一 判断题（在本题的每一小题的括号中，正确的填入√，错误的填入 X。每题 2 分）

1. (F)网络软件的漏洞和“后门”没有区别。
2. (F)网络物理威胁中的身份识别错误与身份鉴别威胁具有相同的意义。
3. (T)电子窃听不一定要把窃听设备安装在线路上。
4. (F)特洛依木马程序不需要安装便可运行，并按照编制者的意图行事。
5. (T)计算机网络通信安全即数据在网络中的传输过程的安全，是指如何保证信息在网络传输过程中不被旁路与不被攻击的问题。
6. (F)通信数据加密与文件加密是同一个概念。
7. (F)设置非常安全的站点，可以避免被破坏。
8. (F)DES 密码体系中加密和解密使用的是相同的算法，加密和解密时所采用的密钥也是相同的。
9. (F)块加密具有比流加密更高的安全性。
10. (F)RSA 密码体系只能用于数据加密和解密，不能用于数字签名。
11. (F)RSA 采用的是著名的也是理论上较为成功的私钥密码体系。
12. (F)流量填充机制保持流量基本恒定，提供针对网络窃听的保护。
13. (F)只是从被感染磁盘上复制文件到硬盘上并不运行其中的可执行文件不会使系统感染病毒.
14. (F)将文件的属性设为只读不可以保护其不被病毒感染.
15. (T)VBS 脚本病毒一般是直接通过自我复制来感染文件的，病毒中的绝大部分代码都可以直接附加在其他同类程序的中间.
16. (T)不是所有的引导型病毒都攻击 BOOT 扇区或主引导扇区.
17. (T)蠕虫病毒是指一个程序（或一组程序），它会自我复制、传播到别的计算机系统中去.
18. (F)Outlook Express 中仅仅预览邮件的内容而不打开邮件的附件是不会中毒.
19. (F)Windows NT 网络中域控制器(Domain Controller)起控制域名解析的作用.
20. (F)当服务器遭受到 DoS (Denial of Service)攻击的时候,只需要重启动系统就可以阻止攻击.
21. (T)一般情况下, 采用 Port scan 可以比较快速地了解某台主机上提供了哪些网络服务.
22. (F)Internet 设计之初，考虑了核战争的威胁，因此充分考虑到了网络安全问题
23. (T)统计表明，网络安全威胁主要来自内部网络，而不是 Internet
24. (F)蠕虫、特洛伊木马和病毒其实是一回事
25. (F)只要设置了足够强壮的口令，黑客不可能侵入到计算机中
26. (T)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。
27. (T)发起大规模的 DDoS 攻击通常要控制大量的中间网络或系统
28. (T)路由协议如果没有认证功能，就可以伪造路由信息，导致路由表混乱，从而使网络瘫痪
29. (F)目前入侵检测系统可以及时的阻止黑客的攻击。
30. (T)通过伪造用户的 DNS 请求的

