**《计算机网络安全》实验报告**

**实验（1） 安全扫描实验**

学生姓名： 陈华豪 学 号： 6130116238 专业班级： 网络工程161班

实验类型：■ 验证 □ 综合 □ 设计 实验日期：  实验成绩：

**实验目的**

熟悉利用远程控制型木马进行网络入侵的基本步骤，分析冰河木马的工作原理，了解并掌握木马隐藏的常见方法，掌握常见木马的清除方法。

**试验内容**

为了发现系统缺陷和漏洞，入侵者和网络管理员都常常使用扫描的方式来侦测系统和网络，不过两者目的不一致。入侵者是通过扫描技术来收集信息和检测漏洞，为入侵做好前期准备工作；网络管理员则是发现系统漏洞后及时修补，以提高安全性能。但两者殊途同归，都应用了扫描功能。

服务器上所开放的端口就是潜在的通信通道，也就是一个入侵通道。对目标计算机进行端口扫描，能得到许多有用的信息。进行端口扫描的方法很多，可以是手工进行扫描，也可以用端口扫描软件进行。

扫描器通过选用远程TCP/IP不同端口的服务，并记录目标给予的回答，通过这种方法可以搜集到很多关于目标主机的各种有用的信息，如远程系统是否支持匿名登录、是否存在可写的FTP目录、是否开放Telnet服务和HTTPD服务等。

