操作系统安全简论——Windows NT操作系统安全(四)

卿斯汉 （中科院信息安全技术工程研究中心 100080）

5 Windows NT安全漏洞及对策

Windows NT通过合理的配置可以达到C2级安全，这样很少有黑客能对其进行有效的攻击。但是很不幸，由于Windows NT是一个非常庞大的软件，它本身存在多种漏洞。并且，那些看起来考虑很周到的Windows NT应用软件，如IE等也存有缺陷。特别是，在那些与因特网实现互连的网络环境中，黑客们往往利用这些漏洞对Windows NT系统发起攻击。下面，我们介绍若干重要的，Windows NT本身和常用的Windows NT应用软件的安全漏洞及安全对策。

5.1 Windows NT安全漏洞及对策

漏洞1：安全帐号管理(SAM)数据库可以由以下用户复制：管理员帐号、管理员工作组的所有成员、备份操作员、服务器操作员以及所有具有备份特权的人员。SAM数据库的一个备份拷贝能够被某些工具所利用，用于破解口令。

对策：严格限制管理员工作组和备份工作组帐号的成员资格；加强对这些帐号的跟踪，尤其是管理员帐号的登录失败和注销失败。对SAM进行的任何权限改变和对其本身的修改进行审计，并且设置给管理员发送警告；切记要改变默认权限设置，预防这个漏洞。

漏洞2：每次紧急修复盘(Emergency Repair Disk-ERD)更新时，整个SAM数据库被复制到%system%＼repair＼sam.。在缺省的权限设置下，每个人对该文件都有"读"的访问权，管理员和系统本身具有"完全控制"的权利，Power User有"改变"的权利。

对策：确保%system%＼repair＼sam.在每次ERD更新后，对所有人不可读。严格控制对该文件的读权利。不应该有任何用户或者工作组对该文件拥有任何访问权。最好的办法是，不要给管理员访问该文件的权力，如果需要更新该文件，管理员暂时改变一下权力，当更新操作完成后，管理员立即把权限设置成不可访问。

漏洞3：SAM数据库和其他Windows NT服务器文件可能被Windows NT的SMB(服务器消息块)所读取。SMB有很多尚未公开的"后门"，能不用授权就可以存取SAM和Windows NT服务器上的其他文件。通过SMB协议可访问的服务的准确数目尚未有任何记载。另外，如何控制访问这些服务的方法也尚未有任何记载。另一漏洞，SMB在验证用户身份时，使用一种简易加密的方法发送申请包。因此，它的文件传输授权机制很容易被击溃。

对策：在防火墙上，截断从端口135到142的所有TCP和UDP的连接。这样可以有利于控制，包括对基于远程过程调用(RPC)工作于端口135的安全漏洞的控制。

最安全的方法是利用代理限制或完全拒绝网络上基于SMB的连接。然而，限制SMB的连接可能导致系统功能的限制。在内部路由器上设置存取控制表(ACL)，在各个独立子网之间，截断端口135到142，这可以完全拒绝网络上基于SMB协议的连接。

漏洞4：特洛伊木马(Trojan Horses)和病毒，可能依靠缺省的权力做SAM的备份，获取访问SAM中的口令信息，或者通过访问紧急修复盘ERD的更新盘。

对策：所有具有管理员和备份特权的帐号绝对不能浏览WEB，严格限制与外部的联系。所有帐号只能具有User或者Power User工作组的权限。

漏洞5：能够物理上访问Windows NT机器的任何人，可能利用某些工具获得管理员的访问权限。重装Windows NT软件，就可以获得管理员级别的访问权。重装整个操作系统，覆盖原来的系统，就可以获得管理员特权。

