

全国 2015 年 4 月高等教育自学考试

计算机网络安全试题

课程代码:04751

请考生按规定用笔将所有试题的答案涂、写在答题纸上。

选择题部分

注意事项:

1. 答题前,考生务必将自己的考试课程名称、姓名、准考证号用黑色字迹的签字笔或钢笔填写在答题纸规定的位置上。
2. 每小题选出答案后,用 2B 铅笔把答题纸上对应题目的答案标号涂黑。如需改动,用橡皮擦干净后,再选涂其他答案标号。不能答在试题卷上。

一、单项选择题(本大题共 15 小题,每小题 2 分,共 30 分)

在每小题列出的四个备选项中只有一个是符合题目要求的,请将其选出并将“答题纸”的相应代码涂黑。错涂、多涂或未涂均无分。

1. PPDR 模型中,D 代表  
A. 安全策略                      B. 检测                              C. 防护                              D. 响应
2. 以下对拒绝服务攻击的描述,正确的是  
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. 使系统响应减慢,阻止合法用户获得服务  
D. 若目标系统没有漏洞,远程攻击就不会成功
3. 端到端加密位于 OSI  
A. 网络层以上                      B. 网络层以下                      C. 数据链路层以下                      D. 物理层
4. 机房内的相对湿度一般控制在  
A. 10%~30%                      B. 40%~60%                      C. 70%~80%                      D. 80%~90%
5. 静电对电子设备的损害的特点不包括  
A. 隐蔽性                              B. 潜在性                              C. 复杂性                              D. 稳定性
6. 单钥加密算法的典型代表是  
A. RSA                                  B. DSR                                  C. DES                                  D. DER
7. 已知凯撒密码加密变换  $e_k(m) = (3+m) = c \pmod{26}$ ,若明文为字母 A,则密文为字母  
A. A                                      B. B                                      C. C                                      D. D
8. IDEA 算法的明文块与密文块都是  
A. 32bit                                  B. 56bit                                  C. 64bit                                  D. 128bit

9. SSL 的中文含义是

- A. 电子信息交换      B. 安全套接字层      C. 信息交易      D. 金融交易

10. 基于 libpcap 的轻量级网络入侵检测系统是

- A. x-Probe      B. NMAP      C. Snort      D. PGP

11. 下列说法正确的是

- A. 网络防火墙不能解决来自内部网络的攻击和安全问题  
B. 网络防火墙可以防止自然或人为的故意破坏  
C. 网络防火墙可以防止本身安全漏洞的威胁  
D. 网络防火墙可以防止受病毒感染的文件的传输

12. 若漏洞威胁描述为“低影响度,中等严重度”,则该漏洞威胁等级为

- A. 1 级      B. 2 级      C. 3 级      D. 4 级

13. 下列属于按照寄生方式分类的病毒类型是

- A. 嵌入型病毒      B. 外壳型病毒      C. 源码型病毒      D. 引导型病毒

14. 关于校验和法检测病毒的特点,下列说法错误的是

- A. 若遇到变更口令,会发生误报警      B. 不能识别病毒名称  
C. 对隐蔽性病毒同样有效      D. 方法简单能发现未知病毒

15. “禁止跟踪中断”属于

- A. 隐藏技术      B. 反动跟踪技术      C. 反静态跟踪技术      D. 加密技术

## 非选择题部分

注意事项:

用黑色字迹的签字笔或钢笔将答案写在答题纸上,不能答在试题卷上。

二、填空题(本大题共 10 小题,每小题 2 分,共 20 分)

