保证路由器安全的十大基本技巧 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/296/2021_2022__E4_BF_9D_E8_AF_81_E8_B7_AF_E7_c101_296159.htm 要不是思科最新发布的安全警告的提醒，很多网络管理员还没有认识到他们的路由器能够成为攻击的热点。路由器操作系统同网络操作系统一样容易受到黑客的攻击。大多数中小企业没有雇佣路由器工程师，也没有把这项功能当成一件必须要做的事情外包出去。因此，网络管理员和经理人既不十分了解也没有时间去保证路由器的安全。下面是保证路由器安全的十个基本的技巧。 1、更新你的路由器操作系统:就像网络操作系统一样，路由器操作系统也需要更新，以便纠正编程错误、软件瑕疵和缓存溢出的问题。要经常向你的路由器厂商查询当前的更新和操作系统的版本。 2、修改默认的口令:据卡内基梅隆大学的计算机应急反应小组称，80%的安全事件都是由于较弱或者默认的口令引起的。避免使用普通的口令，并且使用大小写字母混合的方式作为更强大的口令规则。 3、禁用HTTP设置和SNMP(简单网络管理协议):你的路由器的HTTP设置部分对于一个繁忙的网络管理员来说是很容易设置的。但是，这对路由器来说也是一个安全问题。如果你的路由器有一个命令行设置，禁用HTTP方式并且使用这种设置方式。如果你没有使用你的路由器上的SNMP，那么你就不需要启用这个功能。思科路由器存在一个容易遭受GRE隧道攻击的SNMP安全漏洞。 4、封锁ICMP(互联网控制消息协议)ping请求:ping和其它ICMP功能对于网络管理员和黑客都是非常有用的工具。黑客能够利用你的路由器上启用的ICMP功

能找出可用来攻击你的网络的信息。 5、禁用来自互联网的telnet命令:在大多数情况下，你不需要来自互联网接口的主动的telnet会话。如果从内部访问你的路由器设置会更安全一些。 6、禁用IP定向广播:IP定向广播能够允许对你的设备实施拒绝服务攻击。一台路由器的内存和CPU难以承受太多的请求。这种结果会导致缓存溢出。 7、禁用IP路由和IP重新定向:重新定向允许数据包从一个接口进来然后从另一个接口出去。你不需要把精心设计的数据包重新定向到专用的内部网路。 8、包过滤:包过滤仅传递你允许进入你的网络的那种数据包。许多公司仅允许使用80端口(HTTP)和110/25端口(电子邮件)。此外，你可以封锁和允许IP地址和范围。 9、审查安全记录:通过简单地利用一些时间审查你的记录文件，你会看到明显的攻击方式，甚至安全漏洞。你将为你经历了如此多的攻击感到惊奇。 10、不必要的服务:永远禁用不必要的服务，无论是路由器、服务器和工作站上的不必要的服务都要禁用。思科的设备通过网络操作系统默认地提供一些小的服务，如echo(回波), chargen(字符发生器协议)和discard(抛弃协议)。这些服务，特别是它们的UDP服务，很少用于合法的目的。但是，这些服务能够用来实施拒绝服务攻击和其它攻击。包过滤可以防止这些攻击。google_ad_client = "pub-1295960146753136".google_ad_width = 300.google_ad_height = 250.google_ad_format = "300x250_as".google_ad_type = "text_image".google_ad_channel = "".google_ui_features = "rc:6".// 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