电脑报 总策划

黑客防线丛书

黑客入门实战

电脑报 编

精彩看点

黑客攻防新手入门

必知必会的黑客术语
黑客入侵前的信息搜集

黑客攻防上手实战

聊天软件攻防、密码攻防
进程、端口、共享资源攻防

黑客进阶实例操练

病毒木马、网络炸弹攻击与防范
远程控制操作实例演练

安全配置与防范

网站与服务器安全攻防
防火墙安全配置与入侵检测

超值光盘

黑客攻防视频教程　防毒反黑工具　系统优化工具
网络检测工具　数据加密工具　恶意软件清理工具

云南人民电子音像出版社

黑客防线 专辑

黑客入门实战

电脑报 编

云南人民电子音像出版社

内容提要

本书主要讲解了黑客入门必备的基础知识，并详细地剖析了黑客常用的攻击手段和攻防实例，同时给出了行之有效的防范措施，可帮助读者认识黑客，了解黑客，远离黑客入侵。

全书共分11章，首先讲解了黑客入门的基础知识，包括黑客必知必会的一些概念、术语，以及黑客入侵前的信息搜集；接下来，以实例剖析的形式为大家展示了黑客常用的攻防技巧，包括聊天软件攻防、密码攻防、进程与端口攻防、共享资源攻防、网络炸弹攻防等内容，让大家全面认识黑客，从而有针对性地防范网络侵袭；此外，本书还安排了病毒木马防范、远程控制实例演练、网站与服务器攻防、系统安全分析与入侵检测等方面的内容，以帮助读者掌握网络安全系统防范技巧，真正拒黑客于千里之外！

本书是一本黑客理论与实战相结合的入门图书，可供初级读者学习、进阶之用。

警告：文中涉及到的黑客攻防相关内容，仅供读者学习之用，如用于非法用途，后果自负。

光盘要目

- 黑客攻防视频教程
- 网络安全检测工具
- 恶意软件清理工具
- 病毒木马查杀工具
- 系统优化维护工具
- 数据加密解密软件

书　　名：黑客入门实战
编　　者：电脑报
责任编辑：西　捷　王　燕
技术编辑：李　勇
封面设计：程　佳
出版单位：云南人民电子音像出版社
地　　址：昆明市环城西路609号
邮政编码：650034
发　　行：云南人民电子音像出版社
经　　销：各地新华书店、报刊亭
CD生产：四川省蓥山数码科技有限公司
文本印刷：重庆升光电力印务有限公司
开本规格：787mm×1092mm 1/16　16印张　300千字
版　　号：ISBN 978-7-900392-74-9
版　　次：2008年7月第1版　2008年7月第1次印刷
定　　价：28.00元(1CD+配套书)

黑客防线

从零开始 黑客攻防轻松上路

网络就像一把双刃剑，在带给我们诸多方便的同时，也带来了肆虐的病毒、木马、恶意攻击等，“黑客”一词逐步走入广大网民的生活。在以前，很多用户总认为黑客神秘莫测，防不胜防，而如今，黑客就频繁活跃在你我身边！如何确保自己的电脑安全、如何有效地防范黑客攻击，已经成为每个电脑用户的当务之急。

