衡、降低网络延迟、提升用户体验。如果一个网站托管在 CDN 上，网站用户总是从距离自己最近的 CDN 节点快速地获取缓存内容;当用户请求的内容没有缓存，CDN 节点会将该请求转发到源站服务器，以获取目标文件内容并就地缓存。除了负载均衡和缓存加速，通过 CDN 的分布式架构，访问用户从就近边缘节点获取内容，能够隐藏客户网站的实际 IP 地址，并为其提供 DDoS 攻击保护。

人工智能安全

93962. 人工智能元年一般被认为是：

Options

A. 1944 年
B. 1956 年
C. 1982 年
D. 2006 年

Answers

B. 1956 年

Explain

1956 年达特茅斯夏季研讨会上，“人工智能”的概念被首次明确提出，因此人工智能元年一般被认为是 1956 年

93963. 2016 年由美国社交网络服务公司 Facebook 推出的深度学习框架的名称是（ ）。

Options

A. Theano;
B. PyTorch;
C. Caffe;
D. Keras;

Answers

B. PyTorch;

93964. 2018 年，中国信息通信研究院安全研究所发布了《人工智能安全白皮书》，将人工智能安全风险分为六个方面。以下不属于这六个方面的是（ ）

Options

A. 网络安全风险
B. 算法安全风险
C. 数据安全风险
D. 管理安全风险

Answers

D. 管理安全风险

Explain

六个方面分别是：网络安全风险、数据安全风险、算法安全风险、信息安全风险、社会安全风险和国家安全风险。

93965. 以下那个不属于深度学习框架（ ）

Options

A. TensorFlow
B. PyTorch
C. Jittor
D. Numpy

Answers

D. Numpy

93966. 黑盒攻击往往利用深度学习模型的（ ）

Options

A. 可解释性
B. 迁移性
C. 鲁棒性
D. 保密性

Answers

B. 迁移性

93967. 人工智能比较常见的应用领域包括（ ）

Options

A. 计算机视觉
B. 网络安全
C. 自然语言处理
D. 生物医药

Answers

A. 计算机视觉
B. 网络安全
C. 自然语言处理
D. 生物医药

93968. 利用深度学习框架自身漏洞造成的攻击形式有（ ）

Options

A. 拒绝服务攻击
B. 中间人攻击
C. 堆溢出
D. 窃听

Answers

A. 拒绝服务攻击
C. 堆溢出

93969. 提升模型可解释性的方法包括（ ）

Options

A. 使用可解释的模型
B. 寻找合适的可解释性方法对模型做出解释
C. 对模型进行对抗训练
D. 使用复杂的深层网络模型

Answers

A. 使用可解释的模型
B. 寻找合适的可解释性方法对模型做出解释

93970. FGSM（Fast Gradient Sign Method）算法是一种（ ）

Options

A. 目标攻击算法
B. 无目标攻击算法
C. 白盒攻击算法
D. 黑盒攻击算法

Answers

B. 无目标攻击算法
C. 白盒攻击算法

Explain

从算法原理上理解，需要用到攻击目标的梯度信息，因此是白盒攻击；没有指定攻击目标的类别，因此是无目标攻击

93971. 因为在深度学习领域的杰出贡献而共同获得图灵奖，被并称为深度学习“三巨头”的学者是（ ）。

Options

A. Yoshua Bengio;
B. Geoffery Hinton;
C. Yann LeCun;
D. Andrew Ng;

Answers

A. Yoshua Bengio;
B. Geoffery Hinton;
C. Yann LeCun;

93972. 人工智能算法的局限性包括（ ）

Options

A. 数据局限性
B. 成本局限性
C. 伦理局限性
D. 偏见局限性

Answers

A. 数据局限性
B. 成本局限性
C. 伦理局限性
D. 偏见局限性

93973. 对抗攻击算法难以诱导模型将对抗样本分类到某一特定类别，因此属于无目标攻击。

Answers

0

Explain

