企业网络安全维护案例精粹

曹鹏 编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

企业网络安全维护案例精粹

企业网络安全维护案例精粹

曹　鹏　编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书来自作者的实际工作经验积累，所有章节都由现场精彩案例积累而成，涉及当前经常困扰企业安全管理员的常见问题。本书一开始就从真正的黑客攻击讲起，首先带领读者尝试站在一个攻击者的角度看待系统的脆弱性，体会一个攻击者的攻击思路，为全书的安全防护技巧打下基础。然后从前门攻击、后门攻击、非直接攻击与网络设备的安全隐患全面介绍当前网络攻击者的攻击方式，此外，还介绍了企业环境内安全漏洞的评估方法、入侵与入侵检测系统分析、日志分析、压力测试与性能测试等内容。

本书适合网络安全技术爱好者、企事业单位的网络管理维护人员阅读，也可作为网络工程师、高等院校相关专业师生的学习参考用书。

图书在版编目（CIP）数据

企业网络安全维护案例精粹 / 曹鹏编著. —北京：电子工业出版社，2008.7
ISBN 978-7-121-06964-2

Ⅰ. 企… Ⅱ. 曹… Ⅲ. 企业－计算机网络－安全技术 Ⅳ. TP393.180.8

中国版本图书馆 CIP 数据核字（2008）第 091495 号

策划编辑：高买花
责任编辑：侯丽平
印　　刷：北京市海淀区四季青印刷厂
装　　订：三河市万和装订厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×1 092　1/16　印张：21.75　字数：556.8 千字
印　　次：2008 年 7 月第 1 次印刷
印　　数：4000 册　定价：48.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。
质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。
服务热线：（010）88258888。

前　言

本书来自作者多年的实际工作经验积累，所有的章节都由一个个多年的现场精彩案例积累而成。本书的主要内容是解决当前经常困扰企业安全管理员的常见问题。希望所有阅读过本书的人可以学习并掌握高效率解决这些问题的能力，在解决问题的同时再通过本书系统地提升企业安全防护能力，这是编写本书的初衷。

本书一开始就从真正的黑客攻击讲起，首先带领读者尝试站在一个攻击者的角度去看待系统的脆弱性，体会一个攻击者的攻击思路，这对于后面章节的展开非常重要，也为全书的安全防护技巧打下了基础。

第 1 章至第 3 章从前门攻击、后门攻击、非直接攻击与网络设备的安全隐患全面介绍当前网络攻击者的攻击方式。

第 4 章和第 5 章为读者介绍企业环境内安全漏洞的评估方法与相关工具，同时在工具自动发现漏洞之外，利用真正的专家思路去评估发现问题。通过阅读此两章，读者不仅可以学会如何使用工具，更能掌握一种通用的方法，只有在实际的网络应用环境中，才可以真正开展弱点评估。

第 6 章的入侵者与入侵检测，详细介绍了什么是入侵，入侵者更喜欢入侵哪些系统，以及如何利用入侵检测系统发现攻击者，如何在大量的日志信息中进行更好的配置，发挥入侵检测系统的所有潜力。

第 7 章的日志分析主要写给众多服务器管理员，涉及服务器被黑、异常访问流量、SQL 语句注射攻击等一系列实际案例。阅读本章的读者会发现，其实从日志的脚印分析中就能使以往感觉高深莫测的攻击者原形毕露。

第 8 章将分析思路转移到压力测试与性能测试。压力测试与性能测试对于日常的网络瓶颈查找和必要的工作测试都是非常重要的，虽然没有专业的硬件测试工具的支持，但读者同样可以在本章看到很多精彩的案例分析。

第 9 章和第 10 章又将话题聚焦到信息安全的古老话题——“加密”，首先重点介绍了当前一些主流的服务器加密配置方法与相关加密工具的使用，然后又从无线网络的加密脆弱性开始，将 SSL 和哈希加密算法的常见攻击破坏思路进行了介绍，这是有攻有防的精彩两章。读者会发现在信息安全体系中没有永远坚固的壁垒，很多加密方式坚持到最后都难逃被破解的命运。

