信息科学与技术丛书

信息安全系列

● 唐正军　编著

入侵检测技术导论

机械工业出版社
CHINA MACHINE PRESS

信息科学与技术丛书
信息安全系列

入侵检测技术导论

唐正军　编著

机械工业出版社

这是一本介绍入侵检测技术的入门书籍。全书共分为 14 章，内容包括：黑客攻击主要手段以及入侵检测技术的相关问题；主要操作系统的文件系统和审计机制；基于主机的入侵检测技术知识；RPC 技术；早期著名的主机入侵检测系统 IDES/NIDES 系统；另外一种类型的主机入侵检测技术；网络入侵检测技术的基础设计知识；早期的分布式入侵检测系统 AAFID 系统。

在本书的第 12～14 章中，作者阐述了独立工作的成果。其中包括入侵检测不对称模型的引入、基于神经网络的入侵检测技术以及智能化入侵检测系统的架构设计等。

本书适用于计算机和信息安全专业的高校教师和研究生以及广大网络安全工程技术人员参考之用。

图书在版编目（CIP）数据

入侵检测技术导论/唐正军编著. －北京：机械工业出版社，2004.4
（信息科学与技术丛书信息安全系列）
ISBN 7-111-14079-6

Ⅰ. 入… Ⅱ. 唐… 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（2004）第 014419 号

机械工业出版社（北京市百万庄大街 22 号　邮政编码 100037）
策　　划：胡毓坚
责任编辑：时　静
责任印制：施　红
煤炭工业出版社印刷厂印刷·新华书店北京发行所发行
2004 年 4 月第 1 版·第 1 次印刷
787mm×1092mm　1/16·17.5 印张·434 千字
0001—5000 册
定价：27.00 元

凡购本图书，如有缺页、倒页、脱页，由本社发行部调换
本社购书热线电话（010）68993821、88379646
封面无防伪标均为盗版

出 版 说 明

随着信息科学与技术的迅速发展，人类每时每刻都会面对层出不穷的新技术、新概念。毫无疑问，在节奏越来越快的工作和生活中，人们需要通过阅读和学习大量信息丰富、具备实践指导意义的图书，来获取新知识和新技能，从而不断提高自身素质，紧跟信息化时代发展的步伐。

众所周知，在计算机硬件方面，高性价比的解决方案和新型技术的应用一直备受青睐；在软件技术方面，随着计算机软件的规模和复杂性与日俱增，软件技术受到不断挑战，人们一直在为寻求更先进的软件技术而奋斗不止。目前，计算机在社会生活中日益普及，随着因特网延伸到人类世界的层层面面，掌握计算机网络技术和理论已成为大众的文化需求。也正是由于信息科学与技术在电工、电子、通信、工业控制、智能建筑、工业产品设计与制造等专业领域中已经得到充分、广泛的应用，所以这些专业领域中的研究人员和工程技术人员将越来越迫切需要汲取自身领域信息化所带来的新理念和新方法。

针对人们对了解和掌握新知识、新技能的热切期待，以及由此促成的人们对语言简洁、内容充实、融合实践经验的图书迫切需要的现状，机械工业出版社适时推出了“信息科学与技术丛书”。这套丛书涉及计算机软件、硬件、网络、工程应用等内容，注重理论与实践相结合，内容实用，层次分明，语言流畅，是信息科学与技术领域专业人员不可或缺的图书。

现今，信息科学与技术的发展可谓一日千里，机械工业出版社欢迎从事信息技术方面工作的科研人员、工程技术人员积极参与我们的工作，为推进我国的信息化建设作出贡献。

机械工业出版社

前　言

作者在出版了早期的关于入侵检测技术的书籍之后，陆续接到许多读者的电子邮件，对写作内容提供了许多有益的意见并提出了许多问题。由于时间等因素的影响，未能完全回复所有来信，在此表示歉意。入侵检测技术在国内的发展，已经从几年前的起步阶段逐渐过渡到现在的上升发展期，技术本身也在不断完善。就作者本人而言，对技术的理解也在不断地拓展和加深，因此感到有必要在前面出版书籍的基础上重新组织写作内容，并反映技术进步的内容；同时，作者还是将本书定位于入门技术书籍上，强调写作脉络的清晰和内容介绍的基础性。希望本书的内容组织和写作方式，能够满足读者对入侵检测技术的了解需求。

入侵检测技术随着整体信息安全技术的发展而不断前行，更多的人投入到该领域内的研究工作并取得了一定的成果。更多新的理论运用到入侵检测的研究领域，同时在具体产品或系统的开发上，也取得了很大进步。但是，应该看到的是，在总体迅速发展的背景下，核心技术和创新能力的发展并不乐观。大量的系统在重复着同一水平的工作，对基础研发的投入并不充足，造成的明显现象是实际的系统性能指标距离国外先进水平尚有较大差距。作者写此书的另一个目的就是希望更多的人通过本书入门，能够在此基础上做出更多具有原创性的工作。

