第 3 章


观看视频

攻击检测与系统恢复技术

本章重点：

(1) 网络攻击的原理、步骤，以及黑客攻击企业内部局域网的典型流程。

(2) 网络攻击的防范措施及处理对策。

(3) 入侵检测系统的组成、内容、特点及其数学模型。

(4) 入侵检测的过程。

(5) 异常检测、误用检测、特征检测，基于主机和基于网络的 IDS 各自的特点。

(6) 系统恢复技术。

计算机网络在不断更新换代的同时，安全漏洞也不断地被发现，即使旧的安全漏洞补上了，新的安全漏洞又出现了。网络攻击正是利用这些存在的安全漏洞和缺陷对系统和资源进行攻击。利用入侵检测系统可以检测出攻击者的入侵行为。如果发生了入侵，系统恢复就是必不可少的了。

入侵检测和系统恢复技术都已成为网络安全体系结构中的重要环节。

3.1 网络攻击技术

网络攻击的方法十分丰富，令人防不胜防。分析和研究网络攻击活动的方法和采用的技术，对加强网络安全建设、防止网络犯罪有很好的借鉴作用。

3.1.1 网络攻击概述

1. 攻击的分类

从攻击的行为来分，网络攻击可分为主动攻击和被动攻击。

(1) 主动攻击。包括窃取、篡改、假冒和破坏。字典式口令猜测、IP 地址欺骗和服务拒绝攻击等都属于主动攻击。一个好的身份认证系统(包括数据加密、数据完整性校验、数字签名和访问控制等安全机制)可以用于防范主动攻击，但要想杜绝主动攻击很困难，因此对付主动攻击的另一措施是及时发现并及时恢复所造成的破坏，现在有很多实用的攻击检测工具。

(2) 被动攻击。被动攻击就是网络窃听，截取数据包并进行分析，从中窃取重要的敏感信息。被动攻击很难被发现，因此预防很重要，防止被动攻击的主要手段是数据加密传输。

从攻击的位置来分，网络攻击可分为远程攻击、本地攻击和伪远程攻击。

(1) 远程攻击。指外部攻击者通过各种手段，从该子网以外的地方向该子网或者该子网内的系统发动攻击。远程攻击一般发生在目标系统当地时间的晚上或者凌晨时分，远程

攻击发起者一般不会用自己的机器直接发动攻击，而是通过跳板的方式，对目标进行迂回攻击，以迷惑系统管理员，避免暴露真实身份。

（2）本地攻击。指本单位的内部人员，通过所在的局域网，向本单位的其他系统发动攻击。在本机上进行非法越权访问，也是本地攻击。本地攻击也可能使用跳板攻击本地系统。

（3）伪远程攻击。指内部人员为了掩盖攻击者的身份，从本地获取目标的一些必要信息后，攻击过程从外部远程发起，造成外部入侵的现象，从而使追查者误以为攻击者来自外单位。

2. 攻击者与目的

（1）黑客与破坏者：主要出于挑战、自负、反叛等心理，目的是获取访问权限。

（2）间谍：主要为了获取政治、军事等情报信息。

（3）恐怖主义者：主要为了勒索、破坏、复仇、宣传等政治与经济目的，制造恐怖。

（4）公司雇佣者：主要为了竞争经济利益，也可看作是工业间谍。

（5）计算机犯罪：主要为了个人的经济利益。

（6）内部人员：主要因为好奇、挑战、报复、经济利益等原因。

攻击的目的主要包括：进程的执行、获取文件和传输中的数据、获得超级用户权限、对系统的非法访问、进行不许可的操作、拒绝服务、涂改信息、暴露信息、挑战、政治意图、经济利益、破坏等。

3. 攻击者常用的攻击工具

1）DOS攻击工具

如WinNuke通过发送OOB漏洞导致系统蓝屏；Bonk通过发送大量伪造的UDP数据包导致系统重启；TearDrop通过发送重叠的IP碎片导致系统的TCP/IP协议栈崩溃；WinArp通过发送特殊数据包在对方机器上产生大量的窗口；Land通过发送大量伪造源IP的基于SYN的TCP请求导致系统重启动；Flushot通过发送特定IP数据包导致系统凝固；Bloo通过发送大量的ICMP数据包导致系统变慢甚至死机；PIMP通过IGMP漏洞导致系统蓝屏甚至重新启动；Jolt通过大量伪造的ICMP和UDP导致系统变得非常慢甚至重新启动。

2）木马程序

（1）BO2000（BackOrifice）。它是功能最全的TCP/IP构架的攻击工具，可以搜集信息，执行系统命令，重新设置机器，重新定向网络的客户端/服务器应用程序。感染BO2000后机器就完全在别人的控制之下，黑客成了超级用户，用户的所有操作都可由BO2000自带的“秘密摄像机”录制成“录像带”。

（2）“冰河”。冰河是一个国产木马程序，具有简单的中文使用界面，且只有少数流行的反病毒、防火墙才能查出冰河的存在。它可以自动跟踪目标机器的屏幕变化，可以完全模拟键盘及鼠标输入，使在被控端屏幕发生变化且监控端同步时，被监控端的一切键盘及鼠标操作将反映在监控端的屏幕上。它可以记录各种口令信息，包括开机口令、屏幕保护口令、共享资源口令以及绝大多数在对话框中出现过的口令信息；还可以进行注册表操作，包括对主键的浏览、增删、复制、重命名和对键值的读写等所有注册表操作。

（3）NetSpy。可以运行于Windows 95/98/NT/2000等多种平台上，它是一个基于TCP/IP的简单的文件传送软件，但实际上可以将它看作一个没有权限控制的增强型FTP

服务器。通过它,攻击者可以悄悄地下载和上传目标机器上的任意文件,并可以执行一些特殊的操作。

(4) Glacier。该程序可以自动跟踪目标计算机的屏幕变化、获取目标计算机登录口令及各种密码类信息、获取目标计算机系统信息、限制目标计算机系统功能、任意操作目标计算机文件及目录、远程关机、发送信息等。类似于 BO2000。

(5) 键盘幽灵(KeyboardGhost)。Windows 操作系统的核心区保留了一定的字节作为键盘输入的缓冲区,其数据结构形式是队列。键盘幽灵正是通过直接访问这一队列,使键盘上输入用户的电子邮箱、账号、密码(显示在屏幕上的是星号)得以记录,一切涉及以星号形式显示出来的密码窗口的所有符号都会被记录下来,并在系统根目录下生成一文件名为 KGDAT 的隐含文件。

(6) ExeBind。这个程序可以将指定的攻击程序捆绑到任何一个广为传播的热门软件上,使宿主程序执行时,寄生程序也在后台被执行,且支持多重捆绑。实际上是通过多次分割文件,多次从父进程中调用子进程来实现的。

3) 分布式工具

攻击者分发攻击工具到多台主机,通过协作方式攻击特定的目标。

3.1.2 网络攻击的原理

随着 Internet 的发展,现代攻击已从以系统为主的攻击转变到以网络为主的攻击。攻击者为了实现其目的,会使用各种各样的工具,采用多种多样的攻击方法,甚至由软件程序自动完成目标攻击。攻击的方法不同,其原理也不相同。

1. 口令入侵

口令入侵是指使用某些合法用户的账号和口令登录到目标主机,然后再实施攻击活动。这种方法的前提是必须先得到该主机上的某个合法用户的账号,然后再进行合法用户口令的破译。

1) 获取用户账号的方法

获取用户账号的方法很多,有如下几种。

(1) 利用目标主机的 Finger 功能。当用 Finger 命令查询时,主机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。

(2) 利用目标主机的 X500 服务。有些主机没有关闭 X500 的目录查询服务,也给攻击者提供了获得信息的一条简易途径。

(3) 从电子邮件地址中收集。有些用户电子邮件地址常会透露其在目标主机上的账号。

(4) 查看主机是否有习惯性的账号。有经验的用户都知道,很多系统会使用一些习惯性的账号,造成账号的泄露。

2) 获取用户口令的方法

被用来窃取口令的服务包括 FTP、TFTP、邮件系统、Finger 和 Telnet 等。所以,系统管理员对口令的使用应十分小心、谨慎。下面简要介绍获取用户口令的三种方法。

(1) 通过网络监听非法得到用户口令。目前很多协议根本就没有采用任何加密或身份认证技术,如在 Telnet、FTP、HTTP、SMTP 等传输协议中,用户账号和口令都是以明文格

式传输的，攻击者利用数据包截取工具便可很容易地收集到用户的账号和口令。

还有一种中途截击攻击方法更为厉害，它可以在用户同服务器端完成“三次握手”建立连接之后，在通信过程中扮演“第三者”的角色，假冒服务器身份欺骗用户，再假冒用户向服务器发出恶意请求，其造成的后果不堪设想。

另外，攻击者有时还会利用假的登录程序来骗取其他人的账号和口令，若是在这个假的登录程序上输入账号和口令，它就会记下所骗到的账号和口令，然后提示输入错误，要求再试一次。接下来假的登录程序便自动结束，将控制权还给操作系统。

现在网络上出现了一个专门用来探测 NT 口令的程序 L0pht Crack，它能利用各种可能的口令，反复模拟 NT 的编码过程：利用单向散列(Hash)函数编码处理，并将所编出来的口令与存放在 SAM 数据库内的口令比较，如果两者相同，就表示得到了正确的口令。

(2) 在知道用户的账号后(如电子邮件@前面的部分)，利用一些专门软件强行破解用户口令，这种方法不受网段限制。例如，采用字典攻击法来破解用户的口令时，攻击者可以通过一些工具程序，自动地从黑客字典中取出一个单词，作为用户的口令，然后用与原系统中一样的加密算法(加密算法是公开的)来加密此口令，将加密的结果与文件中的加密口令比较，若相同则猜对了。因为很少有用户使用随机组合的数字和字母作为口令，许多用户使用的口令都可在一个特殊的黑客字典中找到。在字典攻击中，入侵者并不穷举所有字母、数字的排列组合来猜测口令，而仅用黑客字典中的单词来尝试。攻击者已经构造了这样的字典，不仅包括英语或其他语言中的常见单词，还包括黑客词语、拼写有误的单词和一些人名。已有的黑客字典中包括大约 20 万个单词，用来猜测口令非常成功，而对现代的计算机来说，几个小时就可以把字典里的所有单词都尝试一遍。LetMein Version 2.0 是这类程序的典型代表。

(3) 利用系统安全漏洞。

在 Windows/UNIX 操作系统中，用户的基本信息、口令分别存放在某些固定的文件中，攻击者获取口令文件后，就会使用专门的破解程序来解口令。同时，由于为数不少的操作系统都存在许多安全漏洞、Bug 或一些其他设计缺陷，这些缺陷一旦被找出，攻击者就可以长驱直入。

常见的“密码/口令文件”有如下三种。

① *.pwl：Windows 系统中的使用者的口令文件。一个 PW1 口令文件存放一个使用者的口令，这个口令可能是用户的电子邮件密码、企业内部网络(Intranet)密码、注册登录密码。只要用系统配置编辑程序查看目标计算机 C:\WINDOWS\System.ini 文件中的 PasswordLists 字段，即可知道目标计算机有哪些 PW1 口令文件。再将这些 PW1 口令文件下载到攻击者的计算机中，然后可以用 CAIN、Cracking 等软件来破解口令文件。

② Tree.dat、Smdata.dat、Sm.dat：不同版本的 CuteFTP 有不同的 DAT 口令文件。其中，Tree.dat 是 3.x 版以前的 CuteFTP 所使用的口令文件，Smdata.dat 是 3.x 版 CuteFTP 所使用的口令文件，Sm.dat 是 4.x 版 CuteFTP 所使用的口令文件。破解 Tree.dat 口令文件的方法：用 FireFTP 破解软件即可破解出 Tree.dat 口令，再将口令文件输出到文本文件(例如 passout.txt)中，就可以用文本编辑器(例如记事本)查看结果了。

破解 Smdata.dat、Sm.dat 口令文件的方法：必须用手动方式破解口令。首先进入 MS-DOS 模式，再用 LIST 查看口令文件。可以看出 1 表示 FTP 站名(明文)，2 表示 IP 地址

(明文),3 表示用户名(明文),4 表示口令(密文)。其中,口令的编码原理很简单,只要使用 ASCII 对照表,例如,a=┌,b=┐,c=V2,以此类推,攻击者只要找出每个字符(a～z)和数字(0～9)所对应的 ASCII 字符,就可以破解口令文件了。

③ system.dat 和 user.dat:Windows 登录文件里面包含攻击者感兴趣的重要资料,如某软件的注册序号等。当攻击者下载了目标计算机的 system.dat 和 user.dat 文件后,可以使用专门分析 system.dat 和 user.dat 等 Windows 登录文件的软件 RegistryAnalyzer 来分析登录文件。

RegistryAnalyzer 的分析步骤:运行 RegistryAnalyzer,选择 Open Registry file,选择所下载的登录文件,分析登录文件。

2. 放置特洛伊木马程序

特洛伊木马程序可以直接侵入用户的计算机并进行破坏,它常被伪装成工具程序或者游戏等诱使用户打开带有特洛伊木马程序的邮件附件或从网上直接下载,一旦用户打开了这些邮件的附件或者执行了这些程序之后,它们就会像古特洛伊人在敌人城外留下的藏满士兵的木马一样留在自己的计算机中,并在自己的计算机系统中隐藏一个可以在 Windows 启动时悄悄执行的程序。当用户连接到因特网上时,这个程序就会通知攻击者,并报告用户的 IP 地址以及预先设定的端口。攻击者在收到这些信息后,再利用这个潜伏在其中的程序,就可以任意地修改用户计算机的参数设定、复制文件、窥视用户整个硬盘中的内容等,从而达到控制用户计算机的目的。

3. WWW 的欺骗技术

一般 Web 欺骗使用两种技术手段,即 URL 地址重写技术和相关信息掩盖技术。攻击者修改网页的 URL 地址,即攻击者可以将自己的 Web 地址加在所有 URL 地址的前面。当用户浏览目标网页的时候,实际上是向攻击者的服务器发出请求,于是用户的所有信息便处于攻击者的监视之下,攻击者就达到欺骗的目的了。但由于浏览器一般均设有地址栏和状态栏,当浏览器与某个站点链接时,用户可以在地址栏和状态栏中获得连接中的 Web 站点地址及其相关的传输信息,由此发现已出了问题。所以攻击者往往在 URL 地址重写的同时,利用相关信息掩盖技术(一般用 JavaScript 程序来重写地址栏和状态栏),以掩盖欺骗。