最后，第 11 章和第 12 章以应急响应工具箱介绍与常见 PDCERF 方法学作为收尾，介绍了很多日常需随身携带的工具箱软件，尤其是本地系统分析与 Sniffer 网络分析两类软件更是汇聚了多年来的很多实际问题处理案例经验。最后三个实际的应急处理的小故事为读者未来处理类似事件树立了信心，其实攻击者不可怕，只要我们认真分析。

本书的所有章节都尽量去回避那些高深的理论体系与枯燥知识，毕竟理论知识的获取途径实在是太多了。我们力图将所有章节都聚焦在真正解决问题的方法与工具上，贯穿始终的

是这几年在工作中实际碰到的案例分析，正是因为这些案例的启发和触动才有了这本书写作下去的动力，随着未来我们在信息安全道路上的不断探索与追求，相信此书永远都是处于更新状态的精彩书稿。

本书适合网络安全技术爱好者、企事业单位的网络管理维护人员阅读，也可作为网络工程师、高等院校相关专业师生的学习参考用书。

限于作者的水平，书中不当甚至错误之处在所难免，诚恳期待广大读者提出宝贵意见。

编 著 者

2008 年 4 月

目　录

第1章　隐蔽的非直接攻击

今天的信息安全技术已不再简单地停留在理论探讨的层面，网络中无所不在的攻击者随时可能出现，真正掌握信息安全技术操作非常关键。本书的重点是介绍一种真正可以操作的日常信息安全管理技术。信息安全风险包含的范围很大，本书仅仅是探讨由于攻击者出现所带来的实际威胁和服务器的安全弱点，让我们从了解攻击和攻击者开始本书的内容吧。

攻击的分类在不同的安全标准和安全专家的解释中都是不大相同的，对于一些专门研究攻击方法的组织来说可能细化到 10 多个种类。本着将复杂的事情尽量简单化的原则，我们将攻击的种类分成了 3 类：即非直接攻击、前门攻击和后门攻击，这种分类方法简单可行并且容易理解和记忆。

1.1　目标服务信息收集（踩点）

很多时候收集被攻击目标的各种信息是攻击者开始一次攻击的第一个步骤，把它放在非直接攻击来讲是因为我们很难分清正常访问和攻击者踩点访问的区别，他们都是通过正常的开放端口进来访问，只不过获取的信息不同而已。当一个攻击者确定了一个攻击目标主机后第一步做的就是对目标主机进行一次详细的信息收集，扫描工具是必不可少的，但如果仅仅依靠扫描工具的可怜的报告来判断我们的目标存在什么漏洞是非常不可信的。到目前为止，还没看到哪款软件可以产生完全让人满意和信服的报告结果。显然，真正的攻击者也早就意识到了这一点，下面介绍手动的信息收集步骤，希望可以对读者有所帮助。

1.1.1　小心域名服务解析你的站点结构

通过 DNS 查询得到目标的网络拓扑基本情况，目前很多主机的 DNS 服务器配置得并不安全，用 ls 命令就可以泄露出自己的内部网络结构，得到这些信息可以方便我们摸清对方网络的组成情况。

下面是利用 nslookup 命令来查询网站 www.isfocus.net 的过程。

```
C:\>nslookup
Default Server:  dns0.interway.com.cn
Address:  192.168.153.250

> www.isfocus.net      （这里是要查询的地址）
Server:  dns0.interway.com.cn
Address:  192.168.153.250

Non-authoritative answer:
```

```
Name:    www.isfocus.net
Address:  192.168.4.12

> set q=all
> server isfocus.net
DNS request timed out.
timeout was 2 seconds.
Default Server:  isfocus.net
Address:  192.168.4.12
> server www.isfocus.net
Default Server:  www.isfocus.net
Address:  192.168.4.12

> ls isfocus.net
[www.isfocus.net]
 isfocus.net.          NS    server = ns1.cnmay.com   （一个很有用的结果，下一步会用到）
 isfocus.net.          A     192.168.4.12
 mail                  A     192.168.4.32
 www                   A     192.168.4.12
> server ns1.cnmay.com   （这里用到了刚才的查询结果）
Default Server:  ns1.cnmay.com
Address:  192.168.4.32

> ls cnmay.com
[ns1.cnmay.com]
 cnmay.com.            NS    server = ns1.cnmay.com
 cnmay.com.            A     192.168.4.10
 admin12               A     192.168.4.12
 mayu                  A     192.168.4.12
 dns2                  A     192.168.4.10
 firstdir              A     192.168.4.12
 dns                   A     192.168.4.32
 oicq                  A     192.168.4.12
 agent                 A     192.168.4.11
 photo                 A     192.104.4.12
 mail                  A     192.168.4.32
 test                  A     192.168.4.12   （这是一个引起注意的二级域名）
 www                   A     192.168.4.10
 rabjin                A     192.168.4.10
 ns1                   A     192.168.4.32
```

