课程名称	保密技术基础 A		实验课时	4
实验项目名称和序号	端口扫描实验	2	同组者姓　名	无
实验目的	1. 理解端口的概念； 2. 了解常用的端口扫描原理； 3. 能够熟练的使用常用的端口扫描工具进行弱点检测和修复。			
实验环境	1. 具备基本的局域网环境； 2.　PC 机一台； 3. 版本为 3.3 的 X-Scan 端口扫描工具。			
实验内容和原理	**实验内容：** 1. 学习或听任课老师介绍关于端口扫描的基础知识； 2. 安装 X-Scan 扫描工具； 3. 使用 X-Scan 进行扫描； 4. 记录并分析扫描结果； 5. 根据扫描结果采取相应的措施巩固系统。 **实验原理：** 网络服务或应用程序提供的功能由服务器或主机上的某个或多个进程来实现，端口则相当于进程间的大门，可以随便定义，其目的是为了让两台计算机能够找到对方的进程。“端口”在计算机网络领域是非常重要的概念，它是专门为网络通信而设计的，它是由通信协议 TCP/IP 定义，其中规定由 IP 地址和端口作为套接字，它代表 TCP 连接的一个连接端，一般 称为 SOCKET，具体来说，就是用[IP：端口]来定位主机中的进程。 可见，端口与进程是一一对应的，如果某个进程正在等待连接，称之为该进程正在监听。在计算机[开始]-[运行]里输入 cmd 进入 dos 命令行，然后输入 netstat-a 可以查看本机有哪些进程处于监听状态。根据 TCP 连接过程（三次握手），入侵者依靠端口扫描可以发现远程计算机上处于监听状态的进程，由此可判断出该计算机提供的服务，端口扫描除了能判断目标计算机上开放了哪些服务外还提供如判断目标计算机上运行的操作系统版本（每种操作系统都开放有不同的端口供系统间通信使用，因此从端口号上也可以大致判断目标主机的操作系统，一般认为开有 135、139 端口的主机为 Windows 系统，如果除了 135、139 外，还开放了 5000 端口，则该主机为			

Windows XP 操作系统。）等诸多强大的功能。一旦入侵者获得了上述信息，则可以利用系统漏洞或服务漏洞展开对目标的攻击。

由上所述，端口扫描是一帮助入侵的工具，但是安全人员同样可以使用端口扫描工具定期检测网络中关键的网络设备和服务器，以查找系统的薄弱点，并尽快修复，因此理解端口扫描原理和熟练使用端口扫描工具对防治入侵有很大的帮助。

常见的 TCP 端口号：

服务名称	端口号	说明
FTP	21	文件传输服务
Telnet	23	远程登陆服务
Http	80	网页浏览服务
Pop3	110	邮件服务
Smtp	25	简单邮件传输服务
Socks	1080	代理服务

