计算机网络安全与防御策略

张媛　贾晓霞　著

天津出版传媒集团
天津科学技术出版社

计算机网络安全与防御策略

张媛 贾晓霞 著

天津出版传媒集团
天津科学技术出版社

图书在版编目（CIP）数据

计算机网络安全与防御策略 / 张媛，贾晓霞著. -- 天津 : 天津科学技术出版社，2019.5

ISBN 978-7-5576-6810-5

Ⅰ. ①计… Ⅱ. ①张… ②贾… Ⅲ. ①计算机网络－网络安全－研究 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2019)第 140469 号

计算机网络安全与防御策略

JISUANJI WANGLUO ANQUAN YU FANGYU CELUE

责任编辑：王　冬

责任印制：兰　毅

出　　版：天津出版传媒集团
天津科学技术出版社

地　　址：天津市西康路 35 号

邮　　编：300051

电　　话：（022）23332397

网　　址：www.tjkjcbs.com.cn

发　　行：新华书店经销

印　　刷：济南大地图文快印有限公司

开本 787×1092 1/16　印张 9.5　字数 140 000

2019 年 5 月第 1 版第 1 次印刷

定价：49.00

前　言

以因特网为代表的信息网络技术应用正日益普及和广泛，应用领域从传统小型业务系统逐渐向大型关键业务系统扩展，典型的例如党政部门信息系统、金融业务系统、企业商务系统等。网络安全已经成为影响网络效能的重要问题，而因特网所具有的开放性、自由性和国际性在增加应用自由度的同时，对安全提出了更高级别的要求。一般来说，网络安全由信息安全和控制安全两部分组成。信息安全指信息的完整性、可用性、保密性和可靠性；控制安全则指身份认证、不可否认性、授权和访问控制。互联网的开放性、分散性和交互性特征为信息交流、信息共享、信息服务创造了理想空间，网络技术的迅速发展和广泛应用，为人类社会进步提供了巨大推动力。然而，正是由于互联网的特性，产生了信息污染、信息泄漏、信息不易受控等诸多安全问题。

总之，网络环境的多变性、复杂性，以及信息系统的脆弱性，决定了网络安全威胁的客观存在。网络安全建设是涉及我国经济发展、社会发展和国家安全的重大问题。网络时代所引发的安全问题不仅涉及国家的金融安全、经济安全，同时也涉及国家的国防安全、文化安全和政治安全。因此，可以说，在当前社会里，没有计算机网络安全保障，国家和单位就没有安全屏障。基于此，本书就计算机网络安全与防御策略展开研究。

本书由张媛、贾晓霞执笔撰写，由于时间仓促，加之水平有限，难免存在纰漏之处，恳请读者提出宝贵意见。

目　录

第一章　计算机网络安全概述

第一节　网络安全的界定

信息安全的内容随着技术的发展在不断丰富和发展。当前，计算机系统信息安全可定义为：“计算机的硬件、软件和数据得到保护，不因偶然和恶意的原因而遭到破坏、更改和泄露，保障系统连续正常运行”。美国国家信息基础设施（NII）定义了信息安全的五个目标：保密性、完整性、不可抵赖性、可用性和可靠性。

网络安全的内容与其保护的信息对象有关，但都是保证信息在网络上传输或在计算机系统中静态存储时仅允许授权用户访问，而不能被未授权用户非法访问。它希望存储在通信主机上的数据不被破坏、篡改和泄露；希望计算机之间的通信内容不会被非法窃听；希望通信的对方主机是真实而不是假冒的；希望通信的内容不会在传输过程中被非法修改；希望如果传输的内容被修改，可以被准确地检测出来。因此，网络安全可定义为：“在分布式网络环境中对信息载体和信息的处理、传输、存储、访问提供安全保护，以防数据和信息内容遭到破坏、更改和泄露，或网络服务中断，或拒绝服务，或被非授权使用和篡改”。

