数据安全法试题

《中华人民共和国数据安全法》于 9 月 1 日正式施行这是我国第一部有关数据安全的专门法律

01 数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备_____的能力。

保障持续安全状态

02 开展数据处理活动，应当遵守法律、法规，尊重_____，遵守_____，诚实守信，履行数据安全保护义务，承担社会责任，不得危害国家安全、公共利益，不得损害个人、组织的合法权益。

社会公德和伦理

商业道德和职业道德

03 国家支持开发利用数据提升公共服务的智能化水平。提供智能化公共服务，应当充分考虑_____的需求，避免对_____的日常生活造成障碍。

老年人、残疾人

老年人、残疾人

04

重要数据的处理者应当按照规定对其数据处理活动定期开展_____，并向有关主管部门报送_____。

风险评估

风险评估报告

05 风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，_____等。

面临的数据安全风险

及其应对措施

06 任何组织、个人收集数据，应当采取合法、正当的方式，不得_____获取数据。

窃取或者以其他非法方式

07 从事数据交易中介服务的机构提供服务，应当要求数据提供方说明数据来源，审核交易双方的身份，并_____。

留存审核、交易记录

08 公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据，应当按照国家有关规定，经过严格的批准手续，依法进行，有关组织、个人应当_____。

予以配合

09 非经_____批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。

中华人民共和国主管机关

10 违反本法规定，给他人造成损害的，依法_____。

承担民事责任

网络攻防考试题库

1．目前，流行的局域网主要有三种，其中不包括：（ D ）。
A．以太网； B．令牌环网；
C．FDDI（光纤分布式数据接口）； D．ATM（异步传输模式）。
2．解决 IP 欺骗技术的最好方法是安装过滤路由器，在该路由器的过滤规则中，正确的是：（ C ）
A．允许包含内部网络地址的数据包通过该路由器进入；
B．允许包含外部网络地址的数据包通过该路由器发出；
C．在发出的数据包中，应该过滤掉源地址与内部网络地址不同的数据包；
D．在发出的数据包中，允许源地址与内部网络地址不同的数据包通过。
3．在以下网络互连设备中，（ D ） 通常是由软件来实现的。
A、中继器 B、网桥
C、路由器 D、网关
4．在网络信息安全模型中，（ A ）是安全的基石。它是建立安全管理的标准和方法。
A．政策，法律，法规； B．授权；
C．加密； D．审计与监控
5．下列口令维护措施中，不合理的是：（ B ）
A．第一次进入系统就修改系统指定的口令；
B．怕把口令忘记，将其记录在本子上；
C．去掉 guest（客人）账号；
D．限制登录次数。
6．病毒扫描软件由（ C ）组成
A．仅由病毒代码库；
B．仅由利用代码库进行扫描的扫描程序；
C．代码库和扫描程序
D．以上都不对
7．网络病毒是由因特网衍生出的新一代病毒，即 Java 及 ActiveX 病毒。由于（ A ），因此

不被人们察觉。
A．它不需要停留在硬盘中可以与传统病毒混杂在一起
B．它停留在硬盘中且可以与传统病毒混杂在一起
C．它不需要停留在硬盘中且不与传统病毒混杂在一起
D．它停留在硬盘中且不与传统病毒混杂在一起
8．用无病毒的 DOS 引导软盘启动计算机后，运行 FDISK 用于（ C ）。
A．磁盘格式化
B．读取或重写软盘分区表
C．读取或重写硬盘分区表
D．仅是重写磁盘分区表
9．以下属于加密软件的是（ C ）
A.CA　　B.RSA　　C.PGP　　D.DES
10．以下关于 DES 加密算法和 IDEA 加密算法的说法中错误的是：（ D ）[IDEA 使用长度为 128bit 的密钥，数据块大小为 64bit; DES 明文按 64 位进行分组， 密钥长 64 位，密钥事实上是 56 位参与 DES 运算]
A. DES 是一个分组加密算法，它以 64 位为分组对数据加密
B. IDEA 是一种使用一个密钥对 64 位数据块进行加密的加密算法
C. DES 和 IDEA 均为对称密钥加密算法
D. DES 和 IDEA 均使用 128 位（16 字节）密钥进行操作
11．以下关于公用/私有密钥加密技术的叙述中，正确的是：（C ）
A．私有密钥加密的文件不能用公用密钥解密
B．公用密钥加密的文件不能用私有密钥解密
C．公用密钥和私有密钥相互关联
D．公用密钥和私有密钥不相互关联
12．关于摘要函数，叙述不正确的是：（ C ）
A．输入任意大小的消息，输出是一个长度固定的摘要
B．输入消息中的任何变动都会对输出摘要产生影响
C．输入消息中的任何变动都不会对输出摘要产生影响
D．可以防止消息被改动
13．如果入侵者仅仅侵入到参数网络的堡垒主机，他只能偷看到（ C ）的信息流。
A．内部网络 B．内部路由器
C．这层网络（参数网络） D．堡垒主机
14．下列不属于扫描工具的是：（ D ）
A．SATAN　B．NSS
C．Strobe　　D．NetSpy[是一个特洛伊木马程序]
15.在网络上，为了监听效果最好，监听设备不应放在（ C ）
A．网关 B．路由器
C．中继器(OSI 物理层设备，对数据信号的重新发送或者转发，来扩大网络传输的距离) D．防火墙
16．在选购防火墙软件时，不应考虑的是：（ B ）
A. 一个好的防火墙应该是一个整体网络的保护者
B. 一个好的防火墙应该为使用者提供唯一的平台
C. 一个好的防火墙必须弥补其他操作系统的不足
D. 一个好的防火墙应能向使用者提供完善的售后服务
17．以下关于过滤路由器的叙述，错误的是：（ D ）
A．　过滤路由器比普通路由器承担更大的责任，是内部网络的保护系统

B． 如果过滤路由器的安全保护失败，内部网络将被暴露
C． 简单的过滤路由器不能修改任务
D． 过滤路由器不仅能容许或否认服务，而且也能够保护在一个服务之内的单独操作
18．以下哪种特点是代理服务所具备的（A ）
A． 代理服务允许用户“直接”访问因特网，对用户来讲是透明的
B． 代理服务能够弥补协议本身的缺陷
C． 所有服务都可以进行代理
D． 代理服务不适合于做日志
19．图一所示属于哪一种防火墙体系结构：（ B ）
A． 双重宿主主机体系结构
B． 主机过滤体系结构
C． 子网过滤体系结构
D． 使用双重宿主主机与子网过滤相结构的体系结构
20．关于堡垒主机的说法，错误的是：（ B ）
A．设计和构筑堡垒主机时应使堡垒主机尽可能简单
B．堡垒主机的速度应尽可能快
C．堡垒主机上应保留尽可能少的用户账户，甚至禁用一切用户账户
D．堡垒主机的操作系统可以选用 UNIX 系统
21．包过滤技术可以允许或不允许某些包在网络上传递，它过滤的判据不包括：（ D ）
A． 数据包的目的地址
B． 数据包的源地址
C． 数据包的传送协议
D． 数据包的具体内容
22．在堡垒主机上，我们需要关闭或保留一些服务，以下做法中哪个是错误的：（ B ）
A． 如果我们不需要该服务，则将它关闭
B． 如果我们不了解该服务的功能，可将其打开
C． 如果我们将该服务关闭后引起系统运行问题，则再将它打开
D． 应该保留一些让堡垒主机提供给内部网用户的服务，如：Telnet、FTP 服务
23．以下关于宏病毒的认识，哪个是错误的：（D ）
A． 宏病毒是一种跨平台式的计算机病毒
B． “台湾 1 号”是一种宏病毒
C． 宏病毒是用 Word Basic 语言编写的
D． 在不同的 Word 版本格式中的宏病毒是互相兼容的，可以相互传播
24．包过滤系统不能够让我们进行以下哪种情况的操作：（ C ）
A． 不让任何用户从外部网用 Telnet 登录
B． 允许任何用户使用 SMTP 往内部网发电子邮件
C． 允许用户传送一些文件而不允许传送其他文件
D． 只允许某台机器通过 NNTP 往内部网发新闻
25．宇宙飞船、卫星等控制系统一般采用容错系统中哪种类型：（ B ）
A．关键任务计算系统 B．长寿命系统
C．高可用度系统 D．高性能计算系统
26. 联网上网服务营业场所管理办法》规定的。
A．记录有关上网信息，记录备份保存 60 日；
B．经营含有暴力内容的电脑游戏；

C．向未成年人开放的时间限于国家法定节假日每日 8 时至 21 时；
D．有与营业规模相适应的专业技术人员和专业技术支持；
27. 在建立口令时最好要遵循的规则是 【D】 。
A．使用英文单词；B．选择容易记的口令；
C．使用自己和家人的名字；D．尽量选择长的口令.
28. 病毒扫描软件由 【D】 组成
A．仅由病毒代码库； B．仅由利用代码库进行扫描的扫描程序；
C．仅由扫描程序 D．代码库和扫描程序
29. 在选购防火墙软件时，不应考虑的是： 【A】
E. 一个好的防火墙应该为使用者提供唯一的平台；
F. 一个好的防火墙必须弥补其他操作系统的不足；
G. 一个好的防火墙应该是一个整体网络的保护者；
H. 一个好的防火墙应能向使用者提供完善的售后服务。
30. 包过滤工作在 OSI 模型的 【C】
A. 应用层； B. 表示层； C. 网络层和传输层； D. 会话层
31. 如果路由器有支持内部网络子网的两个接口，很容易受到 IP 欺骗，从这个意义上讲，将 Web 服务器放在防火墙 【A】 有时更安全些。
A. 外面； B. 内部； C. 一样； D. 不一定
32.Windows NT 网络安全子系统的安全策略环节由 【D】 构成。
A．身份识别系统
B．资源访问权限控制系统
C．安全审计系统
D．以上三个都是
33. 关于堡垒主机叙述正确的是 【D】 。
A．堡垒主机应放置在有机密信息流的网络上
B．堡垒主机应具有较高的运算速度
C．建立堡垒主机的基本原则是：复杂原则和预防原则
D．堡垒主机上禁止使用用户账户
34. 不属于操作系统脆弱性的是 【C】 。
A．体系结构 B．可以创建进程
C．文件传输服务 D．远程过程调用服务
35. 关于摘要函数，叙述不正确的是 【C】 。
A．输入任意大小的消息，输出是一个长度固定的摘要
B．输入消息中的任何变动都会对输出摘要产生影响
C．输入消息中的任何变动都不会对输出摘要产生影响
D．可以防止消息被改动
36. 提高数据完整性的办法是 【D】 。
A．备份 B．镜像技术 C．分级存储管理
D．采用预防性技术和采取有效的恢复手段
37. 网络安全性策略应包括网络用户的安全责任、 【B】 、正确利用网络资源和检测到安全问题时的对策
A．技术方面的措施
B．系统管理员的安全责任
C．审计与管理措施

D．方便程度和服务效率

38. 数据库的故障是指从保护安全的角度出发，数据库系统中会发生的各种故障。这些故障主要包括：_【C】 、系统故障、介质故障和计算机病毒与黑客。

A． 丢失修改故障

B． 不能重复读故障

C． 事务内部的故障

D． 不正确数据读出故障

39. 网络病毒是由因特网衍生出的新一代病毒，即 JAVA 及 ACTIVEX 病毒。 【A】 ，不被人们察觉。

A. 它不需要停留在硬盘中可以与传统病毒混杂在一起

B. 它停留在硬盘中且可以与传统病毒混杂在一起

C. 它不需要停留在硬盘中且不与传统病毒混杂在一起

D. 它停留在硬盘中且不与传统病毒混杂在一起

40. 在通用的两类加密算法中，限制使用的最大问题是加密速度，由于这个限制，该算法的加密技术，目前主要用于网络环境中的加密。【B】

A. RSA，固定的信息

B. RSA，不长的信息

C. DES，不长的信息

D. IDEA，不长的信息

41.外部路由器真正有效的任务就是阻断来自 【A】 上伪造源地址进来的任何数据包。

A. 外部网 B. 内部网

C. 堡垒主机 D. 内部路由器

42. 以下各图中那一种是属于“主机过滤体系结构”的防火墙 【B】 。

A B

43. 如果入侵者仅仅侵入到参数网络的堡垒主机，他只能偷看到 【C】 的信息流。

A. 内部网络

B. 内部路由器

C. 参数网络

D. 堡垒主机

44. 在公钥密码系统中，发件人用收件人的加密信息，收件人用自己的解密，而且也只有收件人才能解密。【B】

A． 公钥，公钥

B． 公钥，私钥

C． 私钥，私钥

D． 私钥，公钥

45.在用户使用 Telnet 或 FTP 连接到远程主机上时，在因特网上传输的口令是没有加密的，那么入侵系统的一个方法就是通过监视携带用户名和口令的 【B】 获取用户信息。

A. TCP 包 B. IP 包

C. ICMP 包 D. UDP 包

46. 以下哪个是扫描工具 【D】 。

A. Xhost B. NNTP

C. UUCP D. Etheral

47.最有效的保护 E-mail 的方法是使用数字签名，常用的数字签名软件有 【C】 。

A. KDC B. OTP

C. PGP　　D. IDEA

48. 在网络上，为了监听效果最好，监听设备不应放在 【D】 。

A．网关 B．路由器

C．防火墙 D．中继器

49.以下哪种特点是代理服务所具备的 【A】 。

A. 代理服务允许用户“直接”访问因特网，对用户来讲是透明的

B. 代理服务能够弥补协议本身的缺陷

C. 所有服务都可以进行代理

D. 代理服务不适合于做日志

50.包过滤技术可以允许或不允许某些包在网络上传递，它过滤的判据不包括： 【D】

A. 数据包的目的地址

B. 数据包的源地址

C. 数据包的传送协议

E. 数据包的具体内容

51.Windows NT 网络安全子系统的安全策略环节由 D 构成。

A．身份识别系统

B．资源访问权限控制系统

C．安全审计系统

D．A、B、C

52.用无病毒的 DOS 引导软盘启动计算机后，运行 FDISK 用于____C_____。

A． 磁盘格式化

B． 读取或重写软盘分区表

C． 读取或重写硬盘分区表

D． 仅是重写磁盘分区表

53. PGP 是一个对电子邮件加密的软件。其中 D

A．用来完成数字签名的算法是 RSA，加密信函内容的算法是非对称加密算法 IDEA。

B．用来完成数字签名的算法是 IDEA，加密信函内容的算法是对称加密算法 MD5。

C．用来完成数字签名的算法是 MD5，加密信函内容的算法是非对称加密算法 IDEA。

D．用来完成身份验证技术的算法是 RSA，加密信函内容的算法是对称加密算法 IDEA。

54. 代理服务 B 。

A．需要特殊硬件，大多数服务需要专用软件

B．不需要特殊硬件，大多数服务需要专用软件

C．需要特殊硬件，大多数服务不需要专用软件

D．不需要特殊硬件，大多数服务不需要专用软件险

55．对于 IP 欺骗攻击，过滤路由器不能防范的是 C 。

A．伪装成内部主机的外部 IP 欺骗

B．外部主机的 IP 欺骗

C．伪装成外部可信任主机的 IP 欺骗

D．内部主机对外部网络的 IP 地址欺骗

56．FTP 服务器上的命令通道和数据通道分别使用 A 端口。

A．21 号和 20 号 B．21 号和大于 1023 号

C．大于 1023 号和 20 号 D．大于 1023 号和大于 1023 号

57．屏蔽路由器数据包过滤 A 。

A．允许已经由数据包过滤的服务

B．不允许已经由数据包过滤的服务
C．允许来自内部主机的所有连接
D．不允许数据包从因特网向内部网移动
58．采用公用/私有密钥加密技术， C 。
A．私有密钥加密的文件不能用公用密钥解密
B．公用密钥加密的文件不能用私有密钥解密
C．公用密钥和私有密钥相互关联
D．公用密钥和私有密钥不相互关联
59．建立口令不正确的方法是 C 。
A．选择 5 个字符串长度的口令
B．选择 7 个字符串长度的口令
C．选择相同的口令访问不同的系统
D．选择不同的口令访问不同的系统
60．包过滤系统 B。
A．既能识别数据包中的用户信息，也能识别数据包中的文件信息
B．既不能识别数据包中的用户信息，也不能识别数据包中的文件信息
C．只能识别数据包中的用户信息，不能识别数据包中的文件信息
D．不能识别数据包中的用户信息，只能识别数据包中的文件信息
61．关于堡垒主机的配置，叙述正确的是 A 。
A．堡垒主机上禁止使用用户账户
B．堡垒主机上应设置丰富的服务软件
C．堡垒主机上不能运行代理
D．堡垒主机应具有较高的运算速度
62．有关电子邮件代理，描述不正确的是 C 。
A．SMTP 是一种“存储转发”协议，适合于进行代理
B．SMTP 代理可以运行在堡垒主机上
C．内部邮件服务器通过 SMTP 服务，可直接访问外部因特网邮件服务器，而不必经过堡垒主机
D．在堡垒主机上运行代理服务器时，将所有发往这个域的内部主机的邮件先引导到堡垒主机上
63．在通用的两类加密算法中，限制_____使用的最大问题是加密速度，由于这个限制，该算法的加密技术，目前主要用于网络环境中的_____加密。（B）
A. RSA，固定的信息
B. RSA，不长的信息
C. DES，不长的信息
D. IDEA，不长的信息
64．对于包过滤系统，描述不正确的是 。（B）
A．允许任何用户使用 SMTP 向内部网发送电子邮件
B．允许某个用户使用 SMTP 向内部网发送电子邮件
C．只允许某台机器通过 NNTP 往内部网发送新闻
D．不允许任何用户使用 Telnet 从外部网登录
65．对于数据完整性，描述正确的是 。(A)
A．正确性、有效性、一致性
B．正确性、容错性、一致性

C．正确性、有效性、容错性
D．容错性、有效性、一致性
66．按照密钥类型，加密算法可以分为 。(D)
A.. 序列算法和分组算法
B．序列算法和公用密钥算法
C．公用密钥算法和分组算法
D．公用密钥算法和对称密钥算法
67．不属于代理服务缺点的是 。(B)
A．每个代理服务要求不同的服务器
B．一般无法提供日志
C．提供新服务时，不能立刻提供可靠的代理服务
D．对于某些系统协议中的不安全操作，代理不能判断
68．在 Windows NT 中，当系统管理员创建了一个新的用户账户后，不可以 。(B)
A．对用户访问时间作出规定
B．对用户访问因特网的次数作出规定
C．对用户口令作出必要的规定
D．对普通用户口令作出强制性规定
69．关于摘要函数，叙述不正确的是 。(C)
A．输入任意大小的消息，输出是一个长度固定的摘要
B．输入消息中的任何变动都会对输出摘要产生影响
C．输入消息中的任何变动都不会对输出摘要产生影响
D．可以防止消息被改动
70．对于回路级代理描述不正确的是 。(D)
A．在客户端与服务器之间建立连接回路
B．回路级代理服务器也是公共代理服务器
C．为源地址和目的地址提供连接
D．不为源地址和目的地址提供连接
71．提高数据完整性的办法是 。(D)
A．备份 B．镜像技术 C．分级存储管理
D．采用预防性技术和采取有效的恢复手段
72．关于加密密钥算法，描述不正确的是 。(A)
A． 通常是不公开的，只有少数几种加密算法
B． 通常是公开的，只有少数几种加密算法
C． DES 是公开的加密算法
D． IDEA 是公开的加密算法
73．在子网过滤体系结构的防火墙中，外部路由器真正有效的任务就是阻断来自_____上伪造源地址进来的任何数据包。(A)
A． 外部网
B． 内部网
C． 堡垒主机
D． 内部路由器
74．如果路由器有支持内部网络子网的两个接口，很容易受到 IP 欺骗，从这个意义上讲，将 Web 服务器放在防火墙____有时更安全些。(A)
B. 外面； B.内；C.一样； D.不一定

75．防火墙采用的最简单的技术是：(C)
A.安装维护卡; B.隔离; C.包过滤; D.设置进入密码

75、许多黑客攻击都是利用软件实现中的缓冲区溢出的漏洞，对于这一威胁，最可靠的解决方案是什么? 【 B 】
A 安装防病毒软件 B 给系统安装最新的补丁
C 安装防火墙 D 安装入侵检测系统

76、使网络服务器中充斥着大量要求回复的信息，消耗带宽.导致网络或系统停止正常服务，这属于什么攻击类型？ 【 A 】
A 拒绝服务 B 文件共享
C BIND 漏洞 D 远程过程调用

77 下面哪一个情景属于身份验证(Authentication)过程。 【 B 】
A 用户在网络上共享了自己编写的一份 0ffice 文档，并设定哪些用户可以阅读，哪些用户可以修改
B 用户护照系统提示输入用户名和口令
C 某个人尝试登录到你的计算机中，但是口令输入的不对．系统提示口令错误，并将这次失畋的登录过程纪录在系统日志中
D 用户使用加密软件对自己编写的 Ofrice 文档进行加密,解密后看到文档中的内容

78 一个数据包过滤系统被设计成只允许你要求服务的数据包进入，而过滤掉不必要的服务。这属于什么基本原则? 【 A 】
A 最小特权 B 阻塞点 c 失效保护状态 D 防御多样化

78 下面的说法正确的是_____ 【 D 】
A 信息的泄漏只在信息的传输过程中发生。
B 信息的泄漏只在信息的存储过程中发生。
c 信息的泄漏只在信息的传输和存储过程中发生.
D 上面三个都不对

79 在以下人为的恶意攻击行为中．属于主动攻击的是 【 D 】
A 身份假冒 B 数据窃听
c 数据流分析 D 非法访问

80 防火墙____通过它的连接。【 A 】
A 不能控制 B 能控制
C 能过滤 D 能禁止

81 以下不属于代理服务技术优点的是【 C 】
A 可以实现身份认证
B 内部地址的屏蔽和转换功能

C 可以实现访问控制
D 可以防范数据驱动攻击

82 安全审计跟踪是_____ 【 D 】
A 安全审计系统检测并追踪安全事件的过程
B 安全审计系统收集用于安全审计的数据
c 人利用日志信息进行安全事件分析和追溯的过程
D 对计算机系统中的某种行为的详尽跟踪和观察

83 在建立堡垒主机时 【 A 】
A 在堡垒主机上应设置尽可能少的网络服务
B 在堡垒主机上应设置尽可能多的网络服务
c 对必须设置的服务给予尽可能高的权限
D 不论发生任何入侵情况．内部网络始终信任堡垒主机

84 下列说法中不正确的是【 D】
A IP 地址甩于标识连八 Internet 上的计算机
B 在 lpv4 协议中。一个 lP 地址由 32 位二进制数组成
c．在 lDw 拚议中．1P 地址常用带点的十进制标记法书写
D. A、B、C 类地址是单播地址，D、E 类是组播地址

85 Unix 和 Window NT 操作系统是符合哪个级别的安全标准【 C 】
A A 级 B B 级
C C 级 D D 级

86 域名服务系统(DNS)的功能是【A 】
A 完成域名和 Ip 地址之间的转换
B．完成域名和两卡地址之问的转换
c．完成主机名和 IP 地址之同的转换
D 完成域名和电子邮件之阑的转换

87 防止用户被冒名所欺骗的方法是:【 A】
A 对信息源发方进行身份验证
B 进行数据加密
c 对访问网络的流量进行过滤和保护
D 采用防火墙

88 关于 80 年代 Morris 蠕虫危害的描述。哪句话是错误的? 【B 】
A 占用了大量的计算机处理器的时阿，导致拒绝服务
B 窃取用户的机密信息，破坏计算机数据文件
C 该蠕虫利用 Unix 系统上的漏洞传播
D 丈量的流量堵塞了硒络，导致网络瘫痪

89 以下关于防火墙的设计原则说法正确的是 【A 】

A 保持设计的简单性
B 不单单要提供防火培的功能，还要尽量使用较大的组件
90 保留尽可能多的服务和守护进程．从而能提供更多的网络服务
D 一套防火墙就可以保护全部的网络

91 数据链路层的数据单元一般称为【A 】
A 帧 B 段
c 丹组或包　　D 比特

92 以下哪一项不属于入侵检测系统的功能 【C 】
A．监视网络上的通信数据流
B 捕捉可疑的网络活动
C 提供安全审计报告
D 过滤非法的数据包

93 Tcp/IP 协议中，负责寻址和路由功能的是哪一层?【 D】
A 传输层
B 数据链路层
c．应用层
D 网络层

94 计算机网络按威胁对象大体可分为两种：一是对网络中信息的威胁；二是:【 B】
A 人为破坏
B 对网络中设备的威胁
c 病毒威胁
D 对网络人员的威胁

92 物理安全的管理应做到　　【 D 】
A 所有相关人员都必须进行相应的培训．明确个人工作职责
B 制定严格的值班和考勤制度，安排人员定期检查各种设备的运行情况
c 在重要场所的进出口安装监视器，并对进出情况进行录像
D 以上均正确

93 为了防御网络监听，屈常用的方法是【B 】
A 采用物理传输(非网络)
B 信息加密
c 无线网
D 使用专线传输

94 容灾的目的和实质是 【C 】
A 数据备份　　B 心理安慰　C 保持信息系统的业务持续性　　D 以上均正确

95 向有限的空间输入超量的字符串是哪一种攻击手段?　【 C】
A 网络监听　　B 拒绝服务

C 缓冲区溢出　D IP 欺骗

96 美国国防部发布的可信计算机系统评估标准(TcsEc)定义了（） 个等级 【C 】
A 五　　B 六　C 七　D 八

97 数据保密性是指 【 A】
A 保护网络中各系统之间交换的数据，防止因数据被截获而造成泄密
B 提供连接实体身份的鉴别
c 防止非法实体对用户的主动攻击，保证数据接受方收到的细腻些与发送方发送的信息完全一致
D 确保数据是由合法实体发出的

98 下面不是数据库的基本安全机制的是 【D 】
A 用户认证
B 用户授权
c 审计功能
D 电磁屏蔽

99 包过滤技术与代理服务技术相比较 【 B】
A 包过滤技术安全性较弱、但不会对两络性能产生明显影响
B 包过滤技术对应用和用户是绝对透明的
c 代理服务技术安全性较高、但不会对网络性能产生明显影响
D 代理服务技术安全性高．对应用和用户透明度也很高

100 防火墙是(　)在网络环境中的应用。　　【 B 】
A 字符串匹配
B 访问控制技术
c 入侵检测技术
D 防病毒技术

101 当同一网段中两台工作站配置了相同的 IP 地址时，会导致　　【 A 】
A 先入者被后入者挤出网络而不能使用
B 双方都会得到警告。但先入者继续工作，而后入者不能
C 双方可以同时正常工作，进行数据的传输
D 双方都不能工作，都得到网址冲突的警告

102 基于网络的^侵检测系统的信息源是:【B 】
A 系统的审计日志 B 系统的行为数据
C 应用程序的事物日志　　D 刚络中的数据包

103 黑客利用 IP 地址进行攻击的方法有:【A 】
A IP 欺骗　　B 解密
C 窃取口令　　D 发送病毒

104 下面关于响应的说法正确的是： 【D 】

A 主动响应和被动响应是互相对立的，不能同时采用

B 被动响应是入侵检测系统的唯一响应方式

C 入侵检测系统提供的警报方式只能显示在屏幕上的警告信息或窗口

D 主支响应的方式可以自动发送邮件给入侵发起主的系统管理员请求协助以识别问题和处理问题

105 屏蔽路由器型防火墙采用的技术是基于【 B】

A 代理服务技术 B 数据包过滤技术

c 应用网关技术 D 三种技术的结合

106 下面病毒出现的时间展晚的类型是 【 B】

A． 携带特洛伊木马的病毒

B． 以网络钓鱼为目的的病毒

C． 通过网络传播的蠕虫病毒

D. office 文档携带的宏病毒

107 CA 指的是： 【 B】

A 加密认证 B 证书授权

C 虚拟专用网 D 安全套接层

108 不能防止计算机感染病毒的措施是： 【 A】

A 定时备份重要文件

B 经常更新操作系统

c 除非确切知道附件内容．否则不要打开电子邮件附件

D 重要部门的计算机尽量专机专用与外界隔绝

109 以下关于计算机病毒的特征说法正确曲是： 【C 】

A 计算机病毒只具有破坏性，没有其他特征

B．计算机病毒具有破坏性，不具有传染性

C 破坏性和传染性是计算机病毒的两大主要特征

D 计算机病毒只具有传染性．不具有破坏性

110 下列内容过滤技术中在我国没有得到广泛应用的是 【 A】

A 内容分级审查

B 关键字过滤技术

c 启发式内容过滤拄术

D 机器学习技术

111 防火墙中地址翻译的主要作用是:【 B】

A 提供代理服务

B 隐藏内部网络地址

C 进行入侵检测

D 防止病毒入侵

1.下面不是计算机网络面临的主要威胁的是（　B　）
A.恶意程序威胁　　B.计算机软件面临威胁
C.计算机网络实体面临威胁　D.计算机网络系统面临威胁
2.密码学的目的是（　D　）
A.研究数据加密　　B.研究数据解密
C.研究数据保密　　D.研究信息安全
3.假设使用一种加密算法，它的加密方法很简单：将每一个字母加 5，即 a 加密成 f。这种算法的密钥就是 5，那么它属于（　D　）
A.对称加密技术　　B.分组密码技术
C.公钥加密技术　　D.单向函数密码技术
4.根据美国联邦调查局的评估，80%的攻击和入侵来自（　B　）
A.接入网　　B.企业内部网
C.公用 IP 网　　D.个人网
5.下面_____不是机房安全等级划分标准。（　A　）
A.D 类　B.C 类
C.B 类　　D.A 类
6.下面有关机房安全要求的说法正确的是（　D　）
A.电梯和楼梯不能直接进入机房　　B.机房进出口应设置应急电话
C.照明应达到规定范围　D.以上说法都正确
7.关于机房供电的要求和方式，说法不正确的是（　A　）
A.电源应统一管理技术　B.电源过载保护技术和防雷击计算机
C.电源和设备的有效接地技术 D.不同用途的电源分离技术
8.下面属于单钥密码体制算法的是（　　C　）
A.RSA　B.LUC
C.DES　D.DSA
9.对网络中两个相邻节点之间传输的数据进行加密保护的是（　A　）
A.节点加密　　B.链路加密
C.端到端加密　D.DES 加密
10.一般而言，Internet 防火墙建立在一个网络的（　A　）
A.内部网络与外部网络的交叉点　　B.每个子网的内部
C.部分内部网络与外部网络的结合处　　D.内部子网之间传送信息的中枢
11.下面是个人防火墙的优点的是（D　　）
A.运行时占用资源
B.对公共网络只有一个物理接口
C.只能保护单机，不能保护网络系统
D.增加保护级别
12.包过滤型防火墙工作在（　C　）
A.会话层　　B.应用层
C.网络层　　D.数据链路层
13.入侵检测是一门新兴的安全技术，是作为继_____之后的第二层安全防护措施。（　B　）
A.路由器　　B.防火墙
C.交换机　　D.服务器

14._____是按照预定模式进行事件数据搜寻，最适用于对已知模式的可靠检测。（ D ）
A.实时入侵检测 B.异常检测
C.事后入侵检测 D.误用检测
15._____的目的是发现目标系统中存在的安全隐患，分析所使用的安全机制是否能够保证系统的机密性、完整性和可用性。（ A ）
A.漏洞分析 B.入侵检测
C.安全评估 D.端口扫描
16.端口扫描的原理是向目标主机的_____端口发送探测数据包，并记录目标主机的响应。（ C ）
A.FTP B.UDP
C.TCP/IP D.WWW
17.计算机病毒是（ B ）
A.一个命令 B.一个程序
C.一个标记 D.一个文件
18.下面关于恶意代码防范描述正确的是（ D ）
A.及时更新系统，修补安全漏洞 B.设置安全策略，限制脚本
C.启用防火墙，过滤不必要的服务 D.以上都正确
19.计算机网络安全体系结构是指（ A ）
A.网络安全基本问题应对措施的集合 B.各种网络的协议的集合
C.网络层次结构与各层协议的集合 D.网络的层次结构的总称
20.下面不是计算机信息系统安全管理的主要原则的是（ B ）
A.多人负责原则 B.追究责任原则
C.任期有限原则 D.职责分离原则
1.TCP/IP 协议安全隐患不包括(D)
A.拒绝服务 B.顺序号预测攻击
C.TCP 协议劫持入侵 D.设备的复杂性
2.IDEA 密钥的长度为(D)
A.56 B.64
C.124 D.128
3.在防火墙技术中，内网这一概念通常指的是(A)
A.受信网络 B.非受信网络
C.防火墙内的网络 D.互联网
4.《计算机场、地、站安全要求》的国家标准代码是(B)
A.GB57104-93B.GB9361-88
C.GB50174-88D.GB9361-93
5.在 Kerberos 中，Client 向本 Kerberos 的认证域以内的 Server 申请服务的过程分为几个阶段?(A)
A.三个 B.四个
C.五个 D.六个
6.信息安全技术的核心是(A)
A.PKI B.SET
C.SSL D.ECC
7.Internet 接入控制不能对付以下哪类入侵者? (C)
A.伪装者 B.违法者

C.内部用户 D.地下用户
8.CA 不能提供以下哪种证书? (D)
A.个人数字证书 B.SSL 服务器证书
C.安全电子邮件证书 D.SET 服务器证书
9.我国电子商务走向成熟的重要里程碑是(A)
A.CFCA B.CTCA
C.SHECA D.RCA
10.通常为保证商务对象的认证性采用的手段是(C)
A.信息加密和解密 B.信息隐匿
C.数字签名和身份认证技术 D.数字水印
11.关于 Diffie-Hellman 算法描述正确的是(B)
A.它是一个安全的接入控制协议 B.它是一个安全的密钥分配协议
C.中间人看不到任何交换的信息 D.它是由第三方来保证安全的
12.以下哪一项不在证书数据的组成中? (D)
A.版本信息 B.有效使用期限
C.签名算法 D.版权信息
13.计算机病毒的特征之一是(B)
A.非授权不可执行性 B.非授权可执行性
C.授权不可执行性 D.授权可执行性
14.在 Kerberos 中，Client 向本 Kerberos 认证域外的 Server 申请服务包含几个步骤? (C)
A.6 B.7
C.8 D.9
15.属于 PKI 的功能是(C)
A.PAA，PAB，CA B.PAA，PAB，DRA
C.PAA，CA，ORA D.PAB，CA，ORA

1、当你感觉到你的 Win2000 运行速度明显减慢，当你打开任务管理器后发现 CPU 的使用率达到了百分之百，你最有可能认为你受到了哪一种攻击。 B
A、特洛伊木马 B、拒绝服务
C、欺骗 D、中间人攻击

2、RC4 是由 RIVEST 在 1987 年开发的，是一种流式的密文，就是实时的把信息加密成一个整体，它在美国一般密钥长度是 128 位，因为受到美国出口法的限制，向外出口时限制到多少位？ C
A、64 位 B、56 位
C、40 位 D、32 位

3、假如你向一台远程主机发送特定的数据包，却不想远程主机响应你的数据包。这时你使用哪一种类型的进攻手段？ B
A、缓冲区溢出 B、地址欺骗
C、拒绝服务 D、暴力攻击

4、小李在使用 super scan 对目标网络进行扫描时发现，某一个主机开放了 25 和 110 端口，

此主机最有可能是什么？ B
A、文件服务器 B、邮件服务器
C、WEB 服务器 D、DNS 服务器

5、你想发现到达目标网络需要经过哪些路由器，你应该使用什么命令？ C
A、ping B、nslookup
C、tracert D、ipconfig

6、以下关于 VPN 的说法中的哪一项是正确的？ C
A、VPN 是虚拟专用网的简称，它只能只好 ISP 维护和实施
B、VPN 是只能在第二层数据链路层上实现加密
C、IPSEC 是也是 VPN 的一种
D、VPN 使用通道技术加密，但没有身份验证功能

7、下列哪项不属于 window2000 的安全组件？ D
A、访问控制
B、强制登陆
C、审计
D、自动安全更新
8、以下哪个不是属于 window2000 的漏洞？ D
A、unicode
B、IIS hacker
C、输入法漏洞
D、单用户登陆
9、你是一企业网络管理员，你使用的防火墙在 UNIX 下的 IPTABLES，你现在需要通过对防火墙的配置不允许 192.168.0.2 这台主机登陆到你的服务器，你应该怎么设置防火墙规则？ B
A、iptables—A input—p tcp—s 192.168.0.2—source—port 23—j DENY
B、iptables—A input—p tcp—s 192.168.0.2—destination—port 23—j DENY
C、iptables—A input—p tcp—d 192.168.0.2—source—port 23—j DENY
D、iptables—A input—p tcp—d 192.168.0.2—destination—port 23—j DENY
10、你的 window2000 开启了远程登陆 telnet，但你发现你的 window98 和 unix 计算机没有办法远程登陆，只有 win2000 的系统才能远程登陆，你应该怎么办？ D
A、重设防火墙规则
B、检查入侵检测系统
C、运用杀毒软件，查杀病毒
D、将 NTLM 的值改为 0
11、你所使用的系统为 win2000，所有的分区均是 NTFS 的分区，C 区的权限为 everyone 读取和运行，D 区的权限为 everyone 完全控制，现在你将一名为 test 的文件夹，由 C 区移动到 D 区之后，test 文件夹的权限为？ B
A、everyone 读取和运行
B、everyone 完全控制
C、everyone 读取、运行、写入
D、以上都不对

12、你所使用的系统为 UNIX，你通过 umask 命令求出当前用户的 umask 值为 0023，请问该用户在新建一文件夹，具体有什么样的权限？ A

A、当前用户读、写和执行，当前组读取和执行，其它用户和组只读

B、当前用户读、写，当前组读取，其它用户和组不能访问

C、当前用户读、写，当前组读取和执行，其它用户和组只读

D、当前用户读、写和执行，当前组读取和写入，其它用户和组只读

13、作为一个管理员，把系统资源分为三个级别是有必要的，以下关于级别 1 的说法正确的是？ A

A、对于那些运行至关重要的系统，如，电子商务公司的用户帐号数据库

B、对于那些必须的但对于日常工作不是至关重要的系统

C、本地电脑即级别 1

D、以上说法均不正确

14、以下关于 window NT 4.0 的服务包的说法正确的是？ C

A、sp5 包含了 sp6 的所有内容

B、sp6 包含了 sp5 的所有内容

C、sp6 不包含 sp5 的某些内容

D、sp6 不包含 sp4 的某些内容

15、你有一个共享文件夹，你将它的 NTFS 权限设置为 sam 用户可以修改，共享权限设置为 sam 用户可以读取，当 sam 从网络访问这个共享文件夹的时候，他有什么样的权限？ A

A、读取

B、写入

C、修改

D、完全控制

16、SSL 安全套接字协议所使用的端口是： B

A、80

B、443

C、1433

D、3389

17、Window2000 域或默认的身份验证协议是： B

A、HTML

B、Kerberos V5

C、TCP/IP

D、Apptalk

18、在 Linux 下 umask 的八进制模式位 6 代表： C

A、拒绝访问

B、写入

C、读取和写入

D、读取、写入和执行

19、你是一个公司的网络管理员，你经常在远程不同的地点管理你的网络（如家里），你公司使用 win2000 操作系统，你为了方便远程管理，在一台服务器上安装并启用了终端服务。最近，你发现你的服务器有被控制的迹象，经过你的检查，你发现你的服务器上多了一个不熟悉的帐户，你将其删除，但第二天却总是有同样的事发生，你应该如何解决这个问题？ C

A、停用终端服务

B、添加防火墙规则，除了你自己家里的 IP 地址，拒绝所有 3389 的端口连入

C、打安全补丁 sp4
D、启用帐户审核事件，然后查其来源，予以追究
20、以下不属于 win2000 中的 ipsec 过滤行为的是： D
A、允许
B、阻塞
C、协商
D、证书
21、以下关于对称加密算法 RC4 的说法正确的是： B
A、它的密钥长度可以从零到无限大
B、在美国一般密钥长度是 128 位，向外出口时限制到 40 位
C、RC4 算法弥补了 RC5 算法的一些漏洞
D、最多可以支持 40 位的密钥
22、你配置 UNIX 下的 Ipchains 防火墙，你要添加一条规则到指定的 chain 后面，你应该使用参数： A
A、—A
B、—D
C、—S
D、—INPUT

一、填空题
1、网络安全的特征有： 保密性、 完整性、 可用性、 可控性。
2、网络安全的结构层次包括：物理安全、 安全控制、 安全服务。
3、网络安全面临的主要威胁：黑客攻击、 计算机病毒、 拒绝服务
4、计算机安全的主要目标是保护计算机资源免遭：毁坏、 替换、 盗窃、 丢失。
5、就计算机安全级别而言，能够达到 C2 级的常见操作系统有：UNIX、Xenix、 Novell 3.x、Windows NT。
6、一个用户的帐号文件主要包括： 登录名称、 口令、 用户标识号、 组标识号、用户起始目标。
7、数据库系统安全特性包括：数据独立性、 数据安全性、 数据完整性、 并发控制、故障恢复。
8、数据库安全的威胁主要有：篡改、 损坏、 窃取。
9、数据库中采用的安全技术有：用户标识和鉴定、 存取控制、 数据分级、 数据加密。
10、计算机病毒可分为：文件病毒、 引导扇区病毒、 多裂变病毒、 秘密病毒、异性病毒、宏病毒 等几类。
11、文件型病毒有三种主要类型：覆盖型、 前后依附型、 伴随型。
12、密码学包括：密码编码学、 密码分析学
13、网络安全涉及的内容既有 技术方面的问题，也有管理方面的问题。
14、网络安全的技术方面主要侧重于防范 外部非法用户的攻击。
15、网络安全的管理方面主要侧重于防止 内部人为因素的破坏。
16、保证计算机网络的安全，就是要保护网络信息在存储和传输过程中的 保密性、完整性 、可用性、可控性和真实性。
17、传统密码学一般使用 置换和替换两种手段来处理消息。
18、数字签名能够实现对原始报文的 鉴别和 防抵赖 .。
19、数字签名可分为两类：直接签名和仲裁签名。

20、为了网络资源及落实安全政策，需要提供可追究责任的机制，包括： 认证、 授权和 审计。
21、网络安全的目标有： 保密性 、 完整性、 可用性 、 可控性和 真实性。
22、对网络系统的攻击可分为： 主动攻击和被动 攻击两类。
23、防火墙应该安装在内部网 和 外部网之间 。
24、网络安全涉及的内容既有 技术 方面的问题，也有管理方面的问题。
25、网络通信加密方式有 链路 、节点加密和端到端加密三种方式。
26、密码学包括： 密码编码学、 密码分析学

二、1. 目前，典型的网络结构通常是由一个主干网和若干段子网组成，主干网与子网之间通常选用 路由器 进行连接。
2. 以太网的介质访问控制方式是：_载波监听多路访问/冲突检测(CSMA/CD。
3. 计算机网络安全受到的威胁主要有：黑客的攻击、计算机病毒和拒绝服务访问攻击。
4. 设置信息包筛的最常用的位置是路由器，信息包筛可以审查网络通信并决定是否允许该信息通过。
5. 选择性访问控制不同于强制性访问控制。强制性访问控制是从 B1 级的安全级别开始出现。
6. 对一个用户的认证，其认证方式可分为三类：用生物识别技术进行鉴、用所知道的事进行鉴别和使用用户拥有的物品进行鉴别。
7. 对数据库构成的威胁主要有： 篡改 、 损坏 和__窃取 。
8. 检测计算机病毒中，检测的原理主要是基于四种方法： 比较法 、 搜索法 、计算机病毒特征字的识别法和分析法。
9. 基于密钥的加密算法通常有两类，即 对称算法和 公用密钥算法 。
10. 因特网的许多事故的起源是因为使用了薄弱的、静态的口令。因特网上的口令可以通过许多方法破译，其中最常用的两种方法是 把加密的口令解密 和 通过监视信道窃取口令 。
11. 存储子系统是网络系统中最易发生故障的部分，实现存储系统冗余的最为流行的几种方法是 磁盘镜像 、 磁盘双联和 RAID 。
12. 依靠伪装发动攻击的技术有两种，一种是 源地址伪装，另一种是 途中人的攻击。
13. 证书有两种常用的方法：CA 的分级系统和信任网。
14. 网络安全的特征应具有保密性、完整性、可用性和可控性 四个方面的特征。
15. 网络信息安全模型中 政策、法律、法规 是安全的基石，它是建立安全管理的标准和方法。
16. 再生机制（或自我复制机制）是判断是不是计算机病毒的最重要的依据。
17. 解决 IP 欺骗技术的最好方法是： 安装过滤路由器。
18. 防火墙有 双重宿主主机 、 主机过滤 和 子网过滤 三种体系结构。
19. 在包过滤系统中，常用的方法有依据 地址 和 服务进行过滤。
20. 黑客攻击的三个阶段是： 收集信息 、 探测系统安全弱点 和 网络攻击 。
21. 堡垒主机目前一般有三种类型：无路由双宿主主机， 牺牲主机 ，内部堡垒主机。
22. 包过滤系统不能识别 数据包中的用户信息 ，同样包过滤系统也不能识别 数据包中的文件信息 。
23. Unix 和 Windows NT 操作系统能够达到 C2 安全级别。
24. 《中华人民共和国计算机信息安全保护条例》中定义的“编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码”是指 计算机病毒 。
25. 从逻辑上讲，防火墙是分离器、限制器和分析器。

26. 数据库系统对付故障有两种办法：一是尽可能提高系统的可靠性，另一种办法是在系统出故障后把数据库恢复至原来的状态。
27. 网络监听本来是为了管理网络，监视网络的状态和数据流动情况，但是由于它能有效地截获网上的数据，因此也成了网上黑客使用得最多的方法。
28. 若包过滤系统中没有任何一条规则与该包对应，那就将它拒绝，这就是隐含默认“拒绝”原则。
29. 和 Windows NT 基于对象的访问控制不同，Unix 系统的资源访问控制是基于文件的。
30. 通常，简单的防火墙就是位于内部网或 Web 站点与因特网之间的一个路由器或一台计算机，又称为堡垒主机 。
31. 设计和建立堡垒主机的基本原则有两条：最简化原则和预防原则。
32. 恢复技术大致分为: 纯以备份为基础的恢复技术 ，以备份和运行日志为基础的恢复技术和基于多备份的恢复技术等三种。
33. 将一台具有两个以上网络接口的机器配置成在这两个接口间无路由的功能，需进行两个操作：关闭所有可能使该机器成为路由器的程序；关闭 IP 向导。
34. 身份认证是基于 加密 技术的，它的作用就是用来确定用户是否是真实的。
35. 代理服务 是运行在防火墙上的一些特定的应用程序或者服务程序。
36. 包过滤技术依据包的目的地址、源地址和传送协议，允许或禁止包在网络上的传递。
37. 容错是指当系统出现某些指定的硬件或软件错误时，系统仍能执行规定的一组程序，或者说程序不会因系统中的故障而中断或被修改，并且执行结果也不包含系统中故障所引起的差错。
38. 在包过滤系统中，最简单的方法是依据地址进行过滤。
39. 内部网需要防范的三种攻击有：间谍、盗窃和破坏系统。
40. 制订包过滤规则时应注意的两个事项有：联机编辑过滤规则； 要用 IP 地址值，而不用主机名。
41. NTFS 文件系统是一种安全的文件系统，因为它支持文件访问控制，人们可以设置文件和目录的访问权限，控制谁可以使用这个文件，以及如何使用这个文件。
42.摘要算法从给定的文本块中产生一个数字签名，数据签名可以用于防止有人从一个签名上获取文本信息或改变文本信息内容。
43. 除提供机密性外，密码学通常还有其他作用，如 鉴别、完整性、抗抵赖。

l 按病毒存在的媒体分类，病毒分为 文件型 病毒、 引导型 病毒、 混合型 病毒。
2 防火墙的结构通常有三种方案：双宿主主机 结构、 屏蔽主机 结构、 屏蔽子网 结构。
3 报文过滤的弱点可以用 应用层网关 解决。
4 有两种加密体制，分别是 对称加密体制、公钥（非对称）加密体制。
5 安全的一个基本要素分别是：机密性、完整性、可用性、可控性、可审查性。
6 SMTP 的目的是使得 电子邮件 传输可靠和高效。
7 拒绝服务攻击（DOS） 会让系统资源无法正常使用。
8 ActiveX 是 Microsoft 公司开发的用来在 Internet 上分发软件的技术。
9 使 Web 成为交互媒体的两种机制是 表格 和 网关。
10 安全套接层 SSL 的目的在于提高 应用层协议 的安全性。
11 通过对用户和组授权，访问控制表（或 ACL） 允许配置整个门户网站资源的访问权。
12 网络内部威胁有两种情况，一是 蓄意的安全破坏， 一是无意识的操作失误。
13 安全威胁主要可以归结为物理威胁、网络威胁、身份鉴别、编程、系统漏洞等方面。
14 身份认证方式可分以下三类：用 本身特征 进行鉴别、用所知道的事进行鉴别、用用户

拥有的物品进行鉴别。
15 标准 UNIX 系统属于 C1 级。
16 强制性访问控制是基于被访问信息的 敏感性。
17 在因特网上，典型的威胁有 4 种：部件失败、信息浏览、使用错误、入侵。
18 备份操作有 4 种方式：全盘备份、增量备份、差别备份、按需备份。
19 TCP/IP 由四个层次组成：网络接口层、网间网层、传输层、应用层。
20 Windows NT 安全性基于用户 帐户、组、权力和 权限 的概念。
21.PPDR 模型包含四个主要部分：安全策略、防护、、检测、响应。
22.电磁辐射的防护措施有屏蔽、滤波、隔离、接地。
23.明文是作为加密输入的原始信息，即消息的原始形式，通常用 m 或 p 表示。
24.从工作原理角度看，防火墙主要可以分为网络层和应用层。
25.基于检测理论的分类，入侵检测又可以分为异常检测和误用检测。
26.安全威胁分为：人为和非人为。
27.安全威胁是指所有能够对计算机网络信息系统的网络服务和网络信息的机密性、可用性和完整性产生阻碍、破坏或中断的各种因素。
28.防范计算机病毒主要从管理和技术两个方面着手。
29.恶意代码的关键技术：**生存技术**、**攻击技术**和**隐藏技术**。
30.**保护、监测、响应、恢复**涵盖了对现代网络信息系统保护的各个方面，构成了一个完整的体系，使网络信息安全建筑在更坚实的基础之上。

1、P2DR （PPDRPolicy Protection Detection Response）模型是一种常用的计算机网络安全模型，包含 4 个主要组成部分，分别是：（ 安全策略 ）、(防护)、(检测)和(响应)。

PDRR（Protect/Detect/React/Restore）：是保护（Protect）、检测（Detect）、反应（React）、恢复（Restore）

2．网络安全的管理方面主要侧重于防止(**内部人为因素**)的破坏。
3．密码体制从原理上可分为两大类，即单钥密码体制和双秘钥密码体制。
4．在加密系统中，作为输入的原始信息称为明文，加密变换后的结果称为(**密文**)。
5．从系统构成上看，入侵检测系统应包括数据提取、入侵分析、响应处理和远程管理四大部分。
6．黑客攻击的三个阶段是：(收集信息)、探测系统安全弱点和**网路攻击**。
7．(网络监听)本来是为了管理网络，监视网络的状态和数据流动情况，但是由于它能有效地截获网上的数据，因此也成了网上黑客使用得最多的方法。
网络安全涉及的内容既有技术方面的问题，也有(管理)方面的问题。

2、ARP 协议的功能是将(ip 地址)地址转换成(MAC 地址)地址。
3、在 IDS 的报警中，可以分为错误报警和正确的报警两种类型。其中错误报警中，将 IDS 工作于正常状态下产生的报警称为(错报)；而将 IDS 对已知的入侵活动未产生报警的现象称为(漏报)。
4、解决 IP 欺骗技术的最好方法是：（安装过滤路由器）
5、VPN 是利用 Internet 等（公共互联网络）的基础设施，通过（隧道 ）技术，为用户提供一条与专网相同的安全通道。

3、数字签名能够实现对原始报文的 (不可否认性) 和 (鉴别) 。
4、网络信息安全模型中(政策、法律、法规)是安全的基石，它是建立安全管理的标准和方法。

4、构成 VPN 的主要内容有：（PPTP Point to Point Tunneling Protocol：即点对点隧道协议）、（L2TP L2TP 提供包头压缩、隧道验证，而 PPTP 不支持）、（ IPSEC）
6、计算机网络安全领域的 3A 是指认证、授权和(审计) 。

2、常见扫描攻击包括（IP 扫描）和（端口扫描） 。
3、为了网络资源及落实安全政策，需要提供可追究责任的机制，包括：（认证）、 授权和审计 。
4、防火墙应该安装在（内网）和（外网） 之间 。
5、 基于密钥的加密算法通常有两类，即（对称算法）和（ 公用密钥算法）。
6、网络安全面临的主要威胁：（黑客的攻击）、（ 计算机病毒）和（拒绝服务访问攻击）。

1.MD-4 散列算法中输入消息可以任意长度，但要进行分组，其分组的位数是(512)
2.SHA 的含义是(安全散列算法)
3.对身份证明系统的要求之一是(验证者正确识别示证者的概率极大化)
4.阻止非法用户进入系统使用(接入控制技术)
5.以下不是数据库加密方法的是(信息隐藏)

1．简述计算机网络安全的定义
计算机网络安全是指利用管理控制和技术措施，保证在一个网络环境里，信息数据的机密性、完整性及可使用性受到保护。

2.简述物理安全在计算机网络安全中的地位，并说明其包含的主要内容
物理安全是整个计算机网络系统安全的前提，物理安全主要包括：①机房环境安全②通信线路安全③设备安全④电源安全 。

3、防火墙的五个主要功能是什么？防火墙的主要功能：
①过滤进、出网络的数据
②管理进、出网络的访问行为
③封堵某些禁止的业务
④记录通过防火墙的信息和内容
⑤对网络攻击检测和告警

4.基于数据源所处的位置，入侵检测系统可以分为哪 5 类？
答：按数据源所处的位置，把入侵检测系统分为五类：即基于主机、基于网络、混合入侵检测、基于网关的入侵检测系统及文件完整性检查系统。

5.. 什么是计算机网络安全漏洞？
答：计算机网络安全漏洞是在硬件、软件和协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。

6、网络安全的含义是什么？
答：通过各种计算机、网络、密码技术、信息安全技术，保护在公用网络中传输、交换和存储信息的机密性、完整性和真实性，并对信息的传播及内容具有控制能力。

7、网络安全的本质是什么？
答：网络安全的本质就是网络上的信息安全，是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或恶意的原因而遭到破坏、更改或泄漏；系统连续、可靠、正常地运行；网络服务不中断。

8、网络安全主要有哪些关键技术？
答：主机安全技术，身份认证技术，访问控制技术，密码技术，防火墙技术，安全审计技术，安全管理技术。

9、简述信息包筛选的工作原理
答：信息包筛选通常由路由器来实现，它允许某些数据信息包通过而阻止另一些数据包通过；这取决于信息包中的信息是否符合给定的规则，规则由路由器设置。

10、简述计算机系统安全技术的主要内容
答：算机系统安全技术主要有：实体硬件安全技术，软件系统安全技术，数据信息安全技术，网络站点安全技术，运行服务安全技术，病毒防治技术，防火墙技术和计算机应用系统的安全评价。其核心技术是：加密技术、病毒防治和计算机应用系统的安全评价。

11、访问控制的含义是什么？
答：系统访问控制是对进入系统的控制。其主要作用是对需要访问系统及其数据的人进行识别，并检验其身份的合法性。

12、建立口令应遵循哪些规则？
答：1）选择长的口令；2）最好是英文字母和数字的组合；3）不要使用英语单词；4）访问不同的系统使用不同的口令 5）不要使用自己的名字、家人的名字和宠物的名字；6）不要选择不易记忆的口令。

13、什么是计算机病毒？
答：计算机病毒是一种“计算机程序”，它不仅能破坏计算机系统，而且还能够传播和感染到其它系统。它通常隐藏在其它看起来无害的程序中，能生成自身的复制并将其插入到其它的程序中，执行恶意的行动。
14、简述计算机病毒的特点
答：1）刻意编写人为破坏：计算机病毒是人为编写的有意破坏、严禁精巧的程序段。
2）具有自我复制能力：具有再生和传染能力。
3）夺取系统控制权：计算机病毒能够夺取系统控制权，执行自己设计的操作。
4）隐蔽性：病毒程序与正常程序不易区别，代码短小。
5）潜伏性：可长期潜藏在系统中，传染而不破坏，一旦触发将呈现破坏性。
6）不可预见性：病毒代码钱差万别，执行方式也不尽相同。

15、简述数据保密性
答：数据保密性是网络信息不被泄漏给非授权的用户和实体，信息只能以允许的方式供授权用户使用的特性。也就是说，保证只有授权用户才可以访问数据，限制非授权用户对数据的访问。

16、写出五种安全机制
答：加密机制、数字签名机制、访问控制机制、数据完整性机制、鉴别机制、业务填充机制、路由控制机制和公正机制。

17、安全服务有哪些？
答：鉴别、访问控制、数据保密、数据完整性和不可否认性。

18、何为消息认证？
答：使预定消息的接收者能够验证接受的消息是否真实。验证的内容包括证实数据的发送源、数据的内容是否遭到偶然或者恶意的篡改等。

19、简述数字签名过程
答：发送方从报文中生成报文摘要，以自己的专用密钥加密形成数字签名；这个签名作为报文的附件和报文一起发送到接收方；接收方先从接收到的原始报文中算出报文摘要，然后用发送方的公开密钥解密发送方的数字签名，跟自己算出的报文摘要作比较。

20、简述数字签名的性质
答：必须能证实作者签名和签名的时间和日期；必须能对内容进行鉴别；必须能被第三方证实。

21、数据包过滤的安全策略基于哪几种方式？
答：（1）数据包的源地址，（2）数据包的目的地址，（3）数据包的 TCP/UDP 源端口，（4）数据包的 TCP/UDP 目的端口，（5）数据包的标志位，（6）传送数据包的协议。

21、简述包过滤技术。
答：防火墙在网络层中根据数据包的包头信息有选择地允许通过和阻断。依据防火墙内事先设定的规则检查数据流中每个数据包的头部，根据数据包的源地址、目的地址、TCP/UDP 源端口号、TCP/UDP 目的端口号和数据包头中的各种标志位等因素来确定是否允许数据包通过。**其核心是安全策略即过滤规则设计**。

22、计算机病毒的特征是什么
答：1）传染性：病毒通过各种渠道从已被感染的计算机扩散到未被感染的计算机。
2）隐蔽性：病毒一般是具有很高的编程技巧的、短小精悍的一段代码，躲在合法程序当中。很难与正常程序区别开来。
3）潜伏性：病毒进入系统后一般不会马上发作，可以在一段时间内隐藏起来，默默地进行传染扩散而不被发现。一旦触发条件满足就发作。
4）多态性：病毒试图在每次感染时改变形态；使对它的检测变得困难。病毒代码的主要部分相同，但表达方式发生了变化。
5）破坏性：病毒一旦被触发就会发作而产生破坏作用。比如毁坏数据或降低系统性能，甚至破坏硬件。

23、计算机病毒一般由哪几个部分构成，各部分作用是什么？

答：计算机病毒主要由潜伏机制模块、传染机制模块和表现机制模块构成。

1）潜伏机制的功能包括：初始化、隐藏和捕捉；潜伏机制模块随着感染的宿主程序进入内存，初始化其运行环境，使病毒相对独立于其宿主程序，为传染机制做准备。利用各种隐藏方式躲避检测。不停地捕捉感染目标交给传染机制；不停地捕捉触发条件交给表现机制。

2）传染机制的功能包括：判断和感染；传染机制首先通过感染标记判断侯选目标是否已被感染，一旦发现侯选目标没有感染标记，就对其进行感染。

3）表现机制的功能包括：判断和表现；表现机制首先对触发条件进行判断，然后根据不同的触发条件决定什么时候表现，如何表现。

24、DES 算法主要有哪几个步骤？

答：1）将明文按 64 位为单位进行分组；

2）将 64 位明文按照初始置换表进行置换；

3）将置换后的明文分成左右两部分，各 32 位长；

4）进行 16 轮叠代，算法：Li=Ri-1,Ri=Li-1^f(Ri-1,Ki)；

5）逆初始置换；

6）输出。

25、在 DES 算法中，密钥 Ki 的生成主要分几步？

答：1）将 56 位密钥插入第 8，16，24，32，40，48，56，64 位奇偶校验位，然后根据压缩置换表压缩至 56 位；

2）将压缩后的 56 位密钥分成左右两部分，每部分 28 位；根据 i 的值这两部分分别循环左移 1 位或 2 位；3）左右两部分合并，根据压缩置换表选出 48 位子密钥 Ki。

26、说明加密函数 f 的计算过程

答：1）将上一轮的右 32 位按照扩展置换表进行置换，产生 48 位输出；

2）将上一步的 48 位输出与 48 位子密钥进行异或，产生 48 位输出；

3）将上一步的 48 位输出分成 8 组，每组 6 位，分别输入 8 个 S 盒，每个 S 盒产生 4 位输出，共输出 32 位；

4）进行 P 盒置换得到结果。

27. 信息安全的定义是什么？简述信息安全的需求背景，举出信息安全的几个例子。

答：信息安全的定义：“客观上不存在威胁，主观上不存在恐惧”，不受外来的威胁和侵害。信息安全的需求背景是：计算机的广泛应用，计算机网络的迅速发展，特别是因特网的广泛应用。信息安全的例子有：

1. 国家信息体系（银行、军事指挥系统）
2. 国家信息技术安全
3. 电子商务的应用等等。

28. 简述密码学与信息安全的关系。

【答】现在网络上应用的保护信息安全的技术如数据加密技术、数字签名技术、消息认证与身份识别技术、防火墙技术以及反病毒技术等都是以密码学为基础的。电子商务中应用各种支付系统如智能卡也是基于密码学来设计的，可以说密码学是信息安全技术的基础。由此可见现代密码学的应用非常广泛。现在任何企业、单位和个人都可以应用密码学来保护自己的信息安全。

29. 分组密码与流密码的区别是什么?

