网络安全实用丛书

网络安全防范手册

朱建军　熊　兵　著

人 民 邮 电 出 版 社
北　　京

图书在版编目（CIP）数据

网络安全防范手册/朱建军，熊兵著.—北京：人民邮电出版社，2007.7
（网络安全实用丛书）
ISBN 978-7-115-16072-0

Ⅰ. 网… Ⅱ. ①朱… ②熊… Ⅲ. 计算机网络—安全技术 Ⅳ. TP393.08

中国版本图书馆 CIP **数据核字（**2007**）第** 048667 **号**

内 容 提 要

本书通过对计算机接入互联网方式的分析，揭示在各种接入方式下可能存在的黑客入侵的途径；然后通过对网络安全生态圈中的各个组织的目的和行为进行深入的探讨，以透视和剖析各种黑客、黑客组织和安全组织与计算机网络安全的关系以及对网络安全产生的影响；站在黑客的思维视角对网络安全防护产品在什么情况下可以防御黑客的入侵，在什么情况下不能防御黑客入侵进行解析；在深入分析各种安全漏洞的成因和原理的基础上，给出了各种类型漏洞的防御方法；以故事的方式生动地向读者讲述了各种防范黑客入侵的方法和防御措施，具有新意，增加了阅读的趣味；详细阐述了黑客入侵过程的骗术；对木马病毒程序的原理、检测和清除方法进行了详细的描述。通过一些事实向读者证明了计算机网络的脆弱性后，向读者介绍了网络安全的最后一道防线——数据和文件加密。最后为了向读者揭示开放式网络连接的不安全性，具体讲解了一个网络数据包窃听和还原的实例。

通过阅读本书，读者可以增强自身的上网安全方面的意识，学习到一些防御黑客入侵的方法以及检测和清除木马程序的技术。本书适合广大的网络用户、网络技术爱好者阅读。本书可作为信息网络安全工程师、网络管理员的工作参考手册；同时也可供大专院校信息或网络安全、通信、网络、计算机等信息类专业的师生阅读使用。

网络安全实用丛书

网络安全防范手册

- **著　　朱建军　熊　兵**
  责任编辑　刘　洋
- **人民邮电出版社出版发行　　北京市崇文区夕照寺街** 14 **号**
  邮编 100061　**电子函件** 315@ptpress.com.cn
  网址 http://www.ptpress.com.cn
  北京隆昌伟业印刷有限公司印刷
  新华书店总店北京发行所经销
- **开本：**787×1092 1/16
  印张：18
  字数：438 **千字**　　2007 **年** 7 **月第** 1 **版**
  印数：1 – 4 000 **册**　　2007 **年** 7 **月北京第** 1 **次印刷**

ISBN 978-7-115-16072-0/TN

定价：34.00 **元**

读者服务热线：(010)67129258　印装质量热线：(010)67129223

自 序

Foreword

在我从事网络渗透和网络安全方面的研究过程中，针对接入互联网的计算机做过一些利用漏洞入侵、用木马病毒程序远程控制及窃取用户的输入信息、防范黑客利用漏洞和木马病毒程序的入侵以及中木马病毒后的清除等等实验。在这些实验的过程中，我发现很多被作为实验对象的计算机网络的使用者对计算机网络安全方面的知识掌握得还是很少，安全意识也很淡薄。我想这也是造成国内安全入侵事件频繁发生的一个重要的原因。

应一些高校和 IT 企业的邀请，我曾经做过一些关于计算机网络安全攻防的演讲和计算机网络安全方面的培训。在作这些演讲和培训的过程中，我经常被一些高校大学生和 IT 企业的计算机网络技术人员问到：“黑客到底是用什么方法入侵互联网上的机器的？他们又是如何远程控制互联网上的计算机的？木马病毒到底是怎么回事？杀毒软件为什么有时候杀不了计算机病毒？”等等一些问题。在多次被问及这些问题后，我就想，何不把我所讲的一些知识和对这些问题的解答补充完善后写成一本书，让更多的人通过这本书了解和学习到这些信息和知识，以便更好地防御黑客利用各种漏洞对接入互联网的计算机的入侵和破坏，使我们的广大计算机使用者能通过自身对计算机网络安全方面知识的学习相对安全地使用计算机网络来工作和生活。

在我写这本书的过程中，得到了很多老师、同学和朋友的支持，他们给了我很多非常好的建议和帮助。特别是要向华中科技大学计算机学院网络安全与应用研究室的陈晓苏导师和肖道举老师致以诚挚的谢意，感谢他们一直以来在工作、生活和学习上给予我的帮助。

另外，我也需要向人民邮电出版社的刘洋编辑道一声衷心的感谢。在我和刘洋编辑接触出版这本书的过程中，我感受到了刘洋编辑对工作的责任心和对作者的热心。我相信有这样好的责任编辑的出版社，一定可以为广大的读者奉献出一本本的精品书籍。

