

<<网络入侵检测系统的设计与实现>>

图书基本信息

书名：<<网络入侵检测系统的设计与实现>>

13位ISBN编号：9787505374140

10位ISBN编号：7505374141

出版时间：2002-4

出版时间：电子工业出版社

作者：唐正军等

页数：541

字数：886

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<网络入侵检测系统的设计与实现>>

内容概要

这是国内第一本全面覆盖网络入侵检测系统从设计基础到源码实现的技术书籍。

本书所介绍的知识清晰全面，从入侵检测的概念、网络数据流的捕获技术开始，到入侵检测的不同方法，如基于专家系统的入侵检测、基于统计分析的入侵检测等等，最后是对系统具体源代码实现内核的深入剖析，可使用户对于入侵检测技术有一个比较全面的理解。

读者如果想要学习入侵检测技术，可以从阅读本书中介绍的知识开始。

<<网络入侵检测系统的设计与实现>>

书籍目录

目 录?

第1章 概述

- 1.1 入侵检测系统的组成部分
- 1.2 滥用入侵检测系统?
- 1.3 非规则入侵检测系统?
- 1.4 两种分析技术的比较?
- 1.5 入侵检测系统的层次体系?
- 1.6 进一步发展的若干方向
 - 1.6.1 宽带高速网络的实时入侵检测技术
 - 1.6.2 大规模分布式入侵检测技术
 - 1.6.3 入侵检测的数据融合技术
 - 1.6.4 先进检测算法的应用?
- 1.7 面临的挑战?

第2章 网络编程基础知识?

- 2.1 分层协议模型?
- 2.2 开放系统互联参考模型OSI/ISO?
- 2.3 TCP/IP参考模型?
- 2.4 UNIX网络编程技术概述?
- 2.5 TCP/IP协议
 - 2.5.1 网络接口层协议
 - 2.5.2 ARP协议和RARP协议
 - 2.5.3 IP协议
 - 2.5.4 ICMP协议
 - 2.5.5 TCP协议
 - 2.5.6 UDP协议?

第3章 网络数据包截获机制分析?

- 3.1 基本的网络数据包截获机制?
- 3.2 高效的数据包截获/过滤机制
 - 3.2.1 概述
 - 3.2.2 BPF的工作原理
 - 3.2.3 BPF虚拟机的实现
 - 3.2.4 BPF程序源代码?
- 3.3 数据包截获的Libpcap库函数接口
 - 3.3.1 概述
 - 3.3.2 Libpcap库函数接口
 - 3.3.3 采用Libpcap库的数据包截获实例?

第4章 入侵检测引擎的设计?

- 4.1 IDES系统概述
 - 4.1.1 什么是IDES系统
 - 4.1.2 IDES的系统设计
 - 4.1.3 IDES的审计记录格式?
- 4.2 用于入侵检测的统计分析测量值
 - 4.2.1 用户测量值
 - 4.2.2 目标系统
 - 4.2.3 远程主机?

<<网络入侵检测系统的设计与实现>>

4.3 基于统计分析的分析算法

- 4.3.1 IDES分数值 (score)
- 4.3.2 分数值T2如何从单个测量值获得
- 4.3.3 单个测量值类型
- 4.3.4 S与Q联系的启发式描述
- 4.3.5 从Q计算S的算法
- 4.3.6 计算Q的频率分布
- 4.3.7 计算活动强度测量值的Q值
- 4.3.8 计算审计记录分布测量值的Q值
- 4.3.9 计算类别测量值的统计值Q
- 4.3.10 计算序数测量值的Q值?

4.4 相关的数据结构及函数接口

- 4.4.1 数据结构
- 4.4.2 函数接口?

第5章 专家系统的应用?

- 5.1 概述?
- 5.2 由一个简单实例开始?
- 5.3 PBEST的基本语法?
- 5.4 更详细的语法介绍?
- 5.5 专家系统的外部接口?
- 5.6 一个示例Makefile?
- 5.7 PBEST语法图表?
- 5.8 带参数的pbcc调用?

第6章 入侵检测规则语言的设计?

- 6.1 概述?
- 6.2 N-Code语言的词法元素
 - 6.2.1 字符集
 - 6.2.2 注释
 - 6.2.3 运算符
 - 6.2.4 变量
 - 6.2.5 保留字
 - 6.2.6 常量?

