网络信息战的工具和技巧

续 敏 （山东曲阜师范大学电教系 273165）

摘要：〖HTK〗计算机网络安全越来越受到人们的关注。本文分析一些用于攻破联网的计算机系统或检测已联网的计算机系统安全性的技巧和工具，通过剖析一个攻击实例，主要是针对TCP/IP网络的UNIX主机为主，以期对有关的网络安全需要提供参考。

关键词：计算机网络安全 主机 防火墙 工具

1 引言

多年来，计算机系统一直遭受黑客的多种方式的入侵，计算机系统安全已经成为一个严重的、亟待解决的问题。现在整个计算机界，商业界、工业界，都在致力于解决计算机网络系统的安全性问题，黑客和计算机安全专家在同时研究着软件工具，包括如何入侵计算机系统和如何检查出一个计算机网络系统中的潜在的安全问题。本文从计算机黑客攻击网络系统的工具和技巧入手，通过剖析一个攻击实例，拟对网络安全需要提供有关参考。

2 已成功使用的入侵工具

对已经被成功攻击的计算机系统做检查，我们发现一些特定的模式。从被攻击系统和入侵者的计算机系统所得到的数据来看，不同的入侵者在如何选择和攻击他们的牺牲品方面存在很多相似性。许多用于进行攻击的组件都是通过使用复杂、高级的软件包来自动、方便地实现的。下面我们将对一些由黑客成功使用的入侵工具进行分类。根据不同的功能，本文把这些工具和技巧分为五类：

扫描器

远程攻击工具

本地攻击工具

监视工具

隐藏工具

2.1 扫描器

扫描器是一个用于获得一个主机或网络信息的工具。一般来说，这些工具是一些脚本的松散组合，由与安全有关的系统管理员或系统的攻击者开发或组织，用于探测网络并且汇报与安全有关的信息。扫描器可以进一步分为两个基本类型：网络审计工具和基于主机的静态审计工具。网络审计工具用于浏览一个远程主机或一个网络上的一系列主机，然后汇报每个主机与安全有关的弱点。基于主机的静态审计工具用于浏览一个本地主机，然后汇报它的安全弱点。

2.1.1 网络审计工具

比较著名的如：

Internet Security Scanner(ISS)，在这个软件包中包含了许多常用的安全测试方法。

Security Analysis Tool for Auditing Networks(SATAN)，在ISS的基础之上，通过增加了更多的测试方法，从而具有更强大的功能。SATAN被设计成可移植的，可以运行在许多不同的平台之上。SATAN简单易用，其结果导致了好奇的用户和特意的系统入侵者大量使用，造成了对大量计算机系统的非授权的浏览。作为对于SATAN的反应，系统管理员开发了可以检测到SATAN攻击的软件。Courtney就是一个浏览检测器。

现在，系统管理员和系统入侵者都有许多免费和商业上的网络安全审计软件包可以选择。这些软件包有一个共同的目标：查处并且汇报网络安全弱点或漏洞。例如，SATAN将浏览一定范围内的主机网络地址，并且汇报下列信息：

网络上有响应的（可以通信的）主机

在响应主机上的可用的服务

通过网络文件系统（NFS）支持的共享磁盘

通过网络信息服务（Network Information Service，一个分布式的共享信息数据库）提供的文件访问

远程执行的可能性

邮件系统的弱点（如Sendmail的有些版本可以被欺骗以用于执行恶意的命令）

简单文件传输协议TFTP的访问和配置（可以用来下

载口令文件）

远程命令解释器的访问（提供了在另外一个系统上不需输入口令就可以执行命令的能力）

无限制的自由的X窗口系统(任何一个人都可以连接到这个服务器从而侦察它的用户)

可读/写的FTP目录（允许任何一个用户上载商业软件或者色情的资料）

如果SATAN汇报了上述特征的存在，那么哪个系统，进一步到哪个网络，是容易受到外部攻击的。这些类型的问题对于黑客家族是众所周知的，并且利用它们的工具是很容易得到的，例如可以通过WWW，匿名FTP，秘密的BBS等，许多用于突破网络安全防范的工具也可以由Web搜索引擎轻松得到。