本书的内容共分为 5 大部分。第 1 部分包括第 1 章内容，在概要介绍黑客攻击手段类型的基础上，介绍入侵检测技术的概念、对应的安全模型、通用 CIDF 模型架构以及相关的管理评测和法律问题。这部分主要是学习入侵检测技术的基础背景知识和总体框架。第 2 部分包括第 2～6 章共 5 章内容，主要介绍了主机入侵检测技术。其中第 2、3、4 章为技术基础内容，涉及到操作系统发展及审计机制知识。第 5 章介绍了主机入侵检测系统的经典代表 IDES 系统以及后继版本 NIDES 系统，其中涉及到统计分析算法、专家系统算法和架构模块设计等知识。第 6 章介绍了基于状态转移分析技术的主机入侵检测系统 STAT，对其包含的基本算法思想和检测算法设计及系统架构设计等内容进行了论述。STAT 系统的基本思想是具有创新性的一种思路，读者通过学习，应该可以得到更多的启发。第 3 部分包括了第 7～10 章的内容，主要介绍了网络入侵检测技术。第 7、8、9 章内容提供了网络入侵检测技术的基础设计知识，包括基础协议知识、数据流截获技术和网络检测引擎的基础设计等内容。在此基础上，在第 10 章里，作者结合著名的开放源码 Snort 系统，介绍了其最新 2.0 版本引入的若干设计特色，包括快速检测引擎设计、改进 IP 重组和流重组技术等。Snort 系统作为开放源代码的学习型系统，应该说为国内入侵检测系统的启蒙设计起到了不可低估的促进作用。从 Snort 版本的不断演变过程中，如果加以较为细致的耐心分析，不难看出其中所折射出的不断追求创新的精神内涵。此时，分析代码或跟随设计架构应该不再成为尽力追求的重点，作者深切感到通过学习而发展出自己的创新核心设计，才是真正的学习精髓所在。第 4 部分包括第 11 章的内容，主要介绍了 Purdue 大学所提出的自治代理入侵检测技术及其实现原型 AAFID 系统。AAFID 系统在分布式入侵检测系统的发展历史上，起到了重要的推动作用。尽管其原型系统所采用的实现技术，并非严谨的工程实现，但是自治代理的检测理念却代表了一种新的设计思路。第 11 章内将会介绍 AAFID 系统的设计架构、代理的概念以及模块函数的功能设计等。第 5 部分包括第 12～14 章的内容，主要介绍了作者在入侵检测领域内所

作的一点工作成果。其中包括入侵检测不对称模型的引入、基于神经网络入侵检测算法的分析以及智能化入侵检测系统的设计等。

本书在成稿期间，得到了上海交通大学信息安全工程学院诸多老师的帮助和指导。信息安全工程学院常务副院长李建华教授对本书的写作多次给出中肯的意见，促进了书稿更好地完成。李生红老师担任了诸多与出版社进行沟通协调的繁琐事务，为本书的顺利出版奠定了基础。本书的写作是在作者参与国家 863 重大项目“信息安全工程实践综合实验平台与集成”的研发工作期间完成的，负责项目总协调的杨树堂老师此间给予了很多帮助，在此表示感谢。另外还要感谢作者所在的上海交大入侵检测研究小组（SJTU-IDRG）诸位成员的大力帮助，他（她）们是伍星、刘永陆、马思佳、陈一航、罗自立、陈杰、丁海波、肖惠玲等。

本书第 12～14 章的内容是在解放军第二炮兵工程学院刘代志教授的指导下，作者独立完成的工作。不妥和谬误之处，由作者本人负责。

最后，希望本书能够为入侵检测技术的普及和发展起到一定的推进作用。

唐正军

目　录

第1章 概 述

1.1 主要入侵攻击手段简介

随着人类社会生活对 Internet 需求的日益增长，网络安全逐渐成为 Internet 及各项网络服务和应用进一步发展所需解决的关键问题，尤其是从 1993 年以来，随着 Internet/Intranet 技术日趋成熟，通过 Internet 进行的各种电子商务和电子政务活动日益增多，很多组织和企业都建立了自己的内部网络并将之与 Internet 联通。这些电子商务和政务应用和企业网络中的商业秘密便是攻击者的目标。据统计，目前网络攻击手段多达数千种，使网络安全问题变得极其严峻。美国商业杂志《信息周刊》公布的一项调查报告称，黑客攻击和病毒等安全问题仅在 2000 年就造成了上万亿美元的经济损失，在全球范围内每隔数秒就发生一起网络攻击事件。随着 Internet 的发展，网络安全技术也在与网络攻击的对抗中不断发展。从总体上看，经历了从静态到动态、从被动防范到主动防范的发展过程。