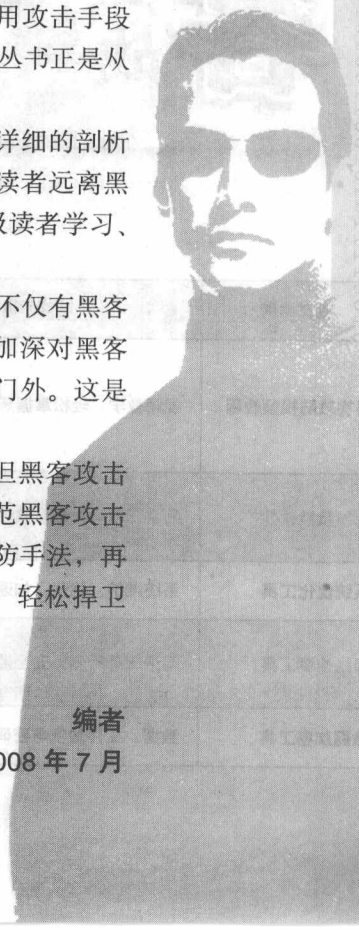
为了帮助大家更好地维护网络安全，我们专门策划并制作了“**黑客防线**”系列图书，该系列图书通过解析黑客的各种攻击行为和攻击实例，让用户认识黑客的各种攻击手段，从而采取行之有效的防范措施。“知己知彼，百战不殆”，只有充分了解和掌握黑客们常用的攻防手段，才能找到黑客入侵的防御要领，进而做好相应的安全配置，甚至可以从黑客留下的蛛丝马迹上“追踪”黑客，从而帮助大家远离黑客的困扰。

掌握黑客攻防知识不妨从以下两方面着手：其一是了解黑客常用的攻击手段和攻防工具，其二是通过大量攻防实例来加深对黑客常用攻击手段的认识。“理论联系实际，以实例诠释理论”，“**黑客防线**”系列丛书正是从这两方面展开，丛书包含：

《黑客入门实战》：首先讲述了黑客入门的基础知识，继而详细的剖析了黑客常用的攻击手段，同时给出行之有效的防范措施，帮助读者远离黑客入侵。这是一本黑客理论与实战相结合的入门图书，可供初级读者学习、进阶之用。

《黑客攻防案例 100%》：100 余个黑客攻击与防范的实例，不仅有黑客工具的应用，还有黑客攻防的谋略技巧，通过这些实例的学习加深对黑客常用手段的认识，并采取对应的防范措施，真正做到拒黑客于门外。这是一本全实战演练黑客攻防的操作指南。

通过本系列图书的学习，你会发现：黑客其实并不高深，但黑客攻击手段却“花样百出”，甚至会不断“推陈出新”，因此，有效防范黑客攻击并非朝夕之功，但“万变不离其宗”，只要掌握了常见的黑客攻防手法，再举一反三，相信大家都可以轻松应对黑客！洞悉黑客绝技高招，轻松捍卫网络安全！



编者

2008 年 7 月

黑客防线

《黑客入门实战》
多媒体光盘内容简介

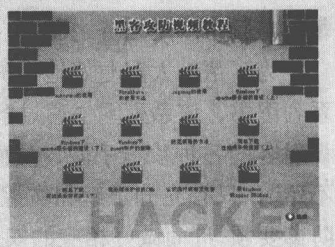
防毒反黑软件

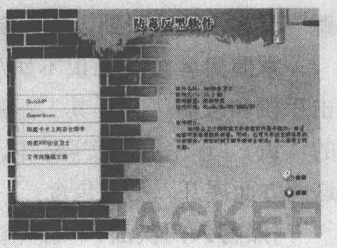
黑客攻防视频教程

网络检测工具

系统优化工具

数据加密工具





精彩导读

资源类别	功能用途	详细内容
黑客攻防视频教程	视频教学，轻松掌握黑客攻防技巧	autoruns的使用、FinalData的使用方法、regsnap的使用、Windows下apache服务器的建设、Windows下guest账户的删除、简单下载在线娱乐类资源、批处理保护你的CMD、认识流行病毒及危害、防范病毒的方法、用Windows的ipsec防DDos
防毒反黑软件	病毒、木马、恶意软件查杀与清理	QuickIP、SuperScan、奇虎360安全卫士、瑞星卡卡上网安全助手、文件夹隐藏大师
系统优化工具	系统维护、优化、加速	Windows优化大师、Windows优化精灵、变速精灵、超级兔子魔法设置
网络检测工具	网络流量检测、安全监控	网络数据包拦截软件、BMSetup、WinPcap、局域网查看工具、探索网络监视器
数据加密工具	数据、文件加密与密码管理	超级密码卫士、WinGuard Pro、绝对隐私、万能加密器