4. 电子邮件攻击

电子邮件是 Internet 上运用得十分广泛的一种通信方式。攻击者可以使用一些邮件炸弹软件或 CGI 程序向目标邮箱发送大量内容重复、无用的垃圾邮件,从而使目标邮箱被撑爆而无法使用。当垃圾邮件的发送流量特别大时,还有可能造成邮件系统对于正常的工作反应缓慢,甚至瘫痪。相对于其他的攻击手段来说,这种攻击方法具有简单、见效快等优点。

电子邮件攻击主要表现为以下两种方式。

(1) 邮件炸弹:指的是用伪造的 IP 地址和电子邮件地址向同一信箱发送数以千计、万计甚至无穷多次的内容相同的垃圾邮件,致使受害人邮箱被“炸”,严重者可能会给电子邮件服务器操作系统带来危险,甚至瘫痪。

(2) 电子邮件欺骗:攻击者佯称自己为系统管理员,给用户发送邮件要求用户修改口令(口令可能为指定字符串)或在貌似正常的附件中加载病毒或其他木马程序。

5. 通过一个结点来攻击其他结点

攻击者在突破一台主机后，往往以此主机作为根据地，攻击其他主机，以隐蔽其入侵路径，避免留下蛛丝马迹。他们可以使用网络监听方法，尝试攻破同一网络内的其他主机；也可以通过 IP 欺骗和主机信任关系，攻击其他主机。

这类攻击很狡猾，但由于某些技术很难掌握，如 TCP/IP 欺骗攻击，攻击者通过外部计算机伪装成另一台合法机器来实现。它能破坏两台计算机间通信链路上的数据，其伪装的目的在于哄骗网络中的其他机器误将其攻击者作为合法机器加以接受，诱使其他机器向它发送数据或允许它修改数据。TCP/IP 欺骗可以发生在 TCP/IP 系统的所有层次上，包括数据链路层、网络层、运输层及应用层均容易受到影响。如果底层受到损害，则应用层的所有协议都将处于危险之中。另外，由于用户本身不直接与底层相互交流，因而对底层的攻击更具有欺骗性。

6. 网络监听

网络监听是主机的一种工作模式，在这种模式下，主机可以接收到本网段在同一条物理通道上传输的所有信息，而不管这些信息的发送方和接收方是谁。因为系统在进行密码校验时，用户输入的密码需要从用户端传送到服务器端，而攻击者就能在两端之间进行数据监听。此时若两台主机进行通信的信息没有加密，只要使用某些网络监听工具如 NetXRay、Sniffer 等就可轻而易举地截取包括口令和账号在内的信息资料。虽然网络监听获得的用户账号和口令具有一定的局限性，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。

7. 利用黑客软件攻击

利用黑客软件攻击是 Internet 上比较多的一种攻击手法。例如，利用特洛伊木马程序可以非法地取得用户计算机的超级用户级权限，除了可以进行完全的控制操作外，还可以进行对方桌面抓图、取得密码等操作。这些黑客软件分为服务器端和用户端，当黑客进行攻击时，会使用用户端程序登录已安装好服务器端程序的计算机，这些服务器端程序都比较小，一般会附带于某些软件上。因此当用户下载了一个小游戏并运行时，黑客软件的服务器端有可能就安装完成了，而且大部分黑客软件的重生能力比较强，给用户进行清除造成一定的麻烦。特别是最近出现了一种 TXT 文件欺骗手法，表面看上去是一个 TXT 文本文件，但实际上却是一个附带黑客程序的可执行程序，另外有些程序也会伪装成图片和其他格式的文件。

8. 安全漏洞攻击

许多系统都有这样那样的安全漏洞(Bugs)。其中一些是操作系统或应用软件本身具有的，如缓冲区溢出攻击。由于很多系统在不检查程序与缓冲之间变化的情况下，就任意接受任意长度的数据输入，把溢出的数据放在堆栈里，系统还照常执行命令。这样攻击者只要发送超出缓冲区所能处理的长度的指令，系统便进入不稳定状态。若攻击者特别配置一串准备用作攻击的字符，甚至可以访问根目录，从而拥有对整个网络的绝对控制权。

另一些是利用协议漏洞进行攻击。如攻击者利用 POP3 一定要在根目录下运行的这一漏洞发动攻击，破坏根目录，从而获得超级用户的权限。

又如，ICMP 也经常被用于发动拒绝服务攻击。它的具体手法就是向目标服务器发送大量的数据包，几乎占取该服务器所有的网络宽带，从而使其无法对正常的服务请求进行处

理,而导致网站无法进入、网站响应速度大大降低或服务器瘫痪。现在常见的蠕虫病毒或与其同类的病毒都可以对服务器进行拒绝服务攻击。拒绝服务的目的在于瘫痪系统,并可能取得伪装系统的身份。拒绝服务通常是利用系统提供特定服务时的设计缺陷,消耗掉大量服务能力,若系统设计不良,也可能造成系统崩溃。而分布式的拒绝服务,则进一步利用其他遭侵入的系统同时要求大量的服务。拒绝服务攻击发生时,系统通常并不会遭到破解,但该服务会丧失有效性。尽管主动过滤可以在一定程度上保护用户,但是由于拒绝服务攻击不容易识别,往往让人防不胜防。

9. 端口扫描攻击

端口扫描,就是利用 Socket 编程与目标主机的某些端口建立 TCP 连接、进行传输协议的验证等,从而侦知目标主机的扫描端口是否处于激活状态、主机提供了哪些服务、提供的服务中是否含有某些缺陷等。常用的扫描方式有 Connect 扫描、Fragmentation 扫描。

3.1.3 网络攻击的步骤

攻击者在一次攻击过程中的通常做法是:首先隐藏位置,接着进行网络探测和资料收集、对系统弱点进行挖掘、获得系统控制权、隐藏行踪,最后实施攻击、开辟后门等,如图 3-1 所示。

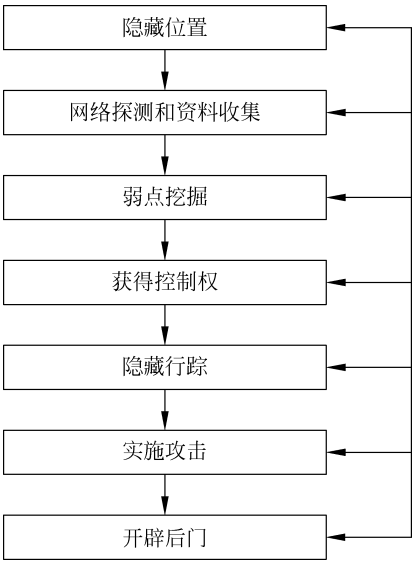


图 3-1 攻击步骤

1. 隐藏位置

在 Internet 上的网络主机均有自己的网络地址,若没有采取保护措施,很容易反查到某台网络主机的位置,如 IP 地址和域名。因此,有经验的黑客在实施攻击活动时的首要步骤是设法隐藏自己所在的网络位置,包括自己的网络域及 IP 地址,这样使调查者难以发现真正的攻击者来源。

隐藏位置就是有效地保护自己。Internet 以松散方式构成,容易隐藏攻击者的踪迹。攻击者经常使用如下技术隐藏其真实的 IP 地址或者域名。

(1) 利用被侵入的主机作为跳板,如在安装 Windows 的计算机内利用 WinGate 软件作

为跳板，利用配置不当的 Proxy 作为跳板。

（2）使用电话转接技术隐蔽自己，如利用 800 电话的无人转接服务连接 ISP。

（3）盗用他人的账号上网，通过电话连接一台主机，再经由主机进入 Internet。

（4）免费代理网关。

（5）伪造 IP 地址。

（6）假冒用户账号。

2. 网络探测和资料收集

网络探测和资料收集主要是为了寻找目标主机和收集目标信息。

攻击者首先要寻找目标主机并分析目标主机。在 Internet 上能真正标识主机的是 IP 地址，域名是为了便于记忆主机的 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。当然，知道了要攻击目标的位置还是远远不够的，还必须对主机的操作系统类型及其所提供的服务等资料做全面的了解，为攻击做好充分的准备。攻击者感兴趣的信息主要包括：操作系统信息、开放的服务端口号、系统默认账号和口令、邮件账号、IP 地址分配情况、域名信息、网络设备类型、网络通信协议、应用服务器软件类型等。

1）锁定目标

攻击者首先要寻找目标主机。DNS 协议不对转换或信息性的更新进行身份认证，只需实施一次域转换操作就能得到所有主机的名称以及内部 IP 地址。攻击者会利用下列公开协议或工具，收集留在网络系统中的各个主机系统的相关信息。

SNMP：用来查阅网络系统路由器路由表，从而了解目标主机所在网络的拓扑结构及其内部细节。

TraceRoute 程序：能够用该程序获得到达目标主机所要经过的网络数和路由器数。

Whois 协议：该协议的服务信息能提供所有有关的 DNS 域和相关的管理参数。

DNS 服务器：该服务器提供了系统中可以访问的主机的 IP 地址表和它们所对应的主机名。

Finger 协议：可以用 Finger 来获取一个指定主机上所有用户的详细信息，如用户注册名、电话号码、最后注册时间以及他们有没有读邮件等。

Ping 实用程序：可以用来确定一个指定的主机的位置。

自动 Wardialing 软件：可以向目标站点一次连续拨出大批电话号码，直到遇到某一正确的号码使其 MODEM 响应。

向主机发送虚假消息，然后根据返回“Host Unreachable”这一消息特征判断出哪些主机是存在的。

2）服务分析

一是使用不同应用程序测试。例如，使用 Telnet、FTP 等用户软件向目标主机申请服务，如果主机有应答就说明主机提供了这个服务，开放了这个端口的服务，这种方法比较麻烦并且获取的资料不全。

二是使用一些端口扫描工具软件，对目标主机一定范围的端口进行扫描，这样可以全部掌握目标主机的端口情况。

3）系统分析

使用具有已知响应类型的数据库的自动工具，对来自目标主机做出的响应进行检查，确

定目标主机的操作系统。例如,打开 Windows 的“运行”窗口,输入命令:

```
Telnet x x x x x x x x(目标主机)
```

然后单击“确定”按钮,可以发现如下响应:

```
Digital Unix(x x x x x x x x) (ttyp1)
Login:
```

4) 获取账号信息

对于陌生的目标主机可能只知道它有一个 ROOT 用户,至于其他账号一无所知,而攻击者要想登录目标主机至少要知道一个普通用户,一般会进行以下尝试。

(1) 利用目标主机的 Finger 功能。Finger 很可能暴露入侵者的行为,为了避免 Finger 查询产生标记,可以使用 Finger 网关。

(2) 利用电子邮件地址。有些用户电子邮件地址(指@符号前面的部分)与其取邮件的账号是一致的。

(3) 利用目录服务。有些主机提供了 X500 的目录查询服务。如何知道是否提供 X500 的功能,可扫描目标主机的端口,如果端口 105 的状态已经被“激活”,则在自己的机器上安装一个 X500 的客户查询工具,选择目标主机,可以获得意想不到的信息。

(4) 尝试习惯性常用账号。根据平时的经验,一些系统总有一些习惯性的常用账号,这些账号都是系统中因为某种应用而设置的。例如,制作 WWW 网站的账号可能是 HTML、WWW、Web 等,安装 Oracle 数据库的可能有 Oracle 的账号,用户培训或教学而设置的 user1、user2、student1、student2、Client1、Client2 等账号,一些常用的英文名字也经常会使用,如 Tom、John 等,因此可以根据系统所提供的服务和在其主页得到的工作人员的名字信息进行猜测。

5) 获得管理员信息

使用查询命令 host,入侵者可获得保存在目标域服务器中的所有信息。Whois 查询可识别出技术管理人员。

使用搜索引擎查询 Usenet 和 Web。系统管理员的职责是维护站点的安全,当他们遇到各种问题时,许多管理员会迫不及待地将这些问题发到 Usenet 或邮件列表上以寻求答案,他们常常指明组织结构、网络的拓扑结构和面临的问题。

可以使用各种方法来识别在目标网络上使用的操作系统的类型及版本。首先判断出目标网络上的操作系统和结构,下一步列出每个操作系统和机器的类型,然后对每个平台进行研究并找出它们中的漏洞。

3. 弱点挖掘

系统中漏洞的存在是系统受到各种安全威胁的根源。外部攻击者的攻击主要利用了系统提供的网络服务中的漏洞;内部人员作案则利用了系统内部服务及其配置上的漏洞;而拒绝服务攻击主要是利用资源分配上的漏洞,长期占用有限资源不释放,使其他用户得不到应得的服务,或者是利用服务处理中的漏洞,使该服务崩溃。攻击者攻击的重要步骤就是尽量挖掘出系统的弱点/漏洞,并针对具体的漏洞研究相应的攻击方法。常见的漏洞如下。

(1) 系统或应用服务软件漏洞。攻击者根据系统提供的不同服务用不同的方法以获取系统的访问权限。如果攻击者发现系统提供了 UUCP 服务,就可以利用 UUCP 的安全漏

洞来获取系统的访问权；如果系统还提供其他一些远程网络服务，如邮件服务、WWW 服务、匿名 FTP 服务、TFTP 服务，攻击者就可以利用这些远程服务中的弱点获取系统的访问权。

(2) 主机信任关系漏洞。攻击者寻找那些被信任的主机，这些主机可能是管理员使用的机器，或是一台被认为很安全的服务器。例如，他可以利用 CGI 的漏洞，读取/etc/host s allow 文件等。通过这个文件，就可以大致了解主机间的信任关系。接下来，就是探测这些被信任的主机哪些存在漏洞。

(3) 寻找有漏洞的网络成员。尽量去发现有漏洞的网络成员对攻击者往往起到事半功倍的效果，堡垒最容易从内部攻破就是这个缘故。用户网络安全防范意识弱，选取弱口令，使得攻击者很容易从远程直接控制主机。

