**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、二章内容 |
| **本周实际完成进度：**了解漏洞分析的发展历程还有各个阶段的主要安全问题、主流分析方法及重要的防护手段。从中读出些漏洞分析发展的规律和趋势。 |
| **详细内容：**   1. **软件漏洞分析的概念和发展历程**   **1. 基本概念**  漏洞分析包括广义的和狭义两个层面，广义漏洞分析是指围绕漏洞所进行的漏洞挖掘、漏洞检测、漏洞应用、漏洞消除和漏洞管控等方面。而狭义的漏洞分析则指的是漏洞挖掘。漏洞挖掘技术包括静态和动态分析两种技术，静态分析在无需执行程序的情况下对代码进行扫描以发现其中的漏洞，分析范围较为广泛，但容易发生误报；动态分析通过执行程序后收集运行时的信息进行漏洞挖掘，结果较为准确但容易发生漏报，该技术常用于发现未知的漏洞。狭义的漏洞分析-漏洞挖掘，包括架构安全分析、源代码漏洞分析、二进制漏洞分析和运行系统漏洞分析，即通过各种方法对软件生命周期各个阶段生产出的软件产品进行分析，发现其中的漏洞。  **2. 发展历程**  原始萌芽阶段的分析工作以通信的密码破解为主，这一阶段的主要防御措施包括信息加密保护等。文章中列举了几种那个时期的加密算法。  初步发展阶段：时间上为70~90年代。漏洞分析较为单一，焦点在于计算机安全上。此阶段中主要采用的防御措施包括操作系统访问权限控制，分类管理用户，根据不同的的用户身份给予不同的访问权限。包括动态口令身份认证系统等，典型的防御像Linux、Unix等。  高速发展阶段：时间上为20世纪90年代~2000年左右，即互联网诞生至21世纪初。这一阶段分析围绕网络进行安全攻防，漏洞分析呈现多样化，通常采用多种分析技术，包括模糊测试、污点分析、渗透测试等。防护措施主要包括网络防护，例如防火墙、杀毒软件和IDS等。  ①二进制漏洞分析：就是指二进制代码比对技术。通过对同一个软件系统的不同二进制版本进行比较，将它们之间的差异找出来，从而找到在语义上的差别与变化。实现原理及方法主要有三种：基于文本的对比、基于同图构的对比、基于结构化的比对。  ②源代码漏洞分析技术：主要是分析工具，例如词法分析工具ITS4，它将源文件预处理为Token流，然后将该流与库中的缺陷结构进行匹配；符号执行工具BOON可以简单的进行数学抽象；PREfix基于程序调用图进行分析等等。  ③漏洞收集发布机制：专门的商业公司进行漏洞的广泛搜集并将其进行简单分析和发布综合性的报告。   1. **信息系统的防护和综合治理（包含体系建设）** 2. **网际安全**   主要阐述了信息安全的威胁更加棘手。  **2. 系统化监管漏洞**  ①建立政策法规  ②系统化漏洞分析：(1)智能漏洞挖掘技术、集群化漏洞分析技术和APT检测技术。其相对应的代表技术分别是动态污点分析和动态符号执行、分布式模糊测试、发现APT攻击。(2)漏洞分析工具（3）漏洞分析服务；  ③规范软件开发流程  **3．防御体系建设**  上升至国家。。。 |
| **相关文件及参考资料：** 软件漏洞分析技术的第二章内容 |
| **遇到的问题及该阶段学习的想法：**读过之后觉得太抽象了，基本上全是对以往的总结和对一些技术的核心描写。看来接下来的知识可能会比较难以接受。 |
| **接下来的进度计划：** 接下来一周阅读第三第四章内容，多查资料。 |