【答】分组密码与流密码的不同之处在于输出的每一位数字不是只与相应时刻输入的明文数字有关，而是与一组长为 m 的明文数字有关。

30. 什么是变换？

【答】 在信息理论中，把“运动状态和方式”映射为信号的过程称为变换。

31. 安全机制是什么？主要的安全机制有哪些？

【答】根据 ISO 提出的，安全机制是一种技术，一些软件或实施一个或更多安全服务的过程。

ISO 把机制分成特殊的和普遍的。一个特殊的安全机制是在同一时间只对一种安全服务上实施一种技术或软件。加密就是特殊安全机制的一个例子。尽管你可以通过使用加密来保证数据的保密性，数据的完整性和不可否定性，但实施在每种服务时你需要不同的加密技术。一般的安全机制都列出了在同时实施一个或多个安全服务的执行过程。特殊安全机制和一般安全机制不同的另一个要素是一般安全机制不能应用到 OSI 参考模型的任一层上。普通的机制包括：

1) 信任的功能性：指任何加强现有机制的执行过程。例如，当你升级你的 TCP/IP 堆栈或运行一些软件来加强你的 Novell，NT,UNIX 系统认证功能时，你使用的就是普遍的机制。

2)事件检测：检查和报告本地或远程发生的事件

3)审计跟踪：任何机制都允许你监视和记录你网络上的活动

4)安全恢复：对一些事件作出反应，包括对于已知漏洞创建短期和长期的解决方案，还包括对受危害系统的修复。

32. 密码学的五元组是什么？它们分别有什么含义？

【答】密码体系是一个五元组（P,C,K,E,D)满足条件：

（1）P 是可能明文的有限集；（明文空间）

（2）C 是可能密文的有限集；（密文空间）

（3）K 是一切可能密钥构成的有限集；（密钥空间）

（4）任意 k∈ K，有一个加密算法 ek∈E 和相应的解密算法 dk∈D ，使得 ek : P→C 和 dk : C→P 分别为加密解密函数， 满足 dk(ek(x))=x ，这里 x ∈P。

32. 密码分析主要有哪些方式？各有何特点？

【答】密码分析（或称攻击）可分为下列四类：

1） 唯密文分析（攻击），密码分析者取得一个或多个用同一密钥加密的密文；

2） 已知明文分析（攻击），除要破译的密文外，密码分析者还取得一些用同一密钥加密的明密文对；

3） 选择明文分析（攻击），密码分析者可取得他所选择的任何明文所对应的密文（当然不包括他要恢复的明文），这些明密文对和要破译的密文是用同一密钥加密的；

4） 选择密文分析（攻击），密码分析者可取得他所选择的任何密文所对应的明文（要破译的密文除外），这些密文和明文和要破译的密文是用同一解密密钥解密的，它主要应用于公钥密码体制。

33. 什么是单向函数？它在密码学中有什么意义？

【答】不严格地说，一个单向函数是一个函数 ，由 x 计算函数值 y 是容易的，但由 y 计算函数的逆 是困难的（在某种平均意义下），“容易”和“困难”的确切含意由计算复杂性理论定义。单向函数是现代密码学的一个基本工具，大部分安全的密码系统（包括协议）的构造依赖于“单向函数存在”这一假设，所以十分重要。

34. 简述三种数据加密方式？四种传统加密方法？

答：三种数据加密方式：

①链路加密方式。把网络上传输的数据报文的每一位进行加密。目前一般网络通信安全主要采取这种方法。

②节点对节点加密方式。为了解决在节点中的数据是明文的缺点，在中间节点里装有用于加、解密的保护装置即由这个装置来完成一个密钥向另一个密钥的变换。

③端对端加密方式。为了解决链路加密方式和节点对节点加密方式的不足，提出了端对端加密方式，也称为面向协议的加密方式。加密、解密只是在源节点和目的节点进行，是对整个网络系统采用保护措施。端对端加密方式是将来的发展的趋势。

四种传统加密方法：

①代码加密。通信双方预先设定的一组代码，代码可以是日常词汇、专用名词或特定用语，但都有一个预先指定的确切的含义。

②替换加密。如：明文为 student，若密钥为 3 时，密文可为 vwxghqw。

③变位加密。其中又分为：变位加密、列变位加密、矩阵变位加密。

④一次性密码簿加密。

35. 试用形式化描述公钥密码体制。

【答】一个公钥密码体制是这样的一个 5 元组{M,C, ， E ， D }，且满足如下的条件：

1.M 是可能消息的**；

2.C 是可能的密文的**；

3. 密钥空间 是一个可能密钥的有限集；

4．对每一个 ={ ， } K，都对应一个加密算法 E E, E :M C 和解密算法 D D,D :C M,满足对于任意的 m M,都有 c= E （m）,m= D (c)=D (E （m）)=m；

5．对于所有的 K，在已知 E 的情况下推出 D 是计算上不可能的；

36. 试说明识别和身份验证之间的区别。

【答】识别（identification）和身份验证（authentication）是不同的。当说到身份验证时，通常存在一些承载信息的消息在通信双发之间交换，其通信的一方或双方需要被验证。识别（有时称为实体验证）是对一个用户身份的实时验证，它不需要交换承载信息的消息。

37. 怎样的识别协议才是安全的？

【答】一个安全的识别协议至少应该满足以下两个条件：

1） 证明者 A 能向验证者 B 证明他的确是 A；

2） 在证明者 A 向验证者 B 证明他的身份后，验证者 B 没有获得任何有用的信息，B 不能模仿 A 向第三方证明他是 A。

38. 试用形式化描述签名方案。

【答】一个签名方案是一个 5 元组（M,A, K,S,V）,满足如下的条件：

(1) M 是一个可能消息的有限集；

(2) A 是一个可能签名的有限集；
(3)密钥空间 K 是一个可能密钥的有限集；
(4)对每一个 =（ ， ） K，都对应一个签名算法 Sig(S)和验证算法 Ver (V)。每一个 Sig : M A 和 Ver : M A {TRUE ,FALSE}是一个对每一个消息 x M 和每一个签名 y A 满足下列方程的函数：Ver(x,y)=,对每一个 K，函数 Sig 和 Ver 都是为多项式时间可计算的函数。Ver 是一个公开函数,称作公钥；而 Sig 是一个秘密函数， 称作私钥，由用户秘密地保存。

39. 如何将一个识别协议转化为一个签名方案？
【答】有一个标准的方法可将一个识别协议转化为一个签名方案。基本的观点是用一个公开的 Hash 函数来代替验证者 B。

40. 说明交互式用户身份证明协议的性质。
【答】针对一般交互式用户身份证明协议，都必须满足以下三种性质。
（1） 完全性（Completeness）：若用户与验证者双方都是诚实地执行协议，则有非常大的概率（趋近于 1），验证者将接受用户的身份。
（2） 健全性或合理性（Soundness）：若用户根本不知道与用户名字相关的密钥，且验证者是诚实的，则有非常大的概率，验证者将拒绝接受用户的身份。
（3） 隐藏性（Witness hiding）：若用户是诚实的，则不论协议进行了多少次以及不论任何人（包括验证者）都无法从协议中推出用户的密钥，并且无法冒充用户的身份。

41. 试述数字签名和报文摘要的区别。
答：1)数字签名是对整个明文进行加密并产生签名信息，其功能包括鉴别和保密，由于加密很慢，所以速度及费用较高。
2)报文摘要并不是对明文进行加密，而是提供一种鉴别功能，辨别该明文发出人的真实身份。

42.假设在某机构中有 100 个人，如果他们任意两人之间可以进行秘密对话，如果使用保密密钥，则共需要 4950 个密钥，而且每个人应记住 99 个密钥，如果机构人数更多，则保密密钥的分发就产生了问题。目前，哪能种方案可以解决这个问题？请简述其原理。
答：Kerberos 提供了一种解决这个问题的较好方案，它是由 MIT 发明的，使保密密钥的管理和分发变得十分容易。Kerberos 建立了一个安全的、可信任的密钥分发中心（KDC），每个用户只要知道一个和 KDC 进行通信的密钥就可以了，而不需要知道成百上千个不同的密钥。

43. 网络系统备份的主要目的以及网络系统备份体系主要包括哪几方面?
答：网络备份系统的目的是：尽可能快地恢复计算机或者计算机网络系统所需要的数据和系统信息。
网络备份实际上不仅仅是指网络上各计算机的文件备份，它实际上包含了整个网络系统的一套备份体系，主要包括如下几个方面：
a. 文件备份和恢复；
b. 数据库备份和恢复；
c. 系统灾难恢复；
d. 备份任务管理。

44. 简述防火墙的概念和功能。
答：（1）概念：防火墙是在被保护网络和因特网之间执行访问控制策略的一种或一组系统，包括硬件和软件，目的是保护网络不被他人侵扰。

（2）功能：① 强化安全策略，② 记录网上的活动情况，③ 可以防止一个网段的问题向另一个网段传播，④ 安全策略的检查站。

45. 简述防火墙的功能及不足之处。
答：防火墙的基本功能：
（1）防火墙能够强化安全策略
（2）防火墙能有效地记录因特网上的活动
（3）防火墙限制暴露用户点
（4）防火墙是一个安全策略的检查站
防火墙的不足之处：
（1）不能防范恶意的知情者
（2）防火墙不能防范不通过它的连接
（3）防火墙不能防备全部的威胁

46. 网上监听成了网上黑客使用的最多的方法，请简述检测黑客在网上监听的一些简单方法(至少两种)？
①方法一：对于怀疑运行监听程序的机器，用正确的 IP 地址和错误的物理地址去 ping，运行监听的机器会有响应。
②方法二：往网上发大量不存在的物理地址包，由于监听程序将处理这些包，将导致性能下降。通过比较前后该机器性能（icmp echo delay 等方法）加以判断。
③方法三：一个看起来可行的检查监听程序的方法是搜索所有主机运行的进程。
④方法四：去搜索监听程序，入侵者可能使用的是一个免费软件。

47. 简述黑客入侵的过程。
答：过程如下所述：

a. 收集信息：信息收集的目的是为了进入要攻击的目标网络的数据库.黑客会利用公开的协议或者工具（如用 RaceToute 获取到达目标主机所要经过的网络数和路由器数），收集驻留在网络系统中的各个主机系统的相关信息。

b. 系统安全弱点的探测：在收集到攻击目标的一批网络信息之后，黑客会探测网络上的每台主机，以寻求该系统的安全漏洞或者安全弱点，黑客可能使用自编程序或者利用公开的工具（像因特网的电子安全扫描程序 ISS 等）方式自动扫描驻留在联网上的主机。

c. 网络攻击：黑客使用上述方法，收集或者探测到一些“有用”信息之后，就可能会对目标系统实施攻击，如果黑客在某台受损系统上获得了特许权，那么他就可以读取邮件，搜索和盗窃私人文件，毁坏重要数据，从而破坏整个系统的信息，造成不堪设想的后果。

48. 增加代理服务到双重宿主主机，说明代理服务如何工作的？
答：代理服务有两个主要的部件:代理服务器和代理客户.代理服务器运行在双重宿主主机上.代理客户是正常客户程序的特殊版本(即 Telnet 或者 FTP 客户),用户与代理服务器交谈而不是面对远在因特网上的“真正的”服务器。代理服务器评价来自客户的请求，并且决定认可哪一个或否定哪一个。如果一个请求被认可，代理服务器代表客户接触真正的服务器，并且转发从代理客户到真正的服务器的请求，并将服务器的响应传送回代理客户。

49.简述计算机病毒的工作方式和破坏作用。
答：（1）计算机病毒的工作方式：感染引导扇区病毒、文件型病毒、变异、设置触发条件、破坏和高级功能（隐身和多态）病毒。
（2）计算机病毒的破坏作用：攻击系统数据区、文件、内存、CMOS；干扰系统运行；干扰键盘、喇叭、屏幕、打印机等设备；传播网络病毒。

50.过滤路由器与普通路由器的区别？
答：普通路由器只是简单地查看每一个数据包的目标地址，并且选取数据包发往目标地址的最佳路径。
①将数据包发往目标地址
②如不能发往目标地址，则返还数据包，并向源地址发送“不能到达目标地址”的消息
作为过滤路由器，它将更严格地检查数据包，除普通路由器的功能外，还决定数据包是否应该发送。“应该”或“不应该”由站点的安全策略决定，并由过滤路由器强制设置。

51.请解释虚拟企业网络（虚拟专用网络）概念？
答：VPN 可以在防火墙与防火墙或移动的 client 间对所属网络传输的内容加密，建立一个虚拟通道，让两者间在同一个网络上，可以安全且不受拘束地互相存取。

52.根据“可信任计算机标准评价准则”（安全标准“橙皮书”），计算机安全级别标准是如何定义的？并简单说明各安全级别是如何解释评估的？
答：计算机安全级别定义为 7 级。
D 级，为不可信级。如 DOS、Windows 98 等；
C1 级，为选择性安全保护级。描述了典型的用在 Unix 系统上的安全级别。对系统硬件有一定保护作用，用户拥有对文件和目录的访问权，但不能控制进入系统的用户的访问权限；
C2 级，为访问控制级。如 Unix、Windows NT 等；
B1 级，为标志安全保护级。系统安全措施由操作系统决定；
B2 级，为结构保护级。系统中的所有对象有标签，对设备分配 1 个或多个安全级别；
B3 级，安全域级。通过安装硬件来加强域的安全；
A 级，为验证设计级。包括严格的设计、控制和验证过程。

53. 如果您所在的是 C 类网络 202.202.202.0，在内部被保护网络与外部不信任网络之间设置了过滤路由器，以下的表格中列出了服务方向往外的某种服务的包过滤规则，请简述各条规则的含义。
规则 方向 源地址 目标地址 协议 源端口 目标端口 ACK 位 操作
A 外 202.202.202.0 任意 TCP >1023 23 0 或 1 允许
B 内 任意 202.202.202.0 TCP 23 >1023 1 允许
C 双向 任意 任意 任意 任意 任意 0 或 1 拒绝
答：规则 A 允许 Telnet 数据包外出到远程服务器；规则 B 允许相应返回的数据包，但要核对相应的 ACK 位和端口号，这样就可以防止入侵者通过 B 规则来攻击；规则 C 则是个默认的规则，如若数据包不符合 A 或 B，则被拒绝。

54. 如何防止同网段内盗用 IP 地址？并请说明原因。
答：防止盗用 IP 可以绑定 IP 和物理地址。这是因为在一个网段内的网络寻址不是依靠 IP

而是物理地址。IP 只是在网际间寻址使用的。因此在网段的路由器上有 IP 和物理的动态对应表。这是由 ARP 协议来生成并维护的。配置路由器时，可以指定静态的 ARP 表，这样，路由器会根据静态 ARP 表检查数据，如果不能对应，则不进行处理。所以通过设置路由器上的静态 ARP 表，可以防止在本网段盗用 IP。

信息安全考试题库

理论题

单选题（第一部分 200 题）

1、SSL 协议工作在哪一层（B）
（A）应用层
（B）应用层与传输层之间
（C）传输层
（D）传输层与网络层之间

2、下面不属于 SSL 握手层功能的是（B）
（A）验证实体身份
（B）应用层数据实施加解密
（C）协商密钥交换算法
（D）生成及交换密钥

3、一个数据包过滤系统被设计成允许你要求服务的数据包进入，而过滤掉不必要的服务。这属于（A）原则。
（A）最小特权
（B）阻塞点
（C）失效保护状态
（D）防御多样化

4、案例分析（Windows 系统环境）
以 Administrator 用户登录系统，新建 common 用户，默认隶属 Users 用户组；在本地磁盘 C 中新建名为 test 的文件夹，设置其对 common 用户只有读取和执行权限；在 test 目录下新建子文件夹 subtest，设置其对 common 用户只有写权限。以 common 用户登录系统，其对 c:\test\subtest 目录拥有的权限是（C）。
（A）仅写权限
（B）仅读取和执行权限
（C）读取、写和执行权限

（D）Users 组默认权限

5、不属于安全策略所涉及的方面是（D）
（A）物理安全策略
（B）访问控制策略
（C）信息加密策略
（D）防火墙策略

6、Windows 主机推荐使用（C）格式
（A）FAT32
（B）EXT3
（C）NTFS
（D）FAT

7、Linux2.6 内核将系统用户的加密口令存储在（B）文件中
（A）/etc/passwd
（B）/etc/shadow
（C）/etc/group
（D）/etc/hosts

8、按照 TCSEC（由美国国防部提出的可信计算机系统评测标准）标准，Windows Server 2003 系统的安全级别是(D)，未启用 SELinux 保护的 Linux 系统的安全级别是(D)，启用 SELinux 保护的 Linux 系统的安全级别是（B）
（A）A 级
（B）B1 级
（C）B2 级
（D）C2 级

9、使用 shell 命令 umask 重新为文件分配默认权限为 rwxr—r--，umask 的作用代码（A）
（A）033
（B）744
（C）022
（D）722

10、在 Linux FC5 系统环境中，SELinux 配置文件（D）
（A）/etc/sysconfig/selinux/config
（B）/usr/etc/selinux/config
（C）/usr/share/selinux/config
（D）/etc/selinux/config

11、在 HTTP 错误消息中，表示访问被拒绝的代码是（C）
（A）400
（B）401
（C）403
（D）404

12、在 FTP 应答消息中，表示命令正常执行的代码是（A）
（A）200

（B）220
（C）331
（D）500

13、案例分析

运行网络审计工具的主机系统与企业发布信息的 Web、FTP、MySQL 服务器位于同一网段。分析审计日志，发现在某一时间段，网络中有大量包含“GET”负载的数据流入本网段。假设在此时间段，网络中发生了异常的网络行为，则此种异常行为最可能是（B）。

（A）SQL 注入攻击
（B）Web 漏洞扫描
（C）FTP 弱口令扫描
（D）Flood 攻击

14、案例分析

运行网络审计工具的主机系统与企业发布信息的 Web、FTP、MySQL 服务器位于同一网段。分析审计日志，发现在某一时间段，网络中有大量包含“USER”、“PASS”负载的数据流入本网段。假设在此时间段，网络中发生了异常的网络行为，则此种异常行为最可能是（C）。

（A）SQL 注入攻击
（B）Web 漏洞扫描
（C）FTP 弱口令扫描
（D）Flood 攻击

15、下列措施中不能增强 DNS 安全的是（C）
（A）使用最新的 BIND 工具
（B）双反向查找
（C）更改 DNS 的端口号
（D）不要让 HINFO 记录被外界看到

16、为了防御网络监听，最常用的方法是（B）
（A）采用物理传输（非网络）
（B）信息加密
（C）无线网
（D）使用专线传输

17、IPSec 认证报头（AH）不提供的功能（A）
（A）数据机密性
（B）数据源认证
（C）抗重播保护
（D）数据完整性

18、IPSec 传输模式下，针对 IPv4 数据包，AH 不进行验证保护的数据是（C）
（A）原始 IP 头
（B）AH 报头
（C）封装后 IP 头
（D）上层负载数据

19、Windows 2003 SAM 存放在（C）
（A）WINDOWS

（B）WINDOWS\system32
（C）WINDOWS\system32\config
（D）WINDOWS\system

20、TCP 端口全扫描方式，扫描、被扫描端口（开放）间的会话过程（A）
（A）SYN－>SYN+ACK－>ACK－>ACK+FIN
（B）SYN－>SYN+ACK－>RST
（C）SYN－>ACK+RST
（D）SYN－>SYN+ACK－>ACK+FIN

21、TCP 端口半扫描方式，扫描、被扫描端口（开放）间的会话过程（B）
（A）SYN－>SYN+ACK－>ACK－>ACK+FIN
（B）SYN－>SYN+ACK－>RST
（C）SYN－>ACK+RST
（D）SYN－>SYN+ACK－>ACK+FIN

22、TCP 端口半扫描方式，扫描、被扫描端口（关闭）间的会话过程（C）
（A）SYN－>SYN+ACK－>ACK－>ACK+FIN
（B）SYN－>SYN+ACK－>RST
（C）SYN－>ACK+RST
（D）SYN－>SYN+ACK－>ACK+FIN

23、FTP 弱口令扫描时，被扫描主机响应代码 331，表示（D），被扫描主机响应代码 230，表示（B）
（A）用户不存在
（B）扫描成功
（C）口令失败
（D）要求输入用户密码

24、利用 socket 开发基于原始套接字的网络嗅探器时，需创建的 socket 类型是（D）
（A）SOCK_DGRAM
（B）SOCK_STREAM
（C）SOCK_ALL
（D）SOCK_RAW

25、TCP/IP 协议是（A）的，数据包在网络上通常是（D），容易被（B）
（A）开放的
（B）窃听和欺骗
（C）加密传输
（D）明文传输

26、安全漏洞产生的原因很多，其中口令过于简单，很容易被黑客猜中属于（A）
（A）配置管理和使用不当
（B）系统和软件设计存在缺陷
（C）技术实现不充分
（D）通信协议不完备

27、以下（C）方法主要通过查证文件或者对象是否被修改过，从而判断是否遭到入侵

（A）签名分析
（B）统计分析
（C）数据完整性分析
（D）水印分析

28、在一条地址消息的尾部添加一个字符串，而收信人可以根据这个字符串验明发信人的身份，并可进行数据完整性检查，称为（B）
（A）身份验证
（B）数字签名
（C）数据保密
（D）数字证书

29、向程序的缓冲区（堆、栈等）中写入超出其长度的数据是（A）攻击手段
（A）缓冲区溢出
（B）端口扫描
（C）SQL 注入
（D）木马植入

30、不属于黑客被动攻击的是（B）
（A）网页木马
（B）缓冲区溢出
（C）浏览恶意网页
（D）打开病毒附件

31、案例分析
阅读如下 C 代码片段（其中 Y 表示代码指令地址）：

```
Y1：void overflow(char* pShellcode, int iLen)
{
    char buffer[8];
Y2:  memcpy(buffer, pShellcode, dwLen);
Y3:  ……
}
Y4:  int main()
{
Y5:  ……
Y6:  overflow("123456789123456789",18);
Y7:  ……
}
```

main 主程序调用执行 overflow 函数后，指令指针指向（D）
（A）Y3
（B）Y7
（C）0x34353637
（D）0x37363534

32、使网络服务器中充斥着大量要求回复的信息，消耗带宽，导致网络或系统停止正常服务，这属于（D）攻击手段
（A）IP 欺骗
（B）端口扫描
（C）病毒传播

（D）拒绝服务

33、案例分析（Linux 系统环境）

实现 IP 地址：172.16.0.152 与 MAC 地址：00-0c-29-95-b5-e9 绑定的命令是（C）

（A）arp -s 00:0c:29:95:b5:e9 172.16.0.152

（B）arp -s 00-0c-29-95-b5-e9 172.16.0.152

（C）arp -s 172.16.0.152 00:0c:29:95:b5:e9

（D）arp -s 172.16.0.152 00-0c-29-95-b5-e9

34、为防止企业内部人员对网络进行攻击的最有效的手段是（A）

（A）漏洞评估

（B）防火墙

（C）防水墙

（D）安全审计

35、（B）防火墙技术通过检查网络应用程序信息，来判断传输层 TCP 的端口是否需要临时打开，且当传输结束时，TCP 端口马上恢复为关闭状态，它从 TCP 连接的建立到终止全过程跟踪检测。

（A）包过滤

（B）状态检测

（C）NAT

（D）以上都是

36、设置 iptables 防火墙策略，默认禁止与本地进程进行通信，以下语法正确的是（D）

（A）iptables -t filter -I INPUT ACCEPT

（B）iptables -t filter -A INPUT ACCEPT

（C）iptables -t nat -A INPUT ACCEPT

（D）iptables -P INPUT DROP

37、最大的优点是对用户透明，并且隐藏真实 IP 地址，同时解决合法 IP 地址不够用的问题。这种防火墙技术称为（C）

（A）包过滤技术

（B）状态检测技术

（C）NAT 技术

（D）应用代理技术

38、下面关于入侵检测（IDS）系统的说法，错误的是（D）

（A）假如说防火墙是一幢大楼的门锁，那么 IDS 就是这幢大楼里的监视系统

（B）IDS 只能够检测并发现异常，并不能阻止异常

（C）IDS 报警存在误报和漏报问题

（D）IDS 必须通过监控网络行为才能够发现异常行为

39、Snort 是（B）系统

（A）基于主机的入侵检测系统

（B）基于网络的入侵检测系统

（C）基于网络的明文嗅探系统

（D）基于网络的安全审计系统

40、可用于网络入侵检测系统开发的工具包是（A）
（A）libnids
（B）libdnet
（C）libnet
（D）libpcap

41、在公共网络中建立专用网络，数据通过安全的“加密管道”在公共网络中传播的技术是（C）
（A）P2P
（B）PKI
（C）VPN
（D）AAA

42、下列不是隧道协议的是（A）
（A）PPP
（B）PPTP
（C）L2TP
（D）IPSec

43、（D）属于第三层隧道协议
（A）PPP
（B）PPTP
（C）L2TP
（D）IPSec

44、（B）属于第二层隧道协议
（A）PPP
（B）PPTP
（C）GRE
（D）IPSec

45、除建立 VPN 隧道外，还可对内部协议、私有地址进行封装的隧道协议是（D）
（A）PPTP
（B）L2TP
（C）IPSec
（D）GRE

46、PPTP 数据隧道化过程采用了多层封装方法，其中实现对原始数据（IP 数据报、IPX 数据报等）加密、压缩的封装报头是（D）
（A）数据链路层报头
（B）IP 报头
（C）GRE 报头
（D）PPP 报头

47、（C）协议试图通过对 IP 数据包进行加密，从根本上解决 Internet 的案例问题。同时又是远程访问 VPN 网的基础，可以在 Internet 上创建出案例通道来。
（A）安全套接层协议（SSL）
（B）传输层安全协议（TLS）

（C）IP 安全协议（IPSec）
（D）公钥基础设施（PKI）

48、关于 OpenVPN 下列说法正确的是（A）
（A）主要特征包括跨平台的可移植性、支持动态 IP 地址及 NAT
（B）可以使用 Web 浏览器作为 OpenVPN 客户端
（C）它只能对特定服务的应用层数据流形成“隧道”
（D）它与 PPTP、L2TP 或 IPSec 相兼容

49、追踪黑客踪迹、分析黑客攻击手段的最佳方案是（A）
（A）蜜罐/蜜网
（B）入侵检测系统
（C）安全审计系统
（D）反木马、反病毒软件

50、蜜罐的核心价值体现在（B）
（A）它的防御手段
（B）对异常活动进行监视、检测和分析
（C）形态多样性
（D）易部署

51、蜜罐的劣势在于（D）
（A）容易遭受攻击
（B）部署位置受到严格限制
（C）不限于解决某个具体问题
（D）对非自动化攻击无能为力

52、下列哪项不属于 Windows 自启动机制（D）
（A）自启动文件和文件夹
（B）注册表 Run 设置
（C）注册表系统服务
（D）系统环境变量

53、下列哪项不是“灰鸽子”木马具有的功能（B）
（A）文件管理
（B）感染局域网内其它主机
（C）Telnet
（D）捕获屏幕

54、下列哪项是“灰鸽子”木马的运行进程（C）
（A）svchost.exe
（B）winlogon.exe
（C）IEXPLORE.exe
（D）WINLOGON.exe

55、反弹型木马与传统的木马有何区别（A）
（A）更容易突破防火墙的过滤
（B）响应时间短，执行效率更高

（C）不容易被杀毒软件查杀
（D）不产生服务端口

56、哪一项不是文件型病毒的特点（C）
（A）寄生文件中，依托文件的执行动作而修改 DOS 的中断向量，并常驻内存
（B）在潜伏期内，感染可感染文件，使之成为被感染的对象，直至发作
（C）不能独立运行，需要它的宿主程序的运行来激活它
（D）根据激活条件，选择发作时间

57、下列叙述不正确的是（C）
（A）JavaScript 是面向对象的语言，对象在程序中占有重要地位
（B）对象是具有共同特征的集合体，由属性和方法两种基本元素组成
（C）JavaScript 语言需要编译才能运行
（D）JavaScript 是客户端脚本语言

58、计算机蠕虫的一般攻击方式是（B）
（A）扫描→复制→攻击
（B）扫描→攻击→复制
（C）复制→扫描→攻击
（D）复制→攻击→扫描

59、作为低交互度的蜜罐，BOF 实现了对（A）进行模拟仿真
（A）应用服务
（B）主机系统
（C）网络拓扑
（D）以上都不是

60、关于 Honeyd 下列说法正确的是（D）
（A）Honeyd 是一种虚拟蜜罐工具
（B）Honeyd 可以模拟服务、监听端口
（C）Honeyd 可以仿真主机与网络
（D）以上都对

61、作为低交互度的蜜罐，Honeyd 能够仿真（C）
（A）Honeyd 所有主机系统
（B）已存在的主机系统
（C）不存在的主机系统
（D）所有主机系统

62、下列不属于 Honeyd 配置语法的是（D）
（A）create
（B）set
（C）add
（D）run

63、DES 算法的明文分组、密文分组、密钥分组的位数分别是（A）
（A）64 位、64 位、64 位
（B）64 位、32 位、64 位

（C）32 位、64 位、32 位
（D）128 位、64 位、128 位

64、AES 算法中每个 S 盒的输入、输出个数分别是（B）
（A）8、6
（B）8、8
（C）6、6
（D）6、8

65、DES 算法的每一个密钥分组分别经过如下几个过程，产生出 16 个子密钥，供各次加密迭代使用，这几个过程按照先后顺序分别是（C）
（A）子置换选择 2、循环左移、置换选择 1
（B）循环左移、子置换选择 1、置换选择 2
（C）子置换选择 1、循环左移、置换选择 2
（D）循环左移、置换选择 2、子置换选择 1

66、SHA1 算法对输入按照一定的输入位数进行分组，并以分组为单位进行处理，该输入位数是（D）
（A）64 位
（B）128 位
（C）256 位
（D）512 位

67、对于 RSA 的数字签名，加密和签名的顺序如何才能保护安全性（B）
（A）先签名后加密
（B）先加密后签名
（C）安全性与加密、签名的先后顺序无关

68、AES 算法中对于每个明文分组的加密过程按照如下顺序进行（A）
（A）将明文分组放入状态矩阵中、AddRoundKey 变换、10 轮循环运算
（B）AddRoundKey 变换、将明文分组放入状态矩阵中、10 轮循环运算
（C）10 轮循环运算、AddRoundKey 变换、将明文分组放入状态矩阵中
（D）AddRoundKey 变换、10 轮循环运算、将明文分组放入状态矩阵中

69、DES 算法中对于每个明文分组的加密过程按照如下顺序进行（C）
（A）16 轮循环运算、初始置换、终结置换
（B）初始置换、终结置换、16 轮循环运算
（C）初始置换、16 轮循环运算、终结运算
（D）16 轮循环运算、终结置换、初始置换

70、按密钥的使用方法划分，下列属于序列密码的是（C）
（A）DES
（B）AES
（C）RC4
（D）RSA

71、按密钥加密体制分类，下列属于公开密钥密码（非对称密钥加密机制）的是（D）
（A）DES

（B）AES
（C）RC4
（D）RSA

72、下列哪一个密码学算法可以用来验证文件的完整性（B）
（A）DES
（B）MD5
（C）RSA
（D）ECC

73、下列哪一个密码学算法可用于数字签名（C）
（A）Kaiser
（B）AES
（C）RSA
（D）SHA1

74、关于密码学下列说法错误的是（A）
（A）密码的安全不仅依赖密钥的保密，而且还依赖算法的保密
（B）理论上绝对安全的密码是存在的，即一次一密
（C）理论上，任何实用的密码都是可破的
（D）所谓计算机上的安全，就是使用可利用的计算资源不能破译

75、关于 DES 加密算法下列说法错误的是（B）
（A）明文、密文和密钥的分组长度都是 64 位
（B）加密与解密算法不同
（C）能够加解密任何形式的计算机数据
（D）对称密钥加密算法

76、关于 AES 加密算法下列说法错误的是（C）
（A）明文长度 128 位，密文长度、密钥长度可变
（B）能够加密任何形式的计算机数据
（C）加密与解密算法相同
（D）非对称密钥加密算法

77、关于非对称密钥加密算法下列说法错误的是（B）
（A）多数算法都是基于某个数学难题的
（B）加密效率优于对称密钥加密算法
（C）收发双方持有不同的密钥
（D）即可实现加密，也可实现数字签名

78、关于对称密钥加密算法下列说法错误的是（D）
（A）算法可以被证明是安全的
（B）算法综合运用了置换、代替、代数等多种密码技术
（C）加密效率优于非对称密钥加密算法
（D）即可实现加密，也可实现数字签名

79、在 Windows Server 2003 系统里，具有容错能力的卷集是（D）
（A）简单卷、跨区卷

（B）镜像卷、带区卷
（C）跨区卷、RAID-5 卷
（D）镜像卷、RAID-5 卷

80、Linux 操作系统下实现 RAID1、RAID5 和 RAID 0+5 最少分别需要几块硬盘（D）
（A）2 块、3 块、5 块
（B）3 块、3 块、9 块
（C）3 块、3 块、6 块
（D）2 块、3 块、6 块

81、为了确保通信安全，在正式传送报文之前，应首先认证通信是否在意定的站点之间进行，这一过程称为（A）
（A）站点认证
（B）报文认证
（C）身份认证
（D）数字签名

82、（B）必须使通信方能够验证每份报文的发送方、接收方、内容和时间性的真实性和完整性
（A）站点认证
（B）报文认证
（C）身份认证
（D）数字签名

83、（C）是程序的秘密入口点，它使得知情者可以绕开正常的安全访问机制而直接访问程序
（A）逻辑炸弹
（B）特洛伊木马
（C）后门
（D）僵尸

84、病毒将与其自身完全相同的副本植入其他程序或磁盘的某些系统区域，是属于病毒生命周期中的（B）阶段
（A）睡眠
（B）传播
（C）触发
（D）执行

85、（A）病毒感染主引导记录（MBR）或者其他引导记录，当系统从包含这种病毒的磁盘启动时，病毒将传播开来
（A）引导区病毒
（B）文件型病毒
（C）蠕虫病毒
（D）宏病毒

86、（C）病毒可以自行复制，并通过网络连接将病毒副本从一台计算机发送到其他计算机中
（A）引导区病毒
（B）文件型病毒
（C）蠕虫病毒

（D）宏病毒

87、将一份需要保密的信息隐藏到另外一个可以公开的媒体之中的技术是（C）
（A）信息签名
（B）信息捆绑
（C）信息隐藏
（D）信息封装

88、用信号处理的方法在数字化的多媒体数据中嵌入隐藏的标记的技术是（B）
（A）数字签名
（B）数字水印
（C）数字认证
（D）数字加密

89、在 Linux FC5 系统中，更改/opt/target 文件访问权限为所有者可读、写、执行，属组可读、执行，其它人仅允许读。执行命令（C）
（A）chmod u+r+w+x g+r+x o+r /opt/target
（B）chmod a+r u+w+x g+x /opt/target
（C）chmod 754 /opt/target
（D）chmod 023 /opt/target

90、在 Linux FC5 系统中,更改/opt/target/目录及其下全部子目录和文件的所有者为 tom，属组为 apache。执行命令（B）
（A）chgrp tom -R /opt/target
    chown apache -R /opt/target
（B）chown tom:apache -R /opt/target
（C）chgrp tom:apache -R /opt/target

（D）chmod tom:apache -R /opt/target

91、网络安全中“安全”的含义（B）
（A）security（安全）
（B）security（安全）和 safety（可靠）
（C）safety（可靠）
（D）risk（风险）

92、网络安全中“安全”的含义（B）
（A）security（安全）
（B）security（安全）和 safety（可靠）
（C）safety（可靠）
（D）risk（风险）

93、数字签名是使用（A）
（A）自己的私钥签名
（B）自己的公钥签名
（C）对方的私钥签名
（D）对方的公钥签名

94、PKI 基于以下哪种方式保证网络通讯安全（A）
（A）公开密钥加密算法
（B）对称加密算法
（C）加密设备
（D）其它

95、下列对子网系统的防火墙的描述错误的是（D）
（A）控制对系统的访问
（B）集中的安全管理
（C）增强的保密性
（D）防止内部和外部的威胁

96、特洛伊木马攻击的威胁类型属于（B）
（A）授权侵犯威胁
（B）植入威胁
（C）渗入威胁
（D）旁路控制威胁

97、如果发送方使用的加密密钥和接收方使用的解密密钥不相同，从其中一个密钥难以推出另一个密钥，这样的系统称为（C）
（A）常规加密系统
（B）单密钥加密系统
（C）公钥加密系统
（D）对称加密系统

98、用户 A 通过计算机网络向用户 B 发消息，表示自己同意签订某个合同，随后用户 A 反悔，不承认自己发过该条消息。为了防止这种情况，应采用（A）
（A）数字签名技术
（B）消息认证技术
（C）数据加密技术
（D）身份认证技术

99、通过发送大量的欺骗性包，每个包可能被几百个主机接收到，成倍的响应涌到目标系统，占据系统所有的资源。这种攻击属于以下哪种拒绝服务攻击（D）
（A）SYN flood
（B）Teardrop
（C）IP 地址欺骗
（D）Smurf

100、在大多数情况下，病毒入侵计算机系统以后（D）
（A）病毒程序将立即破坏整个计算机软件系统
（B）计算机系统将立即不能执行我们的各项任务
（C）文件操作有异常
（D）一般并不立即发作，等到满足某种条件的时候，才会出来活动捣乱、破坏

101、网络信息探测中第一步要做的是什么工作（A）
（A）扫描
（B）Ping

（C）隐藏自己
（D）溢出

102、1TLGHx5co$vq6xMOWG1hYfIV1AZEWgD.此值是什么系统的密码加密值（B）
（A）windows
（B）linux
（C）unix
（D）Aix

103、下面哪个是流行的加壳鉴别工具（B）
（A）superscan
（B）peid
（C）upxshell
（D）Armadillo

104、下面哪种不是壳对程序代码的保护方法（D）
（A）加密
（B）指令加花
（C）反跟踪代码
（D）限制启动次数

105、请根据下面的 shellcode 代码，选择 number 正确的值完善 shellcode 代码（）

```
/* shellcode.c */
#include <windows.h>
#include <winbase.h>
Char shellcode[]={
0x8b,0xe5 /* mov esp,ebp */
0x55, /* push ebp */
0x8b,0xec, /* mov ebp,esp */
0x83,0xec,0x0c, /* sub esp,0000000c */
0xb8,0x63,0x6f,0x6d,0x6d /* move ax,6d6d6f63 */
……..略
};
int main（）
{
    int *ret;
    LoadLibrary（“msvcrt,dll”）;
    ret = （int *）&ret + number;
     （*ret） = （int）shellcode
}
```

（A）1
（B）2
（C）3
（D）4

106、增加主机抵抗 DoS 攻击能力的方法之一是（）
（A）缩短 SYN Timeout 时间
（B）调整 TCP 窗口大小
（C）增加 SYN Timeout 时间
（D）IP-MAC 绑定

107、Linux 系统日志文件通常是存放在（A）
（A）/var/log
（B）/usr/adm
（C）/etc/
（D）/var/run

108、下面选项中关于交换机安全配置方法正确的是（）
（A）在 MAC/CAM 攻击方式中，可采用增大 CAM 表来防止 MAC 被填满。
（B）防止交换机 ARP 欺骗可以采取打开 snooping binding 来防止。
（C）当交换机打开了 SNMP 后，只需将 SNMP 置为只读就能防止 SNMP Snarf 攻击。
（D）对于 IP/MAC 欺骗对交换机进行攻击，需要对交换机进行 port security 配置。

109、用一个特别打造的 SYN 数据包，它的原地址和目标地址都被设置成某一个服务器地址。这样将导致接收服务器向他自己的地址发送 SYN-ACK 信息，结果这个地址又发回 ACK 信息并创建一个空连接，被攻击的服务器每接收到一个这样的连接就将其保存，直到超时，这种拒绝服务攻击是下列中的（）
（A）SYN Flooding 攻击
（B）Teardrop 攻击
（C）UDP Storm 攻击
（D）Land 攻击

110、下列方法中不能用来进行 DNS 欺骗的是（）
（A）缓存感染
（B）DNS 信息劫持
（C）DNS 重定向
（D）路由重定向

111、某网站管理后台验证文件内容如下，则在不知道管理员用户名与密码的情况下，如何进入管理后台（）

```
adminname=Request.form("username")
password=Request.Form("password")
set rs=server.createobject("adodb.recordset")
sql="select * from tbl_administrators where strID='"&adminname&"' and strPwd='"&password&"'"
rs.open sql,conn,1,1
if not rs.eof then
    session("hadmin")="uestcjccadmin"
    response.redirect "admin_index.asp"
else
    response.redirect "admin_login.asp?err=1"
end if
```

（A）用户名：admin 密码 admin：
（B）用户名：’ or ‘1’=’1 密码：’ or ‘1’=’1
（C）用户名：adminname 密码：password
（D）用户名：admin 密码’ or ‘1’=’1

112、属于被动攻击的恶意网络行为是（）
（A）缓冲区溢出
（B）网络监听

（C）端口扫描
（D）IP 欺骗

113、保障信息安全最基本、最核心的技术是（）
（A）信息加密技术
（B）信息确认技术
（C）网络控制技术
（D）反病毒技术

114、当你感觉到你的 Win2000 运行速度明显减慢，当你打开任务管理器后发现 CPU 的使用率达到了百分之百，你最有可能认为你受到了哪一种攻击（）
（A）特洛伊木马
（B）拒绝服务
（C）欺骗
（D）中间人攻击

115、向有限的空间输入超长的字符串是哪一种攻击手段？（）
（A）缓冲区溢出
（B）网络监听
（C）拒绝服务
（D）IP 欺骗

116、下列关于网络嗅探技术说明错误的是（）
（A）嗅探技术对于已加密的数据无能为力
（B）将网卡设为混杂模式来进行嗅探对于使用交换机且进行了端口和 MAC 绑定的局域网无能为力
（C）将网卡设为混杂模式可以对任意局域网内的数据包进行窃听
（D）可以通过配置交换机端口镜像来实现对镜像端口的数据包进行窃听

117、下列关于主机扫描说法正确的是（）
（A）主机扫描只适用于局域网内部
（B）主机扫描必须在对被扫描主机取得完全控制权以后才能进行
（C）如果被扫描主机没有回应，则说明其不存在或不在线
（D）主机扫描本质上仍然是通过对相应主机的端口进行扫描，根据其回复来判断相应主机的在线情况

118、下列关于口令破解，说法错误的是（）
（A）字典攻击本质上仍然是一种穷举攻击，其通过对字典中的条目进行逐一尝试其是否是正确口令
（B）在设置口令时，包含电话号码、生日等个人信息对于口令安全没有影响
（C）将口令设置得位数多一些增加了破解难度，有利于口令安全
（D）在口令设置时尽可能包括数字、大小写英文字母以及特殊字符有助于提高口令的安全性

119、下列关于网页恶意代码叙述错误的是（）
（A）网页恶意代码通常使用 80 端口进行通信，所以一般来讲防火墙无法阻止其攻击
（B）网页恶意代码一般由 JavaScript、VBScript 等脚本所编写，所以可以通过在浏览器中禁止执行脚本来对其进行防范

（C）网页恶意代码仅能对通过网络传输的用户信息进行窃取，而无法操作主机上的各类用户资源
（D）网页恶意代码与普通可执行程序的重要区别在于，其实解释执行的而不需要进行编译

120、下列关于加壳与脱壳说法正确的是（）

（A）对于执行加了壳的应用程序，首先运行的实际上是壳程序，然后才是用户所执行的应用程序本身
（B）由于加壳的原因，加壳后程序所占的存储空间将会比原程序大上好几倍
（C）加过壳的程序无法直接运行，必须要先进行脱壳才能运行
（D）对于加过壳的程序，可以对其进行反编译，得到其源代码进行分析，并进行脱壳>>

121、下列关于 ARP 协议及 ARP 欺骗说法错误的是（）
（A）通过重建 ARP 表可以一劳永逸的解决 ARP 欺骗
（B）ARP 欺骗的一种方式是欺骗路由器或交换机等网络设备，使得路由器或交换机等网络设备将数据包发往错误的地址，造成被攻击主机无法正确接收数据包。
（C）除了攻击网络设备外，还可以伪造网关，使本应发往路由器或交换机的数据包发送到伪造的网关，造成被攻击主机无法上网。
（D）ARP 协议的作用是实现 IP 地址与物理地址之间的转换

122、下列关于拒绝服务攻击说法错误的是（）
（A）带宽消耗是拒绝服务攻击的一种样式
（B）反射式拒绝服务攻击是攻击方直接向被攻击方发送封包
（C）拒绝服务攻击的目的之一是使合法用户无法正常访问资源
（D）分布式拒绝服务攻击是同时利用大量的终端向目标主机发动攻击

123、下列有关 Windows 日志说明错误的是（）
（A）可以通过管理工具中的事件查看器查看各类日志
（B）Windows 的日志包含了安全日志、系统日志、应用程序日志等多种日志
（C）为了保证安全日志、系统日志、应用程序日志三类 Windows 自带的系统日志文件的安全，其全部经过加密再存放在相应的文件夹中
（D）可以自行设定相应的审核规则（如：文件访问），系统将会把符合规则的行为写入日志文件

124、下列关于 Linux 操作系统说明错误的是（）
（A）在 Linux 中，password 文件中并未保存用户密码，而是将加密后的用户密码保存在 shadow 文件中
（B）在 Linux 中，如果两个用户所设置的密码相同，则其在密码的密文也相同
（C）在 Linux 中，文件或文件夹的属性中保存了文件拥有者、所属的用户组及其它用户对其的访问权限
（D）Linux 与 Windows 的访问控制一样，都通过将合法用户划分为不同的用户组，并明确其可以访问的资源

125、下面不属于漏洞分析步骤的是（）
（A）shellcode 定位
（B）shellcode 功能分析
（C）漏洞触发原因分析

（D） 汇编代码编写

126、下列不是内核调试器的是哪一个（）
（A）WinDBG
（B）Syser Debugger
（C）OllyDBG
（D）SoftICE

127、对 PE 结构中节头（Image_Section_Table）的节标志（Characteristics），下列说法有误的一项（）
（A）0x20000000，说明该节可执行
（B）0x40000000，说明该节可写
（C）0xC0000000，说明该节可读、可写
（D）0xE0000000，说明该节可读、可写、可执行

128、下面那种方法不属于对恶意程序的动态分析（）
（A）文件校验,杀软查杀
（B）网络监听和捕获
（C）基于注册表，进程线程，替罪羊文件的监控
（D）代码仿真和调试

129、扫描工具（）
（A）只能作为攻击工具
（B）只能作为防范工具
（C）既可作为攻击工具也可以作为防范工具
（D）既不能作为攻击工具也不能作为防范工具

130、可信计算机系统评估准则(Trusted Computer System Evaluation Criteria，FCSEC)共分为（）大类（）级。
（A）4 7
（B）3 7
（C）4 5
（D）4 6

131、（）是采用综合的网络技术设置在被保护网络和外部网络之间的一道屏障，用以分隔被保护网络与外部网络系统防止发生不可预测的、潜在破坏性的侵入，它是不同网络或网络安全域之间信息的唯一出入口。
（A）防火墙技术
（B）密码技术
（C）访问控制技术
（D）VPN

132、网络监听是怎么回事？（）
（A）远程观察一个用户的电脑
（B）监视网络的状态、数据流动情况
（C）监视 PC 系统运行情况
（D）监视一个网站的发展方向

133、监听的可能性比较低的是（）数据链路
（A）Ethernet
（B）电话线
（C）有线电视频道
（D）无线电

134、下面那个命令可以显示本机的路由信息（）
（A）Ping
（B）Ipconfig
（C）Tracert
（D）Netstat

135、计算机病毒的核心是（）
（A）引导模块
（B）传染模块
（C）表现模块
（D）发作模块

136、Code Red 爆发于 2001 年 7 月，利用微软的 IIS 漏洞在 Web 服务器之间传播。针对这一漏洞，微软早在 2001 年三月就发布了相关的补丁。如果今天服务器仍然感染 Code Red，那么属于哪个阶段的问题?（）
（A）系统管理员维护阶段的失误
（B）微软公司软件的设计阶段的失误
（C）最终用户使用阶段的失误
（D）微软公司软件的实现阶段的失误

137、Windows NT 和 Windows 2000 系统能设置为在几次无效登录后锁定帐号,这可以防止（）
（A）木马
（B）暴力攻击
（C）IP 欺骗
（D）缓存溢出攻击

138、不会在堆栈中保存的数据是（）
（A）字符串常量
（B）函数的参数
（C）函数的返回地址
（D）函数的局部变量

139、下列说法有误的是（）
（A）WinDBG 调试器用到的符号文件为“*.pdb”
（B）OllyDBG 调试器可以导入“*.map”符号文件
（C）手动脱壳时，使用“Import REC”工具的目的是为了去找 OEP
（D）PEiD 检测到的关于壳的信息有些是不可信的

140、在下面的调试工具中，用于静态分析的是（）
（A）windbg
（B）Softice
（C）IDA

（D）Ollydbg

141、下列关于路由器叙述错误的是（）
（A）可以通过对用户接入进行控制，来限制对路由器的访问，从而加强路由器的安全
（B）不合法的路由更新这种欺骗方式对于路由器没有威胁
（C）路由器也有自己的操作系统，所以定期对其操作系统进行更新，堵住漏洞是非常重要的
（D）可以通过禁用路由器上不必要的服务来减少安全隐患，提高安全性

142、下列有关防火墙叙述正确的是（）
（A）包过滤防火墙仅根据包头信息来对数据包进行处理，并不负责对数据包内容进行检查
（B）防火墙也可以防范来自内部网络的安全威胁
（C）防火墙与入侵检测系统的区别在于防火墙对包头信息进行检测，而入侵检测系统则对载荷内容进行检测
（D）防火墙只能够部署在路由器等网络设备上

143、在利用 Serv-U 提升权限中，默认的端口和用户名为（）
（A）43958 LocalAdministrator
（B）43959 LocalAdministrator
（C）43958 Administrator
（D）43959 Administrator

144、Windows NT/2000 SAM 存放在（）
（A）WINNT
（B）WINNT/SYSTEM32
（C）WINNT/SYSTEM
（D）WINNT/SYSTEM32/config

145、下列哪个是加壳程序（）
（A）resfixer
（B）exeScope
（C）aspack
（D）7z

146、NT 系统的安全日志如何设置（）
（A）事件查看器
（B）服务管理器
（C）本地安全策略
（D）网络适配器里

147、在 IA32 的架构下，程序缓冲区溢出的原理是（）
（A）程序对缓冲区长度没有进行检查
（B）定义缓冲区长度太小
（C）内存分配出错了
（D）函数调用地址在缓冲区的上方

148、5EE56782EDE1F88747A7C68C75A91BFC:A12C6863303D3F0296338E6B40628643 此 hash 值由哪两部分组成（）

（A）NT hash+LM hash
（B）Md5 hash+Lm hash
（C）Md5 hash+NT hash
（D）Md4 hash+Md5 hash

149、以下不属于非对称加密算法的是（）
（A）DES
（B）AES
（C）RSA
（D）DEA

150、你有一个共享文件夹，你将它的 NTFS 权限设置为 sam 用户可以修改，共享权限设置为 sam 用户可以读取，当 sam 从网络访问这个共享文件夹的时候，他有什么样的权限？（）
（A）读取
（B）写入
（C）修改
（D）完全控制

151、在对目标进行安全漏洞探测时，主要采用哪个手段（A）
（A）工具扫描
（B）人工判断
（C）端口判断
（D）命令查看

152、\x32\x2E\x68\x74\x6D 此加密是几进制加密（D）
（A）十进制
（B）二进制
（C）八进制
（D）十六进制

153、PE 文件格式的开头两个字符是（D）
（A）EX
（B）PE
（C）MS
（D）MZ

154、手动脱压缩壳一般是用下列方法（C）
（A）使用 upx 脱壳
（B）使用 fi 扫描后，用 unaspack 脱壳
（C）确定加壳类型后，ollyice 调试脱壳
（D）D.使用 winhex 工具脱壳

155、请根据下面的 shellcode 代码，选择 number 正确的值完善 shellcode 代码（B）

```
/* shellcode.c */
#include <windows.h>
#include <winbase.h>
Char shellcode[]={
0x8b,0xe5 /* mov esp,ebp */
0x55, /* push ebp */
0x8b,0xec, /* mov ebp,esp */
0x83,0xec,0x0c, /* sub esp,0000000c */
0xb8,0x63,0x6f,0x6d,0x6d /* move ax,6d6d6f63 */
……..略
};
int main（）
{
    int *ret;
    LoadLibrary（“msvcrt,dll”）;
    ret = （int *）&ret + number;
     （*ret） = （int）shellcode
}
```

（A）1
（B）2
（C）3
（D）4

156、下面哪项不是防范 ARP 攻击的有效方法（C）
（A）IP-MAC 静态绑定
（B）使用类似 port security 的功能
（C）加强用户权限控制
（D）DHCP Snooping+DAI 技术

157、DNS 欺骗的核心是伪造什么（D）
（A）TCP 序列号
（B）端口号
（C）MAC 地址
（D）DNS 标识 ID

158、IP 欺骗的核心是获得（B）
（A）DNS 标识 ID
（B）TCP 序号
（C）端口号
（D）TCP payload

159、不属于 Dos 攻击的是（C）
（A）SYN FLOOD
（B）Ping FLOOD
（C）TCP session hijacking
（D）Teardrop

160、下面哪项不是 SYN 攻击保护方法（D）
（A）safereset
（B）syn cookie/syn proxy

（C）syn 重传
（D）ICMP Filter

161、windows 2003 中系统日志默认存放目录 users 组用户的权限为（B）
（A）读取和运行
（B）列出文件夹目录
（C）修改
（D）特别的权限

162、下面的选项中关于路由器攻击及防范的描述错误的是（B）
（A）cisco 启用了 PMTUD 会导致 ICMP Dos 攻击，防范措施可以禁用 PMTUD 或者更新补丁。
（B）cisco 路由器需要对外部打开了至少一种管理方式（telnet、ssh、http）用于远程管理，当路由器被 Dos 字典攻击时，可以采取更新补丁方式增强路由器的抗 Dos 能力来进行防范。
（C）对于 STUN（串行隧道）攻击可以采用严格控制 CON 口的访问来防范。
（D）当路由器受到 ARP 攻击时，可以采取 IP/MAC 绑定的方法进行防范。

163、（A）是采用综合的网络技术设置在被保护网络和外部网络之间的一道屏障，用以分隔被保护网络与外部网络系统防止发生不可预测的、潜在破坏性的侵入，它是不同网络或网络安全域之间信息的唯一出入口。
（A）防火墙技术
（B）密码技术
（C）访问控制技术
（D）VPN

164、以下关于计算机病毒的描述中，只有（ A）是对的。
（A）计算机病毒是一段可执行程序，一般不单独存在
（B）计算机病毒除了感染计算机系统外，还会传染给操作者
（C）良性计算机病毒就是不会使操作者感染的病毒
（D）研制计算机病毒虽然不违法，但我们也不提倡

165、防火墙中地址翻译的主要作用是（B）
（A）提供代理服务
（B）隐藏内部网络地址
（C）进行入侵检测
（D）防止病毒入侵

166、以下关于 Smurf 攻击的描述，那句话是错误的？（A）
（A）攻击者最终的目标是在目标计算机上获得一个帐号
（B）它使用 ICMP 的包进行攻击
（C）它依靠大量有安全漏洞的网络作为放大器
（D）它是一种拒绝服务形式的攻击

167、“[Microsoft][ODBC SQL Server Driver][SQL Server]将 nvarchar 值 ’XX’ 转换为数据类型为 int 的列时发生语法错误。”这句是由以下那句命令造成的（A）
（A）and user>0
（B）And (Select count(*) from XXX)<>0
（C）and ‘XX’=’XX’

（D）D. group by XX 1=1--

168、

```
00401064   .    CALL ncrackme.00401230
00401069   .    TEST EAX,EAX
0040106B   .    PUSH 0                                   ; /Style = MB_OK|MB_APPLMODAL
0040106D   .    PUSH ncrackme.00405080                   ; |Title = "ncrackme"
00401072   .    JNZ SHORT ncrackme.0040108F              ; |
00401074   .     MOV EAX,DWORD PTR DS:[4056B8]            ; |
00401079   .    PUSH ncrackme.00405064                   ; |Text = "Registration successful."
0040107E   .     PUSH EAX
0040107F   .    CALL DWORD PTR DS:[<&USER32.MessageBoxA>>; \MessageBoxA
00401085   .    CALL ncrackme.00401330
0040108A   .    XOR EAX,EAX
0040108C   .    RETN 10
0040108F   .    MOV ECX,DWORD PTR DS:[4056B8]            ; |
00401095   .    PUSH ncrackme.00405050                   ; |Text = "Registration fail."
0040109A   .    PUSH ECX
0040109B   .   CALL DWORD PTR DS:[<&USER32.MessageBoxA>>; \MessageBoxA
```

对于在破解过程中，经过一系列的努力，我们找到了如上内容，则要完成暴力破解，应该修改的位置是（D）

（A）00401079

（B）00401095

（C）0040109B

（D）00401072

169、windows2003 中上传文件默认的大小限制为（C）

（A）、50K

（B）、100K

（C）、200K

（D）、500K

170、在一次安全检测中，登录页面中进需要输入密码，其源代码中验证部分内容如下，则以下判断正确的是（C）

```
Var Words
="%0A%3CSCRIPT%3E%0A%0A%3CSCRIPT%20language%3DJavascript%3E%0A%0A%0A%0Afunction%20PassConfir
m%28%29%20%7B%0A%0Avar%20ever%3Ddocument.password.pass.value%3B%0A%0Aif%20%28ever%3D%3D%22ev
il%u3000%22%29%20%7Balert%28%27%u606D%u559C%u8FC7%u5173%uFF0C%u8FDB%u5165%u7B2C%u4E8C%u5173%
uFF01%27%29%3B%0A%0Awindow.open%28%22nextlvel.html%22%2C%22_self%22%29%20%7D%0A%0Aelse%20%7B
document.password.pass.value%3D%27%27%3Breturn%20false%3B%0A%0Awindow.open%28%22
nextlevl.html%22%2C%22_self%22%29%20%7D"
function SetNewWords()
{
    var NewWords;
    NewWords = unescape(Words);
    document.write(NewWords);
}
```

（A）密码为:evil

（B）密码为:ever

（C）登录后页面为:nextlvel.html

（D）登录后页面为:nextlevl.html

171、某主机遭受到拒绝服务攻击后，其结果是（D）
（A）信息不可用
（B）应用程序不可用
（C）阻止通信
（D）以上三项都是

172、下列协议报文不是用 IP 数据报传送的是（A）
（A）ARP
（B）UDP
（C）TCP
（D）ICMP

173、计算机安全评估的第一个正式标准是（A）
（A）TCSEC
（B）ITSEC
（C）CTCPEC
（D）CC

174、Linux 系统中的帐号文件是（B）
（A）/etc/passwd
（B）/etc/shadow
（C）/etc/password
（D）/etc/gshadow

175、小李在使用 super scan 对目标网络进行扫描时发现，某一个主机开放了 25 和 110 端口，此主机最有可能是什么？（B）
（A）文件服务器
（B）邮件服务器
（C）WEB 服务器
（D）DNS 服务器

176、假如你向一台远程主机发送特定的数据包，却不想远程主机响应你的数据包。这时你使用哪一种类型的进攻手段？（B）
（A）缓冲区溢出
（B）地址欺骗
（C）拒绝服务
（D）暴力攻击

177、用户收到了一封可疑的电子邮件,要求用户提供银行账户及密码,这是属于何种攻击手段？（B）
（A）缓存溢出攻击
（B）钓鱼攻击
（C）暗门攻击
（D）DDOS 攻击

178、下列关于在使用交换机的交换网络中进行嗅探技术的说法错误的是（D）

（A）如果交换机配置了端口和 MAC 地址映射，则无法通过简单将网卡设为混杂模式来实现嗅探
（B）如果交换机配置了端口和 MAC 地址映射，可以通过将 MAC 地址设置为局域网内其它主机的 MAC 来实现对相应主机的数据包的嗅探
（C）如果交换机配置了端口和 MAC 地址映射，可以通过 ARP 欺骗来实现对局域网内其它主机的数据包进行嗅探
（D）如果交换机配置了端口和 MAC 地址映射，可以通过将 IP 伪装成其它主机的 IP 来实现对局域网内其它主机的数据包进行嗅探

179、下列关于各类扫描技术说法错误的是（D）
（A）可以通过 ping 进行网络连通性测试，但是 ping 不通不代表网络不通，有可能是路由器或者防火墙对 ICMP 包进行了屏蔽
（B）域名扫描器的作用是查看相应域名是否已经被注册等信息
（C）端口扫描通过向特定的端口发送特定数据包来查看，相应端口是否打开，是否运行着某种服务
（D）whois 服务是一个端口扫描的例子

180、如果一条口令长度为 10，则下列关于该口令说法正确的是（C）
（A）如果该口令仅由数字构成，则其所有可能组合为 10(10-1)
（B）如果该口令仅由数字构成，则其所有可能组合为 910
（C）如果该口令由数字和大小写英文字母所构成，则其所有可能组合为 6210
（D）如果该口令由数字和大小写英文字母所构成，则其所有可能组合为 62(10-1)

181、下列关于各类恶意代码说法错误的是（D）
（A）蠕虫的特点是其可以利用网络进行自行传播和复制
（B）木马可以对远程主机实施控制
（C）Rootkit 即是可以取得 Root 权限的一类恶意工具的统称
（D）所有类型的病毒都只能破坏主机上的各类软件，而无法破坏计算机硬件

182、下列关于操作系统漏洞说法错误的是（B）
（A）操作系统漏洞是由于操作系统在设计与实现的时候产生的错误
（B）在安装了防火墙之后，操作系统的漏洞也就无法被攻击者或者恶意软件所利用了
（C）操作系统漏洞可以能通过手动安装补丁程序、操作系统系统自动更新或者各类自动打补丁的应用程序来修补
（D）著名的“冲击波”病毒便是利用了 RPC 服务的漏洞进行传播的

183、下列关于各类协议欺骗说法错误的的是（D）
（A）DNS 欺骗是破坏了域名与 IP 之间的对应关系
（B）IP 欺骗是利用 IP 与用户身份之间的对应关系，进而进行身份的欺骗
（C）ARP 欺骗是破坏了 MAC 地址与 IP 之间的对应关系
（D）通常说的 MAC 地址绑定，即将 MAC 地址与交换机的端口进行绑定，可以防范 ARP 攻击

184、下列关于各类拒绝服务攻击样式说法错误的是（D）
（A）SYN Flood 攻击通过对 TCP 三次握手过程进行攻击来达到消耗目标资源的目的
（B）ping of death 利用 ICMP 协议在处理大于 65535 字节 ICMP 数据包时的缺陷进行攻击
（C）teardrop 攻击利用了 TCP/IP 协议在重组重叠的 IP 分组分段的缺陷进行攻击
（D）Land 攻击实质上一种利用大量终端同时对目标机进行攻击的分布式拒绝服务攻击

185、下列有关 Linux 用户登录日志说明错误的是（D）
A lastlog 文件记录了最近几次成功登录和最后一次不成功登录的有关信息
B utmp 文件记录了当前登录用户的有关信息
C wtmp 文件记录了用户登录和退出的有关信息
D btmp 文件记录了用户成功登录的有关信息

186、下列关于 windows 操作系统安全策略说明错误的是（C）
A 可以通过禁用 Guest 账户来增强系统的安全性
B 可以通过启用密码最小长度、密码复杂度等策略来加强系统的安全性
C 可以利用自带的 EFS 加密对 SAM 数据库加密来加强系统的安全性
D 可以通过对用户登录、文件访问等设置审核策略来加强系统的安全性

187、以下不会导致缓冲区溢出的函数是（D）
（A）memcopy
（B）memmove
（C）strncpy
（D）malloc

188、在 X86 汇编代码中，retn 和 ret 的关系（B）
（A）两者是相同的
（B）两者不同，retn 先进行 esp 加 n 操作，而 ret 没有此项操作
（C）两者不同，retn 先进行 esp 加 n 操作，而 ret 进行减 esp 减 n 操作
（D）两者不同，retn 先进行 esp 减 n 操作，而 ret 没有此项操作

189、堆和栈的关系正确的是（D）
（A）两者是同一个概念的不同表述
（B）栈和堆是用来存放局部变量的
（C）栈溢出漏洞可以利用，而堆溢出漏洞不能被利用
（D）堆和栈都是内存片段

190、对于 OllyDBG 断点的说法，下列不正确的是（A）
（A）只能有一个硬件断点
（B）可以有多个普通断点
（C）只能有一个内存断点
（D）“bp GetProcAddress”，相当于在函数 GetProcAddress 开始处下了一个普通断点

191、下列哪一种 Rootkit Hook 的技术不能同时在 Ring3 和 Ring0 层同时采用?（D）
（A）IAT Hook
（B）Inline Hook
（C）EAT Hook
（D）DKOM Hook

192、Web 网页木马就是木马利用 Web 页面传播的一种方式，Web 网页木马的最典型特点的是（C）
（A）系统无法响应自带的应用程序。
（B）进程加载变化，即一旦在用户的计算机中加载成功，运行时也会占用一个进程。
（C）浏览器长时间无法打开一个网页，网页木马利用构造大量数据溢出浏览器或组件的缓冲区来执行攻击代码的，从而造成 CPU 占用率很高，浏览器窗口没有响应，导致无法打开该

网页。
（D）在访问目标网页时，杀毒软件会报警。

193、在开始进入一轮 DES 时先要对密钥进行分组、移位。 56 位密钥被分成左右两个部分，每部分为 28 位。根据轮数，这两部分分别循环左移（A）
（A）1 位或 2 位
（B）2 位或 3 位
（C）3 位或 4 位
（D）4 位或 5 位

194、下面基于网络链路层协议的攻击是（A）
（A）ARP 欺骗
（B）IP 欺骗
（C）会话劫持
（D）DNS 欺骗

195、在网络上监听别人口令通常采用（B）
（A）蜜罐技术
（B）嗅探技术
（C）IP 欺骗
（D）拒绝服务

196、TCP/IP 协议中，负责寻址和路由功能的是哪一层？（D）
（A）传输层
（B）数据链路层
（C）应用层
（D）网络层

197、你想发现到达目标网络需要经过哪些路由器，你应该使用什么命令？（C）
（A）ping
（B）nslookup
（C）tracert
（D）ipconfig

198、下列说法正确的是（C）
（A）一张软盘经反病毒软件检测和清除后，该软盘就成为没有病毒的干净盘
（B）若发现软盘带有病毒，则应立即将软盘上的所有文件复制到一张干净软盘上，然后将原来的有病毒软盘进行格式化
（C）若软盘上存放有文件和数据，且没有病毒，则只要将该软盘写保护就不会感染上病毒
（D）如果一张软盘上没有可执行文件，则不会感染上病毒

199、计算机蠕虫是一种特殊的计算机病毒，它的危害比一般的计算机病毒要大许多。要想防范计算机蠕虫就需要区别开其与一般的计算机病毒，这些主要区别在于（A）
（A） 蠕虫不利用文件来寄生
（B）蠕虫病毒的危害远远大于一般的计算机病毒
（C）二者都是病毒，没有什么区别
（D）计算机病毒的危害大于蠕虫病毒

200 、 http://IP/scripts/..%255c..%255winnt/system32/cmd.exe?/c+del+c:\tanker.txt 可以（C）
（A）显示目标主机目录
（B）显示文件内容
（C）删除文件
（D）复制文件的同时将该文件改名

单选题（第二部分 200 题）

1、计算机网络是地理上分散的多台（C）遵循约定的通信协议，通过软硬件互联的系统。
（A）计算机
（B）主从计算机
（C）自主计算机
（D）数字设备

2、密码学的目的是（C）
（A）研究数据加密
（B）研究数据解密
（C）研究数据保密
（D）研究信息安全

3、假设使用一种加密算法，它的加密方法很简单：将每一个字母加 5，即 a 加密成 f。这种算法的密钥就是 5，那么它属于（A）。
（A）对称加密技术
（B）分组密码技术
（C）公钥加密技术
（D）单向函数密码技术

4、网络安全最终是一个折衷的方案，即安全强度和安全操作代价的折衷，除增加安全设施投资外，还应考虑（D）。
（A）用户的方便性
（B）管理的复杂性
（C）对现有系统的影响及对不同平台的支持
（D）上面 3 项都是

5、A 方有一对密钥（KA 公开，KA 秘密），B 方有一对密钥（KB 公开，KB 秘密），A 方向 B 方发送数字签名 M，对信息 M 加密为：M'= KB 公开（KA 秘密（M））。B 方收到密文的解密方案是（C）。
（A）KB 公开（KA 秘密（M'））
（B）KA 公开（KA 公开（M'））
（C）KA 公开（KB 秘密（M'））
（D）KB 秘密（KA 秘密（M'））

6、"公开密钥密码体制"的含义是（C）。
（A）将所有密钥公开
（B）将私有密钥公开，公开密钥保密

（C）将公开密钥公开，私有密钥保密
（D）两个密钥相同

7、信息安全的基本属性是（D）。
（A）机密性
（B）可用性
（C）完整性
（D）上面 3 项都是

8、"会话侦听和劫持技术"是属于（B）的技术。
（A）密码分析还原
（B）协议漏洞渗透
（C）应用漏洞分析与渗透
（D）DOS 攻击

9、对攻击可能性的分析在很大程度上带有（B）。
（A）客观性
（B）主观性
（C）盲目性
（D）上面 3 项都不是

10、从安全属性对各种网络攻击进行分类，阻断攻击是针对（B）的攻击。
（A）机密性
（B）可用性
（C）完整性
（D）真实性

11、从安全属性对各种网络攻击进行分类，截获攻击是针对（A）的攻击。
（A）机密性
（B）可用性
（C）完整性
（D）真实性

12、从攻击方式区分攻击类型，可分为被动攻击和主动攻击。被动攻击难以（C），然而（C）这些攻击是可行的；主动攻击难以（C），然而（C）这些攻击是可行的。
（A）阻止,检测,阻止,检测
（B）检测,阻止,检测,阻止
（C）检测,阻止,阻止,检测
（D）上面 3 项都不是

13、窃听是一种（A）攻击，攻击者（A）将自己的系统插入到发送站和接收站之间。截获是一种（A）攻击，攻击者（A）将自己的系统插入到发送站和接受站之间。
（A）被动,无须,主动,必须
（B）主动,必须,被动,无须
（C）主动,无须,被动,必须
（D）被动,必须,主动,无须

14、拒绝服务攻击的后果是（D）。

（A）信息不可用
（B）应用程序不可用
（C）阻止通信
（D）上面几项都是

15、机密性服务提供信息的保密，机密性服务包括（D）。
（A）文件机密性
（B）信息传输机密性
（C）通信流的机密性
（D）以上 3 项都是

16、最新的研究和统计表明，安全攻击主要来自（B）。
（A）接入网
（B）企业内部网
（C）公用 IP 网
（D）个人网

17、攻击者用传输数据来冲击网络接口，使服务器过于繁忙以至于不能应答请求的攻击方式是（A）。
（A）拒绝服务攻击
（B）地址欺骗攻击
（C）会话劫持
（D）信号包探测程序攻击

18、攻击者截获并记录了从 A 到 B 的数据，然后又从早些时候所截获的数据中提取出信息重新发往 B 称为（D）。
（A）中间人攻击
（B）口令猜测器和字典攻击
（C）强力攻击
（D）回放攻击

19、网络安全是在分布网络环境中对（D）提供安全保护。
（A）信息载体
（B）信息的处理、传输
（C）信息的存储、访问
（D）上面 3 项都是

20、ISO7498-2 从体系结构观点描述了 5 种安全服务，以下不属于这 5 种安全服务的是(B)。
（A）身份鉴别
（B）数据报过滤
（C）授权控制
（D）数据完整性

21、ISO 7498-2 描述了 8 种特定的安全机制，以下不属于这 8 种安全机制的是（A）。
（A）安全标记机制
（B）加密机制
（C）数字签名机制
（D）访问控制机制

22、用于实现身份鉴别的安全机制是（A）。
（A）加密机制和数字签名机制
（B）加密机制和访问控制机制
（C）数字签名机制和路由控制机制
（D）访问控制机制和路由控制机制

23、在 ISO/OSI 定义的安全体系结构中，没有规定（A）。
（A）数据可用性安全服务
（B）数据保密性安全服务
（C）访问控制安全服务
（D）数据完整性安全服务

24、ISO 定义的安全体系结构中包含（B）种安全服务。
（A）4
（B）5
（C）6
（D）7

25、（D）不属于 ISO/OSI 安全体系结构的安全机制。
（A）通信业务填充机制
（B）访问控制机制
（C）数字签名机制
（D）审计机制

26、ISO 安全体系结构中的对象认证服务，使用（B）完成。
（A）加密机制
（B）数字签名机制
（C）访问控制机制
（D）数据完整性机制

27、CA 属于 ISO 安全体系结构中定义的（D）。
（A）认证交换机制
（B）通信业务填充机制
（C）路由控制机制
（D）公证机制

28、数据保密性安全服务的基础是（D）。
（A）数据完整性机制
（B）数字签名机制
（C）访问控制机制
（D）加密机制

29、可以被数据完整性机制防止的攻击方式是（D）。
（A）假冒源地址或用户的地址欺骗攻击
（B）抵赖做过信息的递交行为
（C）数据中途被攻击者窃听获取
（D）数据在途中被攻击者篡改或破坏

30、数字签名要预先使用单向 Hash 函数进行处理的原因是（C）。
（A）多一道加密工序使密文更难破译
（B）提高密文的计算速度
（C）缩小签名密文的长度，加快数字签名和验证签名的运算速度
（D）保证密文能正确还原成明文

31、Kerberos 的设计目标不包括（B）。
（A）认证
（B）授权
（C）记账
（D）审计

32、身份鉴别是安全服务中的重要一环，以下关于身份鉴别叙述不正确的是（B）。
（A）身份鉴别是授权控制的基础
（B）身份鉴别一般不用提供双向的认证
（C）目前一般采用基于对称密钥加密或公开密钥加密的方法
（D）数字签名机制是实现身份鉴别的重要机制

33、基于通信双方共同拥有的但是不为别人知道的秘密，利用计算机强大的计算能力，以该秘密作为加密和解密的密钥的认证是（C）。
（A）公钥认证
（B）零知识认证
（C）共享密钥认证
（D）口令认证

34、(C)是一个对称 DES 加密系统，它使用一个集中式的专钥密码功能，系统的核心是 KDC。
（A）TACACS
（B）RADIUS
（C）Kerberos
（D）PKI

35、访问控制是指确定（A）以及实施访问权限的过程。
（A）用户权限
（B）可给予哪些主体访问权利
（C）可被用户访问的资源
（D）系统是否遭受入侵

36、下列对访问控制影响不大的是（D）。
（A）主体身份
（B）客体身份
（C）访问类型
（D）主体与客体的类型

37、为了简化管理，通常对访问者（A），以避免访问控制表过于庞大。
（A）分类组织成组
（B）严格限制数量
（C）按访问时间排序，删除长期没有访问的用户
（D）不作任何限制

