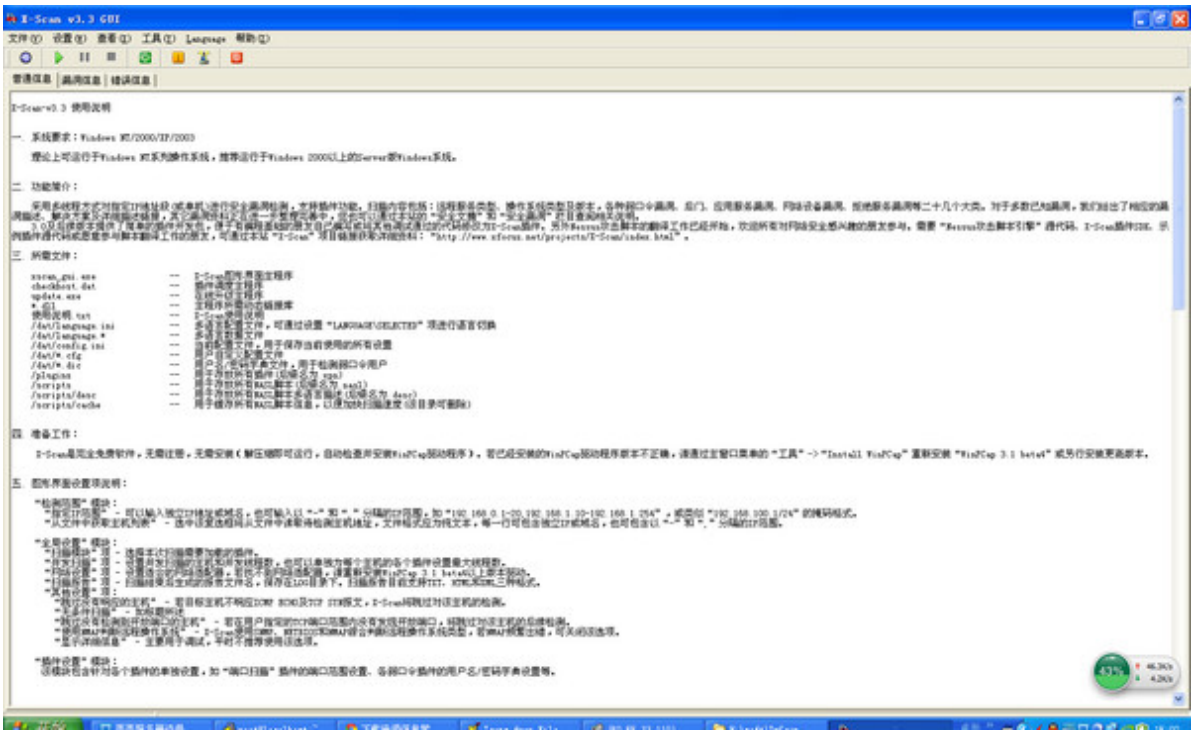
X-Scan

下载地址

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。

X-Scan扫描器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，xscan软件还支持插件功能，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。对于一些已知漏洞，我们给出了相应的漏洞描述、利用程序及解决方案，其它漏洞资料正在进一步整理完善中，您也可以通过作者网站的“安全文献”和“漏洞引擎”栏目查阅相关说明。

X-Scan 软件截图(或写成 xscan)：



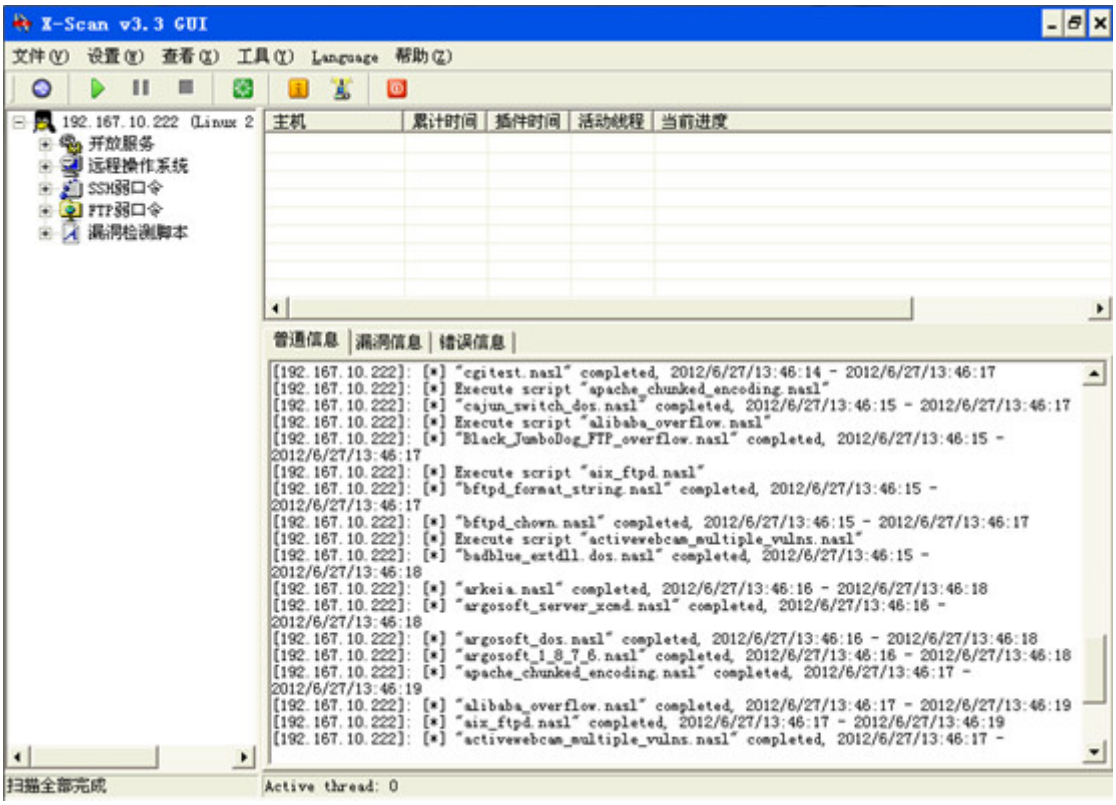
X-Scan扫描器安装说明：
华军软件园提供的X-Scan为3.3 简体中文版，**由于软件功能的特殊性可能存在报毒现象**，请大家自行选择，解压后直接运行“xscan_gui.exe”即可启动。

