1. 以下哪项是计算机网络中用于防止未授权访问的物理安全措施？（A）

A. 防火墙

B. 加密技术

C. 访问控制

D. 视频监控

2. 以下哪个是一种常用的对称加密算法？（B）

A. RSA

B. DES

C. AES

D. SSL

3. 计算机病毒是一种\_\_\_\_\_\_\_。（C）

A. 硬件故障

B. 操作系统错误

C. 恶意软件

D. 网络攻击

4. 以下哪个术语表示将数据转换为无法读取的形式？（A）

A. 加密

B. 解密

C. 编码

D. 压缩

5. 以下哪个是一种网络攻击手段，攻击者通过伪造IP地址来隐藏自己的真实身份？（D）

A. DDoS攻击

B. 钓鱼攻击

C. 中间人攻击

D. IP地址伪造

6. 以下哪个术语表示将数据从一种形式转换为另一种形式？（C）

A. 加密

B. 解密

C. 编码

D. 压缩

7. 以下哪项是网络安全中的一个重要概念，用于保护网络免受未授权访问和攻击？（A）

A. 防火墙

B. 数据加密

C. 访问控制

D. 漏洞扫描

8. 以下哪项是一种常见的网络攻击，攻击者通过猜测或破解密码来获取未授权访问？（B）

A. 病毒攻击

B. 密码攻击

C. 拒绝服务攻击

D. 钓鱼攻击

9. 以下哪个术语表示将加密后的数据转换回原始数据？（B）

A. 加密

B. 解密

C. 编码

D. 压缩

10. 以下哪个是一种常用的非对称加密算法？（A）

A. RSA

B. DES

C. AES

D. SSL

11. 以下哪个术语表示在网络通信过程中，数据传输双方使用相同的密钥进行加密和解密？（B）

A. 非对称加密

B. 对称加密

C. 哈希函数

D. 数字签名

12. 以下哪个是一种网络安全工具，用于检测和报告网络中的漏洞和弱点？（D）

A. 防火墙

B. 加密技术

C. 访问控制

D. 漏洞扫描

13. 以下哪个术语表示在网络通信过程中，数据传输双方使用不同的密钥进行加密和解密？（A）

A. 非对称加密

B. 对称加密

C. 哈希函数

D. 数字签名

14. 以下哪项是一种网络攻击手段，攻击者通过篡改或伪造数据来误导接收者？（C）

A. DDoS攻击

B. 钓鱼攻击

C. 中间人攻击

D. IP地址伪造

15. 以下哪个术语表示在网络安全中，对网络资源进行管理和控制以防止未授权访问？（C）

A. 防火墙

B. 数据加密

C. 访问控制

D. 漏洞扫描

16. 以下哪项是一种网络攻击手段，攻击者通过发送大量请求来使目标服务器瘫痪？（A）

A. DDoS攻击

B. 密码攻击

C. 拒绝服务攻击

D. 钓鱼攻击

17. 以下哪个术语表示在网络安全中，用于保护数据传输过程的安全性？（B）

A. 哈希函数

B. 加密技术

C. 数字签名

D. 访问控制

18. 以下哪个术语表示在网络安全中，用于验证数据完整性和来源的机制？（D）

A. 哈希函数

B. 加密技术

C. 数字签名

D. 访问控制

19. 以下哪个术语表示在网络安全中，用于验证用户身份的机制？（A）

A. 身份验证

B. 访问控制

C. 加密技术

D. 防火墙

20. 以下哪项是一种网络攻击手段，攻击者通过利用系统漏洞来获取未授权访问？（D）

A. DDoS攻击

B. 密码攻击

C. 中间人攻击

D. 漏洞利用

21. 以下哪个术语表示在网络安全中，用于保护网络设备免受未授权访问的措施？（B）

A. 数据加密

B. 物理安全

C. 访问控制

D. 防火墙

22. 以下哪个术语表示在网络安全中，用于确保数据在传输过程中不被篡改或伪造的机制？（A）

A. 数字签名

B. 哈希函数

C. 加密技术

D. 访问控制

23. 以下哪项是一种网络攻击手段，攻击者通过发送恶意软件来感染目标系统？（B）

A. DDoS攻击

B. 病毒攻击

C. 拒绝服务攻击

D. 钓鱼攻击

24. 以下哪个术语表示在网络安全中，用于验证数据来源和完整性的技术？（C）

A. 加密技术

B. 身份验证

C. 数字签名

D. 访问控制

25. 以下哪个术语表示在网络安全中，用于防止网络设备受到物理损害或盗窃的措施？（D）

A. 数据加密

B. 网络隔离

C. 访问控制

D. 物理安全

26. 以下哪个是网络安全中的基本安全原则之一？（A）

A. 机密性

B. 公开性

C. 无关性

D. 不可否认性

27. 在网络安全中，CIA三元素模型指的是哪三个原则？（B）

A. 可用性. 完整性. 保密性

B. 机密性. 完整性. 可用性

C. 公开性. 完整性. 可用性

D. 不可否认性. 完整性. 保密性

28. 以下哪个原则主要关注保护信息的保密性？（A）

A. 机密性

B. 完整性

C. 可用性

D. 可追溯性

29. 以下哪个原则主要关注保护信息的完整性？（B）

A. 机密性

B. 完整性

C. 可用性

D. 可追溯性

30. 以下哪个原则主要关注保护信息的可用性？（C）

A. 机密性

B. 完整性

C. 可用性

D. 可追溯性

31. 以下哪个原则主要关注确保信息的来源不可否认？（D）

A. 机密性

B. 完整性

C. 可用性

D. 可追溯性

32. 以下哪个模型是网络安全中的一个重要安全模型？（A）

A. Bell-LaPadula模型

B. OSI七层模型

C. TCP/IP模型

D. 身份验证模型

33. 以下哪个模型主要关注保护信息的保密性？（A）

A. Bell-LaPadula模型

B. OSI七层模型

C. TCP/IP模型

D. 身份验证模型

34. 以下哪个模型主要关注保护信息的完整性和保密性？（B）

A. Bell-LaPadula模型

B. OSI七层模型

C. TCP/IP模型

D. 身份验证模型

35. 以下哪个模型主要关注保护信息的可用性？（C）

A. Bell-LaPadula模型

B. OSI七层模型

C. TCP/IP模型

D. 身份验证模型

36. 以下哪个模型主要关注保护信息的不可否认性？（D）

A. Bell-LaPadula模型

B. OSI七层模型

C. TCP/IP模型

D. 身份验证模型

37. 以下哪个原则是网络安全中的基本安全原则之一？（A）

A. 机密性

B. 公开性

C. 无关性

D. 不可否认性

38. 在网络安全中，Bell-LaPadula模型主要关注哪两个原则？（B）

A. 可用性. 完整性

B. 机密性. 完整性

C. 公开性. 可用性

D. 不可否认性. 完整性

39. 以下哪个术语表示确保信息只能被授权用户访问的安全原则？（A）

A. 机密性

B. 完整性

C. 可用性

D. 可追溯性

