

# HW12

PB17111614

王嵘晨

1. 计算机病毒：隐藏在计算机系统中，在一定条件下被执行，破坏系统，程序的功能和数据，影响系统软件和硬件正常使用，并能复制其他程序和自身复制。
- (1) 病毒：具有自我复制能力，通过计算机网络传播。
- (2) 特洛伊木马：潜伏在计算机中达到某种特殊目的，不具有自我复制功能，不会感染其他程序。
- (3) Rootkit：用于获取目标主机root权限，隐藏攻击者访问痕迹，使攻击者不被发现，从而能长期拥有管理员权限，具有极好的隐蔽性与潜伏性，难以检测。
2. 计算机病毒的特征：
- (1) 破坏性
  - (2) 传染性
  - (3) 隐蔽性
  - (4) 潜伏性
  - (5) 多态性
  - (6) 不可预见性
3. 计算机病毒检测技术：
- (1) 特征判定技术：根据病毒程序的特征，对病毒进行分类处理，而病毒程序中凡有相似的特征出现，则认定是病毒。
  - (2) 行为判定技术：利用病毒特有的行为进行检测，一旦发现病毒行为立即报警。
4. 木马的服务器端部分可定制，攻击者通过客户端与被入侵计算机的服务器端建立远程连接，一旦连接建立，木马控制者就可以通过被入侵计算机发送指令来控制它。
5. 计算机病毒传播方式：
- (1) 自动执行
  - (2) 复制式：依靠自身传播，通过自身复制将病毒代码传播给针对的目标对象。
  - (3) 搜索机制：搜索的是网络中所有某种漏洞的主机。
  - (4) 破坏性传播：主要是整个网络。
  - (5) 不需要计算机用户参与信息传播，被意识到已经传播广泛。