上面首先查询了站点 www.isfocus.net，然后根据得到的地址 ns1.cnmay.com 来进行下一步的查询，很简单而且很方便地就摸清了所用的主机 ns1.cnmay.com 的整个网络分布的大概情况。尤其是当发现存在一个 test 的名称时，我们很快就想到这应该是一个在当初网站测试的时候临时建立的一个用户名。既然是临时建立的用户名，它的密码应该也不会过于复杂，所以我们尝试用 FTP 的方式登录，结果运气非常好，用 test/test 同样的用户名和口令就进去了，而且还拥有一个可以执行的 PHP 的 Web 空间，上传一个 Web Shell 就轻松地获取到了服务器的权限。这个结果对于下一步入侵整个网络来说是非常有用的资料。

1.1.2　无声息的路由追踪

Traceroute 用于路由追踪，如判断从你的主机到目标主机经过哪些路由器、跳计数、响应时间如何、是否有路由器当掉等。大多数操作系统，包括 UNIX、Novell 和 Windows NT，若配置了 TCP/IP 协议的话都会有自己版本的 traceroute 程序。使用 traceroute，可以推测出网络的物理布局，包括该网络连接 Internet 所使用的路由器。traceroute 还可以判断出响应较慢的节点和数据包在路由过程中的跳计数。利用 Tracert 命令可以查看与目标主机之间的网络结构，简单地说就是看看数据包都经过了哪些路径走到目标主机的，这样可以很方便地确定目标主机的上层路由器和网络接入设备。以现在的网络设备来说，很多都是 CISCO 的东西。现在国内的 CISCO 都有配置问题，所以说不定哪个就可以被你利用，成为进入目标主机的最后一个跳板。当然还有一个可怕的地方就是控制一个边界路由器，如果有人想做些破坏的话，危害和后果简直是不可想象的。

图 1.1 是在本地计算机测试的“tracert　61.141.197.150”的结果，如果按照这些地址去层层追查应该也会有些收获的。

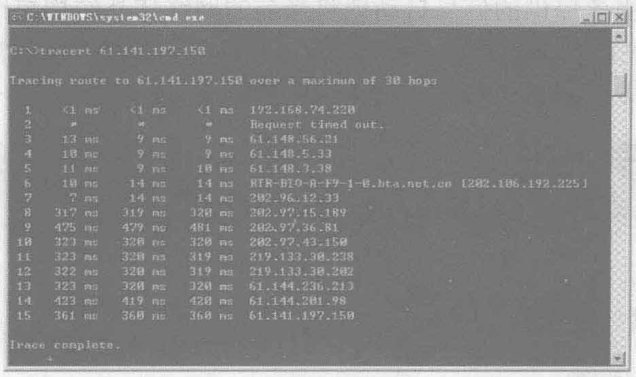

图 1.1

1.1.3　SNMP 服务可以透露多少小秘密

收集服务器和网络信息最有用的获取手段就是利用 SNMP 服务的信息收集了。在 Windows 下 SNMP 简单网络管理这个组件默认是没有安装的，但实际中还是有很多人配置不当或是网络管理的需要而将这个组件安装上了，而且在默认情况下的团体字就是 Public。这样用 SNMP 协议我们可以很方便地得到对方主机的很多有用信息，SNMP 利用 UDP 协议中的

161、162 两个端口来传输数据。扫描 SNMP 的工具其实很多，但能把 SNMP 中的信息全部都挖出来的就不多了。很多漏洞扫描软件仅仅就是报告 SNMP 里面的团体字简单而已，并没有进行很详细的信息收集工作。这里用 SolarWinds 这个专业的网络管理工具来帮助我们做个实验。

