安全威胁每周警讯

2012/04/22～2012/04/29

本周威胁指数

***TrendMicro* 中国区网络安全监控中心**

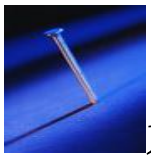
前十大病毒警讯

排名	病毒名称	威胁类型	风险等级	趋势	病毒行为描述
1	WORM_DOWNAD.AD	蠕虫	★★★★	↑	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
2	WORM_DOWNAD	蠕虫	★★★★	↑	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
3	TROJ_DOWNAD.INF	木马	★★★	↓	DOWNAD 蠕虫关联木马
4	TROJ_IFRAME.CP	木马	★★★	→	GIF、jpg 和 SWF 文件中被插入一个恶意的 iframe 标记时，趋势科技会将其判断为 TROJ_IFRAME.CP 病毒。当这些文件被执行时，会重定向到这些 URL，并下载恶意程序
5	X97M_LAROUX.BK	脚本病毒	★★	↑	Office 宏病毒，主要感染 Excel 文件，会在 Excel 中创建一个名为 *StartUp* 的自启动宏脚本
6	HTML_IFRAME.BWC	网页病毒	★★	↑	网页病毒,通常在网页在插入一个恶意 iframe,用户在访问该网页时会下载恶意文件或重定向到恶意网站
7	HTML_IFRAME.AZ	网页病毒	★★	↑	网页病毒,通常在网页在插入一个恶意 iframe,用户在访问该网页时会下载恶意文件或重定向到恶意网站
8	WORM_ECODE.E-CN	蠕虫	★★★★	↑	E 语言病毒,产生与当前文件夹同名 exe 文件
9	JS_EXPLOIT.MO	脚本病毒	★★	↑	该病毒为 Java 脚本病毒，通常是用户访问恶意网站是所感染的。
10	X97M_LAROUX.CO	脚本病毒	★★	↑	Office 宏病毒，由其他恶意软件或访问恶意网站感染

系统漏洞信息

MS12-016 ： .NET Framework 和 Microsoft Silverlight 中的漏洞可能允许远程执行代码 (2651026)

Windows XP
Windows Server 2003
Windows Vista
Windows Server 2008
Windows 7
Windows Server 2008 R2
描述：http://technet.microsoft.com/zh-cn/security/bulletin/MS12-016



系统安全技巧

1、强化：密码管理

设定登录密码是一项非常重要的安全措施，如果用户的密码设定不合适，就很容易被破译，尤其是拥有超级用户使用权限的用户，如果没有良好的密码，将给系统造成很大的安全漏洞。

目前密码破解程序大多采用字典攻击以及暴力攻击手段，而其中用户密码设定不当，则极易受到字典攻击的威胁。很多用户喜欢用自己的英文名、生日或者账户等信息来设定密码，这样，黑客可能通过字典攻击或者是社会工程的手段来破解密码。所以建议用户在设定密码的过程中，应尽量使用非字典中出现的组合字符，并且采用数字与字符相结合、大小写相结合的密码设置方式，增加密码被黑客破解的难度。而且，也可以使用定期修改密码、使密码定期作废的方式，来保护自己的登录密码。

在多用户系统中，如果强迫每个用户选择不易猜出的密码，将大大提高系统的安全性。但如果 passwd 程序无法强迫每个上机用户使用恰当的密码，要确保密码的安全度，就只能依靠密码破解程序了。实际上，密码破解程序是黑客工具箱中的一种工具，它将常用的密码或者是英文字典中所有可能用来作密码的字都用程序加密成密码字，然后将其与 Linux 系统的/etc/passwd 密码文件或/etc/shadow 影子文件相比较，如果发现有吻合的密码，就可以求得明码了。在网络上可以找到很多密码破解程序，比较有名的程序是 crack 和 john the ripper。用户可以自己先执行密码破解程序，找出容易被黑客破解的密码，先行改正总比被黑客破解要有利。

