1、 数据保密性安全服务的基础是（）。

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

2、 数字签名要预先使用单向 Hash 函数进行处理的原因是（）。

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

3、 （）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

4、 包过滤型防火墙原理上是基于（）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

5、 VPN 的加密手段为（）。

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

6、（）通过一个使用专用连接的共享基础设施，连接企业总部、远程办事处和分支机构。

A. Access VPN　B. Intranet VPN　C. Extranet VPN　D. Internet VPN

7、 计算机病毒是计算机系统中一类隐藏在（）上蓄意破坏的捣乱程序。

A. 内存　　B. 软盘　　C. 存储介质　　D. 网络

8、 “公开密钥密码体制”的含义是（）。

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

9、“会话侦听和劫持技术”是属于（）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

10、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（）。

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

11、 在 ISO/OSI 定义的安全体系结构中，没有规定（）。

A. 对象认证服务　　B.数据保密性安全服务

C. 访问控制安全服务　　D. 数据可用性安全服务

12、 PKI 的主要组成不包括（）。

A. 证书授权 CA　　B. SSL

C. 注册授权 RA　　D. 证书存储库 CR

13、下列选项中能够用在网络层的协议是（）。

A. SSL　B. PGP　C. PPTP　D. IPSec

14、（）协议是一个用于提供 IP 数据报完整性、身份认证和可选的抗重播保护的机制，但不提供数据机密性保护。

A. AH 协议　B. ESP 协议　C. IPSec 协议　D. PPTP 协议

15、IPSec 协议中负责对 IP 数据报加密的部分是（）。

A. 封装安全负载（ESP）　　B. 鉴别包头（AH）

C. Internet 密钥交换（IKE）　　D. 以上都不是

16、SSL 产生会话密钥的方式是（）。

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

17、为了降低风险，不建议使用的 Internet 服务是（）。

A. Web 服务　　B. 外部访问内部系统

C. 内部访问 Internet　　D. FTP 服务

18、火墙用于将 Internet 和内部网络隔离，（）。

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

19、 属于第二层的 VPN 隧道协议有（）。

A. IPSec　　B. PPTP　　C.GRE　　D. 以上皆不是

20、不属于隧道协议的是 C)。

A. PPTP　　B. L2TP　　C. TCP/IP　　D. IPSec

21、 PPTP 和 L2TP 最适合于（）。

A. 局域网　　B. 企业内部虚拟网

C. 企业扩展虚拟网　　D. 远程访问虚拟专用网

22、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

（）。

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’））

23、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. 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

24、CA 属于 ISO 安全体系结构中定义的（）。

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

25、目前，VPN 使用了（）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

26、IPSec VPN 不太适合用于（）。

A、已知范围的 IP 地址的网络

B、固定范围的 IP 地址的网络

C、动态分配 IP 地址的网络

D、TCP/IP 协议的网络

27、 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. 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

28、 从安全属性对各种网络攻击进行分类，截获攻击是针对（）的攻击。

A. 机密性　B. 可用性　C. 完整性　D. 真实性

29、最新的研究和统计表明，安全攻击主要来自（）。

A. 接入网　　B. 企业内部网　　C. 公用 IP 网　　D. 个人网

30、用于实现身份鉴别的安全机制是（）。

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

31、 一般而言，Internet 防火墙建立在一个网络的（）。

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

32、VPN 的英文全称是（）。

A. Visual Protocol Network　　B. Virtual Private Network

C. Virtual Protocol Network　　D. Visual Private Network

33、 信息安全的基本属性是（）。

A. 机密性　　B. 可用性

C. 完整性　　D. 上面 3 项都是

34、ISO 安全体系结构中的对象认证服务，使用（）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

35、 传输层保护的网络采用的主要技术是建立在（）基础上的（）。

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

36、以下（）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

37、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（）。

A. 内联网 VPN　B. 外联网 VPN　　C. 远程接入 VPN　　D. 无线 VPN

38、 窃听是一种（）攻击，攻击者（）将自己的系统插入到发送站和接收站之间。截获是一种（）攻击，攻击者（）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

39、不属于 VPN 的核心技术是（）。

A. 隧道技术　　B. 身份认证　　C. 日志记录　　D. 访问控制

40、（）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

41、 拒绝服务攻击的后果是（）。

A. 信息不可用　B. 应用程序不可用

C. 系统宕机　D. 阻止通信

42、通常所说的移动 VPN 是指（）。

A. Access VPN　B. Intranet VPN

C. Extranet VPN　D. 以上皆不是