信息安全本科生 2020—2021 学年 第（二）学期

《信息对抗技术》课程作业 范例

学号：_____ 姓名：_____ 成绩：_____

实验 5 X-scan 的使用实验报告

一、 实验目的

1. 熟练掌握 X-Scan 扫描器的使用。
2. 了解本机操作系统的漏洞，找出计算机安全方面的安全隐患

二、 实验环境

Windows XP

X-scan v3.3

三、 实验原理

1. X-scan

X-scan 是著名的综合扫描器之一，它把扫描报告和安全焦点网站相连接，对扫描到的每个漏洞进行“风险等级”评估，并提供漏洞描述、漏洞溢出程序，方便网管测试、修补漏洞。

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：远程操作系统类型及版本，标准端口状态及端口 BANNER 信息，CGI 漏洞，IIS 漏洞，RPC 漏洞，SQL-SERVER、FTP-SERVER、SMTP-SERVER、POP3-SERVER、NT-SERVER 弱口令用户，NT 服务器 NETBIOS 信息等。扫描结果保存在/log/目录中，index_*.htm 为扫描结果索引文件。

2. 设置说明

(1) 检测范围

“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。

全局设置

“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。

(2) 其他设置

“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。

“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。

四、 实验过程

1. 下载并解压 x-scan v3.3

首先在 Windows10 系统中尝试进行试验，但是运行学院网站上下载的工具时提示缺少 NPPTools.dll 文件，百度搜索发现该软件一般支持系统 Win9x/NT/2000/XP/2003/Win7，于是又转移到 WindowsXP 虚拟机中进行实验。重新下载 x-scan v3.3 并直接运行 xscan_gui.exe，会看到如下界面：

2. 设置扫描参数

可以设置的部分包括：检测范围、全局设置、插件设置。

(1) 检测范围

这里用来设置带扫描的 IP 地址范围，可以手动输入正确格式（包括 localhost），也可以从文件中导入。

(2) 全局设置

这里主要是设置一些全局的扫描参数，包括需要扫描的模块（可以由我们自行勾选需要的模块，本实验中尝试进行本地扫描，主机数目较少，所以将所有模块全选；如果需要扫描的主机数过多，可以进行有针对性的扫描）、并发扫描（设置最大并发扫描的主机数和最大的并发线程数）、扫描报告（扫描结束之后可以选择自动生成并显示报告，她会生成一个检测 IP 或域名的报告文件，报告文件的类型可以选择 HTML/TXT/XML 三种）、其他设置（如果

设置了‘跳过没有响应的主机’,对方禁止了 PING 或防火墙设置使对方没有响应的话,X-SCAN 会自动跳过，自动检测下一台主机。如果用‘无条件扫描’的话，X-SCAN 会对目标进行详细检测，这样结果会比较详细也会更加准确。但扫描时间会更长）。

(3) 插件设置

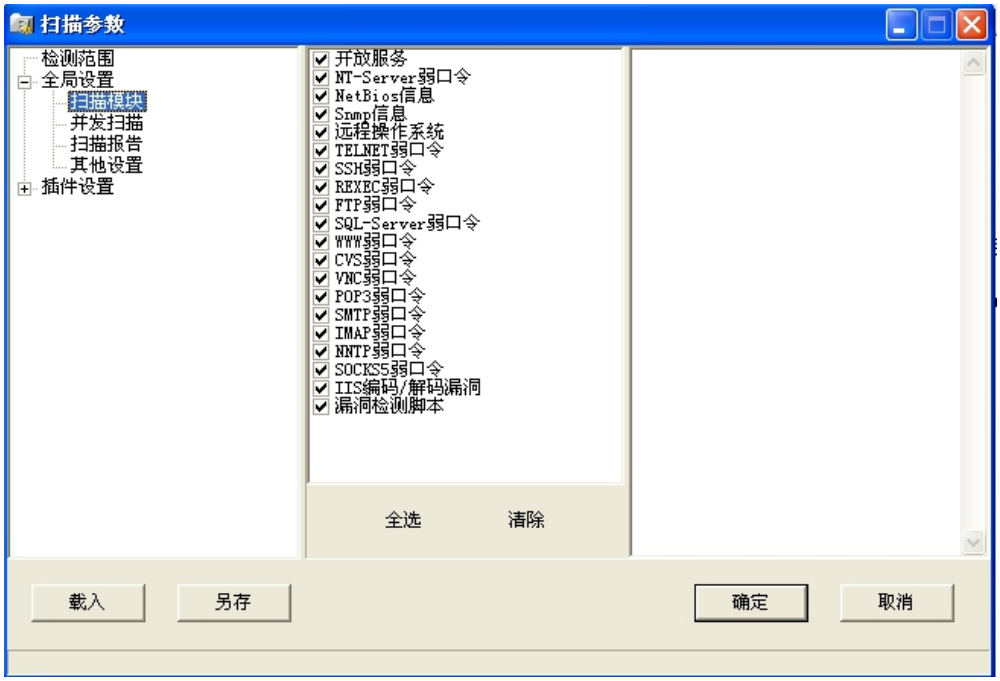
端口相关设置：可以自定义一些需要检测的端口。检测方式“TCP”、“SYN”两种，TCP 方式容易被对方发现，准确性要高一些，SYN 则相反。

