网络安全技术

单选(140)--电大资源网：http://www.dda123.cn/（微信搜：905080280）

1、2021 年 11 月 1 日，我国第一部完整规定个人信息处理规则的法律正式施行。这部法律厘清了个人信息、敏感个人信息、自动化决策、去标识化、匿名化的基本概念，从适用范围、个人信息处理的基本原则、处理规则、跨境传输规则等多个方面对个人信息保护进行了全面规定。这部法律是（）。-->A.《中华人民共和国个人信息保护法》
2、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
3、SQL 注入是一种非常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
4、（）是为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定的法律。该法由全国人民代表大会常务委员会于 2016 年 11 月 7 日表决通过，自 2017 年 6 月 1 日起施行。-->D.《中华人民共和国网络安全法》
5、（）主要规定了数据加密和保护的相关内容。-->C.《中华人民共和国密码法》
6、《中华人民共和国密码法》主要为了规范-->A.密码应用和管理
7、《中华人民共和国网络安全法》正式施行的时间是()。-->A.2017 年 6 月 1 日
8、《中华人民共和国网络安全法》正式施行的时间是()。-->A.2021 年 11 月 1 日
9、安全电子邮件使用（）协议？-->A.PGP
10、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
11、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？-->B.拒绝服务攻击
12、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
13、对于数字证书，哪个组织负责其全球互认？-->C.PKI
14、防火墙一般不负责哪项功能？-->C.多租户管理
15、根据 Endsley 模型，可以将态势感知划分为三个层级，不包括（）。-->C.事件审计
16、根据 Endsley 模型，可以将态势感知划分为三个层级，不包括（）。-->C.安全审计
17、根据 Endsley 模型，哪一项不是态势感知的三个层级之一？-->C.事件审计
18、根据秘铜的特点，可以将密码体制分为（）-->A.对称和非对称密码体制
19、关于勒索软件，下列哪个说法是正确的？-->B.勒索软件通过加密文件进行勒索
20、关于勒索软件，以下哪个说法是正确的（）。-->B.勒索软件通过加密受害者的文件并试图通过威胁勒索获利
21、关于勒索软件，以下哪个说明是错误的（）。-->C.解密高手可以破解勒索软件的密钥，从而恢复出被加密的文件
22、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？-->B.DMARC
23、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
24、加密算法的功能是实现信息的（）。-->A.不可否认性
25、加密算法的功能是实现信息的（）。-->B.保密性
26、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
27、进行网络渗透测试通常遵循哪种顺序？-->C.侦查阶段、入侵阶段、控制阶段
28、口令破解工具是攻击者最常用的攻击工具，常见的口令破解方式有口令猜制、穷举搜索、撞库等，以下哪个工具能用于口令破解（）-->B.hydra
29、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？-->B.hydra
30、勒索软件通常如何进行传播？-->A.邮件附件
31、没有网络安全就没有（），就没有（），广大人民群众利益也难以得到保障。（）。-->B.国家安全、经济社会稳定运行
32、某单位员工收到一封电子邮件，提示其账号即将过期，要求其立马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（）-->B.钓鱼邮件攻击
33、某单位员工收到一封仿冒的邮件，要求其立马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？（）。-->B.钓鱼邮件攻击
34、某单位员工在非官方网站下载了一个软件工具的安装包，安装完成后发现所有个人文件都被加密无法访问，并被提示向一个数字货币钱包地址转账后获取解密方式，该员工受到的是什么类型的攻击？-->C.勒索攻击
35、某网站后台密码过于简单，被黑客破解登录了后台，并篡改了后台登录密码导致管理员无法登录，该网站遭受到了什么类型的攻击？-->A.非授权访问
36、哪个选项不是深度学习在网络安全中的应用场景？-->D.线稿上色
