论文阅读手札

论文名称：1.利用多线程技术改造Snort系统(XXXX)

评价： ☆☆☆☆☆ ☆

参考价值：☆☆☆☆☆

主要内容：

提出使用多线程改进snort NIDS，在各个处理模块之间加入缓冲区，每个模块加入忙闲检测位，每个模块使用一个线程处理，相信确实能够提高处理效率。

评价：相当具有参考价值，可以重点考虑。

评论：

libpcap会将网卡数据复制到内核缓冲区，在复制到用户缓冲区，由于用户处理效率不足，数据包的丢失就产生了。考虑为snort分配两个总线程，pcap\_loop抓包之后，将数据包放入缓冲队列，以队列方式组织。ProcessPacket（）分别运行在两个内核的两个线程上，从缓冲队列取数据包，在大线程里面可以在分小线程，在耗时部分分配更多资源。

论文名称：2. Snort报文捕获机制的研究与改进

评价： ☆☆

参考价值：☆☆

主要内容：

允许丢包，因为处理效率跟不上抓包效率，抓包时采取采样的方法，通过统计学规律分析系统的行为和动作。

评论：无

论文名称：3. Snort匹配机制的改进

评价： ☆☆☆

参考价值：☆☆☆

主要内容：

1. 增加了一个预处理模块，匹配数据包的应用层，先过滤一遍（让我联想到了iptables L7）。
2. 改进了字符匹配算法BM的效率

评论：认为该方法可以参考，有一定的参考价值

论文名称：4. 提高snort性能的方法

评价： ☆☆☆☆

参考价值：☆

主要内容：

论述了一些改进snort性能的方法，但是没有对snort进行改动，仅仅改动了配置，如使用高性能的处理器，使用高性能网卡，认真配置snort规则等等。

评论：可以看一下，但是参考价值不大。

论文名称：5. 基于snort与免疫原理混合入侵检测系统模型设计(XXX)

评价： ☆☆☆☆☆

参考价值：☆☆☆

主要内容：

阐述了要将误用检测（例如snort）与异常检测（如bro）结合起来的方法，但是在本文中是将异常检测作为一个插件加载进snort的。

评论：

参考价值很高，但是难度极大。若我们自己开发异常检测引擎，耗时会不少。可以采用bro这个现成的异常检测引擎，会比价好，关键是如何融合的问题。

论文名称：6. Snort数据包捕获性能的分析与改进

评价： ☆☆☆☆☆

参考价值：☆☆☆☆

主要内容：

1. 采用NAP I技术,减少中断调用次数;
2. 采用内存映射技术,使内核空间与用户空间共享同一块内存区域,从而避免了每

次读取数据包都需要经过系统调用的问题。（数据包零拷贝）

评论：

可以考虑，但是论文中没有提到具体的实现方法，所以难度较大，另外，对效率的提高也是有极限的。

论文名称：7. Snort检测引擎的分析与改进

评价： ☆☆☆☆

参考价值：☆☆☆

主要内容：

Snort模式匹配算法分为：BM、AC、AC-BM等，本文提出了一种改进的算法，但是我对算法比较头大，所以这篇文章没怎么看。

评论：

要是改进某个匹配算法的话我没多大信心，因为我算法不好，而且我觉得这些算法相对比较成熟了，提高也不会提高多少，但是貌似作者验证自己的算法对snort性能的提高还是蛮大了，所以对算法的改进也在考虑之列了吧。

论文名称：8. 基于Snort的入侵检测系统的改进(XXX)

评价： ☆☆☆☆☆

参考价值：☆☆☆☆☆

主要内容：

Snort 系统数据包捕获大约占用了系统时间的20%;其中大量的时间用于软中断和系统调用。攻击检测约占用了系统时间的57 % ,其中大量的时间用于模式匹配。

提出改进snort性能的一些方法：

1. 零拷贝，方法可以使用DMA数据传输技术和内存区域映射技术
2. 将分析程序放在核心态，避免频繁的进程切换。
3. 改进模式匹配算法。

评论：

要是改进某个匹配算法的话我没多大信心，因为我算法不好，而且我觉得这些算法相对比较成熟了，提高也不会提高多少，但是貌似作者验证自己的算法对snort性能的提高还是蛮大了，所以对算法的改进也在考虑之列了吧。

论文名称：9. 基于Snort的入侵检测系统性能优化.

评价： ☆☆

参考价值：☆☆

主要内容：

读了一下，觉得没啥意思，两个方法，一个是改进匹配算法，另一个是改进了链表结构

评论：

本人认为没什么参考价值，但是还是推荐看一下，原因是——这篇文章是川大计算机学院的研究生写的，发表与2008年。

未完待续。。。。。。

论文名称：10. 入侵检测系统Snort的不足与改进

评价： ☆☆

参考价值：☆☆

主要内容：

评论：

随想：

iptables L7

我们想到的都是改进，可不可以大胆一些，大刀阔斧的改革或是整个颠覆snort？

神经网络算法，snort增加自我学习能力

人工免疫算法，snort增加异常检测

常用的异常检测方法有：专家系统、神经网络、机器学习、和人工免疫等。

文章中提到了很多测试环节，认为在项目开发初期就要策划测试环节。