**国开电大 2025《24218 网络安全技术》期末考试题库小抄（按字母排版）**

总题量 (472):单选题(232)多选题(75)判断题(140)填空题(10)主观题(15)

**单选题**(232)微信号：zydz_9527

1.[1]1. 对于发弹端口型的木马，（ ）主动打开端口，并处于监听状态。
Ⅰ.木马的客户端 Ⅱ.木马的服务器端
Ⅲ.第三服务器答案：Ⅰ或 Ⅲ

2.AES算法属于哪一类型的加密算法？答案：对称加密

3.AES算法属于哪一类型的算法？（_____）答案：对称加密算法

4.CA认证中心的主要作用是？答案：发放数字证书

5.CA认证中心（证书认证中心）的主要作用是？（_____）答案：发放数字证书

6.CA指的是：（ ）答案：证书授权

7.DDos攻击破坏了（ ）答案：可用性

8.[″]″DES是一种数据分组的加密算法，DES它将数据分成长度为多少位的数据块,其中一部分用作奇偶校验,剩余部分作为密码的长度？″答案：64位

9.DES算法是一种（ ）加密算法。答案：对称密钥

10.SQL注入是一种常见的数据库攻击手段，SQL注入漏洞也是最普遍的漏洞之一。以下哪个工具是SQL注入常用的工具？答案：SQLMap

11.SSL指的是：答案：安全套接层协议

12.Window Server 2003的注册表根键（ ）是确定不同文件后缀的文件类型。答案：HKEY_CLASSES_ROOT

13.Windows操作系统的安全日志通过（ ）设置。答案：本地安全策略

14.[A]安全电子邮件使用（____）协议？答案：PGP

15.[B]包过滤技术与代理服务技术相比较答案：包过滤技术对应用和用户是绝对透明的

16.[B]被动攻击主要是监视公共媒体传输的信息，下列属于典型被动攻击的是（_____）。答案：解密通信数据

17.[B]被动攻击主要是监视公共媒体传输的信息，下列属于典型被动攻击的是答案：解密通信数据

18.[B]病毒为什么会将自己附着在主机可执行程序中？答案：因为病毒不能独立执行

19.[（]（ ）不是防火墙的功能。答案：保护存储数据安全

20.[D]当感觉到操作系统运行速度明显减慢，打开任务管理器后发现CPU的使用率达到100%时，最有可能受到（ ）攻击。答案：拒绝服务

21.[D]当某一服务器需要同时为内网用户和外网用户提供安全可靠的服务时，该服务器一般要置于防火墙的答案：DMZ区

22.[D]当你感觉到你的Win10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。答案：拒绝服务

23.[D]当你感觉到你的电脑运行速度明显减慢，打开任务管理器后发现CPU的使用率达到了百分之百，你认为你受到了哪一种攻击？答案：拒绝服务攻击

24.[D]对称密钥密码体制的主要缺点是：答案：密钥的分配和管理问题

25.[D]对利用软件缺陷进行的网络攻击，最有效的防范方法是答案：及时更新补丁程序

26.[D]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（ ）。答案：状态检测技术

27.[D]对于电子邮件附件，哪一种做法最不安全？答案：打开来自不明发送者的附件

28.[D]对于发弹端口型的木马，（ ）主动打开端口，并处于监听状态。答案：木马的客户端或第三服务器

29.[D]对于数字证书，哪个组织负责其全球互认？（_____）答案：PKI（公钥基础设施）

30.[D]对于数字证书，哪个组织负责其全球互认？答案：PKI

31.[F]防病毒产品可以实施在网络的哪三个层次中？答案：网关、服务器、桌面

32.[F]防火墙技术可分为（ ）等3大类型。答案：包过滤、状态检测和应用代理

33.[F]防火墙一般不负责哪项功能？（_____）答案：多租户管理

34.[F]防火墙中地址翻译（NAT）的主要作用是：答案：隐藏内部网络地址

35.[F]防止用户被冒名所欺骗的方法是：答案：对信息源发方进行身份验证

36.[F]防止重放攻击最有效的方法是答案：使用“一次一密”加密方式

37.[《]《个人信息保护法》的主要立法目的是什么？（_____）答案：保护个人信息权益，规范个人信息处理活动

38.[G]根据Endsley模型，可以将态势感知划分为三个层级，不包括（ ）。答案：安全审计

39.[G]根据Endsley模型，哪一项不是态势感知的三个层级之一？（_____）答案：安全审计

40.[G]根据Endsley模型，哪一项不是态势感知的三个层级之一？答案：事件审计

41.[G]根据秘钥的特点，可以将密码体制分为（_____）。答案：对称和非对称密码体制

42.[G]关于CA和数字证书的关系，以下说法不正确的是：答案：数字证书一般依靠CA中心的对称密钥机制来实现

43.[G]关于勒索软件，下列哪个说法是正确的？答案：勒索软件通过加密文件进行勒索

44.[G]关于勒索软件，以下哪个说明是错误的：答案：解密高手可以破解勒索软件的密钥，从而恢复出被加密的文件

45.[H]黑客利用IP地址进行攻击的方法有：答案：IP欺骗

46.[J]即使域名邮箱配置了SPF和DKIM，添加哪种策略也可以进一步强化电子邮件的安全性？答案：DMARC

47.[J]计算机病毒具有答案：传染性、潜伏性、破坏性

48.[J]计算机病毒是一种答案：程序

49.[J]计算机网络的安全是指（ ）。答案：网络中信息的安全

50.[J]加密技术不能实现：答案：基于IP头信息的包过滤

51.[J]加密算法的功能是实现信息的（ ）：答案：保密性

52.[J]加密算法的功能是实现信息的（_____）。答案：保密性

53.[J]加密算法的功能是实现信息的

（_____），数字签名算法可实现信息的（_____）。答案：保密性，不可否认性

54. [J]加密有对称密钥加密、非对称密钥加密两种，其中对称密钥加密的代表算法是：答案：DES

55. [J]加密有对称密钥加密、非对称密钥加密两种，其中非对称密钥加密的代表算法是：答案：RSA

56. [J]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？答案：地址欺骗

57. [J]进行网络渗透测试通常遵循哪种顺序？答案：侦查阶段、入侵阶段、控制阶段

58. [ (]（ ）就是通过各种途径对所要攻击的目标进行多方面的了解（包括任何可得到的蛛丝马迹，但要确保信息的准确），确定攻击的时间和地点。答案：踩点

59. [J]局域网中如果某台计算机受到了ARP欺骗，那么它发出去的数据包中，（ ）地址是错误的。答案：目标MAC地址

60. [J]拒绝服务攻击答案：用超出被攻击目标处理能力的海量数据包消耗可用系统、带宽资源等方法的攻击

61. [K]口令破解是攻击者常用的手段，以下哪个工具可用于口令破解？答案：hydra

62. [L]勒索软件通常如何进行传播？（_____）答案：邮件附件

63. [ (]（ ）类型的软件能够阻止外部主机对本地计算机的端口扫描。答案：个人防火墙

64. [M]没有网络安全就没有_____，就没有_____，广大人民群众利益也难以得到保障。答案：国家安全、经济社会稳定运行

65. [M]没有网络安全就没有（_____），就没有（_____），广大人民群众利益也难以得到保障。答案：国家安全、经济社会稳定运行

66. [M]没有网络安全就没有（_____），就没有（_____），广大人民群众利益也难以得到保障。答案：国家安全、经济社会稳定运行

67. [M]没有网络安全就没有（_____），就没有（_____），广大人民群众利益也难以得到保障。答案：国家安全、经济社会稳定运行

68. [M]没有网络安全就没有（_____），就没有（_____），广大人民群众利益也难以得到保障。答案：国家安全、经济社会稳定运行

69. [M]没有网络安全就没有（_____），就没有（_____），广大人民群众利益也难以得到保障。答案：国家安全、经济社会稳定运行

70. [M]明文保存的用户口令容易被直接利用，很多系统对口令进行哈希加密运算后再保存。对这种加密后口令，以下哪个说法是正确的：答案：加密储存的口令可以被“撞库”攻击

71. [M]某单位员工收到了一封电子邮件，发件人显示为网络管理员，邮件内容里提示其帐户过期，要求他重置密码，并给出了一个重置密码的链接。该员工点开链接发现网站要求他输入当前使用的用户名和密码。该员工经过观察，发现网站页面内容显示有问题，URL的地址栏并不是熟悉的域名。请问该员工遇到攻击手段的类型是：答案：社会工程攻击

