保护Windows机密数据远离Google黑客 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/140/2021_2022__E4_BF_9D_E6_8A_A4Wind_c100_140821.htm 使用适当的对策，可以帮助你将高度机密信息远离Google，不能够被Google黑客搜索到。这里有四个步骤，你可以尝试做一下： 1.巩固你的服务器，并将其与外部环境隔离 有一个很不幸的事实是，许多关键服务器仍然完全暴露在Internet上，现在请收紧你服务器的存取控制，并将其放在防火墙之后。 2.设置Robots.txt文件，禁止Google索引你的网页 你能够通过设置“ googlebot ”的“ User-agent： ”参数的方法保护网络服务器的文件和目录免受Google索引，方法是在“ Disallow： ”部分列出你想保密的信息。 或者，如果你想所有的Web机器人都不访问你的网站和网页，就请将“ User-agent： ”参数设置为“ * ”，不过记住，怀有恶意的在网上到处闲逛的人能够从你的WebServer上得到此文件，并且看到你不想被别人看到的是哪些信息。如果这看起来像互联网的弱点，那么它就是。你可以不用robots.txt文件，但你应该允许机器人只能索引那些具体的公开页面，或者通过输入“ Disallow/ ”禁止它们索引任何以根目录开始的信息。 3.将高度机密的信息从公众服务器上去除 制定一项组织策略用来保护高度机密的信息（例如密码、机密文件等）远离公众可以访问的服务器。否则，使用任何可能的存取控制措施来保护它们，并且确保这些策略能够被强制执行，并且管理那些违规者。 4.保证你的服务器是安全的 为了维护服务器安全，请使用我在这一系列技巧中讨论过的Google测试工具和Google查询对其进行黑客测试。 我高度

推荐使用自动化测试工具，譬如SiteDigger和Gooscan进行黑客测试，手工执行多个查询的方式不仅缓慢枯燥，还不易于管理。 记住，这些测试只是通过Google进行的挖掘测试，它们并不能代表所有的黑客和Internet安全，这些也不是测试所有系统漏洞的最好工具。作为替代，你必须使用“ 多层 ”测试手段：同时使用Google和其它免费的、开源的，以及——据我看来，最具有综合性和可靠性的——商业性的工具进行测试，这些商业性的工具我推荐的有SPIDynamics公司的WebInspect（应用于Web应用程序）、ApplicationSecurity公司的AppDetective（用于Web数据库）和Qualys公司的QualysGuard（用于操作系统和网络漏洞）。 如果模拟黑客、渗入测试和普通的网络安全审计是你工作职责的一部分，这些Google黑客技术和相应的工具将成为你需要的安全工具箱中的一部分。为了安全的缘故，请现在就开始执行它，并且以后也经常执行。 关于作者：KevinBeaver是一位独立的信息安全顾问、作者，也是位于亚特兰大的PrincipleLogic，LLC公司的发言人，他专门为那些需要严格安全保护，或者突发安全事件寻求解决方法的公司提供信息安全研究服务。