由于时间仓促，本人水平有限，书中难免存在一些错误和遗漏之处，恳请读者批评指正，同时也希望读者朋友给我来信交流和探讨计算机网络攻防方面的问题。

朱建军　2007 年 3 月于喻园

Zjj258@126.com

Zjj256@hotmail.com

前 言

Preface

第一次互联网络泡沫破灭后，互联网产业正逐渐地向务实和有序的方向发展，正在回归互联网建立的初衷——方便人们的沟通，缩短人与人之间的距离；很多与互联网相关的法律和规则也正在修订和完善中。目前互联网络已经成为人们交流和沟通的必备工具，而且很多人也正在通过互联网创立自己的事业，比如说现在很多个人在网络上开设网店出售各种各样的商品。网民不用出门忍受拥挤的交通和污浊的空气以及承受潜在的各种安全威胁就可以在网上悠闲地选购自己需要和喜爱的商品，同时还可以节省大量的时间和金钱。

但是，在我们享受这些便利的同时，也面临着来自于网络黑客的威胁。在现实的网络生活中，已经有大量这样的案件发生。如：2005 年发生的湖南 3 名黑客盗窃他人网银资金 10 余万元。2005 年 1 月 21 日发生的廖某、林某等 4 名犯罪嫌疑人利用木马程序盗取了南宁市市民陆某的网上银行账户及密码，28 日，4 人通过网上银行将陆某的 21400 元存款全部转出并进行分配。除了这些网络安全事件外，还经常会有一些网民的 QQ 号、网游账号、E-mail 信箱密码等被盗的事件发生。

现在当我们畅游互联网的时候，是不是会担心突然哪一天我们的淘宝网店的密码被人窃取，我们苦心经营了很长时间的网店被破坏，或者突然有一天我们网上银行的资金被人侵吞一空。由此可见，网络安全已经严重到了快要阻碍互联网健康发展的程度。

一直以来，很多计算机网络安全防护方面的书籍都是片面地向读者介绍一些纯技术和方法方面的知识，没有深入地考虑计算机网络攻防的因缘以及计算机网络攻防人员圈子与计算机网络攻防之间的一些微妙的关系，本书对这方面的的问题做了一些尝试性的探讨，引导读者来思索这样的问题，是先有攻还是先有防，他们之间又是一个怎样的相互作用和利益渗透的关系，这些问题对互联网用户安全使用接入互联网的计算机又会造成什么样的影响等等。从计算机网络攻防的发展历程来看，一直是攻击技术在推进计算机网络安全的防护技术，大多数是攻击事件发生后才会引起人们对计算机网络安全防护问题的重视，才会引发人们来研究计算机安全防护机制和计算机安全防护技术。以上的论述向我们证明，计算机网络攻击技术实际上一直是走在计算机网络安全防护技术的前面的。所以计算机网络安全防护的核心应该是预先研究黑客最新的攻击方法和动向，才能把握先机做好计算机网络安全防护。

总结上面的观点，黑客之所以能入侵我们的机器，是因为我们了解和认识的计算机网络安全方面的知识与黑客了解和认识的计算机网络安全方面的知识不对称。也就是说，黑客知道了我们不知道的计算机网络和计算机系统的漏洞以及利用网络和系统漏洞攻击的方法，我

们就有可能被黑客侵入我们的计算机网络和计算机系统。所以我们要防御黑客的入侵，就要在网络攻防方面取得与黑客相对称的知识。

最后需要说明的是，本书不是一本教读者如何去攻击他人计算机的书籍，它的目的是以故事的方式介绍和讲述一些防御入侵的实例，让读者切身体会黑客是通过什么样的途径入侵互联网上的计算机的，在了解这些知识后，读者可以获得一些对应的预防黑客入侵自己的计算机的知识和经验。

作者

2007 年 3 月

目 录

■CO N TEN TS

第 1 章

黑客是怎样侵入你的机器的

CHAPTER 1

某一天，当我们回到家里，突然发现家被盗贼入侵了，我们的第一反应就是迅速向公安机关报告案情，然后清点哪些财物失窃。剩下来能做的事情恐怕就是等待着警察能抓到盗贼，以尽可能多地挽回损失。然后呢？我们是不是该反省一下：盗贼是怎么进入我们的家中的，是利用什么样的住宅安全防范上的漏洞的，住宅的安全防范措施存在哪些问题，应该进行哪些安全补救措施以防止盗贼的再次入侵？亡羊补牢，为时未晚，当这样的事情发生在我们身上后，这一系列问题就是我们应该思考的了。

