开源安全技术的四大好处Linux认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E5_BC_80_E6_BA_90_E5_AE_89_E5_c103_644664.htm 为使IT架构正常运作，企业往往要将信息安全作为一个关键因素引入到技术和管理体系中。在某些特定领域，与商业安全产品相比，开源安全技术有相当大的优势。 k开源安全产品的开发、测试和发布过程完全是透明的，同时提供产品的源代码及完善的文档。企业可以清楚地了解开源安全技术的工作原理和实现方法，在选择开源安全技术时更有把握，也更容易得到质量更好的安全方案。开源安全方案的开发者大多是经验丰富的安全厂商或技术人员，这就保证了开源安全技术除功能上不逊于封闭源代码的商业安全方案外，同时还具有更高的可靠性、灵活性以及更低的采购和使用成本。 案例一：Snort入侵检测系统 Snort是开源安全技术领域中最有名的入侵检测系统，截至目前，Snort各版本的下载次数已达数百万次，Snort已成为世界上使用最广泛的入侵检测系统。Snort使用针对攻击行为标志(Signature-Based)和 网络通讯协议(Protocols)的检测方式实现以下功能：实时通讯分析和数据包记录，数据包有效载荷检查，协议分析和内容查询匹配，探测缓冲区溢出、秘密端口扫描、CGI攻击、SMB探测、操作系统侵入尝试，使用系统日志、指定文件、Unix socket或通过Samba的WinPopus四种入侵行为的实时报警和日志记录。 有三种工作模式：数据包嗅探、数据包记录和成熟的侵入探测系统。与大部分开源软件相类似，Snort支持各种形式的插件、扩充和定制，包括数据库或XML记录、小帧探测和异常探测统计等。数据包

有效载荷探测是Snort最有用的一个特点，这就意味着可以探测到很多额外种类的敌对行为。近年来，随着描述入侵行为的入侵规则语言(Rules language)及检测技术的发展，Snort已经成为最富弹性而且最精确的入侵检测系统之一。 带来的好处：Snort在企业安全市场的成功应用，代表了市场对开源安全技术的“比封闭源代码的商业安全产品更好的质量”这一宗旨的广泛接受。Snort成为世界上使用最广泛的入侵检测系统的原因也在于此。它不完全依靠安全厂商进行产品的升级和支持，广大的开源社区用户及安全研究组织也在为改进Snort本身所用技术、Snort检测威胁数量和Snort部署方法而努力，因此Snort才能成为最富弹性及最精确的入侵检测系统之一。开源安全产品的开发、测试和发布过程完全是透明的，同时产品的源代码及完善的文档也会在开源社区公布。企业可以清楚地了解开源安全技术的工作原理和实现方法，在选择开源安全技术时更有把握，也更容易得到质量更好的安全方案。尤其对于一些很重视企业内部信息保密的特定行业企业来说，开源安全技术的源代码开放性还是一个关键的选择因素。因为这些特殊的企业用户需要掌握自己所部署的所有IT(包括安全)方案的内部运作原理，并要求对IT产品的源代码进行审计。这对封闭源代码的商业安全产品来说是不可逾越的鸿沟，而使用开源安全技术则完全没有这方面的问题。 案例二：SNARE日志管理和事件报告方案 RSNARE是一个开放源代码的跨平台系统日志审计和入侵检测产品，它的开发厂商InterSect Alliance 有非常丰富的多种操作系统Solaris、Windows 2000/NT/XP/2003、Novell Netware、AIX、even MVS (ACF2/RACF). 日志审计和入侵检测经验，并为*部门、

商业组织等提供专业服务。这些经验都反映在SNARE上，使SNARE成为一个功能强大的日志管理和事件报告方案。SNARE在逻辑上分成三个部分：1.内核动态加载模块，该模块封装了系统内的危险调用，并收集用户和程序所执行的可疑系统调用信息.2.用户空间审核程序，该程序负责收集内核动态加载模块所收集的审计信息，并按照一定的格式进行整理和保存.3.SNARE日志分析前端，由于SNARE审计程序所产生的审计信息对用户来说仍然是难于阅读和理解的，因此SNARE还提供了一个图形化的日志分析前端，用户可以通过日志分析前端，得到可自定义的、规范的系统日志管理和事件报告。 带来的好处： 企业用户可以把SNARE部署成客户/服务器结构的中央日志管理和报告系统。这样不单可以简化系统部署的复杂性和减轻管理员的工作强度，企业还可以享受SNARE的跨平台特性。这对内部网络结构复杂、同时使用多种操作系统平台的企业来说尤其重要。企业整体部署SNARE日志管理和事件报告方案，除了可以在信息安全方面获得更高的保障和更快的事件响应速度之外，还可以因此而满足企业外部环境对企业合规性(Compliance)的强制要求，如SOX法案、HIPPA、PCIDSS、ISO 27001等对企业系统日志审计的需求。 开源安全方案的开发者大多是经验丰富的安全厂商或技术人员。这除了能保证开源安全技术从功能上不输于封闭源代码的商业安全方案，同时还能保证它具有更高的可靠性。此外，由于开源安全技术的实现是完全透明的，众多第三方机构和技术人员还能够对开源安全产品进行完善的二次测试工作，进一步保证开源安全产品的稳定和可靠性。企业在选择开源安全产品时，在产品和部署的可靠性上要比

选择封闭源代码的、只经过生产厂商测试的商业安全产品有更多保证。如果用户在开源安全技术的部署和管理过程中遇到问题的话，还能在互联网上得到相关开源社区及广大热心用户的免费帮助和支持。而企业选择商业安全技术的话，往往要付费才能获得安全厂商的支持。 案例三：Untangle 安全网关 Untangle Network Gateway是一款使用开源安全技术的、功能完备、高集成度、高灵活性的安全网关，在2007年荣获LinuxWorld Best Security Solution等多项由有影响的开源杂志所颁发的奖项。Untangle还被认为是商用级安全网关的优秀替代产品，可以很好地满足从作为大型企业的部门级/分公司级的安全网关，到中小型企业的内部网络出口网关的不同需求。 Untangle安全网关包含14个不同的功能模块： 1.提高生产效率的3个模块，垃圾邮件拦截(Spam blocker)、Web内容过滤(Web filtering)和协议控制(Protocol Control)。 2.用于安全用途的6个模块，病毒拦截(Virus blocker)、间谍软件拦截(Spyware blocker)、网络钓鱼拦截(Phish blocker)、入侵拦截(Intrusion Prevention)、攻击拦截(Attack blocker)和防火墙(Firewall)。 3.用于提供远程访问的2个模块，远程访问Portal (Remote Access Portal)和OpenVPN (SSL VPN功能)。 4.用于发送报告的功能模块和Untangle报告(Untangle Reports)模块。 5.用于网络连接的路由器 (Router)模块。 