

南开大学

《信息对抗技术》课程实验报告

实验五：x_scan 的使用



学 院_____网络空间安全学院
专 业_____信息安全
学 号_____2112060
姓 名_____孙璐

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

1. 系统环境：Windows NT/2000/XP/2003，理论上可运行于 Windows NT 系列操作系统，推荐运行于 Windows 2000 以上的 Server 版 Windows 系统。
2. 使用软件：X-scan v3.3-cn

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。

X-Scan 是国内最著名的综合扫描器之一，它完全免费，是不需要安装的绿色软件、界面支持中文和英文两种语言、包括图形界面和命令行方式。主要由国内著名的民间黑客组织“安全焦点”完成，从 2000 年的内部测试版 X-Scan V0.2 到目前的最新版本 X-Scan 3.3-cn 都凝聚了国内众多黑客的心血。最值得一提的是，X-Scan 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。可以利用该软件对 VoIP 设备、通讯服务器进行安全评估。

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。

(2) 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。

(3) 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” - 若为用户指定的 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。

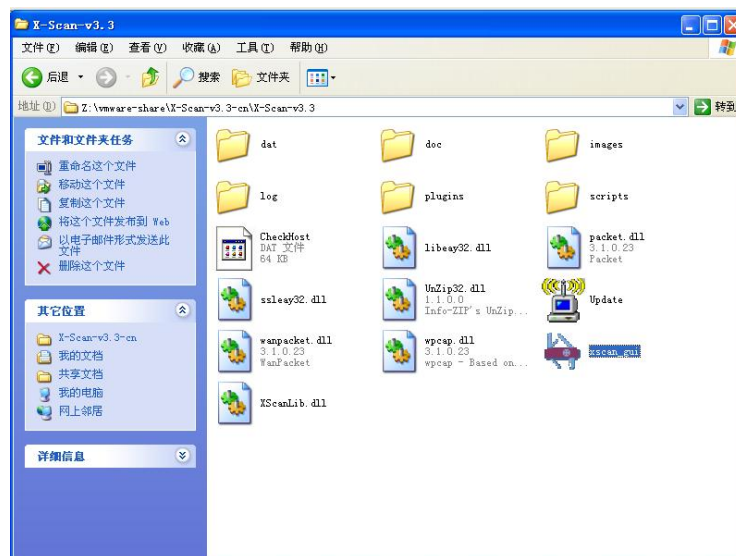
“插件设置”模块：

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

(一) X_scan 的安装与使用