第二节　网络系统面临的安全威胁

当前，网络系统面临的主要安全威胁包括恶意代码、远程入侵、拒绝服务攻击、身份假冒、信息窃取和篡改等，下面具体分析。

一、恶意代码

恶意代码指经过存储介质和网络进行传播，从一台计算机系统到另外一台

计算机系统，未经授权认证破坏计算机系统完整性的程序或代码。它包括计算机病毒（Computer Virus）、蠕虫（Worms）、特洛伊木马（Trojan Horse）、逻辑炸弹（Logic Bombs）、系统后门（Backdoor）、Root kits、恶意脚本（Malicious Scripts）等。它有两个显著的特点：非授权性和破坏性。

计算机病毒是一种具有自我复制能力并会对系统造成巨大破坏的恶意代码，它通常寄生于某个正常程序中，运行时会感染其他文件、驻留系统内存、接管某些系统软件。

蠕虫与病毒类似，也具有自我复制能力，但是它的自我复制能力不像病毒那样需要人工干预，是完全自动地完成。它首先自动寻找有漏洞的系统，并向远程系统发起连接和攻击，完成自我复制。蠕虫的危害性要远大于计算机病毒，但是其生命期通常也比病毒短得多。

特洛伊木马是一种与远程主机建立连接，使得远程主机能够控制本地主机的程序。它通常隐藏在正常程序中，悄悄地在本地主机运行，削弱系统的安全控制机制，在用户毫无察觉的情况下让攻击者获得远程访问和控制系统的权限。大多数特洛伊木马包括客户端和服务器端两个部分。

逻辑炸弹指在特定逻辑条件满足时实施破坏的计算机程序，该程序触发后可能会造成灾难性后果。与病毒相比，它强调破坏作用本身，而实施破坏的程序本身不具有传染性。

系统后门一般是指那些绕过安全性控制而获取对程序或系统访问权的程序方法。在软件的开发阶段，程序员常常会在软件内创建后门程序以便可以修改程序设计中的缺陷。但是，如果这些后门被其他人知道，或是在发布软件之前没有删除后门程序，那么它就成为安全风险，容易被黑客当成漏洞进行攻击。

Root kits 是一种特殊的恶意软件，用于隐藏自身及指定的文件、进程和网络链接等信息，通常与木马、后门等恶意代码结合使用。它一般通过加载特殊的驱动，修改系统内核，进而达到隐藏信息的目的。它能够持久并毫无察觉地驻留在目标计算机中，对系统进行操纵，并通过隐秘渠道收集数据，危害性极大。

恶意脚本是指一切以制造危害或者损害系统功能为目的而从软件系统中增加、改变或删除的任何脚本，包括 Java 攻击小程序（Java attack applets）和危

险的 Active X 控件。它具有变形简单的特点，能够通过多样化的混淆机制隐藏自己。它依赖于浏览器，利用浏览器漏洞下载木马并向用户传播。

二、远程入侵

远程入侵也可称为远程攻击。RFC2828 将攻击定义为有意违反安全服务和侵犯系统安全策略的智能行为，远程入侵即从网络中某台主机发起，针对网络中其他主机的攻击行为。美国警方一般把远程入侵称为“Hacking”，入侵者称为黑客（Hacker）或者黑客（Cracker）。

黑客通常指精通网络、系统、外设以及软硬件技术的程序员，他们熟知系统漏洞及其原因，在操作系统和编程语言方面具备深厚扎实的专业知识，并不断追求更深更新的知识。一名优秀的黑客需要具备多种素质，包括：

（1）Free（自由、免费）的精神：需要在网络上与其他黑客进行广泛的交流，并有一种奉献精神，将自己的心得和编写的工具与其他黑客共享。

（2）探索与创新的精神：所有的黑客都是喜欢探索软件程序奥秘的人，他们探索程序与系统的漏洞，在发现问题的同时会提出解决问题的方法。

（3）反传统的精神：找出系统漏洞，并策划相关的手段利用该漏洞进行攻击，这是黑客永恒的工作主题，而所有的系统在没有发现漏洞之前都号称是安全的。

（4）合作的精神：成功的入侵和攻击，单靠一个人的力量没有办法完成，通常需要数人或数十人的通力协作才能完成任务，互联网提供了不同国家黑客交流合作的平台。

黑客通常指恶意非法地试图破解或破坏某个程序、破解系统及网络安全的程序员。他们与黑客相同的特点是都喜欢破译解密，但是黑客一般怀有不良企图，具有明确的破坏目的，会给主机带来巨大破坏。