Win7无法运行X-Scan解决办法：
X-Scan在XP运行是没任何问题的，如果在win7系统出现了npptools.dll丢失的情况，那么下载“npptools.dll”，然后将其放置到X-Scan文件夹下即可，注意一定要你X-Scan的文件夹，不是system32文件夹。

X-Scan扫描器使用教程

一、界面

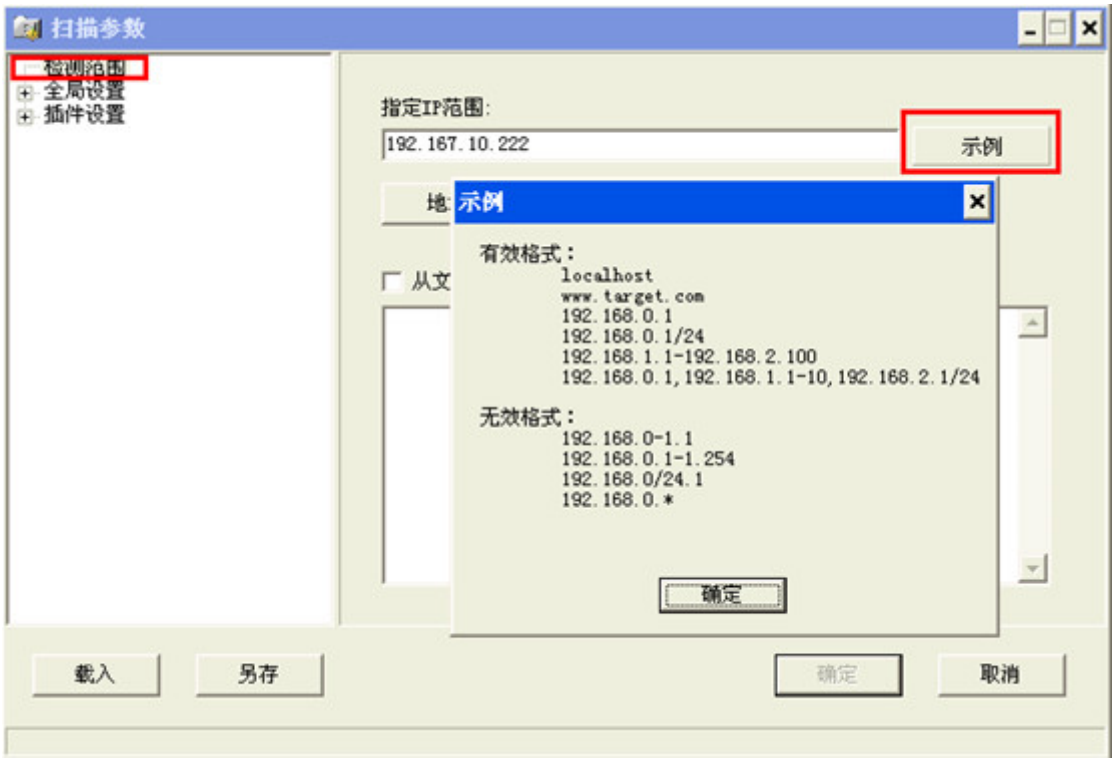
X-Scan界面如下图显示，大体分为三个区域，界面上面为菜单栏，界面下方为状态栏，若软件为英文版，可以在菜单栏的Language菜单将语言设置为中文。