(4) 安全策略配置漏洞。主机的网络服务配置不当，开放有漏洞的网络服务。

(5) 通信协议漏洞。通过分析目标网络所采用的协议信息，寻找漏洞，如 TCP/IP 就存在漏洞。

(6) 网络业务系统漏洞。通过掌握目标网络的业务流程信息，发现漏洞，例如，在 WWW 服务中，允许普通用户远程上传文件。

扫描工具能找出目标主机上各种各样的漏洞，许多网络入侵首先是用扫描程序开始的。常用扫描工具有撒旦(SATAN)ISS 等。典型的端口扫描程序的工作原理如下。

Internet 上任何软件的通信都基于 TCP/IP，它是计算机的门户。TCP/IP 规定，计算机可以有 256×256 个端口，通过这些端口进行数据传输。例如，当发送电子邮件的时候，信件被送到邮件服务器的 25 号端口；当接收邮件时，是从邮件服务器的 110 号端口取信；通过 80 号端口，访问某一个服务器；个人计算机的默认端口为 139 号，上网的时候就是通过这个端口与外界联系的。端口扫描程序会自动扫描这些端口，并记录哪些端口是开放的。一般除了 139 号端口外，其他端口最好不要开放，攻击者入侵就不那么容易了。

4. 获得控制权

攻击者要想入侵一台主机，首先要有该主机的一个账号和口令，再想办法去获得更高的权限，如系统管理账户的权限。获取系统管理权限通常有以下途径。

(1) 获得系统管理员的口令，如专门针对 ROOT 用户的口令攻击。

(2) 利用系统管理上的漏洞，如错误的文件许可权、错误的系统配置、某些 SUID 程序中存在的缓冲区溢出问题等。

(3) 让系统管理员运行一些特洛伊木马程序，使计算机内的某一端口开放，再通过这一端口进入用户的计算机。例如，如果不小心运行了特洛伊木马程序 netspy 的 Server 端软件，那么它会强制 Windows 在以后每次打开计算机时都要运行它，并开放 7306 号端口。

攻击者进入目标主机系统并获得控制权之后，主要做两件事：清除记录和留下后门。如更改某些系统设置、在系统中置入特洛伊木马或其他一些远程操纵程序，以便日后可以不被觉察地再次进入系统。大多数后门程序是预先编译好的，只需要想办法修改时间和权限就可以使用了，甚至新文件的大小都和原文件一模一样。在用清除日志、删除复制的文件等手段来隐藏自己的踪迹之后，攻击者就开始下一步的行动。

5. 隐藏行踪

作为一个入侵者，攻击者总是担心自己的行踪被发现，所以在进入系统之后，聪明的攻击者要做的第一件事就是隐藏自己的行踪，攻击者隐藏自己的行踪通常要用到如下技术。

(1) 连接隐藏,如冒充其他用户、修改 LOGNAME 环境变量、修改 utmp 日志文件、使用 IPSPOOF 技术等。

(2) 进程隐藏,如使用重定向技术减少 PS 给出的信息量、用特洛伊木马代替 PS 程序等。

(3) 篡改日志文件中的审计信息。

(4) 改变系统时间,造成日志文件数据紊乱,以迷惑系统管理员。

6. 实施攻击

不同的攻击者有不同的攻击目的,可能是为了获得机密文件的访问权,或者是为了破坏系统数据的完整性,也可能是为了获得整个系统的控制权(系统管理权限)等。一般说来,可归结为以下几种方式。

(1) 下载敏感信息。

(2) 在目标系统中安装探测器软件,以便进一步收集攻击者感兴趣的信息,或进一步发现受损系统在网络中的信任等级。

(3) 攻击其他被信任的主机和网络。

(4) 使网络瘫痪。

(5) 修改或删除重要数据。

7. 开辟后门

一次成功的入侵通常要耗费攻击者大量的时间与精力,所以精于算计的攻击者在退出系统之前会在系统中制造一些后门,以方便自己的下次入侵。攻击者设计后门时通常会考虑采用以下方法。

(1) 放宽文件许可权。

(2) 重新开放不安全的服务,如 REXD、TFTP 等。

(3) 修改系统的配置,如系统启动文件、网络服务配置文件等。

(4) 替换系统本身的共享库文件。

(5) 安装各种特洛伊木马程序,修改系统的源代码。

(6) 安装 Sniffer。

通过分析可以得出以下结论。

第一,一次完整的攻击过程可以划分为三个阶段,分别为:获取系统访问权前的攻击过程,获得系统控制权的攻击过程,获得系统访问权或控制权之后的攻击活动。完成第一阶段的攻击过程,获得了系统的访问权,攻击者就已成功了一半,而完成第二阶段的攻击过程,获得系统的管理权限之后,攻击者已近于完全成功。此时,管理员已经很难阻止攻击者的破坏活动,但可以尽早地采取一些补救措施,如备份系统、关掉系统的网络连接、关机等。备份系统是为了便于事后进行系统重建;失掉系统的网络连接或者关机可以驱赶外部或内部的攻击者,但很多关键应用系统是不容许断掉网络连接或关机的,所以这两种措施只能作为在万不得已情况下的选择,而且采取以上三种措施时,攻击者可能已经完成了他的攻击目标。第二阶段的攻击成功之后,第三阶段中的活动只是有经验攻击者的例行公事。

第二,攻击者攻击成功的关键在于第一、第二阶段的成功,在于尽早地发现或者利用目标系统的安全漏洞或弱点的能力。

第三,由于内部用户已经拥有了系统的一般访问权,而且更容易知道系统提供了哪些服

务及服务软件的版本、系统的安全状况如系统配置或权限设置上的弱点、管理员的管理水平等，因此，内部攻击者不用像外部攻击者那样花费额外的时间去搜集信息、挖掘弱点，花费精力去突破系统的访问控制，可以减少攻击步骤，只要找到系统的漏洞、弱点或缺陷，想办法获取系统管理权限，就可以随心所欲地进行破坏活动了，如图 3-2 所示。

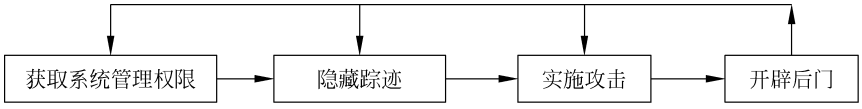


图 3-2　内部攻击者的攻击步骤

3.1.4　黑客攻击实例

黑客攻击拨号上网计算机和攻击局域网计算机的流程是不一样的，下面分别讲述。

1. 黑客攻击拨号上网计算机实例

攻击拨号上网计算机的流程如图 3-3(a)所示。

1) 用 Winipcfg 查询拨号上网用户计算机的 IP

Winipcfg 可以用来查询目前拨号上网用户的 IP 地址，而这个地址也就是拨号上网用户的 ISP 公司所使用的接入账号地址。

2) 用 Legion 扫描 IP

因为同一时间应该有很多用户同时上网，黑客可以用刚才查询到的拨号上网用户的 IP 地址来查询整个 C 类或 B 类的其他上网用户计算机的 IP 地址，以获得“共享资源”。

典型的 Legion 入侵的具体步骤如下。

(1) 只要是已安装了 Legion 的计算机，都可通过“开始”|“程序”|Legion，运行 Legion 扫描器程序。

(2) 屏幕出现 Legion 主画面。根据步骤(1)查询到的拨号上网用户的 IP 地址，输入所要扫描的 IP 地址范围，然后单击 Scan 按钮开始扫描。

(3) 稍等片刻，在右边方框中会出现很多扫描到的硬盘、文件或文件夹。选中任一感兴趣的硬盘、文件或文件夹，单击鼠标右键，在弹出的快捷菜单中选择“复制”命令。

(4) 打开 IE 浏览器，在地址栏中单击鼠标右键，在弹出的快捷菜单中选择“粘贴”命令。也可以通过“开始”|“运行”，打开“运行”对话框，在“打开”栏内单击鼠标右键，在弹出的快捷菜单中选择“粘贴”命令，然后单击“确定”按钮。

(5) 被选中的硬盘、文件或文件夹的资料全部被显示出来。

如果黑客用上述方法扫描到的目标计算机提供完全的资源共享，黑客就可以随意地查看、复制、修改、删除文件或文件夹。如果目标计算机提供只读状态的资源共享，黑客就只能随意查看、复制，但不能修改、删除文件或文件夹，但黑客可以进入下一步，尝试破解密码，进而完全控制目标计算机。

3) 盗取他人账号和口令

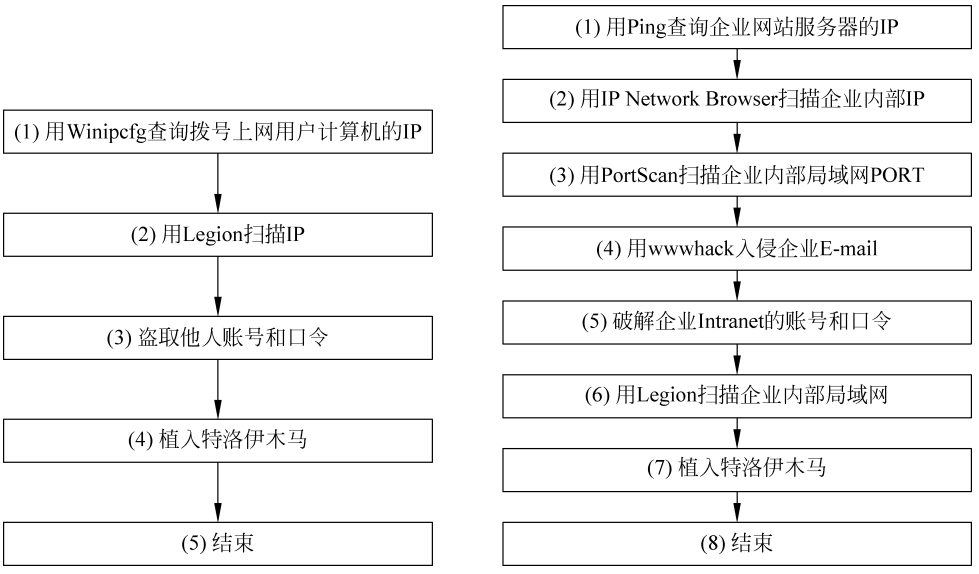
当使用 Legion 查询到某个 IP 的“资源共享”后，可以进一步盗取他人密码文件(将密码文件复制到本地计算机中)，然后再加以破解，得到账号和口令。

4) 植入特洛伊木马

植入特洛伊木马，以便进一步管控该计算机。

2. 黑客攻击企业内部局域网实例

入侵企业内部局域网计算机的流程如图 3-3(b)所示。



(a) 黑客攻击拨号上网计算机的流程　　(b) 黑客攻击局域网计算机的流程

图 3-3　黑客攻击实例的流程图

(1) 用 Ping 查询企业网站服务器的 IP。企业通常有 WWW 网站和 E-mail 服务器地址,可以用 Ping 命令来查询得知企业的 IP 地址。

(2) 用 IP Network Browser 扫描企业内部 IP。得知企业的 WWW 网址和 E-mail 服务器地址,接着可以用 IP Network Browser 扫描整个企业 C 级的 IP 地址,从而获得企业 Intranet 内部网络的网址。

(3) 用 PortScan 扫描企业内部局域网 PORT。用 PortScan 可以扫描企业内部 Intranet 地址,得知有哪些 PORT 端口服务,PORT 端口服务越多,入侵的渠道越多。

(4) 用 wwwhack 入侵企业 E-mail。用 wwwhack 可以获取企业内部 E-mail 的账号和口令。

(5) 破解企业 Intranet 的账号和口令。用各种方法(如 NAT)来破解企业 Intranet 账号和口令。如果破解了 Intranet 的账号和口令,就可以入侵内部 Intranet 了。

(6) 用 Legion 扫描企业内部局域网。借助 Ping 命令和 IP Network Browser 软件查询公司内部的 IP 之后,就可以使用 Legion 软件来扫描企业内部局域网以取得公司内部的"资源共享"。

(7) 植入特洛伊木马。同样地,如果碰到企业内部某台计算机可以"写入"就会植入特洛伊木马,以便进一步管控该计算机。

3.1.5　网络攻击的防范措施及处理对策

在对网络攻击进行分析与识别的基础上,用户应当认真制定有针对性的策略。明确安全对象,设置强有力的安全保障体系。有的放矢,在网络中层层设防,发挥网络中每个层的作用,使每一层都成为一道关卡,才能全方位地抗拒各种不同的威胁和脆弱性,确保网络信

息的保密性、完整性、可用性。

1. 防范措施

1）提高安全意识

（1）不要随意打开来历不明的电子邮件及文件，不要运行来历不明的软件和盗版软件。

（2）不要随便从 Internet 上下载软件，尤其是不可靠的 FTP 站点和非授权的软件分发点。即使从知名网站上下载的软件也要及时用最新的杀病毒软件进行扫描。

（3）防字典攻击和口令保护。选择 12～15 个字符组成口令，尽可能使用字母数字混排，并且在任何字典上都查不到，那么口令就不能被轻易窃取了。不要使用个人信息（如生日、名字等），口令中要有一些非字母（数字、标点符号、控制字符等），还要好记一些，不能写在纸上或计算机中的文件中，选择口令的一个好方法是将两个相关的词用一个数字或控制字符相连。重要的口令最好经常更换。

（4）及时下载安装系统补丁程序。

（5）不要随便运行黑客程序，许多此类程序运行时会发出用户的个人信息。

（6）在支持 HTML 的 BBS 上，如发现提交警告，先要查看源代码，因为这很可能是骗取密码的陷阱。

（7）经常运行专门的反黑客软件，必要时应在系统中安装具有实时检测、拦截、查找黑客攻击程序的工具。经常采用扫描工具软件进行扫描，以发现漏洞并及早采取弥补措施。

2）使用能防病毒、防黑客的防火墙软件

防火墙是一个用以阻止网络中的黑客访问某个机构网络的屏障，也可称之为控制进/出两个方向通信的门槛。在网络边界上通过建立起来的相应网络通信监控系统来隔离内部和外部网络，以阻挡外部网络的侵入。

将防毒、防黑客当成日常例行工作，定时更新防毒组件，将防毒软件保持在常驻状态，以彻底防毒。由于黑客经常会针对特定的日期发动攻击，用户在此期间应特别提高警戒。

3）设置代理服务器，隐藏自己的 IP 地址

保护自己的 IP 地址很重要。事实上，即便用户的计算机上被安装了木马程序，若没有用户的 IP 地址，攻击者也是没有办法的，而保护 IP 地址的最好方法就是设置代理服务器。代理服务器能起到外部网络申请访问内部网络的中间转接作用，其功能类似于一个数据转发器，它主要控制哪些用户能访问哪些服务类型。当外部网络向内部网络申请某种网络服务时，代理服务器接受申请，然后它根据其服务类型、服务内容、被服务的对象、服务者申请的时间、申请者的域名范围等来决定是否接受此项服务，如果接受，它就向内部网络转发这项请求。

