目录

第一章

1

2 分

我国的（ ）主要规定了关于数据电文、电子签名与认证及相关的法律责任

A.《中华人民共和国宪法》；B.《中华人民共和国网络空间安全法》；C.《中华人民共和国电子签名法》；D.《商用密码管理条例》

正确答案是：C 你的答案是：C 此题得分：2

展开解析

2

2 分

传输层用于控制数据流量，以确保通信顺利，该层次的常用协议包括（ ）

A.IP；B.TCP；C.FTP；D.PPP

正确答案是：B 你的答案是：C 此题得分：0

展开解析

3

2 分

人员管理是信息安全管理体系的重要组成部分，下列关于人员管理的描述中错误的是（ ）

A.人员管理应该全面提升管理人员的业务素质、职业道德、思想素质等。；B.网络安全管理人员在通过法律意识的审查后，还需要进行适合的安全教育培训；C.安全教育培训

对象包含网络管理人员、研发人员等，不包括用户、管理者；D.安全意识教育和安全技术教育都属于安全教育培训内容

正确答案是：C　你的答案是：C　此题得分：2

展开解析

4

2 分

（　）作为接受服务的另一方，为客户提供本地服务

A.客户端；B.服务器端；C.中间人；D.以上都不正确

正确答案是：A　你的答案是：C　此题得分：0

展开解析

5

2 分

2017 年 WannaCry 在全球范围大爆发，感染了大量的计算机，WannaCry 属于（　）病毒

A.木马；B.后门；C.蠕虫；D.脚本

正确答案是：C　你的答案是：C　此题得分：2

展开解析

6

2 分

网络中能对其他机器提供某些服务的计算机系统被称为（　）

A.服务器端；B.客户端；C.中间人；D.以上都不正确

正确答案是：A　你的答案是：A　此题得分：2

展开解析

7

2 分

WWW 服务是目前应用最广的一种基本互联网应用，默认的网络端口号是（　）

A.22；B.21；C.8080；D.80

正确答案是：D　你的答案是：C　　此题得分：0

展开解析

8

2 分

服务对外开放时需要用到端口，其中 21 端口号对应以下哪个服务？

A.FTP；B.POP3；C.Telnet；D.以上都不正确

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

9

2 分

计算机病毒指攻击者在计算机程序中插入破坏计算机功能的代码，从而影响计算机使用，其中寄生在磁盘引导区或主引导区的计算机病毒被称为（　）

A.文件型病毒；B.引导型病毒；C.宏病毒；D.以上都不正确

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

10

2 分

计算机病毒给计算机的功能及数据带来巨大威胁，其中通过操作系统的文件系统进行感染的病毒被称作（　）

A.文件型病毒；B.引导型病毒；C.目录型病毒；D.以上都不正确

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

11

2 分

为增强无线网络安全性，常用的无线网络安全技术有（　）

A.访问控制技术；B.数据加密技术；C.端口访问技术；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

12

2 分

《中华人民共和国网络安全法》（　）正式实施

A.1949 年；B.1999 年；C.2008 年；D.2017 年

正确答案是：D　你的答案是：B　　此题得分：0

展开解析

13

2 分

信息时代的海量数据，促进了大数据的形成和发展，其中大数据应用的核心资源是（　）

A.隐私；B.数据；C.人；D.互联网

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

14

2 分

物联网是新一代信息技术的主要组成部分，下列选项中对其描述错误的是（　）

A.智能摄像头属于物联网终端；B.物联网可应用于智能医疗；C.物联网就是互联网；D.物联网英文简写为 IoT

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

15

2 分

数据备份作为容灾的基础，用于防止操作失误或系统故障等因素而造成数据丢失，下列选项中不属于数据备份方式的是（　）

A.完全备份；B.差异备份；C.增量备份；D.抄录备份

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

16

2 分

网络环境日益复杂，网络安全问题已然成为人们关注的重点，下列属于信息系统安全威胁的是（　）

A.系统的开放性；B.系统的复杂性；C.系统本身固有的漏洞；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

17

2 分

计算机由硬件和软件组成，下列选项中不属于软件的是（　）

A.计算机系统程序；B.计算机应用程序；C.与计算机程序有关的文档；D.CPU

正确答案是：D　你的答案是：D　此题得分：2

展开解析

18

2 分

存储数据的载体被称为存储介质，以下不属于存储介质的是（　）

A.光盘；B.显示器；C.硬盘；D.磁盘阵列

正确答案是：B　你的答案是：B　此题得分：2

展开解析

19

2 分

身份认证技术具有多种认证方式，在保护网络数据中起着至关重要的作用，以下不属于基于生物特征的身份认证方式的是（　）

A.指纹；B.人脸；C.虹膜；D.智能卡

正确答案是：D　你的答案是：D　此题得分：2

展开解析

20

2 分

随着网络安全问题的日益凸显，安全设备也呈现多样化趋势，以下不属于网络安全设备的是（　）

A.防火墙；B.入侵检测系统；C.路由器；D.漏洞扫描系统

正确答案是：C　你的答案是：C　此题得分：2

展开解析

21

2 分

从信息系统安全角度处理信息安全问题，设备安全已然成为人们关注的重点，以下属于设备安全的要求的是（　）

A.稳定性；B.可靠性；C.可用性；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

22

2 分

密码学用于研究如何隐秘地传递信息，其研究内容包括（　）

A.对称密码；B.公钥密码；C.生物密码//流密码；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

23

2 分

数据加密是保障数据安全的重要手段，以下不属于密码体制的是（　）

A.明文空间；B.密文空间；C.密钥空间；D.通信协议

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

24

2 分

网络环境中的口令安全一直是人们关注的重点，一个好的口令应具备（　）

A.使用多种字符；B.尽量随机；C.定期更换；D.以上都是

正确答案是：D　你的答案是：D　此题得分：2

展开解析

25

2 分

VPN 用于在公用网络上建立专用网络，从而进行加密通讯。通常 VPN 无需在以下哪项使用数字证书和（）PKI？

A.身份验证；B.密钥管理；C.访问控制；D.部署安装

正确答案是：D　你的答案是：A　此题得分：0

展开解析

26

2 分

时代的快速发展，使得计算机成为信息社会必不可少的工具，下列关于计算机和操作系统的说法不正确的是（　）

A.操作系统是一种软件；B.计算机是一个资源的集合体，包括软件资源和硬件资源；C.计算机硬件是操作系统工作的实体，操作系统的运行离不开硬件的支持；D.操作系统是独立于计算机系统的，它不属于计算机系统

正确答案是：D　你的答案是：D　此题得分：2

展开解析

27

2 分

安全模型是安全策略的清晰表述，具有以下哪些特点？（　）

A.精确的、无歧义的；B.简单的、抽象的，易于理解；C.只涉及安全性质，不限制系统的功能及其实现；D.以上都是

正确答案是：D　你的答案是：D　此题得分：2

展开解析

28

2 分

在设计操作系统的安全机制的过程中，需要遵循的原则包括（　）

A.安全不应影响遵守规则的用户；B.便于用户的授权存取；C.便于用户的控制存取；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

29

2 分

中国电子商务认证机构管理中心的主要职能包括（　）

A.国内 PKI 认证体系的统筹规划；B.规范国内认证机构的服务；C.对国内各认证机构的管理人员进行培训；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

30

2 分

防火墙由软件和硬件设备组成，用于信息安全防护。防火墙的优点包括（　）

A.集中的安全管理，强化网络安全策略，经济易行；B.便于用户进行日志的记录和审计；C.监测网络的安全性并及时告警；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

31

2 分

网络环境日益复杂，人们对安全防护技术的要求也在不断提高，以下关于防火墙技术的发展要求说法错误的是（　）

A.信息过滤的深度越来越浅；B.安全协议的优化是必要的；C.与操作系统相耦合越来越紧密；D.由被动防护转变为智能、动态地保护内部网络

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

32

2 分

包过滤防火墙通过查看流经数据包的包头，决定接受或丢弃数据包，以下属于包过滤的优点的是（　）

A.处理包的数据比代理服务器快；B.实现包过滤几乎不需要额外费用；C.对用户是透明的，因此不需要用户进行特殊的培训；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

33

2 分

防火墙在网络安全防护中发挥着重要的作用，在选购防火墙时参考标准包括（　）

A.总成本；B.稳定性；C.可升级性；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

34

2 分

正确的选择防火墙能够更加有效的防护网络安全，在选择防火墙类型时基本原则包括（　）

A.大企业根据部署位置选择防火墙；B.中小企业根据网络规模选择防火墙；C.考查厂商的服务；D.以上都是

正确答案是：D　你的答案是：D　此题得分：2

展开解析

35

2 分

网络代理技术即通过代理服务器代理网络用户取得网络信息，在代理服务器上可对信息进行合法性验证，从而保护用户的安全。以下关于网络代理技术的说法错误的是（　）

A.代理技术又称为应用层网关技术；B.代理技术具备一定的安全防御机制；C.代理技术能完全代替防火墙功能；D.代理服务器能够管理网络信息

正确答案是：C　你的答案是：C　此题得分：2

展开解析

36

2 分

在 Linux 系统中，用于配置和显示 Linux 内核中网络接口的命令是（　）

A.ping；B.tracert；C.ifconfig；D.以上都不正确

正确答案是：C　你的答案是：C　此题得分：2

展开解析

37

2 分

以下命令中，可以检查网络是否连通的命令是（　）

A.ipconfig；B.ifconfig；C.ping；D.以上都不正确

正确答案是：C　你的答案是：C　此题得分：2

展开解析

38

2 分

Nmap 是一款全球有名的扫描工具，以下属于其主要作用的是哪个？

A.扫描网上电脑开放的网络连接端；B.提高网络中的数据传输速度；C.查询目标主机的日志信息；D.以上都不正确

正确答案是：A　你的答案是：A　此题得分：2

展开解析

39

2 分

入侵检测系统是一种对网络传输数据进行监控并采取应对措施的一种安全设备。以下关于入侵检测系统的描述错误的是（　）

A.系统和网络日志文件属于入侵系统中需要收集的信息；B.一切目录和文件的内容属于入侵系统中需要收集的信息；C.程序执行中不期望的行为属于入侵系统中需要收集的信息；D.入侵信息属于入侵系统中需要收集的信息

正确答案是：B　你的答案是：D　此题得分：0

展开解析

40

2 分

以下哪一项不属于对软件开发团队进行安全培训的内容？

A.对环境、网络、代码、文档等方面的安全意识培训；B.对安全配置管理的培训；C.对安全编程、安全测试、知识产权的培训；D.对软件项目管理的培训

正确答案是：D　你的答案是：B　此题得分：0

展开解析

41

2 分

数据不被泄露给非授权用户、实体或过程的特性指的是下列哪项？

A.保密性；B.不可否认；C.可用性；D.完整性

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

42

2 分

在网络传输过程中数据丢失，这破坏了数据的下列哪个特性？

A.可用性；B.完整性；C.保密性；D.以上都是

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

43

2 分

用户 A 和用户 B 的通信过程被 C 窃听，这破坏了数据的以下哪个特性？

A.可用性；B.完整性；C.保密性；D.以上都是

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

44

2 分

DNS 即网域名称系统，它将域名和 IP 地址建立映射。DNS 服务对应的网络端口号是（　）

A.23；B.80；C.21；D.53

正确答案是：D　你的答案是：B　　此题得分：0

展开解析

45

2 分

密码体制中，伪装前和伪装后的数据分别称为（　）

A.密文、明文；B.明文、密文；C.秘钥、公钥；D.公钥、秘钥

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

46

2 分

网络监听本是网络安全管理人员用于监视网络状态、数据流动等的技术，但当攻击者将其作为一种攻击手段时，也会引发安全问题。以下对防御网络监听的描述正确的是（　）

A.使用无线网可有效防御网络监听；B.使用信息加密技术可有效防御网络监听；C.使用专线传输可防御所有网络监听；D.以上都不正确

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

47

2 分

缓冲区溢出攻击指利用缓冲区溢出漏洞所进行的攻击行为。以下对缓冲区溢出攻击描述正确的是（　）

A.缓冲区溢出攻击不会造成严重后果；B.缓冲区溢出攻击指向有限的空间输入超长的字符串；C.缓冲区溢出攻击不会造成系统宕机；D.以上都不正确

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

48

2 分

计算机病毒严重威胁着网络安全，以下能对计算机病毒防治措施描述正确的是（　）

A.及时升级可靠的反病毒产品；B.新购置的计算机软件无需病毒检测；C.重要的资料，无需定期备份；D.以上都不正确

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

49

2 分

物理层位于 OSI 模型的最底层，其数据单位是（　）

A.Bit；B.Byte；C.GB；D.TB

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

50

2 分

数据链路层具有流量控制功能，其数据单位是（　）

A.Bit；B.Packet；C.Frame；D.Segment

正确答案是：C　你的答案是：A　　此题得分：0

目录

第二章

1

2 分

OSI 模型中位于最顶层并向应用程序提供服务的是（　）

A.网络层；B.应用层；C.传输层；D.表示层

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

2

2 分

GPS 是英文 Global Positioning System 的简称，以下对于 GPS 的叙述错误的是？（　）

A.它是全球定位系统；B.GPS 定位可以结合地图的可视化，清晰、准确地定位出事件发生的地点以及与该事件相关事件发生的位置；C.GPS 有助于挖掘事件之间的关联关系；D.GPS 无安全性问题

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

3

2 分

在系统发生告警信息时，通过网络 IP 电话拨号拨打给工作管理人员手机号码的告警方式是（　）

A.短信告警；B.邮件告警；C.电话告警；D.多媒体语音告警

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

4

2 分

日志可以描述电脑的使用记录，以下不属于日志特点的是？（　）

A.日志种类多；B.大型企业的系统日志数据量很小；C.网络设备日志具有时空关联性；D.网络入侵者可能对日志信息进行篡改

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

5

2 分

信息系统审计是通过收集评价审计证据，科学判断信息系统安全性的过程，以下不属于信息系统审计主要作用的是？（　）

A.有效提高信息系统的可靠性；B.提高信息系统的安全性；C.提高信息系统运行的效率；D.降低数据资源的利用率

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

6

2 分

计算机硬件是计算机系统中各种物理装置的总称，以下不属于计算机硬件的是？（　）

A.中央处理器；B.存储器；C.外部设备；D.运行的程序

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

7

2 分

以下不属于常见的故障预测技术方法的是（　）

A.基于统计的方法；B.基于数学的方法；C.基于随机选择的方法；D.基于人工智能的方法

正确答案是：C　你的答案是：D　　此题得分：0

展开解析

8

2 分

目前通用的网络模型有两种，OSI 模型分为 7 层，TCP/IP 模型分为（　）层

A.3；B.4；C.6；D.7

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

9

2 分

数据传输可分为有线传输和无线传输，有线传输的介质不包括（　）

A.同轴电缆；B.光纤；C.双绞线；D.无线电波

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

10

2 分

PPP 协议提供了中在点到点链路上封装网络层协议信息的标准方法，其英文是（　）

A.The Point-to-Point Protocol；B.Point-to-Point Protocol over Ethernet；C.Ethernet Protocol；D.Point- Point-Point Protocol

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

11

2 分

MAC 地址由 24 位厂商编号和 24 位序列号构成，MAC 地址又称为（　）

A.软件地址；B.网络地址；C.通信地址；D.物理地址

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

12

2 分

操作系统用于管理和控制计算机硬件与软件资源。下列选项中，属于操作系统管理功能的是（　）

A.进程管理；B.更新管理；C.删除管理；D.查询管理

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

13

2 分

操作系统的管理功能包括作业管理、文件管理、存储管理、设备管理和进程管理。管理文件的读写执行权限属于操作系统的（　）

A.存储管理；B.设备管理；C.文件管理；D.进程管理

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

14

2 分

用户身份鉴别指用户在访问计算机资源时，提供有效的身份信息以认证身份的真实性。以下选项中，属于用户身份鉴别方式的是（　）

A.更新功能；B.浏览功能；C.口令验证；D.查询功能

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

15

2 分

用户鉴别指对用户身份的确认，输入用户名和密码属于基于（　）的鉴别

A.用户行为；B.USB key；C.口令；D.生物特征

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

16

2 分

网上证券交易是按照用户类型来划分权限的，保证只有经过授权的用户才能使用被授权的资源，它所对应的安全需求是（　）

A.通信安全；B.身份认证与访问控制；C.业务安全；D.信息完整性

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

17

2 分

计算机病毒会导致计算机功能或数据损坏，下列属于网络病毒主要传播途径的是（　）

A.通信系统；B.移动存储设备；C.无线通道；D.以上都是

正确答案是：D　你的答案是：D　此题得分：2

展开解析

18

2 分

恶意代码会破坏计算机数据的安全性，并且为进行自我保护使用了（　）技术

A.自我复制；B.查询功能；C.加密；D.中断功能

正确答案是：C　你的答案是：A　此题得分：0

展开解析

19

2 分

计算机病毒会破坏计算机数据或功能，并能寄生于其他程序，其中被寄生的程序称为（　）

A.更新程序；B.不可执行程序；C.宿主程序；D.修改程序

正确答案是：C　你的答案是：C　此题得分：2

展开解析

20

2 分

通过 Internet 进行的商务活动称为电子商务，而高效的电子现金系统在其中得到广泛关注。以下对电子现金的描述错误的是（　）

A.一种用电子形式模拟现金的技术；B.具有可传递性；C.具有不可伪造性；D.不可以进行任意金额的支付

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

21

2 分

操作系统的管理功能包括作业管理、文件管理、存储管理、设备管理和进程管理。监视系统中设备的运行状态属于操作系统的（　）

A.文件管理；B.设备管理；C.存储管理；D.作业管理

正确答案是：B　你的答案是：D　　此题得分：0

展开解析

22

2 分

密码学中运用（　）算法，加密和解密使用不同秘钥

A.随机加密；B.公钥；C.Hash；D.对称

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

23

2 分

防火墙是一个位于内外网之间的网络安全系统，以下对防火墙作用的描述不正确的是（　）

A.抵抗外部攻击；B.保护内部网络；C.防止恶意访问；D.阻止所有访问

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

24

2 分

随着网络环境的日益复杂，防火墙也在不断发展，以下对防火墙发展趋势的描述不正确的是（　）

A.模式转变；B.功能扩展；C.性能提高；D.安全需求降低

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

25

2 分

防火墙由软件以及硬件组成，在内外网间构建安全屏障，以下对防火墙的功能的说法不正确的是（　）

A.过滤进出网络的数据；B.管理进出网络的访问行为；C.拦截所有用户访问；D.对网络攻击检测和告警

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

26

2 分

CIA 指信息安全的三大要素，其中 C、I、A 依次代表（　）

A.保密性、完整性、可用性；B.可控性、完整性、可用性；C.保密性、即时性、可用性；D.以上都不正确

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

27

2 分

保证信息不被篡改，使信息能正确生成、存储以及传输，体现了信息安全的哪个性质？

A.完整性；B.即时性；C.可控性；D.保密性

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

28

2 分

网络环境日益复杂，网络攻击也从人工启动工具发起攻击，发展到由攻击工具本身主动发起攻击，体现了网络攻击的哪种发展趋势？

A.网络攻击自动化；B.网络攻击人群的大众化；C.网络攻击单一化；D.网络攻击普遍化

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

29

2 分

智能性的网络攻击工具的出现，使得攻击者能够在较短时间内向安全性低的计算机网络系统发起攻击，体现了网络攻击的哪一种发展趋势？

A.网络攻击自动化；B.网络攻击智能化；C.网络攻击单一化；D.网络攻击复杂化

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

30

2 分

信息不泄漏给非授权的个人、实体或过程，体现了信息安全哪一个性质？

A.保密性；B.可用性；C.完整性；D.即时性

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

31

2 分

某网站受到 DDoS 攻击无法正常为用户提供服务，这破坏了数据的（　）

A.完整性；B.可控性；C.不可否认性；D.可用性

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

32

2 分

随着网络攻击的智能化，许多攻击工具能根据环境自适应地选择策略，这体现了攻击工具的（　）

A.智能动态行为；B.破坏性；C.单一性；D.以上都不正确

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

33

2 分

攻击工具发展至今，已经可以通过升级或更换工具的一部分迅速变化自身，进而发动迅速变化的攻击，且在每一次攻击中会出现多种形态，这说明了攻击工具的（　）

A.变异性；B.单一性；C.顺序性；D.循环性

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

34

2 分

若发现应用软件的安全漏洞，为修复漏洞，以下做法正确的是（　）

A.使用厂商发布的漏洞补丁；B.忽略安全漏洞；C.重启应用软件；D.安装所有发布的补丁

正确答案是：A　你的答案是：A　此题得分：2

展开解析

35

2 分

对流通在网络系统中的信息传播及具体内容实现有效控制体现了信息系统的（　）

A.可控性；B.不可否认性；C.可用性；D.保密性

正确答案是：A　你的答案是：A　此题得分：2

展开解析

36

2 分

拒绝服务攻击指攻击者使用大量的连接请求攻击计算机，使得所有系统的（　）被消耗殆尽，最终导致计算机无法处理合法用户的请求

A.可用资源；B.硬件资源；C.软件资源；D.以上都不正确

正确答案是：A　你的答案是：C　此题得分：0

展开解析

37

2 分

网络攻击的不断发展，使得网络安全形势日益严峻，以下对网络攻击发展趋势的描述不正确的是（　）

A.漏洞发现和利用速度越来越快；B.网络攻击损失越来越严重；C.针对个人的网络攻击更加普遍；D.网络攻击工具逐渐自动化

正确答案是：C　你的答案是：B　　此题得分：0

展开解析

38

2 分

在 Windows 系统中，用于查询本机 IP 信息的命令是（　）

A.ping；B.ipconfig；C.tracert；D.以上都不正确

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

39

2 分

某用户将登陆密码设置为“123456”，该密码属于（　）

A.弱口令密码；B.强口令密码；C.不可猜测密码；D.以上都不正确

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

40

2 分

弱口令一直是威胁网络安全的一个重大问题，以下对弱口令的描述正确的是（　）

A.容易被破解从而威胁用户计算机安全；B.仅仅包含简单数字和字母的口令；C.不推荐用户使用弱口令；D.以上都正确

正确答案是：D　你的答案是：D　此题得分：2

展开解析

41

2 分

弱口令威胁一直是网络安全领域关注的重点，其中弱口令字典指（　）

A.容易被猜测或被工具破解的口令集合；B.容易被猜测但不容易被工具破解的口令集合；C.不容易被猜测但容易被工具破解的口令集合；D.以上都不正确

正确答案是：A　你的答案是：A　此题得分：2

展开解析

42

2 分

SSH 是专为远程登录会话和其他网络服务提供安全性的协议，以下关于其全称正确的是（　）

A.Secure Shell；B.Search Shell；C.Send Shell；D.以上都不正确

正确答案是：A　你的答案是：A　此题得分：2

展开解析

43

2 分

SSL 是为网络通信提供安全及数据完整性的一种安全协议，以下关于其全称正确的是（　）

A.Search Sockets Layer；B.Secure Sockets Layer；C.Send Sockets Layer；D.以上都不正确

正确答案是：B　你的答案是：B　此题得分：2

展开解析

44

2 分

IDS 依照一定的安全策略，对网络、系统的运行状况进行监视，其全称为（　）

A.Intrusion Detection Systems；B.Integrity Detection Systems；C.Integrity Design Systems；D.以上都不正确

正确答案是：A　你的答案是：B　　此题得分：0

展开解析

45

2 分

SNMP 是 TCP/IP 协议簇的一个应用层协议，以下是其全称的为（　）

A.Simple Network Management Protocol；B.Same Network Management Protocol；C.Search Network Management Protocol；D.以上都不正确

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

46

2 分

DNS 在万维网上作为域名和 IP 地址相互映射的一个分布式数据库，全称为（　）

A.Domain Name System；B.Document Name System；C.Domain Network System；D.以上都不正确

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

47

2 分

数据链路层可分为 LLC 和 MAC，LLC 的英文全称为（　）

A.Logic Link Control；B.Logic Layer Control；C.Limited Link Control；D.Limited Layer Control

正确答案是：A　你的答案是：C　此题得分：0

展开解析

48

2 分

PDU 是指对等层次之间传送的数据单元，PDU 的英文全称是（　）

A.Protocol Data Unit；B.Power Distribution Unit；C.Protocol Distribution Unit；D.Power Data Unit

正确答案是：A　你的答案是：A　此题得分：2

展开解析

49

2 分

通过 VPN 可在公网上建立加密专用网络，VPN 的英文全称是（　）

A.Visual Protocol Network；B.Virtual Private Network；C.Virtual Protocol Network；D.Visual Private Network

正确答案是：B　你的答案是：B　此题得分：2

展开解析

50

2 分

网络地址转换协议用于减缓可用 IP 地址空间的枯竭，下列哪一个选项是网络地址转换协议的英文全称？

A.Network Address Translation；B.Simple Mail Transfer Protocol；C.Simple Network Management Protocol；D.File Transfer Protocol

正确答案是：A　你的答案是：A　此题得分：2

第三章

1

2 分

DES 是一种使用密钥加密的块算法，其英文全称是（　）

A.Data Encryption Standard；B.Dynamic Encryption Standard；C.Dynamic Ellipse System；D.Digital Ellipse System

正确答案是：A　你的答案是：B　此题得分：0

展开解析

2

2 分

CIDF（Common Intrusion Detection Framework）致力于将入侵检测标准化，其全称为（　）

A.通用入侵检测框架；B.入侵检测数据标准草案；C.安全部件互动协议；D.入侵检测接口标准协议

正确答案是：A　你的答案是：A　此题得分：2

展开解析

3

2 分

SQL 是一种用于数据库访问的标准语言，具有查询、更新、管理数据库等功能，其英文全称为（　）

A.Structured Query Language；B.Standard Query Language；C.Security Query Language；D.Standard Query Layer

正确答案是：A　你的答案是：B　此题得分：0

展开解析

4

2 分

IP 指网络之间互连的协议，其全称为（　）

A.Internet Positon；B.Internet Protocol；C.Image Protocol；D.以上都不正确

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

5

2 分

OSI 把层与层之间交换的数据的单位称为 SDU，SDU 的中文名称是（　）

A.信号数据单元；B.协议数据单元；C.服务数据单元；D.接口数据单元

正确答案是：C　你的答案是：A　　此题得分：0

展开解析

6

2 分

以下不属于数据库风险的来源的是（　）

A.超级管理用户 sa；B.用户分配权限过小；C.启用网络协议过多；D.数据库使用默认端口

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

7

2 分

RIP 是一种分布式的基于距离向量的路由选择协议，它的英文全称为（　）

A.Routing Information Protocol；B.Routing Informercial Protocol；C.Routine Information Protocol；D.Routine Informercial Protocol

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

8

2 分

按照数据结构来组织、存储和管理数据的仓库被称作数据库，在一个支持事务的数据库中，事务完成后，该事物对数据库做的修改将持久的保存在数据库中，这体现了数据库的哪一个性质？

A.一致性；B.持久性；C.原子性；D.隔离性

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

9

2 分

随着网络安全威胁日益凸显，人们越来越重视网络安全，其包括在网络环境中对（　）提供安全防护措施

A.信息处理及传输；B.信息存储及访问；C.信息载体；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

10

2 分

日志分为应用程序日志、安全日志和系统日志等，以下不属于安全日志的是？

A.SQL Server 数据库程序进行备份设定的日志；B.对系统进行登录成功信息；C.删除系统文件；D.创建系统文件

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

11

2 分

以下属于网络安全设备的是？

A.路由器；B.交换机；C.集线器；D.防火墙

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

12

2 分

网络安全设备是保护网络安全的设施，以下不属于安全设备的是？

A.防火墙 //Firewall；B.虚拟专用网络 //VPN Network；C.WEB 应用防火墙 //Waf；D.摄像头

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

13

2 分

Apache 内建的有记录服务器活动的功能，以下对于 Apache 服务器日志叙述正确的是？

A.其日志大致分为两类：访问日志、错误日志；B.其日志大致分为三类：访问日志、错误日志、警告日志；C.其日志只有访问日志；D.其日志只有错误日志

正确答案是：A　你的答案是：B　　此题得分：0

展开解析

14

2 分

数据库是按照数据结构储存管理数据的仓库，以下关于数据库的叙述不正确的是？

A.一般都使用事务的工作模型运行；B.所有用户可同时存取数据库中的数据；
C.Oracle、Sqlserver、Apache 都是数据库；D.数据库都具有事务日志

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

15

2 分

数据库事务是指单个逻辑单元执行的一系列操作，以下关于事务的叙述不正确的是？

A.事务在完成时，必须使所有的数据都保持一致状态；B.事务必须满足原子性，所封装的操作或者全做或者全不做；C.事务管理系统保证多个事务并发执行，满足 ACID 特性；
D.数据库不必有事务日志

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

16

2 分

FTP 是 File Transfer Protocol 的缩写,以下对于 FTP 的叙述错误的是？

A.它是用于在网络上进行文件传输的一套标准协议；B.它使用客户/服务器工作模式；
C.它只有一种传输模式；D.它用于 Internet 上的控制文件的双向传输

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

17

2 分

采集系统日志的方法有很多，以下属于以文本方式采集系统日志方式的是？

A.多媒体语音；B.微信；C.邮件；D.电话

正确答案是：C　你的答案是：C　此题得分：2

展开解析

18

2 分

以下对于 Web Service 的叙述错误的是？

A.是一个 Web 应用程序；B.不能跨平台；C.可使用开放的 XML 标准来描述；D.具有开放性

正确答案是：B　你的答案是：B　此题得分：2

展开解析

19

2 分

以下对于 XML 的叙述错误的是？

A.它不能实现各种数据的集成管理；B.XML 严格地定义了可移植的结构化数据；C.它具有自描述性、可扩展性、层次性、异构系统间的信息互通性等特征；D.XML 是一种 Internet 异构环境中的数据交换标准

正确答案是：A　你的答案是：A　此题得分：2

展开解析

20

2 分

以下属于一对一递归关联的是？

A.指同类对象之间是一对一的关系；B.指不同类对象中存在着一个实体对应关联多个实体；C.指同类实体中关联的关系是多对多；D.指同类实体中关联的关系是多对一

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

21

2 分

以下属于多对多递归关联的是（　）

A.指同类对象之间是一对一的关系；B.指同一个类对象中存在着一个实体对应关联多个实体；C.指同类实体中关联的关系是多对多；D.指同类实体中关联的关系是多对一

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

22

2 分

以下属于一对多递归关联的是（　）

A.指同类对象之间是一对一的关系；B.指同一个类对象中存在着一个实体对应关联多个实体；C.指同类实体中关联的关系是多对多；D.指不同类对象中存在着一个实体对应关联多个实体

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

23

2 分

在关联规则的驱动下，（　）引擎能够进行多种方式的事件关联

A.递归关联分析；B.事件关联分析；C.统计关联分析；D.时序关联分析

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

24

2 分

（ ）技术可以更好地了解看似无关的但设备之间存在着理论相关性的关联分析

A.递归关联；B.统计关联；C.时序关联；D.跨设备事件关联

正确答案是：D 你的答案是：D 此题得分：2

展开解析

25

2 分

以下关于数据库数据查询描述有误的是（ ）

A.普通的条件查询就是按照已知确定的条件进行查询；B.查询的功能是通过 SQL 语句在数据库中进行操作实现；C.用户通常需要查询表中所有数据行的信息；D.模糊查询则是通过一些已知但不完全确定的条件进行查询

正确答案是：C 你的答案是：C 此题得分：2

展开解析

26

2 分

计算机系统一般有其相应的日志记录系统。其中，日志指系统所指定对象的某些操作和其操作结果按时间有序的集合，下列对其的叙述不正确的是（ ）

A.它是由各种不同的实体产生的“事件记录”的集合；B.它可以记录系统产生的所有行为并按照某种规范将这些行为表达出来；C.日志信息可以帮助系统进行排错、优化系统的性能；D.日志只在维护系统稳定性方面起到非常重要的作用

正确答案是：D 你的答案是：D 此题得分：2

展开解析

27

2 分

下列问题可能出现在原始日志信息中的有（　）

A.信息不全面；B.IP 地址错误；C.重复记录；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

28

2 分

计算机系统一般具有相应的日志记录系统，并且其日志文件记录具有许多作用，以下关于日志文件记录功能的描述不正确的是（　）

A.可以提供监控系统资源；B.可以审计用户行为；C.可以确定入侵行为的范围；D.不能为计算机犯罪提供证据来源

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

29

2 分

以下关于日志归一化的叙述中不正确的是（　）

A.它将不同格式的原始日志归一化为一种具有统一格式的日志；B.它降低了日志审计系统的审计效率；C.它方便了其他模块对日志数据的利用；D.它提高了日志数据的质量

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

30

2 分

XML 是可扩展标记语言的简称，以下选项中对其的描述不正确的是（　）

A.是一种用于标记电子文件的标记语言；B.具有良好的扩展性；C.具有良好的结构和约束机制；D.数据通过 XML 标记后表达方式更加复杂

正确答案是：D　你的答案是：D　此题得分：2

展开解析

31

2 分

递归关联的表达方式不包括以下哪种？

A.一对一递归关联；B.一对多递归关联；C.多对多递归关联；D.零对一递归关联

正确答案是：D　你的答案是：D　此题得分：2

展开解析

32

2 分

日志的存储格式不包括以下哪种？

A.基于文本的格式；B.基于二进制的格式；C.基于压缩文件的格式；D.基于 PNG 的格式

正确答案是：D　你的答案是：D　此题得分：2

展开解析

33

2 分

网络安全日志的数量庞大，为提高分析系统和生成报告的效率，通常将一些信息存入关系数据库，这些信息不包括（　）

A.头信息；B.序号；C.消息体；D.分析和总结

正确答案是：B　你的答案是：D　此题得分：0

展开解析

34

2 分

HDFS 是 Hadoop 分布式文件系统的简称，被设计成适合运行于通用硬件。以下其的描述不正确的是（　）

A.HDFS 的扩展性很弱；B.它是 Hadoop 实现的一个分布式文件系统；C.HDFS 满足超大规模的数据集需求；D.HDFS 支持流式的数据访问

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

35

2 分

操作系统是用户和计算机的接口，同时也是计算机硬件和其他软件的接口。下列哪个选项不是计算机操作系统（　）

A.Windows；B.Linux；C.Unix；D.Https

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

36

2 分

以下哪个选项不属于安全开发生命周期（SDL）在实现阶段减少漏洞的措施？

A.使用指定的工具；B.弃用不安全函数；C.不进行参数检查；D.静态分析

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

37

2 分

软件保证成熟度模型（SAMM）的目标是（　）

A.创建明确定义和可衡量的目标；B.涉及到软件开发的任何业务；C.可用于小型、中型和大型组织；D.以上都是

正确答案是：D　你的答案是：D　此题得分：2

展开解析

38

2 分

以下关于综合的轻量应用安全过程（CLASP）的描述，错误的是（　）

A.CLASP 包括 30 个特定的活动和辅助资源；B.CLASP 能够和多种软件开发模型结合使用；C.CLASP 的安全活动必须是基于访问列表安排的；D.CLASP 执行的安全活动及执行顺序的选择是开放的