37、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》
38、哪一部法律是专门针对个人信息处理规则而制定的？-->A.《中华人民共和国个人信息保护法》
39、哪一项不是加密算法的主要功能？-->C.不可否认性
40、哪一项不是数字签名算法的主要功能？-->C.保密性
41、哪一项是 Endsley 模型中的第一个层级？-->A.要素感知
42、哪一项是 Endsley 模型中的最后一个层级？-->D.态势预测
43、哪种认证方法最容易受到社会工程学攻击？-->A.口令认证
44、区块链技术在安全性方面的一个主要优点是什么？-->B.数据不可篡改
45、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》？-->B.2016 年
46、使用 HTTPS 的主要目的是什么？-->B.提供数据加密
47、使用哪种方法存储口令最不安全？-->B.明文存储
48、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？-->C.C/C++
49、使用数字签名来确保信息在传输过程中没有被篡改，这属于保障了信息的哪个属性？-->B.完整性
50、数据安全在云环境中的要求是什么？-->B.相对于传统环境更高
51、数据被非法篡改破坏了信息安全的（）。-->A.完整性
52、数字签名算法可实现信息的（）。-->A.不可否认性
53、数字签名算法可实现信息的（）。-->C.保密性
54、数字签名算法主要用于确保信息的哪两项？-->D.完整性和不可否认性
55、随着攻防对抗技术的不断演进，在进行检测时往往需要扫描目标机器开放的端口，以下哪个工具或者命令具有扫描开放端口的功能？-->C.nmap
56、随着攻防技术对抗的不断演进，一些漏洞扫描工具在检测目标系统的脆弱点时，还会进行攻击的概念验证（POC），从而确认此脆弱点是否可以被利用。以下哪个工具有攻击概念验证的功能（）。-->D.fscan
57、随着攻防技术对抗的不断演进，在进行检测时往往需要扫描目标机器开放的端口，以下哪个工具或者命令具有扫描开放端口的功能（）。-->C.nmap
58、态势感知中哪一项需要先于其他项进行？-->A.要素感知
59、网络安全的基本属性不包括（）。-->D.不可抵赖性
60、网络安全的基本属性有（）。可用性、完整性和（）。-->C.保密性
61、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。-->B.开放范围
62、网络安全的基本属性有：可用性、完整性和（）。-->C.保密性
63、网络防御技术所包含的身份认证基本方法，不包括（）。-->D.基于签名证书的身份认证

64、网络防御技术中，哪项技术常用于阻止未经授权的数据访问？-->A.访问控制
65、网络防御技术中，哪一项不是用于数据保密的？-->D.电子邮件过滤
66、网络防御技术中，哪种方法用于识别合法用户？-->A.身份认证
67、网络防御中，哪项技术主要用于信息加密？-->A.公钥基础设施
68、网络防御中，以下哪种技术是用于预防数据泄露的？-->A.数据加密
69、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？-->C.ipconfig
70、网络扫描是信息收集的重要手段。通过扫描可以发现存活主机、开放端口，进而发现其运行的服务、操作系统等信息。以下哪个工具不属于网络扫描工具（）。-->C.ipconfig
71、网络嗅探器（NetworkSniffer）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？-->C.snort
72、网络嗅探器（NetworkSniffer）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？-->C.wireshark
73、网络嗅探器（NetworkSniffer）是一种常用的网络管理工具，也常常被攻击者利用来进行信息获取。以下哪个工具可以进行网络嗅探（）。-->C.wireshark
74、网络嗅探器（NetworkSniffer）是一种常用的网络管理工具，也常常被攻击者利用来进行信息获取。以下哪个工具可以进行网络嗅探（）。-->C.snort
75、物联网网络层分为（）。-->A.核心网和接入网
76、下列关于 VPN 的说法中哪一项是正确的？-->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
77、下列哪个不是网络攻击的主要目的（）。-->D.造成人员伤亡
78、下列哪项不是防火墙的部署位置？-->D.远程桌面
79、下列哪项不是网络攻击的主要目的？-->D.造成人员伤亡
80、下面哪个口令安全性相对更高？-->B.!@7es6RFE.