CONTENT 目录

第一章 新手起步——黑客入门必修课

当电脑已经普及，网络已经融入我们的生活与工作时，每台电脑都可能会遭到病毒、木马和黑客的攻击，只要电脑连接到Internet，随时都会面临着这样或那样的安全威胁。怎么办呢？不能因噎废食而选择不使用电脑和网络，更不能坐以待毙，惟一的方法就是多学黑客攻防知识，从而做到心中有数，知己知彼，方能有效防范黑客。因此，本章将首先和读者们探讨黑客以及防范黑客的各种基础知识。

第二章 锁定目标——黑客入侵前的信息搜集

通常来讲，除了傻瓜黑客外，真正的黑客在进行攻击前总会花很多时间和精力去搜集目标主机的相关信息，比如对方使用的什么操作系统、管理员账号是否为空口令或者弱口令、系统是否存在某些严重的漏洞……掌握了这些信息，攻击成功又多了几分胜算，越成熟的黑客花费在信息搜索上的时间往往越多。信息搜集、筛选、分析……这是最枯燥却也是最重要的工作，那么黑客是如何进行这些信息搜集工作的呢？本章将为大家一一讲解。

目录 CONTENT

第五章 细节入手——进程与端口攻防

Windows进程和端口是用户最容易忽略的，可能甚至有的新用户都不知道它们的存在，然而，进程和端口在系统安全中都起着非常重要的作用，黑客常常会利用系统开放的端口入侵你的电脑，因此，不是必须开启的端口应该尽量关闭。而黑客或者病毒恶意程序入侵你的电脑后，通常会在系统进程中有所体现，所以，把好进程关则可以很好地防范黑客和各种有害程序。

第六章 近水楼台——局域网共享资源攻防

共享是文件分享的一种方式，通常在局域网中进行，因此，用户具有“近水楼台先得月”的地理位置优势。对于初级的黑客来说，通过共享漏洞入侵目标电脑是他们常干的事情，这种入侵方法比较简单且成功率高。原因很简单：很多用户认为共享理所当然，并不会有任何安全隐患顾虑，所以出现漏洞的几率相当高，进而给黑客带来可乘之机。本章将剖析共享漏洞入侵的方法与防范措施。

目录 CONTENT

第七章 全面围剿——病毒与木马查杀

几乎每位电脑用户都要与病毒、木马打交道，随着网络的普及，病毒、木马也更加泛滥。如果机器中不安装杀毒软件和防火墙工具“裸奔”，估计你的电脑很快就会被病毒木马破坏，因此，本章将与大家一起学习病毒、木马防范的相关知识，并给大家推荐一些比较好用的查杀工具，让大家轻松应对病毒、木马。

第八章 防不胜防——网络炸弹攻击与防范

有时候，当我们在浏览网页，准备查找所需要的信息时，突然发生“蓝屏事件”，或者突然网络断线；打开邮箱准备收信，却发现邮箱里面灌满了垃圾邮件；在论坛上正和朋友们聊得欢，突然发现有人正冒充我们的名字大放厥词……不用害怕，以上种种，其实是中了网络炸弹所致。在本章中，将剖析各种网络炸弹的入侵方式，并介绍相应的防御方法。

目录 CONTENT

第九章 运筹帷幄——远程控制操作演练

在黑客攻防中，远程控制也是非常关键的黑客技术。控制与反控制一直是黑客与安全人员之间的一对矛盾，他们在相互较量中不断上演着一幕又一幕“魔高一尺，道高一丈”的好戏。本章我们将带领大家学习远程控制的实战操作与技巧。

