

1.用户在电子商务网站上使用网上银行支付时,必须通过( )在 Internet 与 银行专用网之间进行数据交换。

- A.支付网关      B.防病毒网关      C.出口路由器      D.堡垒主机

2.防火墙通常分为内网、外网和 DMZ 三个区域,按照受保护程度,从低到高正确的排列次序为( )

- A.内网、外网和 DMZ      B.外网、DMZ 和内网      C.DMZ、内网和外网      D.内网、DMZ 和外网

3.包过滤防火墙对( )的数据报文进行检查。

- A.应用层      B.物理层      C.网络层      D.链路层

4.下列不能用于远程登录或控制的是( )。

- A.IGMP      B.SSH      C.Telnet      D.RFB

5.AES 是一种( )算法。

- A.公钥加密      B.流密码      C.分组加密      D.消息摘要

6.以下可以有效防治计算机病毒的策略是( )。

- A.部署防火墙      B.部署入侵检测系统      C.安装并及时升级防病毒软件      D.定期备份数据文件

7.通常使用( )为 IP 数据报文进行加密。

- A.IPsec      B.PPTP      C.HTTPS      D.TLS

8.SQL 是一种数据库结构化查询语言,SQL 注入攻击的首要目标是( )。

- A.破坏 Web 服务      B.窃取用户口令等机密信息  
C.攻击用户浏览器,以获得访问权限      D.获得数据库的权限

9.下列算法中属于非对称加密算法的是( )。

- A.DES      B.RSA      C.AES      D.MD5

10.下列攻击类型中,( )是以被攻击对象不能继续提供服务为首要目标

- A.跨站脚本      B.拒绝服务      C.信息篡改      D.口令猜测

11.下列协议中,属于安全远程登录协议的是( )。

- A.TLS      B.TCP      C.SSH      D.TFTP

12.所有资源只能由授权方或以授权的方式进行修改,即信息未经授权不能进行改变的特性是指信息的( )。

- A.完整性      B.可用性      C.保密性      D.不可抵赖性

13.访问控制是对信息系统资源进行保护的重要措施,适当的访问控制能够阻止未经授权的用户有意或者无意地获取资源。计算机系统中,访问控制的任务不包括( )。

- A.审计      B.授权      C.确定存取权限      D.实施存取权限

14. 以下关于认证和加密的叙述中，错误的是（ ）。

- A. 加密用以确保数据的保密性
- B. 认证用以确保报文发送者和接收者的真实性
- C. 认证和加密都可以阻止对手进行被动攻击
- D. 身份认证的目的在于识别用户的合法性，阻止非法用户访问系统

15. 某电子商务网站向 CA 申请了数字证书，用户可以通过使用（ ）验证（ ）的真伪来确定该网站的合法性。

问题 1: A. CA 的公钥      B. CA 的签名      C. 网站的公钥      D. 网站的私钥

问题 2: A. CA 的公钥      B. CA 的签名      C. 网站的公钥      D. 网站的私钥

16. Kerberos 系统中可通过在报文中加入（ ）来防止重放攻击。

- A. 会话密钥      B. 时间戳      C. 用户 ID      D. 私有密钥

17. 下列算法中，不属于公开密钥加密算法的是（ ）。

- A. ECC      B. DSA      C. RSA      D. DES

18. 下列协议中，与电子邮箱服务的安全性无关的是（ ）。

- A. SSL      B. HTTPS      C. MIME      D. PGP

19. 浏览器开启了无痕浏览模式后，（ ）依然会被保存下来。

- A. 浏览历史      B. 搜索历史      C. 下载文件      D. 临时文件

20. 震网（Stuxnet）病毒是一种破坏工业基础设施的恶意代码，利用系统漏洞攻击工业控制系统，是一种危害性极大的（ ）。

- A. 引导区病毒      B. 宏病毒      C. 木马病毒      D. 蠕虫病毒

21. 用户 A 和 B 要进行安全通信，通信过程需确认双方身份和消息不可否认。A 和 B 通信时可使用（ ）来对用户的身份进行认证；使用（ ）确保消息不可否认。