81、下面哪个口令安全性相对更高？-->B.RM3dkw．tg
82、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
83、要完全杜绝计算机系统受到恶意攻击，应该采取哪种方法？-->D.没有万无一失的方法
84、以下关于恶意代码的描述错误的是-->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
85、以下关于数字签名说法正确的是（）。-->D.数字签名用于解决篡改、伪造等安全性问题
86、以下关于愿意代码的描述错误的是（）-->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
87、以下哪个不是常见的恶意代码（）。-->D.细菌
88、以下哪个不是常见的网络防御技术（）.-->C.电子邮件技术
89、以下哪个不是常见的网络攻击手段（）-->C.物理关机
90、以下哪个不是常见的网络攻击手段（）。-->B.破坏供电系统造成服务器停电
91、以下哪个不是常见的网络攻击手段（）。-->B.进入机房将服务器下电
92、以下哪个不是常见的网络攻击手段？-->B.进入机房将服务器下电
93、以下哪个不是常见的网络攻击手段？-->B.破坏供电系统造成服务器停电
94、以下哪个不是常见的网络攻击手段？-->C.物理关机
95、以下哪个不是防火墙的基本功能（）。-->D.防范垃圾邮件功能
96、以下哪个不是计算机病毒的类别（）-->A.操作系统病毒
97、以下哪个不是计算机病毒的类别（）。-->A.脏病毒
98、以下哪个不是计算机病毒的类别（）。-->A.电子病毒
99、以下哪个不是计算机病毒的类别？-->A.脏病毒
100、以下哪个不是计算机病毒的类别？-->A.操作系统病毒
101、以下哪个不是计算机病毒的生命周期（）。-->A.感染阶段
102、以下哪个不是漏洞数据库（）。-->D.CVE
103、以下哪个不属于物联网安全防护层次（）。-->D.业务层安全
104、以下哪个不属于物联网安全防护层次（）。-->D.应用层安全
105、以下哪个口令相对最为安全（）-->B.pAsswOrd
106、以下哪个口令相对最为安全？-->B.78g@tw23．Y
107、以下哪个口令相对最为安全？-->C.pAsswOrd
108、以下哪个口令相对最为安全？-->B.pAsswOrd@3!!
109、以下哪个口令相对最为安全？-->C.p%ss#w8Rd
110、以下哪个口令相对最为安全？（）。-->C.pAsswOrd
111、以下哪个是常见的恶意代码类型（）。-->B.木马
112、以下哪项属于防火墙的基本功能（）。-->D.访问控制功能
113、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
114、以下哪一种是防止系统不受恶意代码威胁的最简单、最完美的方法（）。-->D.没有这样通用的、完美的保护系统的方法
115、以下哪种不是常见的安全认证技术？-->D.基于已有知识的认证技术
116、以下哪种不是常见的安全认证技术方法（）-->D.基于已有知识的认证技术
117、以下哪种不是用于保护电子邮件安全的技术？-->C.验证码
118、以下哪种加密算法相对最安全？-->B.RSA
119、以下哪种密码体制不需要密钥？-->D.ROT13
120、以下哪种认证方式相对最安全？-->D.多因素认证
121、以下哪种认证方式相对最安全？-->D.人脸识别加短信验证码认证
122、以下哪种认证方式相对最安全？（）。-->D.多因素认证
123、以下哪种是常见的恶意代码类型？-->B.木马
124、以下哪种是常见的网站拒绝服务攻击技术()-->B.HTTPFlood
125、以下哪种是常见的网站拒绝服务攻击技术？-->B.CC 攻击
126、以下哪种算法不属于古典密码体制？-->B.RSA 算法
127、以下哪种通用方法可以完美杜绝恶意软件对系统的影响？-->D.没有通用且完美的方法
128、以下算法中属于非对称算法的是（）。-->B.RSA
129、在 Endsley 模型中，态势预测是基于（）的。-->B.态势理解
130、在电子邮件安全中，哪一项策略能够向接收服务器提示如何处理失败的 SPF 和 DKIM 检查？-->C.DMARC
131、在古典密码中，哪种方法是基于破译明文攻击的？-->B.频率分析
132、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
133、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（）。-->C.保密性
134、在以下古典密码体制中，不属于置换密码的是-->C.凯撒密码
135、在以下古典密码体制中，不属于置换密码的是（）。-->B.逆序密码
