扫描工具 X-Scan 使用说明

1 X-Scan 简介

X-scan 是国内相当出名的扫描工具，是安全焦点又一力作。完全免费，无需注册，无需安装（解压缩即可运行），无需额外驱动程序支持。可以运行在 Windows 9x/NT4/2000 上，但在 Windows 98/NT 4.0 系统下无法通过 TCP/IP 堆栈指纹识别远程操作系统类型，在 Windows 98 系统下对 Netbios 信息的检测功能受限。

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

解压完后 X-scan 的目录中有以下几个目录及文件：

xscan_gui.exe-- X-Scan for Windows 9x/NT4/2000 图形界面主程序

xscan.exe -- X-Scan for Windows 9x/NT4/2000 命令行主程序

使用说明.txt -- X-Scan 使用说明

oncrpc.dll -- RPC 插件所需动态链接库

libeay32.dll -- SSL 插件所需动态链接库

/dat/language.ini -- 多语言数据文件，可通过设置"LANGUAGE\SELECTED"项进行语言切换

/dat/config.ini -- 用户配置文件，用于保存待检测端口列表、CGI 漏洞检测的相关设置及所有字典文件名称(含相对路径)

/dat/config.bak -- 备份配置文件，用于恢复原始设置

/dat/cgi.lst -- CGI 漏洞列表

/dat/rpc.ini -- 用于保存 RPC 程序名称及漏洞列表

/dat/port.ini -- 用于保存已知端口的对应服务名称

/dat/*_user.dic -- 用户名字典文件，用于检测弱口令用户

/dat/*_pass.dic -- 密码字典，用于检测弱口令用户

/dat/os.finger -- 识别远程主机操作系统所需的操作系统特征码配置文件

/dat/wry.dll -- "IP-地理位置"地址查询数据库文件

/plugin -- 用于存放所有插件(后缀名为.xpn)，插件也可放在 xscan.exe 所在目

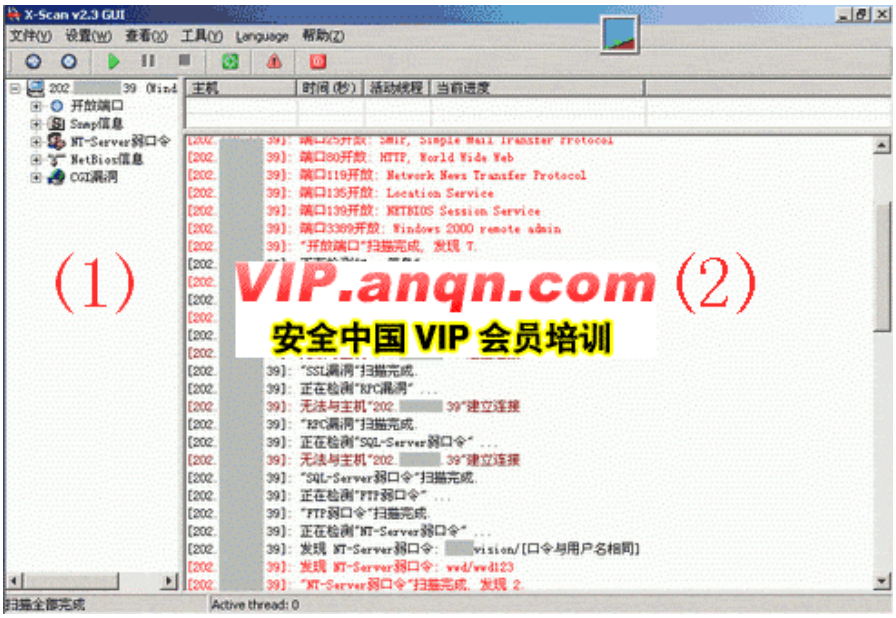
录的其他子目录中，程序会自动搜索。