问题 1: A. 数字证书      B. 消息加密      C. 用户私钥      D. 数字签名

问题 2: A. 数字证书      B. 消息加密      C. 用户私钥      D. 数字签名

22. 下述协议中与安全电子邮箱服务无关的是（ ）。

- A. SSL      B. HTTPS      C. MIME      D. PGP

23. （ ）防火墙是内部网和外部网的隔离点，它可对应用层的通信数据流进行监控和过滤。

- A. 包过滤      B. 应用级网关      C. 数据库      D. Web

24. MD5 是（ ）算法，对任意长度的输入计算得到的结果长度为（ ）位。

问题 1: A. 路由选择      B. 摘要      C. 共享密钥      D. 公开密钥

问题 2: A. 56      B. 128      C. 140      D. 160

25. 计算机病毒的特征不包括（ ）。

- A. 传染性      B. 触发性      C. 隐蔽性      D. 自毁性

26.DES 是（ ）算法。

- A. 公开密钥加密      B. 共享密钥加密      C. 数字签名      D. 认证

27.攻击者通过发送一个目的主机已经接收过的报文来达到攻击目的，这种攻击方式属于（ ）攻击。

- A. 重放      B. 拒绝服务      C. 数据截获      D. 数据流分析

28.在网络安全管理中，加强内防内控可采取的策略有（ ）。

①控制终端接入数量

②终端访问授权，防止合法终端越权访问

③加强终端的安全检查与策略管理

④加强员工上网行为管理与违规审计

- A. ②③      B. ②④      C. ①②③④      D. ②③④

29.在安全通信中，S 将所发送的信息使用（ ）进行数字签名，T 收到该消息后可利用（ ）验证该消息的真实性。

问题 1: A.S 的公钥      B.S 的私钥      C.T 的公钥      D.T 的私钥

问题 2: A.S 的公钥      B.S 的私钥      C.T 的公钥      D.T 的私钥

30.网络管理员通过命令行方式对路由器进行管理，需要确保 ID、口令和会话内容的保密性，应采取的访问方式是（ ）。

- A. 控制台      B. AUX      C. TELNET      D. SSH

31.以下关于防火墙功能特性的叙述中，不正确的是（ ）。

- A. 控制进出网络的数据包和数据流向  
B. 提供流量信息的日志和审计  
C. 隐藏内部 IP 以及网络结构细节  
D. 提供漏洞扫描功能

32.（ ）不属于入侵检测技术。

- A. 专家系统      B. 模型检测      C. 简单匹配      D. 漏洞扫描

33.下列攻击行为中，属于典型被动攻击的是（ ）。

- A. 拒绝服务攻击      B. 会话拦截      C. 系统干涉      D. 修改数据命令

34.与 HTTP 相比，HTTPS 协议对传输的内容进行加密，更加安全。HTTPS 基于（ ）安全协议，其默认端口是（ ）。

问题 1: A.RSA      B.DES      C.SSL      D.SSH

问题 2: A.1023      B.443      C.80      D.8080

35.假定用户 A、B 分别在 I1 和 I2 两个 CA 处取得了各自的证书，下面（ ）是 A、B 互信的必要条件。

- A. A、B 互换私钥      B. A、B 互换公钥  
C. I1、I2 互换私钥      D. I1、I2 互换公钥