1.1.1 黑客入侵的步骤

黑客们究竟为什么要入侵某一目标？一般来说黑客攻击手段可分为两类：非破坏性攻击和破坏性攻击。有一部分黑客本身就是怀着特定的目的，他们企图通过入侵某些系统盗取机密信息以获取经济上的利益；或者通过获取特殊权限使得目标系统成为自己的傀儡机，从而可以为所欲为。上述可以归纳为破坏性攻击，是以侵入他人电脑系统、盗窃系统保密信息以及破坏目标系统的数据为目的。也有些黑客仅仅是为了证明自己的能力，一般是为了扰乱系统的运行，并不盗窃系统资料，通常以目标系统为对象造成其拒绝服务或采用信息炸弹等造成意外后果，可以被认为是非破坏性攻击。一般的攻击还是偶然的因素居多，不过能够让黑客有机可乘还是有许多必然的原因，如系统本身存在一些安全漏洞或 Bug 等。

黑客通常采用以下的几个步骤来实现入侵目标主机的目的。

第一步：搜集信息，寻找目标主机并分析要攻击的环境。在 Internet 上每个 IP 地址对应惟一的主机，域名往往是为了方便记忆主机的 IP 地址而另起的名字，只要利用域名和 IP 地址就可以顺利地找到目标主机。黑客攻击的对象可能是一台主机，也可能是多台主机或一个网段，如果属于后者还要知道目标机器数目。而每一台主机都有其特殊性，因此仅仅知道要攻击目标的位置还是远远不够的，需要了解的信息还包括主机的操作系统类型及其所提供服务等资料。通常黑客在锁定目标后首先可以从该目标（网站等）公布的信息找到有用的资源，也可以利用对方提供的服务（如 Telnet）到对方主机，服务的提示信息也会泄漏目标特性。此外他们还常会使用一些扫描器工具，目前扫描工具非常强大，是黑客最有力的工具之一。通过扫描目标系统，黑客可以轻松获取目标主机运行的是哪种操作系统以及哪个版本，系统有哪些账户，WWW、FTP、Telnet 、SMTP 等服务器程序是何种版本等等资料，为入侵作好充分的准备。

第二步：实施入侵，获取账号和密码，登录主机。黑客要想入侵一台主机，首先应该获得该主机的一个账号及其密码，登录主机后再实施下一步的入侵动作。如果目标主机开放Finger 服务或 X.500 服务等，可以直接利用此类服务查询有效的账号；或者尝试各系统默认的习惯性账号，有些系统会使用弱口令甚至口令为空。如果这几条捷径都不成功，黑客往往先设法盗窃账户文件，进行破解，获取用户账号和口令，然后再以此身份登录主机。还有较常用的方法是利用网络监听技术，将以太网接口设为混杂模式截获用户所在网段的全部数据包。有许多形式的用户名与密码甚至是名文传送的，这就给黑客带来了极大的便利，使他们轻而易举就获得了入侵主机的钥匙。另一种方法是采用 IP 欺骗技术，利用主机间的信赖关系获取对目标主机的非法的访问权限。此外，利用某些工具或系统漏洞登录主机也是黑客们常用的技法。

第三步：提升权限，得到超级用户权限，上传/下载数据，并控制主机。黑客一旦获得了普通用户的账号，便可以利用 FTP、Telnet 等工具进入目标主机。在进入目标主机后，他们会想方设法获得超级用户权力，然后就可以进行任意操作。提升权限的方法一般包括下面几种类型：通过网络监听或密码破解等途径获得管理员密码，再次进入系统时就可以利用该密码了；或者新建一个用户，并将这个用户添加到管理员组使其拥有管理员权限，以后就用该账号访问目标系统；另一种方法就是安装后门或木马来保持访问；利用系统本身的漏洞获取超级用户权限也是一种常用的方法，在公布的漏洞中缓冲区溢出漏洞大约占了 70%左右，其巨大的威胁性与较高的成功率，以及使用的便利性使之成为黑客的首选。黑客首先上传具有破坏性的攻击脚本，然后利用缓冲区溢出跳转到该段代码执行攻击程序，获得控制权限。