2.1.2 基于主机的静态审计工具

这是另外一种被安全团体所使用的扫描器。起初，这些工具是被用于加强本地系统的安全性，现在也被黑客用于获得非授权的特权访问。COPS软件包就是一种浏览本地系统的各类脚本的集合，用于找出并汇报安全弱点。TIGER工具包扩展了COPS的思想，增加了更多更强大的功能。所有这些工具执行详尽的系统检查，汇报下列系统弱点：

关于文件、目录、设备的访问许可问题

容易猜测的、简单的口令

安全性很差的口令文件或组定义文件

众所周知的易受攻击服务，例如匿名FTP配置，没有正确配置的服务

一些关键文件，特别是二进制文件，是否已经受到攻击

对于黑客和系统管理员，静态审计器都是一个很有价值的工具。如果黑客能够获得系统非特权的帐户，本地扫描器将指出存在于主机中的可以达到未授权的特权访问常见的安全弱点。

2.2 远程攻击工具

远程攻击工具是一个程序，或者说是一个方法，可以被一个没有帐户的人员利用来渗透入一个远程计算机系统。对远程攻击工具不利的因素是防火墙和网络审计工具的发展。防火墙可被定义为一个或一组用于两个网络之间加强访问控制策略的系统。防火墙通过定义它所提供的外部服务、隐藏内部网络信息来保护内部网络。当能够正确配置和维护一个防火墙时，防火墙能够减小内部网络对于外部网络的暴露程度，从而起到保护内部网络的作用。减少提供给外部网络的服务数目可以使内部网络所能受到的远程攻击器的攻击减少。

远程攻击是和网络中的计算机所提供的服务相联系的。绝大多数服务打开一个通信端口，然后在这个端口上侦听连接请求。以sendmail（一个处理电子邮件的程序）为例，这个程序打开一个通信端口，并且在这个端口上侦听从其他邮件服务器发来的连接请求。一个sendmail服务器接受一个使用SMTP的客户系统发起连接并与之相互通信。如果这个sendmail服务器存在一些可被用户定义的数据利用的安全漏洞，则该服务器所在的主机就容易受到在任一个与之有连接的系统上的用户的攻击。这就是为什么远程攻击器是最可怕和最危险的主要理由，因此也是在所有工具中作为最主要的防范对象。

一个远程攻击器的子类是基于协议的攻击器。协议攻击器是通过对TCP/IP协议族的操纵获得对目标计算机的非授权访问。TCP/IP具有许多可以被攻击的地方。例如：一个有敌意的主机（A）可以盗取另一台主机（B）的地址。如果一个目标系统（T）使用基于地址验证的协议来判断对方主机（B）的真伪，则有敌意的主机（A）就有能力假冒对方主机(B)的地址，然后以被信任主机(B)的身份与目标主机（T）通信。TCP/IP的一些易被攻击的弱点有：

会话抢夺

伪冒IP（IP spoofing，包括TCP和UDP）

路由信息协议（RIP）

ICMP

2.3 本地攻击器

本地攻击器是由具有帐户的用户为获得非授权权利而使用的一种工具。这个帐户可以是合法帐户，也可以是通过远程攻击器获得的，或者其他途径(例如与黑客的交易，从网络传输中获得)。大多数本地攻击器是利用特权程序软件设计或实现中的错误，这些程序允许一个非特权的用户执行具有特权的有敌意的命令，或者访问、修改特权数据。一旦特权访问权利被获得，黑客就控制的系统。在大多数UNIX系统中，入侵者能够修改系统日志来隐藏他们的非法活动，并且安装一个后门（backdoor）程序，这个程序可以使特权的、未被记录的对系统的访问继续。鉴于本地攻击器的危害性，有一些软件，如COPS，TIGER可以帮助系统抵御其攻击。