对策：改善保安措施，保证Windows NT机器物理上安全。

漏洞6：如果Guest帐号是开放的，当用户登录失败的次数达到设置次数时，可以获得Windows NT工作站的Guest访问权，从而进入Windows NT域。

对策：Windows NT4.0已经解决了这个问题，升级到Windows NT4.0。关闭Guest帐号，或者给它一个难记的口令。

漏洞7：所有用户可以通过命令行方式，试图连接管理系统的共享资源。任何一个用户可以在命令行下，键入"＼＼IP address＼C$(或者＼＼IP address＼D$，＼＼IP address＼WINNT$)"试图连接任意一个Windows NT平台上管理系统的共享资源。

对策：限制远程管理员访问Windows NT平台。

漏洞8：由于没有定义尝试注册的失败次数，导致可以被无限制地尝试连接系统管理的共享资源。这样的系统设置相当危险，它无异于授权给黑客们进行连续不断的连接尝试。

对策：限制远程管理员访问Windows NT平台。

漏洞9：如果系统中只有一个管理员帐号，当注册失败的次数达到设置次数时，该帐号也不能被锁住。这种情况是Windows NT的一个特征，也是一种危险。这种情况在Windows NT域和Windows NT工作站中会发生。

对策：除了系统默认创建的管理员帐号，还应该至少创建一个具有管理员特权的帐号，并且把默认的管理员帐号改成另一个名字。

漏洞10：具有管理员特权的帐号在达到注册失败的次数时将被锁住，然而，

30分钟后自动解锁。帐号策略中，可对帐号的加锁和解锁进行设置。

对策：对于所有管理员帐号，应该使用难猜的口令。

漏洞11：默认地，Windows NT在注册对话框中显示最近一次注册的用户名。这是Windows NT的一个特征，也是一种风险，给潜在的黑客提供了信息。

对策：在域控制器上，修改注册表中Winlogon的设置，关闭这个功能。

漏洞12：Windows NT的客户可以将口令保存在文件中，以便快速存取。任何人可能通过访问内存获取加密的口令，或者通过访问Windows NT工作站的ADMINST.PWD文件以及Windows 95的ADMINST.PWL文件读取口令，获得默认管理员的访问权。

对策：严格限制Windows NT域中Windows 95客户的使用。限制Windows NT工作站上管理员的特权。

漏洞13：Windows NT口令可能被非Windows NT平台口令取代。如果Windows 95中的"Change Windows Password"工具在Windows NT系统中已被授权，就可以做到这一点。结果是一个强的口令被一个弱的口令所代替。

对策：在与Windows NT平台连接时，不能运行"Change Windows Password"工具。

漏洞14：管理员从非安全的工作站上进行远程登录的能力会带来许多危害系统安全的问题。

对策：加强计算机设施的保安工作。关闭系统管理员的远程能力，管理员只允许直接访问控制台。可以从【用户管理器】【帐号策略】进行设置。使用加密的对话。在管理员的属性中，限制他可以从哪些工作站上进行远程登录。

漏洞15：注册表的默认权限设置可以被任何人完全控制和创建。这种设置可能引起注册表文件被删除或替换。

对策：对于注册表，严格限制只可进行本地注册，不可远程访问。在Windows NT工作站上，限制对注册表编辑工具的访问，使用第三方工具软件，比如Enterprise Administrator (Mission Critical Software)，锁住注册表。或者至少把所有人默认的完全控制权力改为只能创建。实际上，如果把这种权力设置为只读，将会给系统带来许多潜在的功能性问题。因此，在实现之前，一定要小心谨慎地进行测试。在Windows NT 4.0中引入了一个注册表键来关闭非管理员的远程注册表访问。在Windows NT服务器上，这是一个默认的注册表键值，对于Windows NT工作站，必须把这个注册表键添加到注册表数据库中。

漏洞16：在Windows 95上，或在系统管理的共享资源上运行regedit.exe，将允许客户交互地、远程地访问Windows NT域服务器。

对策：严格限制Windows 95客户的使用。使用注册表审计。制定规章制度限制管理员的操作程序，禁止这样的访问，或者明确授权给指定的几个系统管理员。

漏洞17：通过访问其他的并存的操作系统，有可能绕过NTFS的安全设置。已经有很多工具，不许要任何特权，就可以访问基于Intel系统上的NTFS格式的硬盘驱动器，就可以操纵Windows NT的各种安全配置。