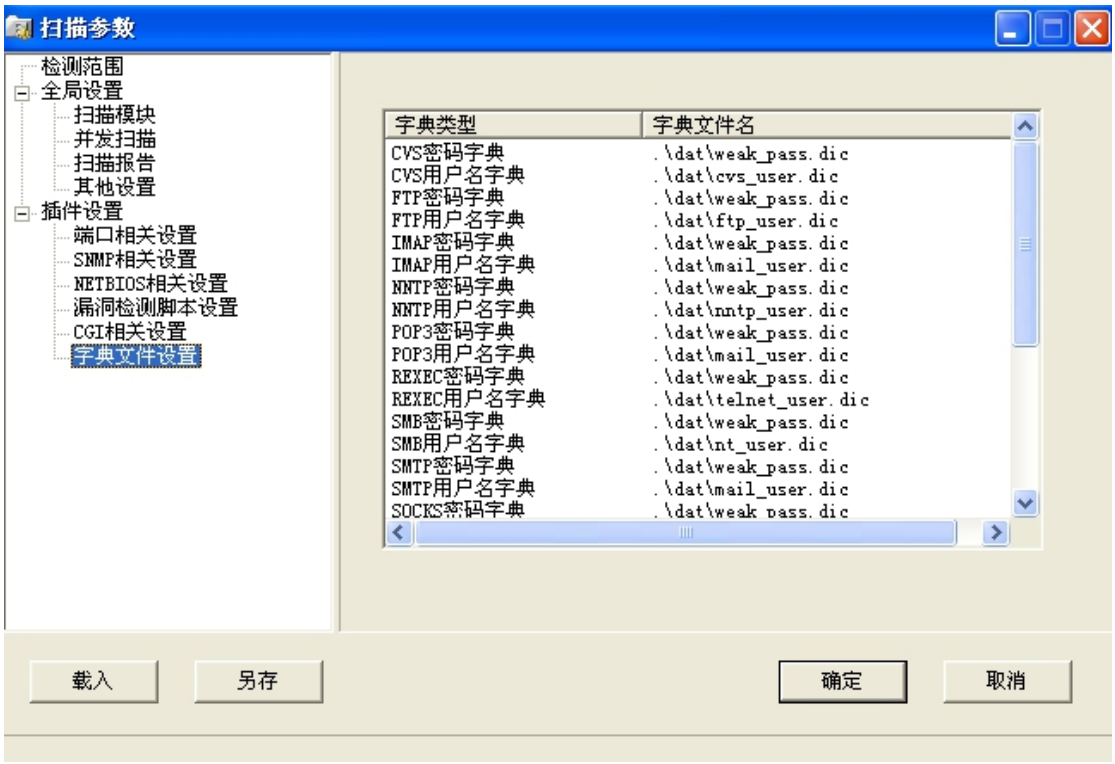
SNMP 相关设置：用来针对 SNMP 信息的一些检测设置，在监测主机数量不多的时候可以全选。