38、PKI 支持的服务不包括（D）。
（A）非对称密钥技术及证书管理
（B）目录服务
（C）对称密钥的产生和分发
（D）访问控制服务

39、PKI 的主要组成不包括（B）。
（A）证书授权 CA
（B）SSL
（C）注册授权 RA
（D）证书存储库 CR

40、PKI 管理对象不包括（A）。
（A）ID 和口令
（B）证书
（C）密钥
（D）证书撤消

41、下面不属于 PKI 组成部分的是（D）。
（A）证书主体
（B）使用证书的应用和系统
（C）证书权威机构
（D）AS

42、PKI 能够执行的功能是（A）和（C）。
（A）鉴别计算机消息的始发者
（B）确认计算机的物理位置
（C）保守消息的机密
（D）确认用户具有的安全性特权

43、SSL 产生会话密钥的方式是（C）。
（A）从密钥管理数据库中请求获得
（B）每一台客户机分配一个密钥的方式
（C）随机由客户机产生并加密后通知服务器
（D）由服务器产生并分配给客户机

44、（C）属于 Web 中使用的安全协议。
（A）PEM、SSL
（B）S-HTTP、S/MIME
（C）SSL、S-HTTP
（D）S/MIME、SSL

45、传输层保护的网络采用的主要技术是建立在（A）基础上的（A）。
（A）可靠的传输服务，安全套接字层 SSL 协议
（B）不可靠的传输服务，S-HTTP 协议
（C）可靠的传输服务， S-HTTP 协议
（D）不可靠的传输服务，安全套接字层 SSL 协议

46、一般而言，Internet 防火墙建立在一个网络的（C）。
（A）内部子网之间传送信息的中枢
（B）每个子网的内部
（C）内部网络与外部网络的交叉点
（D）部分内部网络与外部网络的结合处

47、包过滤型防火墙原理上是基于（C）进行分析的技术。
（A）物理层
（B）数据链路层
（C）网络层
（D）应用层

48、为了降低风险，不建议使用的 Internet 服务是（D）。
（A）Web 服务
（B）外部访问内部系统
（C）内部访问 Internet
（D）FTP 服务

49、对非军事 DMZ 而言，正确的解释是（D）。
（A）DMZ 是一个真正可信的网络部分
（B）DMZ 网络访问控制策略决定允许或禁止进入 DMZ 通信
（C）允许外部用户访问 DMZ 系统上合适的服务
（D）以上 3 项都是

50、对动态网络地址交换（NAT），不正确的说法是（B）。
（A）将很多内部地址映射到单个真实地址
（B）外部网络地址和内部地址一对一的映射
（C）最多可有 64000 个同时的动态 NAT 连接
（D）每个连接使用一个端口

51、以下（D）不是包过滤防火墙主要过滤的信息？
（A）源 IP 地址
（B）目的 IP 地址
（C）TCP 源端口和目的端口
（D）时间

52、防火墙用于将 Internet 和内部网络隔离，（B）。
（A）是防止 Internet 火灾的硬件设施
（B）是网络安全和信息安全的软件和硬件设施
（C）是保护线路不受破坏的软件和硬件设施
（D）是起抗电磁干扰作用的硬件设施

53、通常所说的移动 VPN 是指（A）。
（A）Access VPN
（B）Intranet VPN
（C）Extranet VPN
（D）以上皆不是

54、属于第二层的 VPN 隧道协议有（B）。
（A）IPSec
（B）PPTP
（C）GRE
（D）以上皆不是

55、GRE 协议的乘载协议是（D）。
（A）IP
（B）IPX
（C）AppleTalk
（D）上述皆可

56、VPN 的加密手段为（C）。
（A）具有加密功能的防火墙
（B）具有加密功能的路由器
（C）VPN 内的各台主机对各自的信息进行相应的加密
（D）单独的加密设备

57、将公司与外部供应商、客户及其他利益相关群体相连接的是（B）。
（A）内联网 VPN
（B）外联网 VPN
（C）远程接入 VPN
（D）无线 VPN

58、PPTP、L2TP 和 L2F 隧道协议属于（B）协议。
（A）第一层隧道
（B）第二层隧道
（C）第三层隧道
（D）第四层隧道

59、不属于隧道协议的是（C）。
（A）PPTP
（B）L2TP
（C）TCP/IP
（D）IPSec

60、不属于 VPN 的核心技术是（C）。
（A）隧道技术
（B）身份认证
（C）日志记录
（D）访问控制

61、目前，VPN 使用了（A）技术保证了通信的安全性。
（A）隧道协议、身份认证和数据加密
（B）身份认证、数据加密
（C）隧道协议、身份认证
（D）隧道协议、数据加密

62、（A）通过一个拥有与专用网络相同策略的共享基础设施，提供对企业内部网或外部网的远程访问。
（A）Access VPN
（B）Intranet VPN
（C）Extranet VPN
（D）Internet VPN

63、L2TP 隧道在两端的 VPN 服务器之间采用（A）来验证对方的身份。
（A）口令握手协议 CHAP
（B）SSL
（C）Kerberos
（D）数字证书

64、计算机病毒是计算机系统中一类隐藏在（C）上蓄意破坏的捣乱程序。
（A）内存
（B）软盘
（C）存储介质
（D）网络

65. 在以下人为的恶意攻击行为中，属于主动攻击的是（A）
（A）身份假冒
（B）数据窃听
（C）数据流分析
（D）非法访问

66、 数据保密性指的是（C）
（A）保护网络中各系统之间交换的数据，防止因数据被截获而造成泄密
（B）提供连接实体身份的鉴别
（C）防止非法实体对用户的主动攻击，保证数据接受方收到的信息与发送方发送的信息完全一致
（D）确保数据数据是由合法实体发出的

67、以下算法中属于非对称算法的是（B）
（A）Hash 算法
（B）RSA 算法
（C）IDEA
（D）三重 DES

68、在混合加密方式下，真正用来加解密通信过程中所传输数据（明文）的密钥是（B）
（A）非对称算法的公钥
（B）对称算法的密钥
（C）非对称算法的私钥
（D）CA 中心的公钥

69、以下不属于代理服务技术优点的是（D）
（A）可以实现身份认证
（B）内部地址的屏蔽和转换功能
（C）可以实现访问控制

（D）可以防范数据驱动侵袭

70、包过滤技术与代理服务技术相比较（B）
（A）包过滤技术安全性较弱、但会对网络性能产生明显影响
（B）包过滤技术对应用和用户是绝对透明的
（C）代理服务技术安全性较高、但不会对网络性能产生明显影响
（D）代理服务技术安全性高，对应用和用户透明度也很高

71、在建立堡垒主机时（A）
（A）在堡垒主机上应设置尽可能少的网络服务
（B）在堡垒主机上应设置尽可能多的网络服务
（C）对必须设置的服务给与尽可能高的权限
（D）不论发生任何入侵情况，内部网始终信任堡垒主机

72、当同一网段中两台工作站配置了相同的 IP 地址时，会导致（B）
（A）先入者被后入者挤出网络而不能使用
（B）双方都会得到警告，但先入者继续工作，而后入者不能
（C）双方可以同时正常工作，进行数据的传输
（D）双主都不能工作，都得到网址冲突的警告

73、Linux 和 Windows NT 操作系统是符合哪个级别的安全标准（C）
（A）A 级
（B）B 级
（C）C 级
（D）D 级

74、黑客利用 IP 地址进行攻击的方法有（A）
（A）IP 欺骗
（B）解密
（C）窃取口令
（C）发送病毒

75、防止用户被冒名所欺骗的方法是（A）
（A）对信息源发方进行身份验证
（B）进行数据加密
（C）对访问网络的流量进行过滤和保护
（D）采用防火墙

76、屏蔽路由器型防火墙采用的技术是基于（B）
（A）数据包过滤技术
（B）应用网关技术
（C）代理服务技术
（D）三种技术的结合

77、以下关于防火墙的设计原则说法正确的是（A）
（A）保持设计的简单性
（B）不单单要提供防火墙的功能，还要尽量使用较大的组件
（C）保留尽可能多的服务和守护进程，从而能提供更多的网络服务

（D）一套防火墙就可以保护全部的网络

78、SSL 指的是（B）
（A）加密认证协议
（B）安全套接层协议
（C）授权认证协议
（D）安全通道协议

79、CA 指的是（A）
（A）证书授权
（B）加密认证
（C）虚拟专用网
（D）安全套接层

80、在安全审计的风险评估阶段，通常是按什么顺序来进行的（A）
（A）侦查阶段、渗透阶段、控制阶段
（B）渗透阶段、侦查阶段、控制阶段
（C）控制阶段、侦查阶段、渗透阶段
（D）侦查阶段、控制阶段、渗透阶段

81、以下哪一项不属于入侵检测系统的功能（D）
（A）监视网络上的通信数据流
（B）捕捉可疑的网络活动
（C）提供安全审计报告
（D）过滤非法的数据包

82、入侵检测系统的第一步是（B）
（A）信号分析
（B）信息收集
（C）数据包过滤
（D）数据包检查

83、以下哪一项不是入侵检测系统利用的信息（C）
（A）系统和网络日志文件
（B）目录和文件中的不期望的改变
（C）数据包头信息
（D）程序执行中的不期望行为

84、入侵检测系统在进行信号分析时，一般通过三种常用的技术手段，以下哪一种不属于通常的三种技术手段（D）
（A）模式匹配
（B）统计分析
（C）完整性分析
（D）密文分析

85、以下哪一种方式是入侵检测系统所通常采用的（A）
（A）基于网络的入侵检测
（B）基于 IP 的入侵检测

（C）基于服务的入侵检测
（D）基于域名的入侵检测

86、以下哪一项属于基于主机的入侵检测方式的优势（C）
（A）监视整个网段的通信
（B）不要求在大量的主机上安装和管理软件
（C）适应交换和加密
（D）具有更好的实时性

87、以下关于计算机病毒的特征说法正确的是（C）
（A）计算机病毒只具有破坏性，没有其他特征
（B）计算机病毒具有破坏性，不具有传染性
（C）破坏性和传染性是计算机病毒的两大主要特征
（D）计算机病毒只具有传染性，不具有破坏性

88、以下关于宏病毒说法正确的是（B）
（A）宏病毒主要感染可执行文件
（B）宏病毒仅向办公自动化程序编制的文档进行传染
（C）宏病毒主要感染软盘、硬盘的引导扇区或主引导扇区
（D）CIH 病毒属于宏病毒

89、以下哪一项不属于计算机病毒的防治策略（D）
（A）防毒能力
（B）查毒能力
（C）解毒能力
（D）禁毒能力

90、以下关于 SNMP v1 和 SNMP v2 的安全性问题说法正确的是（A）
（A）SNMP v1 不能阻止未授权方伪装管理器执行 Get 和 Set 操作
（B）SNMP v1 能提供有效的方法阻止第三者观察管理器和代理程序之间的消息交换
（C）SNMP v2 解决不了篡改消息内容的安全性问题
（D）SNMP v2 解决不了伪装的安全性问题

91、在 OSI 七个层次的基础上，将安全体系划分为四个级别，以下那一个不属于四个级别（D）
（A）网络级安全
（B）系统级安全
（C）应用级安全
（D）链路级安全

92、审计管理指（C）
（A）保证数据接收方收到的信息与发送方发送的信息完全一致
（B）防止因数据被截获而造成的泄密
（C）对用户和程序使用资源的情况进行记录和审查
（D）保证信息使用者都可有得到相应授权的全部服务

93、加密技术不能实现（D）
（A）数据信息的完整性
（B）基于密码技术的身份认证

（C）机密文件加密
（D）基于 IP 头信息的包过滤

94、所谓加密是指将一个信息经过（A）及加密函数转换，变成无意义的密文，而接受方则将此密文经过解密函数、（A）还原成明文。
（A）加密钥匙、解密钥匙
（B）解密钥匙、解密钥匙
（C）加密钥匙、加密钥匙
（D）解密钥匙、加密钥匙

95、以下关于对称密钥加密说法正确的是（C）
（A）加密方和解密方可以使用不同的算法
（B）加密密钥和解密密钥可以是不同的
（C）加密密钥和解密密钥必须是相同的
（D）密钥的管理非常简单

96、以下关于非对称密钥加密说法正确的是（B）
（A）加密方和解密方使用的是不同的算法
（B）加密密钥和解密密钥是不同的
（C）加密密钥和解密密钥匙相同的
（D）加密密钥和解密密钥没有任何关系

97、以下关于混合加密方式说法正确的是（B）
（A）采用公开密钥体制进行通信过程中的加解密处理
（B）采用公开密钥体制对对称密钥体制的密钥进行加密后的通信
（C）采用对称密钥体制对对称密钥体制的密钥进行加密后的通信
（D）采用混合加密方式，利用了对称密钥体制的密钥容易管理和非对称密钥体制的加解密处理速度快的双重优点

98、以下关于数字签名说法正确的是（D）
（A）数字签名是在所传输的数据后附加上一段和传输数据毫无关系的数字信息
（B）数字签名能够解决数据的加密传输，即安全传输问题
（C）数字签名一般采用对称加密机制
（D）数字签名能够解决篡改、伪造等安全性问题

99、以下关于 CA 认证中心说法正确的是（C）
（A）CA 认证是使用对称密钥机制的认证方法
（B）CA 认证中心只负责签名，不负责证书的产生
（C）CA 认证中心负责证书的颁发和管理、并依靠证书证明一个用户的身份
（D）CA 认证中心不用保持中立，可以随便找一个用户来做为 CA 认证中心

100、关于 CA 和数字证书的关系，以下说法不正确的是（B）
（A）数字证书是保证双方之间的通讯安全的电子信任关系，他由 CA 签发
（B）数字证书一般依靠 CA 中心的对称密钥机制来实现
（C）在电子交易中，数字证书可以用于表明参与方的身份
（D）数字证书能以一种不能被假冒的方式证明证书持有人身份

101、以下关于 VPN 说法正确的是（B）

（A）VPN 指的是用户自己租用线路，和公共网络物理上完全隔离的、安全的线路
（B）VPN 指的是用户通过公用网络建立的临时的、安全的连接
（C）VPN 不能做到信息认证和身份认证
（D）VPN 只能提供身份认证、不能提供加密数据的功能

102、Ipsec 不可以做到（D）
（A）认证
（B）完整性检查
（C）加密
（D）签发证书

103、包过滤是有选择地让数据包在内部与外部主机之间进行交换，根据安全规则有选择的路由某些数据包。下面不能进行包过滤的设备是（C）
（A）路由器
（B）一台独立的主机
（C）交换机
（D）网桥

104、计算机网络按威胁对象大体可分为两种：一是对网络中信息的威胁；二是（B）
（A）人为破坏
（B）对网络中设备的威胁
（C）病毒威胁
（D）对网络人员的威胁

105、防火墙中地址翻译的主要作用是（B）
（A）提供代理服务
（B）隐藏内部网络地址
（C）进行入侵检测
（D）防止病毒入侵

106、加密有对称密钥加密、非对称密钥加密两种，数字签名采用的是（B）
（A）对称密钥加密
（B）非对称密钥加密
（C）都不是
（D）都可以

107、以下那些属于系统的物理故障（A）
（A）硬件故障与软件故障
（B）计算机病毒
（C）人为的失误
（D）网络故障和设备环境故障

108、对状态检查技术的优缺点描述有误的是（C）
（A）采用检测模块监测状态信息
（B）支持多种协议和应用
（C）不支持监测 RPC 和 UDP 的端口信息
（D）D 配置复杂会降低网络的速度

109、JOE 是公司的一名业务代表，经常要在外地访问公司的财务信息系统，他应该采用的安全、廉价的通讯方式是（B）
（A）PPP 连接到公司的 RAS 服务器上
（B）B 远程访问 VPN
（C）电子邮件
（D）与财务系统的服务器 PPP 连接

110、数据在存储或传输时不被修改、破坏，或数据包的丢失、乱序等指的是（A）
（A）数据完整性
（B）数据一致性
（C）数据同步性
（D）数据源发性

111、可以通过哪种安全产品划分网络结构，管理和控制内部和外部通讯（A）
（A）防火墙
（B）CA 中心
（C）加密机
（D）方病毒产品

112、IPSec 协议是开放的 VPN 协议。对它的描述有误的是（C）
（A）适应于向 IPv6 迁移
（B）提供在网络层上的数据加密保护
（C）支持动态的 IP 地址分配
（D）不支持除 TCP/IP 外的其它协议

113、IPSec 在哪种模式下把数据封装在一个 IP 包传输以隐藏路由信息（A）
（A）隧道模式
（B）管道模式
（C）传输模式
（D）安全模式

114、有关 PPTP（Point-to-Point Tunnel Protocol)说法正确的是（C）
（A）PPTP 是 Netscape 提出的
（B）微软从 NT3.5 以后对 PPTP 开始支持
（C）PPTP 可用在微软的路由和远程访问服务上
（D）它是传输层上的协议

115、有关 L2TP（Layer 2 Tunneling Protocol)协议说法有误的是（D）
（A）L2TP 是由 PPTP 协议和 Cisco 公司的 L2F 组合而成。
（B）L2TP 可用于基于 Internet 的远程拨号访问。
（C）为 PPP 协议的客户建立拨号连接的 VPN 连接。
（D）L2TP 只能通过 TCT/IP 连接。

116、针对下列各种安全协议，最适合使用外部网 VPN 上，用于在客户机到服务器的连接模式的是（C）
（A）IPsec
（B）PPTP
（C）SOCKS v5

（D）L2TP

117、下列各种安全协议中使用包过滤技术，适合用于可信的 LAN 到 LAN 之间的 VPN，即内部网 VPN 的是（D）
（A）PPTP
（B）L2TP
（C）SOCKS v5
（D）IPsec

118、目前在防火墙上提供了几种认证方法，其中防火墙设定可以访问内部网络资源的用户访问权限是（C）
（A）客户认证
（B）回话认证
（C）用户认证
（D）都不是

119、Firewall －1 是一种（D）
（A）方病毒产品
（B）扫描产品
（C）入侵检测产品
（D）防火墙产品

120、能够在网络通信中寻找符合网络入侵模式的数据包而发现攻击特征的入侵检测方式是（A）
（A）基于网络的入侵检测方式
（B）基于文件的入侵检测方式
（C）基于主机的入侵检测方式
（D）基于系统的入侵检测方式

121、使用安全内核的方法把可能引起安全问题的部分冲操作系统的内核中去掉，形成安全等级更高的内核,目前对安全操作系统的加固和改造可以从几个方面进行。下面错误的是(D)
（A）采用随机连接序列号
（B）驻留分组过滤模块
（C）取消动态路由功能
（D）尽可能地采用独立安全内核

122、在防火墙实现认证的方法中，采用通过数据包中的源地址来认证的是（B）
（A）Password-Based Authentication
（B）Address-Based Authentication
（C）Cryptographic Authentication
（D）None of Above.

123、网络入侵者使用 sniffer 对网络进行侦听，在防火墙实现认证的方法中，下列身份认证可能会造成不安全后果的是（A）
（A）Password-Based Authentication
（B）Address-Based Authentication
（C）Cryptographic Authentication
（D）None of Above.

124、随着 Internet 发展的势头和防火墙的更新，防火墙的哪些功能将被取代（D）
（A）使用 IP 加密技术
（B）日志分析工具
（C）攻击检测和报警
（D）对访问行为实施静态、固定的控制

125、当你感觉到你的 Win2000 运行速度明显减慢，当你打开任务管理器后发现 CPU 的使用率达到了百分之百，你最有可能认为你受到了哪一种攻击（B）
（A）特洛伊木马
（B）拒绝服务
（C）欺骗
（D）中间人攻击

126、RC4 是由 RIVEST 在 1987 年开发的，是一种流式的密文，就是实时的把信息加密成一个整体，它在美国一般密钥长度是 128 位，因为受到美国出口法的限制，向外出口时限制到多少位？（C）
（A）64 位
（B）56 位
（C）40 位
（D）32 位

127、假如你向一台远程主机发送特定的数据包，却不想远程主机响应你的数据包。这时你使用哪一种类型的进攻手段？（B）
（A）缓冲区溢出
（B）地址欺骗
（C）拒绝服务
（D）暴力攻击

128、以下关于 VPN 的说法中的哪一项是正确的？（C）
（A）VPN 是虚拟专用网的简称，它只能只好 ISP 维护和实施
（B）VPN 是只能在第二层数据链路层上实现加密
（C）IPSEC 是也是 VPN 的一种
（D）VPN 使用通道技术加密，但没有身份验证功能

129、下列哪项不属于 window2003 的安全组件？（D）
（A）访问控制
（B）强制登陆
（C）审计
（D）自动安全更新

130、以下哪个不是属于 window2000 的漏洞？（D）
（A）unicode
（B）IIS hacker
（C）输入法漏洞
（D）单用户登陆

131、你是一企业网络管理员，你使用的防火墙在 Linux 下的 IPTABLES，你现在需要通过对防火墙的配置不允许 192.168.0.2 这台主机登陆到你的服务器，你应该怎么设置防火墙规则？

（B）
（A）iptables—A input—p tcp—s 192.168.0.2—source—port 23—j DENY
（B）iptables—A input—p tcp—s 192.168.0.2—destination—port 23—j DENY
（C）iptables—A input—p tcp—d 192.168.0.2—source—port 23—j DENY
（D）iptables—A input—p tcp—d 192.168.0.2—destination—port 23—j DENY

132、你的 window2000 开启了远程登陆 telnet，但你发现你的 window98 和 unix 计算机没有办法远程登陆，只有 win2000 的系统才能远程登陆，你应该怎么办？（D）
（A）重设防火墙规则
（B）检查入侵检测系统
（C）运用杀毒软件，查杀病毒
（D）将 NTLM 的值改为 0

133、你所使用的系统为 win2000，所有的分区均是 NTFS 的分区，C 区的权限为 everyone 读取和运行，D 区的权限为 everyone 完全控制，现在你将一名为 test 的文件夹，由 C 区移动到 D 区之后，test 文件夹的权限为？（B）
（A）everyone 读取和运行
（B）everyone 完全控制
（C）everyone 读取、运行、写入
（D）以上都不对

134、你所使用的系统为 Linux，你通过 umask 命令求出当前用户的 umask 值为 0023，请问该用户在新建一文件夹，具体有什么样的权限？（A）
（A）当前用户读、写和执行，当前组读取和执行，其它用户和组只读
（B）当前用户读、写，当前组读取，其它用户和组不能访问
（C）当前用户读、写，当前组读取和执行，其它用户和组只读
（D）当前用户读、写和执行，当前组读取和写入，其它用户和组只读

135、作为一个管理员，把系统资源分为三个级别是有必要的，以下关于级别 1 的说法正确的是？（A）
（A）对于那些运行至关重要的系统，如，电子商务公司的用户帐号数据库
（B）对于那些必须的但对于日常工作不是至关重要的系统
（C）本地电脑即级别 1
（D）以上说法均不正确

136、你有一个共享文件夹，你将它的 NTFS 权限设置为 sam 用户可以修改，共享权限设置为 sam 用户可以读取，当 sam 从网络访问这个共享文件夹的时候，他有什么样的权限？（A）
（A）读取
（B）写入
（C）修改
（D）完全控制

137、SSL 安全套接字协议所使用的端口是（B）
（A）80
（B）443
（C）1433
（D）3389

138、Window2000/XP/2003 域或默认的身份验证协议是（B）
（A）HTML
（B）Kerberos V5
（C）TCP/IP
（D）Apptalk

139、在 Linux 下 umask 的八进制模式位 6 代表（C）
（A）拒绝访问
（B）写入
（C）读取和写入
（D）读取、写入和执行

140、你是一个公司的网络管理员，你经常在远程不同的地点管理你的网络（如家里），你公司使用 win2000 操作系统，你为了方便远程管理，在一台服务器上安装并启用了终端服务。最近，你发现你的服务器有被控制的迹象，经过你的检查，你发现你的服务器上多了一个不熟悉的帐户，你将其删除，但第二天却总是有同样的事发生，你应该如何解决这个问题？（C）
（A）停用终端服务
（B）添加防火墙规则，除了你自己家里的 IP 地址，拒绝所有 3389 的端口连入
（C）打安全补丁 sp4
（D）启用帐户审核事件，然后查其来源，予以追究

141、以下不属于 win2000 中的 ipsec 过滤行为的是（D）
（A）允许
（B）阻塞
（C）协商
（D）证书

142、以下关于对称加密算法 RC4 的说法正确的是（B）
（A）它的密钥长度可以从零到无限大
（B）在美国一般密钥长度是 128 位，向外出口时限制到 40 位
（C）RC4 算法弥补了 RC5 算法的一些漏洞
（D）最多可以支持 40 位的密钥

143、你配置 UNIX 下的 Ipchains 防火墙，你要添加一条规则到指定的 chain 后面，你应该使用参数（A）
（A）—A
（B）—D
（C）—S
（D）—INPUT

144、在网络攻击的多种类型中，以遭受的资源目标不能继续正常提供服务的攻击形式属于哪一种？（A）
（A）拒绝服务
（B）侵入攻击
（C）信息盗窃
（D）信息篡改

145、电子邮件的发件人利用某些特殊的电子邮件软件在短时间内不断重复地将电子邮件寄

给同一个收件人，这种破坏方式叫做（B）
（A）邮件病毒
（B）邮件炸弹
（C）特洛伊木马
（D）逻辑炸弹

146、对企业网络最大的威胁是（D），请选择最佳答案。
（A）黑客攻击
（B）外国政府
（C）竞争对手
（D）内部员工的恶意攻击

147、以下对 TCP 和 UDP 协议区别的描述，哪个是正确的（B）
（A）UDP 用于帮助 IP 确保数据传输,而 TCP 无法实现
（B）UDP 提供了一种传输不可靠的服务，主要用于可靠性高的局域网中，TCP 的功能与之相反
（C）TCP 提供了一种传输不可靠的服务，主要用于可靠性高的局域网中，UDP 的功能与之相反
（D）以上说法都错误

148、黑客攻击某个系统之前，首先要进行信息收集，那么通过技术手段收集如何实现（A）
（A）攻击者通过 Windows 自带命令收集有利信息
（B）通过查找最新的漏洞库去反查具有漏洞的主机
（C）通过发送加壳木马软件或者键盘记录工具
（D）通过搜索引擎来来了解目标网络结构、关于主机更详细的信息

149、以下描述黑客攻击思路的流程描述中，哪个是正确的（C）
（A）一般黑客攻击思路分为预攻击阶段、实施破坏阶段、获利阶段
（B）一般黑客攻击思路分为信息收集阶段、攻击阶段、破坏阶段
（C）一般黑客攻击思路分为预攻击阶段、攻击阶段、后攻击阶段
（D）一般黑客攻击思路分为信息收集阶段、漏洞扫描阶段、实施破坏阶段

150、以下对于黑色产业链描述中正确的是（A）
（A）由制造木马、传播木马、盗窃账户信息、第三方平台销赃形成了网上黑色产业链
（B）黑色产业链上的每一环都使用肉鸡倒卖做为其牟利方式
（C）黑色产业链中制作的病毒都无法避免被杀毒软件查杀掉
（D）黑色产业链一般都是个人行为

151、在身份鉴别技术中，用户采用字符串作为密码来声明自己的身份的方式属于哪种类型（C）
（A）基于对称密钥密码体制的身份鉴别技术
（B）基于非对称密钥密码体制的身份鉴别技术
（C）基于用户名和密码的身份鉴别技术
（D）基于 KDC 的身份鉴别技术

152、以下哪个部分不是 CA 认证中心的组成部分（A）
（A）证书生成客户端
（B）注册服务器

（C）证书申请受理和审核机构
（D）认证中心服务器

153、以下哪种是常用的哈希算法(HASH)（B）
（A）DES
（B）MD5
（C）RSA
（D）ong

154、企业在选择防病毒产品时，选择单一品牌防毒软件产品的好处是什么？（D）
（A）划算的总体成本
（B）更简化的管理流程
（C）容易更新
（D）以上都正确

155、对称密钥加密技术的特点是什么（A）
（A）无论加密还是解密都用同一把密钥
（B）收信方和发信方使用的密钥互不相同
（C）不能从加密密钥推导解密密钥
（D）可以适应网络的开放性要求

156、屏蔽主机式防火墙体系结构的优点是什么（A）
（A）此类型防火墙的安全级别较高
（B）如果路由表遭到破坏，则数据包会路由到堡垒主机上
（C）使用此结构，必须关闭双网主机上的路由分配功能
（D）此类型防火墙结构简单，方便部署

157、常用的口令入侵手段有？（D）
（A）通过网络监听
（B）利用专门软件进行口令破解
（C）利用系统的漏洞
（D）以上都正确

158、以下哪条不属于防火墙的基本功能（D）
（A）控制对网点的访问和封锁网点信息的泄露
（B）能限制被保护子网的泄露
（C）具有审计作用
（D）具有防毒功能

159、企事业单位的网络环境中应用安全审计系统的目的是什么（D）
（A）为了保障企业内部信息数据的完整性
（B）为了保障企业业务系统不受外部威胁攻击
（C）为了保障网络环境不存在安全漏洞，感染病毒
（D）为了保障业务系统和网络信息数据不受来自用户的破坏、泄密、窃取

160、下列各项中，哪一项不是文件型病毒的特点（B）
（A）病毒以某种形式隐藏在主程序中，并不修改主程序
（B）以自身逻辑部分取代合法的引导程序模块，导致系统瘫痪

（C）文件型病毒可以通过检查主程序长度来判断其存在
（D）文件型病毒通常在运行主程序时进入内存

161、虚拟专网的重点在于建立安全的数据通道，构造这条安全通道的协议必须具备多项条件，以下哪条不属于构造的必备条件（C）
（A）保证数据的真实性
（B）保证数据的完整性
（C）提供网络信息数据的纠错功能和冗余处理
（D）提供安全防护措施和访问控制

162、SOCK v5 在 OSI 模型的哪一层控制数据流，定义详细的访问控制（B）
（A）应用层
（B）会话层
（C）表示层
（D）传输层

163、用户通过本地的信息提供商（ISP）登陆到 Internet 上，并在现在的办公室和公司内部网之间建立一条加密通道。这种访问方式属于哪一种 VPN（B）
（A）内部网 VPN
（B）远程访问 VPN
（C）外联网 VPN
（D）以上皆有可能

164、哪些文件会被 DOS 病毒感染（A）
（A）可执行文件
（B）图形文件
（C）文本文件
（D）系统文件

165、网络传播型木马的特征有很多，请问哪个描述是正确的（B）
（A）利用现实生活中的邮件进行散播，不会破坏数据，但是他将硬盘加密锁死
（B）兼备伪装和传播两种特征并结合 TCP/IP 网络技术四处泛滥，同时他还添加了"后门"和击键记录等功能
（C）通过伪装成一个合法性程序诱骗用户上当
（D）通过消耗内存而引起注意

166、蠕虫程序有 5 个基本功能模块，哪个模块可实现搜集和建立被传染计算机上信息（D）
（A）扫描搜索模块
（B）攻击模式
（C）传输模块
（D）信息搜集模块

167、哪个手机病毒的特点是会给地址簿中的邮箱发送带毒邮件，还能通过短信服务器中转向手机发送大量短信（B）
（A）EPOC_LIGHTS.A
（B）Timofonica
（C）Hack.mobile.smsdos
（D）Trojanhorse

168、关于防病毒软件的实时扫描的描述中，哪种说法是错误的（B）
（A）扫描只局限于检查已知的恶意代码签名，无法检测到未知的恶意代码
（B）可以查找文件是否被病毒行为修改的扫描技术
（C）扫描动作在背景中发生，不需要用户的参与
（D）在访问某个文件时，执行实时扫描的防毒产品会检查这个被打开的文件;

169、通过检查电子邮件信件和附件来查找某些特定的语句和词语、文件扩展名或病毒签名进行扫描是哪种扫描技术（D）
（A）实时扫描
（B）完整性扫描
（C）启发式扫描
（D）内容扫描

170、以下关于混合加密方式说法正确的是（B）
（A）采用公开密钥体制进行通信过程中的加解密处理
（B）采用公开密钥体制对对称密钥体制的密钥进行加密后的通信
（C）采用对称密钥体制对对称密钥体制的密钥进行加密后的通信
（D）采用混合加密方式，利用了对称密钥体制的密钥容易管理和非对称密钥体制的加解密处理速度快的双重优点

171、包过滤是有选择地让数据包在内部与外部主机之间进行交换，根据安全规则有选择的路由某些数据包。下面不能进行包过滤的设备是（C）
（A）路由器
（B）一台独立的主机
（C）交换机
（D）网桥

172、以下那些属于系统的物理故障（A）
（A）硬件故障与软件故障
（B）计算机病毒
（C）人为的失误
（D）网络故障和设备环境故障

173、可以通过哪种安全产品划分网络结构，管理和控制内部和外部通讯（A）
（A）防火墙
（B）CA 中心
（C）加密机
（D）防病毒产品

174、IPSec 协议是开放的 VPN 协议。对它的描述有误的是（C）
（A）适应于向 IPv6 迁移
（B）提供在网络层上的数据加密保护
（C）支持动态的 IP 地址分配
（D）不支持除 TCP/IP 外的其它协议

175、目前在防火墙上提供了几种认证方法，其中防火墙设定可以访问内部网络资源的用户访问权限是（C）
（A）客户认证

（B）回话认证
（C）用户认证
（D）都不是

176、请问以下哪个不是计算机病毒的不良特征（D）
（A）隐蔽性
（B）感染性
（C）破坏性
（D）自发性

177、根据计算机病毒的感染特性看，宏病毒不会感染以下哪种类型的文件（B）
（A）Microsoft Word
（B）Microsoft Basic
（C）Microsoft Excel
（C）Visual Basic

178、指在公司总部和远地雇员之间建立的 VPN 是什么类型的 VPN（B）
（A）内部网 VPN
（B）远程访问 VPN
（C）外联网 VPN
（D）以上皆有可能

179、以下哪个不属于完整的病毒防护安全体系的组成部分（D）
（A）人员
（B）技术
（C）流程
（D）设备

180、按趋势科技的病毒命名规则，以下哪个病毒是木马病毒（B）
（A）Worm_downad.dd
（B）Troj__generic.apc
（C）Tspy_qqpass.ajr
（D）Bkdr_delf.hko

181、哪种类型的漏洞评估产品是可以模拟黑客行为，扫描网络上的漏洞并进行评估的（A）
（A）网络型安全漏洞评估产品
（B）主机型安全漏洞评估产品
（C）数据库安全漏洞评估产品
（D）以上皆是

182、按感染对象分类，CIH 病毒属于哪一类病毒（B）
（A）引导区病毒
（B）文件型病毒
（C）宏病毒
（D）复合型病毒

183、哪个信息安全评估标准给出了关于 IT 安全的保密性、完整性、可用性、审计性、认证性、可靠性 6 个方面含义，并提出了以风险为核心的安全模型（A）

（A）ISO13335 标准
（B）BS7799 标准
（C）AS/NZS 4360：1999 标准
（ D ） OCTAVE （ Operationally Critical Threat, Asset, and Vulnerability Evaluation）

184、世界上第一个病毒 CREEPER（爬行者）出现在哪一年（B）
（A）1961
（B）1971
（C）1977
（D）1980

185、正常的系统启动都有一定的顺序，请问以下哪个是正确的启动顺序（C）
A. 电源开启自检过程。
B. 引导程序载入过程。
C. 用户登录过程。
D. 即插即用设备的检测过程
E. 检测和配置硬件过程
F. 初始化启动过程
G. 内核加载过程
（A）A B C D E F G
（B）A F G C E D B
（C）A F B E G C D
（D）D E G A C F B

186、什么是网页挂马（A）
（A）攻击者通过在正常的页面中（通常是网站的主页）插入一段代码。浏览者在打开该页面的时候，这段代码被执行，然后下载并运行某木马的服务器端程序，进而控制浏览者的主机
（B）黑客们利用人们的猎奇、贪心等心理伪装构造一个链接或者一个网页，利用社会工程学欺骗方法，引诱点击，当用户打开一个看似正常的页面时，网页代码随之运行，隐蔽性极高
（C）把木马服务端和某个游戏/软件捆绑成一个文件通过 QQ/MSN 或邮件发给别人，或者通过制作 BT 木马种子进行快速扩散
（D）与从互联网上下载的免费游戏软件进行捆绑。被激活后，它就会将自己复制到 Windows 的系统文件夹中，并向注册表添加键值，保证它在启动时被执行。

187、安全模型简称 MDPRR，有关 MDPRR 正确的是（D）
（A）many--M detection--D protect--P recovery--R reaction--R
（B）management--M detection--D people--P recovery--R reaction--R
（C）man--M detection--D protect--P redo--R reaction--R
（D）management--M detection--D protect--P recovery--R reaction--R

188、按明文形态划分，对两个离散电平构成 0、1 二进制关系的电报信息加密的密码是什么密码（C）
（A）离散型密码
（B）模拟型密码

（C）数字型密码
（D）非对称式密码

189、以下对特洛伊木马的概念描述正确的是（B）
（A）特洛伊木马不是真正的网络威胁，只是一种游戏
（B）特洛伊木马是指隐藏在正常程序中的一段具有特殊功能的恶意代码，是具备破坏和删除文件、发送密码、记录键盘和攻击 Dos 等特殊功能的后门程序。
（C）特洛伊木马程序的特征很容易从计算机感染后的症状上进行判断
（D）中了特洛伊木马就是指安装了木马的客户端程序，若你的电脑被安装了客户端程序，则拥有相应服务器端的人就可以通过网络控制你的电脑。

190、TCP 协议是攻击者攻击方法的思想源泉，主要问题存在于 TCP 的三次握手协议上,以下哪个顺序是正常的 TCP 三次握手过程（B）
1. 请求端 A 发送一个初始序号 ISNa 的 SYN 报文；
2.A 对 SYN+ACK 报文进行确认，同时将 ISNa+1，ISNb+1 发送给 B
3.被请求端 B 收到 A 的 SYN 报文后，发送给 A 自己的初始序列号 ISNb，同时将 ISNa+1 作为确认的 SYN+ACK 报文
（A）1 2 3
（B）1 3 2
（C）3 2 1
（D）3 1 2

191、信息接收方在收到加密后的报文，需要使用什么来将加密后的报文还原（D）
（A）明文
（B）密文
（C）算法
（D）密钥

192、用每一种病毒体含有的特征字节串对被检测的对象进行扫描，如果发现特征字节串，就表明发现了该特征串所代表的病毒，这种病毒的检测方法叫做（B）
（A）比较法
（B）特征字的识别法
（C）搜索法
（D）分析法

193、关于包过滤技术的理解正确的说法是哪个（C）
（A）包过滤技术不可以对数据包左右选择的过滤
（B）通过设置可以使满足过滤规则的数据包从数据中被删除
（C）包过滤一般由屏蔽路由器来完成
（D）包过滤技术不可以根据某些特定源地址、目标地址、协议及端口来设置规则

194、通过 SNMP、SYSLOG、OPSEC 或者其他的日志接口从各种网络设备、服务器、用户电脑、数据库、应用系统和网络安全设备中收集日志，进行统一管理、分析和报警。这种方法属于哪一种安全审计方法（A）
（A）日志安全审计
（B）信息安全审计
（C）主机安全审计

（D）网络安全审计

195、以下对于反病毒技术的概念描述正确的是（A）
（A）提前取得计算机系统控制权，识别出计算机的代码和行为，阻止病毒取得系统控制权
（B）与病毒同时取得计算机系统控制权，识别出计算机的代码和行为，然后释放系统控制权
（C）在病毒取得计算机系统控制权后，识别出计算机的代码和行为，然后释放系统控制权
（D）提前取得计算机系统控制权，识别出计算机的代码和行为，允许病毒取得系统控制权

196、Jolt 通过大量伪造的 ICMP 和 UDP 导致系统变的非常慢甚至重新启动，这种攻击方式是（B）
（A）特洛伊木马
（B）DDos 攻击
（C）邮件炸弹
（D）逻辑炸弹

197、有记录在线离线记录特征的木马属于哪种特洛伊木马（B）
（A）代理木马
（B）键盘记录木马
（C）远程访问型
（D）程序杀手木马

198、一封垃圾邮件的发送人和接收人都在邮件服务器的本地域，那么垃圾邮件是如何进行发送的（A）
（A）使用第三方邮件服务器进行发送
（B）在本地邮件服务器上进行发送
（C）这种邮件不可能是垃圾邮件
（D）使用特殊的物理设备进行发送

199、网络钓鱼使用的最主要的欺骗技术是什么（B）
（A）攻破某些网站，然后修改他的程序代码
（B）仿冒某些公司的网站或电子邮件
（C）直接窃取用户电脑的一些记录
（D）发送大量垃圾邮件

200、信息安全存储中最主要的弱点表现在哪方面（A）
（A）磁盘意外损坏，光盘意外损坏，信息存储设备被盗
（B）黑客的搭线窃听
（C）信息被非法访问
（D）网络安全管理

单选题（第三部分 200 题）

1、文件型病毒传染的对象主要是（B）类文件
（A）.EXE 和.WPS
（B）.COM 和.EXE
（C）.WPS

（D）.DBF

2、标准网络安全漏洞可以分为各个等级，C 级漏洞表示（C）
（A）允许本地用户提高访问权限，并可能使其获得系统控制的漏洞
（B）允许恶意入侵者访问并可能会破坏整个目标系统的漏洞
（C）允许用户中断、降低或阻碍系统操作的漏洞
（D）以上都不正确

3、一般的数据加密可以在通信的三个层次来实现:链路加密、节点加密、端到端加密。其中在节点处信息以明文出现的是（A）
（A）链路加密方式
（B）端对端加密方式
（C）节点加密
（D）都以明文出现

4、网际协议 IP（Internet Protocol）是位于 ISO 七层协议中哪一层的协议（A）
（A）网络层
（B）数据链路层
（C）应用层
（D）会话层

5、现存的计算机平台中，哪些系统目前还没有发现被病毒感染（D）
（A）Windows
（B）Unix/Linux
（C）Dos
（D）以上都不是

6、初始化硬件检测状态时，计算机会读取哪个文件（C）
（A）Boot.ini
（B）Ntldr
（C）Ntdetect.com
（D）Bootsect.dos

7、一台计算机出现了类似病毒的现象，用户在任务管理器中排查进程时发现有个叫 lsass.exe 的进程，请问该进程是否为系统的正常进程（A）
（A）是
（B）不是

8、以下算法中属于非对称算法的是（B）
（A）Hash 算法
（B）RSA 算法
（C）IDEA
（D）三重 DES

9、什么是 SSL VPN（D）
（A）SSL VPN 是一个应用范围广泛的开放的第三层 VPN 协议标准。
（B）SSL VPN 是数据链路层的协议，被用于微软的路由和远程访问服务。
（C）SOCK v5 是一个需要认证的防火墙协议，可作为建立高度安全的 VPN 的基础。

（D）SSL VPN 是解决远程用户访问敏感公司数据最简单最安全的解决技术。

10、哪种类型的漏洞评估产品最主要是针对操作系统的漏洞做更深入的扫描（B）
（A）网络型安全漏洞评估产品
（B）主机型安全漏洞评估产品
（C）数据库安全漏洞评估产品
（D）以上皆是

11、如果染毒文件有未被染毒的备份的话，用备份覆盖染毒文件即可,这种病毒清除方式适用于（A）
（A）文件型病毒的清除
（B）引导型病毒的清
（C）内存杀毒
（D）压缩文件病毒的检测和清除

12、计算机在未运行病毒程序的前提下，用户对病毒文件做下列哪项操作是不安全的（B）
（A）查看病毒文件名称
（B）执行病毒文件
（C）查看计算机病毒代码
（D）拷贝病毒程序

13、蠕虫程序的基本功能模块的作用是什么（A）
（A）完成复制传播流程
（B）实现更强的生存
（C）实现更强的破坏力
（D）完成再生功能

14、通过加强对浏览器安全等级的调整，提高安全等级能防护 Spyware（A）
（A）对
（B）不对

15、SMTP 协议是位于 OSI 七层模型中的哪一层的协议（A）
（A）应用层
（B）会话层
（C）传输层
（D）数据链路层

16、在防火墙技术中，代理服务技术的又称为什么技术（B）
（A）帧过滤技术
（B）应用层网关技术
（C）动态包过滤技术
（D）网络层过滤技术

17、信息系统测评的基础是什么（A）
（A）数据采集和分析
（B）量化评估
（C）安全检测
（D）安全评估分析

18、以下对于计算机病毒概念的描述哪个是正确的（B）
（A）计算机病毒只在单机上运行
（B）计算机病毒是一个程序
（C）计算机病毒不一定具有恶意性
（D）计算机病毒是一个文件

19、计算机病毒有哪几个生命周期（A）
（A）开发期，传染期，潜伏期，发作期，发现期，消化期，消亡期
（B）制作期，发布期，潜伏期，破坏期，发现期，消化期，消亡期
（C）开发期，传染期，爆发期，发作期，发现期，消化期
（D）开发期，传染期，潜伏期，发作期,消化期，消亡期

20、关于"I LOVE YOU"病毒描述正确的是（C）
（A）"I LOVE YOU"病毒属于宏病毒
（B）"I LOVE YOU"病毒属于 PE 病毒
（C）"I LOVE YOU"病毒属于脚本病毒
（D）"I LOVE YOU"病毒属于 Java 病毒

21、根据病毒的特征看，不具有减缓系统运行特征的是哪种病毒（D）
（A）宏病毒
（B）脚本病毒
（C）Java 病毒
（D）Shockwave 病毒

22、蠕虫病毒是最常见的病毒，有其特定的传染机理，请问他的传染机理是什么（A）
（A）利用网络进行复制和传播
（B）利用网络进行攻击
（C）利用网络进行后门监视
（D）利用网络进行信息窃取

23、请问在 OSI 模型中，应用层的主要功能是什么（D）
A.确定使用网络中的哪条路径
B.允许设置和终止两个系统间的通信路径与同步会话
C.将外面的数据从机器特有格式转换为国际标准格式
D.为网络服务提供软件

24、最大的优点是对用户透明，并且隐藏真实 IP 地址，同时解决合法 IP 地址不够用的问题。这种防火墙技术称为（C）
（A）包过滤技术
（B）状态检测技术
（C）代理服务技术
（D）以上都不正确

25、哪种木马隐藏技术的特点是在没有增加新文件、不打开新的端口、没有生成新的进程的情况下进行危害（A）
（A）修改动态链接库加载
（B）捆绑文件
（C）修改文件关联

（D）利用注册表加载

26、每种网络威胁都有其目的性，那么网络钓鱼发布者想要实现什么目的（D）
（A）破坏计算机系统
（B）单纯的对某网页进行挂马
（C）体现黑客的技术
（D）窃取个人隐私信息

27、以下对于手机病毒描述正确的是（C）
（A）手机病毒不是计算机程序
（B）手机病毒不具有攻击性和传染性
（C）手机病毒可利用发送短信、彩信，电子邮件，浏览网站，下载铃声等方式进行传播
（D）手机病毒只会造成软件使用问题，不会造成 SIM 卡、芯片等损坏

28、关于病毒流行趋势,以下说法哪个是错误的（B）
（A）病毒技术与黑客技术日益融合在一起
（B）计算机病毒制造者的主要目的是炫耀自己高超的技术
（C）计算机病毒的数量呈指数性成长，传统的依靠病毒码解毒的防毒软件渐渐显得力不从心
（D）计算机病毒的编写变得越来越轻松，因为互联网上可以轻松下载病毒编写工具

29、以下关于 ARP 协议的描述哪个是正确的（B）
（A）工作在网络层
（B）将 IP 地址转化成 MAC 地址
（C）工作在网络层
（D）将 MAC 地址转化成 IP 地址

30、使用安全内核的方法把可能引起安全问题的部分从操作系统的内核中去掉，形成安全等级更高的内核，目前对安全操作系统的加固和改造可以从几个方面进行。下面错误的是(D)
（A）采用随机连接序列号
（B）驻留分组过滤模块
（C）取消动态路由功能
（D）尽可能地采用独立安全内核

31、在防火墙技术中，代理服务技术的最大优点是什么（）
（A）透明性
（B）有限的连接
（C）有限的性能
（D）有限的应用

32、入侵分析技术按功能不同，可分为几种类型；以下哪种技术是用来检测有无对系统的已知弱点进行的攻击行为（A）
（A）签名分析法
（B）统计分析法
（C）数据完整性分析法
（D）数字分析法

33、"网银大盗"病毒感染计算机系统后，病毒发送者最终先实现什么目的（B）

（A）破坏银行网银系统
（B）窃取用户信息
（C）导致银行内部网络异常
（D）干扰银行正常业务

34、什么是宏病毒（B）
（A）宏病毒会感染所有文件
（B）宏病毒是一组指令
（C）宏病毒只感染 Microsoft office 的组件
（D）宏病毒会自动运行，不需要随文档一起运行

35、实现蠕虫之间、蠕虫同黑客之间进行交流功能的是哪种蠕虫程序扩展功能模块（C）
（A）隐藏模块
（B）破坏模块
（C）通信模块
（D）控制模块

36、基于用户名和密码的身份鉴别的正确说法是（D）
（A）将容易记忆的字符串作密码，使得这个方法经不起攻击的考验
（B）口令以明码的方式在网络上传播也会带来很大的风险
（C）更为安全的身份鉴别需要建立在安全的密码系统之上
（D）以上都正确

37、计算机病毒对系统或网络都有一定的破坏性，请问破坏性是由什么因素决定的（D）
（A）被感染计算机的软件环境
（B）被感染计算机的系统类型
（C）感染者本身的目的
（D）病毒设计者的目的

38、入侵检测系统在进行信号分析时，一般通过三种常用的技术手段，以下哪一种不属于通常的三种技术手段（D）
（A）模式匹配
（B）统计分析
（C）完整性分析
（D）密文分析

39、病毒的传播途径多种多样，哪种病毒的传播不需要通过互联网下载进行（A）
（A）宏病毒
（B）脚本病毒
（C）Java 病毒
（D）Shockwave 病毒

40、以下哪个不是公钥密码的优点（D）
（A）适应网络的开放性要求
（B）密钥管理问题较为简单
（C）可方便的实现数字签名和验证
（D）算法复杂

41、网络攻击的有效载体是什么（C）
（A）黑客
（B）网络
（C）病毒
（D）蠕虫

42、以下对于入侵检测系统的解释正确的是（B）
（A）入侵检测系统有效地降低黑客进入网络系统的门槛入侵
（B）检测系统是指监视（或者在可能的情况下阻止）入侵或者试图控制你的系统或者网络资源的行为的系统
（C）入侵检测系统能够通过向管理员收发入侵或者入侵企图来加强当前的存取控制系统
（D）入侵检测系统在发现入侵后，无法及时做出响应，包括切断网络连接、记录事件和报警等

43、特洛伊木马与远程控制软件的区别在于木马使用了什么技术（C）
（A）远程登录技术
（B）远程控制技术
（C）隐藏技术
（D）监视技术

44、实现调整蠕虫行为、更新其它功能模块、控制被感染计算机功能的是哪个蠕虫程序扩展功能模块（D）
（A）隐藏模块
（B）破坏模块
（C）通信模块
（D）控制模块

45、信息安全评估标准将计算机系统的安全分为 4 类，几个级别（C）
（A）5
（B）6
（C）7
（D）8

46、以下哪个不是密码系统包涵的要素（C）
（A）明文与密文空间
（B）密钥空间
（C）应用领域
（D）密码算法

47、GB/T 9387.2-1995 定义了 5 大类安全服务，提供这些服务的 8 种安全机制以及相应的开放系统互连的安全管理，并可根据具体系统适当地配置于 OSI 模型的七层协议中。
以下哪一项不是 P2DR 的含义项（A）
（A）认证
（B）保护
（C）探测
（D）反应

48、密钥分配中心的英文缩写是（A）

（A）KDC
（B）KMC
（C）KGC
（D）KSC

49、密钥管理不包括（B）
（A）生成、分配
（B）应用、认证
（C）存储、备份
（D）恢复、销毁。

50、1976 年，谁在著名的论文“密码学的新方向”中首次提出了公钥密码的概念，展示了在发端和收端不需要传输密钥的保密通信的可能性，从而开创了公钥密码学的新纪元（C）
（A）Kahn
（B）Rivest，Shamir 和 Adleman
（C）Diffie 和 Hellman
（D）Zimmerman

51、下列哪一个是常用的防范 NetBIOS 漏洞攻击的方法（A）
（A）利用 ICP/IP 筛选
（B）卸载 NetBIOS
（C）绑定 NetBIOS 与 TCP/IP 协议
（D）用防病毒软件

52、非法入侵定义了四类七个安全级别，由低到高分别是 D、C1、C2、B1、B2、B3、A1，并规定在下面那一个级别以上的操作系统必须具备审计功能，并记录日志（C）
（A）D
（B）C1
（C）C2
（D）B1

53、下面关于 Windows 2003 中的加密文件系统特点说法不正确的是（C）
（A）只有 NTFS 卷上的文件或文件夹才能被加密
（B）只有对文件实施加密的用户才能打开它
（C）不能共享加密文件
（D）如果用户将加密的文件复制或移动到 FAT 卷，此文件不会被解密

54、在 Linux 系统中，那一个命令用来设置和查看系统中创建文件时的缺省权限（B）
（A）config
（B）umask
（C）set

（D）creat

55、下列哪些不是计算机犯罪的特征（C）
（A）计算机本身的不可或缺性和不可替代性
（B）在某种意义上作为犯罪对象出现的特性
（C）行凶所使用的凶器

（D）明确了计算机犯罪侵犯的客体

56、下面是关于计算机病毒的两种论断，经判断（A）

（1）计算机病毒也是一种程序，它在某些条件上激活，起干扰破坏作用，并能传染到其他程序中去；

（2）计算机病毒只会破坏磁盘上的数据.

（A）只有(1)正确

（B）只有(2)正确

（C）(1)和(2)都正确

（D）(1)和(2)都不正确

57、通常所说的“病毒”是指（D）

（A）细菌感染

（B）生物病毒感染

（C）被损坏的程序

（D）特制的具有破坏性的程序

58、对于已感染了病毒的软盘，最彻底的清除病毒的方法是（D）

（A）用酒精将软盘消毒

（B）放在高压锅里煮

（C）将感染病毒的程序删除

（D）对软盘进行格式化

59、计算机病毒造成的危害是（B）

（A）使磁盘发霉

（B）破坏计算机系统

（C）使计算机内存芯片损坏

（D）使计算机系统突然掉电

60、计算机病毒的危害性表现在（B）

（A）能造成计算机器件永久性失效

（B）影响程序的执行，破坏用户数据与程序

（C）不影响计算机的运行速度

（D）不影响计算机的运算结果，不必采取措施

61、以下措施不能防止计算机病毒的是（A）

（A）软盘未写保护

（B）先用杀病毒软件将从别人机器上拷来的文件清查病毒

（C）不用来历不明的磁盘

（D）经常关注防病毒软件的版本升级情况，并尽量取得最高版本的防毒软件

62、计算机病毒主要是造成（C）损坏

（A）磁盘

（B）磁盘驱动器

（C）磁盘和其中的程序和数据

（D）程序和数据

63、文件型病毒传染的对象主要是（C）

（A）DBF
（B）PRG
（C）COM 和 EXE
（D）C

64、文件被感染上病毒之后，其基本特征是（C）
（A）文件不能被执行
（B）文件长度变短
（C）文件长度加长
（D）文件照常能执行

65、黑客攻击造成网络瘫痪，这种行为是（A）
（A）违法犯罪行为
（B）正常行为
（C）报复行为
（D）没有影响

66、信息系统安全保护法律规范的基本原则是（A）
（A）谁主管谁负责的原则、突出重点的原则、预防为主的原则、安全审计的原则和风险管理的原则
（B）突出重点的原则、预防为主的原则、安全审计的原则和风险管理的原则
（C）谁主管谁负责的原则、预防为主的原则、安全审计的原则和风险管理的原则
（D）谁主管谁负责的原则、突出重点的原则、安全审计的原则和风险管理的原则

67、计算机信息系统可信计算基能创建和维护受保护客体的访问审计跟踪记录，并能阻止非授权的用户对它访问或破坏，这种做法是（A）
（A）审计
（B）检查
（C）统计
（D）术管理

68、编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码是（B）
（A）计算机程序
（B）计算机病毒
（C）计算机游戏
（D）计算机系统

69、使网络服务器中充斥着大量要求回复的信息，消耗带宽，导致网络或系统停止正常服务，这属于什么攻击类型？（A）
（A）拒绝服务
（B）文件共享
（C）BIND 漏洞
（D）远程过程调用

70、为了防御网络监听，最常用的方法是（B）
（A）采用物理传输（非网络）
（B）信息加密

（C）无线网
（D）使用专线传输

71、向有限的空间输入超长的字符串是哪一种攻击手段？（A）
（A）缓冲区溢出
（B）网络监听
（C）拒绝服务
（D）IP 欺骗

72、主要用于加密机制的协议是(D)
（A）HTTP
（B）FTP
（C）TELNET
（D）SSL

73、用户收到了一封可疑的电子邮件,要求用户提供银行账户及密码,这是属于何种攻击手段？(B)
（A）缓存溢出攻击
（B）钓鱼攻击
（C）暗门攻击
（D）DDOS 攻击

74、Windows XP 系统能设置为在几次无效登录后锁定帐号,这可以防止(B)
（A）木马
（B）暴力攻击
（C）IP 欺骗
（D）缓存溢出攻击

75、在以下认证方式中，最常用的认证方式是（A）
（A）基于账户名 / 口令认证
（B）基于摘要算法认证
（C）基于 PKI 认证
（D）基于数据库认证

76、以下哪项不属于防止口令猜测的措施？(B)
（A）严格限定从一个给定的终端进行非法认证的次数
（B）确保口令不在终端上再现
（C）防止用户使用太短的口令
（D）使用机器产生的口令

77、下列不属于系统安全的技术是（B）
（A）防火墙
（B）加密狗
（C）认证
（D）防病毒

78、抵御电子邮箱入侵措施中，不正确的是（D）
（A）不用生日做密码

（B）不要使用少于 5 位的密码
（C）不要使用纯数字
（D）自己做服务器

79、不属于常见的危险密码是（D）
（A）跟用户名相同的密码
（B）使用生日作为密码
（C）只有 4 位数的密码
（D）10 位的综合型密码

80、不属于计算机病毒防治的策略的是（D）
（A）确认您手头常备一张真正“干净”的引导盘
（B）及时、可靠升级反病毒产品
（C）新购置的计算机软件也要进行病毒检测
（D）整理磁盘

81、针对数据包过滤和应用网关技术存在的缺点而引入的防火墙技术，这是（D）防火墙的特点
（A）包过滤型
（B）应用级网关型
（C）复合型防火墙
（D）代理服务型

82、当今 IT　的发展与安全投入，安全意识和安全手段之间形成（B）
（A）安全风险屏障
（B）安全风险缺口
（C）管理方式的变革
（D）管理方式的缺口

83、信息安全风险缺口是指（A）
（A）IT　的发展与安全投入，安全意识和安全手段的不平衡
（B）信息化中，信息不足产生的漏洞
（C）计算机网络运行，维护的漏洞
（D）计算中心的火灾隐患

84、信息网络安全的第三个时代（A）
（A）主机时代，专网时代，多网合一时代
（B）主机时代，PC 机时代，网络时代
（C）PC 机时代，网络时代，信息时代
（D）主机时代，专网时代，信息时代

85、网络安全在多网合一时代的脆弱性体现在（C）
（A）网络的脆弱性
（B）软件的脆弱性
（C）管理的脆弱性
（D）应用的脆弱性

86、网络攻击与防御处于不对称状态是因为（C）

(A)管理的脆弱性　(B)应用的脆弱性　(C)网络软，硬件的复杂性　(D)软件的脆弱性

87、风险评估的三个要素（D）
（A）政策，结构和技术
（B）组织，技术和信息
（C）硬件，软件和人
（D）资产，威胁和脆弱性

88、信息网络安全（风险）评估的方法（A）
（A）定性评估与定量评估相结合
（B）定性评估
（C）定量评估
（D）点评估

89、PDR 模型与访问控制的主要区别（A）
（A）PDR 把安全对象看作一个整体
（B）PDR 作为系统保护的第一道防线
（C）PDR 采用定性评估与定量评估相结合
（D）PDR 的关键因素是人

90、信息安全中 PDR 模型的关键因素是（A）
（A）人
（B）技术
（C）模型
（D）客体

91、以下关于 DOS 攻击的描述，哪句话是正确的？（C）
（A）不需要侵入受攻击的系统
（B）以窃取目标系统上的机密信息为目的
（C）导致目标系统无法处理正常用户的请求
（D）如果目标系统没有漏洞，远程攻击就不可能成功

92、许多黑客攻击都是利用软件实现中的缓冲区溢出的漏洞，对于这一威胁，最可靠的解决方案是什么？（C）
（A）安装防火墙
（B）安装入侵检测系统
（C）给系统安装最新的补丁
（D）安装防病毒软件

93、下面哪个功能属于操作系统中的安全功能（C）
（A）控制用户的作业排序和运行
（B）实现主机和外设的并行处理以及异常情况的处理
（C）保护系统程序和作业，禁止不合要求的对程序和数据的访问
（D）对计算机用户访问系统和资源的情况进行记录

94、下面哪个功能属于操作系统中的日志记录功能（D）
（A）控制用户的作业排序和运行
（B）以合理的方式处理错误事件，而不至于影响其他程序的正常运行

（C）保护系统程序和作业，禁止不合要求的对程序和数据的访问
（D）对计算机用户访问系统和资源的情况进行记录

95、下面哪一个情景属于身份验证（Authentication）过程（A）
（A）用户依照系统提示输入用户名和口令
（B）用户在网络上共享了自己编写的一份 Office 文档，并设定哪些用户可以阅读，哪些用户可以修改
（C）用户使用加密软件对自己编写的 Office 文档进行加密，以阻止其他人得到这份拷贝后看到文档中的内容
（D）某个人尝试登录到你的计算机中，但是口令输入的不对，系统提示口令错误，并将这次失败的登录过程纪录在系统日志中

96、下面哪一个情景属于授权（Authorization）（B）
（A）用户依照系统提示输入用户名和口令
（B）用户在网络上共享了自己编写的一份 Office 文档，并设定哪些用户可以阅读，哪些用户可以修改
（C）用户使用加密软件对自己编写的 Office 文档进行加密，以阻止其他人得到这份拷贝后看到文档中的内容
（D）某个人尝试登录到你的计算机中，但是口令输入的不对，系统提示口令错误，并将这次失败的登录过程纪录在系统日志中

97、下面哪一个情景属于审计（Audit）（D）
（A）用户依照系统提示输入用户名和口令
（B）用户在网络上共享了自己编写的一份 Office 文档，并设定哪些用户可以阅读，哪些用户可以修改
（C）用户使用加密软件对自己编写的 Office 文档进行加密，以阻止其他人得到这份拷贝后看到文档中的内容
（D）某个人尝试登录到你的计算机中，但是口令输入的不对，系统提示口令错误，并将这次失败的登录过程纪录在系统日志中

98、黑客的主要攻击手段包括（A）
（A）社会工程攻击、蛮力攻击和技术攻击
（B）人类工程攻击、武力攻击及技术攻击
（C）社会工程攻击、系统攻击及技术攻击
（D）人类工程攻击、蛮力攻击和技术攻击

99、从统计的情况看，造成危害最大的黑客攻击是（C）
（A）漏洞攻击
（B）蠕虫攻击
（C）病毒攻击
（D）口令破解

100、口令攻击的主要目的是（B）
（A）获取口令破坏系统
（B）获取口令进入系统
（C）以上都不是
（D）以上都是

101、计算机紧急应急小组的简称是（A）
（A）CERT
（B）FIRST
（C）SANA
（D）INSPC

102、邮件炸弹攻击主要是（B）
（A）破坏被攻击者邮件服务器
（B）添满被攻击者邮箱
（C）破坏被攻击者邮件客户端
（D）破坏被攻击者接收的邮件

103、逻辑炸弹通常是通过（B）
（A）必须远程控制启动执行，实施破坏
（B）指定条件或外来触发启动执行，实施破坏
（C）通过管理员控制启动执行，实施破坏
（D）来机自启，实施破坏

104、扫描工具（C）
（A）只能作为攻击工具
（B）只能作为防范工具
（C）既可作为攻击工具也可以作为防范工具
（D）只能够扫描主机、服务端口

105、DDOS 攻击是利用（C）进行攻击
（A）其他网络
（B）通讯握手过程问题
（C）中间代理
（D）网络时间

106、黑客造成的主要安全隐患包括（A）
（A）破坏系统、窃取信息及伪造信息
（B）攻击系统、获取信息及假冒信息
（C）进入系统、损毁信息及谣传信息
（D）窥视系统、篡改信息及发布信息

107、从统计的资料看，内部攻击是网络攻击的（B）
（A）次要攻击
（B）最主要攻击
（C）不是攻击源
（D）无关

108、传入我国的第一例计算机病毒是（B）
（A）大麻病毒
（B）小球病毒
（C）1575 病毒
（D）米开朗基罗病毒

109、我国是在____年出现第一例计算机病毒(C)
(A)1980　　(B)1983　　(C)1988　　(D)1977

110、1994 年我国颁布的第一个与信息安全有关的法规是（D）
（A）国际互联网管理备案规定
（B）计算机病毒防治管理办法
（C）网吧管理规定
（D）中华人民共和国计算机信息系统安全保护条例

111、网页病毒主要通过以下途径传播（C）
（A）邮件
（B）文件交换
（C）网络浏览
（D）光盘

112、《计算机病毒防治管理办法》是在哪一年颁布的（C）
（A）1994
（B）1997
（C）2000
（D）1998

113、边界防范的根本作用是（C）
（A）对系统工作情况进行检验与控制，防止外部非法入侵
（B）对网络运行状况进行检验与控制，防止外部非法入侵
（C）对访问合法性进行检验与控制，防止外部非法入侵
（D）对网络流量进行控制，防止外部非法入侵

114、路由设置是边界防范的（A）
（A）基本手段之一
（B）根本手段
（C）无效手段
（D）最有效手段

115、网络物理隔离是指（C）
（A）两个网络间链路层在任何时刻不能直接通讯
（B）两个网络间网络层在任何时刻不能直接通讯
（C）两个网络间链路层、网络层在任何时刻都不能直接通讯
（D）两个完全独立的网络体系

116、VPN 是指（A）
（A）虚拟的专用网络
（B）虚拟的协议网络
（C）虚拟的包过滤网络
（D）虚拟的公共网络

117、带 VPN 的防火墙的基本原理流程是（A）
（A）先进行流量检查

（B）先进行协议检查
（C）先进行合法性检查
（D）先进行地址检查

118、防火墙主要可以分为（A）
（A）包过滤型、代理性、混合型
（B）包过滤型、系统代理型、应用代理型
（C）包过滤型、内容过滤型、混合型
（D）包过滤型、行为检测型、应用代理型

119、VPN 通常用于建立（A）之间的安全通道
（A）总部与分支机构、与合作伙伴、与移动办公用户
（B）客户与客户、与合作伙伴、与远程用户
（C）总部与分支机构、与外部网站、与移动办公用户
（D）用户与用户之间

120、在安全区域划分中 DMZ　区通常用做（B）
（A）数据区
（B）对外服务区
（C）重要业务区
（D）安全网络区

121、目前用户局域网内部区域划分通常通过（B）实现
（A）物理隔离
（B）Vlan（虚拟局域网）划分
（C）防火墙防范
（D）路由器划分

122、防火墙的部署（B）
（A）只需要在与 Internet　相连接的出入口设置
（B）在需要保护局域网络的所有出入口设置
（C）需要在出入口和网段之间进行部署
（D）两个不同网段间进行部署

123、防火墙是一个（A）
（A）分离器、限制器、分析器
（B）隔离器、控制器、分析器
（C）分离器、控制器、解析器
（D）分离器、检测器、隔离器

124、目前的防火墙防范主要是（B）
（A）主动防范
（B）被动防范
（C）不一定
（D）反跟踪防范

125、IP 地址欺骗通常是（A）
（A）黑客的攻击手段

（B）防火墙的专门技术
（C）IP 通讯的一种模式
（D）又叫 ARP 欺骗

126、现代主动安全防御的主要手段是（A）
（A）探测、预警、监视、警报
（B）嘹望、烟火、巡更、敲梆
（C）调查、报告、分析、警报
（D）探测、报告、分析、警报

127、计算机信息系统的安全保护，应当保障（A），运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。
（A）计算机及其相关的和配套的设备、设施(含网络)的安全
（B）计算机的安全
（C）计算机硬件的系统安全
（D）计算机操作人员的安全

128、关于计算机病毒知识，叙述不正确的是（D）
（A）计算机病毒是人为制造的一种破坏性程序
（B）大多数病毒程序具有自身复制功能
（C）安装防病毒卡,并不能完全杜绝病毒的侵入
（D）不使用来历不明的软件是防止病毒侵入的有效措施

129、木马程序一般是指潜藏在用户电脑中带有恶意性质的（A），利用它可以在用户不知情的情况下窃取用户联网电脑上的重要数据信息。
（A）远程控制软件
（B）计算机操作系统
（C）木头做的马
（D）硬盘浏览软件

130、为了防止各种各样的病毒对计算机系统造成危害，可以在计算机上安装防病毒软件，并注意及时（B），以保证能防止和查杀新近出现的病毒。
（A）分析
（B）升级
（C）检查
（D）报警