远程入侵包括非法接入和非法访问两类。非法接入指非授权人员连接到网络系统内部并获得访问系统内部资源的途径，它通常是远程入侵系统的前奏。攻击者可以通过窃取用户口令、接入交换机端口、远程 VPN 接入和利用无线局域网接入等方式非法接入系统。非法访问指非授权用户通过远程登录或黑客工

具远程访问主机资源，造成非法访问的主要原因有恶意代码、操作系统漏洞、网络服务程序漏洞和安全配置错误等。例如木马在服务端运行后，可以接收远程客户端发出的指令，在服务端非法访问系统资源。操作系统漏洞可以使普通用户获得特权用户的访问权限，从而使非授权用户访问到本来无权访问的资源。

三、拒绝服务攻击

拒绝服务攻击（Denial of Service，DoS）即攻击者想办法让目标主机或系统停止提供服务或资源访问，这些资源包括磁盘空间、内存、进程甚至网络带宽，从而阻止正常用户的访问。一类是对网络带宽进行的消耗性攻击，使得网络无法正常传输信息。例如，攻击者向服务器发送大量 IP 分组，导致正常用户请求服务的分组无法到达该服务器，因而无法得到服务。该类攻击目前比较难解决，因为此类攻击是由于网络协议本身的安全缺陷造成的。另一类是利用系统漏洞使得系统崩溃，从而该系统无法继续提供有效服务。例如，攻击者往往利用 C 程序中存在的缓冲区溢出漏洞进行攻击，发送精心编写的二进制代码，导致程序崩溃，系统停止服务。

四、身份假冒

身份假冒分为 IP 地址假冒和用户假冒。IP 地址是信息发送者的重要标识符，接收者常用 IP 分组的源 IP 地址来确定发送者的身份。攻击者经常用不存在的或合法用户的 IP 地址，作为自己发送的 IP 分组的源 IP 地址，由于网络的路由协议并不检查 IP 分组的源 IP 地址，所以攻击者很容易进行 IP 欺骗。

网络世界中，用户的身份信息使用一组特定的数据来表示，系统只能识别用户的数字身份，所有对用户的授权也是针对用户数字身份的授权。身份鉴别方法包括短信口令、静态密码、智能卡、生物识别等，攻击者往往通过社会工程学方法或网络监听的方式窃取这些特定数据，从而利用这些数据欺骗远程系统，达到假冒合法用户的目的。

五、信息窃取和篡改

信息窃取和篡改是网络传输过程面临的主要安全威胁，分为主动攻击和被

动攻击两类。信息窃取和流量分析属于被动攻击。因为IP协议在设计之初没有考虑安全问题，攻击者只要在通信双方的物理线路上安装信号接收装置即可窃听通信内容。如果信息没有加密，则信息被窃取；如果信息经过适当加密，但是攻击者可以通过分析窃听到的信息模式进行流量分析，可能推测出通信双方的位置和身份并观察信息的频率和长度，这些信息对于猜测传输过程的某些性质很有帮助。窃取和流量分析属于针对保密性的一种攻击。被动攻击非常难以检测，因为它们根本不改变数据，通信双方都不知道有第三方已经窃取了信息。但是，防范这些攻击还是切实可行的，因此对付被动攻击的重点是防范而不是检测。

主动攻击包括重放（replay）、篡改、冒充、伪造和阻断。重放指窃取到信息后按照它之前的顺序重新传输，以此进行非授权访问或接入。篡改指将窃取到的信息进行修改、延迟或重排，再发给接收方，从而达到非授权访问或接入的目的。冒充通常是先窃取到认证过程的全部信息，在发现其中包含有效的认证信息流后重放这些信息，这样就可能冒充合法用户的身份。伪造指攻击者冒充合法身份在系统中插入虚假信息，并发给接收方。重放、篡改、冒充和伪造都是针对完整性的攻击。阻断指攻击者有意中断通信双方的网络传输过程，是针对可用性的一种攻击。