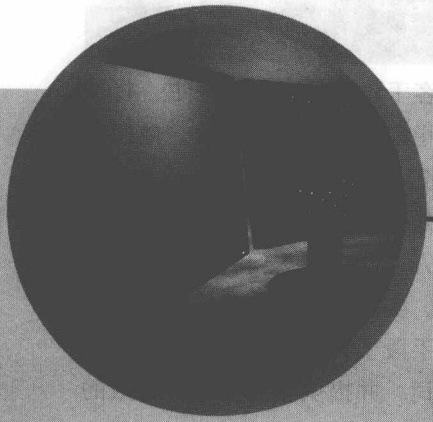
第十章 围追堵截——网站与服务器攻防

网站和服务器都是黑客最喜欢下手的对象，不过，由于网站和服务器都具有基本的保护措施，所以相对于一般上网的个人电脑而言显得较不易入侵成功。然而，由于很多服务器软件或操作系统的设计不良，常会造成各种各样的漏洞导致黑客们有机可乘，甚至造成网络灾难。在本章中，将剖析黑客对网站或各类服务器的入侵及攻击流程，以及如何进行相应的防范。

第十一章 终极防范——安全分析与入侵检测

如果有人问你的系统是否安全？你该如何作答？是毫无所知，听天由命，还是胸有成竹，信心十足？其实回答这个问题的最好办法就是学会进行系统的安全分析与服务器的入侵检测技术。只有对自己的机器有充分的了解，才可能真正地将安全威胁屏蔽。

目录 CONTENT



第一章

新手起步——黑客入门必修课

当电脑已经普及，网络已经融入我们的生活与工作时，每台电脑都可能会遭到病毒、木马和黑客的攻击，只要电脑连接到Internet，随时都会面临着这样或那样的安全威胁。怎么办呢？不能因噎废食而选择不使用电脑和网络，更不能坐以待毙，惟一的方法就是多学黑客攻防知识，从而做到心中有数，知己知彼，方能有效防范黑客。因此，本章将首先和读者们探讨黑客以及防范黑客的各种基础知识。

1.1 黑客简介

在许多人眼里，“黑客”（Hacker）是一群高深莫测的神秘人物，他们利用掌握的技术肆意展开各种攻击，他们无往而不利……再加上一些媒体对黑客事件不负责任地夸大报道，使得黑客以及黑客技术对普通的电脑用户而言，无形中就多了几许神秘的色彩！

其实，黑客以及黑客技术并不神秘，也并不高深。比方说，一名普通的电脑用户，只需掌握一定的基础技能，就能轻松地迈入黑客之门——甚至无需学习任何知识，只要能学会黑客软件的使用方法，也可以展开一些黑客行动。这些都是如今网络中“黑客”如此盛行的原因。

1.1.1 黑客是什么

很多电脑用户在上网的时候，都会或多或少地听过“某某被黑了”这样的话。似乎，黑客就是一些破坏分子！显然，在很多人眼中，“黑客”与“网络破坏者”这两个词的“意思”都是一样的。真的是这样吗？其实，很多人都不了解什么是真正的黑客。

其实，真正的黑客是指喜欢探索软件程序奥秘、并从中增长其个人才干的人。他们不像绝大多数电脑使用者，只规规矩矩地了解别人指定了解范围内的知识。

除了上述解释外，再让我们听听几位国内不同水平的“黑客”是如何诠释“黑客”这个名词的吧。

黑客一：某黑客软件开发程序员

简历：某下载量、使用率较高的黑客软件开发程序员，当前职业为专职PHP程序员。

“其实我的资历很浅，让我谈黑客真是勉为其难。我2000年才接触电脑，之前连开机都不会的。开发黑客软件纯属兴趣，做一件有挑战性的事情没有浓厚的兴趣是不行的，做黑客也是这样，都需要有兴趣才行。三天打鱼两天晒网，很快就会把学会的技术忘掉的，黑客技术永远都不会长进，永远都是末流黑客……”