72. [M]某单位员工收到一封电子邮件，提示其账号即将过期，要求其立即通过邮件里的链接更新账号密码，该员工受到的是什么类型的电子邮件攻击？答案：钓鱼邮件攻击

73. [M]某单位员工收到一封仿冒的邮件，要求其立即通过邮件里的链接更新账号密码，该员工受到的是什么类型的电子邮件攻击？（_____）答案：钓鱼邮件攻击

74. [M]某单位员工收到一封仿冒的邮件，要求其立马通过邮件里的链接更新账号密码，该员工受到的是什么类型的电子邮件攻击？答案：钓鱼邮件

75. [M]某单位员工收到一封仿冒邮件，要求其立马通过邮件里的链接更新账号密码，该员工受到了电子邮件什么类型的攻击？答案：钓鱼邮件

76. [M]某网站后台密码过于简单，被黑客破解登录了后台，并篡改了后台登录密码导致管理员无法登录，该网站遭受到了什么类型的攻击？答案：非授权访问

77. [M]木马病毒是：答案：基于服务/客户端病毒

78. [N]哪一部法律明确了个人信息跨境传输规则的相关内容？答案：《中华人民共和国个人信息保护法》

79. [N]哪一部法律是专门针对个人信息处理规则而制定的？答案：《中华人民共和国个人信息保护法》

80. [N]哪一项不是加密算法的主要功能？（_____）答案：不可否认性

81. [N]哪一项不是数字签名算法的主要功能？（_____）答案：保密性

82. [N]哪一项是Endsley模型中的第一个层级？答案：要素感知

83. [N]哪一项是Endsley模型中的最后一个层级？答案：态势预测

84. [N]哪种认证方法最容易受到社会工程学攻击？答案：口令认证

85. [N]哪个选项不是深度学习在网络安全中的应用场景？（_____）答案：线稿上色

86. [N]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？答案：tracert

87. [P]屏蔽路由器型防火墙采用的技术是基于：答案：应用网关技术

88. [Q]区块链技术在安全性方面的一个主要优点是什么？答案：数据不可篡改

89. [Q]全国人民代表大会常务委员会于哪一年表决通过了《中华人民共和国网络安全法》？答案：2016年

90. [R]人脸识别采用了哪个认证技术：答案：基于生物特征

91. [R]入侵检测系统的第一步是：（ ）答案：信息收集

92. [R]入侵检测系统在进行信号分析时，一般通过三种常用的技术手段，以下哪一种不属于通常的三种技术手段：（ ）答案：密文分析

93. [S]设置Windows账户的密码长度最小值，通过（ ）进行设置。答案：本地安全策略

94. [S]使用HTTPS的主要目的是什么？答案：提供数据加密

95. [S]使用HTTPS协议而非HTTP协议的主要目的是什么？（_____）答案：提供数据加密

96. [S]使用哪种方法存储口令最不安全？（_____）答案：明文存储

97. [S]使用哪种语言编写的软件通常更容易出现缓冲区溢出漏洞？答案：C/C++

98. [S]使用数字签名来确保信息在传输过程中没有被篡改，这属于保障了信息的哪个属性？答案：完整性

99. [ (]（ ）是网络通信中标志通信各方身份信息的一系列数据，提供了一种在Internet中认证身份的方式。答案：数字证书

100. [S]收到一条短信，声称你的快递包裹有问题，需要点击链接进行确认，你应该怎么做？（_____）答案：不点击链接，直接联系快递公司客服核实

101. [S]数据安全在云环境中的要求是什么？答案：相对于传统环境更高

102. [S]数据被非法篡改破坏了信息安全的（_____）。答案：完整性

103. [S]数据完整性指的是答案：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
104. [S]数字签名技术是公开密钥算法的一个典型应用，在发送端，采用（ ）对要发送的信息进行数字签名。答案：发送者的私钥
105. [S]数字签名是用来作为：答案：身份鉴别的方法
106. [S]数字签名算法可实现信息的（ ）：答案：不可否认性
107. [S]数字签名算法可实现信息的（_____）。答案：不可否认性
108. [S]数字签名算法主要用于确保信息的哪两项？答案：完整性和不可否认性
109. [S]数字签名为保证其不可更改性，双方约定使用答案：RSA算法
110. [S]数字证书采用公钥体制时，每个用户设定一把公钥，由本人公开，用其进行答案：加密和验证签名
111. [S]随着攻防对抗技术的不断演进，一些漏洞扫描工具在检测目标系统的脆弱点时，还会进行攻击概念验证（POC），从而确认此脆弱点是否可以被利用。以下哪个工具具有攻击概念验证的功能？答案：fscan
112. [S]随着攻防对抗技术的不断演进，在进行检测时往往需要扫描目标机器开放的端口，以下哪个工具或者命令具有扫描开放端口的功能？答案：nmap
113. [S]随着攻防技术对抗的不断演进，一些漏洞扫描工具在检测目标系统的脆弱点时，还会进行攻击的概念验证（POC），从而确认此脆弱点是否可以被利用。以下哪个工具有攻击概念验证的功能：答案：fscan
114. [S]所谓加密是指将一个信息经过（ ）及加密函数转换，变成无意义的密文，而接受方则将此密文经过解密函数、（ ）还原成明文。答案：加密钥匙、解密钥匙
115. [T]态势感知中哪一项需要先于其他项进行？答案：要素感知
116. [W]网络安全的基本属性不包括：答案：不可抵赖性
117. [W]网络安全的基本属性有：可用性、完整性和_____。答案：保密性
118. [W]网络安全的基本属性有：可用性、完整性和保密性，保密性是指对信息资源（_____）的控制。答案：开放范围
119. [W]网络层安全性的优点是：（ ）答案：保密性
120. [W]网络防御技术所包含的访问控制技术内容，不包括（ ）。答案：负载均衡
121. [W]网络防御技术所包含的访问控制技术内容，不包括（ ）。答案：负载均衡
122. [W]网络防御技术所包含的身份认证基本方法，不包括（ ）。答案：基于数字签名的身份认证
123. [W]网络防御技术中，哪项技术常用于阻止未经授权的数据访问？（_____）答案：访问控制
124. [W]网络防御技术中，哪一项不是用于数据保密的？答案：电子邮件过滤
125. [W]网络防御技术中，哪种方法用于识别合法用户？答案：身份认证
126. [W]网络防御中，哪项技术主要用于信息加密？答案：公钥基础设施
127. [W]网络防御中，以下哪种技术是用于预防数据泄露的？答案：数据加密
128. [W]网络监听是答案：监视网络的状态、传输和数据流
129. [W]网络扫描是信息收集的重要手段，以下哪个工具不属于网络扫描工具？答案：ipconfig
130. [W]网络嗅探器（Network Sniffer）常用于网络管理，也经常被攻击者用于信息获取。以下哪个工具可用于网络嗅探？答案：wireshark
131. [W]网络嗅探器（Network Sniffer）常用于网络管理，也经常被攻击者用于信息获取。以下哪个工具可用于网络嗅探？答案：snort
132. [W]网络嗅探器（Network Sniffer）是一种常用的网络管理工具，也常常被攻击者利用来进行信息获取，以下哪个工具可以进行网络嗅探：答案：snort
133. [W]为保证计算机信息安全，通常使用（ ），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。答案：密码
134. [W]为了保证Window Server 2003服务器不被攻击者非法启动，管理员应该采取（ ）措施。答案：使用SYSKEY
135. [W]为确保企业局域网的信息安全，防止来自Internet的黑客入侵，采用（ ）可以实现一定的防范作用。答案：防火墙
136. [X]下列关于VPN的说法中哪一项是正确的？答案：使用VPN技术，可以建立安全通道，并能使用VPN提供的安全服务
137. [X]下列关于防火墙的说法正确的是（ ）。答案：防火墙的安全性能是根据系统安全的要求而设置的
138. [X]下列哪项不是防火墙的部署位置？答案：远程桌面
139. [X]下列哪项不是网络攻击的主要目的？答案：造成人员伤亡
140. [X]下列哪个不是网络攻击的主要目的：答案：造成人员伤亡
141. [X]下面哪个口令安全性相对更高？答案：!@7es6RFE,
142. [X]下面哪个口令安全性相对更高？答案：RM3dkw.tg
143. [X]向有限的存储空间输入超长的字符串属于（____）攻击手段。答案：缓冲区溢出
144. [X]信息不泄漏给非授权的用户、实体或过程，指的是信息（ ）的特性。答案：保密性
145. [X]熊猫烧香病毒是一种答案：蠕虫病毒
146. [Y]要完全杜绝计算机系统受到恶意攻击，应该采取哪种方法？答案：没有万无一失的方法
147. [Y]以下（ ）不是保证网络安全的要素。答案：数据存储的唯一性
148. [Y]以下不属于代理服务技术优点的是答案：可以防范数据泄密
149. [Y]以下不属于代理服务技术优点的是（ ）答案：可以防范数据驱动侵袭
150. [Y]以下关于对称密钥加密说法正确的是：答案：加密密钥和解密密钥必须是相同的
151. [Y]以下关于恶意代码的描述错误的是答案：安全知识、系统补丁和一个好的防病毒软件能有效地保护系统不受恶意代码的威胁
152. [Y]以下关于恶意代码的说法，哪个是错误的：答案：恶意代码无法独立运行，需要与捆绑在正常软件上才能运行。
153. [Y]以下关于防火墙的设计原则说法正确的是：（ ）答案：保持设计的简单性
154. [Y]以下关于非对称密钥加密说法正确的是：（ ）答案：加密密钥和解密密钥是不同的
155. [Y]以下关于宏病毒说法正确的是：答案：宏病毒仅向办公自动化程序编制的文档进行传染
156. [Y]以下关于混合加密方式说法正确的是：答案：采用公开密钥体制对对称密钥体制的密钥进行加密后的通信
157. [Y]以下关于计算机病毒的特征说法正确的是：答案：破坏性和传染性是计算机病毒的两大主要特征
158. [Y]以下关于加密说法正确的是答案：密钥的位数越多，信息的安全性越高
159. [Y]以下关于数字签名说法正确的是：答案：数字签名能够解决篡改、伪造等安全性问题
160. [Y]以下关于数字签名说法正确的是