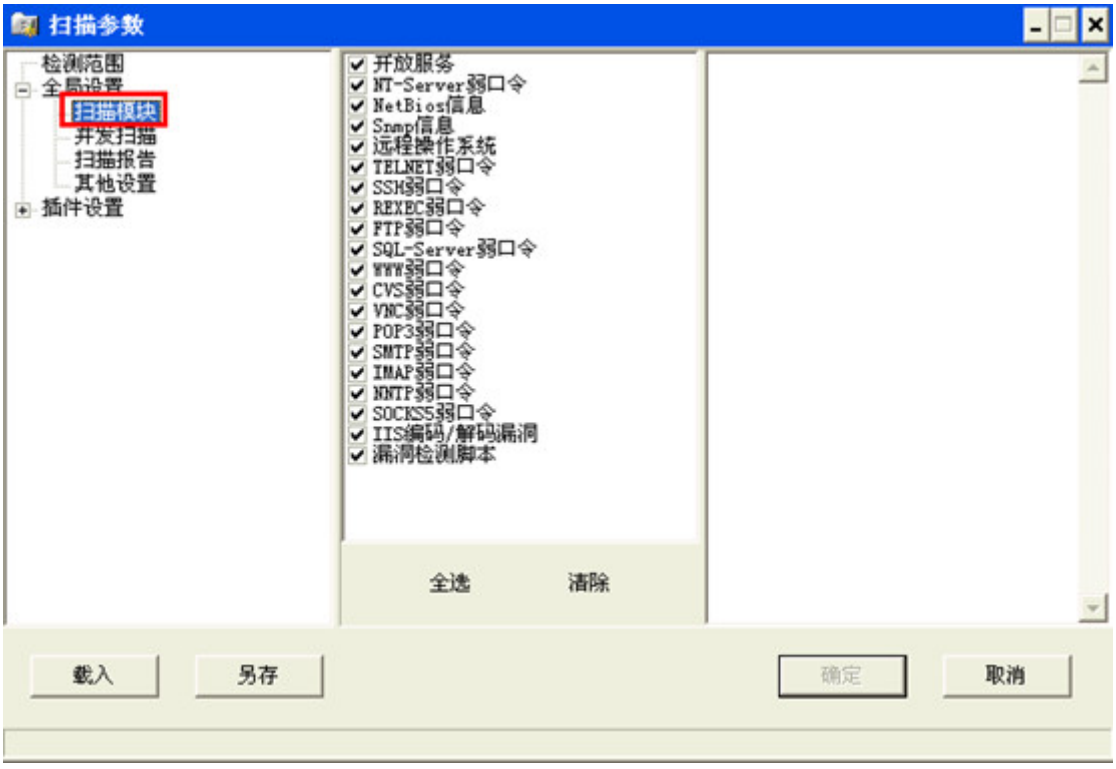
二、参数设置

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。

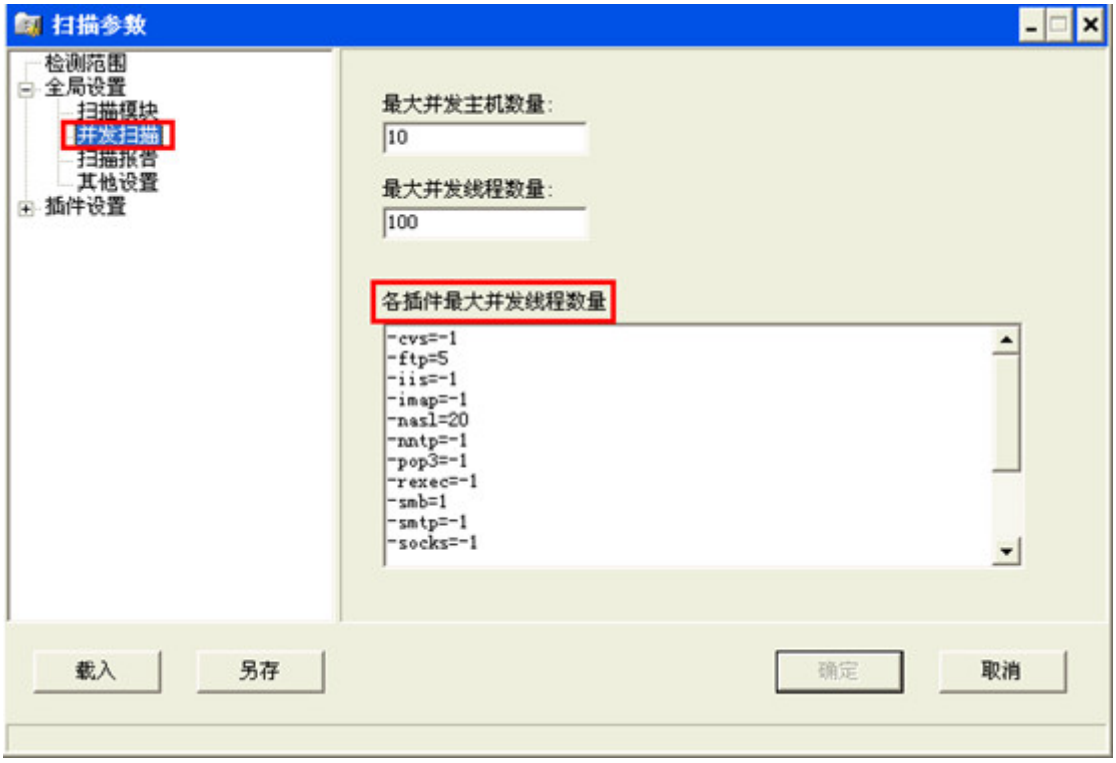
1、检测范围：设置待扫描的IP，可以按示例方式设置检测范围，或者从文件获取主机列表。