16. 计算机网络安全是指利用管理控制和技术措施,保证信息数据的机密性、\_\_\_\_\_及  
可使用性受到保护。

17. GB2887-2000 将供电方式分为三类,其中一类供电需建立\_\_\_\_\_供电系统。

18. 认证技术可以分为三个层次:\_\_\_\_\_、认证体制和密码体制。

19. 代理服务分为应用层网关和\_\_\_\_\_。

20. NAT 有三种类型:静态 NAT、动态地址 NAT 和\_\_\_\_\_。

21. 入侵检测采用误用检测或\_\_\_\_\_的方式,发现非授权或恶意的系统及网络行  
为,为防范入侵行为提供有效的手段。

22. 入侵检测系统有基于数据源、基于检测理论和基于\_\_\_\_\_的分类方法。

23. IDXP 的中文全称为\_\_\_\_\_。

24. 恶意代码的生存技术主要包括 4 个方面:反跟踪技术、加密技术、模糊变换技术和\_\_\_\_\_。

25. 常见的网络通信隐蔽技术有 http tunnel 和\_\_\_\_\_。

### 三、简答题(本大题共 6 小题,每小题 5 分,共 30 分)

26. 物理安全主要包括哪四个方面?

27. 简述单钥密码体制的本质特征。

28. 简述状态检测防火墙的优点。

29. 简述分布式入侵检测的技术难点。

30. 恶意代码按照工作原理和传输方式分为哪几类?

31. 网络信息安全包括了建立安全环境的哪几个重要组成部分?

### 四、综合分析题(本大题共 2 小题,每小题 10 分,共 20 分)

32. 已知某用户的 RSA 公钥  $e$  为 3, 私钥  $d$  为 7, 模  $n$  为 33。设要进行数字签名的消息  $m=3$ , 要求:

(1) RSA 密钥对中, 哪个密钥用于对消息  $m$  进行数字签名? (选填: 公钥/私钥)

(2) 计算数字签名的结果, 即密文  $s$  的值。

(3) 对密文  $s$  进行解密, 将计算解密的  $t$  与原来的消息进行比较, 即对数字签名进行验证。

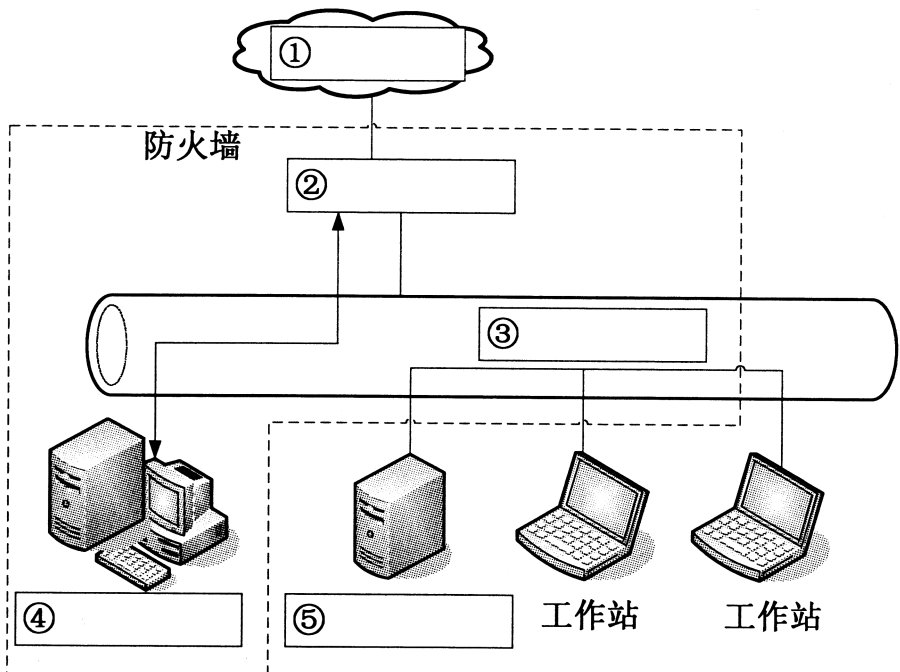
33. 根据防火墙的体系结构知识回答下列问题。

(1) 补充完整题 33 图中①~⑤处的组件名称。(在答题纸相应位置作答)

可选组件: 外部网络、堡垒主机、路由器、内部主机、内部网络

(2) 题 33 图所示是哪种防火墙的体系结构?

(3) 试分析题 33 图的防火墙体系结构存在的安全弱点和解决办法。



题 33 图