（_____）。答案：数字签名用于解决篡改、伪造等安全性问题

161. [Y]以下关于云计算安全的说法，哪个是错误的：答案：云计算的用户资源相互会干扰，需要让不同用户使用的资源在物理环境中分开

162. [Y]以下哪项属于防火墙的基本功能？答案：访问控制功能

163. [Y]以下哪一项不是入侵检测系统利用的信息：（　　）答案：数据包头信息

164. [Y]以下哪一项不属于计算机病毒的防治策略：答案：禁毒能力

165. [Y]以下哪一项不属于入侵检测系统的功能：（　　）答案：过滤非法的数据包

166. [Y]以下哪一项属于基于主机的入侵检测方式的优势：（　　）答案：适应交换和加密

167. [Y]以下哪一种方法最有效防范针对口令攻击答案：设置复杂的系统认证口令

168. [Y]以下哪一种方式是入侵检测系统所通常采用的：（　　）答案：基于网络的入侵检测

169. [Y]以下哪一种是防止系统不受恶意代码威胁的良好习惯？答案：学习安全知识、及时更新系统补丁，以及安装一个好的防病毒程序

170. [Y]以下哪一种是防止系统不受恶意代码威胁的最简单最完美的方法？答案：没有这样通用的完美的保护系统的方法

171. [Y]以下哪种不是常见的安全认证技术？答案：基于已有知识的认证技术

172. [Y]以下哪种不是用于保护电子邮件安全的技术？答案：验证码

173. [Y]以下哪种密码体制不需要密钥？答案：ROT13

174. [Y]以下哪种认证方式相对最安全？答案：人脸识别加短信验证码认证

175. [Y]以下哪种认证方式相对最安全？答案：多因素认证

176. [Y]以下哪种是常见的恶意代码类型？（_____）答案：木马

177. [Y]以下哪种是常见的恶意代码类型？（_____）答案：木马、蠕虫、病毒

178. [Y]以下哪种是常见的恶意代码类型？答案：木马

179. [Y]以下哪种是常见的网站拒绝服务攻击技术？答案：HTTP Flood

180. [Y]以下哪种是常见的网站拒绝服务攻击技术？答案：CC攻击

181. [Y]以下哪种算法不属于古典密码体制？答案：RSA算法

182. [Y]以下哪种通用方法可以完美杜绝恶意软件对系统的影响？（_____）答案：没有通用且完美的方法

183. [Y]以下哪个不是常见的恶意代码：答案：细菌

184. [Y]以下哪个不是常见的网络攻击手段：答案：破坏供电系统造成服务器停电

185. [Y]以下哪个不是常见的网络攻击手段？答案：进入机房将服务器下电

186. [Y]以下哪个不是常见的网络攻击手段？答案：物理关机

187. [Y]以下哪个不是防火墙的基本功能：答案：防范钓鱼邮件功能

188. [Y]以下哪个不是防火墙的基本功能？（_____）答案：防垃圾邮件功能

189. [Y]以下哪个不是防火墙的基本功能？答案：防范垃圾邮件功能

190. [Y]以下哪个不是计算机病毒的类别：答案：电子病毒

191. [Y]以下哪个不是计算机病毒的类别？（_____）答案：操作系统病毒

192. [Y]以下哪个不是计算机病毒的类别？答案：朊病毒

193. [Y]以下哪个不是计算机病毒的生命周期：答案：感染阶段

194. [Y]以下哪个不是漏洞数据库：答案：CVE

195. [Y]以下哪个不是预防计算机病毒的方法：答案：不使用容易被猜到弱口令

196. [Y]以下哪个不属于物联网安全防护层次：答案：应用层安全

197. [Y]以下哪个不属于物联网安全防护层次？答案：业务层安全

198. [Y]以下哪个口令相对最为安全？答案：pAsswOrd

199. [Y]以下哪个口令相对最为安全？（_____）答案：p%ss#w8Rd

200. [Y]以下哪个口令相对最为安全？答案：pAsswOrd@3!!

201. [Y]以下算法中属于非对称算法的是答案：RSA算法

202. [Y]以下算法中属于非对称算法的是（_____）。答案：RSA - 以发明者Rivest, Shamir 和 Adleman命名

203. [Y]以下算法中属于非对称算法的是（_____）。答案：RSA

204. [Y]用于电子邮件安全的加密协议叫做（_____）？答案：PGP协议（优良保密协议）

205. [Y]有些病毒为了在计算机启动的时候自动加载，可以更改注册表，（　　）键值更改注册表自动加载项。答案：HKLM\software\microsoft\windows\currentversion\run

206. [Y]有一个主机专门被用作内部网络和外部网络的分界线。该主机有两块网卡，分别连接两个网络。防火墙里面的系统可以与这台主机通信，防火墙外面系统也可以与这台主机通信，这是（　　）防火墙。答案：屏蔽主机式体系结构

207. [Z]在Endsley模型中，态势预测是基于（_____）的。答案：态势理解

208. [Z]在Endsley模型中，态势预测是基于（_____）的。答案：态势理解

209. [Z]在OSI七个层次的基础上，将安全体系划分为四个级别，以下那一个不属于四个级别（　　）答案：链路级安全

210. [Z]在安全审计的风险评估阶段，通常是按什么顺序来进行的：（　　）答案：侦查阶段、渗透阶段、控制阶段

211. [Z]在电子邮件安全中，哪一项策略能够向接收服务器提示如何处理失败的SPF和DKIM检查？答案：DMARC

212. [Z]在公开密钥体制中，加密密钥即（　　）。答案：公开密钥

213. [Z]在古典密码中，哪种方法是基于破译明文攻击的？答案：频率分析

214. [Z]在混合加密方式下，真正用来加解密通信过程中所传输数据（明文）的密钥（　　）答案：对称算法的密钥

215. [Z]在混合加密方式下，真正用来加解密通信过程中所传输数据（明文）的密钥是答案：对称算法的密钥

216. [Z]在建立网站的目录结构时，最好的做法是：答案：按栏目内容建立子目录

217. [Z]在漏洞管理中，哪个麻省理工大学相关的组织负责发布通用漏洞和暴露（CVE）编号？（_____）答案：MITRE

218. [Z]在漏洞管理中，哪个组织负责发布通用漏洞和暴露（CVE）编号？答案：MITRE

219. [Z]在网络安全的三大基本属性中，关注信息不被非授权访问和泄露的是（_____）。答案：保密性

220. [Z]在网络攻击活动中，死亡之PING是（　）类的攻击程序。答案：拒绝服务

221. [Z]在以下古典密码体制中，不属于置换密码的是（　　）：答案：倒序密码

222. [Z]在以下古典密码体制中，不属于置换密码的是答案：凯撒密码

223. [Z]在以下人为的恶意攻击行为中，属于主动攻击的是答案：数据篡改及破坏

224. [Z]在以下人为的恶意攻击行为中，属于主动攻击的是（　）答案：数据篡改及破坏

225.[Z]在云环境中，责任主体（_____）。答案：相对于传统环境更加复杂
226.[Z]针对恶意软件的防御，哪一项是不推荐的？答案：不安装任何第三方软件以确保系统安全
227.[Z]中国国家信息安全漏洞库（China National Vulnerability Database of Information Security）的简称是什么？（_____）答案：CNNVD
228.[Z]中国国家信息安全漏洞库（China National Vulnerability Database of Information Security）的简称是什么？答案：CNNVD
229.[《]《中华人民共和国密码法》主要为了规范（_____）。答案：密码应用和管理
230.[《]《中华人民共和国密码法》主要为了规范答案：密码应用和管理
231.[《]《中华人民共和国网络安全法》正式施行的时间是？答案：2017年6月1日
232.[（]（_____）主要规定了数据加密和保护的相关内容。答案：《中华人民共和国密码法》

**多选题**(75)微信号：zydz_9527
1.[2]2019年5月13日，《信息安全技术网络安全等级保护基本要求》（简称等保2.0）正式发布，并已于2019年12月1日起正式实行。“等保2.0”保护对象包括：答案：基础信息网络（广电网、电信网等）;信息系统（采用传统技术的系统）;云计算平台、以及大数据平台;移动互联、物联网和工业控制系统等
2.CTF（Capture The Flag）中文一般译作夺旗赛，常见的竞赛模式包含哪几项？答案：解题模式（Jeopardy）;
攻防模式（Attack-Defense）;
混合模式（Mix）
3.CTF（Capture The Flag）中文一般译作夺旗赛，在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。常见的CTF竞赛模式有：答案：解题模式（Jeopardy）;攻防模式（Attack-Defense）;混合模式（Mix）
4.PKI系统包含以下哪些部分：答案：权威认证机构CA;证书库;密钥备份及恢复系统;证书废止处理系统;PKI应用接口系统
5.[A]按照对验证对象要求提供的认证凭据的类型数量，认证可以分成：答案：单因素认证;双因素认证;多因素认证
6.[A]按照访问控制方式不同，防火墙可以分为（　　）。答案：包过滤防火墙;应用代理防火墙;状态检测防火墙
7.[A]按照访问控制方式不同，防火墙可以分为哪几种？答案：包过滤防火墙;
应用代理防火墙;
状态检测防火墙
8.[D]当前网络安全面临的主要问题有哪些？答案：APT组织持续对重要行业实施攻击;
个人信息数据泄露风险问题突出;
仿冒诈骗和钓鱼邮件层出不穷
9.[D]电子邮件面临的主要安全威胁包括哪些？（_____）答案：恶意链接;钓鱼邮件;勒索病毒
10.[D]电子邮件面临的主要安全威胁有哪些：答案：钓鱼邮件;勒索病毒;恶意链接
11.[D]端口扫描工具能获取以下哪些信息：答案：端口开放信息;端口提供的服务;主机的操作系统
12.[D]端口扫描工具能获取以下哪些信息？答案：端口开放信息;
端口提供的服务;
主机的操作系统
13.[E]恶意代码的行为表现可能包括哪些？答案：系统破坏;
数据窃取;
非授权访问
14.[E]恶意代码防范技术中，哪些是可行的有效手段？答案：定期更新安全补丁;
安装防火墙;
使用反病毒软件
15.[E]恶意软件主要采用以下哪些传播途径进行传播：答案：软件捆绑;利用漏洞;移动介质;远程下载;社会工程学
16.[E]恶意软件主要通过哪些方式进行传播？答案：软件捆绑;
利用漏洞;
远程下载
17.[F]防范恶意代码需要重点注意的方面有哪些？答案：操作系统更新;
安装安全补丁;
用户安全培训
18.[F]防火墙的典型部署模式包括（　　）。答案：屏蔽主机模式;双宿/多宿主机模式;屏蔽子网模式
19.[F]防火墙根据形态主要有哪些类型？答案：软件防火墙;
硬件防火墙;
专用防火墙
20.[G]高级持续威胁（APT）的特征有：答案：它比传统攻击具有更高的定制程度和复杂程度，需要花费大量时间和资源来研究确定系统内部的漏洞;这类攻击持续监控目标，对目标保有长期的访问权;攻击目标通常是特定的重要目标，攻击方一旦得手，往往会给被攻击目标造成巨大的经济损失或政治影响，乃至于毁灭性打击
21.[G]高级持续威胁（APT）攻击的主要特征包括哪些？答案：高度定制和复杂性;
持续监控目标并保持长期访问权;
攻击目标通常重要，造成巨大的损失或影响
22.[G]根据密码分析者破译时已具备的前提条件，通常将攻击类型分为哪几种？答案：
唯密文攻击;
已知明文攻击;
选择明文攻击
23.[G]关于MITRE公司提出的Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) 网络攻击矩阵模型，哪些说法是正确的？答案：ATT&CK模型从攻击者的视角描述攻击阶段使用的技术;
Enterprise ATT&CK框架包含14个战术阶段;
ATT&CK常见的应用场景包括网络威胁情报收集
24.[G]关于防火墙规则的描述，哪些是错误的？答案：入站规则即你的电脑连接其他主机的规则;
出站规则即其他主机连入你的电脑的规则;
默认情况下防火墙拒绝所有传入连接
25.[G]关于计算机病毒，以下哪些说法是正确的？答案：有些病毒仅能攻击某一种操作系统，如Windows;
病毒一般附着在其他应用程序上;
有些病毒能损坏计算机硬件
26.[G]关于区块链技术的适用场景，以下说法正确的是（_____）。答案：多方参与，缺乏统一背书主体的场景;强调公开透明的场景;信任密集，而非计算存储密集的场景
27.[G]关于网络攻击，哪些因素通常是攻击者的驱动因素？答案：政治因素;
经济利益;
技术炫耀
28.[J]僵尸网络常被用于进行哪些类型的攻击？（_____）答案：发送垃圾邮件;分布式拒绝服务攻击;特定领域攻击
29.[J]近代密码阶段，典型的加密算法包括哪些？答案：RSA;
AES;
DES
30.[K]可以通过以下哪种方式来获取网络安全情报与科技信息（　　）答案：网络安全会议;网络安全期刊;网络安全网站;CTF比赛
31.[L]零信任遵循的原则有：答案：不做任何假定;不相信任何人;随时检查一切;防范动态威胁;做最坏打算
32.[L]零信任遵循的原则有哪些？答案：不做任何假定;
随时检查一切;
防范动态威胁