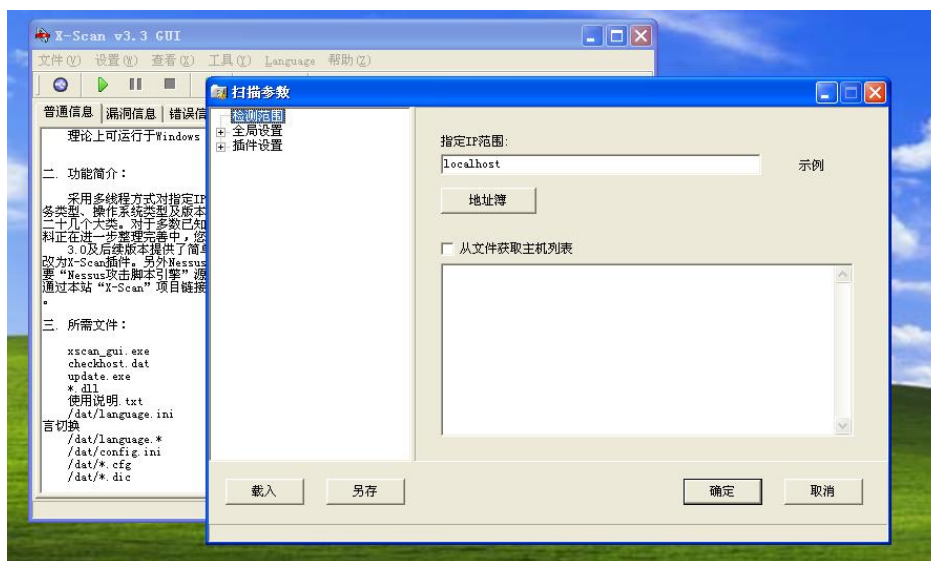
解压后运行 xscan_gui.exe 即可运行 xscan



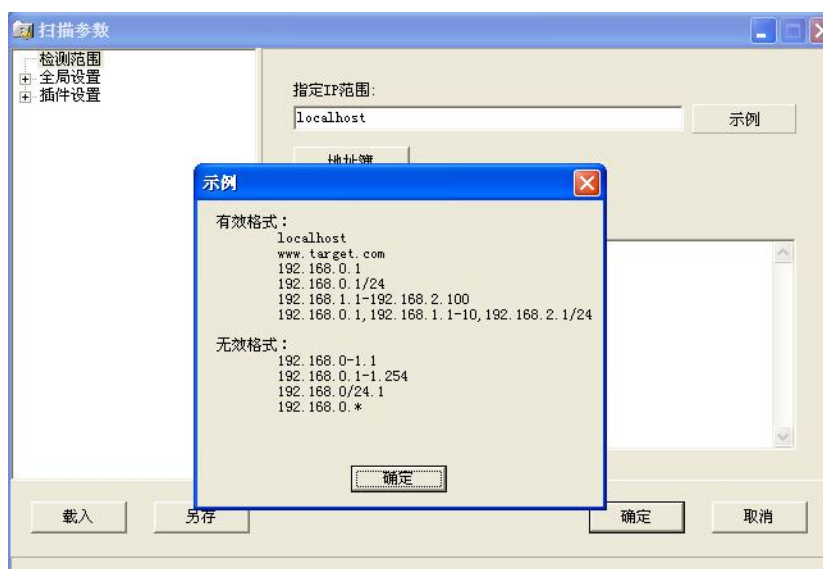
（二）参数设置

点击“设置”菜单，选择“扫描参数”或者直接点击工具栏的蓝色按钮进入扫描参数设置



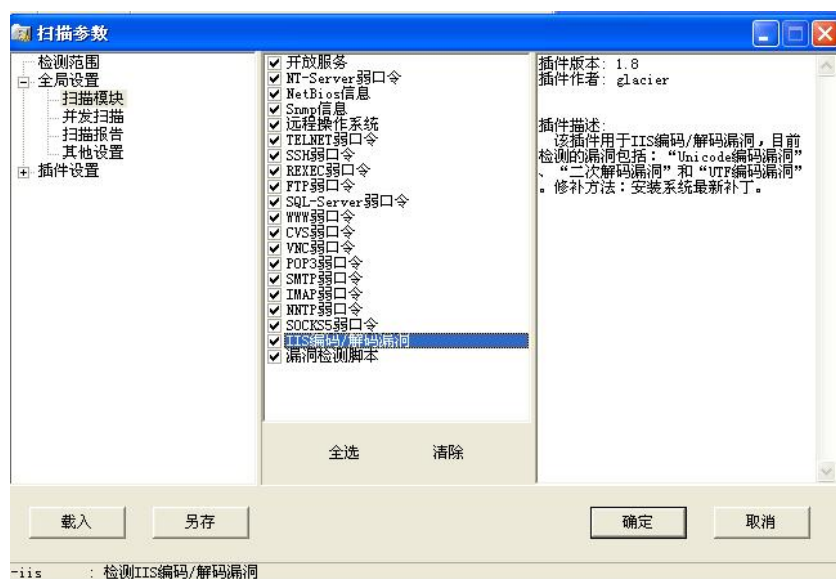


1. 检测范围。设置待扫描的 IP，按示例方式设置检测范围，或者从文件获取主机列表。



2. 全局设置。用来设置全局的扫描参数，具体如下：

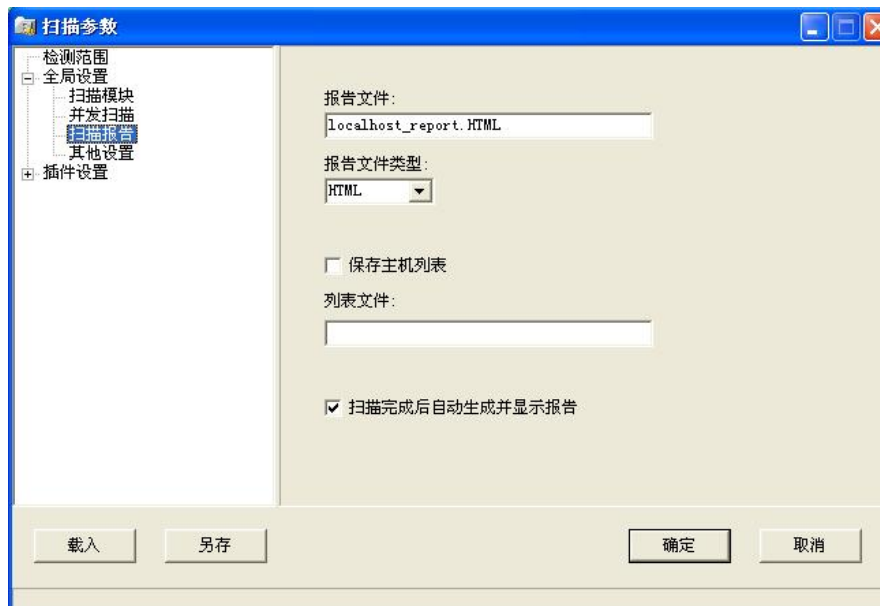
- 扫描模块：设置需要扫描的模块，对于单台设备的扫描，可以选择全部模块，如果扫描某个范围里面的设备，可以按需勾选需要扫描的模块。



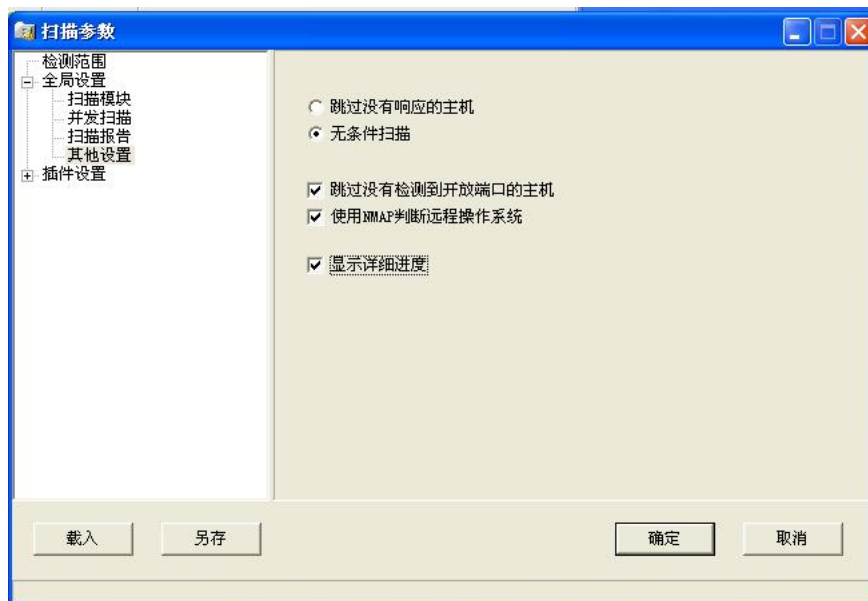
- 并发扫描：设置扫描的并发量，默认即可。如果机器性能好，带宽足够，可以适当增大并发量