NETBIOS 相关设置：是针对 WINDOWS 系统的 NETBIOS 信息的检测设置，包括的项目有很多种，根据实际需要进行选择。

如需同时检测很多主机的话，要根据实际情况选择特定的漏洞检测脚本。CGI 相关设置默认就可以。

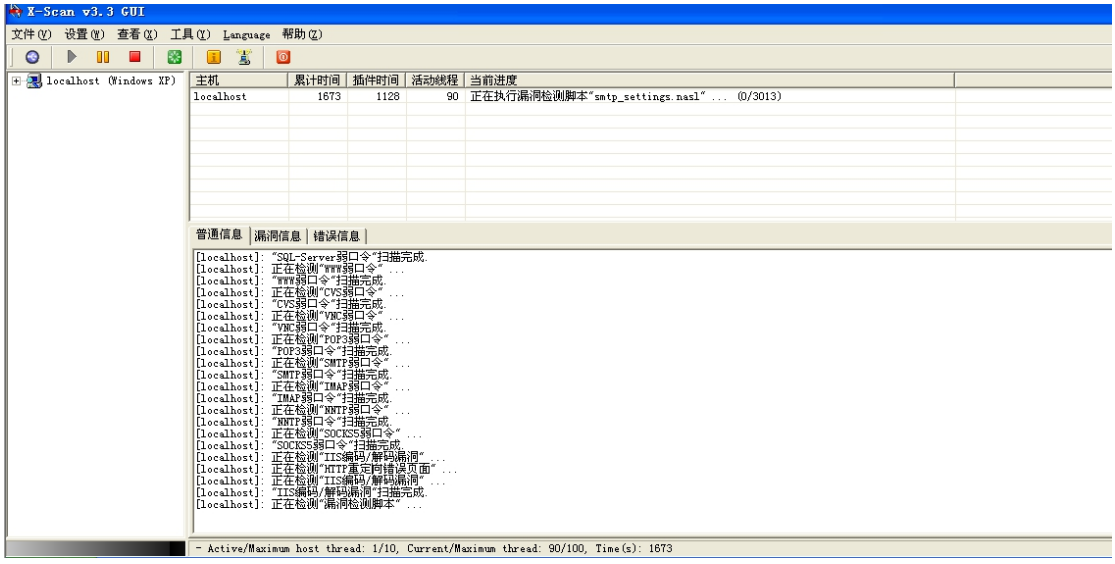
字典文件设置：是 X-SCAN 自带的一些用于破解远程账号所用的字典文件，这些字典都是简单或系统默认的账号等。我们可以选择自己的字典或手工对默认字典进行修改。默认字典存放在“DAT”文件夹中。字典文件越大，探测时间越长，此处无需设置。





这里就不将设置过程一一截图了。

3. 开始进行扫描



可以看到它将在我们开始设置扫描的端口一一进行检查：

主机	累计时间	插件时间	活动线程	当前进度
localhost	5	4	1	正在检测"端口: 65301" ...

指示出各种服务可能运行的端口，并将对应结果依次展示，如果存在漏洞信息也会提示出来：

普通信息 | 漏洞信息 | 错误信息

```
[localhost]: 开放服务: 25/tcp
[localhost]: 开放服务: 80/tcp
[localhost]: 开放服务: 135/tcp
[localhost]: 开放服务: 443/tcp
[localhost]: 开放服务: 445/tcp
[localhost]: 开放服务: 1025/tcp
[localhost]: 443/tcp - "https"服务可能运行于该端口.
[localhost]: 445/tcp - "microsoft-ds"服务可能运行于该端口.
[localhost]: 25/tcp - "SMTP"服务运行于该端口
[localhost]: 135/tcp - "epmap"服务可能运行于该端口.
[localhost]: 1025/tcp - "network_blackjack"服务可能运行于该端口.
[localhost]: 80/tcp - "WEB"服务运行于该端口
[localhost]: "开放服务"扫描完成, 发现 6.
[localhost]: 发现 "NetBios信息".
[localhost]: 远程操作系统 "Windows XP"
[localhost]: 发现 "远程操作系统".
```