响应报文，可以把用户对目标域名的访问引入到一个伪造的站点，实现域名欺骗。

31. (F)Windows NT 中用户登录域的口令是以明文方式传输的
32. (F)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
33. (F)Smurf 攻击是通过将目的地址设置为被攻击者的地址造成的
34. (T)脚本语言病毒可以通过网络主动传播
35. (F)蠕虫只能通过邮件传播
36. (T)红色代码、尼姆达 Nimda 病毒、口令蠕虫可以造成网络阻塞
37. (F)包过滤防火墙主要是防范应用层的攻击
38. (F)通过信息交流服务器实现的逻辑隔离，由于只允许特定的信息通过，所以可以代理物理隔离
39. (T)防火墙要处理应用层的内容，首先需要进行数据包重组
40. (T)VPN 的所采取的两项关键技术是认证与加密
41. (F)网络安全防范是一个目标而不是一个过程
42. (T)防火墙的安全防范被动性表现在防范策略的配置是预先制定的
43. (T)基于网络的入侵检测就是通过连接在网络上的站点捕获网上的包，并分析其是否具有已知的攻击模式,以此来判别是否为入侵者。当驱动引擎发现某些可疑的现象时会向中心控制台产生告警信号
44. (T)基于主机的入侵检测的主要作用是实时监视可疑的连接、系统日志检查，非法访问的闯入等
45. (T)IDS 与 FW 互动是通过 IDS 发起控制命令而 FW 执行控制指令
46. (T)信息加密就是将信息的一种表现形式经过一种变换变成另一种表现形式
47. (T)加密技术中验证这一重要环节采用的关键技术是数字签名
48. (T)加密技术中封装这一重要环节采用的关键技术仅是摘要算法
49. (F)摘要算法不属于非对称算法
50. (T)摘要算法是不可逆的
51. (F)一个摘要算法对不同长度的文字进行运算所得的结果长度是不同的
52. (T)PKI 是公开密钥体系
53. (F)数字签名主要使用的算法是对称加密算法
54. (F)对称加密时，密钥只需要在加密信息解密时使用
55. (F)不使用密钥的变换就一定不是加密算法
56. (T)公钥与私钥总是成对出现的
57. (F)RSA 算法作为主要的非对称算法，使用公钥加密的密文一定要采用公钥来解
58. (T)CA 的主要内容是签发机构对用户公钥的签名
59. (F)数字签名比较的是摘要结果长度是否都是 128 位的
60. (F)通常密钥的长度越长的算法安全性就越高
61. (T)512、1024、2048 位密钥通常为非对称加密使用的密钥
62. (F)文件压缩变换是一个单向加密过程
63. (T)SSL 协议是安全套接字层协议
64. (T)CA 是注册的认证机构

信息安全导论 复习题

二 选择题（在本题的每一小题的备选答案中，请把你认为正确答案的题号，填入题干的括号内。多选不给分。每题 2 分）

1. DES 算法中的密钥长度为：（3）
   ①32 位 ②48 位 ③56 位 ④64 位
2. A 用户向 B 用户发送信息，并且要实现身份鉴别的功能，可以按照如下方法：(4)
   ①发送方用 A 用户的公钥加密，接收方用 B 用户的私钥解密
   ②发送方用 A 用户的私钥加密，接收方用 B 用户的公钥解密
   ③发送方用 A 用户的公钥加密，接收方用 A 用户的私钥解密
   ④发送方用 A 用户的私钥加密，接收方用 A 用户的公钥解密
3. 关于 IPSec 的协议，下列哪种论述是错误的：（3）
   ①AH 协议可以提供完整性保护和认证的功能
   ②ESP 协议不仅提供完整性保护和认证的功能，还可以提供保密功能
   ③AH 协议在传输模式下不能穿越 NAT，在隧道模式下可以穿越 NAT
   ④隧道模式比传输模式占用更大的带宽
4. 在 CIDF 中，完成入侵检测信息收集工作的部件是：(3)
   ①R 盒 ②D 盒 ③E 盒 ④A 盒
5. 关于防火墙技术，下列哪种论述是错误的：（4）
   ①静态包过滤技术允许外部客户与内部主机的直接连接
   ②动态包过滤技术允许动态地打开和关闭端口，也允许动态地增加和删除过滤规则
   ③应用级网关技术必须理解应用层协议，对每一种应用都要有专门的代理实现
   ④电路级网关技术能够识别在同一个协议栈上运行的不同的应用
6. 在 DES 加密方法中，每一个数据加密分组的长度为……（ ① ）
   ①64 位 ②56 位 ③48 位 ④32 位
7. 在 DES 加密方法中，密钥的原始长度为……（ ① ）
   ①64 位 ②56 位 ③48 位 ④32 位
8. 在 DES 加密方法中，密钥去除奇偶校验位后的长度为……（ ② ）
   ①64 位 ②56 位 ③48 位 ④32 位
9. 经过多少轮就能完成一次 DES 加密……（ ④ ）
   ①56 ②48 ③32 ④16
10. ESP 中，认证数据的大小必须是多少的倍数……（ ③ ）
    ①8 ②16 ③32 ④64
11. IP 认证头为 IP 包提供的安全服务不包括……（ ④ ）
    ①无连接完整性 ②数据源认证
    ③防重放攻击保护 ④密钥管理
12. 我国国家标准《计算机信息安全保护等级划分准则》将计算机信息系统安全保护等级划分成几个级别……（ ② ）
    ①4 ②5 ③6 ④7

