网络攻击的种类分析

何欣

摘要:随着 INTERNET 的进一步发展,各种网上活动日益频繁,尤其网上办公、交易越来越普及,使得网络安全问题日益突出,各种各样的网络攻击层出不穷,如何防止网络攻击,保护个人、单位的网络环境变得尤为重要。

关键词:网络攻击 种类

1 网络攻击概述

网络安全是一个永恒的话题,因为计算机只要与网络连接就不可能彻底安全,网络中的安全漏洞无时不在,随着各种程序的升级换代,往往是旧的安全漏洞补上了,又存在新的安全隐患,网络攻击的本质实际上就是寻找一切可能存在的网络安全缺陷来达到对系统及资源的损害。

网络攻击一般分为三个阶段:

第一阶段:获取一个登录账号 对 UNLX 系统进行攻击的首要目标是设法获取登录账号及口令,攻击者一般先试图获取存在于 /etc/passwd 或 NIS 映射中的加密口令文件,得到该口令文件之后,就对其运行 Crack,借助于口令字典,Crack 甚至可以在几分钟内破译一个账号。

第二阶段:获取根访问权 进入系统后,入侵者就会收集各种信息,寻找系统中的种种漏洞,利用网络本身存在的一些缺陷,设法获取根访问权,例如未加限制的 NFS 允许根对其读和写。利用 NFS 协议,客户给与服务器的安装守护程序先交换信息,信息交换后,生成对 NFS 守护程序的请求,客户通过这些请求对服务器上的文件进行读或写操作。因此,当客户机安装文件系统并打开某个文件时,如果入侵者发出适当各式的 UDP 数据报,服务器就将处理 NFS 请求,同时将结果回送客户,如果请求是写操作,入侵者旧可以把信息写入服务器中的磁盘。如果是读操作,入侵者就可以利用其设置于服务器和客户机之间的窥探器了解服务器磁盘中的信息,从而获得根访问权。

第三阶段:扩展访问权 一旦入侵者拥有根访问权,则该系统即可被用来供给网络上的其他系统。例如:可以对登录守护程序作修改以便获取口令;增加包窥探仪可获取网络通信口令;或者利用一些独立软件工具动态地修改 UNLX 内核,以系统中任何用户的身份截击某个终端及某个连接,获得远程主机的访问权。

2 攻击的种类及其分析

普通的攻击一般可分以下几种:

2.1 拒绝服务攻击 拒绝服务攻击不损坏数据,而是拒绝为用户服务,它往往通过大量不相关的信息来阻断系统或通过向系统发出会,毁灭性的命令来实现。例如入侵者非法侵入某系统后,可向与之相关连的其他系统发出大量信息,最终导致接收系统过载,造成系统误操作甚至瘫痪。这种供给的主要目的是降低目标服务器的速度,填满可用的磁盘空间,用大量的无用信息消耗系统资源,是服务器不能及时响应,并同时试图登录到工作站上的授权账户。例如,工作站向北供给服务器请求 NISpasswd 信息时,攻击者服务器则利用被攻击服务器不能及时响应这一特点,替代被攻击服务器做出响应并提供虚假信息,如没有口令的纪录。由于被攻击服务器不能接收或及时接收软件包,它就无法及时响应,工作站将把虚假的响应当成正确的来处理,从而使带有假的 passwd 条目的攻击者登录成功。

2.2 同步(SYN)攻击 同步供给与拒绝服务攻击相似,它摧毁正常通信握手关系。在 SYN 供给发生时,攻击者的计算机不回应其它计算机的 ACK,而是向他发送大量的 SYN ACK 信息。通常计算机有一缺省值,允许它持特定树木的 SYN ACK 信息,一旦达到这个数目后,其他人将不能初始化握手,这就意味着其他人将不能进入系统,因此最终有可能导致网络的崩溃。

2.3 Web 欺骗攻击 Web 欺骗的关键是要将攻击者伪造的

(上接第 296 页)

认证、授权、审计有机地结合,保证只有合法用户才能使用其拥有运维权限的关键资源。为 IT 操作风险控制、内控安全和合规性等方面提供一套完善、有效的审计手段。

3.3.1 实现对基于 TELNET、FTP、SFTP、SSH、RDP、VNC 等协议进行审计,支持 IBM AIX、Digital UNIX、HP UNIX、SUN Solaris、SCO UNIX、LINUX、WINDOWS 等各种主流操作系统环境。

3.3.2 系统具有完整的身份管理和认证功能。为了确保合法用户才能访问其拥有权限的后台资源,解决 IT 系统中普遍存在的交叉运维而无法定位到具体人的问题,满足审计系统"谁做的"要求。系统必须具有完整的身份管理和认证功能,并能结合第三方的的安全认证方式,实现静态口令、动态口令、证书 KEY 和第三方的令牌认证方式的安全认证管理,实现密码强度、密码效期、口令尝试死锁、用户激活等安全管理功能。