4）安装过滤器路由器，防止 IP 欺骗

防止 IP 欺骗站点的最好办法是安装一台过滤器路由器，该路由器限制对本站点外部接口的输入，监视数据包，可发现 IP 欺骗。不允许那些以本站点内部网为源地址的包通过，还应当滤去那些以不同于内部网为源地址的包输出，以防止从本站点进行 IP 欺骗。

5）建立完善的访问控制策略

访问控制是网络安全防范和保护的主要策略，它的主要任务是保证网络资源不被非法使用和非常访问，也是维护网络系统安全、保护网络资源的重要手段。要正确地设置入网访问控制、网络权限控制、目录等级控制、属性安全控制、网络服务的安全控制，设置网络端口

和结点的安全控制、防火墙控制等安全机制。各种安全访问控制互相配合,可以达到保护系统的最佳效果。

6) 采用加密技术

不要在网络上传输未经加密的口令和重要文件、信息。

7) 做好备份工作

经常检查系统注册表,做好数据备份工作。

2. 处理对策

1) 发现攻击者

一般很难发现网络系统是否被人入侵。即便系统上有攻击者入侵,也可能永远不被发现。如果攻击者破坏了网络系统的安全性,则可以追踪他们。借助下面一些途径可以发现攻击者。

(1) 攻击者正在行动时,捉住攻击者。例如,当管理员正在工作时,发现有人使用超级用户的账号通过拨号终端登录,而超级用户口令只有管理员本人知道。

(2) 根据系统发生的一些改变推断系统已被入侵。

(3) 从其他站点的管理员那里收到邮件,称有人从本站点对"他"的站点大肆活动。

(4) 根据网络系统中一些奇怪的现象,发现攻击者。例如,不正常的主机连接及连接次数、系统崩溃、突然的磁盘存储活动或者系统突然变得非常缓慢等。

(5) 经常注意登录文件并对可疑行为进行快速检查,检查访问及错误登录文件,检查系统命令如 login 等的使用情况。在 Windows NT 平台上,可以定期检查 EventLog 中的 SecurityLog,以寻找可疑行为。

(6) 使用一些工具软件可以帮助发现攻击者。

2) 处理原则

(1) 不要惊慌。发现攻击者后,会有许多选择。但是不管发生什么事,没有慎重地思考就去行动,只会使事情变得更糟。

(2) 记录每一件事情,甚至包括日期和时间。

(3) 估计形势。估计入侵造成的破坏程度,攻击者是否还滞留在系统中?威胁是否来自内部?攻击者的身份及目的是什么?若关闭服务器,是否能承受得起失去有用系统信息的损失?

(4) 采取相应措施。一旦了解形势之后,就应着手做出决定并采取相应的措施:能否关闭服务器?若不能,也可关闭一些服务或至少拒绝一些人。是否追踪攻击者?若打算如此,则不要关闭 Internet 连接,因为这会失去攻击者的踪迹。

3) 发现攻击者后的处理对策

发现攻击者后,网络管理员的主要目的不是抓住他们,而应把保护用户、保护网络系统的文件和资源放在首位。因此,可采取下面的某些对策。

(1) 不理睬。

(2) 使用 write 或者 talk 工具询问他们究竟想要做什么。

(3) 跟踪这个连接,找出攻击者的来路和身份。这时候,nslookup、Finger、rusers 等工具很有用。

(4) 管理员可以使用一些工具来监视攻击者,观察他们正在做什么。这些工具包括

snoop、ps、lastcomm、ttywatch 等。

(5) 杀死这个进程来切断攻击者与系统的连接。断开调制解调器与网络线的连接,或者关闭服务器。

(6) 找出安全漏洞并修补漏洞,再恢复系统。

(7) 最后,根据记录的整个文件的发生发展过程,编档保存,并从中吸取经验教训。

3.1.6　网络攻击技术的发展趋势

尽管网络安全的研究已经得到越来越多的关注,但网络安全问题并没有因此而减少;相反,随着网络规模飞速扩展、结构日益复杂和应用领域的不断扩大,网络安全事件呈迅速增长的趋势,造成的损失也越来越大。最近几年,新发现的安全漏洞每年都要增加一倍,发现安全漏洞越来越快,网络攻击技术和攻击工具也日新月异,其变化趋势如下。

1. 攻击技术越来越先进

随着网络新技术的不断涌现,入侵者的网络背景知识、技术能力也随之提升,攻击技术越来越先进。

(1) 网络攻击自动化。网络攻击者能够利用现有攻击技术编制自动攻击工具软件。

(2) 网络攻击组织化。网络攻击工具的传播,使得越来越多的人掌握了攻击方法,出现了有组织的网络攻击行为。

(3) 网络攻击目标扩大化。网络攻击从以往的以 UNIX 主机为主转向网络的各个层面,网络通信协议、密码协议、网络域名服务、网络的路由服务系统和网络应用服务系统,甚至网络安全保障系统均成为攻击对象。例如,防火墙渗透攻击。

(4) 网络攻击协同化。攻击者利用 Internet 的巨大计算资源,开发特殊的程序实现将分布在不同地域的计算机协同起来,向特定的目标发起攻击。2000 年 2 月,黑客就曾以 DDoS(Distributed Denial Of Service)攻击 Yahoo!、CNN 新闻网等著名网站,导致其服务瘫痪。http://www.distributed.net 提供了一个协同攻击密码算法的典型实例。

(5) 网络攻击智能化。网络攻击与病毒程序相结合,病毒的复制传播特点使得攻击程序如虎添翼。

(6) 网络攻击主动化。网络攻击者掌握主动权,而防御者被动应对。攻击者处于暗处,而攻击目标则在明处。网络中的弱点往往是入侵者先发现,这样网络安全防御就处于被动局面。如果网络安全防御者未消除新公布的弱点,则网络攻击者就有机可乘。

2. 攻击工具越来越复杂

有了攻击工具,使得攻击的技术门槛降低,攻击变得更加容易了,即使在完全不了解一个系统类型的情形下,都可能破解这套系统。与以前相比,现在攻击工具的特征更难被发现,更难利用特征进行检测。主要表现在以下四方面。

(1) 反侦破。攻击者采用隐蔽攻击工具特性的技术,使安全专家分析新攻击工具和了解新攻击行为所耗费的时间增多。

(2) 动态行为。早期的攻击工具是以单一确定的顺序执行攻击步骤,现在的自动攻击工具可以根据随机选择、预先定义的决策路径或通过入侵者直接管理,来改变它们的模式和行为。

(3) 攻击工具的成熟性。与早期的攻击工具不同,目前的攻击工具可以通过升级或更

换工具的一部分,发动迅速变化的攻击,且在每一次攻击中会出现多种不同形态的攻击工具。

(4) 跨平台。攻击工具越来越普遍地被开发,使其可在多种操作系统平台上执行。许多常见攻击工具使用 IRC 或 HTTP 等协议,从入侵者那里向受攻击的计算机发送数据或命令,使得人们将攻击特性与正常、合法的网络传输流区别开变得越来越困难。

3. 发现安全漏洞越来越快

新发现的安全漏洞每年都要增加一倍,管理人员不断用最新的补丁修补这些漏洞,而且每年都会发现安全漏洞的新类型。入侵者经常能够在厂商修补这些漏洞前发现攻击目标。

4. 越来越高的防火墙渗透率

防火墙是人们用来防范入侵者的主要保护措施。但是越来越多的攻击技术都可以绕过防火墙实施攻击。例如,IPP(Internet 打印协议)和 WebDAV(基于 Web 的分布式创作与翻译)都可以被攻击者利用来绕过防火墙。

5. 越来越不对称的威胁

Internet 上的安全是相互依赖的。每个 Internet 系统遭受攻击的可能性取决于连接到全球 Internet 上其他系统的安全状态。由于攻击技术的进步,一个攻击者可以比较容易地利用分布式系统,对一个受害者发动破坏性的攻击。随着部署自动化程度和攻击工具管理技巧的提高,威胁的不对称性将继续增加。

3.2 入侵检测系统

只要允许内部网络与 Internet 相连,攻击者入侵的危险就会存在。由于入侵行为与正常的访问或多或少有些差别,通过收集和分析这种差别可以发现绝大部分入侵行为,入侵检测系统(Intrusion Detection System,IDS)应运而生。

3.2.1 入侵检测系统概述

入侵检测系统是一个比较复杂和难度较大的研究领域。首先,入侵检测系统是网络安全与管理和信息处理技术的结合,为了了解入侵检测系统,必须同时具备这两方面的知识,入侵检测系统的检测效果依赖于对这些知识的掌握和融合。其次,入侵事件往往是人为的入侵,由黑客主动实现,黑客对网络安全以及入侵检测系统本身有一定的了解。最后,入侵检测系统是一个计算机网络安全产品或工具,是一个实实在在的计算机程序,所以它的运行效率和检测效果也与程序编写的技术有关。

1. 入侵检测及其内容

入侵检测是对入侵行为的发觉,是一种试图通过观察行为、安全日志或审计数据来检测入侵的技术。

入侵检测的内容包括:检测试图闯入、成功闯入、冒充其他用户、违反安全策略、合法用户的泄露、独占资源以及恶意使用等破坏系统安全性的行为。

2. 入侵检测系统

入侵检测系统从计算机网络或计算机系统的关键点收集信息并进行分析,从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象,使安全管理员能够及时地处理入

侵警报，尽可能减少入侵对系统造成的损害。

入侵检测系统实际上是一种使监控和分析过程自动化的产品，可以是软件，也可以是硬件，最常见的是软件与硬件的组合。所以，通常把负责入侵检测的软/硬件组合体称为入侵检测系统。

一个成功的入侵检测系统至少要满足以下5个要求。

(1) 实时性要求。如果攻击或者攻击的企图能够被尽快发现，就有可能查出攻击者的位置，阻止进一步的攻击活动，就有可能把破坏控制在最小限度，并记录下攻击过程，可作为证据回放。实时入侵检测可以避免管理员通过对系统日志进行审计以查找入侵者或入侵行为线索时的种种不便与技术限制。

(2) 可扩展性要求。攻击手段多而复杂，攻击行为特征也各不相同。所以必须建立一种机制，把入侵检测系统的体系结构与使用策略区分开。入侵检测系统必须能够在新的攻击类型出现时，通过某种机制在无须对入侵检测系统本身体系进行改动的情况下，使系统能够检测到新的攻击行为。在入侵检测系统的整体功能设计上，也必须建立一种可以扩展的结构，以便适应扩展要求。

(3) 适应性要求。入侵检测系统必须能够适用于多种不同的环境，如高速大容量的计算机网络环境，并且在系统环境发生改变，如增加环境中的计算机系统数量、改变计算机系统类型时，入侵检测系统应当依然能够正常工作。适应性也包括入侵检测系统本身对其宿主平台的适应性，即跨平台工作的能力，适应其宿主平台软、硬件配置的不同情况。

(4) 安全性与可用性要求。入侵检测系统必须尽可能地完善与健壮，不能向其宿主计算机系统及其所属的计算机环境引入新的安全问题及安全隐患，并且入侵检测系统在设计和实现时，应该考虑可以预见的、针对该入侵检测系统类型与工作原理的攻击威胁及其相应的抵御方法，确保该入侵检测系统的安全性与可用性。

(5) 有效性要求。能够证明根据某一设计所建立的入侵检测系统是切实有效的。即对于攻击事件的错报与漏报能够控制在一定范围内；入侵检测系统在发现入侵后，能够及时做出响应，有些响应是自动的，如通过控制台、电子邮件等方式通知网络安全管理员，中止入侵进程、关闭系统、断开与Internet的连接，使该用户无效，或者执行一个准备好的命令等。

另外，入侵检测系统还应该能够使系统管理员时刻了解网络系统(包括程序、文件和硬件设备等)的任何变更；为网络安全策略的制定提供指南；它应该管理、配置简单，从而使非专业人员能够非常容易地获得网络安全；规模应根据网络威胁、系统构造和安全需求的改变而改变。

3. 入侵检测系统的组成

入侵检测系统通常由两部分组成：传感器(Sensor)与控制台(Console)。传感器负责采集数据(网络包、系统日志等)、分析数据并生成安全事件。控制台主要起到中央管理的作用，商品化的IDS通常提供图形界面的控制台。

4. 入侵检测系统的特点

入侵检测系统的主要特点如下。

1) 入侵检测技术是动态安全技术的最核心技术之一

传统的操作系统加固技术和防火墙隔离技术等都是静态安全防御技术，对网络环境下

日新月异的攻击手段缺乏主动的反应。入侵检测技术通过对入侵行为的过程与特征的研究,使安全系统对入侵事件和入侵过程能做出实时响应。

2) 入侵检测是防火墙的合理补充

防火墙是计算机网络安全策略中一个很重要的方面,能够在内外网之间提供安全的网络保护,可以限制一些地址(例如攻击者的地址)不能访问用户的机器或者限制攻击者不能访问用户机器的某些服务,这样尽管用户的机器上存在安全漏洞,攻击者也不能进行攻击,降低了网络安全风险。但是,仅使用防火墙还远远不够。入侵者可寻找防火墙背后可能敞开的后门;入侵者可能就在防火墙内,甚至来自本地(这样的入侵防火墙阻止不了);由于性能的限制,防火墙通常不能提供实时的入侵检测能力。

入侵检测是防火墙的合理补充,帮助系统对抗网络攻击,扩展了系统管理员的安全管理能力(包括安全审计、监视、进攻识别和响应),提高了信息安全基础结构的完整性。

入侵检测被认为是防火墙之后的第二道安全闸门,提供对内部攻击、外部攻击和误操作的实时保护。这些都通过它执行以下任务来实现。

(1) 监视、分析用户及系统活动,查找非法用户和合法用户的越权操作。

(2) 系统构造和弱点的审计,并提示管理员修补漏洞。

(3) 识别反映已知进攻的活动模式并向相关人士报警,能够实时对检测到的入侵行为产生反应。

(4) 异常行为模式的统计分析,发现入侵行为的规律。

(5) 评估重要系统和数据文件的完整性,如计算和比较文件系统的校验和。

(6) 操作系统的审计跟踪管理,并识别用户违反安全策略的行为。

3) 入侵检测系统是黑客的克星

入侵检测和安全防护有根本性的区别:安全防护和黑客的关系是"防护在明,黑客在暗",入侵检测和黑客的关系则是"黑客在明,检测在暗"。安全防护主要修补系统和网络的缺陷,增加系统的安全性能,从而消除攻击和入侵的条件;入侵检测并不是根据网络和系统的缺陷,而是根据入侵事件的特征去检测(入侵事件的特征一般与系统缺陷有逻辑关系),所以入侵检测系统是黑客的克星。

