网络安全技术（统设课）

【题目】1. 网络安全的基本属性有：可用性、完整性和保密性，保密性是指对信息资源（\_\_\_\_\_\_\_\_）的控制。

A. 使用设备

B. 开放范围

C. 保存介质

D. 存储环境

答案： B

解析 网络安全的基本属性。

【题目】2. 数据被非法篡改破坏了信息安全的（\_\_\_\_\_）。

A. 完整性

B. 可用性

C. 保密性

D. 不可抵赖性

答案： A

解析 网络安全的基本属性。

【题目】3. 在网络安全的三大基本属性中，关注信息不被非授权访问和泄露的是（\_\_\_\_\_）。

A. 可用性

B. 完整性

C. 保密性

D. 透明性

答案： C

解析 网络安全的基本属性。

【题目】4. 哪一部法律明确了个人信息跨境传输规则的相关内容？

A. 《中华人民共和国个人信息保护法》

B. 《中华人民共和国数据安全法》

C. 《中华人民共和国密码法》

D. 《中华人民共和国网络安全法》

答案： A

解析 关于重要安全法规的信息。

【题目】5. 全国人民代表大会常务委员会于哪一年表决通过了《中华人民共和国网络安全法》？

A. 2015年

B. 2016年

C. 2017年

D. 2018年

答案： B

解析 关于重要安全法规的信息。

【题目】6. （\_\_\_\_\_\_\_）主要规定了数据加密和保护的相关内容。

A. 《中华人民共和国个人信息保护法》

B. 《中华人民共和国数据安全法》

C. 《中华人民共和国密码法》

D. 《中华人民共和国网络安全法》

答案： C

解析 关于重要安全法规的信息。

【题目】7. 随着攻防对抗技术的不断演进，一些漏洞扫描工具在检测目标系统的脆弱点时，还会进行攻击概念验证（POC），从而确认此脆弱点是否可以被利用。以下哪个工具具有攻击概念验证的功能？

A. ping

B. netstat

C. ipconfig

D. fscan

答案： D

解析 网络安全工具和使用。

【题目】8. 被动攻击主要是监视公共媒体传输的信息，下列属于典型被动攻击的是

A. 解密通信数据

B. 会话拦截

C. 系统干涉

D. 修改数据

答案： A

解析 网络安全工具和使用。

【题目】9. 网络扫描是信息收集的重要手段，以下哪个工具不属于网络扫描工具？

A. nmap

B. zmap

C. ipconfig

D. masscan

答案： C

解析 网络安全工具和使用。

【题目】10. 下列哪项不是网络攻击的主要目的？

A. 获取目标的重要信息和数据

B. 对目标系统进行信息篡改和数据资料删除

C. 让目标无法正常提供服务

D. 造成人员伤亡

答案： D

解析 网络安全工具和使用。

【题目】11. 以下哪个不是常见的网络攻击手段？

A. 端口和漏洞扫描

B. 进入机房将服务器下电

C. 网络窃听

D. 使用MS17-010漏洞获取服务器权限

答案： B

解析 网络攻击手段。

【题目】12. 向有限的存储空间输入超长的字符串属于（\_\_\_\_）攻击手段。

A. 缓冲区溢出

B. 运行恶意软件

C. 浏览恶意代码网站

D. SQL注入

答案： A

解析 网络攻击手段。

【题目】13. SQL注入是一种常见的数据库攻击手段，SQL注入漏洞也是最普遍的漏洞之一。以下哪个工具是SQL注入常用的工具？

A. SQLMap

B. PostgresSQL

C. SQLite

D. Wireshark

答案： A

解析 网络攻击手段。

【题目】14. 网络嗅探器（Network Sniffer）常用于网络管理，也经常被攻击者用于信息获取。以下哪个工具可用于网络嗅探？

A. fscan

B. hydra

C. wireshark

D. metasploit

答案： C

解析 常用攻击工具和其使用。

【题目】15. 口令破解是攻击者常用的手段，以下哪个工具可用于口令破解？

A. fscan

B. hydra

C. wireshark

D. nmap

答案： B

解析 常用攻击工具和其使用。

【题目】16. 进行网络渗透测试通常遵循哪种顺序？

A. 控制阶段、侦查阶段、入侵阶段

B. 入侵阶段、侦查阶段、控制阶段

C. 侦查阶段、入侵阶段、控制阶段

D. 侦查阶段、控制阶段、入侵阶段

答案： C

解析 常用攻击工具和其使用。

【题目】17. 以下哪种是常见的恶意代码类型？

A. PoC

B. 木马

C. 漏洞信息

D. IoC

答案： B

解析 常用攻击工具和其使用。

【题目】18. 中国国家信息安全漏洞库（China National Vulnerability Database of Information Security）的简称是什么？