targeted-FGSM 是目标攻击

93974. 可解释性模型包括决策树模型、逻辑回归模型等。

Answers

1

93975. 模型可视化技术有助于提升模型的可解释性和鲁棒性。

Answers

1

93976. 不公正的数据集会将人类世界的偏见带入深度学习模型中

Answers

1

93977. 开发人工智能算法的经济开销主要体验在收集数据和训练模型上，模型训练完成就不会有经济投入了

Answers

0

93978. 我国现有法律法规的适用主体也包括机器人和人工智能模型

Answers

0

93979. 卷积神经网络一般包括：卷积层、___和全连接层

Answers

池化层

93980. 算法安全层面，从网络结构是否公开透明的角度，可以将攻击分为___和___；从攻击类别是否定向的维度，可以将攻击分为目标攻击和___

Answers

黑盒攻击
白盒攻击
无目标攻击

93981. 已经过期、产生错误或者对业务没有意义的数据被称为___

Answers

脏数据

93982. 1982 年 Hopfield 神经网络提出的全新的神经网络的训练方法被称为___。

Answers

反向传播/backpropagation

93983. 人工智能算法的基础平台和常用操作被统称为___。

Answers

深度学习框架

93984. CVE-2020-5215 揭露出 TensorFlow 在 1.15.2 版本和 2.0.1 版本之前，如果开发者将 Python 中的字符串 string 转换为___格式，将会导致___模式下的分段错误。

Answers

tf.float16

Eager

93985. CVE-2017-12852 指出 NumPy 1.13.1 及之前的版本中的____函数存在安全漏洞，该漏洞源于函数缺少对输入数据的验证，当输入的需要填充的 array 为空列表或者 numpy.ndarray 类型时，该函数会陷入无限循环，攻击者可以利用该漏洞造成拒绝服务（DoS）攻击。

Answers

numpy.pad

93986. CVE-2017-12597 指出 OpenCV 在 3.3 版本之前在使用___函数读取图像文件时，在 utils.cpp 中的函数 FillColorRow1 中会出现越界写入错误，导致堆溢出。

Answers

cv::imread

93987. 简要说明“图灵测试”的过程。

Answers

图灵测试是指如果一台机器能够与人类展开对话（通过电传设备）而不能被辨别出其机器身份，那么称这台机器具有智能。在测试过程中，测试者与被测试者（一个人和一台机器）隔开的情况下，通过一些装置（如键盘）向被测试者随意提问。进行多轮测试后，如果机器让平均每个测试者做出超过一定数量的误判，那么这台机器就通过了测试，并被认为具有人类智能。

93988. 开发和执行环境带给深度学习框架的漏洞有哪些？请具体说明。

Answers

第三方基础库带来的安全漏洞：拒绝服务攻击、堆溢出、整数溢出等；可移植软件容器带来的安全漏洞：节点劫持、部署后门容器、部署恶意容器、获得恶意代码执行机会等。

93989. Keras 框架的设计遵循了哪些原则？

Answers

用户友好、模块化、易扩展性、基于 Python 实现。

93990. 数据投毒攻击和对抗攻击的区别是什么？

Answers

最主要的区别：投毒攻击直接将恶意数据投入到训练集中，污染模型；对抗攻击则作用于模型的测试和使用阶段，攻击者根据参数已经固定的模型，使用特定算法制造对抗样本[合理即可]

93991. 简述 PGD 算法

Answers

PGD 算法可以理解为迭代的 FGSM 算法，沿着梯度方向多步更新样本

$$x^0 = x$$

$$x^{(t+1)} = clip\left(x^{(t)} + \varepsilon \cdot sgn\left(\nabla_x \mathcal{L}\left(x^{(t)}\right)\right)\right)$$

其中，$x_i{}^{(t)}$表示第t步迭代生成的对抗样本，$clip(x)$表示对x梯度裁剪。[合理即可]