此处会显示一些错误信息，比如针对某插件脚本运行时超时强制终止的提示：

普通信息 | 漏洞信息 | 错误信息

```
[localhost]: 插件"SMTP弱口令"运行超时, 强行终止
[localhost]: 插件"IIS编码/解码漏洞"运行超时, 强行终止
[localhost]: 插件"漏洞检测脚本"运行超时, 强行终止
```

最后，检测结束之后会自动弹出检测报告（我们之前设置过，让它自动显示的），报告中可以看到我们扫描的主机中存活了几个（这里我只设置了一个 localhost，所以存活数只能为 1 了），另外检测到漏洞的数量为 0（还是比较安全的），以及警告数量和提示数量（警告和提示内容见下方）：

2017-4-14 12:34:46 - 2017-4-14 13:03:57

检测结果	
存活主机	1
漏洞数量	0
警告数量	1
提示数量	6

主机列表

主机	检测结果
localhost	发现安全警告
主机摘要 - OS: Windows XP; PORT/TCP: 25, 80, 135, 443, 445, 1025	

[返回顶部]

主机分析: localhost

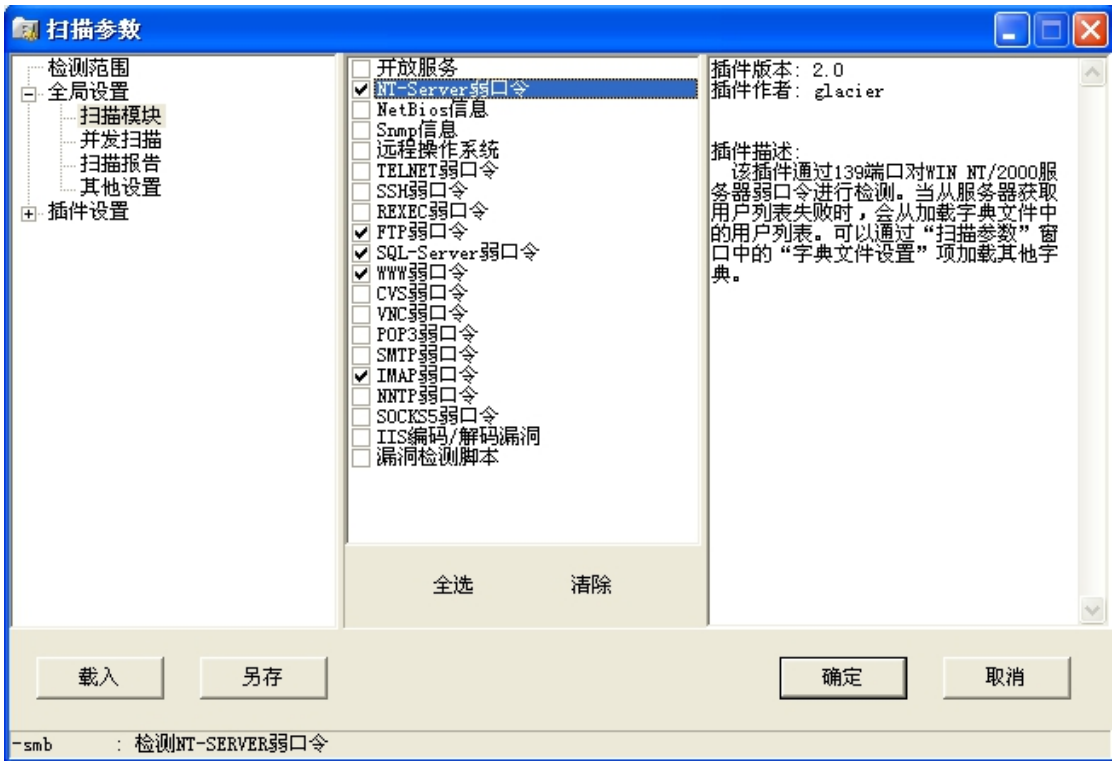
主机地址	端口/服务	服务漏洞
localhost	https (443/tcp)	发现安全提示
localhost	microsoft-ds (445/tcp)	发现安全提示
localhost	smtp (25/tcp)	发现安全提示
localhost	epmap (135/tcp)	发现安全提示
localhost	network blackjack (1025/tcp)	发现安全提示
localhost	www (80/tcp)	发现安全提示
localhost	netbios-ssn (139/tcp)	发现安全警告