本文主要介绍 X-scan 的图形界面，文后会附命令行模式的语法介绍。

2 X-Scan 基本功能介绍

2.1 系统运行

运行 xscan_gui.exe，下图就是 X-scan v2.3 的界面：

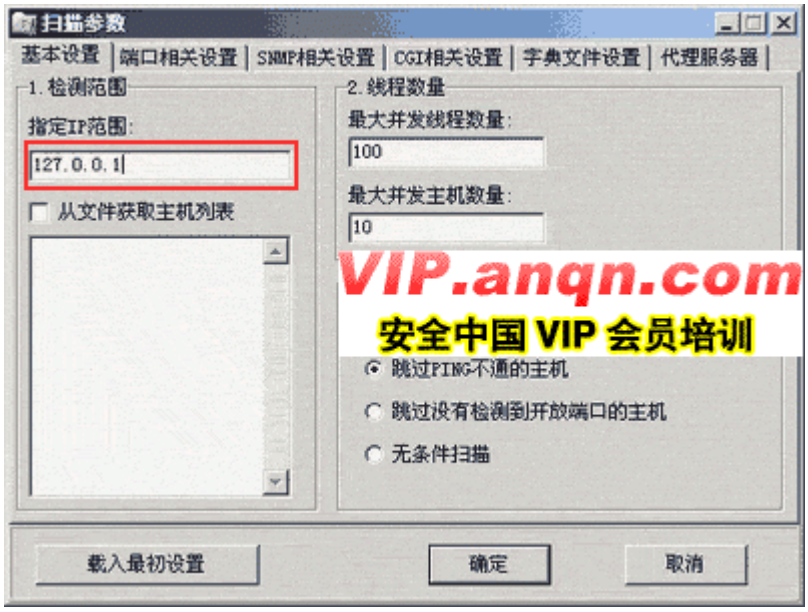


下面介绍一下工具栏（所有工具栏上的功能均可以在菜单中找到）

从左至右分别是:、扫描参数、开始扫描、暂停扫描、中止扫描、检测报告、使用说明、退出。

2.2 工作步骤

以下讲解具体的扫描步骤：先点击扫描参数，在下面红框内输入你要扫描主机的 ip 地址（或是一个范围）



其中跳过 PING 不通的的主机，跳过没有开放端口的主机，这样可以大幅度提高了扫描的效率，还有强制扫描。其它的如“端口相关设置”等可以进行比如进扫描某一特定端口等特殊操作（其实 X-scan 默认也只是扫描一些常用端口）。

参数设定好之后再点击扫描模块，可以选择扫描的项目

全部选择完后可以点击开始扫描进行扫描。在右边就会出现扫描的进度(如第一张图中标着(2)窗口）。

全部扫描完成后在左边出现漏洞的列表(如第一张图中标着(1)窗口），点击检测报告就会出现如下图报告

点击[详细资料]就会详细地介绍各个漏洞，并可以连接上 X-Focus 的站点，安全焦点有着庞大的数据库可供查询，网管可以通过他来找到漏洞的解决办法，入侵者可以利用他可以事半功倍。

X-scan 有着很全并且不断更新 CGI/IIS 漏洞库，点击菜单项的安全工具—〉CGI 列表维护会出现如下界面

在这可以对 CGI/IIS 的漏洞列表进行维护。

以上是对 X-scan 的一些简单的介绍。总之，X-scan 的确绝对是一款超经典

的扫描器，更确切的说是一款漏洞检查器，他和国内其他著名的同类软件（如流光、X-way 等）但相比扫描更加全面又无时间、IP 等限制，像流光功能强大且集成了许多工具，但其有使用时间限制和 IP 限制，并且新版的流光不能在 win9x 下运行，故 X-scan 更适合初学者使用。用他来检查自己系统的漏洞可以使配置自己系统的安全设置更方便。

2.3 命令行模式的语法介绍

命令格式: xscan -host <起始 IP>[-<终止 IP>] <检测项目> [其他选项]

xscan -file <主机列表文件名> <检测项目> [其他选项]

其中<检测项目> 含义如下:

