1. 状态检测防火墙什么时候实施规则变更备份？
   A. 防火墙变更之前
   B. 防火墙变更之后
   C. 作为完全备份的一部分
   D. 作为增量备份的一部分

2. FTP 的风险？
   A. 没有目标认证
   B. 明文传输

3. VOIP 在语音通信过程当中，弱点?
   A. 没有目标认证
   B. 没有源认证

4. (1) 假如：T 为 IDS 控制成本费用 200000 美元
   E 为每年恢复数据节省费用 50000 美元
   R 是为实施控制措施之前的每年恢复费用 100000 美元
   问：实际投资回报为：
   A. -50000
   B. -100000
   C. 100000
   D. 150000

A (投资回报就是控制前-控制后，投资回报负值就是省了多少，正值就是赚了多少)

(2) 问年度预期损失 ALE 怎么计算：
   A. (R+E)/T
   B.（R-E）+T
   C. (R-T)*E
   D. T/(R-E)

5. ipsec 隧道模式下的端到端加密，ip 包头
   A. 加密，数据不加密
   B. 和数据一起加密
   C. 不加密，数据加密

6. 实施一个安全计划，最重要的是：
   A 获取安全计划所需的资源
   B 与高层管理者访谈

7. 安全要求属于：
   A. ST 安全目标
   B. PP
   C. TOE

8. TOE 属于

A. CC

B. 可信计算机

9. 公司进行信息安全评估，打算把所有应用程序维护外包，问对服务提供商什么是最重要的？

A. BIA

B. 风险管理

C. SLA

10. 公司运维外包服务，问什么时候跟服务提供商确定安全要求？

A. 合同谈判

B. 合同定义

11. 外部审计师违反了公司安全要求，问惩罚判定来源：

A. 公司安全要求

B. 外部审计公司要求

C. 双方协议

12. 公司实施一个纵深防御政策，问由保护逐级增加的层次设计？

A. 边界 场地 出入口 办公区 计算机 机房

B. 围墙 场地 出入口 计算机 机房 办公区域

13. 802. 1 b 具有什么功能？

共享密钥

14. SSL 协议双向认证，部分使用，除了客户端验证服务器，还有？

A. 服务器对客户端自我验证

B. 客户端对服务器自我验证

15. 实现机密性，使用以下哪个算法？

（DES 不安全. SHA 是散列函数，RSA 速度慢，当然前提这道题目得有条件，如加密消息时）

A. DES

B. SHA-1

C. AES

D. RSA

16. 以下哪项可以实现数字签名. 完整性？

A. RSA

B. DSA

17. 同步. 异步令牌

同步令牌

18. 在 PKI 中哪个组件负责现实世界身份/“主体身份”（real world identity）与公钥证书绑定？

A. 注册机构

B. 根证书颁发机构

C. 中间证书颁发机构

19. 是怎么预防电缆产生的电磁辐射。

A. 套金属管.

B. 几根线缆缠在一起等等。

20. 在医院里面，使用了 RFID 技术确定人员和设备的位置，有什么好处？

可以更好的分辨药品，另一个是：

A. 提高医务人员的效率

B. 实现 MAC（介质访问控制）

21. 这个技术是通过什么技术实现控制？

A. MAC 介质访问控制

B. MPLS 多标签协议交换

22. 一个公司设计灭火系统，要冒大量的水出来，问哪种合适. ？

A. 干管

B. 湿管

C. 豫反应

D. 洪灾

23. 哪个访问控制模型是 WELL-FORMED 的？

A. BLP

B. BIBA

C. CLARK-WILSON

24. 有这样一个场景： C （只要是数据劫持相关的，都是中间人，AD 是用户，C 是攻击者。B 是路由器功能，防火墙支持路由，NAT，只是附加的功能）

A ---- B ----- C （网络 1）

|

|

D （网络 2）

网络 1 和网络 2 都通过设备 A 访问互联网，设备 B 负责网络 1 和网络 2 之间的 NAT，问：如果设备 C 利用设备 D 的 IP 地址进行操作，叫什么攻击？