131、企业重要数据要及时进行（C），以防出现以外情况导致数据丢失。
（A）杀毒
（B）加密
（C）备份
（D）存储

132、操作系统中哪种格式具有文件加密功能（A）
（A）NTFS
（B）FAT32
（C）FAT
（C）LINUX

133、计算机病毒通常容易感染扩展名为（A）的文件
（A）EXE、COM
（B）EXE、SYS
（C）BAT、BAK
（D）SYS、HLP

134、下列不属于计算机病毒症状的是（B）
（A）系统有效存储空间变小
（B）文件打不开
（C）系统启动时的引导过程变慢
（D）无端丢失数据

135、以下关于 DOS 攻击的描述，哪句话是正确的？（C）
（A）不需要侵入受攻击的系统
（B）以窃取目标系统上的机密信息为目的
（C）导致目标系统无法处理正常用户的请求
（D）如果目标系统没有漏洞，远程攻击就不可能成功

136、许多黑客攻击都是利用软件实现中的缓冲区溢出的漏洞，对于这一威胁，最可靠的解决方案是什么？（C）
（A）安装防火墙
（B）安装入侵检测系统
（C）给系统安装最新的补丁
（D）安装防病毒软件

137、下面哪个功能属于操作系统中的安全功能（C）
（A）控制用户的作业排序和运行
（B）实现主机和外设的并行处理以及异常情况的处理
（C）保护系统程序和作业，禁止不合要求的对程序和数据的访问
（D）对计算机用户访问系统和资源的情况进行记录

138、下面哪个功能属于操作系统中的日志记录功能（D）
（A）控制用户的作业排序和运行
（B）以合理的方式处理错误事件，而不至于影响其他程序的正常运行
（C）保护系统程序和作业，禁止不合要求的对程序和数据的访问
（D）对计算机用户访问系统和资源的情况进行记录

139、Windows NT 提供的分布式安全环境又被称为（A）
（A）域（Domain）
（B）工作组
（C）对等网
（D）安全网

140、下面哪一个情景属于身份验证（Authentication）过程（A）
（A）用户依照系统提示输入用户名和口令
（B）用户在网络上共享了自己编写的一份 Office 文档，并设定哪些用户可以阅读，哪些用户可以修改
（C）用户使用加密软件对自己编写的 Office 文档进行加密，以阻止其他人得到这份拷贝后

看到文档中的内容
（D）某个人尝试登录到你的计算机中，但是口令输入的不对，系统提示口令错误，并将这次失败的登录过程纪录在系统日志中

141、下面哪一个情景属于授权（Authorization）（B）
（A）用户依照系统提示输入用户名和口令
（B）用户在网络上共享了自己编写的一份 Office 文档，并设定哪些用户可以阅读，哪些用户可以修改
（C）用户使用加密软件对自己编写的 Office 文档进行加密，以阻止其他人得到这份拷贝后看到文档中的内容
（D）某个人尝试登录到你的计算机中，但是口令输入的不对，系统提示口令错误，并将这次失败的登录过程纪录在系统日志中

142、下面哪一个情景属于审计（Audit）（D）
（A）用户依照系统提示输入用户名和口令
（B）用户在网络上共享了自己编写的一份 Office 文档，并设定哪些用户可以阅读，哪些用户可以修改
（C）用户使用加密软件对自己编写的 Office 文档进行加密，以阻止其他人得到这份拷贝后看到文档中的内容
（D）某个人尝试登录到你的计算机中，但是口令输入的不对，系统提示口令错误，并将这次失败的登录过程纪录在系统日志中

143、以网络为本的知识文明人们所关心的主要安全是（C）
（A）人身安全
（B）社会安全
（C）信息安全

144、第一次出现"HACKER"这个词是在（B）
（A）BELL 实验室
（B）麻省理工 AI 实验室
（C）AT&T 实验室

145、可能给系统造成影响或者破坏的人包括（A）
（A）所有网络与信息系统使用者
（B）只有黑客
（C）只有跨客

146、黑客的主要攻击手段包括（A）
（A）社会工程攻击、蛮力攻击和技术攻击
（B）人类工程攻击、武力攻击及技术攻击
（C）社会工程攻击、系统攻击及技术攻击

147、从统计的情况看，造成危害最大的黑客攻击是（C）
（A）漏洞攻击
（B）蠕虫攻击
（C）病毒攻击

148、第一个计算机病毒出现在（B）

（A）40 年代
（B）70　年代
（C）90 年代

149、口令攻击的主要目的是（B）
（A）获取口令破坏系统
（B）获取口令进入系统
（C）仅获取口令没有用途

150、通过口令使用习惯调查发现有大约___%的人使用的口令长度低于 5 个字符的（B）
（A）50.5
（B）51.5
（C）52.5

151、通常一个三个字符的口令破解需要（B）
（A）18 毫秒
（B）18 秒
（C）18 分

152、黑色星期四是指（A）
（A）1998 年 11 月 3 日星期四
（B）1999 年 6 月 24 日星期四
（C）2000 年 4 月 13 日星期四

153、大家所认为的对 Internet 安全技术进行研究是从_____时候开始的 （C）
（A）Internet　诞生
（B）第一个计算机病毒出现
（C）黑色星期四

154、计算机紧急应急小组的简称是（A）
（A）CERT
（B）FIRST
（C）SANA

155、邮件炸弹攻击主要是（B）
（A）破坏被攻击者邮件服务器
（B）添满被攻击者邮箱
（C）破坏被攻击者邮件客户端

156、逻辑炸弹通常是通过（B）
（A）必须远程控制启动执行，实施破坏
（B）指定条件或外来触发启动执行，实施破坏
（C）通过管理员控制启动执行，实施破坏

157、1996 年上海某寻呼台发生的逻辑炸弹事件，造事者被判"情节轻微，无罪释放"是因为（C）
（A）证据不足
（B）没有造成破坏
（C）法律不健全

158、扫描工具（C）
（A）只能作为攻击工具
（B）只能作为防范工具
（C）既可作为攻击工具也可以作为防范工具

159、DDOS 攻击是利用_____进行攻击（C）
（A）其他网络
（B）通讯握手过程问题
（C）中间代理

160、全国首例计算机入侵银行系统是通过（A）
（A）安装无限 MODEM 进行攻击
（B）通过内部系统进行攻击
（C）通过搭线进行攻击

161、黑客造成的主要安全隐患包括（A）
（A）破坏系统、窃取信息及伪造信息
（B）攻击系统、获取信息及假冒信息
（C）进入系统、损毁信息及谣传信息

162、从统计的资料看，内部攻击是网络攻击的（B）
（A）次要攻击
（B）最主要攻击
（C）不是攻击源

163、江泽民主席指出信息战的主要形式是（A）
（A）电子战和计算机网络战
（B）信息攻击和网络攻击
（C）系统破坏和信息破坏

164、广义地说，信息战是指敌对双方为达成各自的国家战略目标，为夺取_____在等各个领域的信息优势，运用信息和信息技术手段而展开的信息斗争（B）
（A）政治、经济、国防、领土、文化、外交
（B）政治、经济、军事、科技、文化、外交
（C）网络、经济、信息、科技、文化、外交

165、狭义地说，信息战是指军事领域里的信息斗争。它是敌对双方为争夺信息的_____，通过利用、破坏敌方和保护己方的信息、信息系统而采取的作战形式　（C）
（A）占有权、控制权和制造权
（B）保存权、制造权和使用权
（C）获取权、控制权和使用权

166、信息战的战争危害较常规战争的危害（C）
（A）轻
（B）重
（C）不一定

167、信息战的军人身份确认较常规战争的军人身份确认（A）
（A）难

（B）易
（C）难说

168、互联网用户应在其网络正式联通之日起_____内，到公安机关办理国际联网备案手续（A）
（A）三十日　　（B）二十日　　（C）十五日　　（D）四十日

169、一般性的计算机安全事故和计算机违法案件可由_____受理（C）
（A）案发地市级公安机关公共信息网络安全监察部门
（B）案发地当地县级（区、市）公安机关治安部门。
（C）案发地当地县级（区、市）公安机关公共信息网络安全监察部门
（D）案发地当地公安派出所

170、计算机信息系统发生安全事故和案件，应当_____在内报告当地公安机关公共信息网络安全监察部门（D）
（A）8 小时
（B）48 小时
（C）36 小时
（D）24 小时

171、对计算机安全事故的原因的认定或确定由_____作出（B）
（A）人民法院
（B）公安机关
（C）发案单位
（D）以上都可以

172、对发生计算机安全事故和案件的计算机信息系统，如存在安全隐患的，_____应当要求限期整改（B）
（A）人民法院
（B）公安机关
（C）发案单位的主管部门
（D）以上都可以

173、传入我国的第一例计算机病毒是（B）
（A）大麻病毒
（B）小球病毒
（C）1575 病毒
（D）米开朗基罗病毒

174、我国是在____年出现第一例计算机病毒（C）
（A）1980
（B）1983
（C）1988
（D）1977

175、计算机病毒是（A）
（A）计算机程序
（B）数据
（C）临时文件

（D）应用软件

176、1994 年我国颁布的第一个与信息安全有关的法规是（D）
（A）国际互联网管理备案规定
（B）计算机病毒防治管理办法
（C）网吧管理规定
（D）中华人民共和国计算机信息系统安全保护条例

177、网页病毒主要通过以下途径传播（C）
（A）邮件
（B）文件交换
（C）网络浏览
（D）光盘

178、故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，将受到____处罚（A）
（A）处五年以下有期徒刑或者拘役
（B）拘留
（C）罚款
（D）警告

179、计算机病毒防治产品根据____标准进行检验（A）
（A）计算机病毒防治产品评级准测
（B）计算机病毒防治管理办法
（C）基于 DOS 系统的安全评级准则
（D）计算机病毒防治产品检验标准

180、《计算机病毒防治管理办法》是在哪一年颁布的（C）
（A）1994
（B）1997
（C）2000
（D）1998

181、边界防范的根本作用是（C）
（A）对系统工作情况进行检验与控制，防止外部非法入侵
（B）对网络运行状况进行检验与控制，防止外部非法入侵
（C）对访问合法性进行检验与控制，防止外部非法入侵

182、路由设置是边界防范的（A）
（A）基本手段之一
（B）根本手段
（C）无效手段

183、网络物理隔离是指（C）
（A）两个网络间链路层在任何时刻不能直接通讯
（B）两个网络间网络层在任何时刻不能直接通讯
（C）两个网络间链路层、网络层在任何时刻都不能直接通讯

184、VPN 是指（A）

（A）虚拟的专用网络
（B）虚拟的协议网络
（C）虚拟的包过滤网络

185、带 VPN 的防火墙的基本原理流程是（A）
（A）先进行流量检查
（B）先进行协议检查
（C）先进行合法性检查

186、防火墙主要可以分为（A）
（A）包过滤型、代理性、混合型
（B）包过滤型、系统代理型、应用代理型
（C）包过滤型、内容过滤型、混合型

187、VPN 通常用于建立____之间的安全通道（A）
（A）总部与分支机构、与合作伙伴、与移动办公用户
（B）客户与客户、与合作伙伴、与远程用户
（C）总部与分支机构、与外部网站、与移动办公用户

188、在安全区域划分中 DMZ　区通常用做（B）
（A）数据区
（B）对外服务区
（C）重要业务区

189、目前用户局域网内部区域划分通常通过____实现（B）
（A）物理隔离
（B）Vlan（虚拟局域网）划分
（C）防火墙防范

190、防火墙的部署（B）
（A）只需要在与 Internet　相连接的出入口设置
（B）在需要保护局域网络的所有出入口设置
（C）需要在出入口和网段之间进行部署

191、防火墙是一个（A）
（A）分离器、限制器、分析器
（B）隔离器、控制器、分析器
（C）分离器、控制器、解析器

192、目前的防火墙防范主要是（B）
（A）主动防范
（B）被动防范
（C）不一定

193、目前的防火墙防范主要是（B）
（A）主动防范
（B）被动防范
（C）不一定

194、IP 地址欺骗通常是（A）
（A）黑客的攻击手段
（B）防火墙的专门技术
（C）IP　通讯的一种模式

195、现代主动安全防御的主要手段是（A）
（A）探测、预警、监视、警报
（B）嘹望、烟火、巡更、敲梆
（C）调查、报告、分析、警报

196、计算机信息系统的安全保护，应当保障（A），运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。
（A）计算机及其相关的和配套的设备、设施(含网络)的安全
（B）计算机的安全
（C）计算机硬件的系统安全
（D）计算机操作人员的安全

197、当前奇瑞股份有限公司所使用的杀毒软件是：（C）
（A）瑞星企业版
（B）卡巴斯基
（C）趋势防病毒网络墙
（D）诺顿企业版

198、计算机病毒是指：（C）
（A）带细菌的磁盘
（B）已损坏的磁盘
（C）具有破坏性的特制程序
（D）被破坏了的程序

199、计算机连网的主要目的是（A）
（A）资源共享
（B）共用一个硬盘
（C）节省经费
（D）提高可靠性

200、关于计算机病毒知识，叙述不正确的是（D）
（A）计算机病毒是人为制造的一种破坏性程序
（B）大多数病毒程序具有自身复制功能
（C）安装防病毒卡,并不能完全杜绝病毒的侵入
（D）不使用来历不明的软件是防止病毒侵入的有效措施

多选题（220 题）

1、SSL 协议的基本安全服务有哪些（ABD）
（A）加密服务
（B）认证服务
（C）隧道服务

（D）数据完整性

2、SSL 协议由以下哪几个协议组成（CD）
（A）会话协议
（B）Internet 密钥交换协议 IKE
（C）握手协议
（D）记录协议

3、SSL 握手阶段，客户和服务器依次完成的阶段会话是（BDCA）
（A）建立安全连接，发送应用层数据
（B）建立安全协商
（C）客户鉴别与密钥交换
（D）服务器鉴别与密钥交换

4、对文件和对象的审核，正确的项是（ABD）
（A）文件和对象访问成功和失败
（B）用户及组管理成功和失败
（C）文件名更改成功和失败
（D）安全规则更改成功和失败

5、下列（ABCD）项属于用户权限管理的基本原则
（A）拒绝优先
（B）权限最小化
（C）权限累加
（D）权限继承

6、下列（ABCD）文件系统是 Linux2.6 内核支持的类型
（A）NTFS
（B）ext2
（C）ext3
（D）NFS

7、关于/etc/shadow 文件，下列说法正确的是（BC）
（A）存储着用户主目录
（B）存储着加密后的用户口令
（C）只有 root 用户才能读取
（D）存储着用户 ID

8、（ACD）是 SELinux 的三种工作模式
（A）enforcing
（B）impossible
（C）permissive
（D）disabled

9、与启用了 SELinux 保护的 Linux 系统相比，Linux 系统的不安全性表现在（BCD）
（A）系统服务存在诸如漏洞等不安全因素
（B）root 用户操作不会受到约束
（C）文件访问权限划分不够细

（D）文件目录所有者可以对文件进行所有的操作

10、案例分析（Linux 环境）

在启用 SELinux 前，以 root 用户身份创建 Web 服务（Apache 服务器）虚拟目录，并赋予虚拟目录读、写与执行访问权限。在 Web 服务正常工作的前提下，启动 SELinux，使用 Web 浏览器访问虚拟目录中的页面，访问失败。可能导致访问失败的原因有（AC）。

（A）Apache 系统用户对虚拟目录缺少读取与执行权限
（B）SELinux 使用了 permissive 工作模式
（C）虚拟目录未设置 httpd_sys_content_t 安全上下文
（D）SELinux 应用了 strict 策略

11、属于 Web 服务器安全措施的是（ABC）
（A）保证注册账户的时效性
（B）删除死账户
（C）强制用户使用不易破解的密码
（D）所有用户使用一次性密码

12、下列哪种网络技术可以防御网络监听（AB）
（A）信息加密技术
（B）VPN 技术
（C）防火墙技术
（D）入侵检测技术

13、IPsec 封装安全载荷（ESP）是插入 IP 数据包内的一个协议头，以便为 IP 提供（ABCD）
（A）数据机密性
（B）数据源认证
（C）抗重播保护
（D）数据完整性

14、目前虚拟专用网络的解决方案有（ACD）
（A）IPSec
（B）Kerberos
（C）PPTP
（D）OpenVPN

15、公钥基础设施（PKI）由以下部分组成（AD）
（A）认证中心，登记中心
（B）质检中心
（C）咨询服务
（D）证书持有者，用户，证书库

16、在一个典型的 Kerberos 领域必须包含的角色有（BC）
（A）域服务器
（B）主 KDC
（C）从 KDC
（D）应用服务器

17、能够实现安全 telnet 操作的方法是（BD）

（A）SSL
（B）kerberos 化 telnet 服务器
（C）rlogin
（D）SSH

18、Linux 系统中，下列哪些方法可以限制客户端访问 Web 服务（ABD）
（A）配置 http.conf 文件
（B）配置 xinet
（C）关闭 Web 服务
（D）配置防火墙规则

19、与 NetBIOS 主机发现相比，ARP 主机发现的优势是（BC）
（A）多信息
（B）效率高
（C）系统无关
（D）可实现跨网段发现

20、网卡是网络中主机接收发送数据的硬件设备。网卡接收数据的几种工作模式（ABCD）
（A）广播模式
（B）组播模式
（C）直接模式
（D）混杂模式

21、攻击者搜集目标信息一般有四个阶段（BADC）
（A）找到活动主机
（B）确定网络地址范围
（C）分析端口服务
（D）识别操作系统

22、与基于 TCP/IP 协议栈捕获数据包相比，基于 Winpcap 捕获数据包可实现（AD）
（A）捕获链路层数据
（B）捕获网络层数据
（C）自动校验数据
（D）不进行数据校验

23、通过（BCD）方法可以防范缓冲区溢出
（A）细划文件执行权限
（B）安全编程
（C）使用支持数据执行保护（DEP）的系统
（D）优化编译器设置项

24、关于 SYN Flood 攻击，说法正确的是（AC）
（A）发送大量的伪造的 TCP 连接请求
（B）利用 TCP 协议漏洞进行攻击
（C）是拒绝服务攻击的一种
（D）仅对 Windows 服务器起作用

25、TFN2K 是知名的分布式拒绝服务攻击工具，它由（CD）部分组成

（A）监控端
（B）传感终端
（C）主控端
（D）代理端

26、关于 Smurf 攻击，说法正确的是（ACD）
（A）拒绝服务攻击的一种
（B）基于 IGMP 协议实现
（C）受害者被 IP 欺骗
（D）通过 IP/MAC 地址绑定可防御此攻击

27、关于 ARP 协议，说法错误的是（BD）
（A）不能够跨越路由器
（B）位于 TCP/IP 模型的第二层
（C）不具备认证机制是其致使缺陷
（D）承载 ARP 数据的链路地址只能是广播地址

28、常用的口令入侵手段有（ABCD）
（A）通过网络监听
（B）利用专门软件进行口令破解
（C）利用系统的漏洞
（D）利用系统管理员的失误

29、木马与病毒的区别在于（BCD）
（A）非法性
（B）目的性
（C）传播性
（D）复制性

30、关于网页木马，下列说法错误的是（AB）
（A）只要浏览了嵌入木马的网页就会感染木马
（B）网页木马仅对 IE 浏览器有效
（C）通过安装浏览器插件可以有效地防止网页木马
（D）禁止 IE 浏览器运行 vb、Javascript 脚本可防止网页木马

31、安全的网络必须具备哪些特征（ABCD）
（A）保密性
（B）完整性
（C）可用性
（D）可控性

32、iptables 防火墙可实现（ABC）功能
（A）包过滤
（B）状态检测
（C）NAT
（D）应用代理

33、iptables 防火墙工作在 ISO 七层模型的第（ABC）层

（A）二
（B）三
（C）四
（D）五

34、默认情况下，Linux iptables 的 filter 表由（ABD）规则链组成。
（A）INPUT
（B）OUTPUT
（C）NAT
（D）FORWARD

35、案例分析
FTP 服务（服务端口默认）与 iptables 运行于同台主机，iptables 默认策略禁止与本地进程进行通信。确保客户能够正常访问 FTP 服务，下列 iptables 规则正确的有（BC）。
（A）iptables -A INPUT -p tcp --dport 21 -j ACCEPT
（B）iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
（C）iptables -A INPUT -p tcp --dport 21 -j ACCEPT
iptables -A INPUT -m state --state NEW -j ACCEPT
（D）iptables -A INPUT -p tcp --dport 20 -j ACCEPT

36、按技术类型划分，NAT 有（BCD）几种类型
（A）通用 NAT
（B）静态 NAT
（C）动态 NAT
（D）网络地址端口转换 NAPT

37、关于基于网络的入侵检测系统（NIDS），下列说法错误的是（CD）
（A）与操作系统无关
（B）需要快速处理数据的能力
（C）可发现特定主机的异常行为
（D）可发现未知的网络异常行为

38、Snort 可实现的功能有（ABD）
（A）嗅探网络数据包
（B）记录网络数据包
（C）预测未知的网络异常行为
（D）检测网络异常行为

39、Snort 体系由 4 部分组成，按功能实现的先后顺序，它们是（CADB）
（A）预处理器
（B）报警或日志
（C）数据包嗅探
（D）检测引擎

40、下列哪些不属于 Snort 预置的规则动作（AD）
（A）detect
（B）alert
（C）dynamic/activate

（D）record

41、Snort 规则头中包含的检测信息有（ACD）
（A）协议类型
（B）数据包长度
（C）数据方向
（D）源、目的信息

42、VPN 采用了（ABCD）技术，来保证数据传输的安全性
（A）隧道技术
（B）加解密技术
（C）密钥管理技术
（D）身份认证技术

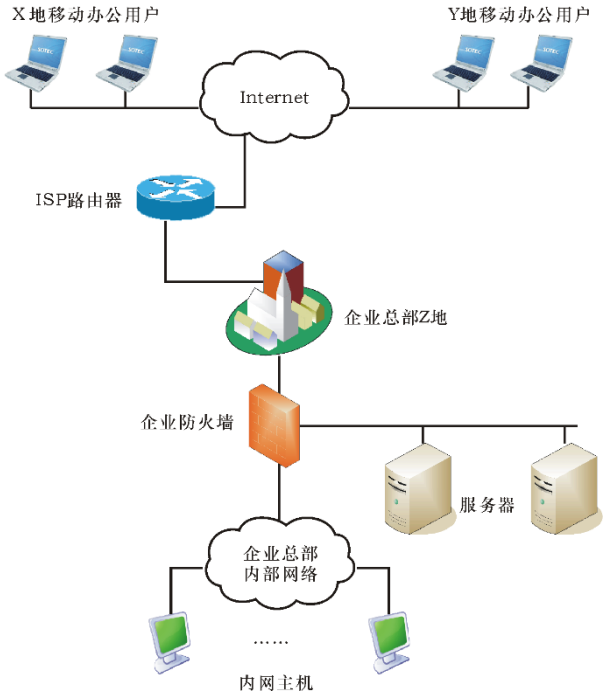
43、下列属于二层隧道协议的有（AB）
（A）PPTP
（B）L2TP
（C）IPSec
（D）GRE

44、下列属于三层隧道协议的有（CD）
（A）PPTP
（B）L2TP
（C）IPSec
（D）GRE

45、与第二层隧道协议相比，第三层隧道协议的优点在于（ACD）
（A）安全性
（B）支持多种协议封装
（C）扩展性
（D）可靠性

46、PPTP 数据包的接收处理过程（CABD）
（A）处理并去除 IP 报头
（B）处理并去除 GRE 和 PPP 报头
（C）处理并去除数据链路层报头和报尾
（D）处理 PPP 有效负载

47、案例分析
如下图所示：



为搭建高效、安全的企业网络环境，需在企业防火墙上部署（AB）策略

（A）允许内网主机访问 Internet

（B）允许 Internet 访问服务器

（C）允许服务器访问内网主机

（D）允许 Internet 访问内网主机

48、关于 OpenVPN 下列说法正确的是（ABD）

（A）它是一个开源项目

（B）它是一个 SSL VPN 解决方案

（C）它只能对特定服务的应用层数据流形成“隧道”

（D）它基于 OpenSSL 库实现

49、关于蜜罐下列说法错误的是（CD）

（A）蜜罐是一种毫无产品价值可言的安全资源

（B）任何发送给蜜罐的活动都应受到怀疑

（C）蜜罐提供了一种防御机制

（D）蜜罐具有固定的表现形态

50、蜜罐可具有同（ABCD）相似的功能

（A）包过滤防火墙

（B）入侵检测系统

（C）网络嗅探器

（D）主机/网络仿真系统

51、交互级别可为我们提供了一种可以对蜜罐进行测试和比较的标尺。交互级别分为(ABCD)

（A）低交互级别

（B）中交互级别

（C）高交互级别

（D）蜜网

52、防御木马和后门的方法有哪些（BCD）
（A）决不浏览不知名的网站
（B）定期端口扫描
（C）安装防火墙与杀毒软件
（D）勤打系统升级补丁

53、后门为攻击者提供的访问类型包括（ABCD）
（A）本地权限的提升
（B）单个命令的远程执行
（C）远程命令解释器访问
（D）远程控制 GUI

54、最常用的修改特征码方法有（BD）
（A）修改入口点
（B）直接修改法
（C）添加花指令
（D）跳转修改法

55、Word 宏病毒主要寄生在哪几个宏中（ABD）
（A）AutoNew
（B）AutoOpen
（C）AutoExec
（D）AutoClose

56、PE 文件的主要加载过程（DCAEB）
（A）PE 加载器读取段表中的信息，并采用文件映射方法将这些段映射到内存，同时附上段属性
（B）按照 PE 文件的程序入口指针所指地址执行程序
（C）PE 加载器检查 PE 头的有效性
（D）PE 加载器检查 DOS MZ 头里的 PE 头偏移量 e_lfanew，并跳至 PE 头
（E）PE 加载器按文件的实际加载基址修改引入表等逻辑部分

57、网页中恶意代码的作用包括下列哪几项（ABCD）
（A）消耗系统资源
（B）非法向用户的硬盘写入文件
（C）IE 泄密
（D）利用邮件非法安装木马

58、“爱虫”病毒运行后，会在系统中留下哪些文件（BCD）
（A）\WINDOWS\system32\eventquery.vbs
（B）\WINDOWS\Win32DLL.vbs
（C）\system\MSKernel.vbs
（D）\system\LOVE-LETTER-FOR-YOU.TXT.vbs

59、目前主流的服务器容错技术包括哪些（ACD）
（A）服务器集群技术
（B）RAID
（C）双机热备份技术

（D）单机容错技术

60、数字水印的基特性有（ABC）
（A）隐蔽性
（B）安全性
（C）鲁棒性
（D）不可否认性

61、人脸检测方法包括（ABCD）
（A）神经网络方法
（B）相关性模板方法
（C）子空间法
（D）基于知识的人脸检测

62、BOF（Back Officer Friendly）是一种低交互度的蜜罐，关于 BOF 说法错误的是（BC）
（A）BOF 只能监听那些当前没被占用的端口
（B）BOF 模拟了 7 种 TCP 服务
（C）BOF 主要作为威慑型蜜罐使用
（D）BOF 可针对 HTTP 请求完成 TCP 三次握手

63、作为低交互度的蜜罐，Honeyd 实现了对（ABC）进行模拟仿真
（A）应用服务
（B）主机系统
（C）网络拓扑
（D）以上都不是

64、按照部署目的蜜罐可分为（AB）
（A）研究型蜜罐
（B）产品型蜜罐
（C）封闭型蜜罐
（D）开放型蜜罐

65、下列网络安全工具，可作为蜜罐工具使用的是（ABCD）
（A）BOF
（B）Honeyd
（C）Netcat
（D）Snort

66、关于 Honeyd 下列说法正确的是（ABD）
（A）Honeyd 可以同时模拟不同的操作系统
（B）Honeyd 可以检测任意 TCP 端口上的连接
（C）Honeyd 不能够模拟路由器
（D）在遭受攻击时，Honeyd 会承担起受害者的身份

67、案例分析
运行 Honeyd，仿真“Microsoft Windows XP Home Edition”主机系统，并开放 80/tcp 端口，其它服务关闭，虚拟主机 IP 地址 192.168.0.10。在 Honeyd 配置文件中用到的配置语法有（BCD）

（A）run
（B）create
（C）add
（D）bind

68、Honeyd 可用于仿真网络的特性有（BC）
（A）支持操作系统仿真
（B）支持多重路由仿真
（C）支持网络延迟、丢包率和带宽仿真
（D）支持 IP 协议栈仿真

69、我们国家的密码分组有（ABCD）
（A）核心密码
（B）普通密码
（C）商用密码
（D）个人密码

70、对称密钥加密体制的缺点有（BD）
（A）密码算法简单
（B）收发双方持有相同密钥，密钥分配困难
（C）密文容易被破译
（D）不能方便地实现数字签名

71、密码体制的构成（ABCD）
（A）明文空间
（B）密文空间
（C）密钥空间
（D）加、解密算法

72、密码体制的分类（ABC）
（A）从加密密钥与解密密钥是否相等划分为对称密钥密码与非对称密钥密码
（B）从密钥的使用方式划分为序列密码和分组密码
（C）从密码的演变过程划分为典型密码和新型密码

73、古典密码的三种编码方法是（BCD）
（A）乘法
（B）置换
（C）代替
（D）加法

74、以 AES 作为加密算法开发出的文件加密软件系统具有的特点（ACD）
（A）具有文件加解密功能
（B）可确保密码后数据的真实性
（C）加密速度较快
（D）具有加解密速度统计功能

75、序列密码的分类（CD）
（A）非同步序列密码

（B）非自同步序列密码
（C）同步序列密码
（D）自同步序列密码

76、对称密钥加密算法中长度小于分组长度的数据块称为短块，解决短块加密问题的处理技术有（ABC）
（A）填充技术
（B）密文挪用技术
（C）序列加密技术
（D）块替换技术

77、非对称密钥密码的基本思想（ABCD）
（A）将密钥 K 一分为二，公钥 K_e 用来专门加密，私钥 K_d 专门用来解密，K_e 不等于 K_d
（B）由 K_e 不能计算机出 K_d，可以将 K_e 公开，使密钥分配变得简单
（C）由于 K_e 不等于 K_d，且由 K_e 不能计算机出 K_d，于是 K_d 成为用户的指纹
（D）用户应用 K_d 可以实现数字签名

78、使用公钥证书的主要好处有（BD）
（A）用户只要获得 CA 的公钥，就可以安全地认证其他用户的私钥
（B）用户只要获得 CA 的公钥，就可以安全地认证其他用户的公钥
（C）用户只要获得其他用户的证书，就可以获得其他用户的私钥
（D）用户只要获得其他用户的证书，就可以获得其他用户的公钥

79、下列组合中前者是传统分组密码，后者是非对称密钥密码的是（BC）
（A）DES、IDEA
（B）AES、RSA
（C）IDEA、ELGamal
（D）RC4、ECC

80、在 DES 算法 16 轮循环运算的每个轮次中，右半部分需要经过一系列的子加密过程，这个子加密过程也叫做 f 函数，它包括（ABCD）
（A）扩展置换
（B）异或运算
（C）S 盒置换
（D）直接置换

81、在公钥基础设施 PKI 中，CA 的作用是（ABCD）
（A）负责证书的签发、管理和撤销
（B）是所有注册用户所依赖的权威机构
（C）在给用户签发证书时要加上自己的签名，以保护证书信息的真实性
（D）为方便用户对证书进行验证，CA 也给自己签发证书

82、下列常用的 RAID 中，具有数据冗余能力的是（BCD）
（A）RAID 0
（B）RAID 1
（C）RAID 5
（D）RAID 0+5

83、一种完善的数字签名应满足以下（ABD）三个条件
（A）签名者事后不能抵赖自己的签名
（B）任何其他人不能伪造签名
（C）不可被攻击
（D）签名真伪是可以验证的

84、（CD）是 Hash 函数具有的功能
（A）加密明文
（B）独立完成数字签名
（C）错误检测能力
（D）辅助数字签名

85、目前广泛应用的是基于密码的认证技术，主要有（BCD）
（A）安全认证
（B）身份认证
（C）站点认证
（D）报文认证

86、认证和数字签名的区别（ACD）
（A）认证总是在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）认证能够验证收发双方的真实性，而数字签名只能验证发送方的真实性
（C）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
（D）数字签名具有发送方不能抵赖、接收方不能伪造和能够公开验证解决纠纷，而认证则不一定具备

87、典型病毒的生命周期包含以下（ABCD）阶段
（A）睡眠阶段
（B）传播阶段
（C）触发阶段
（D）执行阶段

88、下列属于宏病毒典型特征的是（ABD）
（A）与系统平台无关
（B）感染目的是文档
（C）驻留内存
（D）易于传播

89、感染 PE 文件的实现方式有（ACD）
（A）将病毒代码写入新加的段中
（B）将病毒代码捆绑到目标文件尾
（C）将病毒代码附加在最后一个段上
（D）将病毒代码写入到 PE 文件各个段所保留的未用空间中

90、与其它病毒相比，网络蠕虫的典型特征是（CD）
（A）破坏性大
（B）传播速度快

（C）病毒为独立个体
（D）病毒自身拷贝

91、在电子商务应用中，下面说法正确的是（ABC）
（A）证书上具有证书授权中心的数字签名
（B）证书上列有证书拥有者的基本信息
（C）证书上列有证书拥有者的公开密钥
（D）证书上列有证书拥有者的私有密钥

92、与加密体制有关的概念是（ABD）
（A）密钥空间
（B）明文空间
（C）系统空间
（D）密文空间

93、保证网络安全是使网络得到正常运行的保障，以下哪一种说法是正确的（ABC）
（A）绕过防火墙，私自和外部网络连接，可能造成系统安全漏洞
（B）越权修改网络系统配置，可能造成网络工作不正常或故障
（C）有意或无意地泄露网络用户或网络管理员口令是危险的
（D）解决来自网络内部的不安全因素必须从技术方面入手

94、以下是检查文件是否被病毒感染的有效方法是（BD）
（A）检查文件是否能够正常运行
（B）用反病毒软件扫描文件
（C）检测文件的长度是否无故变化
（D）检查磁盘目录中是否有病毒文件

95、常见的拒绝服务攻击有（ABC）
（A）SYN Flood
（B）Smurf 攻击
（C）Teardrop
（D）缓冲区溢出

96、现代入侵检测系统主要有哪几种类型（BD）
（A）基于用户的
（B）基于主机的
（C）基于病毒的
（D）基于网络的

97、网络传输加密常用的方法有（ACD）
（A）链路加密
（B）包加密
（C）端到端加密
（D）节点加密

98、防火墙主要有哪几种类型（ABC）
（A）包过滤防火墙
（B）代理防火墙

（C）双穴主机防火墙
（D）单穴主机防火墙

99、根据访问权限可以将用户分为哪几类（BCD）
（A）常用用户
（B）一般用户
（C）特殊用户
（D）审计用户

100、造成计算机不安全的因素有（ABCD）
（A）技术原因
（B）自然原因
（C）人为原因
（D）管理原因

101、目前，上海驾驶员学习的过程中利用的指纹来识别学员，从而管理相关的学习过程；而在工商银行推广的网上银行业务中使用了 USB KEY 来保障客户的安全性；这分别利用那些特性？（BC）
（A）学员知道的某种事物
（B）学员自有的特征；
（C）学员拥有物
（D）学员的某种难以仿制的行为结果

102、在安全服务中，不可否认性包括两种形式，分别是（AB）
（A）原发证明
（B）交付证明
（C）数据完整
（D）数据保密

103、以下安全标准属于 ISO7498-2 规定的是（AC）
（A）数据完整性
（B）Windows NT 属于 C2 级
（C）不可否认性
（D）系统访问控制

104、利用密码技术，可以实现网络安全所要求的（ABCD）
（A）数据保密性
（B）数据完整性
（C）数据可用性
（D）身份认证

105、在加密过程中，必须用到的三个主要元素是（ABC）
（A）所传输的信息（明文）
（B）加密钥匙（Encryption key）
（C）加密函数
（D）传输信道

106、加密的强度主要取决于（ABD）

（A）算法的强度
（B）密钥的保密性
（C）明文的长度
（D）密钥的强度

107、以下对于对称密钥加密说法正确的是（BCD）
（A）对称加密算法的密钥易于管理
（B）加解密双方使用同样的密钥
（C）DES 算法属于对称加密算法
（D）相对于非对称加密算法，加解密处理速度比较快

108、相对于对称加密算法，非对称密钥加密算法（ACD）
（A）加密数据的速率较低
（B）更适合于现有网络中对所传输数据（明文）的加解密处理
（C）安全性更好
（D）加密和解密的密钥不同

109、以下对于混合加密方式说法正确的是（BCD）
（A）使用公开密钥密码体制对要传输的信息（明文）进行加解密处理
（B）使用对称加密算法队要传输的信息（明文）进行加解密处理
（C）使用公开密钥密码体制对称加密密码体制的密钥进行加密后的通信
（D）对称密钥交换的安全信道是通过公开密钥密码体制来保证的

110、在通信过程中，只采用数字签名可以解决（ABC）等问题。
（A）数据完整性
（B）数据的抗抵赖性
（C）数据的篡改
（D）数据的保密性

111、防火墙不能防止以下哪些攻击行为（ABD）
（A）内部网络用户的攻击
（B）传送已感染病毒的软件和文件
（C）外部网络用户的 IP 地址欺骗
（D）数据驱动型的攻击

112、指出下列关于计算机病毒的正确论述（ABCDF）。
（A）计算机病毒是人为地编制出来、可在计算机上运行的程序
（B）计算机病毒具有寄生于其他程序或文档的特点
（C）计算机病毒只要人们不去执行它，就无法发挥其破坏作用
（D）计算机病毒在执行过程中，可自我复制或制造自身的变种
（E）只有计算机病毒发作时才能检查出来并加以消除
（F）计算机病毒具有潜伏性，仅在一些特定的条件下才发作

113、信息技术对企业的吸引力在于它能够被用来获取竞争优势。主要体现在速度优势方面的信息技术包括（AD）。
（A）无线通信
（B）开放式系统
（C）人工智能

（D）电子商务

114、信息系统的特征体现在（ABC）。
（A）附属性
（B）间接性
（C）整体性
（D）直接性

115、信息系统对组织的影响作用体现枉（BCD）。
（A）信息系统对组织的作用是直接的
（B）信息系统对组织战略提供支持
（C）信息系统对组织变革提供支持
（D）信息系统可能成为组织的累赘

116、ERP 的核心管理思想主要体现在（AB）。
（A）对整个供应链资源管理的思想
（B）体现精益生产、同步工程和敏捷制造的思想
（C）体现事后控制的思想
（D）考虑能力约束
117、网络安全工作的目标包括（ABCD）
（A）信息机密性
（B）信息完整性
（C）服务可用性
（D）可审查性

118、计算机信息系统安全保护的目标是要保护计算机信息系统的（ABCD）
（A）实体安全
（B）运行安全
（C）信息安全
（D）人员安全

119、计算机信息系统的运行安全包括（ABC）
（A）系统风险管理
（B）审计跟踪
（C）备份与恢复
（D）电磁信息泄漏

120、实施计算机信息系统安全保护的措施包括（AB）
（A）安全法规
（B）安全管理
（C）组织建设
（D）制度建设

121、计算机信息系统安全管理包括（ACD）
（A）组织建设
（B）事前检查
（C）制度建设
（D）人员意识

122、公共信息网络安全监察工作的性质（ABCD）
（A）是公安工作的一个重要组成部分
（B）是预防各种危害的重要手段
（C）是行政管理的重要手段
（D）是打击犯罪的重要手段

123、公共信息网络安全监察工作的一般原则（ABCD）
（A）预防与打击相结合的原则
（B）专门机关监管与社会力量相结合的原则
（C）纠正与制裁相结合的原则
（D）教育和处罚相结合的原则

124、安全员应具备的条件:（ABD）
（A）具有一定的计算机网络专业技术知识
（B）经过计算机安全员培训，并考试合格
（C）具有大本以上学历
（D）无违法犯罪记录

125、网络操作系统应当提供哪些安全保障（ABCDE）
（A）验证（Authentication）
（B）授权（Authorization）
（C）数据保密性（Data Confidentiality）
（D）数据一致性（Data Integrity）
（E）数据的不可否认性（Data Nonrepudiation）

126、Windows NT 的"域"控制机制具备哪些安全特性？（ABC）
（A）用户身份验证
（B）访问控制
（C）审计（日志）
（D）数据通讯的加密

127、从系统整体看，安全"漏洞"包括哪些方面（ABC）
（A）技术因素
（B）人的因素
（C）规划，策略和执行过程

128、从系统整体看，下述那些问题属于系统安全漏洞（ABCDE）
（A）产品缺少安全功能
（B）产品有 Bugs
（C）缺少足够的安全知识
（D）人为错误
（E）缺少针对安全的系统设计

129、应对操作系统安全漏洞的基本方法是什么？（ABC）
（A）对默认安装进行必要的调整
（B）给所有用户设置严格的口令
（C）及时安装最新的安全补丁
（D）更换到另一种操作系统

130、造成操作系统安全漏洞的原因（ABC）
（A）不安全的编程语言
（B）不安全的编程习惯
（C）考虑不周的架构设计

131、严格的口令策略应当包含哪些要素（ABC）
（A）满足一定的长度，比如 8 位以上
（B）同时包含数字，字母和特殊字符
（C）系统强制要求定期更改口令
（D）用户可以设置空口令

132、计算机安全事件包括以下几个方面（ABCD）
（A）重要安全技术的采用
（B）安全标准的贯彻
（C）安全制度措施的建设与实施
（D）重大安全隐患、违法违规的发现，事故的发生

133、计算机案件包括以下几个内容（ABC）
（A）违反国家法律的行为
（B）违反国家法规的行为
（C）危及、危害计算机信息系统安全的事件
（D）计算机硬件常见机械故障

134、重大计算机安全事故和计算机违法案件可由（AC）受理
（A）案发地市级公安机关公共信息网络安全监察部门
（B）案发地当地县级（区、市）公安机关治安部门
（C）案发地当地县级（区、市）公安机关公共信息网络安全监察部门
（D）案发地当地公安派出所

135、现场勘查主要包括以下几个环节（ABCD）
（A）对遭受破坏的计算机信息系统的软硬件的描述及被破坏程度
（B）现场现有电子数据的复制和修复
（C）电子痕迹的发现和提取，证据的固定与保全
（D）现场采集和扣押与事故或案件有关的物品

136、计算机安全事故原因的认定和计算机案件的数据鉴定，（ABC）
（A）是一项专业性较强的技术工作
（B）必要时可进行相关的验证或侦查实验
（C）可聘请有关方面的专家，组成专家鉴定组进行分析鉴定
（D）可以由发生事故或计算机案件的单位出具鉴定报告

137、有害数据通过在信息网络中的运行，主要产生的危害有（ABC）
（A）攻击国家政权，危害国家安全
（B）破坏社会治安秩序
（C）破坏计算机信息系统，造成经济的社会的巨大损失

138、计算机病毒的特点_____（ACD）
（A）传染性

（B）可移植性
（C）破坏性
（D）可触发性

139、计算机病毒按传染方式分为（BCD）
（A）良性病毒
（B）引导型病毒
（C）文件型病毒
（D）复合型病毒

140、计算机病毒的危害性有以下几种表现（ABC）
（A）删除数据
（B）阻塞网络
（C）信息泄漏
（D）烧毁主板

141、计算机病毒由（ABD）部分组成
（A）引导部分
（B）传染部分
（C）运行部分
（D）表现部分

142、以下哪些措施可以有效提高病毒防治能力（ABCD）
（A）安装、升级杀毒软件
（B）升级系统、打补丁
（C）提高安全防范意识
（D）不要轻易打开来历不明的邮件

143、计算机病毒的主要传播途径有（ABCD）
（A）电子邮件
（B）网络
（C）存储介质
（D）文件交换

144、计算机病毒的主要来源有（ACD）
（A）黑客组织编写
（B）计算机自动产生
（C）恶意编制
（D）恶作剧

145、发现感染计算机病毒后，应采取哪些措施（ABC）
（A）断开网络
（B）使用杀毒软件检测、清除
（C）如果不能清除，将样本上报国家计算机病毒应急处理中心
（D）格式化系统

146、计算机病毒能够（ABC）
（A）破坏计算机功能或者毁坏数据

（B）影响计算机使用
（C）能够自我复制
（D）保护版权

147、广域网技术用于连接分布在广大地理范围内计算机，它常用的封装协议有哪些(ABCDE)
A.SDLC 协议和 HDLC（High-Level Data Link Control）高层数据链路协议
B.Frame Relay(帧中继)
C.PPP（Point-to-Point Protocol，点到点协议）
D.ISDN（综合业务数字网协议）
E.ADSL（非对称数字用户线）

148、木马的隐藏技术可以利用操作系统的哪些方面实现 （ABCDE）
A.任务管理器
B.端口
C.任务栏
D.系统文件加载
E.注册表

149、加密的强度主要取决于（ABD）
A.算法的强度
B.密钥的保密性
C.明文的长度
D.密钥的强度

150、以下对于对称密钥加密说法正确的是（BCD）
A.对称加密算法的密钥易于管理
B.加解密双方使用同样的密钥
C.DES 算法属于对称加密算法
D.相对于非对称加密算法，加解密处理速度比较快

151、以下关于包过滤技术与代理技术的比较，正确的是（ABC）
A.包过滤技术的安全性较弱，代理服务技术的安全性较高
B.包过滤不会对网络性能产生明显影响
C.代理服务技术会严重影响网络性能
D.代理服务技术对应用和用户是绝对透明的

152、信息安全的 CIA 模型指的是以下哪三个信息安全中心目标（ABC）
A.保密性
B.完整性
C.可用性
D.可控性

153、网络安全审计做为企业越来越重要的信息安全防护一部分，它的发展趋势有哪些特征（ABD）
A.体系化
B.控制化
C.主观化
D.智能化

154、脆弱性扫描产品作为与入侵检测产品紧密配合的部分，用户在选择时需要考虑哪些问题（ACDE）
A.是否具有针对网络和系统的扫描系统
B.产品的数据精确性
C.产品的扫描能力
D.产品的评估能力
E.产品的漏洞修复能力及报告格式

155、相对于对称加密算法，非对称密钥加密算法（ACD）
A.加密数据的速率较低
B.更适合于现有网络中对所传输数据（明文）的加解密处理
C.安全性更好
D.加密和解密的密钥不同

156、对于防火墙的设计准则，业界有一个非常著名的标准，即两个基本的策略（BC）
A.允许从内部站点访问 Internet 而不允许从 Internet 访问内部站点
B.没有明确允许的就是禁止的
C.没有明确禁止的就是允许的
D.只允许从 Internet 访问特定的系统

157、漏洞评估技术具有哪些主要优点（AC）
A.预知性
B.精确性
C.重点防护
D.技术成熟

158、请问计算机病毒的传播途径有哪些（ABCDE）
A.系统漏洞
B.P2P 共享软件
C.即时通信软件
D.网络共享
E.电子邮件

159、以下关于节点加密的描述，哪些是正确的（AD）
A.节点加密是对传输的数据进行加密，加密对用户是透明的
B.节点加密允许消息在网络节点以明文形式存在
C.节点加密的过程使用的密钥与节点接收到的信息使用的是相同的密钥
D.节点加密要求报头和路由信息以明文形式传输

160、一个好的入侵检测系统应具有哪些特点（ABCD）
A.不需要人工干预
B.不占用大量系统资源
C.能及时发现异常行为
D.可灵活定制用户需求

161、信息安全漏洞主要表现在以下几个方面（ABCD）
A.非法用户得以获得访问权
B.系统存在安全方面的脆弱性

C.合法用户未经授权提高访问权限
D.系统易受来自各方面的攻击

162、在信息安全中，最常用的病毒稳蔽技术有哪几种（ABC）
A.Hook 挂钩机制
B.修改注册表
C.修改内存指针地址
D.以上都不是

163、系统被安装 Spywarer 后，会出现哪些症状（ABC）
A.系统可能无缘无故的挂起并死机
B.发现浏览器的工具栏出现了新的用户并不清楚的按钮
C.运行时显示广告条的应用程序
D.计算机的音频视频设备不能使用

164、垃圾邮件对于企业或个人的危害性体现在哪些方面（BC）
A.对计算机系统造成破坏
B.造成邮件服务器负载过重
C.消耗带宽和网络存储空间
D.不会影响个人的正常工作

165、IPSec 采取了哪些形式来保护 ip 数据包的安全（ABCD）
A.数据源验证
B.完整性校验
C.数据内容加密
D.防重演保护

166、关于"云安全"技术，哪些描述是正确的（ABD）
A."云安全"技术是应对病毒流行和发展趋势的有效和必然选择
B."云安全"技术是"云计算"在安全领域的应用
C."云安全"将安全防护转移到了"云"，所以不需要用户的参与
D.Web 信誉服务是"云安全"技术应用的一种形式

167、"云安全"体系结构主要由以下哪几个部分组成（ABCD）
A.智能威胁收集系统
B.计算"云"
C.服务"云"
D.安全子系统

168、以下哪些不是网络型漏洞扫描器的功能（ACD）
A.重要资料锁定
B.阻断服务扫描测试
C.专门针对数据库的漏洞进行扫描
D.动态式的警讯

169、针对安全评估可以采用一系列技术措施以保证评估过程的接口统一和高效，主要包括哪些技术（ABCD）
A.数据采集和分析

B.量化评估
C.安全检测
D.安全评估分析

170、包过滤技术的优点有哪些（ACD）
A.对用户是透明的
B.安全性较高
C.传输能力较强
D.成本较低

171、"网络钓鱼"的主要伎俩有哪些（ABCDE）
A.发送电子邮件，以虚假信息引诱用户中圈套
B.建立假冒网站，骗取用户账号密码实施盗窃
C.利用虚假的电子商务进行诈骗
D.利用木马和黑客技术等手段窃取用户信息后实施盗窃活动
E.利用用户弱口令等漏洞破解、猜测用户帐号和密码

172、即时通信病毒的传播主要利用的是哪些工具 （ABCD）
A.QQ
B.MSN
C.网络泡泡
D.雅虎通

173、防火墙的构建要从哪些方面着手考虑 （ADE）
A.体系结构的设计
B.体系结构的制订
C.安全策略的设计
D.安全策略的制订
E.安全策略的实施

174、VLAN 是建立在物理网络基础上的一种逻辑子网，那么他的特性有哪些呢（ABCD）
A.可以缩小广播范围，控制广播风暴的发生
B.可以基于端口、MAC 地址、路由等方式进行划分
C.可以控制用户访问权限和逻辑网段大小，提高网络安全性
D.可以使网络管理更简单和直观

175、蠕虫有自己特定的行为模式，通常分为哪几个步骤（ABC）
A.搜索
B.攻击
C.复制
D.破坏

176、在通信过程中，只采用数字签名可以解决（ABC）等问题。
A.数据完整性
B.数据的抗抵赖性
C.数据的篡改
D.数据的保密性

177、防火墙不能防止以下那些攻击行为（ABD）
A.内部网络用户的攻击
B.传送已感染病毒的软件和文件
C.外部网络用户的 IP 地址欺骗
D.数据驱动型的攻击

178、以下属于包过滤技术的优点的是（BC）
A.能够对高层协议实现有效过滤
B.具有较快的数据包的处理速度
C.为用户提供透明的服务，不需要改变客户端的程序和自己本身的行为
D.能够提供内部地址的屏蔽和转换功能

179、以下关于信息系统弱点的描述中哪些是正确的（AC）
A.信息系统弱点无处不在，无论采用多么强大的安全防护措施
B.信息系统的弱点通常只存在于设计不完美的操作系统和应用软件环境中
C.信息系统弱点可以通过有效的防护措施将风险降到可以接受的范围内
D.信息系统弱点主要是技术因素造成的

180、复合型病毒是一种具有多种病毒特征的病毒，那么它同时可以感染哪两种类型的文件呢（AC）
A.引导扇区
B.常驻内存
C.可执行文件
D.系统自启动型

181、宏病毒具有哪些特征（ABC）
A.在以前不含有宏的文件中出现了宏
B.该应用程序将所有文件保存为模板
C.该应用程序经常会提醒用户保存那些只是被查看了但没有被修改的文档
D.使用 Word2000 打开 Word97 文档时，提示用户保存没有做任何修改的文档

182、"云安全"的应用形式有哪些（ABC）
A.邮件信誉服务
B.文件信誉服务
C.WEB 信誉服务
D.网络协议信誉服务

183、网络设备多种多样，各自的功能也不同；那么具有即可以智能地分析数据包，并有选择的发送功能的设备是哪种（AB）
A. 交换机
B.路由器
C.集线器
D.光纤收发器

184、企业网络中使用"云安全"技术的优势有哪些（ABC）
A."云"端超强的计算能力
B.本地更少的病毒码存储资源占用
C.病毒码更新时更少的带宽占用

D.能检测的病毒量更少

185、建立堡垒主机的一般原则（AC）
A.最简化原则
B.复杂化原则
C.预防原则
D.网络隔断原则

186、局域网是一个允许很多独立的设备相互间进行通信的通信系统，那么它有哪些特性呢（AB）
A.提供短距离内多台计算机的互连
B.造价便宜、极其可靠，安装和管理方便
C.连接分布在广大地理范围内计算机
D.造价昂贵

187、入侵检测系统能够增强网络的安全性，那么它的优点体现在哪些方面（ACDEF）
A.能够使现有的安防体系更完善
B.能够在没有用户参与的情况下阻止攻击行为的发生
C.能够更好地掌握系统的情况
D.能够追踪攻击者的攻击线路
E.界面友好，便于建立安防体系
F.能够抓住肇事者

188、路由器（Router）是目前网络上最常用的设备，那么路由器具有哪些功能（BCD）
A.只负责把多段介质连接在一起，不对信号作任何处理
B.判断网络地址和选择路径的功能
C.能在多网络互联环境中建立灵活的连接
D.可用完全不同的数据分组和介质访问方法连接各种子网

189、 IPSec 可有效保护 IP 数据报的安全，但该协议也有不足之处，那么他的缺点体现在哪些方面（ABC）
A.不太适合动态 IP 地址分配（DHCP）
B.除 TCP/IP 协议外，不支持其他协议
C.除包过滤外，没有指定其他访问控制方法
D.安全性不够

190、虽然网络防火墙在网络安全中起着不可替代的作用，但它不是万能的，有其自身的弱点，主要表现在哪些方面（ABCD）
A.不具备防毒功能
B.对于不通过防火墙的链接无法控制
C.可能会限制有用的网络服务
D.对新的网络安全问题无能为力

191、在信息安全领域中，各安全厂商对于病毒命名规则的都不同，那么趋势科技对于病毒的命名规则是由哪几部分组成的（ABD）
A.病毒名
B.病毒类型
C.病毒感染方式

D.病毒变种名

192、计算机病毒诊断技术有多种方式方法，以下哪些是病毒的检测方法（ABDE）
A.比较法
B.特征码比对法
C.漏洞评估法
D.行为监测法
E.分析法

193、黑客攻击某个系统之前，首先要进行信息收集，那么哪些信息收集方法属于社会工程学范畴（BD）
A.通过破解 SAM 库获取密码
B.通过获取管理员信任获取密码
C.使用暴力密码破解工具猜测密码
D.通过办公室电话、姓名、生日来猜测密码

194、Windows 病毒与 DOS 病毒有哪些不同特征（BCD）
A.病毒的破坏性不同
B.病毒攻击的可执行文件不同
C.病毒恶意代码不同
D.病毒攻击的操作系统不同

195、Spyware 通过哪些手段窃取用户的信息（ABCD）
A.记录上网浏览的 cookies
B.安装屏幕捕捉程序
C.安装事件记录程序
D.对于键盘击键进行记录

196、 TCP/IP 协议的攻击类型共有四类，那么针对网络层攻击中，哪几个协议攻击是利用的比较多的（ACD）
A.ICMP 协议
B.ARP 协议
C.IGMP 协议
D.IP 协议

197、在安全服务中，不可否认性包括两种形式，分别是（AB）
A.原发证明
B.交付证明
C.数据完整
D.数据保密

198、以下对于混合加密方式说法正确的是（BCD）
A.使用公开密钥密码体制对要传输的信息（明文）进行加解密处理
B.使用对称加密算法队要传输的信息（明文）进行加解密处理
C.使用公开密钥密码体制对称加密密码体制的密钥进行加密后的通信
D.对称密钥交换的安全信道是通过公开密钥密码体制来保证的

199、黑客通过 Windows 空会话可以实现哪些行为（ABC）

A.列举目标主机上的用户和共享
B.访问小部分注册表
C.访问 everyone 权限的共享
D.访问所有注册

200、对于链路接加密的描述中，哪些是正确的（ABCDE）
A.对于在两个网络节点间的某一次通信链路，链路加密能为网上传输的数据提供安全保证
B.由于每条通信链路上的加密是独立进行的，因此当某条链路受到破坏时，不会影响其他链路上传输的信息的安全性
C.不会减少网络的有效带宽
D.只有相邻节点使用同一密钥，因此，密钥容易管理
E.加密对于用户是透明的，用户不需要了解加密、解密的过程

201、对于计算机病毒的描述，以下哪些是正确的（CD）
A.感染病毒不会对计算机系统文件造成破坏
B.感染病毒只会对文件造成破坏，不会造成数据丢失;
C.感染病毒，有时会窃取敏感信息，给用户带来经济损失
D.感染病毒不一定会对计算机软硬件带来危害

202、状态包检测技术有哪些特点(ABCD)
A.安全性较高
B.效率高
C.可伸缩易扩展
D.应用范围广

203、计算机网络具有复杂的结构,可分为 OSI 七层模型或 TCP/IP 四层模型，那么 OSI 模型中哪几层对应 TCP/IP 模型中应用层的呢（ABC）
A. 应用层
B.表示层
C.会话层
D.传输层

204、入侵检测系统的功能有哪些（ACD）
A.让管理员了解网络系统的任何变更
B.对网络数据包进行检测和过滤
C.监控和识别内部网络受到的攻击
D.给网络安全策略的制定提供指南

205、安全评估分析技术采用的风险分析方法基本要点是围绕信息的哪几项需求（ABCD）
A.保密性
B.完整性
C.可用性
D.可控性

206、一个完整的木马程序有两部分组成,请问是哪两部分（AB）
A.服务器端
B.控制器端
C. 接收木马端

D.发送木马端

207、关于企业防毒体系构建的说法，错误的是（BC）
A.病毒防护体系是一项复杂的系统工程，是技术、流程、人员的有机结合
B.病毒防护只要能做好桌面安全防护就可以了，这个方案最经济
C.在病毒防护解决方案中，防病毒产品是最重要的因素，防毒产品能检测到的病毒数量越多说明方案越优越
D.病毒防护解决方案应该重视事前防御而不是"亡羊补牢"

208、对信息安全风险评估的描述以下哪些是正确的（BD）
A.信息安全评估是建立安全防护体系的起点，任何企业在构建安全防护体系的时候，第一步就必须要进行信息安全评估
B.信息安全评估是建立安全防护体系的关键，它连接着安全防护重点和商业需求
C.安全评估就是对网络现状的分析，仅利用一些漏洞评估工具就可以实现了
D.进行风险评估，有助于制订消除、减轻或转移风险的安防控制措施并加以实施

209、数据库漏洞的防范在企业中越来越重视，通过哪些方法可以实施防范（ABCD）
A.更改数据库名
B.更改数据库里面常用字段成复杂字段
C.给数据库关键字段加密，对于管理员账户设置复杂密码
D.在你的数据库文件文件中建一个表，并在表中取一字段填入不能执行的 ASP 语句

210、人为的恶意攻击分为被动攻击和主动攻击，在以下的攻击类型中属于主动攻击的是
A.数据 GG（BC）
B.数据篡改及破坏
C.身份假冒
D.数据流分析

211、在加密过程中，必须用到的三个主要元素是（ABC）
A.所传输的信息（明文）
B.加密钥匙（Encryption key）
C.加密函数
D.传输信道

212、以下哪些是蠕虫病毒的特征（AB）
A.利用系统漏洞进行主动攻击
B.传播速度更快，方式更多样化
C.感染系统后入驻内存
D.只在一台计算机内进行文件感染

213、信息安全方案设计的基本原则有哪些（ABCD）
A.木桶原则
B.动态化原则
C.预防性原则
D.多层次原则

214、随着技术的进步和客户需求的进一步成熟的推动，当前主流市场的 SSL VPN 和几年前面市的相比已经发生很大的变化，主要表现在以下哪些方面（BCD）

A.对数据的要求更精确
B.对应用的支持更广泛
C.对网络的支持更加广泛
D.对终端的安全性要求更严格

215、蠕虫和传统意义上的病毒是有所区别的，具体表现在哪些方面（ABCD）
A.存在形式
B.传染机制
C.传染目标
D.触发感染

216、建立完整的信息安全管理体系通常要经过以下哪几个步骤（ABCD）
A.计划（Plan）
B 实施 (Do)
C 检查 (Check)
D 改进 (Action)

217、以下安全标准属于 ISO7498-2 规定的是（AC）
A.数据完整性
B.Windows NT 属于 C2 级
C.不可否认性
D.系统访问控制

218、利用密码技术，可以实现网络安全所要求的（ABCD）
A.数据保密性
B.数据完整性
C.数据可用性
D.身份认证

219、基于主机的入侵检测始于 20 世纪 80 年代早期，通常采用查看针对可疑行为的审计记录来执行，那么它的缺点是什么呢（ABCD）
A.看不到网络活动的状况
B.运行审计功能要占用额外系统资源
C.主机监视感应器对不同的平台不能通用
D.管理和实施比较复杂

220、基于网络的入侵检测系统使用原始的裸网络包作为源，那么他有哪些缺点(ABC)
A.对加密通信无能为力
B.对高速网络无能为力
C.不能预测命令的执行后果
D.管理和实施比较复杂

判断题（100 题）

1、SSL 协议位于 TCP/IP 模型的传输层和应用层之间，由下到上分别是记录协议层和握手协议层。（√）

2、ssldump 是一个 SSL/TLS 网络协议分析工具，在不需要知晓密钥的情况下，它可以将连接双方的应用层数据显示出来。（×）

3、Windows 文件审核中的对象访问事件 560 表示允许访问一个已存在的对象。（√）

4、在支持阴影口令的系统中，只要窃取到加密后的口令密文，就可以破译出用户口令。（×）

5、SElinux 默认策略类型有两种：targeted 和 strict，targeted 用于对整个系统进行保护，strict 用于对网络服务进行保护。（×）

6、在 Windows2003 系统中，WWW 服务日志的默认位置是 C:\WINDOWS\system32\LogFiles\w3svc1。（√）

7、IPSec 认证报头（AH）不能提供数据机密性服务。（√）

8、IPSec 体系中，AH 只能实现地址源认证和数据完整性服务，ESP 只能实现信息保密性服务。（×）

9、SSL 协议中，多个会话（session）可以同时利用同一个连接（connection）的参数。（√）

10、在 SSL 握手协议的过程中，Server-Hello 消息必须包含服务器的公钥证书。（×）

11、非对称密钥加密体制比对称密钥加密体制更为安全。（×）

12、IPsec 安全关联（SA）是发送方和接收方间的单向关系，因此在 IPSec 通信环境中，两个节点之间的安全通信必须建立在两个或两个以上的 SA 才能进行双向的安全通信。（√）

13、PGP 软件中共涉及两种密钥：公钥和私钥。（×）

14、开放性是 Linux 系统一大特点。（√）

15、Linux 系统中，通过配置 xinetd 能够防止 SYN 洪水攻击。（√）

16、利用 ARP 协议可以进行跨网段主机发现。（×）

17、利用 NetBIOS 与 WINS 协议可以进行跨网段主机发现。（√）

18、UDP 端口扫描方法向目标发送一个 UDP 协议组，若目标端口关闭，返回 UDP 端口不可达报文。（×）

19、TCP 全扫描完成了一次完整的 TCP 协议三次握手过程，而 TCP SYN 扫描则没有完成。（√）

20、FTP 弱口令扫描原理是，扫描器首先发送 USER 命令，若被扫描主机响应代码为 230，则继续发送 PASS 命令，此时被扫描主机若响应 331 代码，则表示口令扫描成功。（×）

21、一般情况下，网卡的缺省配置支持广播模式、直接模式和混杂模式。（×）

22、无论是基于 TCP/IP 协议栈、还是利用 Winpcap 捕获数据包，两种方式都受防火墙规则影响。（×）

23、进程通常被定义为一个正在运行的程序的实例，缓冲区溢出则不可能发生在进程空间的代码段。（√）

24、拒绝服务攻击（Dos）利用了 TCP、ICMP 等协议自身的漏洞。（×）

25、必须通过攻击手段，才能够将后门程序植入到目标主机中。（×）

26、后门程序都是有监听端口的。（×）

27、将木马捆绑到 EXE 文件后面是隐藏木马的一种方式。（ √ ）

28、。（ √ ）

29、包过滤防火墙工作在网络层。（ √ ）

30、iptables 防火墙工作在网络层。（ × ）

31、iptables 防火墙工作在 ISO 七层模型的第二、三、四层。（ √ ）

32、iptables 防火墙 filter 表内规则仅检测与本地进程进行通信的数据包。（ × ）

33、利用 NAT 技术能够屏蔽企业网络内部网络分布。（ √ ）

34、多数网络入侵检测系统（NIDS）都是可以检测未知的网络异常行为。（ × ）

35、由于网络入侵检测系统（NIDS）所使用的规则库都是准确无误的，所以入侵检测报警结果也是准确的。（ × ）

36、基于网络的入侵检测系统（NIDS）需定期更新规则库（ √ ）

37、入侵检测系统自身同样具有阻断网络连接的功能。（ × ）

38、VPN 认证包括预共享密钥（PSK）和 x.509 证书两种方式。（ √ ）

39、网络隧道是指在专用网建立一条数据通道（隧道），让数据包通过这条隧道传输。（ × ）

40、PPTP、IPSec、GRE 均是第三层隧道协议。（ × ）

41、PPTP 隧道协议使用 PPP 协议对原始数据进行第一层封装，之后使用 GRE 协议进行第二层封装。（ √ ）

42、OpenVPN 是一个具备完全特征的 SSL VPN 解决方案，支持远程访问、站点与站点间 VPN、WiFi 安全及企业级远程访问，并与 PPTP、IPSec 相兼容。（ × ）

43、蜜罐只有在受到攻击情况下才能够展现出其价值。（ √ ）

44、蜜罐是一种安全资源，其目标就是被别人探测、攻击，甚至是攻破。（ √ ）

45、正常情况下，应该没有任何人或者资源与蜜罐进行通信。（ √ ）

46、PE 文件在磁盘上的数据结构与在内存中的结构是不一致的。（ × ）

47、Word 文件是通过模板来创建的，模板是为了形成最终文档而提供的特殊文件。（ √ ）

48、。新型的邮件病毒邮件正文即为病毒，用户接收到带毒邮件后，即使不将邮件打开，只要将鼠标指向邮件，通过预览功能病毒也会被自动激活。（ √ ）

49、计算机蠕虫病毒与普通病毒一样，能把自身加载到其它程序（包括操作系统）上。它不能独立的运行，而需要有它的宿主程序的运行来激活它。（ × ）

50、无线网卡即无线上网卡，可以实现在任何位置接入 Internet，用户可通过流量计费和包月付费来定制服务。（ × ）

51、作为低交互度的蜜罐，BOF 模拟了 7 种 TCP 服务，并可针对 HTTP、FTP 请求完成 TCP 三次握手。（ × ）

52、作为低交互度的蜜罐，Honeyd 主要是一种用于对攻击进行检测的产品型蜜罐。（ √ ）

53、与产品型蜜罐相比，研究型蜜罐更容易部署。（ × ）

54、蜜罐可以是网络上存在的物理主机。（√）

55、Honey 只能接收非存在系统的流量。（√）

56、如果能够根据密文系统地确定出明文或者密钥，或者能够根据明文－密文对来系统地确定出密钥，则我们说这个密码是可破译的。（√）

57、绝对不可破译的密码学在理论上是存在的。（√）

58、DES 算法中每个 S 盒有 6 个输入，6 个输出 ，是一种线性压缩变换。（×）

59、S 盒是 DES 算法中的唯一非线性变换，它是 DES 算法安全的关键所在。（√）

60、DES 的运算是对和运算，解密和加密可以共用同一个运算，且子密钥使用的顺序也相同。（×）

61、AES 的运算也是对和运算，解密和加密可以共用同一个运算，只是子密钥使用的顺序不同。（×）

62、AES 算法的明文分组 128 位，密文和密钥分组位数都是可变的。（√）

63、AES 的加密算法中每一轮都要经过 S 盒变换即 ByteSub(State)、行移位变换即 ShiftRow(State)、列混合变换即 MixColumn(State)和密钥加变换即 AddRoundKey(State,RoundKey)。（×）

64、中国商用密码算法 SMS4 是一种对称密钥加密算法。（√）

65、RC4 序列密码算法的优点是算法简单、高效，是目前应用最广的商密级序列密码。（√）

66、RC4 算法是一种基于非线性数据表变换的序列密码，它以一个足够大的数据表为基础。（√）

67、RSA 算法是基于“离散对数”这个数论难题的基础上的。（×）

68、ELGamal 算法的安全性是基于求“大数分解和素性检测”这个数学难题上的。（×）

69、MD5 算法所产生的摘要比 SHA1 长 32 位。（×）

70、MD5 算法的链接变量是 4 个，而 SHA1 的连接变量是 5 个。（√）

71、认证和加密的区别在于，加密是确保数据的保密性，而认证是确保数据发送者和接收者的真实性以及数据的完整性。（√）

72、密码体制的安全应当只取决于密钥的安全，而不取决于对密码算法的保密。（√）

73、对于任何实用密码只要有足够的资源，都可以用穷举攻击将其攻破。（√）

74、RAID 1 又称镜像方式，对存储的数据进行百分之百的备份，备份数据占了总存储空间的一半，因此，镜像的磁盘空间利用率低，存储成本高。（√）

75、Windows NT/2000/XP/Server 2003 可以提供 RAID 0、RAID 1、RAID 5 三种方式的软 RAID，也同样支持 RAID 0+1 和 RAID 0+5。（×）

76、在 Windows Server 2003 系统里，从“基本磁盘”升级到“动态磁盘”，以及从“动态磁盘”返回到“基本磁盘”磁盘数据都是不会改变的。（×）

77、Windows 和 Linux 操作系统的主硬盘（系统所在硬盘）都支持软 RAID 1。（×）

78、启动管理器是存储在磁盘开始扇区中的一段程序，它的任务就是将控制传送给操作系统，完成启动过程。（√）

79、认证和加密的区别：加密用以确保数据的保密性，而认证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。（√）

80、宏病毒感染的目标既可以是文件，也可以是可执行的代码估。（×）

81、宏病毒利用了 Word 或其他 Office 应用软件中的一种称为宏的机制。（√）

82、邮件型病毒只能以附件的形式进行传播。（×）

83、基于变换域的水印技术可以嵌入大量比特数据而不会导致可察觉的缺陷。（√）

84、在 Linux FC5 系统中，命令 chown apache:lucy /opt/target 表示变更/opt/target 的所有者为 lucy，属组为 apache。（×）

85、在 Linux FC5 系统中，以 root 用户身份执行 chmod o-w-x /opt/target（文件）后，target 文件所有者对 target 文件失去了写和执行权限。（×）

86、iptables 防火墙可工作在 OSI 模型的第二、三和四层。（√）

87、数字水印的最大缺点是文件格式的变换会导致水印数据的丢失。（×）

88、一个数字水印算法，它既能够嵌入大量信息到文件，同时嵌入后文件不会有明显的降质，并且不易被察觉，则此算法是一个较好的水印算法。（×）

89、文件嵌入水印后会增加文件大小。（×）

90、数字水印鲁棒性是指在经历多种无意或有意的信号处理过程后，数字水印仍能保持完整性或仍能被准确鉴别。（√）

91、CA 机构能够提供证书签发、证书注销、证书更新和信息加密功能。（×）

92、一个好的加密算法安全性依赖于密钥安全性。（√）

93、某应用程序感染了文件型病毒，则该文件的大小变化情况一般是变小。（×）

94、在拒绝服务攻击中，Smurf 攻击只是对目标主机产生攻击，对中间目标不会造成影响。（×）

95、访问控制是网络防范和保护的主要策略。（√）

96、在 SSL 握手协议的过程中，Server-Hello 消息必须包含服务器的公钥证书。（×）

97、包过滤防火墙对应用层是透明的，增加这种防火墙不需要对应用软件做改动。（√）

98、现代密码体制把算法和密钥分开，只需要保证密钥的保密性就行了，算法是可以公开的。（√）

99、目前常用的信息加密方式是采用 VPN（虚拟专用网）加密技术。（√）

100、公钥证书是不能在网络上公开的，否则其他人可能假冒我的身价或仿造我的数字签名。（×）

简答题（100 题）

1、通过个人对 Kaiser 密码算法原理的掌握情况，请计算出当密钥 k=3 时，对应明文：data security has evolved rapidly 的密文。

GDWD VHFXULWB KDV HYROYHG UDSLGOB

2、什么是反弹端口型木马？它利用了防火墙的什么特性？

反弹端口型木马的服务端（被控制端）使用主动端口，客户端（控制端）使用被动端口。木马定时监测控制端的存在，发现控制端上线后立即弹出端口主动连接控制端打开的被动端口。服务端通常会把打开的端口伪装成应用软件的端口，从而进一步降低被防火墙发现的概率。

分析防火墙的特性后可以发现，一般情况下，防火墙对于连入的链接往往会进行非常严格的过滤，但是对于连出的链接却疏于防范。反弹端口型木马正是利用了这一特性。

3、snort 的四大软件模块组成。

数据包嗅探模块、预处理模块、检测模块、报警/日志模块

4、分别解释”./snort -v -d -e”这条命令中各个参数的具体含义。

参数 -v 的含义是：使 snort 输出 IP 和 TCP/UDP/ICMP 的包头信息；

参数 -d 的含义是：使 snort 输出应用层的数据信息；

参数 -e 的含义是：使 snort 输出显示数据链路层的数据信息；

5、简述 ARP 欺骗成为可能的原因。

ARP 的致命缺陷是：它不具备任何的认证机制。当有个人请求某个 IP 地址的 MAC 时，任何人都可以用 MAC 地址进行回复，并且这种响应也会被认为是合法的。ARP 并不只在发送了 ARP 请求后才接收 ARP 应答。当主机接收到 ARP 应答数据包的时候，就会对本机的 ARP 缓存进行更新，将应答中的 IP 和 MAC 地址存储在 ARP 缓存表中。此外，由于局域网中数据包不是根据 IP 地址，而是按照 MAC 地址进行传输的。所以对主机实施 ARP 欺骗就成为可能。

6、为什么说 ICMP 是一个很理想的无端口后门传输机制。

首先 ICMP 不包括端口的概念，端口是一个 TCP 和 UDP 的概念，用于编制和区分用于通信的资源和目的的文件处理终端。由于 ICMP 和端口无关，通过 ICMP 查找命令传输的后门监听程序就不会像基于 TCP 和 UDP 协议的工具一样显示出来；其次，因为许多网络允许某些类型的 ICMP 信息通过防火墙，但是却阻止大部分 TCP 和 UDP 通信；最后，攻击者使用基于 ICMP 的后门还有一个原因，那就是有效字段可在任意一个 ICMP 消息的类型末尾被弄丢。攻击者可以利用将要发送给后门的指令加在这个有效字段，任何来自后门的响应可以同样地传回给另一个 ICMP 消息的有效字段。

7、简述主动攻击与被动攻击的特点，并列举主动攻击与被动攻击现象。

主动攻击是攻击者通过网络线路将虚假信息或计算机病毒传入信息系统内部，破坏信息的真实性、完整性及系统服务的可用性，即通过中断、伪造、篡改和重排信息内容造成信息破坏，使系统无法正常运行。被动攻击是攻击者非常截获、窃取通信线路中的信息，使信息保密性遭到破坏，信息泄露而无法察觉，给用户带来巨大的损失。

8、简述对称密钥密码体制的原理和特点。

对称密钥密码体制，对于大多数算法，解密算法是加密算法的逆运算，加密密钥和解密密钥相同，同属一类的加密体制。它保密强度高但开放性差，要求发送者和接收者在安全通

信之前，需要有可靠的密钥信道传递密钥，而此密钥也必须妥善保管。

9、具有 N 个节点的网络如果使用公开密钥密码算法，每个节点的密钥有多少？网络中的密钥共有多少？

每个节点的密钥是 2 个，网络中的密钥共有 2N 个。

10、对称密码算法存在哪些问题？

适用于封闭系统，其中的用户是彼此相关并相互信任的，所要防范的是系统外攻击。随着开放网络环境的安全问题日益突出，而传统的对称密码遇到很多困难：密钥使用一段时间后需要更换，而密钥传送需要可靠的通道；在通信网络中，若所有用户使用相同密钥，则失去保密意义；若使用不同密钥 N 个人之间就需要 N(N-1)/2 个密钥，密钥管理困难。无法满足不相识的人之间私人谈话的保密性要求。对称密钥至少是两人共享，不带有个人的特征，因此不能进行数字签名。

11、IDEA 是对称加密算法还是非对称加密算法？加密密钥是多少位？

IDEA 是一种对称密钥算法，加密密钥是 128 位。

12、什么是序列密码和分组密码？

序列密码是一种对明文中的单个位（有时对字节）运算的算法。分组密码是把明文信息分割成块结构，逐块予以加密和解密。块的长度由算法设计者预先确定。

13、简述公开密钥密码机制的原理和特点？

公开密钥密码体制是使用具有两个密钥的编码解码算法，加密和解密的能力是分开的；这两个密钥一个保密，另一个公开。根据应用的需要，发送方可以使用接收方的公开密钥加密消息，或使用发送方的私有密钥签名消息，或两个都使用，以完成某种类型的密码编码解码功能。

14、什么是 MD5？

MD 消息摘要算法是由 Rivest 提出，是当前最为普遍的 Hash 算法，MD5 是第 5 个版本，该算法以一个任意长度的消息作为输入，生成 128 位的消息摘要作为输出，输入消息是按 512 位的分组处理的。

15、TCP/IP 协议的网络安全体系结构的基础框架是什么？

由于 OSI 参考模型与 TCP/IP 参考模型之间存在对应关系，因此可根据 GB/T 9387.2-1995 的安全体系框架，将各种安全机制和安全服务映射到 TCP/IP 的协议集中，从而形成一个基于 TCP/IP 协议层次的网络安全体系结构。

16、密钥的产生需要注意哪些问题?