36.以下加密算法中适合对大量的明文消息进行加密传输的是（ ）。

- A.RSA    B.SHA-1    C.MD5    D.RC5

37.HTTPS 使用（ ）协议对报文进行封装

- A.SSH    B.SSL    C.SHA-1    D.SET

38.在网络设计和实施过程中要采取多种安全措施，其中（ ）是针对系统安全需求的措施。

- A.设备防雷击    B.入侵检测    C.漏洞发现与补丁管理    D.流量控制

39.（ ）不是数字签名的作用。

- A.接收者可验证消息来源的真实性  
B.发送者无法否认发送过该消息  
C.接收者无法伪造或篡改消息  
D.可验证接收者合法性

40.可用于数字签名的算法是（ ）。

- A.RSA    B.IDEA    C.RC4    D.MD5

41.传输经过 SSL 加密的网页所采用的协议是（ ）。

- A.HTTP    B.HTTPS    C.S-HTTP    D.HTTP-S

42.为了攻击远程主机，通常利用（ ）技术检测远程主机状态。

- A.病毒查杀    B.端口扫描    C.QQ 聊天    D.身份认证

43.防火墙不具备（ ）功能。

- A.记录访问过程    B.查毒    C.包过滤    D.代理

44.（ ）不属于主动攻击。

- A.流量分析    B.重放    C.IP 地址欺骗    D.拒绝服务

45.安全需求可划分为物理线路安全、网络安全、系统安全和应用安全。下面的安全需求中属于系统安全的是（ ），属于应用安全的是（ ）。

问题 1: A.机房安全    B.入侵检测    C.漏洞补丁管理    D.数据库安全

问题 2: A.机房安全    B.入侵检测    C.漏洞补丁管理    D.数据库安全

46.（ ）协议在终端设备与远程站点之间建立安全连接。

- A.ARP    B.Tenlnet    C.SSH    D.WEP

47.PPP 中的安全认证协议是（ ），它使用三次握手的会话过程传送密文。

- A.MD5    B.PAP    C.CHAP    D.HASH

48.（ ）不是蠕虫病毒。

- A.熊猫烧香    B.红色代码

C.冰河                      D.爱虫病毒

49.以下关于拒绝服务攻击的叙述中，不正确的是（ ）。

- A.拒绝服务攻击的目的是使计算机或者网络无法提供正常的服务
- B.拒绝服务攻击是不断向计算机发起请求来实现的
- C.拒绝服务攻击会造成用户密码的泄漏
- D.DDoS 是一种拒绝服务攻击形式

50.网络系统中，通常把（ ）置于 DMZ 区。

- A.网络管理服务器      B.Web 服务器      C.入侵检测服务器      D.财务管理服务器

51.以下关于包过滤防火墙和代理服务防火墙的叙述中，正确的是（ ）。

- A.包过滤成本技术实现成本较高，所以安全性能高
- B.包过滤技术对应用和用户是透明的
- C.代理服务技术安全性较高，可以提高网络整体性能
- D.代理服务技术只能配置成用户认证后才建立连接

52.防火墙的工作层次是决定防火墙效率及安全的主要因素，以下叙述中，正确的是（ ）。

- A.防火墙工作层次越低，工作效率越高，安全性越高
- B.防火墙工作层次越低，工作效率越低，安全性越低
- C.防火墙工作层次越高，工作效率越高，安全性越低
- D.防火墙工作层次越高，工作效率越低，安全性越高

53.以下关于木马程序的叙述中，正确的是（ ）。

- A.木马程序主要通过移动磁盘传播
- B.木马程序的客户端运行在攻击者的机器上
- C.木马程序的目的是使计算机或网络无法提供正常的服务
- D.Sniffer 是典型的木马程序

