Linux安全与LIDS PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/462/2021_2022_Linux_E5_AE_89_E5_85_c103_462228.htm LIDS(Linux入侵侦察系统)是Linux内核补丁和系统管理员工lidsadm)，它加强了Linus内核。 它在内核中实现了一种安全模式 -- 参考模式以及内核中的Mandatory Access Control（命令进入控制）模式。本文将阐述LIDS的功能和如何使用它来建立一个安全的Linux系统。 1.为什么选择LIDS 随着互连网上Linux越来越受欢迎 ,越来越多现有GNU/LINUX系统上的应用软件中的安全漏洞被发现。很多程序利用了程序员的粗心，例如缓存溢出、格式化代码攻击。当系统安全受到程序的危及，黑客获得ROOT权限以后，整个系统将被入侵者控制。 由于代码的开放性，我们可以获得很多所希望Linux应用程序的原代码，并且根据我们的需要来修改。所以bug能很容易地被找到，并很快修补。但是当漏洞被揭示后，而系统管理员疏于给漏洞打补丁，从而造成很容易地就被入侵，更糟的是黑客能获得ROOT SHELL。利用现有的GNU/Linux系统，他为所欲为。这正是LIDS想要解决的问题。 首先看看现有的GNU/Linux系统存在哪些问题。文件系统未受到保护 系统中的很多重要的文件，例如/bin/login，一旦黑客入侵后，他可以上传修改过的login文件来代替/bin/login ，然后他就可以不需要任何登陆名和密码就登陆系统。这常被称为Trojan house。 进程未受到保护 系统上运行的进程是为某些系统功能所服务的，例如HTTPD是一个web服务器来满足远程客户端对于web的需求。作为web服务器系统，保护其进程不被非法终止是很重要的。但是当入

侵者获得了ROOT权限后，我们却无能为力。 系统管理未受保护 很多系统管理，例如，模块的装载/卸载，路由的设置，防火墙的规则，能很容易就被修改，如果用户的ID是0。所以当入侵者获得ROOT权限后，就变得很不安全。 超级用户(root)作为ROOT可能滥用权限 他可以为所欲为。作为ROOT他甚至可以对现有的权限进行修改。 综上所述，我们发现在现有的Linux系统中的进入控制模式是不足以建立一个安全的Linux系统。我们必须在系统中添加新的模式来解决这些问题。这就是LIDS所要做的。 2. LIDS的特色 Linux入侵侦察系统是Linux内核补丁和系统管理员工具，它加强了内核的安全性。它在内核中实现了参考监听模式以及Mandatory Access Control（命令进入控制）模式。当它起作用后，选择文件进入，每一个系统/网络的管理操作，任何使用权限，raw device， mem和 I/O 进入将可以禁止甚至对于ROOT也一样。它使用和扩展了系统的功能，在整个系统上绑定控制设置，在内核中添加网络和文件系统的安全特性，从而加强了安全性。你可以在线调整安全保护，隐藏敏感进程，通过网络接受安全警告等等。 简而言之，LIDS提供了保护、侦察、响应的功能，从而是LINUX系统内核中的安全模式得以实现。 2.1 保护 LIDS提供以下的保护 ： 保护硬盘上任何类型的重要文件和目录，任何人包括ROOT都无法改变。 能保护重要进程不被终止 能防止非法程序的RAW IO 操作。保护硬盘，包括MBR保护，等等。 能保护系统中的敏感文件，防止未被授权者(包括ROOT)和未被授权的程序进入。 2.2 侦察 当有人扫描你的主机， LIDS能侦察到并报告系统管理员。 LIDS也可以检测到系统上任何违法规则的进程。 2.3 响应 当有人违反

规则， LIDS会将非法的运作细节记录到受LIDS保护的系统log文件中。 LIDS还可以将log信息传到你的信箱中。LIDS也可以马上关闭与用户的对话。