常见的 UDP 端口号：

服务名称	端口号	说明
Rpc	111	远程调用
Snmp	161	简单网络管理
TFTP	69	简单文件传输

常见的端口扫描工具：

X-Scan、X-Port、Superscan、PortScanner 等。

实验步骤

方　　法

关键代码

实验步骤：

1. X-Scan 是免安装软件，解压后直接双击 xscan_gui.exe 图标，如图 1 所示；

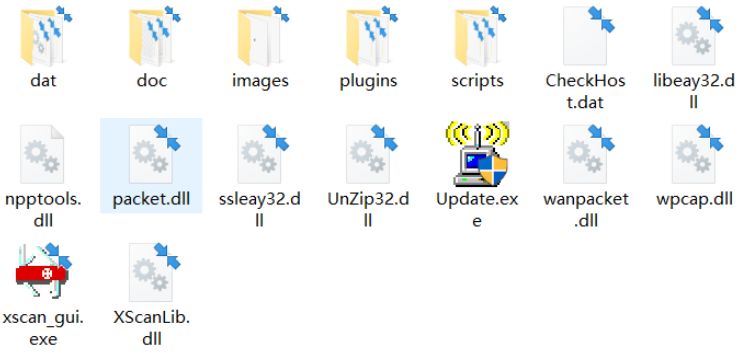

图 1　X-Scan 文件内容

2. 双击 xscan_gui.exe 图标打开 X-Scan 主界面，如图 2 所示；

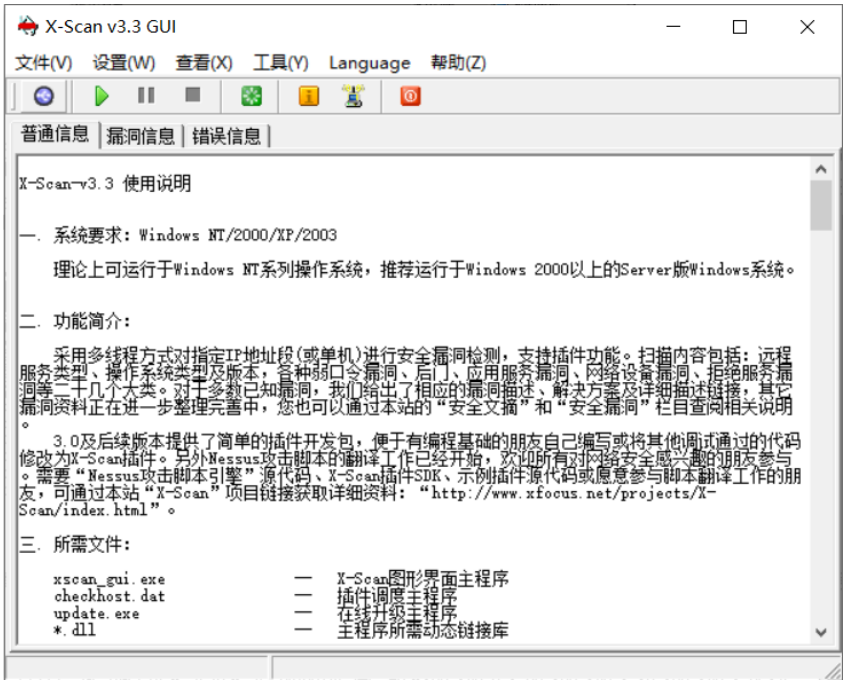

图 2　X-Scan 主界面

3. 认真学习主界面上的使用说明；

4．选择菜单中的设置选项，打开下拉菜单，选择扫描参数，打开扫描参数对话框，如图 3 所示；在该对话框的左边有三个设置选项 ①检测范围，②全局设置，③插件设置。使用扫描工具主要是理解扫描参数的作用；

图 3　X-Scan 扫描参数对话框

扫描参数设置说明

“检测范围”模块：

“指定 IP 范围” - 可以输入独立 IP 地址或域名，也可输入以“-”和“,”分隔的 IP 范围，如“192.168.0.1-20,192.168.1.10-192.168.1.254”，或类似“192.168.100.1/24”的掩码格式。

“从文件中获取主机列表” - 选中该复选框将从文件中读取待检测主机地址，文件格式应为纯文本，每一行可包含独立 IP 或域名，也可包含以“-”和“,”分隔的 IP 范围。

图 4 “检测范围”模块

“全局设置”模块：

“扫描模块”项 - 选择本次扫描需要加载的插件。

“并发扫描”项 - 设置并发扫描的主机和并发线程数，也可以单独为每个主机的各个插件设置最大线程数。

“网络设置”项 - 设置适合的网络适配器，若找不到网络适配器，请重新安装 WinPCap 3.1 beta4 以上版本驱动。

“扫描报告”项 - 扫描结束后生成的报告文件名，保存在 LOG 目录下。扫描报告目前支持 TXT、HTML 和 XML 三种格式。

“其他设置”项 ：

“跳过没有响应的主机” - 若目标主机不响应 ICMP ECHO 及 TCP SYN 报文，X-Scan 将跳过对该主机的检测。

“无条件扫描” - 如标题所述

“跳过没有检测到开放端口的主机” - 若在用户指定的 TCP 端口范围内没有发现开放端口，将跳过对该主机的后续检测。

“使用 NMAP 判断远程操作系统” - X-Scan 使用 SNMP、NETBIOS 和 NMAP 综合判断远程操作系统类型，若 NMAP 频繁出错，可关闭该选项。

