实验 2 端口扫描程序设计实验

#### 实验目的

通过编程扫描主机端口开放情况，掌握端口扫描的基本工作原理，掌握常见端口扫描的 实现方法和编程实现。

#### 实验准备

（1）具备一定的 TCP/IP 的知识。

（2）具备简单的Windows下socket编程知识，能进行简单的编程。

（3）掌握TCP全连接扫描技术的原理和实现方法。

#### 实验内容

编程实现TCP全连接扫描（也叫TCP Connect扫描），对指定目标主机实现端口扫描。

（1）关闭主机防火墙，用自行开发的扫描程序对目标主机扫描，发现目标主机端口开放情况。

（2）打开主机防火墙，再次扫描主机端口开放情况，比较两次扫描结果的不同。

#### 实验要求

（1）本实验在 Windows 操作系统上进行。

（2）画出扫描程序流程框架图。

（2）写出详细试验步骤。

（3）记录扫描结果并进行分析，得出分析报告。

（4）分析目标主机防火墙对扫描结果的影响。