随堂作业之四

1. 在 Linux2.6 以上系统中，如果一个用户 X 要将其文件 file 的读的权限授予 Y 用户，Y 用户与 X 用户属于统一用户组 group1，下面哪个操作是正确的？(　　)
   A. chmod 740 file
   B. chmod g+r file
   C. chmod u+r file
   D. setfacl –m u:Y:r, file

2. 多级安全定义了安全级由密级和范畴集合组成，假设主体 A 的安全级为{top secret: NATO，NUCLEAR，CRYPTO}，客体 X 的安全级为{secret: NATO，NUCLEAR}，客体 Y 的安全级为: {top secret: NATO，CRYTPO}，请根据 BLP 简单安全规则和*规则，判定 A 对 X,Y 的访问权限 ？ (　　)
   A. A 允许读 X，允许 写 Y
   B. A 允许读 X，允许 读 Y
   C. A 允许写 X，允许 读 Y
   D. A 允许写 X，允许 写 Y

3. 可追踪机制主要包括哪些机制?
   A. 标识与鉴别
   B. 客体重用
   C. 可信路径
   D. 安全审计

4. 用户在登录、定义用户的安全属性或改变文件的安全级时，他必须确定自己是在与真实的安全内核通信，而不是与一个特洛伊木马打交道。为此，系统必须提供的机制是什么？(　　)
   A. 标识与鉴别
   B. 强制访问控制
   C. 可信路径
   D. 自主访问控制

5. 对用户建立可信路径的实现方法是，使用通用终端向核心发一个特殊信号，这个信号是不可信软件无法拦截、覆盖或伪造的，这个信号称为安全注意键。Linux 系统中实现的安全注意键是那些键的组合？(　　)
   A. Ctrl + Alt + Del
   B. Alt + SysRq + k
   C. Ctrl + Shift + Space
   D. Alt + Ctrl + C

6. 安全审计的主要目的是检测和阻止那些行为？(　　)
   A. 非法用户对计算机系统的入侵行为
   B. 合法用户的误操作
   C. 系统的意外错误和故障
   D. 管理员的权限滥用

7. 连续保护机制主要包括哪些机制？(　　)
   A. 最小特权管理
   B. 隐蔽通道分析
   C. 系统完整性保护
   D. 可信恢复

8. 最小特权原则主要是为了减少哪些危害行为？(　　)
   A. 管理员的误操作
   B. 管理员滥用特权
   C. 特权程序意外出错
   D. 特权程序被恶意利用

9. 在操作系统中实现最小特权管理，需要将超级用户的特权进行划分，并通常是分别分配

给 4 个不同的管理员，包括：安全管理员、安全操作员、审计员和网络管理员等。根据课程介绍，你认为系统安全策略的配置权限应该分给如下哪个管理员？(　　)
A. 网络管理员
B. 安全审计员
C. 安全操作员
D. 安全管理员

10. 操作系统的系统调用 exec 是以新的进程映像去代替原来的进程映像，也就是说，exec 系统调用并没有创建新的进程，只是替换了原来进程上下文的内容，例如：进程的代码段、数据段、堆栈段被替换了。关于 exec 这种说法正确的本质原因是什么？(　　)
A. exec 时，进程的真实用户标识不变
B. exec 时，进程的有效用户标识不变
C. exec 时，进程的 PID 保持不变
D. exec 时，进程的权能状态不变

11. 根据收发双方利用的共享资源不同，隐蔽通道通常分为哪两种类型？(　　)
A. 隐蔽存储通道
B. 潜在隐蔽通道
C. 隐蔽定时通道
D. 真实隐蔽通道

12. TCSEC 从哪个级别开始要求对系统的隐蔽通道进行分析，CC 标准又是从哪个级别开始要求的？(　　)
A. TCSEC B1, CC EAL 4
B. TCSEC B2, CC EAL 4
C. TCSEC B2, CC EAL 5
D. TCSEC B3, CC EAL 5

13. 隐蔽通道分析可以在从抽象的安全模型到系统机器代码的任何一个层次上进行，共享资源矩阵法主要适用于在哪个层次进行隐蔽通道分析？(　　)
A. 安全模型级
B. 描述性顶层规范级
C. 源代码级
D. 机器代码级

14. Tsai 等人提出的带有语义分析的信息流法，可以从源代码级标识隐蔽通道。试问，从源代码级标识隐蔽通道具有的明显优点有哪些？(　　)
A. 能找出所有隐蔽通道（除了硬件导致的通道以外）
B. 能找出所有隐蔽存储通道（除了硬件导致的通道以外）
C. 能找出放置审计代码、延迟和噪音的位置
D. 能评估访问控制检查点是否设置得合适

15. 隐蔽通道的常用处理方法主要有消除、限制带宽和审计三种，根据你对本课程提及的基于最近访问时间的隐蔽通道原理的理解，你认为这种通道可以采取哪些方法进行处理？(　　)
A. 消除
B. 加入噪音
C. 加入延时
D. 审计

16. 传输过程中对数据的完整性进行保护有多种要求，其中要求由接收者 TCB 自己，无需来自源可信 IT 产品的任何帮助，即能恢复被破坏的数据为原始用户数据，这属于那种要求？(　　)
A. 数据交换完整性检测
B. 目的数据交换恢复
C. 源数据交换恢复
D. 基本回退

答案参考：（仅代表 chatgpt）

1. (B)
2. (B)
3. (A, C, D)
4. (A)
5. (B)
6. (D)
7. (A, C, D)
8. (B)
9. (C)
10. (B)
11. (A, C)
12. (A)
13. (C)
14. (C)
15. (B, C)
16. (C)