综合扫描实验

应用场景

随着计算机网络的普及和发展，人们利用网络可以方便快捷地进行各种信息处理，例如，网上办公、电子商务、分布式数据处理等。但网络也存在不容忽视的问题，例如，用户的数据被篡改、合法用户被冒充、通信被中断等。面临着大量的网络入侵事件，就必须要求在一个开放式的计算机网络物理环境中构造一个封闭的逻辑环境来保障敏感信息和保密数据不受到攻击。为此迫切需要对网络安全作分类研究，把各种网络安全问题清楚有序地组织起来，从而构建一个合理、安全、高效的网络防御体系。

网络安全保护的核心是如何在网络环境下保证数据本身的秘密性、完整性与操作的正确性、合法性与不可否认性。而网络攻击的目的正相反，其立足于以各种方式通过网络破坏数据的秘密性和完整性或进行某些非法操作。

网络及其应用的广泛发展，安全威胁呈现出攻击的种类、方法和总体数量越来越多、破坏性和系统恢复难度也越来越大。这就要求我们对攻击方法有更进一步的研究;对安全策略有更完善的发展，建立起一个全面的、可靠的、高效的安全体系。

漏洞扫描程序对于每个漏洞都有自己的探测程序并以插件形式来调用，用户可以根据需要扫描的漏洞来调度相应的探测程序。探测程序的来源有两种:首先是提炼漏洞的特征码构造发送数据包，其次是直接采用一些安全站点公布的漏洞试探程序。其本质就是模拟黑客的入侵过程，但是在程度上加以限制，以防止侵害到目标主机。可以看出要恰到好处的控制探测程度是非常关键并具有较大难度的。因为程度太浅就无法保证探测的准确性，程度太深就会变成黑客入侵工具。有效的探测程序不仅仅取决于漏洞特征码的提炼是否精确而且受到漏洞本身特性的影响。例如对缓冲区溢出漏洞的探测，黑客的攻击通常是发送精心构造的一串字符串到目标主机没有加以边界判别的缓冲区，作为探测程序，为了模拟这个过程，我们可以同样发送一串很长但没有任何意义的字符串，查看目标主机有没有报错应答。如果有，说明对该缓冲区的边界长度的越界作出了判断，但是如果没有回应，作为探测程序无法再继续发送精心构造的字符串来查看对方的应答，因为这样可能导致入侵的发生。其后的处理方式一种是认定对方存在这种漏洞，一种是交给用户去判断，因为可能尽管目标主机没有报错但是实际上已经进行了处理。