同样地，当哪天我们遇上了某一起计算机网络安全事故，发现计算机被黑客植入了木马程序而导致我们的网上银行的资金被黑客窃取了后，我们所能想到的恐怕就是怎么样赶快把木马程序从机器里清除出去。如果造成了巨大的经济损失或其他的很大的不良影响，我们也只能求助负责处理网络入侵事件的网络警察，希望他们能通过一些技术手段抓获犯案的黑客以挽回我们的经济损失和不良影响。但我们有没有想过：我们的计算机是怎么被黑客入侵的呢，黑客采用的是什么样的攻击手段，我们可以做些什么工作来防范黑客的再次入侵呢？

要防御黑客入侵我们的计算机系统，我们首先必须了解清楚黑客要入侵我们的计算机该怎么做。首先我们得了解一些常用的计算机接入互联网的方式和网络结构，然后进一步了解在这些计算机接入互联网的方式下黑客可以用什么样的方法和通过什么样的途径入侵网络用户的计算机系统，这些入侵方法各自走的什么样的网络路径。了解黑客入侵的路径对我们有效地预防黑客的入侵是非常有帮助的，在了解清楚黑客的入侵路径后，我们可以在源头上消除黑客对计算机系统构成的威胁。

在我们了解清楚一般的接入互联网的方式后，我们将在后面的章节中对当前黑客的主要入侵途径做一些详细的分析，帮助读者清楚地认识到通过不同的接入互联网的方式各自存在着哪些威胁和风险，以便读者能够针对这些威胁和风险采取一些有效的预防和防御措施，避免黑客对互联网用户的计算机系统的入侵和破坏。

1.1 接入互联网的方式与网络安全之间关系的分析

计算机用户接入互联网主要有 4 种方式（在这我们将忽略非主流的互联网接入方式），

第一种接入互联网方式是家庭用户在家中采用单台计算机的网络适配器（通常称为网卡）通过双绞线连接 ADSL 调制解调器接入互联网，这种接入互联网的方式一般需要采用一个虚拟的拨号软件。采用这种方式接入互联网的过程是：当计算机用户需要连接互联网的时候，先启动或运行一个虚拟拨号软件，然后在虚拟拨号软件上填入网络连接服务商提供的上网账号和密码，然后开始拨号接入互联网。图 1-1 为家庭用户接入互联网的网络拓扑图。

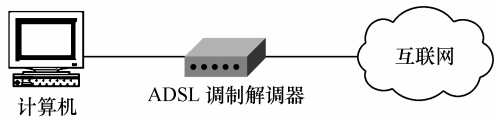

图 1-1　家庭用户接入互联网方式

在这种接入方式中，联网计算机首先以本地网络 IP（Internet Protocol）地址将数据通过本机网络适配器（网卡）以 PPPoE 协议（PPP over Ethernet，以太网点对点协议）发送给 ADSL 调制解调器与计算机连接的本地网络接口，然后再由 ADSL 调制解调器通过连接 WAN（Wide Area Network）的端口发送给计算机网络用户要访问的远程目标主机。远程的计算机要访问我们的计算机，首先要通过 WAN 把数据发到 ADSL 调制解调器，然后再由 ADSL 调制解调器通过 PPPoE 协议发给我们的个人计算机系统。下面为了向读者进一步说明在这种接入方式下进出数据包的情况，先来看一个 PPPoE 协议连接的详细过程。

PPPoE 协议建立一个以太网上点对点协议会话包括两个阶段。

1．发现（Discovery）阶段

在发现过程中，拨号上网用户主机以广播方式寻找可以连接的所有接入设备，获得其以太网 MAC 地址，然后选择需要连接的用户主机并最后获得所要建立的 PPP 会话的 SESSION_ID。在发现过程中，节点间是客户机/服务器关系，一个用户主机（客户机）最终要发现一个接入设备（服务器）。在网络拓扑中，一般有不止一个的接入设备可以通信，发现阶段允许用户主机发现所有的接入设备，并从中选择一个。当发现阶段结束时， 用户主机和接入设备之间都获得了可供在以太网上建立 PPP 连接的全部信息。发现阶段保持无连接状态直到一个 PPP 会话的建立。一旦 PPP 连接建立，用户主机和接入设备都必须为 PPP 虚拟端口分配资源。

2．PPP 会话阶段

用户主机与在发现阶段确定的接入设备进行 PPP 协商，这个协商过程与标准的 PPP 协商并没有任何区别。在 PPP 会话阶段，节点间是对等关系。

典型的发现阶段共包括 4 个步骤。

（1）拨号上网用户主机发出 PPPoE 有效发现初始（PADI）包。以太网目的地址为广播地址 0xffffffff，CODE 字段为 0x09，SESSION_ID 为 0x0000。PADI 包必须至少包含一个服务名称类型（Service-Name）的标签（标签类型字段为 0x0101），向接入设备提出所要求提供的服务。一个完整的 PADI（包括 PPPoE 头）不能超过 1484 字节，以留下充足的预留给 agent 设备增加 Relay-Session-Id 标识。