第三节　网络安全涉及的内容

一、网络安全体系

网络是由多层功能组合而成的复杂系统，当前互联网用于表示不同网络功能层之间关系的网络体系结构是TCP/IP五层体系结构，从高到低依次是应用层、传输层、网络层、链路层和物理层。任何一种单一技术都无法有效解决网络安全问题，必须在网络的每一层增加相应的安全功能，而且各层的安全功能必须相互协调，相互作用，构成有机整体，这样一个由各层安全功能构成的有机整体就是网络安全体系。

构建一个能够保证网络内用户不受攻击，机密信息不被窃取，所有网络服务能够正常进行的安全网络，是网络安全研究的目标，但是实现这个目标非常困难。可能针对特定网络环境，可以构建一个相对有效的网络安全体系，但是无法构建一个适用于所有网络应用环境的网络安全体系，所以研究网络安全体系，必须与具体的应用环境相结合。

根据网络的应用现状和 TCP/IP 协议结构，可以将网络安全体系的层次划分为物理层安全、系统层安全、网络层安全、应用层安全和管理层安全，每个层次上采取若干安全服务保证该系统单元的安全性。例如，网络平台需要节点之间的认证和访问控制；应用平台需要针对用户进行身份认证、访问控制，需要保证数据传输的完整性和保密性，需要有抗抵赖和审计功能，需要保证系统的可用性和可靠性。如果一个网络的各个系统单元都有相应的安全措施来满足安全需要，那么可以认为该网络是安全的。

1.物理层安全

物理层安全指物理环境的安全性，包括通信线路的安全、物理设备的安全和机房安全等。主要包括五个方面：

（1）防盗。像其他物体一样，主机也是偷窃者的目标。偷窃行为所造成的损失可能远远超过主机本身的价值，因此必须采取严格的防范措施，以确保主机设备不会丢失。

（2）防火。机房发生火灾一般是由于电气原因、人为事故或外部火灾蔓延引起。电气设备和线路因为短路、过载、接触不良、绝缘层破坏或静电等原因引起电打火而导致火灾。人为事故是指由于操作人员不慎，吸烟、乱扔烟头等，使存在易燃物质（如纸片、磁带、胶片等）的机房起火，当然也不排除人为故意放火。外部火灾蔓延是因外部房间或其他建筑物起火而蔓延到机房而引起火灾。

（3）防静电。静电是由物体间的相互摩擦、接触而产生的，计算机显示器也会产生很强的静电。静电产生后，由于未能释放而保留在物体内，会有很高的电位（能量不大），从而产生静电放电火花，造成火灾。

（4）防雷击。雷击可能使大规模集成电器损坏，这种损坏可能是在不知不

觉情况下造成的。利用引雷机理的传统避雷针防雷，不但增加雷击概率，而且产生感应雷，而感应雷是电子信息设备被损坏的主要杀手，也是易燃易爆品被引燃起爆的主要原因。雷击防范的主要措施：根据电气、微电子设备的不同功能及不同受保护程序和所属保护层，确定防护要点并做分类保护；根据雷电和操作瞬间过电压危害的可能通道，从电源线到数据通信线路都应做多层保护。

（5）防电磁泄漏。电子计算机和其他电子设备一样，工作时要产生电磁发射。电磁发射包括辐射发射和传导发射。这两种电磁发射可被高灵敏度的接收设备接收并进行分析、还原，造成计算机的信息泄露。屏蔽是防电磁泄漏的有效措施，屏蔽主要有电屏蔽、磁屏蔽和电磁屏蔽三种类型。

2.系统层安全

系统层安全指操作系统的安全性，它是整个网络与计算机系统的安全基础，没有操作系统的安全，就不可能真正解决网络安全和其他应用软件的安全问题。系统的安全问题主要表现在三方面：

