解决方案：金融安全问题新方案 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/170/2021_2022__E8_A7_A3_E5_86_B3_E6_96_B9_E6_c40_170905.htm 随着我国金融改革的进行，各个银行纷纷将竞争的焦点集中到服务手段上，不断加大信息化建设的投入，扩大计算机网络规模和应用范围。但电子化在给银行带来利益的同时，也给银行带来了新的安全问题，并且这个问题现在显得越来越紧迫。 原因主要有三个：一是伴随我国经济体制改革，特别是金融体制改革的深入、对外开放的扩大，金融风险迅速增大。防范和化解金融风险成了各级政府和金融部门非常关注的问题。二是当前计算机网络应用频繁，系统的安全性漏洞风险也随之增加。多年以来，银行迫于竞争压力，不断扩大电子化网点、推出电子化新品种，忽略了计算机管理制度和安全措施的建设，使计算机安全问题日益突出。三是计算机知识日益普及，金融网络向国际化发展，计算机犯罪技术也在不断提高，利用计算机技术进行犯罪的案件呈逐年上升趋势，这也迫切要求银行信息系统具有更高的安全防范体系。 银行信息系统安全性总的原则可以归纳为：制度防内，技术防外。所谓“ 制度防内 ”，是要建立严密的计算机管理规章制度、运行规程，形成内部各层人员、各职能部门、各应用系统的相互制约关系，杜绝内部漏洞，并建立良好的故障处理反应机制，保障银行信息系统的安全正常运行。“ 技术防外 ”主要是指从技术手段上加强安全措施，防止外部黑客的入侵。在本案例中，我们在不影响银行正常业务的基础上建立了银行的安全防护体系，从而使银行网络系统的安全性达到令人放心的水平。

系统环境 某省建设银行网络系统是一个综合信息系统，由总部和多个支行组成。其中总部和各个支行都有内部业务网和内部办公网，通过DDN与人行、银联、税务、证券公司等重要的金融部门相连，并通过光纤和Internet相连，网络架构十分庞大、复杂。 现有网络采用内外两套物理上完全独立的网络，分别用做内部业务网和内部办公网，联接入Internet使用。应用系统上的安全，主要考虑了包括WEB、FTP、邮件系统、DNS等网络基本服务，以及业务系统、办公自动化系统、电子商务系统等等在内的安全性。 由于该省建设银行的网络系统庞大，结构复杂，如果采用传统的机架方式的或者软件方式的网络漏洞扫描产品，很难在短时间内有效地进行网络漏洞的扫描和及时的进行系统加固，所以考虑采用榕基手持式漏洞扫描产品进行系统漏洞的侦测。 RJ-iTop网络隐患扫描系统的手持式扫描产品分成手持式硬件设备和主机端软件。手持式硬件设备主要负责漏洞信息的收集，主机端软件负责安全评估分析和报表打印。在扫描建行的网络时，只需要单独使用手持式设备就可以了。手持式设备在使用过程中只需要一个用户提供一个端口，支持TCP/IP协议就可以开始扫描工作，与用户的网络环境相对独立，不需要额外的其他配置。而软件方式的扫描工具，需要用户提供特定的运行环境和平台安装扫描软件，无形中花费了较多的时间，降低了工作效率。扫描的对象主要包括提供主要服务的核心区主机和网络设备（路由器、交换机、防火墙等），针对这些不同的情况，在扫描的过程中选择了系统预设的扫描策略，进行针对服务和平台的扫描，提高了扫描的有效性，加快了扫描进度。 其次，扫描结束后，可以将庞大的网络系统中各个节点

系统的扫描结果集中放到网管机中，并生成扫描报告，分析并及时的实施加固。 RJ-iTop可扫描国际最新的CVE漏洞库中公布的全部漏洞，榕基公司通过各种渠道也收集了大量最新出现的系统漏洞，数量已达到1850个，对用户来说，及时发现这些系统漏洞将对维护系统的安全性有直接的帮助。 在对该省建行网络系统进行扫描的时候需要扫描网络中位于不同的防火墙或者是交换机后面的服务器，针对这种分布式的网络结构，榕基手持扫描器充分发挥了支持分布式扫描的特性，进行轻易的移动就可以完成扫描。 最后，由于手持式扫描设备的软件完全固化，使软件自身安全得到更好的保障，在扫描的整个过程中对被查单位的目标系统不会造成影响。榕基的漏洞扫描产品通过了国家公安部、安全部、解放军等多个部门的许可认证，目前已经在上述领域得到了广泛的应用。 