13. 为了抵御网络攻击，Windows NT 5.0 所提出的网络安全性方案是……（ ③ ）
①EFS ②Kerberos
③IP Security ④Service Pack
14. SQL 杀手蠕虫病毒发作的特征是什么 A
①大量消耗网络带宽
②攻击个人 PC 终端
③破坏 PC 游戏程序
④攻击手机网络
15. 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：1234
①实体安全
②运行安全
③信息安全
④人员安全
16. 关于 80 年代 Mirros 蠕虫危害的描述，哪句话是错误的？2
①该蠕虫利用 Unix 系统上的漏洞传播
②窃取用户的机密信息，破坏计算机数据文件
③占用了大量的计算机处理器的时间，导致拒绝服务
④大量的流量堵塞了网络，导致网络瘫痪
17. telnet 协议在网络上明文传输用户的口令，这属于哪个阶段的安全问题？1
①协议的设计阶段
②软件的实现阶段
③用户的使用阶段
④管理员维护阶段
18. 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? 3
①微软公司软件的设计阶段的失误
②微软公司软件的实现阶段的失误
③系统管理员维护阶段的失误
④最终用户使用阶段的失误
19. 以下关于 DOS 攻击的描述，哪句话是正确的？3
①不需要侵入受攻击的系统
②以窃取目标系统上的机密信息为目的
③导致目标系统无法处理正常用户的请求
④如果目标系统没有漏洞，远程攻击就不可能成功
20. 以下关于垃圾邮件泛滥原因的描述中，哪些是错误的？3
①早期的 SMTP 协议没有发件人认证的功能
②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

③SMTP 没有对邮件加密的功能是导致垃圾邮件泛滥的主要原因

④Internet 分布式管理的性质，导致很难控制和管理

21. 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？3

①安装防火墙

②安装入侵检测系统

③给系统安装最新的补丁

④安装防病毒软件

22. 世界上最早的应急响应组是什么？3

①CCERT

②FIRST

③CERT/CC

④APCERT

23. 以下关于 Smurf 攻击的描述，那句话是错误的？4

①它是一种拒绝服务形式的攻击

②它依靠大量有安全漏洞的网络作为放大器

③它使用 ICMP 的包进行攻击

④攻击者最终的目标是在目标计算机上获得一个帐号

24. 网络操作系统应当提供哪些安全保障 1234

①验证(Authentication)

②授权(Authorization)

③数据保密性(Data Confidentiality)

④数据一致性(Data Integrity)

25. Windows NT 的"域"控制机制具备哪些安全特性？123

①用户身份验证

②访问控制

③审计(日志)