正确答案是：C　你的答案是：D　此题得分：0

展开解析

39

2 分

以下关于安全需求分析过程的描述，错误的是（　）

A.需求分析是一个持续的过程，跨越整个项目的生存周期；B.软件安全需求分析需要进行系统调查的过程；C.安全需求分析是一个一劳永逸的过程；D.可以采用概率统计的方法分析系统的脆弱点和安全威胁

正确答案是：C　你的答案是：C　此题得分：2

展开解析

40

2 分

以下关于 SQUARE 过程模型的描述，错误的是（　）

A.使用 SQUARE 过程模型时，软件项目的安全开发过程不必考虑其运行环境；B.当项目发生变化时，应重新应用 SQUARE 过程模型分析安全需求；C.统一定义是安全需求工程的首要条件；D.专用检查方法和同行审查都可以用来检查安全需求

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

41

2 分

以下关于安全关键单元的描述，错误的是（　）

A.安全关键单元的错误可能导致系统潜在严重危险；B.安全性关键单元包括产生对硬件进行自主控制信号的单元；C.安全关键的计时单元可以由程序控制，随意修改；D.安全关键单元至少受控于两个独立的单元

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

42

2 分

以下关于危险建模过程的描述中，错误的是（　）

A.威胁建模有助于降低软件的攻击面；B.威胁建模可以一次性完成，不需要重复进行；C.威胁建模是一种风险管理模型；D.威胁建模在软件生命周期需求设计阶段就会介入

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

43

2 分

缓解威胁常用的技术手段不包括（　）

A.验证系统输入；B.增大攻击面；C.进行模糊测试；D.采用访问控制手段

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

44

2 分

缓冲区溢出作为一种较为普遍以及危害性较大的漏洞，在各操作系统以及应用软件中广泛存在，下列选项中对其描述错误的是（　）

A.缓冲区是存储数据的一组地址连续的内存单元；B.缓冲区溢出在软件的开发和测试阶段一定可以发现；C.并非所有的缓冲区溢出都会造成软件漏洞；D.著名的心脏流血漏洞是缓冲区漏洞

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

45

2 分

C 语言作为一种计算机编程语言，获得广泛应用。下列选项中对其描述错误的是（　）

A.C 语言是面向对象的开发语言；B.C 语言拥有强大的操控内存的能力；C.C 语言可以应用于操作系统、浏览器和嵌入式开发等领域；D.C 语言拥有强大的底层操作能力

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

46

2 分

Java 作为一种计算机编程语言，功能非常强大。以下不属于 Java 的特点的是（　）

A.跨平台；B.多线程；C.面向过程；D.面向对象

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

47

2 分

以下关于路径遍历的描述，错误的是（　）

A.路径遍历漏洞允许攻击者访问受限的目录，获取系统文件及服务器的配置文件；B.Web 服务器提供访问控制列表和根目录访问的安全机制；C.使用 GET 或是 POST 的请求方法可以获得输入；D.路径遍历漏洞没有任何危害

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

48

2 分

哈希算法之所以被认为安全，主要是基于以下哪两种性质？

A.无冲突和不可逆；B.冲突性和不可逆；C.冲突性和随机性；D.随机性和可逆性

正确答案是：A　你的答案是：D　　此题得分：0

展开解析

49

2 分

下列选项中关于 Java 语言的异常处理机制描述错误的是（　）

A.可以根据 catch 程序段的上下文抛出另一个适合的异常；B.在异常传递的过程中，应该对敏感信息进行过滤；C.尽量要在 finally 程序段非正常退出；D.记录日志时应避免异常

正确答案是：C　你的答案是：D　　此题得分：0

展开解析

50

2 分

下列选项中关于 Java 语言线程的描述，错误的是（　）

A.多线程是 Java 语言的特性之一；B.良好的线程调度，有助于发挥系统的性能；C.Thread Group 中所有方法都是安全的，提倡使用；D.调用 Thread 的 start 方法可启动一个新线程

正确答案是：C　你的答案是：C　　此题得分：2

第四章

1

2 分

以下不属于 Session 攻击常用防护措施的是（　）

A.定期更换 Session ID；B.通过 URL 传递隐藏参数；C.设置 Http Only；D.开启透明化 Session ID

正确答案是：D　你的答案是：C　　此题得分：0

展开解析

2

2 分

在 PHP 开发中，不属于命令注入攻击的防范方法的是（　）

A.尽量不要执行外部的应用程序或命令；B.对输入命令不做任何检查；C.使用安全函数处理相关参数；D.使用自定义函数或函数库实现外部应用程序或命令的功能

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

3

2 分

以下不属于 Pyhton 开发优点的是（　）

A.可阅读性；B.非开源；C.可跨平台；D.可嵌入性

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

4

2 分

Python 是一门有条理的、强大的面向对象的程序设计语言，以下对 Pyhton 的应用描述错误的是（　）

A.Python 是数据科学中最流行的语言之一；B.Python 广泛应用于金融分析、量化交易领域；C.Python 在网络游戏开发中也有较多应用；D.Python 在各个领域中的应用不可替代。

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

5

2 分

在信息安全中密码至关重要，以下对密码的描述中错误的是（　）

A.用户名密码是用户身份认证的关键因素；B.密码是保护服务器和用户敏感数据的关键因素；C.密码明文直接存储十分安全；D.弱口令密码易被破解

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

6

2 分

以下不属于文件上传漏洞的防范措施的是（　）

A.使用固定数改写文件名和文件路径；B.对上传文件类型进行检查；C.将文件上传目录设置为不可执行；D.单独设置文件服务器的域名

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

7

2 分

软件安全性测试包括程序、网络、数据库安全性测试。以下关于软件安全测试的描述，错误的是（　）

A.狭义的软件安全测试是执行安全测试用例的过程；B.广义的软件安全测试是所有关于安全性测试的活动；C.软件安全测试的对象只包括代码；D.软件安全测试与传统软件测试的测试用例不相同

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

8

2 分

以下属于常用的安全测试的方法的是（　）

A.黑盒测试；B.白盒测试；C.灰盒测试；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

9

2 分

PDCA 循环的含义是将质量管理分为四个阶段，即计划（plan）、执行（do）、检查（check）、处理（Act）。以下不属于 PDCA 循环特点的选项是（　）

A.开环系统，运行一次；B.顺序进行，循环运转；C.大环套小环，小环保大环，相互制约，相互补充；D.不断前进，不断提高

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

10

2 分

渗透测试通过以下哪种方法来评估系统的安全状况（　）

A.模拟恶意黑客攻击；B.模拟用户正常操作；C.更新系统代码；D.以上都不正确

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

11

2 分

以下属于渗透测试的测试对象的是（　）

A.操作系统；B.应用系统；C.网络设备；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

12

2 分

最终安全审查的流程包括（　）

A.评估资源可用性；B.确定合格的特征评估发现者的漏洞；C.评估和制定修复计划；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

13

2 分

在 Web 应用系统中，数据层主要负责对数据的操作，以下属于数据层操作的是（　）

A.对数据的读取；B.对数据的增加；C.对数据的修改；D.以上都是

正确答案是：D　你的答案是：D　此题得分：2

展开解析

14

2 分

以下关于 WAF 产品功能的描述中，不正确的是（　）

A.WAF 可以阻止非授权访问的攻击者窃取客户端或者网站上含有敏感信息的文件；B.WAF 产品应该具备针对应用层 DOS 攻击的防护能力；C.基于 URL 的应用层访问控制和 HTTP 请求的合规性检查，都属于 WAF 的应用合规功能；D.WAF 的应用交付能力可以完全保障用户的敏感信息的安全

正确答案是：D　你的答案是：D　此题得分：2

展开解析

15

2 分

近年来，随着云计算、大数据技术逐渐应用到安全领域，基于软件即服务（Software-as-a-service，SaaS）模式的 Web 应用安全监测十分具有市场潜力，通常情况下的 SaaS 软件主要应用于哪些企业管理软件？

A.客户关系管理；B.人力资源管理；C.供应链管理；D.以上都是

正确答案是：D　你的答案是：D　此题得分：2

展开解析

16

2 分

Web 网页就是万维网上的一个按照 HTML 格式组织起来的文件。当访问 Web 网站的某个页面资源不存在时，HTTP 服务器发回的响应状态代码是（　）

A.200；B.500；C.401；D.404

正确答案是：D　你的答案是：D　此题得分：2

展开解析

17

2 分

在接收到 HTTP 请求报文后，服务器会返回一个 HTTP 响应报文，HTTP 响应报文由三部分组成。不属于 HTTP 响应报文的组成部分的是（　）

A.状态行；B.响应头；C.响应实体；D.主机登录密码

正确答案是：D　你的答案是：D　此题得分：2

展开解析

18

2 分

HTTP 是超文本传输协议，是为了提供一种发布和接收 HTML 页面的方法。HTTP 服务默认 TCP 端口号是（　）

A.80；B.21；C.23；D.25

正确答案是：A　你的答案是：A　此题得分：2

展开解析

19

2 分

HTTP 报文分为请求报文和响应报文两种，HTTP 请求报文的组成部分不包含（　）

A.请求行；B.开放端口；C.请求实体；D.请求头

正确答案是：B　你的答案是：B　此题得分：2

展开解析

20

2 分

HTTP 请求是指从客户端到服务器端的请求消息。下列选项中不是 HTTP 请求方法的是（ ）

A.BODY ； B.POST； C.HEAD； D.GET

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

21

2 分

HTTP 消息（HTTP HEADER）又称 HTTP 头，包括请求头等四部分。请求头只出现在 HTTP 请求中，请求头允许客户端向服务器端传递请求的附加信息以及客户端自身的信息，常用的 HTTP 请求报头不包括（　）

A.Line； B.Cookie； C.Accept； D.Host

正确答案是：A　你的答案是：C　　此题得分：0

展开解析

22

2 分

HTTP 访问控制主要针对网络层的访问控制，通过配置面向对象的通用包过滤规则实现控制域名以外的访问行为。以下属于具体访问控制的是（　）

A.对访问者访问的 URL 的控制，允许或不允许访问设定的 URL 对象； B.对访问者的 HTTP 方法的控制，允许或不允许设定的 HTTP 方法访问； C.对访问者的 IP 的控制，允许或不允许设定的 IP 对象访问； D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

23

2 分

Web 应用程序设计普遍采用三层架构，这三层架构不包含（　）

A.业务表示层；B.数据访问层；C.物理层；D.逻辑层

正确答案是：C　你的答案是：A　　此题得分：0

展开解析

24

2 分

一般情况下，以下属于 SQL 注入攻击特点的是（　）

A.普遍性；B.隐蔽性；C.危害性；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

25

2 分

SQL 注入攻击方式有很多种，但本质上都是由 SQL 语言的属性来决定的。下列不属于 SQL 注入攻击的攻击方式的是（　）

A.重言式攻击；B.非法或逻辑错误查询攻击；C.联合查询攻击；D.社会工程学攻击

正确答案是：D　你的答案是：A　　此题得分：0

展开解析

26

2 分

在开发一个新 Web 应用系统时，最好采用安全的程序设计方法，以避免或减少 SQL 注入漏洞。下列属于避免 SQL 注入漏洞的程序设计是（　）

A.使用存储过程；B.使用抽象层；C.处理敏感数据；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

27

2 分

跨站请求伪造（Cross-Site Request Forgery，CSRF）是一种对网站的恶意利用。以下属于跨站请求伪造攻击的必要条件的是（　）

A.浏览器自动发送标识用户对话的信息而无须用户干预；B.攻击者对 Web 应用程序 URL 的了解；C.浏览器可以访问应用程序的会话管理信息；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

28

2 分

关于 Web 应用防火墙，目前防御　CSRF 攻击的三种策略不包括（　）

A.取消 HTTP Refresh 字段的验证；B.验证 HTTP Referer 字段；C.在请求地址中添加 token 并验证；D.在 HTTP 头中自定义属性并验证

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

29

2 分

网络爬虫按照系统结构和实现技术，大致可以分为多种类型，以下属于爬虫分类的是（　）

A.通用网络爬虫；B.聚焦网络爬虫；C.增量式网络爬虫；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

30

2 分

目前网络爬虫的检测手段多种多样，往往需要综合利用，提高检测的准确率。下列属于网络爬虫的检测手段的是（　）

A.检测 HTTP User-Agent 报头；B.检查 HTTP Referer 报头；C.检测客户端 IP；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

31

2 分

攻击者对 Web 服务器进行攻击的时候，首先通过各种渠道获取 Web 服务器的各种信息，尤其是 Web 服务器的各种敏感信息。常见敏感信息泄露方式不包括（　）

A.Banner 收集；B.源码泄漏；C.处理敏感信息不当；D.正常信息页面显示

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

32

2 分

关于 Web 应用防火墙，Web 服务器防范敏感信息泄露的方式不包括（　）

A.不采取认证措施；B.关键词检测；C.严格控制服务器的写访问权限；D.对 IIS 目录采用严格的访问策略

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

33

2 分

长期以来，弱密码一直是各项安全检查、风险评估报告中最常见的高风险安全问题，成为攻击者控制系统的主要途径。弱口令漏洞有三大特点不包括（　）

A.危害大；B.难猜测；C.修补难；D.易利用

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

34

2 分

网页篡改通过恶意破坏或更改网页内容导致网站无法正常工作。关于 Web 应用防火墙，攻击者常用的网页篡改方法不包括（　）

A.社会工程学；B.在 Web 页面中插入 HTML 代码；C.控制 DNS 服务器；D.ARP 攻击

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

35

2 分

网页防篡改系统对网页文件提供实时动态保护，对未经授权的非法访问行为一律进行拦截，防止非法人员篡改、删除受保护的文件，确保网页文件的完整性。一般网页防篡改措施的过程不包括（　）

A.给正常文件颁发通行证；B.检测和防护 SQL 注入攻击；C.检测网络带宽；D.检测和防护 DNS 攻击

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

36

2 分

DDos 攻击将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DDoS 攻击，从而成倍地提高拒绝服务攻击的威力。关于 DDoS 的攻击现象一般不包括（　）

A.被攻击主机上有大量等待的 TCP 连接；B.网络中充斥着大量的无用的数据包；C.源地址为假，制造高流量无用数据，造成网络拥塞，使目标主机无法正常和外界通讯；D.用户访问无网络延时，正常访问 Web 服务

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

37

2 分

关于 DDoS 攻击防范策略不包括（　）

A.通过合理的配置系统，达到资源最优化和利用最大化；B.限制内网用户访问；C.通过加固 TCP/IP 协议栈来防范 DDoS 攻击；D.通过防火墙、路由器等过滤网关，有效地探测攻击类型并阻击攻击

正确答案是：B　你的答案是：A　　此题得分：0

展开解析

38

2 分

Linux 系统中通过编辑（　）文件，可以修改密码设置，如密码设置最长有效期等。

A.Passwd；B.profile；C.login.defs；D.init.d

正确答案是：C　你的答案是：A　　此题得分：0

展开解析

39

2 分

威胁情报的出现将网络空间安全防御从传统被动式防御转移到主动式防御里。传统情报应具备准确性、针对性和及时性等特征，以下不属于安全威胁情报的基本特征的是（　）

A.时效性；B.相关性；C.模糊性；D.可操作性

正确答案是：C　你的答案是：D　　此题得分：0

展开解析

40

2 分

威胁情报的用途多种多样，除去攻击检测方面的价值外，实际上威胁情报的使用场景更加广泛。下列不属于威胁情报的用途的是（　）

A.安全体系建设与完善；B.攻击检测和防御；C.安全部门汇报；D.安全分析及事件响应

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

41

2 分

下列概念不属于 WAF 为解决 Web 安全问题而遵循的是（　）

A.重塑网站边界；B.智能化防护理念；C.开放服务端口；D.纵深防御体系

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

42

2 分

以下属于网站敏感信息泄露的主要原因是（　）

A.网站信息繁多；B.黑客攻击水平高；C.黑客数量多；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

43

2 分

下列不属于常见的服务器端脚本程序的是（　）

A.ASP；B.JSP；C.PHP；D.HTML

正确答案是：D　你的答案是：B　　此题得分：0

展开解析

44

2 分

Web 服务器可以解析各种动态语言，让动态语言生成的程序最终能显示在浏览的页面上。下列不属于常见的 Web 服务器的是（　）

A.Microsoft IIS；B.Apple；C.Apache；D.Nginx

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

45

2 分

以下属于 2019 年 OWASP 十大安全漏洞的是（　）

A.SQL 注入；B.XSS 漏洞；C.敏感信息泄露；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

46

2 分

网络环境下的信息安全体系是保证信息安全的关键。以下不属于常用的信息安全技术的是（　）

A.DNS 系统；B.防火墙系统；C.入侵防护系统（PS）；D.访问控制系统

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

47

2 分

防火墙是一种位于内部网络与外部网络之间的网络安全系统。以下不属于防火墙作用的是（　）

A.隔离不同信任级别网络；B.保护内部网络；C.数据备份；D.限制内部用户访问特殊站点

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

48

2 分

软件开发生命周期的思想方法是按什么分程的（　）

A.时间；B.状态；C.空间；D.完成度

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

49

2 分

近十几年来，信息系统作为一个专门领域迅速形成和发展。以下不属于构成信息系统核心要素的是（　）

A.人；B.漏洞；C.技术；D.组织

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

50

2 分

信息系统是以信息为系统核心因素而构成的为人类服务的一类重要工具。以下关于信息系统功能的说法，错误的是（　）

A.信息系统中信息处理一般包括信息的输入、存储、处理、输出和控制；B.企业信息系统可以将基础信息处理成对企业生产经营和管理有用的信息；C.信息系统中，信息加工的方法一般是基于数据仓库技术的联机分析处理和数据挖掘技术；D.企业信息系统的业务处理只有联机事务处理一种类型

正确答案是：D　你的答案是：D　　此题得分：2

第五章

1

2 分

目前，我国对网络安全形势高度重视，以下关于网络安全形势的描述中，错误的是（　）

A.我国的网络安全态势非常好，不面临任何攻击的威胁；B.高级持续性威胁常态化，我国面临的攻击十分严重；C.大量联网智能设备遭受恶意程序攻击形成僵尸网络，被用于发起大流量 DDoS 攻击；D.网站数据和个人信息泄露屡见不鲜

正确答案是：A 你的答案是：A 此题得分：2

2

2 分

信息安全问题是一个系统问题，而不是单一的信息本身的问题，根据系统安全的整体结构，可将信息系统安全分为 5 个层次。以下不属于信息系统安全五个层面的是（　）

A.物理安全；B.网络安全；C.数据安全；D.端口安全

正确答案是：D 你的答案是：D 此题得分：2

3

2 分

信息安全已经成为社会的焦点问题，以下不属于信息系统安全运营原则的是（ ）

A.合规性与风险控制结合的原则；B.绝对安全原则；C.统一管控原则；D.易操作性原则

正确答案是：B 你的答案是：B 此题得分：2

4

2 分

作为全方位的、整体的信息安全防范体系是分层次的，以下关于企业信息系统层次划分的描述，错误的是（ ）

A.越接近内部的网络安全要求等级越低，越接近外部的网络安全要求等级越高；B.业务专用网是企业为了特殊工作需要而建造的专用网络；C.互联网区域用于日常的互联网业务，安全防护等级要求最低；D.企业内网是企业的核心网络，拥有最高的安全防护等级

正确答案是：A 你的答案是：A 此题得分：2

5

2 分

信息资产是企业拥有和控制的一项特殊资产，以下属于信息资产的存在形式的是（ ）

A.数据资产；B.软件资产；C.服务资产；D.以上都是

正确答案是：D 你的答案是：D 此题得分：2

6

2 分

信息安全风险评估是信息系统安全工程的重要组成部分，以下数据的操作与安全风险评估无关的是（ ）

A.数据篡改；B.数据采集；C.数据处理；D.数据分析

正确答案是：A 你的答案是：A 此题得分：2

7

2 分

目前广泛应用于浏览器与服务器之间身份认证和加密数据传输的协议是（ ）

A.SSL 协议；B.APR 协议；C.HTTP 协议；D.SMTP 协议

正确答案是：A 你的答案是：A 此题得分：2

8

2 分

防火墙是一种非常有效的保障网络安全的工具，以下不属于防火墙的主要功能的是（ ）

A.基础组网和防护功能；B.实现内外网数据加密传输；C.限定内部用户访问特殊站点；D.过滤进出网络的数据

正确答案是：B 你的答案是：B 此题得分：2

9

2 分

漏洞扫描是指检测、扫描系统中存在的漏洞或缺陷，以下不属于漏洞扫描系统的应用场景的是（ ）

A.业务上线前的安全扫描；B.业务运行中的安全监控；C.业务运行中的安全预警；D.业务结束后的数据清除

正确答案是：D 你的答案是：D 此题得分：2

10

2 分

在网络空间安全事件响应活动中，以下不能体现安全事件的响应能力的是（ ）

A.决策能力；B.定位能力；C.攻击能力；D.行动能力

正确答案是：C 你的答案是：C 此题得分：2

11

2 分

以下关于安全信息收集和处理的描述，错误的是（ ）

A.安全信息的收集和处理，是整个安全分析和决策的基础；B.采集到的原始安全数据中没有任何的无效数据；C.数据清洗一般可以由准备、检测、定位、修正、验证组成；D.原始采集的数据通常不会完全的清洁和规范

正确答案是：B 你的答案是：B 此题得分：2

12

2 分

数据备份是数据容灾的基础，以下不是数据备份方法的是（ ）

A.磁带库备份；B.磁盘无规律备份；C.磁盘阵列备份；D.磁盘镜像备份

正确答案是：B 你的答案是：B 此题得分：2

13

2 分

容灾是为了在遭遇灾害时能保证信息系统能正常运行，帮助企业实现业务连续性的目标，以下属于容灾技术范畴的是（ ）

A.数据容灾；B.系统容灾；C.应用容灾；D.以上都是

正确答案是：D 你的答案是：D 此题得分：2

14

2 分

容灾系统就是为计算机信息系统提供的一个能应付各种灾难的环境，以下不属于容灾抗毁能力评判指标的是（　）

A.恢复时间目标；B.降级操作目标；C.防火墙恢复目标；D.网络恢复目标

正确答案是：C 你的答案是：C 此题得分：2

15

2 分

随着网络空间安全重要性的不断提高，网络安全态势感知（NSSA）的研究与应用正在得到更多的关注。以下关于 NSSA 的描述，错误的是（　）

A.态势感知的数据来源丰富；B.态势感知结果丰富实用；C.态势感知适用范围十分窄；D.态势感知能对网络安全状况的发展趋势进行预测

正确答案是：C 你的答案是：C 此题得分：2

16

2 分

网络安全态势感知是中国互联网安全的创新方向之一，以下不属于态势感知的三个层次的是（　）

A.规则；B.感知；C.理解；D.预测

正确答案是：A 你的答案是：A 此题得分：2

17

2 分

态势感知在网络安全方面具有检测、分析、预测、防御的能力。以下不属于网络安全态势预测方法的是（　）

A.神经网络；B.时间序列预测；C.无规则预测；D.支持向量机

正确答案是：C 你的答案是：C 此题得分：2

18

2 分

数据融合技术作为数据处理的新兴技术，在近 10 年中得到惊人发展。以下属于数据融合技术的是（ ）

A.基于逻辑关系的融合方法；B.基于数学模型的融合方法；C.基于概率统计的融合方法；D.以上都是

正确答案是：D 你的答案是：D 此题得分：2

19

2 分

常见的网络扫描器都是可以从 Internet 上免费获得的，以下不属于网络扫描器的是（ ）

A.Nmap；B.Nessus；C.X-Scan；D.Google

正确答案是：D 你的答案是：D 此题得分：2

20

2 分

“Internet 协议安全性 (IPSec)”是一种开放标准的框架结构，通过使用加密的安全服务以确保在 Internet 协议 (IP) 网络上进行保密而安全的通讯。IPSec 是为（ ）提供加密和认证的协议规范

A.物理层；B.网络层；C.运输层；D.应用层

正确答案是：B 你的答案是：B 此题得分：2

21

2 分

SSL 协议能够在客户端和服务器之间建立起一个安全通道，所有消息都经过加密处理以后进行传输，网络中的非法黑客无法窃取，体现了 SSL 协议的（ ）

A.秘密性；B.灵活性；C.认证性；D.具体性

正确答案是：A 你的答案是：A 此题得分：2

22

2 分

SSL 上层协议用于对 SSL 交换进行管理，以下不属于 SSL 高层协议的是（ ）

A.握手协议；B.改变密码说明协议；C.警报协议；D.确认与回复协议

正确答案是：D 你的答案是：D 此题得分：2

23

2 分

网络安全态势的预测方法有多种，以下关于神经网络预测网络安全态势的描述，错误的是（ ）

A.神经网络预测方法没有任何缺点；B.神经网络是目前最常用的网络态势预测方法；C.神经网络具有自学习、自适应性和非线性处理的优点；D.神经网络具有良好的容错性和稳健性

正确答案是：A 你的答案是：A 此题得分：2

24

2 分

网络追踪溯源技术正处于不断发展的阶段，还面临着一些困难和挑战，以下关于溯源面临挑战的描述，错误的是（ ）

A.当前网络通信协议中没有对传输信息进行加密认证的措施，出现各种 IP 地址伪造技术；B.攻击者通过俘获大量主机资源，发起间接攻击并隐藏自己；C.虚拟专用网络采用的 IP 隧道技术，无法获取数据报文信息；D.溯源单靠技术手段能解决所有问题

正确答案是：D 你的答案是：D 此题得分：2

25

2 分

网络追踪溯源技术是网络对抗中的关键技术之一，以下关于溯源意义的说法，错误的是（ ）

A.利用追踪溯源技术提高了网络主动防御的及时性和有效性；B.利用追踪溯源技术花费大量成本和代价，得不偿失；C.利用追踪溯源技术可追踪定位网络内部攻击行为，防御内部攻击；D.利用追踪溯源技术可以记录各种网络攻击过程，为司法取证

正确答案是：B 你的答案是：B 此题得分：2

26

2 分

参考《信息安全等级保护管理办法》，对信息系统建议采取五级划分，以下说法错误的是（ ）

A.第一级：信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益；B.第二级：信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全；C.第三级：信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害；D.第四级：信息系统受到破坏后，会对国家安全造成特别严重损害

正确答案是：D 你的答案是：D 此题得分：2

27

2 分

网络安全系统中，网络安全设备是必不可少的，下列设备中不属于网络安全设备的是（ ）

A.防火墙；B.入侵防御系统；C.显示器；D.漏洞扫描系统

正确答案是：C 你的答案是：C 此题得分：2

28

2 分

在解决问题时往往需要遵循一定的原则，下列关于安全策略管理基本设计原则的说法中错误的是（　）

A.先易后难，即优先解决技术难度较低的安全问题，以最快的时间减少最多的安全漏洞为目标；B.先急后缓，即优先解决紧急的安全问题，优先关注重要业务相关的系统；C.先众后寡，即优先解决普遍性的安全问题，对于此类安全问题主要考虑安全问题的影响面；D.先地后云，在当前的网络环境下，本地终端的影响范围和影响深度都远大于云端服务的安全问题

正确答案是：D 你的答案是：D 此题得分：2

29

2 分

一套信息系统安全策略应该全面地保护信息系统整体的安全，在设计策略的范围时，主要考虑（　）

A.物理安全策略；B.网络安全策略；C.数据加密策略；D.以上都是

正确答案是：D 你的答案是：D 此题得分：2

30

2 分

安全应急响应是整个安全防御体系中一个不可缺少的环节，下列选项中不是应急响应的主体的是（　）

A.政府部门；B.个人；C.基础设施管理经营单位；D.大型机构

正确答案是：B 你的答案是：B 此题得分：2

31

2 分

应急响应通常分为准备、事件检测、抑制、根除、恢复、报告等阶段，下列选项中关于网络安全应急响应活动的说法中错误的是（　）

A.网络应急响应的活动应该主要包括两个方面：第一是未雨绸缪，第二是亡羊补牢；B.事前的计划和准备为事件发生后的响应动作提供了指导框架；C.事后的响应可能发现

事前计划的不足，从而吸取教训，进一步完善安全计划；D.目前网络安全应急响应相关工作满足实际工作需求，网络安全应急标准体系已经完善

正确答案是：D 你的答案是：D 此题得分：2

32

2 分

我们可根据信息安全事件的起因、表现、结果等将信息安全事件分类，以下选项中属于信息安全事件的是（ ）

A．恶意程序事件；B．网络攻击事件；C．信息破坏事件；D．以上都是

正确答案是：D 你的答案是：D 此题得分：2

33

2 分

信息安全事件一般包括恶意程序事件、网络攻击事件、信息破坏事件、设备设施故障、灾害性事件等，下列选项中不属于信息破坏事件的是（ ）

A.信息篡改事件；B.信息传播事件；C.信息假冒事件；D.信息泄漏事件

正确答案是：B 你的答案是：B 此题得分：2

34

2 分

恶意程序事件是指蓄意制造、传播有害程序，或是因受到有害程序性的影响而导致的信息安全事件，下列选项中不属于恶意程序事件的是（ ）

A.后门攻击事件；B.计算机病毒事件；C.蠕虫事件；D.特洛伊木马事件

正确答案是：A 你的答案是：A 此题得分：2

35

2 分

下列选项中关于企业网络安全应急响应工作所面临的主要对象及特点的说法错误的是（　）

A.企业网络最关注的是系统或软件漏洞引发的网络与信息安全问题；B.企业既面临程序开发导致的漏洞，也有协议架构或系统管理流程上的漏洞，还有硬件上的漏洞；C.企业网络安全应急响应不需要关注 DDoS 攻击事件的应急响应；D.对于跨区域大型企业，由于其内部网络的复杂度高，将使企业信息系统安全应急响应复杂度、隐患排查难度大大提高

正确答案是：C 你的答案是：C 此题得分：2

36

2 分

网络安全应急管理是网络安全工作的重要内容，下列选项中关于网络安全应急能力建设的说法错误的是（　）

A.网络安全领域的应急保障需要依靠自动化的现代分析工具，实现对不同来源海量信息的自动采集、识别和关联分析；B.网络安全日常管理与应急响应之间没有区别，业务类型相同，响应流程也相同；C.在实现网络与信息安全应急指挥业务的过程中，应注重用信息化手段建立完整的业务流程；D.研判、处置重大网络信息安全事件，需要多个单位、部门和应急队伍进行支撑和协调

正确答案是：B 你的答案是：B 此题得分：2

37

2 分

近年来，我国企业信息化的应用水平逐步深入，各企业都在不同程度上建立了自己的信息系统。以下不属于当前企业信息系统特点的是（　）

A.规模庞大；B.体系复杂；C.类型单一；D.地域广泛

正确答案是：C 你的答案是：C 此题得分：2

38

2 分

电子邮件是 Internet 应用最广的服务，以下用于邮件系统发送电子邮件的协议是（　）

A．SMTP；B．POP3；C．FTP；D．IMAP

正确答案是：A 你的答案是：A 此题得分：2

39

2 分

信息安全防护框架从下至上可分为六个层面，以下不属于数据层安全管控内容的是（　）

A.防止数据被非法访问；B.防止数据被非法传播；C.防止数据被非法篡改；D.防止数据被授权使用

正确答案是：D 你的答案是：D 此题得分：2

40

2 分

现在局域网已非常广泛地使用，下列关于局域网的选项中，不正确的是（　）

A.局域网可以实现文件管理、应用软件共享等功能；B.局域网是覆盖全世界的；C.局域网是将各种计算机、外部设备、数据库等互相连接起来组成的计算机通信网；D.局域网的全称为 Local Area Network，LAN

正确答案是：B 你的答案是：B 此题得分：2

41

2 分

按网络的作用范围可将计算机网络分为广域网、城域网、局域网和个人区域网，下列关于广域网、城域网的选项中，不正确的是（　）

A.城域网通常跨接很大的物理范围，能连接多个城市、国家；B.城域网的一个重要用途是用作骨干网；C.Internet 是目前最大的广域网；D.在计算机网络和工业业务发展初期，各企业管理信息系统和访问信息系统的用户基本都处在局域网内

正确答案是：A 你的答案是：A 此题得分：2

42

2 分

远程办公是指通过现代互联网技术，实现非本地办公：在家办公、异地办公、移动办公等远程办公模式。下列关于远程办公的选项，不正确的是（ ）

A.远程办公往往价格昂贵；B.远程办公数据传输一般不安全；C.远程办公早期缺少访问控制；D.远程办公能彻底代替本地办公

正确答案是：D 你的答案是：D 此题得分：2

43

2 分

移动办公即办公人员可在任何时间(Anytime)、任何地点(Anywhere)处理与业务相关的任何事情(Anything)。关于移动办公的风险中，以下描述不正确的是（ ）

A.移动终端难管控；B.移动终端环境安全难保障；C.移动终端安装了最新的安卓系统；D.终端准入难设定

正确答案是：C 你的答案是：C 此题得分：2

44

2 分

VPN 是一种能够将物理上分布在不同地点的网络通过公用骨干网，尤其是 Internet 连接而成的逻辑上的虚拟子网。关于 VPN 的内容和特点，以下描述不正确的是（ ）

A.VPN 的全称是 Validated Public Network ； B.VPN 依靠 Internet 服务提供商和网络服务提供商建立虚拟的加密专用网络通道；C.VPN 一般应用于企业内部网络；D.VPN 特有的经济性和安全性等特点使得其应用领域不断扩大

正确答案是：A 你的答案是：A 此题得分：2

45

2 分

VPN 在企业网络中有广泛应用。下列关于 VPN 优势的描述中，不正确的是（　）

A.对用户而言，IP 地址安全；B.不应用于移动业务；C.廉价；D.可实现多业务

正确答案是：B 你的答案是：B 此题得分：2

46

2 分

VPN 是在公网中形成的企业专用链路。下列关于 VPN 的发展趋势的描述中，正确的是（）

A.弱化用户验证；B.取消地址分配；C.提升多协议支持；D.关闭密钥管理

正确答案是：C 你的答案是：C 此题得分：2

47

2 分

VPN 适用于大中型企业的总公司和各地分公司或分支机构的网络互联和企业同商业合作伙伴之间的网络互联。下列关于 VPN 业务发展趋势的描述中，不正确的是（　）

A.运营商取消建设专有 VPN 网络；B.大型企业 VPN 网络需求增高；C.VPN 厂商竞争更加激烈；D.VPN 厂商的服务质量将会有实质性的提高

正确答案是：A 你的答案是：A 此题得分：2

48

2 分

在 VPN 方面，目前企业采用的保障业务安全的解决方案不包括（　）

A.统一安全接入平台；B.系统支持多种认证方式；C.不使用任何防火墙和杀毒引擎；D.统一派发设备，强管控

正确答案是：C 你的答案是：C 此题得分：2

49

2 分

安全传输层协议 TLS 用于在两个通信应用程序之间提供保密性和数据完整性，它的英文全称是（ ）

A.Transport Layer Security Protocol ； B.Transfer Layer Security Protocol ； C.Transport Layer Secure Protocol ； D.Transfer Layer Secure Protocol

