第一章 基本概念

1 病毒和木马

病毒、蠕虫和木马三者都对电脑有一定的危害，但是三者有其不同之处。

1.1 病毒

指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码

往往具有很强的**感染性、潜伏性、破坏性、特定的触发性**

病毒必须满足两个条件：

- **自我执行**（它通常将自己的代码置于另一个程序的执行路径中）
- **自我复制**（它可能用受病毒感染的文件副本替换其他可执行文件）

1.2 蠕虫

利用网络进行复制和传播，是自身包含的程序，通过网络连接，能够将自身功能拷贝到其他计算机中

普通病毒需要传播驻留文件（受感染的）来进行复制，但是蠕虫**不需要驻留文件就可以在系统之间进行复制**，蠕虫病毒的传染目标是互联网所有的计算机

两个典型的蠕虫病毒：

- **震网病毒**：第一个专门定向攻击真实世界中基础（能源）设施的“蠕虫”病毒
- **比特币勒索病毒**：WannaCry（又叫Wanna Decryptor），一种“蠕虫式”的勒索病毒

1.3 木马

是表面上有用的软件、实际目的却是危害计算机安全并导致严重破坏的计算机程序，具有

- **非授权性**：是指一旦控制端与服务端连接后，控制端将**窃取到服务端的很多操作权限**，就不需要你进行授权
- **隐蔽性**：采用多种手段隐藏木马
- 是一种**远程控制**的黑客工具

1.4 木马与病毒的区别

木马**不具有传染性**，不能像病毒那样复制自身，是将自身伪装起来，让用户下载执行，主要目的是窃取用户相关的信息或者隐蔽性控制，就是说**病毒是破坏你的信息，木马窥视你**

2 软件漏洞

分清楚**软件缺陷&软件漏洞**:

软件缺陷是，导致程序不能运行；软件漏洞不是bug，而是一个安全上的漏洞

电脑肉鸡:

就是说，自己的电脑被别人远程控制了，攻击者通过寻找漏洞来主动控制电脑，植入木马

漏洞分类:

- $0day$漏洞：还处于未公开状态的漏洞。这类漏洞只在攻击者个人或者小范围黑客团体内使用，网络用户和厂商都不知情，因此没有任何防范手段，危害非常大，
- $1day$漏洞：补丁发布在1天内的漏洞，通常指发布补丁时间不长的漏洞，仍然存在一定的危害
- 已公开漏洞：厂商已经发布了补丁和修补方法，危害比较小

漏洞产业链:

上游（技术开发部门，编写恶意软件）、中游（执行产业部门，实现病毒的传播，网络攻击）、下游（销赃产业部门，贩卖木马、病毒等）

3 漏洞库

国内外有许多的漏洞库，都是公开的

- CVE：**通用漏洞列表**，实现了安全漏洞命名机制的规范化和标准化，为每个漏洞确定了唯一的名称和标准化的描述
- NVD：**美国国家漏洞数据库**，同时收录三个漏洞数据库的信息，CVE漏洞公告、$US-CERT$漏洞公告、$US-CERT$安全警告
- $CNNVD$：**中国国家信息安全漏洞库**，是国内的数据库
- $CNVD$：**国家信息安全漏洞共享平台**
- 其他漏洞库，如EDB漏洞库等

4 渗透测试

渗透测试是通过模拟恶意黑客的攻击方法，来评估计算机网络系统安全的一种评估方法。渗透测试是指渗透人员在不同的位置（比如从内网、从外网等位置）利用各种手段对某个特定网络进行测试，以期发现和挖掘系统中存在的漏洞，然后输出渗透测试报告，并提交给网络所有者。

渗透测试是一个渐进的过程，不影响业务系统的正常运行。

渗透测试方法

- 黑箱测试：对系统一无所知的状态下，进行测试

- 白盒测试：测试者可以通过正常渠道向被测单位取得各种资料
- 隐秘测试：接受渗透测试的单位网络管理部门会收到通知，在某些时段进行测试。因此能够监测网络中出现的变化