④数据通讯的加密

26. 从系统整体看，安全"漏洞"包括哪些方面 123

①技术因素

②人的因素

③规划，策略和执行过程

27. 造成操作系统安全漏洞的原因 123

①不安全的编程语言

②不安全的编程习惯

③考虑不周的架构设计

28. 严格的口令策略应当包含哪些要素 123

①满足一定的长度，比如 8 位以上

②同时包含数字，字母和特殊字符

③系统强制要求定期更改口令

④用户可以设置空口令

29. 下面哪一个情景属于身份验证（Authentication）过程 1

①用户依照系统提示输入用户名和口令

②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

③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

④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

30. 下面哪一个情景属于授权（Authorization）2

①用户依照系统提示输入用户名和口令

②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

③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

④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

31. 下面哪一个情景属于审计（Audit）4

①用户依照系统提示输入用户名和口令

②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

③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

④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

32. BO 是 1

①蠕虫

②系统漏洞

③后门

33. 红色代码是 2

①只是蠕虫

②蠕虫病毒

③普通病毒

34. 3389 端口开放所引起的是 3

①操作系统漏洞

②数据库漏洞

③输入法漏洞

35. NMAP 是 2

①网络协议

②扫描工具

③防范工具

36. 邮件炸弹攻击主要是 2

② 破坏被攻击者邮件服务器

②填满被攻击者邮箱

③破坏被攻击者邮件客户端

37. 扫描工具 3

①只能作为攻击工具

②只能作为防范工具

③既可作为攻击工具也可以作为防范工具

38. 缓冲区溢出 3

①只是系统层漏洞

②只是应用层漏洞

③既是系统层漏洞也是应用层漏洞

39. DOS 攻击的 Smurf 攻击是利用____进行攻击 1

①其他网络

②通讯握手过程问题

③中间代理

40. DDOS 攻击是利用_____进行攻击 3

①其他网络

②通讯握手过程问题

③中间代理

41. DOS 攻击的 Syn flood 攻击是利用_____进行攻击 2

①其他网络

②通讯握手过程问题

③中间代理

42. 计算机病毒能够_____123

①破坏计算机功能或者毁坏数据

②影响计算机使用

③能够自我复制

④保护版权

43. 计算机病毒的特点_____134

①传染性

②可移植性

③破坏性

④可触发性

44. 计算机病毒按传染方式分为____234

①良性病毒

②引导型病毒

③文件型病毒

④复合型病毒

45. 文件型病毒可以通过以下途径传播 123

①文件交换

②邮件

③网络

④系统引导

46. 宏病毒感染以下类型的文件 134

①DOC

②EXE

③XLS

④DOT

47. 以下哪些措施可以有效提高病毒防治能力 1234

①安装、升级杀毒软件

②升级系统、打补丁

③提高安全防范意识

④不要轻易打开来历不明的邮件

48. 木马程序常用的激活方式有____1234

① 修改注册表中的 HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion 下所有以“run”开头的键值

②修改 Win.ini 中的 windows 字段中有启动命令“load=”和“run=”