A. 源欺诈

B. ARPA 中毒

C. 中间攻击

25. 某机构需要设计安全控制来只允许高级数据的读，以及限制低级数据的写入，该机构需

要采用什么安全模型？

A．BLP
B．BIBA
C．Clark-Wilson
D．中国墙

26．数据库管理员休假，其他人代替他的岗位，发现网络中有很多隐藏流量，防火墙规则被更改，问?：
A．最小特权．
B．职责分离

27．数据挖掘的风险：
A． 可以分析不同来源的数据
B． 每个数据库的隐私标准不同

28．根据 MTBF 最大故障间隔时间选择产品：
A．高
B．中
C．低

29．使用 SAML 的特点：
A． 扩展身份认证
B． 强规则执行

30．反垃圾邮件机制，通过检查邮件头部以及相关内容有效性，问使用下面哪个机制?
A． SMTP 黑名单
B． 邮件头分析

31．光盘介质使用哪种方式处理更彻底？A（我选的 AOK）
A． 破坏
B． 消磁

32．消息加密，部分数据为已知常量，问可以使用什么攻击方式？
A．已知明文攻击
B．已知密码攻击
C．密文攻击

33．哪个算法用来创建数字签名？其他为对称算法．
RSA

34．访问控制表，BLP 模型：谁能够访问 3 级文档；
类似表格：

User	Clearance	File	Label
A	Public	1	Public
B	Sensitive	2	Sensitive
C	Secret	3	Secret
D	Top Secret	4	Top Secret

（1）. 能够拥有最小写权限的用户是？

A. Public
B. Sensitive
C. Secret
D. Top Secret

（2）. 下面哪个是正确的？

A. C和D能够共享文件1和2
B. A和B能够共享文件3和4
C. B和C能够共享文件2和3
D. A和C能够共享文件1和2

35. 要实施一个防火墙之前，应该先：

A. 先进行风险评估

36. 使用一个公共无线局域网 WLAN 连接一个私有网络

客户端装个人防火墙并使用 VPN 连接网络

37. 哪一个是防止电子邮件欺骗的最有效手段:

A. 加密签名.
B. 实施主机 IDS.
C. 反垃圾邮件过滤.

38. 应急响应的最后阶段：

A. 调查.
B. 遏制.
C. 分析.
D. 教育

39. 跨国数据传输：

专利. 版权和商业秘密法律不是标准的

40. 对抗网络窃听：

加密

41. 还有一道场景题，好像是公司新来了个安全顾问，打算提高公司的安全防护水平，但是公司预算有限。那么他首先打算怎么做？

A．和公司高层开会讨论
B．设置安全基线
C．做预算表，考虑安全和成本的平衡
D．制定公司安全策略

42. 一个安全工程师被指派去处理公司正在遭受的 flood 攻击。公司有一个提供电子商务服务的网站。安全策略要求公司可以应对各种攻击，还要保证网站的可用性。
（1）问：安全策略最应该关注的是？
A． 花更多的钱在互联网专有线路上
B． 抵抗僵尸网络的持续攻击
C． 每天备份网站内容

（2）攻击者可能带来的威胁是？
A．忘了
B． 通过威胁公司采取拒绝服务攻击勒索钱财
C． 使远程邮件服务器无法工作

43. 操作系统中，父进程创建子进程最需要关注的安全问题是？
A． 开放设计
B． TOU
C． TOC

44. 黑客使用硬件密钥存储比软件密钥存储的优势是？
A． 物理性弱点多
B． 可存储数据文件
C． 可将数据传输到 web
D． 可针对更多人

45. 一项控制措施花费一亿，上线后，每天减少损失一百万，系统宕机一天损失一百万，问年度预期损失。

系统宕机一天的损失，一百万

46. 一下哪个用来区分多实例
A． 聚合
B． 推理
C． 安全级别

47. 某公司想做系统配置 cms 和软件配置，大概是统一配置管理。有一次因为系统和软件配置不一致导致业务出问题？
（1）． 请问你做为公司安全经理还是管理员了，你要做什么？

A. 职责分离

B. 生产系统和测试系统配置不一致

（2）上线 CMS 后可？

防止开发人员访问生产环境

48. bcp 测试活动

消防演习

49. 输入 id,密码后，还要输入手机接收到的 pin 码，pin 属于你知道的还是拥有的？

A. 知道

B. 拥有

50. 隐蔽通道

计时和存储

51. 渗透攻击时候有时候发生以下哪种意外

A. 造成拒绝服务攻击

B. 临时打开端口

52. 有个审计师要审计隐私策略，第一步是

A. 同管理层交流

B. 法律法规

53. 为每个用户创立了数据库的多个实例

如果区分

A. 按照安全分类

B. 键重要性(key important)

54. 下面哪个说法对 C

A. 很短的 RPO 意味很低的软件和硬件价值

B. 很短的 RPO 意味很高的软件和硬件价值

C. 很短的 RPO 意味着高的货币价值

D. 很短的 RPO 意味着低的货币价值

55. 下面哪项是不道德的??