2、限定：网络服务管理

早期的 Linux 版本中，每一个不同的网络服务都有一个服务程序（守护进程，Daemon）在后台运行，后来的版本用统一的/etc/inetd 服务器程序担此重任。Inetd 是 Internetdaemon 的缩写，它同时监视多个网络端口，一旦接收到外界传来的连接信息，就执行相应的 TCP 或 UDP 网络服务。由于受 inetd 的统一指挥，因此 Linux 中的大部分 TCP 或 UDP 服务都是在/etc/inetd.conf 文件中设定。所以取消不必要服务的第一步

就是检查/etc/inetd.conf 文件，在不要的服务前加上“＃”号。

一般来说，除了 http、smtp、telnet 和 ftp 之外，其他服务都应该取消，诸如简单文件传输协议 tftp、网络邮件存储及接收所用的 imap/ipop 传输协议、寻找和搜索资料用的 gopher 以及用于时间同步的 daytime 和 time 等。还有一些报告系统状态的服务，如 finger、efinger、systat 和 netstat 等，虽然对系统查错和寻找用户非常有用，但也给黑客提供了方便之门。例如，黑客可以利用 finger 服务查找用户的电话、使用目录以及其他重要信息。因此，很多 Linux 系统将这些服务全部取消或部分取消，以增强系统的安全性。Inetd 除了利用/etc/inetd.conf 设置系统服务项之外，还利用/etc/services 文件查找各项服务所使用的端口。因此，用户必须仔细检查该文件中各端口的设定，以免有安全上的漏洞。

在后继的 Linux 版本中（比如 Red Hat Linux7.2 之后），取而代之的是采用 xinetd 进行网络服务的管理。

当然，具体取消哪些服务不能一概而论，需要根据实际的应用情况来定，但是系统管理员需要做到心中有数，因为一旦系统出现安全问题，才能做到有步骤、有条不紊地进行查漏和补救工作，这点比较重要。

3、严格审计：系统登录用户管理

在进入 Linux 系统之前，所有用户都需要登录，也就是说，用户需要输入用户账号和密码，只有它们通过系统验证之后，用户才能进入系统。

与其他 Unix 操作系统一样，Linux 一般将密码加密之后，存放在/etc/passwd 文件中。Linux 系统上的所有用户都可以读到/etc/passwd 文件，虽然文件中保存的密码已经经过加密，但仍然不太安全。因为一般的用户可以利用现成的密码破译工具，以穷举法猜测出密码。比较安全的方法是设定影子文件 etc/shadow，只允许有特殊权限的用户阅读该文件。

在 Linux 系统中，如果要采用影子文件，必须将所有的公用程序重新编译，才能支持影子文件。这种方法比较麻烦，比较简便的方法是采用插入式验证模块（PAM）。很多 Linux 系统都带有 Linux 的工具程序 PAM，它是一种身份验证机制，可以用来动态地改变身份验证的方法和要求，而不要求重新编译其他公用程序。这是因为 PAM 采用封闭包的方式，将所有与身份验证有关的逻辑全部隐藏在模块内，因此它是采用影子档案的最佳帮手。

此外，PAM 还有很多安全功能：它可以将传统的 DES 加密方法改写为其他功能更强的加密方法，以确保用户密码不会轻易地遭人破译；它可以设定每个用户使用电脑资源的上限；它甚至可以设定用户的上机时间和地点。

Linux 系统管理人员只需花费几小时去安装和设定 PAM，就能大大提高 Linux 系统的安全性，把很多攻击阻挡在系统之外。

4、设定：用户账号安全等级管理

除密码之外，用户账号也有安全等级，这是因为在 Linux 上每个账号可以被赋予不同的权限，因此在建

立一个新用户 ID 时，系统管理员应该根据需要赋予该账号不同的权限，并且归并到不同的用户组中。

在 Linux 系统中的部分文件中，可以设定允许上机和不允许上机人员的名单。其中，允许上机人员名单在/etc/hosts.allow 中设置，不允许上机人员名单在/etc/hosts.deny 中设置。此外，Linux 将自动把允许进入或不允许进入的结果记录到/var/log/secure 文件中，系统管理员可以据此查出可疑的进入记录。

