1. 被动攻击包括\_\_传输报文泄露\_\_\_和\_通信流量分析\_\_\_。
2. 网络安全信息服务应包括\_机密性服务，完整性服务，可用性服务，可审计服务\_。
3. 服务器检测到Dos攻击，若攻击数据包里面源IP和目的IP相同，则该Dos攻击可能为\_Land攻击;若服务器接收到大量的ICMP-Echo-Reply响应包，则该Dos攻击可能为\_Smurf\_攻击;若服务器上面出现大量的TCP半连接，则该Dos攻击可能为\_SYN Flood\_攻击。
4. 因特网的域名系统被设计成一个\_联机分布式数据库系统\_，并且采用\_分层树状结构\_的命名方法。
5. DNS查询方式分为递归查询和迭代查询，客户端与服务器之间通常采用\_递归查询\_,服务器之间通常采用\_迭代查询\_。
6. 端口扫描某服务器，若发现53号端口开放，则该服务器可能开放的服务是\_DNS\_；若发现23号端口开放，则该服务器可能开放的服务是\_Telnet\_;若发现21号端口开放，则该服务器可能开放的服务是\_FTP\_。
7. 秘密扫描技术是一种\_\_不被审计工具所检测\_的端口扫描技术，现有的秘密扫描技术有\_\_TCP FIN,TCP ACK,TCP NULL,TCP XMAS,TCP分段扫描\_。其中\_TCP ACK\_扫描无法获得目标主机端口开放情况。
8. 安全策略的实施原则有\_\_最小特权原则，最小泄露原则，多级安全策略\_\_。
9. 强制访问控制模型中，考虑到偏序关系，主体对客体的访问方式主要有\_\_向下读，向下写，向上读，向上写\_。
10. MAC模型中的几种主要模型有\_\_Lattice模型，BLP模型，Biba模型\_\_\_。其中\_Lattice\_模型适合需要对信息资源进行明显分类的系统;其中强调信息的机密性而忽略了信息完整性的模型是\_BLP\_模型。
11. 防火墙是位于2个或多个网络间实施\_网间访问控制\_的一组组件集合。
12. 防火墙访问控制方法有\_服务控制，行为控制，用户控制，方向控制\_。
13. \_状态检测\_防火墙是在动态包过滤防火墙基础上加上状态检测机制形成的。
14. 防火墙体系架构中\_屏蔽子网\_体系架构相对来说是入侵者最难攻破的。该体系架构中的主要组成部分有\_外部路由器，堡垒主机，内部路由器\_。其中\_堡垒主机\_是整个架构的核心。
15. CIDF的主要组成部件包括\_事件产生器，事件分析器，响应单元，事件数据库\_\_。
16. 常见的通用入侵检测模型有\_denning模型\_\_。
17. 基于异常的入侵检测的检测原理是\_1)正常行为的特征轮廓2)检测系统运行情况3)是否偏离预设门限\_；其常用检测算法是\_统计分析\_，该检测算法的一个最大缺点是\_利用统计轮廓的动态自适应性\_，这常常会导致系统将入侵行为判为正常行为。
18. 基于误用入侵检测的原理是\_根据已知系统或软件的漏洞来检测入侵行为\_；常用的检测算法有\_\_专家系统，模型推理，完整性分析\_。
19. VPN的定义是\_依靠ISP或其它NSP在公用网络基础设施之上构建的专用的数据通信网络\_。其特点是\_封闭的用户群，安全性高，服务质量有保证\_。其功能有\_\_数据源身份验证，数据机密性保护，数据完整性保护，重放攻击保护\_。
20. 隧道技术实际是一种\_数据封装\_，将一种协议X封装在另外一种协议Y中，从而实现协议X对公用传输网络(采用协议Y)的透明性。
21. 隧道协议包含\_乘客协议，封装协议，运载协议\_三种协议。
22. 根据网络类型的差异，可以将VPN分为\_\_Client-LAN\_和\_LAN-LAN\_\_这2种类型。
23. PPTP和L2TP协议都是链路层安全协议，其中\_PPTP\_协议要求互联网必须为IP网络。

L2TP协议体系主要由\_LAC\_和\_LNS\_构成。

1. IPSec体系包含AH和ESP协议，其中\_AH\_协议只有认证功能；\_ESP\_协议有认证和加密功能。
2. 在IPSec协议体系中，IKE协议的作用是\_在通信双方之间通过协商建立SA\_。
3. IKE密钥交换第一阶段的目的是\_在通信双方之间建立一对ISAKMP SA,进而建立一条安全的通信信道\_。第二阶段的目的是\_在通信双方之间建立IPSec SA\_。
4. IKE密钥交换第一阶段主模式分3个步骤，这3个步骤分别是\_策略协商交换，DH公开值及nonce交换，身份验证交换\_。
5. SSL协议分2层，低层是\_SSL记录\_协议，高层是\_SSL握手协议，SSL密码变化协议和SSL告警\_协议。
6. 邮件数据处理顺序是签名-->压缩-->加密，压缩在签名之后的目的是\_便于使用多种压缩算法\_；加密在压缩之后的目的是\_减少消息的冗余量，使得加密强度更大，密码分析难度变大\_。
7. PGP功能有\_数字签名，消息加密，压缩，邮件兼容，数据分段\_。