- 扫描报告：设置扫描报告的名称和类型等

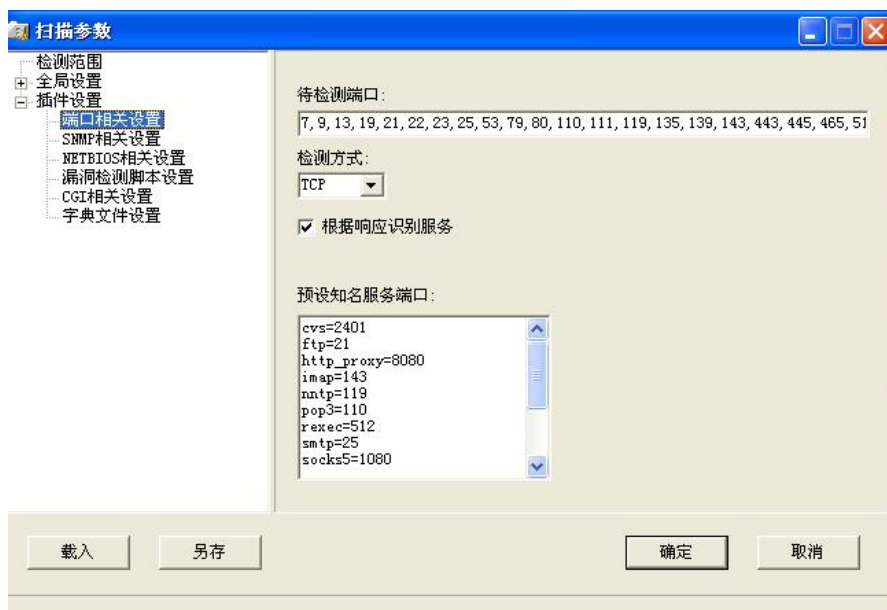


- 其它设置：设置对目标设备的检测机制等，如果是单个设备，建议使用无条件扫描，因为测试发现 x scan 判断主机是否存活不是很准确。

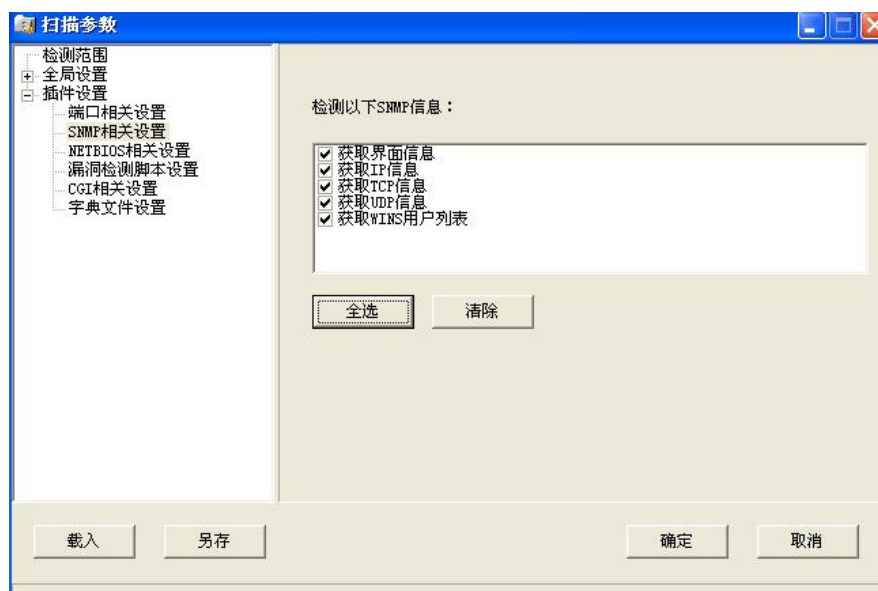


3. 插件设置：设置各插件的相关选项

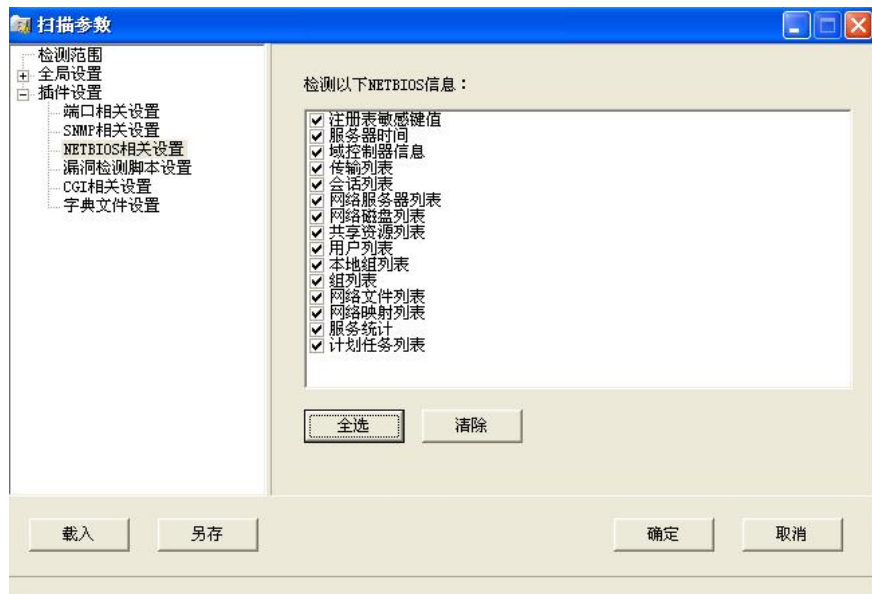
- 端口相关设置：设置与端口有关的项。待检测端口可以是任意端口的组合。检测方式使用 TCP 能够提高 x-scan 的准确性，但容易被对方的防火墙阻塞，SYN 却相反。根据响应识别服务，x-scan 能够根据响应判断运行的服务，即使端口已被更改。预设知名服务端口，可以自定义某些端口为知名服务端口。