（2）接入设备收到在服务范围内的 PADI 包后，发送 PPPoE 有效发现提供（PADO） 包以响应请求。其 CODE 字段为 0x07，SESSION_ID 仍为 0x0000。PADO 包必须包含一个接入设备名称类型（AC-Name）的标签（标签类型字段为 0x0102）以及一个或多个服务名称类型标签，表明可向用户主机提供的服务种类。

（3）用户主机在可能收到的多个 PADO 包中选择一个合适的接入设备，选择的原则是根据 PADO 中接入设备名称类型标签和服务名称类型标签的内容。然后向所选择的接入设备发送 PPPoE

有效发现请求（PADR）包。其 CODE 字段为 0x19，SESSION_ID 仍为 0x0000。PADR 包必须包含一个服务名称类型标签，确定向接入设备请求的服务种类。当一个用户主机在确定时间内没有收到 PADO，它会重发一个 PADI，同时等待两倍的时间。这种过程可以根据需要重复多次。

（4）接入设备收到 PADR 包后准备开始 PPP 会话，它发送一个 PPPoE 有效发现会话确认（PADS）包。其 CODE 字段为 0x65，SESSION_ID 为接入设备所产生的一个唯一的 PPPoE 会话标识号码。0xffff 作为预留资源，目前不能被使用作 SESSION_ID。PADS 包也必须包含一个服务名称类型的标签，确认向用户主机提供的服务。当用户主机收到 PADS 包确认后，双方就进入 PPP 会话阶段。如果接入设备不能识别 PADR 中的服务名称类型的标签，则会回一个包含服务名称错误（Service-Name-Error）标签的 PADS ，其 SESSION_ID 仍然是 0x0000。如果用户主机在确定时间内没收到 PADS 包，与没收到 PADO 作同样处理。

还有一种 PPPoE 有效发现终止（PADT）包，在一个 PPP 会话建立后，它随时可由用户主机或接入设备中的任何一方发送，指示 PPP 会话已终止。PADT 包不需要任何标签，其 CODE 字段为 0xa7，SESSION_ID 为需要终止的 PPP 会话的会话标识号码。

从上面的 PPPoE 协议过程中可以发现，PPPoE 协议为了实现以太网的计算机与互联网上的计算机的双向通信，对进入采用 ADSL 调制解调器拨号上网的计算机的数据包除了做了一些防御 DoS（拒绝服务）攻击的数据包外，对其他进入的数据包，都会无条件地转发给拨号接入互联网的计算机。所以对于这种接入互联网的方式，黑客的攻击数据包是可以主动进入拨号上网的那台计算机的系统的。

下面的实验也证明了在采用 ADSL 调制解调器拨号接入互联网的方式下，黑客的数据包是可以主动进入上网的计算机的系统的。

图 1-2 所示的是实验用一个端口扫描器软件以采用 ADSL 调制解调器拨号上网后网络供应商动态分配的 IP 地址对一台采用 ADSL 调制解调器拨号上网的计算机的开放端口扫描的参数设置界面，程序界面中“指定 IP 范围”下的“221.235.70.53”是拨号上网后网络供应商动态分配的一个 C 类 IP 地址（关于 IP 地址类别的相关知识，请读者参考 TCP/IP 协议方面的书籍和资料）。

接下来以刚才设置的 IP 地址对采用 ADSL 调制解调器拨号上网的计算机进行开放端口的扫描，图 1-3 显示的结果是这次扫描实验机器开放的服务端口的情况，从图中可以看出，这台采用 ADSL 调制解调器拨号上网的计算机开放了 21 端口为远程的网络访问者提供了 FTP 服务。

从上面的实验过程来看，现在有些家庭可能配备有多台计算机，或者物理距离相邻的几户邻居配备有多台计算机，一些用户为了节省上网成本，他们一般会考虑另一种家庭用户接入互联网的方法。第二种接入互联网方式的网络拓扑图如图 1-4 所示。

从图 1-4 可以看出，实际上，家庭用户的多台计算机组成了一个小型的局域网，然后使用一个小路由器通过 ADSL 调制解调器拨号接入互联网，这种接入互联网的方式与第一种接入互联网的方式不同之处在于，拨号上网的任务是由一台有一个外网网口和多个内网网口的小路由器来完成的。在这种接入互联网的方式下，上网计算机发出的数据包的流程是：要上网的计算机先把数据发给小路由器，然后由小路由器发给 ADSL 调制解调器，再由调制解调器通过电话线路发给远程的互联网上的主机；进入上网计算机的数据包的流程是：互联网上的计算机通过网络供应商的电话线路把数据包发给 ADSL 调制解调器，然后调制解调器把数据包转发给小路由器，再由小路由器决定是否要把数据包转给连接小路由器的计算机系统。在这里决定是否要把主动连接进来的数据包转给连接小路由器的计算机中的哪一台，决定权