正确答案是：A 你的答案是：A 此题得分：2

50

2 分

远程认证接入用户服务（RADIUS）协议是一种提供在网络接入服务器和共享认证服务器间传送认证、授权和配置信息等服务的协议，它的英文全称是（ ）

A.Remote Authentic Dial In User Service ； B.Remove Authentic Dial In User Service ； C.Remote Authentication Dial In User Service ； D.Remove Authentication Dial In User Service

正确答案是：C 你的答案是：C 此题得分：2

第六章

1

2 分

SSH 协议是在（ ）与（ ）之间的加密隧道应用协议

A.网络层 传输层 ； B.传输层 应用层； C.传输层 应用层； D.数据链路层 网络层

正确答案是：B 你的答案是：A 此题得分：0

展开解析

2

2 分

蜜罐技术是一种主动防御技术，是入侵检测技术的一个重要发展方向，以下关于蜜罐特点的描述正确的是（　）

A.相对于其他安全措施，蜜罐最大的优点就是简单；B.占用资源少；C.数据收集面狭窄；D.以上都对

正确答案是：D　你的答案是：D　此题得分：2

展开解析

3

2 分

Honeyd 是一种很强大的具有开放源代码的蜜罐，运行在（　）系统上，可以同时模仿 400 多种不同的操作系统和上千种不同的计算机

A.UNIX；B.Linux；C.Windows；D.MacOS

正确答案是：A　你的答案是：B　此题得分：0

展开解析

4

2 分

Tor 是目前最流行、最受开发者欢迎的网络匿名访问手段，其英文全称为（　）

A.The Onion Router；B.To Onion Router；C.The Online Router；D.To Online Router

正确答案是：A　你的答案是：C　此题得分：0

展开解析

5

2 分

网络入侵即利用网络存在的漏洞和安全缺陷对网络系统的硬件、软件及其系统中的数据进行攻击。以下选项中属于网络入侵对象的是（　）

A.进程；B.应用系统；C.服务器；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

6

2 分

用于备份的设备有硬盘、光盘、磁带。以下关于这三种设备说法正确的是（　）

A.硬盘存取速度最快，成本最高；B.光盘无法获得网络系统的完全备份；C.磁带技术可对整个系统进行备份，易于保存；D.以上都对

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

7

2 分

以下关于网络入侵的发展趋势说法错误的是（　）

A.网络入侵的自动化程序和入侵速度不断提高；B.入侵工具越来越复杂；C.攻击网络基础设施产生的破坏效果越来越小；D.黑客利用安全漏洞的速度越来越快

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

8

2 分

扫描器是一种通过收集系统的信息来自动检测远程或本地主机安全弱点的程序。以下关于扫描器的说法正确的是（　）

A.就攻击角度来说，与端口扫描器相比，漏洞扫描器更为直接；B.扫描器并不是直接实施攻击的工具，它仅仅能帮助网络入侵者发现目标系统的某些内在的弱点；C.按照扫描的目的来分类，扫描器可以分为端口扫描器和漏洞扫描器；D.以上都对

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

9

2 分

端口扫描器可以扫描常用的端口和指定的端口是否开放，（　）是最常用的端口扫描工具

A.ISS；B.SATAN；C.Nmap；D.NESSUS

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

10

2 分

高级持续性威胁 APT 攻击利用先进的攻击手段对特定目标进行长期持续性网络攻击的攻击形式，它是一种以（　）目的为前提的特定攻击

A.公共安全；B.商业或者政治；C.安全测试；D.入侵检测

正确答案是：B　你的答案是：D　　此题得分：0

展开解析

11

2 分

以下哪项属于入侵防御系统的入侵防护技术？

A.恶意站点检测；B.Web 分类过滤；C.专业抗 DDoS；D.以上都是

正确答案是：D　你的答案是：D　此题得分：2

展开解析

12

2 分

以下选项中不属于渗透测试流程的是（　）

A.信息收集；B.探测系统安全漏洞；C.横向渗透；D.清除痕迹

正确答案是：C　你的答案是：C　此题得分：2

展开解析

13

2 分

入侵防御系统（IPS）一般布于防火墙和外来网络的设备之间，依靠对数据包的检测进行防御，以下选项中不属于 IPS 的主要功能的是（　）

A.实时监视和拦截攻击；B.虚拟补丁；C.保护客户端；D.实时异常告警

正确答案是：D　你的答案是：B　此题得分：0

展开解析

14

2 分

电磁泄漏是指信息系统的设备在工作时能经过地线、电源线、信号线、寄生电磁信号或谐波等辐射出去，产生电磁泄漏。电磁泄露的解决办法有（　）

A.低泄射产品；B.电磁干扰器；C.处理涉密信息的电磁屏蔽室的技术；D.以上都是

正确答案是：D　你的答案是：D　此题得分：2

展开解析

15

2 分

主机入侵防御系统（HIPS）是一种能监控你电脑中文件的运行和文件运用了其他的文件以及文件对注册表的修改，并向你报告请求允许的软件。下列属于基于主机的入侵防御系统优点的是（　）

A.软件直接安装在系统上，可以保护系统免受攻击；B.当移动系统接入受保护网络时，保护特定主机免受攻击；C.保护系统免受本地攻击；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

16

2 分

基本的入侵检测联动响应框架中，联动的基本过程是（　）、（　）、（　）

A.报警、转换、响应；B.转换、响应、报警；C.报警、响应、转换；D.转换、报警、响应

正确答案是：A　你的答案是：C　　此题得分：0

展开解析

17

2 分

以下属于木马攻击关键技术的是（　）

A.木马植入技术；B.自动加载技术；C.隐藏技术；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

18

2 分

在 TCP/IP 协议中，由于 TCP 协议提供可靠的连接服务，于是采用有保障的（　）来创建一个 TCP 连接；由于 TCP 连接是全双工的，因此每个方向都必须单独进行关闭，采用（　）来断开 TCP 连接

A.三次握手 四次挥手；B.四次握手 四次挥手；C.三次挥手 四次握手；D.三次握手 三次挥手

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

19

2 分

事件分析器接收事件信息，并对其进行分析，判断是否为入侵行为或异常现象，最后将判断的结果转变为告警信息。以下属于其分析方法的有（　）

A.模式匹配；B.统计分析；C.完整性分析；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

20

2 分

跨站脚本攻击（XSS）指利用网站漏洞从用户那里恶意盗取信息。以下属于 XSS 危害的是（　）

A.会话劫持和 cookie 信息盗取；B.突破外网内网不同安全设置；C.屏蔽和伪造页面信息；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

21

2 分

现在的网站存在着两种类型，分别是（　）和（　）

A.静态网站、动态网站；B.展示型网站、营销型网站；C.响应式网站与非响应式网站；D.以上都不是

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

22

2 分

SQL 注入攻击是黑客对数据库进行攻击的常用手段之一。以下属于 SQL 注入攻击特点的是（　）

A.广泛性；B.技术难度不高；C.危害性大；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

23

2 分

以下选项中不属于常见的网络安全威胁的是（　）

A.SARS 病毒；B.拒绝服务；C.信息泄露；D.身份欺骗

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

24

2 分

能保障用户无法在事后否认曾经对信息进行的生成、签发、接受等行为，体现了计算机实体及信息的（　）

A.机密性；B.完整性；C.抗否认性；D.可用性

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

25

2 分

以下哪个不属于容错系统的工作方式？

A.自动侦查；B.自动切换；C.自动恢复；D.自动隔离

正确答案是：D　你的答案是：B　　此题得分：0

展开解析

26

2 分

下列属于容错系统设计策略的是（　）

A.冗余性；B.预防性；C.恢复性；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

27

2 分

操作系统具有或应具有的安全功能，如存储保护、运行保护、标识与鉴别、安全审计等，体现了操作系统的（　）

A.安全性；B.保密性；C.完整性；D.可用性

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

28

2 分

根据形成安全威胁的途径来分，操作系统面临的安全威胁的有（　）

A.不合理的授权体制；B.不恰当的代码执行；C.不恰当的主体控制；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

29

2 分

BLP 模型是 1973 年提出的一种对应于军事类型安全密级分类的计算机操作系统模型，以下关于其说法正确的是（　）

A.BLP 模型是最早的一种安全模型，也是最有名的多级安全策略模型；B.BLP 模型是一个严格形式化的模型，并给出了形式化的证明；C.既有自主访问控制，又有强制访问控制；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

30

2 分

设备的防盗、防毁、防电磁信息辐射泄露、防止线路截获、抗电磁干扰及电源保护等体现了计算机系统中物理安全的（　）

A.场地安全；B.设备安全；C.媒体安全；D.信息安全

正确答案是：B　你的答案是：A　　此题得分：0

展开解析

31

2 分

PGP 是美国的 PhilZimmermann 研究出来的一个基于（　）体系的邮件加密软件

A.RSA 私钥加密；B.DSA 私钥加密；C.RSA 公钥加密；D.DSA 公钥加密

正确答案是：C　你的答案是：D　　此题得分：0

展开解析

32

2 分

TCP 是面向连接的协议，提供可靠的、全双工的、面向字节流的端到端服务，它使用（ ）次握手来建立连接，大大增强了可靠性。

A.一；B.二；C.三；D.四

正确答案是：C　你的答案是：C　此题得分：2

展开解析

33

2 分

电子邮件系统的主要功能包括撰写、显示、处理、传输和报告五项基本功能。其中（　）（　）、处理是用户代理至少应当具有的三个功能，而传输和（　）是邮件服务器应该具备的功能。

A.报告 撰写 显示；B.撰写 显示 报告；C.撰写 报告 显示；D.显示 报告 撰写

正确答案是：B　你的答案是：B　此题得分：2

展开解析

34

2 分

（　）是保证 TCP 可靠性的重要措施。TCP 每发送一个报文段，就对这个报文段设置一次计时器，只要计时器设置的重传时间到但还没有收到确认，就要重传这一报文段。

A.拥塞控制；B.差错检验；C.重传机制；D.透明传输

正确答案是：C　你的答案是：C　此题得分：2

展开解析

35

2 分

域名系统 DNS 是一个联名分布式数据库系统，它的功能是把 Internet 中的主机域名解析为对应的（　）

A.MAC 地址；B.端口号；C.IP 地址；D.socket 地址

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

36

2 分

SMTP 的工作方式是客户服务器的方式，负责发送邮件的 SMTP 进程就是 SMTP 客户，负责接收邮件的 SMTP 进程是 SMTP 服务器，它在传输层使用（　）协议进行传输。

A.UDP；B.TCP；C.IP；D.ARP

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

37

2 分

FTP 的功能是实现在客户机（本地机）和 FTP 服务器（远程计算机）之间文件的传送，通常把文件从 FTP 服务器上拷到本地计算机，称为（　）；把本地计算机的文件送到 FTP 服务器上，称为上载。

A.下载；B.请求；C.浏览；D.拷贝

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

38

2 分

TFTP 是 TrivialFTP 的缩写，常被称为简单文件传送协议，它采用客户/服务器方式，传输层使用（　）数据报，因此 TFTP 需要有自己的差错改正措施。

A.TCP；B.ip；C.ARP；D.UDP

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

39

2 分

Telnet 的目的是提供一个相对通用的、双向的通信机制，使得用户能够登录进入远程主机系统，把自己仿真成远程主机的终端。因此，Telnet 有时也被称为（　）协议。

A.简单邮件传送协议；B.虚拟终端；C.简单网络管理协议；D.内部网关协议

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

40

2 分

WWW 称为（　），有时简写为 Web。严格的说，WWW 并不是一种网络，而是一种信息组织方式。

A.互联网；B.互连网；C.万维网；D.因特网

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

41

2 分

应用层协议定义了运行在不同端系统上的应用程序进程如何相互传递报文。下列不属于应用层协议的是（　）

A.TCP；B.HTTP；C.Telnet；D.FTP

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

42

2 分

在以计算机文件为基础的现代事物处理中，应采用电子形式的签名，即（　）

A.手签；B.数字签名；C.印章；D.手印

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

43

2 分

认证和加密的区别在于：（　）用于确保数据的保密性，阻止对手的被动攻击，如截取，窃听等；而（　）用以确保报文发送者和接收者的真实性以及报文的完整性，阻止对手的主动攻击，如冒充、篡改、重播等

A.加密 认证；B.认证 加密；C.加密 加密；D.认证 认证

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

44

2 分

Internet 中有数百万台以上的主机和路由器，IP 地址可以确切的标识它们。IP 地址的划分经过了三个阶段：（　）；（　）；（　）

A.分类的 IP 地址 无分类编址 子网的划分；B.分类的 IP 地址 子网的划分 无分类编址；C.无分类编址 子网的划分 分类的 IP 地址；D.无分类编址 分类的 IP 地址 子网的划分

正确答案是：B　你的答案是：D　　此题得分：0

展开解析

45

2 分

由于 Internet 规模太大，所以常把它划分成许多较小的自制系统 AS。通常把自制系统内部的路由协议称为（　），自制系统之间的协议称为（　）

A.内部网关协议 外部网关协议；B.内部网关协议 相邻网关协议；C.外部网关协议 内部网关协议；D.相邻网关协议 外部网关协议

正确答案是：A　你的答案是：B　　此题得分：0

展开解析

46

2 分

网络中的一个机器具有逻辑地址和物理地址两种地址，地址解析协议 ARP 是将（　）地址转换为（　）地址

A.逻辑 物理；B.物理 逻辑；C.硬件 软件；D.软件 硬件

正确答案是：A　你的答案是：B　　此题得分：0

展开解析

47

2 分

TCP 和 UDP 是 Internet 传输层的两个协议。以下关于它们的说法错误的是（　）

A.TCP 是面向连接的协议；B.TCP 提供可靠的、全双工的、面向字节流的端到端服务；C.UDP 是面向连接的协议；D.UDP 提供数据报服务

正确答案是：C　你的答案是：A　　此题得分：0

展开解析

48

2 分

建立网络安全保护措施的目的是确保经过网络传输和交换的数据不会发生增加、修改、丢失和泄露等。数据是正确的、真实的、未被篡改的、完整无缺的体现数据的（　）

A.秘密性；B.可用性；C.完整性；D.安全性

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

49

2 分

信息系统设备的安全是信息系统安全的首要问题。设备能在一定时间内正常执行任务的概率体现设备的（　）

A.可靠性；B.可用性；C.稳定性；D.安全性

正确答案是：A　你的答案是：B　　此题得分：0

展开解析

50

2 分

数据安全本质上是一种静态的安全，而行为安全是一种动态安全。当行为的过程出现偏离预期时，能够发现、控制或纠正体现了行为的（　）

A.秘密性；B.完整性；C.可靠性；D.可控性

正确答案是：D　你的答案是：D　　此题得分：2

第七章

1

2 分

信息内容安全是信息安全在政治、法律、道德层次上的要求。信息内容安全领域的研究内容主要有（　）

A.信息内容的获取、分析与识别；B.信息内容的管理和控制；C.信息内容安全的法律保障；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

2

2 分

信息对抗是为消弱、破坏对方电子信息设备和信息的使用效能，保障己方电子信息设备和信息正常发挥效能而采取的综合技术措施，其主要研究内容有（　）

A.通信对抗；B.雷达对抗；C.计算机网络对抗；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

3

2 分

访问控制理论是网络空间安全学科所特有的理论基础。以下属于访问控制的有（　）

A.密码技术；B.身份认证；C.信息隐藏；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

4

2 分

风险评估的方法有很多种，概括起来可分为三大类：定量的风险评估方法、定性的风险评估方法、定性与定量相结合的评估方法。运用数量指标来对风险进行评估是（　）的评估方法

A.定性；B.定量；C.定性与定量相结合；D.以上都不是

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

5

2 分

Internet 控制报文协议 ICMP 允许路由器报告差错情况和提供有关异常情况的报告，它的英文全称是（　）。

A.Internet Control Messag Protocol；B.Internet Control Message Protocol；C.Internet Contract Message Protocol；D.Internet Control Message Prototype

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

6

2 分

密码学作为信息安全的关键技术，其安全目标主要包括三个非常重要的方面：保密性、完整性和可用性。（　）是确保信息仅被合法用户访问，二不被泄露给非授权的用户、实体或过程，或供其利用的特性。

A.保密性；B.完整性；C.可用性；D.以上都不是

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

7

2 分

密码学作为信息安全的关键技术，其安全目标主要包括三个非常重要的方面：保密性、完整性和可用性。（　）是指所有资源只能由授权方式以授权的方式进行修改，即信息未经授权不能进行改变的特性。

A.保密性；B.完整性；C.可用性；D.以上都不是

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

8

2 分

消息认证码 MAC 是消息内容和秘密钥的公开函数，其英文全称是（　）。

A.Message Authentication Code；B.Messag Authentication Code；C.Message Authentication Date；D.Messag Authentication Code

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

9

2 分

计算机网络的各层及其协议的集合，也就是这个计算机网络及其部件所应完成的功能的精确定义，称为（　）。

A.网络协议；B.计算机网络；C.计算机网络的体系结构；D.计算机网络的标准

正确答案是：C　你的答案是：D　　此题得分：0

展开解析

10

2 分

以下关于序列密码说法不正确的是（　）

A.序列密码是单独地加密每个明文位；B.由于序列密码小而快，所以它们非常合适计算资源有限的应用；C.序列密码的加密和解密使用相同的函数；D.现实生活中序列密码的使用比分组密码更为广泛，例如 Internet 安全领域

正确答案是：D　你的答案是：C　　此题得分：0

展开解析

11

2 分

CIDR 常采用如 123.11.48.0/20 表示法，即在 IP 地址后面加一个斜线“/”，然后在“/”下方写上网络前缀所占的比特数，网络前缀所占的比特数隐含地指出 IP 地址为 123.11.48.0 的掩码是（　）

A.255.255.255.0；B.255.255.240.0；C.255.255.192.0；D.255.255.0.0

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

12

2 分

APT 高级持续性威胁攻击是一种以商业或者政治目的为前提的特定攻击，其通过一系列具有针对性的攻击行为以获取某个阻止甚至国家的重要信息，其英文全称是（　）。

A.Advanced Persistent Threat；B.Advanced Persistent Thread；C.Advanced Persist Threat；D.Advanced Persist Thread

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

13

2 分

一般 APT 攻击过程可细化为 5 个步骤：情报收集、防线突破、通道建立、横向渗透、信息收集及外传。攻击者在突破防线并控制员工电脑后，在员工电脑与入侵服务器之间开始建立命令控制通道属于哪个步骤？

A.情报收集；B.防线突破；C.通道建立；D.横向渗透

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

14

2 分

目前我国网络安全问题日益突出，以下哪些是制约我国提高网络安全防御能力的主要因素？

A.缺乏自主的计算机网络和软件核心技术；B.安全意识淡薄是网络安全的瓶颈；C.运行管理机制的缺陷和不足制约了安全防范的力度；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

15

2 分

安全设备是指企业在生产经营活动中，将危险、有害因素控制在安全范围内，以及减少、预防和消除危害所配备的装置和采取的设备，以下哪个选项不属于安全设备？

A.防火墙；B.VPN；C.IDS；D.集线器

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

16

2 分

以下哪个选项是攻击者的攻击策略？

A.信息收集；B.分析系统的安全弱点；C.模拟攻击；D.以上都是

正确答案是：D　你的答案是：D　此题得分：2

展开解析

17

2 分

木马（Trojan）也称木马病毒，是指通过特定的程序来控制另一台计算机。下列哪项不属于常见的木马类型？

A.DOS 攻击型；B.密码发送型；C.绿色安全型；D.键盘记录型

正确答案是：C　你的答案是：C　此题得分：2

展开解析

18

2 分

病毒和木马都是一种人为的程序，都属于电脑病毒。以下关于病毒和木马说法错误的是（　）

A.病毒和木马很容易区分清楚；B.病毒和木马一般可以统称为恶意程序或恶意软件；C.病毒具有一定的显性破坏性，木马更倾向于默默地窃取；D.病毒具有自传播性，即能够自我复制，而木马则不具备这一点

正确答案是：A　你的答案是：D　此题得分：0

展开解析

19

2 分

在移动互联网出现之前，针对浏览器的攻击方法中最主要的两种方式是挂马和钓鱼，以下说法正确的是（　）

A.挂马是指在某个页面中植入木马程序，导致用户在浏览该页面的时候下载木马，然后利用木马窃取用户信息或者数据；B.钓鱼页面与用户想要浏览的页面几乎一样，普通用户在不注意的情况会在钓鱼网站输入自己的用户名与密码，这样钓鱼者可以直接

获得用户信息；C.两者都是 WEB 攻击方式，不过挂马是在原有页面基础上进行，钓鱼是在新制作的假页面上进行的；D.以上都对

正确答案是：D　你的答案是：D　此题得分：2

展开解析

20

2 分

钓鱼网站通常指伪装成银行及电子商务，窃取用户提交的银行帐号、密码等私密信息的网站，其实质是内容具有（　）

A.完整性；B.机密性；C.欺骗性；D.不可否认性

正确答案是：C　你的答案是：C　此题得分：2

展开解析

21

2 分

下列哪项属于常见的 Web 攻击？

A.SQL 注入；B.跨站脚本；C.Cookie 攻击；D.以上都是

正确答案是：D　你的答案是：D　此题得分：2

展开解析

22

2 分

拒绝服务攻击 DOS 是攻击者想办法让目标机器停止提供服务，是黑客常用的攻击手段之一。下列哪项属于 DOS 攻击方式？

A.服务过载；B.信息接地；C.消息流；D.以上都是

正确答案是：D　你的答案是：D　此题得分：2

展开解析

23

2 分

计算机互联的主要目的是

A.制定网络协议；B.将计算机技术与通信技术相结合；C.集中计算；D.资源共享

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

24

2 分

INTERNET 最初创建的目的是用于

A.政治；B.经济；C.教育；D.军事

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

25

2 分

在局域网中，MAC 指的是

A.逻辑链路控制子层；B.介质访问控制子层；C.物理层；D.数据链路层

正确答案是：B　你的答案是：C　　此题得分：0

展开解析

26

2 分

相邻层间交换的数据单元称之为服务数据单元，其英文缩写是

A.SDU；B.IDU；C.PDU；D.ICI

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

27

2 分

一般来说，用户上网要通过因特网服务提供商，其英文缩写为

A.IDC；B.ICP；C.ASP；D.ISP

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

28

2 分

在以下四种传输介质中，带宽最宽、抗干扰能力最强的是

A.双绞线；B.无线信道；C.同轴电缆；D.光纤

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

29

2 分

IP 协议是无连接的，其信息传输方式是

A.点对点；B.数据报；C.广播；D.虚电路

正确答案是：B　你的答案是：C　　此题得分：0

展开解析

30

2 分

路由选择协议为路由器提供网络最佳路径所需要的相互共享的路由信息。路由选择协议位于

A.物理层；B.数据链路层；C.网络层；D.应用层

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

31

2 分

世界上第一个计算机网络是

A.ARPANET；B.INTERNET；C.CHINANET；D.CERNET

正确答案是：A　你的答案是：B　　此题得分：0

展开解析

32

2 分

在互联网设备中，工作在物理层的互联设备是

A.集线器；B.网桥；C.路由器；D.交换机

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

33

2 分

数据链路层是 OSI 参考模型中的第二层，介乎于物理层和网络层之间。下列不属于数据链路层功能的是

A.帧定界功能；B.电路管理功能；C.差错检测功能；D.链路管理功能

正确答案是：B　你的答案是：A　　此题得分：0

展开解析

34

2 分

路由选择协议为路由器提供最佳路径所需要的相互共享的路由信息，下列不属于路由选择协议的是

A.RIP；B.ICMP；C.BGP；D.OSPF

正确答案是：B　你的答案是：A　　此题得分：0

展开解析

35

2 分

通信系统必须具备的三个基本要素是

A.终端、电缆、计算机；B.信号发生器、通信线路、信号接收设备；C.信源、通信媒体、信宿；D.终端、通信设施、接收设备

正确答案是：C　你的答案是：D　　此题得分：0

展开解析

36

2 分

UDP 协议全称是用户数据报协议，在网络中它与 TCP 协议一样用于处理数据包，是一种无连接的协议，UDP 协议工作在

A.应用层；B.传输层；C.网络互联层；D.网络接口层

正确答案是：B　你的答案是：C　　此题得分：0

展开解析

37

2 分

下面协议中，用于电子邮件 Email 传输控制的是

A.SNMP；B.SMTP；C.HTTP；D.HTML

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

38

2 分

在同一个信道上的同一时刻，能够进行双向数据传送的通信方式是

A.单工；B.半双工；C.全双工；D.以上三种均不是

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

39

2 分

在 OSI 中，为实现有效可靠的数据传输，必须对传输操作进行严格的控制和管理，完成这项工作的层次是

A.物理层；B.数据链路层；C.网络层；D.运输层

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

40

2 分

帧中继是在用户--网络接口之间提供用户信息流的双向传送，并保持信息顺序不变的一种承载业务，帧中继网是什么类型的网络？

A.广域网；B.局域网；C.ATM 网；D.以太网

正确答案是：A　你的答案是：C　　此题得分：0

展开解析

41

2 分

提供 FTP 服务的默认 TCP 端口号是多少？

A.80；B.25；C.23；D.21

正确答案是：D　你的答案是：A　　此题得分：0

展开解析

42

2 分

以下关于 100BASE-T 的描述中错误的是

A.数据传输速率为 100Mbit/S ；B.信号类型为基带信号；C.采用 5 类 UTP，其最大传输距离为 185M；D.支持共享式和交换式两种组网方式

正确答案是：C　你的答案是：D　　此题得分：0

展开解析

43

2 分

在以下四个 www 网址中，哪一个网址不符合 www 网址书写规则？

A.www.163.com；B.www.nk.cn.edu；C.www.863.org.cn；D.www.tj.net.jp

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

44

2 分

Internet 上的各种不同网络及不同类型的计算机进行相互通信的基础是

A.HTTP；B.IPX/SPX；C.X.25；D.TCP/IP

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

45

2 分

集线器的主要功能是对接收到的信号进行再生整形放大，以扩大网络的传输距离，同时把所有节点集中在以它为中心的节点上。下面关于集线器的描述正确的是

A.集线器不能延伸网络可操作的距离；B.集线器不能过滤网络流量；C.集线器不能成为中心节点；D.集线器不能放大变弱的信号

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

46

2 分

DHCP 客户机申请 IP 地址租约时首先发送的信息是

A.DHCP discover；B.DHCP offer ；C.DHCP request ；D.DHCP positive

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

47

2 分

传染性是计算机病毒的本质属性，可以根据寄生部位或传染对象对病毒进行分类。根据计算机病毒寄生方式划分，不属于病毒类型的是（　）

A.嵌入型病毒；B.引导性病毒；C.文件型病毒；D.复合型病毒

正确答案是：A　你的答案是：C　　此题得分：0

展开解析

48

2 分

系统漏洞可以被不法者利用，通过网络植入木马、病毒等方式来攻击或控制整个电脑，窃取电脑中的重要资料和信息，甚至破坏系统。以下关于漏洞的描述中不正确的是（　）

A.通过安全软件扫描就一定能发现所有漏洞；B.漏洞是一种系统的状态或条件，一般表现为不足或者缺陷；C.漏洞有可能会影响大范围的软硬件设备；D.漏洞通常由不正确的系统设计如错误逻辑等造成

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

49

2 分

无线广域网是把物理距离极为分散的局域网连接起来的通信方式。无线广域网进行数据通信需要使用（　）

A.公共数据网；B.光纤；C.通信卫星；D.电话线

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

50

2 分

无线局域网是相当便利的数据传输系统，硬件设备包含无线网卡，无线 AP 和无线天线，其中 AP 的作用是（　）

A.无线接入；B.路由选择；C.业务管理；D.用户认证

正确答案是：A　你的答案是：A　　此题得分：2

第八章

1

2 分

在计算机系统中，无论是在系统内部或者应用程序中，都会在逻辑或者程序上或多或少存在着漏洞，关于漏洞的定义,下列描述中不正确的是（　）

A.漏洞是计算机系统的硬件、软件、协议在系统设计、具体实现、系统配置或安全策略上存在的缺陷和不足；B.冯·诺依曼认为计算机系统的缺陷只能是天生的,不可能在使用和发展的过程中产生；C.每个平台无论是硬件还是软件都可能存在漏洞；D.漏洞本身并不会导致损害，但它可能被攻击者利用,从而获得计算机系统的额外权限

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

2

2 分

下列技术中，不属于网络隔离技术的是（）

A.网络蜜罐；B.IDS；C.VLAN 划分；D.防火墙

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

3

2 分

路由器、防火墙、交换机等网络设备是整个互联网世界的联系纽带，占据着非常重要的地位，是计算机网络的节点。网络设备的安全性尤为重要，目前来看各个国家和地区针

对 PC 端和移动端的安全都提到了非常重视的高度。下列漏洞中不属于网络设备漏洞的是（ ）

A.交换机设备漏洞；B.Windows 系统漏洞；C.防火墙漏洞；D.网络摄像头漏洞

正确答案是：B 你的答案是：C 此题得分：0

展开解析

4

2 分

主流应用的无线网络分为 GPRS 手机无线网络上网和无线局域网两种方式。GPRS 手机上网方式，是一种借助移动电话网络接入 Internet 的无线上网方式，因此只要你所在城市开通了 GPRS 上网业务，你在任何一个角落都可以通过手机来上网。无线局域网的标准是（ ）

A.802.3u；B.802.11；C.802.3；D.802.2

正确答案是：B 你的答案是：B 此题得分：2

展开解析

5

2 分

体域网是附着在人体身上的一种网络，由一套小巧可移动、具有通信功能的传感器和一个身体主站(或称 BAN 协调器)组成。每一传感器既可佩戴在身上，也可植入体内。无线体域网最典型的应用是（ ）

A.危险场合应用；B.校园网应用；C.医疗健康应用；D.日常生活应用

正确答案是：C 你的答案是：A 此题得分：0

展开解析

6

2 分

当用户在使用服务器系统数据库时，对数据库的安全性能要求是十分严格的，但数据库仍有可能会出现漏洞，关于数据库漏洞成因，以下描述中不正确的是（　）

A.数据库管理不当；B.用户登录到数据库；C.数据库权限管理不够严格；D.数据库本身存在安全漏洞

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

7

2 分

在使用数据库时，不要对规模小的数据表建立索引，数据量超过 300 的表应该有索引；对于规模小的数据表建立索引，不仅不会提高功能，相反使用索引查找可能比简单的全表扫描还要慢而且建索引还会占用一部分的存储空间。数据库扫描的任务中不包括（　）

A.分析内部不安全配置，防止越权访问；B.用户授权状况扫描，便于找到宽泛权限账户；C.彻底删除敏感、保密数据；D.弱口令猜解，发现不安全的口令设置

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

8

2 分

"白盒"法是穷举路径测试。在使用这一方案时，测试者必须检查程序的内部结构，从检查程序的逻辑着手，得出测试数据。关于白盒测试，以下描述中不正确的是（　）

A.白盒测试技术可应用于数据库漏洞扫描；B.白盒检测方法的前提是已知数据库用户名和口令；C.白盒检测方法方法的优势是：命中率高、可扩展性高；D.白盒检测方法完全不能扫描出数据库的低安全配置和弱口令

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

9

2 分

IEEE 802.11 是无线局域网通用的标准，它是由 IEEE 所定义的无线网络通信的标准。其中 IEEE 802.11 标准定义的 Ad hoc 网络是（　）

A.一种需要 AP 支持的无线局域网络；B.一种不需要 AP 支持的点对点无线网络；C.一种采用特殊协议的有线网络；D.一种高速骨干数据网络

正确答案是：B　你的答案是：D　　此题得分：0

展开解析

10

2 分

BYOD（Bring Your Own Device）指携带自己的设备办公，在机场、酒店、咖啡厅等，登录公司邮箱、在线办公系统，不受时间、地点、设备、人员、网络环境的限制。以下哪一项不属于 BYOD 设备？

A.个人笔记本电脑；B.手机；C.电视；D.平板电脑

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

11

2 分

手机杀毒软件能够有效的清除手机应用的漏洞或挂载在软件上的病毒，对手机的安全防护起到十分重要的作用，以下哪个不是安装手机杀毒软件的目的？

A.提高手机的安全性；B.查杀手机病毒；C.防止骚扰电话；D.扩大手机的硬盘空间

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

12

2 分

国家计算机病毒应急处理中心近期通过对互联网监测，发现有许多违法有害移动应用存在于移动应用发布平台中，其主要危害涉及隐私窃取和流氓行为两类。移动应用流氓行为的主要表现是（　）

A.自动弹出广告信息；B.利用蓝牙、红外、无线网络通信技术向其他移动终端发送恶意代码；C.下载恶意代码、感染其他文件；D.由控制端主动发出指令进行远程控制

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

13

2 分

数据库漏洞扫描将数据库的安全自查由低效的人工方式提升到高效准确的自动检查方式，并以报表的方式呈现给用户，适时提出修补方法和安全实施策略。关于数据库漏洞处理，以下描述中不正确的是（　）

A.数据库系统的安全信息员应对数据库定期进行安全扫描；B.数据库系统的安全信息员需要时刻关注官方发布的信息，及时更新数据库系统；C.数据库系统的安全信息员应重点关注数据库漏洞，完全不用更新数据库所在的应用系统；D.数据库系统的安全信息员应注意防范 SQL 注入

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

14

2 分

数据库安全防护是防止数据意外丢失和不一致数据的产生，以及当数据库遭受破坏后迅速恢复正常。关于数据库安全防护体系，以下描述中不正确的是（　）

A.数据库安全防护体系通过事前预警、事中防护和事后审计的方式，全方位地保护数据安全；B.数据库安全防护体系中数据库监控扫描系统可以对数据库系统进行全自动的监控和扫描，及早发现数据库中已有的漏洞，并提供修复指示；C.数据库防火墙系统通过权限控制和加密存储，用户只需要普通权限就可以对核心数据进行加密处理，设置访问权限；D.数据库审计系统对数据库的所有操作进行审计，实时记录、分析、识别和确定风险，提供审计报告

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

15

2 分

对于设备的安全配置漏洞扫描是指基于漏洞数据库，通过扫描等手段对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利用漏洞的一种安全检测（渗透攻击）行为。安全配置漏洞扫描不包括（　）

A.检测软件是否及时更新；B.检测是否使用或安装了不必要的功能；C.检测用户文件是否保存；D.检测错误处理机制是否防止堆栈跟踪

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

16

2 分

电子邮件安全协议提供了身份认证和数据加密服务，（　）属于电子邮件安全协议

A.HTTP；B.HTTPS；C.MIME；D.S/MIME

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

17

2 分

局域网是将各种计算机、外部设备、数据库等互相连接起来组成的计算机通信网，下列关于局域网的选项中，不正确的是（　）

A.办公网络可称为局域网；B.局域网的一个重要用途是用作城市骨干网；C.局域网可以实现文件管理、应用软件共享等功能；D.局域网的全称为 Local Area Network，LAN