3.2.2 入侵检测系统的数学模型

1. 通用模型

入侵检测的概念最早由 Anderson 在 1980 年提出。随后,Denning 对 Anderson 的工作进行了扩展,并于 1987 年提出了一种通用的入侵检测模型。数学模型的建立有助于更精确地描述入侵问题,特别是异常入侵检测。

通用模型采用的是一个混合结构,包含一个异常检测器和一个专家系统,如图 3-4 所示。异常检测器采用统计技术描述异常行为,专家系统采用基于规则的方法检测已知的危害行为。异常检测器对行为的渐变是自适应的,因此引入专家系统能有效防止逐步改变的入侵行为,提高准确率。该模型由以下 6 个主要部分构成。

(1) 主体(Subjects):在目标系统上活动的实体,如用户。

(2) 对象(Objects):系统资源,如文件、设备、命令等。

(3) 审计记录(Audit Records):由六元组(Subject、Action、Object、Exception Condition、

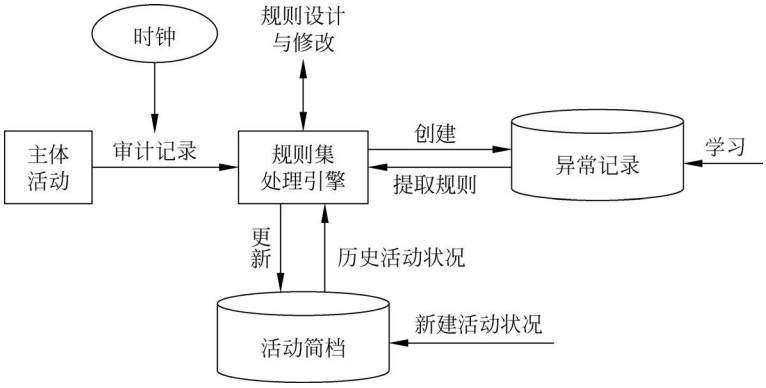


图 3-4　Denning 的通用入侵检测模型

Resource Usage、Time Stamp)构成。其中,活动(Action)是主体对目标的操作,对操作系统而言,这些操作包括读、写、登录、退出等;异常条件(Exception Condition)是指系统对主体的该活动的异常报告,如违反系统读写权限;资源使用状况(Resource Usage)是系统的资源消耗情况,如 CPU、内存使用率等;时间戳(Time Stamp)是活动发生时间。

(4) 活动简档(Activity Profile):用以保存主体正常活动的有关信息,具体实现依赖于检测方法,在统计方法中从事件数量、频度、资源消耗等方面度量,可以使用方差、马尔可夫模型等方法实现。

(5) 异常记录(Anomaly Record):由(Event,Time Stamp,Profile)组成,用以表示异常事件的发生情况。

(6) 活动规则:规则集是检查入侵是否发生的处理引擎,结合活动简档用专家系统或统计方法等分析接收到的审计记录,调整内部规则或统计信息,在判断有入侵发生时采取相应的措施。

Denning 模型基于这样一个假设:由于袭击者使用系统的模式不同于正常用户的使用模式,通过监控系统的跟踪记录,可以识别袭击者异常使用系统的模式,从而检测出袭击者违反系统安全性的情况。

Denning 模型独立于特定的系统平台、应用环境、系统弱点以及入侵类型,为构建入侵检测系统提供了一个通用的框架,为后来各种模型的发展奠定了基础,导致了随后几年内一系列系统原型的研究,如 Discovery、Haystack、MIDS、NADIR、NSM、WisdomandSense 等。

2. 统一模型

入侵检测系统统一模型由 5 个主要部分(信息收集器、分析器、响应、数据库以及目录服务器)组成,如图 3-5 所示。

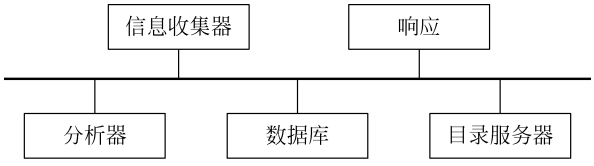


图 3-5　入侵检测统一模型

(1) 信息收集器:用于收集事件的信息。收集的信息将被用来分析、确定是否发生入侵。信息收集器可以被划分成不同级别,通常分为网络级别、主机级别和应用程序级别。对

于网络级别,它的处理对象是网络数据包。对于主机级别,它的处理对象一般是系统的审计记录。对于应用程序级别,它的处理对象一般是程序运行的日志文件。被收集的信息可以送到分析器处理,或者存放在数据库中待处理。

(2) 分析器:对由信息源生成的事件做实际分析处理,确定哪些事件与正在发生或者已发生的入侵有关。两个最常用的分析方法是误用检测和异常检测。分析器的结果可以被响应,或者保存在数据库中做统计。

(3) 响应:响应就是当入侵事件发生时,系统采取的一系列动作。这些动作常被分为主动响应和被动响应两类。主动响应能自动干涉系统;被动响应向管理员提供信息,再由管理员采取行动。

(4) 数据库:保存事件信息,包括正常和入侵事件。数据库还可以用来临时处理数据,扮演各个组件之间的数据交换中心。

(5) 目录服务器:保存入侵检测系统各个组件及其功能的目录信息。在一个比较大的入侵检测系统中,这部分会起到很重要的作用,可以改进系统的维护和可扩展性。

3.2.3 入侵检测的过程

1. 入侵信息的收集

入侵检测的第一步是信息收集,收集的内容包括系统、网络、数据及用户活动的状态和行为。通常需要在计算机网络系统中的若干不同关键点(不同网段和不同主机)收集信息,这除了尽可能扩大检测范围的因素外,还有一个重要的因素就是:从一个源来的信息有可能看不出疑点,但从几个源来的信息的不一致性却是可疑行为或入侵的最好标识。

入侵检测很大程度上依赖于收集信息的可靠性和正确性,因此,有必要利用所知道的真正的和精确的软件来报告这些信息。因为入侵者经常替换软件以搞混和移走这些信息,例如,替换被程序调用的子程序、库和其他工具。入侵者对系统的修改可能使系统功能失常但看起来仍跟正常的一样,这就需要保证用来检测网络系统的软件的完整性,特别是入侵检测系统软件本身应具有相当强的坚固性,防止因被篡改而收集到错误的信息。

入侵检测利用的信息一般来自以下四方面。

1) 系统和网络日志

如果不知道入侵者在系统上都做了什么,是不可能发现入侵的。日志提供了当前系统的细节,哪些系统被攻击了,哪些系统被攻破了。因此,充分利用系统和网络日志文件信息是检测入侵的必要条件。日志中包含发生在系统和网络上的不寻常和不期望活动的证据,这些证据可以指出有人正在入侵或已成功侵入了系统。通过查看日志文件,能够发现成功的入侵或入侵企图,并很快地启动相应的应急响应程序。日志文件中记录了各种行为类型,每种类型又包含不同的信息,例如,记录“用户活动”类型的日志,就包含登录、用户 ID 改变、用户对文件的访问、授权和认证信息等内容。很显然,对用户活动来讲,不正常的或不期望的行为就是重复登录失败、登录到不期望的位置以及非授权地企图访问重要文件等。

由于日志的重要性,所有重要的系统都应定期做日志,而且日志应被定期保存和备份,因为随时都可能会需要它。许多专家建议定期向一个中央日志服务器上发送所有日志,而这个服务器使用一次性写入的介质来保存数据,这样就避免了攻击者篡改日志。系统本地日志与发到一个远端系统保存的日志提供了冗余和一个额外的安全保护层。现在两个日志

可以互相比较，任何不同都显示了系统的异常。

2）目录和文件中的不期望的改变

网络环境中的文件系统包含很多软件和数据文件，而包含重要信息的文件和私有数据文件经常是攻击者修改或破坏的目标。目录和文件中的不期望的改变（包括修改、创建和删除），特别是那些正常情况下限制访问的，很可能就是一种入侵产生的指示和信号。攻击者经常替换、修改和破坏他们获得访问权的系统上的文件，同时为了隐藏他们在系统中的表现及活动痕迹，都会尽力去替换系统程序或修改系统日志文件。

3）程序执行中的不期望行为

网络系统上的程序执行一般包括操作系统、网络服务、用户起动的程序和特定目的的应用，如数据库服务器。每个在系统上执行的程序由一到多个进程来实现。每个进程执行在具有不同权限的环境中，这种环境控制着进程可访问的系统资源、程序和数据文件等。

一个进程的执行行为由它运行时执行的操作来表现，操作执行的方式不同，它利用的系统资源也就不同。操作包括计算、文件传输、设备和其他进程，以及与网络间其他进程的通信。

一个进程出现了不期望的行为可能表明攻击者正在入侵系统。攻击者可能会将程序或服务的运行分解，从而导致它失败，或者是以非用户或管理员意图的方式操作。

4）物理形式的入侵信息

这包括两方面的内容：一是未授权的对网络硬件的连接，二是对物理资源的未授权访问。入侵者会想方设法去突破网络的周边防卫，如果他们能够在物理上访问内部网，就能安装他们自己的设备和软件，也就可以了解和掌握网上由用户加上去的不安全（未授权）设备，然后利用这些设备访问网络。

2. 信号分析

对上述四类收集到的有关系统、网络、数据及用户活动的状态和行为等信息，一般通过四种技术手段进行分析，即模式匹配、统计分析、专家系统和完整性分析。其中前三种方法用于实时的入侵检测，而完整性分析则用于事后分析。目前在入侵检测系统中绝大多数属于模式匹配的特征检测系统，其他少量是采用概率统计的统计检测系统与基于日志的专家知识库系统。

1）模式匹配

模式匹配又称特征检测，就是先对已知的攻击或入侵的方式做出确定性的描述，形成相应的事件模式。当收集到的信息与已知的入侵事件模式相匹配时，即报警。其原理与专家系统相仿，检测方法与计算机病毒的检测方式类似。目前，基于对包特征描述的模式匹配应用较为广泛。该方法预报检测的准确率较高，但是对于无经验知识的入侵与攻击行为无能为力，需要不断地升级以对付不断出现的黑客攻击手法。

2）统计分析

统计分析方法首先为系统对象（如用户、文件、目录和设备等）创建一个统计描述，统计正常使用时的一些测量属性（如访问次数、操作失败次数、间隔时间、资源消耗情况等）的平均值。即基于对系统对象历史行为的建模系统要根据每个对象以前的历史行为，生成每个对象的历史行为记录库。

测量属性将被用来与网络、系统的目前行为进行比较，任何观察值在正常值范围之外

时,就认为有入侵发生。例如,统计分析可能标识如下不正常行为:一个在晚八点至早六点从不登录的账号却在深夜两点试图登录。其优点是可检测到未知的入侵和更为复杂的入侵;缺点是误报、漏报率高,且不适应系统对象正常行为的突然改变。

常用的入侵检测统计模型如下。

(1) 操作模型。该模型假设异常可通过测量结果与一些固定指标相比较得到,固定指标可以根据经验值或一段时间内的统计平均得到。例如,在短时间内的多次失败的登录很有可能是口令尝试攻击。

(2) 方差。计算参数的方差,设定其置信区间,当测量值超过置信区间的范围时表明有可能是异常。

(3) 多元模型。操作模型的扩展,通过同时分析多个参数实现检测。

(4) 马尔可夫过程模型。将每种类型的事件定义为系统状态,用状态转移矩阵来表示状态的变化,当一个事件发生时,若状态矩阵该转移的概率较小则可能是异常事件。

(5) 时间序列分析。将事件计数与资源耗用根据时间排成序列,如果一个新事件在该时间发生的概率较低,则该事件可能是入侵。

3) 专家系统

专家系统是在统计分析的基础上进一步发展起来的。用专家系统对入侵进行检测,经常是针对有特征的入侵行为。规则即知识,不同的系统与设备具有不同的规则,且规则之间往往无通用性。专家系统的建立依赖于知识库的完备性,知识库的完备性又取决于审计记录的完备性与实时性。入侵的特征抽取与表达,是入侵检测专家系统的关键。在系统实现中,将有关入侵的知识转换为 if-then 结构(也可以是复合结构),if 部分为入侵特征,then 部分是系统防范措施。运用专家系统防范有特征入侵行为的有效性完全取决于专家系统知识库的完备性。

该技术根据安全专家对可疑行为的分析经验来形成一套推理规则,然后在此基础上建立相应的专家系统,由此专家系统自动进行对所涉及的入侵行为的分析工作。该系统应当能够随着经验的积累而利用其自学习能力进行规则的扩充和修正。

4) 完整性分析

完整性分析主要关注某个文件或对象是否被更改,包括文件和目录的内容及属性,它在发现被更改的、被特洛伊化的应用程序方面特别有效。完整性分析使用消息摘要函数(如 MD5),它能识别哪怕是微小的变化。其优点是不管模式匹配方法和统计分析方法能否发现入侵,只要是成功的攻击导致了文件或其他对象的任何改变,它都能够发现;缺点是一般以批处理方式实现,不用于实时响应。尽管如此,完整性检测方法还应该是网络安全产品的必要手段之一。例如,可以在每一天的某个特定时间内开启完整性分析模块,对网络系统进行全面的扫描检查。

3. 响应

入侵检测响应方式分为被动响应和主动响应。

(1) 被动响应系统只会发出告警通知,将发生的不正常情况报告给管理员,本身并不试图降低所造成的破坏,更不会主动对攻击者采取反击行动。

(2) 主动响应系统可以分为对被攻击系统实施控制的系统和对攻击系统实施控制的系统。

对被攻击系统实施控制(防护),是通过调整被攻击系统的状态,阻止或减轻攻击影响,如断开网络连接、增加安全日志、杀死可疑进程等;对攻击系统实施控制(反击),这种系统多被军方所重视和采用。

