武汉大学计算机学院

2016－2017 学年度

《网络安全》期末考试试卷　(A)

学号：　　姓名：　　专业：　　班级：　　分数：

说明：所有答案直接写在试卷上相应地方，　将答案写在试卷之外的其它纸张上的，　一律无效。

一、选择题：以下每题有　A、B、C、D 四个答案，将最恰当的一个的号码（　A、B、C、D）填写在下面的答案表中。每题　2 分，共 15 题、30 分。

答案表

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

1. 从攻击目的的角度来讲，下列哪一种攻击不属于破坏型攻击
   A. 拒绝服务攻击
   B. Ping of Death 攻击
   C. 后门程序攻击
   D. TearDrop 攻击

2. 下列关于逻辑炸弹攻击的说法，哪种是错误的
   A. 比较短小，附着在系统或文件上
   B. 触发方式包括时间触发、特定操作触发等
   C. 能够自动复制，具备传染性
   D. 攻击性强，会删除系统内程序、破坏数据等

3. 能够提供保密性的　IPSec 技术是
   A. AH
   B. ESP
   C. 传输模式
   D. 隧道模式

4. 在以下人为的恶意攻击行为中，属于主动攻击的是
   A. 数据篡改及破坏
   B. 数据窃听
   C. 数据流分析
   D. 非法访问

5. Biba 模型实现强制访问控制的基本思想是
   A. 高完整性进程可以读、但不能写低完整性信息；低完整性进程可以写、但不能读高完整性信息
   B. 高完整性进程可以写、但不能读低完整性信息；低完整性进程可以读、但不能写高

完整性信息

C. 高完整性进程可以读、写低完整性信息；低完整性进程可以读、但不能写高完整性信息

D. 高完整性进程可以读、写低完整性信息；低完整性进程不能读、写高完整性信息

6. 以下哪一项不属于入侵检测系统的功能：

A. 监视网络上的通信数据流

B. 捕捉可疑的网络活动

C. 提供安全审计报告

D. 过滤非法的数据包

7. 在防火墙的规则中， Reject的处理方式为：

A. 允许数据包或信息通过，并且通知信息源该信息被允许通过

B. 拒绝数据包或信息通过，并且通知信息源该信息被禁止

C. 直接将数据包或信息丢弃，并且不通知信息源

D. 直接将数据包或信息丢弃，并且通知信息源

8. 下列概念中，不能用于身份认证的手段是

A. 杀毒软件

B. 虹膜

C. 用户名和密码

D. 智能卡

9. 在防火墙技术中，包过滤技术与代理服务技术相比较

A. 包过滤技术安全性较弱、但会对网络性能产生明显影响

B. 包过滤技术对应用和用户是绝对透明的

C. 代理服务技术安全性较高、但不会对网络性能产生明显影响

D. 代理服务技术安全性高，对应用和用户透明度也很高

10. 下列关于入侵检测系统 IDS 的说法，哪种是错误的

A. IDS 主要通过模式匹配、异常统计或状态分析等方法来确定入侵行为

B. IDS 通过监视网络和系统资源使用情况来检测入侵行为， 并能主动地对入侵活动和攻击性网络流量进行拦截

C. 基于异常 IDS 具备自学习能力，能检测出全新的入侵行为并补充到模式数据库中

D. 基于误用 IDS 通过对检查各个主体、 对象统计量的偏差， 从而检测出不正常的行为

11. 以下关于计算机病毒的特征说法正确的是

A. 计算机病毒只具有破坏性，没有其他特征

B. 计算机病毒具有破坏性，不具有传染性

C. 破坏性和传染性是计算机病毒的两大主要特征

D. 计算机病毒只具有传染性，不具有破坏性

12. VPN 为保证通信的安全性采用了

A. 身份验证

B. 隧道协议

C. 数据加密

D. 以上三种均采用

13. 以下关于 VPN 说法正确的是
    A. VPN 指的是用户自己租用线路，和公共网络物理上完全隔离的、安全的线路
    B. VPN 指的是用户通过公用网络建立的临时的、安全的连接
    C. VPN 不能做到信息认证和身份认证
    D. VPN 只能提供身份认证、不能提供加密数据的功能

14. 哪种扫描与网络安全无关
    A. 帐号扫描
    B. 图像扫描
    C. 漏洞扫描
    D. 端口扫描

15. 下列活动中不属于入侵检测系统的是
    A. 识别反映已知进攻的活动模式
    B. 异常行为模式的统计分析
    C. 将攻击者从关键系统引诱开并能记录所有行为
    D. 操作系统的审计跟踪管理，并识别用户违反安全策略的行为

二、判断题。如果判断为错误，请说明理由（每题 **2** 分，共 **10** 分。）

答案表

1	2	3	4	5

1. 基于误用 IDS 具备自学习能力，能检测出全新的入侵行为并补充到模式数据库中。
2. 利用 ICMP 数据包来发现远程主机开放的端口以及服务的方法叫作主机扫描。
3. 用户和资源都是一个固定的安全属性， 系统利用安全属性来决定一个用户是否可以访问某个资源，这种方式叫作自主访问控制（ DAC）。
4. 在双向 IP 欺骗中攻击者不考虑回传的数据包。
5. 逻辑炸弹是计算机入侵者攻击网上其它计算机成功后为方便下次进入这台被攻击计算机而采取的一些欺骗手段和程序。

三、名词解释题（每题 **3** 分，共 **15** 分。）

1. 基于网络的入侵检测系统。
2. 包过滤防火墙。
3. 计算机病毒。
4. 缓冲区溢出攻击。
5. 强制访问控制。

四、简答题（每题　**9**分，共 **45**分。）

1. 网络攻击一般可分为几个步骤（或阶段）？分别指出各步骤（或阶段）的主要内容及相关注意事项。

2. 试说明逻辑炸弹与病毒有哪些相同点与不同点？

3. 简述 TearDrop攻击的基本原理，并指出如何防范　TearDrop攻击。

4. 防火墙所使用的主要技术有哪些，并分别指出其各自的概念。

5. 基于误用和基于异常两种方式的　IDS 引擎的各自特征，分析其各自的优势和劣势。