算法的安全性依赖于密钥，如果用一个弱的密钥产生方法，那么整个系统都将是弱的。DES 有 56 位的密钥，正常情况下任何一个 56 位的数据串都能成为密钥，所以共有 256 种可能的密钥。在某些实现中，仅允许用 ASCII 码的密钥，并强制每一字节的最高位为零。有的实现甚至将大写字母转换成小写字母。这些密钥产生程序都使得 DES 的攻击难度比正常情况下低几千倍。因此，对于任何一种加密方法，其密钥产生方法都不容忽视。

大部分密钥生成算法采用随机过程或者伪随机过程来生成密钥。随机过程一般采用一个随机数发生器，它的输出是一个不确定的值。伪随机过程一般采用噪声源技术，通过噪声源的功能产生二进制的随机序列或与之对应的随机数。

17、KDC 在密钥分配过程中充当何种角色？

KDC 在密钥分配过程中充当可信任的第三方。KDC 保存有每个用户和 KDC 之间共享的唯

一密钥，以便进行分配。在密钥分配过程中，KDC 按照需要生成各对端用户之间的会话密钥，并由用户和 KDC 共享的密钥进行加密，通过安全协议将会话密钥安全地传送给需要进行通信的双方。

18、数字签名有什么作用？

当通信双方发生了下列情况时，数字签名技术必须能够解决引发的争端：

否认，发送方不承认自己发送过某一报文。

伪造，接收方自己伪造一份报文，并声称它来自发送方。

冒充，网络上的某个用户冒充另一个用户接收或发送报文。

篡改，接收方对收到的信息进行篡改。

19、请说明数字签名的主要流程。

(1) 采用散列算法对原始报文进行运算，得到一个固定长度的数字串，称为报文摘要(Message Digest)，不同的报文所得到的报文摘要各异，但对相同的报文它的报文摘要却是惟一的。在数学上保证，只要改动报文中任何一位，重新计算出的报文摘要值就会与原先的值不相符，这样就保证了报文的不可更改性。

（2）发送方用目己的私有密钥对摘要进行加密来形成数字签名。

（3）这个数字签名将作为报文的附件和报文一起发送给接收方。

（4）接收方首先对接收到的原始报文用同样的算法计算出新的报文摘要，再用发送方的公开密钥对报文附件的数字签名进行解密，比较两个报文摘要，如果值相同，接收方就能确认该数字签名是发送方的，否则就认为收到的报文是伪造的或者中途被篡改。

20、数字证书的原理是什么？

数字证书采用公开密钥体制（例如 RSA）。每个用户设定一仅为本人所知的私有密钥，用它进行解密和签名；同时设定一公开密钥，为一组用户所共享，用于加密和验证签名。采用数字证书，能够确认以下两点：

（1）保证信息是由签名者自己签名发送的，签名者不能否认或难以否认。

（2）保证信息自签发后到收到为止未曾做过任何修改，签发的信息是真实信息。

21、解释身份认证的基本概念。

身份认证是指用户必须提供他是谁的证明，这种证实客户的真实身份与其所声称的身份是否相符的过程是为了限制非法用户访问网络资源，它是其他安全机制的基础。

身份认证是安全系统中的第一道关卡，识别身份后，由访问监视器根据用户的身份和授权数据库决定是否能够访问某个资源。一旦身份认证系统被攻破，系统的所有安全措施将形同虚设，黑客攻击的目标往往就是身份认证系统。

22、单机状态下验证用户身份的三种因素是什么？

（1）用户所知道的东西：如口令、密码。

（2）用户所拥有的东西：如智能卡、身份证。

（3）用户所具有的生物特征：如指纹、声音、视网膜扫描、DNA 等。

23、有哪两种主要的存储口令的方式，各是如何实现口令验证的？

（1）直接明文存储口令

有很大风险，只要得到了存储口令的数据库，就可以得到全体人员的口令。比如攻击者可以设法得到一个低优先级的帐号和口令，进入系统后得到明文存储口令的文件，这样他就可以得到全体人员的口令。

（2）Hash 散列存储口令

散列函数的目的是为文件、报文或其他分组数据产生"指纹"。对于每一个用户，系统存储帐号和散列值对在一个口令文件中，当用户登录时，用户输入口令 x，系统计算 F(x)，然后与口令文件中相应的散列值进行比对，成功即允许登录。

24、使用口令进行身份认证的优缺点？

优点在于黑客即使得到了口令文件,通过散列值想要计算出原始口令在计算上也是不可能的，这就相对增加了安全性。

严重的安全问题(单因素的认证)，安全性仅依赖于口令，而且用户往往选择容易记忆、容易被猜测的口令（安全系统最薄弱的突破口），口令文件也可被进行离线的字典式攻击。

25、利用智能卡进行的双因素的认证方式的原理是什么？

智能卡具有硬件加密功能，有较高的安全性。每个用户持有一张智能卡，智能卡存储用户个性化的秘密信息，同时在验证服务器中也存放该秘密信息。进行认证时，用户输入 PIN（个人身份识别码），智能卡认证 PIN，成功后，即可读出智能卡中的秘密信息，进而利用该秘密信息与主机之间进行认证。

双因素的认证方式（PIN+智能卡），即使 PIN 或智能卡被窃取，用户仍不会被冒充。智能卡提供硬件保护措施和加密算法，可以利用这些功能加强安全性能。

26、有哪些生物特征可以作为身份认证的依据，这种认证的过程是怎样的？

以人体唯一的、可靠的、稳定的生物特征（如指纹、虹膜、脸部、掌纹等）为依据，采用计算机强大的计算功能和网络技术进行图象处理和模式识别。该技术具有很好的安全性、可靠性和有效性。

所有的工作有 4 个步骤：抓图、抽取特征、比较和匹配。生物捕捉系统捕捉到生物特征的样品,唯一的特征将会被提取并且被转化成数字符号,这些符号被存成那个人的特征摸板,人们同识别系统交互进行身份认证，以确定匹配或不匹配授权与访问控制

27、解释访问控制的基本概念。

访问控制是建立在身份认证基础上的，通过限制对关键资源的访问，防止非法用户的侵入或因为合法用户的不慎操作而造成的破坏。

访问控制的目的：限制主体对访问客体的访问权限（安全访问策略），从而使计算机系统在合法范围内使用。

28、访问控制有几种常用的实现方法？它们各有什么特点？

（1）访问控制矩阵

行表示客体（各种资源），列表示主体（通常为用户），行和列的交叉点表示某个主体对某个客体的访问权限。通常一个文件的 Own 权限表示可以授予(Authorize)或撤消(Revoke)其他用户对该文件的访问控制权限。

（2）访问能力表

实际的系统中虽然可能有很多的主体与客体，但两者之间的权限关系可能并不多。为了减轻系统的开销与浪费，我们可以从主体（行）出发，表达矩阵某一行的信息，这就是访问能力表（Capabilities）。

只有当一个主体对某个客体拥有访问的能力时，它才能访问这个客体。但是要从访问能力表获得对某一特定客体有特定权限的所有主体就比较困难。在一个安全系统中，正是客体本身需要得到可靠的保护，访问控制服务也应该能够控制可访问某一客体的主体集合，于是出现了以客体为出发点的实现方式--ACL。

（3）访问控制表

也可以从客体（列）出发，表达矩阵某一列的信息，这就是访问控制表（Access Control

List)。它可以对某一特定资源指定任意一个用户的访问权限，还可以将有相同权限的用户分组，并授予组的访问权。

（4）授权关系表

授权关系表(Authorization Relations)的每一行表示了主体和客体的一个授权关系。对表按客体进行排序，可以得到访问控制表的优势；对表按主体进行排序，可以得到访问能力表的优势。适合采用关系数据库来实现。

29、访问控制表 ACL 有什么优缺点？

ACL 的优点：表述直观、易于理解，比较容易查出对某一特定资源拥有访问权限的所有用户，有效地实施授权管理。

ACL 应用到规模大的企业内部网时，有问题：

（1）网络资源很多，ACL 需要设定大量的表项，而且修改起来比较困难，实现整个组织

范围内一致的控制政策也比较困难。

（2）单纯使用 ACL，不易实现最小权限原则及复杂的安全政策。

30、有哪几种访问控制策略？

三种不同的访问控制策略：自主访问控制（DAC）、强制访问控制（MAC）和基于角色的访问控制（RBAC），前两种属于传统的访问控制策略，而 RBAC 是 90 年代后期出现的，有很大的优势，所以发展很快。

每种策略并非是绝对互斥的，我们可以把几种策略综合起来应用从而获得更好、更安全的系统保护--多重的访问控制策略。

31、为什么说在 PKI 中采用公钥技术的关键是如何确认某个人真正的公钥？如何确认？

信息的可认证性是信息安全的一个重要方面。认证的目的有两个：一个是验证信息发送者的真实性，确认他没有被冒充；另一个是验证信息的完整性，确认被验证的信息在传递或存储过程中没有被篡改、重组或延迟。

在认证体制中,通常存在一个可信的第三方,用于仲裁、颁发证书和管理某些机密信息。公钥密码技术可以提供网络中信息安全的全面解决方案。采用公钥技术的关键是如何确认某个人真正的公钥。在 PKI 中，为了确保用户及他所持有密钥的正确性，公开密钥系统需要一个值得信赖而且独立的第三方机构充当认证中心(CA),来确认声称拥有公开密钥的人的真正身份。

要确认一个公共密钥，CA 首先制作一张"数字证书"，它包含用户身份的部分信息及用户所持有的公开密钥，然后 CA 利用本身的私钥为数字证书加上数字签名。

任何想发放自己公钥的用户，可以去认证中心(CA)申请自己的证书。CA 中心在认证该人的真实身份后，颁发包含用户公钥的数字证书，它包含用户的真实身份、并证实用户公钥的有效期和作用范围(用于交换密钥还是数字签名)。其他用户只要能验证证书是真实的，并且信任颁发证书的 CA，就可以确认用户的公钥。

32、什么是数字证书？现有的数字证书由谁颁发，遵循什么标准，有什么特点？

数字证书是一个经证书认证中心(CA)数字签名的包含公开密钥拥有者信息以及公开密钥的文件。认证中心(CA)作为权威的、可信赖的、公正的第三方机构，专门负责为各种认证需求提供数字证书服务。认证中心颁发的数字证书均遵循 X.509 V3 标准。X.509 标准在编排公共密钥密码格式方面已被广为接受。X.509 证书已应用于许多网络安全，其中包括 IPSec(IP 安全)、SSL、SET、S/MIME。

33、X.509 规范中是如何定义实体 A 信任实体 B 的？在 PKI 中信任又是什么具体含义？

X.509 规范中给出了适用于我们目标的定义：

当实体 A 假定实体 B 严格地按 A 所期望的那样行动，则 A 信任 B。在 PKI 中，我们可以把这个定

义具体化为:如果一个用户假定 CA 可以把任一公钥绑定到某个实体上,则他信任该 CA。

34、简述认证机构的严格层次结构模型的性质？

层次结构中的所有实体都信任惟一的根 CA。在认证机构的严格层次结构中，每个实体(包括中介 CA 和终端实体)都必须拥有根 CA 的公钥,该公钥的安装是在这个模型中为随后进行的所有通信进行证书处理的基础，因此，它必须通过一种安全（带外）的方式来完成。

值得注意的是，在一个多层的严格层次结构中.终端实体直接被其上层的 CA 认证(也就是颁发证书)，但是它们的信任锚是另一个不同的 CA (根 CA)。

35、Web 信任模型有哪些安全隐患？

Web 模型在方便性和简单互操作性方面有明显的优势,但是也存在许多安全隐患。例如,因为浏览器的用户自动地信任预安装的所有公钥,所以即使这些根 CA 中有一个是"坏的"(例如，该 CA 从没有认真核实被认证的实体)，安全性将被完全破坏。

另外一个潜在的安全隐患是没有实用的机制来撤消嵌入到浏览器中的根密钥。如果发现一个根密钥是"坏的"(就像前而所讨论的那样)或者与根的公钥相应的私钥被泄密了,要使全世界数百万个浏览器都自动地废止该密钥的使用是不可能的。

36、以用户为中心的信任模型是怎样实现信任关系的？哪个实际系统是使用这种模型的？

PGP 最能说明以用户为中心的信任模型，在 PGP 中，一个用户通过担当 CA（签署其他实体的公钥）并使其公钥被其他人所认证来建立（或参加）所谓的信任网（Web of Trust)。

例如，当 Alice 收到一个据称属于 Bob 的证书时，她将发现这个证书是由她不认识的 David 签署的,但是 David 的证书是由她认识并且信任的 Catherine 签署的。在这种情况下，Alice 可以决定信任 Bob 的密钥（即信任从 Catherine 到 David 再到 Bob 的密钥链)，也可以决定不信任 Bob 的密钥（认为"未知的"Bob 与"已知的"Catherine 之间的"距离大远")。

因为要依赖于用户自身的行为和决策能力,因此以用户为中心的模型在技术水平较高和利害关系高度一致的群体中是可行的，但是在一般的群体（它的许多用户有极少或者没有安全及 PKI 的概念）中是不现实的。

37、构造证书库的最佳方法是什么？

证书库是证书的集中存放地，是网上的一种公共信息库，用户可以从此处获得其他用户的证书和公钥。构造证书库的最佳方法是采用支持 LDAP 协议的目录系统，用户或相关的应用通过 LDAP 来访问证书库。系统必须确保证书库的完整性，防止伪造、篡改证书

38、什么是 X.500 目录服务？

X.500 是一种 CCITT 针对已经被 ISO 接受的目录服务系统的建议，它定义了一个机构如何在一个企业的全局范围内共享名字和与它们相关的对象。

一个完整的 X.500 系统称为一个"目录"，X.500 是层次性的，其中的管理性域(机构、分支、部门和工作组)可以提供这些域内的用户和资源的信息。它被认为是实现一个目录服务的最好途径。

X.500 目录服务是一种用于开发一个单位内部人员目录的标准方法，这个目录可以成为全球目录的一部分，任何人都可以查询这个单位中人员的信息。这个目录有一个树型结构:国家，单位(或组织)，部门和个人。一个知名和最大的 X.500 目录是用于管理域名注册的 InterNIC。

X.500 目录服务可以向需要访问网络任何地方资源的电子函件系统和应用，或需要知道

在网络上的实体名字和地点的管理系统提供信息。这个目录是一个目录信息数据库(DIB)。

39、什么是 X.509 方案，它是如何实现数字签名的？

X.509 是一种行业标准或者行业解决方案--X.509 公共密钥证书，在 X.509 方案中，默认的加密体制是公钥密码体制。

为进行身份认证，X.509 标准及公共密钥加密系统提供了数字签名的方案。用户可生成一段信息及其摘要(指纹)。用户用专用密钥对摘要加密以形成签名，接收者用发送者的公共密钥对签名解密，并将之与收到的信息"指纹"进行比较，以确定其真实性。

40、X.500 和 LDAP 有什么联系和区别？

LDAP 协议基于 X.500 标准，但是比较简单，并且可以根据需要定制，LDAP 支持 TCP/IP。在企业范围内实现LDAP可以让运行在几乎所有计算机平台上的所有的应用程序从LDAP目录中获取信息（电子邮件地址、邮件路由信息、人力资源数据、公用密钥、联系人列表）。

41、实施 PKI 的过程中产生了哪些问题，如何解决？

首先是实施的问题，PKI 定义了严格的操作协议和信任层次关系。任何向 CA 申请数字证书的人必须经过线下(offline)的身份验证(通常由 RA 完成)，这种身份验证工作很难扩展到整个 Internet 范围，因此，现今构建的 PKI 系统都局限在一定范围内，这造成了 PKI 系统扩展问题。

由于不同 PKI 系统都定义了各自的信任策略，在进行互相认证的时候，为了避免由于信任策略不同而产生的问题，普遍的做法是忽略信任策略。这样，本质上是管理 Internet 上的信任关系的 PKI 就仅仅起到身份验证的作用了。

提出用 PMI 解决。

42、什么是证书链？根 CA 证书由谁签发？

由于一个公钥用户拥有的可信证书管理中心数量有限，要与大量不同管理域的用户建立安全通信需要 CA 建立信任关系，这样就要构造一个证书链。证书链是最常用的用于验证实体它的公钥之间的绑定的方法。一个证书链一般是从根 CA 证书开始，前一个证书主体是后一个证书的签发者。也就是说，该主题对后一个证书进行了签名。而根 CA 证书是由根自己签发的。

43、叙述基于 X.509 数字证书在 PKI 中的作用。

X.509 数字证书是各实体在网络中的身份证明，它证书了实体所声明的身份与其公钥的匹配关系。从公钥管理的机制讲，数字证书是非对称密码体制中密钥管理的媒介。即在非对称密码体制中，公钥的分发、传送是通过数字证书来实现的。通过数字证书，可以提供身份的认证与识别，完整性、保密性和不可否认等安全服务。

44、电子邮件存在哪些安全性问题？

1）垃圾邮件包括广告邮件、骚扰邮件、连锁邮件、反动邮件等。垃圾邮件会增加网络负荷，影响网络传输速度，占用邮件服务器的空间。

2）诈骗邮件通常指那些带有恶意的欺诈性邮件。利用电子邮件的快速、便宜，发信人能迅速让大量受害者上当。

3）邮件炸弹指在短时间内向同一信箱发送大量电子邮件的行为，信箱不能承受时就会崩溃。

4）通过电子邮件传播的病毒通常用 VBScript 编写，且大多数采用附件的形式夹带在电子邮件中。当收信人打开附件后，病毒会查询他的通讯簿，给其上所有或部分人发信，并将自身放入附件中，以此方式继续传播扩散。

45、端到端的安全电子邮件技术，能够保证邮件从发出到接收的整个过程中的哪三种安全性？

端到端的安全电子邮件技术，保证邮件从被发出到被接收的整个过程中，内容保密、无法修改、并且不可否认。目前的 Internet 上，有两套成型的端到端安全电子邮件标准：PGP 和 S/MIME。它一般只对信体进行加密和签名，　　而信头则由于邮件传输中寻址和路由的需要，必须保证原封不动。

46、为什么 PGP 在加密明文之前先压缩它？

PGP 内核使用 Pkzip 算法来压缩加密前的明文。一方面对电子邮件而言，压缩后加密再经过 7 位编码密文有可能比明文更短，这就节省了网络传输的时间。另一方面，经过压缩的明文，实际上相当于多经过了一次变换，信息更加杂乱无章，能更强地抵御攻击

47、在服务器端和用户端各有哪些方式防范垃圾邮件？

在服务器端，应该设置发信人身份认证，以防止自己的邮件服务器被选做垃圾邮件的传递者。现在包括不少国内知名电子邮件提供者在内的诸多邮件服务器被国外的拒绝垃圾邮件组织列为垃圾邮件来源。结果是：所有来自该服务器的邮件全部被拒收!

48、什么是 SET 电子钱包？

SET 交易发生的先决条件是，每个持卡人(客户)必须拥有一个惟一的电子(数字)证书，且由客户确定口令，并用这个口令对数字证书、私钥、信用卡号码及其他信息进行加密存储，这些与符合 SET 协议的软件一起组成了一个 SET 电子钱包。

49、简述一个成功的 SET 交易的标准流程。

(1) 客户在网上商店选中商品并决定使用电子钱包付款，商家服务器上的 POS 软件发报文给客户的浏览器要求电子钱包付款。

(2) 电子钱包提示客户输入口令后与商家服务器交换"握手"消息，确认客户、商家均为合法，初始化支付请求和支付响应。

(3) 客户的电子钱包形成一个包含购买订单、支付命令(内含加密了的客户信用卡号码)的报文发送给商家。

(4) 商家 POS 软件生成授权请求报文(内含客户的支付命令)，发给收单银行的支付网关。

(5) 支付网关在确认客户信用卡没有超过透支额度的情况下，向商家发送一个授权响应报文。

(6) 商家向客户的电子钱包发送一个购买响应报文，交易结束，客户等待商家送货上

50、什么是防火墙，为什么需要有防火墙？

防火墙是一种装置，它是由软件/硬件设备组合而成，通常处于企业的内部局域网与 Internet 之间，限制 Internet 用户对内部网络的访问以及管理内部用户访问 Internet 的权限。换言之，一个防火墙在一个被认为是安全和可信的内部网络和一个被认为是不那么安全和可信的外部网络(通常是 Internet)之间提供一个封锁工具。

如果没有防火墙，则整个内部网络的安全性完全依赖于每个主机，因此，所有的主机都必须达到一致的高度安全水平，这在实际操作时非常困难。而防火墙被设计为只运行专用的访问控制软件的设备，没有其他的服务，因此也就意味着相对少一些缺陷和安全漏洞，这就使得安全管理变得更为方便，易于控制，也会使内部网络更加安全。

火墙所遵循的原则是在保证网络畅通的情况下，尽可能保证内部网络的安全。它是一种被动的技术，是一种静态安全部件。

51、防火墙应满足的基本条件是什么？

作为网络间实施网间访问控制的一组组件的集合，防火墙应满足的基本条件如下：

(1) 内部网络和外部网络之间的所有数据流必须经过防火墙。

(2) 只有符合安全策略的数据流才能通过防火墙。

(3) 防火墙自身具有高可靠性，应对渗透(Penetration)免疫，即它本身是不可被侵入的。

52、列举防火墙的几个基本功能？

(1) 隔离不同的网络，限制安全问题的扩散，对安全集中管理，简化了安全管理的复杂程度。

(2) 防火墙可以方便地记录网络上的各种非法活动，监视网络的安全性，遇到紧急情况报警。

(3) 防火墙可以作为部署 NAT 的地点，利用 NAT 技术，将有限的 IP 地址动态或静态地与内部的 IP 地址对应起来，用来缓解地址空间短缺的问题或者隐藏内部网络的结构。

(4) 防火墙是审计和记录 Internet 使用费用的一个最佳地点。

(5) 防火墙也可以作为 IPSec 的平台。

(6) 内容控制功能。根据数据内容进行控制，比如防火墙可以从电子邮件中过滤掉垃圾邮件，可以过滤掉内部用户访问外部服务的图片信息。只有代理服务器和先进的过滤才能实现。

53、状态检测防火墙的原理是什么，相对包过滤防火墙有什么优点？

状态检测又称动态包过滤，所以状态检测防火墙又称动态防火墙，最早由 CheckPoint 提出。

状态检测是一种相当于 4、5 层的过滤技术，既提供了比包过滤防火墙更高的安全性和更灵活的处理，也避免了应用层网关的速度降低问题。要实现状态检测防火墙，最重要的是实现连接的跟踪功能，并且根据需要可动态地在过滤规则中增加或更新条目。防火墙应当包含关于包最近已经通过它的"状态信息"，以决定是否让来自 Internet 的包通过或丢弃。

54、应用层网关的工作过程是什么？它有什么优缺点？

主要工作在应用层，又称为应用层防火墙。它检查进出的数据包，通过自身复制传递数据，防止在受信主机与非受信主机间直接建立联系。应用层网关能够理解应用层上的协议，能够做复杂的访问控制，并做精细的注册和审核。

基本工作过程是：当客户机需要使用服务器上的数据时，首先将数据请求发给代理服务器，代理服务器再根据这一请求向服务器索取数据，然后再由代理服务器将数据传输给客户机。

常用的应用层网关已有相应的代理服务软件，如 HTTP、SMTP、FTP、Telnet 等，但是对于新开发的应用，尚没有相应的代理服务，它们将通过网络层防火墙和一般的代理服务。

应用层网关有较好的访问控制能力，是目前最安全的防火墙技术。能够提供内容过滤、用户认证、页面缓存和 NAT 等功能。但实现麻烦，有的应用层网关缺乏"透明度"。应用层网关每一种协议需要相应的代理软件，使用时工作量大，效率明显不如网络层防火墙。

55、代理服务器有什么优缺点？

代理服务技术的优点是：隐蔽内部网络拓扑信息；网关理解应用协议，可以实施更细粒度的访问控制；较强的数据流监控和报告功能。（主机认证和用户认证）缺点是对每一类应用都需要一个专门的代理，灵活性不够；每一种网络应用服务的安全问题各不相同，分析困难，因此实现困难。速度慢。

56、静态包过滤和动态包过滤有什么不同？

静态包过滤在遇到利用动态端口的协议时会发生困难，如 FTP，防火墙事先无法知道哪些端口需要打开，就需要将所有可能用到的端口打开，会给安全带来不必要的隐患。

而状态检测通过检查应用程序信息(如 FTP 的 PORT 和 PASV 命令)，来判断此端口是否需要临时打开，而当传输结束时，端口又马上恢复为关闭状态。

57、解释 VPN 的基本概念。

VPN 是 Virtual Private Network 的缩写，是将物理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。

Virtual 是针对传统的企业"专用网络"而言的。VPN 则是利用公共网络资源和设备建立一个逻辑上的专用通道，尽管没有自己的专用线路，但它却可以提供和专用网络同样的功能。

Private 表示 VPN 是被特定企业或用户私有的，公共网络上只有经过授权的用户才可以使用。在该通道内传输的数据经过了加密和认证，保证了传输内容的完整性和机密性。

58、简述 VPN 使用了哪些主要技术。

1）隧道（封装）技术是目前实现不同 VPN 用户业务区分的基本方式。一个 VPN 可抽象为一个没有自环的连通图，每个顶点代表一个 VPN 端点（用户数据进入或离开 VPN 的设备端口），相邻顶点之间的边表示连结这两对应端点的逻辑通道，即隧道。

隧道以叠加在 IP 主干网上的方式运行。需安全传输的数据分组经一定的封装处理，从信源的一个 VPN 端点进入 VPN，经相关隧道穿越 VPN（物理上穿越不安全的互联网），到达信宿的另一个 VPN 端点，再经过相应解封装处理，便得到原始数据。（不仅指定传送的路径，在中转节点也不会解析原始数据）

2）当用户数据需要跨越多个运营商的网络时，在连接两个独立网络的节点该用户的数据分组需要被解封装和再次封装，可能会造成数据泄露，这就需要用到加密技术和密钥管理技术。目前主要的密钥交换和管理标准有 SKIP 和 ISAKMP（安全联盟和密钥管理协议）。

3）对于支持远程接入或动态建立隧道的 VPN，在隧道建立之前需要确认访问者身份，是否可以建立要求的隧道，若可以，系统还需根据访问者身份实施资源访问控制。这需要访问者与设备的身份认证技术和访问控制技术。

59、简述常见的黑客攻击过程。

（1）目标探测和信息攫取

先确定攻击目标并收集目标系统的相关信息。一般先大量收集网上主机的信息，然后根据各系统的安全性强弱确定最后的目标。

1）踩点（Footprinting）

黑客必须尽可能收集目标系统安全状况的各种信息。Whois 数据库查询可以获得很多关于目标系统的注册信息，DNS 查询(用 Windows/UNIX 上提供的 nslookup 命令客户端)也可令黑客获得关于目标系统域名、IP 地址、DNS 务器、邮件服务器等有用信息。此外还可以用 traceroute 工具获得一些网络拓扑和路由信息。

2）扫描（Scanning）

在扫描阶段，我们将使用各种工具和技巧(如 Ping 扫射、端口扫描以及操作系统检测等)确定哪些系统存活着、它们在监听哪些端口(以此来判断它们在提供哪些服务)，甚至更进一步地获知它们运行的是什么操作系统。

3）查点（Enumeration）

从系统中抽取有效账号或导出资源名的过程称为查点，这些信息很可能成为目标系统的祸根。比如说，一旦查点查出一个有效用户名或共享资源，攻击者猜出对应的密码或利用与资源共享协议关联的某些脆弱点通常就只是一个时间问题了。查点技巧差不多都是特定于操作系统的，因此要求使用前面步骤汇集的信息。

（2）获得访问权（Gaining Access）

通过密码窃听、共享文件的野蛮攻击、攫取密码文件并破解或缓冲区溢出攻击等来获得系统的访问权限。

（3）特权提升（Escalating Privilege）

在获得一般账户后，黑客经常会试图获得更高的权限，比如获得系统管理员权限。通常可以采用密码破解(如用LOphtcrack破解NT的SAM文件)、利用已知的漏洞或脆弱点等技术。

（4）窃取（Stealing）

对敏感数据进行篡改、添加、删除及复制（如Windows系统的注册表、UNIX的rhost文件等）。

（5）掩盖踪迹（Covering Tracks）

此时最重要就隐藏自己踪迹，以防被管理员发觉，比如清除日志记录、使用rootkits等工具。

（6）创建后门（Creating Bookdoor）

在系统的不同部分布置陷阱和后门，以便入侵者在以后仍能从容获得特权访问。

60、什么是病毒的特征代码？它有什么作用？

病毒的特征代码是病毒程序编制者用来识别自己编写程序的唯一代码串。因此检测病毒程序可利用病毒的特征代码来检测病毒，以防止病毒程序感染。

61、什么是网络蠕虫？它的传播途径是什么？

网络蠕虫是一种可以通过网络（永久连接网络或拨号网络）进行自身复制的病毒程序。一旦在系统中激活,蠕虫可以表现得象计算机病毒或细菌。可以向系统注入特洛伊木马程序，或者进行任何次数的破坏或毁灭行动。普通计算机病毒需要在计算机的硬件或文件系统中繁殖，而典型的蠕虫程序会在内存中维持一个活动副本。蠕虫是一个独立运行的程序，自身不改变其他的程序，但可以携带一个改变其他程序功能的病毒。

62、系统阐述“ICMP很适合传输后门命令”的原因。

答：

（1）ICMP不包括端口的概念。端口是一个TCP和UDP的概念，用于编制和区分用于通信的资源和目的的文件处理终端。由于ICMP和端口无关，通过ICMP查找命令传输的后门监听程序就不会像基于TCP和UDP协议的工具一样显示出来。

（2）许多网络允许某些类型的ICMP信息通过防火墙，但是却阻止大部分TCP和UDP通信。

（3）有效字段可在任意一个ICMP消息的类型末尾被弄丢。攻击者可以利用将要发送给后门的指令加在这个有效字段，任何来自后门的响应可以同样地传回给另一个ICMP消息的有效字段

63、如何防范SQL注入攻击

答：通过以下若干方法来防范SQL注入攻击。

（1）对前台传入参数按的数据类型，进行严格匹配（如查看描述数据类型的变量字符串中，是否存在字母）。

（2）对于单一变量（如上面的K，N）如果有必要，过滤或替换掉输入数据中的空

（3）将一个单引号（“’”），替换成两个连续的单引号（“’’”）。

（4）限制输入数据的有效字符种类，排除对数据库操作有特殊意义的字符（如“--”）。

（5）限制表单或查询字符串输入的长度。

（6）用存储过程来执行所有的查询。

（7）检查提取数据的查询所返回的记录数量。如果程序只要求返回一个记录，但实际返回的记录却超过一行，那就当作出错处理。

（8）将用户登录名称、密码等数据加密保存。加密用户输入的数据，然后再将它与数据库中保存的数据比较，这相当于对用户输入的数据进行了“消毒”处理，用户输入的数据不再对数据库有任何特殊的意义，从而也就防止了攻击者注入 SQL 命令。

总而言之，就是要尽可能地限制用户可以存取的数据总数。另外，对用户要按“最小特权”安全原则分配权限，即使发生了 SQL 注入攻击，结果也被限制在那些可以被正常访问到的数据中。

64、请解释 5 种"窃取机密攻击"方式的含义。

（1）网络踩点（Footprinting）

攻击者事先汇集目标的信息，通常采用 Whois、Finger、Nslookup、Ping 等工具获得目标的一些信息，如域名、IP 地址、网络拓扑结构、相关的用户信息等，这往往是黑客入侵所做的第一步工作。

（2）扫描攻击（Scanning）

这里的扫描主要指端口扫描，通常采用 Nmap 等各种端口扫描工具，可以获得目标计算机的一些有用信息，比如机器上打开了哪些端口，这样就知道开设了哪些网络服务。黑客就可以利用这些服务的漏洞，进行进一步的入侵。这往往是黑客入侵所做的第二步工作。

（3）协议栈指纹（Stack Fingerprinting）鉴别（也称操作系统探测）

黑客对目标主机发出探测包，由于不同OS厂商的IP协议栈实现之间存在许多细微差别，因此每种 OS 都有其独特的响应方法，黑客经常能够确定目标主机所运行的 OS。这往往也可以看作是扫描阶段的一部分工作。

（4）信息流嗅探（Sniffering）

通过在共享局域网中将某主机网卡设置成混杂（Promiscuous）模式，或在各种局域网中某主机使用 ARP 欺骗，该主机就会接收所有经过的数据包。基于这样的原理，黑客可以使用一个嗅探器（软件或硬件）对网络信息流进行监视，从而收集到帐号和口令等信息。
这是黑客入侵的第三步工作。

（5）会话劫持（Session Hijacking）

所谓会话劫持，就是在一次正常的通信过程中，黑客作为第三方参与到其中，或者是在数据流里注射额外的信息，或者是将双方的通信模式暗中改变，即从直接联系变成交由黑客中转。这种攻击方式可认为是黑客入侵的第四步工作--真正的攻击中的一种。

65、请解释 5 种"非法访问"攻击方式的含义。

（1）口令破解

攻击者可以通过获取口令文件然后运用口令破解工具进行字典攻击或暴力攻击来获得口令，也可通过猜测或窃听等方式获取口令，从而进入系统进行非法访问，选择安全的口令非常重要。这也是黑客入侵中真正攻击方式的一种。

（2）IP 欺骗

攻击者可通过伪装成被信任源 IP 地址等方式来骗取目标主机的信任，这主要针对 Linux/UNIX 下建立起 IP 地址信任关系的主机实施欺骗。这也是黑客入侵中真正攻击方式的一种。

（3）DNS 欺骗

当 DNS 服务器向另一个 DNS 服务器发送某个解析请求（由域名解析出 IP 地址）时，因为不进行身份验证，这样黑客就可以冒充被请求方，向请求方返回一个被篡改了的应答（IP 地址），将用户引向黑客设定的主机。这也是黑客入侵中真正攻击方式的一种。

（4）重放（Replay）攻击

在消息没有时间戳的情况下，攻击者利用身份认证机制中的漏洞先把别人有用的消息记录下来，过一段时间后再发送出去。

（5）特洛伊木马（Trojan Horse）

把一个能帮助黑客完成某一特定动作的程序依附在某一合法用户的正常程序中，而一旦用户触发正常程序，黑客代码同时被激活，这些代码往往能完成黑客早已指定的任务（如监听某个不常用端口，假冒登录界面获取帐号和口令等）。

66、请解释下列网络信息安全的要素。

保密性、完整性、可用性、可存活性

67、列举并解释 ISO/OSI 中定义的 5 种标准的安全服务。

（1）鉴别

用于鉴别实体的身份和对身份的证实，包括对等实体鉴别和数据原发鉴别两种。

（2）访问控制

提供对越权使用资源的防御措施。

（3）数据机密性

针对信息泄露而采取的防御措施。分为连接机密性、无连接机密性、选择字段机密性、通信业务流机密性四种。

（4）数据完整性

防止非法篡改信息，如修改、复制、插入和删除等。分为带恢复的连接完整性、无恢复的连接完整性、选择字段的连接完整性、无连接完整性、选择字段无连接完整性五种。

（5）抗否认

是针对对方否认的防范措施，用来证实发生过的操作。包括有数据原发证明的抗否认和有交付证明的抗否认两种。

68、常规加密密钥的分配有几种方案，请对比一下它们的优缺点。

（1）集中式密钥分配方案

由一个中心节点或者由一组节点组成层次结构负责密钥的产生并分配给通信的双方，在这种方式下，用户不需要保存大量的会话密钥，只需要保存同中心节点的加密密钥，用于安全传送由中心节点产生的即将用于与第三方通信的会话密钥。这种方式缺点是通信量大，同时需要较好的鉴别功能以鉴别中心节点和通信方。目前这方面主流技术是密钥分配中心 KDC 技术。我们假定每个通信方与密钥分配中心 KDC 之间都共享一个惟一的主密钥，并且这个惟一的主密钥是通过其他安全的途径传递。

（2）分散式密钥分配方案

使用密钥分配中心进行密钥的分配要求密钥分配中心是可信任的并且应该保护它免于被破坏。如果密钥分配中心被第三方破坏，那么所有依靠该密钥分配中心分配会话密钥进行通信的所有通信方将不能进行正常的安全通信。如果密钥分配中心被第三方控制，那么所有依靠该密钥分配中心分配会话密钥进行进信的所有通信方之间的通信信息将被第三方窃听到。

69、电子邮件存在哪些安全性问题？

1）垃圾邮件包括广告邮件、骚扰邮件、连锁邮件、反动邮件等。垃圾邮件会增加网络负荷，影响网络传输速度，占用邮件服务器的空间。

2）诈骗邮件通常指那些带有恶意的欺诈性邮件。利用电子邮件的快速、便宜，发信人能迅速让大量受害者上当。

3）邮件炸弹指在短时间内向同一信箱发送大量电子邮件的行为，信箱不能承受时就会

崩溃。

4）通过电子邮件传播的病毒通常用 VBScript 编写，且大多数采用附件的形式夹带在电子邮件中。当收信人打开附件后，病毒会查询他的通讯簿，给其上所有或部分人发信，并将自身放入附件中，以此方式继续传播扩散。

70、端到端的安全电子邮件技术，能够保证邮件从发出到接收的整个过程中的哪三种安全性？

端到端的安全电子邮件技术，保证邮件从被发出到被接收的整个过程中，内容保密、无法修改、并且不可否认。目前的 Internet 上，有两套成型的端到端安全电子邮件标准：PGP 和 S/MIME。它一般只对信体进行加密和签名，　　而信头则由于邮件传输中寻址和路由的需要，必须保证原封不动。

71、讨论一下为什么 CGI 出现的漏洞对 Web 服务器的安全威胁最大？

相比前面提到的问题，CGI 可能出现的漏洞很多，而被攻破后所能造成的威胁也很大。程序设计人员的一个简单的错误或不规范的编程就可能为系统增加一个安全漏洞。一个故意放置的有恶意的 CGI 程序能够自由访问系统资源，使系统失效、删除文件或查看顾客的保密信息(包括用户名和口令)。

72、比较 JavaApplet 和 ActiveX 实现安全性的不同。

JavaApplet 就是活动内容的一种。它使用 Java 语言开发，可以实现各种各样的客户端应用。这些 Applet 随页面下载下来，只要浏览器兼容 Java，它就可在客户机上自动运行。Java 使用沙盒(Sandbox)根据安全模式所定义的规则来限制 JavaApplet 的活动。

ActiveX 是另一种活动内容的形式，可以用许多程序设汁语言来开发，但它只能运行在安装 Windows 的计算机上。ActiveX 在安全性方面不如 JavaApplet。一旦下载，它就能像其他程序一样执行，能访问包括操作系统代码在内的所有系统资源，这是非常危险的。

73、说明 SSL 的概念和功能。

安全套接层协议 SSL 主要是使用公开密钥体制和 X.509 数字证书技术保护信息传输的机密性和完整性，但它不能保证信息的不可抵赖性，主要适用于点对点之间的信息传输。它是 Netscape 公司提出的基于 Web 应用的安全协议，它包括服务器认证、客户认证(可选)、SSL 链路上的数据完整性和 SSL 链路上的数据保密性。SSL 通过在浏览器软件和 Web 服务器之间建立一条安全通道，实现信息在 Internet 中传送的保密性。

在 TCP/IP 协议族中，SSL 位于 TCP 层之上、应用层之下。这使它可以独立于应用层，从而使应用层协议可以直接建立在 SSL 之上。SSL 协议包括以下一些子协议;SSL 记录协议、SSL 握手协议、SSL 更改密码说明协议和 SSL 警告协议。SSL 记录协议建立在可靠的传输协议(例如 TCP)上，用来封装高层的协议。SSL 握手协议准许服务器端与客户端在开始传输数据前，能够通过特定的加密算法相互鉴别。

74、什么是 SET 电子钱包？

SET 交易发生的先决条件是，每个持卡人(客户)必须拥有一个惟一的电子(数字)证书，且由客户确定口令，并用这个口令对数字证书、私钥、信用卡号码及其他信息进行加密存储，这些与符合 SET 协议的软件一起组成了一个 SET 电子钱包。

75、简述 SSL 的记录协议和握手协议。

SSL 记录协议是建立在可靠的传输协议（如 TCP）之上，为更高层提供基本的安全服务，如提供数据封装、眼所、加密等基本功能的支持。

SSL 记录协议用来定义数据传输的格式，它包括的记录头和记录数据格式的规定。在 SSL 协议中，所有的传输数据都被封装在记录中。

SSL 握手协议负责建立当前会话状态的参数。双方协商一个协议版本，选择密码算法，相互认证（不是必须的），并且使用公钥加密技术通过一系列交换的消息在客户端和服务器之间生成共享密钥。

76、什么是防火墙，为什么需要有防火墙？

防火墙是一种装置，它是由软件/硬件设备组合而成，通常处于企业的内部局域网与 Internet 之间，限制 Internet 用户对内部网络的访问以及管理内部用户访问 Internet 的权限。换言之，一个防火墙在一个被认为是安全和可信的内部网络和一个被认为是不那么安全和可信的外部网络(通常是 Internet)之间提供一个封锁工具。

如果没有防火墙，则整个内部网络的安全性完全依赖于每个主机，因此，所有的主机都必须达到一致的高度安全水平，这在实际操作时非常困难。而防火墙被设计为只运行专用的访问控制软件的设备，没有其他的服务，因此也就意味着相对少一些缺陷和安全漏洞，这就使得安全管理变得更为方便，易于控制，也会使内部网络更加安全。

防火墙所遵循的原则是在保证网络畅通的情况下，尽可能保证内部网络的安全。它是一种被动的技术，是一种静态安全部件。

77、防火墙应满足的基本条件是什么？

作为网络间实施网间访问控制的一组组件的集合，防火墙应满足的基本条件如下：

(1) 内部网络和外部网络之间的所有数据流必须经过防火墙。

(2) 只有符合安全策略的数据流才能通过防火墙。

(3) 防火墙自身具有高可靠性，应对渗透(Penetration)免疫，即它本身是不可被侵入的。

78、列举防火墙的几个基本功能？

(1) 隔离不同的网络，限制安全问题的扩散，对安全集中管理，简化了安全管理的复杂程度。

(2) 防火墙可以方便地记录网络上的各种非法活动，监视网络的安全性，遇到紧急情况报警。

(3) 防火墙可以作为部署 NAT 的地点，利用 NAT 技术，将有限的 IP 地址动态或静态地与内部的 IP 地址对应起来，用来缓解地址空间短缺的问题或者隐藏内部网络的结构。

(4) 防火墙是审计和记录 Internet 使用费用的一个最佳地点。

(5) 防火墙也可以作为 IPSec 的平台。

(6) 内容控制功能。根据数据内容进行控制，比如防火墙可以从电子邮件中过滤掉垃圾邮件，可以过滤掉内部用户访问外部服务的图片信息。只有代理服务器和先进的过滤才能实现。

79、包过滤防火墙的过滤原理是什么？

包过滤防火墙也称分组过滤路由器，又叫网络层防火墙，因为它是工作在网络层。路由器便是一个网络层防火墙，因为包过滤是路由器的固有属性。它一般是通过检查单个包的地址、协议、端口等信息来决定是否允许此数据包通过，有静态和动态两种过滤方式。

这种防火墙可以提供内部信息以说明所通过的连接状态和一些数据流的内容，把判断的信息同规则表进行比较，在规则表中定义了各种规则来表明是否同意或拒绝包的通过。包过滤防火墙检查每一条规则直至发现包中的信息与某规则相符。如果没有一条规则能符合，防火墙就会使用默认规则（丢弃该包）。在制定数据包过滤规则时，一定要注意数据包是双向的。

80、状态检测防火墙的原理是什么，相对包过滤防火墙有什么优点？

状态检测又称动态包过滤，所以状态检测防火墙又称动态防火墙，最早由 CheckPoint 提出。

状态检测是一种相当于 4、5 层的过滤技术，既提供了比包过滤防火墙更高的安全性和更灵活的处理，也避免了应用层网关的速度降低问题。要实现状态检测防火墙，最重要的是实现连接的跟踪功能，并且根据需要可动态地在过滤规则中增加或更新条目。防火墙应当包含关于包最近已经通过它的“状态信息”，以决定是否让来自 Internet 的包通过或丢弃。

81、应用层网关的工作过程是什么？它有什么优缺点？

主要工作在应用层，又称为应用层防火墙。它检查进出的数据包，通过自身复制传递数据，防止在受信主机与非受信主机间直接建立联系。应用层网关能够理解应用层上的协议，能够做复杂的访问控制，并做精细的注册和审核。

基本工作过程是：当客户机需要使用服务器上的数据时，首先将数据请求发给代理服务器，代理服务器再根据这一请求向服务器索取数据，然后再由代理服务器将数据传输给客户机。

常用的应用层网关已有相应的代理服务软件，如 HTTP、SMTP、FTP、Telnet 等，但是对于新开发的应用，尚没有相应的代理服务，它们将通过网络层防火墙和一般的代理服务。

应用层网关有较好的访问控制能力，是目前最安全的防火墙技术。能够提供内容过滤、用户认证、页面缓存和 NAT 等功能。但实现麻烦，有的应用层网关缺乏“透明度”。应用层网关每一种协议需要相应的代理软件，使用时工作量大，效率明显不如网络层防火墙。

82、代理服务器有什么优缺点？

代理服务技术的优点是：隐蔽内部网络拓扑信息；网关理解应用协议，可以实施更细粒度的访问控制；较强的数据流监控和报告功能。（主机认证和用户认证）缺点是对每一类应用都需要一个专门的代理，灵活性不够；每一种网络应用服务的安全问题各不相同，分析困难，因此实现困难。速度慢。

83、什么是堡垒主机，它有什么功能？

堡垒主机(Bastion Host) 的硬件是一台普通的主机（其操作系统要求可靠性好、可配置性好），它使用软件配置应用网关程序，从而具有强大而完备的功能。它是内部网络和 Internet 之间的通信桥梁，它中继（不允许转发）所有的网络通信服务，并具有认证、访问控制、日志记录、审计监控等功能。它作为内部网络上外界惟一可以访问的点，在整个防火墙系统中起着重要的作用，是整个系统的关键点。

84、什么是双宿主机模式，如何提高它的安全性？

双宿主主机模式是最简单的一种防火墙体系结构，该模式是围绕着至少具有两个网络接口的堡垒主机构成的。双宿主主机内外的网络均可与双宿主主机实施通信，但内外网络之间不可直接通信（不能直接转发）。双宿主主机可以通过代理或让用户直接到其上注册来提供很高程度的网络控制。

由于双宿主机直接暴露在外部网络中，如果入侵者得到了双宿主主机的访问权（使其成为一个路由器），内部网络就会被入侵，所以为了保证内部网的安全，双宿主主机首先要禁止网络层的路由功能，还应具有强大的身份认证系统，尽量减少防火墙上用户的账户数。

85、边界防火墙有哪些缺陷？分布式防火墙的组成是什么，它有哪些优势？

首先是结构性限制。随着企业业务规模的扩大，数据信息的增长，使得企业网的边界已成为一个逻辑边界的概念，物理的边界日趋模糊，因此边界防火墙的应用受到越来越多的结构性限制。

其次是内部威胁。当攻击来自信任的地带时，边界防火墙自然无法抵御，被攻击在所难免。

最后是效率和故障。边界防火墙把检查机制集中在网络边界处的单点上，一旦被攻克，整个内部网络将完全暴露在外部攻击者面前。

86、分布式防火墙是三部分组成的立体防护系统：

1）网络防火墙(Network Firewall)：它承担着传统边界防火墙看守大门的职责；

2）主机防火墙(Host Firewall)：它解决了边界防火墙不能很好解决的问题(例如来自内部的攻击和结构限制等)；

3）集中管理(Central Management)：它解决了由分布技术而带来的管理问题。

87、分布式防火墙的优势主要有：

(1) 保证系统的安全性。分布式防火墙技术增加了针对主机的入侵检测和防护功能，加强了对来自于内部的攻击的防范，对用户网络环境可以实施全方位的安全策略，并提供了多层次立体的防范体系。

(2) 保证系统性能稳定高效。消除了结构性瓶颈问题，提高了系统整体安全性能。

(3) 保证系统的扩展性。伴随网络系统扩充，分布式防火墙技术可为安全防护提供强大的扩充能力。

88、解释 VPN 的基本概念。

VPN 是 Virtual Private Network 的缩写，是将物理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。

Virtual 是针对传统的企业“专用网络”而言的。VPN 则是利用公共网络资源和设备建立一个逻辑上的专用通道，尽管没有自己的专用线路，但它却可以提供和专用网络同样的功能。

Private 表示 VPN 是被特定企业或用户私有的，公共网络上只有经过授权的用户才可以使用。在该通道内传输的数据经过了加密和认证，保证了传输内容的完整性和机密性。

89、简述 VPN 使用了哪些主要技术。

1）隧道（封装）技术是目前实现不同 VPN 用户业务区分的基本方式。一个 VPN 可抽象为一个没有自环的连通图，每个顶点代表一个 VPN 端点（用户数据进入或离开 VPN 的设备端口），相邻顶点之间的边表示连结这两对应端点的逻辑通道，即隧道。

隧道以叠加在 IP 主干网上的方式运行。需安全传输的数据分组经一定的封装处理，从信源的一个 VPN 端点进入 VPN，经相关隧道穿越 VPN（物理上穿越不安全的互联网），到达信宿的另一个 VPN 端点，再经过相应解封装处理，便得到原始数据。（不仅指定传送的路径，在中转节点也不会解析原始数据）

2）当用户数据需要跨越多个运营商的网络时，在连接两个独立网络的节点该用户的数据分组需要被解封装和再次封装，可能会造成数据泄露，这就需要用到加密技术和密钥管理技术。目前主要的密钥交换和管理标准有 SKIP 和 ISAKMP（安全联盟和密钥管理协议）。

3）对于支持远程接入或动态建立隧道的 VPN，在隧道建立之前需要确认访问者身份，是否可以建立要求的隧道，若可以，系统还需根据访问者身份实施资源访问控制。这需要访问者与设备的身份认证技术和访问控制技术。

90、VPN 有哪三种类型？它们的特点和应用场合分别是什么？

1.Access VPN（远程接入网）

即所谓移动 VPN，适用于企业内部人员流动频繁和远程办公的情况，出差员工或在家办公的员工利用当地 ISP 就可以和企业的 VPN 网关建立私有的隧道连接。

通过拨入当地的 ISP 进入 Internet 再连接企业的 VPN 网关，在用户和 VPN 网关之间建立一个安全的“隧道”，通过该隧道安全地访问远程的内部网（节省通信费用，又保证了安全性）。

拨入方式包括拨号、ISDN、ADSL 等，唯一的要求就是能够使用合法 IP 地址访问 Internet。

2. Intranet VPN（内联网）

如果要进行企业内部异地分支结构的互联，可以使用 Intranet VPN 的方式，即所谓的网关对网关 VPN。在异地两个网络的网关之间建立了一个加密的 VPN 隧道，两端的内部网络可以通过该 VPN 隧道安全地进行通信。

3. Extranet VPN（外联网）

如果一个企业希望将客户、供应商、合作伙伴连接到企业内部网，可以使用 Extranet VPN。其实也是一种网关对网关的 VPN，但它需要有不同协议和设备之间的配合和不同的安全配置。

91、举例说明什么是乘客协议、封装协议和传输协议？

（1）乘客协议：用户真正要传输（也即被封装）的数据，如 IP、PPP、SLIP 等。

（2）封装协议：用于建立、保持和拆卸隧道，如 L2F、PPTP、L2TP、GRE。

（3）传输协议：乘客协议被封装后应用传输协议，例如 UDP 协议。

92、了解第三层隧道协议——GRE。

GRE 是通用的路由封装协议，支持全部的路由协议（如 RIP2、OSPF 等），用于在 IP 包中封装任何协议的数据包（IP、IPX、NetBEUI 等）。在 GRE 中，乘客协议就是上面这些被封装的协议，封装协议就是 GRE，传输协议就是 IP。在 GRE 的处理中，很多协议的细微差别都被忽略，这使得 GRE 不限于某个特定的“X over Y”的应用，而是一种通用的封装形式。

原始 IP 包的 IP 地址通常是企业私有网络规划的保留 IP 地址，而外层的 IP 地址是企业网络出口的 IP 地址，因此，尽管私有网络的 IP 地址无法和外部网络进行正确的路由，但这个封装之后的 IP 包可以在 Internet 上路由——最简单的 VPN 技术。（NAT，非 IP 数据包能在 IP 互联网上传送）

GRE VPN 适合一些小型点对点的网络互联。

93、简述常见的黑客攻击过程。

1.目标探测和信息攫取

先确定攻击目标并收集目标系统的相关信息。一般先大量收集网上主机的信息，然后根据各系统的安全性强弱确定最后的目标。

1) 踩点（Footprinting）

黑客必须尽可能收集目标系统安全状况的各种信息。Whois 数据库查询可以获得很多关于目标系统的注册信息，DNS 查询(用 Windows/UNIX 上提供的 nslookup 命令客户端)也可令黑客获得关于目标系统域名、IP 地址、DNS 务器、邮件服务器等有用信息。此外还可以用 traceroute 工具获得一些网络拓扑和路由信息。

2) 扫描（Scanning）

在扫描阶段，我们将使用各种工具和技巧(如 Ping 扫射、端口扫描以及操作系统检测等)确定哪些系统存活着、它们在监听哪些端口(以此来判断它们在提供哪些服务)，甚至更进一步地获知它们运行的是什么操作系统。

3) 查点（Enumeration）

从系统中抽取有效账号或导出资源名的过程称为查点，这些信息很可能成为目标系统的祸根。比如说，一旦查点查出一个有效用户名或共享资源，攻击者猜出对应的密码或利用与资源共享协议关联的某些脆弱点通常就只是一个时间问题了。查点技巧差不多都是特定于操作系统的，因此要求使用前面步骤汇集的信息。

2．获得访问权（Gaining Access）

通过密码窃听、共享文件的野蛮攻击、攫取密码文件并破解或缓冲区溢出攻击等来获得系统的访问权限。

3．特权提升（Escalating Privilege）

在获得一般账户后，黑客经常会试图获得更高的权限，比如获得系统管理员权限。通常可以采用密码破解(如用LOphtcrack破解NT的SAM文件)、利用已知的漏洞或脆弱点等技术。

4．窃取（Stealing）

对敏感数据进行篡改、添加、删除及复制（如Windows系统的注册表、UNIX的rhost文件等）。

5．掩盖踪迹（Covering Tracks）

此时最重要就隐藏自己踪迹，以防被管理员发觉，比如清除日志记录、使用 rootkits 等工具。

6．创建后门（Creating Bookdoor）

在系统的不同部分布置陷阱和后门，以便入侵者在以后仍能从容获得特权访问。

94、安全扫描系统的逻辑结构是什么？

（1）策略分析部分

用于控制网络安全扫描系统的功能，即根据系统预先设定的配置文件，它应当检测哪些Internet域内的主机并进行哪些检测(简单、中级和高级)。

（2）获取检测工具部分

用于决定对给定的目标系统进行检测的工具。目标系统可以是一个主机，或是某个子网上的所有主机。确定目标系统后，该部分就可以根据策略分析部分得出的测试级别类，确定需要应用的检测工具。

（3）获取数据部分

对于给定的检测工具，获取数据部分运行对应的检测过程，收集数据信息并产生新的事实记录。最后获得的新的事实记录是事实分析部分的输入。

（4）事实分析部分

对于给定的事实记录，事实分析部分能产生出新的目标系统、新的检测工具和新的事实记录。新的目标系统作为获取检测工具部分的输入，新的检测工具又作为获取数据部分的输入，新的事实记录又再一次作为事实分析部分的输入。循环直到不产生新的事实记录为止。

（5）报告分析部分

报告分析部分将关于目标系统的大量有用的信息组织起来，用HTML界面显示，使用户可以通过Web浏览器方便查看运行的结果。

95、什么是漏洞扫描？

系统漏洞检测又称漏洞扫描，就是对重要网络信息进行检查，发现其中可被攻击者利用的漏洞。

96、什么是IDS，它有哪些基本功能？

入侵检测系统 IDS，它从计算机网络系统中的若干关键点收集信息，并分析这些信息，检查网络中是否有违反安全策略的行为和遭到袭击的迹象。入侵检测被认为是防火墙之后的第二道安全闸门。

1）监测并分析用户和系统的活动，查找非法用户和合法用户的越权操作；

2）核查系统配置和漏洞并提示管理员修补漏洞；

3）评估系统关键资源和数据文件的完整性；

4）识别已知的攻击行为，统计分析异常行为；

5）操作系统日志管理，并识别违反安全策略的用户活动等。

97、什么是基于主机的 IDS、基于网络的 IDS、分布式 IDS？

（1）基于主机的入侵检测系统

基于主机的 IDS 的输入数据来源于系统的审计日志，即在每个要保护的主机上运行一个代理程序，一般只能检测该主机上发生的入侵。它在重要的系统服务器、工作站或用户机器上运行，监视操作系统或系统事件级别的可疑活动（如尝试登录失败）。此类系统需要定义清楚哪些是不合法的活动，然后把这种安全策略转换成入侵检测规则。

（2）基于网络的入侵检测系统

基于网络的 IDS 的输入数据来源于网络的信息流，该类系统一般被动地在网络上监听整个网段上的信息流，通过捕获网络数据包，进行分析，能够检测该网段上发生的网络入侵。

（3）分布式入侵检测系统

分布式 IDS 一般由多个部件组成，分布在网络的各个部分，完成相应功能，分别进行数据采集、数据分析等。通过中心的控制部件进行数据汇总、分析、产生入侵警报等。在这种结构下，不仅可以检测到针对单独主机的入侵，同时也可以检测到针对整个网络上的主机的入侵。

98、IDS 有哪两类分析方法，并对两者分析比较。

（1）异常检测

假定所有入侵行为都是与正常行为不同的，如果建立系统正常行为的轨迹（特征文件 Profiles），那么理论上可以通过统计那些不同于我们已建立的特征文件的所有系统状态的数量，来识别入侵企图，即把所有与正常轨迹不同的系统状态视为可疑企图。

例如，一个程序员的正常活动与一个打字员的正常活动肯定不同，打字员常用的是编辑/打印文件等命令；而程序员则更多地使用编辑/编译/调试/运行等命令。这样，根据各自不同的正常活动建立起来的特征文件，便具有用户特性。入侵者使用正常用户的账号，但其行为并不会与正常用户的行为相吻合，从而可以被检测出来。对于异常阀值与特征的选择是异常发现技术的关键。比如，通过流量统计分析将异常时间的异常网络流量视为可疑。

异常检测指根据使用者的行为或资源使用状况来判断是否入侵，所以也被称为基于行为(Behave—based)的检测。

（2）误用探测（基于知识(Knowledge—based)检测）

假定所有入侵行为和手段(及其变种)都能够表达为一种模式或特征，那么所有已知的入侵方法都可以用匹配的方法发现。因为很大一部分的入侵是利用了系统的脆弱性，通过分析入侵过程的特征、条件、排列以及事件间关系能具体描述入侵行为的迹象。

