以防火墙为代表的访问控制技术和以LIDS/Snort为代表的检测技术是加固Linux系统的安全防线的基础，将其有效的结合，取长补短，便可以打造出一个稳定、安全的Linux操作系统，为用户的应用和服务提供强有力的保证。在浪潮睿捷存储管理系统中将会采用这种组合优势，从而为客户提供更加安全的服务和应用。

加固Linux系统的安全防线(下)

浅谈基于snort+iptables互动式入侵防御机制

文 | 田国航

在Internet上，安全是一个相对概念。防火墙通常放置在网络的入口处，通过监视流经网络的数据包的源地址，目的地址，端口等信息，限制对受保护网络的非法访问，实现对内部网络的保护。但是防火墙只能对数据包进行粗粒度的检查，不能对数据包中包含的应用层的信息进行过滤，这样黑客可以通过防火墙允许的访问网络的正常途径入侵网络，例如采用http蠕虫方式攻击网络，防火墙则毫不知情。入侵检测系统并联在网络上，采用旁路监听的方式，检查网络上传输的所有数据包中携带的应用层信息，能及时发现具有威胁的访问，及时地纪录、报警。但是它检测到入侵后只能采取纪录、报警，而不能有效、及时地阻止入侵行为。

事实上，根据CSI/FBI的安全报告显示，90%的入侵行为可以绕过防火墙；在网络安全事件中，86%的用户使用了防火墙，42%的用户使用了入侵检测。因为在传统的安全方案中，防火墙和入侵检测系统是相互独立的，不能相互利用，取长补短。因此，入侵防御系统正是解决以上不足之处的有效途径。图1所示即为一个结合防火墙和入侵检测机制的应用场景。

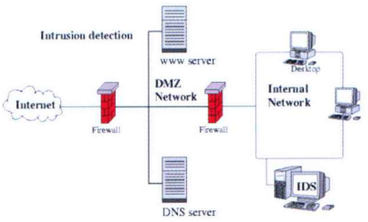

图1 防火墙和入侵检测结合的应用场景

在前面两期的科技浪潮中，我们已经介绍过Linux上的防火墙和入侵检测技术，特别是加固Linux系统安全防线的iptables技术和LIDS技术，本文将介绍如何通过防火墙和网络入侵检测联动来构建一个有效的安全的系统。

网络入侵检测Snort

Snort是一个开放源码的网络入侵检测系统（NIDS），是构建入侵网络安全系统的重要组件。NIDS是用来检测网络上的信息流的入侵检测系统（IDS），迄今为止它还是一门相当新的技术，而Snort在NIDS中处于领先的地位。

Snort是一个轻量级的入侵检测系统，它具有截取网络数据报文，进行网络数据实时分析、报警，以及日志的能力。snort具有以下特点。

（1）其报文截取代码基于libpcap库，继承了libpcap库的平台兼容性。使用一种灵活的规则语言来描述网络数据报文，因此可以对新的攻击作出快速地翻译，并且还能够记录网络数据；

（2）Snort具有实时流量分析和日志IP网络数据包的能力。能够快速地检测网络攻击，及时发出报警。Snort的报警机制很丰富，例如：syslog、用户指定的文件、一个UNIX套接字，还有使用SAMBA协议向Windows客户程序发出WinPopup消息。利用XML插件，snort可使用SNML（简单网络标记语言，simple network markup language）把日志存放到一个文件或适时报警；

（3）具有良好的扩展能力。它支持插件体系，可以通过其定义的接口，很方便地加入新的功能。Snort的输出plugin为我

们提供了丰富的报警输出方式：输出到文件，syslog，数据库，Unix域Socket等。其中当Snort的报警输出到Unix域Socket时，输出模块相当于一个报警的客户端，Snort的用户可以通过编写服务器端代码，获取snort的报警输出消息，并根据这些消息采取相应的对策；

（4）Snort能够进行协议分析，内容的搜索／匹配。现在snort能够分析的协议有TCP、UDP和ICMP。它能够检测多种方式的攻击和探测，例如：缓冲区溢出、秘密端口扫描、CGI攻击、SMB探测、探测操作系统指纹特征的企图等等。