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

18

2 分

下列基本原则中，属于数据库访问控制需满足的安全原则有（ ）

A.木桶原则；B.最小特权原则；C.任意共享原则；D.开放系统原则

正确答案是：B 你的答案是：B 此题得分：2

展开解析

19

2 分

APT 攻击造成的损害日益严重，通常 APT 攻击步骤为情报收集→防线突破→（ ）

A.通道建立→横向渗透→信息收集及外传；B.横向渗透→通道建立→信息收集及外传；C.通道建立→横向渗透→信息收集及外传；D.横向渗透→通道建立→信息收集及外传

正确答案是：A 你的答案是：A 此题得分：2

展开解析

20

2 分

身份验证是正确识别用户身份，合理分配用户权限的保障，VPN 客户端所支持的身份验证不包括（ ）

A.共享的保密口令；B.3DES 协议；C.RADIUS 身份验证；D.数字证书

正确答案是：B 你的答案是： 此题得分：

展开解析

21

2 分

UNIX 系统的（ ）可以监控系统中发生的事件，以保证安全机制正确工作并及时对系统异常报警提示

A.文件系统机制；B.密码机制；C.存取机制；D.审计机制

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

22

2 分

（　）游戏是计算机病毒的第一个雏形，体现了病毒自我复制的基本思想

A.星际大战；B.群雄争霸；C.磁芯大战；D.以上都不正确

正确答案是：C　你的答案是：D　　此题得分：0

展开解析

23

2 分

病毒的种类有很多，其中是指利用邮件服务器进行传播和破坏的病毒

A.邮件病毒；B.特洛伊木马；C.蠕虫；D.恶意代码

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

24

2 分

第一个实用的、迄今为止应用最广的公钥密码体制是（　）

A.RSA；B.DES；C.IDEA；D.AES

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

25

2 分

在电子投票中，为了实现投票者所投票内容的匿名性，最有可能使用的签名方案（　）

A.代理签名；B.群签名；C.多重签名；D.盲签名

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

26

2 分

在电子拍卖中，只有注册的竞拍者能够出价，未中标时需要实现竞拍者身份的匿名性，为实现这个目标，最有可能使用的签名方案是（　）

A.代理签名；B.群签名；C.多重签名；D.盲签名

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

27

2 分

数字水印技术是将一些标识信息嵌入数字媒体中的技术，下面哪个领域不是数字水印的应用领域（　）

A.版权保护；B.盗版追踪；C.保密通信；D.拷贝保护

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

28

2 分

在“运行”对话框中输入（　）可以运行注册表编辑器

A.CMD；B.REGEDIT；C.PING；D.Calc

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

29

2 分

防火墙是一种位于内部网络与外部网络之间的安全防护系统，以下不属于防火墙的组成要素的是（　）

A.安全策略技术手段；B.内部网；C.外部网；D.加密措施

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

30

2 分

防火墙是一种位于内部网络与外部网络之间的安全防护系统，以下对防火墙的描述正确的是（　）

A.防火墙能防范任何新的网络安全问题；B.防火墙能防范因配置不当引起的安全问题；C.防火墙不能完全阻止病毒的传播；D.防火墙能完全防止来自内部网的攻击

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

31

2 分

关于屏蔽子网防火墙体系结构中内部路由器的说法，错误的是（　）

A.保护内部网络的安全；B.保护外部网络的安全；C.即使堡垒主机被攻占，也可以保护内部网络；D.应按“最小特权原则”设计堡垒主机与内部网的通信策略

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

32

2 分

防火墙从诞生开始，已经历了四个发展阶段，其中不包括（　）

A.基于路由器的防火墙；B.用户化的防火墙工具套件；C.个人智能防火墙；D.具有安全操作系统的防火墙

正确答案是：C　你的答案是：D　此题得分：0

展开解析

33

2 分

入侵检测系统的分类方法很多，根据（　）可将入侵检测系统分为异常入侵检测和误用入侵检测

A.检测方法；B.数据来源；C.体系结构；D.传输方式

正确答案是：A　你的答案是：A　此题得分：2

展开解析

34

2 分

在网络攻击中，修改完整性检测标签能够实现（　）

A.攻击痕迹清除；B.攻击实施；C.信息收集；D.以上都不正确

正确答案是：A　你的答案是：D　此题得分：0

展开解析

35

2 分

SSL 是为网络通信提供安全及数据完整性的一种安全协议，其在哪一层对网络连接进行加密？

A.应用层；B.物理层；C.传输层；D.以上都不正确

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

36

2 分

访问控制是根据用户身份分配对应的用户权限的一种技术，以下不属于访问控制三个要素的是（　）

A.主体；B.客体；C.控制策略；D.中间人

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

37

2 分

访问控制是根据用户身份限制其对某些信息的访问，或限制使用某些功能的一种技术，以下不属于访问控制主要内容的是（　）

A.认证；B.控制策略实现；C.审计；D.查询

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

38

2 分

网关和路由器都是在网络中用来连接不同子网主机的硬件设施，其区别在于（　）

A.网关有数据包转发功能而路由器没有；B.路由器有数据包转发功能而网关没有；C.路由器有路由选择功能而网关没有；D.网关有路由的功能而路由器没有

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

39

2 分

根据防火墙使用的技术，可将防火墙分为（　）

A.包过滤型防火墙和应用代理型防火墙；B.软件防火墙，硬件防火墙和芯片级防火墙；C.单一主机防火墙、路由器集成式防火墙和分布式防火墙；D.边界防火墙、个人防火墙和混合防火墙

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

40

2 分

混合型病毒综合的是以下哪两种病毒寄生方式？

A.引导型病毒和文件型病毒；B.引导型病毒和嵌入型病毒；C.文件型病毒和嵌入型病毒；D.以上都不正确

正确答案是：A　你的答案是：C　　此题得分：0

展开解析

41

2 分

入侵检测是一种能够及时发现并报告系统中未授权或异常现象的技术，下列哪项不属于入侵检测技术？

A.基于统计方法的入侵检测技术；B.基于神经网络的入侵检测技术；C.基于专家系统的入侵检测技术；D.基于交通灯管理办法的入侵检测技术

正确答案是：D　你的答案是：D　此题得分：2

展开解析

42

2 分

HIDS（Host-based Intrusion Detection System）是基于主机型入侵检测系统，下列哪项属于 HIDS 的缺点？

A.如果主机数目过多，代价过大；B.能监控网络上的情况；C.审计内容不全面；D.不能适用于加密及交换环境

正确答案是：A　你的答案是：A　此题得分：2

展开解析

43

2 分

VPN 是指利用密码技术和访问控制技术在公共网络中建立的专用通信网络，以下不属于阻碍 VPN 发展的原因是（　）

A.IPsec 实现的互操作性的缺乏；B.当前 Qos 标准的缺乏；C.当前密码协议的缺乏；D.Internet 基础设施仍然在很大程度上将重点放在提供网络互联，而不是提供互联外的服务

正确答案是：C　你的答案是：D　此题得分：0

展开解析

44

2 分

VPN 中的隧道技术（Tunneling）是一种在网络之间传递数据的方式，一般隧道技术在以下哪层使用？

A.网络层；B.物理层；C.传输层；D.应用层

正确答案是：A　你的答案是：A　此题得分：2

展开解析

45

2 分

SA（Security Associations，安全联盟）是在为通信双方协商决定使用的算法和密钥而建立的，以下哪项不能确定 SA？

A.目的 IP 地址；B.安全协议标识符；C.SPI（Security Parameter Index，安全参数索引）；D.源 IP 地址

正确答案是：D　你的答案是：B　　此题得分：0

展开解析

46

2 分

隧道协议都是由传输的载体、不同的封装格式以及用户数据包组成的，链路层隧道技术不包括以下哪个协议？

A.PPTP；B.L2F；C.IPsec；D.L2TP

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

47

2 分

IPSec（Internet Protocol Security）提供主动的保护以确保在　Internet 协议　(IP) 网络上进行保密而安全的通讯，下列哪项安全服务是 IPSec 不提供的？

A.数据机密性；B.数据完整性；C.防重放攻击；D.渗透测试

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

48

2 分

UNIX/LINUX 安全模块是一种轻量级通用访问控制框架，以下模块中不属于 UNIX/LINUX 安全模块的是？

A.SELinux；B.DTE Linux；C.openwall；D.terminal

正确答案是：D　你的答案是：C　　此题得分：0

展开解析

49

2 分

路由器在其端口根据特定协议区分包和限制包的能力被称为包过滤（Packet Filtering）技术，包过滤技术需要处理的部分不包括哪个？

A.IP 源地址和目的地址；B.TCP 源端口和目的端口；C.TTL 字段；D.TCP 报头的 ACK 位

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

50

2 分

Sniffer 是常用的网络流量监控工具，用 Sniffer 进行流量监控时，目标机的网卡设置为（　）

A.单播模式；B.组播模式；C.广播模式；D.混杂模式

正确答案是：D　你的答案是：C　　此题得分：0

第九章

1

2 分

网络钓鱼欺骗是社会工程学的一种方式，下列关于社会工程学的说法中错误的是（ ）

A.社会工程学利用了人性的弱点；B.社会工程学需要结合常识；C.社会工程学的目的是获取秘密信息；D.谎言越多，社会工程学的欺骗效果越好

正确答案是：D 你的答案是：D 此题得分：2

展开解析

2

2 分

根据恶意代码特征对恶意代码前缀命名，Worm.Sasser 病毒属于（ ）

A.引导区病毒；B.蠕虫病毒；C.木马病毒；D.宏病毒

正确答案是：B 你的答案是：B 此题得分：2

展开解析

3

2 分

安全策略通常指在安全区域内用于实施安全相关活动的一套规则，在实施过程中需要遵循最小特权原则，以下对该原则描述正确的是（ ）

A.主体执行操作时，按照主体所需权力的最小化原则分配给主体权力；B.主体执行任务时，按照主体所需要知道的信息最小化的原则分配给主体权力；C.主体和客体间的数据流向和权限控制按照安全级别划分；D.以上都不正确

正确答案是：A 你的答案是：A 此题得分：2

展开解析

4

2 分

修改 Widows 系统的密码策略，使得新设置的密码不与上次设置的密码重复，应设置强制密码历史值为（　）

A.0；B.1；C.NULL；D.∞

正确答案是：B　你的答案是：B　此题得分：2

展开解析

5

2 分

虚拟机的大量创建，致使回收计算资源或清理虚拟机的工作越来越困难的现象被称为以下哪个？

A.虚拟机蔓延；B.虚拟机逃逸；C.虚拟机跳跃；D.虚拟机移植

正确答案是：A　你的答案是：A　此题得分：2

展开解析

6

2 分

入侵检测系统是一种监控数据包并作出处理措施的网络安全设备。下列哪项不属于入侵检测系统构件？

A.事件产生器；B.事件分析器；C.密码锁；D.事件数据库

正确答案是：C　你的答案是：C　此题得分：2

展开解析

7

2 分

按实现技术分类，防火墙不包括（　）

A.包过滤防火墙；B.屏蔽主机防火墙；C.代理防火墙；D.状态检测防火墙

正确答案是：B　你的答案是：C　此题得分：0

展开解析

8

2 分

关于访问控制列表，下列说法中错误的是（　）

A.访问控制列表是一系列基于 InternetIP 地址、服务端口的允许和拒绝条件的集合；B.由访问控制列表来实现包过滤设备的过滤策略；C.对于进入的数据包，必须按顺序取出访问控制列表中的所有规则进行匹配；D.访问控制列表包括标准访问控制列表和扩展访问控制列表

正确答案是：C　你的答案是：C　此题得分：2

展开解析

9

2 分

按照授权性质，下列对网络安全策略的分类正确的是（　）

A.基于身份的安全策略；基于规则的安全策略；基于角色的安全策略；B.基于文件的安全策略；基于规则的安全策略；基于角色的安全策略；C.基于身份的安全策略；基于文件的安全策略；基于角色的安全策略；D.基于身份的安全策略；基于规则的安全策略；基于文件的安全策略

正确答案是：A　你的答案是：D　此题得分：0

展开解析

10

2 分

关于风险分析方法，下列说法不正确的是（　）

A.定性分析使用风险计算来预测经济损失的程度以及每种威胁发生的可能性；B.定量风险分析不基于个人直觉；C.在进行定量分析时，最常使用的公式为单一损失预期和年度损失预期；D.真正的定量分析是不可能实现的

正确答案是：A　你的答案是：D　　此题得分：0

展开解析

11

2 分

3DES 是 DES 的扩展，执行了三次 DES，对其加密方式描述正确的是（　）

A.三次加密使用相同密钥；B.第一次和第二次加密使用相同密钥；C.第一次和第三次加密使用相同密钥；D.第二次和第三次加密使用相同密钥

正确答案是：C　你的答案是：B　　此题得分：0

展开解析

12

2 分

UNIX 系统 access( )函数用于检查指定文件的存储类型，使用参数 6 代表（　）

A.检查文件是否存在；B.检查文件是否可读；C.检查文件是否可写；D.检查文件是否可读可写执行

正确答案是：D　你的答案是：C　　此题得分：0

展开解析

13

2 分

耗尽网络可用资源是网络攻击的常见手段，在网络攻击中，一段代码的执行陷入无穷的循环，最终导致资源耗尽被称为（　）

A.死循环；B.SQL 注入；C.缓冲区溢出；D.以上都不正确

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

14

2 分

将数据的访问量不太大的数据存放在性能较低的存储设备上，经常应用于数字电视中的播出控制系统的存储方式是（　）

A.近线存储；B.离线存储；C.远线存储；D.云存储

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

15

2 分

自动磁带库属于近线存储，近线存储优点不包括

A.响应速度快；B.节省空间；C.可为网络中心存储设备提供安全备份；D.空间利用率低

正确答案是：D　你的答案是：C　　此题得分：0

展开解析

16

2 分

是业务逻辑中不可或缺的一种报表，是数据库中专门存放中间计算结果的数据表

A.预定义报表；B.自定义审计报表；C.评估报表；D.中间表

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

17

2 分

键值数据库是使用键值储存数据库的一种类型，以下不属于键值数据库特点的是？

A.无数据模式；B.复制相对简单；C.接口复杂；D.数据最终一致性

正确答案是：C　你的答案是：A　此题得分：0

展开解析

18

2 分

键值数据库系统总体架构中包含许多层次，以下不属于键值数据库架构层次的是？

A.网络连接层；B.公共服务层；C.物理存储层；D.存储引擎层

正确答案是：C　你的答案是：A　此题得分：0

展开解析

19

2 分

数据库的种类有很多，以下不属于关系数据库的是

A.Oracle；B.db2；C.sqlserver；D.php

正确答案是：D　你的答案是：D　此题得分：2

展开解析

20

2 分

syslog 协议的应用十分广泛，以下对于 syslog 的叙述错误的是？

A.syslog 是一种工业标准的协议,可用来记录设备的日志；B.它分为客户端和服务器端；C.Unix/Linux 系统中的大部分日志都是通过一种叫做 Syslog 的机制产生和维护的；D.它是一种标准的 UDP 协议

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

21

2 分

路由汇聚是把小的子网汇聚成大的网络，将 172.2.193.0/24/、172.2.194.0/24、172.2.196.0/24、172.2.198.0/24 子网进行路由汇聚后的网络地址是

A.172.2.192.0/21；B.172.2.198.0/21；C.172.2.192.0/24；D.172.2.198.0/24

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

22

2 分

Hash 函数可提供报文认证服务，其特性不包括（）

A.单向性；B.双向性；C.强碰撞性；D.弱碰撞性

正确答案是：B　你的答案是：A　　此题得分：0

展开解析

23

2 分

依据《中华人民共和国标准法》将标准级别划分为 4 个层次，不包括（　）

A.国际标准；B.国家标准；C.行业标准；D.地方标准

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

24

2 分

IP 地址为 192.168.72.5，子网掩码是 255.255.224.0，则网络地址为（　）

A.192.168.100.0；B.192.168.100.255；C.192.168.64.0；D.192.168.64.255

正确答案是：C　你的答案是：B　　此题得分：0

展开解析

25

2 分

不同 Internet 协议工作在不同层次，下列协议中工作在传输层的协议是（　）

A.ARP；B.IP；C.HTTP；D.UDP

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

26

2 分

根据用途不同，IP 地址可划分为公共地址和私有地址。192.168.22.78 可用于（　）

A.公共网络；B.私有网络；C.两者都可；D.两者都不

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

27

2 分

冒充域名服务器，把查询的 IP 地址设为攻击者的 IP 地址，属于以下哪种网络欺骗方式？

A.ARP 欺骗；B.IP 欺骗；C.DNS 欺骗；D.手工欺骗

正确答案是：C　你的答案是：B　　此题得分：0

展开解析

28

2 分

关于无线网路安全方案的设计策略，下列叙述不正确的是（　）

A.在设计无线网络的安全方案时需要考虑用户客户端的移动性需求。；B.为了保障无线网络的安全，可以忽略网络效率以保障系统的安全性。；C.在设计无线网络的安全方案时，需要分析网络和系统中的信任模型明确方案中涉及的链路的信任程度。；D.由于无线网络是动态的网络，无线网络的安全方案需要动态调整，以保障无线网络的安全性。

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

29

2 分

某公司为防止信息泄露，停止运行，这属于风险处理中的风险（　）

A.规避；B.缓解；C.转移；D.接受

正确答案是：A　你的答案是：B　　此题得分：0

展开解析

30

2 分

PDR 模型的全称是（　）

A.防护-检测-响应；B.预测-依赖-响应；C.预测-检测-恢复；D.防护-依赖-恢复

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

31

2 分

关于 VPN 的内容和特点，以下描述不正确的是（　）

A.VPN 是一个临时的通信隧道；B.PPTP 可应用于 VPN；C.VPN 可应用于移动办公；
D.VPN 是 WLAN

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

32

2 分

关于数据库的四大特性 ACDI，下列说法中错误的是（　）

A.A 指原子性；B.C 指一致性；C.D 指依赖性；D.I 指隔离性

正确答案是：C　你的答案是：A　　此题得分：0

展开解析

33

2 分

不属于 TCP/IP 体系结构的层级是（　）

A.应用层；B.安全层；C.网络层；D.传输层

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

34

2 分

以下关于 TCP 协议的描述中，错误的有（　）

A.TCP 协议使用三次握手来建立连接；B.TCP 无拥塞控制；C.TCP 连接：=（socket1,socket2）=（（IP1：port1）（IP2：port2））；D.TCP 提供可靠地、全双工的、端到端的服务

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

35

2 分

下列关于 TCP 和 UDP 协议区别的描述中，错误的是（　）

A.TCP 协议发送数据之前不需要建立连接，UDP 需要建立连接；B.UDP 的主机不需要维持复杂的连接状态表；C.TCP 协议比 UDP 协议可靠性高。；D.UDP 协议比 TCP 协议的安全性差

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

36

2 分

应急响应计划是在（　）阶段建立的

A.响应；B.发布；C.实现；D.设计

正确答案是：D　你的答案是：B　　此题得分：0

展开解析

37

2 分

白盒测试是常用的软件测试方法，属于（　）

A.单元测试；B.系统测试；C.集成测试；D.确认测试

正确答案是：B　你的答案是：D　　此题得分：0

展开解析

38

2 分

一般地，IP 分配会首先把整个网络根据地域、区域，每个子区域从它的上一级区域里获取 IP 地址段，这种分配方法称为（　）分配方法

A.自顶向下；B.自下向上；C.自左向右；D.自右向左

正确答案是：A　你的答案是：B　　此题得分：0

展开解析

39

2 分

以下对访问控制中主体的描述不正确的是（　）

A.是提出请求或要求的实体；B.是某一操作动作的发起者和执行者；C.主体可以是某一用户；D.主体可以是用户启动的进程

正确答案是：B　你的答案是：D　　此题得分：0

展开解析

40

2 分

实现主体对客体的管理，由主体决定是否将客体访问权或部分访问权授予其他主体的访问控制模型是（　）

A.自主访问控制；B.强制访问控制；C.基于角色的访问控制；D.基于客体的访问控制

正确答案是：A　你的答案是：D　　此题得分：0

展开解析

41

2 分

以下对 SYN Flood 攻击的描述不正确的是（　）

A.是拒绝服务攻击常用手段之一；B.利用 TCP 三次握手机制实现攻击；C.通过发送 SYN 报文，并回应 ACK 报文，实现资源的消耗；D.SYN Flood 攻击属于 DoS 攻击的一种方式

正确答案是：C　你的答案是：D　　此题得分：0

展开解析

42

2 分

数据的完整性体现为（　）

A.数据不被泄露给非授权用户、实体或过程；B.数据源不能够否认所发送的数据；C.数据可被授权实体访问并按需求使用；D.数据未经授权不能进行更改

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

43

2 分

以下对 ECC 算法的描述不正确的是（　）

A.ECC 算法是一种对称密钥算法；B.160 位长的 ECC 的安全性相当于 1024 位的 RSA 密码；C.ECC 算法带宽要求低；D.ECC 算法计算量小

正确答案是：A　你的答案是：D　　此题得分：0

展开解析

44

2 分

在容灾备份技术中，实现磁盘到另一个磁盘数据的完全复制，数据在两处存储方式完全相同的技术是（　）

A.网络互联技术；B.存储虚拟化；C.快照技术；D.数据镜像

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

45

2 分

下列对全备份的描述正确的是（　）

A.全备份指对整个系统包括系统文件和应用数据的完全备份；B.此备份方式数据恢复所需时间较短；C.备份数据量大，备份所需时间短；D.备份数据中不存在重复数据

正确答案是：A　你的答案是：B　　此题得分：0

展开解析

46

2 分

以下对云安全管理平台的描述不正确的是（　）

A.支持一站式管理；B.支持多方位联动防护；C.支持威胁可视化；D.不同用户的访问控制权限相同

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

47

2 分

某公司数据库管理员在本月 1 号对数据库进行了完全备份，之后每日进行差异备份。因为存储不当，当月 15 号的数据被损坏。则公司数据库管理员应

A.还原当月 1 号的完全备份；B.还原当月 4 号的差异备份；C.还原当月 1 号的完全备份和 14 号的差异备份；D.还原当月 1 号的完全备份和从 2 号至 14 号所有的差异备份

正确答案是：C　你的答案是：D　　此题得分：0

展开解析

48

2 分

VPN 为数据传输和服务供应提供安全通道，下列关于 VPN 的说法中正确的是（　）

A.VPN 是用户通过公用网络建立的永久的、安全的连接；B.VPN 采用数据加密技术保护数据传输的可用性；C.VPN 提供身份认证服务；D.上述说法均正确

正确答案是：C　你的答案是：D　　此题得分：0

展开解析

49

2 分

下列关于进程和程序的说法中正确的是（　）

A.进程是动态的，程序是静态的；B.程序是系统进行资源分配和调度的一个独立单位；C.一个程序只对应一个进程；D.进程和程序的划分粒度相同

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

50

2 分

SHA1 算法输入为长度小于 264 位的报文，输出为（　）位的报文摘要

A.29；B.57；C.160；D.33

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

第十章

1

2 分

根据明文密文的划分方式不同，可将密码体制分为分组密码和序列密码。下列属于分组密码的是（　）

A.AES；B.RC4；C.ZUC；D.SM2

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

2

2 分

PKI 是一种标准的公钥密码的密钥管理平台，在 PKI 中负责签发、撤销证书的是（　）

A.CA(Certification Authority)；B.RA(Registration Authority)；C.PKC(Public Key Certificate)；D.CRL(Certificate Revocation List)

正确答案是：A　你的答案是：C　　此题得分：0

展开解析

3

2 分

IP 协议是一种无连接、不可靠的协议，（　）协议可提高 IP 层的安全性

A.PGP；B.IPSec；C.TLS；D.以上都是

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

4

2 分

（ ）存在严重的密钥分发问题，但加密以及解密的速度快

A.对称密码算法；B.非对称密码算法；C.杂凑函数；D.RSA 算法

正确答案是：A 你的答案是：C 此题得分：0

展开解析

5

2 分

X.509 是由国际电信联盟制定的数字证书标准，下列关于 X.509 的说法中错误的是（ ）

A.X.509 是基于公钥密码体制和数字签名的服务；B.X.509 定义了一种区别命名规则以确保用户名的唯一性；C.X.509 可应用于安全电子交易；D.以上说法均错误

正确答案是：B 你的答案是：D 此题得分：0

展开解析

6

2 分

为保障业务连续性，某公司要求其数据库备份时不能关闭，则适合该公司的备份方式为（ ）

A.冷备份；B.热备份；C.两者均可；D.两者都不

正确答案是：B 你的答案是：B 此题得分：2

展开解析

7

2 分

增量备份对上一次备份之后增加或修改的数据进行备份，这里的上一次备份指的是（ ）

A.完全备份；B.差异备份；C.增量备份；D.完全备份、差异备份、增量备份

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

8

2 分

以下关于冷备份的说法正确的是（　）

A.冷备份较热备份的维护成本低；B.冷备份可以实时备份也可以周期备份；C.冷备份的备份时间较热备份更快；D.冷备份属于逻辑备份

正确答案是：A　你的答案是：C　　此题得分：0

展开解析

9

2 分

在 IPsec 中，两个 VPN 网关之间实现身份验证的协议是（　）

A.ESP；B.AH；C.IKE；D.PPTP

正确答案是：C　你的答案是：A　　此题得分：0

展开解析

10

2 分

IP 报文是在网络层传输的数据单元。IP 报文头的最前端是下列哪一个选项？

A.报文头长度；B.标识；C.目的地址；D.版本

正确答案是：D　你的答案是：B　　此题得分：0

展开解析

11

2 分

建立在关系模型基础上的数据库被称作关系数据库，在关系数据库中，关系中的主属性值不能为空且不能有相同值，这体现了完整性约束条件中的（　）

A.参照完整性；B.用户定义的完整性；C.实体完整性；D.以上都不正确

正确答案是：C　你的答案是：C　此题得分：2

展开解析

12

2 分

IPv4 是互联网协议的第四版，IP 报文是在网络层传输的数据单元，报头包括固定长度部分和可变长度部分，其中 IPv4 的固定长度部分为（　）字节

A.10；B.20；C.25；D.40

正确答案是：B　你的答案是：D　此题得分：0

展开解析

13

2 分

信息在传输、交换、存储和处理过程保持非修改、非破坏和非丢失的特性被称为信息安全的完整性，下列哪种攻击能被系统的信息完整性机制防御？

A.伪造 IP 地址进行地址欺骗；B.否认做过信息的提交；C.信息在传输过程中被恶意篡改；D.拒绝服务攻击

正确答案是：C　你的答案是：C　此题得分：2

展开解析

14

2 分

单向散列函数能把任意长的输入变化成固定长的输出。其运用于数字签名的预先处理，主要原因是（　）

A.确保密文能够正确还原成明文；B.缩小签名密文的长度，加快数字签名的运算速度；C.增加密文破译难度；D.以上都不正确

正确答案是：B　你的答案是：A　　此题得分：0

展开解析

15

2 分

三次握手方法用于

A.传输层连接的建立；B.数据链路层的流量控制；C.传输层的重复检测；D.传输层的流量控制

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

16

2 分

防火墙是位于内部网络与外部网络之间的网络安全系统，防火墙的作用不包括

A.支持虚拟专用网 VPN；B.禁止未授权数据包进出内网；C.数据加密；D.网络地址转换

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

17

2 分

防火墙是指位于两个或多个网络之间实施网络间访问控制的一组组件的集合，并且需要满足三个条件，以下哪个选项不是条件之一？

A.网络内部和外部之间的所有数据流必须经过防火墙；B.防火墙的组件中必须包含硬件；C.只有符合安全策略的数据流才能通过防火墙；D.防火墙自身应具有高可靠性，对渗透免疫

正确答案是：B　你的答案是：D　　此题得分：0

展开解析

18

2 分

IP 电话使用的数据交换技术是

A.电路交换；B.报文交换；C.分组交换；D.包交换

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

19

2 分

计算机网络中所说的防火墙，是指设置在不同网络之间的一系列包括软硬件在内的部件组合。关于传统防火墙，以下说法正确的是

A.传统防火墙能防范新的网络安全问题；B.传统防火墙完全不能防止来自内部网的攻击；C.传统防火墙不能完全阻止病毒的传播；D.传统防火墙能防范数据驱动型攻击

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

20

2 分

防火墙通常使用的安全控制手段主要有包过滤、状态检测、代理服务等。关于状态检测型防火墙和包过滤型防火墙的描述正确的是

A.包过滤防火墙不需要对每个进入防火墙的数据包进行规则匹配；B.因为 UDP 协议为面向无连接的协议，因此状态检测型防火墙无法对 UDP 报文进行状态表的匹配；C.状态检测型防火墙对报文进行检查时，同一连接的前后报文不具有相关性；D.状态检测型防火墙只需要对数据流的第一个报文进行访问规则的匹配，后续报文根据会话进行转发

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

21

2 分

CSMA/CD 是 IEEE802.3 所定义的协议标准，它适用于

A.令牌环网；B.令牌总线网；C.网络互连；D.以太网

正确答案是：D　你的答案是：A　　此题得分：0

展开解析

22

2 分

ARP 欺骗是在网络中发送虚假的 ARP respones，关于 ARP 欺骗攻击的描述错误的是

A.ARP 实现机制只考虑业务的正常交互，对非正常业务交互或恶意行为不做任何验证；B.ARP 欺骗攻击只能通过 ARP 应答来实现，无法通过 ARP 请求实现；C.当某主机发送正常 ARP 请求时，攻击者会抢先应答，导致主机建立一个错误的 IP 和 MAC 映射关系；D.ARP 静态绑定是解决 ARP 欺骗攻击的一种方案，主要应用于网络规模不大的场景。

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

23

2 分

入侵防御系统 IPS 拥有众多的过滤器，能够防止各种攻击。IPS 的基本过程不包括

A.信息收集；B.告警与响应；C.信息打包；D.信息分析

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

24

2 分

下列说法中哪些是正确的？(1)虚电路与电路交换中的电路没有实质不同；(2)在通信的两站间只能建立一条虚电路；(3)虚电路也有连接建立、数据传输、连接释放三阶段；(4)虚电路的各个结点不需要为每个分组作路径选择判定

A.(1),(2)；B.(2),(3)；C.(3),(4)；D.(1),(4)

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

25

2 分

下面针对简单网关监控协议 SGMP 的组管理描述错误的是

A.下一代防火墙引入 SGMP 来实现对 VRRP 备份组的统一管理；B.不能解决多个 VRRP 备份组状态的不一致的问题；C.如果 SGMP 组检测到其中一个 VRRP 备份组的状态变化，则 SGMP 组会控制组中的所有 VRRP 备份组统一进行状态切换；D.防火墙上的所有 VRRP 备份组都加入到一个 SGMP 组中，由 SGMP 组来集中监控并管理所有的 VRRP 备份组状态

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

26

2 分

防火墙透明模式是指防火墙对用户透明即用户意识不到防火墙的存在，下列关于它的描述错误的是

A.透明模式下的防火墙在数据链路层连接局域网；B.防火墙对于子网用户和路由器透明；C.可以为穿越防火墙的流量提供 IP 路由功能；D.透明模式下防火墙支持 ACL 规则检查、防攻击检查等

正确答案是：B　你的答案是：C　此题得分：0

展开解析

27

2 分

下列有关计算机网络叙述错误的是

A.利用 Internet 网可以使用远程的超级计算中心的计算机资源；B.计算机网络是在通信协议控制下实现的计算机互联；C.建立计算机网络的最主要目的是实现资源共享；D.以接入的计算机多少可以将网络划分为广域网、城域网和局域网

正确答案是：D　你的答案是：D　此题得分：2

展开解析

28

2 分

对下一代防火墙支持的 LDAP 用户认证，描述错误的是

A.LDAP 认证使用 Https 加密传输用户登录信息；B.LDAP 主要应用于存储经常改变的数据；C.LDAP 全称是轻量目录访问协议，是基于 TCP/IP 的目录访问协议；D.启用 LDAP 认证后，用户需要出示用户名和密码

正确答案是：B　你的答案是：C　此题得分：0

展开解析

29

2 分

对下一代防火墙反病毒功能模块的作用描述错误的是

A.升级特征库可以提升病毒检测能力和检测效率；B.反病毒特性的主体配置是反病毒配置文件和安全策略；C.文件过滤特性中的全局参数包括最小解压层数、最小解压文件大小等；D.反病毒配置文件中定义了协议、传输方向和动作，以及病毒例外和应用例外

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

30

2 分

下列关于电子邮件的说法错误的是

A.电子邮件是 Internet 提供的一项最基本的服务；B.电子邮件具有快速、高效、方便、价廉等特点；C.通过电子邮件，可向世界上任何一个角落的网上用户发送信息；D.可发送的多媒体信息只有文字和图像

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

31

2 分

针对下一代防火墙的文件过滤功能，下列说法错误的是

A.可以根据文件类型进行过滤；B.可以根据文件扩展名对文件进行过滤；C.若与内容过滤相结合，会降低过滤效率和质量；D.文件过滤有阻断和告警两种动作

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

32

2 分

为了实现外部网络对内部网络中某些特定设备（如服务器）的访问，使用哪种技术比较合适？

A.静态 NAT 技术；B.动态 NAT 技术；C.端口转换技术；D.DHCP 服务技术

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

33

2 分

IP 协议是将多个包交换网络连接起来，它在源地址和目的地址之间传送一种称之为数据包的东西。关于 IP 协议说法正确的是

A.它是无连接协议，负责处理会话的建立、管理；B.它是无连接协议，负责数据报的编址和路由；C.它是面向连接的协议，负责数据报的编址和路由；D.它是面向连接的协议，负责错误检测和数据流控制

正确答案是：B　你的答案是：A　　此题得分：0

展开解析

34

2 分

广域网提供两种服务模式，对应于这两种服务模式，广域网的组网方式有

A.虚电路方式和总线型方式；B.总线型方式和星型方式；C.虚电路方式和数据报方式；D.数据报方式和总线型方式

正确答案是：C　你的答案是：B　　此题得分：0

展开解析

35

2 分

针对攻击防护功能，下列说法错误的是

A.下一代防火墙对 HTTP、DNS、DHCP 协议提供应用层防护；B.防火墙防御 DDoS 攻击采用的方式是 TC 源认证方式；C.下一代防火墙针对局域网多播广播、IP 地址欺骗等提供了专门的防护；D.下一代防火墙可提供 IP 欺骗、DHCP 监控辅助检查

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

36

2 分

计算机病毒（Computer Virus）是编制者在计算机程序中插入的破坏计算机功能或者数据的代码，能影响计算机使用，能自我复制的一组计算机指令或者程序代码。关于计算机病毒的描述正确的是

