第 19 卷第 4 期　　广西科学院学报　　Vol. 19, No. 4
2003 年 11 月　　Journal of Guangxi Academy of Sciences　　November 2003

协议分析技术在 NIDS 中的应用*

Application of Protocol Analysis Technology in NIDS

葛志辉　　李陶深
Ge Zhihui　Li Taoshen

（广西大学计算机与信息工程学院　南宁　530004）
(Coll. of Comp. & Info. Engi., Guangxi Univ., Nanning, 530004)

摘要　简要分析 NIDS 中传统模式匹配方法存在的不足，介绍第三代入侵检测系统中使用的协议分析技术，给出一个在 Linux 平台下实现该技术的模型。

关键词　模式匹配　协议分析　入侵检测　NIDS
中图法分类号　TP393

Abstract　The flaw of traditional pattern matching used in NIDS is analyzed. The third Generation Intrusion Detection Technology (Protocol Analysis technology) is discussed. And a implementation model of the technology under Linux platform is also presented.

Key words　pattern matching, protocol analysis, intrusion detection, NIDS (Network Intrusion Detection Systems)

随着 Internet/Intranet 网络技术的迅速发展和广泛应用，使得网络流量急剧增长。目前网络入侵检测系统 (Network Intrusion Deteetion System，以下简称 NIDS) 的瓶颈就是对数据的分析处理。如何解决对高速度、大流量的网络进行无漏包监听和实时分析处理问题成为决定 NIDS 性能的关键。

传统的模式匹配方法由于存在计算量大、消耗系统资源较多等缺点，已经不适应于当前网络系统的需求。因此，迫切需要研究出一种新的方法来取代传统的模式匹配方法，或者改进现有的模式匹配方法，以提高 NIDS 的整体性能。

采用对数据包的结构进行分析的方法可以解决传统模式匹配方法面临的问题。它不仅可以大大减小模式匹配的计算量，还可以提高匹配的精确度，减少误报率。

1　模式匹配方法概述

模式匹配方法是入侵检测系统中最常用的一种数据分析方法，其任务就是把存在入侵检测系统规则集中的已知入侵规则（模式）与系统正在检测的网络数据包中的文本进行比较，如

2003-06-10 收稿。
* 广西科技攻关项目（桂科攻 033008-9）资助。

果匹配成功，则可以判定发生了攻击。其工作原理如下：

已知一长度为 $n(n>0)$ 的文本串：

$$T=T_1T_2\cdots T_n,$$

和一长度为 $m(m\leqslant n)$ 的模式字符串：

$$P=P_1P_2\cdots P_m,$$

查找 T 中是否存在长度为 m 的子串

$$T_{i-1}T_{i-2}\cdots T_{i-m},$$

使得

$$T_{i-j}=P_j,(j=1,2,\cdots,m;i\leqslant n-m).$$

模式匹配方法将数据看作是随机变化的字节流，通过应用固定的特征模式来探测网络的攻击。但是，该方法存在 2 个弱点：

（1）算法的计算量非常大。以一个全负载的 100 M 以太网为例，所需的计算量为：攻击特征字节数×网络数据包字节数×每秒数据包数量×攻击特征数量。假定一个特征有 20 字节，包平均大小有 300 字节，包到达速率为每秒 30000，库中有 4000 个特征，那么所需的计算量为：$20\times300\times30000\times4000=7.2\times10^{11}$次/秒。

（2）探测准确率有限。由于该方法是使用固定的特征模式去探测攻击，所以只能检测到特定的攻击特征。对于那些哪怕是只有微小改动的攻击变种，该方法都无法检测到。

2 协议分析方法概述

协议分析方法是第三代入侵检测系统中用来探测攻击特征的技术。协议分析利用网络协议高度有效化的特点，快速地探测攻击，并在不丢包的情况下对包进行详细分析。下面简单介绍协议分析方法的工作原理。

协议规范指出：以太网络数据包中第 13 字节处包含了 2 个用作第三层协议标识的字节。基于协议分析的入侵检测系统就是利用这个知识来开始检测，其具体工作步骤如下：

（1）跳过前面 12 个字节，读取 13 字节处的 2 个字节（协议标识），如果值为 0800，根据协议规范可以判断这个网络数据包是 IP 包。

（2）IP 协议规定：IP 包的第 24 字节有一个用作第四层协议标识的字节。根据这一规定，系统跳到 24 字节直接读取第四层协议标识，如果值为 06，则这个数据包是 TCP 协议。

（3）TCP 协议规定：第 35、36 两个字节用于应用层协议的标识（端口号）。据此，系统跳到 35 字节直接读取端口号，如果值为 80，则说明该数据包是一个 HTTP 协议的数据包。

（4）HTTP 协议规定：第 55 字节是 URL 的开始处。因此，如果我们要检测基于 HTTP 协议的攻击的话，只要仔细检测这个 URL 就可以了。

可以看出，利用协议分析可以大大减小模式匹配的计算量，提高匹配的精确度，减少误报率。

3 协议分析方法实现模型

基于上述技术，提出一个在 Linux 平台下协议分析技术的实现模型。其主要由分组捕获器、网络协议解码器和数据包分析器 3 个模块组成，其实现流程图如图 1 所示。

