单选题 每道1分，共30道（简单10道，一般10道，困难10道） 30分

双选题 每道2分，共10道（简单3道， 一般3道， 困难4道 ） 20分

判断题 每道1分，共30道（简单10道，一般10道，困难10道） 30分

主观题 每道5分，共4道 （简单1道， 一般1道， 困难2道 ） 20分

【单选题 导入60道 （简单20道，一般20道，困难20道） 】

【双选题 导入20道 （简单6道，一般7道，困难7道） 】

【判断题 导入60道 （简单20道，一般20道，困难20道） 】

【主观题 导入10道 （简单3道，一般3道，困难4道） 】

## 单选题

1 （）不是数字证书的功能。

A.保证交易者身份的真实性 B.保证交易的不可否认性

C.保证数据的完整性 D.保证系统的可靠性

2 数据的（ ）是指保护网络中存储和传输数据不被非法改变。

A完整性 B 结构化 C 共享性 D独立性

3 由于IP协议提供无连接的服务，在传送过程中若发生差错就需要（ ）协议向源节点报告差错情况，以便源节点对此做出相应的处理。

A. RARP B. TCP C.ICMP D. UDP

4 网络认证协议Kerberos v5所采用的加密算法是\_\_\_\_。

A.RSA B.MD5 C.三重DES D.RC4

5 按实现原理不同将防火墙分为\_\_\_\_\_\_\_\_\_\_3类。

A. 包过滤防火墙、应用层网关防火墙和状态检测防火墙

B. 包过滤防火墙、应用层网关防火墙和代理防火墙

C．包过滤防火墙、代理防火墙和软件防火墙

D．状态检测防火墙、代理防火墙和动态包过滤防火墙

6 网络系统的故意威胁中，以下哪个不是主动攻击类型（ ）。

A.窃取

B.中断

C.篡改

D.伪造

【主动攻击：更改信息和拒绝用户使用资源的攻击，攻击者对某个连接中通过的 PDU 进行各种处理。被动攻击：截获信息的攻击，攻击者只是观察和分析某一个协议数据单元 PDU 而不干扰信息流。】