40. 以下哪个术语表示确保信息在传输过程中不被篡改的安全原则？（B）

A. 机密性

B. 完整性

C. 可用性

D. 可追溯性

41. 以下哪个术语表示确保信息在传输过程中能够被授权用户访问的安全原则？（C）

A. 机密性

B. 完整性

C. 可用性

D. 可追溯性

42. 以下哪个术语表示确保信息在传输过程中不被篡改或伪造的安全原则？（B）

A. 机密性

B. 完整性

C. 可用性

D. 可追溯性

43. 以下哪个术语表示确保信息在传输过程中能够正常使用和访问的安全原则？（C）

A. 机密性

B. 完整性

C. 可用性

D. 可追溯性

44. 以下哪个术语表示确保信息在传输过程中的来源不可否认的安全原则？（D）

A. 机密性

B. 完整性

C. 可用性

D. 可追溯

45. 以下哪个是网络安全中的基本安全属性之一？（A）

A. 机密性

B. 公开性

C. 可用性

D. 不可追溯性

46. 在网络安全中，哪一个原则关注保护信息不被未授权访问？（A）

A. 机密性

B. 完整性

C. 可用性

D. 可追溯性

47. 以下哪一个模型是用于描述网络安全策略和规则的？（B）

A. Bell-LaPadula模型

B. 访问控制矩阵

C. OSI七层模型

D. TCP/IP模型

48. 以下哪一个术语表示在网络安全中，确保信息在传输过程中不被泄露给未授权的用户？（A）

A. 机密性

B. 完整性

C. 可用性

D. 可追溯性

49. 以下哪一个原则是指在网络安全中，确保信息在传输过程中保持未被篡改的状态？（B）

A. 机密性

B. 完整性

C. 可用性

D. 可追溯性

50. 以下哪一个原则是指在网络安全中，确保信息可以被授权用户在需要时访问？（C）

A. 机密性

B. 完整性

C. 可用性

D. 可追溯性

51. 以下哪一个原则是指在网络安全中，确保无法否认已经发生的行为或交易？（D）

A. 机密性

B. 完整性

C. 可用性

D. 可追溯性

52. 以下哪一个模型用于定义如何在网络中保护信息的保密性和完整性？（A）

A. Bell-LaPadula模型

B. 访问控制矩阵

C. OSI七层模型

D. TCP/IP模型

53. 以下哪一个术语表示在网络安全中，对信息进行加密以保护其保密性？（A）

A. 机密性

B. 完整性

C. 可用性

D. 可追溯性

54. 以下哪一个术语表示在网络安全中，对信息进行加密以保护其完整性？（B）

A. 机密性

B. 完整性

C. 可用性

D. 可追溯性

55. 以下哪一个术语表示在网络安全中，对信息进行加密以保护其可用性？（C）

A. 机密性

B. 完整性

C. 可用性

D. 可追溯性

56. 以下哪一个术语表示在网络安全中，确保信息的来源可以被验证和追溯？（D）

A. 机密性

B. 完整性

C. 可用性

D. 可追溯性

57. 以下哪一个原则是网络安全中的基本安全原则之一？（A）

A. 机密性

B. 公开性

C. 可用性

D. 不可追溯性

58. 在网络安全中，哪一个原则关注保护信息不被未授权修改？（B）

A. 机密性

B. 完整性

C. 可用性

D. 可追溯性

59. 以下哪一个模型是用于描述如何保护网络系统免受未经授权的访问和攻击的？（A）

A. Bell-LaPadula模型

B. 访问控制矩阵

C. OSI七层模型

D. TCP/IP模型

60. 以下哪一个术语表示在网络安全中，确保信息在传输过程中保持未被泄露的状态？（A）

A. 机密性

B. 完整性

C. 可用性

D. 可追溯性

61. 以下哪一个原则是指在网络安全中，确保信息在传输过程中保持未被篡改的状态？（B）

A. 机密性

B. 完整性

C. 可用性

D. 可追溯性

62. 以下哪一个原则是指在网络安全中，确保信息可以被授权用户在需要时访问？（C）

A. 机密性

B. 完整性

C. 可用性

D. 可追溯性

63. 以下哪一个原则是指在网络安全中，确保无法否认已经发生的行为或交易？（D）

A. 机密性

B. 完整性

C. 可用性

D. 可追溯性

64. 以下哪个是加密技术中最常用的算法之一？（A）

A. AES

B. RSA

C. DES

D. MD5

65. 在加密技术中，AES算法支持哪种密钥长度？（A）

A. 128位. 192位. 256位

B. 40位. 56位. 128位

C. 64位. 80位. 1024位

D. 32位. 48位. 64位

66. 以下哪个是一种非对称加密算法？（B）

A. DES

B. RSA

C. AES

D. MD5

67. 以下哪个是一种单向散列函数，通常用于验证数据的完整性？（D）

A. DES

B. RSA

C. AES

D. MD5

68. 以下哪个是加密技术中最基本的概念之一？（A）

A. 密钥

B. 加密

C. 解密

D. 散列

69. 在加密技术中，哪个过程将明文转换为密文？（B）

A. 散列

B. 加密

C. 解密

D. 认证

70. 以下哪个是用于加密和解密数据的密钥？（A）

A. 公钥

B. 私钥

C. 密钥

D. 密码

71. 以下哪个是一种对称加密算法？（C）

A. DES

B. RSA

C. AES

D. MD5

72. 在加密技术中，公钥通常用于哪个过程？（B）

A. 加密

B. 解密

C. 认证

D. 散列

73. 以下哪个是一种安全的加密算法，广泛用于保护网络通信的安全？（A）

A. AES

B. RSA

C. DES

D. MD5

74. 以下哪个是一种加密技术，它使用两个密钥，一个公钥和一个私钥？（B）

A. 对称加密

B. 非对称加密

C. 单向加密

D. 双向加密

75. 以下哪个是一种将数据分割成多个部分，然后对每个部分独立加密的加密技术？（A）

A. 分组加密

B. 分发加密

C. 分层加密

D. 分区加密

76. 以下哪个是一种加密技术，它使用多个密钥对数据进行加密？（B）

A. 对称加密

B. 非对称加密

C. 单向加密

D. 双向加密

77. 以下哪个是加密技术中的一个重要概念，用于确保数据在传输过程中的安全性？（A）

A. 加密

B. 解密

C. 认证

D. 完整性

78. 在加密技术中，哪个过程将密文转换为明文？（B）

A. 散列

B. 解密

C. 加密

D. 认证

79. 以下哪个是一种常见的对称加密算法，广泛用于保护数据的保密性？（C）

A. DES

B. RSA

C. AES

D. MD5

80. 以下哪个是一种安全的加密算法，它的密钥长度可达到256位？（A）

A. AES

B. RSA