第四步：清除日志记录，打扫战场，隐藏自己。在黑客真正控制主机后，就可以盗取甚至篡改某些敏感数据信息，同时也会更改某些系统设置、在系统中置入特洛伊木马或其他一些远程操纵程序，安插后门。入侵目的任务完成后，黑客往往还需要清除日志、删除复制的文件，以此来隐藏自己的踪迹。有些黑客可能会将所有日志文件删除，这样做虽然可以起到保护自己的作用，但是很容易被对方管理员发现本系统受到过入侵，及时作出相应的防护措施，修改密码，删除后门等等。有经验的黑客选择仅删除日志中与之相关的几条记录，当对方审查日志时不会感觉异常，因此具有更强的隐蔽性。之后，他便可以实现远程控制，更为方便地进出俘虏到的主机。

1.1.2 黑客攻击的原理和方法

1．网络监听

网络监听最初是为了协助网络管理员监测网络传输数据，排除网络故障而开发的技术，因而一直倍受网络管理员的青睐。然而，在另一方面网络监听也给以太网安全带来了极大的隐患，许多网络入侵往往都伴随着以太网内网络监听行为。当信息在网络中传播时，黑客将网络接口设置为监听模式，利用网络监听工具便可将网络中正在传播的信息截获，并利用这些信息进行攻击。通常当黑客登录网络主机并取得超级用户权限后，若要登录其他主机，使用网络监听可以有效地截获网上的数据。网络监听在网络中的任何一个位置都可实施进行，但是，网络监听只能应用于物理上连接于同一网段的主机。虽然有一定的局限性，但监听者往往能够获得其所在网段的所有用户账号及口令，尤其是如果两台主机进行通信的信息没有加密，威胁往往是最大的。

一般局域网内的十几台甚至上百台主机都是通过一个电缆、一个集线器连接在一起的，以太网协议的工作方式正是将要发送的数据包发往连在一起的所有主机。在数据包头部包含着应该接收数据包的主机的正确地址。因此，只有地址为数据包目标地址的那台主机才能接收到数据包。但是，当主机工作在监听模式下时，无论数据包中的目标物理地址是什么，主机都将接收。因为无论是同一网络中的两台主机通信时，源主机将写有目的地址的数据包直接发向目的主机，或者是网络中的一台主机同外界的主机通信时，源主机将写有目的的主机IP 地址的数据包发向网关，这种数据包都必须从 TCP/IP 协议的 IP 层通过网络接口交给数据链路层。数据包到了数据链路层是以物理地址作为惟一标识的。数据链路层将 IP 层传递来的数据包增加一个以太帧的头部信息，在帧头中包含源主机和目的主机的物理地址，并且一个 IP 地址惟一地对应一个物理地址。网关主机位于多个网络的交接点，因此在每个网络中都有一个 IP 地址，而发向网络外的帧中继携带的就是网关的物理地址。局域网中数字信号在电缆上传输信号，能够到达线路上的每一台主机。当数字信号到达一台主机的网络接口时，正常状态下网络接口对读入的数据帧进行检查，如果数据帧的目的物理地址是自己的地址或者是广播地址，就上交 IP 层处理。但是当主机设置为监听模式，所有的数据帧都将交付上层协议软件处理，也就是说监听主机捕获了本网全部数据包。

网路监听得以实现是因为现在网络中所使用大多数协议的设计都是基于友好的、通信的双方充分信任的基础之上的。很多时候用户口令甚至是以明文的方式在网上传输的，因此通过网络监听获得用户信息是黑客进行攻击的一条捷径。而且实现网络监听也十分方便，Windows 操作系统的用户可以直接运行监听软件，并且对用户权限无特别要求。UNIX 系统用户首先必须拥有超级用户权限，然后只需要向网络接口发送 I/O 控制命令把主机设置成监听模式了。

网络监听也有一定的弱点。首先，监听软件对本网络所有数据都不加选择的进行监听，占用大量处理器时间。其次，网络数据流量巨大，如果实时进行处理会造成数据包丢失，因此往往采取数据存储等待处理，这样需要收集的信息量就非常大。最后，监听到的海量数据结果是按照时间顺序存放在数据文件中的，因此要分析出两台主机间的活动还须花费较大周折，工作繁重。尽管网络监听有一些缺陷，并且只能监听物理上连接于同一网段的主机，但是在捕获用户口令时，这还是一种简便有效的办法。

2．端口扫描

端口扫描可以说是一把双刃剑，既是黑客入侵攻击的问路石，又是网络安全管理员分析自己网络的评估工具。端口扫描包括本地扫描和网络扫描两大类，黑客一般采用网络扫描侦察目标系统的情况，搜集目标系统的信息，再决定下一步行动。端口扫描的目的可以概括为发现一台活动的主机或一个网络；勘察什么服务正运行在该主机的哪个端口；确定目标系统的操作系统类型及版本信息。端口扫描得到的信息对一般网络用户而言可能毫无意义，但是对于熟悉计算机网络的黑客而言却找到了通向目标系统的大门，因为两台主机连接时都必须通过端口进行连接，也就是说每一个端口都是潜在的攻击通道。