③修改文件关联

④修改 System.ini 中的启动项

49. 以下哪些病毒可以通过网络主动传播 1234

①红色代码病毒

②尼姆达病毒

③口令蠕虫病毒

④CIH 病毒

50. 计算机病毒的主要传播途径有 1234

①电子邮件

②网络

③存储介质

④文件交换

51. VPN 是指 1

①虚拟的专用网络
②虚拟的协议网络
③虚拟的包过滤网络

52. 防火墙主要可以分为 1
①包过滤型、代理性、混合型
②包过滤型、系统代理型、应用代理型
③包过滤型、内容过滤型、混合型

53. 包过滤型防火墙检查的是数据包的 1
①包头
②包内容
③包头和内容

54. 代理型防火墙的主要特征是 2
①不需要认证
②需要认证
③可以认证也可以不认证

55. 代理型防火墙较包过滤型防火墙 3
①效率高
②功能全
③性能高

56. NAT 是指 2
①网络地址传输
②网络地址转换
③网络地址跟踪

57. 包过滤规则 1
①可以按协议设置
②不可以按协议设置
③一般不按协议设置

58. 在安全区域划分中 DMZ 区通常用做 2
①数据区
②对外服务区
③重要业务区

59. 目前用户局域网内部区域划分通常通过____实现 2
①物理隔离
②Vlan 划分
③防火墙防范

60. 防火墙的部署 2
①只需要在与 Internet 相连接的出入口设置
②在需要保护局域网络的所有出入口设置

③需要在出入口和网段之间进行部署

61. 目前的防火墙防范主要是 2
    ①主动防范
    ②被动防范
    ③不一定
62. 防火墙 3
    ①能够防止外部和内部入侵
    ②不能防止外部入侵而能内部入侵
    ③能防止外部入侵而不能防止内部入侵
63. 代理服务器通常在_____实现 3
    ①网络层
    ②传输层
    ③应用层
64. 目前的 IDS 的防范作用主要是 1
    ①主动防范
    ②被动防范
    ③不一定
65. IDS 的基本流程是信息收集_____、_____、____、执行对策 1
    ①分析器、模式匹配器、对策生成
    ②模式匹配器、分析器、对策生成
    ③对策生成、分析器、模式匹配器
66. IDS 的基本机构包括 3
    ①网络监视中心、引擎、通讯三部分
    ②管理控制中心、数据分析器、通讯三部分
    ③管理控制中心、引擎、通讯三部分
67. IDS 与 FW 互动是 3
    ①IDS 与 FW 互相发控制信息
    ②FW 向 IDS 发控制信息
    ③IDS 向 FW 发控制信息
68. 信息的加密保存、加密传输主要是为了 2
    ①防止抵赖、防止窃取、防止假冒
    ②防止篡改、防止窃取、防止假冒
    ③防止抵赖、防止窃取、防止篡改
69. 加密技术的三个重要方法是 3
    ①数据加工、变换、验证
    ②封装、变换、身份认证
    ③封装、变换、验证
70. 加密算法分为 2

② 对称加密与数字签名

②对称加密与非对称加密

③非对称加密与摘要

71. 对称加密需要____个密钥 2

①0

②1

③2

72. 非对称加密需要 _____对密钥 3

①1 或 2

②0 或 2

③0 或 1

73. 常见的对称加密算法有 1

①DES、TripleDES、RC2、RC4

②RSA、椭圆算法

③MD5、SHA

74. 常见的摘要加密算法有 3

①DES、TripleDES、RC2、RC4

②RSA、椭圆算法

③MD5、SHA

75. 身份认证需要解决的关键问题和主要作用是 2

①身份的确认、应用的限制

②身份的确认、权利的控制

③应用的限制、权利控制

76. PKI 体系所遵循的国际标准是 2

①ISO 17799

②ISO X.509

③ISO 15408

77. 目前身份认证采用的主要标式为 1

①CA 证书、用户名/密码、指纹、虹膜、设备特征

②CA 证书、用户名/密码、指纹、DNA、系统特征

③CA 证书、用户名/密码、DNA、虹膜、信息特征

78. 典型的邮件加密的过程一是发送方和接收方交换 2

①双方私钥

②双方公钥

③双方通讯的对称加密密钥

79. SSL 是_____层加密协议 3

①网络

②通讯

③应用

80. “信息安全”中“安全”通常是指信息的 4
    ①保密性
    ②完整性
    ③可用性
    ④以上三者都是
81. “信息安全”中的“信息”是指 3
    ①以电子形式存在的数据
    ②计算机网络
    ③信息本身、信息处理设施、信息处理过程和信息处理者
    ④软硬件平台
82. 信息安全风险应该是以下哪些因素的函数？1
    ①信息资产的价值、面临的威胁以及自身存在的脆弱性等
    ②病毒、黑客、漏洞等
    ③保密信息如国家秘密、商业秘密等
    ④网络、系统、应用的复杂程度
83. Some virus will modify registry to auto-load when computer reboot . Which registry key may be modifed by virus to auto-load. (Choose all possible answers.) 1
    ① hkey_local_machine\software\microsoft\windows\currentversion\run
    ② hkey_local_machine\software\microsoft\windows\currentversion\runonce
    ③ hkey_local_machine\software\microsoft\windows\currentversion\runservices
    ④ hkey_local_machine\software\microsoft\windows\currentversion\runservicesonce
84. 有一主机专门被用作内部网和外部网的分界线。该主机里插有两块网卡，分别连接到两个网络。防火墙里面的系统可以与这台主机进行通信，防火墙外面的系统（Internet 上的系统）也可以与这台主机进行通信，但防火墙两边的系统之间不能直接进行通信,这是_____的防火墙。 3
    ① 屏蔽主机式体系结构
    ② 筛选路由式体系结构
    ③ 双网主机式体系结构
    ④ 屏蔽子网（Screened SubNet）式体系结构
85. 数据加密技术可以应用在网络及系统安全的哪些方面？ 4
    ① 数据保密
    ② 身份验证
    ③ 保持数据完整性
    ④ 以上都正确
86. 漏洞评估产品在选择时应注意_____。 4
    ① 是否具有针对网络、主机和数据库漏洞的检测功能
    ② 产品的扫描能力