综上所述，正因为Snort强大的插件支持和良好的可扩展性，才使其作为一种比较成熟的网络入侵检测工具被广泛使用。

规则模式库匹配

IDS可以按照一定的规则，对接受到的数据包信息进行模式匹配和处理，这些规则的集合就构成了模式库。模式库也是入侵检测和防火墙有效互动的基础。

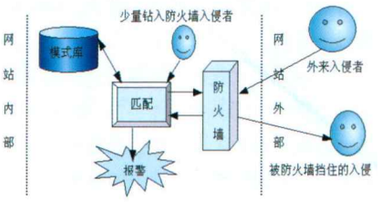

图2 防火墙与IDS结合的整体模型图

如图2，当有外来入侵者时，一部分入侵由于没有获得防火墙的信任，首先就被防火墙隔离在外，而另一部分骗过防火墙的攻击，或者干脆是内部攻击没经过防火墙的，再一次受到了入侵检测系统的盘查，受到怀疑的数据包经预处理模块分检后，送到相应的模块里去进一步检查。当对规则树进行扫描后，发现某些数据包与规则库中的某些攻击特征相符，则立即切断这个IP访问请求，或者报警。

从上面可以看出，系统安全的程度取决于规则模块的完整性和模式库匹配的高效性。其中，规则模块包括解析规则文件、建立规则语法树、实现规则匹配的算法等。单个数据报的检测流程详细的分析如下：首先对收集到的数据报进行解码，然后调用预处理函数对解码后的报文进行预处理，再利用规则树对数据报进行匹配。在规则树匹配的过程中，IDS要从上到下依次对规则树进行判断，从链首、链表到规则头节点，一直到规则选项节点。

模式库规则匹配的过程就是对从网络上捕获的每一条数据报文和上面描述的规则树进行匹配的过程。如果发现存在一条规则匹配的报文，就表示检测到一个攻击，然后按照规则指定的行为进行处理（如发送警告等），如果搜索完所有的规则都没有找到匹配的规则，就表示报文是正常的报文。

从上面的讨论可知，IDS规则模式库要能够根据攻击的变化自适应、自更新，使其与防火墙更加完美的结合，这样才会更加有利于提高系统的安全防护能力。

入侵检测和防火墙的互动

实现入侵检测系统和防火墙之间的互动一般有两种方式。

一种方式是实现紧密结合，即把入侵检测系统嵌入到防火墙中，即入侵检测系统的数据来源不再来源于数据包，而是流经防火墙的数据流。所有通过的包不仅要接受防火墙的检测规则的验证，还要判断是否是有攻击，以达到真正的实时阻断。这样实际上是把两个产品合成到一起。但是由于入侵检测系统本身也是一个很庞大的系统，所以无论从实施难度上，还是合成后的整体性能上，都会受很大的影响。

第二种方式是通过开放接口来实现互动。即防火墙或者入侵检测系统开放一个接口供对方使用，双方按照固定的协议进行通信，完成网络安全事件的传输。这种方式比较灵活，不影响防火墙和入侵检测系统的性能。

经过比较之后，我们会发现将IDS与防火墙通过开放接口结合起来实现互动要比将两者紧密结合在一起要好，因为系统越复杂其自身的安全问题就难以解决。所以选择将防火墙或者入侵检测系统开放一个接口供对方使用，双方按照固定的协议进行通信，完成网络安全事件的传输。

当防火墙和入侵检测系统互动时，所有数据通信通过认证和加密来确保传输信息的可靠性和保密性。通信双方可事先约定并设定通信端口，并且相互正确配置对方IP地址，防火墙以服务器（Server）模式来运行，IDS以客户端（Client）模式来运行。我们设计的互动模式原理如图3所示。

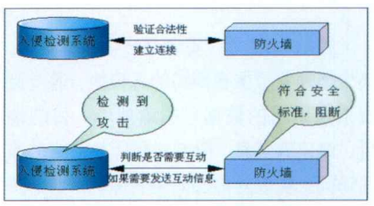

图3 防火墙（Firewall）与入侵检测系统（IDS）互动的原理图

具体步骤如下。（1）初始化通信连接时，一般由IDS向Firewall发起连接；（2）建立正常连接后，当IDS产生需要通知Firewall的安全事件时，通过发送约定格式的数据包来传递必要的互动信息；（3）Firewall收到互动信息后，可以实施互动行为，并将结果（成功与否）以约定格式的数据包反馈给IDS。

IPS入侵防御系统模型

IPS（Intrusion Prevention System）入侵防御系统是指不但能检测入侵发生，且能通过一定的响应方式，实时中止入侵行为的发生和发展，实时保护信息系统不受实质性攻击的一种安全机制。（下转第17页）

（上接第27页）

防火墙和入侵检测的互动是实现IPS入侵防御的基础。在Linux系统上构建IPS，首先用snort来进行监控，并记录日志，然后通过guardian程序对日志文件进行分析，发现有恶意IP访问时自动将其转给iptables并将拒绝其访问请求。基于这种思想，再加上WEB和PHP页面处理，就可以构建一个网络防御系统，总体结构如图4所示。