A. CNVD

B. NVD

C. CNNVD

D. CVE

答案： C

解析 漏洞库和勒索软件相关。

【题目】19. 使用哪种语言编写的软件通常更容易出现缓冲区溢出漏洞？

A. Python

B. Java

C. C/C++

D. JavaScript

答案： C

解析 漏洞库和勒索软件相关。

【题目】20. 在漏洞管理中，哪个组织负责发布通用漏洞和暴露（CVE）编号？

A. MITRE

B. ISO

C. IETF

D. NIST

答案： A

解析 漏洞库和勒索软件相关。

【题目】21. 以下关于恶意代码的描述错误的是

A. 独立的恶意代码能够独立传播、运行

B. 蠕虫与病毒类似，但传播能力更强，可以自动进行传播

C. 安全知识、系统补丁和一个好的防病毒软件能有效地保护系统不受恶意代码的威胁

D. 后门需要嵌入某个完整的程序中，成为该程序的一个组成部分来运行

答案： C

解析 抵御恶意软件。

【题目】22. 要完全杜绝计算机系统受到恶意攻击，应该采取哪种方法？

A. 仅安装最新的操作系统

B. 购买最贵的安全软件

C. 只在知名网站上浏览

D. 没有万无一失的方法

答案： D

解析 抵御恶意软件。

【题目】23. 以下哪一种是防止系统不受恶意代码威胁的良好习惯？

A. 学习安全知识、及时更新系统补丁，以及安装一个好的防病毒程序

B. 来历不明的U盘先插到个人电脑上杀毒后使用

C. 安全补丁攒到一定数量再一起安装，节省系统资源

D. 系统的管理员密码保存到桌面上防止丢失

答案： A

解析 抵御恶意软件。

【题目】24. 当你感觉到你的电脑运行速度明显减慢，打开任务管理器后发现CPU的使用率达到了百分之百，你认为你受到了哪一种攻击？

A. 特洛伊木马

B. 拒绝服务攻击

C. 欺骗攻击

D. 中间人攻击

答案： B

解析 当CPU使用率达到百分之百时，通常是因为遭受了拒绝服务攻击，因此选项B是答案。抵御病毒。

【题目】25. 以下哪个不是计算机病毒的类别？

A. 朊病毒

B. 宏病毒

C. 文件型病毒

D. 电子邮件病毒

答案： A

解析 选项A“朊病毒”实际上是一种生物病毒，不是计算机病毒，因此是答案。抵御病毒。

【题目】26. 对于电子邮件附件，哪一种做法最不安全？

A. 打开来自不明发送者的附件

B. 先使用防病毒软件扫描附件

C. 仅打开来自已知联系人的附件

D. 先将附件保存在隔离区域，然后打开

答案： A

解析 直接打开来自不明发送者的附件是最不安全的行为，因为这样容易感染计算机病毒。因此选项A是答案。抵御病毒。

【题目】27. 以下哪个不是防火墙的基本功能？

A. 访问控制功能

B. 内容控制功能

C. 日志功能

D. 防范垃圾邮件功能

答案： D

解析 防火墙功能。选项D“防范垃圾邮件功能”并非防火墙的基本功能，因此是答案。

【题目】28. 下列哪项不是防火墙的部署位置？

A. 网络边缘

B. 内部网络

C. 数据中心

D. 远程桌面

答案： D

解析 防火墙功能。选项D“远程桌面”不是防火墙的常见部署位置，因此是答案。

【题目】29. 网络防御技术中，哪一项不是用于数据保密的？

A. 加密算法

B. 身份认证

C. 访问控制

D. 电子邮件过滤

答案： D

解析 网络防御技术。选项D“电子邮件过滤”不是用于数据保密的，因此是答案。

【题目】30. 网络防御技术中，哪种方法用于识别合法用户？

A. 身份认证

B. 入侵检测

C. 数据加密

D. 数据备份

答案： A

解析 网络防御技术。选项A“身份认证”用于识别合法用户，因此是答案。

【题目】31. 在Endsley模型中，态势预测是基于（\_\_\_\_\_\_）的。

A. 要素感知

B. 态势理解

C. 事件审计

D. 风险控制

答案： B

解析 态势感知。答案是B，因为在Endsley模型中，态势预测是基于“态势理解” 。

【题目】32. 哪一项是Endsley模型中的第一个层级？

A. 要素感知

B. 态势理解

C. 事件审计

D. 态势预测

答案： A

解析 态势感知。答案是A，因为在Endsley模型中，第一个层级是“要素感知” 。