2.4 监视工具

一个监视工具允许使用者监视计算机系统、网络数

据。入侵者利用这些信息准备攻击其他的计算机系统。这些工具包括：

2.4.1 终端窥探器（Snooper）

终端窥探器通过终端或终端模拟监视用户的活动，进程的内存，记录用户的击键。通过观察该用户的行为，入侵者可以获得信息，然后利用这些信息攻击网络上的其他系统。

2.4.2 网络侦听器（Sniffer）

网络侦听器监视并且记录网络数据。通过一个主机的网络接口的网络数据包含了许多对于入侵者非常有用的信息，例如用户名和用户口令对。许多系统并不对要在网络上传输的数据进行加密。可以物理地访问网络的用户或黑客能在网络上插入一个网络侦听器，监视网络数据流量，获得足够的信息，从而能够访问网络上的其他系统。

2.5 隐藏（后门）工具

隐藏工具可帮助一个非法用户修改系统日志，删除所有与其活动有关的记录。隐藏工具包通常包含后门程序。后门程序一般替代系统中的一些重要的负责身份验证和系统汇报的程序。后门程序可以：

当其被激活时，提供继续的、未被记录的系统使用。激活机制通常是编译在程序中的加密的口令

隐藏可疑的进程和文件，不被用户和系统管理员发现

给用户和系统管理员汇报错误的系统状态

汇报被修改的程序的错误的校验码、长度等信息

3 各种工具的综合运用

掌握了以上这些工具，入侵者就可以对一个计算机网络进行攻击了。许多入侵者随机地选择一些目标进行攻击，并无明确的目的，只是处于好奇或智力上的挑战。然而，也有相当数量的攻击是由专门组织发起的，具有特定的目的的。

无论入侵者的目的如何，攻击总是以一种或几种手段的组合：

盲目的远程攻击

用户级攻击

物理级攻击

3.1 盲目的远程攻击

此种攻击者没有被攻击对象的合法口令，但是知道其网络地址。这是一种基本的攻击方式。利用目标系统的地址或名称，入侵者利用网络扫描器或其他方法获得与该系统安全相关的信息。在浏览和探测了系统的防御体系之后，入侵者从其工具包中利用合适的远程攻击器来对具有安全漏洞或弱点的系统服务进行攻击。如果成功，入侵者至少可以拥有被攻击系统的用户级访问权限。

3.2 用户级攻击

此时入侵者已经拥有了目标系统的用户口令，这个口令可能由多种途径得到，合法的或非法的。攻击的第一步是获得该系统和它的用户的信息。一个本地扫描器（如COPS或TIGER）可以用来监测或汇报一般的常见安全弱点和漏洞。在对本地系统进行过浏览之后，入侵者在利用合适的本地攻击器来攻击系统。如果成功，则入侵者将会拥有特权访问能力并可以对系统造成损害。如果一个节点被成功入侵，那么入侵者可以通过监视系统的本地数据或网络数据流动获得足够的信息，从而攻击与该节点相连的其他机器。

3.3 物理级攻击

如果入侵者可以在物理上和被攻击对象相连，则入侵者可以利用网络监视器监视和记录其网络数据流动。在监听到足够的信息之后，入侵者可以通过远程或本地获得对被攻击对象的访问权利。

在每种手段中，入侵者会执行一系列的、分步的操作。整个渗透过程可分为七个阶段：

(1) 侦察：获得目标系统或网络的相关信息

(2) 探测和攻击：探测系统的安全弱点或漏洞，并布置工具

(3) 获得立足点：利用系统的安全弱点，获得进入系统的入口

(4) 进一步发展：从非特权帐户到特权帐户

(5) 隐藏：擦除攻击痕迹，安装后门程序

(6) 建立侦听基地：在系统内获得并建立可以自由侦听的地位

(7) 控制并扩展：从一个主机扩展到网络上的其他主机

每种入侵方式将使用这七个步骤中的某些步。例如在盲目远程攻击手段中，入侵者至少使用前三个步骤。入侵者首先试图收集目标系统的相关信息（第一步）。然后，利用这些信息，入侵者使用远程攻击工具和技巧来试图获得一个立足点（第二步）。如果渗透企图成功并且这个立足点（第三步）是一个特权帐户，则入侵者可以立刻清除其所有攻击过程中所留下的痕迹，并且建立一个侦听基地（第五到第七步）。如果立足点不是一个特权帐户，入侵者还要利用本地攻击器扩大其权利，以获得特权用户（第四步）。一旦获得了特权用户，入侵者就可以实施进一步的