A.计算机病毒只感染可执行文件；B.计算机病毒只感染文本文件；C.计算机病毒只能通过软件复制的方式进行传播；D.计算机病毒可以通过读写磁盘或网络等方式进行传播

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

37

2 分

对于下列说法，错误的是

A.TCP 协议可以提供可靠的数据流传输服务；B.TCP 协议可以提供面向连接的数据流传输服务；C.TCP 协议可以提供全双工的数据流传输服务；D.TCP 协议可以提供面向非连接的数据流传输服务

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

38

2 分

代理 ARP 一般使用在没有配置默认网关和路由策略的网络上。关于代理 ARP，说法错误的是

A.代理 ARP 是 ARP 协议的一个变种；B.代理 ARP 就是将一个主机作为对另一个主机 ARP 进行应答；C.代理 ARP 能够对网络拓扑进行网络概括；D.代理 ARP 可能会带来巨大的风险

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

39

2 分

RADIUS 是网络远程接入设备的客户和包含用户认证与配置信息的服务器之间信息交换的标准客户/服务器模式。关于 RADIUS 用户认证，说法错误的是

A.RADIUS 的全称是用户远程拨号认证服务；B.RADIUS 是一个分布式客户端/服务器协议；C.RADIUS 主要针对的远程登录类型有：SLIP、PPP、Telnet 等；D.RADIUS 的不足是协议的应用范围较小

正确答案是：D　你的答案是：D　此题得分：2

展开解析

40

2 分

TCP/IP 协议簇包含一个提供对电子邮箱邮件进行远程获取的协议，称为

A.POP；B.SMTP；C.FTP；D.TELNET

正确答案是：A　你的答案是：A　此题得分：2

展开解析

41

2 分

IPSec VPN 指采用 IPSec 协议来实现远程接入的一种 VPN 技术。有关 IPSec VPN，说法正确的是

A.IPSec VPN 是基于应用层的 VPN；B.IPSec VPN 组网灵活，便于调整用户 IPSec 策略；C.IPSec VPN 安全性差；D.IPsec 由 AH 协议和 ESP 协议组成

正确答案是：D　你的答案是：B　此题得分：0

展开解析

42

2 分

静态路由是指由用户或网络管理员手工配置的路由信息。下列对静态路由描述错误的是

A.静态路由主要应用于较复杂的网络环境；B.静态路由需要由用户或网络管理员手工配置路由信息；C.网络管理员可以通过对路由器进行设置使静态路由成为共享的；D.静态路由具有单向性，仅允许数据包沿着下一跳的方向进行路由

正确答案是：A　你的答案是：D　　此题得分：0

展开解析

43

2 分

虚拟系统是指现有操作系统的全新虚拟镜像。以下关于虚拟系统的管理和配置，下列说法错误的是

A.根虚拟系统管理员是权限最大的管理员；B.根虚拟系统管理员可以创建子虚拟系统管理员；C.一个子虚拟系统管理员只能管理一个子虚拟系统；D.一个子虚拟系统只能有一个子虚拟系统管理员

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

44

2 分

IP 协议是将多个包交换网络连接起来，它在源地址和目的地址之间传送一种称之为数据包的东西。关于 IP 协议说法错误的是

A.各个局域网根据 IP 协议相互连接，最终构成覆盖全球的 Internet；B.UDP 可以不通过网络层的 IP 数据包来传递信息；C.TCP 必须通过网络层的 IP 数据包来传递信息；D.IP 包分为头部和数据两部分

正确答案是：B　你的答案是：C　　此题得分：0

展开解析

45

2 分

动态主机配置协议 DHCP 是一个局域网的网络协议，使用 UDP 协议工作，以下不属于 DHCP 工作流程的是

A.广播寻找 DHCP 服务器；B.提供 IP 地址租用；C.拒绝 IP 租约；D.租约确认

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

46

2 分

IPv6 是 IETF 设计的用于替代现行版本 IP 协议（IPv4）的下一代 IP 协议，下列哪一项不是 IPv4 向 IPv6 过渡的技术

A.双协议栈；B.隧道技术；C.传输技术；D.附带协议转换器的网络地址转换器

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

47

2 分

下列关于防火墙的描述，错误的是

A.防火墙最基础的两大功能是“隔离”和“访问控制”；B.防火墙可以抵御来自内部网络的攻击；C.防火墙系统的组合可以是硬件、软件或者是软硬件结合；D.最早的防火墙使用的是静态包过滤技术

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

48

2 分

SSL（安全套接层）协议是一种在 Internet 上保证发送信息安全的通用协议，关于 SSL VPN 描述正确的是

目录

A.基于 C/S 架构；B.工作在传输层和应用层之间；C.加密后改变 IP 和 TCP 报文头；D.访问控制基于会话层

正确答案是：B　你的答案是：D　　此题得分：0

展开解析

49

2 分

设有 2 条路由 21.1.193.0/24 和 21.1.194.0/24，如果进行路由汇聚，覆盖这 2 条路由的地址是

A.21.1.200.0/22；B.21.1.192.0/23；C.21.1.192.0/21；D.21.1.224.0/20

正确答案是：C　你的答案是：B　　此题得分：0

展开解析

50

2 分

虚拟局域网（VLAN）是一组逻辑上的设备和用户，关于 VLAN 的说法错误的是

A.基于网络层的 VLAN 可以按协议划分，也可以按 MAC 地址划分；B.VLAN 可以控制广播活动，提高网络安全性；C.VLAN 可减少网络设备移动的开销；D.静态 VLAN 按照局域网交换机端口来定义 VLAN 成员

正确答案是：A　你的答案是：B　　此题得分：0

第十一章

以下选项中不属于单包攻击的是

A.Ping of Death 攻击；B.IP 地址扫描攻击；C.ICMP 重定向报文攻击；D.分布式拒绝服务（DDoS）攻击

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

2

2 分

地址解析协议（ARP）是根据 IP 地址获取物理地址的一个 TCP/IP 协议，关于 ARP 描述正确的是

A.不需要对 IP 地址和物理地址进行缓存；B.建立在网络中主机相互信任的基础上；C.发送包含源 IP 地址的 ARP 请求广播；D.根据 IP 地址获取物理地址的 UDP 协议

正确答案是：B　你的答案是：C　　此题得分：0

展开解析

3

2 分

数据库安全受到的威胁有一些网络不法分子通过网络，局域网等途径通过入侵电脑使系统无法正常启动，或超负荷让机子运行大量算法，并关闭 cpu 风扇，使 cpu 过热烧坏等破坏性活动，黑客对数据库漏洞进行入侵，并盗取想要的资料。关于数据库漏洞，以下描述中不正确的是（　）

A.常见的数据库漏洞主要有数据库账号特权提升、数据库敏感数据未加密以及错误配置数据库等；B.拥有管理员权限的攻击者没有数据库的相关凭证就不能从一个应用程序跳转到数据库；C.数据库特权提升通常与错误配置数据库有关；D.数据库出现问题可能是由老旧未补的漏洞或默认账户配置参数引起的

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

4

2 分

在常规密码中，收信方和发信方使用相同的密钥，即加密密钥和解密密钥是相同或等价的。优点是有很强的保密强度，且经受住时间的检验和攻击，但其密钥必须通过安全的途径传送。因此，其密钥管理成为系统安全的重要因素。有线等价加密的核心加密算法是（　）

A.RSA 算法；B.MD5 算法；C.RC4 序列密码算法；D.DES 算法

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

5

2 分

加密的分类主要包括共享秘钥认证和开放系统认证，WEP 加密是共享秘钥式，而 TKIP、CCMP 和 802.1x 则是开放系统，WEP 在选择加密算法中选择了（　）算法，WEP 规定的密钥长度为（　）

A.RC4，40bit；B.RC3，40bit；C.RC4，64bit；D.RC3，64bit

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

6

2 分

WEB 漏洞通常是指网站程序上的漏洞，可能是由于代码编写者在编写代码时考虑不周全等原因而造成的漏洞，常见的 WEB 漏洞有 SQL 注入、XSS 漏洞、上传漏洞等。关于 Web 漏洞，以下描述中不正确的是（　）

A.CSRF 跨站请求伪造攻击利用一个透明的 iframe 框，诱使用户在该页面上进行操作；B.SQL 注入攻击（SQL Injection）是 WEB 开发中常见的一种安全漏洞。；C.XSS 跨站脚本攻击是一种广泛出现的 Web 客户端漏洞；D.程序在实现上没有充分过滤用户输入的“../”之类的目录跳转符可能会造成目录遍历漏洞

正确答案是：A　你的答案是：C　　此题得分：0

展开解析

7

2 分

常见的漏洞扫描器有 Nmap，Nessus 以及 WEB 应用扫描器，每一种扫描器都有各自擅长的应用场景和优势，关于漏洞扫描器，以下描述中不正确的是（　）

A.Nmap 可以进行操作系统的服务判定和操作系统指纹的判定；B.Nmap 根据端口扫描的结果去判定其他信息；C.WEB 应用扫描器只能检测系统和网络的基础情况；D.Nessus 可以检查系统漏洞和部分的配置失误

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

8

2 分

一般来说，wifi 的加密方式有 WEP，CCMP，AES 和 TKIP，其中 CCMP 以及 TKIP 是 WLAN 中哪个协议标准里包含的内容？

A.IEEE802.11x；B.IEEE802.11h；C.IEEE802.11s；D.IEEE802.11i

正确答案是：D　你的答案是：B　　此题得分：0

展开解析

9

2 分

Nmap 是不少技术人员爱用的工具。系统管理员可以利用 Nmap 来探测工作环境中未经批准使用的服务器，但是黑客会利用 Nmap 来搜集目标电脑的网络设定，从而计划攻击的方法。对于 Nmap 的工作流程：1、服务识别；2、存活性扫描；3、操作系统识别；4、端口扫描。正确的顺序为（　）

A.4->2->3->1；B.4->2->1->3；C.2->4->1->3；D.2->4->3->1

正确答案是：C　你的答案是：D　此题得分：0

展开解析

10

2 分

规避技术是指能够绕过信息安全设备进行入侵，攻击或植入恶意软件到目标网络或系统而不被发现的技术。关于规避技术，以下描述中不正确的是（　）

A.向目标主机发送的 IP 包中填充错误的字段值可以探测目标主机和网络设备；B.构造的数据包长度只需要超过目标系统所在路由器的 PMTU 就可以探测内部路由器；C.反向映射探测用于探测被过滤设备或防火墙保护的网络和主机；D.规避技术利用被探测主机产生的 ICMP 错误报文来进行复杂的主机探测

正确答案是：B　你的答案是：A　此题得分：0

展开解析

11

2 分

指纹识别技术是把一个人同他的指纹对应起来，通过比较他的指纹和预先保存的指纹进行比较，就可以验证他的真实身份。关于指纹识别技术，以下描述中不正确的是（　）

A.主动指纹识别技术采用主动发包并多次试探、筛选不同信息；B.指纹识别技术的目的包括辨识一个操作系统的种类；C.主动识别技术的探测精度只与配置有关，不受目标主机与源主机之间跳数影响；D.被动识别技术一般不需要发送数据包

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

12

2 分

路由器在大多数网络中几乎到处都有。按照惯例，它们只是被用来作为监控流量的交通警察而已。而现代的路由器具备了完备的安全功能，有时候甚至要比防火墙的功能还全。关于路由器安全防护措施，以下描述中不正确的是（　）

A.对路由器设置特定的 IP 地址；B.进行网络分段和无线 MAC 地址过滤；C.结合使用端口转发和 IP 过滤；D.对路由器使用无线安全设置，不必配置其他参数

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

13

2 分

要保证网络安全，进行网络安全建设，第一步首先要全面了解系统，评估系统安全性，认识到自己的风险所在，从而迅速、准确的解决内网安全问题。关于网络设备安全防护措施，以下做法中不正确的是（　）

A.定期检查设备软件版本；B.修改默认管理员账号和密码；C.完全可以使用“Telnet”方式对设备进行管理；D.设置设备日志定期发送到专门的服务器保存

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

14

2 分

路由器是一种多端口设备，它可以连接不同传输速率并运行于各种环境的局域网和广域网，也可以采用不同的协议。路由器 PIN 指的是（　）

A.快速连接识别码；B.个人代号；C.个人地址；D.个人信用

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

15

2 分

当客观存在的潜在威胁攻击系统脆弱点时，就会产生风险，导致系统的破坏和受损。风险评估是解释和分析风险的过程。风险评估的目的是发现风险和控制风险。无线网络安全评估会（　）

A.浪费资金投入；B.预防所有安全问题；C.影响用户使用网络；D.识别可能影响或威胁企业网络、任务和用户的安全性问题

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

16

2 分

移动办公是全新的办公模式，可以让办公人员摆脱时间和空间的束缚。单位信息可以随时随进行交互流动，工作将更加轻松有效，整体运作更加协调。关于移动办公的风险中，以下描述不正确的是（　）

A.移动终端难管控；B.移动终端安装了最新的安卓系统；C.终端准入难设定；D.移动终端环境安全难保障

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

17

2 分

操作系统是用户和计算机的接口，同时也是计算机硬件和其他软件的接口。操作系统的功能包括管理计算机系统的硬件、软件及数据资源，控制程序运行，改善人机界面，为其它应用软件提供支持，让计算机系统所有资源最大限度地发挥作用。操作系统的管理功能不包括（　）

A.作业管理；B.文件管理；C.用户事务管理；D.进程与处理机管理

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

18

2 分

Windows 操作系统本身所存在技术缺陷，系统漏洞往往会被病毒利用侵入并攻击用户计算机。Windows 操作系统供应商将定期对已知的系统漏洞发布补丁程序，用户只要定期下载并安装补丁程序，可以保证计算机不会轻易被病毒入侵。关于 Windows 操作系统漏洞，以下描述中不正确的是（　）

A.Microsoft Windows 中的 Edge 存在提权漏洞，该漏洞源于程序没有正确的强制执行跨域策略；B.Microsoft Windows RPC 存在远程代码执行漏洞，由于远程访问服务处理请求方式不当，远程攻击者可利用漏洞执行任意代码；C.Microsoft Windows 中的 Device Guard 存在安全绕过漏洞，该漏洞源于程序未能正确的验证不可信的文件；D.Microsoft Windows 中的 Kernel API 存在本地信息泄露漏洞，攻击者可借助特制的应用程序利用该漏洞注入跨进程通信，中断系统功能

正确答案是：D　你的答案是：C　　此题得分：0

展开解析

19

2 分

越狱是我们利用 ios 系统里的一些漏洞，突破系统的封闭式环境。当使用 ios 系统时，普通用户是无法安装自由的安装一些游戏软件或者一些其他的小软件等等，极大的限制了用户的自由，所以能更好的使用 ios 系统，我们需要“越狱”。越狱是为了获得（　）

A.Small 权限；B.big 权限；C.Root 权限；D.Key 权限

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

20

2 分

UNIX 操作系统，是一个强大的多用户、多任务操作系统，支持多种处理器架构，按照操作系统的分类，属于分时操作系统。关于 Unix 操作系统漏洞，以下描述中不正确的是（ ）

A.Path 的攻击方法是利用了 Path 环境变量文件路径的值和顺序；B.IFS 变量只决定传给 Shell 的字符串的内容；C.在建立文件之前先建立一个 Umask 值可以使文件更安全；D.利用 Home 环境变量可以对 Unix 系统进行攻击

正确答案是：B 你的答案是：B 此题得分：2

展开解析

21

2 分

一个操作系统内可以注册许多的用户，也可以有不同的管理员，这使得系统需要定义一些权限来管理不同的用户，也防止用户进行一些违规或者不可挽回的误操作。其中系统中的 root 目录是（ ）

A.超级用户的主目录；B.系统的根目录；C.动态连接库；D.系统管理根目录

正确答案是：A 你的答案是：D 此题得分：0

展开解析

22

2 分

Linux 是一种类 Unix 操作系统，是一个基于 POSIX 和 UNIX 的多用户、多任务、支持多线程和多 CPU 的操作系统。它能运行主要的 UNIX 工具软件、应用程序和网络协议。关于 Linux 操作系统漏洞，以下描述中不正确的是（ ）

A.Linux 中利用管理文件的写操作会导致文件被篡改；B.进程终止后未重置或清空其运行时使用的内存可能会造成泄密；C.攻击者可利用 Linux Kernel 绕过 KASLR 安全限制；D.内核无线扩展完全不可能造成内存泄漏漏洞

正确答案是：D　你的答案是：D　此题得分：2

展开解析

23

2 分

ROOT 权限，系统权限的一种，也叫根权限，与 SYSTEM 权限可以理解成一个概念，但高于 Administrator 权限，root 是 Linux 和 Unix 系统中的超级管理员用户帐户，该帐户拥有整个系统最高的权限，所有对象它都可以操作。下列对 ROOT 权限范围描述正确的是（　）

A.可以访问所有文件，包括修改核心；B.只能修改内核态下的系统；C.只能修改用户态的一般进程；D.修改控制器、运算器、输入输出设备。

正确答案是：A　你的答案是：A　此题得分：2

展开解析

24

2 分

协议栈指纹识别是一项强大的技术，能够以很高的概率迅速确定操作系统的版本。因为由于各个厂家在编写自己的 TCP/IP 协议栈存在差别，而我们通过这些细微的差别，可以确定各位操作系统的版本。关于 TCP/IP 协议栈的指纹探测技术，以下描述中不正确的是（　）

A.主动协议栈指纹技术只能被动地捕获远程主机发送的数据包；B.TCP/IP 协议栈指纹技术是通过探测各种操作系统在实现 TCP/IP 协议栈时存在的一些细微差别，来确定目标主机的操作系统类型；C.主动协议栈指纹技术通过提取和分析响应数据包的特征信息，来判断目标主机的操作系统信息；D.被动协议栈指纹技术捕捉到一个数据包后可以从生存期（TTL）、滑动窗口大小（WS）、分片允许位（DF）和服务类型（TOS）4 个方面进行法分析

正确答案是：A　你的答案是：A　此题得分：2

展开解析

25

2 分

TCP 协议通过对传输数据进行确认来实现可靠的数据传输，然而在真实网络环境中，数据丢失是很有可能发生的，所以 TCP 会设置一个重发定时器，当定时器溢出后，还没有收到确认，就进行数据的重传，重传定时器的时间间隔称为 RTO。关于基于 RTO 采样的指纹识别，以下描述中不正确的是（ ）

A.RTO 全称为 Retransmission Timeout；B.基于 RTO 采样的指纹识别方法完全不会在网络中产生畸形的数据包且花费扫描时间短；C.利用不同操作系统在计算 RTO 时使用的方法是不同的可实现对远程主机操作系统的探测；D.用堵塞模块阻止目标端口响应的 SYN/ACK 包到达扫描主机会迫使目标主机不断超时重发 SYN/ACK 包

正确答案是：B 你的答案是：B 此题得分：2

展开解析

26

2 分

在端口扫描中，当一个主机向远端一个服务器的某一个端口提出建立一个连接的请求，如果对方有此项服务，就会应答，利用这个原理，如果对所有熟知端口或自己选定的某个范围内的熟知端口分别建立连接，并记录下远端服务器所给予的应答，通过查看记录就可以知道目标服务器上都安装了哪些服务。关于端口扫描技术，以下描述中不正确的是（ ）

A.全 TCP 扫描根据 connect()连接情况的返回值判断目标机监听端口的开放情况；B.在 TCP FIN 扫描中，扫描主机发送的数据包中的 FIN 位被置位，若目标端口是关闭的，则探测数据包被丢掉；C.UDP ICMP 扫描向 UDP 端口发送 UDP 探测包，若目标端口是关闭的，则返回 ICMP 端口不可达数据包；D.端口扫描一般指向目标主机的 TCP 或 UDP 端口发送探测数据包

正确答案是：B 你的答案是：C 此题得分：0

展开解析

27

2 分

Windows 架构的特性使得微软的程序员在设计或编写时会产生一些错误，使得 Windows 操作系统中存在着大量的漏洞。关于 Windows 系统的漏洞防护措施，以下做法中不正确的是（ ）

A.根据自己系统的需要，把无需使用和有危险性的服务选择关闭；B.修改注册表来禁止默认共享；C.设置系统盘格式为 FAT/FAT32；D.修改注册表来禁止空连接

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

28

2 分

在传统的 VPN 组网场合中,GRE 隧道技术得到了广泛的应用。下列关于 GRE 隧道技术的描述中，不正确的是（　）

A.从负责封装后报文传输的网络来看，GRE 隧道源地址就是实际发送报文的接口 IP 地址；B.从负责封装后报文传输的网络来看，GRE 隧道本端的目的地址就是隧道目的端的源地址；C.不需要为隧道接口分配 IP 地址；D.隧道接口的封装类型是指该隧道接口对报文进行的封装方式

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

29

2 分

CHAP 是 PPP 通信中重要的身份认证方式。关于 CHAP 身份认证，以下选项不正确的是（）

A.CHAP 全称为挑战握手认证协议（Challenge Handshake Authentication Protocol）；B.CHAP 身份认证采用两次握手机制；C.CHAP 认证可以是单向或者双向的；D.CHAP 认证的过程分为认证方发送挑战信息、被认证方回复认证请求、认证方告知被认证方认证是否通过

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

30

2 分

在 PPP 通信中，可以采用 PAP（密码认证协议）或者 CHAP（质询握手认证协议）身份认证方式对连接用户进行身份认证，以防非法用户的 PPP 连接。关于 PAP 身份认证，以下描述不正确的是（　）

A.PAP 认证过程非常简单，采用单次握手机制；B.PAP 认证可以在一方进行，也可以进行双向身份认证；C.PAP 服务器端在收到客户端发来的认证请求帧后，先查看 PAP 服务器本地配置的用户账户数据库，看是否有客户端提供的用户名；D.如果第一次认证失败，并不会马上将链路关闭，而是会在 PAP 客户端提示可以尝试新的用户账户信息进行再次认证，只有当认证不通过的次数达到一定值时（一般缺省值为 4）才会关闭链路

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

31

2 分

MD5 即 Message-Digest Algorithm 5(信息-摘要算法 5)，是计算机广泛使用的杂凑算法之一。下列关于 MD5 身份认证算法的特点的描述中，不正确的是（　）

A.任意长度的数据，算出的 MD5 值的长度都是固定的。；B.从原数据计算出 MD5 值很容易；C.对原数据进行任何改动，哪怕只修改 1 个比特，所得到的 MD5 值都有很大区别。；D.想找到两个不同的数据，使它们具有相同的 MD5 值是容易的。

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

32

2 分

SHA 算法是公认的最安全的散列算法之一，并被广泛使用。以下关于 SHA 算法的描述中，不正确的是（　）

A.安全哈希算法（Secure Hash Algorithm，SHA）主要适用于数字签名，也是一种不可逆的 MAC 算法；B.SHA 算法比 MD5 算法更加安全；C.SHA 算法先把原始消息划分成固定长度的块，最后加上用于标识原始消息长度的位；D.不同 SHA 版本中用于标识原始消息长度的位数都是相同的

正确答案是：D　你的答案是：B　　此题得分：0

展开解析

33

2 分

数据加密技术是网络安全技术的基石。以下关于数据加密技术的描述中，不正确的是（ ）

A.VPN 需要利用加密算法提供安全保障；B.VPN 主要采用非对称密钥加密算法保障数据通信安全；C.VPN 主要采用非对称密钥加密算法保障身份认证安全；D.数据加密技术的基本思想是伪装信息，使未授权者不能理解它的真实含义

正确答案是：B　你的答案是：C　　此题得分：0

展开解析

34

2 分

对称密钥加密算法是传统常用的算法。以下关于对称密钥加密原理的描述中，不正确的是（　）

A.在加密传输中最初是采用对称密钥方式，也就是加密和解密都用相同的密钥；B.通信双方要事先协商好对称密钥；C.对称密钥加密缺点是安全性差和扩展性差；D.RSA 属于对称加密算法

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

35

2 分

非对称加密算法是一种密钥的保密方法。以下关于非对称密钥加密原理的描述中，不正确的是（　）

A.非对称密钥加密方法，又称为公钥加密方法；B.非对称密钥加密方法是指加密和解密用不同的密钥，其中一个称之为公钥，可以对外公开，通常用于数据加密；另一个称之为私钥，需要保密，通常用于数据解密；C.常见的非对称密钥加密算法有 AES、DES 等；D.非对称密钥具有比对称密钥加解密方式更高的安全性，缺点是算法非常复杂

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

36

2 分

分组密码是对称密钥加密算法的一种加密模式。以下关于分组密码工作模式的描述中，不正确的是（　）

A.ECB 模式解密过程与加密过程相逆；B.密码分组链接模式对相同的两个明文块加密后得到的密文块不相同；C.CFB 模式能够将块密文转换为流密文；D.OFB 模式直接加密明文块

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

37

2 分

DES 加密算法是一种常规密码体制的密码算法，以下关于 DES 加密算法的描述中，不正确的是（　）

A.密钥较短；B.存在弱密钥；C.3DES 完全改变了 DES 算法的内容；D.3DES 支持 CBC 、ECB、CFB、OFB 等几种工作模式

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

38

2 分

AES 加密算法用来替代原先的 DES，已经被多方分析且广为全世界所使用。以下关于 AES 加密算法的描述中，不正确的是（　）

A.AES 的全称是 Advanced Encryption Standard；B.AES 分组长度为 128 位，支持 128 位 、192 位和 256 位的密钥；C.AES 同 DES 一样支持 ECB、CBC、CFB 和 OFB 等工作模式；D.AES 完全无法抵抗差分攻击和线性攻击

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

39

2 分

DH 算法是安全性基于在有限域中计算离散对数的难度的一种加密算法。以下关于 DH 算法的描述中，不正确的是（　）

A.Diffie-Hellman 由 Whitfield Diffie 和 Martin Hellman 在 1976 年公布的一种密钥一致性算法；B.由于该算法本身限于密钥交换的用途，被许多商用产品用作密钥交换技术，因此该算法通常称之为 Diffie-Hellman 密钥交换；C.DH 算法能防止重演攻击；D.DH 算法是计算密集性的，因此容易遭受阻塞性攻击，即对手请求大量的密钥

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

40

2 分

RSA 算法是目前应用最为广泛的公钥密码算法。以下关于 RSA 算法的描述中，不正确的是（　）

A.RSA 算法基于一个十分简单的数论事实：将两个大质数相乘十分容易，但是想要对其乘积进行因式分解却极其困难；B.RSA 是对称加密算法；C.为提高保密强度，RSA 密钥至少为 500 位长，一般推荐使用 1024 位；D.钥匙的长度足够长，用 RSA 加密的信息实际上是很难被破解的

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

41

2 分

AH 协议是用以保证数据包的完整性和真实性，防止黑客截断数据包或向网络中插入伪造数据包的协议。下列不属于 AH 协议提供的安全功能的是（　）

A.数据完整性服务；B.数据验证；C.防止数据重放攻击；D.数据加密

正确答案是：D　你的答案是：B　　此题得分：0

展开解析

42

2 分

ESP 协议是　IPsec 体系结构中的一种主要协议，下列关于 ESP 协议的说法正确的是（　）

A.ESP 协议提供了数据的第 3 层保护；B.ESP 不提供对用户数据的加密；C.ESP 的数据验证和完整性服务包括 ESP 头、有效载荷和外部的 IP 头；D.外部的 IP 头如果被破坏，ESP 可以检测

正确答案是：A　你的答案是：C　　此题得分：0

展开解析

43

2 分

Internet 密钥交换协议(IKE)用于交换和管理在 VPN 中使用的加密密钥。下列关于 IKE 协议的说法不正确的是（　）

A.IKE 的全称是 Internet Key Exchange，Internet 即密钥交换；B.IKE 协议只可以用来协商 VPN，不可以被远程用户用于接入安全主机和网络；C.IKE 协议是混合协议；D.IKE 同样支持客户协商,在这种模式下，终端实体的身份信息是隐藏的

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

44

2 分

ISAKMP 定义了一个通用的可以被任何密钥交换协议使用的框架。下列不属于 ISAKMP 消息载荷类型的是（　）

A.交换载荷；B.变换载荷；C.证书载荷；D.安全联盟（SA）载荷

正确答案是：A　你的答案是：B　　此题得分：0

展开解析

45

2 分

IKE SA 负责 IPSec SA 的建立和维护。下列不是 IKE SA 的安全属性的是（　）

A.加密算法（如 DES、3DES 等）；B.哈希算法（如 MD5、SHA1 等）；C.认证方法（预共享密钥、数字签名、公钥方式、改进的公钥方式）；D.SPI 的生命周期

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

46

2 分

安全关联 SA 是　IPSec 的基础，是通信双方建立的一种协定。下列关于 IPSec SA 建立的说法不正确的是（　）

A.IPSec SA 的建立阶段在已经建立的 IKE SA 保护下进行，通信双方协商拟定 IPSec 的各项特征；B.IPSec SA 的建立阶段通过使用来自 IKE SA 的 SKEYIDa 作为认证密钥，对快速交换模式的整个消息进行验证，该验证除了提供数据完整性保护外，还提供数据源身份验证；C.通过使用来自 IKE SA 的 SKEYIDa 对交换的消息进行加密，保证消息的机密性；D.IPSec SA 的建立共用了 3 条消息

正确答案是：C　你的答案是：D　　此题得分：0

展开解析

47

2 分

SSL 协议是为网络通信提供安全及数据完整性的一种安全协议。下列关于 SSL 的说法错误的是（　）

A.SSL 的全称是 Secure Sockets Layer 即安全套接字层；B.SSL 协议是位于计算机网络体系结构的网络层和传输层之间的套接字（Socket）协议的安全版本,可为基于公网(如 Internet)的通信提供安全保障；C.SSL VPN 使用的是 SSL 协议；D.SSL 可保障客户端与服务器之间的通信不被攻击者窃听,并且远程客户端通过数字证书始终对服务器(SSL VPN 网关)进行认证,还可选择对客户端进行认证

正确答案是：B　你的答案是：C　　此题得分：0

展开解析

48

2 分

SSL 是对计算机之间整个会话进行加密的协议。以下不是 SSL 协议的特点的是（　）

A.提供较高的安全性保证；B.支持各种应用层协议；C.部署复杂；D.建立在可靠的 TCP 传输控制协议之上

正确答案是：C　你的答案是：D　　此题得分：0

展开解析

49

2 分

TCP(Transmission Control Protocol 传输控制协议)是一种面向连接的、可靠的、基于字节流的传输层通信协议，下列不属于基于 TCP 的服务的是（　）

A.Ping 服务；B.Telnet 服务；C.桌面共享服务；D.邮件服务

正确答案是：A　你的答案是：D　　此题得分：0

展开解析

50

2 分

Linux 系统中可使用 ls 命令列出文件存取权限，如“-rw-r-xrw- 1 root root 1397 Oct 11 9:40 passwd”，其中存取权限位第二组“r-x”表示（）

A.文件拥有者具有读写及执行权限；B.文件拥有者同组用户允许读和执行操作；C.其他用户允许读和执行操作；D.文件拥有者允许读和执行操作

正确答案是：B　你的答案是：B　此题得分：2

展开解析

第十二章

1

2 分

强制性标准是由法律规定必须遵照执行的标准，强制性国家标准的代号为（）

A.GB；B.GB/T；C.JB；D.JB/T

正确答案是：A　你的答案是：C　此题得分：0

展开解析

2

2 分

由 4 位 0~9 数字组合的密码采用穷举破解至多需尝试（）次

A.4444；B.1000；C.9999；D.10000

正确答案是：C　你的答案是：C　此题得分：2

展开解析

3

2 分

恶意代码给计算机安全带来巨大威胁，以下属于恶意代码的特征的是（）

A.具有恶意的目的；B.本身不属于计算机程序；C.不执行也能发生作用；D.以上都不正确

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

4

2 分

入侵检测系统能对网络传输数据进行即时监测，关于入侵检测系统的安装位置，以下说法不适合的是（）

A.边界防火墙之内；B.任何非网络环境中；C.主要的网络中枢；D.一些安全级别需求高的子网

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

5

2 分

木马程序指潜伏在计算机中，可被攻击者控制以达到窃取数据或者获取控制权目的的程序，下列哪项列举的恶意程序不属于木马程序？

A.广外女生；B.灰鸽子；C.熊猫烧香；D.冰河

正确答案是：C　你的答案是：D　　此题得分：0

展开解析

6

2 分

计算机越来越普遍，而操作系统用于管理和控制计算机的硬件和软件资源，以下哪个选项不属于 LINUX 操作系统的特点？

A.LINUX 不支持多任务；B.LINUX 支持多用户会话；C.LINUX 可以提供分层文件系统；D.LINUX 可以提供广泛的网络功能，支持大多数互联网通信协议和服务

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

7

2 分

在 Windows 系统中，用户登录密码的散列一般保存在（）　文件中

A.USER；B.PASSWD；C.ADMIN；D.SAM

正确答案是：D　你的答案是：B　　此题得分：0

展开解析

8

2 分

在现在的 Linux 系统中，用户密码散列一般保存在（）文件中

A.USER；B.ADMIN；C.SHADOW；D.PASSWD

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

9

2 分

网络隔离保障了可信网络内数据的安全性，网络隔离设备不包括（）

A.防火墙；B.蜜罐；C.IPS；D.网闸

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

10

2 分

以下哪个技术指标是是衡量容灾系统安全性和可靠性的重要指标？

A.恢复配置目标；B.恢复时间目标；C.恢复网络目标；D.恢复任务目标

正确答案是：B　你的答案是：A　　此题得分：0

展开解析

11

2 分

在 Windows 操作系统中，下列哪个命令可用于加密文件？

A.cipher；B.ipconfig；C.ping；D.send

正确答案是：A　你的答案是：D　　此题得分：0

展开解析

12

2 分

强口令即长度不小于 8 个字符、同时包含大写和小写字符、至少有一个数字的字符串。下列密码中，属于强口令的是（）

A.123456；B.19950429；C.qwertyuiop；D.dllgs7kn8nk2

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

13

2 分

以下关于软件说法错误的是（）

A.软件是一种逻辑实体，而不是物理实体，具有抽象性；B.软件是开发出来的，而不是制造出来的；C.在软件的运行和使用期间，没有硬件那样的机械磨损、老化问题；D.与硬件相比，软件很简单，一定不会发生故障的情况

正确答案是：D　你的答案是：D　此题得分：2

展开解析

14

2 分

以下哪个不是做好软件安全测试的必要条件？（）（）

A.充分了解软件安全漏洞；B.拥有软件的全部开发过程文档和源代码；C.评估软件安全风险；D.高效的软件安全测试技术和工具

正确答案是：B　你的答案是：B　此题得分：2

展开解析

15

2 分

状态检测防火墙依据网络层截取的数据包信息采取相应的包处理措施，以下关于状态检测防火墙的特性不包括（）

A.高安全性；B.高效性；C.无法扩展；D.便捷性

正确答案是：C　你的答案是：C　此题得分：2

展开解析

16

2 分

防火墙是一个软硬件结合的安全防护设备。防火墙的选购标准中，不考虑以下哪项？（）

A.安全性；B.可见性；C.可管理性；D.易用性

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

17

2 分

网络安全已经引起了全球的关注，网络安全威胁的不对称性逐渐增加表现在下列哪项？

A.Internet 上的安全相互独立，而攻击破坏性逐渐增大；B.Internet 上的安全相互依赖，而攻击破坏性逐渐增大；C.Internet 上的安全相互独立，而攻击破坏性逐渐减小；D.Internet 上的安全相互依赖，而攻击破坏性逐渐减小