7 \_\_\_\_\_\_\_\_系统是一种自动检测远程或本地主机安全性弱点的程序。

A．入侵检测 B．防火墙 C．漏洞扫描 D．入侵防护

8数据在存储或传输时不被修改、破坏，或数据包的丢失、乱序等是指：

A 数据完整性

B 数据一致性

C 数据同步性

D 数据源发性

9由一台过滤路由器与外部网络相连，再通过一个可提供安全保护的主机与外部网络相连，这是一种( )体系的防火墙。

A.包过滤防火墙 B. 主机过滤防火墙

C.代理服务器防火墙 D. 子网过滤防火墙

10 加密工具PGP用的是杂合加密算法，从下面列表中选出一正确答案。

A RSA和对称加密算法

B Diffie-Hellman和传统加密算法

C Elgamal和传统加密算法

D RSA和Elgamal

11 下列关于防火墙的说法中错误的是\_\_\_\_\_\_\_\_\_\_。

A. 防火墙无法阻止来自防火墙内部的攻击

B. 防火墙可以防止感染病毒的程序或文件的传输

C. 防火墙通常由软件和硬件组成

D. 防火墙可以记录和统计网络利用数据以及非法使用数据的情况

12 网络操作系统主要解决的问题是（ ）。

A．网络用户使用界面

B．网络资源共享与网络资源安全访问限制

C．网络资源共享

D．网络安全防范

13在对称密钥体制中，根据加密方式的不同又可分为：

A分组密码方式和密钥序列方式

B 分组密码方式和序列密码方式

C 序列密码方式和数据分组方式

D 密钥序列方式和数据分组方式

14 一般机房的洁净度要求灰尘颗粒直径小于\_\_\_\_\_\_\_μm。

A、0.3 B、0.4 C、0.5 D、0.6

15在通信系统的每段链路上对数据分别进行加密的方式称为：

A 链路层加密

B 节点加密

C 端对端加密

D 连接加密

16 windowsNT的域用户验证是在OSI参考模型的哪一层提供安全保护的？

A 应用层

B 表示层

C 会话层

D 传输层

17 在Windows的网络属性配置中，“默认网关”应该设置为\_\_\_\_\_\_\_\_的地址。

A．路由器 B. Web服务器 C. DNS服务器 D. 交换机

18 在\_\_\_\_\_\_\_模式下使用命令：service password-encrytion，可将路由器的用户口令从明文密码变为密文密码。

A、用户 B、特权 C、端口 D、全局

19 在网络排除故障时不使用的命令是\_\_\_\_\_\_\_\_\_。

A. ping B. netstat C. traceroute D. dir

20 数字证书不包含以下哪项内容？（ ）

A 公匙的有效期 B 数字证书的级别

C 数字证书的序列号 D 证书拥有者的信息和公匙

21 确保学校局域网的信息安全，防止来自Internet的黑客入侵，采用\_\_\_\_\_\_以实现一定的防范作用。

A) 防火墙 B) 邮件列表 C) 网管软件 D) 杀毒软件

22 下列关于加密的说法中，不正确的是( )。

A）3重DES是一种对称加密算法

B）RivestCipher5是一种不对称加密算法

C）不对称加密算法又称为公开密钥算法，其密钥是公开的

D）RSA和Elgamal是常用的公钥体制

23 对网络用户来说，操作系统是指（ ）。

A．能够运行自己应用软件的平台

B．提供一系列的功能、接口等工具来编写和调试程序的裸机

C．一个资源管理者

D．实现数据传输和安全保证的计算机环境

24 张三从安全认证中心CA得到了李四的数字证书，张三可以从该数字证书中得到李四的\_\_\_\_

A.数字签名 B. 公钥 C.口令 D. 私钥

25 在操作系统安全机制中访问控制系统一般包括：（ ）。

A、主体、客体、安全访问策略

B、实体、虚体、安全访问策略

C、主体、客体、隔离控制

D、实体、虚体、隔离控制

26 IP地址131.107.254.255属于哪一类的地址

A A类

B B类

C C类

D D类

27 WindowsNT的安全体系基于哪种安全模式

A 企业

B 域

C 工作组

D 可信

~~27以下哪些是网络扫描工具：~~

~~A SATAN~~

~~B Snoop~~

~~C firewall-2~~

~~D NETXRay~~

28防火墙系统中应用的包过滤技术应用于OSI七层结构中的

A 物理层

B 网络层

C 会话层

D 应用层

29哪种防火墙类型的安全级别最高：

A 屏蔽路由器型

B 双重宿主主机型

C 被屏蔽子网型

D 被屏蔽主机型

30 如果加密密钥和解密密钥相同或接近，这样的密码系统称为（ ）系统。

A.对称密码 B.非对称密码 C.公钥密码 D.分组密码

31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 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