每个账号 ID 应该有专人负责。在企业中，如果负责某个 ID 的职员离职，管理员应立即从系统中删除该账号。很多入侵事件都是借用了那些很久不用的账号。

在用户账号之中，黑客最喜欢具有 root 权限的账号，这种超级用户有权修改或删除各种系统设置，可以在系统中畅行无阻。因此，在给任何账号赋予 root 权限之前，都必须仔细考虑。

Linux 系统中的/etc/securetty 文件包含了一组能够以 root 账号登录的终端机名称。例如，在 RedHatLinux 系统中，该文件的初始值仅允许本地虚拟控制台（rtys）以 root 权限登录，而不允许远程用户以 root 权限登录。最好不要修改该文件，如果一定要从远程登录为 root 权限，最好是先以普通账号登录，然后利用 su 命令升级为超级用户。

5、谨慎使用：“r 系列”远程程序管理

在 Linux 系统中有一系列 r 字头的公用程序，比如 rlogin，rcp 等等。它们非常容易被黑客用来入侵我们的系统，因而非常危险，因此绝对不要将 root 账号开放给这些公用程序。由于这些公用程序都是用.rhosts 文件或者 hosts.equiv 文件核准进入的，因此一定要确保 root 账号不包括在这些文件之内。

由于 r 等远程指令是黑客们用来攻击系统的较好途径，因此很多安全工具都是针对这一安全漏洞而设计的。例如，PAM 工具就可以用来将 r 字头公用程序有效地禁止掉，它在/etc/pam.d/rlogin 文件中加上登录必须先核准的指令，使整个系统的用户都不能使用自己 home 目录下的.rhosts 文件。

6、限制：root 用户权限管理

Root 一直是 Linux 保护的重点，由于它权力无限，因此最好不要轻易将超级用户授权出去。但是，有些程序的安装和维护工作必须要求有超级用户的权限，在这种情况下，可以利用其他工具让这类用户有部分超级用户的权限。sudo 就是这样的工具。

sudo 程序允许一般用户经过组态设定后，以用户自己的密码再登录一次，取得超级用户的权限，但只能执行有限的几个指令。例如，应用 sudo 后，可以让管理磁带备份的管理人员每天按时登录到系统中，取得超级用户权限去执行文档备份工作，但却没有特权去作其他只有超级用户才能作的工作。

sudo 不但限制了用户的权限，而且还将每次使用 sudo 所执行的指令记录下来，不管该指令的执行是成功还是失败。在大型企业中，有时候有许多人同时管理 Linux 系统的各个不同部分，每个管理人员都有用 sudo 授权给某些用户超级用户权限的能力，从 sudo 的日志中，可以追踪到谁做了什么以及改动了系统的哪些部分。

值得注意的是，sudo 并不能限制所有的用户行为，尤其是当某些简单的指令没有设置限定时，就有可

能被黑客滥用。例如，一般用来显示文件内容的/etc/cat 指令，如果有了超级用户的权限，黑客就可以用它修改或删除一些重要的文件。

7、追踪黑客踪迹：日志管理

当用户仔细设定了各种与 Linux 相关的配置（最常用日志管理选项），并且安装了必要的安全防护工具之后，Linux 操作系统的安全性的确大为提高，但是却并不能保证防止那些比较熟练的网络黑客的入侵。

在平时，网络管理人员要经常提高警惕，随时注意各种可疑状况，并且按时检查各种系统日志文件，包括一般信息日志、网络连接日志、文件传输日志以及用户登录日志等。在检查这些日志时，要注意是否有不合常理的时间记载。例如：