VM Server　　VM Client

实验目标：

- 掌握漏洞扫描技术原理

- 了解常见的系统漏洞及防范方法
- 掌握典型的综合扫描工具

实验环境：

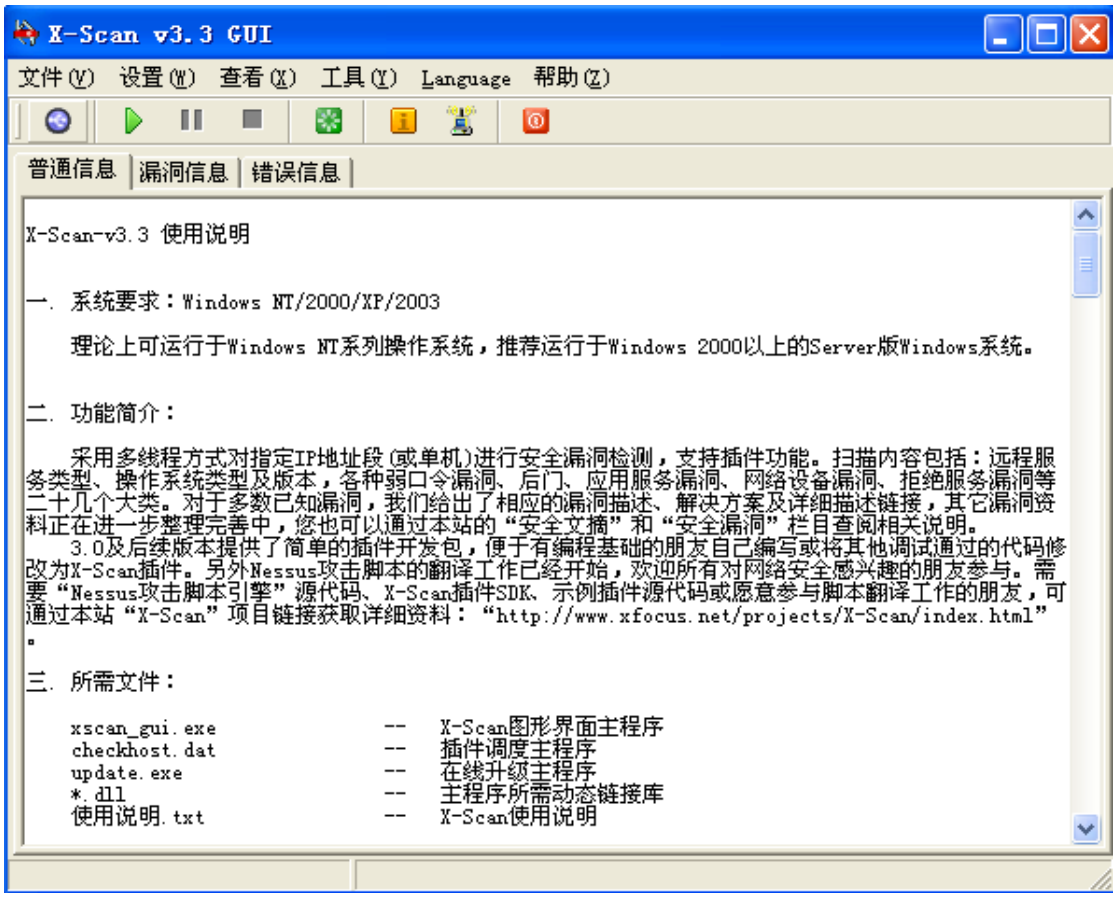
虚拟机： Windows 2000，XP，2003，X-SCAN 扫描软件

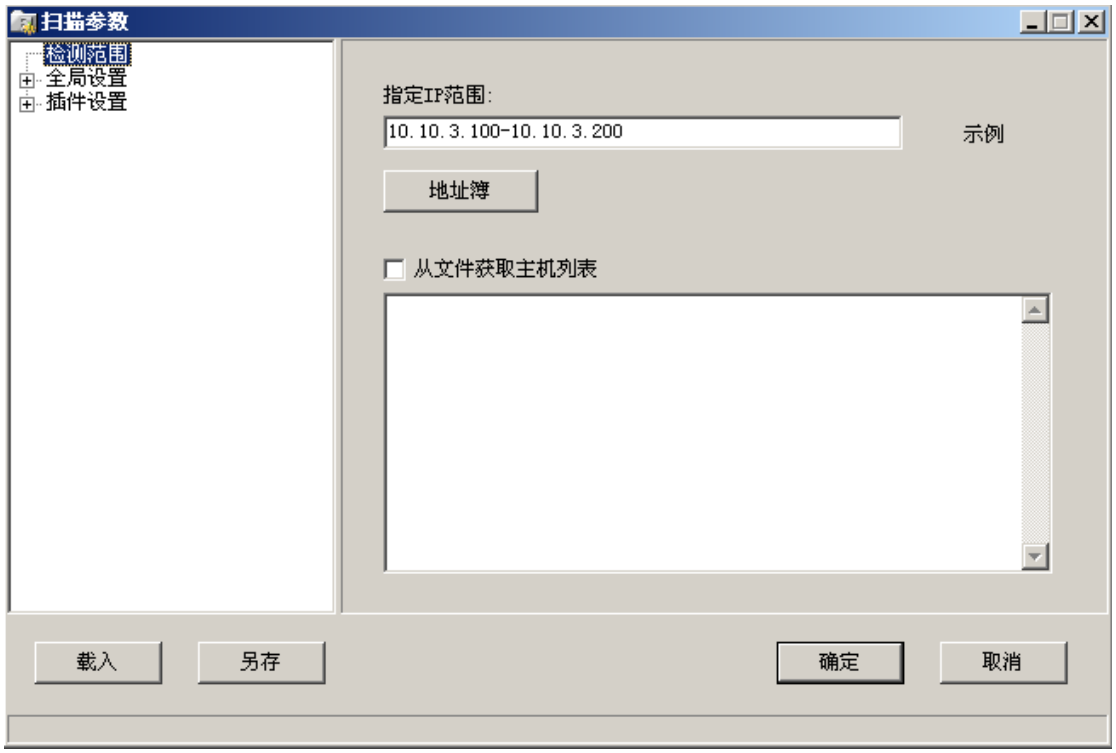
实验过程指导：