A. CISSP 训练者让别人上他的课

B. CISSP 给别的 CISSP 背书 endrod（背书好像是担保的意思

56. 审计师在审计流程时发现一个不称职的系统管理员

A. 他是去审查招聘程序

B. 他是去审查培训程序

C．他是让一个熟练的系统管理员去 review 所有的系统

57．一个 BCP 计划里最可能的包括

A．文档存放位置联系人名单

58．一年有一天发生了火灾，100 万的软件年损失是多少？

100*1

投资回报是多少？

59．审计师认为以下情况是严重的情况：

一个发工资的程序是一月一发，最大可以允许时间 MTD 是一个月？

大于一个月

60．为了保证安全使用双向认证

A．服务器的证书，

B．服务器认证用户

C．用户认证服务器

61．S/MIME 是靠什么来交换密钥

A．共享

B．公钥

C．证书

D．ＩＫＥ

62．硬盘取证时，除了ＨＡＳＨ整个磁盘外要考虑什么？

A．考虑除此以外的其他证据情况

B．加密整个磁盘

63．开发人员在设计错误信息弹出的时候要考虑？

A． 保密性和完整性

B．可审计性和用户满意度

C．风险和效益

64．L2TP 是为了通过什么协议实现？

A．PPP

B．PCP

65．对硬盘记忆取证之前，要考虑？

A．是否有更多证据需要收集，扩展收集范围

B． 拆下硬盘，以及所有可以启动的组件

C． 进行 HASH 散列映像

66. 任命安全隐私管 CPO，第一步是：（收集信息包括识别法律法规）

A. 法律. 法规，合规性

B. 收集信息

67. 杀毒软件匹配内部已知规则，问是哪种？

A. 基于签名

B. 行为

68. 使用是在 CMMI 的第二个阶段？

A. 不可预测

B. 可重复

C. 可定义

D. 可管理

E. 可优化

69. 可重复使用是在 SDLC 的哪个阶段？

开发阶段

70. CC 对一个产品实施认证是为了证明这个产品对组织的作用：

A. TOE

B. ST

C. 组织策略安全.

71. IPSEC 使用哪个进行密钥交换：

IKE

72. 如何证明参加了 DRP 培训：

A. 通过参加一次真正的 DRP 来验证.

B. 参与者明确了在 DRP 中角色和与他人互动的流程

73. 说要变更数据中心方案，最重要的是什么

A. DRP 放在项目的最后去考虑

B. 只有一个出入口

C. 可适应性

74. CCTV 最重要考虑什么

A. 光线

75. 学生在家访问大学的资源，要怎么实施最易于部署/省钱

A. VPN+IPSEC

B. 家用 VPN 路由

76. 问了一个机密性组织更关注哪类错误？

A. 二类错误

77. 问了一个同步令牌和异步令牌
A. 同步令牌根据时间，
B. 异步令牌基于挑战值

78. 问了一个防数据库篡改的安全模型
A. graham-denning

79. 问了一个 FRAGGLE dos 攻击
A. Udp

80. 问选安全顾问，哪个在伦理上有问题
A. 一个有经验的顾问不选，选了个没经验的
B. 选用户推荐的顾问
C. 跟你私下有关系的，但是不合资质的顾问

81. 认证到认可是什么过程 B
A. 什么系统策略实施的过程
B. 管理层对确认风险
C. D 忘记拉

82. 情境题，一个公司规定“专利未发布前，知道此信息的员工不能买股票，除非已对公众公布”，次日，该公司在报纸上发布该消息，问员工能不能买股票
A. 可以买，得到管理层同意
B. 可以买，因为已经公布
C. 不可以买，管理层不同意
D. 不可以买，未公布公众

83. CA 信息层次包含那个
A. 网络交叉协议
B. X.509
C. PKI
D. X.500

84. 关于网络层走什么数据的题
A. 端口筛选
B. 数据包筛选
C. 应用程序筛选

85. 取证人员在硬盘发现 MD5 散列?