正确答案是：B　你的答案是：D　　此题得分：0

展开解析

18

2 分

网络监听、会话劫持、拒绝服务攻击分别破坏了网络信息的以下哪些特性？（）

A.网络信息的保密性；网络信息的完整性；网络服务的可用性；B.网络信息的完整性；网络信息的保密性；网络服务的可用性；C.网络信息的保密性；网络信息的完整性；网络服务的保密性；D.网络信息的完整性；网络信息的保密性；网络服务的保密性

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

19

2 分

信息安全主要包括信息的保密性、真实性、完整性等，当完整性受到破坏时，信息可能受到了以下哪种攻击？（）

A.篡改；B.中断；C.窃听；D.以上都不正确

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

20

2 分

网络入侵攻击的方法层出不穷，在网络攻击中，端口扫描能够实现以下哪个目的？（）

A.信息收集；B.痕迹清除；C.身份隐藏；D.以上都不正确

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

21

2 分

网络入侵攻击的方法层出不穷，在网络攻击中，篡改日志文件的审计信息能够实现以下哪个目的？

A.攻击实施；B.攻击痕迹清除；C.信息收集；D.以上都不正确

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

22

2 分

身份隐藏即通过技术手段隐藏攻击者的身份信息。以下关于网络攻击中身份隐藏的说法正确的是（）

A.MAC 地址和 IP 地址能够被欺骗，邮件账户不能被欺骗；B.MAC 地址、IP 地址以及邮件账户都能被欺骗；C.IP 地址能够被欺骗，MAC 地址以及邮件账户不能被欺骗；D.以上都不正确

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

23

2 分

以下关于 Windows 环境下和 Linux 环境下 ping 命令的描述正确的是（）

A.ping 命令的参数完全相同；B.ping 命令的参数有所不同；C.ping 命令的使用方法完全相同；D.ping 命令在两个环境下的作用完全不同

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

24

2 分

以下不属于网络安全策略实施原则的是（）

A.最小特权原则；B.最小泄露原则；C.多级安全策略；D.最大传输原则

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

25

2 分

主体执行任务时，按照主体需要知道的信息最小化的原则分配给主体权力指下列哪个实施原则？

A.最小特权原则；B.最小泄露原则；C.多级安全策略；D.以上都不正确

正确答案是：B　你的答案是：A　　此题得分：0

展开解析

26

2 分

主机防火墙是指驻留在网络主机并对主机系统提供安全防护的软件产品。以下对主机防火墙的描述正确的是（）

A.主机防火墙是一种软件防火墙产品；B.主机防火墙是一种硬件防火墙产品；C.主机防火墙是一种防病毒产品；D.以上都不正确

正确答案是：A　你的答案是：C　　此题得分：0

展开解析

27

2 分

以下对混合型病毒的描述正确的是（）

A.破坏性不大，易于查杀；B.只能感染磁盘的引导记录，不能感染可执行文件；C.既能感染磁盘的引导记录，也能感染可执行文件；D.以上都不正确

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

28

2 分

传输层协议允许应用程序同其他应用程序通信。以下属于传输层协议的是（）

A.TCP；B.ipconfig；C.ping；D.register

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

29

2 分

网络层协议处理机器到机器的通信。以下属于网络层协议的是（）

A.IP；B.ping；C.register；D.以上都不正确

正确答案是：A　你的答案是：C　　此题得分：0

展开解析

30

2 分

OSI 即开放式系统互联，以下不属于 OSI 七层网络模型的是（）

A.应用层；B.网络层；C.传输层；D.软件层

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

31

2 分

小明收到陌生中奖短信，要求其提供身份信息领奖，小明可能受到以下哪种攻击？（）

A.蠕虫病毒；B.社会工程学；C.勒索病毒；D.木马

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

32

2 分

TCP 协议是一种面向连接的、可靠的、基于字节流的通信协议。TCP 协议应用于下列哪个通信层？（）

A.传输层；B.物理层；C.应用层；D.网络层

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

33

2 分

以下关于源代码审核的简介正确的是（）

A.源代码审核过程不必遵循信息安全保障技术框架模型；B.源代码审核中有利于发现软件编码中存在的安全问题，相关的审核工具既有商业化的工具，也有开源工具；C.源代码审核效率一定很高；D.源代码审核能起到很好的安全保证作用，如果执行了源代码审核，则不需要在对该软件进行安全测试

正确答案是：B　你的答案是：B　此题得分：2

展开解析

34

2 分

以下关于变更管理说法错误的是（）

A.一个项目从开始就处于变化之中；B.软件开发组织需要有一个正式的变更管理过程；C.需求变化、测试发现问题、人员流失都会引起变更的发生；D.Bug 管理、需求管理和风险控制等与变更管理无关

正确答案是：D　你的答案是：C　此题得分：0

展开解析

35

2 分

关于测试用例，下列说法中正确的是（）

A.测试用例应由输入数据和预期的输出数据两部分组成；B.测试用例只需选用合理的输入数据；C.程序员可以很全面地测试自己的程序；D.测试用例只需检查程序是否做了该做的事即可

正确答案是：A　你的答案是：A　此题得分：2

展开解析

36

2 分

如果发送方使用的加密密钥和接受方使用的解密密钥不相同，从其中的一个密钥很难推出另一个密钥，它属于以下哪个系统？

A.公钥加密系统；B.单密钥加密系统；C.对称加密系统；D.常规加密系统

正确答案是：A　你的答案是：B　　此题得分：0

展开解析

37

2 分

以下属于 MAC（Media Access Control，介质访问控制）地址的是（）

A.192.168.3.91；B.172.43.119.168:21；C.00-01-6C-06-A6-29；D.Fec0:0:0:ffff::1%1

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

38

2 分

由某个组织构建、专门供内部成员或合作伙伴使用的云被称作以下哪项？（）

A.公有云；B.私有云；C.混合云；D.以上均不是

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

39

2 分

将 CPU、网络和磁盘等原始虚拟计算基础设施作为服务交付给用户的模型被称作下列哪项？

A.基础设施即服务；B.平台即服务；C.软件即服务；D.存储即服务

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

40

2 分

以下对云计算数据中心安全部署的描述错误的是（）

A.遵循的安全原则是保护基础设施、网络、应用安全；B.部署方式与传统数据中心完全相同；C.需实现虚拟机之间的安全防护；D.需形成安全风险快速反应机制

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

41

2 分

以下身份认证方式不属于强认证方式的是（）

A.密码认证；B.实物认证；C.身份认证；D.多因子认证

正确答案是：A　你的答案是：B　　此题得分：0

展开解析

42

2 分

关于对称密码体制，下列说法中错误的是（）

A.对称密码体制即传统密码体制；B.对称密码体制不使用密钥；C.对称密码体制加密和解密都使用相同密钥；D.对称密码体制也可被称为私钥密码体制

正确答案是：B　你的答案是：A　　此题得分：0

展开解析

43

2 分

VPN 即虚拟专用网络，用于传输隐私信息。关于 VPN 的基本功能，下列描述中错误的是（）

A.发送明文数据包；B.身份认证；C.访问控制；D.数据完整性和机密性

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

44

2 分

下面哪个选项不是未来 VPN 的发展方向？

A.基于网络的 VPN；B.基于 MPLS 的 VPN；C.防火墙和 VPN 设备的集成；D.基于明文传输的 VPN

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

45

2 分

VPN 网络设计的安全性原则不包括（）

A.无隧道；B.数据验证；C.用户识别与设备验证；D.入侵检测与网络接入控制

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

46

2 分

一个安全操作系统的开发过程不包括（）

A.系统需求分析；B.系统功能描述；C.配置管理和文档管理；D.系统实现

正确答案是：C　你的答案是：B　　此题得分：0

展开解析

47

2 分

PKI 即公钥基础设施，以下不属于 PKI 性能要求的是（）

A.透明性和易用性；B.不可扩展性；C.互操作性；D.多用性

正确答案是：B　你的答案是：B　此题得分：2

展开解析

48

2 分

逻辑安全方面的威胁不包括下列哪项？

A.掉电；B.假冒；C.截取；D.篡改

正确答案是：A　你的答案是：A　此题得分：2

展开解析

49

2 分

SSL 即安全套接层，它主要提供三方面的服务，不包括下列哪项？

A.认证用户和服务器；B.加密数据以隐藏被传送的数据；C.维护数据的完整性；D.声波传输

正确答案是：D　你的答案是：D　此题得分：2

展开解析

50

2 分

以下不属于计算机网络安全服务的是哪个？

A.保密性服务；B.HTTP 服务；C.认证服务；D.非否认服务

正确答案是：B　你的答案是：D　　此题得分：0

展开解析

第十三章

1

2 分

组织识别风险后，可采取的处理方式不包括（）

A.缓解风险；B.转移风险；C.接受风险；D.忽略风险

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

2

2 分

密码分析者仅能通过截获的密文破解密码，这种攻击密码的类型为（）

A.选择明文攻击；B.选择密文攻击；C.仅知密文攻击；D.已知明文攻击

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

3

2 分

密码分析者已知“明文-密文对”，以此来破解密码，这种攻击密码的类型为（）

A.选择密文攻击；B.仅知密文攻击；C.选择明文攻击；D.已知明文攻击

正确答案是：D　你的答案是：D　此题得分：2

展开解析

4

2 分

密码分析者不仅得到了一些“明文-密文对”，还可以选择被加密的明文，并获得相应的密文，这种攻击密码的类型为（）

A.选择明文攻击；B.已知明文攻击；C.选择密文攻击；D.仅知密文攻击

正确答案是：A　你的答案是：A　此题得分：2

展开解析

5

2 分

密码分析者可以选择一些密文，并得到相应的明文，这种攻击密码的类型为（）

A.仅知密文攻击；B.已知明文攻击；C.选择明文攻击；D.选择密文攻击

正确答案是：D　你的答案是：D　此题得分：2

展开解析

6

2 分

常见的并且仍然有效的古典密码有置换密码和代替密码，把明文按行写入、按列读出密文的方式属于

A.置换密码；B.代替密码；C.两者都是；D.两者都不

正确答案是：A　你的答案是：B　此题得分：0

展开解析

7

2 分

UNIX 系统 access( )函数用于文件的存储类型，此函数需要两个参数，分别为（）

A.文件名和要检测的文件类型；B.文件名和文件大小；C.文件名和创建日期；D.文件名和最后修改日期

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

8

2 分

随着网络环境的日益复杂，网络攻击手段也越来越多，其中通过伪造源 IP 地址，从而冒充其他系统或发件人的身份指（）

A.IP 地址欺骗；B.信息篡改；C.MAC 地址欺骗；D.以上都不正确

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

9

2 分

各种各样的网络攻击手段，严重威胁着网络安全。根据攻击方式，可将网络攻击分为（），其中前者会造成数据流的篡改和虚假数据流的产生，后者通常不会对数据信息进行修改

A.破坏性攻击和非破坏性攻击；B.模式攻击和非模式攻击；C.主动攻击和被动攻击；D.以上都不正确

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

10

2 分

操作系统用于管理和控制计算机的硬件和软件资源，而 Windows 操作系统是目前主流操作系统之一，其目录结构是（）结构

A.环状；B.树状；C.线状；D.以上都不正确

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

11

2 分

随着网络环境的日益复杂，网络攻击手段也层出不穷，以下不属于网络攻击中的主动攻击的是（）

A.篡改；B.伪造；C.拒绝服务；D.窃听

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

12

2 分

网络攻击严重威胁着网络安全，根据攻击位置可对网络攻击进行划分，其中外部攻击者通过各种手段，从该子网以外的地方向该子网或者该子网内的系统发动攻击指（）

A.远程攻击；B.本地攻击；C.伪远程攻击；D.以上都不正确

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

13

2 分

数据库用于存储数据。为保证事务过程中数据的正确性，一个支持事务的数据库需要具备 ACID 四个基本性质，其中 A、C、I、D 依次代表（）

A.原子性、一致性、隔离性、持久性；B.原子性、保密性、完整性、持久性；C.可用性、一致性、完整性、持久性；D.可用性、保密性、隔离性、持久性

正确答案是：A　你的答案是：B　　此题得分：0

展开解析

14

2 分

公钥算法中，（）用来加密和验证

A.数字证书；B.注册中心；C.公钥；D.私钥

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

15

2 分

公钥算法中，（）用来解密和签名

A.公钥；B.私钥；C.数字证书；D.注册中心

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

16

2 分

OSI 模型中实现数据分段、传输和组装功能的层级是（）

A.数据链路层；B.网络层；C.传输层；D.应用层

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

17

2 分

以下不属于云存储优势的选项是？（）

A.成本高；B.便捷访问；C.具备海量扩展能力；D.实现负载均衡

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

18

2 分

是一种以数据为中心的存储策略，这种存储策略利用分布式技术将数据按照一定规则保存到满足条件的非本地的节点中

A.关系数据库存储策略；B.日志存储；C.分布式存储；D.键值数据库存储策略

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

19

2 分

Hadoop 分布式文件系统（HDFS）是一种可运行在通用硬件上的分布式文件系统，以下不属于 HDFS 文件系统特点的是（）

A.满足超大规模的数据集需求；B.支持流式的数据访问；C.能容忍节点失效的发生；D.扩展性较弱

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

20

2 分

是建立在关系数据库模型基础上的数据库，借助于集合代数等概念和方法来处理数据库中的数据

A.关系数据库；B.键值数据库；C.非关系数据库；D.面向对象数据库

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

21

2 分

以下对于使用告警查询的描述错误的是？（）

A.告警时间要保证准确；B.告警确认、删除需慎重；C.维护人员可以进行任何时间段本地网内的告警历时的统计。；D.查询告警后，不必对网管数据进行数据备份

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

22

2 分

通信设备运行异常时所触发的消息被称为（）

A.通信请求；B.网络告警；C.事件统计；D.应答响应

正确答案是：B　你的答案是：D　　此题得分：0

展开解析

23

2 分

DHCP 协议提供自动分配 IP 地址的服务，DHCP 协议工作在

A.数据链路层；B.传输层；C.网络层；D.应用层

正确答案是：D　你的答案是：C　　此题得分：0

展开解析

24

2 分

IEEE 802 标准把数据链路层分为两个子层，其中与硬件无关，实现流量控制功能的是

A.逻辑链路控制层；B.媒体介入控制层；C.传输层；D.物理层

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

25

2 分

IEEE 802 标准把数据链路层分为两个子层，其中与硬件相关的是

A.传输层；B.物理层；C.逻辑链路控制层；D.媒体介入控制层

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

26

2 分

CSMA/CD 是一种争用型的介质访问控制协议，下列对其工作原理描述错误的是

A.发送数据前，先监听信道是否空闲；B.发送数据时，边监听边发送；C.若监听到空闲则立刻发送数据；D.发送冲突后立即重传数据

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

27

2 分

IP 地址分为 A、B、C、D、E 五类，其中（）类地址保留用于实验

A.A；B.B；C.D；D.E

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

28

2 分

B 类子网掩码为 255.255.240.0，则其建网比特数为（）

A./16；B./20；C./24；D./30

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

29

2 分

C 类子网掩码为 255.255.255.192，则其子网络数为（）

A.2；B.4；C.6；D.16

正确答案是：B　你的答案是：A　　此题得分：0

展开解析

30

2 分

B 类子网掩码为 255.255.255.224，则其可用主机数为（）

A.26；B.28；C.30；D.32

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

31

2 分

已知 IP 地址为 10.3.8.109，子网掩码为 255.255.128.0，则其广播地址为（）

A.10.3.8.255；B.10.3.127.255；C.10.3.128.255；D.10.3.255.255

正确答案是：B　你的答案是：C　此题得分：0

展开解析

32

2 分

下列关于 WWW 的说法中错误的是（）

A.WWW 全称为 World Wide Web；B.WWW 使用 HTTP 协议；C.WWW 广泛为人们使用；D.WWW 是局域网

正确答案是：D　你的答案是：D　此题得分：2

展开解析

33

2 分

IPV6 使用了（）位的二进制数字来标识网络和终端

A.128；B.32；C.64；D.256

正确答案是：A　你的答案是：D　此题得分：0

展开解析

34

2 分

MD5 信息摘要算法使用（）位摘要值，以确保信息传输的完整性

A.11；B.128；C.13；D.23

正确答案是：B　你的答案是：B　此题得分：2

展开解析

35

2 分

在“运行”对话框中输入（）可以运行命令提示符

A.CMD；B.PING；C.SEND；D.RESPONSE

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

36

2 分

VPN 即虚拟专用网络，用于传输隐私信息。下列说法不正确的是（）

A.虚拟专用网是利用公众网资源为客户构成专用网的一种业务；B.使用 VPN 后就不需要再使用防火墙和入侵检测系统，VPN 可以提供完善的安全保障；C.VPN 可以看作是企业网在 Internet 上的延伸；D.安全性是 VPN 设计时的最主要的问题

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

37

2 分

为保障信息系统的安全性，信息系统还需具备不可否认性，其中不可否认性指（）

A.信息在传输、交换、存储和处理过程保持非修改、非破坏和非丢失的特性；B.对流通在网络系统中的信息传播及具体内容能够实现有效控制的特性；C.通信双方在信息交互过程中，所有参与者都不可能否认或抵赖本人的所做的操作；D.信息按给定要求不泄漏给非授权的个人、实体或过程

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

38

2 分

入侵检测系统配合应用规则能更好地记录恶意用户的入侵行为。（）不存在于入侵检测系统的应用规则中

A.源 IP 地址；B.目的 IP 地址；C.日志条目；D.目的端口

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

39

2 分

P2DR 模型是美国 ISS 公司提出的动态网络安全体系的代表模型。（）不属于动态安全模型 P2DR 的组成部分

A.Policy；B.Protection；C.Detection；D.Request

正确答案是：D　你的答案是：C　　此题得分：0

展开解析

40

2 分

数字签名是一种用于鉴别数字信息的方法。现代的数字签名使用（）加密的方法

A.私钥；B.公钥；C.CC；D.RA

正确答案是：A　你的答案是：B　　此题得分：0

展开解析

41

2 分

计算机操作系统是管理和控制计算机软硬件资源的计算机程序。以下不属于操作系统基本特征是（）

A.共享性；B.并发性；C.封闭性；D.异步性

正确答案是：C　你的答案是：C　此题得分：2

展开解析

42

2 分

存储保护技术通过控制对存储器的读写功能来保护计算机的工作状态和数据信息等，存储保护一般（）

A.以硬件为主，软件为辅；B.以软件实现；C.以硬件实现；D.上述都不正确

正确答案是：A　你的答案是：A　此题得分：2

展开解析

43

2 分

现已产生多种方法可用于鉴别病毒，下列选项中，利用病毒的特有行为特征来监测病毒的方法被称为（）

A.代码测试法；B.校验和法；C.行为监测法；D.软件模拟法

正确答案是：C　你的答案是：C　此题得分：2

展开解析

44

2 分

计算机密码学是研究编制密码和破译密码的技术科学，以下不属于密码系统主要组成部分的是（）

A.明文；B.密文；C.传播媒介；D.密钥

正确答案是：C　你的答案是：C　此题得分：2

展开解析

45

2 分

入侵检测系统（IDS）作为一种网络安全设备，能对网络传输流量进行监测。其中入侵检测的规则指（）

A.确定 IDS 应用程序如何工作的具体条目；B.一个完整的特征数据库；C.一个在安全策略中常规应用的术语；D.一个与 IDS 分离的应用程序

正确答案是：A　你的答案是：B　　此题得分：0

展开解析

46

2 分

数据备份是容灾的基础，用于防止操作失误、系统故障等因素导致的数据的丢失。关于数据备份，下列说法中不正确的是（）

A.数据备份不只是简单的数据文件拷贝，多数情况下是指数据库的备份；B.当系统数据由于某种原因丢失或不可用时，可使用备份的数据进行恢复；C.不同的企业和单位需根据自身需求设计数据备份策略；D.数据备份的内容不包括系统数据，由用户自行选择

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

47

2 分

属性证书是一种轻量级的数字证书，（）使用属性证书来强化对特权的管理

A.个人标识信息；B.授权管理基础设施；C.信息传递接口；D.数字签名

正确答案是：B　你的答案是：A　　此题得分：0

展开解析

48

2 分

PKI 运用公钥技术，提供加密和数字签名等服务，它的运作大体包括的策划、（）和运营三个阶段

A.实施；B.准备；C.备份；D.交付

正确答案是：A　你的答案是：B　此题得分：0

展开解析

49

2 分

OSI 是一个开放性的通信系统互连参考模型，共有七层结构，自下而上第五层是（）

A.物理层；B.数据链路层；C.会话层；D.传输层

正确答案是：C　你的答案是：C　此题得分：2

展开解析

50

2 分

（）作为计算机系统内保护装置的总体，建立了一个基本的保护环境

A.软件；B.硬件；C.可信计算基；D.安全策略

正确答案是：C　你的答案是：D　此题得分：0

第十四章

1

2 分

容灾系统可用性与指标 RPO、RTO 的关系是（ ）

A.RPO 和 RTO 越大，可用性越大；B.RPO 和 RTO 越小，可用性越大；C.RPO 越大，RTO 越小，可用性越大；D.RPO 越小，RTO 越大，可用性越大

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

2

2 分

一个基于特征的入侵检测系统根据　　（）对一个攻击做出反应

A.正确配置的域名系统；B.正确配置的规则；C.特征库；D.日志系统

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

3

2 分

PKI 具有两种模式分别为自建和托管，（　）指用户购买单独的软件 PKI/CA 软件构建单独的系统

A.自筹；B.信任；C.委托；D.自建

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

4

2 分

信息隐藏是把机密信息隐藏在大量信息中不让对手察觉的一种技术。下列哪种信息隐藏技术属于基于文本的语义隐藏？（）

A.根据文字表达的多样性进行同义词置换；B.在文件头、尾嵌入数据；C.修改文字的字体来隐藏信息；D.对文本的字、行、段等位置做少量修改

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

5

2 分

防火墙是一个由软硬件组成的安全产品。以下对防火墙的需求描述不正确的是（）

A.保证内部网安全性；B.保证内外网的连通性；C.保证防火墙的绝对安全；D.对渗透的抵御性

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

6

2 分

包过滤技术是指根据数据包的包头信息采取相应的包处理措施。以下关于包过滤的描述错误的是（）

A.包过滤对用户是透明的；B.能阻止任意攻击；C.防火墙维护比较困难；D.处理包的数据比代理服务器快

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

7

2 分

数据备份系统即备份重要数据的系统。数据备份系统的基本构成中不包括下列哪个？

A.存储介质；B.软件；C.硬件；D.备份策略

正确答案是：D　你的答案是：C　　此题得分：0

展开解析

8

2 分

SQL Server 备份为存储其中的关键数据提供了基本的安全保障。下列关于 SQL Server 数据库备份特点描述不正确的是（）

A.备份主要使用内置于 SQL Server 的数据库引擎；B.SQL Server 一定不支持完整备份；C.数据备份可在线完成；D.可以备份到磁带或者磁盘

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

9

2 分

在一个支持事务的数据库中，数据库的原子性体现在事务在执行过程中发生错误时，会进行下列选项中的哪一个操作？（）

A.回滚；B.删除；C.复制；D.更新

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

10

2 分

数据库是按照数据结构来组织、存储和管理数据的仓库，其中层次数据库采用层次模型作为数据的组织方式，它使用哪一种结构表示各类实体以及实体间的联系？

A.树形结构；B.网状结构；C.线性结构；D.星形结构

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

11

2 分

关系数据库指建立在关系模型基础上的数据库，关系模型的数据操纵主要包括查询、插入、删除和更新数据，这些操作必须满足关系的完整性约束条件，包括（）

A.实体完整性；B.参照完整性；C.用户定义的完整性；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

12

2 分

数据库指按照数据结构来组织、存储和管理数据的仓库。在关系数据库中，（）指一个列或多列的组合，其值能唯一标识表中的每条记录

A.主键；B.外键；C.实体；D.属性

正确答案是：A　你的答案是：D　　此题得分：0

展开解析

13

2 分

网络环境日益复杂，网络攻击手段也层出不穷，其中攻击者通过发送一个目的主机已接受过的数据包，以达到欺骗系统的目的的攻击被称为（）

A.拒绝服务攻击；B.重放攻击；C.穷举攻击；D.以上都不正确

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

14

2 分

日志对于系统安全十分重要，以下不属于 UNIX/Linux 系统日志子系统的是？（）

A.登录时间日志子系统；B.进程统计日志子系统；C.漏洞扫描日志子系统；D.错误日志子系统

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

15

2 分

系统日志可以记录系统各类问题，检测系统中发生事件，以下不属于 Windows 系统日志文件的是？（）

A.系统日志；B.账户日志；C.应用程序日志；D.安全日志

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

16

2 分

FTP 是文件传送协议的简称，以下关于 FTP 传输的叙述错误的是（）

A.“下载”文件就是从远程主机拷贝文件至自己的计算机上；B.只能用于 Internet 上的控制文件的单向传输；C.“上传”文件就是将文件从自己的计算机中拷贝至远程主机上；D.FTP 的传输有两种方式：ASCII 传输模式、二进制数据传输模式

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

17

2 分

（）　可以将事件之间的关联关系可视化为一幅事件图，形象地展现出当前事件网络的关系和状态

A.交互图；B.雷达图；C.主动事件图；D.统计图

正确答案是：C　你的答案是：A　　此题得分：0

展开解析

18

2 分

以下对于 Syslog 的叙述不正确的是（）

A.它是一种工业标准的协议；B.它分为客户端和服务器端；C.它是一个在 IP 网络中转发系统日志信息的标准；D.它只能记录系统中的部分事件

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

19

2 分

漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷。以下属于常见的应用软件安全漏洞的是（）

A.爬虫盗链；B.XSS 跨站脚本漏洞；C.SQL 注入漏洞；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

20

2 分

信息技术安全性评估通用标准用于评估信息系统、信息产品的安全性，其又被称为（）

A.ISO 标准；B.HTTP 标准；C.IEEE 标准；D.CC 标准

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

21

2 分

为了提高软件设计的安全性，需遵循安全设计原则，以下不属于安全设计原则的是（）

A.最小特权原则；B.简单原则；C.攻击面最大化原则；D.纵深防御原则

正确答案是：C　你的答案是：C　此题得分：2

展开解析

22

2 分

设计模式总结于众多优秀软件系统，是针对某一类问题的最优解决方案。在 Java 中主要可分为三类，以下选项中不属于此三类模式的是（）

A.数据型模式；B.行为型模式；C.结构型模式；D.创建型模式

正确答案是：A　你的答案是：D　此题得分：0

展开解析

23

2 分

设计模式指针对某一类问题的最优解决方案。在 Java 中可将设计模式分为三类，以下选项中不属于结构型模式的是（）

A.组合模式；B.命令模式；C.桥接模式；D.代理模式

正确答案是：B　你的答案是：A　此题得分：0

展开解析

24

2 分

威胁建模可对影响系统的威胁进行识别和评价，其中分解应用程序阶段执行的任务不包括（）

A.标识数据流；B.标识入口点；C.标识信任边界；D.反编译

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

25

2 分

使用分类的威胁列表识别威胁时，执行的任务包括（）

A.识别网络威胁；B.识别主机威胁；C.识别应用程序威胁；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

26

2 分

整型溢出漏洞是需要注意以及防范的，以下选项中对其的描述错误的是（）

A.在计算机中，整数分为无符号整数以及有符号整数两种；B.将数据放入了比它本身小的存储空间中会出现溢出现象；C.在计算机中，有符号整数会在最高位用 1 表示正数，用 0 表示负数；D.无符号整数的下溢和上溢可能导致安全性漏洞

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

27

2 分

C 语言是一门通用计算机编程语言。在 C 语言中，指针变量不可以指向的位置是（）

A.实际物理地址；B.静态变量；C.堆地址；D.空地址单元

正确答案是：A　你的答案是：D　　此题得分：0

展开解析

28

2 分

C++擅长面向对象程序设计的同时，还可以进行基于过程的程序设计，在 C++语言中，以下情况需要调用拷贝构造函数的是（）

A.对象以值传递的方式传递给函数参数；B.对象以值传递的方式从函数返回；C.对象用于给另一个对象进行初始化；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

29

2 分

Java 是一门面向对象编程的语言，以下对 Java 平台描述不正确的是（）

A.Java 平台由 Java 虚拟机和 Java 应用编程接口两部分构成；B.Java 虚拟机是运行所有 Java 程序的抽象计算机；C.Java 应用编程接口是一些预先定义的函数；D.Java 应用编程接口是实现 Java 语言跨平台特性的关键

正确答案是：D　你的答案是：B　　此题得分：0

展开解析

30

2 分

HASH 算法将任意长输入变换为固定长输出，以下属于该算法的用途的是（）

A.用于消息摘要；B.用于数字签名；C.用于验证消息完整性；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

31

2 分

Java 具有简单易用和功能强大两个特性，以下关于 Java 编码规范的描述正确的是（）

A.良好的编码规范有利于提高编码效率；B.在 clone()方法中调用可重写的方法是绝对安全的；C.“= =”和 equals()都可进行对象的比较，两者没有区别；D.重用公有的标识会降低代码的可读性和可维护性

正确答案是：D　你的答案是：A　此题得分：0

展开解析

32

2 分

PHP 是一种通用开源脚本语言，以下对 PHP 特点的描述不正确的是（）

A.开源自由；B.语法简单；C.具有良好的可扩展性；D.程序编程仅有面向过程

正确答案是：D　你的答案是：D　此题得分：2

展开解析

33

2 分

PHP 语言使用广泛，主要只用于 Web 开发领域。PHP 有其特点，也有缺点，以下不属于 PHP 语言缺点的是（）

A.效率低；B.函数命名不严谨；C.缺乏统一编码规范；D.异常处理功能不广泛

正确答案是：A　你的答案是：A　此题得分：2

展开解析

34

2 分

Session 在网络应用中被称为会话控制，以下对 Session 攻击的描述不正确的是（）

A.Session 有关的攻击主要分为会话劫持和会话固定；B.攻击者获取用户的 Session ID 方法单一；C.会话劫持通过获取用户的 Session ID 冒充被攻击用户进行非法操作；
D.Session 攻击是攻击者最常用的攻击手段之一

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

35

2 分

客户端脚本植入指将可以执行的脚本插入到表单、图片、动画或超链接文字等对象内。当用户打开这些对象后，脚本将被执行，进而进行攻击。下列哪个选项不属于常用的被用作脚本植入的 HTML 标签？

A.<script>标签；

B.<embed>标签；

C.
标签；

D.<form>标签

正确答案是：C　你的答案是：B　　此题得分：0

展开解析

36

2 分

Python 能处理程序运行中出现的异常和错误，以下关于 Python 语言异常处理机制的描述正确的是（）

A.在 Python 中，常使用“try...except...finally...”错误处理机制来进行异常处理；B.在 Python 中，不可能使用相同的 except 语句处理多个异常信息；C.在 Python 中，ImportError 指输入输出错误；D.在 Python 中，IOError 指无法引入模块或包

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

37

2 分

文件上传是 Web 应用常见的功能，若文件上传时未对其正确处理，容易引发安全问题。以下对文件上传攻击的描述不正确的是（）

A.用户上传的文件被安全监测格式化仍可以完成攻击；B.Web 服务器能够访问上传文件；C.上传的文件需要能够被 Web 容器解释执行；D.文件上传攻击是通过上传的可执行脚本文件执行服务器端的命令

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

38

2 分

Python 是一门强大的面向对象的程序设计语言。以下关于 Python 安全编码规范的描述正确的是（）

A.Python 语言对缩进非常敏感；B.编码过程中应为了遵守编码规范而破坏兼容性；C.对于长的多个 with 状态语句，可以直接使用隐式续行；D.Python3 中允许同时使用空格和制表符进行缩进

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

39

2 分

安全测试用于提高软件系统的安全性，以下关于安全测试的描述中错误的是（）

A.黑盒测试主要针对程序所展现给用户的功能；B.白盒测试是针对被测单元内部是如何工作进行的测试；C.灰盒测试是介于黑盒测试和白盒测试之间的一种测试；D.黑盒测试可以完全取代白盒测试

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

40

2 分

DREAD 是用于判断漏洞优先级的典型模型，其名字来源于五条评估条目的首字母，下列选项中不属于这五条评估条目的是（）

A.危害性；B.灵活性；C.复现性；D.受影响用户数

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

41

2 分

模糊测试作为一种软件安全技术，通过对非预期的输入可能产生的异常结果进行监视以发现软件漏洞。以下对其的描述错误的是（）

A.模糊测试介于完全手工测试和完全自动化测试之间；B.模糊测试可以有效地找出安全漏洞；C.模糊测试中常见的测试对象是文件格式和网络协议；D.模糊测试属于白盒测试

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

42

2 分

在模糊测试中，通常使用模糊器生成测试用例。其中本地模糊器通常会关注的输入包括（）

A.命令行参数；B.环境变量参数；C.文件格式；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

43

2 分

WAF 是 Web 应用防护系统的简称，用以弥补防火墙等安全设备对 Web 应用攻击防护能力的不足。以下选项中不属于 WAF 具备的功能的是（）

A.Web 非授权访问的防护功能；B.Web 恶意代码的防护功能；C.Web 攻击的防护功能；D.Web 数据的加密功能

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

44

2 分

HTTP 报文主要分为请求报文和响应报文，以下选项中不属于请求报文组成部分的是（）

A.请求行；B.状态行；C.请求头；D.请求实体

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

45

2 分

服务器在接收到 HTTP 请求报文之后，会返回一个 HTTP 响应报文。以下选项中不属于响应报文组成部分的是（）

A.状态行；B.响应头；C.响应实体；D.请求行

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

46

2 分

HTTP 报文主要分为请求报文和响应报文，其中 HTTP 响应报文由状态行等三个部分组成，以下选项中不属于状态行内容的是（）

A.HTTP 协议版本号；B.状态码；C.描述状态的短语；D.响应正文

正确答案是：D　你的答案是：D　此题得分：2

展开解析

47

2 分

HTTP 协议应用广泛，但是仍然存在许多安全缺陷，以下对其安全缺陷的描述错误的是（）

A.HTTP 协议在设计时未考虑信息的加密和验证；B.HTTP 协议面临数据明文传输问题，但具有良好的消息完整性验证；C.HTTP 协议在数据传输过程中，易被嗅探和篡改；D.HTTP 协议在传输请求和响应时，报文头部包含的传输数据的长度易被篡改