启动虚拟机，并设置虚拟机的 IP 地址，以综合扫描服务端为目标主机进行攻防试验。个别实验学生可以以 2 人一组的形式，互为攻击方和被攻击方来做实验。

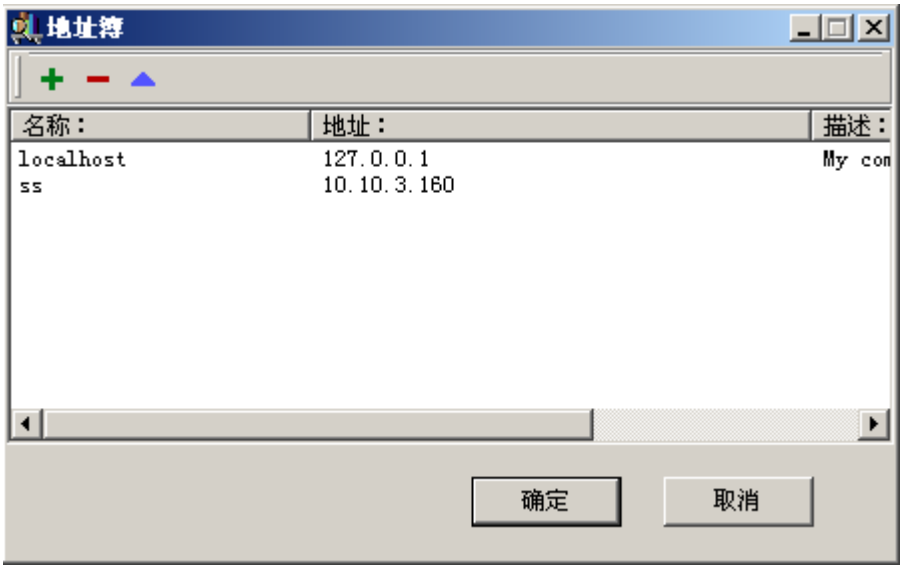
一． 设置X-Scan 参数。

1. 打开综合扫描客户端运行界面进行设置，点击菜单栏“设置”中的参数设置进入参数设置界面如下：





“地址簿”可将预先添加好的各个地址直接加入到 ip 地址内。