136、在以下古典密码体制中，不属于置换密码的是（）。-->B.倒序密码
137、在以下古典密码体制中，属于置换密码的是（）。-->D.周期置换密码
138、在云环境中，责任主体-->B.相对于传统环境更加复杂
139、针对恶意软件的防御，哪一项是不推荐的？-->B.不安装任何第三方软件以确保系统安全
140、中国国家信息安全漏洞库（ChinaNationalVulnerabilityDatabaseofInformationSecurity）的简称是什么？-->C.CNNVD

1、CTF（CaptureTheFlag）中文一般译作夺旗赛，在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。常见的 CTF 竞赛模式有（）。-->(A.解题模式（Jeopardy）B.攻防模式（Attack-Defense）。D.混合模式（Mix）。)
2、Metasploit 工具包括以下哪些功能：-->(A.漏洞探测 C.漏洞查询 D.漏洞利用)
3、按照访问控制方式不同，防火墙可以分为（）。-->(A.包过滤防火墙 C.应用代理防火墙 D.状态检测防火墙)
4、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 C.应用代理防火墙 D.状态检测防火墙)
5、按照形态的不同，防火墙可以分为：-->(A.软件防火墙 B.硬件防火墙 C.专用防火墙)
6、当前网络安全主要面临的问题有哪些？（）-->(A.APT 组织持续对我国的重要行业实施攻击 B.个人信息数据泄露风险问题突出 C.仿冒诈骗和钓鱼邮件层出不穷)
7、电子邮件面临的主要安全威胁包括哪些？-->(A.恶意链接 B.钓鱼邮件 D.勒索病毒)
8、电子邮件面临的主要安全威胁有哪些：-->(A.钓鱼邮件 B.勒索病毒 D.恶意链接)
9、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)
10、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)
11、恶意代码防范技术中，哪些是可行的有效手段？-->(A.定期更新安全补丁 B.安装防火墙 D.使用反病毒软件)
12、恶意软件主要采用以下哪些传播途径进行传播（）。-->(A.软件捆绑 B.利用漏洞 D.远程下载)
13、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 D.远程下载)

14、防范恶意代码需要重点注意的方面有哪些？-->(A.操作系统更新 B.安装安全补丁 D.用户安全培训)
15、防火墙根据形态主要有哪些类型？-->(A.软件防火墙 B.硬件防火墙 C.专用防火墙)
16、高级持续威胁（APT）的特征有（）。-->(A.它比传统攻击具有更高的定制程度和复杂程度，需要花费大量时间和资源来研究确定系统内部的漏洞 B.这类攻击持续监控目标，对目标保有长期的访问权 C.攻击目标通常是特定的重要目标，攻击方一旦得手，往往会给被攻击目标造成巨大的经济损失或政治影响，乃至于毁灭性打击)
17、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)
18、根据密码分析者破译时已具备的前提条件，通常将攻击类型分为哪几种？-->(A.唯密文攻击 C.已知明文攻击 D.选择明文攻击)
19、关于 MITRE 公司提出的 AdversarialTactics,Techniques,andCommonKnowledge（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.EnterpriseATT&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)
20、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 D.默认情况下防火墙拒绝所有传入连接)
21、关于计算机病毒，以下哪些说法是正确的？-->(A.有些病毒仅能攻击某一种操作系统，如 WindowsB.病毒一般附着在其他应用程序上 D.有些病毒能损坏计算机硬件)
22、关于区块链技术的适用场景，以下说法正确的是-->(B.多方参与，缺乏统一背书主体的场景 C.强调公开透明的场景 D.信任密集，而非计算存储密集的场景)
23、关于网络攻击，哪些因素通常是攻击者的驱动因素？-->(A.政治因素 B.经济利益 C.技术炫耀)
24、僵尸网络常被用于进行哪些类型的攻击？-->(A.发送垃圾邮件 B.分布式拒绝服务攻击 C.特定领域攻击)