误用检测系统的关键问题是如何从已知入侵中提取和编写特征，使得其能够覆盖该入侵的所有可能的变种，而同时不会匹配到非入侵活动（把真正入侵与正常行为区分开来）。

99、什么是现代安全审计技术，它提出的意义是什么？

安全审计是一个安全的网络必须支持的功能特性，它记录用户使用计算机网络系统进行所有活动的过程，是提高安全性的重要工具。它不仅能够识别谁访问了系统，还能指出系统正被怎样使用。审计信息对于确定是否有网络攻击和攻击源很重要。同时，系统事件的记录能够更迅速和系统地识别问题，并且它是后面阶段事故处理的重要依据，为网络犯罪行为及泄密行为提供取证基础。

在 TCSEC 中定义的 Accountability 其实已经提出了“安全审计”的基本要求。Accountability 需求中明确指出了：审计信息必须被有选择地保留和保护，与安全有关的活动能够被追溯到负责方，系统应能够选择哪些与安全有关的信息被记录，以便将审计的开销降到最小，可以进行有效的分析。在 C2 等级中，审计系统必须实现如下的功能：系统能

够创建和维护审计数据，保证审计记录不能被删除、修改和非法访问。CC 准则的安全功能需求定义了多达 11 个的安全功能需求类，其中包括安全审计类。在 CC 准则中，对网络安全审计定义了一套完整的功能。

目前对于安全审计这个概念的理解还不统一，安全领域对于怎么样的产品才属于安全审计产品还没有一个普遍接受的认识。

100、计算机病毒的定义和特征是什么？

计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能够自我复制的一组计算机指令或者程序代码。

1）主动传染性

这是病毒区别于其他程序的一个根本特性。病毒能够将自身代码主动复制到其他文件或扇区中，这个过程并不需要人为的干预。

病毒通过各种渠道从已被感染的计算机扩散到未被感染的计算机。所谓“感染”，就是病毒将自身嵌入到合法程序的指令序列中，致使执行合法程序的操作会招致病毒程序的共同执行或以病毒程序的执行取而代之。

2）破坏性

这也是计算机病毒的一个基本特性，比如删除文件、毁坏主板 BIOS、影响正常的使用等。近年来随着将特洛伊木马程序、蠕虫程序等纳入计算机病毒的范畴，将盗取信息、使用他人计算机的资源等也列入了破坏行为的范围。

3）寄生性（隐蔽性）

早期的计算机病毒绝大多数都不是完整的程序，通常都是附着在其他程序中。病毒取得系统控制权后，可以在很短时间里传染大量其他程序，而且计算机系统通常仍能正常运行，用户不会感到任何异常（非常危险）。当然现在的某些病毒本身就是一个完整的程序。

4）潜伏性

病毒进入系统之后一般不会马上发作，可以或长或短地潜伏在合法程序中，进行传染而不被人发现。潜伏的时间越长，传染范围越大。

5）多态性

病毒试图在每一次感染时改变它的形态，使对它的检测变得更困难。一个多态病毒还是原来的病毒，但不能通过扫描特征字符串来发现。病毒代码的主要部分相同，但表达方式发生了变化，也就是同一程序由不同的字节序列表示。

信息安全考试题库（1000 题）

一、1 单项选择题（1-605）

1、 Chinese Wall 模型的设计宗旨是：（）。

A、用户只能访问哪些与已经拥有的信息不冲突的信息　　B、用户可以访问所有信息

C、用户可以访问所有已经选择的信息　　D、用户不可以访问哪些没有选择的信息

2、 安全责任分配的基本原则是：（）。

A、“三分靠技术，七分靠管理”　　B、“七分靠技术，三分靠管理”

C、“谁主管，谁负责”　　D、防火墙技术

3、 保证计算机信息运行的安全是计算机安全领域中最重要的环节之一，以下（）不属于信息运行安全技术的范畴。

A、风险分析　　B、审计跟踪技术　　C、应急技术　　D、防火墙技术

4、 从风险的观点来看，一个具有任务紧急性，核心功能性的计算机应用程序系统的开发和维护项目应该（）。

A、内部实现　　B、外部采购实现　　C、合作实现　　D、多来源合作实现

5、 从风险分析的观点来看，计算机系统的最主要弱点是（）。

A、内部计算机处理　　B、系统输入输出　　C、通讯和网络　　D、外部计算机处理

6、 从风险管理的角度，以下哪种方法不可取？（）

A、接受风险　　B、分散风险　　C、转移风险　　D、拖延风险

7、 当今 IT 的发展与安全投入，安全意识和安全手段之间形成（）。

A、安全风险屏障　　B、安全风险缺口　　C、管理方式的变革　　D、管理方式的缺口

8、 当为计算机资产定义保险覆盖率时，下列哪一项应该特别考虑？（）。

A、已买的软件　　B、定做的软件　　C、硬件　　D、数据

9、 当一个应用系统被攻击并受到了破坏后，系统管理员从新安装和配置了此应用系统，在该系统重新上线前管理员不需查看：（）

A、访问控制列表　　B、系统服务配置情况

C、审计记录　　D、用户账户和权限的设置

10、根据《计算机信息系统国际联网保密管理规定》，涉及国家秘密的计算机信息系统，不得直接或间接地与国际互联网或其它公共信息网络相联接，必须实行（）。

A、 逻辑隔离　　B、物理隔离　　C、安装防火墙　　D、VLAN 划分

11、根据《信息系统安全等级保护定级指南》，信息系统的安全保护等级由哪两个定级要素决定？（）

A、威胁、脆弱性　　B、系统价值、风险

C、信息安全、系统服务安全　　D、受侵害的客体、对客体造成侵害的程度业务

12、公司应明确员工的雇佣条件和考察评价的方法与程序，减少因雇佣不当而产生的安全风险。人员考察的内容不包括（）。

A、身份考验、来自组织和个人的品格鉴定　　B、家庭背景情况调查

C、学历和履历的真实性和完整性　　D、学术及专业资格

13、计算机信息的实体安全包括环境安全、设备安全、（）三个方面。

A 运行安全　　B、媒体安全　　C、信息安全　　D、人事安全

14、目前，我国信息安全管理格局是一个多方“齐抓共管”的体制，多头管理现状决定法出多门，《计算机信息系统国际联网保密管理规定》是由下列哪个部门所指定的规章制度？（）

A、公安部　　B、国家保密局

C、信息产业部　　D、国家密码管理委员会办公室

15、目前我国颁布实施的信息安全相关标准中，以下哪一个标准属于强制执行的标准？（）

A、GB/T 18336-2001 信息技术安全性评估准则

B、GB 17859-1999 计算机信息系统安全保护等级划分准则

C、GB/T 9387.2-1995 信息处理系统开放系统互联安全体系结构

D、GA/T 391-2002 计算机信息系统安全等级保护管理要求

16、确保信息没有非授权泄密，即确保信息不泄露给非授权的个人、实体或进程，不为其所用，是指（）。

A、完整性　　B、可用性　　C、保密性　　D、抗抵赖性

17、如果对于程序变动的手工控制收效甚微，以下哪一种方法将是最有效的？（）

A、自动软件管理　　B、书面化制度　　C、书面化方案　　D、书面化标准

18、如果将风险管理分为风险评估和风险减缓，那么以下哪个不属于风险减缓的内容？（）

A、计算风险　　B、选择合适的安全措施

C、实现安全措施　　D、 接受残余风险

19、软件供应商或是制造商可以在他们自己的产品中或是客户的计算机系统上安装一个“后门”程序。以下哪一项是这种情况面临的最主要风险？（）

A、软件中止和黑客入侵　　B、远程监控和远程维护

C、软件中止和远程监控　　D、远程维护和黑客入侵

20、 管理审计指（）

A、保证数据接收方收到的信息与发送方发送的信息完全一致

B、防止因数据被截获而造成的泄密

C、对用户和程序使用资源的情况进行记录和审查

D、保证信息使用者都可

21、为了保护企业的知识产权和其它资产，当终止与员工的聘用关系时下面哪一项是最好的方法？（）

A、进行离职谈话，让员工签署保密协议，禁止员工账号，更改密码

B、进行离职谈话，禁止员工账号，更改密码

C、让员工签署跨边界协议

D、列出员工在解聘前需要注意的所有责任

22、为了有效的完成工作，信息系统安全部门员工最需要以下哪一项技能？（）

A、人际关系技能　　B、项目管理技能　　C、技术技能　　D、沟通技能

23、我国的国家秘密分为几级？（A）

A、3　　B、4　　C、5　　D、6

24、系统管理员属于（）。

A、决策层　　B、管理层

C、执行层　　D、既可以划为管理层，又可以划为执行层

25、下列哪一个说法是正确的？（）

A、风险越大，越不需要保护　　B、风险越小，越需要保护

C、风险越大，越需要保护　　D、越是中等风险，越需要保护

26、下面哪类访问控制模型是基于安全标签实现的？（）

A、自主访问控制　　B、强制访问控制

C、基于规则的访问控制　　D、基于身份的访问控制

27、下面哪项能够提供最佳安全认证功能？（）

A、这个人拥有什么　　B、这个人是什么并且知道什么

C、这个人是什么　　D、这个人知道什么

28、下面哪一个是国家推荐性标准？（）

A、GB/T 18020-1999　　应用级防火墙安全技术要求

B、SJ/T 30003-93　　电子计算机机房施工及验收规范

C、GA243-2000　　计算机病毒防治产品评级准则

D、ISO/IEC 15408-1999　信息技术安全性评估准则

29、下面哪一项关于对违反安全规定的员工进行惩戒的说法是错误的？（）

A、对安全违规的发现和验证是进行惩戒的重要前提

B、惩戒措施的一个重要意义在于它的威慑性

C、处于公平，进行惩戒时不应考虑员工是否是初犯，是否接受过培训

D、尽管法律诉讼是一种严厉有效的惩戒手段，但使用它时一定要十分慎重

30、下面哪一项最好地描述了风险分析的目的？（）

A、识别用于保护资产的责任义务和规章制度

B、识别资产以及保护资产所使用的技术控制措施

C、识别资产、脆落性并计算潜在的风险

D、识别同责任义务有直接关系的威胁

31、下面哪一项最好地描述了组织机构的安全策略？（）

A、定义了访问控制需求的总体指导方针

B、建议了如何符合标准

C、表明管理意图的高层陈述

D、表明所使用的技术控制措施的高层陈述

32、下面哪一种风险对电子商务系统来说是特殊的？（D）

A、服务中断　　B、应用程序系统欺骗

C、未授权的信息泄露　　D、确认信息发送错误

33、下面有关我国标准化管理和组织机构的说法错误的是？（C）

A、国家标准化管理委员会是统一管理全国标准化工作的主管机构

B、国家标准化技术委员会承担国家标准的制定和修改工作

C、全国信息安全标准化技术委员负责信息安全技术标准的审查、批准、编号和发布

D、全国信息安全标准化技术委员负责统一协调信息安全国家标准年度技术项目

34、项目管理是信息安全工程师基本理论，以下哪项对项目管理的理解是正确的？（A）

A、项目管理的基本要素是质量，进度和成本

B、项目管理的基本要素是范围，人力和沟通

C、项目管理是从项目的执行开始到项目结束的全过程进行计划、组织

D、项目管理是项目的管理者，在有限的资源约束下，运用系统的观点，方法和理论，对项目涉及的技术工作进行有效地管理

35、信息安全的金三角是（C）。

A、可靠性，保密性和完整性　　B、多样性，冗余性和模化性

C、保密性，完整性和可用性　　D、多样性，保密性和完整性

36、信息安全风险缺口是指（A）。

A、IT 的发展与安全投入，安全意识和安全手段的不平衡

B、信息化中，信息不足产生的漏洞

C、计算机网络运行，维护的漏洞

D、计算中心的火灾隐患

37、信息安全风险应该是以下哪些因素的函数？（A）

A、信息资产的价值、面临的威胁以及自身存在的脆弱性等

B、病毒、黑客、漏洞等

C、保密信息如国家密码、商业秘密等

D、网络、系统、应用的复杂的程度

38、信息安全工程师监理的职责包括？（A）

A、质量控制，进度控制，成本控制，合同管理，信息管理和协调

B、质量控制，进度控制，成本控制，合同管理和协调

C、确定安全要求，认可设计方案，监视安全态势，建立保障证据和协调

D、确定安全要求，认可设计方案，监视安全态势和协调

39、信息安全管理最关注的是？（C）

A、外部恶意攻击　　B、病毒对 PC 的影响

C、内部恶意攻击　　D、病毒对网络的影响

40、信息分类是信息安全管理工作的重要环节，下面哪一项不是对信息进行分类时需要重点考虑的？（C）

A、信息的价值　　B、信息的时效性

C、信息的存储方式　　D、法律法规的规定

41、信息网络安全的第三个时代是（A）

A、主机时代，专网时代，多网合一时代　　B、主机时代，PC 时代，网络时代

C、PC 时代，网络时代，信息时代　　D、2001 年，2002 年，2003 年

42、一个公司在制定信息安全体系框架时，下面哪一项是首要考虑和制定的？（A）

A、安全策略　　B、安全标准　　C、操作规程　　D、安全基线

43、以下哪个不属于信息安全的三要素之一？（C）

A、机密性　　B、完整性　　C、抗抵赖性　　D、可用性

44、以下哪一项安全目标在当前计算机系统安全建设中是最重要的？（C）

A、目标应该具体　　B、目标应该清晰

C、目标应该是可实现的　　D、目标应该进行良好的定义

45、以下哪一项计算机安全程序的组成部分是其它组成部分的基础？（A）

A、制度和措施　　B、漏洞分析

C、意外事故处理计划　　D、采购计划

46、以下哪一项是对信息系统经常不能满足用户需求的最好解释？（C）

A、没有适当的质量管理工具　　B、经常变化的用户需求

C、用户参与需求挖掘不够　　D、项目管理能力不强

47、以下哪一种人给公司带来了最大的安全风险？（D）

A、临时工　　B、咨询人员　　C、以前的员工　　D、当前的员工

48、以下哪种安全模型未使用针对主客体的访问控制机制？（C）

A、基于角色模型　　B、自主访问控制模型

C、信息流模型　　D、强制访问控制模型

49、以下哪种措施既可以起到保护的作用还能起到恢复的作用？（C）

A、对参观者进行登记　　B、备份

C、实施业务持续性计划　　D、口令

50、以下哪种风险被定义为合理的风险？（B）

A、最小的风险　　B、可接受风险

C、残余风险　　D、总风险

51、以下人员中，谁负有决定信息分类级别的责任？（B）

A、用户　　B、数据所有者　　C、审计员　　D、安全官

52、有三种基本的鉴别的方式：你知道什么，你有什么,以及（C）。

A、你需要什么　　B、你看到什么　　C、你是什么　　D、你做什么

53、在对一个企业进行信息安全体系建设中，下面哪种方法是最佳的？（B）

A、自下而上　　B、自上而下　　C、上下同时开展　　D、以上都不正确

54、在风险分析中，下列不属于软件资产的是（D）

A、计算机操作系统　　B、网络操作系统

C、应用软件源代码　　D、外来恶意代码

55、在国家标准中，属于强制性标准的是：（B）

A、GB/T　XXXX-X-200X　　B、GB XXXX-200X

C、DBXX/T　XXX-200X　　D、QXXX-XXX-200X

56、在任何情况下，一个组织应对公众和媒体公告其信息系统中发生的信息安全事件？（A）

A、当信息安全事件的负面影响扩展到本组织意外时

B、只要发生了安全事件就应当公告

C、只有公众的什么财产安全受到巨大危害时才公告

D、当信息安全事件平息之后

57、在信息安全策略体系中，下面哪一项属于计算机或信息安全的强制性规则？（A）

A、标准（Standard）　　B、安全策略（Security policy）

C、方针（Guideline）　　D、流程(Proecdure)

58、在信息安全管理工作中“符合性”的含义不包括哪一项？（C）

A、对法律法规的符合　　B、对安全策略和标准的符合

C、对用户预期服务效果的符合　　D、通过审计措施来验证符合情况

59、在许多组织机构中，产生总体安全性问题的主要原因是（A）。

A、缺少安全性管理　　B、缺少故障管理

C、缺少风险分析　　D、缺少技术控制机制

60、职责分离是信息安全管理的一个基本概念。其关键是权利不能过分集中在某一个人手中。职责分离的目的是确保没有单独的人员（单独进行操作）可以对应用程序系统特征或控制功能进行破坏。当以下哪一类人员访问安全系统软件的时候，会造成对“职责分离”原则的违背？（D）

A、数据安全管理员　　B、数据安全分析员

C、系统审核员　　D、系统程序员

61、中国电信的岗位描述中都应明确包含安全职责，并形成正式文件记录在案，对于安全职责的描述应包括（D）。

A、落实安全政策的常规职责　　B、执行具体安全程序或活动的特定职责

C、保护具体资产的特定职责　　D、以上都对

62、终端安全管理目标：规范支撑系统中终端用户的行为，降低来自支撑系统终端的安全威胁，重点解决以下哪些问题？（A）。

A、终端接入和配置管理；终端账号、秘密、漏洞补丁等系统安全管理；桌面及主机设

置管理；终端防病毒管理

B、终端账号、秘密、漏洞补丁等系统安全管理；桌面及主机设置管理；终端防病毒管理

C、终端接入和配置管理；桌面及主机设置管理；终端防病毒管理

D、终端接入和配置管理；终端账号、秘密、漏洞补丁等系统安全管理；桌面及主机设置管理

63、著名的橘皮书指的是（A）。

A、可信计算机系统评估标准(TCSEC)　　B、信息安全技术评估标准（ITSEC）

C、美国联邦标准（FC）　　D、通用准则（CC）

64、资产的敏感性通常怎样进行划分？（C）

A、绝密、机密、敏感　　B、机密、秘密、敏感和公开

C、绝密、机密、秘密、敏感和公开等五类

D、绝密、高度机密、秘密、敏感和公开等五类

65、重要系统关键操作操作日志保存时间至少保存（C）个月。

A、1　　B、2　　C、3　　D、4

66、安全基线达标管理办法规定：BSS 系统口令设置应遵循的内控要求是（C）

A、数字+字母　　B、数字+字母+符号

C、数字+字母+字母大小写　　D、数字+符号

67、不属于安全策略所涉及的方面是（D）。

A、物理安全策略　　B、访问控制策略

C、信息加密策略　　D、防火墙策略

68、“中华人民共和国保守国家秘密法”第二章规定了国家秘密的范围和密级，国家秘密的密级分为：（C）。

A、“普密”、“商密”两个级别　　B、“低级”和“高级”两个级别

C、“绝密”、“机密”、“秘密”三个级别

D、“一密”、“二密”，“三密”、“四密”四个级别

69、对 MBOSS 系统所有资产每年至少进行（A）次安全漏洞自评估。

A、1　　B、2　　C、3　　D、4

70、下列情形之一的程序，不应当被认定为《中华人民共和国刑法》规定的“计算机病毒等破坏性程序”的是：（A）。

A、能够盗取用户数据或者传播非法信息的

B、能够通过网络、存储介质、文件等媒介，将自身的部分、全部或者变种进行复制、传播，并破坏计算机系统功能、数据或者应用程序的

C、能够在预先设定条件下自动触发，并破坏计算机系统功能、数据或者应用程序的

D、其他专门设计用于破坏计算机系统功能、数据或者应用程序的程序

71、中国电信各省级公司争取在 1-3 年内实现 CTG-MBOSS 系统安全基线“达标”（C）级以上。

A、A 级　　B、B 级　　C、C 级　　D、D 级

72、下面对国家秘密定级和范围的描述中，哪项不符合《保守国家秘密法》要求？（C）

A、国家秘密和其密级的具体范围，由国家保密工作部门分别会同外交、公安、国家安全和其他中央有关规定

B、各级国家机关、单位对所产生的秘密事项，应当按照国家秘密及其密级的具体范围的规定确定密级

C、对是否属于国家和属于何种密级不明确的事项，可有各单位自行参考国家要求确定和定级，然后国家保密工作部门备案

D、对是否属于国家和属于何种密级不明确的事项，由国家保密工作部门，省、自治区、直辖市的保密工作部门，省、自治区、直辖市的保密工作部门，省、自治区政府所在地的市和经国务院批准的较大的市的保密工作部门或者国家保密工作部门审定的机关确定。

73、获取支付结算、证券交易、期货交易等网络金融服务的身份认证信息（B）组以上的可以被《中华人民共和国刑法》认为是非法获取计算机信息系统系统认定的“情节严重”。

A、5　　B、10　　C、-15　　D、20

74、基准达标项满（B）分作为安全基线达标合格的必要条件。

A、50　　B、60　　C、70　　D、80

75、《国家保密法》对违法人员的量刑标准是（A）。

A、国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重的，处三年以下有期徒刑或者拘役；情节特别严重的，处三年以上七年以下有期徒刑

B、国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重的，处四年以下有期徒刑或者拘役；情节特别严重的，处四年以上七年以下有期徒刑

C、国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重的，处五年以下有期徒刑或者拘役；情节特别严重的，处五年以上七年以下有期徒刑

D、-国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重，处七年以下有期徒刑或者拘役；情节特别严重的，处七年以下有期徒刑

76、$HOME/.netrc 文件包含下列哪种命令的自动登录信息？（C）

A、rsh　　B、ssh　　C、ftp　　D、rlogin

77、/etc/ftpuser 文件中出现的账户的意义表示（A）。

A、该账户不可登录 ftp　　B、该账户可以登录 ftp　　C、没有关系　　D、缺少

78、按 TCSEC 标准，WinNT 的安全级别是（A）。

A、C2　　B、B2　　C、C3　　D、B1

79、Linux 系统/etc 目录从功能上看相当于 Windows 的哪个目录？（B）

A、program files　B、Windows　　C、system volume information　　D、TEMP

80、Linux 系统格式化分区用哪个命令？（A）

A、fdisk　　B、mv　　C、mount　　D、df

81、在 Unix 系统中，当用 ls 命令列出文件属性时，如果显示-rwxrwxrwx,意思是（A）。

A、前三位 rwx 表示文件属主的访问权限；中间三位 rwx 表示文件同组用户的访问权限；后三位 rwx 表示其他用户的访问权限

B、前三位 rwx 表示文件同组用户的访问权限；中间三位 rwx 表示文件属主的访问权限；后三位 rwx 表示其他用户的访问权限

C、前三位 rwx 表示文件同域用户的访问权限；中间三位 rwx 表示文件属主的访问权限；后三位 rwx 表示其他用户的访问权限

D、前三位 rwx 表示文件属主的访问权限；中间三位 rwx 表示文件同组用户的访问权限；后三位 rwx 表示同域用户的访问权限

82、Linux 系统通过（C）命令给其他用户发消息。

A、less　　B、mesg　　C、write　　D、echo to

83、Linux 中，向系统中某个特定用户发送信息，用什么命令？（B）

A、wall　　B、write　　C、mesg　　D、net send

84、防止系统对 ping 请求做出回应，正确的命令是：（C）。

A、echo 0>/proc/sys/net/ipv4/icmp_ehco_ignore_all

B、echo 0>/proc/sys/net/ipv4/tcp_syncookies

C、echo 1>/proc/sys/net/ipv4/icmp_echo_ignore_all

D、echo 1>/proc/sys/net/ipv4/tcp_syncookies

85、NT/2K 模型符合哪个安全级别？（B）

A、B2　　B、C2　　C、B1　　D、C1

86、Red Flag Linux 指定域名服务器位置的文件是（C）。

A、etc/hosts　　B、etc/networks　　C、etc/rosolv.conf　　D、/.profile

87、Solaris 操作系统下，下面哪个命令可以修改/n2kuser/.profile 文件的属性为所有用户可读、科协、可执行？（D）

A、chmod 744 /n2kuser/.profile　　B、 chmod 755 /n2kuser/.profile

C、 chmod 766 /n2kuser/.profile　　D、 chmod 777 /n2kuser/.profile

88、如何配置，使得用户从服务器 A 访问服务器 B 而无需输入密码？（D）

A、利用 NIS 同步用户的用户名和密码

B、在两台服务器上创建并配置/.rhost 文件

C、在两台服务器上创建并配置$HOME/.netrc 文件

D、在两台服务器上创建并配置/etc/hosts.equiv 文件

89、Solaris 系统使用什么命令查看已有补丁列表？（C）

A、uname –an　　B、showrev　　C、oslevel –r　　D、swlist –l product ‘PH??’

90、Unix 系统中存放每个用户信息的文件是（D）。

A、/sys/passwd　　B、/sys/password　　C、/etc/password　　D、/etc/passwd

91、Unix 系统中的账号文件是（A）。

A、/etc/passwd　　B、/etc/shadow　　C、/etc/group　　D、/etc/gshadow

92、Unix 系统中如何禁止按 Control-Alt-Delete 关闭计算机？（B）

A、把系统中“/sys/inittab”文件中的对应一行注释掉

B、把系统中“/sysconf/inittab”文件中的对应一行注释掉

C、把系统中“/sysnet/inittab”文件中的对应一行注释掉

D、把系统中“/sysconf/init”文件中的对应一行注释掉

93、Unix 中。可以使用下面哪一个代替 Telnet，因为它能完成同样的事情并且更安全？（）

A、S-TELNET　　B、SSH　　C、FTP　　D、RLGON

94、Unix 中，默认的共享文件系统在哪个位置？（C）

A、/sbin/　　B、/usr/local/　　C、/export/　　D、/usr/

95、Unix 中，哪个目录下运行系统工具，例如 sh,cp 等？（A）

A、/bin/　　B、/lib/　　C、/etc/　　D、/

96、U 盘病毒依赖于哪个文件打到自我运行的目的？（A）

A、autoron.inf　　B、autoexec.bat　　C、config.sys　　D、system.ini

97、Windows nt/2k 中的.pwl 文件是？（B）

A、路径文件　　B、口令文件　　C、打印文件　　D、列表文件

98、Windows 2000 目录服务的基本管理单位是（D）。

A、用户　　B、计算机　　C、用户组　　D、域

99、Windows 2000 系统中哪个文件可以查看端口与服务的对应？（D）

A、c:\winnt\system\drivers\etc\services　　B、c:\winnt\system32\services

C、c:\winnt\system32\config\services　　D、c:\winnt\system32\drivers\etc\services

100、Windows NT/2000 SAM 存放在（D）。

A、WINNT　　B、WINNT/SYSTEM32

C、WINNT/SYSTEM　　D、WINNT/SYSTEM32/config

101、 Windows NT/2000 中的.pwl 文件是？（B）

A、路径文件　　B、口令文件　　C、打印文件　　D、列表文件

102、Windows NT 的安全标识（SID）串是由当前时间、计算机名称和另外一个计算机变量共同产生的，这个变量是什么？（C）

A、击键速度　　B、用户网络地址

C、处理当前用户模式线程所花费 CPU 的时间　　D、PING 的响应时间

103、Windows NT 和 Windows 2000 系统能设置为在几次无效登录后锁定账号，可以防止：（B）。

A、木马　　B、暴力破解　　C、IP 欺骗　　D、缓冲区溢出攻击

104、Windows 主机推荐使用（A）格式。

A、NTFS　　B、FAT32　　C、FAT　　D、Linux

105、XP 当前的最新补丁是（C）。

A、SP1　　B、SP2　　C、SP3　　D、SP4

106、按 TCSEC 标准，WinNT 的安全级别是（A）。

A、C2　　B、B2　　C、C3　　D、B1

107、当你感觉到你的 Win2003 运行速度明显减慢，当打开任务管理器后发现 CPU 使用率

达到了 100%，你认为你最有可能受到了（D）攻击。

A、缓冲区溢出攻击　　B、木马攻击　　C、暗门攻击　　D、DOS 攻击

108、档案权限 755，对档案拥有者而言，是什么含义？（A）

A、可读，可执行，可写入　　B、可读

C、可读，可执行　　D、可写入

109、如何配置，使得用户从服务器 A 访问服务器 B 而无需输入密码（D）。

A、利用 NIS 同步用户的用户名和密码

B、在两台服务器上创建并配置/.rhosts 文件

C、在两台服务器上创建并配置$HOME/.netrc 文件

D、在两台服务器上创建并配置/et/hosts.equiv 文件

110、要求关机后不重新启动，shutdown 后面参数应该跟（C）。

A、–k　　B、–r　　C、-h　　D、 –c

111、一般来说，通过 web 运行 http 服务的子进程时，我们会选择（D）的用户用户权限方式，这样可以保证系统的安全。

A、root　　B、httpd　　C、guest　　D、nobody

112、以下哪项技术不属于预防病毒技术的范畴？（A）

A、加密可执行程序　　B、引导区保护

C、系统监控与读写控制　　D、校验文件

113、用户收到了一封可疑的电子邮件，要求用户提供银行账户及密码，这是属于何种攻击手段？（B）

A、缓冲区溢出攻击　　B、钓鱼攻击　　C、暗门攻击　　D、DDos 攻击

114、与另一台机器建立 IPC$会话连接的命令是（D）。

A、net user \\192.168.0.1\IPC$

B、net use \\192.168.0.1\IPC$ user:Administrator / passwd:aaa

C、net user \192.168.0.1IPC$　　D、net use \\192.168.0.1\IPC$

115、在 NT 中，如果 config.pol 已经禁止了对注册表的访问，那么黑客能够绕过这个限制吗？怎样实现？（B）

A、不可以　　B、可以通过时间服务来启动注册表编辑器

C、可以通过在本地计算机删除 config.pol 文件　　D、可以通过 poledit 命令

116、在 NT 中，怎样使用注册表编辑器来严格限制对注册表的访问？（C）

A、HKEY_CURRENT_CONFIG,连接网络注册、登录密码、插入用户 ID

B、HKEY_CURRENT_MACHINE,浏览用户的轮廓目录，选择 NTUser.dat

C、HKEY_USERS,浏览用户的轮廓目录，选择 NTUser.dat

D、HKEY_USERS,连接网络注册，登录密码，插入用户 ID

117、在 Solaris 8 下，对于/etc/shadow 文件中的一行内容如下“root:3vd4NTwk5UnLC:9038::::::”，以下说法正确的是：（E）。

A、这里的 3vd4NTwk5UnLC 是可逆的加密后的密码

B、这里的 9038 是指从 1970 年 1 月 1 日到现在的天数

C、这里的 9038 是指从 1980 年 1 月 1 日到现在的天数

D、这里的 9038 是指从 1980 年 1 月 1 日到最后一次修改密码的天数

E-以上都不正确

118、在 Solaris 8 下，对于/etc/shadow 文件中的一行内容如下：root:3vd4NTwk5UnLC:0:1:Super-User:/:”，以下说法正确的是：（A）。

A、是/etc/passwd 文件格式　　B、是/etc/shadow 文件格式

C、既不是/etc/passwd 也不是/etc/shadow 文件格式

D、这个 root 用户没有 SHELL，不可登录

E、这个用户不可登录，并不是因为没有 SHELL

119、在 Solaris 系统中，终端会话的失败登录尝试记录在下列哪个文件里面?(D)

A、-/etc/default/login　　B、/etc/nologin

C、/etc/shadow　　D、var/adm/loginlog

120、在 Windows 2000 中，以下哪个进程不是基本的系统进程:(D)

A、smss. exe　　B、csrss. Exe　　C、winlogon. exe　　D、-conime.exe

121、在 Windows 2000 中可以察看开放端口情况的是:(D)。

A、nbtstat　　B、net　　C、net show　　D、netstat

122.、在 Windows 2003 下 netstat 的哪个参数可以看到打开该端口的 PID?(C)（格式到此）

A、a　　B、n　　C、o　　D 、p

123.、在使用影子口令文件(shadowedpasswords)的 Linux 系统中，/etc/passwd 文件和/etc/shadow 文件的正确权限分别是(C)。

A、rw-r-----,-r--------　　B、rw-r--r--,-r--r--r—

C、rw-r--r--,-r--------　　Drw-r--rw-,-r-----r--

124.、制定数据备份方案时，需要重要考虑的两个因素为适合的备份时间和(B)。

A、备份介质　　B、备份的存储位置

C、备份数据量　　D、恢复备份的最大允许时间

125.、周期性行为，如扫描，会产生哪种处理器负荷?(A)

A、Idle Ioad　　B、Usage Ioad　　C、Traffic load　　D、以上都不对

126、主要由于(D)原因，使 Unix 易于移植

A、Unix 是由机器指令书写的　　B、Unix 大部分由汇编少部分用 C 语言编写

C、Unix 是用汇编语言编写的　　D、Unix 小部分由汇编大部分用 C 语言编写

127.、HP-UX 系统中，使用(A)命令查看系统版本、硬件配置等信息。

A、uname -a　　B、ifconfig　　C、netstat　　D、ps -ef

128.、Linux 文件权限一共 10 位长度，分成四段，第三段表示的内容是(C)。

A、文件类型　　B、文件所有者的权限

C、文件所有者所在组的权限　　D、其他用户的权限

129、在云计算虚拟化应用中，VXLAN 技术处于 OS 工网络模型中 2-3 层间，它综合了 2 层交换的简单性与 3 层路由的跨域连接性。它是通过在 UDP/IP 上封装 Mac 地址而实现这一点的。在简单应用场合，vxLAN 可以让虚拟机在数据中心之间的迁移变得更为简单。该技术是哪个公司主推的技术?(C)

A、惠普　　B、Juniper　　C、Cisco 与 Vmware　　D、博科 Brocade

130.、Linux 中，什么命令可以控制口令的存活时间了(A)。

A、chage　　B、passwd　　C、chmod　　D、umask

131.、Qfabric 技术是使用市场上现成的计算和存储网元并利用行业标准的网络接口将它们连接后组建大规模的数据中心，以满足未来云计算的要求。该技术概念是哪个厂家主推的概念?(B)

A、惠普　　B、uniper　　C、Cisco 与 Vmware　　D、博科 Brocade

132、为了检测 Windows 系统是否有木马入侵，可以先通过()命令来查看当前的活动连接端口。

A、ipconfig　　B、netstat -rn　　C、tracert –d　　D、netstat -an

133、网络营业厅提供相关服务的可用性应不低于（A）。

A、99.99%　　B、99.9%　　C、99%　　D、98.9%

134.、IRF(Intelligent Resilient Framework)是在该厂家所有数据中心交换机中实现的私有技术，是应用在网络设备控制平面的多虚拟技术。该技术属于哪个厂家?(A)

A、惠普　　B、Juniper　　C、Cisco 与 Vmware　　D、博科 Brocade

135.、Windows NT 的安全标识符(SID)是由当前时间、计算机名称和另外一个计算机变量共同产生的，这个变量是:(D)。

A、击键速度　　B、当前用户名

C、用户网络地址　　D、处理当前用户模式线程所花费 CPU 的时间

136、脆弱性扫描，可由系统管理员自行进行检查，原则上应不少于(B)。

A、每周一次　　B、每月一次　　C、每季度一次　　D、每半年一次

137、下面哪一个情景属于身份验证(Authentication)过程?(A)

A、用户依照系统提示输入用户名和口令

B、用户在网络上共享了自己编写的一份 Office 文档，并设定哪些用户可以阅读，哪些用户可以修改

C、用户使用加密软件对自己编写的 Office 文档进行加密，以阻止其他人得到这份拷贝后看到文档中的内容

D、某个人尝试登录到你的计算机中，但是口令输入的不对，系统提示口令错误，并将这次失败的登录过程纪录在系统日志中

138、下面哪一个情景属于授权(Authorization)过程?(B)

A、用户依照系统提示输入用户名和口令

B、用户在网络上共享了自己编写的一份 Office 文档，并设定哪些用户可以阅读，哪些用户可以修改

C、用户使用加密软件对自己编写的 Office 文档进行加密，以阻止其他人得到这份拷贝后看到文档中的内容

D、某个人尝试登录到你的计算机中，但是口令输入的不对，系统提示口令错误，并将这次失败的登录过程纪录在系统日志中

139、下列哪一条与操作系统安全配置的原则不符合?(D)

A、关闭没必要的服务　　B、不安装多余的组件

C、安装最新的补丁程序　　D、开放更多的服务

140、关于 DDoS 技术，下列哪一项描述是错误的(D)。

A、一些 DDoS 攻击是利用系统的漏洞进行攻击的

B、黑客攻击前对目标网络进行扫描是发功 DDoS 攻击的一项主要攻击信息来源

C、对入侵检测系统检测到的信息进行统计分析有利于检测到未知的黑客入侵和更为复杂的 DDoS 攻击入侵

D、DDoS 攻击不对系统或网络造成任何影响

141、关于 PPP 协议下列说法正确的是:(C)。

A、PPP 协议是物理层协议

B、PPP 协议是在 HDLC 协议的基础上发展起来的

C、PPP 协议支持的物理层可以是同步电路或异步电路

D、PPP 主要由两类协议组成:链路控制协议族 CLCP)和网络安全方面的验证协议族(PAP 和 CHAP)

142、接口被绑定在 2 层的 zone，这个接口的接口模式是（C）。

A、NAT mode　　B、Route mode

C、-Transparent mode　　D、NAT 或 Route mode

143、接入控制方面，路由器对于接口的要求包括：（D）。

A、串口接入　　B、局域网方式接入　　C、Internet 方式接入　　D、VPN 接入

144、局域网络标准对应 OSI 模型的哪几层？（C）。

A、上三层　　B、只对应网络层　　C、下三层　　D、只对应物理层

145、拒绝服务不包括以下哪一项？（D）。

A、DDoS　　B、畸形报文攻击　　C、Land 攻击　　D、ARP 攻击

146、抗 DDoS 防护设备提供的基本安全防护功能不包括（A）。

A、对主机系统漏洞的补丁升级　　B、检测 DDoS 攻击

C、DDoS 攻击警告　　D、DDoS 攻击防护

147、路由器产品提供完备的安全架构以及相应的安全模块，在软、硬件层面设置重重过滤，保护路由器业务安全。其中不对的说法是：（C）。--》缺少 D 选项

A、路由器产品支持 URPF，可以过滤大多数虚假 IP 泛洪攻击

B、路由器产品支持 CAR 功能，可以有效限制泛洪攻击

C、路由器产品不支持 ACL 配置功能，不能定制过滤规则

D、

148、路由器对于接入权限控制，包括：（D）。

A、根据用户账号划分使用权限　　B、根据用户接口划分使用权限

C、禁止使用匿名账号　　D、以上都是

149、路由器启动时默认开启了一些服务，有些服务在当前局点里并没有作用，对于这些服务：（C）。缺少 D 选项

A、就让他开着，也耗费不了多少资源　　B、就让他开着，不会有业务去访问

C、必须关闭，防止可能的安全隐患　　D、

150、设置 Cisco 设备的管理员账号时，应（C）。

A、多人共用一个账号　　B、多人共用多个账号

C、一人对应单独账号　　D、一人对应多个账号

151、什么命令关闭路由器的 finger 服务？（C）

A、disable finger　　B、no finger　　C、no finger service　　D、no service finger

152、什么是 IDS？（A）

A、入侵检测系统　　B、入侵防御系统　　C、网络审计系统　　D、主机扫描系统

153、实现资源内的细粒度授权，边界权限定义为：（B）。

A、账户　　B、角色　　C、权限　　D、操作

154、使网络服务器中充斥着大量要求回复的信息，消息带宽，导致网络或系统停止正常服务，这属于什么攻击类型？（A）

A、拒绝服务　　B、文件共享　　C、BIND 漏洞　　D、远程过程调用

155、使用 TCP 79 端口的服务是：（D）。

A、telnet　　B、SSH　　C、Web　　D、Finger

156、使用一对一或者多对多方式的 NAT 转换，当所有外部 IP 地址均被使用后，后续的内网用户如需上网，NAT 转换设备会执行什么样的动作？（C）

A、挤掉前一个用户，强制进行 NAT 转换　　B、直接进行路由转发

C、不做 NAT 转换　　D、将报文转移到其他 NAT 转换设备进行地址转换

157、私网地址用于配置本地网络、下列地址中属于私网地址的是？（C）

A、100.0.0.0　　B、172.15.0.0　　C、192.168.0.0　　D、244.0.0.0

158、随着 Internet 发展的势头和防火墙的更新，防火墙的哪些功能将被取代。（D）

A、使用 IP 加密技术　　B、日志分析工作

C、攻击检测和报警　　D、对访问行为实施静态、固定的控制

159、随着安全要求的提高、技术的演进，（D）应逐步实现物理隔离，或者通过采用相当于

物理隔离的技术（如 MPLSVPN）实现隔离。

A、局域网　　B、广域网及局域网　　C、终端　　D、广域网

160、通过向目标系统发送有缺陷的 IP 报文，使得目标系统在处理这样的 IP 包时会出现崩溃，请问这种攻击属于何种攻击？（D）

A、拒绝服务（DoS）攻击　　B、扫描窥探攻击

C、系统漏洞攻击　　D、畸形报文攻击

161、通信领域一般要求 3 面隔离，即转发面、控制面、用户面实现物理隔离，或者是逻辑隔离，主要目的是在某一面受到攻击的时候，不能影响其他面。路由器的安全架构在实现上就支持：（D）

A、转发面和控制面物理隔离　　B、控制面和用户面逻辑隔离

C、转发面和用户面逻辑隔离　　D、以上都支持

162、网管人员常用的各种网络工具包括 telnet、ftp、ssh 等，分别使用的 TCP 端口号是（B）。

A、21、22、23　　B、23、21、22　　C、23、22、21　　D、21、23、22

163、网络安全工作的目标包括：（D）。

A、信息机密性　　B、信息完整性　　C、服务可用性　　D、以上都是

164、网络安全在多网合一时代的脆弱性体现在（C）。

A、网络的脆弱性　　B、软件的脆弱性　　C、管理的脆弱性　　D、应用的脆弱性

165、应限制 Juniper 路由器的 SSH（A），以防护通过 SSH 端口的 DoS 攻击。

A、并发连接数和 1 分钟内的尝试连接数　　B、并发连接数

C、1 分钟内的尝试连接数　　D、并发连接数和 3 分钟内的尝试连接数

166、应用网关防火墙的逻辑位置处在 OSI 中的哪一层？（C）

A、传输层　　B、链路层　　C、应用层　　D、物理层

167、应用网关防火墙在物理形式上表现为？（B）

A、网关　　B、堡垒主机　　C、路由　　D、交换机

168、用来追踪 DDoS 流量的命令式：（C）

A、ip source-route　　B、ip cef　　C、ip source-track　　D、ip finger

169、用于保护整个网络 IPS 系统通常不会部署在什么位置？（D）

A、网络边界　　B、网络核心　　C、边界防火墙内　　D、业务终端上

170、用于实现交换机端口镜像的交换机功能是：（D）

A、PERMIT LIST　　B、PVLAN　　C、VTP　　D、SPAN

171、有关 L2TP（Layer 2 Tunneling Protocol）协议说法有误的是（D）。

A、L2TP 是由 PPTV 协议和 Cisco 公司的 L2F 组合而成

B、L2TP 可用于基于 Internet 的远程拨号访问

C、为 PPP 协议的客户建立拨号连接的 VPN 连接

D、L2TP 只能通过 TCP/IP 连接

172、有关 PPTP（Point-to-Point Tunnel Protocol）说法正确的是（C）。

A、PPTP 是 Netscape 提出的　　B、微软从 NT3.5 以后对 PPTP 开始支持

C、PPTP 可用在微软的路由和远程访问服务上　　D、它是传输层上的协议

173、有一些应用，如微软 Out look 或 MSN。它们的外观会在转化为基于 Web 界面的过程中丢失，此时要用到以下哪项技术：（B）

A、Web 代理　　B、端口转发　　C、文件共享　　D、网络扩展

174、预防信息篡改的主要方法不包括以下哪一项？（A）

A、使用 VPN 技术　　B、明文加密　　C、数据摘要　　D、数字签名

175、域名服务系统（DNS）的功能是（A）。

A、完成域名和 IP 地址之间的转换　　B、完成域名和网卡地址之间的转换

C、完成主机名和 IP 地址之间的转换　　D、完成域名和电子邮件地址之间的转换

176、源 IP 为 100.1.1.1，目的 IP 为 100.1.1.255，这个报文属于什么攻击？（B）（假设该网段掩码为 255.255.255.0）

A、LAND 攻击　　B、SMURF 攻击　　C、FRAGGLE 攻击　　D、WINNUKE 攻击

177、在 AH 安全协议隧道模式中，新 IP 头内哪个字段无需进行数据完整性校验？（A）

A、TTL　　B、源 IP 地址　　C、目的 IP 地址　　D、源 IP 地址+目的 IP 地址

178、在 C/S 环境中，以下哪个是建立一个完整 TCP 连接的正确顺序？（D）

A、SYN，SYN/ACK，ACK　　B、Passive Open,Active Open,ACK,ACK

C、SYN,ACK/SYN,ACK　　D、Active Open/Passive Open,ACK,ACK

179、在 L2TP 应用场景中，用户的私有地址分配是由以下哪个组建完成？（B）

A、LAC　　B、LNS　　C、VPN Client　　D、用户自行配置

180、在 OSI 模型中，主要针对远程终端访问，任务包括会话管理、传输同步以及活动管理等以下是哪一层（A）

A、应用层　　B、物理层　　C、会话层　　D、网络层

181、在 OSI 参考模型中有 7 个层次，提供了相应的安全服务来加强信息系统的安全性。以

下哪一层提供了抗抵赖性？（B）

A、表示层　　B、应用层　　C、传输层　　D、数据链路层

182、在安全策略的重要组成部分中，与 IDS 相比，IPS 的主要优势在哪里？（B）

A、产生日志的数量　　B、攻击减少的速度

C、较低的价格　　D、假阳性的减少量

183、在安全审计的风险评估阶段，通常是按什么顺序来进行的？（A）

A、侦查阶段、渗透阶段、控制阶段　　B、渗透阶段、侦查阶段、控制阶段

C、控制阶段、侦查阶段、渗透阶段　　D、侦查阶段、控制阶段、渗透阶段

184、在层的方式当中，哪种参考模型描述了计算机通信服务和协议？（D）

A、IETF 因特网工程工作小组　　B、ISO 国际标准组织

C、IANA 因特网地址指派机构　　D、OSI 开放系统互联

185、在传输模式 IPSec 应用情况中，以下哪个区域数据报文可受到加密安全保护？（D）

A、整个数据报文　　B、原 IP 头　　C、新 IP 头　　D、传输层及上层数据报文

186、在点到点链路中，OSPF 的 Hello 包发往以下哪个地址？（B）

A、127.0.0.1　　B、224.0.0.5　　C、233.0.0.1　　D、255.255.255.255

187、在建立堡垒主机时，（A）。

A、在堡垒主机上应设置尽可能少的网络服务

B、在堡垒主机上应设置尽可能多的网络服务

C、对必须设置的服务给予尽可能高的权限

D、不论发生任何入侵情况，内部网始终信任堡垒主机

188、在进行 Sniffer 监听时，系统将本地网络接口卡设置成何种侦听模式？（D）

A、unicast 单播模式　　B、Broadcast 广播模式

C、Multicast 组播模式　　D、Promiscuous 混杂模式

189、在零传输（Zone transfers）中 DNS 服务使用哪个端口？（A）

A、TCP 53　　B、UDP 53　　C、UDP 23　　D、TCP23

190、在入侵检测的基础上，锁定涉嫌非法使用的用户，并限制和禁止该用户的使用。这种访问安全控制是？（C）

A、入网访问控制　　B、权限控制　　C、网络检测控制　　D、防火墙控制

191、在思科设备上，若要查看所有访问表的内容，可以使用的命令式（B）

A、show all access-lists　　B、show access-lists

C、show ip interface　　D、show interface

192、在网络安全中，中断指攻击者破坏网络系统的资源，使之变成无效的或无用的这是对（A）。

A、可用性的攻击　　B、保密性的攻击　　C、完整性的攻击　　D、真实性的攻击

193、在一个局域网环境中，其内在的安全威胁包括主动威胁和被动威胁。以下哪一项属于被动威胁？（C）

A、报文服务拒绝　　B、假冒　　C、数据流分析　　D、报文服务更改

194、在以下 OSI 七层模型中，synflooding 攻击发生在哪层？（C）

A、数据链路层　　B、网络层　　C、传输层　　D、应用层

195、在以下哪类场景中，移动用户不需要安装额外功能（L2TP）的 VPDN 软件？（B）

A、基于用户发起的 L2TP VPN　　B、基于 NAS 发起的 L2TP VPN

C、基于 LNS 发起的 L2TP VPN　　D、以上都是

196、账户口令管理中 4A 的认证管理的英文单词为：（B）

A、Account　　B、Authentication　　C、Authorization　　D、Audit

197、只具有（A）和 FIN 标志集的数据包是公认的恶意行为迹象。

A、SYN　　B、date　　C、head　　D、标志位

198、主从账户在 4A 系统的对应关系包含：（D）

A、1 -N　　B、1 -1　　C、N -1　　D、以上全是

199、主动方式 FTP 服务器要使用的端口包括（A）。

A、TCP 21 TCP 20　　B、TCP21 TCP 大于 1024 的端口

C、TCP 20、TCP 大于 1024 端口　　D、都不对

200、下列（D）因素不是影响 IP 电话语音质量的技术因素。

A、时延　　B、抖动　　C、回波　　D、GK 性能

201、下列安全协议中使用包括过滤技术，适合用于可信的 LAN 到 LAN 之间的 VPN（内部 VPN）的是（D）。

A、PPTP　　B、L2TP　　C、SOCKS v5　　D、IPSec

202、下列不是抵御 DDoS 攻击的方法有（D）。

A、加强骨干网设备监控　　B、关闭不必要的服务

C、限制同时打开的 Syn 半连接数目　　D、延长 Syn 半连接的 time out 时间

203、下列措施不能增强 DNS 安全的是（C）。

A、使用最新的 BIND 工具　　B、双反向查找

C、更改 DNS 的端口号　　D、不要让 HINFO 记录被外界看到

204、下列各种安全协议中使用包过滤技术，适合用于可信的 LAN 到 LAN 之间的 VPN，即内部网 VPN 的是（）。

A、PPTP　　B、L2TP　　C、SOCKS v5　　D、IPSec

205、下列哪个属于可以最好的描述系统和网络的状态分析概念，怎么处理其中的错误才是最合适？（D）

A、回应的比例　　B、被动的防御　　C、主动的防御　　D、都不对

206、下列哪项是私有 IP 地址？（A）

A、10.5.42.5　　B、172.76.42.5　　C、172.90.42.5　　D、241.16.42.5

207、下列哪一项能够提高网络的可用性？（B）

A、数据冗余　　B、链路冗余　　C、软件冗余　　D、电源冗余

208、下列哪一种攻击方式不属于拒绝服务攻击：（A）。

A、LOphtCrack　　B、Synflood　　C、Smurf　　D、Ping of Death

209、下列哪一项是 arp 协议的基本功能？（A）

A、通过目标设备的 IP 地址，查询目标设备的 MAC 地址，以保证通信的进行

B、对局域网内的其他机器广播路由地址

C、过滤信息，将信息传递个数据链路层　　D、将信息传递给网络层

210、最早的计算机网络与传统的通信网络最大的区别是什么？（A）

A、计算机网络采用了分组交换技术　　B、计算机网络采用了电路交换技术

C、计算机网络的可靠性大大提高　　D、计算机网络带宽和速度大大提高

211、以下哪个属于 IPS 的功能？（A）

A、检测网络攻击　　B、网络流量检测　　C、实时异常告警　　D、以上都是

212、以下说法错误的是（C）。

A、安全是一个可用性与安全性之间的平衡过程　　B、安全的三要素中包含完整性

C、可以做到绝对的安全　　D、网络安全是信息安全的子集

213、以下属于 4A 策略管理模块可以管理的为（C）。

A、访问控制策略　　B、信息加密策略　　C、密码策略　　D、防火墙策略

214、最早研究计算机网络的目的是什么？（B）

A、共享硬盘空间、打印机等设备　　B、共享计算资源

C、直接的个人通信　　D、大量的数据交换

215、防火墙截取内网主机与外网通信，由防火墙本身完成与外网主机通信，然后把结果传回给内网主机，这种技术称为（C）。

A、内容过滤　　B、地址转换　　C、透明代理　　D、内容中转

216、可以通过哪种安全产品划分网络结构，管理和控制内部和外部通讯（A）。

A、防火墙　　B、CA 中心　　C、加密机　　D、防病毒产品

217、网络隔离技术的目标是确保把有害的攻击隔离，在保证网络内部信息不外泄的前提下，完成网络间数据的安全交换。下列隔离技术中，安全性最好的是（D）。

A、多重安全网关　　B、防火墙　　C、Vlan 隔离　　D、物理隔离

218、下列哪项不是 Tacacs+协议的特性。（A）

A、扩展记账　　B、加密整个数据包　　C、使用 TCP　　D、支持多协议

219、一个数据包过滤系统被设计成只允许你要求服务的数据包进入，而过滤掉不必要的服务。这属于什么基本原则？（A）

A、最小特权　　B、阻塞点　　C、失效保护状态　　D、防御多样化

220、包过滤防火墙工作的好坏关键在于？（C）

A、防火墙的质量　　B、防火墙的功能　　C、防火墙的过滤规则设计　　D、防火墙的日志

221、对于日常维护工作，连接路由器的协议通常使用：（B）。缺少 D 选项

A、TELNET，简单，容易配置　　B、SSH &SSHv2 加密算法强劲，安全性好

C、TELNET 配置 16 位长的密码，加密传输，十分安全　　D、

222、BOTNET 是（C）。

A、普通病毒　　B、木马程序　　C、僵尸网络　　D、蠕虫病毒

223、监听的可能性比较低的是（B）数据链路。

A、Ethernet　　B、电话线　　C、有线电视频道　　D、无线电

224、当 IPS 遇到软件/硬件问题时，强制进入直通状态，以避免网络断开的技术机制称为（B）。

A、pass　　B、bypass　　C、watchdog　　D、HA

225、网络环境下的 security 是指（A）。

A、防黑客入侵，防病毒，窃取和敌对势力攻击

B、网络具有可靠性，可防病毒，窃密和敌对势力攻击

C、网络具有可靠性，容灾性，鲁棒性

D、网络的具有防止敌对势力攻击的能力

226、某一案例中，使用者已将无线 AP 的 SSID 广播设置为禁止，并修改了默认 SSID 值，但仍有未经授权的客户端接入该无线网络，这是因为（D）

A、禁止 SSID 广播仅在点对点的无线网络中有效

B、未经授权客户端使用了默认 SSID 接入

C、无线 AP 开启了 DHCP 服务

D、封装了 SSID 的数据包仍然会在无线 AP 与客户端之间传递

227、为了保护 DNS 的区域传送（zone transfer），应该配置防火墙以阻止（B）。

1.UDP

2.TCP

3.53

4.52

A、1,3　　B、2,3　　C、1,4　　D、2,4

228、以下不属于代理服务技术优点的是（D）。

A、可以实现身份认证　　B、内部地址的屏蔽盒转换功能

C、可以实现访问控制　　D、可以防范数据驱动侵袭

229、应控制自互联网发起的会话并发连接数不超出网上营业厅设计容量的（C）。

A、60%　　B、70%　　C、80%　　D、90%

230、TCP 协议与 UDP 协议相比，TCP 是（B），UDP 是（）。

A、设置起来麻烦；很好设置　　B、容易；困难

C、面向连接的；非连接的　　D、不可靠的；可靠的

231、交换机转发以太网的数据基于：（B）。

A、交换机端口号　　B、MAC 地址　　C、IP 地址　　D、数据类别

232、HTTP，FTP，SMTP 建立在 OSI 模型的哪一层？（D）

A、2 层-数据链路层　　B、3 层-网络层　　C、4 层-传输层　　D、7 层-应用层

233、网络安全的基本属性是（D）。

A、机密性　　B、可用性　　C、完整性　　D、以上都是

234、网络安全的主要目的是保护一个组织的信息资产的（A）。

A、机密性、完整性、可用性　　B、参照性、可用性、机密性、

C、可用性、完整性、参照性　　D、完整性、机密性、参照性

235、DBS 是采用了数据库技术的计算机系统。DBS 是一个集合体，包含数据库、计算机硬件、软件和（C）。

A、系统分析员　　B、程序员　　C、数据库管理员　　D、操作员

236、MySQL -h host -u user -p password 命令的含义如下，哪些事正确的？（D）

A、-h 后为 host 为对方主机名或 IP 地址　　B、-u 后为数据库用户名

C、-p 后为密码　　D、以上都对

237、Oracle 当连接远程数据库或其它服务时，可以指定网络服务名，Oracle9i 支持 5 中命名方法，请选择错误的选项。（D）

A、本地命名和目录命名　　B、Oracle 名称（Oracle Names）

C、主机命名和外部命名　　D、DNS 和内部命名

238、Oracle 的数据库监听器（LISTENER）的默认通讯端口是？（A）

A、TCP 1521　　B、TCP 1025　　C、TCP 1251　　D、TCP 1433

239、Oracle 默认的用户名密码为（A）。

A、Scote/tiger　　B、root　　C、null　　D、rootroot

240、Oracle 数据库中，物理磁盘资源包括哪些（D）。

A、控制文件　　B、重做日志文件　　C、数据文件　　D、以上都是

241、Oracle 中启用审计后，查看审计信息的语句是下面哪一个？（C）

A、select * from SYS.AUDIT$　　B、select * from syslogins

C、select * from SYS.AUD$　　D、AUDIT SESSION

242、SMTP 的端口？（A）

A、25　　B、23　　C、22　　D、21

243、SQL Server 的登录账户信息保存在哪个数据库中？（C）

A、model　　B、msdb　　C、master　　D、tempdb

244、SQL Sever 的默认 DBA 账号是什么？（B）

A、administrator　　B、sa　　C、root　　D、SYSTEM

245、SQL Sever 的默认通讯端口有哪些？（B）

A、TCP 1025　　B、TCP 1433　　C、UDP 1434　　D、TCP 14333　　E、TCP 445

246、SQL Sever 中可以使用哪个存储过程调用操作系统命令，添加系统账号？（B）

A、xp_dirtree　　B、xp_cmdshell　　C、xp_cmdshell　　D、xpdeletekey

247、SQL Sever 中下面哪个存储过程可以执行系统命令？（C）

A、xp_regread　　B、xp_command　　C、xp_cmdshell　　D、sp_password

248、SQL 的全局约束是指基于元祖的检查子句和（C）。

A、非空值约束　　B、域约束子句　　C、断言　　D、外键子句

249、SQL 数据库使用以下哪种组件来保存真实的数据？（C）

A、Schemas　　B、Subschemas　　C、Tables　　D、Views

250、SQL 语句中，彻底删除一个表的命令是（B）。

A、delete　　B、drop　　C、clear　　D、remore

251、SQL 语言可以（B）在宿主语言中使用，也可以独立地交互式使用。

A、-极速　　B、-嵌入　　C、-混合　　D、-并行

252、SSL 安全套接字协议所用的端口是（B）。

A、80　　B、443　　C、1433　　D、3389

253、不属于数据库加密方式的是（D）。

A、库外加密　　B、库内加密　　C、硬件/软件加密　　D、专用加密中间件

254、测试数据库一个月程序主要应对的风险是（B）。

A、非授权用户执行“ROLLBACK”命令　　B、非授权用户执行“COMMIT”命令

C、非授权用户执行“ROLLRORWARD”命令　　D、非授权用户修改数据库中的行

255、查看 Oracle　8i 及更高版本数据库的版本信息的命令是（C）。----缺少 CD 选项

A、cd $Oracle_HOME/orainst　B、C-cd $Oracle_HIME/orainst　　C、　　D、

256、从安全的角度来看，运行哪一项起到第一道防线的作用？（C）

A、远端服务器　　B、WEB 服务器　　C、防火墙　　D、使用安全 shell 程序

257、从下列数据库分割条件中，选出用于抵御跟踪器攻击和抵御对线性系统攻击的一项。（B）。

A、每个分割区 G 有 g=|G|记录，其中 g=0 或 g>=n，且 g 为偶数，

B、记录必须成对地加入 G 或从 G 中删除

C、查询集虚报口各个分割区，如果查询含有一个以上记录的统计信息是从 m 各分割区 G1，G2，… …Gm 中每一个分割区而来的，则统计信息 g（G1VG2V… …VGm）是允许发布

D、记录必须不对地加入 G 或从 G 中删除

258、单个用户使用的数据库视图的描述为（A）。

A、外模式　　B、概念模式　　C、内模式　　D、存储模式

259、对于 IIS 日志记录，推荐使用什么文件格式？（D）

A、Microsoft　IIS 日志文件格式　　B、NCSA 公用日志文件格式

C、ODBC 日志记录格式　　D、W3C 扩展日志文件格式

260、对于 IIS 日志文件的存放目录，下列哪项设置是最好的？（D）----缺少 D 选型

A、%WinDir%\System32\LogFiles　　B、C:\Inetpub\wwwroot\LogFiles

C、C:\LogFiles..)-F:\LogFiles　　D、

261、对于 IIS 日志文件的访问权限，下列哪些设置是正确的？（D）

A、SYSTEM（完全控制）Administrator（完全控制）Users（修改）

B、SYSTEM（完全控制）Administrator（完全控制）Everyone（读取和运行）

C、SYSTEM（完全控制）Administrator（完全控制）Inernet 来宾账户（读取和运行）

D、SYSTEM（完全控制）Administrator（完全控制）

262、对于数据库的描述一下哪项说法是正确的？（A）

A、数据和一系列规则的集合　　B、一种存储数据的软件

C、一种存储数据的硬件　　D、是存放人量数据的软件

263、攻击者可能利用不必要的 extproc 外部程序调用功能获取对系统的控制权，威胁系统安全。关闭 Extproc 功能需要修改 TNSNAMES.ORA 和 LISTENER.ORA 文件删除一下条目，其中有一个错误的请选择出来（A）。

A、sys_ertproc　　B、icache_extproc

C、PLSExtproc　　D、extproc

264、关系数据库中，实现实体之间的联系是通过表与表之间的（D）。

A、公共索引　　B、公共存储

C、公共元组　　D、公共属性

265、关系型数据库技术的特征由一下哪些元素确定的？（A）

A、行和列　　B、节点和分支

C、Blocks 和 Arrows　　D、父类和子类

266、关于 WEB 应用软件系统安全，说法正确的是（D）？

A、Web 应用软件的安全性仅仅与 WEB 应用软件本身的开发有关

B、系统的安全漏洞属于系统的缺陷，但安全漏洞的检测不属于测试的范畴

C、黑客的攻击主要是利用黑客本身发现的新漏洞

D、以任何违反安全规定的方式使用系统都属于入侵

267、目前数据大集中是我国重要的大型分布式信息系统建设和发展的趋势，数据大集中就是将数据集中存储和管理，为业务信息系统的运行搭建了统一的数据平台，对这种做法认识正确的是（D）？

A、数据库系统庞大会提供管理成本　　B、数据库系统庞大会降低管理效率

C、数据的集中会降低风险的可控性　　D、数据的集中会造成风险的集中

268、哪一个是 PKI 体系中用以对证书进行访问的协议（B）？

A、SSL　　B、LDAP　　C、CA　　D、IKE

269、如果一个 SQL Server 数据库维护人员，需要具有建立测试性的数据库的权限，那么应该指派给他哪个权限（A）？

A、Database　Creators　　B、System　Administrators

C、Server　Administrators　　D、Security　Adiministrators

270、如果以 Apache 为 WWW 服务器，（C）是最重要的配置文件。

A、access.conf　　B、srm.cong　　C、httpd.conf　　D、mime.types

271、若有多个 Oracle 数据需要进行集中管理，那么对 sysdba 的管理最好选择哪种认证方式（B）？

A、系统认证　　B、password 文件认证方式　　C、域认证方式　D、以上三种都可

272、数据库管理系统 DBMS 主要由哪两种部分组成？（A）

A、文件管理器和查询处理器　　B、事务处理器和存储管理器

C、存储管理器和查询处理器　　D、文件管理器和存储管理器

273、数据库系统与文件系统的最主要区别是（B）。

A、数据库系统复杂，而文件系统简单

B、文件系统不能解决数据冗余和数据独立性问题，而数据库系统可以解决

C、文件系统只能管理程序文件，而数据库系统能够管理各宗类型的文件

D、文件系统管理的数据量较少，而数据库系统可以管理庞大的数据量

274、为了防止电子邮件中的恶意代码，应该由（A）方式阅读电子邮件。

A、纯文本　　B、网页　　C、程序　　D、会话

275、为了应对日益严重的垃圾邮件问题，人们设计和应用了各种垃圾邮件过滤机制，以下哪一项是耗费计算资源最多的一种垃圾邮件过滤机（D）？

A、SMTP 身份认证　　B、逆向名字解析　　C、黑名单过滤　　D、内容过滤

276、为什么要对数据库进行“非规范化”处理（B）？

A、确保数据完整性　B、增加处理效率　C、防止数据重复　D、节省存储空间

277、下列不属于 WEB 安全性测试的范畴的是（A）？

A、数据库内容安全性　B、客户端内容安全性

C、服务器端内容安全性　D、日志功能

278、下列操作中，哪个不是 SQL Server 服务管理器功能（A）？

A、执行 SQL 查询命令　B、停止 SQL　Server 服务

C、暂停 SQL　Server 服务　D、启动 SQL　Server 服务

279、下列关于 IIS 的安全配置，哪些是不正确的（C）？

A、将网站内容移动到非系统驱动程序　B、重命名 IUSR 账户

C、禁用所有 WEB 服务扩展　D、创建应用程序池

280、下列哪些不是广泛使用 http 服务器？（D）

A、W3C　B、Apache　C、IIS　D、IE

281、下列哪些属于 WEB 脚本程序编写不当造成的（C）？

A、IIS5.0　Webdav Ntdll.dll 远程缓冲区一处漏洞

B、apache 可以通过../../../../../../etc/passwd 方位系统文件

C、登陆页面可以用 password=’a’or’a’=’a’绕过

D、数据库中的口令信息明文存放

282、下列哪种方法不能有效的防范 SQL 进入攻击（C）？

A、对来自客户端的输入进行完备的输入检查

B、把 SQL 语句替换为存储过程、预编译语句或者使用 ADO 命令对象

C、使用 SiteKey 技术

D、关掉数据库服务器或者不使用数据库

283、下列哪种工具不是 WEB 服务器漏洞扫描工具（B）？

A、Nikto　B、Web　Dumper　C、paros　Proxy　D、Nessus

284、下列哪种攻击不是针对统计数据库的（D）？

A、小查询集合大查询集攻击　B、中值攻击　C、跟踪攻击　D、资源解析攻击

285、下列哪项中是数据库中涉及安全保密的主要问题（A）？

A、访问控制问题　B、数据的准确性问题

C、数据库的完整性问题　　D、数据库的安全性问题

286、下列应用服务器中，不遵循 J2EE 规范的是（C）？

A、MTS　　B、WebLogic　　C、Oracle 9iApplication Server　　D、WebSpere

287、下面关于 IIS 报错信息含义的描述正确的是（B）？

A、401-找不到文件　　B、403-禁止访问　　C、404-权限问题　　D、500-系统错误

288、下面关于 Oracle 进程的描述，哪项是错误的（B）？

A、运行在 Windows 平台上的 Oracle 能让每个用户组程序化地打开新的进程，这是一个安全隐患

B、在 Windows 平台，除了 Oracle.exe 进程外还有其他的独立进程

C、unix 平台上有多个独立运行的进程，包括数据写进程、日志写进程、存档进程、系统监控进程、进程监控进程

D、有一个特殊的内存区域被映射为*nix 平台上的所有进程，此区域时系统全局去

289、下面哪一项是与数据库管理员（DBA）职责不相容的（C）？

A、数据管理　　B、信息系统管理　　C、系统安全　　D、信息系统规划

290、下面选型中不属于数据库安全控制的有（D）。

A、信息流控制　　B、推论控制　　C、访问控制　　D、隐通道控制

291、下面选型中不属于数据库安全模型的是（D）。

A、自主型安全模型　　B、强制型安全模型　　C、基于角色的模型　　D、访问控制矩阵

292、一般来说，通过 WEB 运行 http 服务的子进程时，我们会选择（D）的用户权限方式，这样可以保证系统的安全。

A、root　　B、httpd　　C、guest　　D、nobody

293、一下不是数据库的加密技术的是（D）。

A、库外加密　　B、库内加密　　C、硬件加密　　D、固件加密

294、一下对于 Oracle 文件系统描述错误的是（B）？

A、*nix 下 Oracle 的可执行文件在$Oracle_HOME/bin/Oracle,$Oracle_HOME/bin 也应该包含在路径环境变量内

B、Windows 下 Oracle 的可执行文件在%Oracle_HOME%\bin\Oracle.exe,其他

C、硬件加密　　D、固件加密

295、以下几种功能中，哪个是 DBMS 的控制功能（A）？

A、数据定义　　B、数据恢复　　C、数据修改　　D、数据查询

296、以下哪个安全特征和机制是 SQL 数据库所特有的（B）？

A、标识和鉴别　　B、数据恢复　　C、数据修改　　D、数据查询

297、以下哪个是数据库管理员（DBA）可以行使的职责（A）？

A、系统容量规划　　B、交易管理　　C、审计　　D、故障承受机制

298、以下哪条命令能利用“SQL 注入”漏洞动用 XP_cmdshell 存储过程，获得某个子目的清单？（A）

A、http://localhost/script?':EXEC+master..XP_cmdshell+'dir':--

B、http://localhost/script?1':EXEC+master..XP_cmdshell+'　dir':--

C、http://localhost/script?0':EXEC+master..XP_cmdshell+'　dir':--

D、http://localhost/script?1':EXEC+master..XP_cmdshell+'　dir'--

299、以下哪条命令能利用“SQL”漏洞动用 XP_cmdshell 存储过程，启动或停止某项服务？（B）

A、http://localhost/script?':EXEC+master..XP_servicecontrol+'start',+'Server'　;-

B、http://localhost/script?0':EXEC+master..XP_servicecontrol+'start',+'Server'　;--