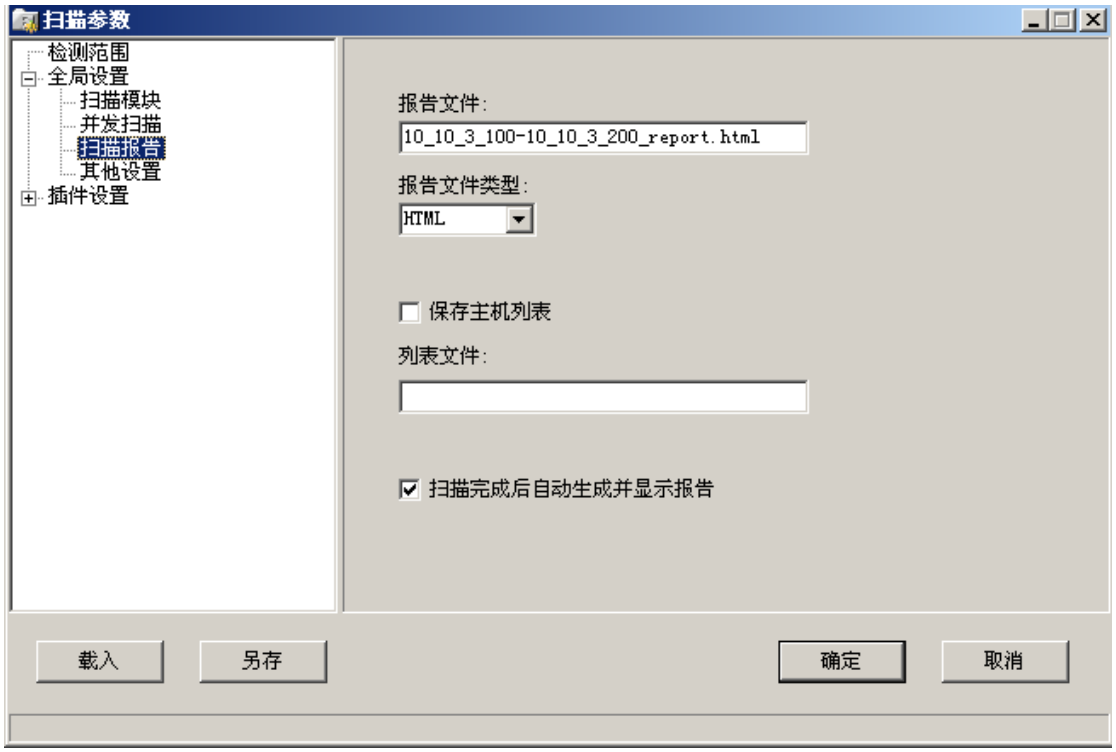


2. 全局设置：此模块包含所有全局性扫描选项。

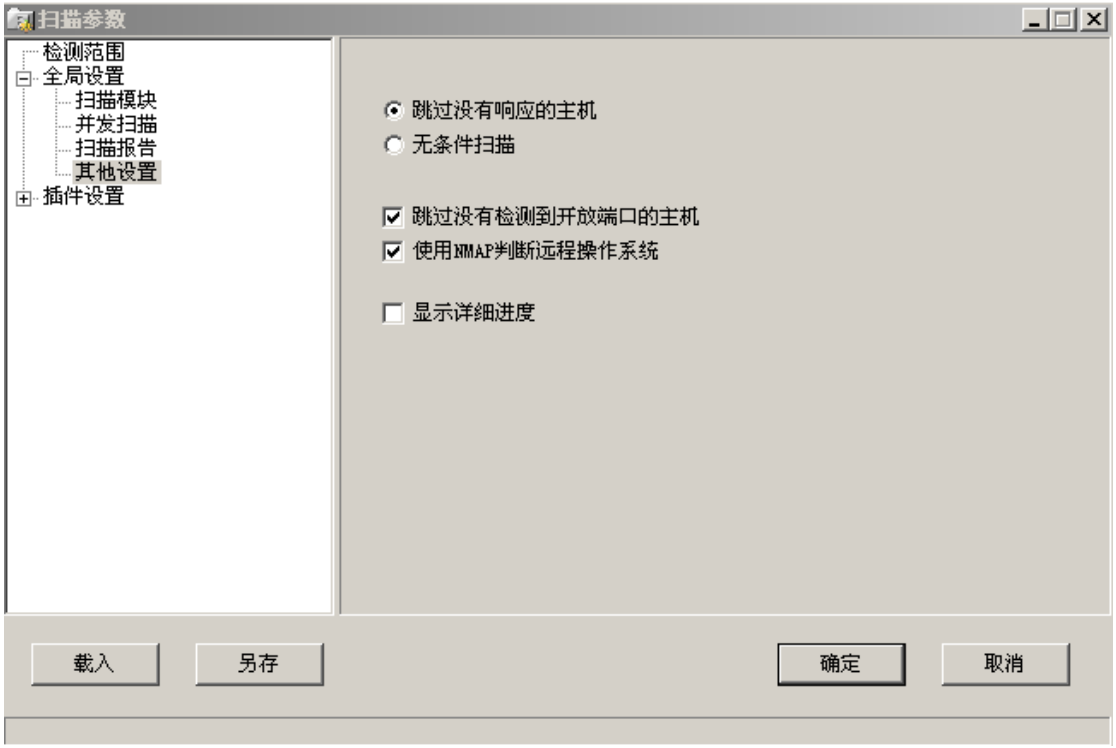
（1） 扫描模块：主要包含一些服务和协议弱口令等信息的扫描，根据字典探测主机各种服务的开启情况及相应的弱口令，对应到每一项都有相应的说明，如图所示的远程操作系统。