**3．实验过程**

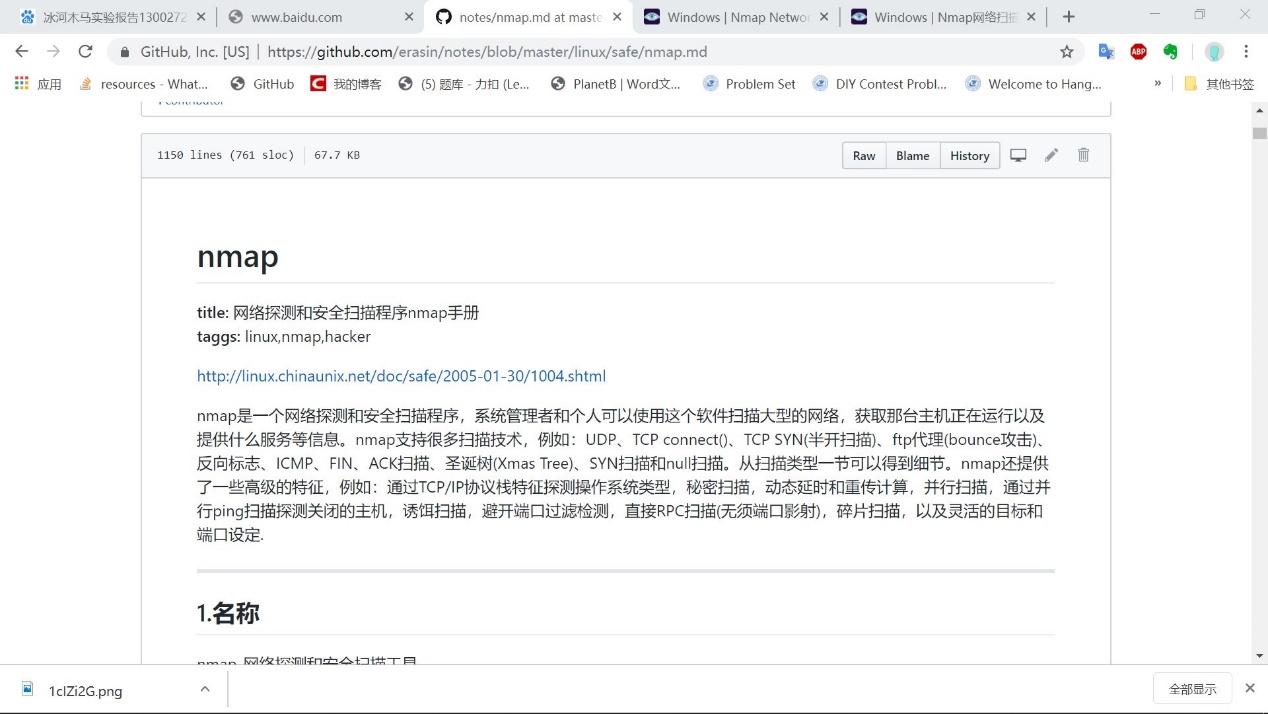
3．1实验环境

Nmap是一个免费的开源实用程序，它可以对网络进行探查和安全审核。Nmap可以运行在所有主要的计算机操作系统上，并且支持控制台和图形两种版本。

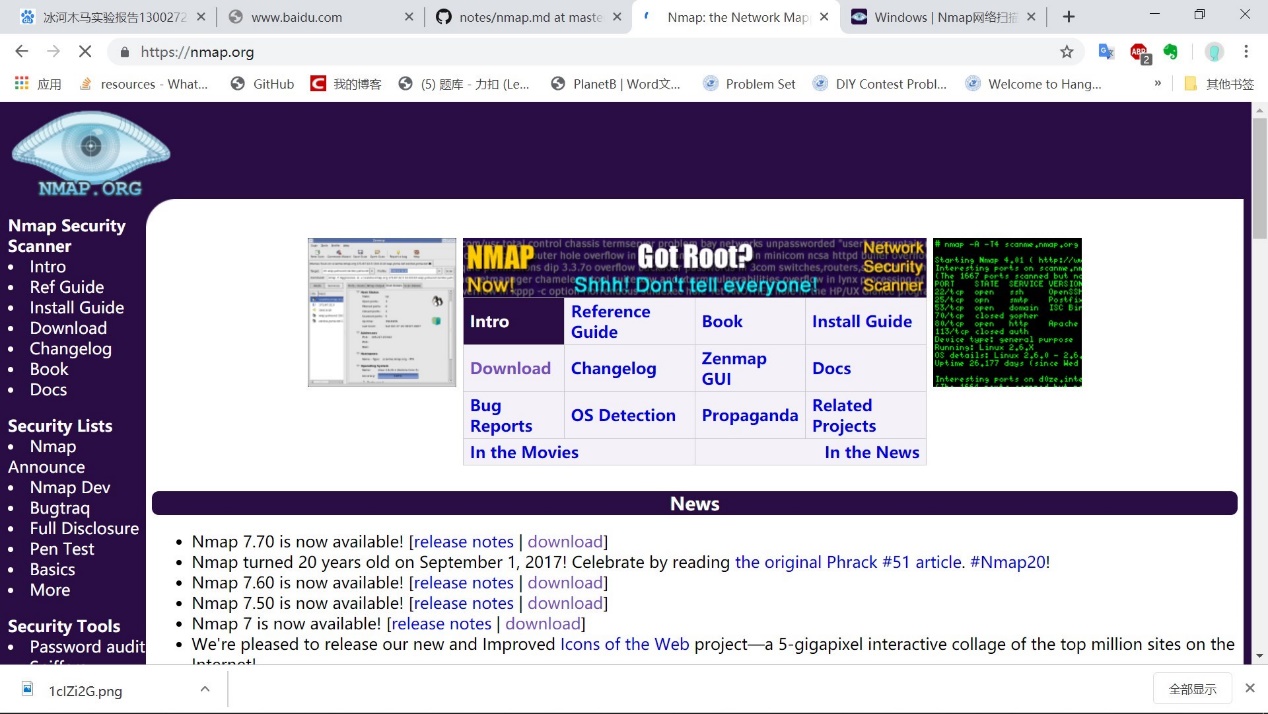
3．2关键实验步骤及配置

（1）查找nmap相关资料。

1. github页面：<https://github.com/erasin/notes/blob/master/linux/safe/nmap.md>



2. nmap首页：[https://nmap.org](https://nmap.org/)



（2）下载windows上nmap自安装程序。

**图片包含 屏幕截图

描述已自动生成**

（3）安装nmap。

图片包含 屏幕截图

描述已自动生成

（4）打开管理员模式运行cmd，进入nmap安装目录，输入nmap，查看是否安装完成。

图片包含 屏幕截图

描述已自动生成

（5）运行测试：nmap -sVC -O -T4 scanme.nmap.org

图片包含 屏幕截图

描述已自动生成

（6）快速扫描指定主机：ccogito.xyz。

图片包含 屏幕截图

描述已自动生成

**实验结果**

图片包含 屏幕截图

描述已自动生成

**实验总结**

通过扫描方法检测目的主机端口使用情况可以有效测试出有哪些漏洞。