-tracert : 跟踪路由信息；

-port : 检测常用服务的端口状态(可通过\dat\config.ini 文件的"PORT-SCAN-OPTIONS\PORT-LIST"项定制待检测端口列表)；

-snmp : 检测 Snmp 信息；

-rpc : 检测 RPC 漏洞；

-sql : 检测 SQL-Server 弱口令(可通过\dat\config.ini 文件设置用户名/密码字典文件)；

-ftp : 检测 FTP 弱口令(可通过\dat\config.ini 文件设置用户名/密码字典文件)；

-ntpass : 检测 NT-Server 弱口令(可通过\dat\config.ini 文件设置用户名/密码字典文件)；

-netbios : 检测 Netbios 信息；

-smtp : 检测 SMTP-Server 漏洞(可通过\dat\config.ini 文件设置用户名/密码字典文件)；

-pop3 : 检测 POP3-Server 弱口令(可通过\dat\config.ini 文件设置用户名/密码字典文件)；

-cgi : 检测 CGI 漏洞(可通过\dat\config.ini 文件的"CGI-ENCODE\encode_type"项设置编码方案)；

-iis : 检测 IIS 漏洞(可通过\dat\config.ini 文件的"CGI-ENCODE\encode_type"项设置编码方案)；

-bind : 检测 BIND 漏洞；

-finger : 检测 Finger 漏洞；

-sygate : 检测 sygate 漏洞；

-all : 检测以上所有项目；

[其他选项] 含义如下:

-v: 显示详细扫描进度

-p: 跳过 Ping 不通的主机

-o: 跳过没有检测到开放端口的主机

-t <并发线程数量[,并发主机数量]>: 指定最大并发线程数量和并发主机数量, 默认数量为 100,10

3 X-Scan-v3.3 使用说明

3.1 系统要求

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。

3.2 功能简介

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、拒绝服务漏洞等二十几个大类。对于多数已知漏洞，我们给出了相应的漏洞描述、解决方案及详细描述链接，其它漏洞资料正在进一步整理完善中，您也可以通过本站的“安全文摘”和“安全漏洞”栏目查阅相关说明。

3.0 及后续版本提供了简单的插件开发包，便于有编程基础的朋友自己编写或将其他调试通过的代码修改为 X-Scan 插件。另外 Nessus 攻击脚本的翻译工作已经开始，欢迎所有对网络安全感兴趣的朋友参与。需要“Nessus 攻击脚本引擎”源代码、X-Scan 插件 SDK、示例插件源代码或愿意参与脚本翻译工作的朋友，可通过本站“X-Scan”项目链接获取详细资料：“http://www.xfocus.net/projects/X-Scan/index.html”。

3.3 所需文件：

xscan_gui.exe -- X-Scan 图形界面主程序

checkhost.dat -- 插件调度主程序

update.exe -- 在线升级主程序

*.dll -- 主程序所需动态链接库

使用说明.txt -- X-Scan 使用说明

/dat/language.ini -- 多语言配置文件，可通过设置“LANGUAGE\SELECTED”

项进行语言切换

/dat/language.* -- 多语言数据文件

/dat/config.ini -- 当前配置文件，用于保存当前使用的所有设置

/dat/*.cfg -- 用户自定义配置文件

/dat/*.dic -- 用户名/密码字典文件，用于检测弱口令用户

/plugins -- 用于存放所有插件(后缀名为.xpn)

/scripts -- 用于存放所有 NASL 脚本(后缀名为.nasl)

/scripts/desc -- 用于存放所有 NASL 脚本多语言描述(后缀名为.desc)

/scripts/cache -- 用于缓存所有 NASL 脚本信息，以便加快扫描速度(该目录可删除)

3.4 准备工作

X-Scan 是完全免费软件，无需注册，无需安装（解压缩即可运行，自动检查并安装 WinPCap 驱动程序）。若已经安装的 WinPCap 驱动程序版本不正确，请通过主窗口菜单的“工具”->“Install WinPCap”重新安装“WinPCap 3.1 beta4”或另行安装更高版本。