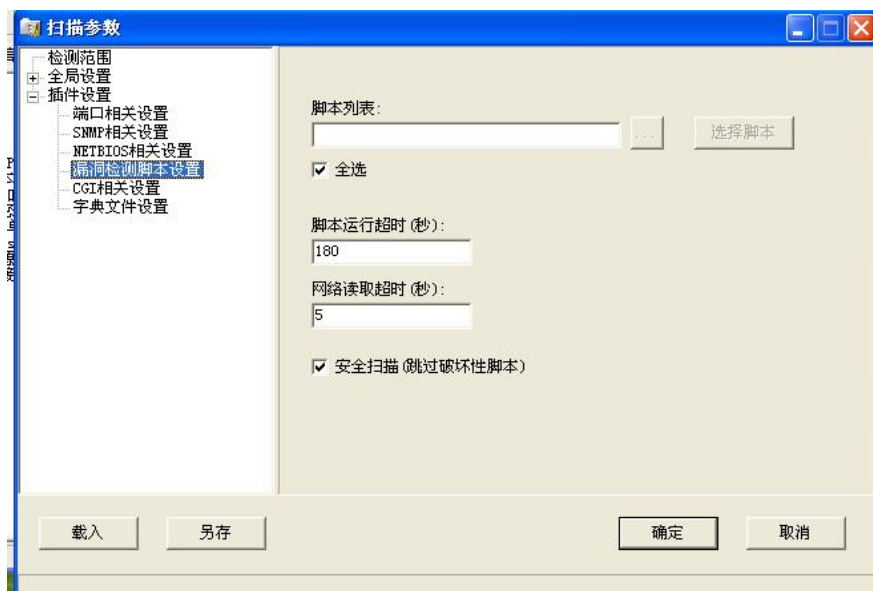
- SNMP 相关设置：设置 SNMP 协议检测项，建议全选。



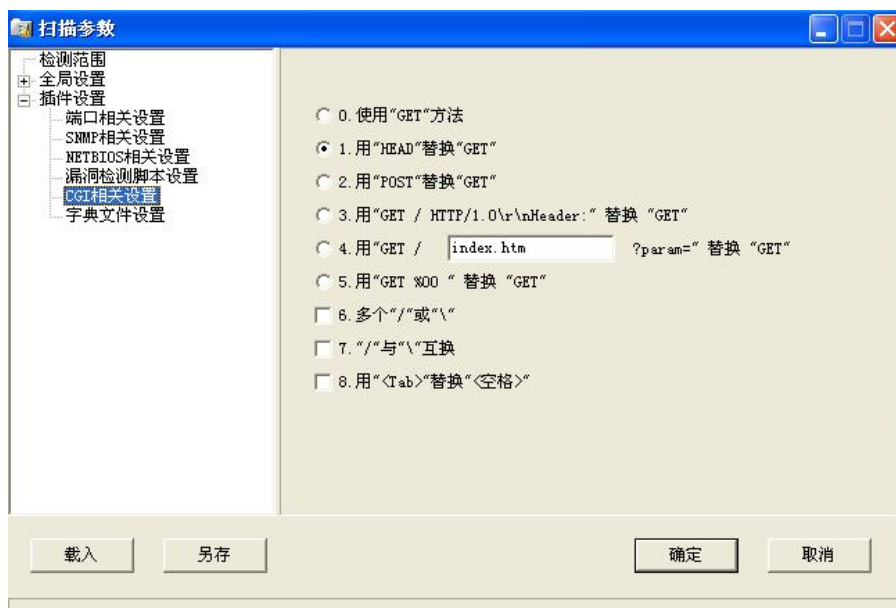
- NETBIOS 相关设置：设置检测的 NETBIOS 信息，主要是针对 windows 系统的 NETBIOS 的检测，单个非 windows 设备测试时勾选也无所谓。