25、僵尸网络是指由被恶意软件感染的计算机组成的网络，僵尸网络常被用于进行以下稠些类型的攻击（）-->(B.发送垃圾邮件 C.分布式拒绝服务攻击 D.特定领域攻击)
26、近代密码阶段，典型的加密算法包括哪些？-->(A.RSAC.AESD.DES)
27、零信任遵循的 ABCDE 原则包括（）-->(A.不做任何假定（Assumenoting）C.随时检查一切（Checkeverything）D.防范动态威胁（Defeatdynamicrisks）。)
28、零信任遵循的原则有（）。-->(A.不做任何假定 C.随时检查一切 D.防范动态威胁)
29、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)
30、漏洞蠕虫破坏力强、传播速度快，它的传播过程一般可以分为（）步骤。-->(A.扫描 B.攻击 C.复制)
31、洛克希德&马丁公司提出的网络杀伤链（KillChain）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）。)
32、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)
33、区块链攻击者常用的一些攻击方法包括：-->(B.路由攻击 C.女巫攻击 D.钓鱼攻击)
34、区块链技术与传统数据库相比，有哪些不同？-->(A.去中心化 C.账本分布存储于多台计算机 D.数据不可篡改)
35、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)
36、区块链是一种类似于数据库的分布式账本，但不由中央机构控制，账本分布存储于多台计算机，区块链技术主要有哪些特点（）-->(A.去中心化 B.不可篡改 D.共识)
37、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)
38、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)
39、使用 VPN 技术，可以建立安全通道，并能用 VPN 提供的安全服务，这些安全服务包括：-->(A.保密性服务 C.完整性服务 D.认证服务)
40、网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的（）的能力：-->(B.完整性 C.保密性 D.可用性)
41、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 D.权限提升、横向移动、后门和持久化)
42、网络攻击的主要目的和形式包括哪些？-->(A.获得数据 B.利用资源 C.破坏业务)
43、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)
44、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)
45、下列哪些步骤属于恶意代码的作用过程：-->(A.入侵系统 B.提升权限 C.实施隐藏)
46、下列哪些步骤属于恶意代码的作用过程：-->(A.入侵系统 B.提升权限 C.实施隐藏 D.潜伏等待 E.执行破坏)
47、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)
48、下列选项中，属于网络安全体系四个级别的是哪些？-->(A.网络级安全 B.系统级安全 C.应用级安全)
49、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)
50、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 D.鉴别实体)
51、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 D.鉴别实体)
52、以下关于高级持续威胁（APT）的说法不正确的有：-->(A.APT 攻击由于出现频次低，因此威胁性较小 B.APT 攻击往往一次得手后，便不再对目标进行后续攻击 D.APT 攻击可以被专业的杀毒软件发现并查杀阻断)
53、以下关于认证机制说法正确的是：-->(A.根据认证依据所利用的时间长度分类，可分为一次性口令和持续认证 B.根据要求提供的认证凭据的类型分类，可分为单因素认证、双因素认证和多因素认证 D.认证一般由标识和鉴别两部分组成)
54、以下哪些是政务网站安全防护的内容（）-->(A.网页防篡改 B.网站安全监控 D.人侵防御)
55、以下哪些是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)
56、以下哪些是政务网站安全防护的内容：-->(B.网页防篡改 C.网络/数据库审计 D.入侵防御和病毒防护)