【题目】33. 哪一项是Endsley模型中的最后一个层级？

A. 要素感知

B. 态势理解

C. 事件审计

D. 态势预测

答案： D

解析 态势感知。答案是D，因为在Endsley模型中，最后一个层级是“态势预测” 。

【题目】34. 加密算法的功能是实现信息的（\_\_\_\_\_\_\_），数字签名算法可实现信息的（\_\_\_\_\_\_）。

A. 保密性，不可否认性

B. 不可否认性，保密性

C. 完整性，可用性

D. 真实性，保密性

答案： A

解析 加密算法和签名算法。答案是A，因为加密算法用于实现信息的“保密性”，而数字签名算法用于实现信息的“不可否认性” 。

【题目】35. 以下算法中属于非对称算法的是（\_\_\_\_\_\_\_）。

A. DES

B. RSA

C. IDEA

D. AES

答案： B

解析 加密算法和签名算法。答案是B，因为“RSA”是一种非对称加密算法。

【题目】36. AES算法属于哪一类型的加密算法？

A. 非对称加密

B. 对称加密

C. 哈希算法

D. 流加密

答案： B

解析 加密算法和签名算法。答案是B，因为“AES”是一种对称加密算法。

【题目】37. 以下关于数字签名说法正确的是（\_\_\_\_\_\_\_）。

A. 数字签名是在所传输的数据后附加上一段和传输数据毫无关系的数字信息

B. 数字签名能够解决数据的加密传输，即安全传输问题

C. 数字签名一般采用对称加密机制

D. 数字签名用于解决篡改、伪造等安全性问题

答案： D

解析 签名算法。答案是D，因为数字签名能够解决篡改、伪造等安全性问题。

【题目】38. 数字签名算法主要用于确保信息的哪两项？

A. 完整性和真实性

B. 真实性和不可否认性

C. 保密性和完整性

D. 完整性和不可否认性

答案： D

解析 签名算法。答案是D，因为数字签名算法主要用于确保信息的“完整性”和“不可否认性” 。

【题目】39. 在以下古典密码体制中，不属于置换密码的是

A. 移位密码

B. 逆序密码

C. 凯撒密码

D. 转轮密码

答案： C

解析 考察对古典密码体制中置换密码和替换密码的区别。凯撒密码是一种替换密码，不属于置换密码。因此，选择C是正确的。

【题目】40. 以下哪种密码体制不需要密钥？

A. AES

B. RSA

C. DES

D. ROT13

答案： D

解析 ROT13不需要密钥，因为它是凯撒密码的一个特例，只是将每个字母移动13个位置。因此，选择D是正确的。

【题目】41. 在古典密码中，哪种方法是基于破译明文攻击的？

A. 暴力破解

B. 频率分析

C. 逐字替换

D. 时间戳攻击

答案： B

解析 在古典密码中，频率分析是一种基于破译明文攻击的方法。通过分析字符出现的频率，可以推断可能的密钥或明文内容。因此，选择B是正确的。

【题目】42. 以下哪种认证方式相对最安全？

A. 口令认证技术

B. 人脸识别认证

C. 短信验证码认证

D. 多因素认证

答案： D

解析 多因素认证通常涉及多个独立的认证方法，因此相对更安全。选择D是正确的。

【题目】43. 以下哪种不是常见的安全认证技术？

A. 口令认证技术

B. 人脸识别认证

C. 短信验证码认证

D. 基于已有知识的认证技术

答案： D

解析 基于已有知识的认证技术不是一种常见的安全认证技术方法。选择D是正确的。

【题目】44. CA认证中心的主要作用是？

A. 加密数据

B. 发放数字证书

C. 安全管理

D. 解密数据

答案： B

解析 CA（证书认证中心）主要作用是发放数字证书，用于身份验证和数据加密。选择B是正确的。

【题目】45. 对于数字证书，哪个组织负责其全球互认？

A. IETF

B. ISO

C. PKI

D. ICANN

答案： C

解析 PKI（公钥基础设施）是负责数字证书全球互认的组织。选择C是正确的。

【题目】46. 以下哪个口令相对最为安全？

A. 12345678

B. 1qaz@WSX

C. p%ss#w8Rd

D. p@ssword

答案： C