（2） 并发扫描：主要是对扫描的并发数量进行设置，包括最大并发主机数、最大并发线程数和各插件最大并发数量的设置。

（3） 扫描报告：对主机进行扫描完成后的报告生成情况进行设定。

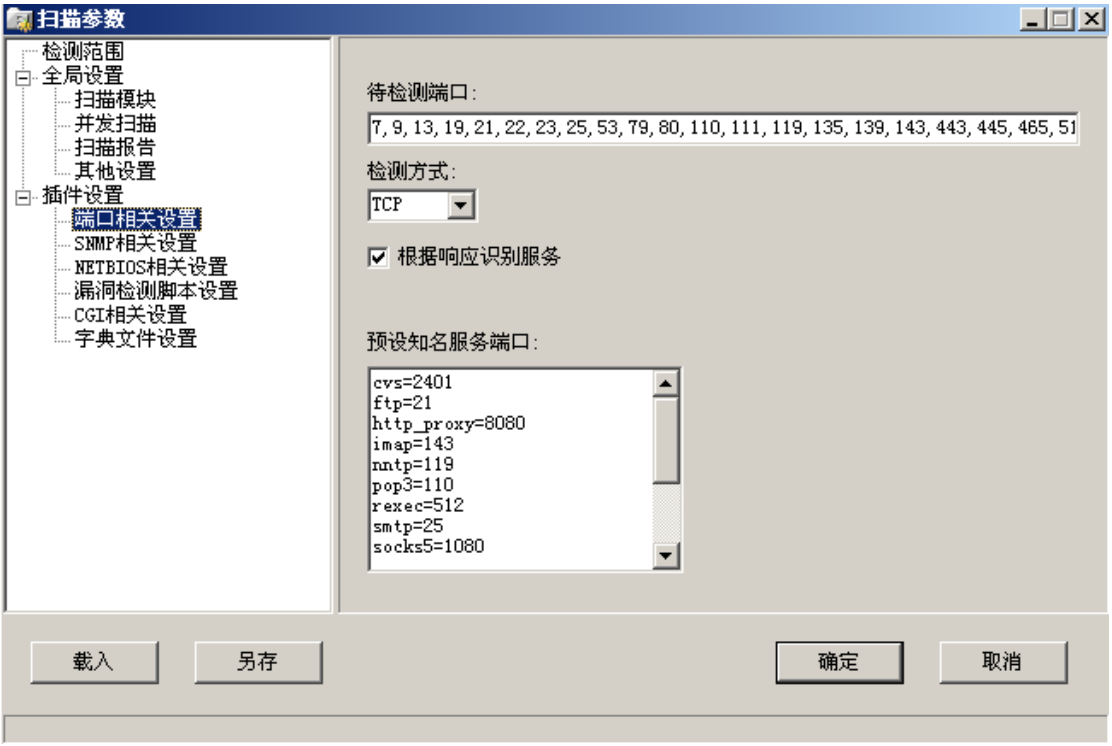


（4） 其它设置：主要是对扫描过程中对扫描进度的显示和附加的一些设置，可根据教学需要进行设置。