6.3 N-Code语言的数据类型

- 6.3.1 概述
- 6.3.2 array
- 6.3.3 ethmac
- 6.3.4 error
- 6.3.5 int
- 6.3.6 ipv4host
- 6.3.7 ipv4net
- 6.3.8 list
- 6.3.9 recorder
- 6.3.10 str
- 6.3.11 pattern?

6.4 N-Code的表达式

- 6.4.1 概述
- 6.4.2 算术运算符

<<网络入侵检测系统的设计与实现>>

- 6.4.3 赋值运算符
- 6.4.4 位运算符
- 6.4.5 逻辑运算符
- 6.4.6 关系运算符
- 6.4.7 其他运算符?
- 6.5 N-Code语句
 - 6.5.1 概述
 - 6.5.2 assignment
 - 6.5.3 block
 - 6.5.4 break
 - 6.5.5 declare
 - 6.5.6 expression
 - 6.5.7 foreach
 - 6.5.8 If
 - 6.5.9 off
 - 6.5.10 on
 - 6.5.11 record
 - 6.5.12 requires
 - 6.5.13 return
 - 6.5.14 while?
- 6.6 N-Code中的函数?
- 6.7 N-Code中的函数声明
 - 6.7.1 概述
 - 6.7.2 函数的声明
 - 6.7.3 过滤器的声明
 - 6.7.4 作用域
 - 6.7.5 声明与赋值
 - 6.7.6 访问?
- 6.8 N-Code数据包变量
 - 6.8.1 ethernet变量组
 - 6.8.2 fddi变量组
 - 6.8.3 icmp变量组
 - 6.8.4 ip变量组
 - 6.8.5 llc变量组
 - 6.8.6 packet变量组
 - 6.8.7 system变量组
 - 6.8.8 tcp变量组
 - 6.8.9 udp变量组?
- 6.9 N-Code异常
 - 6.9.1 长度异常
 - 6.9.2 校验和异常
 - 6.9.3 协议异常
 - 6.9.4 内部异常?
- 第7章 NFR入侵检测系统实例?
 - 7.1 IDA系统的基本工作原理
 - 7.1.1 NFR IDA系统功能概述
 - 7.1.2 IDA系统环境构成

<<网络入侵检测系统的设计与实现>>

- 7.1.3 NFR IDA系统架构
- 7.1.4 IDA引擎组件
- 7.1.5 后端组件
- 7.1.6 警报
- 7.1.7 查询
- 7.1.8 后台进程
- 7.1.9 分布式环境中的应用?
- 7.2 如何使用IDA系统
 - 7.2.1 启动NFR IDA系统
 - 7.2.2 终止NFR IDA系统
 - 7.2.3 使用NFR控制台?
- 7.3 查询数据
 - 7.3.1 建立简单查询
 - 7.3.2 打印查询结果
 - 7.3.3 限制查询
 - 7.3.4 保存查询
 - 7.3.5 载入查询
 - 7.3.6 将数据导出到数据库
 - 7.3.7 使用Perl查询附件 (Perl Query Add-on) ?
- 7.4 查看警告
 - 7.4.1 概述
 - 7.4.2 理解警告组件
 - 7.4.3 使用警告查看器?
- 7.5 配置包与后端组?
 - 7.5.1 启用包与后端组件
 - 7.5.2 禁用包与后端组件
 - 7.5.3 配置磁盘空间
 - 7.5.4 配置值
 - 7.5.5 添加包与后端组件
 - 7.5.6 删除包或后端组件?
- 7.6 配置警告
 - 7.6.1 理解警告组
 - 7.6.2 改变警告规则
 - 7.6.3 建立新规则?
- 7.7 配置访问控制
 - 7.7.1 理解访问控制
 - 7.7.2 理解用户管理
 - 7.7.3 设置权限
 - 7.7.4 配置用户账户?
- 7.8 控制IDA性能
 - 7.8.1 理解系统状态报表
 - 7.8.2 查看系统历史状态
 - 7.8.3 查看系统状态报表?
- 7.9 包与后端组件列表
 - 7.9.1 具有可配置值的后端组件
 - 7.9.2 邮件
 - 7.9.3 网络统计