32数据信息是否被篡改由哪些技术来判断：

A 数据完整性控制技术

B 身份识别技术

C 访问控制技术

D 入侵检测技术

33 对于数字签名，下面说法错误的是：

A 数字签名可以是附加在数据单元上的一些数据

B 数字签名可以是对数据单元所作的密码变换

C数字签名技术能够用来提供诸如抗抵赖与鉴别等安全服务

D数字签名机制可以使用对称或非对称密码算法

34网络级安全所面临的主要攻击是：

A窃听、欺骗

B 自然灾害

C 盗窃

D 网络应用软件的缺陷

35 针对TCP层上的安全协议，微软推出了SSL2的改进版本称为：

A TLSP

B PCT

C SSL3

D MS SSL

36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？

A、缓冲区溢出 B、地址欺骗

C、拒绝服务 D、暴力攻击

37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？

A、文件服务器 B、邮件服务器

C、WEB 服务器 D、DNS 服务器

38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？

A、ping B、nslookup

C、tracert D、ipconfig

39以下关于 VPN 的说法中的哪一项是正确的？

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

40 以下哪个不是属于 window2000 的漏洞？

A、 unicode

B、 IIS hacker

C、 输入法漏洞

D、 单用户登陆

41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？

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

42以下关于 window NT 4.0的服务包的说法正确的是？

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

43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

44 SSL安全套接字协议所使用的端口是：

A、 80

B、 443

C、 1433

D、 3389

45 Window2000 域或默认的身份验证协议是：

A、 HTML

B、 Kerberos V5

C、 TCP/IP

D、 Apptalk

46在 Linux 下 umask的八进制模式位 6 代表：

A、 拒绝访问

B、 写入

C、 读取和写入

D、 读取、写入和执行

47以下不属于 win2000 中的 ipsec过滤行为的是：

A、 允许

B、 阻塞

C、 协商

D、 证书

48 以下关于对称加密算法 RC4 的说法正确的是：

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

49 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

B、—D

C、—S

D、—INPUT

50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

51 中央网络安全和信息化领导小组的组长是（ ）

A.习近平

B.李克强

C.刘云山

D.周小川

52 数据完整性指的是（ 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

53 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

54 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

55 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

56 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

57 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

58 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

59 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

60 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

## 双选题

1 防火墙的主要功能包括

A 包过滤

B 代理

C 用户身份验证

D 网络级服务

2 防火墙一般可以提供四种服务，它们是

A 服务控制

B 网络控制

C 目录控制

D 行为控制

3 从网络高层协议角度，网络攻击可以分为

A 主动攻击

B 被动攻击

C 服务攻击

D 拒绝服务攻击

4 入侵检测技术主要有

A 数据挖掘技术