C. DES

D. MD5

81. 以下哪个是一种非对称加密算法，它使用两个密钥，一个公钥和一个私钥？（B）

A. DES

B. RSA

C. AES

D. MD5

82. 以下哪个是一种单向散列函数，它将数据转换为一个固定长度的散列值？（D）

A. DES

B. RSA

C. AES

D. MD5

83. 在加密技术中，密钥是用于哪个过程的？（A）

A. 加密和解密

B. 散列和认证

C. 解密和认证

D. 加密和散列

84. 以下哪个是一种加密技术，它通过将明文与随机生成的密钥进行异或操作来加密数据？（A）

A. 异或加密

B. 密文交换

C. 秘密共享

D. 对称加密

85. 以下哪个概念涉及到确保加密通信中没有一个密钥被泄露给攻击者？（A）

A. 密钥安全

B. 加密强度

C. 密钥分发

D. 密码学安全

86. 以下哪个是一种加密技术，它通过将数据分割成小块并使用不同的密钥对每个块进行加密？（B）

A. 分组加密

B. 块加密

C. 流加密

D. 散列加密

87. 以下哪个是加密技术中的一个重要概念，它涉及到验证加密消息的来源和完整性？（B）

A. 机密性

B. 认证

C. 完整性

D. 可用性

88. 以下哪个是一种加密技术，它使用一个单一的密钥来加密和解密数据？（A）

A. 对称加密

B. 非对称加密

C. 混合加密

D. 公钥加密

89. 以下哪个是加密技术中的一个基本概念，它涉及到保护信息不被未授权的用户访问？（A）

A. 机密性

B. 完整性

C. 可用性

D. 可追溯性

90. 以下哪个是一种常见的加密算法，它使用一个128位. 192位或256位的密钥来加密数据？（C）

A. DES

B. RSA

C. AES

D. MD5

91. 以下哪个是一种非对称加密算法，它由Ron Rivest. Adi Shamir和Leonard Adleman在1977年提出？（B）

A. DES

B. RSA

C. AES

D. MD5

92. 以下哪个是一种加密技术，它通过使用两个密钥（公钥和私钥）来确保数据的机密性和完整性？（D）

A. 对称加密

B. 非对称加密

C. 混合加密

D. 公钥加密

93. 以下哪个是加密技术中的一个重要概念，它涉及到确保数据在传输过程中不被篡改或伪造？（B）

A. 机密性

B. 完整性

C. 可用性

D. 可追溯性

94. 以下哪个是一种加密技术，它通过将数据流与一个密钥流进行异或操作来加密数据？（A）

A. 流加密

B. 分组加密

C. 块加密

D. 散列加密

95. 以下哪个概念涉及到在加密通信中，即使密钥被泄露，攻击者也无法解密消息？（A）

A. 密钥安全

B. 加密强度

C. 密钥分发

D. 密码学安全

96. 以下哪个是一种常见的非对称加密算法，它使用椭圆曲线密码学来确保数据的安全传输？（C）

A. DES

B. RSA

C. ECC

D. MD5

97抵御电子邮箱入侵措施中，不正确的是（D）

A. 不用生日做密码

B. 不要使用少于5位的密码

C. 不要使用纯数字

D. 自己做服务器

98. 以下哪个是一种加密技术，它通过将明文转换为密文来保护数据的保密性？（B）

A. 散列

B. 加密

C. 解密

D. 认证

99. 以下哪个是一种非对称加密算法，它使用两个密钥（公钥和私钥）来确保数据的机密性和完整性？（B）

A. 对称加密

B. 非对称加密

C. 混合加密

D. 公钥加密

100. 以下哪项不属于防止口令猜测的措施？（B）

A. 严格限定从一个给定的终端进行非法认证的次数;

B. 确保口令不在终端上再现；

C. 防止用户使用太短的口令;

D. 使用机器产生的口令

101. 以下哪个是安全性能度量中用于衡量系统安全性的一个重要指标？（A）

A. 安全性

B. 可靠性

C. 可用性

D. 性能

102. 在安全性能度量中，以下哪个概念涉及到评估系统在受到攻击时的稳定性？（B）

A. 安全性

B. 鲁棒性

C. 可用性

D. 性能

103. 以下哪个是安全性能度量中用于衡量系统在面对恶意输入时的抵抗能力的一个指标？（A）

A. 鲁棒性

B. 脆弱性

C. 安全性

D. 性能

104. 在安全性能度量中，以下哪个概念涉及到评估系统在特定时间内处理安全事件的能力？（B）

A. 响应性

B. 实时性

C. 可用性

D. 性能

105. 以下哪个是安全性能度量中用于衡量系统在正常运行期间受到攻击的风险的一个指标？（A）

A. 安全性

B. 可靠性

C. 脆弱性

D. 性能

106. 在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击后恢复正常运行的能力？（B）

A. 恢复性

B. 韧性

C. 可用性

D. 性能

107. 以下哪个是安全性能度量中用于衡量系统在面临威胁时保持正常运行的能力的一个指标？（A）

A. 安全性

B. 稳定性

C. 韧性

D. 性能

108. 在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击时保护敏感数据的能力？（B）

A. 保密性

B. 完整性

C. 可用性

D. 性能

109. 以下哪个是安全性能度量中用于衡量系统在遭受攻击时保持数据完整性的能力的一个指标？（A）

A. 安全性

B. 可靠性

C. 完整性

D. 性能

110. 在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击时保持数据机密性的能力？（B）

A. 保密性

B. 完整性

C. 可用性

D. 性能

111. 以下哪个是安全性能度量中用于衡量系统在正常运行期间保持数据机密性的能力的一个指标？（A）

A. 安全性

B. 可靠性

C. 保密性

D. 性能

112. 在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击后恢复数据机密性的能力？（B）

A. 恢复性

B. 韧性

C. 保密性

D. 性能

113. 以下哪个是安全性能度量中用于衡量系统在面临威胁时保护数据机密性的能力的一个指标？（A）

A. 安全性

B. 稳定性

C. 韧性

D. 性能

114. 在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击时保护数据完整性的能力？（B）

A. 保密性

B. 完整性

C. 可用性

D. 性能

115. 在以下认证方式中，最常用的认证方式是：（A)

A基于账户名／口令认证；

B基于摘要算法认证；

C基于PKI认证;