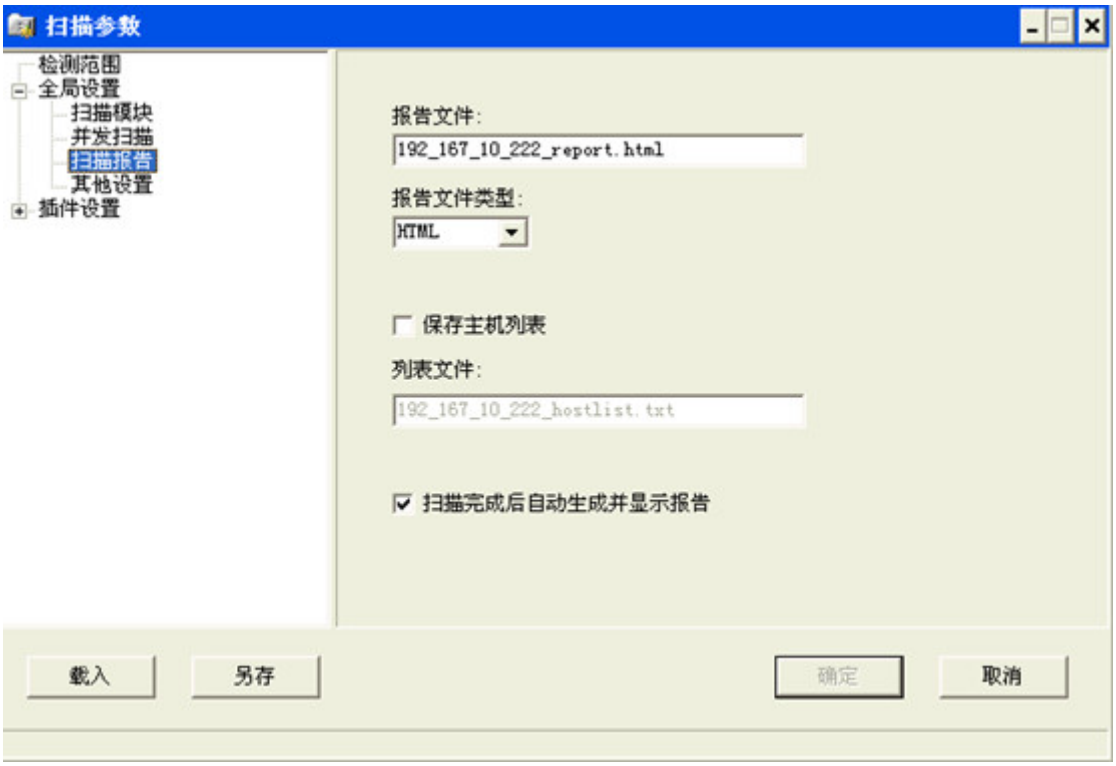
2、全局设置：用来设置全局的扫描参数，具体如下：
扫描模块：设置需要扫描的模块，对于单台设备的扫描，可以选择全部模块，如果扫描某个范围里面的设备，可以按需勾选需要扫描的模块。



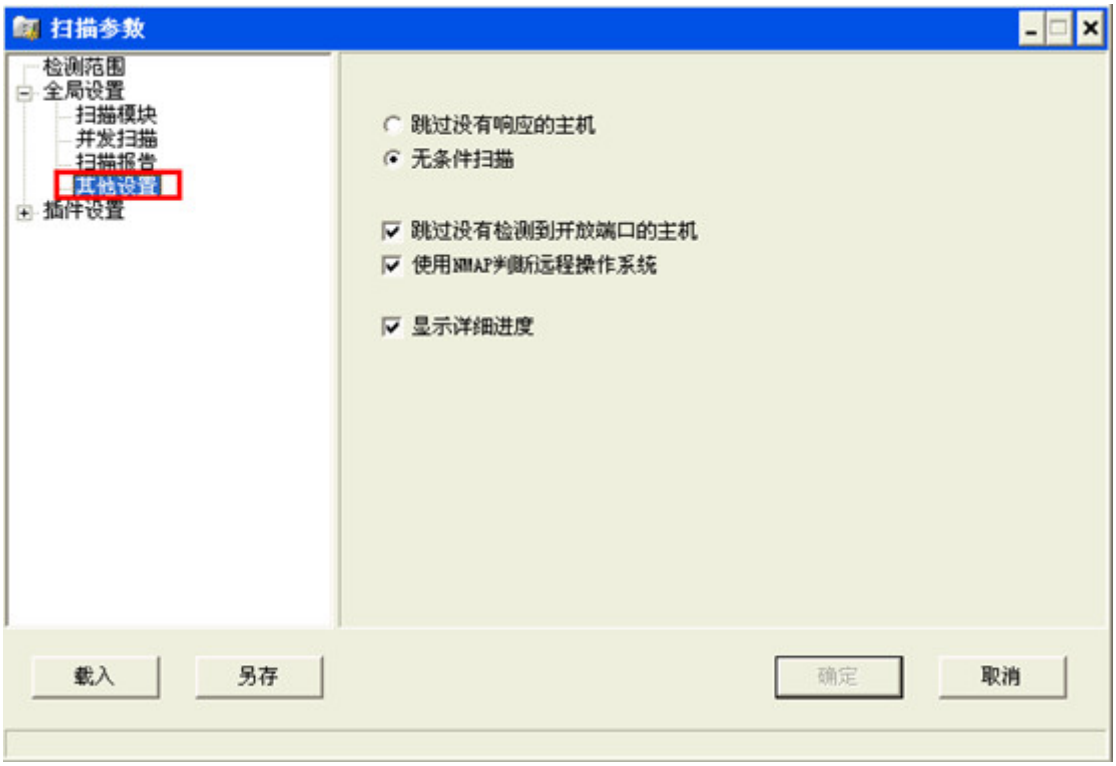
并发扫描：设置扫描的并发量，默认即可。如果机器性能好，带宽足够，可以适当增大并发量