3.5 图形界面设置项说明

3.5.1 “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。

3.5.2 “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。

3.5.3 “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。

3.5.4 “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。

3.5.5 常见问题解答

1) Q：如果没有安装 WinPCap 驱动程序是否能正常使用 X-Scan 进行扫描？

A：如果系统未安装 WinPCap 驱动，X-Scan 启动后会自动安装 WinPCap 3.1；如果系统已经安装了 WinPCap 更高版本，X-Scan 则使用已有版本。

2) Q：扫描一个子网，进程里同时出现 10 个 checkhost.exe 的进程是什么原因？

A：检测每个主机都会单独起一个 Checkhost.exe 进程，检测完毕会自动退出。并发主机数量可以通过图形界面的设置窗口设定，命令行程序通过“-t”参数设定。

3) Q：扫描过程中机器突然蓝屏重启是什么原因？

A：扫描过程中系统蓝屏是有可能的，AtGuard、天网等防火墙的驱动程序在处理特殊包的时候有可能出错导致系统崩溃，另外很多防火墙驱动与 WinPCap 驱动本身也存在冲突，建议先禁止或卸载防火墙程序再试试

4) Q：操作系统识别不正确是什么原因？

A：操作系统识别方面确实不能保证 100%的准确率，目前是综合 NMAP、P0F 的指纹库、NETBIOS 信息和 SNMP 信息进行识别，如果目标机器没有开放 NETBIOS 和 SNMP 协议，TCP/IP 堆栈指纹也不在数据库中，就需要使用者根据其他信息综合分析了。

5) Q：为什么在一次扫描中我选择了“SYN”方式进行端口扫描，但 X-Scan 实际采用的是“TCP”方式，而且也没有被动识别出目标操作系统？

A：端口扫描中的“SYN”方式在 NT4 或 XP+SP2 系统下无法使用，在 windows 2000 等系统下使用时必须拥有管理员权限，否则将自动改用“TCP”方式进行端口扫描。

6) Q：新版本是否兼容 2.3 版本的插件？

A：X-Scan 3.0 以上版本的插件接口做了少量修改，不兼容 2.3 以前版本的插件，需要原作者做相应修改。3.0 以上版本提供了简单的开发库，插件开发方面要比 2.3 版本轻松许多。

7) Q：我看到 Scripts 目录下有很多 nessus 的脚本，是否可以自己从 nessus 的网站上下载最新的 plugin，然后解压到 scripts 目录中，实现扫描最新漏洞？

A：X-Scan 移植了 nessus 的 nasl 引擎，目前对应于 nessus2.2.4，但不包含对本地检测脚本的支持。所以只要是这个版本 nessus 支持的非本地检测脚本，都可以复制到 Scripts 目录下加载。

8) Q：X-Scan 中各项弱口令插件检测范围都很有限，能否自己加入其他需要检测的帐号或口令？

A：在“X-Scan”中内置的密码字典仅为简单示范，使用者如果希望软件有更强的密码猜解能力，可以自己编辑密码字典文件。

9) Q：为什么 nasl 脚本扫描结果中存在大量英文，将来有没有可能会对这些英文信息进行汉化？

A：目前已有将近 2000 个 NASL 脚本，里面的描述信息大都是英文，需要翻译的内容可以在本站“焦点项目”中的 X-Scan 下看到。欢迎大家一起帮忙翻译，通过审核后会直接加入在线升级库供大家下载。

10) Q：用 xscan.exe 在命令行方式下进行扫描时，如何暂停或终止扫描？

A：命令行方式检测过程中，按“[空格]”键可查看各线程状态及扫描进度，按“[回车]”可暂停或继续扫描，按“q”键可保存当前数据后提前退出程序，按“<ctrl+c>”强行关闭程序。

11) Q：X-Scan 如何安装，是否需要注册？

A：X-Scan 是完全免费软件，无需注册，无需安装(解压缩即可运行，自动安装 WinPCap 驱动)。