54.下列算法中，不属于公开密钥加密算法的是（ ）。

- A.ECC      B.DSA      C.RSA      D.DES

55.PKI 体制中，保证数字证书不被篡改的方法是（ ）。

- A.用 CA 的私钥对数字证书签名
- B.用 CA 的公钥对数字证书签名
- C.用证书主人的私钥对数字证书签名
- D.用证书主人的公钥对数字证书签名

56.下列网络攻击行为中，属于 DoS 攻击的是（ ）。

- A.特洛伊木马攻击
- B.SYN Flooding 攻击
- C.端口欺骗攻击
- D.IP 欺骗攻击

57.近年来,在我国出现各类病毒中( )病毒通过木马形式感染智能手机。

- A.欢乐时光    B.熊猫烧香    C.X 卧底    D.CIH

58.防火墙通常分为内网、外网和 DMZ 三个区域,按照受保护程序,从高到低正确的排列次序为( )。

- A.内网、外网和 DMZ    B.外网、内网和 DMZ    C.DMZ、内网和外网    D.内网、DMZ 和外网

59.利用报文摘要算法生成报文接要的目的是( )。

- A.验证通信对方的身份防止假冒  
B.对传输数据进行加密防止数据被窃听  
C.防止发送言否认发送过数据  
D.防止发送的报文被篡改

60.用户 B 收到用户 A 带数字签名的消息 M,为了验证 M 的真实性,首先需要从 CA 获取用户 A 的数字证书,并利用( )验证该证书的真伪,然后利用( )验证 M 的真实性。

问题 1: A.CA 的公钥    B.B 的私钥    C.A 的公钥    D.B 的公钥

问题 2: A.CA 的公钥    B.B 的私钥    C.A 的公钥    D.B 的公钥

61.下列安全协议中,与 TLS 最接近的协议是( )。

- A.PGP    B.SSL    C.HTTPS    D.IPSec

62.IIS6.0 支持的身份验证安全机制有 4 种验证方法,其中安全级别最高的验证方法是( )。

- A.匿名身份验证    B.集成 Windows 身份验证    C.基本身份验证    D.摘要式身份验证

63.甲和乙要进行通信,甲对发送的消息附加了数字签名,乙收到该消息后利用( )验证该消息的真实性。

- A.甲的公钥    B.甲的私钥    C.乙的公钥    D.乙的私钥

64.从认证中心 CA 获取用户 B 的数字证书,该证书用( )作数字签名;从用户 B 的数字证书中可以获得 B 的公钥。

- A.CA 的公钥    B.CA 的私钥    C.B 的公钥    D.B 的私钥

65.通过内部发起连接与外部主机建立联系,由外部主机控制并盗取用户信息的恶意代码为( )。

- A.特洛伊木马    B.蠕虫病毒    C.宏病毒    D.CIH 病毒

66.利用( )可以获取某 FTP 服务器中是否存在可写目录的信息。

- A.防火墙系统    B.漏洞扫描系统    C.入侵检测系统    D.病毒防御系统

67.在 IE 浏览器中,安全级别最高的区域设置是( )。

- A.Internet    B.本地 Intranet    C.可信任站点    D.受限站点

68.宏病毒一般感染以( )为扩展名的文件。

- A.EXE    B.COM    C.DOC    D.DLL

69.用户 A 从 CA 获得用户 B 的数字证书,并利用( )验证数字证书的真实性。

- A.B 的公钥    B.B 的私钥    C.CA 的公钥    D.CA 的私钥

70.公钥体系中，私钥用于（ ），公钥用于（ ）。

问题 1: A.解密和签名 B.加密和签名 C.解密和认证 D.加密和认证

问题 2: A.解密和签名 B.加密和签名 C.解密和认证 D.加密和认证

71.下列选项中，防范网络监听最有效的方法是（ ）。

A.安装防火墙 B.采用无线网络传输 C.数据加密 D.漏洞扫描

72.ARP 攻击造成网络无法跨网段通信的原因是（ ）。

A.发送大量 ARP 报文造成网络拥塞  
B.伪造网关 ARP 报文使得数据包无法发送到网关  
C.ARP 攻击破坏了网络的物理连通性  
D.ARP 攻击破坏了网关设备