扫描报告：设置扫描报告的名称和类型等

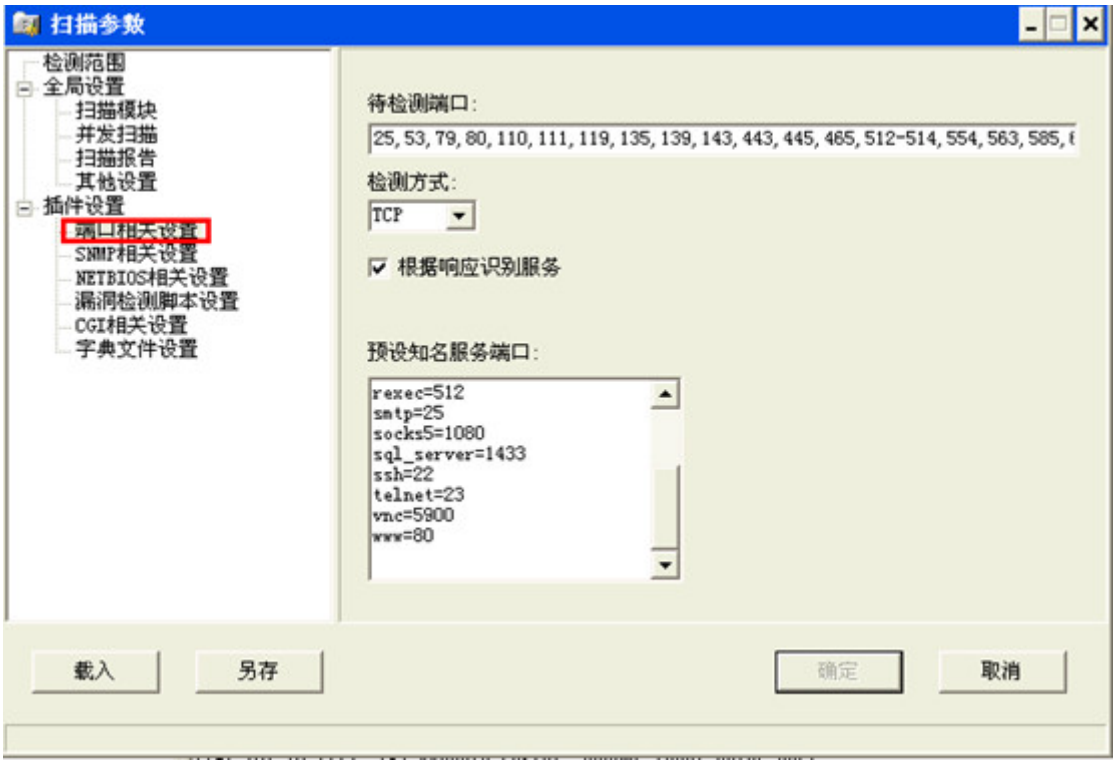


其它设置：设置对目标设备的检测机制等，如果是单个设备，建议使用无条件扫描，因为测试发现xscan判断主机是否存活不是很准确。

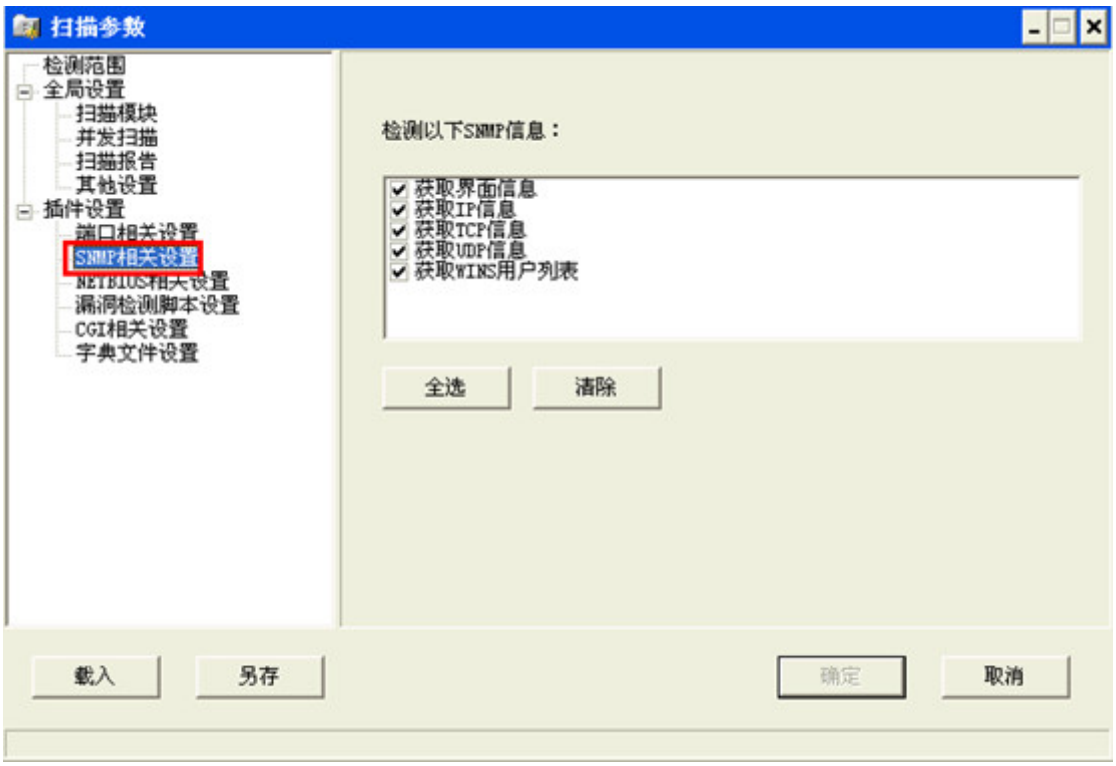


3、插件设置：设置各插件的相关选项