<<网络入侵检测系统的设计与实现>>

- 7.9.4 网络服务
- 7.9.5 攻击特征
- 7.9.6 拒绝服务 (DoS) 检测
- 7.9.7 产品特定模块
- 7.9.8 入侵检测
- 7.9.9 扫描器?
- 7.10 理解数据类型?
- 7.11 术语表?
- 第8? 网络入侵检测系统的具体实现?
 - 8.1 概述
 - 8.1.1 Snort系统概述
 - 8.1.2 系统程序架构?
 - 8.2 初始化、主函数和命令行解析
 - 8.2.1 初始化、主函数和命令行参数分析例程
 - 8.2.2 Snort使用方法
 - 8.2.3 PV数据结构
 - 8.2.4 ParseCmdLine (325)
 - 8.2.5 SetPktProcessor (548)
 - 8.2.6 OpenPcap (666)
 - 8.2.7 主函数main (153)
 - 8.2.8 ProcessPacket (759) ?
 - 8.3 协议解析?程分析
 - 8.3.1 协议解析器 (Decoder) 例程
 - 8.3.2 Packet数据结构 (1243)
 - 8.3.3 DecodeEthPkt (1303)
 - 8.3.4 DecodePppPkt (1573)
 - 8.3.5 DecodeTRPkt (1395)
 - 8.3.6 DecodeNullPkt (1368)
 - 8.3.7 其他的数据链路层协议解析例程
 - 8.3.8 DecodeIP (1681)
 - 8.3.9 DecodeTCP (1800)
 - 8.3.10 DecodeUDP (1845)
 - 8.3.11 DecodeICMP (1877)
 - 8.3.12 DecodeARP (1916)
 - 8.3.13 DecodeIPV6 (1935) 、 DecodeIPX (1951)
 - 8.3.14 DecodeTCPOptions (1967)
 - 8.3.15 DecodeIPOptions (2037) ?
 - 8.4 如何编写Snort的规则
 - 8.4.1 规则头
 - 8.4.2 规则选项
 - 8.4.3 预处理器
 - 8.4.4 输出模块
 - 8.4.5 高级规则概念?
 - 8.5 规则解析例程分析
 - 8.5.1 规则 (Rule) 解析例程
 - 8.5.2 RuleTreeNode数据结构 (2162)
 - 8.5.3 OptTreeNode数据结构 (2142)

<<网络入侵检测系统的设计与实现>>

- 8.5.4 RuleFpList (2129) 、 RuleOptList (2137)
- 8.5.5 ListHead数据结构 (2182)
- 8.5.6 mSplit (3210)
- 8.5.7 ParseRulesFile (2224)
- 8.5.8 规则解析器ParseRule (2287)
- 8.5.9 规则链表头处理例程ProcessHeadNode (2397)
- 8.5.10 AddRuleFuncToList (2487)
- 8.5.11 SetupRTNFuncList (2523)
- 8.5.12 AddrToFunc (2563) 和PortToFunc (2604)
- 8.5.13 ParsePreprocessor (2681)
- 8.5.14 ParseOutputPlugin (2749)
- 8.5.15 ParseListFile (2895)
- 8.5.16 CreateRule (2939)
- 8.5.17 ParseRuleOptions (2966)
- 8.5.18 ParseMessage (3110)
- 8.5.19 ParseLogto (3147)
- 8.5.20 ParseResponse (3178) ?
- 8.6 检测引擎例程分析
 - 8.6.1 检测引擎 (Detection Engine) 例程
 - 8.6.2 Preprocess (3328)
 - 8.6.3 Detect (3351)
 - 8.6.4 EvalPacket (3398)
 - 8.6.5 EvalHeader (3453)
 - 8.6.6 EvalOpts (3501)
 - 8.6.7 CheckBidirectional (3534)
 - 8.6.8 CheckSrcIPEqual (3590)
 - 8.6.9 CheckSrcIPNotEq (3602)
 - 8.6.10 CheckDstIPEqual (3631)
 - 8.6.11 CheckDstIPNotEq (3649)
 - 8.6.12 CheckSrcPortEqual (3658)
 - 8.6.13 CheckSrcPortNotEq (3666)
 - 8.6.14 CheckDstPortEqual (3674)
 - 8.6.15 CheckDstPortNotEq (3682)
 - 8.6.16 CheckAddrPort (3698) ?
- 8.7 插件模块管理例程分析
 - 8.7.1 插件 (Plugins) 管理例程
 - 8.7.2 KeywordXlateList (3841)
 - 8.7.3 PreprocessKeywordList (3852)
 - 8.7.4 OutputKeywordList (3875)
 - 8.7.5 InitPlugins (3896)
 - 8.7.6 InitPreprocessors (3917)
 - 8.7.7 InitOutputPlugins (3929)
 - 8.7.8 RegisterPlugin (3951)
 - 8.7.9 SetupIcmpCodeCheck (4081)
 - 8.7.10 IcmpCodeCheckInit (4095)
 - 8.7.11 ParseIcmpCode (4118)
 - 8.7.12 IcmpCodeCheck (4152)