33. [L]流密码的安全性依赖于哪些因素？答案：密钥序列的随机性；
密钥序列的不可预测性；
收发两端密钥流的精确同步
34. [L]漏洞蠕虫破坏力强、传播速度快，其传播过程一般可以分为哪几个步骤？答案：扫描；
攻击；
复制
35. [L]漏洞蠕虫破坏力强、传播速度快，它的传播过程一般可以分为（　　）步骤。答案：扫描;攻击;复制
36. [L]逻辑隔离的主要技术包括（　　）。答案：虚拟局域网;虚拟路由及转发;多协议标签转换;虚拟交换机
37. [L]洛克希德·马丁公司提出的网络杀伤链（Kill Chain）模型包括哪些阶段？答案：目标侦察（Reconnaissance）；
武器构造（Weaponization）；
载荷投送（Delivery）
38. [M]密码分析学中注重哪几大规律？答案：密码规律；
文字规律；
情况规律
39. [M]目前漏洞挖掘分析技术有多种，主要包括答案：手工测试技术;模糊测试技术;二进制比对技术;静态分析技术;动态分析技术
40. [Q]区块链技术与传统数据库相比，有哪些不同？答案：去中心化；
账本分布存储于多台计算机；
数据不可篡改
41. [Q]区块链技术主要有哪些特点：答案：去中心化;不可篡改;共识
42. [Q]区块链技术主要有哪些特点？答案：去中心化；
不可篡改；
共识
43. [R]认证技术主要有哪些实现方式？答案：口令认证技术；
单点登录技术；
基于生物特征认证技术
44. [R]入侵防御系统主要包括以下几个部分（　　）。答案：应用数据重组;协议识别和协议解析;特征匹配;响应处理
45. [R]入侵检测技术系统分为：答案：基于主机的入侵检测系统;基于网络的入侵检测系统;分布式入侵检测系统
46. [R]入侵检测系统（IDS）的主要功能包括哪些？答案：异常行为识别；
与防火墙联动；
实时保护
47. [R]软件漏洞利用是攻击者利用软件应用程序中的缺陷进行攻击的方法，常见被利用的软件漏洞有：答案：缓冲区溢出漏洞;业务逻辑错误;数据验证问题;身份认证和授权错误;文件处理问题
48. [S]使用VPN技术，可以建立安全通道，并能用VPN提供的安全服务，这些安全服务包括：答案：保密性服务;完整性服务;认证服务
49. [W]网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的（_____）的能力：答案：完整性;保密性;可用性
50. [W]网络攻击的一般过程包括：答案：采集目标信息、脆弱点和漏洞分析；
实施攻击和获取权限；
权限提升、横向移动、后门和持久化
51. [W]网络攻击的主要目的和形式包括哪些？（_____）答案：获得数据;利用资源;破坏业务
52. [W]网站面临的主要安全威胁有哪些：答案：非授权访问;数据泄露;拒绝服务;网站后台管理安全威胁
53. [W]为增强网站和邮件安全，应注意哪些方面？答案：使用强口令；
定期更新安全补丁；
数据备份
54. [W]物联网安全防护主要分为哪几个层次？答案：终端安全；
通信网络安全；
服务端安全
55. [W]物联网安全问题主要分为哪几个层次？答案：终端安全；
通信网络安全；
服务端安全
56. [X]下列哪些步骤属于恶意代码的作用过程：答案：入侵系统;提升权限;实施隐藏;潜伏等待;执行破坏
57. [X]下列哪些是入侵检测系统信息收集的来源？答案：日志文件；
网络流量；
系统目录和文件
58. [X]下列选项中哪些可以增强口令认证的安全性？答案：采用MD5等单向HASH算法保护密码；
在传输过程中对口令进行加密；
采用挑战响应的认证方式
59. [X]下列选项中，哪些选项属于网络安全体系的级别？（_____）答案：网络级安全;系统级安全;应用级安全
60. [X]下列选项中，属于网络安全体系四个级别的是哪些？答案：网络级安全；
系统级安全；
应用级安全
61. [Y]以下哪些是政务网站安全防护的内容：答案：网页防篡改;入侵防御和病毒防护;网络/数据库审计
62. [Y]以下哪些属于身份认证方案的常见类型？答案：基于秘密信息的身份认证；
基于信任物体的身份认证；
基于生物特征的身份认证
63. [Y]以下哪些属于政务网站安全防护的内容？答案：网页防篡改；
网站安全监控；
入侵防御
64. [Y]以下哪些属于政务网站安全防护的内容？答案：网页防篡改；
入侵防御和病毒防护；
网络/数据库审计
65. [Y]以下属于双因素认证的有哪些？（_____）答案：密码加验证码认证;密码加人脸识别认证;电话语音加人脸识别认证
66. [Y]一般来说，认证机制由哪几个部分构成：答案：验证对象;认证协议;鉴别实体
67. [Y]一般来说，认证机制由哪几个部分构成？答案：验证对象；
验证协议；
鉴别实体
68. [Y]邮件安全防护中常用的手段包括哪些？答案：垃圾邮件过滤；
邮件加密；
恶意链接检测
69. [Y]预防计算机病毒，应该注意哪些方面？答案：安装并更新防病毒软件；
确认文件来源后再运行；
及时更新系统和应用补丁
70. [Z]在防范恶意代码方面，哪些技术是有效的？（_____）答案：防火墙;入侵检测系统;蜜罐技术
71. [Z]在网络安全中，哪些是评估系统安全性的关键因素？答案：可用性；
完整性；
保密性
72. [Z]在网络安全中，哪些因素可能导致数据泄露风险增高？（_____）答案：弱密码;未更新的软件;内部人员泄密
73. [Z]在网络杀伤链（Kill Chain）模型中，哪几个步骤直接涉及到植入恶意代码或软件？（_____）答案：武器构造;漏洞利用;安装植入
74. [Z]针对病毒的防护，哪些检测方法是常用的？答案：人工检测；
自动检测；

使用内存监测工具检查

75.[Z]专用防火墙的优势在于什么？（_____）答案：容易配置和管理;本身漏洞较少;处理能力强，性能高

**判断题**(140)微信号：zydz_9527

1.ARP欺骗只会影响计算机，而不会影响交换机和路由器等设备。答案：错

2.DDoS攻击破坏性大，难以防范，也难以查找攻击源，被认为是当前最有效的攻击手法。答案：对

3.DES属于公开密钥算法。答案：错

4.DOS攻击不但能使目标主机停止服务，还能入侵系统，打开后门，得到想要的资料。答案：错

5.GIF和JPG格式的文件不会感染病毒。答案：错

6.IP地址欺骗成功后，被攻击目标机器就没有任何反应了。答案：错

7.IP过滤型防火墙在应用层进行网络信息流动控制。答案：错

8.MITRE公司提出的网络攻击矩阵模型是从防守者视角来描述各阶段攻击技术的模型。答案：×

9.MITRE公司提出的网络攻击矩阵模型是一个站在攻击者视角描述各攻击阶段技术的模型。答案：√

10.MITRE公司提出的网络攻击矩阵模型，它是一个站在防守者的视角来描述攻击中各阶段用到的技术的模型。（　　）答案：错误

11.PGP加密系统不能对磁盘进行加密。答案：错

12.PKI和PMI在应用中必须进行绑定，而不能在物理上分开。答案：错

13.SPF（Sender Policy Framework即“发送方策略框架”）是电子邮件验证中最基本和最常见的保护技术之一。（_____）答案：√

14.SPF是电子邮件验证中最基本和最常见的保护技术之一。答案：√

15.Web应用防火墙是一种用于保护Web服务器和Web应用的网络安全机制。其技术原理是根据预先定义的过滤规则和安全防护规则，对所有访问Web服务器的HTTP请求和服务器响应，进行HTTP协议和内容过滤，进而对Web服务器和Web应用提供安全防护功能。（　　）答案：正确