B 滥用检测技术

C 异常检测技术

D 蜜罐技术

5 网络安全的基本属性是

A 可用性

B 不可重复性

C 完整性

D 不可靠性

6 关于加密和签名，下列说法正确的是

A 加密用对方的公钥

B 签名用自己的公钥

C 加密用自己的公钥

D 签名用自己的私钥

7 在TCP/IP协议体系结构中，传输层有哪些协议

A IP

B TCP

C UDP

D arp

8 加密技术的重要方法有

A 封装

B数据加工

C 验证

D身份认证

9 数据加密的方式有

A 主机加密

B 传输加密

C 链路加密

D 节点加密

10 下列说法错误的是

A 密码学包括密码编码学和密码分析学

B PGP是一个基于RSA公钥加密体系的电子邮件加密软件。

C ping命令是通过arp协议实现的

D 入侵检测系统一般放在防火墙的前面

11以下不属于对称加密算法的是？

A、 DES

B、 RC4

C、 HASH

D、 RSA

12. 在建网时，设计 IP 地址方案首先要（ ）。

A. 给每一硬件设备分配一个 IP 地址 B. 选择合理的 IP 寻址方式

C. 保证 IP 地址不重复 D. 动态获得 IP 地址时可自由安排

13 网络按通信方式分类，可分为（ ）。

A、点对点传输网络

B、广播式传输网络

C、数据传输网

D、对等式网络

14下列说法中属于 ISO/OSI 七层协议中应用层功能的是（ ）。

A、拥塞控制

B、电子邮件

C、防止高速的发送方的数据把低速的接收方淹没

D、目录查询

15如果发现网络变得很慢， 经过观察，发现网络冲突增加很多， 以下哪些情况会引起此类故障 （ ）。

A、电缆太短

B、有网卡工作不正常

C、网络流量增大

D、电缆断路

16 按 TCSEC 安全级别的划分， C1 级安全具有的保护功能有：

A 保护硬件不受到损害 B 系统通过帐号和口令来识别用户是否合法

C 能控制进入系统的用户访问级别 D 决定用户对程序和信息拥有什么样的访问权

17 应用层主要的安全需求是：

A. 身份认证 B. 防止物理破坏 C. 访问控制 D. 防止人为攻击

18 下列加密算法哪些是属于非对称密钥的加密算法？

A 三重 DES B IDEA （国际数据加密标准）

C RSA 算法 D Diffie-Hellman 密钥交换算法

19 数字签名普遍用于银行、电子贸易等，数字签名的特点有哪些？

A 数字签名一般采用对称加密技术 B 数字签名随文本的变化而变化

C 与文本信息是分离的

D 数字签名能够利用公开的验证算法进行验证，安全的数字签名方案能够防止伪造。

20 下列哪些属于数据完整性控制技术？

A 报文认证 B 用户身份认证 C 通信完整性控制 D 口令加密

## 判断题

1 通信加密的两种方式是链路加密和端-端加密【对】

2 被动攻击的特点是偷听或监视传送，其目的是获得信息内容(或正在传送的信息)【对】

3 网络安全特征有不可靠性、完整性、可用性、保密性和不可否认性。【错，可靠】

4 Windows NT的安全管理主要包括账号规则、用户权限规则、审核规则和域管理机制等。【对】

5 计算机病毒对计算机网络系统威胁不大。【否】

6 在非对称密钥密码体制中，发信方与收信方使用不同的密钥。【是】

7 在PGP中用户之间没有信任关系 【否】

8 对路由器的配置可以设置用户访问路由器的权限。【是】

9 在windowsNT操作系统中，域间的委托关系有单向委托和双向委托两种。【是】

10 防火墙中应用的数据包过滤技术是基于数据包的ip地址及TCP端口号的而实现对数据过滤的 【是】

11 病毒只能以软盘作为传播的途径。【否】

12 计算机系统的脆弱性主要来自于网络操作系统的不安全性。【是】

13 Kerberos能为分布式计算机环境提供对用户单方进行验证的方法。 【否】

14 数字证书是由CA认证中心签发的 【是】

15 windowsNT中用户登录域的口令是以明文方式传输的。 【错】

16 禁止使用活动脚本可以防范IE执行本地任意程序 【对】

17 网络中的每个节点（包含了主机、交换机、路由器等）都必须配置ip地址 【错】

18 VPN的主要特点是通过加密使信息能安全的通过internet传递 【对】

19 POP3指邮局协议是一种邮件接收协议。 【对】

20 目前入侵检测系统可以及时的阻止黑客的攻击。 【错】

21 只要选择一种最安全的操作系统，整个系统就可以保障安全。【错】

22 安全审计就是日志的记录 【错】

23 我们通常使用SMTP协议用来接收E-mail 【错】

24 路由器在转发ip分组时，一般不检查ip分组的源地址，因此可以伪造ip分组的源地址进行攻击，使得网络管理员无法追踪。 【对】

25 在设计系统安全策略时要首先评估可能受到的安全威胁 【对】

26 为提高工作效率，外单位人员可以随意接入公司内网。【错】

27 发起大规模的DDos攻击通常要控制大量的中间网络或系统 【对】

28 计算机网络是计算机技术和通信技术结合而形成的一种新的通信形式【对】

29 蠕虫、特洛伊木马和病毒其实是一回事。【错】

30 安全管理从范畴上讲，涉及物理安全策略、访问控制策略、信息加密策略和网络安全管理策略。【对】