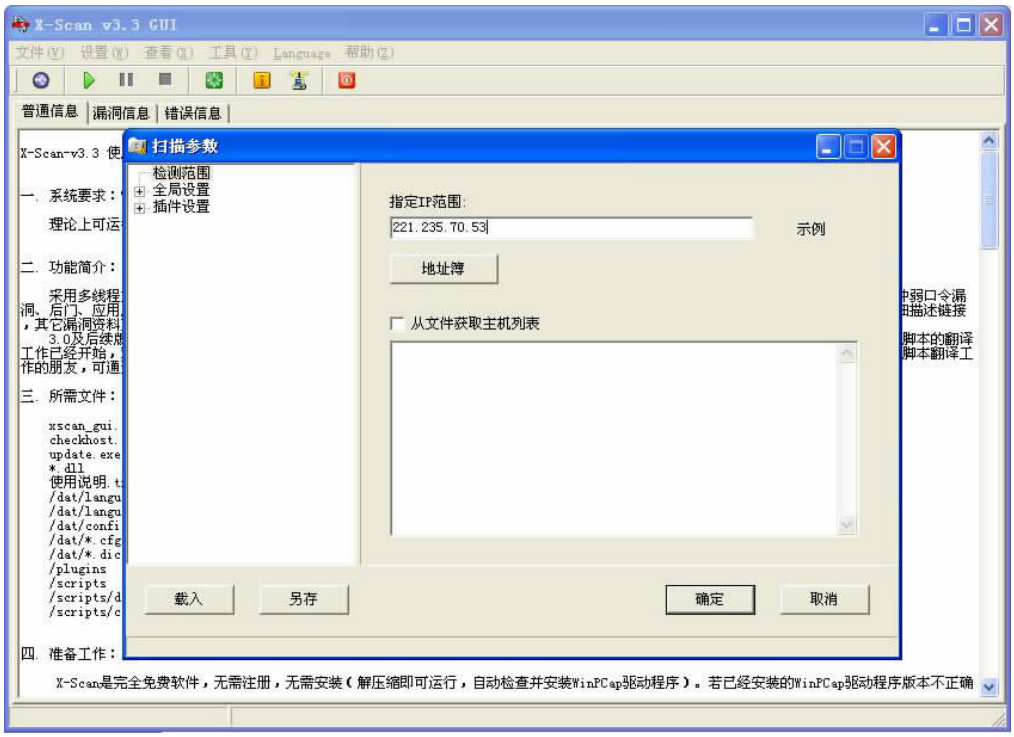

图 1-2　在扫描参数中设置用外网 IP 对拨号上网的计算机进行扫描

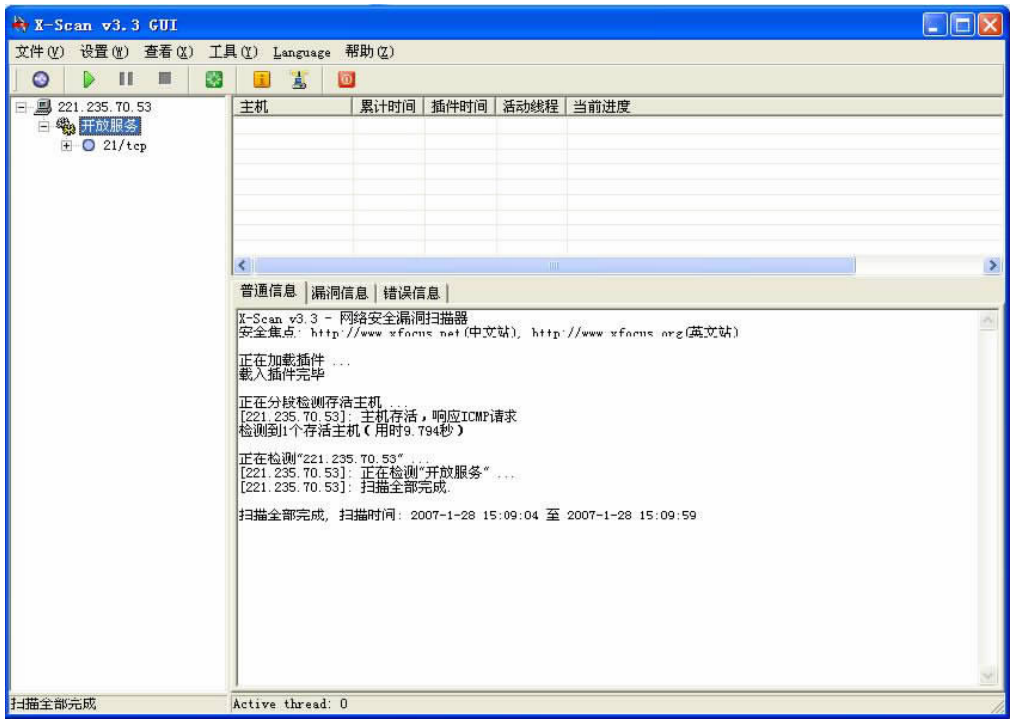

图 1-3　用外网 IP 地址对采用 ADSL 调制解调器拨号上网的计算机进行扫描的结果

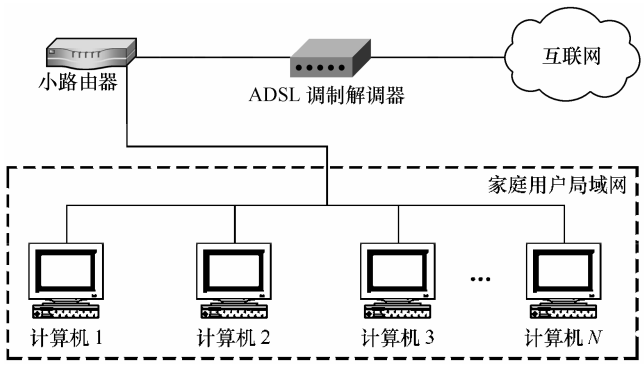

图 1-4　家庭用户多台计算机共享接入互联网的方式

在于小路由器的转发规则的设置。下面以一个转发规则的实例来说明这个问题，图 1-5 所示的是一个小路由器实际转发规则的设置情况。

图 1-5　一个小路由器的进入数据转发实例

图 1-5 所示的转发规则是由网络供应商的网络发给 ADSL 调制解调器后转发给小路由器 WAN 口的目的端口号为 80 的数据包将全部转发给连接小路由器的网络 IP 地址为“ 192.168.1.101 ”的计算机。由此可见，在这种接入互联网的方式下，黑客主动进入的攻击数据包要进入上网的计算机系统，还必须要小路由器的转发才可以成功，一般情况下，黑客主动进入的攻击数据包是很难进入采用这种方式上网的计算机系统的。

第三种接入互联网的方式是在已建成局域网的基础上，通过一台路由器再经过网络边界防火墙将局域网中的计算机接入到互联网上。一般情况下，局域网与路由器之间或路由器与互联网之间会架设一道防火墙来对传输的数据进行过滤。细心的读者可能已经发现，采用这种方式接入互联网与前面介绍的第二种接入互联网的方式很类似，只是中间多了一套专业级的防火墙设备，路由器也变成了专业级的路由器而已。这种方式接入互联网的拓扑图如图 1-6 所示。

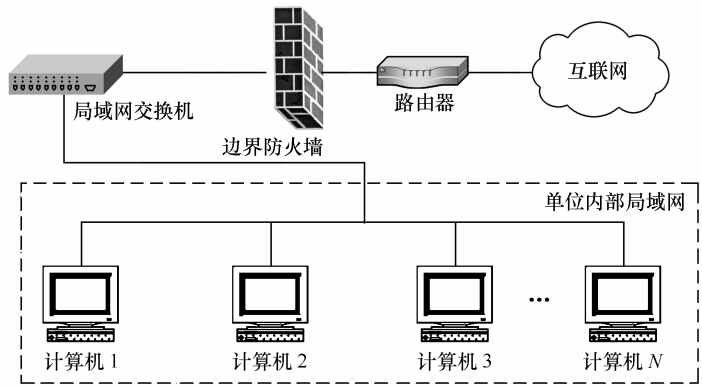

图 1-6　局域网用户接入互联网方式