73.如果使用大量的连接请求攻击计算机，使得所有可用的系统资源都被消耗殆尽，最终计算机无法再处理合法用户的请求，这种手段属于（ ）攻击。

A.拒绝服务 B.口令入侵 C.网络监听 D.IP 欺骗

74.杀毒软件报告发现病毒 Macro.Melissa，由该病毒名称可以推断病毒类型是（ ），这类病毒主要感染目标是（ ）。

问题 1: A.文件型 B.引导型 C.目录型 D.宏病毒

问题 2: A.EXE 或 COM 可执行文件 B.Word 或 Excel 文件 C.DLL 系统文件 D.磁盘引导区

75.驻留在多个网络设备上的程序在短时间内同时产生大量的请求消息冲击某 Web 服务器，导致该服务器不堪重负，无法正常响应其他合法用户的请求，这属于（ ）。

A.网上冲浪 B.中间人攻击 C.DDoS 攻击 D.MAC 攻击

76.相对于 DES 算法而言，RSA 算法的（ ），因此，RSA（ ）。

问题 1:

A.加密密钥和解密密钥是不相同的 B.加密密钥和解密密钥是相同的  
C.加密速度比 DES 要高 D.解密速度比 DES 要高

问题 2:

A.更适用于对文件加密 B.保密性不如 DES  
C.可用于对不同长度的消息生成消息摘要 D.可以用于数字签名

77.感染“熊猫烧香”病毒后的计算机不会出现（ ）的情况。

A.执行文件图标变成熊猫烧香  
B.用户信息被泄漏  
C.系统运行变慢  
D.破坏计算机主板

78.多形病毒指的是（ ）的计算机病毒。

A.可在反病毒检测时隐藏自己 B.每次感染都会改变自己  
C.可以通过不同的渠道进行传播 D.可以根据不同环境造成不同破坏

79.下列行为不属于网络攻击的是（ ）。

- A.连续不停 Ping 某台主机
- B.发送带病毒和木马的电子邮件
- C.向多个邮箱群发一封电子邮件
- D.暴力破解服务器密码

80.下面关于防火墙的说法，正确的是（ ）。





- A.防火墙一般由软件以及支持该软件运行的硬件系统构成
- B.防火墙只能防止未经授权的信息发送到内网
- C.防火墙能准确地检测出攻击来自哪一台计算机
- D.防火墙的主要支撑技术是加密技术

81.如果希望别的计算机不能通过 ping 命令测试服务器的连通情况，可以（ ）。如果希望通过默认的 Telnet 端口连接服务器，则下面对防火墙配置正确的是（ ）。

问题 1:

- A.删除服务器中的 ping.exe 文件
- B.删除服务器中的 cmd.exe 文件
- C.关闭服务器中 ICMP 端口
- D.关闭服务器中的 Net Logon 服务

问题 2:

- A. 
- B. 
- C. 
- D. 

82.计算机感染特洛伊木马后的典型现象是（ ）。

- A.程序异常退出
- B.有未知程序试图建立网络连接
- C.邮箱被垃圾邮件填满
- D.Windows 系统黑屏



83.网络安全包含了网络信息的可用性、保密性、完整性和网络通信对象的真实性。其中,数字签名是对( )的保护。

- A.可用性    B.保密性    C.连通性    D.真实性

84.下面关于漏洞扫描系统的叙述,错误的是( )。

- A.漏洞扫描系统是一种自动检测目标主机安全弱点的程序  
B.黑客利用漏洞扫描系统可以发现目标主机的安全漏洞  
C.漏洞扫描系统可以用于发现网络入侵者  
D.漏洞扫描系统的实现依赖于系统漏洞库的完善

85.某网站向 CA 申请了数字证书,用户通过( )来验证网站的真伪。

- A.CA 的签名    B.证书中的公钥    C.网站的私钥    D.用户的公钥

86.包过滤防火墙对数据包的过滤依据不包括( )。

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

87.网络安全体系设计可从物理线路安全、网络安全、系统安全、应用安全等方面来进行。其中,数据库容灾属于( )。

- A.物理线路安全和网络安全  
B.物理线路安全和应用安全  
C.系统安全和网络安全  
D.系统安全和应用安全