57、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)
58、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)
59、以下哪些属于政务网站安全防护的内容？-->(A.网页防篡改 B.网站安全监控 D.入侵防御)
60、以下属于零信任遵循的原则有：-->(A.不做任何假定 C.随时检查一切 D.防范动态威胁)
61、以下属于双因素认证的有哪些？-->(A.密码加验证码认证 B.密码加人脸识别认证 D.电话语音加人脸识别认证)
62、以下属于挖矿木马的特征是：-->(A.CPU 或 GPU 的占用率持续 90%以上 B.系统频繁崩溃或重新启动 C.存在外连 IP 或可疑域名等异常网络活动)
63、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)
64、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)
65、在防范恶意代码方面，哪些技术是有效的？-->(A.防火墙 B.入侵检测系统 D.蜜罐技术)
66、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 C.完整性 D.保密性)
67、在网络安全中，哪些因素可能导致数据泄露风险增高？-->(A.弱密码 B.未更新的软件 C.内部人员泄密)
68、在网络杀伤链（KillChain）模型中，哪几个步骤直接涉及到植入恶意代码或软件？-->(A.武器构造 B.漏洞利用 C.安装植入)
69、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)
70、专用防火墙的优势在于什么？-->(A.容易配置和管理 B.本身漏洞较少 C.处理能力强，性能高)

判断(112)--电大资源网：http://www.dda123.cn/（微信搜：905080280）

1、MITRE 公司提出的网络攻击矩阵模型，它是一个站在防守者的视角来描述攻击中各阶段用到的技术的模型。-->错
2、MITRE 公司提出的网络攻击矩阵模型，它是一个站在攻击者的视角来描述攻击中各阶段用到的技术的模型。-->对
3、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。-->错
4、MITRE 公司提出的网络攻击矩阵模型是一个站在攻击者视角描述各攻击阶段技术的模型。-->对

5、SPF 是电子邮件验证中最基本和最常见的保护技术之一。-->对
6、Web 应用防火墙是一种用于保护 Web 服务器和 Web 应用的网络安全机制，对 Web 服务器和 Web 应用提供安全防护功能。-->对
7、Web 应用防火墙是一种用于保护 Web 服务器和 Web 应用的网络安全机制。其技术原理是根据预先定义的过滤规则和安全防护规则，对所有访问 Web 服务器的 HTTP 请求和服务器响应，进行 HTTP 协议和内容过滤，进而对 Web 服务器和 Web 应用提供安全防护功能。-->对
8、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。-->对
9、《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。-->错
10、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。-->对
11、按照网络蠕虫的传播途径和攻击性，可以分为传统蠕虫、邮件蠕虫和漏洞蠕虫。其中漏洞蠕虫破坏力强、传播速度快。-->对
12、按照网络蠕虫的传播途径和攻击性，可以分为传统蠕虫、邮件蠕虫和漏洞蠕虫。其中邮件蠕虫主要通过邮件传播。-->对
13、病毒可独立存在，而蠕虫必须寄生在宿主程序中。-->错
14、从广义来说，凡是涉及网络信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论，都是网络安全的研究领域。-->对
15、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。-->对
16、单点登录是指用户访问不同系统时，只需要进行一次身份认证，就可以根据这次认证身份访问授权资源-->对
17、单点登录是指用户访问不同系统时，只需要进行一次身份认证，就可以根据这次认证身份访问授权资源，它简化了认证过程，方便用户使用。-->对
18、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。-->对
19、单点登录要求用户在访问不同授权资源时，每次都需进行新的身份认证。-->错