端口扫描的基本原理可概括为扫描方通过向目标系统的不同端口发送具有特殊标志位的数据包，并记录目标所作的应答，通过分析得出关于目标系统的相关信息。

根据扫描数据包的类型，扫描技术通常可分为 TCP 扫描、ICMP 扫描、UDP 扫描等多种类型。其中，TCP Connect()扫描是最基本的扫描。扫描方利用操作系统提供的 connect()系

统调用，与每一个感兴趣的主机端口进行连接。如果端口处于监听状态，那么 connect()就能成功。如果端口关闭，则 connect()调用失败。这个技术的最大优点是不需要任何权限，系统中的任何用户都有权利使用这个调用。但缺点是这种形式的探测很容易被目标主机察觉并记录下来。因为扫描方与目标系统完成三次握手后就马上断开连接，于是目标系统的记录会显示出一连串的连接及错误信息。

既然 TCP Connect()扫描风险太大，TCP 半公开扫描的出现就势在必行了。TCP 半公开扫描其实就是故意发送违反 TCP 三次握手协议的数据包来对目标进行扫描。参考 TCP 连接三次握手的过程，此类扫描又可以分为下面几种类型：

- TCP SYN 扫描：扫描程序发送一个 SYN 数据包，一个 SYN|ACK 的返回信息表示端口处于侦听状态，这时扫描程序必须再发送一个 RST 信号，来关闭这个连接过程。一个 RST 返回，表示端口没有处于侦听状态。
- TCP SYN|ACK 扫描：这种扫描技术发送的是 SYN|ACK 数据包，就好像在应答目标发出的 SYN 数据包一样。如果目标收到此数据包就会反馈 RST 数据包用于关闭连接，黑客就可以通过这种 TCP RST 报文来判断目标是否存在。
- TCP ACK 扫描：扫描程序发送 ACK 数据包，如果目标收到此数据包，那么它就会反馈 TCP RST 数据包，我们就可以判断目标是否存在。

有的时候可能连 TCP 半公开扫描都不够秘密，因为防火墙和报文过滤设备会对一些指定的端口进行监视，入侵检测系统也能察觉这些扫描。这时候就需要用到 TCP 隐秘扫描了。常见的隐秘扫描包括：

- TCP FIN 扫描：扫描程序发送一个 TCP FIN 数据包给远端主机的指定端口，没有任何反馈的话，主机是存在的，而且正在监听这个端口；如果主机反馈回一个 TCP RST 包，那么主机是存在的，但是没有监听这个端口。
- TCP 空扫描：这种扫描发送不含任何标志位的 TCP 报文。按照 RFC 793，目标系统所有关闭的端口都应该发回一个 RST 分组；如果目标端口处于监听状态，则不反馈任何报文。
- TCP Xmax 树扫描：这种扫描是往目标端口发送一个设置了 FIN|URG|PUSH 位的分组。跟 null 扫描类似，目标系统也应该给所有关闭着的端口发回一个 RST 分组。

其他常见的扫描类型还包括：

- ICMP 查询报文请求及应答扫描：一般的 ICMP 查询报文包括回射请求，时间戳请求，信息请求，地址掩码请求这几类。扫描程序发送 ICMP 请求报文，如果收到应答报文，则说明目标主机正在运行；如果没有应答，则说明目标主机关机或者存在包过滤装置。
- ICMP 差错报文扫描：如果目标主机接收到头部参数有错误的报文或者仅接收到分片报文的部分时，会应答 ICMP 参数问题报文。因此，我们可以故意向目标发送此类报文，如果收到目标应答的报文，则说明目标主机正在运行；否则说明目标主机关闭或者存在包过滤装置。
- UDP 端口不可达扫描：当向一个未打开的 UDP 端口发送一个数据包时，许多主机可能会返回一个 ICMP_PORT_UNREACH 错误，这样就能发现哪个端口是关闭的。

对目标系统作端口扫描并不是一个直接攻击系统漏洞，它仅仅能帮助我们发现目标机的

某些内在的弱点。而绝大部分安全漏洞或缺陷都与操作系统相关，因此辨识目标操作系统类型与版本信息也是端口扫描的重要功能之一。最常用的操作系统的鉴别技术是通过 TCP/IP 堆栈特征探测远程操作系统，即我们通常所说的栈指纹技术。另一种很常用的技术是 ICMP 指纹技术。指纹技术简单的说就是将置有异常标志位或没有意义的数据包发到远端目标系统触发其响应，由于 RFC 对大多数特殊标志位的响应没有规定，因此不同的操作系统对此类数据包的处理方法也是不同的，扫描端就可以根据这些数据进行判断。