完整性

86. RAID5 的最小化原理之类的，

A. 在其中一个驱动器插拉奇偶

B. 在所有驱动器插入奇偶

87. 你在签署渗透测试合同的时候，一定要明确：NDA 只保护第三方.

网络渗透和应用渗透不同.

88. 消息加密，部分数据为已知常量，问可以使用什么攻击方式？

A. 已知明文攻击

B. 已知密码攻击

C. 密文攻击

89. A 和 B 互相交换公钥，B 如何验证 A？

A. 使用 A 的公钥验证

B. 使用私钥去验证

90. 异步与同步密码之间的主要主别：

A. 异同采用的是计数

B. 同步采用的是同一天时间间隔，异步任何时间都可以

C. 同步采用的是 60 分钟内的有效

D. 异步是基本挑战式的方式，同步是计时方式

91. 如果公司要在 24 小时里恢复业务，应选择哪个灾备场所？

A. 热站点

B. 温站点

C. 冷站点

92. 互惠协议的特点？

A. 便于类似的组织进行灾备

B. 对于较复杂的系统容易进行测试

C. 对于较复杂的系统很难进行测试

93. PADDING 技术使用在哪种密码上？

A. 块密码

B. 流密码

94. 应用开发架构项目团队在进行安全审查前首先要关注什么？

A. 了解行业内的标准

B. 了解政府目前发布的和即将发布的政策

95. 以下哪个会引起最严重的道德问题？

A. 一个 CISSP 背书另一个 CISSP

B. 一个 CISSP 资助别人获得其他证书

C. 一个 CISSP 讲师背书自己的学生

D. 一个 CISSP 经理资助自己公司下属

96. 国际间通讯存的问题是什么？

A. 一个国家的加密技术在另一个国家可能无法解密

B. 法律规定国际通讯不能使用加密技术

97. .当在渗透测试期间发现了服务器可以使用任何账户进行特权操作，应该第一时间？

A. 记录问题报告管理层

B. 报告系统管理员

98. 在安全审计时发现服务器管理员没有经过培训，应该？

A. 审查所有培训文档

B. 审查人事招聘流程

C. 找有经验的管理员对服务器进行安全审查

99. 可重复使用是在 CMMI 的哪个阶段？

A. 不可预测

B. 可重复

100. 安全控制有哪些？

A. 技术、管理、运维

B. 技术、管理、运营

101. 说系统已经被入侵了，问如果排除大量的系统文件找到被篡改的文件？

A. 在原系统中对系统文件进行散列

B. 在一个同等配置的干净系统中对系统文件进行散列然后进行对比

102. 问 PCIDSS 哪项是正确的

A. 定期进行更新

B. 每六个月进行更新

C. 按行业要求更新

103. 问电子卡的优点是什么？

A. 可以提供报警

B. 提供和锁一样的功能

104. 下面哪一个违背了伦理道德

A. 参加竞争对手免费的义演活动之类的

B. 在面试时用过期的证书

C. 在线证书论证过期不进行论证之类的

D. 隐瞒犯罪记录

105. 有个服务器一直没有补丁更新，因为要求他的可用性，问怎么解决这个问题？

A. 更新补丁的记录文档

B. 在防火墙的规则里进行限制端口

106. 任命安全隐私管 CPO，第一步是：

A. 法律、法规，合规性

B. 收集信息

107. 说有台主机已经被入侵，问怎么办？

A. 上入侵检测系统

B. 把该系统从可信任里隔离

C. 除了进行个人认证也进行系统认证

108. 审计师发现系统管理员未经培训就上岗，应该怎么做？

A. 报告管理层

B. 更换有经验的管理员先审计一下系统

109. 每次登陆都需要进行身份验证的是哪个？

A. Chap

B. pap

C. ESP

110. SDLC 中，那个过程进行安全鉴别（identification）？

实施中

维护和测试

启动

111. CA 信息层次包含那个

A. 网络交叉协议

B. X.509

C. PKI

D. X.500

112. 出口时设置智能卡读卡器的作用：

A. 与进入的日志匹配

B. 防止尾随

C. 防止时间卡攻击

113. 某信息中心，既没有监控也没有报警措施，容易被攻击者实施尾随，下列措施最有效的解决此问题：