“显示详细信息” - 主要用于调试，平时不推荐使用该选项。

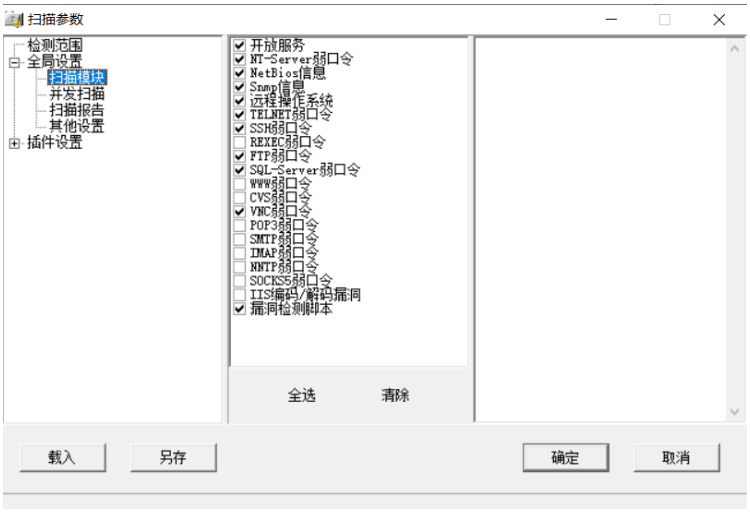

图 5 “全局设置”模块

“插件设置”模块：

该模块包含针对各个插件的单独设置，如“端口扫描”插件的端口范围设置、各弱口令插件的用户名/密码字典设置等。

图 6 “插件设置”模块

5. 检测范围用以确定要扫描的目标或目标范围，现在检测范围内输入 IP 地址段 192.168.4.2-192.168.4.10,如图 7 所示；

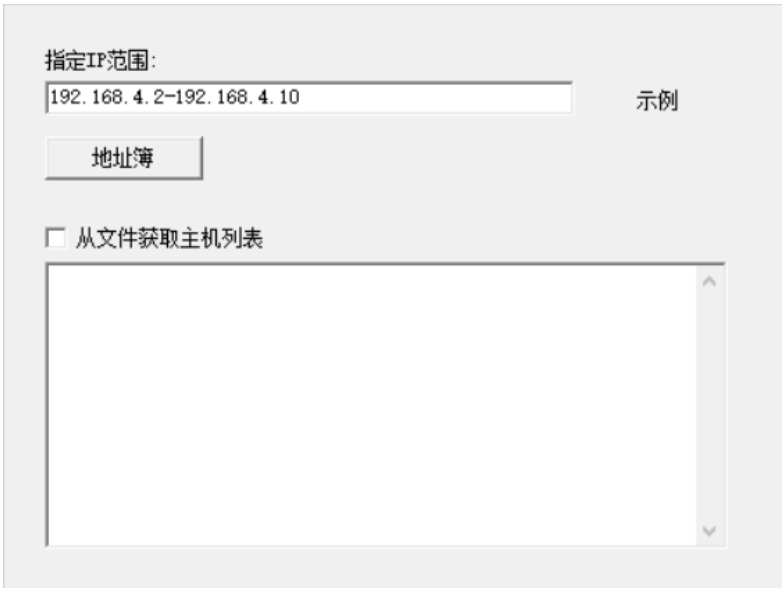

图 7 检测范围设置

6. 展开全局设置选项，我们在“扫描模块”中可以定义扫描的主要内容，选择的内容越多，将可能收集到信息越多，但扫描的时间就越长。“并发扫描”中的“最大并发线程数量”切忌不可设置太大，特别是对自己管理的网络设备或服务器扫描的时候，因为设置太大可能会导致扫描对象的异常。对于一般的扫描，我们可以使用 XScan 的默认设置；

7. “插件设置”中有很多名词术语，如 SNMP 中的 WINS 用户列表、NETBIOS 等，请自行查找资料了解其涵义；

SNMP 相关设置：

“SNMP相关设置”选项主要是用来获取界面信息、IP信息、TCP信息、UPP信息和WINS用户列表的。

NETBIOS 相关设置：

在“NETBIOS相关设置”中，主要是检测“注册表敏感键值”、“服务器时间”、“共享资源列表”、“用户列表”、“本地组列表”等，也就是说利用NETBIOS，我们完全可以获取对方系统中的共享资源和用户帐号。

漏洞检测脚本设置：

“漏洞检测脚本设置”默认是全部选中的，我们也可以取消掉“全选”。点击“选择脚本”然后就可以从脚本中选择要检测的安全漏洞了。比如扫描Windows主机就可以取消掉关于unix/Linux漏洞的脚本，这样可以提高扫描的速度。

字典文件设置：

选中“字典文件设置”后，在右面会列出扫描各种信息时用到的各种字典文件。例如扫描FTP弱口令时我们用weak-pass.dic这个文件，每个字典文件都可以用记事本打开，并且可以对它编辑。在字典文件上右键就会看到“编辑”字样。比如，你可以向弱口令中添加一些新密码，一切设置完成后点击“确定”就完成“扫描参数”的设置了。