本次检测中，在 443/tct、445/tcp、25/tcp、135/tcp、1025/tcp、80/tcp 中分别发现了安全提示，在 139/tcp(netbios-ssn)发现了安全警告，具体信息如下：

类型	端口/服务	安全漏洞及解决方案
提示	https (443/tcp)	**开放服务** "https"服务可能运行于该端口. NESSUS_ID : 10330
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	smtp (25/tcp)	**开放服务** "SMTP"服务运行于该端口 BANNER信息 : 220 erin-76f2756d44 Microsoft ESMTP MAIL Service, Version: 6.0.2600.5512 ready at Fri, 14 Apr 2017 12:34:59 +0800 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	network blackjack (1025/tcp)	**开放服务** "network blackjack"服务可能运行于该端口. NESSUS_ID : 10330
提示	www (80/tcp)	**开放服务** "WEB"服务运行于该端口 BANNER信息 : HTTP/1.1 302 Object moved Server: Microsoft-IIS/5.1 Date: Fri, 14 Apr 2017 04:35:14 GMT Location: localstart.asp Connection: Keep-Alive Content-Length: 121 Content-Type: text/html

在端口 139 处检测到的警告信息中得到了远程注册表信息，可以看出所使用的系统类型为 WindowXP、以及默认的账户名、域名等信息：

警告	netbios-ssn (139/tcp)	**NetBios信息** [远程注册表信息]: [ProductName]: Microsoft Windows XP [SOFTWARE\Microsoft\Windows NT\CurrentVersion]: SubVersionNumber: CurrentBuild: 1.511.1 () (Obsolete data - do not use) InstallDate: E2 78 D9 57 ProductName: Microsoft Windows XP RegDone: RegisteredOrganization: RegisteredOwner: Erin SoftwareType: SYSTEM CurrentVersion: 5.1 CurrentBuildNumber: 2600 BuildLab: 2600.xpsp.080413-2111 CurrentType: Uniprocessor Free CSDVersion: Service Pack 3 SystemRoot: C:\WINDOWS SourcePath: D:\I386 PathName: C:\WINDOWS ProductId: 76481-640-1464517-23578 DigitalProductId: A4 00 00 00 03 00 00 00 37 36 34 38 31 2D 36 34 30 2D 31 34 36 34 35 31 37 2D 32 33 35 37 38 00 2E 00 00 00 41 32 32 2D 30 30 30 30 31 00 00 00 00 00 00 00 26 B8 4F 4C 48 4A 2B 8F 70 1E 30 67 94 9E 00 00 00 00 00 00 2A E7 D9 57 75 39 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 35 33 37 32 30 00 00 00 00 00 00 00 DF 0D 00 00 BD 35 EA E8 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4E FF 81 20 LicenseInfo: E7 00 A3 CE 6A F8 BF 7C F5 E4 99 2D C2 FC 49 1D 9D 41 78 C7 32 A2 D0 B3 24 6D 8D DE CF 87 1D 43 3B 20 3D 62 BA 65 AA 9D 60 3B 01 FB F7 F0 0D 5B 21 65 89 82 AC AD EF 1F [SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]: AutoRestartShell: 01 00 00 00 DefaultDomainName: ERIN-76F2756D44 DefaultUserName: admin1 LegalNoticeCaption: LegalNoticeText: PowerdownAfterShutdown: 0 ReportBootOk: 1 Shell: Explorer.exe ShutdownWithoutLogon: 0 System:



五、 总结

至此完成了本次实验，初步了解了 x-scan 扫描器的使用方法及用途，对扫描器的工作原理有了进一步的理解和掌握，通过实践更有效地拓展了课内知识，希望通过今后的学习，能够对计算机的安全问题有更进一步的认知和理解，充分提高安全意识。