

**长沙理工大学**

计算机与通信工程学院

**《网络安全技术》实验（上机）报告**

**实验名称**： **端口扫描工具使用**

**班 级**： **网络2102班**

**学 号**： **202108060918**

**姓 名**： **王俊**

**完成日期**： **2024 年 4 月**  **19 日**

**指导老师： 夏卓群**

|  |  |  |  |
| --- | --- | --- | --- |
| **实验名称** | 端口扫描 | **综合型** | |
| **实验目的及要求：** | | | |
| 1．网络与系统调查阶段的网络扫描、网络拓扑探测是信息收集的主要手段，本次试验主要内容是掌握网络扫描技术的作用，网络扫描技术是为使系统管理员能够及时了解系统中存在的安全漏洞，并采取相应防范措施，从而降低系统的安全风险。可以对局域网络、Web站点、主机操作系统、系统服务以及防火墙系统等的安全漏洞进行扫描，系统管理员可以了解在运行的网络系统中存在的不安全的网络服务，在操作系统上存在的可能被利用从而导致攻击的安全漏洞。通过实验掌握网络扫描的主要功能，掌握主流的网络扫描技术。 | | | |
| **实验内容：** | | | |
| 1. 通过实验掌握网络扫描技术的原理。 2. 通过实验掌握网络扫描的主要功能。 3. 熟悉使用主流的网络扫描工具Nmap以及会对结果进行分析和利用。 4. 掌握Nmap中的各参数的含义以及所对应的扫描类型。 | | | |
| **运行截图**  **安装Snmp，并简单检测**     1. 隐蔽扫描(Stealth Scanning) TCP SYN scan        1. UDP扫描      1. Ping扫描       4. SCTP INIT scan     1. TCP ACK scan      1. TCP Window scan      1. IPprotocol scan     7. Quick scan模式    8. -v  (提高输出信息的详细度)    9. -p   (只扫描指定的端口)    10. -sV (版本探测)    11. Intense scan    12. --traceroute(路由跟踪)      13. 扫描目标主机的操作系统类型      14. **FIN扫描** | | | |
| **教师评阅：**  **年 月 日** | | | **评分** |
|  |