D基于数据库认证

116. 在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击后恢复数据完整性的能力？（B）

A. 恢复性

B. 韧性

C. 保密性

D. 性能

117. 以下哪个是安全性能度量中用于衡量系统在面临威胁时保护数据完整性的能力的一个指标？（A）

A. 安全性

B. 稳定性

C. 韧性

D. 性能

118. 在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击时保持数据可用性的能力？（B）

A. 保密性

B. 可用性

C. 完整性

D. 性能

119. 以下哪个是安全性能度量中用于衡量系统在遭受攻击时保持服务可用性的能力的一个指标？（A）

A. 安全性

B. 恢复性

C. 韧性

D. 性能

120. 在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击后恢复正常服务的能力？（B）

A. 恢复性

B. 韧性

C. 保密性

D. 性能

121. 以下哪个是安全性能度量中用于衡量系统在面临威胁时保持服务可用性的能力的一个指标？（A）

A. 安全性

B. 稳定性

C. 韧性

D. 性能

122. 在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击时保持正常操作的能力？（B）

A. 安全性

B. 鲁棒性

C. 可用性

D. 性能

123. 以下哪个是安全性能度量中用于衡量系统在遭受攻击时保持正常操作的能力的一个指标？（A）

A. 安全性

B. 可靠性

C. 鲁棒性

D. 性能

124. 在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击后恢复正常操作的能力？（B）

A. 恢复性

B. 韧性

C. 保密性

D. 性能

125. 以下哪个是安全性能度量中用于衡量系统在面临威胁时保持正常操作的能力的一个指标？（A）

A. 安全性

B. 稳定性

C. 韧性

D. 性能

126. 在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击时保持业务连续性的能力？（B）

A. 安全性

B. 业务连续性

C. 可用性

D. 性能

127. 以下哪个是安全性能度量中用于衡量系统在遭受攻击时保持业务连续性的能力的一个指标？（A）

A. 安全性

B. 恢复性

C. 业务连续性

D. 性能

128. 在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击后恢复业务连续性的能力？（B）

A. 恢复性

B. 韧性

C. 保密性

D. 性能

129. 以下哪个是安全性能度量中用于衡量系统在面临威胁时保持业务连续性的能力的一个指标？（A）

A. 安全性

B. 稳定性

C. 韧性

D. 性能

130. 在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击时保持关键资源安全的能力？（B）

A. 安全性

B. 关键资源安全

C. 可用性

D. 性能

131. 以下哪个是安全性能度量中用于衡量系统在遭受攻击时保持关键资源安全的能力的一个指标？（A）

A. 安全性

B. 恢复性

C. 关键资源安全

D. 性能

132. 在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击后恢复关键资源安全的能力？（B）

A. 恢复性

B. 韧性

C. 保密性

D. 性能

133. 以下哪个是安全性能度量中用于衡量系统在面临威胁时保持关键资源安全的能力的一个指标？（A）

A. 安全性

B. 稳定性

C. 韧性

D. 性能

134. 在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击时保持系统完整性的能力？（B）

A. 安全性

B. 系统完整性

C. 可用性

D. 性能

135. 以下哪个是安全性能度量中用于衡量系统在遭受攻击时保持系统完整性的能力的一个指标？（A）

A. 安全性

B. 恢复性

C. 系统完整性

D. 性能

136. 以下哪个是业务连续性管理的目标之一？（A）

A. 确保业务操作在任何情况下都能持续进行

B. 减少员工的工作时间

C. 提高系统的安全性

D. 降低灾难发生的概率

137. 以下哪个不是业务连续性计划（BCP）的关键组成部分？（B）

A. 风险评估

B. 员工培训

C. 应急响应计划

D. 数据备份

138. 以下哪个是业务连续性计划中用于确保关键业务流程在灾难发生后能够继续进行的一项措施？（A）

A. 热备份

B. 冷备份

C. 实时恢复

D. 数据加密

139. 以下哪个不是灾难恢复计划（DRP）的主要目标？（D）

A. 最小化业务中断时间

B. 确保数据的安全和完整性

C. 快速恢复系统运行

D. 预防灾难的发生

140. Windows NT和Windows 2000系统能设置为在几次无效登录后锁定帐号,这可以防止（B)

A. 木马

B. 暴力攻击；

C. IP欺骗；

D. 缓存溢出攻击

141. 以下哪个是业务连续性计划中用于在灾难发生后迅速恢复关键业务功能的一项措施？（A）