对策：使用专门的分区。限制管理员工作组和备份操作员工作组。制定规章制度限制管理员的操作程序，禁止这样的访问，或者明确授权给指定的几个系统管理员。可以考虑采用第3方预引导身份验证机制。

漏洞18：在Windows NT系统中，文件句柄可能从内存中被读取，然后用来访问文件，这样做的前提是在一个用户注册期间，文件已经被访问过。

对策：限制管理员级和系统级的访问控制。

漏洞19：默认权限设置允许任何人对关键目录具有改变级的访问权。该安全漏洞所涉及的关键目录包括：每个NTFS文件系统的根目录、System32目录以及Win32App目录。

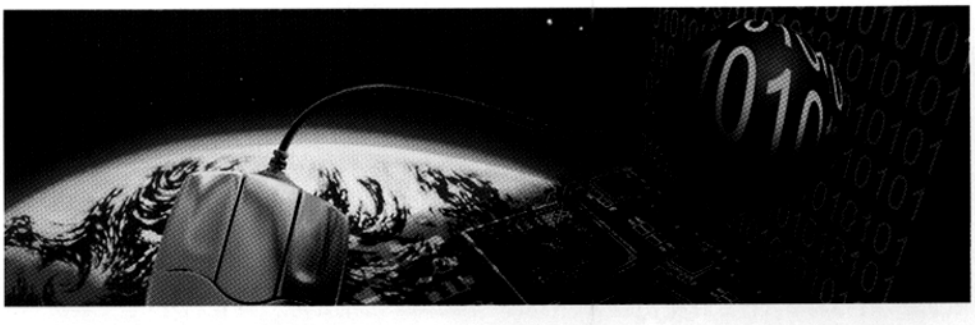
对策：如果可行，改变权限为读。注意：把权限改成读会给系统带来许多潜在的功能性问题。因此，在实现之前，一定要小心谨慎地进行测试。

漏洞20：打印操作员工作组中的任何一个成员对打印驱动程序具有系统级的访问权。黑客可以利用这个安全漏洞，用一个特洛伊木马程序替换任何一个打印驱动程序；或者在打印驱动程序中插入恶意病毒，具有相同效果。

对策：在赋予打印操作员权限时，要采取谨慎态度；要限制人数；要进行系统完整性检查；要适当配置和调整审计功能，并且定期检查审计文件。

漏洞21：通过FTP有可能进行无授权的文件访问。FTP有一个设置选项，允许按照客户进行验证，使其直接进入一个帐户。这种直接访问用户目录的FTP操作，具有潜在的危险，使无须授权而访问用户的文件和文件夹成为可能。

对策：合理配置FTP，确保服务器必须验证



所有的FTP申请。

漏洞22：基于Windows NT的文件访问权限，对于非Windows NT文件系统不可读。当文件被移动或复制到其他文件系统时，附在它们上面的所有Windows NT安全信息不再有效。

对策：使用NTFS，尽可能使用共享方式。

漏洞23：对文件设置"错误"的安全权限是很容易的，比如复制或者移动一个文件时，权限设置将会改变。文件被复制到一个目录，它将会继承该目录的权限。移动一个文件时，无论它被移动到任何目录下，该文件保留原来的权限设置。

对策：经常检查文件的权限设置是否得当，尤其是在复制或是移动文件之后。

漏洞24：在NTFS文件系统中，读权限意味着同时具有读和执行的权限，这个安全漏洞使文件被不正当地读和执行成为可能。

对策：使用策略编辑器设置文件访问的特殊权限。

漏洞25：Windows NT在执行删除权限的时候，有时不能正确地执行删除权限，这个安全漏洞使一个非授权用户任意删除对象成为可能。

对策：定期制作和保存备份。

漏洞26：Windows NT内置的工作组的权力和能力不能被真正删除。当删除一个内置工作组的时候，表面上，系统已经接受了删除。然而，当再次检查时，这些工作组并没有真正删除。有时，当服务器重新启动时，这些内置工作组被附回缺省的权力和能力。