TCP/IP 栈指纹技术的研究已经达到一个相当的高度，大量的实验已经可以找出各类操作系统对特殊的 TCP 包的响应特征，即其指纹，而且很多地方可以得到此类信息。TCP/IP 栈指纹技术适用于整个 TCP/IP 协议的实现和操作系统。栈指纹使用好几种不同方法来探测 TCP/IP 协议栈和操作系统的细微区别。这些信息用来创建一个指纹，然后和已知的指纹进行比较，就可以判断出当前被扫描的操作系统。

3. 口令入侵

口令入侵是指攻击者使用合法的用户账号和口令登录到目的主机，然后再实施攻击行为。攻击者通过猜测、监听和破解用户口令等方法获得对机器或网络的访问权，登录目标系统访问资源，安装后门等等。

利用网络监听是获得用户口令的方法之一。前面已经提到过网络监听可以捕获同一物理网段的全部数据包，危害性极大。当初设计互联网时出于方便、信任的原则很少要求协议采用加密或身份认证技术，许多常用的传输协议，如 Telnet、FTP、HTTP、SMTP 等协议的用户账户和口令信息都是以明文格式传输的，一旦被攻击者利用数据包截取工具捕获就可以轻而易举的得到用户账户和口令，登录目标系统了。

另一种方法是黑客可以通过获得目标系统的合法用户账号，然后利用密码破解软件暴力破解用户口令。获取合法用户账号可以通过许多途径，首先可以利用目标主机的某些服务，如 Finger 服务、X.500 服务等。如果目标主机开放 Finger 服务，就可以用 Finger 命令查询，目标系统会将保存的用户资料（如用户名、登录时间等）显示在终端或计算机上。其次多数用户电子邮件地址往往是其在目标主机上的账号，也可以尝试破解口令登录主机。此外，各操作系统通常有习惯性账号，比如 Windows 操作系统的 guest 用户账号通常是可用的，而且此账号通常伴随着众多的系统漏洞，所以危险性极高。还有部分系统账号的默认口令为空或极易猜测，如果系统管理员没有修改过，实质上就是向黑客打开了一扇大门，后果不堪设想。

在得到用户的账号后，黑客就会开始尝试破解口令以得到对目标系统的访问权限，这种方法一般是将可能的口令一一尝试，直到发现匹配的口令成功登录系统。黑客进行口令破解时通常采用暴力破解方法，利用口令破解软件连续不断的将猜测的有可能的密码输入给远端目标主机，直到找到正确口令或已经将词典的单词全部试完。在线的口令破解是一个不断尝试的过程，用于测试的口令有如下几个来源：

1）口令词典。因为大多数人习惯用英语单词、人名、特殊的日期等常见组合作为口令，方便记忆，因此将这样的组合编成词典文件，进行口令破解时依次从该文件中读取单词送往远端系统。据统计一万个常用单词的口令词典能破解出 70%的用户口令，而遍历十万条记录的词典文件用时大约也只要几个小时就可以了，无论从速度还是效率来说字典破解都是有力的方法。

2）蛮力破解。通常用户口令是字母、数字、特殊符号的组合，只要不断的尝试所有的

组合并且时间足够长，最后总能得到用户口令。不过口令越长蛮力破解需要的时间越长，而且成指数关系增加，所以该方法的效率不如词典破解。

3）组合破解。出于安全性的考虑，大多数用户改变了单纯使用词典单词作口令的习惯，但为了方便记忆，他们往往会选用单词与单词、单词与数字的组合。对应这类口令黑客采取组合破解的办法，从词典中读取单词，后缀数字、符号等送往远端系统进行猜测。

如果黑客能够得到目标主机的密码文件，就可以尝试进行破解，虽然密码文件都是经过加密的，但是黑客只需要在本地将字母、数字等的组合用同样的方法加密，然后逐一与密码文件比较，直到得到结果，其破解速度快，威胁性大。比如 UNIX 操作系统的用户的基本信息默认存放在 passwd 文件中，经过 DES 加密的口令存放在 shadow 的文件中。黑客一旦盗取口令文件就可以使用专门的破解 DES 加密法的程序来破解口令。

4．特洛伊木马

特洛伊木马是一个包含在合法程序中的非法程序，是一种基于远程控制的黑客工具，更是攻击者再次进入网络或者系统而不被发现的隐蔽通道。如果黑客获得了系统的存取权限，可以很容易地建立再次访问的后门。但如果他没有对系统的完全存取权限，往往通过诱使用户执行某些程序，而该程序捆绑有特洛伊木马程序，一旦用户执行了这些程序之后，木马就会留在目标系统中。用户在不知情的情况下运行的特洛伊木马程序可以直接侵入用户的电脑并进行破坏。木马在被植入攻击主机后，当黑客连接到互联网上时，它就会通过一定的方式把入侵主机的信息，包括主机的 IP 地址、预先设定的木马植入端口等发送给攻击者，有了这些信息攻击者就可以与木马里应外合控制攻击主机了。黑客利用特洛伊木马程序可以恣意修改受害电脑的配置、复制任何文件、窥视整个硬盘内的资料等等，达到控制目标计算机的目的。