C、http://localhost/script?1':EXEC+master..XP_servicecontrol+'start',+'Server'　; --

D、http://localhost/script?0':EXEC+master..XP_servicecontrol+'start',+'Server' --

300、以下哪项不属于访问控制策略的实施方式？（D）

A、子模式法　　B、修改查询法　　C、集合法　　D、验证法

301、以下哪一项是和电子邮件系统无关的？（）

A、PEM(Privacy　enhanced　mail)　　B、PGP(Pretty　good　privacy)

C、X.500　　D、X.400

302、以下哪种方法可以用于对付数据库的统计推论？（C）

A、信息流控制　　B、共享资源矩阵　　C、查询控制　　D、间接存取

303、以下是对层次数据库结构的描述，请选择错误描述的选项。（C）

A、层次数据库结构将数据通过一对多或父节点对子节点的方式组织起来

B、一个层次数据库中，根表或父表位于一个类似于树形结构的最上方，它的字表中包含相关数据

C、它的优点是用户不需要十分熟悉数据库结构

D、层次数据库模型的结构就像是一棵倒转的树

304、以下是对单用户数据库系统的描述，请选择错误描述的选项（C）。

A、单用户数据库系统是一种早期的最简单的数据库系统

B、在单用户系统中，整个数据库系统，包括应用程序、DBMS、数据，都装在一台计算机之间不能共享数据

C、在单用户系统中，由多个用户共用，不同计算机之间能共享数据

D、单用户数据库系统已经不适用于现在的使用，被逐步淘汰了

305、以下是对分布式结构数据库系统的描述，请选择错误描述的选项。（D）

A、分布式结构的数据库系统的数据在逻辑上是一个整体，但物理地分布在计算机网络的不同节点上，每个节点上的主机又带有多个终端用户

B、网络中的每个节点都可以独立的处理数据库中的数据，执行全局应用

C、分布式结构的数据库系统的数据分布存放给数据的处理、管理和维护带来困难

D、分布式结构的数据库系统的数据只在存放在服务器端，其他节点只进行处理和执行

306、以下是对关系数据库结构的描述，请选择错误描述的选项。（D）

A、数据存储的主要载体是表，或相关数据组

B、有一对一、一对多、多对多三种表关系

C、表关联是通过引用完整性定义的，这是通过主码和外码（主键或外键约束条件实现的）

D、缺点是不支持 SQL 语言

307、以下是对客户/服务器数据库系统的描述，请选择错误描述的选项。（A）

A、客户端的用户将数据进行处理可自行存放到本地，无须传送到服务器处理，从而显著减少了网络上的数据传输量，提高了系统的性能和负载能力

B、主从式数据库系统中的主机和分布式数据库系统中的每个节点都是一个通用计算机，既执行 DBMS 功能又执行应用程序

C、在网络中把某些节点的计算机专门用于执行 DBMS 核心功能，这台计算机就成为数据库服务器

D、其他节点上的计算机安装 DBMS 外围应用开发工具和应用程序，支持用户的应用，称为客户机

308、以下是对面向对象数据库结构的描述，请选择错误描述的选项。（C）

A、它允许用对象的概念来定义与关系数据库交互

B、面向对象数据库中有两个基本的结构：对象和字面量

C、优点是程序员需要掌握与面向对象概念以及关系数据库有关的存储

D、缺点是用户必须理解面向对象概念，目前还没有统一的标准，稳定性还是一个值得关注的焦点

309、以下是对主从式结构 数据库系统的描述，请选择错误描述的选项。（D）

A、主从式结构是指一个主机带多个终端的多用户结构

B、在这种结构中，数据库系统的应用程序、DBMS、数据等都集中存放在主机上

C、所有处理任务都由主机来完成，各个用户通过主机的终端并发地存取数据，能够共享数据源

D、主从式结构的优点是系统性能高，是当终端用户数目增加到一定程度后，数据的存取通道不会形成瓶颈

311、在 GRUB 的配置文件 grub.conf 中，“timeout=-1”的含义是（C）。

A、不等待用户选择，直接启动默认的系统

B、在 10 秒钟内，等待用户选择要启动的系统

C、一直等待用户选择要启动的系统

D、无效

312、在 Oracle 中，quota 可以限制用户在某个表空间上最多可使用多少字节，如果要限制 data_ts 表 500K，以下哪个是正确的命令？（B）

A、quo 500k in data_ts　　B、quota 500K on data_ts

C、quota data_ts ,imit 500K　　D、quota data_ts on 500K

313、在 Oracle 中，建表约束包括引用完整性约束、check 完整性约束，还有以下三项是正确的，请排除一个错误选项。（D）

A、非空完整性约束　　B、唯一完整性约束

C、主码完整性约束　　D、数据角色性约束

314、在 Oracle 中，将 scott 的缺省表空间改为 data2_ts，下列哪个是正确的？（A）

A、ALTER USER scott DEFAULT TABLESPACE data2_ts

B、ALTER DEFAULT TABLESPACE data2_ts USER scott

C、ALTER USER scott TABLESPACE DEFAULT data2_ts

D、ALTER scott USER DEFAULT TABLESPACE data2_ts

315、在 Oracle 中，将 scott 的资源文件改为 otherprofile，下列哪个是正确的？（C）

A、ALTER PROFILE USER scott otherprofile

B、ALTER otherprofile USER scottPROFILE

C、ALTER USER scott PROFILE otherprofile

D、ALTER scott USER PROFILE otherprofile

316、在 Oracle 中，将当前系统所有角色都授予 scott，除 Payroll 外，下列哪个是正确的？（D）

A、ALTER DEFAULT ROLLE USER scott ALL EXCEPT Payroll

B、ALTER USER DEFAULT ROLLE ALL EXCEPT Payroll

C、ALTER DEFAULT ROLLE ALL EXCEPT USER scott

D、ALTER USER scott DEFAULT ROLLE ALL EXCEPT Payroll

317、在 Oracle 中，用 ALTER 将 scott 的口令改为 hello，下列哪个是正确的？（A）

A、ALTER USER scott IDENTIFIED BY hello

B、ALTER scott USER IDENTIFIED BY hello

C、ALTER USER scott IDENTIFIED AS hello

D、ALTER USER hello IDENTIFIED BY scott

318、在 WEB 应用软件的基本结构中，客户端的基础是（A）。

A、HTML 文档　　B、客户端程序

C、HTML 协议　　D、浏览器

319、在 WEB 应用软件的系统测试技术中，下面不属于安全性测试内容的是（C）。

A、客户端的内容安全性　　B、服务器的内容安全性

C、数据库的内容安全性　　D、Cookie 安全性

320、在典型的 WEB 应用站点的层次结构中，“中间件”是在哪里运行的？（C）

A、浏览器客户端　　B、web 服务器

C、应用服务器　　D、数据库服务器

321、在分布式开放系统的环境中，以下哪个选项的数据库访问服务提供允许或禁止访问的能力？（C）

A、对话管理服务　　B、事务管理服务

C、资源管理服务　　D、控制管理服务

322、主要用于加密机制的协议时（D）。

A、HTTP　　B、FTP　　C、TELNETD　　D、SSL

323、分布式关系型数据库与集中式的关系型数据库相比在以下哪个方面有缺点？（D）

A、自主性　　B、可靠性　　C、灵活性　　D、数据备份

324、下面对 Oracle 的密码规则描述，哪个是错误的？（D）

A、Oracle 密码必须由英文字母，数值，#，下划线(_)，美元字符（$）构成，密码的最大长度为 30 字符，并不能以“$”,“#”,“_”或任何数字卡头；密码不能包含像“SELECT”,“DELETE”,“CREATE”这类的 ORACLE/SQL 关键字

B、Oracle 的若算法加密机制（）两个相同的用户名和密码在两台不同的 ORACLE 数据库机器中，将具有相同的哈希值。这些哈希值存储在 SYS.USER 表中，可以通过像 DBA_USE 这类的试图来访问

C、Oracle 默认配置下，每个中户如果有 10 此的失败登录，此账户将会被锁定

D、SYS 账户在 Oracle 数据库中有最高权限，能够做任何事情，包括启动/关闭 Oracle 数据库，如果 SYS 被锁定，将不能访问数据库

325、无论是哪一种 Web 服务器，都会受到 HTTP 协议本身安全问题的困扰，这样的信息系统安全漏洞属于（C）。

A、设计型漏洞　　B、开发型漏洞　　C、运行型漏洞　　D、以上都不是

326、SSL 加密的过程包括以下步骤：（1）通过验证以后，所有数据通过密钥进行加密，使用 DEC 和 RC4 加密进行加密；（2）随后客户端随机生成一个对称密钥；（3）信息通过 HASH 加密，或者一次性加密（MD5SHA）进行完整性确认；（4）客户端和服务器协商建立加密通道的特定算法。正确的顺序的是（D）

A、（4）（3）（1）（2）　　B、（4）（1）（3）（2）

C、（4）（2）（3）（1）　　D、（4）（2）（3）（1）

327、影响 WEB 系统安全的因素，不包括？（C）

A、复杂应用系统代码量大、开发人员多、难免出现疏忽

B、系统屡次升级、人员频繁变更，导致代码不一致

C、历史遗留系统、试运行系统等对个 WEB 系统运行于不同的服务器上

D、开发人员未经安全编码培训

328、Oracle 通过修改用户密码策略可提高密码强度，以下哪个密码策略参数中文描述是错误的？（A）

A、PASSWORD_MAX　　登录超过有效次数锁定时间

B、FAILED_LOGIN_ATTEMPTS　　最大错误登录次数

C、PASSWORD_GRACE_TIME　　密码失效后锁定时间

D、PASSWORD_LIFE_TIME　　口令有效时间

329、SQL Server 服务有一个启动账号，默认账号是属于 administrators 组，现在为了安全需要创建一个新的服务启动账号，它需要哪些权限既能兼顾安全又能保证启动数据库成功，请排除一个错误的。（D）

A、数据库本地目录的读写权限　　B、启动本地服务的权限

C、读取注册表的权限　　D、通过 API 访问 Windows Resource

330、作为一台运行 IIS 在 Internet 发布站点的 Windows Web 服务器，下面哪项服务不是必需的？（B）

A、IIS Admin　　B、Net Logon

C、Performance Logs and Alerts　　D、World Wide Web Publishing

331、数据库中超级账户不能被锁定，其中 Oracle 的是（），mysql 的是（），SQLServer 的是（C）。

A、sa，root，sys　　B、admin，root，sa

C、sys，root，sa　　D、sys，admin，sa

332，Oracle 的安全机制，是由（A）、实体权限和角色权限这三级体系结构组成的。

A、系统权限　　B、索引权限　　C、操作权限　　D、命令控制

333、对 SQL 数据库来说，以下哪个用户输入符号对系统的安全威胁最大， 需要在数据输入时进行数据过滤？（B）

A、--　　B、-　　C、-=　　D、-+

334、在 Web 页面中增加验证码功能后，下面说法正确的是（A）。

A、可以增加账号破解等自动化软件的攻击难度　　B、可以防止文件包含漏洞

C、可以防止缓冲溢出　　D、可以防止 浏览

335、以下破解 Oracle 密码哈希值的步聚，其中哪个描述是错误的？（B）

A、用 Sqlplus 直接登录到 Oracle 数据库，使用 select username，password form dba_users 命令查看数据库中的用户名和密码，此时看到的密码是哈希值

B、在 Cain 的 Cracker 菜单点击导入用户名和哈希值，可直接显示用户密码明文

C、在 Cain 的 Cracker 菜单点解导入用户名和哈希值，只能通过字典破解

D、在 Cain 的 Rainbow 生成的表会占用大量的硬盘空间和内存，可是破解速度和效率很高

336、在数据库向因特网开放前，哪个步聚是可以忽略的？（B）

A、安全安装和配置操作系统和数据库系统

B、应用系统应该在内网试运行 3 个月

C、对应用软件如 Web 也没、ASP 脚本等进行安全性检查

D、网络安全策略已经生效

337、如果不设置必要的日志审核，就无法追踪回朔安全事件，检查是否启用通用查询日志，打开/etcmy.cnf 文件，查看是否包含如下设置，选出一个正确的（D）。

A、audit=filename　　B、sys=filename　　C、event=filename　　D、log=filename

338、针对一台对外提供 Web 服务的 Windows 服务器，下列关于账户权限控制，哪些项是不合理的？（C）

A、限制匿名账户对 Web 内容的目录写权限

B、从 Everyone 组中删除“从网络访问此计算机”用户权限

C、禁用 IUSR-MACHE 和 IWAN_MACHINE 账户

D、本地登录时必须使用 Administrators 账户

339、网上营业中间件如果启用了 SSl，应采用不低于（C）版本的 SSL，采用经国家密码管理局认可的密码算法。

A、2.0　　B、2.5　　C、3.0　　D、3.1

340、SQL　Server 默认的具有 DBA 权限的账号是什么？（C）

A、root　　B、admin　　C、sa　　D、system

341、（A）是指电子系统或设备在自己正常工作产生的电磁环境下，电子系统或设备之间的相互之间的相互不影响的电磁特性。

A、电磁兼容性　　B、传导干扰　　C、电磁干扰　　D、辐射干扰

342、（C）是指一切与有用信号无关的、不希望有的或对电器及电子设备产生不良影响的电磁发射。

A、电磁兼容性　　B、传导干扰　　C、电磁干扰　　D、辐射干扰

343、《计算机信息系统雷电电磁脉冲安全防护规范》的标准编号是（B）。

A、GA 163-1997　　B、GA 267-2000

C、GA 243-2000　　D、GB 17859-1999

344、安装了合格防雷保安器的计算机信息系统，还必须在（C）雷雨季节前对防雷保安器、保护接地装置进行一次年度检查，发现不合格时，应及时修复或更换。

A、第三年　　B、第二年　　C、每年　　D、当年

345、使用 IIalon 灭火的工作原理是什么？（C）

A、降低温度　　B、隔绝氧气和可燃物

C、破坏氧气和可燃物之间的化学反应　　D、减少氧气

346、白炽灯、高压汞灯与可燃物、可燃结构之间的距离不应小于（C）cm。

A、30　　B、40　　C、50　　D、60

347、被电击的人能否获救，关键在于（D）。

A、触电的方式　　B、人体电阻的大小

C、触电电压的高底　　D、能否尽快脱离电源和施行紧急救护

348、布置电子信息系统信号线缆的路由走向时，以下做法错误的是（A）。

A、可以随意弯折　　B、转弯是，弯曲半径应大于导线直径的 10 倍

C、尽量直线、平整　　D、尽量减小由线缆自身形成的感应环路面积

349、采取适当的措施，使燃烧因缺乏或隔绝氧气而熄灭，这种方法称作（A）。

A、窒息灭火法　　B、隔离灭火法　　C、冷却灭火法

350、长期在高频电磁场作用下，操作者会有什么不良反应？（B）

A、呼吸困难　　B、神经失常　　C、疲劳无力

351、触电事故中，绝大部分是由于（A）导致人身伤亡的。

A、人体接受电流遭到电击　　B、烧伤　　C、触电休克

352、从业人员发现直接危及人身安全的紧急情况时，例如气体灭火系统开始开启时，应（A）。

A、停止作业，立即撤离危险现场　　B、继续作业

C、向上级汇报，等待上级指令

353、从业人员既是安全生产的保护对象，又是实现安全生产的（C）。

A、关键　　B、保证　　C、基本要素

354、低压验电笔一般适用于交、直流电压未（C）伏以下。

A、220　　B、380　　C、500

355、电流为（B）毫安是，称为致命电流。

A、50　　B、100　　C、120　　D、150

356、电器的保险丝只能装在（B）上。

A、零线　　B、火线　　C、底线

357、电器着火是不能用（C）灭火。

A、四氧化碳或 1211 灭火　　B、沙土　　C、水

358、对不符合防雷标准、规范防雷工程专业设计方案，以下（B）应当按照审核结论进行修改并重新报批。

A、建设单位　　B、防雷工程专业设计单位　　C、工程施工单位

359、发现人员触电时，应（B），使之脱离电源。

A、立即用手拉开触电人员　　B、用绝缘物体拨开电源或触电者

C、用铁棍拨开电源线

360、凡设在年平均雷电日大于（C）的地区的计算机信息系统，原则上均应装设计算机信息系统防雷保安器，以防止雷电电磁脉冲过电压和过电流侵入计算机信息系统设备。

A、40　　B、45　　C、5　　D、15

361、废电池随处丢弃会造成（B）的污染。

A、白色污染　　B、重金属污染　　C、酸雨

362、干粉灭火器多长时间检查一次？（A）

A、半年　　B、一年　　C、三个月　　D、两年

363、根据国家相关规定，电压（D）以下不必考虑防止电击的安全？

A、48 伏　　B、36 伏　　C、65 伏　　D、25 伏

364、根据作业环境的不同，安全帽的颜色也不同，如在爆炸性作业场所工作宜戴（A）安全帽。

A、红色　　B、黄色　　C、白色

365、关于空气的正向压力，下面哪项描述是正确的？（B）

A、当门打开时，空气向内流动　　B、当门打开，空气向外流动

C、当发生火灾，系统自动切断电源　　D、当发生火灾，烟雾向另外一间房间流动

366、国家颁布的《安全色》标准中，表示警告、主要的颜色为（C）。

A、红色　　B、蓝色　　C、黄色

367、火灾中对人员威胁最大的是（B）。

A、火　　B、烟气　　C、可燃物

368、机房内电源馈线不得与计算机信号传输线靠近或并排敷设。空间不允许时，两者间距应不少于（B）m。

A、0.1　　B、0.6　　C、1.2　　D、0.3

369、计算机电源系统的所有节点均应镀铅锡处理（B）连接。

A、热压　　B、冷压　　C、焊锡　　D、直接

370、计算机系统接地应采用（A）。

A、专用底线　　B、和大楼的钢筋专用网相连

C、大楼的各种金属管道相连　　D、没必要

371、采取适当的措施，使燃烧因缺乏或隔绝氧气而熄灭，这种方法称作（A）。

A、窒息灭火法　　B、隔离灭火法　　C、冷却灭火法

372、计算机系统应选用（A）电缆。

A、铜芯　　B、铅芯

C、铁芯　　D、没有要求

373、进行腐蚀品的装卸作业应戴（B）手套。

A、帆布　　B、橡胶　　C、棉布

374、人体在电磁场作用下，由于（C）将使人体受到不同程度的伤害。

A、电流　　B、电压　　C、棉布

375、身上着火后，下列哪种灭火方法是错误的（C）。

A、就地打滚　　B、用厚重衣物覆盖压灭火苗　　C、迎风快跑

376、生产经营单位必须为从业人员提供符合国家标准或（C）标准的劳动防护用品。

A、当地　　B、本单位　　C、行业

377、使用新设备，必须了解、掌握其安全技术特征，采取有效的安全防护措施，并对从业人员进行专门的安全生产。（B）

A、当地　　B、本单位　　C、行业

378.实验地点相对湿度大于 75%时，则此实验环境属于易触电的环境：（A）

A、危险　　B、特别危险　　C、一般

379、通过人身的安全交流电流规定在(A)以下。

A、10mA　　B、30mA　　C、50mA

380、下列不属于对物理层信息窃取的是(D)

A、对存储介质的盗取　　B、对监视器的窃听

C、对网络线路的窃听　　D、对设备屏蔽电磁干扰

381、新、改、扩建项目的安全设施投资应当纳入(C)。

A、企业成本　　B、安措经费　　C、建设项目概算

382、液体表面的蒸汽与空气形成可燃气体，遇到点火源时，发生一闪即灭的现象称为(C)

A、爆炸　　B、蒸发　　C、闪燃

383、防雷保安器：防止(B)破坏计算机信息系统的保安装置，可分为两大类：电源线防雷保安器（简称电源防雷保安器）和信号传输线防雷保安器（简称通道防雷保安器）。

A、直击雷　　B、感应雷　　C、雷暴　　D、雷电电磁脉冲

384、EMC 标准是为了保证(D)正常工作而制走的。

A、网络　　B、媒体　　C、信息　　D、系统和设备

385、以下不符合防静电要求的是(B)。

A、穿合适的防静电衣服和防静电鞋　　B、在机房内直接更衣梳理

C、用表面光滑平整的办公家具　　D、经常用湿拖布拖地

386、以下哪些属于系统的物理故障？(A)

A、硬件故障与软件故障　　B、计算机病毒

C、人为的失误　　D、网络故障和设备环境故障

387、用灭火器灭火时，灭火器的喷射口应该对准火焰的(C)。

A、上部　　B、中部　　C、根部

388、运输、携带、邮寄计算机信息媒体进出靖的，应当如实向(A)申报。

A、海关　　B、工商

C、税务　　D、边防

389、在计算机机房或其他数据处理环境中，较高的潮湿环境会带来如下哪些弊端？ (B)

A、产生静电　　B、计算机部件腐蚀

C、有污染物　　D、B+A

390、在空气不流通的狭小地方使用二氧化碳灭火器可能造成的危险是(B)。

A 中毒　　B 缺氧　　C 爆炸

391、在雷雨天不要走近高压电杆、铁塔、避雷针、远离至少(C)米以外。

A、IO 米　　B、15 米　　C、20 米

392、在易燃易爆场所穿(C)最危险。

A、布鞋　　B、胶鞋　　C、带钉鞋

393、在遇到高压电线断落地面时，导线断落点(B)m 内，禁止人员进入。

A、IO　　B、20　　C、30

394、数据处理中心的物理环境中，最佳湿度应该保持在什么样的程度？(C)

A、30%-40%　　B、40%-50%　　C、45%-60%　　D、50%-70%

395、计算机信息系统防护，简单概括起来就是：均压、分流、屏蔽和良好接地。所

以防雷保安器必须有合理的(B)。

A、屏蔽配置　　B、接地配置

C、分流配置　　D、均压配置

396、计算站场地宜采用(A)蓄电池。

A、封闭式　　B、半封闭式

C、开启式　　D、普通任意的

397、多层的楼房中，最适合做数据中心的位置是(D)。

A、楼　　B、地下室

C、顶楼　　D、除以上外的任何楼层

398、计算机机房是安装计算机信息系统主体的关键场所，是(A)工作的重点，所以对计算机机房要加强安全管理。

A、实体安全保护　　B、人员管理

C、媒体安全保护　　D、设备安全保护

399、区域安全，首先应考虑（B），用来识别来访问的用户的身份，并对其合法性进行验证，主要通过特殊标示符、口令、指纹等来实现。

A、来访者所持物　　B、物理访问控制　　C、来访者所具有的特征　　D、来访者所知信息

400、在计算机房出入口处或值班室，应设置（D）和应急断电装置。

A、 电视　　B、电扇　　C、报警器　　D、应急电话

401、下列（A）灭火器是扑救精密仪器火灾的最佳选择。

A、二氧化碳灭火剂　　B、干粉灭火剂　　C、泡沫灭火剂

402、电气安全主要包括人身安全、（B）安全。

A、照明　　B、设备　　C、电器　　D、空调

403、（C）基于 IDEA 算法。

A、S/MIME　　B、SET　　C、PGP　　D、SSL

404、(C）类型的加密，使得不同的文档和信息进行运算以后得到一个唯一的 128 位编码。

A、对称加密　　B、非对称加密　　C、哈希加密　　D、强壮加密

405、(C)是通过使用公开密钥技术和数字证书等来提供网络信息安全服务的基础平台。

A、公开密钥体制　　B、对称加密体制　　C、PKI（公开密钥基础设施）　　D、数字

签名

406、(D)是由权威机构CA发行的一种权威性的电子文档，是网络环境中的一种身份证。

A、认证机构　　B、密码　　C、票据　　D、数字证书

407、（D）协议主要用于加密机制。

A、HTTP　　B、FTP　　C、TELNET　　D、SSL

408、（A）原则保证只有发送方与接收方能访问消息内容。

A、保密性　　B、鉴别　　C、完整性　　D、访问控制

409、（D）原则允许某些用户进行特定访问。

A、保密性　　B、鉴别　　C、完整性　　D、访问控制

410、（B）增加明文冗余度。

A、混淆　　B、扩散　　C、混淆与扩散　　D、都不是

411、3DES 加密算法的密钥长度是：（A）。

A、168　　B、128　　C、56　　D、256

412、AES 密钥长度不能是（D）。

A、128 位　　B、192 位　　C、256 位　　D、512 位

413、AES 算法是哪种算法？（A）。

A、对称密钥加密　　B、非对称密钥加密　　C、哈希算法　　D、流加密

414、AES 属于哪种加密方式？（B）。

A、流加密　　B、分组加密　　C、异或加密　　D、认证加密

415、CA 指的是（A）。

A、证书授权　　B、加密认证　　C、虚拟专用网　　D、安全套接层

416、DES 经过（A）轮运算后，左右两部分合在一起经过一个末置换，输出一个 64 位的密文。（A）

A、16　　B、8　　C、32　　D、4

417、DES 算法是哪种算法？（A）

A、对称密钥加密　　B、非对称密钥加密　　C、哈希算法　　D、流加密

418、DES 属于哪种加密方式？（B）

A、流加密　　B、块加密　　C、异或加密　　D、认证加密

419、DNSSec 中并未采用（C）。

A、数字签名技术　　B、公钥加密技术　　C、地址绑定技术　　D、报文摘要技术

420、ECB 指的是（D）。

A、密文链接模式　　B、密文反馈模式　　C、输出反馈模式　　D、电码本模式

421、EC-DSA 复杂性的程度是（D）。

A、简单　　B、最简单　　C、困难　　D、最困难

422、EFS 可以用在什么文件系统下（C）。

A、FAT16　　B、FAT32　　C、NTFS　　D、以上都可以

423、IDEA 的密钥长度是多少 bit？（D）。

A、56　　B、64　　C、96　　D、128

424、Kerberos 是 80 年代中期，麻省理工学院为 Athena 项目开发的一个认证服务系统，其目标是把认证、记账和（B）的功能扩展到网络环境。

A、访问控制　　B、审计　　C、授权　　D、监控

425、Kerberos 是为 TCP/IP 网络设计的基于（B）的可信第三方鉴别协议，负责在网络上进行仲裁及会话密钥的分配。

A、非对称密钥体系　　B、对称密钥体系　　C、公钥体系　　D、私钥体系

426、Kerberos 是一种网络认证协议。它采用的加密算法是（C）。

A、RSA　　B、PGP　　C、DES　　D、MD5

427、Kerberos 算法是一个（B）。

A、面向访问的保护系统　　B、面向票据的保护系统

C、面向列表的保护系统　　D、面向门与锁的保护系统

428、Kerberos 提供的最重要的安全服务是？（A）。

A、鉴别　　B、机密性　　C、完整性　　D、可用性

429、MD5 产生的散列值是多少位？（C）。

A、56　　B、64　　C、128　　D、160

430、MD5 是按每组 512 位为一组来处理输入的信息，经过一系列变换后，生成一个（B）为散列值。

A、64　　B、128　　C、256　　D、512

431、MD5 是以 512 位分组来处理输入的信息，每一分组又被划分为（A）32 位子分组。

A、16 个　　B、32 个　　C、64 个　　D、128 个

432、MD5 算法将输入信息 M 按顺序每组（D）长度分组，即：M1，M2，...，Mn-1，Mn。

A、64 位　　B、128 位　　C、256 位　　D、512 位

433、PKI（公共密钥基础结构）中应用的加密方式为（B）。

A、对称加密　　B、非对称加密　　C、HASH 加密　　D、单向加密

434、PKI 的全称是（D）。

A、Private Key Intrusion　　B、Public Key Intrusion

C、Private Key Infrastructure　　D、Public Key Infrastructure

435、PKI 无法实现（D）。

A、身份认证　　B、数据的完整性　　C、数据的机密性　　D、权限分配

436、RC4 是由 RIVEST 在 1987 年开发的一种流式的密文，就是实时地把信息加密成一个整体，它在美国一般密钥长度是 128 位，因为受到美国出口法的限制，向外出口时限制到多少位？（C）。

A、64 位　　B、56 位　　C、40 位　　D、32 位

437、RSA 公钥加密系统中，他想给她发送一份邮件，并让她知道是他发出，应选用的加密秘钥是（C）。

A、他的公钥　　B、她的公钥　　C、他的私钥　　D、她的私钥

438、RSA 使用不方便的最大问题是（A）。

A、产生密钥需要强大的计算能力　　B、算法中需要大数

C、算法中需要素数　　D、被攻击过很多次

439、RSA 算法建立的理论基础是（C）。

A、DES　　B、替代想组合　　C、大数分解和素数检测　　D、哈希函数

440、SHA-1 产生的散列值是多少位？（D）。

A、56　　B、64　　C、128　　D、160

441、按密钥的使用个数，密码系统可以分为（C）。

A、置换密码系统和易位密码系统　　B、分组密码系统和序列密码系统

C、对称密码系统和非对称密码系统　　D、密码系统和密码分析系统

442、充分发挥了 DES 和 RSA 两种加密体制的优点，妥善解决了密钥传送过程中的安全问题的技术是：（C）。

A、数字签名　　B、数字指纹　　C、数字信封　　D、数字时间戳

443、从技术角度上看数据安全的技术特征主要包含哪几个方面？（B）。

A、数据完整性、数据的方便性、数据的可用性　　B、数据的完整性、数据的保密性、

数据的可用性　　C、数据的稳定性、数据的保密性、数据的可用性　　D、数据的方便性、数据的稳定性、数据的完整性

444、单项散列函数的安全性来自于他的（A）。

A、单向性　　B、算法复杂性　　C、算法的保密性　　D、离散性

445、电路网关防火墙工作在 OSI 协议的哪一层？（A）。

A、传输层　　B、链路层　　C、应用层　　D、物理层

446、电子邮件的机密性与真实性是通过下列哪一项实现的？（A）

A、用发送者的私钥对消息进行签名，用接受者的公钥对消息进行加密

B、用发送者的公钥对消息进行签名，用接受者的私钥对消息进行加密

C、用接受者的私钥对消息进行签名，用发送者的公钥对消息进行加密

D、用接受者的公钥对消息进行签名，用发送者的私钥对消息进行加密

447、端对端加密只需要保证消息都在哪里进行加密？（A）

A、源点和目的地节点　　B、经过的每一个节点

C、源点和中间经过的每一个节点　　D、所有节点

448、对明文字母重新排列，并不隐藏他们的加密方法属于（C）。

A、置换密码　　B、分组密码　　C、易位密码　　D、序列密码

449、对网络中两个相邻节点之间传输的数据进行加密保护的是（A）。

A、节点加密　　B、链路加密　　C、端到端加密　　D、DES 加密

450、发送消息和用发送方私钥加密哈希加密信息将确保消息的：（A）。

A、真实性和完整性　　B、真实性和隐私　　C、隐私和不可否认性　　D。隐私和不可否性

451、高级加密标准 AES 算法中，加密回合数不可能是（D）。

A、10　　B、12　　C、14　　D、16

452、公钥机制利用一对互相匹配的（B）进行加密，解密。

A、私钥　　B、密钥　　C、数字签名　　D、数字证书

453、公钥加密体制中，没有公开的是（A）。

A、明文　　B、密文　　C、公钥　　D、算法

454、公钥证书提供了一种系统的、可扩展的、统一的（A）。

A、公钥分发方案　　B、实现不可否认方案

C、对称密钥分发方案　　D、保证数据完整性方案

455、关于 CA 和数字证书的关系，以下说法不正确的是（B）。

A、数字证书是保证双方之间的通讯安全的垫子信任关系，它由 CA 签发

B、数字证书一般依靠 CA 中心的对称密钥机制来实现

C、在电子交易中，数字证书可以用于表明参与方的身份

D、数字证书能以一种不能被假冒的方式证明证书持有人身份

456、关于数字签名说法正确的是（A）。

A、数字签名的加密方法以目前的计算机的运算能力来破解是不现实的

B、采用数字签名，不能够保证信息自签发后到收到为止没有做过任何修改（能保证信息收到后没做个任何修改）

C、采用数字签名，能够保证信息是有签名者自己签名发送的，但由于不是真实的签名，签名者容易否认（签名不容易否认）

D、用户可以采用公钥对信息加以处理，形成数字签名（需使用私钥对信息加以处理）

457、基于私有密钥体制的信息认证方法采用的算法是（D）。

A、素数检测　　B、非对称算法　　C、RSA 算法　　D、对称加密算法

458、加密技术不能实现（D）。

A、数据信息的完整性　　B、基于密码技术的身份认证　　C、机密文件加密　　D 基于 IP 头信息的包过滤

459、加密技术不能提供以下哪种安全服务？（D）。

A、鉴别　　B、机密性　　C、完整性　　D 可用性

460、加密有对称密钥加密、非对称密钥加密两种，数字签名采用的是（B）。

A、对称密钥加密　　B、非对称密钥加密　　C、　　D

461、假设使用一种加密算法，它的加密方法很简单：将每一个字母加 5，即 a 加密成 f。这种算法的密钥就是 5，那么它属于（A）。

A、对称加密技术　　B、分组加密技术　　C、公钥加密技术　　D、单项函数密码技术

462、就是通过使用公开密钥技术和数字证书等来提供网络信息安全服务的基础平台。（C）

A、公开密钥体制　　B、对称加密体制　　C、PKI（公开密钥基础设施）　　D、数字签名

463、利用非对称密钥体制实现加密通信时，若 A 要向 B 发送加密信息，则该加密信息

应该使用（B）。

A、A 的公钥加密　B、B 的公钥加密　C、A 的私钥加密　D、B 的私钥加密

464、利用物理设备将各类型的无法预测的输入集中起来生成随机数的设备是（A）。

A、随机数生成器　B、伪随机数生成器　C、中央处理　D、非易失存储

465、链路加密要求必须先对链路两端的加密设备进行（C）。

A、异步　B、重传　C、同步　D、备份

466、密码处理依靠使用密钥，密钥是密码系统里的最重要因素。以下哪一个密钥算法在加密数据与解密时使用相同的密钥？（C）

A、对称的公钥算法　B、非对称私钥算法　C、对称密钥算法　D、非对称密钥算法

467、密码分析的目的是什么？（A）

A、确定加密算法的强度　B、增加加密算法的代替功能

C、减少加密算法的换为功能　D、确定所使用的换位

468、请从下列各项中选出不是 HASH 函数算法的一项。（D）

A、MD5　B、SHA　C、HMAC　D、MMAC

469、如今，DES 加密算法面临的问题是（A）。

A、密钥太短，已经能被现代计算机暴力破解　B、加密算法有漏洞，在数学上已被破解　C、留有后门，可能泄露部分信息　D、算法过于陈旧，已经有更好的替代方案

470、若单项散列函数的输入串有很小的变化，则输出串（A）。

A、可能有很大的变化　B、一定有很大的变化　C、可能有很小的变化　D、一定有很小的变化

471、散列算法可以做哪些事？（C）。

A、碰撞约束　B、入侵检测　C、组合散列　D、随机数生成器

472、身份认证的主要目标包括：确保交易者是交易者本人、避免与超过权限的交易者进行交易和（B）。

A、可信性　B、访问控制　C、完整性　D、保密性

473、数字签名常用的算法有（B）。

A、DES 算法　B、RSA 算法　C、Hash 函数　D、AES 算法

474、数字签名和随机数挑战不能防范以下哪种攻击或恶意行为？（D）。

A、伪装欺骗　B、重放攻击　C、抵赖　D、DOS 攻击

475、数字签名可以解决（D）。

A、数据被泄露　　B、数据被篡改　　C、未经授权擅自访问　　D、冒名发送数据或发送后抵赖

476、数字签名通常使用（B）方式。

A、公钥密码体系中的私钥　　B、公钥密码系统中的私钥对数字摘要进行加密

C、密钥密码体系　　D、公钥密码体系中公钥对数字摘要进行加密

477、数字信封是用来解决（C）。

A、公钥分发问题　　B、私钥分发问题　　C、对称密钥分发问题　　D、数据完整性问题

478、数字证书不包括（B）。

A、签名算法　　B、证书拥有者的信用等级（信用等级并非由数字证书决定）

C、数字证书的序列号　　D、颁发数字证书单位的数字签名

479、数字证书的应用阶段不包括（D）。

A、证书检索　B、证书验证　　C、密钥恢复　　D、证书撤销

480、下列说法中错误的是（D）。

A、非对称算法也叫公开密钥算法　　B、非对称算法的加密密钥和解密密钥是分离的C、非对称算法不需要对密钥通信进行保密　　D、非对称算法典型的有 RSA 算法、AES 算法等

481、下列算法中，哪种不是对称加密算法？（C）

A、AES　　B、DES　　C、RSA　　D、RC5

482、下列算法中属于 Hash 算法的是（C）。

A、DES　　B、IDEA　　C、SHA　　D、RSA

483、以下对于链路加密哪项是正确的？（B）

A、消息只在源点加密，目的节点解密　　B、消息在源点加密，在每一个经过的节点解密并加密　　C、消息在所有经过的节点中都是加密的，但只在目的节点解密　　D、消息以明文形式在节点之间传输

484、以下各种加密算法中属于单钥制加密算法的是（A）。

A、DES 加密算法　　B、Caesar 替代法　　C、Vigenere 算法　　D、Diffie-Hellman 加密算法

485、以下各种加密算法中属于双钥制加密算法的是（D）。

A、DES 加密算法　　B、Caesar 替代法　　C、Vigenere 算法　　D、Diffie-Hellman 加密 486、以下各种算法中属于古典加密算法的是（B）。

A、DES 加密算法　　B、Caesar 替代法　　C、Vigenere 算法　　D、Diffie-Hellman 加密 487、以下关于 CA 认证中心说法正确的是（C）。

A、CA 认证时使用对称密钥机制的认证方法　　B、CA 认证中心支负责签名，不负责证书的产生　　C、CA 认证中心负责证书的颁发和管理、并依靠证书证明一个用户的身份　　D、CA 认证中心不用保持中立，可以随便找一个用户来作为 CA 认证中心

488、以下关于 VPN 说法正确的是（B）。

A、VPN 指的是用户自己租用线路，和公共网络物理上完全隔离的、安全的线路

B、VPN 指的是用户通过公用网络建立的临时的、逻辑隔离的、安全的连接

C、VPN 不能做到信息认证和身份认证　　D、VPN 只能提供身份认证、不能提供加密数据的功能

489、以下关于数字签名说法正确的是（D）。

A、数字签名是在所传输的数据后附上一段和传输数据毫无关系的数字信息

B、数字签名能够解决数据的加密传输，即安全传输问题

C、数字签名一般采用对称加密机制　　D、数字签名能够解决篡改、伪造等安全性问题

490、以下密码使用方法中正确的是（D）。

A、将密码记录在日记本上以避免忘记　　B、任何情况下均不得使用临时性密码

C、密码中的字母不得重复　　D、不要使用全部由字母组成的密码

491、以下哪个不包含在证书中？（C）

A、密钥采取的算法　　B、公钥及其参数　　C、私钥及其参数　　D、签发证书的 CA 名称

492、以下哪个选项不会破坏数据库的完整性？（A）

A、对数据库中的数据执行删除操作　　B、用户操作过程中出错

C、操作系统的应用程序错误　　D、DBMS 或操作系统程序出错

493、以下哪项不属于数据库系统实体安全？（B）

A、环境安全　　B、线路安全　　C、设备安全　　D、媒体安全

494、以下哪一种算法产生最长的密钥？（D）

A、Diffe-Hellman　　B、DES　　C、IDEA　　D、RSA

495、以下认证方式中，最为安全的是（D）。

A、用户名+密码　　B、卡+密码　　C、用户名+密码+验证码　　D、卡+指纹

496、远程访问控制机制是基于一次性口令（one-time password），这种认证方式采用下面哪种认证技术？（B）

A、知道什么　　B、拥有什么　　C、是谁　　D、双因素认证

497、在 3DES 算法中，密钥最高可达到多少位？（C）

A、96　　B、128　　C、168　　D、200

498、在 IPSec 中，（C）是两个通信实体经过协调建立起来的一种协定，觉得用来保护数据包安全的 IPSec 协议、密码算法、密钥等信息。

A、ESP　　B、SPI　　C、SA　　D、SP

499、在 IPSec 中，IKE 提供（B）方法供两台计算机建立。

A、解释域　　B、安全关联　　C、安全关系　　D、选择关系

500、在 RIP 的 MD5 认证报文中，经过加密的密钥是放在哪里的？（B）

A、保温的第一个表项里　　B、报文的最后一个表项里

C、报文的第二个表项里　　D、报文头里

501、在非对称加密算法中，涉及到的密钥个数是？（B）

A、一个　　B、两个　　C、三个　　D、三个以上

502、在高级加密标准 AES 算法中，区块大小为（A）。

A、128 位　　B、192 位　　C、256 位　　D、512 位

503、在给定的密钥体制中，密钥与密码算法可以看成是（A）。

A、前者是可变的，后者是固定的　　B、前者是固定的，后者是可变的

C、两者都是可变的　　D、两者都是固定的

504、在公钥体制中，不公开的是（B）。

A、公钥　　B、私钥　　C、公钥和私钥　　D、私钥和加密算法

505、在密码学中，需要被交换的原消息被称为什么？（D）

A、密文　　B、算法　　C、密码　　D、明文

506、一般证书采用哪个标准？（D）

A、ISO/IEC 15408　　B、ISO/IEC 17799　　C、BS　7799　　D、X. 509V3

507、一个电子邮件的发送者对数据摘要应用了数字签名。这能确保：（D）

A、信息的数据和时间戳　　B、识别发信的计算机

C、对信息内容进行加密　　D、对发送者的身份进行识别

508、在数据库中，下列哪些数据不能加密？（A）

A、索引字段　　B、存放日期字段

C、存放密码的　　D、存放名称字段

509、在一个网络节点中，链路加密仅在以下哪项中提供安全性？（D）

A、数据链路层　　B、物理层

C、通信层　　D、通信链路

510、在以下隧道协议中，属于三层隧道协议的是（D）。

A、L2F　　B、PPTP　　C、L2TP　　D、IPSec

511、以下哪一项是基于一个大的整数很难分解成两个素数因数？（B）

A、ECC　　B、RSA　　C、DES　　D、D-H

512、以下哪种数据加密技术可以在基础架构层面进行？（A）

A、IPSec　　B、Secure Sockets Layer

C、Transport Layer Securit　　D、RSA

513、目前最安全的身份认证机制是（A）。

A、一次口令机制　　B、双因素法

C、基于智能卡的用户身价认证　　D、身价认证的单因素法

514、当数据库由于各种原因而使其完整性遭到破坏时，必须采取以下哪项措施来恢复数据库？（C）

A、重新安装数据库　　B、换一种数据库

C、使用数据库备份　　D、将数据库中的数据利用工具导出，并保存

515、PGP 加密算法是混合使用（B）算法和 IDEA 算法，它能够提供数据加密和数字签名服务，主要用于邮件加密软件。

A、DES　　B、RSA　　C、IDEA　　D、AES

516、以下哪些软件是用于加密的软件？（A）

A、PGP　　B、SHA　　C、EFS　　D、DES

517、如果消息接受方要确定发送方身价，则要使用（B）原则。

A、保密性　　B、鉴别　　C、完整性　　D、访问控制

518、对于现代密码破解，（D）是最常的方法。

A、攻破算法　　B、监听截获　　C、信息猜测　　D、暴力破解

519、非对称密码技术的缺点有哪些？（B）

A、密钥持有量减少　　B、加/解密速度慢　　C、耗用资源较少　　D、以上都是

520、CA 不能提供下列哪种证书？（D）

A、个人数字证书　　B、SSL 服务器证书

C、安全电子邮件证书　　D、SET 服务器证书

521、以下关于混合加密方式说法正确的是（B）。

A、采用公开密钥体制进行通信过程中的加解密处理

B、采用公开密钥体制对对称密钥体制的密钥进行加密后的通信

C、采用对称密钥体制对对称密钥体制的密钥进行加密后的通信

D、采用混合加密方式，利用了对称密钥体制的密钥容易管理和非对称密钥体制的加解密

处理速度快的双重优点

522.、果要保证（C）原则，则不能在中途修改消息内容。

A、保密性　　B、鉴别　　C、完整性　　D、访问控制

523、口令是验证用户身份的最常用手段，以下哪一种口令的潜在风险影响范围最大？（D）

A、长期没有修改的口令　　B、过短的口令

C、两个人共用的口令　　D、设备供应商提供的默认的口令

524.非对称密钥的密码技术具有很多优点，其中不包括：（B）。

A、可提供数字签名、零知识证明等额外服务

B、加密/解密速度快，不需占用较多资源

C、通信双方事先不需要通过保密信道交换密钥

D、密钥持有量大大减少

525．DES 是一种 block（块）密文的加密算法，是把数据加密成多大的块？（B）

A、32 位　　B、64 位　　C、128 位　　D、256 位

526．CA 数字证书中不包含的信息有（C）。

A、CA 的数字签名　　B、证书申请者的个人信息

C、证书申请者的私钥　　D、证书申请者的公钥信息

527．以下关于对称密钥加密说法正确的是（C）。

A、加密方和解密可以使用不同的算法　　B、加密密钥和解密密钥可以是不同的

C、加密密钥和解密密钥必须是相同的　　D、密钥的管理非常简单

528、在为计算机设置使用密码时，下面（D）密码是最安全的。

A、12345678　　B、66666666

C、20061001　　D、72aB@#41

529、（C）的攻击者发生在 Web 应用层？

A、25%　　B、50%

C、75%　　D、90%

530、“U 盘破坏者”病毒（Worm.vhy）采用（B）图标，很容易被用户误点击，点击后就会在后台破坏硬盘数据，致使中毒电脑重新启动的时候完全崩溃。

A、网上邻居　　B、我的电脑

C、我的文档　　D、收藏夹

531、“冲击波”病毒运行时会将自身复制到 Windows 目录下，并命名为（C）

A、Gsrss.exe　　B、msbast.exe

C、msblast.exe　　D、lsass.exe

532、Code Red 爆发于 2001 年 7 月，利用微软的 IIS 漏洞在 Web 服务器之间传播。针对这一漏洞，微软早在 2001 年三月就发布了相关的补丁。如果今天服务器仍然感染 Code Red，那么属于哪个阶段的问题？（A）

A、系统管理员维护阶段的失误　　B、微软公司软件的设计阶段的失误

C、最终用户使用阶段的失误　　D、微软公司软件的实现阶段的失误

533、病毒的传播机制主要有哪些？（D）

A、移动存储　　B、电子邮件　　C、网络共享　　D、以上均是

534、病毒的反静态反汇编技术都有（D）。

A、数据压缩　　B、数据加密　　C、感染代码　　D、以上均是

535、病毒在感染计算机系统时，一般（B）感染系统的。

A、病毒程序都会在屏幕上提示，待操作者确认（允许）后

B、实在操作者不觉察的情况下

C、病毒程序会要求操作者制定存储的磁盘和文件夹后

D、在操作者为病毒制定存储的文件名以后

536、杀毒软件时提示“重新启动计算机后删除文件”其主要原因是（A）

A、文件插入了系统关键进程，杀毒时无法处理

B、文件是病毒文件，无法处理

C、由于病毒的加壳形式不同，杀毒时无法正确处理

D、文件正在运行且无法安全的结束，需要其他处理方法

537、蠕虫的目标选择算法有（D）。

A、随机性扫描　　B、基于目标列表的扫描

C、顺序扫描　　D、以上均是

538、网络钓鱼是指（A）

A、通过大量发送声来自于银行或其他知名机构的欺骗性垃圾邮件，意图引诱收信人给出敏感信息。

B、网上进行钓鱼活动

C、通过网络组织钓鱼活动，从而获得利益　　D、以上都不是

539、不属于常见把入侵主机的信息发送给攻击者的方法是（D）。

A、E-MAIL　　B、UDP　　C、ICMP　　D、连接入侵主机

540、不属于黑客被动攻击的是（A）

A、缓冲区溢出　　B、运行恶意软件　　C、浏览恶意代码网页　　D、打开病毒附件

541、不属于黑客前期收集信息的工具是（D）

A、Nmap　　B、Xscan　　C、Nslookup　　D、LC

542、常见 Web 攻击方法，不包括？（D）

A、利用服务器配置漏洞　　B、恶意代码上传下载

C、构造恶意输入（SQL 注入攻击、命令注入攻击、跨站脚本攻击）

D、业务测试

543、常用的抓包软件有（A）。

A、ethereal　　B、MS office　　C、fluxay　　D、netscan

544.网络窃听（Sniffer）可以捕获网络中流过的敏感信息，下列说法错误的是（A）

A、密码加密后，不会被窃听　　B、Cookie 字段可以被窃听

C、报文和帧可以窃听　　D、高级窃听者还可以进行 ARPSpoof，中间人攻击

545、除了在代码设计开发阶段预防 SQL 注入外，对数据库进行加固也能够把攻击者所能造成的损失控制在一定范围内，下列哪项不是数据库加固范围？（C）

A、禁止将任何高权限账号（例如 sa,dba 等等）用于应用程序数据库访问。更安全的方法是单独为应用创建有限访问账户

B、拒绝用户访问敏感的系统存储过程

C、禁止用户访问的数据库表　　D、限制用户所能够访问的数据库表

546、防止用户被冒名所欺骗的方法是（A）。

A、对信息源发放进行身份验证　　B、进行数据加密

C、对访问网络的流量进行过滤和保护　　D、采用防火墙

547、给电脑设置多道口令，其中进入电脑的第一道口令是（B）。

A、系统口令　　B、CMOS 口令

C、文件夹口令　　D、文档密码

548、攻击者截获并记录了从 A 到 B 的数据，然后又从早些时候所截获的数据中提取出信息重新发往 B 称为（D）。

A、中间人攻击　　B、口令猜测器和字典攻击

C、强力攻击　　D、回放攻击

549、故意制作、传播计算机病毒，造成计算机信息系统不能正常运行，但如果后果不严重就无罪，可以原谅，这种说法（C）。

A、不对，对这种蓄意破坏行为不能原谅　　B、即使不是故意的，后果也不很严重

C、对。我国实行成文法，根据《中华人民共和国刑法》第 286 条的规定，只有造成严重后果者才有罪

D、无法断定

550、关于 80 年代 Mirros 蠕虫危害的描述，哪句话是错误的？（B）

A、占用了大量的计算机处理器的时间，导致拒绝股务

B、窃取用户的机密信息，破坏计算机数据文件

C、该蠕虫利用 Unix 系统上的漏洞传播

D、大量的流量堵塞了网络，导致网络瘫痪

551、关于黑客注入攻击说法错误的是： (D)

A、它的主要原因是程序对用户的输入缺乏过滤

B、一般情况下防火墙对它无法防范

C、对它进行防范时要关注操作系统的版本和安全补丁

D、注入成功后可以获取部分权限

552、基于主机评估报告对主机进行加固时，第一步是（B）。

A、账号、口令策略修改　　B、补丁安装

C、文件系统加固　　D、日志审核增强

553、计算机病毒会对下列计算机服务造成威胁，除了（C）。

A、完整性　　B、有效性

C、保密性　　D、可用性

554、计算机病毒是一段可运行的程序，它一般（C）保存在磁盘中。

A、作为一个文件　　B、作为一段数据

C、不作为单独文件　　D、作为一段资料

555、什么方式能够从远程绕过防火墙去入侵一个网络？(D)

A、IP services_　　B、Active　ports

C、Identified network topology　　D、Modem banks

556、输入法漏洞通过（D）端口实现的。

A、21　　B、23　　C、445　　D、3389

557、特洛伊木马攻击的威胁类型属于（B）。

A、授权侵犯威胁　　B、植入威胁

C、渗入威胁　　D、旁路控制威胁

558、通常黑客扫描目标机的 445 端口是为了(B)。

A、利用 NETBIOS SMB 服务发起 DOS 攻击

B、发现并获得目标机上的文件及打印机共享

C、利用 SMB 服务确认 Windows 系统版本

D、利用 NETBIOS 服务确认 Windows 系统版本

559、网络病毒防范的三个阶段主要是预防范阶段、病毒爆发阶段和哪个阶段？(A)

A、残余风险评估阶段　　B、检查阶段

C、入侵检测系统监控阶段　　D、网络异常流量临控阶段

560、网络病毒预防范阶段的主要措施是什么？(A)

A、强制补丁、网络异常流量的发现　　B、强制补丁、入侵检测系统监控

C、网络异常流量的发现、入侵检测系统的监控阶段　　D、缺少 D 选项

561、下列除了(B)以外，都是防范计算机病毒侵害的有效方法。

A、使用防病毒软件　　B、机房保持卫生，经常进行消毒

C、避免外来的磁盘接触系统　　D、网络使用防病毒网关设备

562、下列除了(A)以外，都是计算机病毒传

A、通过操作员接触传播　　B、通过 U 盘接触传播

C、通过网络传播　　D、通过电子播的途径邮件传播

563、下列措施中，(C)不是减少病毒的传染

和造成的损失的好办法。

A、重要的文件要及时、定期备份，使备份能反映出系统的最新状态

B、外来的文件要经过病毒检测才能使用，不要使用盗版软件

C、不与外界进行任何交流，所有软件都自行开发

D、定期用抗病毒软件对系统进行查毒、杀毒

564、下列哪项是跨站脚本 Cross Site Scripting 攻击具体事例？（B）

A、搜索用户　　B、发帖子，发消息　　C、上传附件　　D、下载文件

565、下列哪项为信息泄露与错误处理不当 Information Leakage and Improper

Error Handlina 攻击具体实例？(D)

A、不明邮件中隐藏的 html 链接　　B、发帖子，发消息

C、上传附件　　D、错误信息揭示路径

566、下面哪一项是黑客用来实施 DDoS 攻击的工具？(D)

A、LC5　　B、Rootkit　　C、Icesword　　D、Trinoo

567、以下哪个工具可以抹去所有 NT/2K 配置，并将其还原到初始状态？(A)

A、Rollback. exe　　B、Recover. exe　　C、Zap. exe　　D、Reset. exe

568、以下哪个工具通常是系统自带任务管理器的替代？(D)

A、Regmon　　B、Filemon　　C、Autoruns　　D、Process explorer

569、以下哪个针对访问控制的安全措施是最容易使用和管理的？(C)

A、密码　　B、加密标志　　C、硬件加密　　D、加密数据文件

570、以下哪项不是分布式拒绝服务攻击常用的工具？(D)

A、Trinoo　　B、Trinoo　　C、TFN　　D、synkill

571、以下哪项不属于针对数据库的攻击？(D)

A、特权提升　　B、强力破解弱口令或默认的用户名及口令

C、SQL 注入　　D、利用 xss 漏洞攻击

572、以下哪项工具不适合用来做网络监听？(B)

A、sniffer　　B、Webscan　　C、 Windump　　D、 D-Iris

573、以下哪项是 SYN 变种攻击经常用到的工具？(B)

A、sessionIE　　B、synkill　　C、TFN　　D、Webscan

574、以下哪一项不是流氓软件的特征？(D)

A、通常通过诱骗或和其他软件捆绑在用户不知情的情况下安装

B、通常添加驱动保护使用户难以卸载

C、通常会启动无用的程序浪费计算机的资源

D、通常会显示下流的言论

575、一个数据仓库中发生了安全性破坏。以下哪一项有助于安全调查的进行？(B)

A、访问路径　　B、时戳　　C、数据定义　　D、数据分类

576、以下哪一项不属于恶意代码？(C)

A、病毒　　B、蠕虫　　C、宏　　D、特洛伊木马

577、以下哪一项不属于计算机病毒的防治策略？(D)

A、防毒能力　　B、查毒能力　　C、杀毒能力　　D、禁毒能力

578、以下哪一项是常见 Web 站点脆弱性扫描工具？(A)

A、Appscan　　B、Nmap　　C、Sniffer　　D、LC

579、以下哪种方法是防止便携式计算机机密信息泄露的最有效的方法？(A)

A、用所有者的公钥对硬盘进行加密处理　　B、激活引导口令（硬件设置口令）

C、利用生物识别设备　　D、利用双因子识别技术将臀陆信息写入记事本

580、以下哪种符号在 SQL 注入攻击中经常用到？(D)

A、$_　　B、1　　C、@　　D、;

581、以下哪种工具能从网络上检测出网络监听软件(A)

A、sniffdet, ,　　B、purify, ,　　C、Dsniff　　D、WireShark

582、以下哪种攻击可能导致某些系统在重组 IP 分片的过程中宕机或者重新启动？(B)

A、分布式拒绝服务攻击　　B、Ping of Death

C、NFS 攻击　　D、DNS 缓存毒化攻击

583、下面哪部分不属于入侵的过程？(B)

A、数据采集　　B、数据存储　　C、数据检测　　D、数据分析

584、以下对木马阐述不正确的是(A)。

A、木马可以自我复制和传播

B、有些木马可以查看目标主机的屏幕

C、有些木马可以对目标主机上的文件进行任意揉作

D、木马是一种恶意程序，它们在宿主机器上运行，在用户毫无察觉的情况下，让攻击者获得了远程访问和控制系统的权限。

585、由于攻击者可以借助某种手段，避开 DBMS 以及应用程序而直接进入系统访问数据，我们通常采取以下哪种方式来防范？(A)

A、数据库加密

B、修改数据库用户的密码，将之改得更为复杂

C、使用修改查询法，使用户在查询数据库时需要满足更多的条件

D、使用集合法

586、在大多数情况下，病毒侵入计算机系统以后，(D)。

A、病毒程序将立即破坏整个计算机软件系统

B、计算机系统将立即不能执行我们的各项任务

C、病毒程序将迅速损坏计算机的键盘、鼠标等操作部件

D、一般并不立即发作，等到满足某种条件的 时候，才会出来活动捣乱、破坏

587、在确定威胁的可能性时，可以不考虑以下哪项？(D)

A、威胁源　　B、潜在弱点

C、现有控制措施　　D、攻击所产生的负面影响

588、在以下人为的恶意攻击行为中，属于主动攻击的是(A)。

A、身份假冒　　B、数据 GG　　C、数据流分析　　D、非法访问

589、下面哪一种攻击方式最常用于破解口 令？(B)

A、哄骗(spoofing)　　B、字典攻击(dictionary attack)

C、拒绝服务(DoS)　　D、WinNuk

590、针对 DNS 服务器发起的查询 DoS 攻击，属于下列哪种攻击类型？(C)

A、syn flood　　B、ack flood　　C、 udpflood　　D、Connection flood

591、下列哪项不是安全编码中输入验证的控制项？(D)

A、数字型的输入必须是合法的数字

B、字符型的输入中对’进行特殊处理

C、验证所有的输入点，包括 Get，Post，Cookie 以及其他 HTTP 头

D、正确使用静态查询语句，如 PreDaredStatement

592、以下关于垃圾邮件泛滥原因的描述中，哪些是错误的？(C)

A、早期的 SMTP 协议没有发件人认证的功能

B、网络上存在大量开放式的邮件中转服务器，导致垃圾邮件的来源难于追查

C、SMTP 没有对邮件加密的功能是导致垃圾邮件泛滥的主要原因

D、Internet 分布式管理的性质，导致很难控制和管理

593、以下哪种方法是防止便携式计算机机密信息泄露的最有效方法？（A）

A、用所有者的公钥对硬盘进行加密处理　　B、激活引导口令（硬件设置口令）

C、利用生物识别设备　　D、利用双因子识别技术将登录信息写入记事本

594、以下哪种攻击属于 DDoS 类攻击？（A）

A、SYN 变种攻击　　B、smurf 攻击　　C、arp 攻击　　D、Fraggle 攻击

595、URL 访问控制不当不包括（D）

A、Web 应用对页面权限控制不严　　B、缺乏统一规范的权限控制框架

C、部分页面可以直接从 URL 中访问　　D、使用分散登录认证

596、Web 应用的认证与会话处理不当，可能被攻击者利用来伪装其他用户身份。强认证手段不包括如下哪种？（A）

A、静态密码　　B、短信挑战　　C、指纹认证　　D、图片认证

597、Web 应用漏洞按类别进行排名，由多到少正确的顺序为？（A）

A、跨站脚本、注入、恶意代码、引用不当

B、注入、跨站脚本、恶意代码、引用不当

C、恶意代码、跨站脚本、注入、引用不当

D、引用不当、跨站脚本、注入、恶意代码

598、从技术角度，以下不是漏洞来源的是（D）

A、软件或协议设计时候的瑕疵　　B、软件或协议实现中的弱点

C、软件本身的瑕疵　　D、显示卡内存容量过低

599、（C）即攻击者利用网络窃取工具经由网络传输的数据包，通过分析获得重要的信息。

A、身份假冒　　B、数据篡改　　C、信息窃取　　D、越权访问

600、有关密码学分支的定义，下列说法中错误的是（D）

A、密码学是研究信息系统安全保密的科学，由两个相互对立、相互斗争、而且又相辅相成、相互渗透的分支科学所组成的、分别称为密码编码学和密码分析学

B、密码编码学是对密码体制、密码体制的输入输出关系进行分析、以便推出机密变量、

包括明文在内的敏感数据

C、密码分析学主要研究加密信息的破译或信息的伪造

D、密码编码学主要研究对信息进行编码，实现信息的隐藏

601、与 RSA（Rivest,Shamir,Adleman）算法相比，DDS（Digital Signature Standard）不包括（C）

A、数字签名　　B、鉴别机制　　C、加密机制　　D、数据完整性

602、以下哪项是数据库加密方法中的库外加密的缺点？（A）

A、即使访问一条数据也要对整个数据库解密　　B、密钥管理比较复杂

C、加密之后不能完整的查询数据　　D、密钥过于简单，容易被破解

603、以下哪项数据中涉及安全保密的最主要问题？（A）

A、访问控制问题　　B、数据完整性　　C、数据正确性　　D、数据安全性

604、以下哪一个最好的描述了数字证书？（A）

A、等同于在网络上证明个人和公司身份的身份证

B、浏览器的一个标准特性，它使得黑客不能得知用户的身份

C、网站要求用户使用用户名和密码登陆的安全机制

D、伴随在线交易证明购买的收据

605、TCP SYN Flood 网络攻击时利用了 TCP 建立连接过程需要（C）次握手的特点而完成对目标进行攻击的。

A、1　　B、2　　C、3　　D、6

二、多项选择题（606-789）

606、COBIT 度量过程的三个纬度分别是（ABC）。

A、能力　　B、绩效　　C、控制度　　D、能力成熟度

607、IT 系统内网与互联网连接检查手段有哪些？（BCD）

A、工具扫描　　B、人员访谈　　C、人工检查　　D、文档检查

608、公司应该采取以下措施，对第三方访问进行控制。（ABCD）

A、公司应于第三发公司法人签署保密协议，并要求其第三方个人签署保密承诺，此项工作应在第三方获得网络与信息资产的访问权限之前完成

B、实行访问授权管理，未经授权，第三方不得进行任何形式的访问

C、公司应加强第三方访问的过程控制，监督其活动及操作，对其进行适当的安全宣传与培训

D、第三方人员应佩戴易于识别的标志，并在访问公司重要场所时有专人陪同

609、计算机信息系统安全的三个相辅相成，互补互通的有机组成部分是（ABD）

A、安全策略　　B、安全法规　　C、安全技术　　D、安全管理

610、劳动合同中应包含网络与信息安全条款，这些条款规定（ACD）。

A、员工的安全责任和违约罚则

B、安全责任不可延伸至公司场所以外和正常工作时间以外

C、安全责任可延伸至公司场所以外和正常工作时间以外

D、如必要，一些安全责任应在雇佣结束后延续一段特定的时间

611、审核是网络安全工作的核心，下列应用属于主动审核的是：（CD）

A、Windows 事件日志记录　　B、数据库的事务日志记录

C、防火墙对访问站点的过滤　　D、系统对非法链接的拒绝

612、通用准则 CC 实现的目标有（ABC）

A、成为统一的国际通用安全产品、系统的安全标准

B、在不同国家达成协议，相互承认产品安全等级评估

C、概述 IT 产品的国际通用性　　D、都不是

613、系统用户账号登记表应包括（ABCD）。

A、使用者姓名、部门、职务、联系电话　　B、账号权限

C、批准人、开通人　　D、开通时间、到期日

614、下列情况哪些是对公司经营管理的影响为“一般”级别的互联网网络安全事件？（ABD）

A、发生未到达“预警”的一般性安全事件

B、出现新的漏洞，尚未发现利用方法或利用迹象

C、有来自境外的网络性能明显下降的报警，并且其技术原因普遍适用于我国互联网

D、出现新的蠕虫/病毒或其它恶意代码，尚未证明可能造成严重危害

615、信息安全的主要原则有（BCD）

A、认证性　　B、保密性　　C、可用性　　D、完整性

616、针对支撑系统，除业务关联性、对业务网络的影响，资产价值主要体现在（ACD）几个方面。　缺少 D 选项

A、业务收益的影响　　B、设备购买成本　　C、面向客户的重要程度　　D、

617、IT 系统病毒泛滥的主要原因有哪些？（ABCD）

A、主机和终端防病毒软件缺乏统一管理

B、主机和终端防病毒软件没有设置为自动更新或更新周期较长

C、防病毒服务器没有及时更新放病毒库

D、缺乏防病毒应急处理流程和方案

618、IT 系统病毒防护评估检查对象包括哪些内容？（ABCD）

A、防病毒服务器　　B、重要应用 Windows 主机

C、Windows 终端　　D、主机管理员

619、互联网连接防火墙设备的安全策略配置要求包括哪几点（ABCD）。

A、远程登录是否禁止 telnet 方式　　B、最后一条策略是否是拒绝一切流量

C、是否存在允许 any to any 的策略

D、是否设置了管理 IP，设备只能从管理 IP 登录维护

620、《安全基线标准》在安全管理层面主要围绕哪几部分考评安全基线？（ABC）

A、组织架构管理　　B、人员安全管理　　C、运维安全管理　　D、制度安全管理

621、IT 系统维护人员权限原则包括（ACD）。

A、工作相关　　B、最大授权　　C、最小授权　　D、权限制约

622、安全系统加固手册中关于造成系统异常中断的各方面因素，主要包括哪三方面（ABD）

A、人为原因　　B、环境原因　　C、生产原因　　D、设备原因

623、IT 系统维护人员权限原则包括（ACD）

A、工作相关　　B、最大授权　　C、最小授权　　D、权限制约

624、计算当前 Linux 系统中所有用户的数量，可以使用（ABC）命令

A、wc -l /etc/passwd　　B、wc -l</etc/passwd

C、cat/etc/passwd|wc -l　　D、cat/etc/passwd>wc -l

625、Solarid 系统中，攻击者在系统中增加账户会改变哪些文件？（AB）

A、shadow　　B、passwd　　C、inetd,conf　　D、hosts

626、Syn Flood 攻击的现象有以下哪些？（ABC）

A、大量连接处于 SYN_RCVD 状态　　B、正常网络访问受阻

C、系统资源使用率高

627、UNIX 安全审计的主要技术手段有哪些？（ABCDEF）

A、文件完整性审计　　B、用户、弱口令审计　　C、安全补丁审计

D、端口审计　　E、进程审计　　F、系统日志审计

628、Unix 系统提供备份工具有（ABCD）

A、cp：可以完成把某一目录内容拷贝到另一目录

B、tar：可以创建、把文件添加到或从一个 tar 档案中解开文件

C、cpio：把文件拷贝进或拷贝出一个 cpio 档案或 tar 档案

D、dump：用来恢复整个文件系统或提取单个文件

629、操作系统应利用安全工具提供以下哪些访问控制功能？（ABC）

A、验证用户身份，必要的话，还应进行终端或物理地点识别

B、记录所有系统访问日志

C、必要时，应能限制用户连接时间　　D、都不对

630、从哪些地方可以看到遗留痕迹？（ABCD）

A、回收站　　B、最近使用过的文件　　C、注册表　　D、文件最后更改的时间戳 631、

632、关于 Windows 活动目录说法正确的是（ABD）。

A、活动目录是采用分层结构来存储网络对象信息的一种网络管理体系

B、活动目录可以提供存储目录数据和网络用户级管理员使用这些数据的方法

C、利用活动目录来实现域内计算机的分布式管理

D、活动目录与域紧密结合构成与目录林和域目录树，使大型网络中庞大、复杂的网络管理、控制、访问变得简单，使网络管理效率更高

633、建立堡垒主机的一般原则是（AC）。

A、最简化原则　　B、复杂化原则　　C、预防原则　　D、网络隔离原则

634、逻辑空间主要包括哪些部分？（ABDE）

A、TABLESPACES　　B、SEGMENTS　　C、DATAFILE

D、EXTENTS　　E、BLOCK

635、哪些属于 Windows 日志？（ABCD）

A、AppEvent.Evt　　B、SecEvent.Evt　　C、SysEvent.Evt　　D、W3C 扩展日志

636、如何设置 listener 口令？（ACDE）

A、以 Oracle 用户运行 lsnrctl 命令　　B、set log_file

C、change_password　　D、set password　　E、save_config

637、审计启动其日志有哪两种存放方式？（BD）

A、NONE　　B、OS　　C、TRUE　　D、SYS.AUD$

638、生产服务器通常都是 UNIX 平台，资产价值最高，不直接连接外部网络，主要的安全需求是（ABD）

A、访问控制　　B、账号口令　　C、数据过滤　　D、权限管理和补丁管理

639、使用 md5sum 工具对文件签名，以下说法正确的是？（ADE）

A、md5sum 对任何签名结果是定长的 16 字节

B、md5sum 对文件签名具有不可抵赖性

C、md5sum 是对文件进行加密运算得出签名，不同文件结果几乎不相同

D、md5sum 是对文件进行哈希运算得出签名，不同文件结果几乎不相同

E、md5sum 对文件签名时，与文件的日期和时间无关

640、为了正确获得口令并对其进行妥善保护，应认真考虑的原则和方法有（ABCD）

A、口令/账号加密　　B、定期更换口令

C、限制对口令文件的访问　　D、设置复杂的、具有一定位数的口令

641、文件系统是构成 Linux 基础，Linux 中常用文件系统有（ABD）？

A、ext3　　B、ext2　　C、hfs　　D、reiserfs

642、下列关于 UNIX 下日志说法正确的是（AC）

A、wtmp 记录每一次用户登录和注销的历史信息

B、acct 记录每个用户使用过的命令

C、sulog 记录 su 命令的使用情况

D、acct 记录当前登录的每个用户

643、下列哪些操作可以看到自启动项目？（ABD）

A、注册表　　B、开始菜单　　C、任务管理器　　D、msconfig

644、下列哪些命令行可用于查看当前进程？（ABC）

A、Ps -ef　　B、Strings -f/proc/[0-9]*/cmdline

C、Ls -al /proc/[0-9]*/exe　　D、Cat/etc/inetd.conf

645、下面操作系统中，哪些是 UNIX 操作系统？（CD）

A、Red-hat Linux　　B、Novell Netware　　C、Free BSD　　D、SCO Unix

646、严格的口令策略应当包含哪些要素（ABC）

A、满足一定的长度，比如 8 位以上　　B、同时包含数字，字母和特殊字符

C、系统强制要求定期更改口令　　D、用户可以设置空口令

647、在 Solaris 8 下，使用 ps -ef 命令列出进程中有一行如下“root 1331 0 00:01:00?　　0:00 /usr/sbin/inetd -s -t”，以下说法正确的是（ABE）