A. 业务恢复中心

B. 数据备份

C. 安全审计

D. 风险评估

142. 以下哪个不是灾难恢复计划中常用的恢复策略？（D）

A. 热备份

B. 温备份

C. 冷备份

D. 数据泄露

143. 以下哪个是业务连续性管理中用于评估组织在灾难发生时可能面临的威胁和风险的一项措施？（A）

A. 风险评估

B. 业务影响分析

C. 灾难模拟

D. 恢复时间目标

144. 用户收到了一封可疑的电子邮件,要求用户提供银行账户及密码,这是属于何种攻击手段？(B）

A. 缓存溢出攻击；

B. 钓鱼攻击；

C. 暗门攻击；

D. DDOS攻击

145. 向有限的空间输入超长的字符串是哪一种攻击手段？(A）

A. 缓冲区溢出;

B. 网络监听；

C. 拒绝服务

D. IP欺骗

146. 在业务连续性管理中，以下哪个步骤通常是最后进行的？（A）

A. 审查和更新BCP

B. 测试BCP

C. 实施BCP

D. 制定BCP

147. 以下哪个是业务连续性计划中用于确保在灾难发生后关键业务功能能够持续运行的一项措施？（A）

A. 连续性运营中心

B. 数据备份

C. 安全审计

D. 风险评估

148. 以下哪个不是灾难恢复计划中常用的恢复时间目标（RTO）的例子？（D）

A. 1小时

B. 4小时

C. 24小时

D. 1周

149. 以下哪个是业务连续性管理中用于评估组织在灾难发生时可能面临的威胁和风险的一项措施？（B）

A. 风险评估

B. 业务影响分析

C. 灾难模拟

D. 恢复时间目标

150. 以下哪个是业务连续性计划中用于确保在灾难发生后关键业务功能能够迅速恢复的一项措施？（B）

A. 数据备份

B. 恢复点目标

C. 安全控制

D. 业务恢复时间目标

151. 以下哪个不是业务连续性管理中常用的术语？（D）

A. 恢复时间目标（RTO）

B. 恢复点目标（RPO）

C. 业务影响评估（BIA）

D. 数据泄露

152. 在业务连续性管理中，以下哪个步骤通常是首先进行的？（A）

A. 制定BCP

B. 测试BCP

C. 实施BCP

D. 审查BCP

153. 以下哪个是业务连续性计划中用于在灾难发生后恢复关键业务功能的一个关键要素？（A）

A. 备用设施

B. 员工士气

C. 业务流程

D. 技术基础设施

154. 以下哪个不是灾难恢复计划中必须考虑的方面？（D）

A. 数据保护

B. 系统恢复

C. 通信恢复

D. 员工休闲活动

155. 以下哪个是业务连续性管理中用于确定组织关键业务功能的恢复时间的一个目标？（A）

A. 恢复时间目标（RTO）

B. 恢复点目标（RPO）

C. 业务影响评估（BIA）

D. 成本效益分析

156. 为了防御网络监听，最常用的方法是(B)

A. 采用物理传输（非网络）

B. 信息加密

C. 无线网

D. 使用专线传输

157. 使网络服务器中充斥着大量要求回复的信息,消耗带宽，导致网络或系统停止正常服务,这属于什么攻击类型?(A）

A. 拒绝服务

B. 文件共享

C. BIND漏洞

D. 远程过程调用

158. 任何组织或者个人注册微博客账号，制作. 复制. 发布. 传播信息内容的，应当使用( A )，不得以虚假. 冒用的居民身份信息. 企业注册信息. 组织机构代码信息进行注册。网站开展微博客服务，应当保证前款规定的注册用户信息真实。

A真实身份信息

B正确的网站信息

C真实的ID

D工商注册信息

159. 王某，未经著作权人许可，以私服营运方式，通过信息网络向公众传播他人网络游戏软件，获利14万余元，其行为均构成( A )。

A. 侵犯著作权罪

B. 侵犯商业秘密罪

C. 非法侵入计算机信息系统罪

D. 非法经营罪

160. 可以被数据完整性机制防止的攻击方式是(D)。

A. 假冒源地址或用户的地址欺骗攻击

B. 抵赖做过信息的递交行为

C. 数据中途被攻击者窃听获取

D. 数据在途中被攻击者篡改或破坏

161. 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)

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

162. 为了防止各种各样的病毒对计算机系统造成危害，可以在计算机上安装防病毒软件，并注意及时 ( B )，以保证能防止和查杀新近出现的病毒。

A. 分析

B. 升级

C. 检查

163. 木马程序一般是指潜藏在用户电脑中带有恶意性质的 ( A )，利用它可以在用户不知情的情况下窃取用户联网电脑上的重要数据信息。

A. 远程控制软件

B. 计算机

C. 木头做的马

164. 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?(C)

A. 微软公司软件的设计阶段的失误

B. 微软公司软件的实现阶段的失误

C. 系统管理员维护阶段的失误

D. 最终用户使用阶段的失误

165. 黑客在攻击中进行端口扫描可以完成( D )。

A. 检测黑客自己计算机已开放哪些端口

B. 口令破译

C. 获知目标主机开放了哪些端口服务

D. 截获网络流量

166. 在业务连续性管理中，以下哪个步骤通常是最后进行的？（B）

A. 制定BCP

B. 审查和更新BCP

C. 测试BCP

D. 实施BCP

167. 目前的防火墙防范主要是( B )