目前,主动响应系统还比较少,即使做出主动响应,一般也都是断开可疑攻击的网络连接,或是阻塞可疑的系统调用,若失败,则中止该进程。但由于系统暴露于拒绝服务攻击下,这种防御一般也难以实施。

3.2.4　入侵检测系统的分类

1. 根据采用的技术和原理分类

根据入侵检测系统采用的技术和原理不同,可以分为异常检测、误用检测和特征检测三种。现有的入侵检测工具大都是使用误用检测方法。异常检测方法虽然还没有得到广泛的应用,但在未来的入侵检测系统中肯定会有更大的发展。

1) 异常检测

基于异常的检测技术有一个假设,就是入侵事件的行为不同于一般正常用户或者系统的行为。通过多种方法可以建立正常或者有效行为的模型。入侵检测系统在检测的时候就把当前行为和正常模型相比较,如果比较结果有一定的偏离,则报警异常。换句话说,所有不符合正常模型的行为都被认为是入侵。如果系统错误地将异常活动定义为入侵,称为错报;如果系统未能检测出真正的入侵行为,则称为漏报。

错报、漏报是衡量入侵检测系统性能很重要的两个指标。

基于异常检测的优点就是它能够检测出新的入侵或者从未发生过的入侵,还可以检测出属于权限滥用类型的入侵。它对操作系统的依赖性较小。

异常检测方法的查全率很高但是查准率很低。过多误警是该方法的主要缺陷,这是因为系统的所有行为不可能用一些有限的训练数据来描述,并且因为系统行为随时改变,所以必须要有一种在线的训练机制,实时地学会被认为误警的行为,使得系统模型尽量覆盖不被认为是入侵的行为。但随着检测模型的逐步精确,异常检测会消耗更多的系统资源。

常见的异常检测方法包括统计异常检测、基于特征选择的异常检测、基于贝叶斯推理的异常检测、基于贝叶斯网络的异常检测、基于模式预测的异常检测、基于神经网络的异常检测、基于贝叶斯聚类的异常检测、基于机器学习的异常检测等。目前一种比较流行的方法就是采用数据挖掘技术,来发现各种异常行为之间的关联性,包括源 IP 关联、目的 IP 关联、特征关联、时间关联等。

2) 误用检测

进行误用检测的前提是所有的入侵行为都有可被检测到的特征。误用检测系统提供攻击特征库,当检测的用户或系统行为与库中的记录相匹配时,系统就认为这种行为是入侵。如果入侵特征与正常的用户行为匹配,则系统会发生错报;如果没有特征能与某种新的攻击行为匹配,则系统会发生漏报。误用检测模型如图 3-6 所示。

采用特征匹配,误用检测能明显降低错报率,并且对每一种入侵都能提出详细资料,使得使用者能够更方便地做出响应,但漏报率随之增加。攻击特征的细微变化,会使得误用检测无能为力。

这种方法的缺陷是入侵信息的收集和更新比较困难,需要很多的时间和很大的工作量,

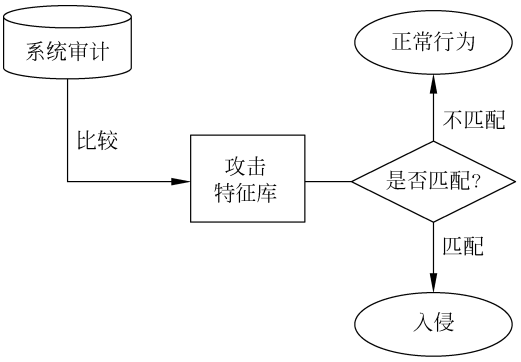


图 3-6 误用检测模型

以及很强的安全知识,如网络攻击、操作系统、系统平台、应用程序等方面的知识。所以,这种方法适用于特殊环境下的检测工具。另外,这种方法难以检测本地入侵(例如权限滥用),因为没有一个确定规则可以描述这些入侵事件。

常见的误用检测方法包括基于条件概率的误用入侵检测、基于专家系统的误用入侵检测、基于状态迁移的误用入侵检测、基于键盘监控的误用入侵检测、基于模型的误用入侵检测等。

以基于条件概率的误用入侵检测方法为例,该方法将入侵方式对应于一个事件序列,然后通过观测事件发生情况来推测入侵出现。这种方法的依据是外部事件序列。根据贝叶斯定理进行推理检测入侵。令 ES 表示事件序列,先验概率为 $P(\text{Intrusion})$,后验概率为 $P(\text{ES}|\text{Intrusion})$,事件出现的概率为 $P(\text{ES})$,则:

$$P(\text{Intrusion} \mid \text{ES}) = P(\text{ES} \mid \text{Intrusion}) \frac{P(\text{Intrusion})}{P(\text{ES})}$$

通常可以给出先验概率 $P(\text{Intrusion})$,对入侵报告数据进行统计处理得出 $P(\text{ES}|\text{Intrusion})$和 $P(\text{ES}|-\text{Intrusion})$,于是可以计算出:

$$P(\text{ES}) = ((P(\text{ES} \mid \text{Intrusion} - P(\text{ES}) \mid -\text{Intrusion})) \times P(\text{Intrusion}) + P(\text{ES} \mid -\text{Intrusion})$$

因此可以通过对事件序列的观测,推算出 $P(\text{Intrusion} \mid \text{ES})$。基于条件概率的误用入侵检测方法是在概率理论基础上的一个普遍的方法。它是对贝叶斯方法的改进,其缺点就是先验概率难以给出,而且事件的独立性难以满足。

3) 特征检测

和以上两种检测方法不同,特征检测关注的是系统本身的行为。定义系统行为轮廓,并将系统行为与轮廓进行比较,对未指明为正常行为的事件定义为入侵。特征检测系统常采用某种特征语言定义系统的安全策略。

这种检测方法的错报与行为特征定义准确度有关,当系统特征不能囊括所有的状态时就会产生漏报。

特征检测最大的优点是可以通过提高行为特征定义的准确度和覆盖范围,大幅度降低漏报和错报率;最大的不足是要求严格定义安全策略,这需要经验和技巧,另外,维护动态系统的特征库通常是很耗时的事情。

由于这些检测各有优缺点,许多实际的入侵检测系统通常同时采用两种以上的方法实现。

4）其他检测技术

一些检测技术不能简单地归类为误用检测或是异常检测，而是提供了一种有别于传统入侵检测视角的技术层次，例如，免疫系统、基因算法、数据挖掘、基于代理的检测等，它们或者提供了更具普遍意义的分析技术，或者提出了新的检测系统架构，因此无论是对于误用检测还是异常检测来说，都可以得到很好的应用。

作为人工智能的一个重要分支，神经网络在入侵检测领域得到了很好的应用，它使用自适应学习技术来提取异常行为的特征，需要对训练数据集进行学习以得出正常的行为模式，并且要求保证训练数据的纯洁性，即不包含任何入侵或异常的用户行为。神经网络由大量的处理元件组成，这些处理元件称为“单元”，单元之间通过带有权值的“连接”进行交互。神经网络所包含的知识体现在网络的结构（单元之间的连接、连接的权值）中，学习过程也就表现为权值的改变和连接的添加或阐述。神经网络的处理包含两个阶段：第一阶段的目的是构造入侵分析模型的检测器，使用代表用户行为的历史数据进行训练，完成网络的构建和组装；第二阶段则是入侵分析模型的实际运作阶段，网络接收输入的事件神经，与参考的历史行为相比较，判断出两者的相似度或偏离度。神经网络使用以下方法来标识异常的事件：改变单元的状态，改变连接的权值，添加连接或删除连接。同时也提供对所定义的正常模式进行逐步修正的功能。神经网络方法对异常检测来说，具有很多优势：由于不使用固定的系统属性集来定义用户行为，因此属性的选择是无关的；神经网络对所选择系统的量度也不要求满足某种统计分布条件，因此与传统的统计分析相比，具备了非参量化统计分析的优点。将神经网络应用在入侵检测中，也存在一些问题。例如，在很多情况下，系统趋向于形成某种不稳定的网络结构，不能从训练数据中学习到特定的知识，目前尚不能完全确定这种情况产生的原因。另外，神经网络对判断为异常的事件不会提供任何解释或说明信息，这导致了用户无法确认入侵的责任人，也无法判定究竟是系统哪方面存在的问题导致了攻击者得以成功地入侵。神经网络应用于入侵检测领域最大的问题在于检测的效率问题。最早提出使用神经网络来构造系统/用户行为模式的是 Fox，他使用 Kohonen 的 Self Organizing Map（SOM）自主学习算法来发现数据中隐藏的结构。杜兰大学的 David Endler 针对 Solaris 系统的 BSM 模块所产生的系统调用审计数据使用神经网络进行机器学习。Anup K. Ghosh 也采用针对特定程序的异常检测，建立软件程序的进程级行为模式，通过区分正常软件行为和恶意软件行为来发现异常。使用预先分类的输入资料对神经网络进行训练，学习区分正常和非正常的程序行为。Ghosh 还对简单的系统调用序列匹配、后向传播网络和 Elman 网络进行了比较。

新墨西哥大学的 Stephanie Forrest 提出了将生物免疫机制引入计算机系统的安全保护框架中。免疫系统最基本也是最重要的能力是识别“自我/非自我”，换句话讲，它能够识别哪些组织是属于正常机体的，不属于正常的就认为是异常，这个概念和入侵检测中异常检测的概念非常相似。研究人员通过大量的实验发现：对一个特定的程序来说，其系统调用序列是相当稳定的，使用系统调用序列来识别“自我”，应该可以满足系统的要求。在这个假设的前提下，该研究小组提出了基于系统调用的短序列匹配算法，并做了大量开创性的工作。

哥伦比亚大学的 Wenke Lee 在完成的博士论文中，提出了将数据挖掘技术应用到入侵检测中，通过对网络数据和主机系统调用数据的分析挖掘，发现误用检测规则或异常检测模

型。具体的工作包括利用数据挖掘中的关联算法和序列挖掘算法提取用户的行为模式,利用分类算法对用户行为和特权程序的系统调用进行分类预测。实验结果表明,这种方法在入侵检测领域有很好的应用前景。Wenke Lee 另一个突出的贡献是提出并验证了将信息论中"熵"的概念引入安全领域,用于解决入侵检测系统中的特性选择问题,构建检测模型。哥伦比亚大学数据挖掘实验室的 Leonid Portnoy 则使用了数据挖掘中的聚类算法,通过计算和比较记录间的矢量距离,对网络连接记录、用户登录记录进行自动聚类,从而完成对审计记录是否正常的判断工作。

基因算法是另外一种较为新颖的分析手段。基因算法是进化算法的一种,引入了达尔文在进化论中提出的自然选择的概念(优胜劣汰、适者生存)对系统进行优化。基因算法利用对"染色体"的编码和相应的变异及组合,形成新的个体。算法通常针对需要进行优化的系统变量进行编码,作为构成个体的"染色体",因此对于处理多维系统的优化是非常有效的。在基因算法的研究人员看来,入侵检测的过程可以抽象为:为审计事件记录定义一种向量表示形式,这种向量或者对应于攻击行为,或者代表正常行为。通过对所定义向量进行的测试,提出改进的向量表示形式,不断重复这个过程直到得到令人满意的结果。在这种方法中,将不同的向量表示形式作为需要进行选择的个体。基因算法的任务是使用"适者生存"的概念,得出最佳的向量表示形式。通常分为两个步骤来完成:首先使用一串比特对所有的个体(向量表示形式)进行编码;然后找出最佳选择函数,根据某些评估准则对系统个体进行测试,得出最为合适的向量表示形式。基因算法的典型代表是 GASSATA 系统。

近年来,一种基于代理的检测技术逐渐引起研究者的重视。所谓代理,实际上可以看作是在网络中执行某项特定监视任务的软件实体。代理通常以自治的方式在目标主机上运行,本身只受操作系统的控制,因此不会受到其他进程的影响。代理的独立性和自治性为系统提供了良好的扩展性和发展潜力。一个代理可以简单到仅对一段时间内某条命令被调用的次数进行计数,也可以复杂到利用数学模型对特定应用环境中的入侵做出判断,这完全取决于开发者的主观意愿。基于代理的入侵检测系统的灵活性保证它可以为保障系统的安全提供混合式的架构,综合运用误用检测和异常检测,从而弥补两者各自的缺陷。例如,可以将一个代理设置成通过模式匹配的算法来检测某种特定类型的攻击行为,同时可以将另一个代理设置为对某项服务程序异常行为的监视器,甚至将入侵检测的响应模块也作为系统的一个代理运行。Purdue 大学的研究人员为基于代理的入侵检测系统提出了一个基本原型,称为入侵检测自治代理(Autonomous Agents For Intrusion Detection,AAFID)。

针对基于代理的检测技术,Purdue 大学的 Terran Lane 提出了一种基于用户行为等级模型的异常检测引擎代理生成方法。等级模型的叶结点表示用户行为的临时结构,较高层次的结点则代表其子结点所表示结构间的相互关系。Lane 采用基于事例学习(IBL)和隐马尔可夫模型(HMM)的方法,通过基于时间的序列数据来学习实体的正常行为模式。对于利用隐马尔可夫模型(HMM)为用户行为建模,用于异常检测方面,Terran Lane 进行了深入的研究。

亚利桑那州大学的 Nong Ye 使用随机过程中的马尔可夫链模型来表示主机系统中的正常模式,通过对系统实际观察到的行为的分析,推导出正常模式的马尔可夫链模型对实际行为的支持程度,从而判断异常。处理的对象是系统中的特权程序所产生的系统调用序列。Nong Ye 还使用贝叶斯概率网络进行异常检测,提出了采用结点间无向连接的对称结构,

取代传统贝叶斯网络中的有向连接。采用接合点概率表取代原先的条件概率表，并修正了证据推论算法。

还有许多国内外的研究人员对入侵检测系统所使用的检测技术做了大量的研究工作，提出并实现了其他一些检测方法和原型系统，例如，基于流量分析的检测、基于入侵策略分析的检测等，在此不再一一介绍。

2. 根据检测的数据源分类

入侵检测系统的一个重要概念是从什么样的数据源检测入侵。根据数据来源的不同，入侵检测系统常被分为基于主机的入侵检测系统、基于网络的入侵检测系统和分布式入侵检测系统。

