第 16 卷第 4 期,增刊　　广西科学院学报　　Vol. 16, No. 4 & Supplement
2000 年 11 月　　Journal of Guangxi Academy of Sciences　　November 2000

计算机网络黑客攻击技术探析

On the Techniques of Hacker Attacking Computer Network

荣京东　　田 梅
Rong Jingdong　　Tian Mei

(桂林陆军学院　桂林　541000)
(Guilin Military College, Guilin, 541000)

摘要　从分析、研究黑客的特征入手，进而对黑客入侵计算机网络的攻击技术，其中特别就攻击目标、攻击层次、攻击策略、攻击方法、攻击工具等作了系统全面的探析。

关键词　网络　黑客　攻击技术
中图法分类号　TP 393.08

Abstract　The characters of hackers and their techniques of invading network such as exploring the objects、hierarchy、strategy、measures and attacking tools are discussed.

Key words　network, hacker, attacking techniques

计算机网络连接形式的多样性、终端分布的不均匀性、网络的开放性以及网络的互联性，致使网络易受黑客、怪客、恶意软件和其他不轨行为的攻击。近年来，黑客对计算机网络的攻击，给用户造成了极大的损害。面对黑客日益严重的威胁，我们除了应当消除恐惧心态去勇敢地面对挑战外，还必须掌握科学的方法和技术。只有掌握足够的计算机网络技术，我们才能有效的抵御黑客的进攻，维护计算机网络的安全。

1　黑客攻击技术

任何以干扰、破坏网络系统为目的的非法授权行为都称之为网络攻击。防止黑客的入侵，应先从分析黑客的特征入手，全面熟悉黑客入侵计算机网络的技术手段，从而实现计算机网络的安全。

1.1　黑客特征

黑客(hacker)这个词刚出现时，指的是那些尽力挖掘计算机程序的最大潜力的电脑精英。最早的黑客都是计算机高手、大名鼎鼎的计算机科学家，而用黑客技术犯罪的叫骇客(cracker)。但现在人们都已不再去区分什么是“黑客”(hacker)，什么是“骇客”(cracker)，

2000-08-27 收稿。

都用“黑客”这个名词来代表计算机网络的入侵者。黑客一般具有下述特点：

（1）能用C、C++或Perl进行编码。因为许多基本的安全工具都是用这些语言编写的。至少能正确地解释、编译和执行这些程序，才可能形成攻击能力。

（2）具有把专门为某特定平台开发的工具移植到黑客自身所使用的平台上的能力，同时还可能具有开发出可扩展的工具，如SATAN和SAFEsuire的能力。

（3）对TCP/IP有透彻的了解。这是任何一个黑客所必须具备的，不十分熟悉TCP/IP协议本身，形成攻击能力是不可能的。

（4）对网络的操作系统，如UNIX操作系统和Windows NT操作系统有深入的了解，其中之一无可置疑的是UNIX/VMS。具有丰富的网络经验，从事系统管理或系统开发的工作，并具备了一些开发客户机/服务器应用程序的经验者。

（5）对经典的、老的、过时的计算机软件感兴趣。实际上许多老的应用软件能执行一些它们的替代品所不能实现的任务，随着其自身攻击经验的增长，收集的这些老的应用工具可能在攻击的过程中发挥奇特的功效。

1.2 攻击目标

黑客一方面可以威胁计算机网络中的信息，另一方面又可以威胁网络中的硬件设备，造成网络中的硬设备破坏性的损害，使设备无法正常工作。对网络中信息的威胁有两种方式：一是主动攻击，它以各种方式有选择地破坏信息的有效性和完整性；二是被动攻击，它是在不影响网络正常工作的情况下，进行截获、窃取、破译以获得重要机密信息，导致机密数据的泄露。我们都知道，网络软件不可能是百分之百的无缺陷和无漏洞的，实际上，网络应用程序、网络操作系统甚至连网络通信所依赖的协议TCP/IP也都存在着一个又一个安全漏洞，这些漏洞和缺陷恰恰是黑客进行攻击的首选目标。另外，软件设计编程人员为了自己方便，在编写软件时自行设置了“后门”，这就是人们所说的“系统漏洞”，一般不为外人所知，但一旦被黑客入侵，“后门”洞开，其造成的后果不堪设想。