解析 安全的口令应该包含大小写字母、数字和特殊字符。因此，选择C是正确的。

【题目】47. 以下哪个口令相对最为安全？

A. ZXCV5TGB

B. pAsswOrd@3!!

C. 1QAZ2WSX

D. p@ssword

答案： B

解析 安全的口令应该包含大小写字母、数字和特殊字符。因此，选择B是正确的。

【题目】48. 以下哪种是常见的网站拒绝服务攻击技术？

A. HTTP Flood

B. SQL注入

C. 目录扫描

D. XSS攻击

答案： A

解析 HTTP Flood是一种常用的网站拒绝服务攻击技术，其目的是使目标服务器无法处理请求。因此，选择A是正确的。

【题目】49. 以下哪种是常见的网站拒绝服务攻击技术？

A. SQL注入

B. CC攻击

C. 目录扫描

D. XSS攻击

答案： B

解析 CC攻击是一种常用的网站拒绝服务攻击技术，旨在使目标网站无法处理合法请求。因此，选择B是正确的。

【题目】50. 安全电子邮件使用（\_\_\_\_）协议？

A. PGP

B. HTTPS

C. MIME

D. DES

答案： A

解析 PGP（Pretty Good Privacy）是用于电子邮件安全的加密协议。因此，选择A是正确的。

【题目】51. 使用HTTPS的主要目的是什么？

A. 加速网站访问

B. 提供数据加密

C. 提高搜索引擎排名

D. 压缩网站数据

答案： B

解析 HTTPS主要用于加密传输的数据，以保护用户信息和数据安全。因此，选择B是正确的。

【题目】52. 某单位员工收到一封仿冒的邮件，要求其立即通过邮件里的链接更新账号密码，该员工受到的是什么类型的电子邮件攻击？

A. 病毒攻击

B. 钓鱼邮件攻击

C. 勒索攻击

D. 窃听攻击

答案： B

解析 这是一种钓鱼邮件攻击，旨在诱导用户点击恶意链接并泄露信息。因此，选择B是正确的。

【题目】53. 下列关于VPN的说法中哪一项是正确的？

A. VPN是虚拟专用网的简称，它只能对ISP实施维护

B. VPN只能在第二层数据链路层上实现加密

C. 使用VPN技术，可以建立安全通道，并能使用VPN提供的安全服务

D. VPN使用通道技术加密，但没有身份验证功能

答案： C

解析 IPSEC是一种用于实现VPN安全的协议。因此，选择C是正确的。

【题目】54. 即使域名邮箱配置了SPF和DKIM，添加哪种策略也可以进一步强化电子邮件的安全性？

A. TLS

B. DMARC

C. PGP

D. S/MIME

答案： B

解析 DMARC策略能够强迫对声称来自我们域名的所有电子邮件执行SPF和DKIM检查，提供更全面的安全性。因此，选择B是正确的。

【题目】55. 区块链技术在安全性方面的一个主要优点是什么？

A. 更快的交易速度

B. 数据不可篡改

C. 低成本

D. 可编程性

答案： B

解析 区块链技术的一个主要安全优点是其数据不可篡改性，由于链式结构和加密机制，一旦数据被添加就很难被修改。因此，选择B是正确的。

【题目】56. 在云环境中，责任主体

A. 相对于传统环境更加简单

B. 相对于传统环境更加复杂

C. 与传统环境相同

D. 没有责任主体

答案： B

解析 在云环境中，责任主体更加复杂，涉及到云服务商、租户和可能的第三方服务提供商。因此，答案是B。

【题目】57. 数据安全在云环境中的要求是什么？

A. 相对于传统环境更低

B. 相对于传统环境更高

C. 与传统环境相同

D. 无要求

答案： B

解析 在云环境中，由于责任主体复杂性和数据存储地点的远离，数据安全要求更高。因此，答案是B。

【题目】58. CTF（Capture The Flag）中文一般译作夺旗赛，常见的竞赛模式包含哪几项？

A. 解题模式（Jeopardy）

B. 攻防模式（Attack-Defense）

C. 对抗模式（Adversarial）

D. 混合模式（Mix）

答案： ABD

解析 网络安全基础知识。CTF常见的竞赛模式包括解题模式（Jeopardy）、攻防模式（Attack-Defense）和混合模式（Mix），没有对抗模式（Adversarial）。因此，答案是ABC。