图 1.2 是 SolarWinds 中的 IP Network Browser 启动界面，填入我们需要探测的 IP 地址或一个 IP 地址范围。

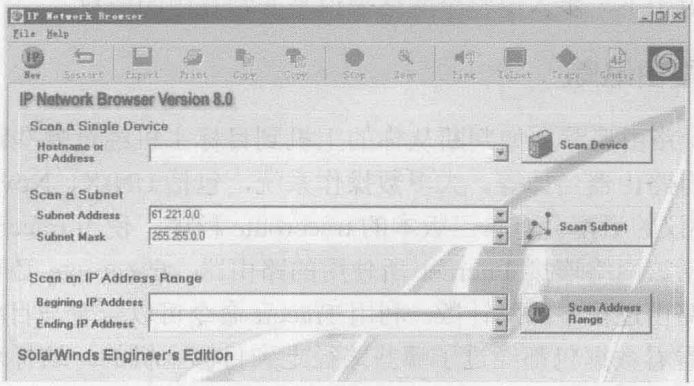

图 1.2

对于开放了 SNMP 协议的主机的所有当前网络状况都可以轻松通过 SNMP 来查询得到满意的结果，这并不是夸张的说法。图 1.3 是 IP Network Browser 的扫描分析结果，读者可以很轻松地看到目标当前开放的端口，以及主机和远程地址的连接状态等等。对于网络设备来说，开放 SNMP 服务还有更危险的地方——可能会泄露自己整个网络的拓扑结构，很多软件可以在网络中依靠 SNMP 服务提供的信息自动地将当前的网络拓扑结构描绘出来。图 1.4 是 SNMP 服务泄露的网络拓扑结构。最近很多系统的 SNMP 服务又发现了远程溢出攻击的问题，看来这项服务应该谨慎对待，如果不需要的话还是不要安装。