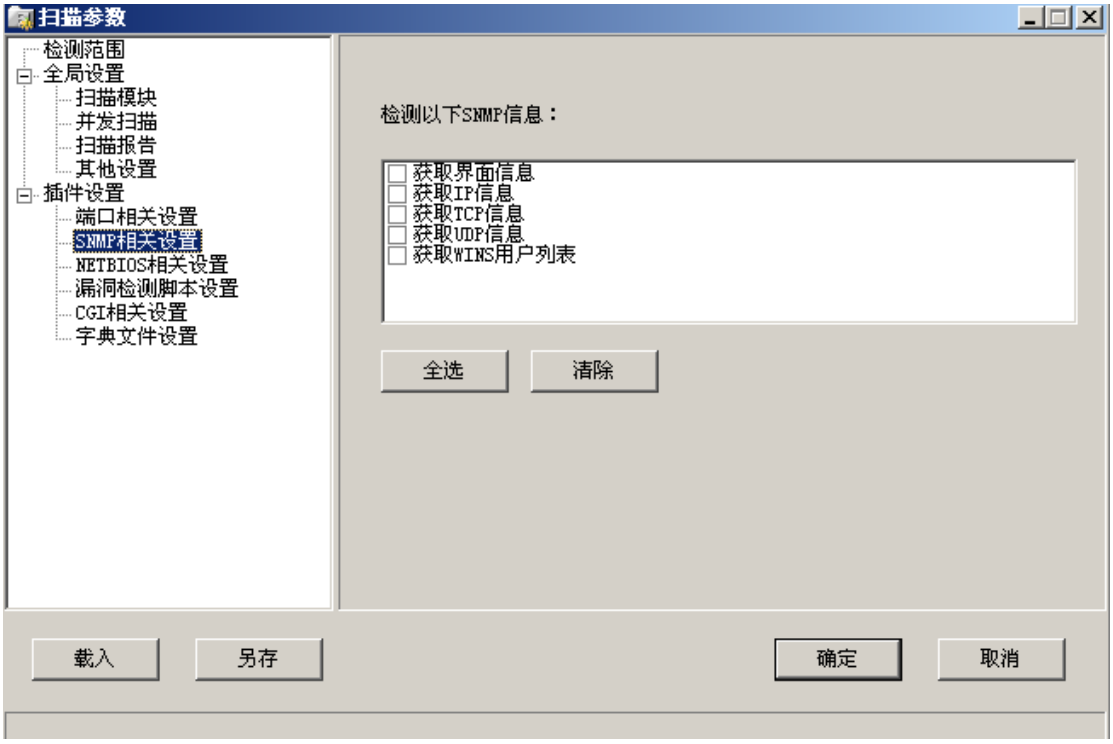


3. 插件设置：此模块包含各扫描插件的相关设置。

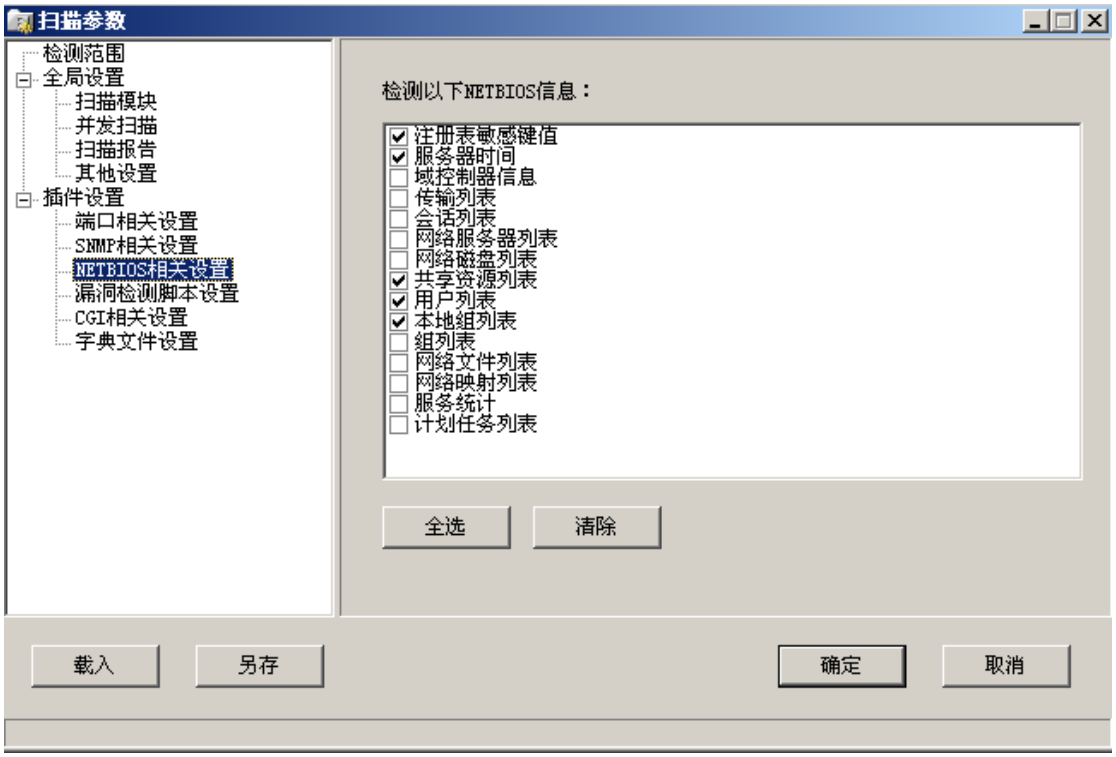
（1） 端口相关设置：主要设置想要扫描的各个端口、检测方式和预设的各个服务协议的端口等内容：