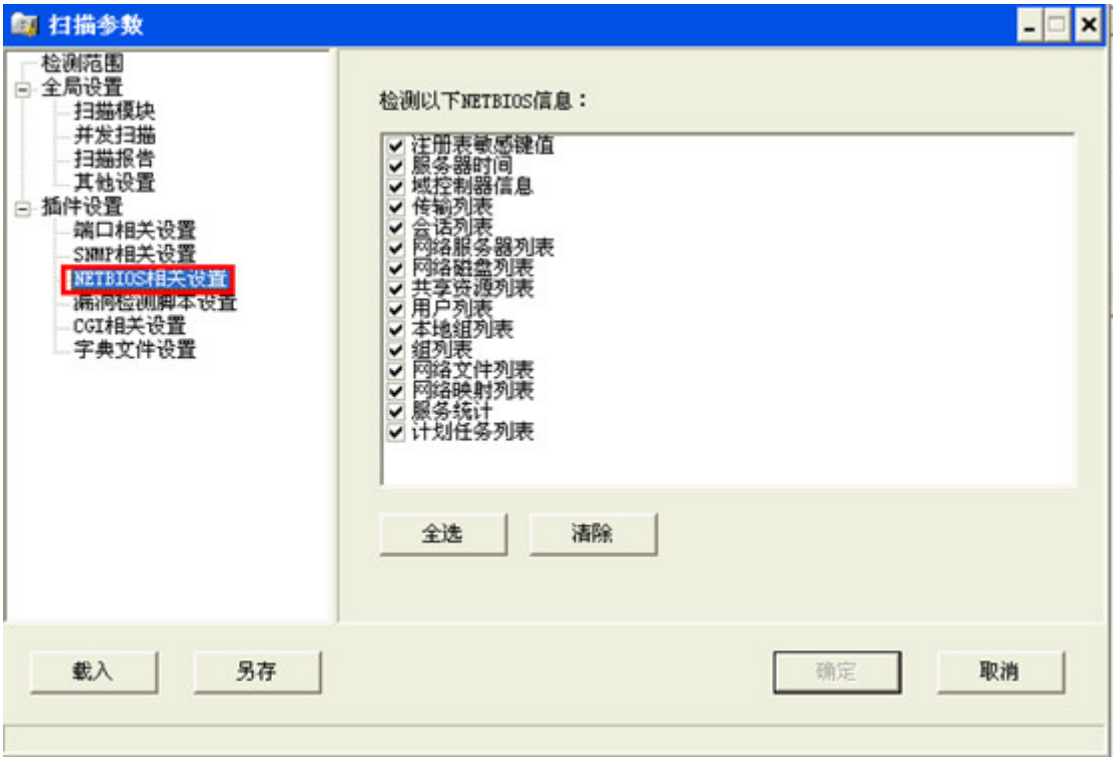
端口相关设置：设置与端口有关的项。待检测端口可以是任意端口的组合。检测方式使用TCP能够提高x-scan的准确性，但容易被对方的防火墙阻塞，SYN却相反。根据响应识别服务，x-scan能够根据响应判断运行的服务，即使端口已被更改。预设知名服务端口，可以自定义某些端口为知名服务端口。