正确答案是：B　你的答案是：D　此题得分：0

展开解析

48

2 分

注入类漏洞是一种常见的安全漏洞，其中 SQL 注入漏洞是一种危害性较大的注入类漏洞。一般情况下，以下不属于 SQL 注入攻击流程的是（）

A.发送大量的数据报文导致系统死机；B.探测 SQL 注入点；C.判断数据库类型；D.提升权限进一步攻击

正确答案是：A　你的答案是：A　此题得分：2

展开解析

49

2 分

SQL 注入攻击会造成较大的危害，以下选项中属于 SQL 注入攻击主要注入方式的是（）

A.利用用户输入注入；B.利用 Cookies 注入；C.利用系统变量注入；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

50

2 分

跨站脚本攻击是一种针对客户端浏览器的注入攻击。根据 XSS 漏洞注入位置和触发流程的不同，可将 XSS 漏洞划分为反射型 XSS 漏洞，存储型 XSS 漏洞以及（）

A.基于 RAM 型 XSS 漏洞；

B.基于 DOM 型 XSS 漏洞；

C.本地利用漏洞；

D.以上都不正确

正确答案是：B　你的答案是：B　　此题得分：2

第十五章

聚焦网络爬虫指选择性地爬行与预先定义好的主题相关的网页。以下属于常用的聚焦爬虫爬行策略的是（）

A.基于内容评价的爬行策略；B.基于链接结构评价的爬行策略；C.基于增强学习的爬行策略；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

2

2 分

网络爬虫按照系统结构和实现技术可分为多种类型，其中对已下载网页采取增量式更新和只爬取新产生的或者已经发生变化网页的爬虫属于（）

A.增量式网络爬虫；B.聚焦网络爬虫；C.通用网络爬虫；D.以上都不正确

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

3

2 分

网络爬虫是搜索引擎的重要组成部分，但网络爬虫也带来了一定的安全风险。爬虫被非法利用可能带来的危害包括（）

A.核心文本被爬；B.注册用户被扫描；C.影响正常用户的访问；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

4

2 分

弱口令是一种危害性较大的安全漏洞，以下不属于针对弱口令攻击方法的是（）

A.穷举攻击；B.跨站脚本攻击；C.社会工程学攻击；D.直接破解系统的口令文件

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

5

2 分

分布式拒绝服务（DDoS）攻击是指攻击者利用分布式的客户端，向服务提供者发起大量请求，消耗或者长时间占用大量资源，从而使合法用户无法正常服务。DDoS 攻击主要表现出的特点不包括（）

A.攻击特征非常明显；B.攻击很容易防御；C.攻击由多个服务器同时发起；D.难以追踪真正的攻击发起者

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

6

2 分

分布式拒绝服务（DDoS）攻击具有多种分类标准。其中根据攻击消耗目标资源特点，可将 DDoS 分为三类，下列选项中不属于此三类的是（）

A.攻击网络带宽资源；B.攻击系统资源；C.攻击应用资源；D.SQL 注入攻击

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

7

2 分

传输控制协议（TCP）是一种面向连接的、可靠的、基于字节流的传输层通信协议，但其仍然存在着安全漏洞易被攻击者利用。以下不属于攻击者利用 TCP 协议的安全漏洞进行攻击的是（）

A.UDP 连接洪水攻击；B.TCP 连接洪水攻击；C.SYN 洪水攻击；D.RST 洪水攻击

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

8

2 分

威胁情报是一种基于证据的知识，它就网络资产可能存在或出现的风险、威胁，给出了相关联的场景、机制、指标、内涵及可行的建议等，可为主体响应相关威胁或风险提供决策信息。以 Web 攻击为例，威胁情报不可以提供（）

A.IP；B.URL；C.域名信息；D.用户密码

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

9

2 分

威胁情报的出现将网络空间安全防御从传统被动式防御转换到主动式防御。以下选项中不属于安全威胁情报基本特征的是（）

A.时效性；B.相关性；C.准确性；D.不可操作性

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

10

2 分

网络钓鱼攻击者通常利用欺骗性的电子邮件和伪造的 Web 站点来骗取用户的敏感信息。以下关于网络钓鱼攻击的防范措施不正确的是（）

A.认真核对邮件来源；B.避免下载来源不明的文件；C.对要求输入账号信息的邮件要提高警惕；D.可在任意网站进行在线交易

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

11

2 分

下列对哈希算法的描述错误的是（）

A.哈希算法输入输出的字符串长度都是任意的；B.安全散列算法是 FIPS 所认证的安全杂凑算法；C.安全哈希算法主要适用于数字签名标准里面定义的数字签名算法；D.哈希算法输出的字符串一般称为 Hash 值

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

12

2 分

以下关于 PHP 安全编码规范的描述，正确的是（）

A.在 PHP 中，可以直接使用“0/1”代替“true/false” ；B.在 PHP 中，单行注释符为“#”；C.在 PHP 项目中，“/scripts”路径下默认存放图片文件；D.在 PHP 项目中，可以将独立的功能模块写成函数

正确答案是：D　你的答案是：B　　此题得分：0

展开解析

13

2 分

Python 是一门有条理且强大的面向对象的程序设计语言，在 Python3 中，默认的源文件编码格式是（）

A.UTF-8 编码；B.ASCII 编码；C.GBK 编码；D.GB2312 编码

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

14

2 分

服务器配置是指根据企业的实际需求针对安装有服务器操作系统的设备进行软件或者硬件的相应设置、操作，从而实现企业的业务活动需求。以下关于企业信息系统中服务器配置的描述中，错误的是（）

A.Apache、Nginx 以及 IIS 都属于 Web 服务器；B.Mail 服务器可用于建立企业专属的邮件系统；C.不同企业信息系统服务器配置相同；D.FTP 服务器可提供安全内部网络的资源共享与文件传输

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

15

2 分

PDRR 安全模型是目前倡导的一种综合的安全解决方法，以下关于 PDRR 安全模型的描述，错误的是（）

A.PDRR 模型包括防护、检测、响应和恢复四个部分；B.PDRR 是一个动态的信息系统安全运营模型；C.PDRR 模型中，检测部分的功能就是检测入侵者的身份；D.响应是 PDRR 模型的最后一个环节，检测出入侵后，响应系统开始响应事件处理和其他业务

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

16

2 分

企业信息系统安全防护体系建设需要划分安全域，以下描述错误的是（）

A.划分安全域前需要确定企业信息系统安全防护体系的防护范围；B.确定安全域是企业信息系统安全防护体系建设的首要任务；C.划分安全域可以设立清晰的防护边界对系统进行保护；D.不能将相同安全防护需求的对象划分到同一个安全域

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

17

2 分

虚拟专用网(Virtual Private Network，VPN)是一种“基于公共数据网，给用户一种直接连接到私人局域网感觉的服务”。以下不属于 VPN 技术的接入方式的是（）

A.拨号 VPN；B.IPsec VPN；C.SSL VPN；D.APR VPN

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

18

2 分

入侵检测系统和入侵防御系统可以弥补防火墙功能的不足，以下关于它们的描述正确的是（）

A.入侵检测系统（IDS）在攻击发生之前，可以预先发出警报；B.入侵检测系统（IDS）倾向于提供主动防护，预先对入侵活动和攻击性网络流量进行拦截；C.入侵防御系统（IPS）不但能精确地检测到攻击行为，而且能通过一定的响应方式实时地终止入侵行为的发生；D.入侵防御系统（IPS）典型的部署方式是多 ISP 部署

正确答案是：C　你的答案是：B　　此题得分：0

展开解析

19

2 分

在自适应的安全防护体系中，关于安全策略基本的设计原则的描述，错误的是（）

A.先难后易；B.先急后缓；C.先众后寡；D.先端后网

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

20

2 分

不同设备、不同类型的安全数据的融合有利于网络安全事件的综合分析，以下不属于数据融合层次的是（）

A.原始数据融合；B.特征级融合；C.决策级融合；D.环境级融合

正确答案是：D　你的答案是：A　　此题得分：0

展开解析

21

2 分

网络中追踪溯源是指确定网络攻击者身份或位置及其中间介质的过程，网络攻击模型涉及到的机器不包括（）

A.僵尸机器；B.VPN 网关；C.攻击者；D.跳板

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

22

2 分

网络取证(network forensics)是抓取、记录和分析网络事件以发现安全攻击或其他的问题事件的来源，以下不属于网络取证特点的是（）

A.动态；B.实时；C.多态；D.稳定

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

23

2 分

网络取证可按照不同的方式划分为不同的类型，以下不属于网络取证分类方法的是（）

A.按照采集方式进行分类；B.按照随机事件进行分类；C.按照取证时延性进行分类；D.按照不同的视角进行分类

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

24

2 分

网络取证是一个迅速发展的研究领域，在网络信息安全方面有着重要的应用前景，以下不属于网络取证特征的是（）

A.客观性；B.关联性；C.随机性；D.合法性

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

25

2 分

蜜罐技术是一种能够主动的网络安全防御技术，以下不属于蜜罐配置模式的是（）

A.无监视配置；B.诱骗服务；C.弱化系统；D.用户模式服务器

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

26

2 分

在互联网出现之前，传统的应急响应技术具有以下特点（）

A.单一行业、专业、领域中的应对与处置，面对的事件复杂性相对较低；B.可以是对于一个区域内常见事件的应对与处置，人们认识角度比较单一；C.传统的多领域协同响应，应急中需要采用的技术手段和管理策略比较明晰；D.以上都是

正确答案是：D　你的答案是：D　此题得分：2

展开解析

27

2 分

信息系统应急响应在网络信息系统中至关重要，下列选项中关于现代应急响应技术的发展趋势特点的说法错误的是（）

A．开展体系性的建设与整合工作，不同层次的应急平台的功能和技术体系要有区别性；B．发达国家重视运用先进的网络技术、遥感技术、传感和信号处理技术，建立和完善网络化的国家级应急预警系统；C．加强应急平台涉及的公共安全基础数据的综合汇集与分级分类管理；D．重视灾害事故的时空风险预测、危险性分析与决策支持

正确答案是：A　你的答案是：D　此题得分：0

展开解析

28

2 分

参照国家标准 GB/Z20986-2007《信息安全事件分类指南》，根据信息安全事件发生的原因、表现形式等，对网络/信息安全事件进行分类，下列选项中说法错误的是（）

A.恶意程序事件是指蓄意制造、传播有害程序，或是因受到有害程序性的影响而导致的信息安全事件；B.网络攻击事件是指通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对信息系统实施攻击；C.信息破坏事件是指利用信息网络发布、传播危害国家安全、社会稳定和公共利益的内容的安全事件；D.设备设施故障是指由于信息系统自身故障或外围保障设施故障而导致的信息安全事件

正确答案是：C　你的答案是：D　此题得分：0

展开解析

29

2 分

根据我国网络安全事件的分类分级标准，将网络安全应急响应分成 4 级，特别重大的是（）

A.Ⅰ级；B.Ⅱ级；C.Ⅲ级；D.Ⅳ级

正确答案是：A　你的答案是：D　　此题得分：0

展开解析

30

2 分

基于闭环控制的动态信息安全理论模型在 1995 年开始逐渐形成并得到了迅速发展，以下不属于信息系统安全运营模型的是（）

A.PDRR 模型；B.WPDRRC 模型；C.PPDR 模型；D.SWOT 模型

正确答案是：D　你的答案是：B　　此题得分：0

展开解析

31

2 分

信息安全防护框架从下至上可分为网络层安全管控、虚拟层安全管控、系统层安全管控、应用层安全管控、数据层安全管控及用户层安全管控，以下不属于网络层安全管控内容的是（）

A．网络安全域控制；B．网络拥塞控制；C．网络准入控制；D．网络流量分析及监测

正确答案是：B　你的答案是：D　　此题得分：0

展开解析

32

2 分

信息系统安全运营大致分为信息系统安全防护和信息系统安全运维，其中信息系统的安全运维工作分为三个层次开展，不包括（）

A．基础实践层；B．安全能力层；C．信息收集层；D．展示决策层

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

33

2 分

对安全数据进行了有效的降维处理、关联、融合之后，开展具体的安全分析可以大致分为三个阶段，不包括（）

A.基础的安全数据分析；B.基于安全数据的行为分析；C.基于数学演算的理论分析；D.基于人工智能的安全分析和预警

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

34

2 分

虚拟专用网络（Virtual Private Network，简称 VPN)指的是在公用网络上建立专用网络的技术。关于 VPN 的发展，以下描述不正确的是（）

A.VPN 诞生之前，企业采用的方式是向电信运营商租赁专线为企业提供二层链路；B.VPN 诞生之前，随着异步传输模式和帧中继技术的兴起，电信运营商开始使用虚电路的方式来为企业建立点到点的二层链路；C.企业在传统网络的支持下，对网络的灵活性、安全性、经济性和扩展性等方面提出需求，VPN 由此应运而生；D.客户端通过 VPN 连接与专用网络中的计算机进行通信时，可以直接将所有数据传输到目的计算机

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

35

2 分

VPN 具有在公用网络上建立专用网络，进行加密通讯的功能。下列关于 VPN 的选项中，不正确的是（）

A.VPN 具有专用和虚拟两个特征；B.根据 VPN 应用平台可分为软件 VPN 和硬件 VPN 平台；C.按实现层次划分，VPN 技术包括基于数据链路层的 VPN、基于网络层的 VPN 技术、基于应用层的 VPN 技术等；D.企业内部虚拟专网指的是企业员工或企业的小分支机构通过公共网络远程拨号的方式构建的虚拟专用网，可以随时随地访问

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

36

2 分

VPN 指依靠 ISP 和其他 NSP（网络服务提供者）在公用网络（如 Internet、Frame Relay、ATM）建立专用的数据通信网络的技术。关于 VPN 支持的接入方式，以下选项不正确的是（）

A.拨号 VPN 远程接入；B.IPsec VPN 远程接入；C.SSL VPN 远程接入；D.Telnet 远程接入

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

37

2 分

SSL VPN 是解决远程用户访问公司敏感数据最简单最安全的解决技术。下列关于 SSL VPN 的特点的描述中，不正确的是（）

A.配置简单；B.成本较高；C.细分控制；D.认证多样

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

38

2 分

不同类型客户对 VPN 存在需求差异，其中不包括（）

A.技术方面的差异；B.客户具体需求的差异；C.IP 地址的差异；D.多样的应用需求差异

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

39

2 分

VPN 实质上就是利用加密技术在公网上封装出一个数据通讯隧道。关于 VPN 隧道技术，下列描述不正确的是（）

A.通过对通信数据进行封装，再在公共网络上建立一条通信双方专用的通道；B.将来自其他企业的数据装入隧道中传输；C.目前主要有两类隧道协议，分别是第二层（链路层）隧道协议和第三层（网络层）隧道协议；D.通过 VPN 隧道可以在 IP 网络中传输 ATM、FR 数据帧，或 IPX、Apple Talk 数据包

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

40

2 分

IPSec 不是一个单独的协议，而是包括一组协议，下列选项中不属于 IPSec 的是（）

A.认证头协议；B.封装有效载荷协议；C.密钥管理协议；D.SMTP 协议

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

41

2 分

分布式拒绝服务 DDoS 攻击是指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DDoS 攻击，从而成倍地提高拒绝服务攻击的威力，其英文全称是（）

A.Distributed Denial of Service；B.Distributed Denial of Standard；C.Dynamic Denial of Service ；D.Digital Distributed of Service

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

42

2 分

网络欺骗就是使入侵者相信信息系统存在有价值的、可利用的安全弱点，并具有一些可攻击窃取的资源（当然这些资源是伪造的或不重要的），并将入侵者引向这些错误的资源。以下哪种属于网络欺骗？

A.ARP 欺骗；B.DNS 欺骗；C.IP 欺骗；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

43

2 分

一个密码系统，通常简称为密码体制，由五部分组成：明文空间、密文空间、密钥空间、（）、解密算法

A.分配密钥；B.伪装数据；C.访问控制；D.加密算法

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

44

2 分

虽然用近代密码学的观点来看，许多古典密码是很不安全的，或者说是极易破译的，但是我们不能忘记古典密码在历史上发挥的巨大作用。以下哪项属于古典密码实例？

A.置换密码；B.代替密码；C.代数密码；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

45

2 分

根据明密文的划分和密钥的使用不同，可以将密码体制分为（）和序列密码。

A.代数密码；B.分类密码；C.分组密码；D.分级密码

正确答案是：C　你的答案是：C　此题得分：2

展开解析

46

2 分

用户的身份认证是许多应用系统的第一道防线，其目的在于识别用户的合法性，从而阻止非法用户访问系统。以下属于身份验证的是（）

A.口令验证；B.生物特征识别；C.手机验证码；D.以上都是

正确答案是：D　你的答案是：D　此题得分：2

展开解析

47

2 分

口令攻击是网络攻击的最简单、最基本的一种形式，以下属于口令攻击类型的是（）

A.字典攻击；B.强行攻击；C.组合攻击；D.以上都是

正确答案是：D　你的答案是：D　此题得分：2

展开解析

48

2 分

BGP 用于在不同的自制系统之间交换路由信息。以下说法错误的是（）

A.BGP 是外部网关协议，允许一个 AS 与另一个 AS 进行通信；B.BGP 支持基于策略的选择；C.BGP 路由信息的传输采用 UDP 协议；D.BGP 允许发送方把路由信息聚集在一起，用一个条目来表示多个相关的目的网络

正确答案是：C　你的答案是：D　　此题得分：0

展开解析

49

2 分

以下关于暗网说法错误的是（）

A.暗网是指那些存储在网络数据库里、不能通过超链接访问而需要通过动态网页技术访问的资源集合；B.暗网是深网的一部分；C.一般来说暗网都使用特定编码关键词技术，只有通过这一技术才能摸着它的边缘部分；D.虚拟网络不属于暗网

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

50

2 分

分布式拒绝服务(DDoS)攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DDoS 攻击，从而成倍地提高拒绝服务攻击的威力。以下属于被 DDoS 攻击时可能的出现的现象的是（）

A.被攻击主机上有大量等待的 TCP 连接；B.网络中充斥着大量的无用的数据包，源地址为假；C.制造高流量的无用数据，造成网络拥塞；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

第十六章

1

2 分

防火墙是一种较早使用、实用性很强的网络安全防御技术，以下关于防火墙说法错误的是（）

A.防火墙阻挡对网络的非法访问和不安全数据的传递；B.防火墙是一种动态安全技术；C.防火墙的安全规则由匹配条件与处理方式两个部分共同构成；D.防火墙使得本地系统和网络免于受到许多网络安全威胁

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

2

2 分

防火墙可以阻挡对网络的非法访问和不安全数据的传递使得本地系统和网络免于受到许多网络安全威胁。防火墙的经典体系结构主要有三种形式：（）、（）和（）

A.双重宿主主机体系结构 被屏蔽主机体系结构 被屏蔽子网体系结构；B.双重宿主主机体系结构 屏蔽主机体系结构 被屏蔽子网体系结构；C.双重宿主主机体系结构 被屏蔽主机体系结构 屏蔽子网体系结构；D.双重宿主主机体系结构 屏蔽主机体系结构 屏蔽子网体系结构

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

3

2 分

入侵检测与防护的技术主要有两种：入侵检测系统 IDS 和入侵防护系统 IPS。下列关于它们说法正确的是（）

A.IDS 注重网络安全状况的监管；B.IPS 倾向于提供主动防护，注重对入侵行为的控制；C.绝大多数 IDS 系统都是被动的；D.以上说法都对

正确答案是：D　你的答案是：A　此题得分：0

展开解析

4

2 分

点对点隧道协议 PPTP、第 2 层隧道协议 L2TP 和 IP 安全协议 IPSec 是三种最常见也是最为广泛实现的隧道技术，关于它们以下说法正确的是（）

A.PPTP 和 L2TP 的使用方式为通过隧道进行远程操作，网络模式为 C/S 模式；B.IPSec 的使用方式为 Intranet、Extranet 和通过隧道进行远程操作，网络模式为主机对主机的对等模式；C.PPTP、L2TP 和 IPSec 都有 IP 协议支持；D.以上说法都对

正确答案是：D　你的答案是：C　此题得分：0

展开解析

5

2 分

网络蜜罐技术是一种主动防御技术，是入侵检测技术的一个重要发展方向，以下关于蜜罐技术说法正确的是（）

A.蜜罐系统最主要的功能是对系统中所有的操作和行为进行监视和记录；B.根据产品设计目的可将蜜罐分为两类：产品型和研究型；C.在受防火墙保护的网络中，蜜罐通常放置在防火墙的外部或放置在防护程度较低的服务网络中；D.以上说法都对

正确答案是：D　你的答案是：C　此题得分：0

展开解析

6

2 分

以计算机资产为犯罪对象的具有严重社会危害性的行为定义为计算机犯罪，以下关于属于计算机犯罪的是（）

A.窃取和破坏计算机资产；B.未经批准使用计算机信息系统资源 ；C.批准或超越权限接受计算机服务；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

7

2 分

网络隔离是一项网络安全技术。它消除了基于网络和基于协议的安全威胁。以下关于网络隔离说法错误的是（）

A.网络隔离无法给出给出一个完整准确的技术定义；B.隔离的概念是基于网络来谈隔离的，没有联网的概念就没有隔离的必要 ；C.隔离的本质是在需要交换信息甚至是共享资源的情况下才出现，既要信息交换或共享资源，也要隔离；D.网络隔离技术的目标是确保把有害的攻击隔离，在可信网络之外和保证可信网络内部信息不外泄的前提下，完成网间数据的安全交换

正确答案是：A　你的答案是：B　　此题得分：0

展开解析

8

2 分

网络防火墙是最常用的网络隔离手段，它有一个显著的缺点：就是防火墙对于（）层没有控制，方便了木马的进入

A.网络；B.应用 ；C.运输；D.数据链路

正确答案是：B　你的答案是：D　　此题得分：0

展开解析

9

2 分

网络隔离技术的目标是确保隔离有害的攻击，在可信网络之外和保证可信网络内部信息不外泄的前提下，完成网间数据的安全交换。以下网络隔离技术说法正确的是（）

A.隔离产品要保证自身要具有高度的安全性；B.要确保网络之间是隔离的；C.要对网间的访问进行严格的控制和检查；D.以上都对

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

10

2 分

数据加密标准 DES 的设计目标是用于加密保护静态存储和传输信道中的数据。以下关于 DES 说法错误的是（）

A.DES 是一种分组密码；B.DES 是对合运算，因而加密和解密共同一算法；C.DES 是面向十六进制的密码算法；D.DES 综合运用了置换、代替、代数等多种密码技术

正确答案是：C　你的答案是：B　　此题得分：0

展开解析

11

2 分

几十年的应用实践证明了 DES 作为商用密码，用于其设计目标是安全的，但同时也不可避免地存在着一些弱点和不足。以下属于 DES 的缺点的是（）

A.密钥较短；B.存在弱密钥；C.存在半弱密钥；D.以上都对

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

12

2 分

由于 RSA 密码既可用于加密，又可用于数字签名，安全、易懂，因此 RSA 密码已成为目前应用最广泛的公开密钥密码。以下关于 RSA 说法正确的是（）

A.RSA 算法具有加解密算法的可逆性，加密和解密运算可交换；B.RSA 密码的核心运算是模幂运算；C.RSA 算法可同时确保数据的秘密性和数据的真实性；D.以上都对

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

13

2 分

认证和数字签名技术都是确保数据真实性的措施，但两者有着明显的区别。以下属于两者区别的是（）

A.认证总是基于某种收发双方共享的保密数据来认证被鉴别对象的真实性，而数字签名中用于验证签名的数据是公开的；B.认证允许收发双方互相验证其真实性，不准许第三者验证，而数字签名允许收发双方和第三者都能验证；C.数字签名具有发送方不能抵赖、接收方不能伪造和具有在公证人前解决纠纷的能力，而认证则不一定具备；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

14

2 分

UNIX 系统在用户选择口令时，如果发现用户给出的口令不同时包含字母和数字，或口令是用户名的某种组合，就拒绝接收口令，体现一个好的口令应当具备（）

A.应有足够的长度；B.应使用多种字符；C.应尽量随机；D.应定期更换

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

15

2 分

为了简化密钥管理工作，可采用密钥分级的策略，将密钥分为三级：初级密钥、二级密钥、主密钥。以下说法错误的是（）

A.初级密钥必须受更高一级的密钥保护，直到它们的生存周期结束为止；B.二级密钥只能由系统自动产生；C.二级密钥的生存周期一般较长，它在较长的时间内保持不变；D.主密钥用于对二级密钥和初级密钥进行保护

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

16

2 分

密码分量不是密钥本身，而是用于产生密钥的部分参数，属于哪种密钥的存储形态？

A.明文形态；B.密文形态；C.分量形态；D.分组形态

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

17

2 分

密码的存储形态有三种：明文形态、密文形态、分量形态。主密钥是最高级的密钥，所以它只能以（）存储，否则便不能工作

A.明文形态；B.密文形态；C.分量形态；D.分组形态

正确答案是：A　你的答案是：C　　此题得分：0

展开解析

18

2 分

路由信息协议 RIP 是一种分布式的基于距离向量的路由选择协议，以下关于 RIP 说法错误的是（）

A.RIP 使用运输层的用户数据报 UDP 进行传送；B.RIP 协议所定义的距离就是经过的路由器的数目；C.RIP 协议属于运输层；D.RIP 协议使用的距离向量算法中距离为 16 表示不可达

正确答案是：C　你的答案是：A　　此题得分：0

展开解析

19

2 分

当路由器不能把数据报转交给目的站时，就向源站发送终点不可达报文，这属于哪种 ICMP 报文类型？（）

A.终点不可达；B.源站抑制；C.改变路由；D.时间超时

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

20

2 分

当需要测试某一目的站点是否可达时，就发送一个 ICMP 回送请求报文，然后目的站点会向发送站回送一个 ICMP 回答报文，这属于哪种 ICMP 报文类型？（）

A.时间戳请求或回答；B.源站抑制；C.回送请求或回答；D.时间超时

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

21

2 分

口令攻击是网络攻击的最简单、最基本的一种形式，它有三种类型：字典攻击、强行攻击、组合攻击。先从字母 a 开始，尝试 aa、ab、ac 等等，然后尝试 aaa、aab、aac……这属于哪种类型？（）

A.字典攻击；B.强行攻击；C.组合攻击；D.以上都不是

正确答案是：C　你的答案是：A　　此题得分：0

展开解析

22

2 分

拒绝服务攻击有许多种，网络的内外部用户都可以发起这种攻击，针对网络连接数进行的拒绝服务攻击属于（）

A.消耗资源；B.长时间占用系统的内存；C.长时间占用 CPU 处理时间；D.流量型攻击

正确答案是：A　你的答案是：D　　此题得分：0

展开解析

23

2 分

Smurf 拒绝服务攻击结合使用了 IP 欺骗和 ICMP 回复方法使大量网络数据充斥目标系统，引起目标系统拒绝为正常请求进行服务。以下措施可以对付 Smurf 攻击的是（）

A.被攻击者利用进行攻击的中间网络应配置路由器禁止 IP 广播包进网，同时配置网络上所有计算机的操作系统，禁止对目标地址为广播地址的 ICMP 包响应；B.被攻击的目标要与 ISP 协商，由 ISP 暂时阻止大量 ICMPECHOREPLY 包的攻击；C.对于从本网络向外部网络发送的数据包，本网络应该将其源地址为其他网络的部分数据包过滤掉；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

24

2 分

在 WEP 机制中，对密钥的生成与分布没有任何的规定，对密钥的使用也没有明确的规定，密钥的使用情况比较混乱，属于 WEP 安全漏洞中的哪种漏洞？（）

A.加密算法中存在的漏洞；B.密钥管理中存在的漏洞；C.身份认证机制中存在的漏洞；D.以上都不是

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

25

2 分

入侵检测技术主要分成两大类型：异常入侵检测和误用入侵检测。Internet 蠕虫攻击使用了 fingered 和 sendmail 的错误属于（）

A.异常入侵检测；B.误用入侵检测；C.外部闯入；D.以上都不是

正确答案是：B　你的答案是：A　　此题得分：0

展开解析

26

2 分

三种最常见的也是最为广泛实现的隧道技术是：点对点隧道协议 PPTP、第 2 层隧道协议 L2TP、IP 安全协议 IPSec。　PPTP 和 L2TP 非常相似，以下关于两者说法错误的是（）

A.L2TP 和 PPTP 都是 PPP 协议的扩展；B.PPTP 只能在两端点间建立单一隧道，L2TP 支持在两端点间使用多隧道；C.L2TP 和 PPTP 都支持隧道验证；D.PPTP 要求互联网络为 IP 网络，L2TP 只要求隧道媒介提供面向数据包的点对点连接

正确答案是：C　你的答案是：B　　此题得分：0

展开解析

27

2 分

SQL 注入（SQL Injection）是攻击者通过在查询操作中插入一系列的 SQL 语句到应用程序中来操作数据，以下关于 SQL 注入攻击描述不正确的是（）

A.SQL 注入攻击是目前网络攻击的主要手段之一，在一定程度上其安全风险高于缓冲区溢出漏洞；B.目前防火墙能对 SQL 注入漏洞进行有效的防范；C.在某些情况下，SQL 注入攻击让受害者承受巨大损失；D.SQL 注入攻击可以通过数据库安全防护技术实现有效防护

正确答案是：B　你的答案是：B　此题得分：2

展开解析

28

2 分

层次化的入侵检测模型将入侵检测系统分为 6 个层次，从低到高数第 5 个层次为（）

A.数据层 ；B.事件层；C.上下文层；D.威胁层

正确答案是：D　你的答案是：B　此题得分：0

展开解析

29

2 分

以下属于层次化入侵测试模型与通用入侵检测模型相比具有的优势的是（）

A.针对不同的数据源，采用了不同的特征提取方法；B.以分布式结构取代单一结构；C.用攻击特征库和安全策略库取代活动记录；D.以上都是

正确答案是：D　你的答案是：D　此题得分：2

展开解析

30

2 分

下列关于主机的入侵检测系统说法不正确的是（）

A.基于主机的入侵检测系统可监测系统、事件和操作系统下的安全记录以及系统记录；B.对于基于主机的入侵检测系统来说，只要将它部署到这些关键主机或服务器中即可；

C.基于主机的入侵检测系统部署在服务器上，对服务器没有任何影响；D.基于主机的入侵检测系统，其检测的目标系统主要是主机系统和本地用户

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

31

2 分

端口扫描指某些别有用心的人发送一组端口测试数据，了解其提供的计算机网络服务类型，下列哪项不属于端口扫描？（）

A.RESET 扫描；B.Connect 扫描；C.FIN 扫描；D.Ping 扫描

正确答案是：D　你的答案是：C　　此题得分：0

展开解析

32

2 分

下列哪项不属于入侵分析的目的？（）

A.重要的威慑力；B.实行反入侵；C.安全规划和管理；D.获取入侵证据

正确答案是：B　你的答案是：A　　此题得分：0

展开解析

33

2 分

下列关于入侵分析的说法错误的是（）

A.入侵分析过程分为 3 个阶段分别为：构建分析器、分析数据、反馈和更新；B.在分析模型中，第一阶段的任务就是构造分析引擎；C.在对实际现场数据分析的阶段中，分析器需要分析现场实际数据，识别入侵和其他重要活动；D.反馈和更新阶段不是很重要

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

34

2 分

在 TCP/IP 协议中，由于 TCP 协议提供可靠的连接服务，于是采用有保障的三次握手来创建一个 TCP 连接，下列关于 TCP 的三次握手描述错误的是（）

A.第一阶段：客户端发送一个带 SYN 标志的 TCP 报文到服务器，表示希望和服务器建立一个 TCP 连接；B.第二阶段：服务器发送一个带有 ACK 标志和 SYN 标志的 TCP 报文给客户端，ACK 用于对客户端发送的 SYN 报文进行回应，SYN 用于询问客户端是否准备好进行数据传输；C.第三阶段：客户端发送一个带有 ACK 标志和 SYN 标志的 TCP 报文（报文 3），作为对服务器发送的 SYN 报文的回应；D.第三阶段：客户端发送一个带有 ACK 标志的 TCP 报文（报文 3），作为对服务器发送的 SYN 报文的回应

正确答案是：C　你的答案是：D　　此题得分：0

展开解析

35

2 分

漏洞扫描可以分为三个阶段：漏洞检测，信息攫取和目标发现。关于漏洞扫描的各个阶段，以下描述中不正确的是（）

A.信息攫取指在发现目标后，进一步获得目标主机的操作系统信息和开放的服务信息；B.如果目标是一个网络，信息攫取无法发现该网络的拓扑结构、路由设备以及各主机的信息；C.漏洞检测是指根据搜集到的信息判断是否存在安全漏洞，或进一步测试系统是否存在可被攻击者利用的安全漏洞；D.目标发现是指通过某种方式发现目标主机或网络

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

36

2 分

HTTP 是一个客户端和服务器端请求和应答的标准（TCP）。客户端是终端用户，服务器端是网站。通过使用 Web 浏览器、网络爬虫或者其它的工具，客户端发起一个到服务器上指定端口（默认端口为 80）的 HTTP 请求。关于 HTTP 请求，以下描述中不正确的是（）

A.HTTP 请求由状态行，请求头，请求正文 3 个部分构成；B.状态行由请求方式、路径、协议等构成，各元素之间以空格分隔；C.请求头可提供用户代理信息；D.POST 请求的请求正文全部为空