【题目】59. 在网络安全中，哪些是评估系统安全性的关键因素？

A. 可用性

B. 可靠性

C. 完整性

D. 保密性

答案： ACD

解析 网络安全基础知识。在网络安全中，可用性、完整性和保密性是评估系统安全性的关键因素。

【题目】60. 端口扫描工具能获取以下哪些信息？

A. 端口开放信息

B. 端口提供的服务

C. 主机的操作系统

D. 主机硬件信息

答案： ABC

解析 端口扫描工具主要获取端口开放信息、端口提供的服务和主机的操作系统。

【题目】61. 网络攻击的一般过程包括：

A. 采集目标信息、脆弱点和漏洞分析

B. 实施攻击和获取权限

C. 关闭目标上运行的服务

D. 权限提升、横向移动、后门和持久化

答案： ABD

解析 网络攻击通常包括目标信息收集、脆弱点和漏洞分析、实施攻击和获取权限，以及权限提升、横向移动、后门和持久化。

【题目】62. 下列哪些是入侵检测系统信息收集的来源？

A. 日志文件

B. 网络流量

C. 系统目录和文件

D. 硬件配置

答案： ABC

解析 入侵检测系统主要从日志文件、网络流量和系统目录和文件中收集信息。

【题目】63. 高级持续威胁（APT）攻击的主要特征包括哪些？

A. 高度定制和复杂性

B. 持续监控目标并保持长期访问权

C. 攻击目标通常重要，造成巨大的损失或影响

D. 容易被专业杀毒软件查杀

答案： ABC

解析 网络安全攻击技术。APT攻击具有高度的定制和复杂性（A选项），持续监控目标并保有长期访问权（B选项），以及攻击目标通常是重要的，可能造成巨大的损失或政治影响（C选项）。因此，选项A、B、C是正确的。

【题目】64. 关于MITRE公司提出的Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) 网络攻击矩阵模型，哪些说法是正确的？

A. ATT&CK模型从攻击者的视角描述攻击阶段使用的技术

B. Enterprise ATT&CK框架包含14个战术阶段

C. ATT&CK常见的应用场景包括网络威胁情报收集

D. ATT&CK只针对Windows系统

答案： ABC

解析 网络安全基础知识。ATT&CK模型从攻击者的视角描述各阶段用到的攻击技术（A选项），其Enterprise版本包括14个战术阶段（B选项），并且它在网络威胁情报收集等多个应用场景中有着广泛的应用（C选项）。因此，选项A、B、C是正确的。

【题目】65. 洛克希德·马丁公司提出的网络杀伤链（Kill Chain）模型包括哪些阶段？

A. 目标侦察（Reconnaissance）

B. 武器构造（Weaponization）

C. 载荷投送（Delivery）

D. 数据加密（Data Encryption）

答案： ABC

解析 网络安全基础知识。网络杀伤链模型包括目标侦察（A选项）、武器构造（B选项）和载荷投送（C选项）等阶段，而数据加密不属于该模型的标准阶段（D选项）。因此，选项A、B、C是正确的。

【题目】66. 漏洞蠕虫破坏力强、传播速度快，其传播过程一般可以分为哪几个步骤？

A. 扫描

B. 攻击

C. 复制

D. 潜伏

答案： ABC

解析 恶意代码及防范技术。漏洞蠕虫的传播一般包括扫描（A选项）、攻击（B选项）和复制（C选项）这几个步骤。潜伏（D选项）不是其一般的传播步骤。因此，选项A、B、C是正确的。