（1）及时修复系统漏洞。漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。系统漏洞是指操作系统在开发过程中存在的技术缺陷或程序错误，这些缺陷可能导致其他用户非法访问或利用病毒攻击计算机系统，从而窃取重要信息，甚至破坏操作系统。如果系统存在漏洞，必须在第一时间打上漏洞补丁，以防止恶意代码攻击造成损失。系统管理员需要经常关注操作系统供应商的安全公告，及时了解最新的系统漏洞及补丁情况，避免系统受到攻击。

（2）防止系统的安全配置错误。现代操作系统本身已经提供一定的访问控制、认证与授权等方面的安全服务，管理员必须根据应用环境的安全需求对这些服务进行安全配置，使系统提供的服务能够正确应付各种入侵。如果错误地配置了这些服务，那么这些安全服务无法生效，系统也就处于危险中。管理员应该经常使用安全配置检查工具，对系统当前配置进行检查，并根据应用环境制定相应的安全策略，检查系统配置是否与预定义的安全策略保持一致，及时发现并纠正配置中可能存在的问题。

（3）防止病毒对系统的威胁。系统感染病毒后，会出现运行变慢、资源莫

名减少的问题，使得系统可用性大大降低，所以对病毒的防护是系统层安全的重要方面。系统必须能及时进行防毒、查毒和杀毒。防毒指根据系统特性，采取相应的系统安全措施预防病毒侵入计算机，可以准确地预警通过不同传输媒介下载到本地的病毒，在病毒入侵时发出警报，并及时对病毒隔离或清除。查毒指对于确定的环境，能够准确地识别病毒名称，该环境包括内存、引导区、可执行文件、文本文件或网络等。杀毒指根据不同类型病毒对感染对象的修改，并按照病毒的感染特性所进行的恢复，该恢复过程不能破坏未被病毒修改的内容。

3.网络层安全

网络层安全指网络系统的安全性，包括身份认证、访问控制、数据传输的保密性和完整性、路由系统安全、入侵检测和防病毒技术等。

（1）身份认证：也称为“身份验证”或“身份鉴别”，指在计算机及计算机网络系统中确认操作者身份的过程，从而确定该用户是否具有对某种资源的访问和使用权限，进而使计算机和网络系统的访问策略能够可靠、有效地执行，防止攻击者假冒合法用户获得资源的访问权限，保证系统和数据的安全以及授权访问者的合法利益。

（2）访问控制：按用户身份及其所归属的某项定义组来限制用户对某些信息项的访问，或限制对某些控制功能的使用的一种技术，通常用于系统管理员控制用户对服务器、目录、文件等网络资源的访问。其功能包括：①防止非法的主体进入受保护的网络资源；②允许合法用户访问受保护的网络资源；③防止合法用户对受保护的网络资源进行非授权的访问。

（3）数据传输的保密性和完整性：保密性指数据传输过程中，传输的信息按给定要求不泄露给除通信方外的其他人、实体或过程，即杜绝有用信息泄露给非授权个人或实体，强调有用信息只被通信方使用的特征。完整性指数据传输过程中，保证信息或数据不会被未授权的篡改或在篡改后能够被通信方检测出。

（4）路由系统安全：路由器是一种网络交换设备，用于连接多个网络或网段，将不同网络或网段之间的信息进行翻译，以使它们能够相互读懂对方的数

据，从而构成一个更大的网络。它是网络系统中的关键节点，如果路由器被攻击者控制，意味着所有经过它的信息都可能会被窃听和篡改，从而破坏数据传输的保密性和完整性。路由系统安全分为路由器操作系统的安全和路由信息传输的安全。路由器操作系统的安全包括及时给路由器打上漏洞补丁，根据安全策略检测路由的安全配置是否正确；路由信息传输的安全主要是保证路由信息的保密性和完整性，防止攻击者发送和传播伪造路由。