16.Web应用防火墙用于保护Web服务器和Web应用，提供安全防护功能。答案：√

17.[A]安全大数据分析是指利用大数据手段对网络安全运维相关数据进行分析和挖掘。答案：√

18.[A]安全大数据分析要以建立科学合理的分析模型作为前提。一般认为安全大数据的分析模型包括但不仅限于：规则模型、关联模型、统计模型、异常检测模型等。答案：正确

19.[A]按照网络蠕虫的传播途径和攻击牲，可以分为传统蠕虫、邮件蠕虫和漏洞蠕虫。其中漏洞蠕虫破坏力强、传播速度快。（　　）答案：正确

20.[B]包过滤防火墙可以防御SYN式扫描。答案：错

21.[B]病毒可独立存在，而蠕虫必须寄生在宿主程序中。（_____）答案：错误

22.[B]病毒可独立存在，而蠕虫必须寄生在宿主程序中。答案：×

23.[C]常见的口令破解方式有口令组合、社会工程学、机器学习破解、撞库等。（　　）答案：错误

24.[C]重新格式化硬盘可以清除所有病毒。答案：错

25.[C]存储和处理涉及国家秘密信息的网络的运行安全保护，除遵守《网络安全法》外，还应遵守保密法律和行政法规。答案：√

26.[D]单点登录是指用户访问不同系统时，只需要进行一次身份认证，就可以根据这次认证身份访问授权资源。（　　）答案：正确

27.[D]单点登录是指用户在访问不同系统时，只需进行一次身份认证，然后可根据该认证访问授权资源。答案：√

28.[D]单点登录要求用户在访问不同授权资源时，每次都需进行新的身份认证。答案：×

29.[D]当服务器受到DOS攻击的时候，只需要重新启动系统即可阻止攻击。答案：错

30.[D]当服务器遭受到Dos攻击的时候，只需要重新启动系统就可以攻击。答案：错

31.[D]当前，由于DES密钥长度仅为56位，DES不被视为绝对安全的加密方法。答案：√

32.[D]当硬件配置相同时，代理防火墙对网络运行性能的影响要比包过滤防火墙小。答案：错

33.[D]迪菲（Diffie）和赫尔曼（Hellman）提出的公钥密码系统是密码学历史上的一次革命。答案：正确

34.[D]迪菲和赫尔曼提出的公钥密码系统在保密通信、密钥分配和鉴别等方面具有深远的影响。答案：√

35.[D]抵抗入侵者的第一道防线通常是口令系统。答案：√

36.[D]钓鱼邮件通过冒充正常邮件来骗取用户信任，进而非法获取密码和盗取敏感数据。答案：√

37.[D]对称密码体制的主要优点是加解密速度快。（_____）答案：√

38.[D]多因素认证通过组合多种鉴别信息提升了认证安全性。答案：√

39.[E]恶意代码的传播源于用户软件的漏洞、操作失误或两者结合。（_____）答案：正确

40.[E]恶意代码的传播源于用户软件的漏洞、操作失误或两者结合。答案：√

41.[F]防火墙和网络隔离技术是完全相同的。答案：×

42.[F]防火墙将限制有用的网络服务。答案：对

43.[F]防火墙是一种硬件设备，不能通过软件来实现。答案：×

44.[F]防火墙一般采用“所有未被允许的就是禁止的”和“所有未被禁止的就是允许的”两个基本准则，其中前者的安全性要比后者高。答案：对

45.[F]非授权访问是由网络配置错误导致的。答案：×

46.[F]非授权访问是由于网站服务的技术缺陷导致的安全漏洞。答案：×

47.[G]各单位应按照“谁主管谁负责，谁运营谁负责”的原则，组织对本单位网络和信息系统进行安全监测。答案：√

48.[《]《国家网络安全事件应急预案》主要内容仅包括组织机构和职责。答案：×

49.[H]横向移动是指攻击者从入口点传播到网络其他部分的过程。（_____）答案：√

50.[H]缓冲区溢出并不是一种针对网络的攻击方法。（　）答案：对

51.[H]缓冲区溢出是一种针对网络的攻击方法。答案：错

52.[H]灰鸽子是传统木马，服务器端主动打开端口。答案：错

53.[J]基于生物特征的认证使用如指纹、人脸、视网膜等信息进行身份验证。（_____）答案：√

54.[J]计算机病毒、网络蠕虫和木马是威胁计算机系统和网络安全的主要元素，均属于恶意代码。（_____）答案：√

55.[J]计算机网络的安全是指网络设备设置环境的安全。答案：错

56.[J]计算机信息系统的安全威胁同时来自内、外两个方面。答案：对

57.[J]仅仅通过法律法规就可以实现网络安全目标，不需要考虑安全策略、组织管理、技术措施等因素。答案：×

58. [K]开启帐户策略可以有效防止口令被暴力攻击。答案：对
59. [K]口令是最常用的资源访问控制机制，其安全性很好，不易出现问题。答案：×
60. [K]口令是最常用的资源访问控制机制，也是最容易被突破的。（　　）答案：正确
61. [K]口令通常是最容易被突破的资源访问控制机制。答案：√
62. [M]冒充信件回复、冒名Yahoo发信、下载电子贺卡同意书，使用的是叫做“字典攻击”的方法。答案：错
63. [M]密码分析学主要是在未知密钥的情况下，推演出密文或密钥。答案：√
64. [M]明文保存的用户口令容易被直接利用，因此很多系统采用单向哈希算法进行加密保存。答案：√
65. [M]目标系统存在的漏洞是产生网络安全威胁的唯一原因。答案：×
66. [M]木马有时也称木马病毒，但是它不具有计算机病毒的主要特征。答案：对
67. [M]木马与传统病毒不同的是：木马不自我复制。答案：对
68. [M]目前没有理想的方法可以彻底根除IP地址欺骗。答案：对
69. [M]目前没有任何技术可以帮助我们应对电子邮件面临的安全威胁。答案：×
70. [M]目前使用较多的网络攻击模型主要包括网络杀伤链模型和网络攻击矩阵模型。答案：√
71. [Q]签名仅用于描述网络中正常数据流的特征。答案：×
72. [Q]窃取用户会话cookie后伪装成该用户，即为会话劫持。答案：√
73. [R]认证方式可以分为单项认证、双向认证和第三方认证。答案：√
74. [R]认证机制是实施访问控制的基础性手段。答案：√
75. [R]认证机制是网络安全的基础保护措施，用于实施访问控制。（_____）答案：√
76. [R]认证是一个实体向另外一个实体证明其所声称的能力的过程。（　　）答案：错误
77. [R]认证是一个实体向另一个实体证明其所声称的凭证的过程。答案：×
78. [R]认证是指一个实体向另一个实体证明其声称的身份。答案：√
79. [R]认证通常由标识（Identification）和鉴别（Authentication）两部分组成。答案：√
80. [R]蠕虫既可以在互联网上传播，也可以在局域网上传播。而且由于局域网本身的特性，蠕虫在局域网上传播速度更快，危害更大。答案：对
81. [R]蠕虫能自动寻找漏洞系统，并发起远程连接和攻击以完成自我复制。（_____）答案：√
82. [R]入侵防御技术在攻击到达的同时或之后会发出告警。答案：√
83. [R]入侵防御系统可通过网络流量分析来检测包括缓冲区溢出攻击、木马和蠕虫等入侵行为。答案：√
84. [R]入侵防御系统通过对解析后的报文特征与签名库进行匹配来发现入侵。（_____）答案：√
85. [R]入侵检测系统能够完成入侵检测任务的前提是监控、分析用户和系统的活动。答案：对
86. [S]三重DES能够抵御中途相遇攻击。答案：√
87. [S]社会工程学攻击不容忽视，面对社会工程学攻击，最好的方法是对员工进行全面的教育。答案：对
88. [S]设计初期，TCP/IP通信协议并没有考虑到安全性问题。答案：对
89. [S]使用PGP加密的电子邮件仅需用密码进行电子邮件服务的身份验证。答案：×
90. [S]使用多重DES能提高DES的安全性，并充分利用现有的软硬件系统资源。（_____）答案：√
91. [S]受感染机器间能够协同工作是区分僵尸网络和其他恶意软件的关键特性。答案：√
92. [S]受感染机器间是否能够协同工作是区分僵尸网络和其他恶意软件的重要特征。答案：正确
93. [S]双重DES的密钥长度为112位，能够抵御中途相遇攻击。答案：×
94. [S]随着社会数字化转型的发展，安全漏洞、数据泄露、网络诈骗、勒索病毒等网络安全威胁日益凸显，有组织、有目的的网络攻击形势愈加明显，为网络安全防护工作带来更多挑战。（_____）答案：正确
95. [S]所谓的陷阱帐号是将名为Administrator的本地帐号加上一个超强口令。答案：错
96. [T]特洛伊木马通过伪装成实用程序赢得用户信任，并趁机控制目标主机。答案：√
97. [T]通常防火墙配置规则的次序为：较详细的特殊的规则在前，较普通的规则在后。答案：对
98. [T]通过电话方式骗取用户账号密码属于社会工程学方法。答案：√
99. [T]通过主机入侵检测系统，对操作系统内的可疑行为，如程序、可执行代码和异常操作，能进行实时监视和审计。答案：√
100. [W]网络安全目标的实现需要综合多方面因素，包括但不限于法律法规、安全策略和技术措施。答案：√
101. [W]网络安全体系仅由技术措施组成，不涉及法律法规和组织管理。（_____）答案：×
102. [W]网络安全体系是由各种网络安全单元构成的，共同实现网络安全目标的一种体系架构，包括法律法规、安全策略、组织管理、技术措施等多方面因素。答案：√
103. [W]网络安全应急体系在网络安全工作中越来越重要，网络安全应急工作作为网络安全工作的重要一环，已纳入国家网络安全顶层设计。（_____）答案：√
104. [W]网络防御技术所包含的访问控制技术内容认证包括负载均衡、认证、控制策略实现等几部分。（　　）答案：错误
105. [W]网络隔离技术的主要目的是隔离网络安全威胁，以保证可信网络内的数据信息安全。（_____）答案：√
106. [W]网络隔离技术总体上分为物理隔离和逻辑隔离两类。答案：√
107. [W]网络隔离技术总体上可以分为物理隔离及逻辑隔离两类方法。　（　　）答案：正确
108. [W]网络蠕虫按传播途径和攻击性可分为传统蠕虫、邮件蠕虫和漏洞蠕虫，其中邮件蠕虫主要依赖邮件传播。答案：√
109. [W]网络蠕虫的危害性通常大于计算机病毒，但其生命周期比计算机病毒短得多。答案：√
110. [W]网络社会的发展为违法犯罪分子提供了一个新的领域，但其社会危害性远不如现实社会中的违法犯罪。答案：×
111. [W]网络社会的形成与发展为现实社会中的违法犯罪分子提供了一个新的违法犯罪领域，但其社会危害性不及现实社会中的违法犯罪。（　　）答案：错误
112. [W]网站仿冒是指攻击者通过网站域名欺骗、网站域名劫持、中间人等技术手段，诱骗网站用户访问以获取敏感信息或提供恶意服务。（　　）答案：正确
113. [W]网站假冒仅通过网站域名欺骗进行。答案：×
114. [W]网站假冒涉及攻击者通过域名劫持和中间人技术，以骗取用户敏感信息或提供恶意服务。（_____）答案：√
115. [W]威胁情报的目的是利用公开的资源、数