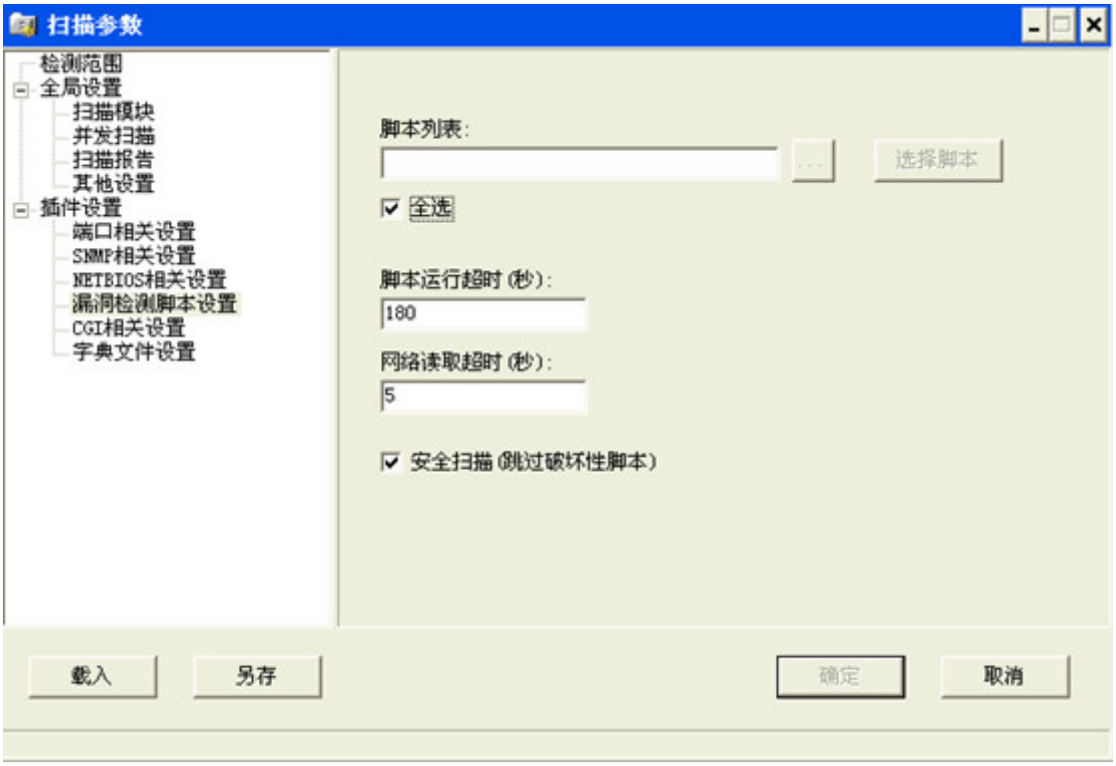
SNMP相关设置：设置SNMP协议检测项，建议全选。



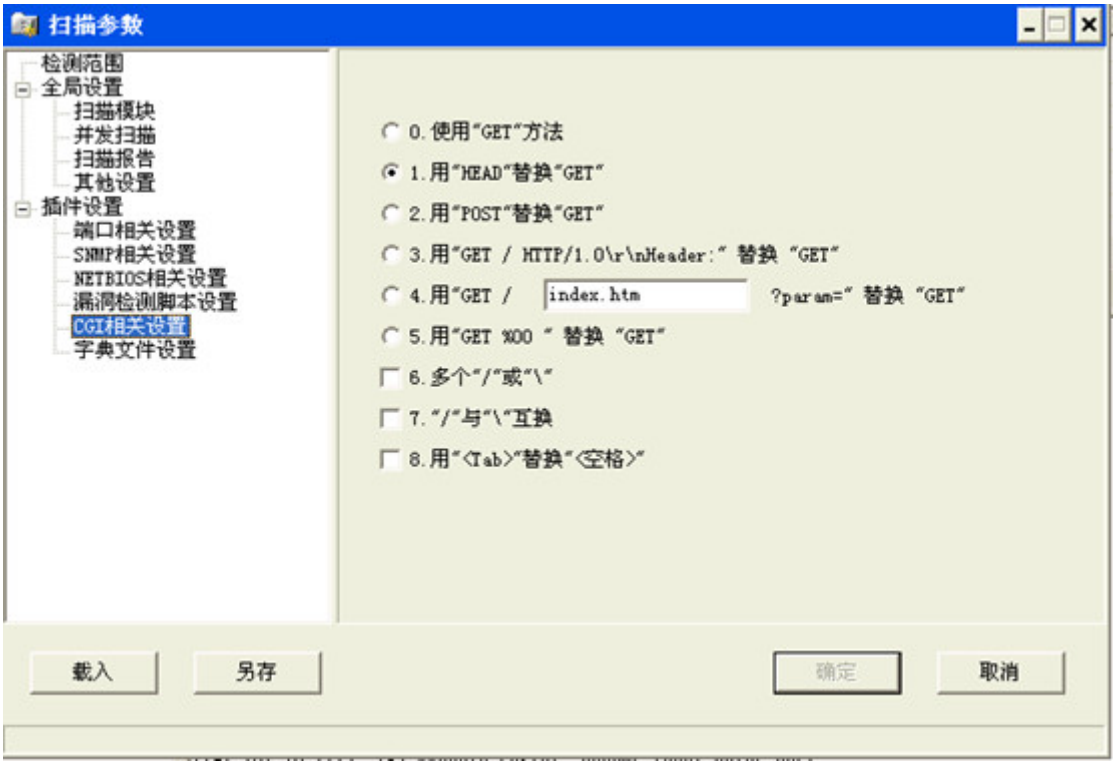
NETBIOS相关设置：设置检测的NETBIOS信息，主要是针对windows系统的NETBIOS的检测，单个非windows设备测试时勾选也无所谓。