【题目】67. 恶意软件主要通过哪些方式进行传播？

A. 软件捆绑

B. 利用漏洞

C. 空气传播

D. 远程下载

答案： ABD

解析

恶意软件主要通过软件捆绑、利用漏洞和远程下载等方式进行传播。C选项（空气传播）通常不是恶意软件的主要传播方式。

【题目】68. 恶意代码的行为表现可能包括哪些？

A. 系统破坏

B. 数据窃取

C. 非授权访问

D. 系统优化

答案： ABC

解析 恶意代码的行为可能包括系统破坏、数据窃取和非授权访问。D选项（系统优化）一般不会是恶意代码的行为表现。

【题目】69. 预防计算机病毒，应该注意哪些方面？

A. 安装并更新防病毒软件

B. 确认文件来源后再运行

C. 及时更新系统和应用补丁

D. 任意下载和运行程序

答案： ABC

解析 预防计算机病毒方面，应注意安装并更新防病毒软件、确认文件来源后再运行，以及及时更新系统和应用补丁三个方面。D选项是不安全的行为，不应作为防病毒的措施。

【题目】70. 针对病毒的防护，哪些检测方法是常用的？

A. 人工检测

B. 自动检测

C. 使用内存监测工具检查

D. 随机删除文件

答案： ABC

解析 原始内容：病毒防护的常用检测方法包括人工检测、自动检测和使用内存监测工具检查。选择答案的原因：D选项随机删除文件并不是一种有效的病毒检测方法。

【题目】71. 按照访问控制方式不同，防火墙可以分为哪几种？

A. 包过滤防火墙

B. 下一代防火墙

C. 应用代理防火墙

D. 状态检测防火墙

答案： ACD

解析 原始内容：防火墙按照访问控制方式可以分为包过滤防火墙、状态检测防火墙和应用代理防火墙。

【题目】72. 关于防火墙规则的描述，哪些是错误的？

A. 入站规则即你的电脑连接其他主机的规则

B. 出站规则即其他主机连入你的电脑的规则

C. 默认情况下防火墙允许所有传出连接

D. 默认情况下防火墙拒绝所有传入连接

答案： ABD

解析 原始内容：防火墙的入站和出站规则及其默认设置，C选项是默认情况。

【题目】73. 入侵检测系统（IDS）的主要功能包括哪些？

A. 异常行为识别

B. 与防火墙联动

C. 实时保护

D. 对入侵行为采取动作

答案： ABC

解析 原始内容：IDS主要作用是监控网络状况，但不会对入侵行为采取动作。能够提供对内部攻击、外部攻击和误操作的实时保护。通常情况下，IDS设备会以旁路的方式接入网络中，与防火墙联动。选择答案的原因：选项A、B和C都准确地描述了IDS的主要功能，而选项D不准确。

【题目】74. 零信任遵循的原则有哪些？

A. 不做任何假定

B. 相信任何人

C. 随时检查一切

D. 防范动态威胁

答案： ACD

解析 原始内容：零信任遵循的原则有：不做任何假定、随时检查一切、防范动态威胁。选择答案的原因：选项A、C和D准确地描述了零信任所遵循的原则，而选项B不准确。

【题目】75. 密码分析学中注重哪几大规律？

A. 密码规律

B. 文字规律

C. 情况规律

D. 算法规律

答案： ABC

解析 原始内容：在密码分析学中，注重以下三大规律——密码规律、文字规律、情况规律。选择答案的原因：选项A、B和C准确地描述了密码分析学中注重的三大规律，而选项D未在课本中提及。

【题目】76. 流密码的安全性依赖于哪些因素？

A. 密钥序列的随机性

B. 密钥序列的不可预测性

C. 收发两端密钥流的精确同步

D. 密码的复杂性

答案： ABC

解析 原始内容：流密码强度完全依赖于密钥序列的随机性（Randomness）和不可预测性（Unpredictability）。设计流密码的核心问题，是密钥流的产生以及保持收发两端密钥流的精确同步。选择答案的原因：选项A、B和C准确地描述了流密码的安全性依赖的因素，而选项D未在课本内容中提及。

【题目】77. 一般来说，认证机制由哪几个部分构成？

A. 验证对象

B. 验证协议

C. 认证口令

D. 鉴别实体

答案： ABD

解析 原始内容：一般来说，认证机制由验证对象、验证协议和鉴别实体构成。选择答案的原因：选项A、B和D准确描述了认证机制通常由哪几个部分构成，而选项C未在原始内容中提及。

【题目】78. 以下哪些属于身份认证方案的常见类型？

A. 基于秘密信息的身份认证

B. 基于信任物体的身份认证

C. 基于生物特征的身份认证

D. 基于用户管理的身份认证

答案： ABC

解析 原始内容：身份认证方案通常分为基于秘密信息、基于信任物体和基于生物特征的类型。选择答案的原因：选项A、B和C准确描述了身份认证方案的常见类型，而选项D未在原始内容中提及。

【题目】79. 认证技术主要有哪些实现方式？

A. 口令认证技术

B. 单点登录技术

C. 基于生物特征认证技术

D. 网络监控技术

答案： ABC

解析 原始内容：认证技术方法主要有口令认证技术、单点登录技术、基于生物特征认证技术等多种实现方式。选择答案的原因：选项A、B和C准确描述了认证技术的主要实现方式，而选项D未在原始内容中提及。

【题目】80. 下列选项中哪些可以增强口令认证的安全性？

A. 采用MD5等单向HASH算法保护密码

B. 在传输过程中对口令进行加密

C. 采用挑战响应的认证方式

D. 采用长度较长的英文单词做口令

答案： ABC

解析 原始内容：增强口令认证的安全性应至少包括：口令信息采用MD5等单向HASH算法加密存储，传输过程中加密口令，以及采用挑战响应的认证方式。选择答案的原因：A、B和C选项准确地描述了如何增强口令认证的安全性，D选项与原文不符。

【题目】81. 以下哪些属于政务网站安全防护的内容？

A. 网页防篡改

B. 入侵防御和病毒防护

C. 网络/数据库审计

D. 钓鱼邮件防护

答案： ABC

解析 原始内容：政务网站安全防护应包括网页防篡改、入侵防御和病毒防护，以及网络/数据库审计。选择答案的原因：A、B和C选项都是政务网站应进行的安全防护措施，而D选项钓鱼邮件防护与政务网站不直接相关。

【题目】82. 邮件安全防护中常用的手段包括哪些？

A. 垃圾邮件过滤

B. 邮件加密

C. 恶意链接检测

D. 网络监控

答案： ABC

解析 原始内容：邮件安全防护通常包括垃圾邮件过滤、邮件加密和恶意链接检测。选择答案的原因：A、B和C选项准确地描述了邮件安全防护中常用的手段，D选项网络监控不是专门针对邮件安全的措施。