A. 主动防范

B. 被动防范

C. 不一定

168. 以下哪个是安全策略的一个关键组成部分？（A）

A. 定义安全规则和标准

B. 定期更换密码

C. 安装最新的安全补丁

D. 进行安全培训

169. 在制定安全策略时，以下哪个不是考虑的因素？（D）

A. 资产的价值

B. 潜在威胁的评估

C. 法律和合规要求

D. 员工的工作满意度

170. 以下哪个不是安全策略的主要目标？（B）

A. 保护数据和信息资产

B. 提高员工的工作效率

C. 防止未授权访问

D. 确保服务的可用性

171. 以下哪个是安全策略中用于指导组织如何保护其信息资产的一个文档？（A）

A. 安全政策

B. 安全标准

C. 安全程序

D. 安全指南

172. 以下哪个不是安全策略中通常包含的内容？（D）

A. 访问控制规则

B. 数据保护措施

C. 安全事故响应流程

D. 员工的个人爱好

173. 以下哪个是安全策略中用于确保员工了解和遵守安全规则的一个关键要素？（A）

A. 安全意识培训

B. 技术控制措施

C. 物理安全措施

D. 定期安全审计

174. 在安全策略中，以下哪个不是常见的风险缓解措施？（D）

A. 加密敏感数据

B. 实施防火墙

C. 定期备份数据

D. 鼓励员工加班工作

175. 以下哪个是安全策略中用于评估组织可能面临的风险和威胁的一个关键步骤？（A）

A. 风险评估

B. 安全审计

C. 合规性检查

D. 技术评估

176. 以下哪个不是安全策略中用于保护组织免受网络攻击的措施？（B）

A. 实施入侵检测系统

B. 要求员工使用复杂的密码

C. 定期更新软件和系统

D. 限制员工访问权限

177. 以下哪个是安全策略中用于确保组织遵守相关法律和行业标准的一个关键要素？（A）

A. 合规性管理

B. 技术控制

C. 安全意识教育

D. 安全监控

178. 在安全策略中，以下哪个不是常见的安全控制类别？（D）

A. 访问控制

B. 加密

C. 监控和审计

D. 员工激励计划

179. 以下哪个是安全策略中用于指导组织如何应对安全事故的一个文档？（A）

A. 应急响应计划

B. 安全标准

C. 安全程序

D. 安全指南

180. 虚拟专用网是指( A )

A. 虚拟的专用网络

B. 虚拟的协议网络

C. 虚拟的包过滤网络

181. SQL 语言的 GRANT 和 REVOKE 语句主要是用来维护数据库的（ C ） 。

A．完整性

B．可靠性

C．安全性

D．一致性

182. 在数据库的安全性控制中，授权的数据对象的（ A ） ，授权子系统就越灵活。

A．范围越小

B．约束越细致

C．范围越大

D．约束范围大

183. 以下（ D ）不属于实现数据库系统安全性的主要技术和方法。

A．存取控制技术

B．视图技术

C．审计技术

D．出入机房登记和加锁

184. HTTPS 是使用以下（ C ）协议。

A．SSH

B．SET

C．SSL

D．TCP

185. 创建 Web 虚拟目录的用途是（ C ） 。

A．用来模拟主目录的假文件夹

B．用一个假的目录来避免感染病毒

C．以一个固定的别名来指向实际的路径，当主目录改变时，相对用户而言是不变的

D．以上都不对

186. 网络监控的主要目的是什么？（A）

A. 检测和防御潜在的网络安全威胁

B. 提高网络性能

C. 收集用户活动数据

D. 分析网络流量模式

187. 以下哪个不是网络监控工具的常见功能？（D）

A. 实时流量分析

B. 入侵检测

C. 防火墙管理

D. 员工考勤记录

188. 流量分析通常涉及哪些类型的数据？（B）

A. 源和目的IP地址

B. 源和目的端口号

C. 数据包大小

D. 所有上述选项

189. 以下哪个不是流量分析中常用的技术？（C）

A. 深度包检测（DPI）

B. 网络流量镜像

C. 数据包嗅探

D. 端口扫描

190. 网络监控中，哪一项措施可以帮助减少误报？（A）

A. 设置合适的阈值

B. 定期更新签名库

C. 增加监控设备

D. 减少监控范围

191. 以下哪个是网络监控中用于识别异常行为的一种技术？（B）

A. 行为分析

B. 异常检测

C. 入侵防御

D. 安全信息与事件管理（SIEM）

192. 以下哪个不是流量分析中可以采取的预防措施？（D）

A. 限制异常流量

B. 增强防火墙规则

C. 应用入侵预防系统（IPS）

D. 增加员工工作时间

193. 网络监控中，哪一项措施可以帮助提高网络安全？（A）

A. 定期审查日志文件

B. 使用强大的密码

C. 关闭不必要的服务

D. 所有上述选项

194. 以下哪个不是流量分析中常用的指标？（C）

A. 传输速率

B. 数据包数量

C. 员工工作效率

D. 数据包大小

195. 网络监控和流量分析对于哪个方面的网络安全至关重要？（A）

A. 及时发现和响应安全事件

B. 提高员工满意度

C. 优化网络性能

D. 确保业务连续性

196. 以下哪个是网络监控中用于监控网络活动的一种技术？（B）

A. 数据包嗅探

B. 流量分析

C. 端口扫描

D. 安全事件管理

197. 以下哪个不是流量分析中可以采取的响应措施？（D）

A. 隔离受感染的设备

B. 阻止恶意流量

C. 应用安全补丁

D. 调整员工工作量

198. 网络监控中，哪一项措施可以帮助减轻网络安全风险？（A）

A. 实施访问控制

B. 定期更换密码

C. 增加监控设备

D. 减少数据传输

199. （ B）是网络通信中标志通信各方身份信息的一系列数据，提供一种在 Internet 上验证身份的方式。

A．数字认证

B．数字证书

C．电子认证

D．电子证书

200. 在建立网站的目录结构时，最好的做法是（ A） 。

A．将所有的文件最好都放在根目录下

B．目录层次选在 3～5 层

C．按栏目内容建立子目录

D．最好使用中文目录

201. 不属于常见的危险密码是(D）

A. 跟用户名相同的密码

B. 使用生日作为密码

C. 只有4位数的密码

D. 10位的综合型密码

202. 不属于计算机病毒防治的策略的是（D)