特洛伊木马有客户端和服务器端两个执行程序，其中客户端是用于攻击者远程控制植入木马机器的程序，服务器端程序即是植入目标系统的木马程序。特洛伊木马具有隐蔽性和非授权性两大特点。隐蔽性是指木马的设计者为了防止木马被发现，采用多种手段隐藏木马，受害主机意识不到木马的存在，或者即使服务端发现木马但无法确定木马的具体位置，也就无法采取清除措施。而非授权性是指一旦控制端与服务端连接后，控制端将享有服务端的大部分操作权限，包括修改文件，修改注册表，控制鼠标，键盘等等，但这些权力并不是服务端赋予的，而是客户端利用木马窃取的。攻击者利用在被攻击者的计算机中安装通过端口进行通信的客户机/服务器程序，使被控制端作为服务器启动一个默认端口，而攻击者作为客户机利用此端口发出连接请求，进而启动被控制端的相应程序，完全控制目标计算机；有时特洛伊木马也会在被攻击的计算机内安装具有触发机制的程序，当对该机操作触发该程序时，可将计算机内的重要信息通过邮件或其他形式传到异地的机器上去。

通常使用木马这种黑客工具进行网络入侵的过程可分为六步：

1）配置木马。这是在安插、使用木马之前进行的步骤，对木马的后续操作进行适当的配置。一方面木马配置程序会采用修改图标、捆绑文件、定制端口、自我销毁等多种伪装手段，以便在服务端更好地隐藏木马。另一方面木马配置程序将需要反馈信息的方式或反馈地址进行设置，包括反馈信息的邮件地址、OICQ 号等。

2）传播木马。黑客主要通过两个途径传播木马：其一是通过电子邮件附件，黑客将木马程序与合法程序捆绑在一起作为附件与电子邮件一起发送出去，收件人只要打开附件，并

运行程序系统就会感染木马。其二是软件下载，一些网站名义上提供软件，实际上将木马捆绑在软件安装程序上，下载后只要一运行这些程序，木马就会自动安装。

3）运行木马。用户在受骗状态下运行木马程序，木马会自动安装。木马首先将自身复制到 Windows 系统文件夹中，然后修改注册表、开始文件夹，设置好木马的触发条件。安装完成以后就可以启动木马了，并且由于木马程序设置为自动运行，目标系统下次启动时也会自动运行木马程序。木马被激活后，进入内存，并开启事先定义的木马端口，准备与控制端建立连接。

4）信息泄露。前面已经提过在配置木马时指定了反馈信息的目的地址，因此木马成功安装后会收集服务器的软硬件信息，并将信息发送回配置的反馈地址。

5）建立连接。如果在目标主机安装了服务端程序，并且服务端和控制端都在线就可以建立连接了。服务/控制两端建立连接有一个必要条件就是控制端必须知道服务端的 IP 地址。有些网络用户的 IP 地址是固定的，从木马反馈的信息就可以获得，并且可以用这个地址保持以后连接。但拨号上网的 IP 地址是动态的，拨号用户每次连接网络的 IP 地址都会发生变化，所以必须获取木马发回的最新信息。当然，一般配置木马时就指定了服务端开放的端口，而目标主机 IP 地址的变化总是在一个范围内的，因此采用对一个网段的木马端口进行遍历扫描也可以找到木马服务端主机。

6）远程控制。控制端与服务端建立连接之后就可以对其进行控制了，可执行的操作包括窃取密码、访问与修改文件、修改注册表、控制对方系统等。木马除了窃取密码文件或缓存中的密码，还提供了击键记录功能，这样就可以盗取非明文形式的密码。黑客对文件的操作就如同对本机文件操作一样，可以进行读取、修改、运行等任何动作，对注册表的访问也一样不受任何限制，这样还有利于黑客更好的隐藏木马。此外黑客使用控制端可以重启或关闭目标操作系统，控制对方鼠标，监视服务端桌面等操作，干扰目标系统的正常运作。

5. 会话劫持

会话劫持是指在一次正常的通信过程中，黑客利用嗅探、欺骗等技术介入通信双方之中，窃取有用信息或者冒充其中之一欺骗另一台主机。会话劫持的形式包括黑客作为第三方参与到连接中，或者是在通信双方数据流中添加额外的信息，或者是将双方的通信模式暗中改变，总之通信双方之间的数据对黑客是可见的，并且可任由黑客随意修改。