黑客的目的是入侵网络的操作系统，或者是联结在网络上的主机的操作系统。UNIX操作系统目前而且可能在相当长的一段时间里都是Internet中的重点，对于一般以攻击Internet服务器系统为主要目标的黑客来说，首选UNIX操作系统。长期以来，一般人员很少接触到UNIX主机，加上UNIX系统价格昂贵，个人无力购买，所以通常能熟练掌握UNIX操作系统的人员较少。但是，随着免费的Linux系统以及FREE BSD系统，也就是UNIX系统的变种的出现，特别是Linux系统作为一种源码开放的系统，为黑客深入了解系统内核提供了极大的便利。Windows NT作为一种容易操作，便于管理的操作系统在Internet网中已开始占据着明显的位置，随着DEC和Microsoft之间达成的协议，Windows NT将变得更流行，许多黑客知道他们必须精通此平台，而Windows NT系统本身的漏洞以及漏洞带来的致命性问题，足以成了黑客最喜欢下手的对象。

1.3 攻击层次

网络的深度通常用“敏感层”这个概念来表示，敏感层本身按网络层次的深度又分为6层。

第1层：邮件炸弹攻击和服务拒绝攻击两种。处在第一层的各种攻击一般是互不相干的，这些攻击的目的只是为了干扰目标的正常工作，拒绝服务发生的可能性很大。

第2层和第3层：本地用户获得非授权读访问和本地用户获得非授权文件的写权限。受到这两种攻击所造成的危害程度，主要是看究竟哪些文件的“读”或“写”的权限被盗窃来

决定。如果本地用户获得了访问 /tmp 目录的权限，那么问题就变得更加严重，因为这可能使本地用户获得“写”权限，从而将第二层攻击推进至第三层攻击（甚至这样继续下去）。此情况主要适用于 UNIX 和 Windows NT 环境。在访问控制的环境中，存在着 2 个和权限有关的关键问题，一是部分配置错误；二是软件内固有的漏洞。每个问题都可能促使第 2 层攻击发展成为第 3、4 或 5 层攻击。当你对权限方案了解不透彻时，部分配置错误这一问题可能会出现，而软件内固有的漏洞问题会比你想象的更为常见，实际上它会出现在任何时候。

第 4 层：远程用户获得非授权的帐号和远程用户获得特权文件的读权限。这一层次的攻击通常涉及到“外人”非法获得访问内部文件的权利。获得的访问权限各不相同，有些只能用于验证某些文件是否存在，有些能读文件。第 4 层攻击还包括远程用户（没有有效帐号的用户）利用一些安全漏洞在你的服务器上执行数量有限的几条命令。

第 5 层和第 6 层：远程用户获得特权文件的写权限和远程用户获得根权限。这两层攻击都是利用了那些不该出现的漏洞。任何第 5、6 层攻击都是致命的。在此级别上，远程用户有读、写和执行文件的权限（通常黑客需要综合使用一些技术才能达到这个阶段）。值得庆幸的是，如果你已杜绝第 2 层、第 3 层和第 4 层的攻击，那么，第 5 和第 6 层攻击几乎不可能出现的，除非是利用软件本身的漏洞。

1.4　攻击的策略

第 1 阶段：获取一个登录帐号。

对 UNIX 系统进行攻击的首要目标是获取一个登录帐号与口令，黑客试图获取存在/etc/passwd 或 NIS 映射中的加密口令拷贝。一旦他们等到这样一个口令文件，他们可以对其运行 Crack 并可能猜出至少一个口令，尽管策略指导与系统软件努力强化使用好的口令选择，但却往往难以做到。黑客登录目标系统的做法是：首先，收集关于存在于不同 UNIX 产品上的安全漏洞信息以及扩大这些漏洞的方法。然后，收集关于目标组织中计算机系统与网络的信息。最后，利用脆弱点获得机会并努力登录进入系统。