③ 产品的评估能力

④ 以上都正确

87. 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____。 2

① 比较法

② 特征字的识别法

③ 搜索法

④ 分析法

88. 下列说法不正确的是_____。 4

① 安防工作永远是风险、性能、成本之间的折衷。

② 网络安全防御系统是个动态的系统，攻防技术都在不断发展。安防系统必须同时发展与更新。

③ 系统的安全防护人员必须密切追踪最新出现的不安全因素和最新的安防理念，以便对现有的安防系统及时提出改进意见

④ 建立 100%安全的网络

89. 关于网络入侵监测的主要优点，哪个不正确。 4

① 发现主机 IDS 系统看不到的攻击

② 攻击者很难毁灭证据

③ 快速监测和响应

④ 独立于操作系统

90. 关于主机入侵监测的主要缺点，哪个不正确。 4

① 看不到网络活动

② 运行审计功能要占用额外资源

③ 主机监视感应器不通用

④ 对加密通信无能为力

91. 对新建的应用连接，状态检测检查预先设置的安全规则，允许符合规则的连接通过，并在内存中记录下该连接的相关信息，生成状态表。对该连接的后续数据包，只要符合状态表，就可以通过。这种防火墙技术称为_____。 2

① 包过滤技术

② 状态检测技术

③ 代理服务技术

④ 以上都不正确

92. 有关对称密钥加密技术的说法，哪个是确切的？ 1

① 又称秘密密钥加密技术，收信方和发信方使用相同的密钥。

② 又称公开密钥加密，收信方和发信方使用的密钥互不相同

③ 又称秘密密钥加密技术，收信方和发信方使用不同的密钥

④ 又称公开密钥加密，收信方和发信方使用的密钥互不相同

93. 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_____？ 2

① 特洛伊木马

② DDos 攻击

③ 邮件炸弹

④ 逻辑炸弹

94. 某种网络安全威胁是通过非法手段取得对数据的使用权，并对数据进行恶意地添加和修改。这种安全威胁属于 2

①窃听数据 ②破坏数据完整性

③拒绝服务 ④物理安全威胁

95. 在公钥密码体系中，下面哪个（些）是不可以公开的？3

①公钥 ②公钥和加密算法

③私钥 ④私钥和加密算法

96. 以下网络攻击中，哪种不属于主动攻击？3

①重放攻击 ②拒绝服务攻击

③通信量分析攻击 ④假冒攻击

97. PGP 是一种电子邮件安全方案，它一般采用的散列函数是 2

①DSS ②RSA ③DES ④SHA

98. 如果每次打开 Word 程序编辑文档时，计算机都会把文档传送到一台 FTP 服务器，那么可以怀疑 Word 程序已经被黑客植入 3

①蠕虫 ②FTP 服务程序 ③特洛伊木马 ④陷门

99. IPSec 不能提供以下哪种服务？4

①流量保密 ②数据源认证

③拒绝重放包 ④文件加密

100. 电子商务应用系统由 4 部分构成，它们是 CA 安全认证系统、业务应用系统、用户及终端系统和 3

①防火墙系统 ②入侵检测系统

③支付网关系统 ④统一的一站式购物系统

三 填空题（每空 2 分）

1. 信息保障模型 IA 的四个方面包括：保护、检测、（反映）和（恢复）。
2. 信息安全的三个基本方面包括保密性、（完整性）和（可用性）。