（5）入侵检测：是对入侵行为的检测。它通过收集和分析网络行为、安全日志、审计数据、其他网络上可以获得的信息以及系统中若干关键点的信息，检查网络或系统中是否存在违反安全策略的行为和被攻击的迹象。它是一种积极主动的安全防护技术，提供了对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前拦截和响应入侵。入侵检测必须在不影响网络性能的情况下对网络进行监测。

（6）防病毒技术：网络防病毒的原理主要是监控和扫描，通过网络中的大量客户端对网络中软件行为的异常监测，获取病毒的最新信息，推送到服务端进行自动分析和处理，再把这些病毒的解决方案分发到每一个客户端。未来杀毒软件将无法有效地处理日益增多的恶意程序，识别和查杀病毒不仅仅依靠服务端本地硬盘中的病毒库，而是依靠庞大的网络服务，实时进行采集、分析以及处理，把网络变成一个巨大的“杀毒软件”，参与者越多，网络就越安全。现有防病毒技术主要有脱壳技术、自我保护技术、主动防御技术、启发技术、虚拟机技术和人工智能技术。

4.应用层安全

应用层安全主要指网络系统应用软件和数据库的安全性，包括 Web 安全、DNS 安全和邮件系统安全等。

（1）Web 安全：互联网中的 Web 服务使用 HTTP 传输数据，该协议的设计目标是灵活实时地传送文件，没有考虑安全因素。但是，基于 HTTP 的 Web 应用都期望提供身份认证，因此导致 Web 应用存在诸多安全隐患，例如，账号和密码信息未经加密即在客户和服务器之间传输。HTTP 是无状态的协议，同一个客户的不同请求之间没有对应关系，使得基于 Web 的身份冒充非常容易。

另外，Web 应用程序可能存在诸多安全漏洞，导致基于 Web 的攻击频繁发生，常见的有 SQL 注入攻击、跨站脚本攻击和跨站伪造请求等。

（2）DNS 安全：由于互联网依赖 DNS 提供域名解析，因此 DNS 的安全性极为重要。DNS 的安全问题主要包括防止 DNS 欺骗和防御 DoS 攻击。由于 DNS 不提供客户与服务器之间的身份认证，一方面，攻击者可以伪造假的 DNS 应答给 DNS 查询方，将用户引导到错误的站点，对用户进行进一步欺骗；另一方面，攻击者可以篡改服务器中的缓存记录来欺骗 DNS 查询方，因为 DNS 优先返回缓存中已经存在的记录。DoS 攻击是目前最为普遍的攻击手段，目标是使得 DNS 服务器无法正常工作，从而影响目标网络的正常运转。通常采取的防御手段包括使用备份域名服务器、最小权限原则、限制区域传输、最少服务原则等。

（3）邮件系统安全：针对邮件系统的攻击分为直接攻击和间接攻击。直接攻击包括窃取邮箱密码、截获邮件内容、伪造邮件内容、发送垃圾邮件等，主要是由于邮件收发协议如 SMTP、POP3 存在先天的安全隐患，仅考虑如何可靠和及时地收发报文，没有考虑加密和认证等安全技术。间接攻击主要是通过邮件传输病毒或木马等恶意程序，将恶意代码放在邮件附件中或者伪造成网页和链接，诱骗用户点击。目前采用的防御手段包括服务端提供验证和过滤机制、邮件病毒扫描、端到端的安全电子邮件协议（如 PGP、S/MIME）等。

5.管理层安全

管理层安全涉及的内容较多，包括技术和设备的管理、管理制度、部门与人员的组织规则等。尤其是安全管理的制度化在网络安全中有着不可忽视的作用，严格的安全管理制度、责任明确的部门安全职责、合理的人员角色配置，都可以有效地增强网络的安全性。

二、网络攻击技术

网络攻击是指对网络的保密性、完整性、不可抵赖性、可用性、可控性产生危害的任何行为，可抽象分为信息泄露、完整性破坏、拒绝服务攻击和非法访问四种基本类型。网络攻击的基本特征：由攻击者发起并使用一定的攻击工