操作与攻击。

在用户级的攻击手段中，入侵者已经获得了进入网络的立足点（第三步）。

在物理级的攻击手段中，入侵者通过发现一个处于活动状态的会晤或重新启动系统来获得特权用户。如果入侵者利用网络监视器对物理网络进行监视，则得到的信息（第一步）可以被用作为突破系统的基础（一到七步）。具有对计算机系统和其网络硬件进行直接物理访问的能力很容易对系统造成危害。

4 攻击实例剖析

在下面的例子中，将具体描述如何使用这些工具和技巧，按照上述七个步骤来渗入一个目标系统。假设在开始渗入时，所知道的信息仅仅是该目标系统所在的公司名称，ABC。

4.1 侦察

入侵者想攻击ABC公司所拥有的计算机系统，于是通过Internet等手段来侦察与该公司有关的信息。如果该公司存在一个Internet连接，Web节点，FTP节点，或电子邮件服务，那么通过一个Web扫描器一般就能发现该公司计算机系统的域名。本例中设为abc.com。如果入侵者拥有了目标系统的域名，就可以利用各种手段获得更多的信息，获得该域上其他机器的一些信息。因为这些信息并不是保密的。

现在假设第一步已成功，从目标系统获得了一系列主机名和网络地址。现在，入侵者可以进一步获得目标系统有关用户的信息。两个与用户信息有关的主要信息源是Web和新闻组。用户列表是非常有用的，因为得到用户名之后，就可以利用多种手段取得或猜测用户口令。

在侦察阶段结束时，入侵者大致可以得到以下信息：主机名、主机地址、主机拥有者、主机机器类型、主机操作系统、网络拥有者、网络上的其他主机、网络配置、被网络信任的其他主机、网络外的主机、用户清单、用户名的分配策略，等等。

4.2 探测和攻击

现在，入侵者开始探测系统的潜在的安全弱点。这个阶段主要是自动完成的。扫描器（Scanner）将是主要工具。正因为这个阶段主要是自动完成，安全专家或系统管理员也可以利用这些工具来发现系统的潜在的不安全因素。SATAN和ISS是主要利用工具。它们将自动的收集和汇报远程主机和网络的安全弱点。当然，这个阶段对于入侵者来说也是最危险的。因为浏览和探测活动是很容易被入侵检测系统（如果安装的话）检测到并记录下来，然后提醒用户或负责安全的系统管理员。

通过一些工具（如strobe），远程主机提供了哪些远程服务是很容易检测的。知道了这些服务之后，可以进一步了解系统的安全弱点。

对主机提供的服务中比较感兴趣的有：FTP，SMTP，finger，WWW，printer，xterm，X Window System Server。现在，入侵者利用他的远程攻击器来对这些服务进行检查和利用。首先，FTP服务的所被知道的弱点和配置错误将被检查。接着，SMTP或sendmail服务将被探测，其服务信息中将包含机器名、软件版本号等。因为有许多邮件服务软件是存在漏洞的，所以如果系统提供假的信息或不提供有关信息，则入侵者的工作将变得更复杂，被检测到的可能性也就更大。每一个服务将被测试，直到发现一个潜在的安全弱点。我们假设除了WWW服务，所有的服务都是安全的。在host.abc.com主机上的WWW服务提供了易受攻击的phf服务，入侵者通过远程攻击器来利用它。