3.3.3 灵活、细粒度的授权功能,系统提供基于用户、运维协议、目标主机、运维时间段(年、月、日、周、时间)、会话时长、运维客户端 IP 等组合的授权功能,实现细粒度授权功能,满足用户实际授权的需求。

3.3.4 后台资源自动登陆功能,后台资源自动登陆功能是运维人员通过系统认证和授权后,系统根据配置策略实现后台资源的自动登录。此功能提供了运维人员到后台资源账户的一种可控对应,同时实现了对后台资源帐户的口令统一保护。针对不同操作系统和设备的特性,可以提供托管和只托不管两种方式实现运维用户自动登录后台资源。

3.3.5 实时监控功能:监控正在运维的会话,信息包括运维用户、运维客户端地址、资源地址、协议、开始时间等;监控后台资源被访问情况;提供在线运维的操作的实时监控功能。针对命令交互性协议可以图像方式实时监控正在运维的各种操作,其信息与运维客户端所见完全一致。

3.3.6 违规操作实时告警与阻断功能:针对运维过程中可能存在潜在操作风险,系统根据用户配置的安全策略实施运维过程中的违规操作检测,对违规操作提供实时告警和阻断,从而达到降低操作风险及提高安全管理与控制的能力。

3.3.7 完整记录网络会话过程功能:系统提供运维协议 Telnet、FTP、SSH、SFTP、RDP(Windows Termina)、AS400 等网络会话的完整会话记录,完全满足内容审计中信息百分百不丢失的要求;会话信息包括运维用户、运维地址、后台资源地址、资源名、协议、起始时间、终止时间、流量大小信息;会话信息包括运维过程中所有进出后台资源的数据。

3.3.8 详尽的会话审计与回放功能。运维操作审计以会话为单位,提供当日和条件查询定位。条件查询支持按运维用户、运维地址、后台资源地址、协议、起始时间、结束时间和操作内容中关键字等组合方式。

3.3.9 完备的审计报表功能,能根据需要智能定制各种报表。

4 结语

IT 基础设施在运行维护过程中的安全是信息系统安全的基础中的基础,而它安全受运行环境、运行人员的操作水平等物理、人文等因素的影响,本文通过分析 IT 基础设备在运行维护管理中存在的风险以及如何针对这些风险采取相关的对策控制和规避这些风险,具体就是加强对 IT 运行环境的监控及管理以保证运行环境满足 IT 基础设施的运行需要、通过对 IT 基础设施的远程集中控制提高设备的物理安全、通过对 IT 基础设施的运行审计从而提高其在维护管理过程中的安全性,提出了一个发电企业管理信息系统的 IT 基础设施的集中管控的解决方案。

Web 服务器在逻辑上置于用户与目的 Web 服务器之间，使用户的所有信息都在攻击者的监视之下。一般 Web 欺骗使用两种技术：URL 地址重写技术和相关信息掩盖技术。

利用 URL 地址重写技术，攻击者重写某些重要的 Web 站点上的所有 URL 地址，使这些地质均指向攻击者的 Web 服务器。

当用户与站点进行安全链接时，则会毫无防备地进入攻击者服务器。此时用户浏览器首先向攻击者服务器请求访问，然后由攻击者服务器向真正的目标服务器请求访问，目标服务器向攻击服务器传回相关信息，攻击者服务器重写传回页面后再传给用户。此时浏览器呈现给用户的的确是一个安全链接，但连接的对象却是攻击者服务器。用户向真正 Web 服务器所提交的信息和真正 Web 服务器传给用户的所有信息均要经过攻击者服务器，并受制于它，攻击者可以对所有信息进行记录和修改。

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连接时，可以在地址栏中和状态栏中获取连接中的 Web 站点地址及相关的传输信息，用户可由此发现问题，所以一般攻击者往往在 URL 地址重写的同时，利用相关信息掩盖技术即一般用的 JavaScript 程序来地址栏和状态栏信息，以达到其掩盖欺骗的目的。

2.4 TCP/IP 欺骗攻击 IP 欺骗可发生在 IP 系统的所有层次上，包括硬件数据链路层、IP 层、传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结构相互交流，有时甚至根本没有意识到这些结构的存在，因而对底层的攻击更具欺骗性。

IP 欺骗供给通常是通过外部计算机伪装成另一台合法机器来实现的。他能破坏两台机器间通信链路上的正常数据流，也可以在通信链路上插入数据，其伪装的目的在于哄骗网络中的其他机器误将攻击者作为合法机器而加以接受，诱使其他机器向它发送数据或允许它修改数据。

由于许多应用程序最初设计时就是把信任建立于发送方 IP 地址的薄，即如果包能够使其置身沿着陆由到达目的地，并且应答包也可以回到原地，则可以肯定源 IP 地址是有效的。因此一个攻击者可以通过发送有效 IP 源地址属于另一台机器的 IP 数据报来实施欺骗。