A. 捕人陷阱
B. 保安

114. 哪一个能供提供最有效的实时的容错机制：
A. 备份
B. 独立的运行相同的服务
C. 回滚

115. 任何改动都会自动生成版本号，是配置管理系统是变更管理的什么手段？
A. 报告
B. 输出
C. 程序
D. 日志

116. 增强了输入数据的完整性：
A. 加密
B. 日志
C. 验证有效地输入范围

117. 法律、法规、合规是用来指导生成：
A. 策略
B. 过程
C. 基线
D. 指南

118. 说审计员发现某个端口被设置为混杂模式，证明发生了什么攻击？
A. 监听
C. SYN

119. 哪个可以通过进行功率差分分析进行攻击？
A. 智能卡
B. 网卡

120. 安全人员取证，恢复了数据，为什么还要恢复时间戳？
A. 记录入侵时间
B. 关联一些事情

121. 问使用隐写术将信息隐藏在 ping 数据包后面，可能存在什么样的风险？
隐藏通道

122. 使用 ISO 27001 ISO27002 进行风险评估，要评估新的变更，...
D. 评估控制措施的有效

123. 某公司人员给网上银行服务台打电话，告诉服务台人员，他向一个自称是银行服务台人员透漏了密码，服务台人员
(1)、检查通信记录，没有这个人。问这是一种什么攻击？

A．网络钓鱼

D．社会工程学

124．为一个计算机房进行安全设计，第一步做什么？

B．确定双因素验证

C．风险评估

125．一个信息系统，用户管理人员在使用系统时不能使用系统管理员的功能，系统管理员不能使用用户管理人员的功能，问这是什么控制？

A．最小权限

B．职责分离

126．在生命周期（SDLC）什么阶段执行认可（关于认证与认可的题）？

A．启动

B．购买/开发

C．实现

D．操作/维护

127．对 IP 数据包的包头进行隐写术会造成哪种影响？

A．隐蔽通道

B．改变路由

C．改变源地址

128．对 IP 数据包的包头进行改变会造成哪种影响？

A．隐蔽通道

B．改变路由

C．改变源地址

129．一员工离职后公司　进行相应的数据恢复，下面哪一个是可能导至无法恢复的原因

A．　認记密钥存放的位置

B．　没有找到审计轨迹方面的日志

C．　文件被损毁

130．2 一个安全经理到一家公司，发现其有洪泛攻击，为了解决此问题　，且又要公司　相关 WEB 上的应用不能停止，应采用的方式为：

A．　增加财务相应的预算

B．　与运营商沟通进行多线号接入

C．　与供应商沟通买相应的软件来解决此问题

D．　做企业培训还是什么忘了？

131. 一个员工将电脑带回家，电脑权限是管理员权限，员工家有个小孩经常玩这台电脑，后来管理员发现电脑上有对等体 P2P 程序，应采取什么措施

A. 限制完全管理员权限

B. 限制管理策略

C. 进行培训教育

欢迎点击这里的链接进入精彩的Linux公社网站

Linux公社（www.Linuxidc.com）于2006年9月25日注册并开通网站，Linux现在已经成为一种广受关注和支持的一种操作系统，IDC是互联网数据中心，LinuxIDC就是关于Linux的数据中心。

Linux公社是专业的Linux系统门户网站，实时发布最新Linux资讯，包括Linux、Ubuntu、Fedora、RedHat、红旗Linux、Linux教程、Linux认证、SUSE Linux、Android、Oracle、Hadoop、CentOS、MySQL、Apache、Nginx、Tomcat、Python、Java、C语言、OpenStack、集群等技术。

Linux公社（LinuxIDC.com）设置了有一定影响力的Linux专题栏目。

Linux公社 主站网址：www.linuxidc.com 旗下网站：www.linuxidc.net

包括：**Ubuntu 专题** **Fedora 专题** **Android 专题** **Oracle 专题** **Hadoop 专题** **RedHat 专题** **SUSE 专题** **红旗 Linux 专题** **CentOS 专题**

Linux 公社微信公众号：linuxidc_com