在这种接入互联网的方式中，局域网内的计算机要访问互联网中的某台主机，局域网内的计算机发送的数据包要经过局域网的边界防火墙后再由防火墙转给路由器，路由器接收到内部局域网的数据包后将数据包重新封装后再通过 WAN 发送给目标主机。而远程的机器要访问局域网的机器，首先通过 WAN 把数据包发给路由器，路由器根据数据包里面的局域网 IP 地址和端口信息经过防火墙向局域网转发，但一般的网络边界防火墙的数据包过滤规则是只管进不管出，也就是说，从内部网发送到互联网的数据包一般是全部放行，而外网主动连接到防火墙内的局域网中的计算机的数据包则要经过防火墙的过滤处理后才决定是否放行。下面来说明一下从互联网进入局域网计算机系统的流：当互联网上的数据包经由路由器到达防火墙时，防火墙根据管理员制定的过滤规则对数据包做过滤处理，若需要则再发给内网的个人主机，就普遍的防火墙的过滤规则而言，除了发往防火墙允许的内网中某服务器的 Web 服务的 80 端口等服务端口放行外，其他主动进入局域网的计算机系统的数据包都是缺省被拒绝。回应内网连接的数据包则通过一种叫做状态检测的机制放行。所谓状态检测机制，是利用 TCP 三次握手的原理，TCP 三次握手的过程如下：客户端向服务器端发送一个 SYN 置位的 TCP 报文，包含客户端使用的端口号和初始序列号 x；服务器端收到客户端发送来的 SYN 报文后，向客户端发送一个 SYN 和 ACK 都置位的 TCP 报文，包含确认号为 $x+1$ 和服务器的初始序列号 y。在这个过程中，防火墙在缓存中记录内网发送出去的 SYN 置位的 TCP 报文，如果从外网进来的数据包是回应这个报文的就被防火墙允许进入，当然一个防火墙的状态检测机制还要考虑更多的问题，请读者参考相关的技术资料。对于防火墙的更详细的技术信息，请参阅防火墙方面的专门书籍。