第 2 阶段：获取根访问权。

攻击的第 2 阶段不一定是一个网络问题。黑客会试图扩大特定 UNIX 系统上的已有漏洞，例如试图发现一个 set-uid 根脚本，以便获取作为根运行的能力。一些网络问题，像未加限制的 NFS 允许根对其读与写，这可以被用来获取根访问权。

第 3 阶段：扩展访问权。

黑客拥有根访问权后，这个系统即可被用来攻击网络上的其它网络。通常的攻击方法包括对登录守护程序作修改以便获取口令（ftpd、telnet、rlogind、login）、增加包窥探仪以获取网络通信口令，并将它们返回给黑客自己，同时还伪装成试图利用受托关系来获取访问权的攻击。通常，一旦黑客控制了你的系统，你几乎无计可施。一个入侵高手可以轻易地通过修改记帐与认证记录抹去其痕迹。一些专业黑客甚至设计了自动程序，完全隐藏他们的行踪，一个流行的版本是 rootkit，这个软件包与 ps、ls、sum、who 等文件一起发布，系统管理员不能肯定二进制的完整性，因为 sum 命令给出的是感染过的信息。类似地 ps 命令不能显示黑客运行的程序。

1.5　攻击方法

1.5.1　程序突破法

利用 UNIX 系统的某些具有超级用户 SID、UID 等权限的应用程序和一些系统漏洞，利

用 C 语言开发一些突破程序，使自己成为超级用户。这种方法需要有很强的 C 语言功底。

1.5.2 密码破解法

使用密码破解法的先决条件是取得系统的密码文件。大部分的系统都对其密码文件进行了 SHADOW 处理，对于看不到的 SHADOW 密码。获取的方法有：

（1）利用系统管理员的失误。系统管理员经常对系统的重要文件进行备份，但在备份时忘记了文件权限的限制，找到这些文件也就找到了密码文件。

（2）利用系统安全漏洞。某些系统在安装后忘记安装了 PATCH，因此系统便留下许多后门，利用这些后门我们可以轻松获得这些文档。可以通过查阅 Internet 安全委员会公布的系统 BUG 和安全补救措施来克服这些安全漏洞。

（3）某些系统工具的错误文件。例如 Solaris 的 FTPD 进程产生的 CORE 文档，WWW 服务器可以抓取密码文件等。

（4）编程的方法。通过利用语言工具将 SHADOW 文件进行转换。

1.5.3 信息截取法

这种方法要求比较高，利用软件和硬件工具时刻监视系统主机的工作，等待用户登陆，记录登陆信息，从而取得用户密码。

1.6 攻击工具

1.6.1 扫描器（系统安全评估工具）

一种是普通扫描器，它是 UNIX 网络应用程序。具体来说是将已知的系统漏洞写入程序，运行后它会搜索某一地址的站点，如果该站点存在某些已知的漏洞，则扫描器最后的报告中会告知你。那么，一名黑客就可以尝试对这些已知的漏洞发动进攻。

另一种是 TCP 端口扫描器。它可以选择 TCP/IP 端口和服务（如 Telnet 或 FTP），并记录目标的回答。用这种方法，扫描器可以轻松地在浩瀚的信息网上快速地找到攻击目标，并同时在对目标主机的分析过程中发现其潜在的漏洞。对于黑客来说，高效、准确的提供网上攻击目标，扫描器无疑是最好的工具。常见的几种 UNIX 平台下的扫描器：NSS（网络安全扫描器）、Strobe（超级优化 TCP 端口检测程序）、SATAN（安全管理员的网络分析工具）、CONNECT、Jakal、IdentTCPscan、FSPScan、XSCAN 等。常见的 Windows 平台扫描器：国人编写的 PROXY HUNTER。还有集 HITP 代理服务器的搜索和验证功能于一身的“代理猎手”。