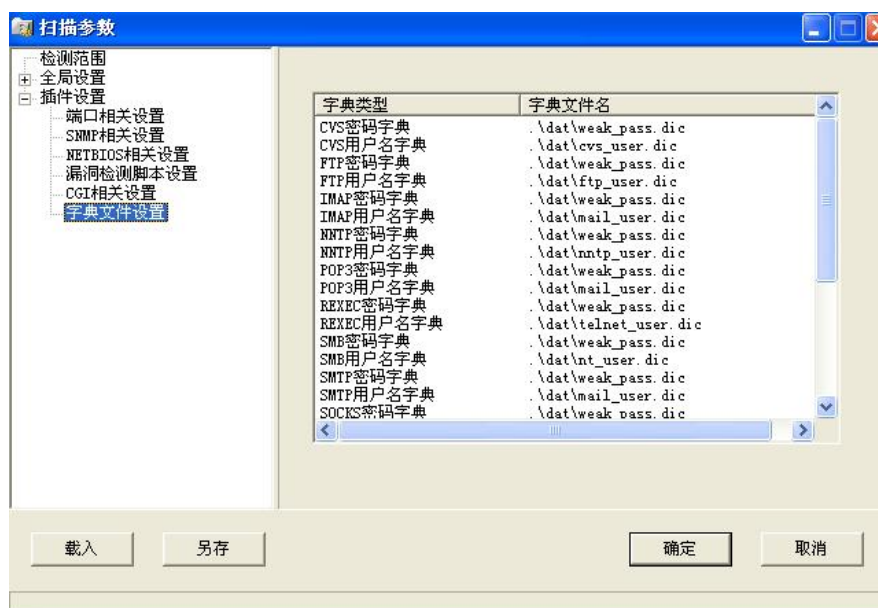
- 漏洞检测脚本设置：默认即可




- CGI 相关设置：设置 CGI（公用网关接口）的扫描策略，主要是针对 web 服务器的扫描。一般默认。



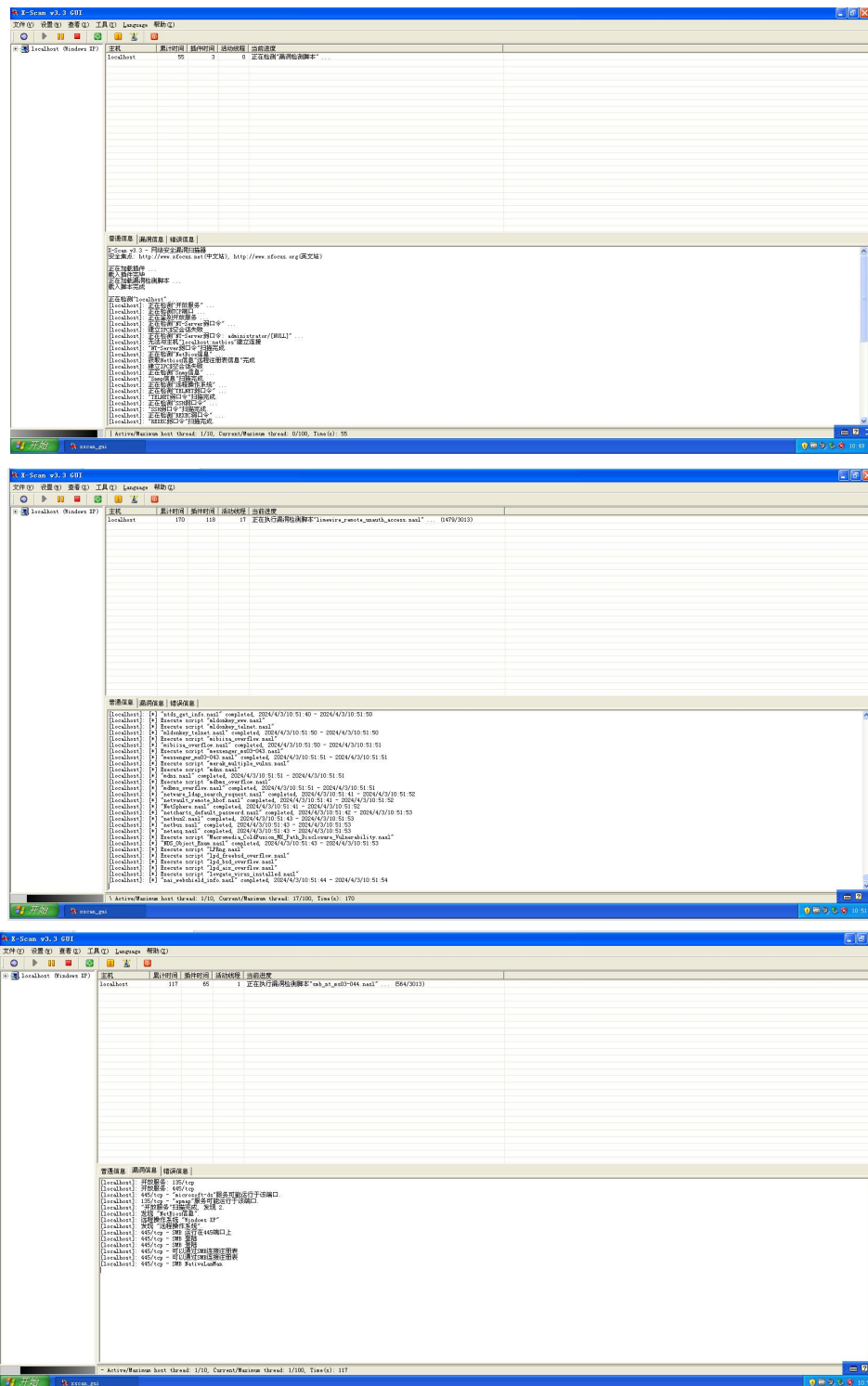
- 字典文件设置：设置扫描弱口令时用到的字典，可以编辑字典以自定义弱口令

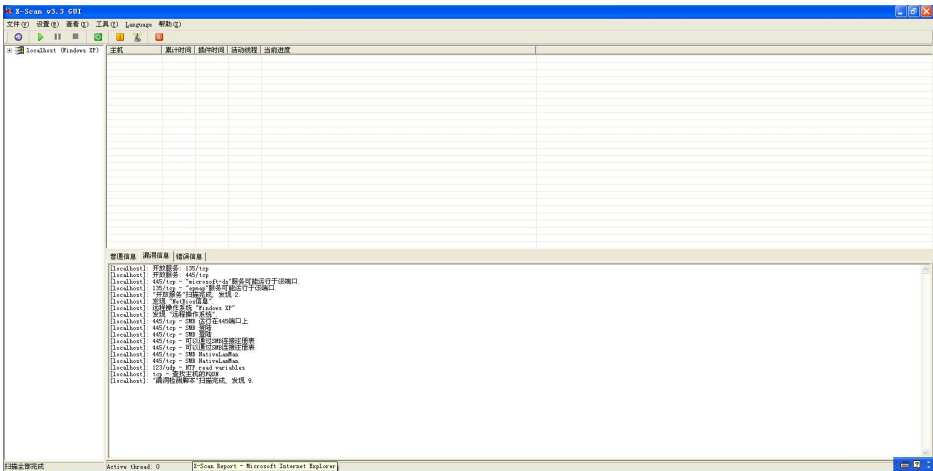


(三) 开始扫描

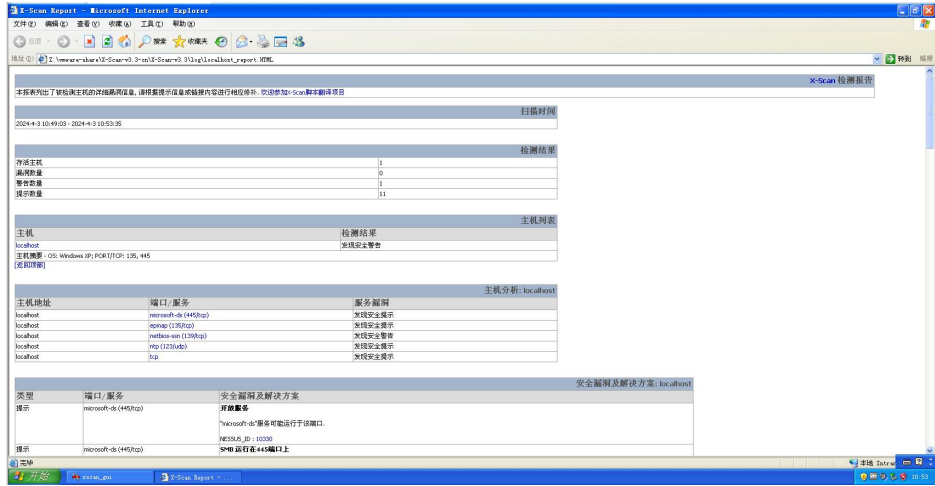
保存好配置后，点击工具栏的开始按钮即可进行扫描，x-scan 界面具有详细的扫描状态，扫描时间视扫描的深度和广度而定。

可以看到它将在我们开始设置扫描的端口一一进行检查，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。还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。





最后，检测结束之后会自动弹出检测报告，报告中可以看到我们扫描的主机中存活了几个（这里只设置了一个 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）



扫描时间	
2024-4-3 10:49:03 - 2024-4-3 10:53:35	

检测结果	
存活主机	1
漏洞数量	0
警告数量	1
提示数量	11

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: 135, 445	
[返回顶部]	

本次检测中在 microsoft-ds(445/tcp)、epmap(135/tcp)、ntp(123/udp)、tcp 中发现了安全提示，netbios-ssn(139/tcp)中发现了安全警告，具体信息如下。

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：

