优化企业服务器系统安全环境，就这么几招 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/181/2021_2022__E4_BC_98_E5_8C_96_E4_BC_81_E4_c101_181889.htm 元旦当天，大兵听到一位网友反应情况，其QQ被人盗取，盗取QQ号的人留下话，大意是：我正在练手，你找一个会反盗窃的人来跟我对攻，攻下了我就把号码还你，攻不下算你倒霉。 在听到上述事情的同时，不由让大兵想起IDC界一次重大的事件：2006年晚些时候，位于北京亦庄网通机房的新网更是在互联网大会当天被黑客攻击，是向世人挑衅或是对手的恶意竞争，新网内部并未给出大众答案，我们也是不得而知。 事情发生后不久，大兵当时跟一位做IDC的朋友交流，他跟我提到一些情况情况：在黑市，一些人专门从事网络或网站攻击业务，由于从业人员的素质相对不是很高，再加近几年加入此地下工作的人员过多，市面非常惨淡，现在以2000元人民币的酬劳，基本可以完成一个专业中型网站或安全级别中级的企业内部网络攻击…… 所有这些，只是近几年IT界安全相关中的一个方面，而所有这些事情、事件、事故，将安全推上企业IT管理关注的一个重点。 那么，怎样防范攻击以更好地保障企业网络正常运行呢？ 对于不同的专项攻击，我们有不同的方式来部署以应对，但是我们都了解：在被攻击前，我们不知道攻击者是采用什么方式来进行攻击过程的。 这可怎么办好呢？ 系统性地部署我们的服务器与网络相关设置！只有这样，我们才能将被攻击的可能降到最低！技巧一：系统安全基础设置 黑客开始对你的网络发起攻击的时候，他们首先会检查是否存在一般的安全漏洞。因此，当你服务器上的数据都

存在一个FAT的磁盘分区的时候，即使安装上世界上所有的安全软件也不会对你有多大帮助的。 因此，你需要从基本做起。将服务器上所有包含了敏感数据的磁盘分区都转换成NTFS格式的。同时，可以为Exchange Server安装反病毒软件，将被感染的邮件在到达用户以前隔离起来。 技巧二：保护你的备份 备份实际上是一个巨大的安全漏洞。应该考虑通过密码保护你的磁带，并且如果你的备份程序支持加密功能，你还可以加密这些数据，如果窃贼还是把磁带弹出来带走的话，磁带上的数据也就毫无价值了。 技巧三：使用RAS回叫功能 Windows NT最酷的功能之一就是对服务器进行远程访问(RAS)的支持。不幸的是，一个RAS服务器对一个企图进入你的系统的黑客来说是一扇敞开的大门。黑客们所需要的一切只是一个电话号码。 你所要使用的技术将在很大程度上取决于你的远程用户如何使用RAS。如果远程用户经常是从家里或是类似的不太变动的地方呼叫主机，建议你使用回叫功能，它允 许远程用户登录以后切断连接。然后RAS服务器拨通一个预先定义的电话号码再次接通用户。黑客也就没有机会设定服务器回叫的号码了。 另一个可选的办法是限定所有的远程用户都访问单一的服务器。这样，即使黑客通过破坏手段来进入主机，那么他们也会被隔离在单一的一台机器上。 最后还有一个技巧就是在你的RAS服务器上使用出人意料的协议，迷惑一些不加提防的黑客。技巧四：考虑工作站的安全问题 工作站是通向服务器的一个端口，在所有的工作站上使用Windows 2000。Windows 2000是一个非常安全的操作系统。你也可以使用Windows NT。锁定工作站，使得一些没有安全访问权的人想要获得网络配置信息变得困难或是不可

能。另，一个技术是将工作站的功能限定一个“聪明的”哑终端，让程序和数据驻留在服务器上但却在工作站上运行。所有安装在工作站上的是一份Windows拷贝以及 一些指向驻留在服务器上的应用程序的图标。当你点击一个图标运行程序时，这个程序将使用本地的资源来运行，而不是消耗服务器的资源。这比你运行一个完全的 哑终端程序对服务器造成的压力要小得多。 技巧五：使用流行的补丁程序 微软雇佣了一个程序员团队来检查安全漏洞并修 补它们。这些补丁被捆绑进一个大的软件包并做为服务包(service pack)发布。通常有两种不同的补丁程序版本:一个40位的版本和一个128位的版本。128位的版本使用128位的加密算法，比40位的版本要安全得 多。微软定期将重要的补丁程序发布在它的FTP站点上。这些热点补丁程序是自上一次服务包发布以后被公布的安全修补程序。要经常查看热点补丁。但要记住一 定要按逻辑顺序使用这些补丁。避免导致一些文件的版本错误。 技巧六：使用强有力的安全政策 要提高安全性，另一个可以做的工作就是制定一个好的，强有力的安全策略。确保每一个人都知道它并知道它是强制执行的。如果你使用Windows 2000 Server，你就有可能指定用户特殊的使用权限来使用你的服务器而不需要交出管理员的控制权，可以授予这种删除和禁用账号权限并限制创建用户或是更改许 可等这些活动的权限了。 技巧七：反复检查防火墙 防火墙是网络的一个重要部分，因为它将你公司的计算机同互联网上那些可能对它们造成损坏的蛊惑仔们隔离开来。 你首先要做的事情是确保防火墙不会向外界开放超过必要的任何IP地址。你总是至少要让一个IP地址对外界可见。这个IP地址被使用来进行所有的互联网通讯

