**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十五章内容 |
| **本周实际完成进度：**阅读完第十四章内容“运行系统漏洞分析”，从运行系统的概念、安全性、运行系统漏洞分析原理和实现方法等角度对系统漏洞分析进行了解。 |
| **详细内容：**   1. **基本原理**   **1. 基本概念**  可以将运行系统理解为由操作系统、基础软件、应用软件、Web应用程序等可能由多种软件共同构成的,处于实际运行状态的系统,这些软件的运行可能是并行的,并存在一定的依赖与协同关系,且构成运行系统的各个软件可能需要不同的运行环境支持并被部署于不同的机器之上,这些机器可能具有不同的操作系统并被划分到不同的子网范围内。基于上述给定的运行系统的概念,可以总结得出运行系统具有以下三方面的特点:①运行系统是处于实际运行状态的系统;②运行系统是多种软件的有机整体，各个软件有一定的运行逻辑关系；运行系统的部署环境复杂多样。  **2. 运行系统漏洞分析**  (1) 基本内容  运行系统所涉及的安全属性 (security element)主要包括运行系统中的配置管理、通信协议、授权认证、数据等的安全性等。基于不同的运行系统安全属性,可以将运行系统漏洞分为不同的类型。*破坏运行系统配置管理安全性的漏洞主要是指配置错误漏洞,此类漏洞的产生是由于软件安装位置、参数配置、访问权限配置等错误导致;破坏运行系统授权认证安全性的漏洞包括:访问验证漏洞、特权提升漏洞等,访问验证漏洞主要是由于运行系统的访问验证部分存在某些可利用的逻辑错误或用于验证的条件不足以确定用户的身份而造成的,特权提升漏洞是在攻击者使用特权账号运行代码时产生的;破坏运行系统通信协议的漏洞主要是指攻击者通过某些攻击方法,破坏了协议的正常功能,从而造成运行系统运行异常;破坏运行系统数据安全性的漏洞主要有:输入验证、数据完整性、数据机密性等漏洞。*  (2) 漏洞分析过程  该过程包含三个阶段：信息收集阶段、漏洞检测阶段、漏洞确认阶段。  漏洞检测阶段主要运行系统配置管理、通信协议、授权认证、数据检验、数据安全性漏洞确认阶段、对疑似漏洞进行确认。   1. **方法实现** 2. **信息收集**   网络拓扑检测、操作系统检测、应用软件检测、基于爬虫的信息收集和公用资源搜索。   1. **网络拓扑检测**   大概分为三步：主机扫描、端口扫描、路由跟踪技术。   1. 主机扫描是通过向目标主机发送不同类型的ICMP或者TCP、UDP请求，从多方面检测主机是否还存活的技术。ICMP是最简单的一种实现存活检测的方法      1. 端口扫描技术，分为TCP、UDP两种。TCP主要有TCPconnect扫描、TCP SYN。上图就是后者的图描述。 2. 路由跟踪技术。在Windows系统中, Trace Route术通过 Tracert命令来实现。执行 Tracert命令可以获得通往某一指定目标主机路径中的每个节点的P地址。漏洞分析人员依次对各个存活的部署运行系统的机器进行路由跟踪,就可以比较准确地还原出目标网络的拓扑结构图。 3. **操作系统探测**   操作系统探测具体的原理为:首先,需要对已知系统的指纹特征建立数据库。将此指纹数据库作为进行指纹对比的样本库。分别挑选一个open和 closed的端口,向其发送经过精心设计的 TCP/UDP/ICMP数据包,根据返回的数据包生成一份系统指纹。将探测生成的指纹与数据库中指纹进行对比,查找匹配的系统。如果无法匹配,以概率形式列举出可能的系统。   1. **应用软件检测**一般步骤如下 2. 如果是TCP端口,尝试建立TCP连接。通常在等待时间内,会接收到目标机发回的" Welcome Banner”信息。将接收到的旗标与软件信息数据库进行对比。查找对应应用程序的名字与版本信息。 3. 如果通过“ Welcome banner”无法确定应用程序版本,那么再尝试发送其他的探测包,将得到回复包与数据库中的软件信息进行对比。如果反复探测都无法得出具体应用,那么打印出应用返回报文,让用户自行进一步判定。 4. 如果是UDP端口,那么直接使用UDP探测包进行探测匹配,根据结果对比分析出UDP应用服务类型。 5. 如果探测到应用程序是SSL,那么调用 openSSL进一步侦查运行在SSL之上的具体应用类型。 6. **基于爬虫的信息收集**   漏洞分析人员可以利用爬虫对运行系统漏洞进行探测。以Web运行系统为例,根据动态查询URL,自动在参数部分进行参数变换,插入引号、分号(SQL注入对其敏感)、“ script标签”(XSS对其敏感)等操作进行试探,并根据Web服务器返回的结果自动判断是否存在安全问题。   1. 公用资源搜索   就是披露或者发现漏洞的公开网站和免费工具。（可见于p417表15.1）   1. **配置管理漏洞检测**   大多数情况下,软件应该遵守通用的配置指导方针以确定运行系统的相对安全性,例如：(1)确保运行系统只开启必需的服务模块。