据、情报等，发现安全威胁并指导企业行动以改善安全状况，可以帮助企业和组织快速了解到敌对方对自己的威胁信息，从而帮助提前威胁防范、攻击检测与响应、事后攻击溯源等能力。答案：正确

116.[W]为防护病毒，需要理解其传播和攻击原理，并根据特性进行检测和消除。答案：√

117.[W]文本文件不会感染宏病毒。答案：错

118.[W]我国网络安全领域的基础性法律《中华人民共和国网络安全法》正式施行，对保护个人信息、治理网络诈骗、保护关键信息基础设施、网络实名制等方面作出明确规定，成为我国网络空间法治化建设的重要里程碑。答案：正确

119.[W]物联网与互联网有本质区别，因此黑客很难攻击物理设备如网络摄像头。（_____）答案：×

120.[Y]移动应用安全和传统的Web安全面临的问题是一样的，可以完全借鉴，不需要专门为移动应用单独考虑安全问题。答案：错误

121.[Y]移动应用安全与传统的Web安全问题相同，不需单独考虑移动应用的安全。答案：×

122.[Y]一般来说，Window XP的进程中有4个以上的svchost.exe进程。答案：对

123.[Y]一般情况下，采用端口扫描可以比较快速了解某台主机上提供了哪些网络服务。答案：对

124.[Y]应根据事件级别，启动相应级别的应急响应流程。答案：√

125.[Y]与IDS相比，IPS具有深层防御的功能。答案：对

126.[Y]云安全是一套包括政策、技术和布署控制方法的广泛体系，用以保护资料和应用程序。答案：√

127.[Y]云环境中的责任主体相对简单。（_____）答案：错误

128.[Y]云环境中的责任主体相对简单。答案：×

129.[Z]在DES加密过程中，S盒对加密的强度不产生影响。答案：×

130.[Z]在DES加密过程中，S盒对加密的强度没有影响。答案：错误

131.[Z]在Outlook Express中仅预览邮件的内容而不打开邮件的附件是不会中毒的。答案：错

132.[Z]在传统的包过滤、代理和状态检测3类防火墙中，只有状态检测防火墙可以在一定程度上检测并防止内部用户的恶意破坏。答案：对

133.[Z]在混合加密体系中，使用对称加密算法对要发送的数据进行加密，其密钥则使用非对称加密算法进行加密。答案：对

134.[Z]在密码学的研究中，应专注于密码算法而非密码破译。答案：×

135.[Z]在设计密码系统时，应遵循Kerckhoffs假设以确保安全性。答案：√

136.[Z]掌握漏洞资源等于掌握了网络安全的绝对主动权。答案：×

137.[Z]支持VLAN的交换机可以通过使用VLAN标签将预定义的端口隔离在各自的广播区域。答案：√

138.[Z]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。答案：错

139.[Z]只要设置了口令，资源就能得到很好的访问控制。（_____）答案：×

140.[Z]状态检测防火墙可以防御SYN式扫描。答案：对

**填空题**(10)微信号：zydz_9527

1.[1]1　是网络安全保障系统的最高层概念抽象，由各种网络安全单元构成的，共同实现网络安全目标的一种体系架构，包括法律法规、安全策略、组织管理、技术措施等多方面因素。答案：网络安全体系

2.[2]2021年11月1日，我国第一步完整规定个人信息处理规则的法律　1　正式施行，厘清了个人信息、敏感个人信息、自动化决策、去标识化、匿名化的基本概念，从适用范围、个人信息处理的基本原则、处理规则、跨境传输规则等多个方面对个人信息保护进行了全面规定。答案：个人信息保护法

3.[D]电子邮件的安全通信主要有 1 和 2 加密手段。答案：端到端加密;PGP加密

4.[G]攻击者通常会在成功入侵后，在目标系统里制造或留下一些　1　，方便再次进入。答案：后门

5.[J]基于行为的身份鉴别是根据（　1　）和风险大小而进行的身份鉴别技术。答案：用户行为

6.[J]加密算法使用用户的　1　进行加密，使用　2　进行解密，数字签名算法使用用户的　3　进行加密，使用　4　进行解密。答案：公钥;私钥;私钥;公钥

7.[L]洛克希德·马丁公司提出的网络杀伤链模型（Kill Chain）将网络攻击活动分成目标侦察、武器构造、载荷投送、　1　、安装植入、　2　、目标行动等七个阶段。答案：漏洞利用;指挥控制

8.[M]密码学按人物可以分为密码　1　学与密码　2　学两个方向。答案：编码;分析

9.[R]认证是一个实体向另外一个实体证明其所声称的　1　的过程。答案：身份

10.[Z]撞库攻击是指通过采集互联网上　1　的用户密码相关数据集，与目标系统的用户信息进行碰撞，从而获得用户密码的过程。答案：泄露

**主观题**(15)微信号：zydz_9527

1.SQL成功注入后,可以通过多种方式对Web服务器进行攻击.

2.防火墙技术有哪些不足之处？试分析防火墙技术的发展趋势。

3.根据实际应用，以个人防火墙为主，简述防火墙的主要功能及应用特...

4.公开密钥体制的主要特点是什么？

5.简述计算机病毒的定义及其破坏性的主要表现。

6.明文为：Wewill graduate from the u...

7.木马攻击的一般过程是什么？

8.什么是SQL注入？SQL注入的基本步骤一般是怎样的？

9.什么是SSL，SSL的工作原理是什么？

10.什么是防火墙？防火墙应具有的基本功能是什么？使用防火墙的好处...

11.什么是拒绝服务攻击？拒绝服务攻击的原理是什么？

12.使用RSA公开密钥体制进行加密。（1）　若p=2，q=5，求...

13.试述网络安全技术的发展趋势。

14.网络安全的含义及特征是什么？

15.网络攻击和防御分别包括哪些内容？

1.SQL成功注入后,可以通过多种方式对Web服务器进行攻击.

答案：答：　攻击方式：

1.　数据库信息泄露：攻击者可以通过注入恶意的SQL语句来获取敏感的数据库信息，如用户名、密码、表结构等，从而进一步入侵和控制数据库。

2.　服务器端执行命令：攻击者可以通过注入特定的SQL语句来执行服务器端的命令，从而获取服务器的控制权，进行恶意操作或横向移动。

3.　文件系统访问：攻击者可以通过注入SQL语句来访问服务器上的文件系统，读取、修改或删除文件，包括敏感的配置文件或用户上传的文件。

4.　远程代码执行：攻击者可以通过注入SQL语句来执行远程的恶意代码，从而在服务器上执行任意的操作，如上传后门、执行破坏性的代码等。

5.　DDOS攻击：攻击者可以利用SQL注入漏洞来发起分布式拒绝服务（DDoS）攻击，通过注入大量的恶意请求，使服务器资源耗尽，导致服

务不可用。
6. 身份伪造和会话劫持：攻击者可以通过注入SQL语句来获取用户的身份信息或会话令牌，从而冒充合法用户或劫持其会话，进行未经授权的操作。 安全措施：
1. 输入验证和过滤：对用户输入进行严格的验证和过滤，确保输入数据的合法性和安全性。
2. 参数化查询或预编译语句：使用参数化查询或预编译语句来构造和执行SQL语句，避免将用户输入直接拼接到SQL语句中。
3. 最小权限原则：为数据库用户和Web服务器分配最小权限，限制其对系统资源的访问和操作。
4. 安全审计和日志记录：记录和监控数据库和服务器的操作，及时发现和响应潜在的攻击行为。
5. 定期更新和维护：及时更新和修补应用程序和服务器的安全漏洞，确保系统的安全性。
2.[F]防火墙技术有哪些不足之处？试分析防火墙技术的发展趋势。
答案：答：1、不足之处：
1、无法检测加密的Web流量。
2、2、普通应用程序加密后，也能轻易躲过防火墙的检测。
3、3、对于Web应用程序，防范能力不足。
4、由于体系结构的原因，即使是最先进的网络防火墙，在防范Web应用程序时，由于无法全面控制网络、应用程序和数据流，也无法截获应用层的攻击。由于对于整体的应用数据流，缺乏完整的、基于会话(Session)级别的监控能力，因此很难预防新的未知的攻击。
2、防火墙技术发展的三个发展趋势：
防火墙可说是信息安全领域最成熟的产品之一，但是成熟并不意味着发展的停滞，恰恰相反，日益提高的安全需求对信息安全产品提出了越来越高的要求，防火墙也不例外，下面我们就防火墙一些基本层面的问题来谈谈防火墙产品的主要发展趋势。