黑客二：某黑客网站站长

简历：参加过著名的中美黑客大战，曾独自或联手攻克数个“顽固”型网站。

“‘会者不难，难者不会’，只要有恒心和毅力，一天学一点，从零开始，很快你就都会了。我们网站的那些菜鸟，最初连‘黑客’概念都搞不清的，现在可都成了‘大虾’了。”

“其实，对于普通用户来说，成为专业的黑客很难，还是先学些黑客软件的使用方法比较好，实战结合理论，是学习黑客技术最佳途

径……”

“但是，我反对用木马病毒之类的东西去害人，这样做是损人不利己。要知道黑客也有职业道德，如果连基本的道德也没有，那即使有点技术也不能算是黑客。”

“漏洞，我喜欢研究系统漏洞，光Windows系统的漏洞就一辈子也研究不完。想想看，连Vista都存在输入法漏洞呢！想破脑袋这种低级漏洞也不应该在Vista中出现吧？”

通过几位“黑客”的言谈，相信读者们都或多或少地明白了什么是黑客，黑客都是怎样炼成的，黑客应该怎么去做了……

1.1.2 黑客时代

从1945年起，电脑作为一门新兴的科学吸引了大量的世界上顶尖的程序员，他们使用机器语言、汇编语言，以及很多古老的语言编写着程序，这些人对电脑硬件与软件了如指掌，此时的“黑客文化”已经开始涌现，黑客文化带来的不是破坏，而是积极地推进电脑的发展，一些编程语言、软件开发和硬件设计中都有着黑客的参与。

当Internet形成全球化趋势时，丰富的资源吸引着大量的黑客，他们把越来越多的精力放到了研究系统内核和寻找各种各样的系统漏洞上。此时，绝大多数的黑客喜欢利用技术让各种系统在性能等方面得到提升，并且把研究成果公布出来免费提供给软件厂商等，这样可以把安全隐患有效降低，他们恪守这样一条准则：“Never damage any system”（永不破坏任何系统）。Linux等系统就因不断得益于很多黑客的不懈努力，才能有今天的非凡成就。

但是，与此同时也有少数的黑客喜欢把漏洞公开化，从而让黑客技术产生了初期的破坏性和负面性。这样，黑客（Hacker）与骇客（Cracker）的区分就出现了。到了后来，黑客（Hacker）与骇客（Cracker）的所作所为区别更加明显——骇客干脆就是以破坏为主、将技术商业化（别人指定一个目标并付款，他们就去完成相应的任务）。

当然，无论是黑客还是骇客，都是具备高超的电脑知识的人，即使要达到骇客的水准其实也是不容易的。实际上，很多黑客或骇客都已经以此为谋生手段了，比方说很多黑客都高薪受聘于网络公司，并提供相对安全、有效的防护措施。

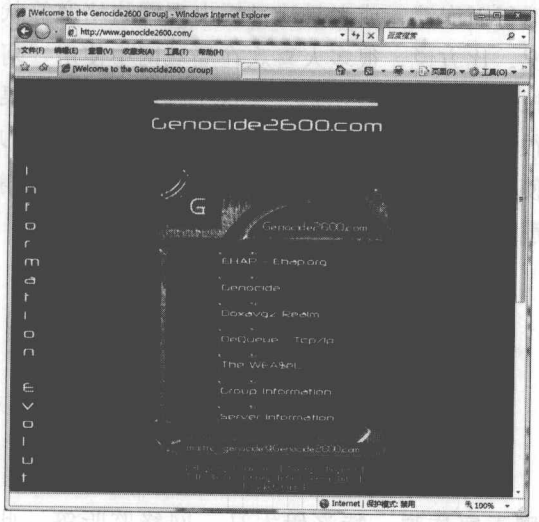
其实，黑客并不是只对网站或是电脑进行破解，比方说挪威黑客组织“反编译工程大师”，就在1999年11月破解了DVD版权保护的解码密钥，该组织编制了一个DVD解码程序公布在互联网上供免费下载。