A、参数-t 是 trace，记录包括 IP 和 PORT 等信息

B、参数-t 对于 UDP 服务无效　　C、进程启动的时间不能确定

D、进程已经运行了 1 分钟　　E、进程的父进程号是 1

648、在 Solaris 8 下，以下说法正确的是：（AB）

A、/etc/rc2.d 里 S 开头的文件在系统缺省安装的缺省级别会自动运行

B、/etc/rc3.d 里 S 开头的文件在系统缺省安装的缺省级别会自动运行

C、/etc/init.d 里的文件在系统启动任何级别时会自动运行

D、init 0 是进入单用户级别　　E、init 6 命令会运行所有级别的 rc 目录下以 S 开头的文件

649、在 Solaris 8 下，以下说法正确的是：（BC）

A、PATH 环境变量最后带有“.”，会使当前目录的命令比其他目录的命令有限执行

B、可以修改/etc/inittab 里 ttymon 的参数，使得登录的 SHELL 在无输入时自动退出

C、在使用/bin/ksh 时，可以设置 TMOUT 值，使得登录的 SHELL 在无输入时自动退出

D、在/etc/login 中，可以设置 TIMEOUT 值，使得登录的 SHELL 在无输入时自动退出

E、tar xvf 命令的意思是以 tar 格式解开输入，并且保持文件属性等参数不变

650、在配置 Apache 访问控制时，Allow 和 Deny 指令可以允许或拒绝来自特定主机名或主机名地址的访问。那么下列哪些配置是不正确的？（AD）

A、Order allow,deny Allow from 192.101.205

B、B、Order deny,allow Deny from all Allow from example

C、C、Order deny,allow Deny from 192.101.205

D、D、Order allow,deny Deny from 192.101.205 Allow from all

651、造成操作系统安全漏洞的原因是（ABC）。

A、不安全的编程语言　　B、不安全的编程习惯

C、考虑不周的架构设计　　D、人为的恶意破坏

652、针对 Linux 主机，一般的加固手段包括（ABC）。

A、打补丁　　B、关闭不必要的服务　　C、限制访问主机　　D、切断网络

653、做系统快照，查看端口信息的方式有（AD）。

A、netstat -an　　B、net share　　C、net use　　D、用 taskinfo 来查看连接情况

654、网厅安全解决方案主要从哪几个方面对网厅安全进行建议和指导？（ABCD）

A、安全管理　　B、安全防护　　C、安全运维　　D、灾备/恢复

655、IT 系统软件设计中应当考虑并执行安全审计功能，详细记录访问信息的活动，包括

（ABCD）。

A、记录的活动以是否有数据的修改、应用程序的异常关闭、异常删除触发

B、应用系统应当配置单独的审计数据库，审计记录应单独存放，并设置严格的边界访问控制，只有安全管理人员才能够看到审计记录

C、信息系统的审计功能包括：事件日期、时间、发起者信息、类型、描述和结果

D、应用系统的审计进程为后台处理，与应用系统运行同步进行，并且对于审计进程应当涉及相应的守护进程，一旦出现异常停止系统可重新启动审计进程，从而保障审计的“完整性”

656、IPSec 的配置步骤包括：（ABCD）

A、防火墙基本配置　　B、定义保护数据流和域间规则

C、配置 IPSec 安全提议　　D、配置 IKEPeer

657、Juniper 路由器在配置 SSH 访问时应注意如下（ABCD）细节。

A、建立允许访问的 SSH-ADDRESSES 过滤器

B、确保只允许来自内部接口的授权用户访问

C、针对 SSH 进行限速以保护路由引擎

D、过滤器应用在 loopback 接口

658、对于使用 RPF 反向地址验证，以下说法错误的是：（BCD）。

A、对称路由可以使用　　B、非对称路由可以使用

C、有些情况不可以使用，但与对称或非对称路由无关

D、在任何情况下都可以使用

659、防病毒服务升级检查包括如下几项内容？（ABC）

A、检查防病毒服务器病毒库下载是否正常，如果不正常及时联系厂商进行问题解决

B、在防病毒系统每次升级后，记录每次版本变更版本号，定期记录病毒库的版本

C、对重要的服务器，定期抽查防病毒客户端的病毒库升级情况

660、防范 DOS 攻击的方法主要有（ABCD）。

A、安装 Dos 检测系统　　B、对黑洞路由表里的地址进行过滤

C、及时打好补丁　　D、正确配置 TCP/IP 参数

661、防火墙 trust 域中的客户机通过 nat 访问 untrust 中的服务器的 ftp 服务，已经允许客户机访问服务器的 tcp21 端口，但只能登陆到服务器，却无法下载文件，以下解决办法中可能的是：（ABC）

A、修改 trust untrust 域间双向的默认访问策略为允许

B、FTP 工作方式为 port 模式时，修改 untrust trust 域间 in 方向的默认访问策略为允许

C、在 trust untrust 域间配置中启用 detect ftp

D、FTP 工作方式为 passive 模式时，修改 untrust trust 域间 in 方向的默认访问策略为允许

662、防火墙不能防止以下哪些攻击？（ABD）

A、内部网络用户的攻击　　B、传送已感染病毒的软件和文件

C、外部网络用户的 IP 地址欺骗　　D、数据驱动型的攻击

663、防火墙常见的集中工作模式有（ABC）。

A、路由　　B、NAT　　C、透明　　D、旁路

664、防火墙的缺陷主要有（ABCD）。

A、限制有用的网络服务　　B、无法防护内部网络用户的攻击

C、不能防备新的网络安全问题　　D、不能完全防止传送已感染病毒的软件或文件

665、防火墙的日志管理应遵循如下原则：（BC）

A、本地保存日志　　B、本地保存日志并把日志保存到日志服务器上

C、保持时钟的同步　　D、在日志服务器保存日志

666、防火墙的特征是（ABCD）。

A、保护脆弱和有缺陷的网络服务　　B、加强对网络系统的访问控制

C、加强隐私，隐藏内部网络结构　　D、对网络存取和访问进行监控审计

667、防火墙的主要功能有哪些？（ABCD）

A、过滤进、出网络的数据　　B、管理进、出网络的访问行为

C、封堵某些禁止的业务，对网络攻击进行检测和报警

D、记录通过防火墙的信息内容和活动

668、防火墙的作用主要有（ABCD）。

A、实现一个公司的安全策略　　B、创建一个阻塞点

C、记录 Internet 活动　　D、限制网络暴露

669、防火墙技术，涉及到（ABCD）。

A、计算机网络技术　　B、密码技术　　C、软件技术　　D、安全操作系统

670、防火墙可以部署在下列位置：（ABCD）。

A、安全域边界　　B、服务器区域边界

C、可信网络区域和不可信网络区域之间　　D、根据网络特点设计方案

671、防火墙配置时应确保（ABCD）服务不开放。

A、Rlogin　　B、NNTP　　C、Finger　　D、NFS

672、启用 Cisco 设备的访问控制列表，可以起到如下作用（ABC）。

A、过滤恶意和垃圾路由信息　　B、控制网络的垃圾信息流

C、控制未授权的远程访问　　D、防止 DDoS 攻击

673、如果 Cisco 设备的 VTY 需要远程访问，则需要配置（ABCD）。

A、至少 8 位含数字、大小写、特写字符的密码　　B、远程连接的并发数目

C、访问控制列表　　D、超市退出

674、如果需要配置 Cisco 路由器禁止从网络启动和自动从网络下载初始配置文件，配置命令包括（AB）。

A、no boot network　　B、no service config　　C、no boot config　　D、no service network

675、入侵检测的内容主要包括：（BC）。

A、独占资源、恶意使用　　B、试图闯入或成功闯入、冒充其他用户

C、安全审计　　D、违反安全策略、合法用户的泄露

676、入侵检测系统包括以下哪些类型？（AC）

A、主机入侵检测系统　　B、链路状态入侵检测系统

C、网络入侵检测系统　　D、数据包过滤入侵检测系统

677、随着交换机的大量使用，基于网络的入侵检测系统面临着无法接收数据的问题。由于交换机不支持共享媒质的模式，传统的采用一个嗅探器（sniffer）来监听整个子网的办法不再可行。可选择解决的办法有（ABCD）。

A、使用交换机的核心芯片上的一个调试的端口

B、把入侵检测系统放在交换机内部或防火墙等数据流的关键入口

C、采用分解器（tap）

D、使用以透明网桥模式接入的入侵检测系统

678、通常要求把路由器的日志存储在专用日志服务器上，假设把 Cisco 路由器日志存储在 192.168.0.100 的 syslog 服务器上，需要在路由器侧配置的操作时：（ABCD）。

A、使用 Router(config)# logging on 启用日志：使用 Router(config)# logging trap information 将记录日志级别设定为“information”

B、使用 Routee(config)# logging192.168.0.100 将记录日志类型设定为“local6”

C、使用(config)# logging facility local6 将日志发送到 192.168.0.100

D、使用(config)# logging sourceinterface loopback0 设定日志发送源 loopback0

679、通过 SSL VPN 接入企业内部的应用，其优势体现在哪些方面：（ABCD）。

A、应用代理　　B、穿越 NAT 和防火墙设备

C、完善的资源访问控制　　D、抵御外部攻击

680、网络地址端口转换（NAPT）与普通地址转换有什么区别？（AD）

A、经过 NAPT 转换后，对于外网用户，所有报文都来自于同一个 IP 地址

B、NAT 只支持应用层的协议地址转换

C、NAPT 只支持网络层的协议地址转换

D、NAT 支持网络层的协议地址转换

681、网络攻击的类型包括以下哪几种？（ABCD）

A、窃取口令　　B、系统漏洞和后门　　C、协议缺陷　　D、拒绝服务

682、网络面临的典型威胁包括（ABCD）。

A、未经授权的访问　　B、信息在传送过程中被截获、篡改

C、黑客攻击　　D、滥用和误用

683、网络蠕虫一般指利用计算机系统漏洞、通过互联网传播扩散的一类病毒程序，该类病毒程序大规模爆发后，会对相关网络造成拒绝服务攻击，为了防止受到网络蠕虫的侵害，应当注意对（ACD）及时进行升级更新。

A、计算机操作系统　　B、计算机硬件　　C、文字处理软件　　D、应用软件

684、下列关于 NAT 地址转换的说法中哪些事正确的：（ABCD）。

A、地址转换技术可以有效隐藏局域网内的主机，是一种有效的网络安全保护技术

B、地址转换可以按照用户的需要，在局域网内向外提供 FTP、WWW、Telnet 等服务

C、有些应用层协议在数据中携带 IP 地址信息，对它们作 NAT 时还要修改上层数据中的 IP 地址信息

D、对于某些非 TCP、UDP 的协议（如 ICMP、PPTP），作上层 NAT 时，会对它们的特征参数（如 ICMP 的 id 参数）进行转换。

685、下列哪两项正确描述了由 WPA 定义的无线安全标准？（BC）

A、使用公开密钥的认证方法　　B、当客户端连接的时候都要进行动态密钥交换

C、包含 PSK 认证　　D、定制了一个经常更换的静态的加密密钥来增强安全性

686、下列配置中，可以增强无线 AP（access point）安全性的有（ABCD）。

A、禁止 SSID 广播　　B、禁用 DHCP 服务

C、采用 WPA2-PSK 加密认证　　D、启用 MAC 地址接入过滤

687、下面可以攻击状态检测的防火墙方法有：（ABD）

A、协议隧道攻击　　B、利用 FTP-pasv 绕过防火墙认证的攻击

C、ip 欺骗攻击　　D、反弹木马攻击

688、下面什么路由协议不可以为 HSRP 的扩充：（ABC）

A、SNMP　　B、CDP　　C、HTTP　　D、VRRP

689、下面什么协议有 MD5 认证：（ABC）

A、BGP　　B、OSPF　　C、EIGER　　D、RIPversion 1

690、下面是网络安全技术的有：（ABC）

A、防火墙　　B、防病毒　　C、PKI　　D、UPS

691、选购一个防火墙时应该考虑的因素有：（ABCD）

A、网络受威胁的程度　　B、可能受到的潜在损失

C、站点是否有经验丰富的管理员　　D、未来扩展的需要

692、一台路由器的安全快照需要保存如下哪些信息？（AB）

A、当前的配置--running-config　　B、当前的开放端口列表

C、当前的路由表　　D、当前的 CPU 状态

693、以下对于包过滤防火墙的描述正确的有（ACD）。

A、难以防范黑客攻击　　B、处理速度非常慢

C、不支持应用层协议　　D、不能处理新的安全威胁

694、以下对于代理防火墙的描述正确的有（ABCD）。

A、能够理解应用层上的协议　　B、时延较高，吞吐量低

C、能做复杂一些的访问控制，并做精细的认证和审核　　D、可伸缩性较差

695、以下关于 L2TP VPN 配置注意事项的说法中正确的有：（ABC）

A、L2TP 的 LNS 端必须配置虚拟接口模板（Virtual-Template）的 IP 地址，该虚拟接口模板需要加入域

B、防火墙缺省需要进行隧道的认证。如果不配置认证，需要 undo tunnel authentication 命令

C、为了使 L2TP 拨号上来的用户分配的地址不能喝内网用户的地址在同一个网段

D、LNS 端不允许配置多个 L2TP-Group

696、以下哪几项关于安全审计和安全审计系统的描述是正确的？（CD）

A、对入侵和攻击行为只能起到威慑作用

B、安全审计不能有助于提高系统的抗抵赖性

C、安全审计是对系统记录和活动的独立审查和检验

D、安全审计系统可提供侦破辅助和取证功能

697、以下哪些属于网络欺骗方式？（ABCD）

A、IP 欺骗　　B、ARP 欺骗　　C、DNS 欺骗　　D、Web 欺骗

698、以下哪些是防火墙规范管理需要的？（ABCD）

A、需要配置两个防火墙管理员　　B、物理访问防火墙必须严密地控制

C、系统软件、配置数据文件在更改后必须进行备份

D、通过厂商指导发布的硬件和软件的 bug 和防火墙软件升级版

699、以下硬件安装维护重要安全提示正确的有：（ABCD）

A、不要在雷雨天气进行故障处理　　B、保持故障处理区域的干净、干燥

C、上防静电手套或防静电腕带再执行安装和更换操作

D、在使用和操作设备时，需要按照正确的操作流程来操作

700、以下属于 DTE(Data Terminal Equipment)数据终端设备的有（AB）

A、路由器　　B、PC　　C、交换机　　D、HUB

701、在防火墙的“访问控制”应用中，内网、外网、DMZ 三者的访问关系为：（ABD）

A、内网可以访问外网　　B、内网可以访问 DMZ 区

C、DMZ 区可以访问内网　　D、外网可以访问 DMZ 区

702、关于 GRE 校验和验证技术，当本端配置了校验和而对端没有配置校验和时，以下叙述正确的有（BC）。

A、本端对接收报文检查校验和　　B、对端对接收报文检查校验和

C、本端对发送报文计算校验和　　D、对端对发送报文计算校验和

703、配置 PPP 链路层协议时，链路层协议状态始终不能转为 Up 状态的处理建议：（ABCD）

A、PPP 链路两端的接口上配置的参数和验证方式都必须一致，LCP 检查才能成功

B、如果 LCP 协商失败，请检查 LCP 配置协商参数

C、请检查验证方式配置是否正确。因为 LCP 协商中，包含验证方式的协商。因为 LCP

协商中，包含验证方式的协商。验证方式协商失败也会导致 LCP 协商失败

D、接口试图下先执行 shutdown 命令将接口关闭，再执行 undo shutdown 命令重启接口

704、对 DNSSEC 的描述正确的有（AC）。

A、为 DNS 数据提供来源验证，即保证数据来自正确的名称服务器

B、DNSSEC 可防御 DNS Query Flood 攻击

C、为域名数据提供完整性验证，即保证数据在传输的过程中没有被篡改

D、实施 DNSSEC 后，只需升级软件系统，对网络、服务器等硬件设备不需考虑

705、MySQL 安装程序会给出三种选择，用户可以根据自身的需要选择一种适合的安装方式，以下哪些是正确的？（ABD）

A、Typical（典型安装）　　B、Compact(最小安装)

C、Full(全部安装)　　D、Custom(选择安装)

706、MySQL 中用 DROP 语句可删除数据库和数据表，以下哪句是正确的语法？（ABCD）

A、DROP TABLE table_name1　　B、DROP TABLE table_name1,table_name2

C、DROP TABLE IF EXISTS table_name1　　D、DROP DATABASE DB name1

707、Oracle 7.2 之前的数据库连接用户名和密码在网络传输时是不进行加密的，为了要和旧版本兼容 Oracle 数据库 9.02 存在 DBLINK_ENCRYPT_LOGIN 参数用来调节数据库连接时用户名和密码的加密特性，以下说法正确的是：（ACD）。

A、DBLINK_ENCRYPT_LOGIN 为 TRUE 时，数据库连接加密用户名和密码

B、DBLINK_ENCRYPT_LOGIN 时，数据库连接不加密用户名和密码

C、DBLINK_ENCRYPT_LOGIN 为 FALSE 时，如果加密的数据库连接失败，会尝试不加密的连接

D、DBLINK_ENCRYPT_LOGIN 为 TRUE 时，加密的数据库连接失败，也不会尝试不加密的连接

708、Oracle 实例主要由哪两部分组成：（AC）

A、内存　　B、Share pool buffer　　C、后台进程　　D、pmon 和 smon

709、Oracle 中如何设置 audit trail 审计，正确的说法是：（ABD）

A、在 init.ora 文件中设置“audit_trail = true”或者“audit_trail = db”

B、以 SYSDBA 身份使用 AUDIT ALL ON SYS.AUD$ BY ACCESS，语句对 audit trail 审计

C、Oracle 不支持对 audit trail 的审计

D、在设置 audit trail 审计前，要保证已经打开 Oracle 的审计机制

710、SQL Server 的登录认证种类有以下哪些？（ACD）

A、Windows 认证模式　　B、双因子认证模式

C、混合认证模式　　D、SQL Server 认证

711、SQL Server 的取消权限的操作有以下哪些？（ABC）

A、在“详细信息”窗格中右击要授予/拒绝/取消其权限的用户定义的角色

B、单击“属性”命令在“名称”下单击“权限”单击列出全部对象

C、选择在每个对象上授予拒绝或废除的权限，选中标志表示授予权限，X 表示拒绝权限，空框表示废除权限，只列出适用于该对象的权限

D、回到“数据库用户属性”对话框中，再点击“确定”按钮，所有的设置就完成了

712、SQL Server 中 ALTER DATABASE 可以提供以下哪些功能选项？（ABCD）

A、更改数据库名称　　B、文件组名称　　C、数据文件　　D、日志文件的逻辑名称

713、SQL Server 中关于实例的描述，请选择正确的答案。（ABD）

A、如果安装选择“默认”的实例名称。这时本 SQL Server 的名称将和 Windows 2000 服务器的名称相同

B、SQL Server 可以在同一台服务器上安装多个实例

C、SQL Server 只能在一台服务器上安装一个实例

D、实例各有一套不为其他实例共享的系统及用户数据库，所以各实例的运行是独立的。

714、SQL Server 中使用企业管理器从数据库中删除数据或日志文件的步骤如下，正确的步骤是？（ABCD）

A、展开服务器组，然后展开服务器

B、展开“数据库”文件夹，右击要从中删除数据或日志文件的数据库，然后单击“属性”命令

C、若要删除数据文件，单击“常规”选项卡。若要删除日志文件，单击“事务日志”选项卡

D、在“文件名”列户，单击要删除的文件名旁边的箭头，再点 DELETE 键，文件名旁出现十字光标，表明将删除此文件

715、参数 REMOTE_LOGIN_PASSWORDFILE 在 Oracle 数据库实例的初始化参数文件中，此参数控制着密码文件的使用及其状态，以下说法正确的是：（ABCD）

A、NONE：只是 Oracle 系统不使用密码文件，不允许远程管理数据库

B、EXCLUSIVE：指示只有一个数据库实例可以使用密码文件

C、SHARED：指示可有多个数据库实例可以使用密码文件

D、以上说法都正确

716、关于 SQL Server 2000 中的 SQL 账号、角色，下面说法正确的是：（ABC）

A、PUBLIC,guest 为缺省的账号　　B、guest 不能从 master 数据库清除

C、可以通过删除 guest 账号的角色，从而消弱 guest 可能带来的安全隐患

D、SQL Server 角色的权限是不可以修改的

717、连接 MySQL 后选择需要的数据库 DB_NAME？以下哪些方法是对的（AC）

A、连接后用 USE DB_NAME 选择数据库

B、连接后用 SET DB_NAME 选择数据库

C、用 mysql -h host -u user -p DB_NAME 连接数据库

D、用 mysql -h host -u user -p -T DB_NAME 连接数据库

718、如果数据库不需要远程访问，可以禁止远程 tcp/ip 连接，以增强安全性。可选择的有效方法：（AC）

A、用防火墙封堵数据库侦听端口避免远程连接　　B、禁止 tcp/ip 协议的使用

C、在 mysqld 服务器中参数中添加 --skip-networking 启动参数来使 mysql

D、在/etc/my.cnf 下添加 remoteConnnect=disable

719、以下哪些 MySQL 中 GRANT 语句的权限指定符？（ABCDEF）

A、ALTER　　B、CREATE　　C、DELETE

D、UPLOAD　　E、DROP　　F、INSERT

720、用 THC 组织的 Oracle 的工具，通过 sniffer 方式抓取数据库的认证信息可有效破解 Oracle 密码，以下哪些数据是必须获取的？（ABC）

A、AUTH_SESSKEY　　B、AUTH_PASSWORD　　C、用户名　　D、实例名

721、在 Oracle 9 数据库可以通过配置$Oracle_HOME\network\admin\sqlnet.ora 文件实现数据库层次的基于 TCP 协议和地址的访问控制。下面说法正确的是：（ABCD）

A、首先需要配置 TCP,VALIDNODE_CHECKING=yes 启用节点检查功能

B、其次配置 TCP.INVITED_NODES=192.168.0.12，192.168.0.33 将会允许地址是 192.168.0 网段的 12 和 33 的主机访问

C、然后配置 TCP.EXCLUDED_NONES=192.168.0.123 将会禁止地址是 192.168.0 网段的 123 的主机访问

D、要以上配置生效必须重启 lsnrctl 监听器

722、在 SQL Server 2000 中，如果想查询当前数据库服务器软件的版本，可以使用下面哪些方式（ABCD）

A、在查询分析器中通过如下语句查询 SELECT ServerPROPERTY('productversion'),ServerPROPERTY('productlevel'),ServerPROPERTY('edition')

B、在命令行下，用 SQL Server 自带的管理工具 osql 连接进入数据库，输入 select@@version

C、企业管理器查看服务器属性　　D、在 SQL Server 服务管理器里面查看"关于"

723、在 SQL Server 2000 中一些无用的存储过程，这些存储过程极容易被攻击者利用，攻击数据库系统。下面的存储过程哪些可以用来执行执行系统命令或修改注册表？（ABC）

A、xp_cmdshell　　B、xp_regwrite　　C、xp_regdeletekey　　D、select * from master

724、在 SQL Server 中创建数据库，如下哪些描述是正确的？（ABCD）

A、创建数据库的权限默认授权 sysadmin 和 dbcreator 固定服务器角色的成员，但是它仍可以授予其他用户

B、创建数据库的用户将成为该数据库的所有者

C、在一个服务器上，最多可以创建 32,767 个数据库

D、数据库名称必须遵循标示符规则

725、在对 SQL Server 2000 的相关文件、目录进行安全配置时，下面可以采用的措施是：（ABCD）

A、删除缺省安装时的例子样本库

B、将存放数据的库文件，配置权限为 administrators 组、system 和启动 SQL Server 服务的用户账号及 DBA 组具有完全控制权限

C、对 SQL Server 安装目录，去除 everyone 的所有控制权限

D、将数据库数据相关的文件，保存在非系统盘的 NTFS 独立分区

726、sybase 数据库文件系统需要哪些裸设备？（ABCD）

A、master　　B、proce　　C、data　　D、log

727、Oracle 支持哪些加密方式？（ABCD）

A、DES　　B、RC4_256　　C、RC4_40　　D、DES40

728、SQL Server 用事件探测器可以帮助排除故障和解决问题，创建跟踪的步骤如下哪些是

正确的？（ABCD）

A、从“模板名称”下拉菜单为你创建跟踪选择一个模板

B、“事件探查器”主界面打开后，从“文件”菜单选择“新跟踪”

C、在“跟踪名称”文本框中输入你想要为这个跟踪创建的跟踪名称

D、修改这些默认的选项设置。通过点击“显示全部事件”和“显示全部列”复选框来查看其他的选项。

729、最重要的电磁场干扰源是：（BCD）

A、电源周波干扰　　B、雷电电磁脉冲 LEMP

C、电网操作过电压 SEMP　　D、静电放电 ESD

730、雷电侵入计算机信息系统的途径主要有：（ABD）

A、信息传输通道线侵入　　B、电源馈线侵入　　C、建筑物　　D、地电位反击

731、电信生产其机房作业，是由专门的值机员、机务员来完成，作业内容是：固定电话、无线电话、电报、载波、短波、微波、卫星和电力等电信通信设备，使设备出去良好状态，保证其正常运行。（ABCD）

A、安装　　B、值守　　C、维护　　D、检修

732、对计算机系统有影响的腐蚀性气体大体有如下几种：（ABCD）

A、二氧化硫　　B、氢化硫　　C、臭氧　　D、一氧化碳

733、防火工作的基本措施有：（ABCD）

A、加强对人员的教育管理　　B、加强对可燃物的管理

C、加强对物的管理　　D、加强对火源、电源的管理

734、会导致电磁泄漏的有（ABCDE）

A、显示器　　B、开关电路及接地系统

C、计算机系统的电源线　　D、机房内的电话

E、信号处理电

735、火灾自动报警、自动灭火系统部署应注意（ABCD）。

A、避开可能招致电磁干扰的区域或设备　　B、具有不间断的专用消防电源

C、留备用电源　　D、具有自动和手动两种触发装置

736、计算机场地安全测试包括（ABCD）。

A、温度，湿度，尘埃　　B、照度，噪声，电磁场干扰环境场强

C、接地电阻，电压、频率　　D、波形失真率，腐蚀性气体的分析方法

737、计算机信息系统设备处于不同雷电活动地区，其雷电电磁场强度有很大差异，根据这一差异，将被防护空间分为下列哪些防护区？（ABCD）

A、直击雷非防护区（LPZOA）　　B、直击雷防护区（LPZOB）

C、第一防护区（LPZI）　　D、后续防护区（LPZ2,3...等）

738、静电的危害有（ABCD）。

A、导致磁盘读写错误，损坏磁头，引起计算机误动作　　B、造成电路击穿或者毁坏

C、电击，影响工作人员身心健康　　D、吸附灰尘

739、灭火的基本方法有（ABCD）。

A、冷却法　　B、隔离法　　C、窒息法　　D、抑制

740、实体安全技术包括（ABD）。

A、环境安全　　B、设备安全　　C、人员安全　　D、媒体安全

741、使用配有计算机的仪器设备时，不应该做的有：（ABCD）

A、更改登机密码和系统设置

B、自行安装软件

C、玩各种电脑游戏

D、将获得的图像、数据等资料存储在未予指定的硬盘分区上

742、硬件设备的使用管理包括（ABCD）。

A、严格按硬件设备的操作使用规程进行操作

B、建立设备使用情况日志，并登记使用过程

C、建立硬件设备故障情况登记表

D、坚持对设备进行例行维护和保养

743、预防静电的措施有（ABCD）。

A、接地　　B、不使用或安装产生静电的设备

C、不在产生静电场所穿脱工作服　　D、作业人员穿防静电鞋

744、在实验室中引起火灾的通常原因包括：（ABCD）

A、明火　　B、电器保养不良

C、仪器设备在不使用时未关闭电源　　D、使用易燃物品时粗心大意

745、直击雷：直接击在（ABCD）并产生电效应、热效应和机械力的雷电放电。

A、建筑物　　B、构建物　　C、地面突进物　　D、大地或设备

746、员工区域安全守则包括：（ABCD）

A、非工作时间，员工进入或离开办公区域，应在值班人员处登记

B、外来人员进入办公区域或机房，相关员工必须全程陪同

C、将物品带入/带出公司，要遵守公司相关的规定及流程

D、参加会议时遵守会前、会中、会后的保密流程

747、机房出入控制措施包括：（ABCD）

A、机房接待前台须核查弄清业务系统安全区域的来访者的身份，并记录其进入和离开安全区域的日期与时间

B、机房须告知进入安全区的来访者，该区域的安全要求和紧急情况下的行动步骤

C、可采用强制性控制措施，对来访者的访问行为进行授权和验证

D、要求所有进出机房人员佩带易于辨识的标识

748、为了减小雷电损失，可以采取的措施有（ACD）

A、机房内应设等电位连接网络　　B、部署 UPS

C、设置安全防护地与屏蔽地

D、根据雷击在不同区域的电磁脉冲强度划分，不同的区域界面进行等电位连接

749、安全要求可以分解为（ABCDE）。

A、可控性　B、保密性　C、可用性　D、完整性　E、不可否认性

750、HASH 加密使用复杂的数字算法来实现有效的加密，其算法包括（ABC）

A、MD2　B、MD4　C、MD5　D、Cost256

751、利用密码技术，可以实现网络安全所要求的。（ABCD）

A、数据保密性　B、数据完整性　C、数据可用性　D、身份验证

752、一个密码体系一般分为以下哪几个部分？（ABCD）

A、明文　B、加密密钥和解密密钥

C、密文　D、加密算法和解密算法

753、公钥密码体质的应用主要在于。（AC）

A、数字签名　B、加密　C、密钥管理　D、哈希函数

754、目前基于对称密钥体制的算法主要有。（BC）

A、RSA　B、DES　C、AES　D、DSA

755、使用 esp 协议时，可以使用的加密运算是。（ABC）

A、DES　B、3DES　C、AES　D、RSA

756、数字签名的作用是。（ACD）

A、确定一个人的身份　　B、保密性

C、肯定是该人自己的签字　　D、使该人与文件内容发生关系

757、以下属于对称加密算法的是：（ABD）

A、DES　　B、3DES　　C、SHA-1　　D、RC4　　E、MD5

758、在加密过程中，必须用到的三个主要元素是（ABC）

A、所传输的信息（明文）　　B、加密 钥匙（Encryption Key）

C、加密函数　　D、传输信道

759、账号口令管理办法适用于所有和 DSMP 系统、智能网系统、彩铃平台相关的（ACD）

A、系统管理员　　B、操作系统

C、操作维护人员　　D、所有上述系统中存在的账号和口令

760、为保证密码安全，我们应采取的正确措施有（ABC）

A、不使用生日做密码　　B、不使用少于 5 为的密码

C、不适应纯数字密码　　D、将密码设的非常复杂并保证 20 位以上

761、公司在使用数据签名技术时，除充分保护私钥的机密性，防止窃取者伪造密钥持有人的签名外，还应注意（ABCD）

A、采取保护公钥完整性的安全措施，例如使用公约证书

B、确定签名算法的类型、属性以及所用密钥长度

C、用于数字签名的密钥应不同于用来加密内容的密钥

D、符合有关数字签名的法律法规，必要时，应在合同或协议中规定使用数字签名的相关事宜

762、相对于对称加密算法，非对称密钥加密算法（ACD）

A、加密数据的速率较低

B、更适合于现有网络中对所传输数据（明文）的加解密处理

C、安全性更好　　D、加密和解密的密钥不同

763、一个典型的 PKI 应用系统包括（ABCD）实体

A、认证机构 CA　　B、册机构 RA　　C、证书及 CRL 目录库　　D、用户端软件

764、加密的强度主要取决于（ABD）

A、算法的强度　　B、密钥的保密性　　C、明文的长度　　D、密钥的强度

765、一下对于对称密钥加密说法正确的是（BCD）

A、对称加密算法的密钥易于管理　　B、加解密双方使用同样的密钥

C、DES 算法属于对称加密算法　D、相对于非对称加密算法，加解密处理速度比较快

766、在通信过程中，只采用数字签名可以解决（ABC）等问题

A、数据完整性　　B、数据的抵抗赖性　　C、数据的篡改　D、数据的保密性

767、对称密钥算法体系包括：（ABCDE）

A、明文(plaintext)：原始消息或数据，作为算法的输入

B、加密算法(encryption algorithm)：加密算法对明文进行各种替换和转换

C、秘密密钥(secret key)：秘密密钥也是算法输入，算法进行的具体替换和转换取决于这个密钥

D、密文(ciphertext)：这是产生的已被打乱的消息输出。它取决于明文和秘密密钥。对于一个给定的消息，两个不同的密钥会产生两个不同的密文

、.解密算法(decryption algorithm)：本质上是加密算法的执行。它使用密文和统一密钥产生原始明文

768、一下对于混合加密方式说法正确的是。（BCD）

A、 使用公开密钥密码体制对要传输的信息（明文）进行加解密处理

B、使用对称加密算法对要传输的信息（明文）进行加解密处理

C、使用公开密钥密码体制对称加密密码体制的密钥进行加密后的通信

D、对称密钥交换的安全信道是通过公开密钥密码体制来保证的

769、电信的网页防篡改技术有（ABC）

A、外挂轮询技术　　B、核心内嵌技术

C、时间触发技术　　D、安装防病毒软件

770、病毒发展的趋势是？（ABC）

A、 范围更广　　B、度更快　　C、方式更多

771、病毒自启动方式一般有（ABC）

A、 修改注册表　　B、将自身添加为服务

C、将自身添加到启动文件夹　　D、修改系统配置文件

772、常见 Web 攻击方法有一下哪种？（ABCD）

A、SQL Injection　　B、Cookie 欺骗　　C、跨站脚本攻击

D、信息泄露漏洞　　E、文件腹泻脚本存在的安全隐患

F、 GOOGLE HACKING

773、宏病毒感染一下哪些类型的文件？（ABCDEF）

A.、DOC　　B、EXE　　C、XLS　　D、DOT

774、木马传播包括一下哪些途径：（ACD）

A.、通过电子邮件的附件传播　　B、通过下载文件传播

C、通过网页传播　　D、通过聊天工具传播

775、目前最好的防病毒软件能做到的是（ABCD）

A.、检查计算机是否感染病毒，消除已感染的任何病毒

B、杜绝病毒对计算的侵害

C、查出计算机已感染的已知病毒，消除其中的一部分

D、检查计算机是否染有已知病毒，并作相应处理

776、通用的 DoS 攻击手段有哪些？（CD）

A、 SYN Attack　　B、ICMP Flood　　C、UDP Flood

D、Ping of Death　　E、Tear Drop　　F、Ip Spoofing

777、以下关于蠕虫的描述正确的有：（ABCDEF）

A、 蠕虫具有自动利用网络传播的特点，在传播的同时，造成了带宽的极大浪费，严重的情况可能会造成网络的瘫痪

B、 隐藏式蠕虫的基本特征，通过在主机上隐藏，使得用户不容易发现它的存在

C、蠕虫需要传播受感染的宿主文件来进行复制

D、蠕虫的传染能力主要是针对计算机内的文件系统。

778、以下哪几种扫描检测技术属于被动式的检测技术？（AB）

A、 基于应用的检测技术　　B、基于主动的检测技术

C、基于目标的漏洞检测技术　　D、基于网络的检测技术

779、以下是检查磁盘与文件是否被病毒感染的有效方法：（BC）

A、 检查磁盘目录中是否有病毒文件　　B、用抗病毒软件检查磁盘的各个文件

C、用放大镜检查磁盘编码是否有霉变现象　　D、检查文件的长度是否无故变化

780、造成计算机不安全的因素有（BD）等多种。

A、 技术原因　　B、自然原因　　C、认为原因　　D、管理原因

781、嗅探技术有哪些特点？（ABCD）

A、间接性　　B、.直接性　　C、隐蔽性　　D、开放性

782、一个恶意的攻击者必须具备哪几点？（ABC）

A、 方法　　B、机会　　C、动机　　D、运气

783、对于 DOS 网络攻击，可以采用以下哪些措施来缓解主机系统被攻击进程。（ACD）

A.、缩短 SYN Timeout 时间和设置 SYN Cookie　　B、增加网络带宽

C、在系统之前增加负载均衡设备　　D、在防火墙上设置 ACL 或黑客路由

784、利用 Bind/DNS 漏洞攻击的分类主要有（ACD）

A、 拒绝服务　　B、匿名登录　　C、.缓冲区溢出

D、DNS 缓存中毒　　E、病毒或后门攻击

785、常见 Web 攻击方法有一下哪种？（ABCD）

A、 SQL Injection　　B、 Cookie 欺骗　　C、 跨站脚本攻击　　D、信息泄露漏洞

786、黑客所使用的入侵技术主要包括（ABCDE）

A.、协议漏洞渗透　　B、密码分析还原　　C、应用漏洞分析与渗透

D、拒绝服务攻击　　E、病毒或后门攻击

787、主动响应，是指基于一个检测到的入侵所采取的措施。对于主动响应来说，其选择的措施可以归入的类别有（ABC）

A、针对入侵者采取措施　　B、修正系统

C、收集更详细的信息　　D、入侵追踪

788、下面哪些漏洞属于网络服务类安全漏洞：（BC）

A.、Windows 2000 中文版输入法漏洞　　B、IS Web 服务存在的 IDQ 远程溢出漏洞

C、RPC DCOM 服务漏洞　　D、Web 服务 asp 脚本漏洞

789、系统感染病毒后的现象有哪些？（ABCD）

A、系统错误或系统崩溃　　B、系统反应慢，网络拥塞

C、陌生的进程或服务　　D、陌生的自启动

三、判断题：（790-1000）

790、TCSEC 将信息安全风机防护等级一共分为 7 个安全等级：D、C1、C2、B1、B2、B3、A。(A)

A、正确　　B、错误

791、通用标准 v2 版（CC）的安全等级是以 EAL 来表示的。（A）

A、正确　　B、错误

792、一个企业的信息安全组织能否顺利开展工作（定期安全评估、日志安全巡检、定期安全审核、应急演练等），主要取决于公司领导对信息安全工作的认识程度和支持力度。（A）

A、正确　　B、错误

793、在信息安全领域，CIA 通常是指：保密性、完整性和可用性。（A）

A、正确　　B、错误

794、信息安全是永远是相对的，并且需要不断持续关注和改进，永远没有一劳永逸的安全防护措施。（A）

A、正确　　B、错误

795、在信息安全领域，CIA 通常是指：保密性、完整性和非抵赖性。（B）

A、正确　　B、错误

796、网络与信息都是资产，具有不可或缺的重要价值。（A）

A、正确　　B、错误

797、信息安全的威胁主体包括内部人员、准内部人员、外部人员、系统自身等方面。（B）

A、正确　　B、错误误

798、互联网网络安全事件根据危害和紧急程度分为一般、预警、报警、紧急、重大五种。（B）

A、正确　　B、错误

799、安全审计是从管理和技术两个方面检查公司的安全策略和控制措施的执行情况，发现安全隐患的过程。（A）

A、正确　　B、错误

800、网络与信息都是资产，具有不可或缺的重要价值。（A）

A、正确　　B、错误

801、计算机系统安全是指应用系统具备访问控制机制，数据不被泄露、丢失、篡改等。（B）

A、正确　　B、错误

802、主机加固完成后，一般可以有效保证主机的安全性增强。（A）

A、正确　　B、错误

803、黑客在进行信息收集时，通常利用 Windows 的 IPC 漏洞可以获得系统用户的列表的信息。（A）

A、正确　　B、错误

804、Solaris 系统中一般需要确认 ROOT 账号只能本地登录，这样有助于安全增强。（A）

A、正确　　B、错误

805、HP-UX 系统加固中在设置 ROOT 环境变量不能有相对路径设置。（A）

A、正确　　B、错误

806、屏幕保护的木马是需要分大小写。（B）

A、正确　　B、错误

807、安全审计就是日志的记录。（B）

A、正确　　B、错误误

808、HP-UX 系统加固中在设置通用用户环境变量不能有相对路径设置。（A）

A、正确　　B、错误

809、AIX 系统加固时，对系统配置一般需要自编脚本完成。（A）

A、正确　　B、错误

810、Windows NT 中用户登录域的口令是以明文方式传输的。（B）

A、正确　　B、错误

811、操作系统普通用户账号审批记录应编号、留档。（A）

A、正确　　B、错误

812、计算机病毒是计算机系统中自动产生的。（B）

A、正确　　B、错误

813、主机系统加固时根据专业安全评估结果，制定相应的系统加固方案，针对不同目标系统，通过打补丁、修改安全配置、增加安全机制等方法，合理进行安全性加强。（A）

A、正确　　B、错误

814、4A 系统的建设能够减轻账户管理员的维护工作。（A）

A、正确　　B、错误

815、4A 系统的接入管理可以管理到用户无力访问的接入。（B）

A、正确　　B、错误

816、Cisco 路由器可以使用 enable password 命令为特权模式的进入设置强壮的密码。（B）

A、正确　　B、错误

817、Cisco 设备的 AUX 端口默认是启用的。（A）

A、正确　　B、错误

818、DHCP 可以向终端提供 IP 地址、网关、DNS 服务器地址等参数。（A）

A、正确　　B、错误误

819、Inbound 方向的 NAT 使用一个外部地址来代表内部地址，用于隐藏外网服务器的实际

IP 地址。（B）

A、正确　　B、错误

820、IPS 设备即使不出现故障，它仍然是一个潜在的网络瓶颈，需要强大的网络结构来配合。（A）

A、正确　　B、错误

821、IPS 的过滤器规则不能自由定义。（B）

A、正确　　B、错误

822、IPS 的某些功能和防火墙类似。（A）

A、正确　　B、错误

823、IPS 和 IDS 都是主动防御系统。（B）

A、正确　　B、错误

824、NAT 是一种网络地址翻译的技术，它能是的多台没有合法地址的计算机共享一个合法的 IP 地址访问 Internet。（A）

A、正确　　B、错误

825、Netscreen 的 ROOT 管理员具有的最高权限，为了避免 ROOT 管理员密码被窃取后造成威胁，应该限制 ROOT 只能通过 CONSOLE 接口访问设备，而不能远程登录。(A)

A、正确　　B、错误

826、Netscreen 防火墙的外网口应禁止 PING 测试，内网口可以不限制。（B）

A、正确　　B、错误

827、OSI 是开放的信息安全的缩写。（B）

A、正确　　B、错误

828、OSI 七层模型中，传输层数据成为段（Segment），主要是用来建立主机端到端连接，包括 TCP 和 UDP 连接。（A）

A、正确　　B、错误

829、OSI 中会话层不提供机密性服务。（A）

A、正确　　B、错误

830、SSH 使用 TCP 79 端口的服务。（B）

A、正确　　B、错误

831、TCP/IP 模型从下至上分为四层：物理层，数据链路层，网络层和应用层。（B）

A、正确　　B、错误

832、TCP/IP 模型与 OSI 参考模型的不同点在于 TCP/IP 把表示层和会话层都归于应用层，所以 TCP/IP 模型从下至上分为五层：物理层，数据链路层，网络层，传输层和应用层。　（A）

A、正确　　B、错误

833、TCP/IP 协议体系结构中，IP 层对应 OSI/RM 模型的网络层。（A）

A、正确　　B、错误

834、默认情况下需要关闭 Cisco 设备的 Small TCP/UDP 服务。（A）

A、正确　　B、错误

835、缺省情况下，防火墙工作模式为路由模式，切换工作模式后可直接进行进一步配置。（B）

A、正确　　B、错误

836、入侵检测具有对操作系统的校验管理，判断是否有破坏安全的用户活动。（A）

A、正确　　B、错误

837、入侵检测可以处理数据包级的攻击。（B）

A、正确　　B、错误

838、入侵检测系统不能弥补由于系统提供信息的质量或完整性的问题。（A）

A、正确　　B、错误

839、入侵检测系统能够检测到用户的对主机、数据库的网络操作行为。（B）

A、正确　　B、错误

840、入侵检测系统是一种对计算机系统或网络事件进行检测并分析这个入侵事件特征的过程。（A）

A、正确　　B、错误

841、统计分析的弱点是需要不断的升级以对付不断出现的黑客攻击手法，不能检测到从未出现过的黑客攻击手段。（B）

A、正确　　B、错误

842、统计分析方法首先给系统对象（如用户、文件、目录和设备等）创建一个统计描述，统计正常使用时的一些测量属性（如访问次数、操作失败次数和延时等）。（A）

A、正确　　B、错误

843、透明代理服务器在应用层工作，它完全阻断了网络报文的传输通道。因此具有很高的

安全性。可以根据协议、地址等属性进行访问控制、隐藏了内部网络结构，因为最终请求是有防火墙发出的。外面的主机不知道防火墙内部的网络结构。解决 IP 地址紧缺的问题。使用代理服务器只需要给防火墙设置一个公网的 IP 的地址。（A）

A、正确　　B、错误

844、完整性分析的缺点是一般以批处理方式实现，不用于实时响应。（A）

A、正确　　B、错误

845、网络安全应具有以下四个方面的特征：保密性、完整性、可用性、可查性。（B）

A、正确　　B、错误

846、网络边界的 Cisco 路由器应关闭 CDP 服务。（A）

A、正确　　B、错误

847、网络边界 Cisco 设备的 CDP 协议可以开放。（B）

A、正确　　B、错误

848、网络层的防护手段（防火墙，SSL，IDS，加固）可以组织或检测到应用层攻击。（B）

A、正确　　B、错误

849、针对不同的攻击行为，IPS 只需要一个过滤器就足够了。（B）

A、正确　　B、错误

850、主机型 IDS 其数据采集部分当然位于其所检测的网络上。（B）

A、正确　　B、错误

851、状态检测防火墙检测每一个通过的网络包，或者丢弃，或者放行，取决于所建立的一套规则。（B）

A、正确　　B、错误

852、IPS 虽然能主动防御，但是不能坚挺网络流量。（B）

A、正确　　B、错误

853、防火墙安全策略定制越多的拒绝规则，越有利于网络安全。（B）

A、正确　　B、错误

854、审计系统进行关联分析时不需要关注日志时间。（B）

A、正确　　B、错误

855、垃圾邮件一般包括商业广告、政治邮件、病毒邮件、而已欺诈邮件（网络钓鱼）等几个方面。（A）

A、正确　　B、错误

856、防止网络窃听最好的方法就是给网上的信息加密，是的侦听程序无法识别这些信息模式。（A）

A、正确　　B、错误

857、侵检测的手机的被容包括系统、网络、数据及用户活动的状态和行为。（A）

A、正确　　B、错误

858、模式匹配就是将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较，从而发现违背安全策略的行为。（A）

A、正确　　B、错误

859、入侵防御是一种抢先的网络安全方法，可以用于识别潜在威胁并快速做出回应。（A）

A、正确　　B、错误

860、VPN 的主要特点是通过加密是信息安全的通过 Internet 传递。（A）

A、正确　　B、错误

861、传输层协议使用端口号（Port）来标示和区分上层应用程序，如：Telnet 协议用的是 23 号端口、DNS 协议使用 69 号端口。（B）

A、正确　　B、错误

862、如果 Web 应用对 URL 访问控制不当，可能造成用户直接在浏览器中输入 URL，访问不该访问的页面。（A）

A、正确　　B、错误

863、如果 Web 应用没有对攻击者的输入进行适当的编码和过滤，就用于构造数据库查询或操作系统命令时，可能导致注入漏洞。（A）

A、正确　　B、错误

864、HTTP 协议定义了 Web 浏览器向 Web 服务器发生 Web 页面请求的格式及 Web 页面在 Internet 上传输的方式。（A）

A、正确　　B、错误

865、HTTP 协议是文本协议，可利用回车换行做边界干扰。（A）

A、正确　　B、错误

866、Init<sid>.ora 文件是 Oracle 启动文件，任何参数的配置错误都会造成 Oracle 不能启动，任何参数的不合理配置都可能造成系统故障。（A）

A、正确　　B、错误

867、Mysqldump 是采用 SQL 级别的备份机制，它将数据表导成 SQL 脚本文件，在不同的

MySQL 版本之间升级时相对比较合适，这也是最常见的备份方法。（A）

A、正确　　B、错误

868、Orabrute 是进行远程破解 Oracle 密码的工具，要猜解的密码可以在 password.txt 中设置。（A）

A、正确　　B、错误

869、Oracle 的 SYS 账户在数据库中具有最高权限，能够做任何事情，包括启动/关闭 Oracle 数据库。即使 SYS 被锁定，也已然能够访问数据库。（A）

A、正确　　B、错误

870、Oracle 的若算法加密机制：两个相同的用户名和密码在两个不同的 Oracle 数据库机器中，将具有相同的哈希值。（A）

A、正确　　B、错误

871、Oracle 密码允许包含像“SELECT”，“DELETE”，“CREATE”这类的 Oracle/SQL 关键字。（B）

A、正确　　B、错误

872、Oracle 的 HTTP 的基本验证可选择 SYS 破解，因为它始终存在和有效。（A）

A、正确　　B、错误

873、Oracle 默认情况下，口令的传输方式是加密。（B）

A、正确　　B、错误

874、Oracle 数据库的归档日志不是在线日志的备份。（B）

A、正确　　B、错误

875、OSI 网络安全体系结构的八类安全机制分别是加密、数字签名、访问控制、数据完整性、鉴别交换、业务流填充、路由控制、公正。（A）

A、正确　　B、错误

876、OSI 网络安全体系结构的五类安全服务是鉴别、访问控制、保密性、完整性、抗否认。（A）

A、正确　　B、错误

877、SMTP 没有对邮件加密的功能是导致垃圾邮件泛滥的主要原因。（A）

A、正确　　B、错误

878、SQL Server 如果设置了不恰当的数据库文件权限，可能导致敏感文件被非法删除或读取，威胁系统安全。（A）

A、正确　　B、错误

879、SQL Server 数据库应禁止使用除 tcp/ip 以外的协议，保护数据库通信安全。（A）

A、正确　　B、错误

880、SQL Server 应该社会自日志审核无法追踪回溯安全事件。（A）

A、正确　　B、错误

881、Web 服务器一般省缺不允许攻击者访问 Web 根目录以外的内容，内容资源不可以任意访问。(A)

882、Web 攻击面不仅仅是浏览器中可见的内容。（A）

A、正确　　B、错误

883、Web 应用对网络通讯中包含的敏感信息进行加密，就不会被窃听。（B）

A、正确　　B、错误

884、暴力猜解不能对 Web 应用进行攻击。（B）

A、正确　　B、错误

885、在 Oracle 自身的配置上做限定方法是：修改$Oracle_HOME\network\admin 目录下面的 SQLNET..ORA 文件，类似设置如下：

Tcp_validnode_checking=YES

Tcp_invited_nodes=

(192.168.0.1,ip2,ip3•...)。

(A)

A、正确　　B、错误

886、不设置必要的日志审核，就无法追踪回溯安全事件，Oracle 中若果要审计记录成功的登陆语句”SQL>audit session whenever successful;”． (A)

A、正确　　B、错误

887、对目标网络进行扫描时发现，某一个主机开放了 25 和 110 端口，此主机最有可能是 DNS 服务器。（B）

A、正确　　B、错误

888、防止 XSS 各种方法都有优劣之处，防范 XSS 的真正挑战不在于全免，而在于细致。（B）

A、正确　　B、错误

889、访问控制、强制登陆、自动安全更新都属于 Window2000 的安全组件（B）

A、正确　　B、错误

890、复杂的系统存在大量的相互引用访问，如果开发者不能有效的进行权限控制，就可能被恶意引用。（A）

A、正确　　B、错误

891、攻击者可以通过 SQL 注入手段获取其他用户的密码。（A）

A、正确　　B、错误

892、几乎所有的关系数据库系统和相应的 SQL 语言都面临 SQL 注入的潜在威胁。（A)

A、正确　　B、错误

893、简单身份验证和安全层（Simple Authentication and Security Layer，SASL）是一种为系统账号提供身份验证和可选安全性服务的框架（B）

A、正确　　B、错误

894、默认可通过 Web 程序来远程管理 Oracle10g 数据库，端口是 8080.（A）

A、正确　　B、错误

895、如果 sa 是空口令，那就意味着攻击者可能侵入系统执行任意操作，威胁系统安全。（A）

A、正确　　B、错误

896、如果在 SQL Server 等领域成功并不意味这该用户已经可以访问 SQL Server 上的数据库。（A）

A、正确　　B、错误

897、如果知道 Oracle 密码长度，用 Rainbow 表生成器来破解其密码哈希值是绝对成功的。（A）

A、正确　　B、错误

898、所有操作系统、数据库、网络设备，包括一部分业务系统，均需要支持基于账号的访问控制功能。（B）

A、正确　　B、错误

899、网络拓扑分析为检查是否有配置错误项泄露内部 IP 地址，从而推断网站系统拓扑。（A）

A、正确　　B、错误

900、为 Oracle 数据库安全考虑，在对人共同对数据库进行维护时应依赖数据库预定义的传统角色。（B）

A、正确　　B、错误

901、为了维护数据库中数据的正确性和一致性，在对关系数据库执行插入、删除和修改操作时必须遵循三类完整性规则：实体完整性规则、引用完整性规则、用户定义的完整性规则。

(A)

A、正确　　B、错误

902、系统类型鉴别为检查主机系统与开放服务是否存在安全漏点。（B）

A、正确　　B、错误

903、系统漏洞扫描为检查目标的操作系统与应用系统信息。（B）

A、正确　　B、错误

904、选择远程破解 Oracle 的最好账户是 SYS，因为此账户永远有效。（A）

A、正确　　B、错误

905、一封电子邮件可以拆分成对个 IP 包，每个 IP 包可以沿不同的路径到达目的地。（A）

A、正确　　B、错误

906、一个共享文件夹。将它的 NTFS 权限设置为 sam 用户可以修改，共享权限设置为 sam 用户可以读取，当 sam 从网络访问这个共享文件夹的时候，他有读取的权限。（A）

A、正确　　B、错误

907、用 Sqlplus 登陆到 Oracle 数据库，使用 slesct username, password form dba_users 命令可查看数据库中的用户名和密码明文。（B）

A、正确　　B、错误

908、有的 Web 应用登陆界面允许攻击者暴力猜解口令，在自动工具与字典表的帮助下，可以迅速找到弱密码用户。（A）

A、正确　　B、错误

909、在 Oracle 所有版本在安装的时候都没有提示修改 SYS 的默认密码。（B）

A、正确　　B、错误

910、在 ORacle 数据库安装补丁时，不需要关闭所有与数据库有关的服务。（B）

A、正确　　B、错误

911、在 SQL Server 安装 SP3 补丁时不需要系统中已经安装了 SP1 或 SP2。（B）

A、正确　　B、错误

912、在 SQL Server 中具有 sysadmin 权限的用户可以通过 xp_cmdshell 存储扩展以 system 的权限执行任意系统命令。（A）

A、正确　　B、错误

913、Oracle 默认配置下，每个账户如果有 30 次的失败登陆，此账户将被锁定。（B）

A、正确　　B、错误

914、定制开发 Web 系统的安全度不如标准的产品。（A）

A、正确　　B、错误

915、对 MySQL 注入攻击时，经常用到注释符号#来屏蔽剩下的内置 SQL 语句。（A）

A、正确　　B、错误

916、一个登录名只能进入服务器，但是不能让用户访问服务器中的数据库资源。每个登录名的定义存放在 msater 数据库的 syslogins 表中。（A）

A、正确　　B、错误

917、Web 错误信息可能泄露服务器型号版本、数据库型号、路径、代码。（A）

A、正确　　B、错误

918、Oracle 的密码哈希值存储在 SYS.USER$表中。可以通过像 DBA USERS 这类的视图来访问。（A）

A、正确　　B、错误

919、产品的定制开发是应用安全中最薄弱的一环。（A）

A、正确　　B、错误

920、Oracle 限制了密码由英文字母，数字，#，下划线（_），美元字符（$）构成，密码的最大长度为 30 字符；并不能以”$”,”#”,”_”或任何数字开头。（A）

A、正确　　B、错误

921、网上营业厅对资源控制制的要求包括：应用软件对访问用户进行记录，当发现相同用户二次进行登录和操作，系统将要求二次认证，验证通过后提供服务。（B）

A、正确　　B、错误

922、计算机场地可以选择在公共区域人流量比较大的地方。（B）

A、正确　　B、错误

923、EMC 测试盒约束用户关心的信息信号的电磁发射、TEMPEST 只测试盒约束系统和设备的所有电磁发射。（B）

A、正确　　B、错误

924、加密传输是一种非常有效并经常使用的方法，也能解决输入和输出端的电磁信息泄露问题。（B）

A、正确　　B、错误

925、出现在导线或电器、电子设备上的超过线路或设备本身正常工作电压和电流并对线路或设备可能造成电气损害的电压和电流，称过电压和过电流。（B）

A、正确　　B、错误

926、红区：红新号的传输通道或单元电路称为红区，反之为黑区。（A）

A、正确　　B、错误

927、机房应设置相应的活在报警和灭火系统。（A）

A、正确　　B、错误

928、计算机机房的建设应当符合国家标准和国家有关规定。在计算机机房附近施工，不得危害计算机信息系统的安全。（A）

A、正确　　B、错误

929、计算机系统接地包括：直流地、交流工作地、安全保护地、电源零线和防雷保护地。（B）

A、正确　　B、错误

930、接地线在穿越墙壁、楼板和地坪时应套钢管或其他非金属的保护套管，钢管应与接地线做电气连通。（A）

A、正确　　B、错误

931、提到防雷，大家很容易联想到避雷针。其实我们平常看到的避雷针是用来保护房屋免遭雷电直击即防直击雷的。计算机信息系统的电子设备雷害一般有感应雷击产生，英因此防护的方法完全不一样。（A）

A、正确　　B、错误

932、在计算机机房附近施工，不负有维护计算机信息系统安全的责任和义务。（B）

A、正确　　B、错误

933、只要手干净就可以直接触摸或者插拔电路组件，不必有进一步的措施。（B）

A、正确　　B、错误

934、主管计算机信息系统安全的公安机关和城建及规划部门，应与设施单位进行协调，在不危害用户利益的大前提下，制定措施。合理施工，做好计算机信息系统安全保护工作。（B）

A、正确　　B、错误

935、防雷措施是在和计算机连接的所有外线上（包括电源线和通信线）加设专用防雷设备——防雷保安器，同时规范底线，防止雷击时在底线上产生的高电位反击。（A）

A、正确　　B、错误

936、对于公司机密信息必须根据公司的相关规定予以适当的标识。（A）

A、正确　　B、错误

937、信息网络的物理安全要从环境安全和设备安全两个角度来考虑。（A）

A、正确　　B、错误

938、如果在电话、电视会议中涉及讨论工伤机密信息，会议主持人或组织人在会议全过程中一定要确认每一个与会者是经授权参与的。（A）

A、正确　　B、错误

939、为防止信息非法泄露，需要销毁存储介质时，应该批准后自行销毁。（B）

A、正确　　B、错误

940、将公司的机密信息通过互联网络传送时，必须予以加密。（A）

A、正确　　B、错误

941、机密信息纸介质资料废弃应用碎纸机粉碎或焚毁。（A）

A、正确　　B、错误

942、有很高使用价值或很高机密程度的重要数据应采用加密等方式进行保密。（A）

A、正确　　B、错误

943、“一次一密”属于序列密码的一种。（A）

A、正确　　B、错误

944、3DES 算法的加密过程就是用一个秘钥对待加密的数据执行三次 DES 算法的加密操作。（B）

A、正确　　B、错误

945、AES 加密算法的秘钥长度为 128、192 或 256 位。（A）

A、正确　　B、错误

946、AES 是一种非对称算法。（B）

A、正确　　B、错误

947、DES3 和 RSA 是两种不同的安全加密算法，主要是用来对敏感数据进行安全加密。（A）

A、正确　　B、错误

948、Diffie-Hellman 算法的安全性取决于离散对数计算的困难性，可以实现秘钥交换。（A）

A、正确　　B、错误

949、DSS(Digital Signature Standard)是利用了安全散列函数（SHA）提出了一种数字加密技术。（A）

A、正确　　B、错误

950、MD5 是一种加密算法。（B）

A、正确　　B、错误

951、PGP 协议缺省的压缩算法是 ZIP，压缩后数据由于冗余信息很少，更容易抵御来自分析类型的攻击。（A）

A、正确　　B、错误

952、PKI 是一个用对称密码算法和技术来实现并提供安全服务的具有通用性的安全基础设施。（B）

A、正确　　B、错误

953、RC4 是典型的的序列密码算法。（A）

A、正确　　B、错误

954、RSA 算法作为主要的非对称算法，使用公钥加密的秘闻一定要采用公钥来街。（B）

A、正确　　B、错误

955、安全全加密技术分为两大类：对称加密技术和非对称加密技术。两者的主要区别是对称加密算法在加密、解密过程中使用同一个秘钥；而非对称加密算法在加密、解密过程中使用两个不同的秘钥。（A）

A、正确　　B、错误

956、常见的公钥密码算法有 RSA 算法、Diffie-Hellman 算法和 EIGamal 算法。（A）

A、正确　　B、错误

957、当通过浏览器一在线方式申请数字证书时，申请证书和下载证书的计算机必须是同一台计算机。（A）

A、正确　　B、错误

958、发送方使用 AH 协议处理数据包，需要对整个 IP 的数据包计算 MAC，包括 IP 头的所有字段和数据。（B）

A、正确　　B、错误

959、分组密码的优点是错误扩展小、速度快、安全程度高。（B）

A、正确　　B、错误

960、公共迷药密码体制在秘钥管理上比对称秘钥密码体制更安全。（A）

A、正确　　B、错误

961、古典加密主要采用的主要方法是置换，代换。（A）

A、正确　　B、错误

962、古典加密主要是对加密算法的保密，现代加密算法是公开的，主要是针对秘钥进行保密。（A）

A、正确　　B、错误

963、基于公开秘钥体制（PKI）的数字证书是电子商务安全体系的核心。（A）

A、正确　　B、错误

964、口令应在 120 天至少更换一次。（B）

A、正确　　B、错误

965、链路加密方式适用于在广域网系统中应用。（B）

A、正确　　B、错误

966、密码保管不善属于操作失误的安全隐患。（B）

A、正确　　B、错误

967、日常所见的校园饭卡是利用身份认证的单因素法。（A）

A、正确　　B、错误

968、身份认证要求对数据和信息来源进行验证，以确保发信人的身份。（B）

A、正确　　B、错误

969、身份认证与权限控制是网络社会的管理基础。（A）

A、正确　　B、错误

970、数据在传输过程中用哈希算法保证其完整性后，非法用户无法无法对数据进行任何修改。（B）

A、正确　　B、错误

971、数字签名比较的是摘要结果长度是否都是 128 位。（B）

A、正确　　B、错误

972、通信数据与文件加密是同一个概念。（B）

A、正确　　B、错误

973、为 AES 开发的 Rijndae1 算法的秘钥长度是 128 位，分组长度也为 128 位。（B）

A、正确　　B、错误

974、为了保证安全性，密码算法应该进行保密。（B）

A、正确　　B、错误

975、文件压缩变换是一个单向加密过程。（B）

A、正确　　B、错误

976、我的公钥证书不能在网络上公开，否则其他人可能冒充我的身份或伪造我的数字签名。（B）

A、正确　　B、错误

977、现代加密算法可以分为对称加密算法和非对称加密。（A）

A、正确　　B、错误

978、虚拟专用网 VPN 的关键技术主要是隧道技术、加解密技术、秘钥管理技术以及使用者与设备身份认证技术。（A）

A、正确　　B、错误

979、以当前的技术来说，RSA 体制是无条件安全的。（B）

A、正确　　B、错误

980、在 4A 系统的远期建设中，应用系统自身不需要保留系统从账户信息。（B）

A、正确　　B、错误

981、在 MD5 算法中，要先将以初始化的 A、B、C、D 这四个变量分别复制到 a、b、c、d 中。（A）

A、正确　　B、错误

982、在 MD5 算法中要用到 4 个变量，分别表示 A、B、C、D，均为 32 位长。（A）

A、正确　　B、错误

983、在 PKI 中，注册机构 RA 是必要的组件。（B）

A、正确　　B、错误

984、在 SSL 握手协议过程中，需要服务器发送自己的证书。（A）

A、正确　　B、错误

985、在非对称加密过程中，加密和解密使用的是不同的秘钥。（A）

A、正确　　B、错误

986、在公钥加密系统中，用公钥加密的密文可以由私钥解密，但用公钥加密的密文，不能用公钥解密。　（B）

A、正确　　B、错误

987、在密码学的意义上，只要存在一个方向，比暴力搜索秘钥还要更有效率，就能视为一

种“破解”。 （A）

A、正确 B、错误

988、账户管理的 Agent 不适用于在网络设备中部署。 （A）

A、正确 B、错误

989、整个 PKI 系统有证书服务器 AS、票据许可服务器 TGS、客户机和应用服务器四部分组成。 （B）

A、正确 B、错误

990、最基本的认证方式选择证书是数字证书。（B）

A、正确 B、错误

991、最小特权、纵深防御是网络安全原则之一。（A）

A、正确 B、错误

992、数字证书是由权威机构 CA 发行的一种权威的电子文档，是网络环境中的一种身份证。（A）

A、正确 B、错误

993、数字证书是由权威机构 PKI 发行的一种权威性的电子文档，是网络环境中的一种身份证。 （B）

A、正确 B、错误

994、信息加密技术是计算机网络安全技术的基础，为实现信息的保密性、完整性、可用性以及抗抵赖性提供了丰富的技术手段。（A）

A、正确 B、错误

995、病毒能隐藏在电脑的 CMOS 存储器里。（B）

A、正确 B、错误

996、对感染病毒的软盘进行浏览会导致硬盘被感染。（B）

A、正确 B、错误

997、已知某应用程序感染了文件型病毒，则该文件的大小变化情况一般是变小。（B）

A、正确 B、错误

998、重新格式化硬盘可以清楚所有病毒。（B）

A、正确 B、错误

999、专业安全评估服务对目标系统通过工具扫描和人工检查，进行专业安全的技术评定，并根据评估结果提供评估报告。 （A）

A、正确　　B、错误

1000、冒充信件回复、假装纯文字 ICON、冒充微软雅虎发信、下载电子贺卡同意书、是使用的叫做字典攻击法的方法。（B）

A、正确　　B、错误