8. 设置完毕后开始扫描，如图 8 所示；

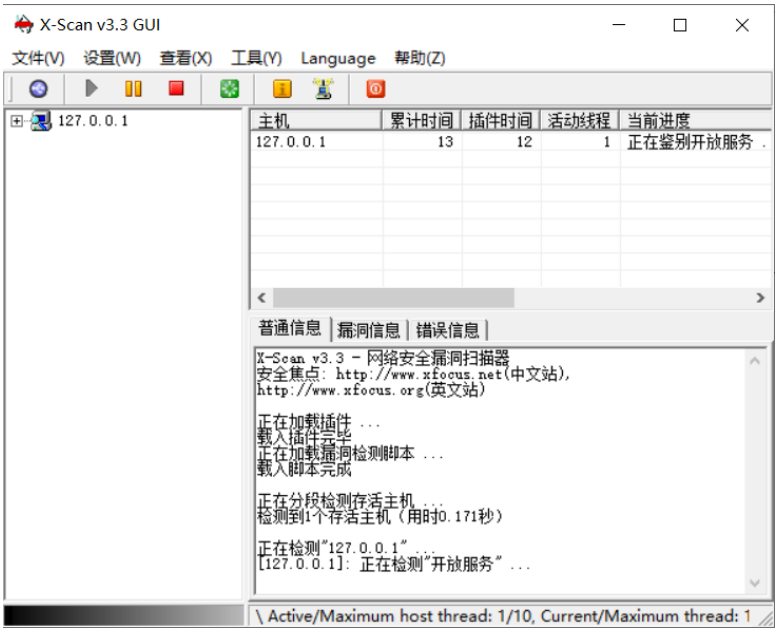

图 8　开始扫描过程

9. 认真观察扫描过程，待扫描结束后认真阅读自动生成的扫描报告（生成的检测报告可以 是 HTML、WORD 等格式类型，可以打印，有时可以直接作为安全测试报告）。

10. 分析扫描目标存在的问题，并拟定解决措施。

测试记录分析结论

开始扫描后，根据我们刚才的设置开始进行测试，如图 9 所示：

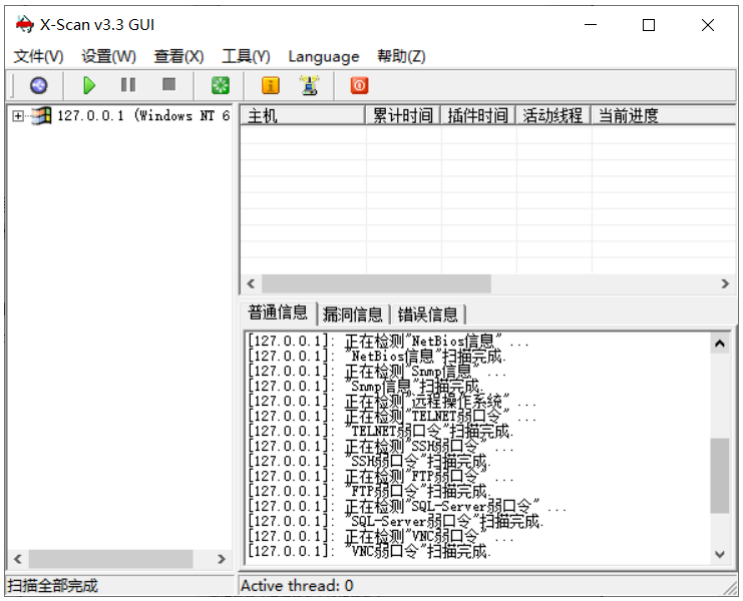

图 9 扫描过程

扫描结果，如图 10 所示：

	检测结果
存活主机	1
漏洞数量	0
警告数量	0
提示数量	65

图 10 X-Scan 扫描结果

具体信息如图 11 所示：

端口/服务	服务漏洞
microsoft-ds (445/tcp)	发现安全提示
epmap (135/tcp)	发现安全提示
DCE/51a227ae-825b-41f2-b4a9-1ac9557a1018 (49664/tcp)	发现安全提示
DCE/d95afe70-a6d5-4259-822e-2c84da1ddb0d (49665/tcp)	发现安全提示
DCE/f6beaff7-1e19-4fbb-9f8f-b89e2018337c (49666/tcp)	发现安全提示
unknown (49667/tcp)	发现安全提示
unknown (49673/tcp)	发现安全提示
DCE/367abb81-9844-35f1-ad32-98f038001003 (49678/tcp)	发现安全提示
DCE/12345778-1234-abcd-ef00-0123456789ac (49664/tcp)	发现安全提示
DCE/b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 (49664/tcp)	发现安全提示
DCE/8fb74744-b2ff-4c00-be0d-9ef9a191fe1b (49664/tcp)	发现安全提示
unknown (49664/tcp)	发现安全提示
DCE/86d35949-83c9-4044-b424-db363231fd0c (49667/tcp)	发现安全提示
DCE/3a9ef155-691d-4449-8d05-09ad57031823 (49667/tcp)	发现安全提示
DCE/12345678-1234-abcd-ef00-0123456789ab (49673/tcp)	发现安全提示
DCE/0b6edbfa-4a24-4fc6-8a23-942b1eca65d1 (49673/tcp)	发现安全提示
DCE/ae33069b-a2a8-46ee-a235-ddfd339be281 (49673/tcp)	发现安全提示
DCE/4a452661-8290-4b36-8fbe-7f4093a94978 (49673/tcp)	发现安全提示
DCE/76f03f96-cdfd-44fc-a22c-64950a001209 (49673/tcp)	发现安全提示