1.1.3 黑客传奇

如今的黑客已经很少是单枪匹马的作战了，在欧美等国有不少完全合法的黑客组织，黑客们经常召开黑客技术交流会——1997年11月，在纽约召开了首次世界性的黑客大会，有五千多人参加了会议，这标志着黑客组织已经发展到一个新阶段，黑客组织化、集团化的趋势已经成熟，黑客组织内的成员可以有效利用各自的特长进行合作式攻击，从而提高成功率。

当前，世界上著名的黑客组织有很多，“大屠杀2600”就是其中的佼佼者。它拥有高达150多万的成员。这个组织之所以叫做大屠杀2600，是因为它的创始人名叫大屠杀（Genocide)。在Genocide上大学一年级的时候，他和几个朋友参照一本名为《2600》的杂志介绍的做法，每周五7点举行一次见面会，谁在黑客技术方面有了新的了解，就讲出来给大家听。于是“大屠杀2600”这个组织就这么诞生了。

大屠杀2600的网址是http://www.genocide 2600.com/，这是一个访问量相当可观的黑客网站，很多杂志和书籍都对其进行了介绍，如图所示。



大屠杀2600中黑客云集，其中各行各业的人士都有，甚至还有保护它的律师。如果你的英文够棒，那么建议经常访问这个网站，将会受益匪浅。

黑客不仅作为一种技术现象，更作为一种文化，已经在网络世界里发展了几十年，并且深深地扎下了根，可以说黑客是伴随电脑工业的发展而产生和演变的。可以预料，在今后相当长的一段时期内，它还会继续发展下去。如果想要靠打击、封杀来消灭黑客是不可能的，只有充分了解黑客、认识黑客才能真正把黑客引向正途，让黑客技术为国家、社会服务。

1.2 黑客技能

怎样才能做一名黑客呢？黑客都常用哪些“绝招”来“攻城掠池”呢？很多人由于对电脑安全防御和黑客入侵原理缺乏必要的了解，常常被黑客攻击了都还蒙在鼓里。因此，本节将一些常见的黑客攻击手段作个简单介绍。

1.2.1 应该具备的技能

如果想做一名够格的黑客，至少需要具备如下技能：

◆ 对网络上常见的操作系统有着深入的研究，如Windows XP、Windows Server 2003、Unix等。

◆ 应该熟悉TCP/IP网络协议的运作流程。

◆ 至少应熟悉Windows 2000及以上系统版本的DOS命令。

◆ 能熟练使用一种网站开发语言，如ASP。

◆ 应经常收集系统和网站漏洞资料，并有使用心得记录。

◆ 熟悉各种实用的黑客工具。

◆ 懂得常见操作系统的安全配置。

◆ 熟练掌握网站开发时的安全设计。

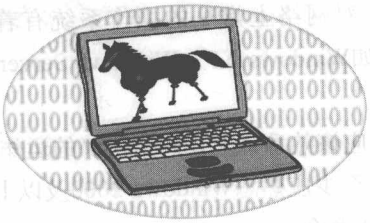
1.2.2 常用的黑客手段

在网络不断走向高速化的今天，全球网民的总量天天都在猛增，安全配置不同的各种电脑、安全意识高低不同的各类用户，都给黑客提供了不可计数的“练兵场”。因而，黑客可以实施的手段呈多样化。

1. 木马与病毒

木马全称为“特洛伊木马”，其名源于古希腊神话。传说古希腊人围困特洛伊城，久攻不下。后来想出了一个妙计，让一些死士躲进巨大的木马中。大部队假装撤退而将木马摈弃于特洛伊城下，让敌人将其作为战利品拖入城内。夜晚特洛伊人正在觥筹交错、庆祝胜利的时候，木马内的士兵乘机爬出来，与城外的部队里应外合而攻下了特洛伊城。