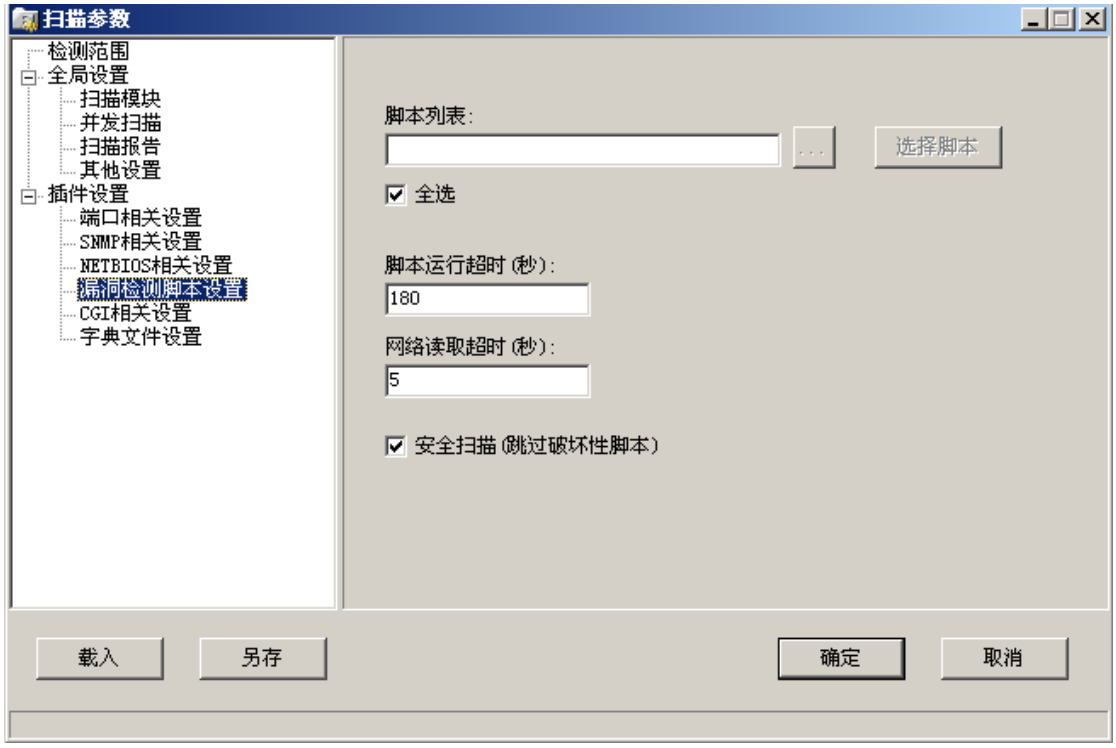
（2） SNMP 相关设置：主要设置检测 SNMP 的相关信息：



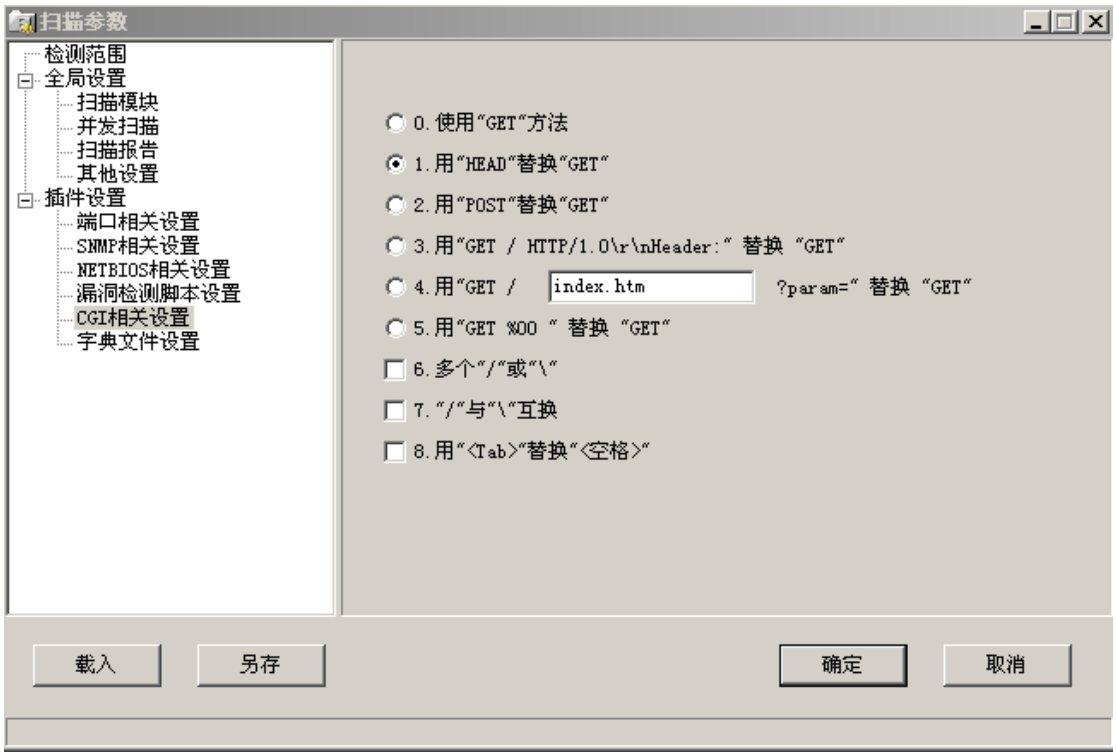
（3） NETBIOS 相关设置：主要设置检测 NETBIOS 的相关信息：



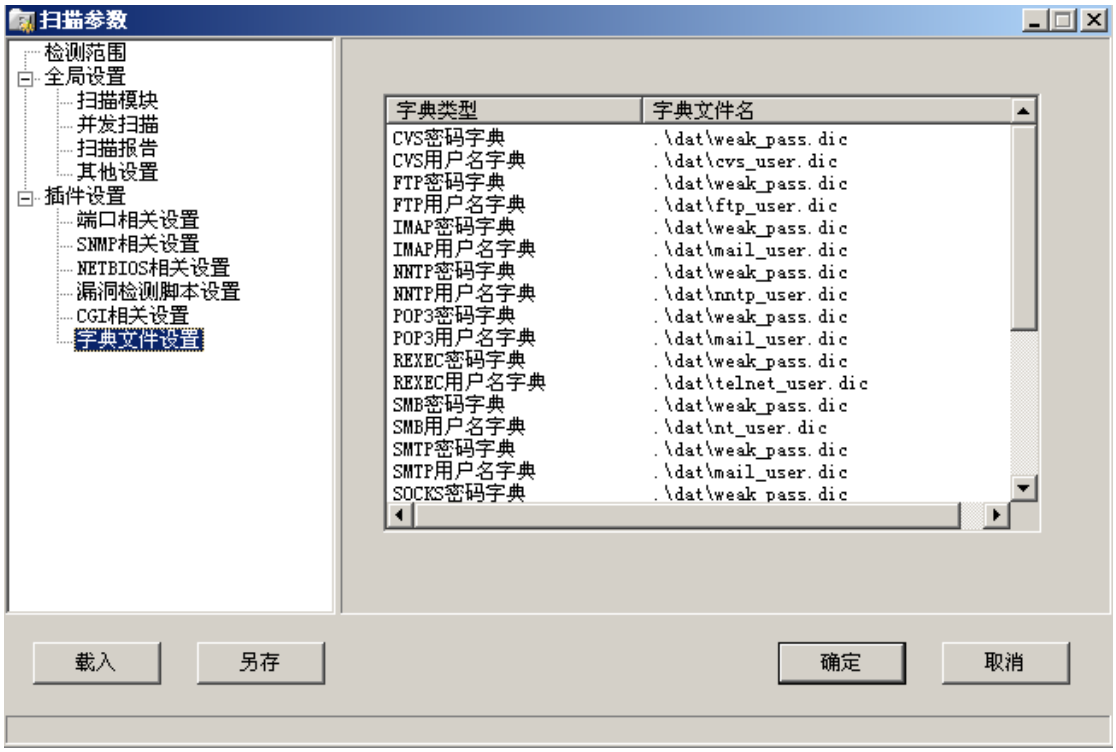
（4） 漏洞检测脚本设置：主要是针对于各个漏洞编写的检测脚本进行筛选，选择需要利用的脚本，为方便起见一般设置为全选，也可格局自己需要选择：