下面来做一个对采用这种方式接入互联网的局域网内的计算机的开放端口的扫描实验，图 1-7 所示的是对一个安装了边界防火墙的接入了互联网的局域网的扫描结果。

从图 1-7 所示的程序界面中可以看出，扫描的结果是在这个用来实验的局域网内没有扫描到存活的主机，这说明被扫描的局域网在局域网的边界安装了边界防火墙，并对主动进入局域网的探测数据包做了拒绝处理。这也说明黑客在这种接入互联网的网络环境下要从外部网络主动入侵内部局域网的计算机是很困难的。但一个值得采用这种接入互联网方式的用户注意的问题是，黑客可以通过一些被动攻击的手段在成功地入侵到有边界防火墙的局域网内的一台计算机后，再用这台计算机作为跳板攻击局域网内其他的计算机，这个问题在后面的章节中有具体的实例说明，下面的实验结果是在这种安装有边界防火墙的局域网内对局域网内部分计算机进行开放的服务端口扫描的情况，图 1-8 是在局域网中的某台计算机扫描局域

网内的部分计算机开放服务端口的结果。

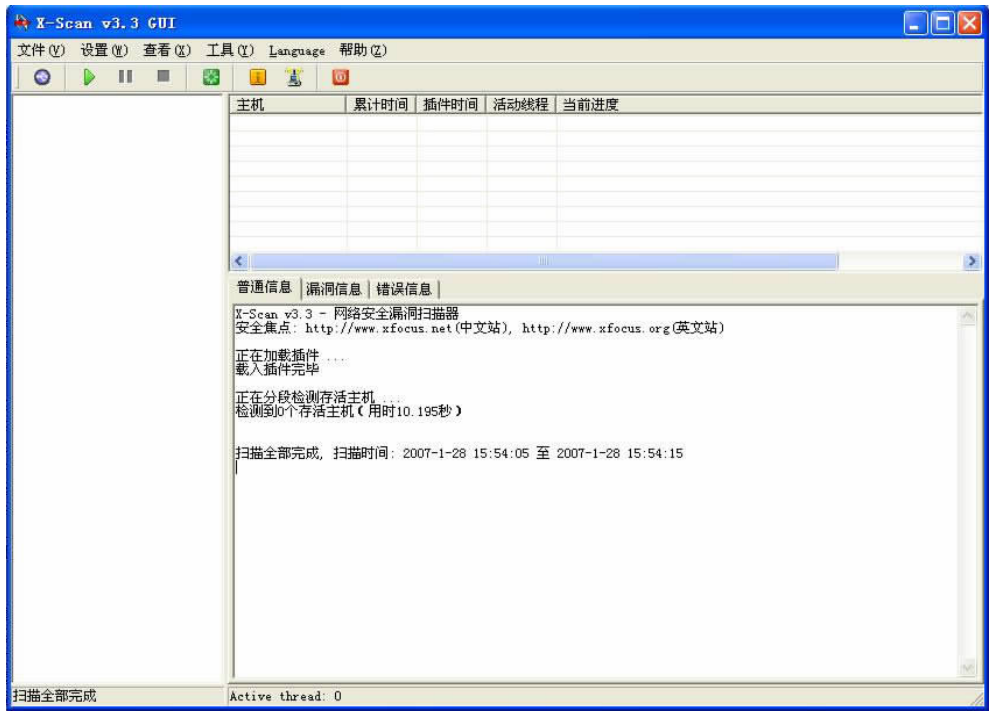

图 1-7　扫描安装了边界防火墙的接入互联网的局域网计算机的结果

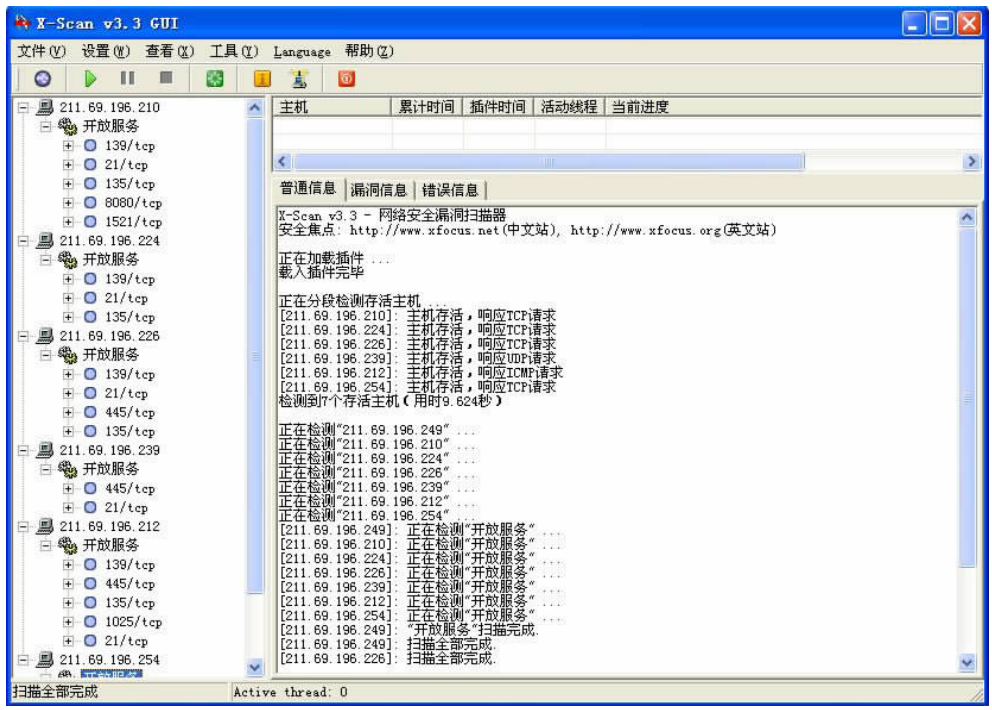

图 1-8　在局域网中的某台计算机上扫描局域网计算机的结果

从图 1-8 所示的扫描结果中可以看出，如果黑客通过局域网中的一台计算机来攻击局域网中其他的计算机，就可以绕过局域网边界防火墙对局域网的保护功能，达到攻击局域网中其他计算机的目的。这一点说明，一个边界防护能力再强的局域网，如果被黑客通过被动攻击的方式在局域网中打开了一个突破口，就有可能对整个局域网构成较大的威胁，导致边界防护系统的安全防御功能失去应有的效果。