【题目】83. 为增强网站和邮件安全，应注意哪些方面？

A. 使用强口令

B. 定期更新安全补丁

C. 数据备份

D. 无线网络加密

答案： ABC

解析 原始内容：为增强网站和邮件的安全性，应注意使用强口令、定期更新安全补丁和进行数据备份。选择答案的原因：A、B和C选项准确地描述了为增强网站和邮件安全应注意的方面，而D选项无线网络加密与本主题不直接相关。

【题目】84. 区块链技术主要有哪些特点？

A. 去中心化

B. 不可篡改

C. 共识

D. 隐私保护

答案： ABC

解析 原始内容：区块链技术主要有去中心化、不可篡改、共识等特点。选择答案的原因：A、B和C选项准确描述了区块链技术的主要特点。

【题目】85. 物联网安全防护主要分为哪几个层次？

A. 终端安全

B. 通信网络安全

C. 服务端安全

D. 物理安全

答案： ABC

解析 物联网安全防护主要分为三个层次：终端安全、通信网络安全和服务端安全。终端安全主要关注硬件、接入、操作系统、业务应用等方面；通信网络安全涉及网络接入技术和数据传输加密；服务端安全主要针对数据管理系统和基于云计算的web应用等。

【题目】86. 网络安全体系是由各种网络安全单元构成的，共同实现网络安全目标的一种体系架构，包括法律法规、安全策略、组织管理、技术措施等多方面因素。

答案： √

解析 原题正确。网络安全体系确实包括了法律法规、安全策略、组织管理和技术措施等多方面因素。

【题目】87. 存储和处理涉及国家秘密信息的网络的运行安全保护，除遵守《网络安全法》外，还应遵守保密法律和行政法规。

答案： √

解析 原题正确。除了遵守《网络安全法》，还应当遵守保密法律和行政法规来确保网络安全。

【题目】88. 网络安全目标的实现需要综合多方面因素，包括但不限于法律法规、安全策略和技术措施。

答案： √

解析 原题正确。实现网络安全目标确实需要综合多方面因素，包括法律法规、安全策略和技术措施。

【题目】89. 网络社会的发展为违法犯罪分子提供了一个新的领域，但其社会危害性远不如现实社会中的违法犯罪。

答案：×

解析 原题错误。网络社会的违法犯罪同样具有很高的社会危害性。

【题目】90. 通过电话方式骗取用户账号密码属于社会工程学方法。

答案： √

解析 原题正确。该行为确实属于社会工程学的一种手法。

【题目】91. 《国家网络安全事件应急预案》主要内容仅包括组织机构和职责。

答案：×

解析 原题错误。《国家网络安全事件应急预案》还包括监测与预警、应急响应、调查评估、预防工作和保障措施等。

【题目】92. 各单位应按照“谁主管谁负责，谁运营谁负责”的原则，组织对本单位网络和信息系统进行安全监测。

答案： √

解析 原题正确。“谁主管谁负责，谁运营谁负责”是正确的安全监测原则。

【题目】93. MITRE公司提出的网络攻击矩阵模型是从防守者视角来描述各阶段攻击技术的模型。

答案：×

解析 原题错误。该模型是从攻击者的视角来描述攻击各阶段用到的技术。

【题目】94. 目前使用较多的网络攻击模型主要包括网络杀伤链模型和网络攻击矩阵模型。

答案： √

解析 原题正确。网络杀伤链模型和网络攻击矩阵模型是目前使用较多的网络攻击模型。

【题目】95. 目标系统存在的漏洞是产生网络安全威胁的唯一原因。

答案：×

解析 原题错误。除了系统漏洞外，还有其他如人为因素、软件缺陷等也可产生网络安全威胁。

【题目】96. 只要设置了口令，资源就能得到很好的访问控制。

答案：×

解析 原题错误。仅设置口令并不能确保资源的充分访问控制，还需其他安全措施。

【题目】97. 抵抗入侵者的第一道防线通常是口令系统。

答案： √

解析 原题正确。口令系统通常是抵抗入侵者的第一道防线。

【题目】98. 口令通常是最容易被突破的资源访问控制机制。

答案： √

解析 原题正确。口令因为其便利性和普遍性往往是最容易被攻破的。

【题目】99. 明文保存的用户口令容易被直接利用，因此很多系统采用单向哈希算法进行加密保存。

答案： √

解析 原题正确。明文保存的口令容易被利用，所以常用单向哈希算法进行加密保存。

【题目】100. 受感染机器间能够协同工作是区分僵尸网络和其他恶意软件的关键特性。

答案： √