1.6.2 口令攻击器

合法的口令，是阻挡黑客入侵网络的第一道防线。UNIX 系统采用的是 DES 加密技术，使黑客无法得到真正的口令明文。其加密过程大致分 3 步：一是以明码正文形式取出口令；二是把口令作为关键词，用一系列的“0”进行屏蔽加密；三是把一个 64 位二进制值转变成为以 56 位为变量基础的唯一的 64 位二进制值，作为关键字再加密。黑客要想进入系统，首先必须破解口令，破解口令的方法有。

表 1 密钥长度与穷举时间

密钥长度（bits）	穷举时间
40	78 s
48	5 h
56	59 d
64	41 a
72	10696 a
80	2738199 a
128	770734505057572442069 a

1.6.2.1 穷举法

一般黑客在找不到更有效的攻击方法的情况下，才采用穷举法来破解口令的。这是因为 56 位关键字可以组成 7×10E16 种不同状态的密码，而实际上使用 56 位关键字以上的密码作为密钥的可能

性更大。经测试，利用穷举法破译 DES 加密的口令，估计所需的时间见表 1。

可见，利用穷举法破译 DES 加密的口令尽管是可能的，但是从表 1 中可以看到，其所耗费的破译时间对于黑客来说，也仅仅是一个理论上的方法，而无法付诸实施。

1.6.2.2　比较法

利用比较法破译 DES 加密的口令，其具体步骤是：一是获得一个字典文件，它是一个单词表；二是用用户的加密程序加密这些单词（符合 DES 标准）；三是把每个单词加密后的结果与目标加密后的结果进行比较，如果匹配，则该单词就是加密关键字。

1.6.2.3　其它口令破译法

前面介绍的破译法都有一个前提，那就是必须获得在/etc 下的 passwd 文件。因为在 UNIX 系统中，用户的基本信息，如用户名以及经 DES 法加密后的用户的口令等，都专门存放在 passwd 文件中。但是，这个文件有时根本无法得到，那么就需要用其它方法来获取用户的口令，其中一个常用的方法就是利用 E-mail 进行口令破译。因为我们国内许多 ISP 提供给用户的口令和其 E-mail 信箱的口令是一致的。软件“网络刺客”，就是用这种方法攻击用户口令的。至于用户名的获取有 2 种方法，一是获取 passwd 文档而得到用户名；二是可根据国人建立用户名的通常习惯，构建出一个文档（比如说，很多人都习惯用自己姓名的拼音缩写，定义为自己的用户名，根据这一不成文的规律，很容易用一个程序构建一个用户名文档），然后再用比较法获取用户名。

至于黑客对 Windows 环境下的口令进行攻击方法更多，手法也更加简单，因为 Windows 进行加密所使用的密钥相当弱，一般用穷举法就可以成功的破解。因此，在 Windows 环境下使用口令，最好不要用保存口令的有关选项。否则，黑客非法获取你的口令是很容易得手的。

1.6.3　特洛伊木马

“特洛伊木马”这类程序提供给黑客几乎是无限的权限，是其在对方不知晓的情况下，控制对方的计算机系统。特洛伊木马出现的时机有几种，一是在黑客想借木马夺取某些权限或获取信息时出现；二是系统被攻破后，为方便日后进入系统而设下各种机关。它可以出现在已经编译过的程序中，也可以出现在系统管理员需要执行的系统命令中，甚至可以作为消息的一部分发送；三是一些邮件头允许用户退到 shell 并执行命令。这一特性使邮件在被阅读时激活，黑客利用它便能给终端发送特定消息。在终端存储一个命令系列并且执行它。目前黑客常用的几种特洛伊木马有：远程访问型特洛伊木马、密码发送型特洛伊木马、键盘记录型特洛伊木马、毁坏型特洛伊木马 、FTP 型特洛伊木马。