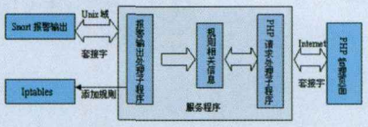

图4 snort和iptables结合的工作流程

从图4可以看出，我们把snort入侵检测规则转换成iptables字符串匹配规则后，Netfilter防火墙工作时只使用iptables规则，不存在snort规则，因此整个入侵防御系统的体系结构更加简单、清晰，这样也给系统带来更高的可靠性。snort入侵检测规则在不断的更新，对于新的snort入侵检测规则，可以转换成iptables规则，方便地加入到我们的入侵防御系统中。同时Netfilter是一个开放的框架，用户可以根据自己的需要编写自己的功能模块或安装需要的补丁到Netfilter中，增强整个入侵防御系统的功能。而且，这样也使得入侵防御系统具有了更好的扩展性。

IDS与防火墙有效互动就可以实现一个较为有效的安全防护体系，可以大大提高整体防护性能，解决了传统信息安全技术的弊端、解决了原先防火墙的粗颗粒防御和检测系统只发现难响应的问题。二者结合使用可以很好的将对方的弱点淡化，而将自己的优点补充上去，使防御系统成为一个更加坚固的围墙。在未来的网络安全技术领域中，将动态技术与静态技术的互动使用，将有很大的发展市场和空间。

总之，以防火墙为代表的访问控制技术和以LIDS/Snort为代表的检测技术是加固Linux系统安全防线的基础，将其有效的结合，取长补短，便可打造出一个稳定、安全的Linux操作系统，为你的应用和服务提供强有力的保证。（全文完）

CIFS、FC或iSCSI）来实现这一功能。

恢复的精细程度

不同的CDP解决方案提供多种不同精细程度的恢复能力。恢复精细程度可以分为如下几种（按由低到高的顺序排列）：卷组、单个卷或文件系统、单个文件夹或文件组、单个文件或应用对象（如电子邮件或日历项目）。

恢复时间应用集成

一些CDP解决方案为某些应用提供一种集成的恢复方法。也就是说，在进行恢复时，CDP解决方案能够了解（并且能够识别）到该应用的先前历史中最优化或最重要的恢复点。这类应用集成可以是完全自动的，也可以是可扩展的。

内置应用集成是一种全自动的方法。例如，一个对数据库非常了解的CDP解决方案可能会自动探测并记录最近连贯事件的信息，如检查点或执行交易等。

CDP解决方案还可以提供一种机制，通过一些外部的输入信息或流程来指定重要的应用恢复点。这类集成是可扩充的。例如，可以利用用户界面活动（或命令行工具）等方式来指定当前是一个重要的时间点，如病毒扫瞄结束，或者是公司财务季度结束等。

需要注意的是，基于应用的CDP解决方案通常可以自动了解重要应用的恢复点。然而，基于文件和块的CDP解决方案还可以通过一种自动或可扩展的方式来提供深层的应用集成。

针对数据库的连续保护支持

许多CDP解决方案都支持一些常见数据库环境（如Oracle或Microsoft SQL）的连续保护。在这里，支持的意思是该解决方案经过了厂商的全面测试和认证，而且还会向用户提供已经准备好的文档内容。

库架构

许多CDP解决方案的架构都是将其作为一种CDP存储库（也就是说，将所有数据中的变化存储在独立的地点），而且这种存储库是局域网、广域网或存储区域网上明确的专用节点。其他的CDP解决方案则依靠受保护的主机，并将数据直接写入独立的CDP存储器上。

复制库

一些CDP解决方案还提供将CDP库复制到另外一个远程库的能力。这样就可以提供更高的灵活性，防止主CDP库可能出现损坏或丢失对恢复能力产生影响。

CDP产品概览及发展趋势

关于CDP的产品可谓五花八门，异彩纷呈，有知名的软件厂商，也有因CDP软件的发展而让人知晓的公司。这些CDP厂商最为纯正的是一些不出名的小软件公司，但是对于这样的安全性要求极高的数据保护系统，用户怎么能够放心使用呢？于是在IT这个圈内，大的著名厂商开始以OEM的方式，取得了专注于CDP软件厂商的产品，以自己的品牌销售，譬如IBM和EMC。这也给我们一个启示，在当前数据安全、法规遵从日益严格的条件下，CDP的发展是一个必然的趋势，而CDP厂商的并购似乎显得也是一个必然的现象。无论是哪种趋势，对于数据容灾来看，CDP是一个很好的选择。