3. 在共享式以太网中，可以将某台主机的网卡设置为（混杂）工作模式，达到监听网络数据的目的。
4. 通过发送超长 ICMP ECHO 数据包达到攻击目的的攻击方法称为（ping to death），通过打开大量半开的 TCP 连接达到攻击目的的攻击方法称为（SYN Flood），通过发送包长为负值的 IP 数据包达到攻击目的的攻击方法称为（Teardrop）。
5. 防火墙体系结构可分为双宿/多宿主机模式、（屏蔽主机模式）和（屏蔽子网模式）。
6. IPChains 内建的缺省规则链是（input）、（output）和（foward）。

7. 入侵检测按照分析方法可分为（异常检测）模型和（误用检测）模型。
8. 网络常见的不安全因素有（环境，资源共享，数据传输，计算机病毒，网络管理）
9. 网络安全的特征有：（保密性，完整性，可用性，可控性）
10. 写出下列术语的全称（中文或英文）：PKI（公开密钥体系）、SET（安全电子交易协议）、 PPTP（点对点隧道协议）
11. 写出下列术语的全称（中文或英文）： IKE（Intenet 密钥交换协议）、SSL（Secure Socket Layer）
12. 参加 SET 协议支付系统的主要成员有：（持卡人，商家，发卡行，收单行，支付网关，认证中心）
13. PGP 协议提供的业务具有以下 5 个主要特征：（ ）
14. 攻击常分为主动攻击和被动攻击两大类，主动攻击有（伪装，回答，修改报文，拒绝服务）;被动攻击有（监听） P26
15. SSL 协议能够抵抗： （重发攻击 中间人攻击 流量分析攻击 SYN flooding）
16. IKE 中的 Cookie 交换用来抗击 ：（中间人攻击 DOS 攻击 重发攻击 IP 伪装）
17. NAT 技术具有以下作用：（缓解 ip 地址不足的压力）、（向局域网外部隐藏内部主机的 ip 地址）、（过滤 ip 地址）、（流量均衡）
18. 当前有哪些协议用于 LAN 间的 VPN：（IPSEC）、（L2TP）、（PPTP ）、（MPLS）
19. MPLS 是一种在骨干网上提供快速交换的技术，它还易于提供：（网络安全 ）（VPN ）（QoS 保证 ）（IP 流量工程）
20. 安全关联有（传输模式）和（隧道模式）两种模式。
21. 网络的安全机制包括加密机制、访问控制机制、（数据完整性）机制、数字签名机制、（交换鉴别）机制、公证机制、（流量填充）机制和路由控制机制。
22. 网络通信在传输过程中可能会有截获、窃听。（篡改）和（伪造）四种攻击类型发生。
23. 防止网络窃听最好的方法就是给网上的信息（加密），使得侦听程序无法识别这些信息模式。
24. 加密可以提高终端和网络通信的安全，有链接加密、（节点加密）和（首尾加密）三种方法加密传输数据。
25. HTTP 在 TCP/IP 协议栈中属于（应用层）。
26. 浏览器向 Web 服务器提交表单数据的方式有（POST）和（GET）两种方式。
27. 第一代防火墙技术使用的是在 IP 层实现的（报文过滤）技术。
28. 根据所加密的数据形式，可将对称加密技术分为（块加密）和（流加密）。
29. 数字签名机制可以解决的安全问题包括（否认）、冒充、（伪造）和篡改。
30. 用于保护 IP 包内容的安全协议有两种指定协议，它们是（认证头或 AH）和（封装安全有效载荷或者 ESP）。