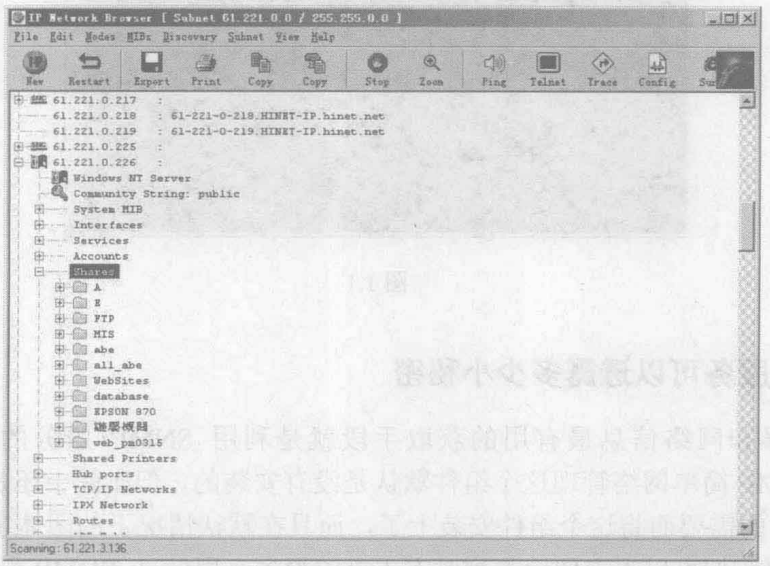

图 1.3

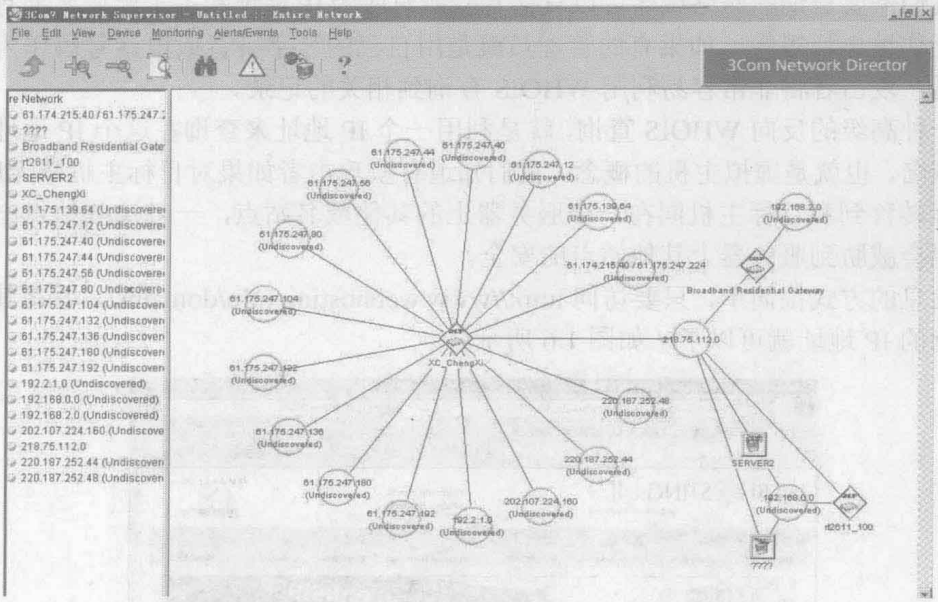

图 1.4

1.1.4　WHOIS 查询与旁注攻击

下面来看看 WHOIS 查询，它是一种 Internet 的目录服务。WHOIS 提供了在 Internet 上一台主机或某个域的所有者的信息，如管理员的姓名、通信地址、电话号码和 E-mail 地址等。这些信息是在官方网站 whois server 上注册的，保存在 InterNIC 的数据库内。WHOIS 通常用于安全审计人员了解网络的情况。一旦你得到了 WHOIS 记录，从查询的结果还可得知 primary 和 secondary 域名服务器的信息。有很多现成的 WHOIS 查询软件，如图 1.5 所示，SolarWinds 里面就集成了一款 DNS/WHOIS 查询软件，实际使用的效果非常理想。

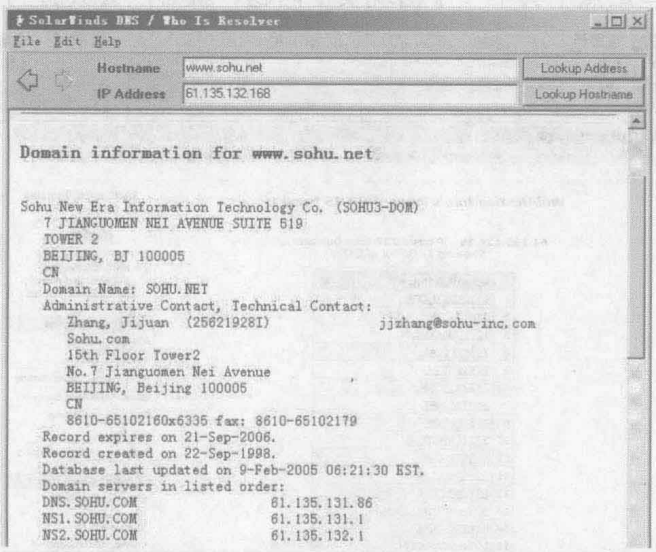

图 1.5

输入我们需要查询的网络域名可以直接看到所对应的IP地址和关于此域名拥有者的个人信息，包括住址电话等等。如果有的管理员就是用自己的名字拼音或电话号码作为自己的个人密码的话，攻击者将非常容易利用WHOIS查询到相关的记录。

还有一种高级的反向WHOIS查询，就是利用一个IP地址来查询在这个IP地址上一共存在多少个域名，也就是虚拟主机的概念。我们知道有些攻击者如果对目标主机毫无所获的话，就会把目标转移到和目标主机同在一个服务器上的其他域名站点，一旦这些站点出现安全问题，肯定也会威胁到服务器上其他站点的安全。

获取信息的方式很简单，只要访问http://www.webhosting.info/domains/，并在其中输入我们希望查询的IP地址就可以了，如图1.6所示。

图1.6

图1.7是whois.webhosting.info的查询结果，可以看到上面的IP地址中，绑定了多达237个顶级域名，如果这些站点中其中一个出现安全问题，就必然会威胁到其他站点的安全性。