具，对目标网络系统进行攻击访问，并呈现出一定的攻击效果，实现了攻击者的攻击意图。

网络攻击方式一般可分为读取攻击、操作攻击、欺骗攻击、泛洪攻击、重定向攻击和 Rootkits 技术等。

（1）读取攻击：用于侦察和扫描，识别目标主机运行的网络服务以及可能的漏洞。

（2）操作攻击：以篡改数据为手段，攻击以特权身份运行的服务程序，取得程序的控制权，如 SQL 注入、缓冲区溢出攻击。

（3）欺骗攻击：将自身伪装成其他用户实施攻击行为，冒充特权用户入侵系统。典型的欺骗攻击如 ARP 欺骗、DNS 欺骗、IP 欺骗和网络钓鱼等。

（4）泛洪攻击：目的是让远程主机无法承受巨大的流量而瘫痪，如 Smurf 攻击、TCP SYN Flood 和 DDoS 攻击等。

（5）重定向攻击：将发往目标的信息全部重定向到攻击者指定的目标主机上，有利于展开下一步攻击。如 ARP 重定向是欺骗受害主机，将攻击者主机伪装成网关，从而截获所有受害主机发往互联网的报文。

（6）Rootkits 技术：Rootkits 是用于隐藏自身及指定文件、进程和链接的恶意软件工具集，集多种攻击技术于一体，常与其他恶意代码结合使用，分为进程注入式和驱动级。驱动级 Rootkits 较为复杂，且加载级别较高，现阶段还没有较好的解决办法。

网络攻击的常用手段包括：

（1）网络监听。大多数网络通信采用未经加密的明文通信，因此只要攻击者获取数据通信的传输路径即可轻易实现监听，监听型攻击会造成数据泄露，危及敏感数据安全。

（2）篡改数据。攻击者对截获的数据进行修改，并使得数据收发双方无法察觉。

（3）网络欺骗。常见的欺骗攻击主要有 IP 欺骗、ARP 欺骗、DNS 欺骗、路由欺骗、网络钓鱼。

（4）弱口令攻击。攻击者通过各种方式成功获取和破解合法用户的口令，

从而冒充合法用户进入系统。

（5）拒绝服务。破坏性攻击，直接使目标系统停止工作或耗尽目标网络的带宽使之无法为正常请求提供服务。

（6）漏洞破解。利用系统漏洞实施攻击，获取系统访问权限。

（7）木马攻击。在正常的 Web 页面或聊天界面中植入恶意代码或链接，诱使用户查看或点击，然后自动下载木马程序到目标用户主机，使得攻击者可以通过木马远程控制用户主机。

实施网络攻击的过程虽然复杂多变，但是仍有规律可循。一次成功的网络攻击通常包括信息收集、网络隐身、端口和漏洞扫描、实施攻击、设置后门和痕迹清除等步骤。

1.信息收集

信息收集指通过各种方式获取目标主机或网络的信息，属于攻击前的准备阶段，也是一个关键的环节。首先要确定攻击目的，即明确要给对方形成何种后果，有的可能是为了获取机密文件信息，有的可能是为了破坏系统完整性，有的可能是为了获得系统的最高权限。其次是尽可能多地收集各种与目标系统有关的信息，形成对目标系统的粗略性认识。收集的信息通常包括：

（1）网络接入方式：拨号接入、无线局域网接入、以太网接入、VPN 远程接入等。

（2）目标网络信息：域名范围、IP 地址范围、具体地理位置等。

（3）网络拓扑结构：交换设备类型、设备生产厂家、传输网络类型等。

（4）网络用户信息：邮件地址范围、用户账号密码等。

收集信息的方式包括：

（1）使用常见的搜索引擎，如 Google、必应、百度等。

（2）使用 dmitry 等工具通过 whois 服务器查询主机的具体域名和地理信息。

（3）使用 netdiscover 等工具查询主机的 IP 地址范围，使用 dnsmap、dnswalk、dig 等工具查询域名空间。

（4）使用社会工程学手段获得有关社会信息，如网站所属公司的名称、规模，管理员的生活习惯、电话号码等，maltego 就是一款收集此类社会信息的查