正常用户在半夜三更登录；

不正常的日志记录，比如日志只记录了一半就切断了，或者整个日志文件被删除了；

用户从陌生的网址进入系统；

因密码错误或用户账号错误被摈弃在外的日志记录，尤其是那些一再连续尝试进入失败，但却有一定模式的试错法；

非法使用或不正当使用超级用户权限 su 的指令；

重新开机或重新启动各项服务的记录。

上述这些问题都需要系统管理员随时留意系统登录的用户状况以及查看相应日志文件，许多背离正常行为的蛛丝马迹都应当引起高度注意。

8、横向扩展：综合防御管理

防火墙、IDS 等防护技术已经成功地应用到网络安全的各个领域，而且都有非常成熟的产品。

在 Linux 系统来说，有一个自带的 Netfilter/Iptables 防火墙框架，通过合理地配置其也能起到主机防火墙的功效。在 Linux 系统中也有相应的轻量级的网络入侵检测系统 Snort 以及主机入侵检测系统 LIDS（Linux Intrusion Detection System），使用它们可以快速、高效地进行防护。

需要提醒注意的是：在大多数的应用情境下，我们需要综合使用这两项技术，因为防火墙相当于安全防护的第一层，它仅仅通过简单地比较 IP 地址/端口对来过滤网络流量，而 IDS 更加具体，它需要通过具体的数据包（部分或者全部）来过滤网络流量，是安全防护的第二层。综合使用它们，能够做到互补，并且发挥各自的优势，最终实现综合防御。

9、评测：漏洞追踪及管理

Linux 作为一种优秀的开源软件，其自身的发展也日新月异，同时，其存在的问题也会在日后的应用中

慢慢暴露出来。黑客对新技术的关注从一定程度上来说要高于我们防护人员，所以要想在网络攻防的战争中处于有利地位，保护 Linux 系统的安全，就要求我们要保持高度的警惕性和对新技术的高度关注。用户特别是使用 Linux 作为关键业务系统的系统管理员们，需要通过 Linux 的一些权威网站和论坛上尽快地获取有关该系统的一些新技术以及一些新的系统漏洞的信息，进行漏洞扫描、渗透测试等系统化的相关配套工作，做到防范于未然，提早行动，在漏洞出现后甚至是出现前的最短时间内封堵系统的漏洞，并且在实践中不断地提高安全防护的技能，这样才是一个比较的解决办法和出路。

10、保持更新：补丁管理

Linux 作为一种优秀的开源软件，其稳定性、安全性和可用性有极为可靠的保证，世界上的 Linux 高手共同维护着个优秀的产品，因而起流通渠道很多，而且经常有更新的程序和系统补丁出现，因此，为了加强系统安全，一定要经常更新系统内核。

Kernel 是 Linux 操作系统的核心，它常驻内存，用于加载操作系统的其他部分，并实现操作系统的基本功能。由于 Kernel 控制计算机和网络的各种功能，因此，它的安全性对整个系统安全至关重要。早期的 Kernel 版本存在许多众所周知的安全漏洞，而且也不太稳定，只有 2.0.x 以上的版本才比较稳定和安全（一般说来，内核版本号为偶数的相对稳定，而为奇数的则一般为测试版本，用户们使用时要多留意），新版本的运行效率也有很大改观。在设定 Kernel 的功能时，只选择必要的功能，千万不要所有功能照单全收，否则会使 Kernel 变得很大，既占用系统资源，也给黑客留下可乘之机。

在 Internet 上常常有最新的安全修补程序，Linux 系统管理员应该消息灵通，经常光顾安全新闻组，查阅新的修补程序。一般情况下，用户可以随时保持对 Red Hat 门户网站（www.redhat.com），Debian Linux 门户网站（www.debian.org）、Turbolinux 门户网站（www.turbolinux.com）、SuSE 门户网站（www.suse.com/index_us.html）、Fedora 门户网站（fedora.redhat.com）等优秀 Linux 发行套件网站的关注，即时的更新系统的最新核心以及打伤安全补丁，这样能较好地保证 Linux 系统的安全。

来源：51CTO

免责声明

该邮件列表仅用于提供信息，此邮件列表内容不负任何担保责任，没有明示或默示的保证，包括但不限于对适销性、特定用途适用性以及不受侵害的暗示保证。用户对此邮件列表的准确性和使用承担全部风险，因依赖该资料所致的任何损失，趋势科技均不负责。