A. 确认您手头常备一张真正“干净”的引导盘

B. 及时. 可靠升级反病毒产品

C. 新购置的计算机软件也要进行病毒检测

D. 整理磁盘

203. 针对数据包过滤和应用网关技术存在的缺点而引入的防火墙技术，这是（)防火墙的特点。（D）

A. 包过滤型

B. 应用级网关型

C. 复合型防火墙

D. 代理服务型

204. 在每天下午5点使用计算机结束时断开终端的连接属于（A）

A. 外部终端的物理安全

B. 通信线的物理安全

C. 窃听数据

D. 网络地址欺骗

205. 2003年上半年发生的较有影响的计算机及网络病毒是什么（B）

A. SARS

B. SQL杀手蠕虫

C. 手机病毒

D. 小球病毒

206. SQL杀手蠕虫病毒发作的特征是什么（A）

A. 大量消耗网络带宽

B. 攻击个人PC终端

C. 破坏PC游戏程序

D. 攻击手机网络

207. 当今IT的发展与安全投入，安全意识和安全手段之间形成(B)

A. 安全风险屏障

B. 安全风险缺口

C. 管理方式的变革

D. 管理方式的缺口

208. 我国的计算机年犯罪率的增长是（C)

A. 10％

B. 160％

C. 60%

D. 300％

209. 信息安全风险缺口是指（A)

A. IT的发展与安全投入，安全意识和安全手段的不平衡

B. 信息化中,信息不足产生的漏洞

C. 计算机网络运行,维护的漏洞

D. 计算中心的火灾隐患

210. 信息网络安全的第一个时代(B)

A. 九十年代中叶

B. 九十年代中叶前

C. 世纪之交

D. 专网时代

211. 信息网络安全的第三个时代(A)

A. 主机时代，专网时代,多网合一时代

B. 主机时代，PC机时代，网络时代

C. PC机时代,网络时代，信息时代

D. 2001年，2002年，2003年

212. 信息网络安全的第二个时代(A）

A. 专网时代

B. 九十年代中叶前

C. 世纪之交

213. 网络安全在多网合一时代的脆弱性体现在（C)

A. 网络的脆弱性

B. 软件的脆弱性

C. 管理的脆弱性

D. 应用的脆弱性

214. 人对网络的依赖性最高的时代(C)

A. 专网时代

B. PC时代

C. 多网合一时代

D. 主机时代

215. 网络攻击与防御处于不对称状态是因为(C）

A. 管理的脆弱性

B. 应用的脆弱性

C. 网络软，硬件的复杂性

D. 软件的脆弱性

216. 网络攻击的种类(A）

A. 物理攻击，语法攻击，语义攻击

B. 黑客攻击，病毒攻击

C. 硬件攻击，软件攻击

D. 物理攻击,黑客攻击,病毒攻击

217. 语义攻击利用的是(A)

A. 信息内容的含义

B. 病毒对软件攻击

C. 黑客对系统攻击

D. 黑客和病毒的攻击

218. 1995年之后信息网络安全问题就是(A）

A. 风险管理

B. 访问控制

C. 消除风险

D. 回避风险

219. 风险评估的三个要素(D）

A. 政策，结构和技术

B. 组织，技术和信息

C. 硬件，软件和人

D. 资产，威胁和脆弱性

220. 信息网络安全(风险）评估的方法(A)

A. 定性评估与定量评估相结合

B. 定性评估

C. 定量评估

D. 定点评估

221. PDR模型与访问控制的主要区别(A）

A. PDR把安全对象看作一个整体

B. PDR作为系统保护的第一道防线

C. PDR采用定性评估与定量评估相结合

D. PDR的关键因素是人

222. 信息安全中PDR模型的关键因素是(A）

A. 人

B. 技术

C. 模型

D. 客体

223. 计算机网络最早出现在哪个年代(B）

A. 20世纪50年代

B. 20世纪60年代

C. 20世纪80年代

D. 20世纪90年代

224. 最早研究计算机网络的目的是什么？(C）

A. 直接的个人通信;

B. 共享硬盘空间. 打印机等设备;

C. 共享计算资源;

225. 邮件炸弹攻击主要是(B)

A. 破坏被攻击者邮件服务器

B. 添满被攻击者邮箱

C. 破坏被攻击者邮件客户端

226. 最早的计算机网络与传统的通信网络最大的区别是什么？(B）

A. 计算机网络带宽和速度大大提高。

B. 计算机网络采用了分组交换技术。

C. 计算机网络采用了电路交换技术。

D. 计算机网络的可靠性大大提高。

227. 关于80年代Mirros蠕虫危害的描述,哪句话是错误的？(B）

A. 该蠕虫利用Unix系统上的漏洞传播

B. 窃取用户的机密信息，破坏计算机数据文件

C. 占用了大量的计算机处理器的时间，导致拒绝服务

D. 大量的流量堵塞了网络，导致网络瘫痪

228. 以下关于DOS攻击的描述,哪句话是正确的？（C）

A. 不需要侵入受攻击的系统

B. 以窃取目标系统上的机密信息为目的

C. 导致目标系统无法处理正常用户的请求

D. 如果目标系统没有漏洞,远程攻击就不可能成功

229. 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？（C)

A. 安装防火墙

B. 安装入侵检测系统

C. 给系统安装最新的补丁

D. 安装防病毒软件

230. 下面哪个功能属于操作系统中的安全功能（C）

A. 控制用户的作业排序和运行

B. 实现主机和外设的并行处理以及异常情况的处理

C. 保护系统程序和作业，禁止不合要求的对程序和数据的访问

D. 对计算机用户访问系统和资源的情况进行记录

231. 下面哪个功能属于操作系统中的日志记录功能（D）

A. 控制用户的作业排序和运行

B. 以合理的方式处理错误事件，而不至于影响其他程序的正常运行

C. 保护系统程序和作业,禁止不合要求的对程序和数据的访问

D. 对计算机用户访问系统和资源的情况进行记录

232. Windows NT提供的分布式安全环境又被称为(A)

A. 域（Domain)

B. 工作组

C. 对等网

D. 安全网

233. 下面哪一个情景属于身份验证（Authentication）过程（A)

A. 用户依照系统提示输入用户名和口令

B. 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

C. 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

D. 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

234. 下面哪一个情景属于授权（Authorization)（B)