一方面现有路由器的某些配置使得网络更容易受到 IP 欺骗攻击。例如有些路由器不保护 IP 包端口源的信息，来自端口的所有 IP 包被装入同一个队列然后逐个处理。假如包指示 IP 源地址来自内部网络，则该包可转发。因此利用这一点网络外不用户只要设法表明是一种内部 IP 地址即可绕过路由器法送报。

另一方面，攻击者使用伪造的 IP 地址发送数据报，不仅可以获取数据报特有的有效请求，还可以通过预测 TCP 字节顺序号迫使接收方相信其合法而与之进行连接，从而达到 TCP 欺骗连接。

3 网络上常见的几种攻击方式

3.1 密码攻击 用户在拨号上网时，如果选择了“保存密码”的功能，则上网密码将被储存在 windows 目录中，以“username.pwl”的形式存放。如果不小心被别人看到这个文件，那就麻烦了，因为从网上可以很轻松地找到诸如 pwlview 这样的软件来观看其中的内容，那上网密码就泄漏了。

有的人使用名字、生日、电话号码等来做密码，更有的人的密码干脆和用户名一样，这样的密码，在黑客攻击软件庞大的字典文件面前简直是不堪一击。

3.2 木马程序攻击 木马程序是一种特殊的病毒，它通过修改注册表等手段使自己悄悄地潜伏在系统中，在用户上网后，种植木马的黑客就可以通过服务器端木马程序控制你的计算机，获取你的口令等重要信息，其危害性非常大。

3.3 垃圾邮件攻击 垃圾邮件是指向他人电子信箱发送未经许可的，难以拒绝的电子邮件或电子邮件列表，其内容包括广告信息、电子杂志、网站信息等。用户的电子信箱被这些垃圾邮件充斥后，会大大占用网络资源，导致网络阻塞，严重的还会使用户的邮箱被“炸”掉，使邮箱不能正常工作。

3.4 通过聊天软件攻击 用户在用聊天软件聊天时，黑客用一些小软件就可查出对方聊天者的 IP 地址，然后通过 IP 炸弹阮家对用户的机器进行轰炸，使之蓝屏或死机。

4 网络攻击的六大趋势

4.1 自动化程度和攻击速度提高 攻击工具的自动化水平不断提高。自动化攻击涉及四个阶段，每个阶段都出新变化。

扫描可能的受害者。自 1997 年起，广泛的扫描变得司空见惯。目前，扫描工具利用更先进的扫描模式来改善扫描效果和提高扫描速度。

损害脆弱的系统。以前，安全漏洞只在广泛的扫描完成后才被加以利用。而现在攻击工具利用这些安全漏洞作为扫描活动的一部分，从而加快了攻击的传播速度。

传播攻击。在 2000 年之前，攻击工具需要人来发动新一轮攻击。目前，攻击工具可以自己发动新一轮攻击。像红色代码和尼姆达这类工具能够自我传播，在不到 18 个小时内就达到全球饱和点。

攻击工具的协调管理。随着分布式攻击工具的出现，攻击者可以管理和协调公布在许多 Internet 系统上的大量一部书的攻击工具。目前，分布式攻击工具能够更有效地发动拒绝服务攻击，扫描潜在的受害者，危害存在安全隐患的系统。

4.2 攻击工具越来越复杂 攻击工具开发者正在利用更先进的技术武装攻击工具。与以前相比，攻击工具的特征更难发现，更难利用特征进行检测。攻击工具有三个特点：反侦破，攻击者采用隐蔽攻击工具特性的技术，这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；动态行为，早期的攻击工具是以但已确定的顺序执行攻击步骤，今天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，来变化它们的模式和行为；攻击工具的成熟性，与早期的攻击工具不同，目前攻击工具可以通过升级或更换工具的一部分迅速变化，发动迅速变化的功绩，且在每一次攻击中会出现多种不同形态的攻击工具。

4.3 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复这些漏洞，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。

4.4 越来越高的防火墙渗透率 防火墙使人们牙防反入侵者的主要保护措施。但是越来越多的攻击技术可以绕过防火墙。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。

4.5 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 上其他系统的阿安全状态。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术的提高，威胁的不对称性将继续增加。

4.6 对基础设施将形成越来越大的威胁 基础设施攻击是大面积影响 Internet 关键组成部分的攻击。由于用户越来越多地依赖 Internet 完成日常业务，基础设施攻击引起人们越来越大的担心。基础设施面临分布式拒绝服务攻击、蠕虫病毒、对 Internet 域名系统 DNS 的攻击和对路由器攻击或利用路由器的攻击。

通过对以上攻击方法和原理的介绍，我们将逐步研究防范攻击的对策，相信攻击与被攻击者的战争还会不断持续下去，这将对我们更深的了解计算机网络安全问题形成巨大的推动力。