20、当前，由于 DES 密钥长度仅为 56 位，DES 不被视为绝对安全的加密方法。-->对
21、迪菲（Diffie）和赫尔曼（Hellman）提出的公钥密码系统解决了密钥安全管理与分发、数字签名等问题，对保密通信、密钥分配和鉴别等领域产生了深远的影响。-->对
22、迪菲（Diffie）和赫尔曼（Hellman）提出的公钥密码系统是密码学历史上的一次革命。-->对
23、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。-->对
24、抵抗入侵者的第一道防线通常是口令系统。-->对
25、钓鱼邮件通过冒充正常邮件来骗取用户信任，进而非法获取密码和盗取敏感数据。-->对
26、钓鱼邮件指恶意邮件冒充正常邮件骗取用户信任，从而非法获得密码、盗取敏感数据、诈骗资金等。-->对
27、对称密码体制的主要优点是加解密速度快。-->对
28、对称密码体制和非对称密码体制的最大区别就是发送方和接收方彼此拥有不同的公私钥。-->对
29、多因素认证技术使用多种鉴别信息进行组合，以提升认证的安全强度。根据认证机制所依赖的鉴别信息的多少，该认证通常被称为双因素认证或多因素认证。-->对
30、多因素认证通过组合多种鉴别信息提升了认证安全性。-->对
31、恶意代码的传播源于用户软件的漏洞、操作失误或两者结合。-->对
32、防火墙本质上就是一种能够限制网络访问的设备或软件，既可以是一个硬件的“盒子”，也可以是计算机和网络设备中的一个“软件”模块。-->对
33、防火墙和网络隔离技术是完全相同的。-->错
34、防火墙是一种硬件设备，不能通过软件来实现。-->错
35、访问控制技术指系统对用户身份及其所属的预先定义的策略，限制其使用数据资源能力的手段，通常用于系统管理员控制用户对服务器、目录、文件等网络资源的访问。-->对
36、非授权访问是由网络配置错误导致的。-->错
37、非授权访问是由于网站服务的技术缺陷导致的安全漏洞。-->错
38、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。-->对
39、横向移动是指攻击者从入口点传播到网络其他部分的过程。-->对
40、基于生物特征的认证使用如指纹、人脸、视网膜等信息进行身份验证。-->对
41、计算机病毒、网络蠕虫和木马是威胁计算机系统和网络安全的主要元素，均属于恶意代码。-->对
42、仅仅通过法律法规就可以实现网络安全目标，不需要考虑安全策略、组织管理、技术措施等因素。-->错
43、口令是最常用的资源访问控制机制，其安全性很好，不易出现问题。-->错
44、口令是最常用的资源访问控制机制，它的安全性很好，不容易出现问题。-->错
45、口令是最常用的资源访问控制机制，也是最容易被突破的。-->对
46、口令通常是最容易被突破的资源访问控制机制。-->对
47、密码分析学主要是在未知密钥的情况下，推演出密文或密钥。-->对
48、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。-->对
49、明文保存的用户口令容易被直接利用。很多系统对口令进行加密运算后再保存，加密运算通常采用单向哈希算法（Hash）。-->对
50、目标系统存在的漏洞是产生网络安全威胁的唯一原因。-->错
51、目前，在数字签名中常用的非对称算法包括 RSA．DSA 和 AES 算法等-->错
52、目前没有任何技术可以帮助我们应对电子邮件面临的安全威胁。-->错
53、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。-->对
54、签名仅用于描述网络中正常数据流的特征。-->错
55、窃取用户会话 cookie 后伪装成该用户，即为会话劫持。-->对
56、认证方式可以分为单项认证、双向认证和第三方认证。-->对
57、认证机制是实施访问控制的基础性手段。-->对
58、认证机制是网络安全的基础保护措施，用于实施访问控制。-->对
59、认证是一个实体向另外一个实体证明其所声称的能力的过程。-->错
60、认证是一个实体向另一个实体证明其所声称的凭证的过程。-->错
61、认证是指一个实体向另一个实体证明其声称的身份。-->对
62、认证通常由标识（Identification）和鉴别（Authentication）两部分组成。-->对
63、蠕虫能自动寻找漏洞系统，并发起远程连接和攻击以完成自我复制。-->对
64、入侵防御技术在攻击到达的同时或之后会发出告警。-->对
65、入侵防御系统可通过网络流量分析来检测包括缓冲区溢出攻击、木马和蠕虫等入侵行为。-->对
66、入侵防御系统通过对解析后的报文特征与签名库进行匹配来发现入侵。-->对
67、三重 DES 能够抵御中途相遇攻击。-->对
68、使用 PGP 加密的电子邮件仅需用密码进行电子邮件服务的身份验证。-->错