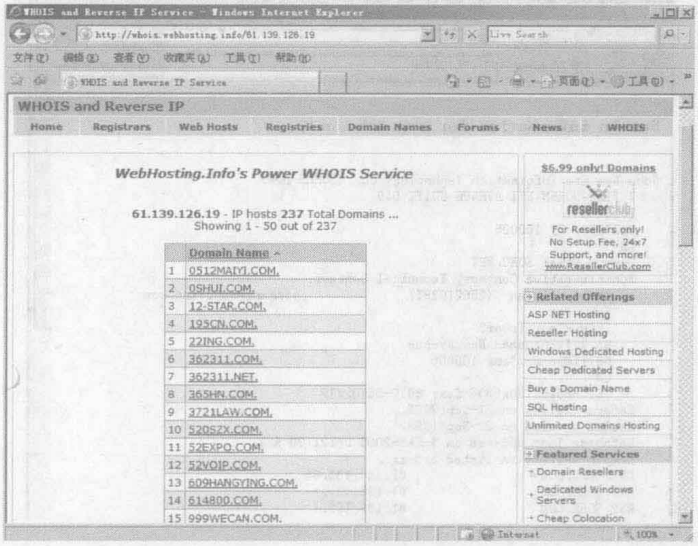

图1.7

当前有不少攻击软件已经具备自动分析一个站点域名、IP 地址后，查找绑定在同一主机下的其他域名，图 1.8 是旁注 Web 综合检测程序使用界面。

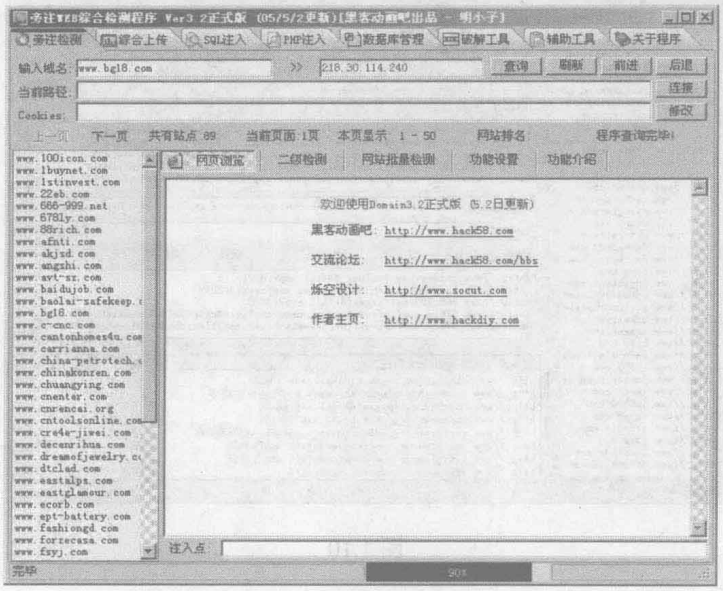

图 1.8

旁注 Web 综合检测程序自动地分析这些域名里面的 ASP 脚本程序，找到有可能有问题的、具有用户输入参数的脚本，如图 1.9 所示。

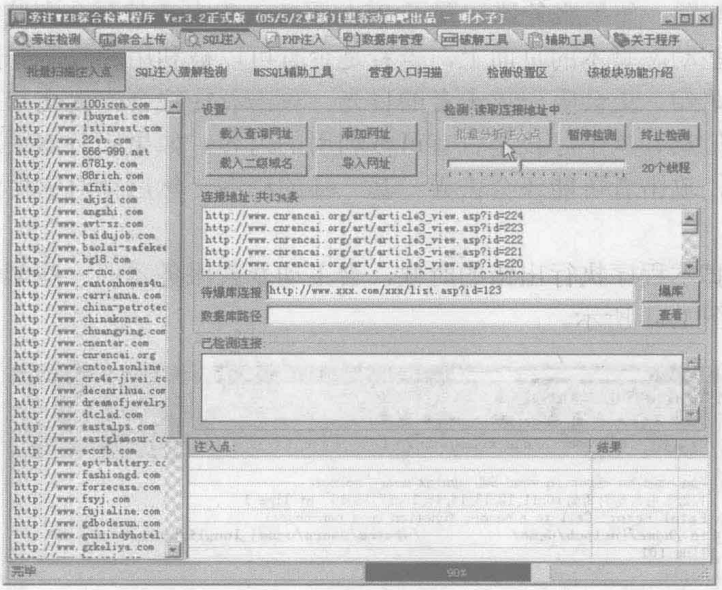

图 1.9

如图 1.10 所示，发现问题后，攻击者就可以利用这些有问题的站点进行所谓的“旁注”攻击，即从一个不安全的 Web 站点首先进行攻击取得一个 Web Shell，然后利用这个 Shell 再进一步地获取权限去攻击同一主机的其他站点。