****

网络安全理论与技术实验

实 验 报 告

|  |  |
| --- | --- |
| **学 院** | 网络空间安全学院 |
| **专 业** | 网络工程 |
| **班 级** | 18272412 |
| **学 号** | 18041618 |
| **学生姓名** | 廖越强 |
| **教师姓名** | 高梦州 |
| **完成日期** | 11.6 |
| **成 绩** |  |
| **实验三 信息收集工具的使用（Nmap）** | | |
| 1. **实验目的**   本次实验主要通过使用Nmap扫描工具，从而对扫描工具有较深的理解，能够完成正确安装Nmap软件，并且能够熟练使用Nmap的各种扫描命令并分析其结果。 | | |
| 1. **实验原理**   Nmap是一个网络扫描软件，是精英黑客俱乐部(w00w00)的成员戈登·费奥多·林恩(Gordon Fyodor Lyon)开发。它可以用来扫描网上电脑开放的网络端口，确定哪些服务运行在哪些端口，并且推断计算机运行哪个操作系统。它是网络管理员必用的软件之一；同时，它也用来评估网络系统。 | | |
| 1. **实验环境/实验拓扑图**   windows10，nmap 7.70版  nmap的GUI操作界面 | | |
| **四、主要操作步骤及实验结果记录**   1. 主机发现（www.baidu.com），可见域名对应的主机之一112.80.248.75可以被扫描      1. 使用zenmap.exe进行扫描，可见主机处于运行状态，开放的端口有80和443     80端口    443端口    操作系统情况无法识别出来，no OS matches for host     1. 使用命令行扫描     要查看主机操作系统还得添加参数-O | | |
| **五、实验分析总结及心得**  通过这次实验，我认识了一款很好用的信息收集工具--Nmap，它非常强大，在GUI界面只需要填入目的的域名或者IP地址即可进行主机的开放状态、端口开放以及主机的操作系统进行分析。在感概工具的强大之时，也更明白了暴露在外的信息是很可能被不法分子利用的，提高了自己的安全意识。 | | |

|  |
| --- |
| **实验三 漏洞扫描实验（Nessus）** |
| 1. **实验目的**   通过本实验对漏洞扫描具有深刻的理解，能够收敛掌握漏洞扫描流程。 |
| 1. **实验原理**   现在，我们已经有了目标计算机的IP地址列表，并知道了这些计算机上开放的端口和已经启用的服务，是时候对目标计算机进行漏洞扫描了。漏洞就是存在于软件或者系统配置中可以被利用的弱点。我们在漏洞扫描中主要讨论Nessus。 |
| **三、实验环境/实验拓扑图**  操作系统windows 10，漏洞扫描工具Nessus |
| **四、主要操作步骤及实验结果记录**   1. Nessus的UI界面      1. 配置扫描，目的为百度的服务器的两个ip地址，112.80.248.76以及112.80.248.76      1. 点击launch进行漏洞扫描，结果如图，很安全      1. 自建扫描策略，扫描个人网站，ping的方式添加UDP     ping Method添加UDP方式    可见，这个个人网站也很安全 |
| **五、实验分析总结及心得**  通过这次实验，我对网络扫描的操作流程有了新的的认识，学会了Nessus的基本操作。也对信息收集这一概念有了自己的理解，明白了暴露到外网的信息对安全的重要性。提高了自己的安全意识。 |