在计算机安全领域中，之所以将一种由服务器端和客户两部分组成的程序叫做“特洛伊木马”，是因为其服务器端在通过种种欺骗（伪装）的方法进入被入侵主机后，可以悄悄地打开系统的一扇门（端口），这样其客户端就可以立即与其相连接，从而一举攻下系统的完整控制权。



木马一般有两种功能，一种是利用此类程序潜入用户电脑，窃取所需要的数据。二是利用在目标电脑中植入服务器端后，黑客在自己的电脑中通过客户端进行鼠标、文件管理等操作。

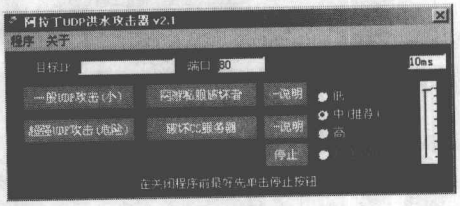
自1988年以来，千奇百怪的计算机病毒有如一场瘟疫迅速传遍了全世界，在步入网络时代后，层出不穷的病毒所带来的危险更是无时不在！“计算机病毒”与医学上的“病毒”有着本质的区别，它不是天然存在的，而是某些计算机程序员利用计算机软、硬件所固有的脆弱性，编写的具有特殊功能的程序。由于它与生物医学上的“病毒”同样有传染和破坏的特性，因此这一名词是由生物医学上的“病毒”概念引申而来。

从广义上定义，凡能够引起计算机故障、破坏计算机数据的程序均可统称为计算机病毒。依据此定义，诸如逻辑炸弹、蠕虫等均可称为计算机病毒。其实正规的病毒定义还是应该根据《中华人民共和国计算机信息系统安全保护条例》来解释。《条例》明确指出：“计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。”此定义具有法律性、权威性。

由于木马程序已经不再是纯粹的远程控制端，而是具有和病毒一样的“潜伏、传染、破坏”等特性，所以杀毒软件现在将木马也归类到了病毒一列中。

2．洪水与炸弹

“洪水”和“炸弹”几乎就是一回事，即通过发送大量的垃圾信息让目标负载超负荷运行而崩溃，或者是让目标出现网络堵塞等状况。比方说，很多人喜欢在局域网中使用“阿拉丁UDP洪水攻击器”，这个程序的攻击效果很好，能轻易地让Windows XP系统出现CPU使用率达到72-99%的现象，从拖慢直至系统崩溃，甚至连防火墙也对其无可奈何。



常见的炸弹攻击有邮件炸弹、逻辑炸弹、聊天室炸弹、特洛伊木马、网络监听等。此外，拒绝服务攻击（也叫分布式D.O.S攻击，Distributed Denial Of Service）也是一种常用的炸弹式攻击。所谓“拒绝服务”就是用超出被攻击目标处理能力的海量数据包来消耗目标的系统可用资源（如带宽资源），致使目标网络服务瘫痪。它的攻击原理是这样的：

攻击者首先通过比较常规的黑客手段侵入并控制某个网站之后，在该网站的服务器上安装并启动一个可由攻击者发出的特殊指令来进行控制的进程。当攻击者把攻击对象的IP地址作为指令下达给这些进程的时候，这些进程就开始对目标主机发起攻击。这种方式集中了成百上千台服务器的带宽能力，对某个特定目标实施攻击，所以威力惊人，在这种悬殊的带宽对比下，被攻击目标的剩余带宽会迅速耗尽，从而导致服务器的瘫痪。

3．密码破解

只要上网冲浪，那么就少不了一系列的密码：拨号上网需要密码，收取电子邮件需要密码，进入免费电子信箱要密码、进入网络社区也要密码，使用QQ还是离不开密码……对于黑客来说，进入一台电脑的系统，同样也需要密码，所以破解系统管理员密码就成了骇客们喜欢做的事情了。密码破解一般有暴力猜解和键