3.1 分组捕获器

分组捕获器主要是收集数据链路层的数据包分组。其功能可以通过 Libpcap 库提供的函数来实现。

Libpcap 实质上是一个系统独立的 API 函数接口，负责用于用户层次的数据包截获工作。它为底层网络监控编程提供了一个易于移植的应用框架，这些底层网络应用包括网络数据的收集、安全监控和网络调试等。

Libpcap 接口支持基于 BSD 数据包过虑器（BPF，Berkeley Packet Filter）的数据过虑机制。Libpcap 函数库中常用函数如下：

（1）pcap _ lookupdev：选择数据包捕获设备；

（2）pcap _ lookupnet：获取网络地址和子网掩码；

（3）pcap _ open _ live：打开设备；

（4）pcap _ compile：编译数据包过虑规则；

（5）pcap _ setfilter：设置数据包过虑规则；

（6）pcap _ loop：捕捉数据包，分发数据包到指定的回调函数。

图 2 给出了数据采集程序的流程图。

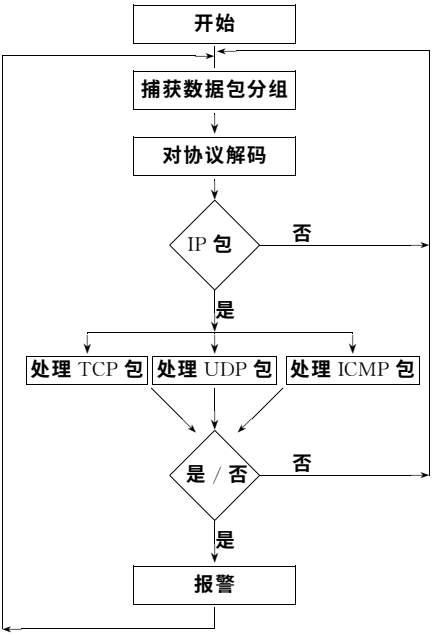

图 1　协议分析流程

3.2 网络协议解码器

网络协议解码器的功能是：首先将捕获到的数据包根据不同的网络协议进行解码，并把解码的结果存入相应的数据结构，然后把它提交给数据包分析器进行异常判断。由于网上的绝大多数攻击都集中于 TCP，UDP 和 ICMP 3 种协议，所以我们把网络协议解码器的重点放在处理 3 种协议上。

3.3 数据包分析器

数据包分析器的功能是：对解码后的数据与已知的攻击模式进行比较，如果相匹配，则报警。

3.4 技术考虑

对于基于网络的入侵检测系统关键是处理速度问题，即如何保证系统能够在不丢包的情况下对数据进行处理。在机器性能已定的情况下，为了进一步提高对数据包的处理速度，可以采用多个进程并行处理的技术，每个进程只处理特定类型的数据包。处理过程 packet—process 可用伪代码表示如下：

```
switch（ip—>protocol）
    {
    case IPPROTO _ TCP：
      do _ tcp （）；//处理 TCP 包的进程
```

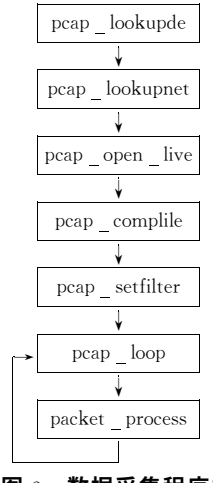

图 2　数据采集程序的流程

```
        break;
    case IPPROTO_UDP:
        do_udp();  //处理 UDP 包的进程
        break;
    case IPPROTO_ICMP:
        do_icmp();  //处理 ICMP 包的进程
        break;
    default:
            do_unknown();  //未能识别协议类型
        break;
    }
```

以上模型在 Red Hat 7.2 平台下通过测试。

4 结束语

使用协议分析方法的 NIDS 比单纯使用模式匹配的方法在性能上有了很大提高，但它也存在着一些不足之处，如可能会产生误报，有时解码引擎必须重新编写，等等。未来 NIDS 的研究应该继续提高模式匹配的效率和协议分析的性能，将 2 个领域的技术在 NIDS 中有机地结合起来，使得 NIDS 可以兼具检测快、不易被欺骗、能识别新型攻击等优点。

参考文献

1 Neil Desai. Increasing Performance in High Speed NIDS. Http://www.snort.org. 2003-02-10.

2 Protocol Analysis and Command Parsing vs. Pattern Matching in Intrusion Detection Systems. Http://www.networkice.com. 2003-02-11.

3 王 勇，王一川. GNU/Linux 编程指南. 林花军等译. 北京：清华大学出版社，2000.

（责任编辑：黎贞崇）

（上接第 266 页）

设置软件。系统设置软件主要功能包括：系统通信方式的设置，系统采样、高通滤波器、低通滤波器、自动标定参数的设置。

3 结束语

嵌入式系统单元的引入使现有的地震仪器变得更加专业化、小型化，在可靠性和易用性上也有较大的提高，特别方便了野外维护、选台、流动地震台的建设。嵌入式系统不仅可应用于地震观测系统，也可应用于工程地震方面的系统中。

参考文献

1 魏 忠，蔡 勇，雷红卫编. 嵌入式开发详解. 北京：电子工业出版社，2003.

2 Jeff Dionne D. Embedded Linux/Microcontroller Project. Http://www.uclinux.org，2002.

（责任编辑：邓大玉）