（ 对）31．城域网采用 LAN 技术。

（错 ）32．TCP/IP 体系有 7 个层次， ISO/OSI 体系有 4 个层次。

（ 错）33．ARP 协议的作用是将物理地址转化为 IP 地址。

（ 对）34. 在差分曼彻斯特编码技术中，不需要增加额外的同步时钟。

（ 错）35．从理论上说，局域网的拓扑结构应当是指它的物理拓扑结构。

（ 对）36. 在 10Mb/s 共享型以太网系统中，站点越多，带宽越窄。

（ 错）37．ADSL 技术的缺点是离交换机越近，速度下降越快。

（ 错）38. TCP 连接的数据传送是单向的。

（ 对）39. 匿名传送是 FTP 的最大特点。

（ 错）40. 网络管理首先必须有网络地址，一般可采用实名制地址。

41防止发送数据方发送数据后否认自已发送过的数据是一种抗抵赖性的形式。 【对】

42 Kerberos 协议是建立在非对称加密算法 RAS 上的 【否】

43 PEM 是专用来为电子邮件提供加密的 【对】

44当一个网络中的主机太多时，可以将一个大网络分成几个子网。 【对】

45操作系统中超级用户和普通用户的访问权限没有差别。 【错】

46保护帐户口令和控制访问权限可以提高操作系统的安全性能 【对】

47审计和日志工具可以记录对系统的所有访问， 可以追踪入侵者的痕迹， 能够找出系统的安全漏动。 【对】

48访问控制是用来控制用户访问资源权限的手段【对】

49防火墙可以用来控制进出它们的网络服务及传输数据。 【对】

50在 NetWare 操作系统中，使用 NIS 提供的层次式的分配和管理网络访问权的办法 【错】

51 近年来，中国在互联网领域的竞争力和话语权逐渐增强，但与发达国家相比仍有差距 【对】

52 《网络安全法》从草案发布到正式出台，共经历了三次审议、两次公开征求意见和修改【对】

53 社会工程学攻击是利用人性弱点（本能反应、贪婪、易于信任等）进行欺骗获取利益的攻击方法【对】

54 服务式攻击就是让被攻击的系统无法正常进行服务的攻击方式 【对】

55 如果计算机后门尚未被入侵，则可以直接上传恶意程序【错】

56 中国信息安全认证中心（ ISCCC）不是我国信息安全管理基础设施之一。 【错】

57 Who is 是一个标准服务，可以用来查询域名是否被注册以及注册的详细资料【对】

58 端口扫描的原理是通过端口扫描确定主机开放的端口，不同的端口对应运行着的不同的网络服务【对】

59 欺骗攻击（ Spoofing ）是指通过伪造源于可信任地址的数据包以使一台机器认证另一台机器的复杂技术 【对】

60 SQL 注入的防御对象是所有内部传入数据 【错】

## 主观题

1 简述SSL协议在通信对话进行安全保护的实现过程。

答：实现过程主要有6个阶段：①接通阶段，客户机通过网络向服务器打招呼，服务器回应。②密码交换阶段，客户机与服务器之间交换双方许可的密码。③会话密码阶段，客户机与服务器之间产生彼此交流的会话密码。④检验阶段，客户机检查服务器取得的密码。⑤客户认证阶段，服务器验证客户机的可信度⑥结束阶段，客户机与服务器之间相互交换结束信息。

2 防火墙按技术分类有哪些？

答： 防火墙的技术分类，可以分为包过滤型和应用代理型两大类。

3 计算机病毒有哪些危害？

答：

①对计算机数据信息的直接破坏作用②占用磁盘空间和对信息的破坏 ③抢占系统资源 ④影响计算机运行速度⑤计算机病毒错误与不可预见的危害⑥计算机病毒的兼容性对系统运行的影响

4 简述面对黑客攻击的防范措施。

答：黑客攻击防范措施有做好计算机的安全设置、隐藏IP地址、关闭不必要的端口、更换管理员账户、安装必要的安全软件、经常升级系统版本、不要回复陌生人的邮件、做好IE的安全设置、及时备份重要数据、使用加密机制传输数据等多个方面。

5 P2DR模型中的P、P、D、R的含义是什么？

答：Policy（安全策略）、Protection（防护）、Detection（检测）、Response（相应）。

6网络安全的含义是什么？

答：网络安全是指利用各种网络管理、控制和技术措施，使网络系统的硬件、软件及其系统中的数据资源受到保护，不因一些不利因素影响而使这些资源遭到破坏、更改、泄露，保证网络系统连续、可靠、安全地运行。

7 OSI网络安全体系涉及几个方面?网络安全服务和安全机制各有哪几项?

答：OSI安全体系结构主要包括网络安全机制和网络安全服务两个方面的内容。(2分)网络安全服务：鉴别服务，访问控制服务，数据完整性服务，数据保密性服务，非否认服务。网络安全机制：加密机制，数字签名机制，访问控制机制，数据完整性机制，交换鉴别机制，息量填充机制，路由控制机制，公证机制。(3分)

8网络安全的特性是什么？

答：网络安全的特性：保密性、完整性、可用性、可控性和可审查性。

9身份认证的技术方法有哪些？

答：常用的身份认证技术主要包括：基于秘密信息的身份认证方法和基于物理安全的身份认证方法。①基于秘密信息的身份认证方法。包括口令认证、单向认证、双向认证和零知识认证等。②基于物理安全的身份认证方法。如身份证、护照、指纹和人像等。

10简介网络安全评估的主要技术

答：网络安全评估的主要技术有：1端口扫描技术。2操作系统探测技术 3漏洞扫描技术4渗透测试技术