图 11 X-Scan 扫描具体信息

安全方法及漏洞解决方案（部分）如下图 12 所示：

类型	端口/服务	安全漏洞及解决方案
提示	microsoft-ds (445/tcp)	**开放服务** "microsoft-ds"服务可能运行于该端口. NESSUS_ID : 10330
提示	epmap (135/tcp)	**开放服务** "epmap"服务可能运行于该端口. NESSUS_ID : 10330
提示	epmap (135/tcp)	**DCE Services Enumeration** Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Solution : filter incoming traffic to this port. Risk factor : Low NESSUS_ID : 10736
提示	epmap (135/tcp)	**DCE Services Enumeration** Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Solution : filter incoming traffic to this port. Risk factor : Low NESSUS_ID : 10736
提示	epmap (135/tcp)	**DCE Services Enumeration** Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Solution : filter incoming traffic to this port. Risk factor : Low NESSUS_ID : 10736
提示	epmap (135/tcp)	**DCE Services Enumeration** Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Solution : filter incoming traffic to this port. Risk factor : Low NESSUS_ID : 10736
提示	epmap (135/tcp)	**DCE Services Enumeration** Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Solution : filter incoming traffic to this port. Risk factor : Low NESSUS_ID : 10736
提示	epmap (135/tcp)	**DCE Services Enumeration** Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Solution : filter incoming traffic to this port. Risk factor : Low NESSUS_ID : 10736

图 12　X-Scan 扫描漏洞及解决方案（部分）

以上，完成了 X-Scan 的端口扫描，在本次实验中，我们主要是对本地主机进行扫描的。

小　结

经过这次实验操作，对端口、漏洞扫描有了更深的了解，能够使用 X-scan 对主机进行扫描。X-scan 采用多线程方式对指定 IP 地址段(或单机)进行安全漏洞检测，支持插件功能，提供了图形界面和命令行两种操作方式，扫描内容包括：远程服务类型、操作系统类型及版本，各种弱口令漏洞、后门、应用服务漏洞、网络设备漏洞、拒绝

	服务漏洞等二十几个大类。 使用 X-scan 可以快速了解系统存在的安全漏洞，方便管理人员快速解决安全问题，对于管理员对系统的安全测试以及安全问题有很大作用。 除了 X-scan，还有很多的漏洞扫描工具。漏洞扫描分为网络漏洞扫描和主机漏洞扫描，网络漏洞扫描就是通过网络扫描，针对网络设备的漏洞和对外提供网络服务的主机网络服务程序进行的端口漏洞扫描，主机漏洞扫描就相当于对主机操作系统的漏洞扫描。 网络漏洞扫描主要通过网络漏洞扫描里面的漏洞脚本库，这个脚本库中包含了大量的模拟攻击脚本和代码，然后向主机发送模拟攻击的数据包，然后检测主机的响应来判断是否存在漏洞。 主机漏洞扫描就是通过漏洞匹配技术，来检测本机操作系统的版本信息和补丁信息来进行扫描。 通过本次实验，让我对计算机间的通信机制有了更进一步的了解和认识，计算机端口是通信的连接点，计算机之间的通信是根据端口来完成的，所以端口的扫描有助于我们发现漏洞和安全隐患，进而防止计算机被入侵、隐私被窃取，更有利于我们学习计算机的安全机制。 **参考文献** [1]neo_will_mvp.X-Scan 使用教程 [EB/OL].https://blog.csdn.net/qq_33468857/article/details/86424455,2019-01-13. [2]lc11535.X-Scan 介绍和使用方法 [EB/OL].https://blog.csdn.net/lc11535/article/details/102570248,2019-10-15.
以下由实验教师填写	
记　事 评　议	
成绩评定	平时成绩_____　　实验报告成绩_____　　综合成绩 _____ 指导教师签名：