**软件漏洞分析技术读书报告**

姓名：仝志欣

|  |
| --- |
| **本周预期完成任务：**阅读软件漏洞分析技术的第一章内容 |
| **本周实际完成进度：**了解了对漏洞的基本概述，包括漏洞与缺陷、瑕疵、错误等的区别和联系、漏洞的分类和分级的方式和方法、典型信息安全事故分析。 |
| **详细内容：**   1. **漏洞的定义和特点**   **1. 基本概念**  漏洞研究发展至今，有很多定义版本。本书的定义是:软件系统或者产品在设计、实现、配置、运行过程中，由操作实体有意或者无意产生的缺陷、瑕疵或者错误，它们以不同形式存在于信息系统的各个层次和环节之中，且随着信息系统的变化而变化。  **2. 特点**  ①持久性和时效性：随着时间推移，旧的漏洞会不断消失，新的漏洞会不断出现，因此漏洞具有持久性。漏洞具有时效性，超过一定的时间限制，漏洞的威胁就会逐渐减少直至消失。  ②广泛性和具体性：会影响到很大范围内的软硬件设备，包括操作系统本身及系统服务软件、网络客户和服务软件、网络路由器和防火墙。漏洞又具有具体性，即它总是存在于具体的环境或者条件中。  ③可利用性与隐蔽性：漏洞具有可利用性，一旦被攻击者利用就会给信息系统带来威胁和损失。这里举的例子是“千年虫问题”。漏洞具有隐蔽性表现在往往需要通过特殊的漏洞分析手段才能发现。例如：VDM漏洞。   1. **漏洞的分类与分级** 2. **漏洞的分类**   书中含有早期分类方法，主要是讲述基于少数因素进行分类。这里主要提及一下，多维度分类综合性分类、和漏洞库分类。  ①多维度漏洞分类  主要是Neumann提出了基于风险来源的漏洞分析方法，将风险来源分为三类：系统设计过程中的问题、系统操作和使用过程中的问题，以及故意滥用。  ②综合性漏洞分类  主要是提出各种多因素的漏洞分析法。  ③漏洞库中的漏洞分类  美国国家漏洞库（NVD）在CVE的基础上NVD将漏洞分为多种类型，在此就不一一列举了。、中国国家信息安全漏洞库（CNNVD）、国家信息安全漏洞共享平台（CNVD）、OSVDB、Bugtraq、Secunia漏洞库、乌云漏洞库。   1. **漏洞分级**   目前主要有三种漏洞级别评价方式：以CNNVD、微软等为代表的按照严重等级进行分级、使用数值表示漏洞级别、利用正在普及的通用漏洞评分系统进行分级。   1. **漏洞的影响**   **1. 漏洞广泛性**  软件漏洞可以引发恶性的Web攻击事件，从而使公民的权益受到侵害。例子包括csdn信息泄露事件；软件漏洞可以引发传播广泛的计算机病毒，造成经济上的损失，例子包括“尼达姆”病毒；软件漏洞可以引发后果严重的系统故障，造成重大安全事故，例子包括航天系统计算值溢出事故；利用软件漏可以实施高级可持续性攻击（APT），例子包括震网病毒。  **2. 用漏洞分析来保障信息安全**  包括ISA、CC、SA,依次对应于信息安全保障、信息技术安全评估通用准则、软件确保。 |
| **相关文件及参考资料：** 软件漏洞分析技术的第一内容 |
| **遇到的问题及该阶段学习的想法：**第一张主要介绍了漏洞的一些概述，基本上是一些理论性了解即可。 |
| **接下来的进度计划：**在下一周里，我打算阅读第三章和第四章。 |