<<网络入侵检测系统的设计与实现>>

- 8.7.13 SetupMinfrag (4169)
- 8.7.14 MinfragInit (4173)
- 8.7.15 ProcessMinfragArgs (4178)
- 8.7.16 CheckMinfrag (4216)
- 8.7.17 SetupFastAlert (4253)
- 8.7.18 FastAlertInit (4265)
- 8.7.19 SpoAlertFast (4275)
- 8.7.20 ParseFastAlertArgs (4291)
- 8.7.21 FastAlertCleanExitFunc (4308) 和FastAlertRestartFunc (4315) ?
- 8.8 预处理器插件模块分析
 - 8.8.1 预处理器 (Preprocessor) 插件模块
 - 8.8.2 PortList数据结构 (4323)
 - 8.8.3 http decode预处理器插件管理例程
 - 8.8.4 SetPorts (4362)
 - 8.8.5 预处理器主模块PreprocUrlDecode (4387)
 - 8.8.6 一组用于端口扫描 (Portscan) 预处理器插件的数据结构
 - 8.8.7 Portscan预处理器插件管理例程
 - 8.8.8 ParsePortscanArgs (4567)
 - 8.8.9 Portscan?ignorehosts?处理器插件管理例程?
 - 8.8.10 CreateServerList (4640)
 - 8.8.11 预处理器主模块PortscanPreprocFunction (4673)
 - 8.8.12 CheckTCPFlags (4784)
 - 8.8.13 ExpireConnections(4877)
 - 8.8.14 RemoveConnection (4955)
 - 8.8.15 NewScan (5041)
 - 8.8.16 NewConnection(5164)
 - 8.8.17 AddConnection (5206)
 - 8.8.18 ClearConnectionInfoFromSource (5272)
 - 8.8.19 LogScanInfoToSeparateFile (5303)
 - 8.8.20 AlertIntermediateInfo (5424)
 - 8.8.21 其他的连接管理例程
 - 8.8.22 几个工具例程?
- 8.9 规则选项关键字插件模块分析
 - 8.9.1 规则选项关键字 (Keyword) 插件模块
 - 8.9.2 参数解析例程ParseDsize (5470)
 - 8.9.3 dsize插件模块CheckDsizeGT (5505)、CheckDsizeLT (5515) 和CheckDsizeEQ (5495)
 - 8.9.4 PatternMatchData数据结构 (5527)
 - 8.9.5 content插件管理例程
 - 8.9.6 参数解析例程ParsePattern (5646)
 - 8.9.7 content插件处理模块CheckPatternMatch (5836)
 - 8.9.8 参数解析例程ParseSession (5914)
 - 8.9.9 session插件处理模块LogSessionData (5934)
 - 8.9.10 DumpSessionData (5953)
 - 8.9.11 OpenSessionFile (5993)
 - 8.9.12 参数解析例程ParseIpOptionData (6082)
 - 8.9.13 ipoptions插件主处理模块CheckIpOptions (6148)
 - 8.9.14 resp插件主模块Respond (6165)

<<网络入侵检测系统的设计与实现>>

8.9.15 SendICMP-UNREACH (6203) 和SendTCPRST (6237)

8.9.16 其他的选项关键字插件处理模块?

8.10 输出插件模块分析

8.10.1 输出 (Output) 插件模块

8.10.2 主处理模块AlertFast (6778)

8.10.3 OpenAlertFile (6826)

8.10.4 ProcessFileOption (6853)

8.10.5 FastAlertCleanExitFunc (6881) 和FastAlertRestartFunc (6888)

8.10.6 主处理函数AlertFull (6921)

8.10.7 PrintIPHeader (6971)

8.10.8 参数解析例程ParseTcpdumpArgs (7108)

8.10.9 TcpdumpInitLogFile (7129)

8.10.10 主处理函数LogTcpdump (7154)

8.10.11 pcap-dump-open (7160) 和pcap-dump (7176)

??

版权说明

本站所提供下载的PDF图书仅提供预览和简介, 请支持正版图书。

更多资源请访问:<http://www.tushu007.com>