会话劫持涉及三方主机：攻击者、目标主机和被劫持主机。TCP 会话劫持适用于任何 TCP 应用，包括 HTTP、FTP、Telnet 等。作为攻击者首先要窥探到正在进行 TCP 通信的两台主机之间传送的报文，以获取该报文的源 IP、源 TCP 端口号、目的 IP、目的 TCP 端号，从而可以得知其中一台主机对将要收到的下一个 TCP 报文段中序列号和应答序列号值的要求。然后，在目标主机收到被劫持主机报文之前，攻击者根据所截获的信息向目标主机发出一个 TCP 报文，如果目标主机先收到攻击报文，就可以在攻击者与目标主机之间建立合法的 TCP 会话。并且发送的攻击报文能够使目标主机对下一个要收到的 TCP 报文中的应答序列号的要求发生变化，导致被劫持主机的请求报文被目标主机拒绝。

具体的攻击步骤可归纳如下：

1）攻击者确定目标主机与被劫持主机的 IP 地址。确信两者之间有可以被利用的建立起信任关系的账号，如 guest 账号等。

2）攻击者在攻击主机上运行会话劫持软件，等待指示已探测到可用会话。

3）攻击者启动 ARP 传递守护进程、RST 守护进程，将选项设定为允许主机名解析。

4）被劫持主机利用 Telnet 等服务登录到目标主机，运行特定程序读取 / 编辑电子邮件。

5）攻击者寻找新的连接，列出全部活动连接，查看哪一个是潜在可用的。如果可被利用，攻击者或者继续观察此会话，或者劫持该会话连接。

6）被劫持主机发现异常，但服务器工作正常，因此被劫持主机无法断定究竟发生了什么事，也就不能采取下一步行动。

7）攻击者观察了这个用户连接，归还这个连接给被劫持主机，使之与目标主机实现重新同步。

8）被劫持主机根据提示重新与目标主机建立了连接。由于发生了异常情况，此用户往往用 root 账号登录以密切关注具体情况。

9）攻击者利用 RST 进程阻止新的连接，等待劫持 root 用户的连接。

10）被劫持主机使用 ssu 获取受保护的 root 外壳。

11）攻击者发现 root 账号登录后成功劫持该会话。

12）被劫持主机再次发现异常提示，失去与服务器的连接。

13）攻击者安放后门，删除相关记录，重新建立正常连接，关闭 RST 进程。

14）被劫持主机只好重新建立连接，原始连接已经丢失。他们通常以为先前是网络故障或者 TCP/IP 栈溢出，系统重启后才恢复正常。

15）攻击者等所有 admin 连接都断开后，用设置的后门登录系统。安装后门工具包，清除日志。

TCP 会话劫持攻击的好处在于使攻击者避开了被攻击主机对访问者的身份验证和安全认证，从而使攻击者直接进入对被攻击主机的访问状态，因此对系统安全构成的威胁比较严重。入侵者寻找一条现有的两台计算机间的连接，通常是服务器和客户间的会话连接，然后穿过未加保护的路由器或不合适的防火墙。入侵者得到合法用户的地址信息后，他模仿用户地址来劫持用户通话，然后主机会断开与合法用户的连接，入侵者就获得了与合法用户同样的访问权。

6. IP 欺骗

IP 欺骗攻击主要针对使用 IP 协议传送的报文，攻击者伪造源 IP 地址，如果冒充的源 IP 地址与目标主机之间的信任关系是基于 IP 地址的，攻击者就可以像合法用户一样对目标主机进行操作了。

这里的信任关系包括使用 Sun RPC 调用的配置、利用 IP 地址认证的网络服务、MIT 的 X Window 系统、R 服务等。在经典的 Phrack Magazine 中对信任关系作了较透彻的解释，该文指出“在 UNIX 领域中很容易获得信任关系。假如你在主机 A 和 B 上各有一个账户，如果不存在信任关系，主机 A 和 B 会把这两个账户当作互不相关的用户。为了方便起见，在主机 A 和主机 B 中建立起两个账户的相互信任关系。在主机 A 和主机 B 上你的 home 目录中创建.rhosts 文件。在主机 A 的 home 目录中输入 echo " B username " ＞ ～/.rhosts；在主机 B 的 home 目录中输入‘echo " A username " ＞～/.rhosts’。至此，你可以自由地使用任何以 r*开头的远程调用命令，而不用每次输入口令了。这些命令将允许以地址为基础的验证，或者允许或者拒绝以 IP 地址为基础的存取服务。” 文中还指出“rlogin 是一个简单的服务器程序，并且它是基于信任关系的验证。当用户从一台主机登录到另一台主机上，如果目录主