通过执行服务器上的一个命令，在入侵者的显示器上产生了一个X窗口系统的终端仿真。这样，入侵者在目标系统上就取得了一个立足点。

4.3 获得立足点

系统的安全弱点已经被利用了，此时系统已经受到的危害：入侵者已经可以活动对系统的访问权了。如果用户标识为超级用户，入侵者就可以直接进入隐藏阶段。如果不是，入侵者还需要从非特权帐户发展的特权帐户。

4.4 进一步发展

入侵者利用主机，操作系统，服务等信息，选择一个合适的本地攻击器。本例中，入侵者已经获得了远程系统的www帐户。现在，他可以使用本地浏览工具（COPS/TIGER）来搜索和汇报系统的配置错误和其他的安全弱点，然后利用本地攻击器。现假设在主机中使用的是AIX* 3.2（Advanced Interactive Executive），并且易受tprof攻击。由此，入侵者从www帐户升级到超级用户，进入下一个阶段。

现在，入侵者已经成功地获得了对系统的控制权。在大多数系统中，任何本地文件都可以被访问和修改。一些恶意的攻击者寻找一些他们感兴趣的数据，然后删掉整个文件系统。而大多数入侵者将保留对系统的访问权，进入下一个阶段：隐藏。

4.5 隐藏

当入侵者获得超级用户口令之后，因为他已经拥有访问一切本地文件的权利，所以入侵者能够编辑日志文件，擦除入侵时留下的痕迹。在这个例子中，入侵者检查WWW服务的访问记录，擦除其相关的非法历史记录。通过替代一些系统二进制代码，入侵者可以隐藏进程，文件信息，以及网络连接信息。

4.6 建立侦听基地

通过使用一些工具，入侵者在原来系统的一些重要程序中修改或增加一些功能，主要有三个目的。第一，保证将来的活动不被记录；第二，建立一些后门程序，保证将来可以继续访问该系统；第三，建立一个可以侦听网络的基地。这个侦听基地主要由一个具有特权用户权限的监听程序（如sniffer）来完成。如果不能侦听网络上的数据，则可以通过监视本地系统上的每个用户的活动，因为网上数据包含一些敏感信息，如用户名和口令对。通过记录这些信息，入侵者可以扩大他的控制范围。

4.7 控制并扩展

通过监视工具和一些本地或远程攻击器，入侵者可以攻击网络上的其他主机。从一个主机的一个安全弱点，入侵者现在可以扩大他的控制范围。通过在一系列主机上安装后门程序，入侵者可以避免检测，并且活动过程不被记录。通过侦听基地获得的口令提供了将来建立新的立足点的可能性。入侵者可以利用这些信息来攻击更多的机器，很快地扩充到整个网络。

5 结束语

随着各种组织、机构变得越来越依靠计算机网络技术，他们也变得越来越容易受到财政上和声誉上的损失。这主要是由于其计算机和通信系统安全性不够，经常受到非法入侵。目前在使用网络的绝大部分组织都存在着安全问题。因此，在安装网络系统的同时，应该特别注意安全问题，如果可能，应当安装安全预警系统，加强系统的安全性。例如，安装防火墙，减少外部攻击；对于内部网络，随机统计抽查各类数据，减低本地攻击。因为没有一个计算机系统是绝对安全的，所以，采取一些基本的预警措施是非常有效的，这样可以大大地降低被成功攻击的可能性。总之，网络安全问题应该引起我们足够的重视。■

参考文献

1 B. Violino and B. Davis, Security: Window of Vulnerability, Information Week, March 10, 1997

2 Vulnerability in NCSA/Apachi CGI Example Code, CERT Advisory CA98.06 June 4, 1999, ftp://info.cert.org/pub/cert_advisories/CA-98.06.cgi_example_code

3 C. Landwehr, et al., A Taxonomy of Computer Program Security Flaws, ACM Computing Surveys, Vol.26, No.3, 1994

4 H.Neil, The S/Key One-time Password System, UNIX Security Symposium V Proceedings, Milan, Italy, 1995