山东大学 软件 学院

网络攻防 课堂报告

|  |  |  |
| --- | --- | --- |
| 学号：202200201095 | 姓名： 杨伟康 | 班级： 22网安 |
| 硬件环境：  处理器 11th Gen Intel(R) Core(TM) i5-11400H @ 2.70GHz 2.69 GHz  机带 RAM 16.0 GB (15.9 GB 可用)  设备 ID 9DCDB7C5-EBBA-4C1F-845F-94B127DFAE09  产品 ID 00342-30515-76480-AAOEM  系统类型 64 位操作系统, 基于 x64 的处理器  笔和触控 没有可用于此显示器的笔或触控输入 | | |
| 软件环境：  Window+ VMware虚拟机 | | |
| Blog记录：   1. Openvas简介   OpenVAS是一个包含着相关工具的网络扫描器，其核心部件是一个服务器，该服务器包括一套网络漏洞测试程序，可以检测远程系统和应用程序中的安全问题。作为信息安全领域的重要工具，OpenVAS广泛应用于企业网络安全测试和评估。   1. 主要功能   1. 强大的扫描引擎：能够检测大量已知的漏洞，包括操作系统、网络设备、应用程序等。  2.广泛的插件库：提供丰富的插件资源，确保能够检测最新的漏洞。  3.详细的报告：生成详细的扫描报告，包括漏洞描述、风险等级和修复建议。  4.开源和免费：作为开源项目，OpenVAS免费提供给用户使用和修改。  5.图形用户界面：提供GUI界面，使得用户能够通过简单的操作完成扫描任务并快速获取结果。使用示例  三、安装与试用  这里使用kali自带的gvm    初始化一下gvm，下载了一个小时……    启动gvm进入登陆界面    进入    各个服务已经成功开启    新建一个任务    或者快速开始，点击魔法棒图标->Task Wizard，输入扫描主机主机名或ip即可。    服务器和网关也同样进行扫描。    等待一会儿，等到Status为Done时，就可以导出报告了    选择上图下载按钮，下载XML、CSV等格式的报告。    下载的报告内容如下 | | |
| 结论分析与体会：  在使用OpenVAS进行网络攻防课堂实践的过程中，我深刻体会到了这款开源网络扫描器在网络安全测试与评估中的重要作用。通过Kali Linux自带的Greenbone Vulnerability Manager (GVM)，我能够轻松地初始化并启动OpenVAS服务，进而开始我的扫描任务。  在实际操作中，我发现OpenVAS的界面设计直观且易于上手，即便是像我这样的初学者也能够迅速掌握其使用方法。通过简单的配置，我就能够指定扫描目标，并启动扫描引擎。等待一段时间后，OpenVAS便能够生成一份详细的扫描报告，其中包含了目标系统中存在的各种漏洞及其风险等级。  这份报告对我来说极具参考价值，它不仅让我了解了目标系统的安全状况，还为我提供了修复这些漏洞的具体建议。通过仔细阅读报告，我能够深入了解到哪些漏洞可能对我的系统构成威胁，并采取相应的措施进行防范。  此外，我还发现OpenVAS的插件库非常丰富，能够检测大量已知的漏洞。这意味着，只要我定期更新插件库，就能够确保OpenVAS始终具备检测最新漏洞的能力。这对于我这样的网络安全爱好者来说，无疑是一个巨大的福音。 | | |