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

37

2 分

以下属于物理层设备的是　　（）

A.中继器；B.以太网交换机；C.网桥；D.网关

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

38

2 分

两个防火墙之间的空间被称为 DMZ 即俗称的隔离区或非军事区，这个区域并不安全，所以 DMZ 中通常不会出现的是　　（）

A.Web 服务器；B.Mail 服务器；C.FTP 服务器；D.机密信息文件

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

39

2 分

传输控制协议 TCP 和用户数据报协议 UDP 协议的相似之处是　　（）

A.面向连接的协议；B.面向非连接的协议；C.传输层协议；D.以上均不对

正确答案是：C　你的答案是：D　此题得分：0

展开解析

40

2 分

防火墙是一种位于内部网络与外部网络之间的网络安全系统，在防火墙定义中没有涉及到的要素是　　（）

A.安全技术；B.内部网；C.外部网；D.加密措施

正确答案是：D　你的答案是：D　此题得分：2

展开解析

41

2 分

在 IP 地址方案中，159.226.181.1 是一个　　地址（）

A.A 类；B.B 类；C.C 类；D.D 类

正确答案是：B　你的答案是：B　此题得分：2

展开解析

42

2 分

防火墙技术中有一个环节是地址转换，目的是对外部网络隐藏内部网的某些信息。地址转换的在安全方面主要作用是　　（）

A.提供数据加密；B.进行入侵检测；C.隐藏内部网络地址；D.防止病毒入侵

正确答案是：C　你的答案是：C　此题得分：2

展开解析

43

2 分

系统的可靠性是指系统能稳定无故障工作多久，一般使用　　指标来度量系统的可靠性

A.平均维修时间；B.平均无故障时间；C.平均运行时间；D.单位时间通过的信息

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

44

2 分

在邮件接收过程中用到的是以下哪个协议　　（）

A.FTP；B.SMTP；C.POP3；D.IMAP

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

45

2 分

衡量防火墙设备性能有多种指标，以下不属于的是　　（）

A.网络吞吐量；B.并发连接数；C.应用层吞吐量；D.网络容错率

正确答案是：D　你的答案是：C　　此题得分：0

展开解析

46

2 分

TCP 的协议数据单元被称为　　（）

A.比特；B.帧；C.分段；D.字符

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

47

2 分

以下的网络分类方法中，哪一组分类方法有误？

A.局域网/广域网；B.对等网/城域网；C.环型网/星型网；D.有线网/无线网

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

48

2 分

状态检测防火墙采用了状态检测包过滤的技术，是传统包过滤上的功能扩展，其工作在　　（）

A.应用层；B.传输层；C.数据链路层和网络层之间；D.数据链路层

正确答案是：B　你的答案是：C　　此题得分：0

展开解析

49

2 分

哪个用户可以在下一代防火墙系统上直接修改用户账户和密码等信息？（）

A.超级管理员用户；B.LDAP 用户；C.Radius 用户；D.所有用户系统

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

50

2 分

在 Internet 的基本服务功能中，远程登录所使用的命令是　　（）

A.ftp；B.telent；C.mail；D.open

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

第十七章

受到了 ARP 欺骗的计算机，发出的数据包，　　地址是错误的（）

A.源 IP；B.目的 IP；C.源 MAC；D.目的 MAC

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

2

2 分

Internet 是一个将设备互联起来的网络，故它是一种　　结构的网络

A.星型；B.环型；C.树型；D.网型

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

3

2 分

下一代防火墙不基于互联网及用户自身的　　（）

A.动态数据检测；B.动态行为检测；C.动态处置响应；D.动态策略配置

正确答案是：D　你的答案是：D　此题得分：2

展开解析

4

2 分

传输层可以通过　　标识不同的应用

A.物理地址；B.端口号；C.IP 地址；D.逻辑地址

正确答案是：B　你的答案是：B　此题得分：2

展开解析

5

2 分

QoS（Quality of Service，服务质量）指一个网络能够利用各种基础技术，为指定的网络通信提供更好的服务能力。以下网络服务中 QoS 不能保证的是　　（）

A.带宽；B.抖动；C.接入位置；D.时延

正确答案是：C　你的答案是：B　此题得分：0

展开解析

6

2 分

关于 LDAP 的描述错误的是

A.是一种轻量目录访问协议；B.基于 TCP/IP 的目录访问协议；C.存储不经常改变的数据；D.是远程数据访问的一种方式

正确答案是：D　你的答案是：C　此题得分：0

展开解析

7

2 分

在中继系统中，中继器处于

A.物理层；B.数据链路层；C.网络层；D.应用层

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

8

2 分

land 攻击是指一种使用相同的源和目的主机和端口发送数据包到某台机器的攻击，关于 land 攻击正确的是

A.TCP 报文中源地址和目的地址不同；B.TCP 报文中源地址和目的地址相同；C.IP 报文中源地址和目的地址不同；D.IP 报文中源地址和目的地址相同

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

9

2 分

系统的可维护性是指系统维护的难易程度，可以使用　　进行评价

A.平均维修资金成本；B.平均无故障时间；C.平均维修时间；D.平均维修人员成本

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

10

2 分

网卡是局域网中连接计算机和传输介质的接口，它位于哪一层？

A.物理层；B.数据链路层；C.物理层和数据链路层；D.数据链路层和网络层

正确答案是：C　你的答案是：D　　此题得分：0

展开解析

11

2 分

随着电信和信息技术的发展，国际上出现了所谓“三网融合”的趋势，下列不属于三网之一的是

A.传统电信网；B.计算机网(主要指互联网)；C.有线电视网；D.卫星通信网

正确答案是：D　你的答案是：B　　此题得分：0

展开解析

12

2 分

拒绝服务攻击是攻击者想办法让目标机器停止提供服务，恶意大量消耗网络带宽是拒绝服务攻击中什么类型？

A.配置修改型；B.基于系统缺陷型；C.资源消耗型；D.物理实体破坏型

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

13

2 分

当数据由计算机 A 传送至计算机 B 时，不参与数据封装工作的是哪一层？

A.物理层；B.数据链路层；C.传输层；D.网络层

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

14

2 分

控制企业内部对外的访问以及抵御外部对内部网的攻击，最好的选择是

A.IDS；B.杀毒软件；C.防火墙；D.路由器

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

15

2 分

TCP/IP 层的网络接口层对应 OSI 的

A.物理层；B.链路层；C.网络层；D.物理层和链路层

正确答案是：D　你的答案是：C　　此题得分：0

展开解析

16

2 分

IPV6 将 32 位地址空间扩展到

A.64 位；B.128 位；C.256 位；D.1024 位

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

17

2 分

Internet 中应用行为控制不包括哪些功能？

A.Post 操作；B.代理上网；C.数据存储；D.文件上传

正确答案是：C　你的答案是：A　　此题得分：0

展开解析

18

2 分

将传输比特流划分为帧，这个功能交于下列 OSI 的哪一层处理？

A.物理层；B.数据链路层；C.传输层；D.网络层

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

19

2 分

当发生安全事件后，下一代防火墙提供了处置响应的配置接口，其中不包括

A.处置受害 IP；B.处置 IOC；C.事件告警；D.数据恢复

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

20

2 分

TCP/IP 协议是 Internet 中计算机之间通信所必须共同遵循的一种

A.信息资源；B.通信规定；C.软件；D.硬件

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

21

2 分

系统可靠性最高的网络拓扑结构是

A.总线型；B.网状型；C.星型；D.树型

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

22

2 分

算法分析是对一个算法需要多少计算时间和存储空间作定量的分析，算法分析的目的是

A.找出数据结构的合理性；B.分析算法的易懂性和文档性；C.研究算法中的输入和输出的关系；D.分析算法的效率以求改进

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

23

2 分

以下不属于 SQL Server 身份验证的优点的是（）

A.允许用户从未知的或不可信的域进行连接；B.允许 SQL Server 支持具有混合操作系统的环境；C.允许用户只提供 Windows 登录名和密码；D.允许 SQL Server 支持基于 Web 的应用程序

正确答案是：C　你的答案是：A　　此题得分：0

展开解析

24

2 分

PGP 是美国 PhilZimmermann 研究出来的一个基于 RSA 公钥加密体系的邮件加密软件，以下关于 PGP 说法错误的是（）

A.PGP 提供世界范围内免费的各种版本，可运行于各种平台；B.PGP 使用的算法被认为是非常安全的算法；C.PGP 既可用于公司、团体中加密文件时所选择的标准模式，也可以在互联网或其他网络上个人间的消息通信加密；D.PGP 是由政府控制的

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

25

2 分

远程认证接入用户服务（RADIUS）协议是一种提供在网络接入服务器和共享认证服务器间传送认证、授权和配置信息等服务的协议，以下关于 RADIUS 说法错误的是（）

A.RADIUS 由客户端和服务器端两部分组成，客户端想服务器发送认证和计费请求，服务器向客户端回送接受或否定消息；B.客户和服务器之间的通信用共享密钥来加密信息后通过网络传送；C.在一个客户端被设置使用 RADIUS 协议后，任何使用这个终端的用户都需要向客户提供认证信息；D. RADIUS 服务器收到请求信息，不用对传输信息的客户端进行验证

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

26

2 分

S/MIME 在 RSA 数据安全性的基础上加强了互联网 E-Mail 格式标准 MIME 的安全性。以下属于 S/MIME 提供的功能有（）

A.封装数据 ；B.透明签名数据；C.签名并封装数据；D. 以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

27

2 分

以下不属于 SSH 协议功能的是（）

A.服务器认证保护；B.增强数据加密性；C.提供数据解压缩；D.保证信息完整性

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

28

2 分

Honeynet 是专门为研究设计的高交互型蜜罐，一般称为蜜网。以下关于蜜网说法错误的是（）

A.Honeynet 不是一个单独的系统而是由多个系统和多个攻击检测应用组成的网络；
B.Honeynet 内可以同时包含多种系统；C.Honeynet 不支持信息控制和信息捕获；
D.Honeynet 的系统都是标准的，这些系统和应用都是用户可以在互联网上找到的真实系统和应用

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

29

2 分

冲击波蠕虫利用的是（）

A.DCOM RPC 缓冲区漏洞；B.XSS 漏洞；C.文件上传漏洞；D.文件下载漏洞

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

30

2 分

拒绝服务攻击是攻击者想办法让目标机器停止提供服务，是黑客常用的攻击手段之一，其目的是（）

A.导致被攻击的服务器无法向外提供服务；B.获取数据库信息；C.远程控制计算机；D.获得访问权

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

31

2 分

下列哪一项不属于拒绝服务攻击可能带来的后果？

A.带宽耗尽；B.内存资源被大量占用；C.获得访问权；D.连接上数被耗尽

正确答案是：C　你的答案是：B　　此题得分：0

展开解析

32

2 分

每逢双十一购物狂欢节，网民们都会在淘宝网上抢购东西，当网民抢购商品高峰期到来时，就经常出现网站崩溃、停机等情况，这实际上可以看作是全国网民通过手动点击淘宝网址引起的一次大规模（）攻击

A.XSS；B.CSRF；C.SQL 注入；D.DDoS

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

33

2 分

僵尸网络是攻击者出于恶意目的，传播僵尸程序控制大量主机，并通过一对多的命令与控制信道所组成的网络，以下关于僵尸网络说法错误是（）

A.僵尸网络是从传统恶意代码形态包括计算机病毒、网络蠕虫、特洛伊木马和后门工具的基础上进化，并通过相互融合发展而成的目前最为复杂的攻击方式之一；B.利用僵尸网络，攻击者可以轻易地控制成千上万台主机对因特网任意站点发起分布式拒绝服

务攻击，并发送大量垃圾邮件，从受控主机上窃取敏感信息或进行点击欺诈以牟取经济利益；C.一般情况下，僵尸网络由僵尸计算机、命令与控制服务器、攻击者组成；D.僵尸网络形成的条件是被控制主机和攻击主机必须有物理链路联通

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

34

2 分

根据系统各个模块运行的分布方式不同，可将入侵检测系统分为集中式入侵检测系统和分布式入侵检测系统，下列关于它们说法错误的是（）

A.集中式的网络入侵检测，一般指对网络中的数据包作为数据源进行分析；B.分布式入侵检测系统适用于网络环境比较简单的情况；C.分布式网络入侵检测系统通常有多个模块组成，这些模块一般分布在网络的不同位置；D.集中式入侵检测系统的各个模块包括数据的收集与分析以及响应都集中在一台主机上运行

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

35

2 分

根据入侵检测方式的不同可将入侵检测系统分为实时检测系统和非实时检测系统，下列关于它们说法错误的是（）

A.非实时的离线批量处理方式不能及时发现入侵攻击，系统的成本更高；B.实时检测系统也称为在线检测系统，通过实时监测并分析网络流量、主机审计记录及各种日志信息来发现攻击；C.非实时检测系统也称为离线检测系统，通常是对一段时间内的被检测数据进行分析来发现入侵攻击，并作出相应的处理；D.在高速网络环境下，要分析的网络流量非常大，往往是用在线检测方式和离线检测方式相结合

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

36

2 分

SYN Flood 是一种广为人知的 DoS，是 DDoS 的方式之一，下列关于 SYN Flood 攻击及 IPS 对其的防御处理说法正确的是（）

A.发动 SYN Flood 攻击，攻击者构造一定数量的 SYN 请求包，当服务器回复 SYN+ACK 后，攻击者不回应 ACK 报文，服务器则一直等待客户端的回应直到超时；B.SYN Flood 攻击是通过消耗系统的并发连接数来实现拒绝服务攻击的；C.SYN Flood 攻击发生的原因是服务器在等待期间是需要占用系统资源的，当数量达到一定量时，就会发生后续的请求不能正常回应；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

37

2 分

下列关于基于网络的入侵防御系统（NIPS）说法错误的是（）

A.网络入侵防御系统兼有、防火墙和反病毒等安全组件的特性，有时亦被称为内嵌式 IDS 或网关式 IDS ；B.受保护的网段与其它网络之间交互的数据流都必须通过 NIPS 设备。当数据包通过 NIPS 时，通信将被监视是否存在攻击；C.NIPS 是串联在网络的主干线上的，它需要一块网卡即可；D.网络入侵防御系统与受保护网段是串联部署的

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

38

2 分

下列关于入侵防御系统技术的说法正确的是（）

A.目前，基于统计和识别网络上异常流量的技术手段有基于特征的异常检测和基于行为的异常检测；B.基于特征的异常检测是根据已经定义好的攻击特征表述，对网络上的数据流量信息进行分析；C.基于行为的异常检测，其前提是入侵活动发生时，其行为活动与正常的网络活动存在异常；D.以上都对

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

39

2 分

下列关于入侵检测系统的联动响应机制的说法正确的是（）

A.目前, 可以与入侵检测系统联动进行响应的安全技术包括防火墙、安全扫描器、防病毒系统、安全加密系统等；B.防火墙联动即当入侵检测系统检测到潜在的网络攻击后,将相关信息传输给防火墙,由防火墙采取响应措施,从而更有效的保护网络信息系统的安全；C.从联动的角度出发，安全设备可以分为两大类：具有发现能力的设备和具有响应能力的设备；D.以上都对

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

40

2 分

入侵防御系统 IPS 是一种智能化的入侵检测和防御产品，以下哪项不属于其主要功能？

A.漏洞扫描；B.SQL 注入检测；C.协议异常检测；D.实时监视和拦截攻击

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

41

2 分

分布式拒绝服务(DDoS)攻击指借助于 C/S 服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DDoS 攻击，从而成倍地提高拒绝服务攻击的威力，下列哪项属于服务器被 DDoS 攻击时的现象？

A.利用受害主机提供的服务或传输协议上的缺陷，反复高速的发出特定的服务请求，使受害主机无法及时处理所有正常请求；B.服务器不能提供正常的服务，严重时会造成系统死机；C.网络中充斥着大量的无用数据包；D.以上都是

正确答案是：D　你的答案是：D　此题得分：2

展开解析

42

2 分

数据备份可以分为完全备份、增量备份、差分备份和渐进式备份等多种备份方式。下列关于它们说法错误的是（）

A.完全备份是指将系统中所有选择的数据对象进行一次全面的备份，不论数据对象自上次备份之后是否修改过；B.增量备份是指只对上次备份后系统中变化过的数据对象的备份；C.差分备份是指上次增量备份以来系统中所有变化过的数据对象的备份；D.渐进式备份是指系统排除完全备份，数据对象只有当发生改变时才被写入到存储介质上

正确答案是：C　你的答案是：C　此题得分：2

展开解析

43

2 分

以下不属于系统安全模型的是（）

A.Biba 模型；B.IDS 模型；C.BLP 模型；D.RBAC 模型

正确答案是：B　你的答案是：A　此题得分：0

展开解析

44

2 分

CFS 是一个经典的加密文件系统，以下关于其说法错误的是（）

A.CFS 使用 DES 来加密文件；B.CFS 客户基于网络文件系统协议运行一个服务器保护程序；C.CFS 的效率很高；D.CFS 的加密操作在用户层完成

正确答案是：C　你的答案是：D　此题得分：0

展开解析

45

2 分

TCFS 是一个受 CFS 启发的 Linux 软件包，以下关于其说法错误的是（）

A.TCFS 具有更大的透明度，用户甚至不需要知道他们的文件被加密了；B.TCFS 对数据进行加密时，对每个文件使用不同的“文件密钥”进行加密，对一个文件的不同部分使用的是不同的“块密钥”进行加密；C.TCFS 的数据加密、解密操作在核心层完成；D.TCFS 对文件名、文件大小、访问时间、目录结构等一些敏感信息有很好的保护

正确答案是：D　你的答案是：A　此题得分：0

展开解析

46

2 分

PING(Packet Internet Groper)因特网包探索器，用于测试网络连接量的程序，它发出的是　　报文

A.TCP 请求；B.TCP 应答；C.ICMP 请求；D.ICMP 应答

正确答案是：C　你的答案是：C　此题得分：2

展开解析

47

2 分

当一台主机从一个 C 类网络移到一个 B 类网络时，为了访问同一网络中其他计算机，以下说法正确的是

A.必须改变它的 IP 地址和 MAC 地址；B.必须改变它的 IP 地址，但不需改动 MAC 地址；C.必须改变它的 MAC 地址，但不需改动 IP 地址；D.MAC 地址、IP 地址都不需改动

正确答案是：B　你的答案是：B　此题得分：2

展开解析

48

2 分

PPP（点到点协议）是为在同等单元之间传输数据包这样的简单链路设计的一个协议 。PPP 协议是哪一层的协议？

A.物理层；B.数据链路层；C.网络层；D.应用层

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

49

2 分

目前网络应用系统采用的主要模型是

A.离散个人计算模型；B.主机计算模型 ；C.客户/服务器计算模型；D.网络/文件服务器计算模型

正确答案是：C　你的答案是：D　　此题得分：0

展开解析

50

2 分

在 OSI 环境中，不同开放系统对等实体之间的通信，需要（N）实体向相邻的上一层（N+1）实体提供一种能力，这种能力称为

A.协议；B.服务；C.用户；D.功能

正确答案是：B　你的答案是：B　　此题得分：2

第十八章

1

2 分

以下各项中，不是数据报操作特点的是

A.每个分组自身携带有足够的信息，它的传送是被单独处理的；B.在整个传送过程中，不需建立虚电路；C.使所有分组按顺序到达目的端系统；D.网络节点要为每个分组做出路由选择

正确答案是：C　你的答案是：A　此题得分：0

展开解析

2

2 分

以下哪一个设置不是上互联网所必须的？

A.IP 地址；B.工作组；C.子网掩码；D.网关

正确答案是：B　你的答案是：B　此题得分：2

展开解析

3

2 分

以下关于 TCP/IP 协议的描述中，错误的是

A.TCP、UDP 协议都要通过 IP 协议来发送、接收数据；B.TCP 协议提供可靠的面向连接服务；C.UDP 协议提供简单的无连接服务；D.TCP/IP 协议属于应用层

正确答案是：D　你的答案是：A　此题得分：0

展开解析

4

2 分

IPV4 的 32 位地址共 40 多亿个，IPV6 的 128 位地址是 IPV4 地址总数的　　倍

A.4；B.96；C.2^4；D.2^96

正确答案是：D　你的答案是：C　　此题得分：0

展开解析

5

2 分

下面关于 IPv6 协议优点的描述中，准确的是

A.IPv6 协议允许全局 IP 地址出现重复；B.IPv6 协议解决了 IP 地址短缺的问题；C.IPv6 协议支持通过卫星链路的 Intemet 连接；D.IPv6 协议支持光纤通信

正确答案是：B　你的答案是：C　　此题得分：0

展开解析

6

2 分

Internet 控制报文协议 ICMP 用于在 IP 主机、路由器之间传递控制消息，下面关于 ICMP 协议的描述中，正确的是

A.ICMP 协议根据 MAC 地址查找对应的 IP 地址；B.ICMP 协议把公网的 IP 地址转换为私网的 IP 地址；C.ICMP 协议用于控制数据报传送中的差错情况；D.ICMP 协议集中管理网络中的 IP 地址分配

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

7

2 分

关于 ARP 表，以下描述中正确的是

A.提供常用目标地址的快捷方式来减少网络流量；B.用于建立 IP 地址到 MAC 地址的映射；C.用于在各个子网之间进行路由选择；D.用于进行应用层信息的转换

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

8

2 分

下列关于 IPv4 地址的描述中错误是

A.IP 地址的总长度为 32 位 ；B.每一个 IP 地址都由网络地址和主机地址组成；C.一个 C 类地址拥有 8 位主机地址，可给 254 台主机分配地址；D.A 类地址拥有最多的网络数

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

9

2 分

路由器在两个网段之间转发数据包时，读取其中的　　地址来确定下一跳的转发路径

A.目标 IP；B.MAC；C.源 IP；D.ARP

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

10

2 分

下面对应用层协议说法正确的有

A.DNS 协议支持域名解析服务，其服务端口号为 80；B.TELNET 协议支持远程登陆应用；C.电子邮件系统中，发送电子邮件和接收电子邮件均采用 SMTP 协议；D.FTP 协议提供文件传输服务，并仅使用一个端口

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

11

2 分

网络监听是一种监视网络状态、数据流程以及网络上信息传输的管理工具，它可以将网络界面设定成监听模式，并且可以截获网络上所传输的信息。关于网络监听组件，以下描述中不正确的是（）

A.通过向网络监听组件发送含有异常数据的包，有可能触发缓冲区溢出；B.绕过网络监听组件身份验证，可能可以获得合法数据库账号和密码；C.数据库的网络监听组件被攻击的可能性一定与其协议的复杂性成反比；D.网络监听组件被触发缓冲区重写，可能导致数据库服务器无法响应客户端

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

12

2 分

对网际控制协议（ICMP）描述错误的是

A.ICMP 封装在 IP 数据报的数据部分；B.ICMP 消息的传输是可靠的；C.ICMP 是 IP 协议的必需的一个部分；D.ICMP 可用来进行拥塞控制

正确答案是：B　你的答案是：C　　此题得分：0

展开解析

13

2 分

数据库引擎是用于存储、处理和保护数据的核心服务。利用数据库引擎可控制访问权限并快速处理事务，从而满足企业内大多数需要处理大量数据的应用程序的要求。关于数据库引擎的安全问题，以下描述中不正确的是（）

A.数据库引擎囊括了能够保证数据库高效平稳运行所必需的多种不同处理逻辑和过程；B.SQL SERVER 2005 的 cve-2008-0107 漏洞允许攻击者通过整数形缓冲区溢出漏洞控制 SQLSERVER 所在服务器；C.数据库引擎可以让用户创建程序在数据库内部执行的运行环境；D.数据库引擎的安全问题在优化设计后可以被完全避免

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

14

2 分

当用户需要远程控制终端服务器的时候，若远程连接服务器存在漏洞则会对用户操作的安全性造成很大的潜在威胁。关于远程服务器漏洞和本地漏洞，以下描述中不正确的是（）

A.本地漏洞指的是必须登录到安装软件的计算机上才能利用的漏洞；B.利用远程服务器漏洞，攻击者可以通过网络在另一台电脑上直接进行攻击，而无需用户进行任何操作；C.本地漏洞因利用方便，威胁也最大；D.远程服务器漏洞主要是指位于提供网络服务的进程中的漏洞

正确答案是：C　你的答案是：A　　此题得分：0

展开解析

15

2 分

近年来，工信部等有关部门出台相关政策，不断强化对手机 APP 行业的规范。同时，由于应用隐私授权等手机安全问题可以依靠用户自身防范进行避免，因此提高用户对于各类安全风险的认知并建立防范意识也是当务之急。APP 应用自身的安全问题不包含哪个方面？

A.设计上的缺陷；B.开发过程导致的问题；C.配置部署导致的问题；D.应用市场安全审查不严谨

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

16

2 分

数据库漏洞扫描是对数据库系统进行自动化安全评估的专业技术，能够充分暴露并证明数据库系统的安全漏洞和威胁并提供智能的修复建议，将企业的数据库安全建设工作由被动的事后追查转变为事前主动预防。关于数据库漏洞扫描的核心技术，以下描述中不正确的是（）

A.智能端口发现技术通常是通过“主动方式”获取指定数据库所运行的端口信息；B.数据库的漏洞种类很多，因此扫描的时候往往可以扫出各种漏洞；C.漏洞库的匹配技术是基于数据库系统安全漏洞知识库，从而按照一定的匹配规则发现漏洞；D.漏洞库的匹配技术的有效性和漏洞库的完整性完全无关

正确答案是：D　你的答案是：D　此题得分：2

展开解析

17

2 分

SQL 注入是比较常见的网络攻击方式之一，它不是利用操作系统的 BUG 来实现攻击，而是针对程序员编程时的疏忽，通过 SQL 语句，实现无帐号登录，甚至篡改数据库。关于防范 SQL 注入，以下描述中不正确的是（）

A.防范 SQL 注入主要在于严密地验证用户输入的合法性；B.为防范 SQL 注入可以对用户输入数据中的等号全部过滤掉；C.为防范 SQL 注入可以使用验证器验证用户的输入；D.为防范防范 SQL 注入可以利用参数化存储过程来访问数据库

正确答案是：B　你的答案是：D　此题得分：0

展开解析

18

2 分

超文本传输协议（HTTP，HyperText Transfer Protocol)是互联网上应用最为广泛的一种网络协议。所有的 WWW 文件都必须遵守这个标准。设计 HTTP 最初的目的是为了提供一种发布和接收 HTML 页面的方法。关于 HTTP 特性，以下描述中不正确的是（）

A.HTTP 是基于连接的；B.HTTP 一般构建于 TCP/IP 协议之上；C.HTTP 协议默认端口号是 80；D.HTTP 可以分为请求和响应两个部分

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

19

2 分

HTTP 服务器会在特定接收端口监听客户端发送过来的请求。一旦收到请求，服务器（向客户端）发回一个状态行，比如"HTTP/1.1 200 OK"，和（响应的）消息，消息的消息体可能是请求的文件、错误消息、或者其它一些信息。关于 HTTP 响应，以下状态码描述不正确的是（）

A.1xx：表示请求已经接受了，继续处理；B.2xx：表示请求已经被处理；C.3xx：一般表示客户端有错误，请求无法实现；D.5xx：一般为服务器端的错误

正确答案是：C　你的答案是：B　　此题得分：0

展开解析

20

2 分

软件动态分析是指在试运行代码的方式下，通过词法分析、语法分析、控制流、数据流分析等技术对程序代码进行扫描，验证代码是否满足规范性、安全性、可靠性、可维护性等指标的一种代码分析技术。常用的软件动态分析技术不包括（）

A.符号执行；B.Fuzz 分析；C.沙箱技术；D.数据流分析

正确答案是：D　你的答案是：A　　此题得分：0

展开解析

21

2 分

目前软件静态分析技术向模拟执行的技术发展以能够发现更多传统意义上动态测试才能发现的缺陷，例如符号执行、抽象解释、值依赖分析等等并采用数学约束求解工具进行路径约减或者可达性分析以减少误报增加效率。常用的静态分析技术不包括（）

A.污点分析；B.Fuzz 分析；C.数据流分析；D.语义分析

正确答案是：B　你的答案是：C　此题得分：0

展开解析

22

2 分

终端软件安全加固是一项面向互联网企业和个人开发者的在线加密服务，现支持安卓应用加密，用户只需提供 APK 包即可快速提高终端软件安全防护性能。终端软件加固不包含哪种方式？

A.终端软件加壳；B.安全启动功能；C.代码混淆；D.反动态调试

正确答案是：B　你的答案是：C　此题得分：0

展开解析

23

2 分

GPS 是英文 Global Positioning System 的简称，以下对于 GPS 的叙述错误的是？（　）

A.它是全球定位系统；B.GPS 定位可以结合地图的可视化，清晰、准确地定位出事件发生的地点以及与该事件相关事件发生的位置；C.GPS 有助于挖掘事件之间的关联关系；D.GPS 无安全性问题

正确答案是：D　你的答案是：D　此题得分：2

展开解析

24

2 分

PPP 协议提供了中在点到点链路上封装网络层协议信息的标准方法，其英文是（　）

A.The Point-to-Point Protocol；B.Point-to-Point Protocol over Ethernet；C.Ethernet Protocol；D.Point- Point-Point Protocol

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

25

2 分

SSH 是专为远程登录会话和其他网络服务提供安全性的协议，以下关于其全称正确的是（　）

A.Secure Shell；B.Search Shell；C.Send Shell；D.以上都不正确

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

26

2 分

IDS 依照一定的安全策略，对网络、系统的运行状况进行监视，其全称为（　）

A.Intrusion Detection Systems；B.Integrity Detection Systems；C.Integrity Design Systems；D.以上都不正确

正确答案是：A　你的答案是：B　　此题得分：0

展开解析

27

2 分

SNMP 是 TCP/IP 协议簇的一个应用层协议，以下是其全称的为（　）

A.Simple Network Management Protocol；B.Same Network Management Protocol；C.Search Network Management Protocol；D.以上都不正确

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

28

2 分

通过 VPN 可在公网上建立加密专用网络，VPN 的英文全称是（　）

A.Visual Protocol Network；B.Virtual Private Network；C.Virtual Protocol Network；D.Visual Private Network

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

29

2 分

以下不属于 Pyhton 开发优点的是（　）

A.可阅读性；B.非开源；C.可跨平台；D.可嵌入性

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

30

2 分

以下不属于 Session 攻击常用防护措施的是（　）

A.定期更换 Session ID；B.通过 URL 传递隐藏参数；C.设置 Http Only；D.开启透明化 Session ID

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

31

2 分

Python 是一门有条理的、强大的面向对象的程序设计语言，以下对 Pyhton 的应用描述错误的是（　）

A.Python 是数据科学中最流行的语言之一；B.Python 广泛应用于金融分析、量化交易领域；C.Python 在网络游戏开发中也有较多应用；D.Python 在各个领域中的应用不可替代。

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

32

2 分

软件安全性测试包括程序、网络、数据库安全性测试。以下关于软件安全测试的描述，错误的是（　）

A.狭义的软件安全测试是执行安全测试用例的过程；B.广义的软件安全测试是所有关于安全性测试的活动；C.软件安全测试的对象只包括代码；D.软件安全测试与传统软件测试的测试用例不相同

正确答案是：C　你的答案是：C　　此题得分：2

展开解析

33

2 分

PDCA 循环的含义是将质量管理分为四个阶段，即计划（plan）、执行（do）、检查（check）、处理（Act）。以下不属于 PDCA 循环特点的选项是（　）

A.开环系统，运行一次；B.顺序进行，循环运转；C.大环套小环，小环保大环，相互制约，相互补充；D.不断前进，不断提高

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

34

2 分

Web 网页就是万维网上的一个按照 HTML 格式组织起来的文件。当访问 Web 网站的某个页面资源不存在时，HTTP 服务器发回的响应状态代码是（　）

A.200；B.500；C.401；D.404

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

35

2 分

HTTP 访问控制主要针对网络层的访问控制，通过配置面向对象的通用包过滤规则实现控制域名以外的访问行为。以下属于具体访问控制的是（　）

A.对访问者访问的 URL 的控制，允许或不允许访问设定的 URL 对象；B.对访问者的 HTTP 方法的控制，允许或不允许设定的 HTTP 方法访问；C.对访问者的 IP 的控制，允许或不允许设定的 IP 对象访问；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

36

2 分

目前网络爬虫的检测手段多种多样，往往需要综合利用，提高检测的准确率。下列属于网络爬虫的检测手段的是（　）

A.检测 HTTP User-Agent 报头；B.检查 HTTP Referer 报头；C.检测客户端 IP；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

37

2 分

容灾是为了在遭遇灾害时能保证信息系统能正常运行，帮助企业实现业务连续性的目标，以下属于容灾技术范畴的是（　）

A.数据容灾；B.系统容灾；C.应用容灾；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

38

2 分

网络安全态势感知是中国互联网安全的创新方向之一，以下不属于态势感知的三个层次的是（　）

A.规则；B.感知；C.理解；D.预测

正确答案是：A　你的答案是：B　　此题得分：0

展开解析

39

2 分

“Internet 协议安全性　(IPSec)”是一种开放标准的框架结构，通过使用加密的安全服务以确保在　Internet 协议(IP) 网络上进行保密而安全的通讯。IPSec 是为（　）提供加密和认证的协议规范

A.物理层；B.网络层；C.运输层；D.应用层

正确答案是：B　你的答案是：C　　此题得分：0

展开解析

40

2 分

网络安全态势的预测方法有多种，以下关于神经网络预测网络安全态势的描述，错误的是（　）

A.神经网络预测方法没有任何缺点；B.神经网络是目前最常用的网络态势预测方法；C.神经网络具有自学习、自适应性和非线性处理的优点；D.神经网络具有良好的容错性和稳健性

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

41

2 分

一套信息系统安全策略应该全面地保护信息系统整体的安全，在设计策略的范围时，主要考虑（　）

A.物理安全策略；B.网络安全策略；C.数据加密策略；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

42

2 分

电子邮件是 Internet 应用最广的服务，以下用于邮件系统发送电子邮件的协议是（　）

A．SMTP；B．POP3；C．FTP；D．IMAP

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

43

2 分

信息对抗是为消弱、破坏对方电子信息设备和信息的使用效能，保障己方电子信息设备和信息正常发挥效能而采取的综合技术措施，其主要研究内容有（　）

A.通信对抗；B.雷达对抗；C.计算机网络对抗；D.以上都是

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

44

2 分

风险评估的方法有很多种，概括起来可分为三大类：定量的风险评估方法、定性的风险评估方法、定性与定量相结合的评估方法。运用数量指标来对风险进行评估是（　）的评估方法

A.定性；B.定量；C.定性与定量相结合；D.以上都不是

正确答案是：B　你的答案是：B　　此题得分：2

展开解析

45

目录

2 分

密码学作为信息安全的关键技术，其安全目标主要包括三个非常重要的方面：保密性、完整性和可用性。（　）是确保信息仅被合法用户访问，二不被泄露给非授权的用户、实体或过程，或供其利用的特性。

A.保密性；B.完整性；C.可用性；D.以上都不是

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

46

2 分

消息认证码 MAC 是消息内容和秘密钥的公开函数，其英文全称是（　）。

A.Message Authentication Code；B.Messag Authentication Code；C.Message Authentication Date；D.Messag Authentication Code

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

47

2 分

以下关于序列密码说法不正确的是（　）

A.序列密码是单独地加密每个明文位；B.由于序列密码小而快，所以它们非常合适计算资源有限的应用；C.序列密码的加密和解密使用相同的函数；D.现实生活中序列密码的使用比分组密码更为广泛，例如 Internet 安全领域

正确答案是：D　你的答案是：D　　此题得分：2

展开解析

48

2 分

病毒和木马都是一种人为的程序，都属于电脑病毒。以下关于病毒和木马说法错误的是（　）

A.病毒和木马很容易区分清楚；B.病毒和木马一般可以统称为恶意程序或恶意软件；C.病毒具有一定的显性破坏性，木马更倾向于默默地窃取；D.病毒具有自传播性，即能够自我复制，而木马则不具备这一点

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

49

2 分

相邻层间交换的数据单元称之为服务数据单元，其英文缩写是

A.SDU；B.IDU；C.PDU；D.ICI

正确答案是：A　你的答案是：A　　此题得分：2

展开解析

50

2 分

路由选择协议为路由器提供网络最佳路径所需要的相互共享的路由信息。路由选择协议位于

A.物理层；B.数据链路层；C.网络层；D.应用层

正确答案是：C　你的答案是：C　　此题得分：2