对策：创建自己定制的工作组，根据最小特权的原则，定制这些工作组的权力和能力，符合业务的需要。可能的话，创建一个新的管理员工作组，使其具有特别指定的权力和能力。

漏洞27：Windows NT的进程定期处理机制有缺陷，这个漏洞可能造成某些服务的拒绝访问。它允许非特权用户运行某些特别程序，导致Windows NT系统崩溃或者挂起。

对策：制定并且执行严格的规章制度，限制管理员的操作程序，明确禁止这样的程序的非授权使用，据说微软公司有一个服务包已经能纠正这个错误，尽快安装最新的服务包。

漏洞28：如果一个帐号被设置成同时具有Guest工作组和另一工作组的成员资格，那么Guest工作组的成员资格可能会失效，导致用户配置文件和其他设置遭受意想不到的损失，从而导致服务的中断。

对策：不要把用户分到Guest工作组。

漏洞29：任何人的默认权力是：可以不受限制地创建公共GUI (图形用户界面) 工作组，如果一个用户创建公共图形用户界面工作组超过了最大数目256，有可能导致系统性能的降低、出现错误的消息或者系统崩溃。

对策：定期检查审计文件。

漏洞30：事件管理器中Security Log (安全日志) 的设置，允许记录被重写，否则事件管理器将导致服务器挂起。因此，可能造成无法审计对系统的闯入。

对策：实现一个适当的备份操作程序和策略。选择Overwrite events greater than 7 days选项。这个数字可以更改，当达到条件设置时，系统将会开始重写最旧的事件。

漏洞31：在Windows NT中，审计文件中保存的内容是不完全的。事实上，有很多事情被遗漏不会记录在审计文件中，如系统的重新装入、备份、恢复以及更改控制面板等，这些都是一些关键的事件。System Log (系统日志) 是完全记录事件的，但是，它们看起来象是密文，很难读懂。

对策：编辑注册表，打开对备份和恢复的审计。定期检查System Log，查看是否出现新类型的事件。

漏洞32：由于跟踪Windows NT域上所有的系统活动，所以很难确定Windows NT域上到底发生了什么事情。当一个事件标识最终被记录到系统的某个地方后，很难把它区分出来。

对策：使用第3方审计工具。

漏洞33：屏幕保护程序有错误，它允许非授权用户访问闲置终端。这个错误允许入侵者饶过屏幕保护获得访问权，甚至不必输入帐号和口令。

对策：据说微软公司最新的服务包已经能纠正这个错误，尽快安装最新的服务包。

漏洞34：任何用户可以通过命令行方式，远程查询任意一台Windows NT服务器上的已注册的用户名。

对策：关闭远程管理员级的访问。定期检查审计文件 (系统日志文件和系统审计文件)。

漏洞35：Windows NT机器允许在安装时，输入空白口令。这将是一个潜在的安全问题。

对策：使用最小口令长度选项，并且关闭"Permit Blank Passwords"选项，阻止空白口令的发生。

漏洞36：作为一个TCP连接的一部分，向Windows NT机器发送out-of-band数据，可使服务拒绝访问成为可能。这种攻击可导致Windows NT系统的崩溃。

对策：微软的Service Pack 3 for NT4.0已经纠正了部分问题，安装最新的服务包。最佳的解决方案是，配置一个坚固的防火墙，只授权可信赖的主机通过防火墙。在防火墙上，截断所有从端口137到139的TCP和UDP连接，这样做有助于加强对远程连接的控制。另外，在内部路由器上，设置存取控制表，在各个独立子网之间，截断所有从端口137到139的TCP和UDP连接。这是一种辅助措施。值得注意的是，有些黑客程序具有选择端口号的能力，可能会成功地攻击其他端口。