模式转变

传统的防火墙通常都设置在网络的边界位置，不论是内网与外网的边界，还是内网中的不同子网的边界，以数据流进行分隔，形成安全管理区域。但这种设计的最大问题是，恶意攻击的发起不仅仅来自于外网，内网环境同样存在着很多安全隐患，而对于这种问题，边界式防火墙处理起来是比较困难的，所以现在越来越多的防火墙产品也开始体现出一种分布式结构，以分布式为体系进行设计的防火墙产品以网络节点为保护对象，可以最大限度地覆盖需要保护的对象，大大提升安全防护强度，这不仅仅是单纯的产品形式的变化，而是象征着防火墙产品防御理念的升华。

防火墙的几种基本类型可以说各有优点，所以很多厂商将这些方式结合起来，以弥补单纯一种方式带来的漏洞和不足，例如比较简单的方式就是既针对传输层面的数据包特性进行过滤，同时也针对应用层的规则进行过滤，这种综合性的过滤设计可以充分挖掘防火墙核心功能的能力，可以说是在自身基础之上进行再发展的最有效途径之一，目前较为先进的一种过滤方式是带有状态检测功能的数据包过滤，其实这已经成为现有防火墙产品的一种主流检测模式了，可以预见，未来的防火墙检测模式将继续整合进更多的范畴，而这些范畴的配合也同时获得大幅的提高。

就目前的现状来看，防火墙的信息记录功能日益完善，通过防火墙的日志系统，可以方便地追踪过去网络中发生的事件，还可以完成与审计系统的联动，具备足够的验证能力，以保证在调查取证过程中采集的证据符合法律要求。相信这一方面的功能在未来会有很大幅度的增强，同时这也是众多安全系统中一个需要共同面对的问题。

功能扩展

现在的防火墙产品已经呈现出一种集成多种功能的设计趋势，包括VPN、AAA、PKI 、IPSec等附加功能，甚至防病毒、入侵检测这样的主流功能，都被集成到防火墙产品中了，很多时候我们已经无法分辨这样的产品到底是以防火墙为主，还是以某个功能为主了，即其已经逐渐向我们普遍称之为IPS（入侵防御系统）的产品转化了。有些防火墙集成了防病毒功能，这样的设计会对管理性能带来不少提升，但同时也对防火墙产品的另外两个重要因素产生了影响，即性能和自身的安全问题，所以我们的意见是应该根据具体的应用环境来做综合的权衡，毕竟这个世界暂时还不存在什么完美的解决方案。

防火墙的管理功能一直在迅猛发展，并且不断地提供一些方便好用的功能给管理员，这种趋势仍将继续，更多新颖实效的管理功能会不断地涌现出来，例如短信功能，至少在大型环境里会成为标准配置，当防火墙的规则被变更或类似的被预先定义的管理事件发生之后，报警行为会以多种途径被发送至管理员处，包括即时的短信或移动电话拨叫功能，以确保安全响应行为在第一时间被启动，而且在将来，通过类似手机、PDA这类移动处理设备也可以方便地对防火墙进行管理，当然，这些管理方式的扩展需要首先面对的问题还是如何保障防火墙系统自身的安全性不被破坏。

性能提高

未来的防火墙产品由于在功能性上的扩展，以及应用日益丰富、流量日益复杂所提出的更多性能要求，会呈现出更强的处理性能要求，而寄希望于硬件性能的水涨船高肯定会出现瓶颈，所以诸如并行处理技术等经济实用并且经过足够验证的性能提升手段将越来越多的应用在防火墙产品平台上；相对来说，单纯的流量过滤性能是比较容易处理的问题，而与应用层涉及越密，性能提高所需要面对的情况就会越复杂；在大型应用环境中，防火墙的规则库至少有上万条记录，而随着过滤的应用种类的提高，规则数往往会以趋进几何级数的程度上升，这是对防火墙的负荷是很大的考验，使用不同的处理器完成不同的功能可能是解决办法之一，例如利用集成专有算法的协处理器来专门处理规则判断，在防火墙的某方面性能出现较大瓶颈时，我们可以单纯地升级某个部分的硬件来解决，这种设计有些已经应用到现有的产品中了，也许未来的防火墙产品会呈现出非常复杂的结构，当然，从某种角度来说，我们祈祷这种状况最好还是不要发生。

另外根据经验，除了硬件因素之外，规则处理的方式及算法也会对防火墙性能造成很明显的影响，所以在防火墙的软件部分也应该会融入更多先进的设计技术，并衍生出更多的专用平台技术，以期缓解防火墙的性能要求。

综上所述，不论从功能还是从性能来讲，防火墙产品的演进并不会放慢速度，反而产品的丰富程度和推出速度会不断的加快，这也反映了安全需求不断上升的一种趋势，而相对于产品本身某个方面的演进，更值得我们关注的还是平台体系结构的发展以及安全产品标准的发布，这些变化不仅仅关系到某个环境的某个产品的应用情况，更关系到信息安全领域的未来。

3.[G]根据实际应用，以个人防火墙为主，简述防火墙的主要功能及应用特点。
答案：答:天网防火墙,它根据系统管理者设定的安全规则(Security Rules)把守网络,提供强大的访问控制、应用选通、信息过滤等功能。它可以帮你抵挡网络入侵和攻击,防止信息泄露,并可与天网安全实验室的网站(WWW.SKY.NET.CN)相配合,根据可疑的攻击信息,
来找到攻击者。
4.[G]公开密钥体制的主要特点是什么？
答案：答： 1. 双向验证：公开密钥体制使用一对密钥，即公钥和私钥。公钥用于加密和验证数字签名，私钥用于解密和生成数字签名。这种双向验证确保了通信的机密性和完整性。
2. 公钥共享：在公开密钥体制中，公钥是公开可见的，任何人都可以获取到。这样，通信双

方可以通过公钥进行安全通信，而无需事先共享密钥。
3. 数字签名：公开密钥体制使用私钥生成数字签名，用于验证数据的完整性和身份的真实性。数字签名可以防止数据被篡改，并确保数据的来源可信。 4. 密钥管理：公开密钥体制中的密钥管理由权威的证书颁发机构（Certificate Authority，CA）负责。CA颁发数字证书，用于验证公钥的真实性和所有者的身份。
5. 可扩展性：公开密钥体制支持大规模的网络通信，可以轻松地添加新的参与者和公钥，而无需重新分发密钥。
6. 安全性：公开密钥体制的安全性依赖于私钥的保护和公钥的真实性。私钥应该妥善保管，而公钥应该通过数字证书进行验证，以确保通信的安全性。

5.[J]简述计算机病毒的定义及其破坏性的主要表现。
答案：答：病毒是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能够自我复制的一组计算机指令或者程序代码。病毒的破坏性的主要表现：直接破坏计算机上的重要信息；抢占系统资源，降低系统性能；窃取主机上的重要信息；破坏计算机硬件；导致网络阻塞，甚至瘫痪；使邮件服务器、Web服务器不能提供正常服务。

6.[M]明文为：Wewill graduate from the university after four years hard study（不考虑空格）试采用传统的古典密码体系中的凯撒密码（k=3），写出密文。
答案：答：密文：Zhzhoo juhhduh iru wkh xqlwvduh duurz irufh vwdwhv

7.[M]木马攻击的一般过程是什么？
答案：答：木马攻击是指攻击者通过植入木马程序（Trojan horse）来获取对目标系统的控制权，从而进行恶意操作。木马攻击的过程包括以下几个步骤： 1. 植入木马：攻击者通过各种手段将木马程序植入目标系统。这可以通过发送恶意邮件、利用漏洞进行远程执行、社会工程学攻击等方式进行。 2. 启动木马：一旦木马程序被植入目标系统，攻击者会触发木马的启动。这可以通过远程命令、自动执行等方式实现。 3. 建立后门：木马程序会在目标系统上建立一个后门，以便攻击者可以随时远程访问和控制目标系统。这样攻击者就可以绕过系统的正常安全控制，进行未经授权的操作。 4. 探测和获取信息：一旦木马程序建立了后门，攻击者可以通过木马程序探测目标系统的信息，如操作系统版本、网络拓扑等。攻击者还可以获取敏感信息，如用户名、密码、银行账号等。 5. 进一步入侵和控制：攻击者可以利用木马程序的功能来进一步入侵和控制目标系统。这包括执行命令、上传和下载文件、修改系统配置等操作，甚至可以通过木马程序植入其他恶意软件。 6. 持久化和隐藏：为了长期控制目标系统，木马程序通常会采取持久化和隐藏的措施。持久化可以通过修改系统配置、注册表等方式实现，而隐藏可以通过伪装成系统进程、隐藏文件等方式来避免被发现。安全措施： 1. 安装杀毒软件和防火墙：定期更新杀毒软件和防火墙，及时检测和阻止木马程序的入侵。 2. 注意安全意识：提高用户的安全意识，不轻易点击未知来源的链接、下载可疑的附件，避免遭受木马攻击。 3. 定期更新和修补系统漏洞：及时更新和修补操作系统和应用程序的安全漏洞，减少被攻击的风险。 4. 限制权限和访问控制：合理配置系统权限和访问控制，限制非必要的系统访问，减少木马攻击的机会。 5. 定期进行安全审计和监控：定期进行安全审计和监控，及时发现和响应潜在的木马攻击行为。

8.[S]什么是SQL注入？SQL注入的基本步骤一般是怎样的？
答案：答：SSL是Netscape公司为了保证Web通信的安全而提出的一种网络安全通信协议.SS协议采用了对称加密技术和公钥加密技术,并使用了X.509数字证书技术实现了Web客户端和服务器端之间数据通信的保
密性、完整性和用户认证。
工作原理:使用SSL安全机制时,首先在客户端和服务器之间建立连接,服务器将数字证书连同公开密钥一起发给客户端.在客户端,随机生成会话密钥,然后使用从服务器得到的公开密钥加密会话密钥,并把加密后的会话密钥在岗络上传送给服务器.服务器使用相应的私人密钥对接收的加密了的会话密钥进行解密,之后,客户端和服务器端就可以通过会话密钥加密通信的数据了.这样客户端和服务器就建立了一个唯一的安全通信通道
.