1.6.4　拒绝服务攻击、网络监听

拒绝服务就是让服务器的 CPU 过载、磁盘饱和、内存不足等等，总之能使受害者的电脑动弹不得的行动，都称之为拒绝服务攻击。

网络监听，是当信息以明文形式在网络上传输时，将网络接口设置为监听模式，安个窃听器，就可以将网上传输的信息截获。

1.6.5　安全“后门”与堆栈溢出

安全“后门”是黑客为了不引起管理员的注意，能躲过日志使自己重返被入侵系统的技术。“后门”的设置，主要是为了实现如下目的：一是保证在管理员改变密码以后，仍然能再次侵入；二是使再次入侵被发现的可能性减至最低；三是利用脆弱性重复攻破机器。我们讨论“后门”时都是假设入侵的黑客，已经成功地取得了系统 root 权限之后的行动。

黑客在取得目标主机的信息之后，用一段程序代码上传并编译运行，造成堆栈溢出来破坏堆栈，用以达到使目标主机无法运行的目的，这是黑客们经常采用的一种手段。

1.6.6 毁灭性工具

E-mail 炸弹 除了对个人的危害之外，还将大规模地浪费网络资源，甚至有可能造成服务器瘫痪等严重后果。由于邮件炸弹具有构造简单、攻击简便（只要知道对方邮件地址便可投放）、以及毁坏性大的特点，E-mail 炸弹目前堪称是最令上网人头疼的事情。

ICQ 炸弹除了具有 E-mail 炸弹的功能外，还有一些强行加入列表、查询密码、泄露目标对象的 IP 地址等功能。因此，使用 ICQ 是一件具有潜在危险的事情，应当提醒人们注意千万不要在一台存储机密信息的计算机上运行 ICQ，否则，极有可能为你所使用的计算机招来“杀身”之祸。

NUKE 工具及端口攻击

NUKE 程序是利用一个叫做 OOB(Out Of Band 的缩写)中的 BUG 产生的。OOB 是 TCP/IP 的一种传输模式。只要向对端的 Windows 95/NT 传送 0 Byte 的数据包就可以导致对方的机器陷于瘫痪。目前比较有名的是针对 Windows 95/NT 进行攻击的 WINNUKE 程序。除了 NUKE 工具之外，另外还有许多可以导致系统无法正常进行网络工作的工具，把这一类称之为端口攻击。比较著名的有通过 TICMP ECHO（即类似 PING）“杀死”系统等，在北约对南斯拉夫空袭时，北约的网站就曾经遭受过这样的袭击。

病毒在黑客手里，既可以被利用达到其入侵系统的手段（如“特洛伊木马”实质上就是一种病毒），也可以被用于作为直接破坏网络通信的方法（如“蠕虫”、“美丽杀”病毒等），甚至可以作为直接破坏计算机系统的工具（如“CIH”病毒等）。因此，病毒是黑客手中最经常、最有效、最具有破坏力毁灭性工具。

2 结语

上面，我们从分析、研究黑客的特征入手，就黑客入侵计算机网络的攻击技术进行系统、全面的探析，了解了黑客在入侵计算机网络时，所选择的攻击目标、攻击层次、攻击策略、攻击方法以及攻击工具等。进而全面熟悉和掌握了黑客入侵计算机网络的技术手段。正如《孙子兵法》所说：“知己知彼，百战不殆”。如果，我们能够对威胁网络安全的各种根源分析清楚，那么，在现实的网络安全战中我们就会立于不败之地。

参考文献

1 Cheswick W R, Bellovin S M. Firewalls and Internet security: repelling the wily hacker. 北京：机械工业出版社，2000. 4.

2 胡昌振，李贵涛等. 面向21世纪网络安全与防护. 北京：希望电子出版社，1999. 10.

3 李 冬. 挑战黑客宝典. 北京：人民邮电出版社，2000. 1.

4 黑客攻防技巧大全. 北京智胜伟业科技发展有限公司出品. 金版电子出版公司出版，2000. 6.

（责任编辑：蒋汉明）