（5） CGI 相关设置：对 CGI 的一些参数进行设置：

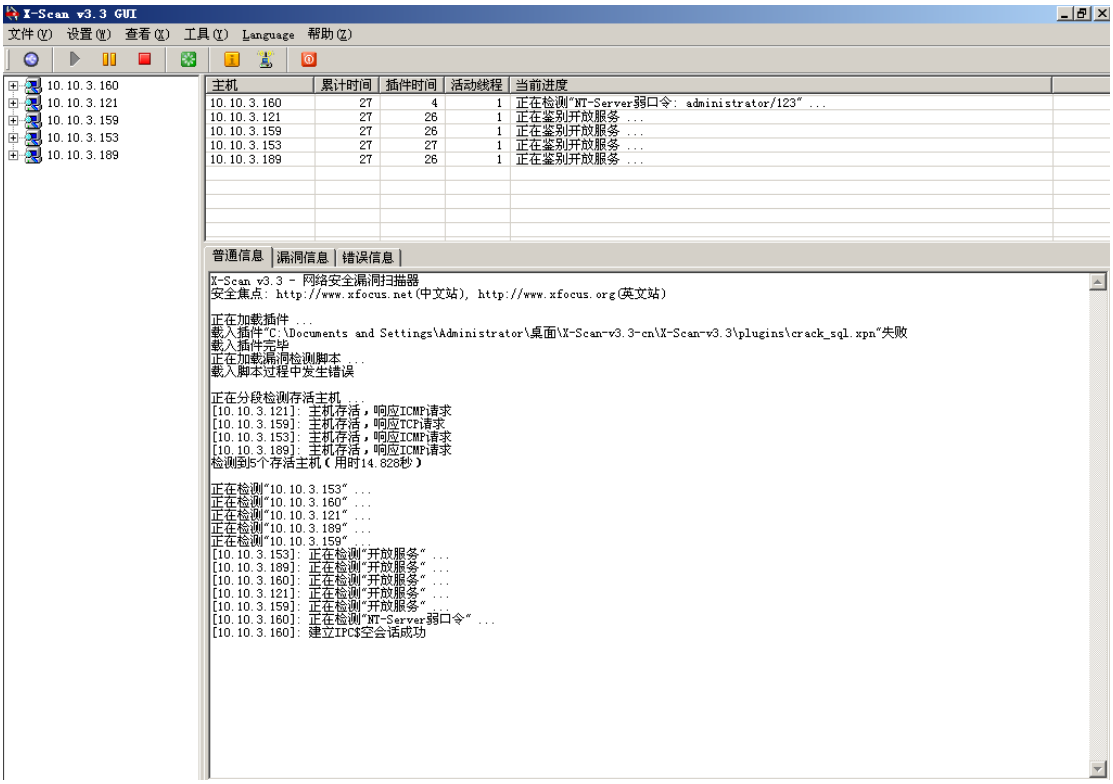


（6） 字典文件设置：主要是对扫描过程中所需要用到的字典进行选取，也可自己手动进行添加数据字典：



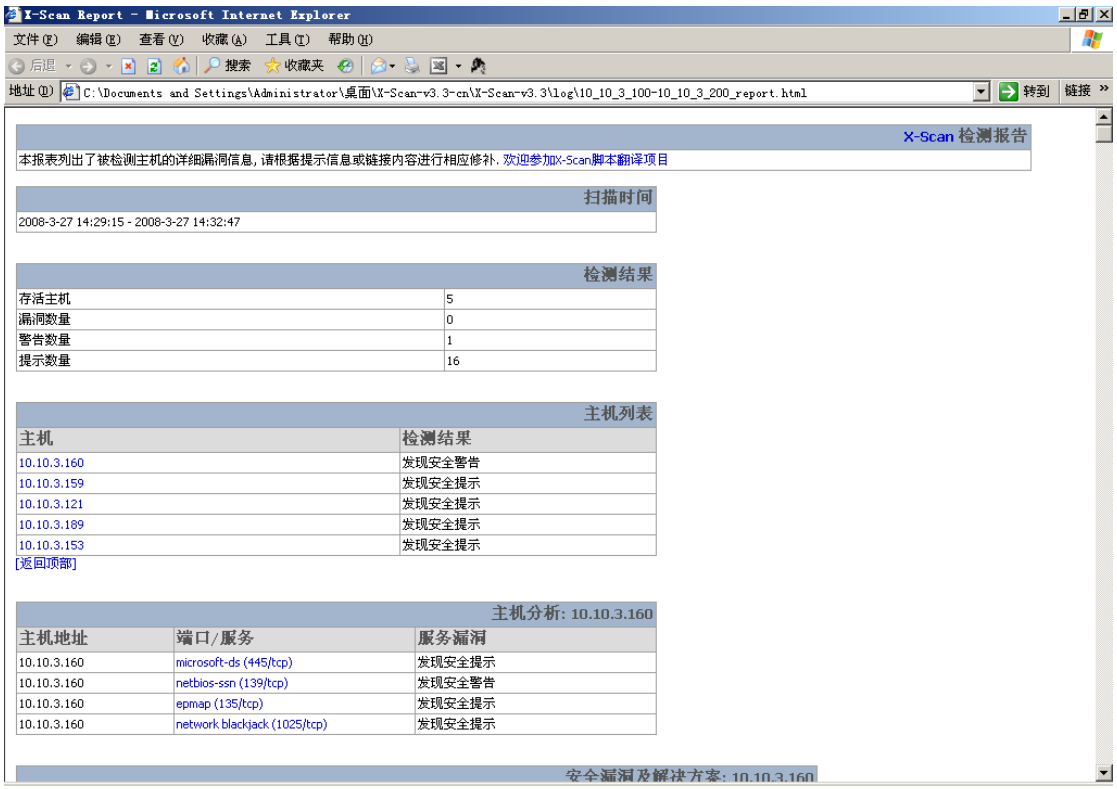
二． 进行扫描：

设置完成后点击绿色按钮或菜单中文件->开始扫描进行探测扫描，此扫描的速度与网络环境情况和本机配置等有关，不尽相同：



1. 报告生成：

扫描完成后会根据报告设置中自动生成报告项生成报告：



2. 根据探测扫描报告取得的信息进行漏洞测试：

检测到 FTP 弱口令漏洞：

主机分析: 10.10.3.159		
主机地址	端口/服务	服务漏洞
10.10.3.159	microsoft-ds (445/tcp)	发现安全提示
10.10.3.159	ftp (21/tcp)	发现安全提示
10.10.3.159	epmap (135/tcp)	发现安全提示
10.10.3.159	network blackjack (1025/tcp)	发现安全提示
10.10.3.159	MySql (3306/tcp)	发现安全提示

安全漏洞及解决方案: 10.10.3.159		
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	ftp (21/tcp)	**开放服务** "ftp"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	network blackjack (1025/tcp)	**开放服务** "network blackjack"服务可能运行于该端口. NESSUS_ID : 10330

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。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。

【实验思考】

1. 自己设计一些安全漏洞并用 X-Scan 进行漏洞抓取测试。
2. 怎样设置能够扫描出更多的漏洞。
3. 远程主机怎样设置才能防止漏洞发生