1）基于主机的入侵检测系统

基于主机的入侵检测系统（HIDS）通常是安装在被重点检测的主机之上，其数据源来自主机，如日志文件、审计记录等。通过监视与分析主机中的上述文件就能够检测到入侵。能否及时采集到上述文件是这些系统的弱点之一，因为入侵者会将主机的审计子系统作为攻击目标以避开入侵检测系统。

尽管基于主机的入侵检测系统不如基于网络的入侵检测系统快捷，但它确实具有基于网络的 IDS 无法比拟的优点。

（1）主要优点。

① 确定攻击是否成功。由于基于主机的 IDS 使用含有已发生事件信息，可以确定攻击是否成功。因此，基于主机的 IDS 是基于网络的 IDS 的完美补充；基于网络的 IDS 可以尽早提供警告，基于主机的 IDS 可以确定攻击成功与否。

② 能够检查到基于网络的入侵检测系统检查不出的攻击。例如，来自主要服务器键盘的攻击不经过网络，可以躲开基于网络的入侵检测系统，但躲不开基于主机的入侵检测系统。

③ 能够监视特定的系统活动。基于主机的 IDS 可以监视主要系统文件和可执行文件的改变，监视用户和访问文件的活动，包括文件访问、改变文件权限，试图建立新的可执行文件以及每位用户在网络中的行为；可以监视只有管理员才能实施的非正常行为，如有关用户账号的增加、删除、更改的情况；还可审计能影响系统记录的校验措施的改变；能够查出那些欲改写重要系统文件或者安装特洛伊木马或后门的尝试并将它们中断。而基于网络的 IDS 要做到这种程度是非常困难的，有时甚至查不到这些行为。

④ 适用被加密的和交换的环境。交换设备可将大型网络分成许多小型网络部件加以管理，所以从覆盖足够大的网络范围的角度出发，很难确定配置基于网络的 IDS 的最佳位置。基于主机的 IDS 可安装在所需的重要主机上，在交换的环境中具有更高的能见度。某些加密方式也向基于网络的 IDS 发出了挑战。由于加密方式位于协议堆栈内，所以基于网络的系统可能对某些攻击没有反应，基于主机的 IDS 则没有这方面的限制，当操作系统及基于主机的 IDS 看到即将到来的业务时，数据流已经被解密了。

⑤ 近于实时的检测和响应。尽管基于主机的 IDS 不能提供真正实时的反应，但如果应用正确，反应速度可以非常接近实时。

⑥ 不要求额外的硬件设备。基于主机的 IDS 存在于现行网络结构之中，包括文件服务器、Web 服务器及其他共享资源，不需要在网络上另外安装登记、维护及管理的硬件设备，

使得基于主机的 IDS 效率很高。

⑦ 低廉的成本。基于网络的入侵检测系统比基于主机的入侵检测系统要昂贵得多。

(2) 主要弱点。

① 基于主机的 IDS 安装在需要保护的设备上,如当一个数据库服务器需要保护时,就要在服务器本身安装入侵检测系统,这会降低应用系统的效率。此外,它也会带来一些额外的安全问题:安装了基于主机的 IDS 后,将本来安全管理员无权访问的服务器变成可以访问了。

② 基于主机的 IDS 依赖于服务器固有的日志与监视能力。如果服务器没有配置日志功能,则必须重新配置,这将会给运行中的业务系统带来不可预见的性能影响。

③ 全面部署基于主机的 IDS 代价较大,用户很难将所有主机用基于主机的 IDS 保护起来,只能选择保护部分重要主机。那些未安装基于主机的 IDS 的主机将成为保护的盲点,入侵者可利用这些机器达到攻击目标。

④ 基于主机的 IDS 除了监测自身的主机以外,根本不监测网络上的情况。对入侵行为的分析的工作量将随着主机数目的增加而增加。

2) 基于网络的入侵检测系统

基于网络的入侵检测系统(NIDS)放置在比较重要的网段内,其数据源是网络上规范的 TCP/IP 数据包,即通过在共享网段上对通信数据的侦听采集数据,对每一个数据包进行特征分析。如果数据包与系统内置的某些规则吻合,NIDS 的响应模块就提供多种选项实现通知、报警并对攻击采取相应的反应。反应因系统而异,但通常都包括通知管理员、中断网络连接、为法庭分析和证据收集而做好会话记录。NIDS 不需要主机提供严格的日志文件、审计记录,对主机资源消耗少,并可以提供对网络通用的保护而无须顾及异构主机的不同架构。目前,大部分入侵检测系统都是基于网络的。

基于网络的 IDS 如图 3-7 所示。第一个入侵检测系统放在防火墙的外面,以探查来自 Internet 的攻击,它不但能检测对内部网的攻击,还能检测对防火墙的攻击,但检测不到来自内部网的攻击。另一个传感器安装在网络内部以检测成功地穿过防火墙的数据包以及内部网络入侵和威胁,这个位置是基于网络的入侵检测系统常放的位置。

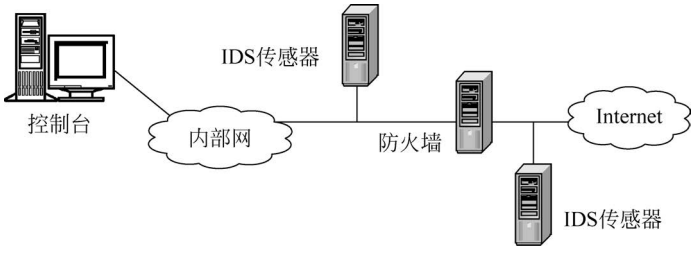


图 3-7 基于网络的 IDS

基于网络的 IDS 已经成为安全策略的实施中的重要组件,其主要特点如下。

(1) 主要优点。

① 成本较低。基于网络的 IDS 可在几个关键访问点上进行策略配置,以观察发往多个系统的网络通信,所以不要求在许多主机上装载并管理软件。由于需监测的点较少,因此成本较低。

② 可检测基于主机的IDS漏掉的攻击。基于网络的IDS检查所有包的头部从而发现恶意的和可疑的行动迹象。基于主机的IDS无法查看包的头部，所以它无法检测到这一类型的攻击。例如，许多来自于IP地址的拒绝服务型和碎片型攻击只要经过网络，都会在基于网络的IDS中被发现。

③ 攻击者不易转移证据。基于网络的IDS使用正在发生的网络通信进行实时攻击的检测，所以攻击者无法转移证据。被捕获的数据不仅包括攻击的方法，而且包括可识别的入侵者身份及对其进行起诉的信息。

④ 实时检测和响应。基于网络的IDS可以在恶意及可疑的攻击发生的同时将其检测出来，并做出更快的通知和响应。

⑤ 检测未成功的攻击和不良意图。基于网络的IDS增加了许多有价值的数据，以判别不良意图。

⑥ 操作系统无关性。基于网络的IDS作为安全检测资源，与主机的操作系统无关。与之相比，基于主机的系统必须在特定的、没有遭到破坏的操作系统中才能正常工作，生成有用的结果。

⑦ 安装简便。基于网络的IDS有向专门的设备发展的趋势，安装这样一个网络入侵检测系统非常方便，只需将定制的设备接上电源，做少量配置，将其连到网络上即可。

(2) 主要弱点。

① 检测范围的局限性。基于网络的IDS只检查它直接连接网段的通信，不能检测在不同网段的网络数据包，而安装多台基于网络的IDS将会使整个成本大大增加。

② 基于网络的IDS为了性能目标通常采用特征检测的方法，它可以检测出普通的一些攻击，而很难实现一些复杂的需要大量计算与分析时间的攻击检测。

③ 基于网络的IDS可能会将大量的数据传回分析系统中，影响系统性能和响应速度。

④ 基于网络的IDS处理加密的会话过程较困难，目前通过加密通道的攻击尚不多，但随着IPv6的普及，这个问题会越来越突出。

基于主机的入侵检测系统的检测范围小，只限于一台主机内，而基于网络的入侵检测系统的检测范围是整个网段。基于主机的入侵检测系统不但可以检测出系统的远程入侵，还可以检测出本地入侵。但是由于主机的信息多种多样，不同的操作系统信息源的格式就不同，使得基于主机的入侵检测系统比较难做。基于网络的入侵检测系统只能检测出远程入侵，对于本地入侵它是看不到的。可是由于网络数据一般都是规范的TCP/IP的数据包，所以基于网络的入侵检测系统比较易于实现。目前，大多数入侵检测的商业产品都是基于网络的入侵检测系统，基于主机的入侵检测系统只限于系统的安全工具。一个真正有效的入侵检测系统应该是基于主机和基于网络的混合，两种方法互为补充。

3) 分布式入侵检测系统

分布式入侵检测系统的数据也是来源于网络中的数据包，不同的是，它采用了分布式检测、集中管理的方法。即在每个网段安装一个黑匣子，该黑匣子相当于基于网络的入侵检测系统，只是没有用户操作界面。黑匣子用来检测其所在网段上的数据流，根据集中安全管理中心制定的安全策略、响应规则等来分析检测网络数据，同时向集中安全管理中心发回安全事件信息。集中安全管理中心是整个分布式入侵检测系统面向用户的界面。它的特点是对数据保护的范围比较大，但对网络流量有一定的影响。目前这种技术在ISS的RealSecure

等产品中已经有了应用。

3. 根据工作方式分类

根据工作方式可以分为离线检测系统与在线检测系统。

1) 离线检测系统

离线检测系统是非实时工作的系统,它在事后分析审计事件,从中检查入侵活动。事后入侵检测由网络管理人员进行,他们具有网络安全的专业知识,根据计算机系统对用户操作所做的历史审计记录判断是否存在入侵行为,如果有就断开连接,并记录入侵证据和进行数据恢复。事后入侵检测是由管理员定期或不定期进行的,不具有实时性。

2) 在线检测系统

在线检测系统是实时联机的检测系统,它包含对实时网络数据包的分析和实时主机审计分析。其工作过程是:实时入侵检测在网络连接过程中进行,系统根据用户的历史行为模型、存储在计算机中的专家知识以及神经网络模型对用户当前的操作进行判断,一旦发现入侵迹象,立即断开入侵者与主机的连接,并收集证据和实施数据恢复。这个检测过程是不断循环进行的。

3.3 系统恢复技术

在系统被入侵之后,就要面临系统的恢复过程。在此过程中应当注意的是,所有步骤都应该与组织的网络安全策略中所描述的相符。如果安全策略中没有描述如何进行系统的恢复,那么可以先和管理人员协商,这样做的好处在于,当管理人员得知系统被入侵后,可以从更高的角度判别出这一入侵事件的重要性,从而系统的恢复过程可以得到更多部门的支持和配合。另外一个重要的用处在于,组织可以因此决定是否进行法律相关的调查,系统在被入侵后,是否要进行法律调查诉讼等问题。

系统的恢复主要有重建系统、通过软件和程序恢复系统等方法。重建系统相对要容易一些,只要考虑到所得的结果,或者抹掉入侵者的痕迹、途径和其他安全隐患,重新试运行系统,或者是重新安装系统之后进行安全配置。一般说来,在系统重建之后,往往要经历一个试运行阶段,以判断目前的系统是否已经足够安全。

3.3.1 系统恢复和信息恢复

通过软件和程序恢复系统可以分为两方面:系统恢复和信息恢复。

(1) 系统恢复:是指根据检测和响应环节提供有关事件的资料修补该事件所利用的系统缺陷,不让黑客再次利用这样的缺陷入侵。一般系统恢复包括系统升级、软件升级、打补丁和除去后门等。

注意:打补丁和除去后门是不同的概念。一般来说,黑客在第一次入侵的时候都是利用系统的缺陷。在第一次成功入侵之后,黑客就会在系统中打开一些后门,如安装一个特洛伊木马。所以,尽管系统缺陷已经被打补丁,黑客下一次还可以通过后门进入系统。

(2) 信息恢复:是指恢复丢失的数据。信息恢复就是从备份的数据恢复原来的数据,其过程有一个显著特点,就是有优先级别。直接影响日常生活和工作的信息必须先恢复,这样可以提高信息恢复的效率。

3.3.2　系统恢复的过程

1. 切断被入侵系统的入侵者访问途径

为了夺回对被侵入系统的控制权，首先需要避免入侵者造成更严重的破坏。如果在恢复过程中，没有断开被侵入系统的入侵者访问途径，入侵者就可能破坏恢复工作。曾经发生过这样的事情，在恢复过程中，系统管理员发现自己所进行的修改完全没有起到预想中的作用，事后才发现当自己修改配置的时候，入侵者同时也在进行操作。切断入侵系统的入侵者访问途径，可以有多种选择。如果入侵者来自于网络，可以将其从网络上断开。如果确认入侵者来自于外部网络，可以在边界防火墙上进行恰当的设置，以确保入侵者无法再进行访问。断开以后，可以进入 UNIX 系统的单用户模式或者 NT 的本地管理者模式进行操作，以夺回系统控制权。不过，这样做的代价是，可能会丢失一些有用的信息，例如，入侵者正在运行的扫描进程或监听进程。另外，如果决定要追踪入侵者，那么也可以不采取这些措施，以避免被入侵者察觉，但是这时应当采取其他措施保护那些内部网络中尚未被入侵的机器，以避免入侵的蔓延。

在对系统进行恢复的过程中，如果系统处于 UNIX 单用户模式下，会阻止用户、入侵者和入侵进程对系统的访问或者对主机的运行状态的意外改变。

2. 复制一份被侵入系统

在进行入侵分析之前，最好先备份被侵入的系统，这些原始的数据和记录，会起到很多的重要作用。如果将来决定进行法律诉讼，那么这些数据也将会成为有力的证据。在必要的时候，可以将这些数据保存为档案。可以使用 UNIX 命令 dd 将被侵入系统复制到另外一个硬盘。

例如，在一个有两个 SCSI 硬盘的 Linux 系统中，以下命令将在相同大小和类型的备份硬盘(/dev/sdb)上复制被侵入系统(在/dev/sda 盘上)的一个副本：

```
#dd if=/dev/sda of=/dev/sdb
```

还有一些其他的方法可以备份被侵入的系统。在 NT 系统中没有类似的内置命令，但可以使用一些第三方的程序复制被侵入系统的整个硬盘。在记录下备份的卷标、标志和日期后，将其保存到一个安全的地方以避免损坏。