9.[S]什么是SSL，SSL的工作原理是什么？
答案：答： SSL（Secure Sockets Layer）是一种加密协议，用于保护在互联网上进行的数据传输的安全性。它是一种基于公钥加密的协议，用于建立安全的通信连接，确保数据在传输过程中的机密性、完整性和身份验证。
SSL的工作原理如下：
1. 握手阶段（Handshake）：在SSL连接建立之前，客户端和服务器之间进行握手协商。这个阶段包括以下几个步骤：
a. 客户端发送一个SSL版本号和加密套件列表给服务器，表示客户端支持的SSL版本和加密算法。
b. 服务器从客户端发送的加密套件列表中选择一个加密套件，并发送自己的SSL证书给客户端。该证书包含服务器的公钥和其他相关信息。
c. 客户端验证服务器的SSL证书的有效性，包括检查证书的签名、有效期等。如果验证通过，客户端生成一个随机的对称密钥，并使用服务器的公钥加密后发送给服务器。
d. 服务器使用自己的私钥解密客户端发送的密钥，得到对称密钥。
2. 密钥交换阶段（Key Exchange）：在握手阶段完成后，客户端和服务器都拥有了相同的对称密钥，用于加密和解密数据。在密钥交换阶段，客户端和服务器使用对称密钥进行加密和解密通信。
3. 数据传输阶段（Data Transfer）：在密钥交换完成后，客户端和服务器之间的通信将使用对称密钥进行加密和解密。这样可以确保数据在传输过程中的机密性和完整性。 SSL通过使用非对称加密和对称加密相结合的方式，实现了安全的数据传输。非对称加密用于在握手阶段进行身份验证和密钥交换，而对称加密用于实际的数据传输，因其效率高，适合大量数据的加密和解密操作。 SSL协议的工作原理和加密算法的选择可以保护数据的机密性和完整性，并防止中间人攻击和数据篡改。它在保护网上交易、用户隐私和敏感数据传输方面起到了重要的作用。

10.[S]什么是防火墙？防火墙应具有的基本功能是什么？使用防火墙的好处有哪些？
答案：答： 防火墙（Firewall）是一种网络安全设备或软件，用于监控和控制网络流量，以保护网络免受未经授权的访问、攻击和恶意活动的影响。它位于网络边界，通过策略和规则来过滤和管理进出网络的数据流量。 防火墙应具有以下基本功能： 1. 包过滤：防火墙可以检查网络数据包的源地址、目标地址、端口号等信息，并根据预设的规则来决定是否允许通过或阻止。 2. 访问控制：防火墙可以基于网络协议、应用程序、用户身份等因素来限制和控制对网络资源的访问。 3. NAT（网络地址转换）：防火墙可以使用NAT技术将内部网络的私有IP地址转换为公共IP地址，以隐藏内部网络的真实拓扑结构。 4. VPN支持：防火墙可以提供虚拟专用网络（VPN）的支持，用于安全地远程访问和连接分支机构。 5. 日志记录和审计：防火墙可以记录网络流量和事件日志，以便进行安全审计、故障排查和威胁分析。 使用防火墙的好处包括： 1. 网络安全增强：防火

墙可以阻止未经授权的访问和恶意攻击，提高网络的安全性。 2. 数据保护：防火墙可以检测和阻止未经授权的数据传输，防止数据泄露和信息被盗取。 3. 网络性能优化：防火墙可以对网络流量进行管理和优化，提高网络的性能和响应速度。 4. 合规性要求满足：防火墙可以帮助组织满足合规性要求，如PCI DSS（支付卡行业数据安全标准）等。 5. 网络资源管理：防火墙可以限制和控制对网络资源的访问，帮助组织更好地管理和分配网络资源。

11.[S]什么是拒绝服务攻击？拒绝服务攻击的原理是什么？

答案：答：拒绝服务攻击（Denial of Service，简称DoS）是一种网络攻击方式，旨在通过超载目标系统的资源，使其无法正常提供服务。攻击者通过发送大量的请求或占用系统资源，导致系统过载，从而使合法用户无法访问或使用目标系统。

拒绝服务攻击的原理如下：

1. 资源耗尽：攻击者利用系统的漏洞或弱点，发送大量的请求或占用系统资源，如网络带宽、CPU、内存等，以消耗目标系统的资源。

2. 阻塞服务：攻击者可以通过发送大量的请求，使目标系统的服务队列或连接池耗尽，导致正常用户的请求无法得到处理，从而阻塞服务。

3. 系统崩溃：攻击者可以通过发送恶意的请求或利用系统漏洞，导致目标系统崩溃或重启，使系统无法正常运行。

4. 网络堵塞：攻击者可以通过向目标系统发送大量的网络流量，使网络带宽或网络设备过载，导致网络拥塞，影响正常的网络通信。

拒绝服务攻击的目的通常有以下几种：

1. 竞争优势：攻击者可能是竞争对手，通过使目标系统无法正常运行，获得竞争上的优势。

2. 报复或破坏：攻击者可能是受害者或对目标系统持有敌意，通过拒绝服务攻击来报复或破坏目标系统。

3. 威胁勒索：攻击者可能以拒绝服务攻击威胁目标系统，要求支付赎金或达到其他目的。

为了防止拒绝服务攻击，可以采取以下措施：

1. 流量分析和过滤：通过网络设备或防火墙，对入站流量进行分析和过滤，过滤掉异常或恶意的流量。

2. 负载均衡和容灾备份：通过负载均衡器和容灾备份机制，将流量分散到多个服务器上，以分担压力和提高系统的可用性。

3. 防火墙和入侵检测系统：配置和更新防火墙和入侵检测系统，及时发现和阻止拒绝服务攻击。

4. 限制资源使用：对系统资源进行限制和调整，限制每个用户或IP地址对系统资源的使用，以防止资源被耗尽。

5. 安全审计和日志记录：记录和监控系统的操作和事件，及时发现和响应潜在的拒绝服务攻击。

12.[S]使用RSA公开密钥体制进行加密。（1） 若p=2，q=5，求公钥e,私钥d？）给出明文m＝2的加解密过程。

答案：答:设 p=2， q=5,n=2*5=10,(n)=(2-1)*(5-1)=4,选择e=3,公钥为(e,n)=(3,10),计算d,(d*e) mod 4=1; d=3; 私钥d,n)=(3,10)。设明文m=2 加密(2)3 mod 10 = 8,解密(8)3 mod 15 = 2

13.[S]试述网络安全技术的发展趋势。

答案：答：

（1）从技术发展的角度看：深度的内容安全是目前热点的技术研究方向。

（2）从产品演变的趋势看，多功能的UTM（统一威胁管理）已经成为新一代安全防护的发展方向。

（3）从硬件支撑方面看，基于多核+FPGA硬件架构已经成为安全业务网关的主流平台。

（4）从解决方案的建设思路看，要实现从被动防御到主动防御，从局部安全到智能安全防护的转变。形成以安全管理中心为主的主动防御体系。

14.[W]网络安全的含义及特征是什么？

答案：答：网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

网络安全的特征：保密性：信息不泄露给非授权的用户、实体或过程，或供其利用的特性。完整性：数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。可用性：可被授权实体访问并按需求使用的特性，即当需要时应能存取所需的信息。网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。可控性：对信息的传播及内容具有控制能力。

15.[W]网络攻击和防御分别包括哪些内容？

答案：答：(1)网络监听:自己不主动去攻击别人,而是在计算机上设置一个程序去监听目标计算机与其他计算机通信的数据。(2)网络扫描:利用程序去扫描目标计算机开放的端口等,目的是发现漏洞,为入侵该计算机做准备。(3)网络入侵:当探测发现对方存在漏洞后,入侵到目标计算机获取信息。(4)网络后门:成功入侵目标计算机后,为了实现对“战利品”的长期控制,在目标计算机中种植木马等后门。(5)网络隐身:入侵完毕退出目标计算机后,将自己入侵的痕迹清除,从而防止被对方管理员发现。防御技术主要包括以下几个方面。(1)安全操作系统和操作系统的安全配置:操作系统是网络安全的关键。(2)加密技术:为了防止被监听和数据被盗取,将所有的数据进行加密。(3)防火墙技术:利用防火墙,对传输的数据进行限制,从而防止被入侵。(4)入侵检测:如果网络防线最终被攻破,需要及时发出被入侵的警报。(5)网络安全协议:保证传输的数据不被截获和监听。