解析 原题正确。受感染机器间的协同工作是僵尸网络和其他恶意软件的区别之一。

【题目】101. 掌握漏洞资源等于掌握了网络安全的绝对主动权。

答案：×

解析 原题错误。虽然掌握漏洞资源能提供一定的主动权，但不能说是绝对的主动权。网络安全涉及多个方面。

【题目】102. 网络蠕虫按传播途径和攻击性可分为传统蠕虫、邮件蠕虫和漏洞蠕虫，其中邮件蠕虫主要依赖邮件传播。

答案： √

解析 原题正确。网络蠕虫确实可以按照传播途径和攻击性进行分类，邮件蠕虫主要通过邮件传播。

【题目】103. 网络蠕虫的危害性通常大于计算机病毒，但其生命周期比计算机病毒短得多。

答案： √

解析 原题正确。网络蠕虫由于自我复制和传播的能力通常比计算机病毒更具危害性，但由于容易被检测和消除，其生命周期通常较短。

【题目】104. 网络隔离技术总体上分为物理隔离和逻辑隔离两类。

答案： √

解析 原题正确。网络隔离技术确实可以分为物理隔离和逻辑隔离两大类。

【题目】105. 入侵防御技术在攻击到达的同时或之后会发出告警。

答案： √

解析 原题正确。入侵防御技术确实可以在攻击到达的同时或之后发出告警。

【题目】106. 签名仅用于描述网络中正常数据流的特征。

答案：×

解析 原题错误。签名实际上是用来描述网络中攻击行为的特征，而非仅用于描述正常数据流的特征。通过将数据流和入侵防御签名进行比较，能够检测和防范攻击。

【题目】107. 迪菲和赫尔曼提出的公钥密码系统在保密通信、密钥分配和鉴别等方面具有深远的影响。

答案： √

解析 迪菲和赫尔曼提出的公钥密码系统确实在保密通信、密钥分配和鉴别等方面有重要作用。

【题目】108. 在设计密码系统时，应遵循Kerckhoffs假设以确保安全性。

答案： √

解析 在设计密码系统时，确实应在Kerckhoffs假设下确保其安全性。

【题目】109. 在DES加密过程中，S盒对加密的强度不产生影响。

答案：×

解析 在DES加密过程中，S盒对加密的强度确实产生影响。

【题目】110. 三重DES能够抵御中途相遇攻击。

答案： √

解析 三重DES确实能够抵御中途相遇攻击。

【题目】111. 单点登录是指用户在访问不同系统时，只需进行一次身份认证，然后可根据该认证访问授权资源。

答案： √

解析 单点登录确实是用户访问不同系统时，只需进行一次身份认证，便可访问授权资源。

【题目】112. 认证通常由标识（Identification）和鉴别（Authentication）两部分组成。

答案： √

解析 认证一般确实由标识（Identification）和鉴别（Authentication）两部分组成。

【题目】113. 认证是指一个实体向另一个实体证明其声称的身份。

答案： √

解析 认证确实是一个实体向另一个实体证明其所声称的身份的过程。

【题目】114. 多因素认证通过组合多种鉴别信息提升了认证安全性。

答案： √

解析 多因素认证确实使用多种鉴别信息进行组合，从而提升认证的安全强度。

【题目】115. 网站假冒仅通过网站域名欺骗进行。

答案：×

解析 网站假冒不仅通过网站域名欺骗，还包括网站域名劫持、中间人等技术手段。

【题目】116. 非授权访问是由于网站服务的技术缺陷导致的安全漏洞。

答案：×

解析 非授权访问是由于网站认证机制的安全缺陷，而不是网站服务的技术缺陷导致的。错误答案：的原因是描述中的“网站服务的技术缺陷”不准确。

【题目】117. Web应用防火墙用于保护Web服务器和Web应用，提供安全防护功能。

答案： √

解析 Web应用防火墙确实是用于保护Web服务器和Web应用的网络安全机制。

【题目】118. SPF是电子邮件验证中最基本和最常见的保护技术之一。

答案： √

解析 SPF确实是电子邮件验证中最基本和最常见的保护技术之一。

【题目】119. 移动应用安全与传统的Web安全问题相同，不需单独考虑移动应用的安全。

答案：×

解析 移动应用安全与传统的Web安全存在差异，需要单独考虑移动应用的安全问题。

【题目】120. 安全大数据分析是指利用大数据手段对网络安全运维相关数据进行分析和挖掘。

答案： √

解析 安全大数据分析确实是利用大数据手段对网络安全运维相关数据进行分析和挖掘。