3. 入侵途径分析

分析入侵途径，重要的在于分析入侵者提升自己权限的手段；否则，即使重新安装了系统，也无法保证系统会是安全的。入侵途径的分析，还有助于发现入侵者留下的后门和对系统的改动。这些信息对于评估系统的受损程度，有着重要的意义。

1) 分析日志文件、显示器输出及新增的文件

对系统情况进行分析并特别注意日志文件、显示器输出以及新增的文件，可以发现入侵者进入的途径。

日志文件是发现入侵者最有力的工具，很多入侵程序都利用了系统或服务程序运行时的异常情况，这些异常情况往往会留下一些记录。有的时候，聪明的入侵者会把这些记录抹去，但是显示器上的输出却仍然留了下来。另外，入侵者所留下的文件有时也可以显示出他所使用的攻击手段。同时，入侵检测系统和防火墙也能够提供最可信的证据。

2) 详细地审查系统日志文件

审查日志,最基本的一条就是检查异常现象。详细地审查系统日志文件,可以了解到系统是如何被侵入的,在入侵过程中,攻击者执行了哪些操作,以及哪些远程主机访问了系统等信息。

(1) UNIX 系统日志。

以下是一个通常使用的 UNIX 系统日志文件列表。由于系统配置的不同,它们在系统中的位置可能有所不同。可以查看/etc/Syslogconf 文件确定日志文件的具体位置。

① Messages: Messages 日志文件保存了大量的信息。可以从这个文件中发现异常信息,检查入侵过程中发生了哪些事情。

② Xferlog: 如果被侵入系统提供 FTP 服务,Xferlog 文件就会记录下所有的 FTP 传输。这些信息可以帮助确定入侵者向系统上传了哪些工具,以及从系统下载了哪些东西。

③ Utmp: 保存当前登录每个用户的信息,使用二进制格式。这个文件只能确定当前登录用户。使用 who 命令可以读出其中的信息。

④ Wtmp: 每次用户成功的登录、退出以及系统重启,都会在 Wtmp 文件中留下记录。

⑤ Syslogconf 文件也使用二进制格式,需要使用工具程序从中获取有用的信息。last 就是一个这样的工具,它输出一个表,包括用户名、登录时间、发起连接的主机名等信息,检查在这个文件中记录的可疑连接,有助于确定牵扯到这起入侵事件的主机,并找出系统中可能被侵入的账号。

⑥ Secure: 某些版本的 UNIX 系统(例如 Red Hat Linux)会将 TCP_wrappers 信息记录到 Secure 文件中。如果系统的 inetd 使用 TCP_wrappers,每当有连接请求超出了 inetd 提供的服务范围,就会在这个文件中加入一条日志信息。通过检查这个日志文件,可以发现一些异常服务请求,或者从陌生的主机发起的连接。

(2) Windows 日志。

Windows NT 或者 Windows 2000 通常使用三个日志文件,记录所有的 NT 事件,每个 NT 事件都会被记录到其中的一个文件中,可以使用 Event Viewer 查看日志文件。其他一些 NT 应用程序可能会把自己的日志放到其他的地方,例如,ISS 服务器默认的日志目录是 c:\winnt\system32\logfiles。

3) 检查入侵检测系统和防火墙

很多入侵者会把所有相关的日志记录全部抹掉,这时,如果系统外部运行有入侵检测系统和防火墙,往往可以提供更宝贵的信息。好的入侵检测系统不仅可以发现有什么样的攻击,还可以判断出这一攻击是否已经成功。而且,入侵者在入侵前所运行的扫描软件,一般也可以被入侵检测系统发觉。检查入侵检测系统,通常就足以发现有关此次入侵途径的足够的信息。

除了这些方法之外,对入侵者遗留物的分析也是一个发现线索的重要内容。遗留物的分析还关系到后门的清除,下面就详细介绍这方面的内容。

4. 遗留物分析

1) 检查入侵者对系统软件和配置文件的修改

(1) 校验系统中所有的二进制文件。

在检查入侵者对系统软件和配置文件的修改时,一定要记住: 所使用的校验工具本身

可能已经被修改过，操作系统的内核也有可能被修改了，这在目前来说，已经越来越普遍了。因此，建议用一个可信的内核启动系统，然后使用一个静态连接的干净的系统来进行检查。对于 UNIX 系统，可以通过建立一个启动盘，然后对其写保护来获得一个可信的操作系统内核。

彻底检查所有的系统二进制文件往往是十分必要的，可以把它们与原始发布介质（例如光盘）做比较，以确保攻击者没有在系统中安装特洛伊木马。在 NT 系统上，特洛伊木马通常会传播病毒，或者所谓的“远程管理程序”，如 BackOrifice 和 NetBus，特洛伊木马会取代处理网络连接的一些系统文件。

目前，由于一些工具的流行，一些木马程序具有和原始二进制文件相同的时间戳和 sum 校验值，通过简单的校验和无法判断文件是否被修改。因此，通常可以采用两种方法进行比较：一种是使用 cmp 程序直接把系统中的二进制文件和原始发布介质上对应的文件进行比较，另外一种则是比较二者的 md5 校验值。

（2）校验系统配置文件。

在 UNIX 系统中，应该进行如下检查。

① 检查/etc/passwd 文件中是否有可疑的用户。

② 检查/etc/inetconf 文件是否被修改过。

③ 如果系统允许使用 r 命令，如 rlogin、rsh、rexec，则需要检查/etc/host sequiv 或者 rhosts 文件。检查新的 SUID 和 SGID 文件。通过下面的命令会打印出系统中的所有 SUID 和 SGID 文件。

对于 NT 系统，通常需要进行如下检查。

① 检查不成对的用户和组成员。

② 检查启动登录或者服务的程序的注册表入口是否被修改。

③ 检查“netshare”命令和服务器管理工具共有的非验证隐藏文件。

④ 检查 pulistexe 程序无法识别的进程。

2）检查被修改的数据

入侵者经常会修改系统中的数据，所以建议对 Web 页面文件、FTP 存档文件、用户目录下的文件以及其他的文件进行校验。

3）检查入侵者留下的工具和数据

入侵者通常会在系统中安装一些工具，以便继续监视被侵入的系统。入侵者一般会在系统中留下如下种类的文件。

（1）网络监听工具。网络监听工具就是监视和记录网络行动的一种工具程序。入侵者通常会使用网络监听工具获得在网络上以明文进行传输的用户名和密码。

（2）特洛伊木马程序。特洛伊木马程序能够在表面上执行某种功能，而实际上执行另外的功能。因此，入侵者可以使用特洛伊木马程序隐藏自己的行为，获得用户名和密码数据，建立后门以便将来再次访问被侵入系统。

（3）安全缺陷攻击程序。系统运行存在安全缺陷的软件是其被侵入的一个主要原因。入侵者经常会使用一些针对已知安全缺陷的攻击工具，以此获得对系统的非法访问权限。这些工具通常会留在系统中，保存在一个隐蔽的目录中。

（4）后门。后门程序将自己隐藏在被侵入的系统中，入侵者通过它就能够不通过正常

的系统验证,不必使用安全缺陷攻击程序就可以进入系统。

由于后门会给系统的安全带来极大的影响,因此在系统被入侵后,后门的清除就成了一个重要的问题。常用的后门检测和清除工具软件有 lsof、Tripwire、chkrootkit 等。

① lsof:一个用于查看进程所打开文件的工具。在系统恢复过程中使用这个工具,最常用的功能是定位端口和进程的关系。通常可以发现一个正在运行的进程所打开的文件,这样,有助于通过可疑进程发现那些入侵者遗留物的具体位置;还可以用来发现某个端口所对应的进程,在系统恢复过程中,常常会用外部扫描程序来发现系统是否有木马存在,如果发现提供后门的端口,那么就需要确定这一端口是由哪个程序所占用,这时使用 lsof 程序,就能够达到这个目的。

② Tripwire:一个完整性检测工具,用来检测对文件系统的未授权修改。

③ chkrootkit:专门为发现系统中的 chkrootkit 而设计的,基本上可以发现所有著名的后门程序(但并不能清除)。chkrootkit 由 7 个小程序组成,主程序是 chkrootkit,用于发现各种后门。其余的几个分别是 ifpromisc,用于检测某个网络接口是否处于混杂模式;chklastlog、chkwtmp、chkwtmpx,用于检测系统的 3 个日志文件是否曾经遭到过破坏;chkproc,用于发现 LKM 隐藏的进程;strings 与 UNIX 自带的 strings 类似。

(5) 入侵者使用的其他工具。以上所列无法包括全部的入侵工具,攻击者在系统中可能还会留下其他入侵工具,包括系统安全缺陷探测工具、对其他站点发起大规模探测的脚本、发起拒绝服务攻击的工具、使用被侵入主机计算网络资源的程序、入侵工具的输出。

还有可能会发现入侵工具程序留下的一些日志文件,其中包含着其他相关站点,例如,攻击者的"大本营"站点,或者是入侵者利用这一系统攻破的其他站点。

因此,建议对系统进行彻底的搜索,找出上面列出的工具及其输出文件。一定要注意:在搜索过程中,要使用没有被攻击者修改过的搜索工具。主要搜索下面的内容。

① 检查 UNIX 系统/dev 下以外的 ASCII 文件。一些特洛伊木马二进制文件使用的配置文件通常在/dev 目录中。

② 仔细检查系统中的隐藏文件和隐藏目录。如果入侵者在系统中建立一个新的账户,那么这个新账户的起始目录及其使用的文件可能是隐藏的。

③ 检查一些名字非常奇怪的目录和文件。例如,(三个点)(两个点)以及空白(在 UNIX 系统中)。入侵者通常会在这样的目录中隐藏文件。对于 NT 系统,应该检查那些名字和一些系统文件名非常接近的目录和文件。

4) 检查网络监听工具

入侵者侵入一个 UNIX 系统后,为了获得用户名和密码信息,一般会在系统上安装一个网络监听程序。对于 NT 系统,入侵者则通常使用远程管理程序实现上述目的。判断系统是否被安装了监听工具,首先要看当前是否有网络接口处于混杂(Promiscuous)模式下。如果任何网络接口处于混杂模式下,就表示系统可能被安装了网络监听程序。使用 ifconfig 命令就可以知道系统网络接口是否处于混杂模式(注意一定使用没有被入侵者修改的 ifconfig):

```
ifconfig -a
```

有一些工具程序如 cpm、ifstatus、nepedc 等可以用来检测系统内的监听程序。

不过一些合法的网络监听程序和协议分析程序也会把网络接口设置为混杂模式,因此,检测到系统处于混杂模式后,还应当找出使用该设备的系统进程。在 UNIX 下,可以使用

lsof 来找出。根据相应的进程名字，才可以断定是否这是一个入侵者建立的监听程序。

还有一个应该注意的问题，监听程序的日志文件通常会增加较快。使用 df 或者 find 程序来发现变化过快的文件或者比较大的文件，有时也可以发现监听程序的蛛丝马迹。使用 lsof 程序发现进程打开文件、设备的情况，也可以起到一定的作用。一旦在系统中发现了监听程序，建议检查监听程序的输出文件以确定哪些主机可能会面临攻击威胁。不过，一些监听程序会给日志文件加密以增加检查的难度。

5. 检查网络上的其他系统和涉及的运送站点

除了已知被侵入的系统外，还应该对网络上所有的系统进行检查。主要检查和被侵入主机的共享网络服务（例如：NIS、NFS）或者通过一些机制（例如：hostsequiv、rhosts 文件，或者 kerberos 服务器）和被侵入主机相互信任的系统，以发现这些系统是否也被入侵了。可以使用 CERT 的入侵检测检查列表进行这一步检查工作。

在审查日志文件、入侵程序的输出文件和系统被侵入以来被修改的和新建立的文件时，要注意哪些站点可能会连接到被侵入的系统。根据经验，那些连接到被侵入主机的站点，通常已经被侵入了。所以要尽快找出其他可能遭到入侵的系统，通知其管理人员。

6. 评估入侵事件的影响，恢复系统

以上所有对入侵的分析，都是为了对入侵所造成的影响进行恰当的评估，借以决定所应采取的措施，同时恢复系统。对入侵所造成的影响进行评估，是一件相当困难的过程。入侵所造成的损害，可以有以下几方面。

（1）对数据保密性的损害。发生入侵之后，需要判断哪些保密的数据有可能已经泄露，这些信息的泄露造成多大的影响，需要采取的应对措施造成的开销。

（2）对数据完整性造成的损害。这些数据的损害、丢失所造成的影响。这些数据是否已经被传给了第三方，是否会因此承受其他损失。

（3）声誉、信任度、媒体报道所造成的影响。这些影响所造成的潜在损失。

当然，影响不仅限于这些方面，尤其是当一次入侵事件广为人知时，所造成的损害更难于评估。

在评估出影响后，根据事件处理当中所得到的资料，组织可以决定出对此次事件是否采取一些追加措施。例如，是否进行入侵追踪，是否借助于媒体进行一些公告，是否向入侵者来源地报告，是否提起法律诉讼等。恰当的追加措施往往能够削减一部分由于入侵产生的不利影响。由于进一步措施的采取涉及很多的法律问题，因此可以向组织的法律顾问进行咨询，在此就不进行详细论述了。

习　　题

1. 攻击者常用的攻击工具有哪些？
2. 简述口令入侵的原理。
3. 简述网络攻击的步骤。画出黑客攻击企业内部局域网的典型流程。
4. 攻击者隐藏自己的行踪时通常采用哪些技术？
5. 简述网络攻击的防范措施。
6. 简述网络攻击的处理对策。

7. 一个成熟的入侵检测系统至少要满足哪5个要求?

8. 简述入侵检测系统的组成、特点。

9. 分别说明入侵检测系统的通用模型和统一模型。

10. 简述入侵检测的过程。

11. 什么是异常检测、误用检测、特征检测?

12. 基于主机的IDS和基于网络的IDS各有什么特点?

13. 你曾遇到过何种类型的网络攻击?采取了哪些措施保护你的计算机网络系统?

14. 攻击者入侵系统后通过更改系统中的可执行文件、库文件或日志文件来隐藏其活动,如果你是系统安全管理员,你将通过何种方法检测出这种活动?

15. 系统恢复过程中应对哪些遗留物进行分析?

16. 简述系统的恢复过程。

17. 上机练习:利用端口扫描程序,查看网络上的一台主机,这台主机运行的是什么操作系统?该主机提供了哪些服务?

18. 上机练习:安装并运行SATAN,查找网上FTP站点的漏洞。