A. 用户依照系统提示输入用户名和口令

B. 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

C. 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

D. 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

235. 下面哪一个情景属于审计（Audit)(D）

A. 用户依照系统提示输入用户名和口令

B. 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

C. 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

D. 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

236. 以网络为本的知识文明人们所关心的主要安全是(C)

A. 人身安全

B. 社会安全

C. 信息安全

237. 第一次出现”HACKER"这个词是在（B）

A. BELL实验室

B. 麻省理工AI实验室

C. AT&T实验室

238. 可能给系统造成影响或者破坏的人包括（A）

A. 所有网络与信息系统使用者

B. 只有黑客

C. 只有跨客

239. 黑客的主要攻击手段包括（A）

A. 社会工程攻击. 蛮力攻击和技术攻击

B. 人类工程攻击. 武力攻击及技术攻击

C. 社会工程攻击. 系统攻击及技术攻击

240. 从统计的情况看，造成危害最大的黑客攻击是(C）

A. 漏洞攻击

B. 蠕虫攻击

C. 病毒攻击

241. 扫描工具(C)

(A）只能作为攻击工具

（B)只能作为防范工具

(C)既可作为攻击工具也可以作为防范工具

242. DDOS攻击是利用进行攻击（C）

A. 其他网络

B. 通讯握手过程问题

C. 中间代理

243. 全国首例计算机入侵银行系统是通过（A）

A. 安装无限MODEM进行攻击

B. 通过内部系统进行攻击

C. 通过搭线进行攻击

244. 黑客造成的主要安全隐患包括（A)

A. 破坏系统. 窃取信息及伪造信息

B. 攻击系统. 获取信息及假冒信息

C. 进入系统. 损毁信息及谣传信息

245. 网络防御中，哪项技术用于确保数据在传输过程中的安全性？（A）

A. 加密

B. 压缩

C. 完整性校验

D. 身份验证

246. 网络防御中，哪项措施可以减少网络拥塞？（C）

A. 限制访问

B. 使用通用账号

C. 优化网络路由

D. 不限制网络访问

247. 网络防御中，哪项策略强调在网络遭受攻击时能够快速恢复正常运行？（D）

A. 预防

B. 检测

C. 响应

D. 灾难恢复

248. 网络防御中，哪项措施有助于防止未授权的远程访问？（A）

A. 实施VPN

B. 使用弱密码

C. 允许所有流量

D. 不限制网络访问

249. 网络防御中，哪项技术用于检测和阻止恶意流量？（B）

A. 防火墙

B. 入侵防御系统

C. 加密

D. 入侵检测系统

250. 网络防御中，哪项措施可以提高网络的透明度？（C）

A. 限制访问

B. 使用通用账号

C. 日志记录和监控

D. 不限制网络访问

251. 计算机网络的安全是指（ C ）

A．网络中设备设置环境的安全

B．网络使用者的安全

C．网络中信息的安全

D．网络的财产安全

252. 信息风险主要是指（ D ）

A．信息存储安全

B．信息传输安全

C．信息访问安全

D．以上都正确

253. 以下（ D ）不是保证网络安全的要素。

A．信息的保密性

B．发送信息的不可否认性

C．数据交换的完整性

D．数据存储的唯一性

254． （ D）不是信息失真的原因。

A．信源提供的信息不完全. 不准确

B．信息在编码. 译码和传递过程中受到干扰

C．信宿（信箱）接受信息出现偏差

D．信息在理解上的偏差

255． （ A ）是用来保证硬件和软件本身的安全的。

A．实体安全

B．运行安全

C．信息安全

D．系统安全

256．黑客搭线窃听属于（ B ）风险。

A．信息存储安全

B．信息传输安全

C．信息访问安全

D．以上都不是

257． （ A ）策略是防止非法访问的第一道防线。

A．入网访问控制

B．网络权限控制

C．目录级安全控制

D．属性安全控制

258．信息不泄露给非授权的用户. 实体或过程，指的是信息（ A ）特性。

A．保密性

B．完整性

C．可用性

D．可控性

259．对企业网络最大的威胁是（ D ） 。

A．黑客攻击

B．外国政府

C．竞争对手

D．内部员工的恶意行为

260．提高 IE 浏览器安全性的措施不包括（ D ） 。

A．禁止使用 Cookies

B．禁止 ActiveX 控件

C．禁止使用 Java 及活动脚本

D．禁止访问国外网站

261．（ C ）是一种登录系统的方法，它不仅绕过系统已有的安全设置，而且还能挫败系统上的各种增强的安全设置。

漏洞

端口

后门

D．服务

262．在（A ）属性对话框中，可以设置几次无效登录后就锁定账户。

A．账户锁定阈值

B．密码策略

C．账户锁定时间

D．复位账户锁定计数器

263．Windows Server 2003 系统的安全日志通过（C ）设置。

A．事件查看器

B．服务管理器

C．本地安全策略

D．网络适配器

264．用户匿名登录主机时，用户名为（D ） 。

A．guest

B．OK

C．Admin

D．Anonymous

265．为保证计算机信息安全，通常使用（C ） ，以使计算机只允许用户在输入正确的保密信息时进入系统。

口令

命令

密码

密钥

266． （ D）不是 Windows 的共享访问权限。

A．只读

B．完全控制

C．更改

D．读取及执行

267．为了保证 Windows Server 2003 服务器不被攻击者非法启动，管理员应该采取（ B ）措施。

A．备份注册表

B．利用 SYSKEY

C．使用加密设备

D．审计注册表和用户权限

268．入侵检测系统是对（D ）的合理补充，帮助网络抵御网络攻击。

A．交换机

B．路由器

C．服务器

D．防火墙

269．防火墙是指（C ） 。

A．一种特定软件

B．一种特定硬件

C．执行访问控制策略的一组系统

D．一批硬件的总称

270．为了保障网络安全，防止外部网络对内部网络的侵犯，多在内部网络与外部网络之间设置（D ） 。

A．密码认证

B．入侵检测

C．数字签名

D．防火墙