(2)确保运行系统的程序错误或错误编码不会返回给终端用户。(3)确保以最小权限部署运行系统的软件。(4)确保运行系统可以正确记录合法登录和错误。(5)确保服务器上的配置可以妥善处理超载,并能防止拒绝服务攻击。确保该服务器已进行适当的性能调整。  为保证系统运行安全性，需要对运行系统配置进行安全性测试，具体过程分为三步：   1. **分析运行系统的业务特性，明确运行系统的安全需求，建立运行系统的安全配置要求。** 2. **测试运行系统各配置是否符合第一步建立的运行系统的安全配置要求。**   测试运行系统各配置是否符合第一步建立的运行系统安全配置要求。测试人员通过人工方式或者利用自动化测试工具(例如,微软基线安全分析器 Microsoft BaselineSecurity Analyzor,MBSA)4进行检测,从而确定运行系统的各个子系统的配置是否符合第一步建立的安全配置要求。检查的层次包括网络层、主机系统层和业务应用层三个层次   1. 网络层:主要是检测路由器、交换机、防火墙等安全设备的软件配置是否符合运行系统的安全配置要求。 2. 主机系统层:主要是检测操作系统补丁安装情况、账号管理及密码策略、文件系统的访问控制、系统对外开放的服务及端口、系统内部审计子系统、防病毒子系统等的配置是否符合运行系统的安全配置要求。 3. 应用层:主要检查运行系统的业务应用系统的配置是否符合运行系统的安全配置要求。 4. **记录不符合安全配置要求的地方，形成配置安全测试报告。** 5. **通信协议漏洞检测**   **对协议的安全分析有两种：形式化方法和攻击验证方法。形式化方法不适用于规模越来越庞大的系统。目前漏洞分析人员都采用攻击验证的方法来验证。通信协议常见的漏洞有：身份认证漏洞、假冒攻击漏洞、保密数据泄露、类型攻击漏洞、新鲜性漏洞。**   1. **授权认证漏洞检测** 2. **授权测试** 3. **路径遍历测试：测试用户是否可以通过漏洞绕过限制访问文件。** 4. **绕过授权测试：验证被授权的对象是否有能力访问受限的资源或者功能。** 5. **提权测试：研究从一个特权等级升级到更高特权等级的问题。** 6. **认证测试**   **基本目的是防止其他实体非法使用已经被认定的身份。测试内容包括：**加密信道测试、用户枚举测试、默认或可猜用户测试、暴力测试、竞争条件测试等。   1. 加密信道测试。测试加密信道是为了确认用户的认证数据是否通过加密信道传输,以避免被恶意用户截获并破解。例如,登录页面是一个包含用户名、密码和提交按钮的表单,运行系统通过这个表单验证后进入应用系统。 2. 用户枚举测试 3. 默认或者可猜用户测试 4. 暴力破解测试 5. 竞争条件测试 6. 数据验证漏洞检测   运行系统常见的一种安全漏洞是不能正确验证来自客户端或外界的数据,例如,跨站脚本、SOL注入、解释器注入、 locale/Unicode、文件系统和缓冲区溢出等漏洞都属于这种类型。   1. 跨站脚本漏洞测试   跨站脚本漏洞( Cross-Site Scripting, XSS)发生在客户端,恶意的攻击者将对客户端有危害的代码放到服务器上作为一个网页内容,使得其他网站用户在观看此网页时,这些代码注入到了用户的浏览器中执行,使用户受到攻击。XSS包括三种类型:反射式跨站脚本漏洞、存储式跨站脚本漏洞、基于DOM跨站脚本漏洞。以反射式跨站脚本漏洞为测试对象进行黑盒测试,包括三个阶段:   1. 检测输入向量。测试必须确定Web应用程序中的变量,及其如何在Web应用程序中输人。 2. 分析每一个输入向量并发现潜在的漏洞。检测ⅹSS漏洞时,测试者通常会对每输入向量使用特制的输入数据。这种输入数据通常是无害的,但会引发发现漏洞的Web浏览器起反应。可通过使用一个Web应用程序 fuzzer或人工方式产生测试数据。 3. 对于每一个前一阶段已经报告的漏洞,测试者将分析相关报告并试图攻击这些漏洞。该攻击会对web应用程序的安全造成实际影响。 4. **SQL注入漏洞测试**   SQL注入漏洞包括通过输入数据从客户端插入或注入SQL查询到应用程序。一个 成功的SQL注入漏洞可以从数据库中获取敏感数据、修改数据库数据(插入/更新/删除 执行数据库管理操作(如关闭数据库管理系统)、恢复存在于数据库文件系统中的指定文件 内容,在某些情况下能对操作系统发布命令。   1. **典型工具**   **1. Nmap**  **2. Nessus**  **3. MBSA**  **4. WVS** |
| **相关文件及参考资料：** 软件漏洞分析技术的第十五章内容 |
| **遇到的问题及该阶段学习的想法：这章内容以web系统为例进行了系统的漏洞分析，收获很多，比如TCP扫描、破解测试、跨站脚本测试** |
| **接下来的进度计划：**机器学习 |