。如果你还有DNS注册的Web服务器或是电子邮件服务器，它们的IP地址也许也要通过防火墙对外界可见。但是，工作站和其他服务器的IP地址必须被隐藏起来。 你还可以查看端口列表验证你已经关闭了所有并不常用的端口地址。例如，TCP/IP 端口80用于HTTP通讯，因此你可能并不想堵掉这个端口。但是，你也许永远都不会用端口81，因此它应该被关掉。你可以在Internet上找到每个端口使用用途的列表。 如果你不希望紧要的数据被病毒或是黑客破坏或是被一个可能用这些数据来对付你的人窃取。就必须掌握一些维护服务器安全的技巧来保障它的安全。 堵住路由器的漏洞 对于黑客来说，利用路由器的漏洞发起攻击通常是一件比较容易的事情。保护路由器安全需要网管员在配置和管理路由器过程中采取相应的安全措施。 堵住安全漏洞 限制系统物理访问是确保路由器安全的最有效方法之一。限制系统物理访问的方法就是将控制台和终端会话配置成在较短闲置时间后自动退出系统。避免将调制解调器连接至路由器的辅助端口也很重要。避免身份危机 黑客常常利用弱口令或默认口令进行攻击。加长口令、选用30到60天的口令有效期等措施有助于防止这类漏洞。用户应该启用路由器上的口令加密功能，这样即使黑客能够浏览系统的配置文件，他仍然需要破译密文口令。 禁用不必要服务 拥有众多路由服务是件好事，但近来许多安全事件都突显了禁用不需要本地服务的重要性。另一个需要用户考虑的因素是定时，即使用户确保了部署期间时间同步，经 过一段时间后，时钟仍有可能逐渐失去同步。用户可以利用名为网络时间协议（NTP）的服务，对照有效准确的时间源以确保网络上的设备时针同步。 限制逻辑访问 限制逻辑访

问主要是借助于合理处置访问控制列表，使用入站访问控制将特定服务引导至对应的服务器。为了避免路由器成为DoS攻击目标，用户应该拒绝以下流量 进入：没有IP地址的包、采用本地主机地址、广播地址、多播地址以及任何假冒的内部地址的包。用户还可以采取增加SYN ACK队列长度、缩短ACK超时等措施来保护路由器免受TCP SYN攻击。 监控配置更改 用户在对路由器配置进行改动之后，需要对其进行监控。如果用户使用SNMP，那么一定要选择功能强大，提供消息加密功能的SNMP。为进一步确保安全管理，用户可以利用SSH与路由器建立加密的远程会话。配置管理的一个重要部分就是确保网络使用合理的路由协议。 实施配置管理 用户应该实施控制存放、检索及更新路由器配置的配置管理策略，并将配置备份文档妥善保存在安全服务器上，以防新配置遇到问题时用户需要更换、重装或回复到原先的配置。编后语： 通看全文，在大兵的理解范围内，觉得应该还有一些东东需要补充，那就是加上如黑洞等的网络方案优化以及防火墙策略的有序部署。 黑洞的设置，可以减少不明IP恶意访问的可能；防火墙策略的有序部署，可以尽快地找出安全隐患点，及时地做出应对反应。 当然，安全的防范不是绝对的，如果有内部专业人员与外部联合的特例，迂回地绕过网络安全设置与系统基础安全设置进行访问，那是技术再高的安全工程师也防范不了的；如果采用DDOS等手段疯狂地进行流量攻击，企业就算有再强大的硬防或网络带宽，要是不尽快找不源头以制止，那再高的带宽或更多的资源进行分流，也是无法阻挡的。 综上，其实我们企业IT管理人员最终可以做的，是尽量多地将安全防范的各种手段掌握住，以最大可

能地保障网络与系统更长时间的安全与稳定。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com