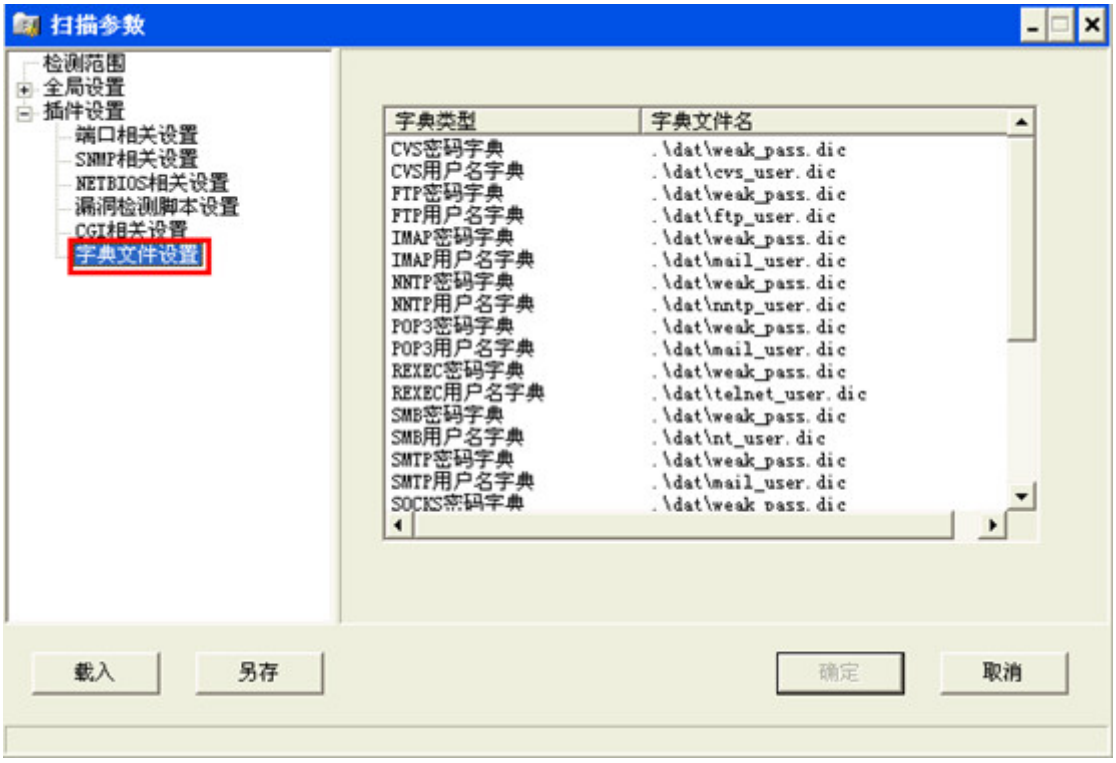
漏洞检测脚本设置：默认即可



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。

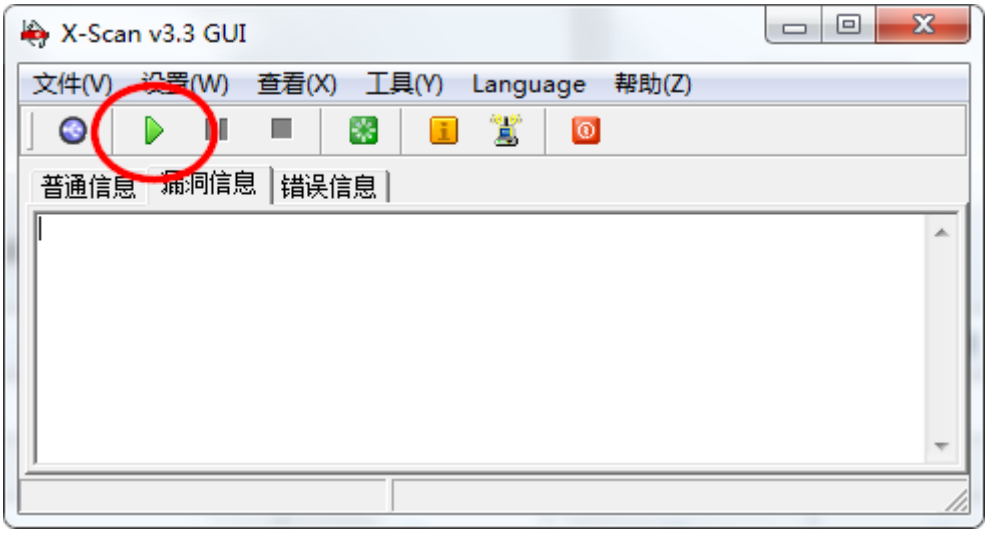


字典文件设置：设置扫描弱口令时用到的字典，可以编辑字典以自定义弱口令



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。



四、扫描结果

扫描结束后，X-Scan会自动弹出扫描结果，结果会详细列出漏洞情况和解决建议，高危漏洞会以红色字体标出。如图：

检测结果	
存活主机	1
漏洞数量	3
警告数量	1
提示数量	10

主机列表	
主机	检测结果
192.167.10.222	发现安全漏洞

[返回顶部]

主机分析: 192.167.10.222		
主机地址	端口/服务	服务漏洞
192.167.10.222	MySql (3306/tcp)	发现安全提示
192.167.10.222	www (80/tcp)	发现安全提示
192.167.10.222	ssh (22/tcp)	发现安全漏洞
192.167.10.222	ftp (21/tcp)	发现安全漏洞

X-Scan扫描器设置说明

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“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。