69、使用多重 DES 能提高 DES 的安全性，并充分利用现有的软硬件系统资源。-->对
70、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。-->对
71、受感染机器间是否能够协同工作是区分僵尸网络和其他恶意软件的重要特征。-->对
72、双重 DES 的密钥长度为 112 位，能够抵御中途相遇攻击。-->错
73、特洛伊木马通过伪装成实用程序赢得用户信任，并趁机控制目标主机。-->对
74、通过电话方式骗取用户账号密码属于社会工程学方法。-->对
75、通过主机入侵检测系统，对操作系统内的可疑行为，如程序、可执行代码和异常操作，能进行实时监视和审计。-->对
76、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。-->对
77、网络安全体系仅由技术措施组成，不涉及法律法规和组织管理。-->错
78、网络安全体系是网络安全保障系统的最高层概念抽象，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。-->对
79、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。-->对
80、网络安全最基本的 3 个属性是保密性、完整性、真实性。-->错
81、网络防御技术所包含的访问控制技术内容包括管理、认证、控制策略实现等几部分。-->错

82、网络防御技术所包含的访问控制技术内容认证包括负载均衡、认证、控制策略实现等几部分。-->错
83、网络隔离技术的主要目标是将有害的网络安全威胁隔离开，以保障数据信息无论在可信网络之内还是之外都可以安全交互。-->错
84、网络隔离技术的主要目的是隔离网络安全威胁，以保证可信网络内的数据信息安全。-->对
85、网络隔离技术总体上分为物理隔离和逻辑隔离两类。-->对
86、网络隔离技术总体上可以分为物理隔离及逻辑隔离两类方法。-->对
87、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。-->对
88、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。-->对
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。-->错
90、网络社会的形成与发展为现实社会中的违法犯罪分子提供了一个新的违法犯罪领域，但其社会危害性不及现实社会中的违法犯罪。-->错
91、网站假冒仅通过网站域名欺骗进行。-->错
92、网站假冒涉及攻击者通过域名劫持和中间人技术，以骗取用户敏感信息或提供恶意服务。-->对
93、网站假冒是指攻击者通过网站域名欺骗、网站域名劫持、中间人等技术手段，诱骗网站用户访问以获取敏感信息或提供恶意服务。-->对
94、为防护病毒，需要理解其传播和攻击原理，并根据特性进行检测和消除。-->对
95、文件类病毒一般会藏匿和感染硬盘的引导扇区。-->错
96、我国网络安全领域的基础性法律《中华人民共和国网络安全法》正式施行，对保护个人信息、治理网络诈骗、保护关键信息基础设施、网络实名制等方面作出明确规定，成为我国网络空间法治化建设的重要里程碑。-->对
97、物联网与互联网有本质区别，因此黑客很难攻击物理设备如网络摄像头。-->错
98、移动应用安全和传统的 Web 安全面临的问题是一样的，不需要专门为移动应用单独考虑安全问题。-->错
99、移动应用安全和传统的 Web 安全面临的问题是一样的，可以完全借鉴，不需要专门为移动应用单独考虑安全问题。-->错
100、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。-->错
101、移动应用安全中的网络攻击都在设备层。-->错
102、应根据事件级别，启动相应级别的应急响应流程。-->对
103、云安全是一套包括政策、技术和布署控制方法的广泛体系，用以保护资料和应用程序。-->对
104、云环境中的责任主体相对简单。-->错
105、在 DES 加密过程中，S 盒对加密的强度不产生影响。-->错
106、在 DES 加密过程中，S 盒对加密的强度不会产生影响。-->错
107、在 DES 加密过程中，S 盒对加密的强度没有影响。-->错
108、在密码学的研究中，应专注于密码算法而非密码破译。-->错
109、在设计密码系统时，应遵循 Kerckhoffs 假设以确保安全性。-->对
110、掌握漏洞资源等于掌握了网络安全的绝对主动权。-->错
111、支持 VLAN 的交换机可以通过使用 VLAN 标签将预定义的端口隔离在各自的广播区域。-->对
112、只要设置了口令，资源就能得到很好的访问控制。-->错