第四种接入互联网的方式是将计算机通过交换机直接与互联网连接，在网络硬件层几乎没有任何的防御设施，网络上的数据包在没有任意管制的情况下可以自由地连接任意计算机操作系统上开放的端口。这种接入互联网方式的网络拓扑图如图 1-9 所示。

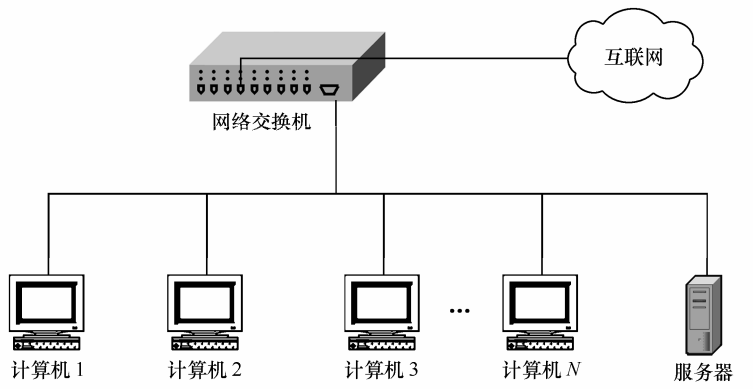

图 1-9　直接通过交换机接入互联网的联网方式

这种方式是所有联网方式中最危险的一种联网方式，因为在这种联网方式下，网络上的数据没有经过任何的过滤处理就进入了用户的计算机。因为这种接入互联网的方式的风险和威胁太高，现在基本上很少有网络用户在不安装边界防火墙的情况下通过这种方式接入互联网，但还是有一些计算机网络安全知识和计算机网络安全意识都很贫乏的用户仍然在采取这种裸露的方式接入互联网。很多黑客通过远程主动入侵可以轻易成功进入的计算机系统估计就是采用这种方式接入互联网的。

1.2　黑客进入联网计算机的途径与安全防御

黑客要入侵进入互联网上的计算机，肯定有一个进入的路径图，这些黑客进入互联网上的计算机的途径是与计算机接入互联网的方式紧密相关的。分析清楚这些黑客对互联网上的计算机的入侵途径，对于我们防御黑客的入侵具有比较重要的意义。

1.2.1　黑客的两种攻击方式与防御

在分析完互联网用户接入互联网的方式后，我们再一起来分析一下黑客在这些互联网的接入方式下实施攻击的方式。从黑客的攻击行为来看，黑客在这些接入互联网的方式下的攻击方式一般来说可以分成两种，一种是由黑客主动发起的攻击，不需要被攻击目标的任何参与和配合，另一种是黑客被动地等待用户自己来运行黑客的攻击程序或打开黑客的程序漏洞