主机分析: localhost		
主机地址	端口 / 服务	服务漏洞
localhost	microsoft-ds (445/tcp)	发现安全提示
localhost	epmap (135/tcp)	发现安全提示
localhost	netbios-ssn (139/tcp)	发现安全警告
localhost	ntp (123/udp)	发现安全提示
localhost	tcp	发现安全提示

安全漏洞及解决方案: localhost		
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	microsoft-ds (445/tcp)	SMB 运行在445端口上 远程主机开放了445端口，设有开放139端口。 两台Windows 2000 主机间的Netbios-less)通讯通过445端口完成。攻击者可以利用该漏洞获取主机的共享连接，用户名列表及其他信息... 解决方案: 过滤该端口收到的数据。 风险等级: 中 A CIFS server is running on this port NESSUS_ID : 11011
提示	microsoft-ds (445/tcp)	SMB 登陆 当前脚本尝试使用多个login/password组合登陆远程主机 参考资料: http://support.microsoft.com/support/kb/articles/Q143/4/74.ASP 参考资料: http://support.microsoft.com/support/kb/articles/Q246/2/61.ASP 风险等级: 中 - NULL sessions are enabled on the remote host CVE_ID : CAN-1999-0504, CAN-1999-0506, CVE-2000-0222, CAN-1999-0505, CAN-2002-1117 BUGTRAQ_ID : 494, 990, 11199 NESSUS_ID : 10394
提示	microsoft-ds (445/tcp)	SMB 登陆 当前脚本尝试使用多个login/password组合登陆远程主机 参考资料: http://support.microsoft.com/support/kb/articles/Q143/4/74.ASP 参考资料: http://support.microsoft.com/support/kb/articles/Q246/2/61.ASP 风险等级: 中 - NULL sessions are enabled on the remote host CVE_ID : CAN-1999-0504, CAN-1999-0506, CVE-2000-0222, CAN-1999-0505, CAN-2002-1117 BUGTRAQ_ID : 494, 990, 11199 NESSUS_ID : 10394
提示	microsoft-ds (445/tcp)	可以通过SMB连接注册表 用户可以使用SMB测试中的login / password 组合远程连接注册表。 允许远程连接注册表存在潜在危险，攻击者可能由此获取更多主机信息。 解决方案: 如果还没有安装service pack 3补丁，先安装之。同时设置注册表子键 HKEYSYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg 的权限，只允许管理员用户浏览其内容。 另外，有必要考虑从相关端口过滤主机接收到的数据。 风险等级: 低 It was not possible to connect to PIPE\winreg on the remote host. If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access' service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials. NESSUS_ID : 10400

五、实验结论及心得体会

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。