第七次作业

姓名：周玉川　　学号：2017221302006

测试点 7-1

(一) 入侵检测如何分类？

第一种，按数据检测方法

可分为异常检测模型（Anomaly Detection)

误用检测模型（Misuse Detection)

第二种，按按系统结构

可分为集中式和分布式。

第三种，按按时效性

可分为离线入侵检测系统（off-line IDS），

在线入侵检测系统（On-line IDS）

第三种，按按数据来源

基于主机的入侵检测系统（HIDS）

基于网络的入侵检测系统（NIDS）

混合型入侵检测系统（Hybrid IDS）

网络节点入侵检测系统（NNIDS）

文件完整性检测系统

(二) 入侵检测系统的主要技术指标有哪些？

入侵检测系统的主要指标有性能指标和功能指标。

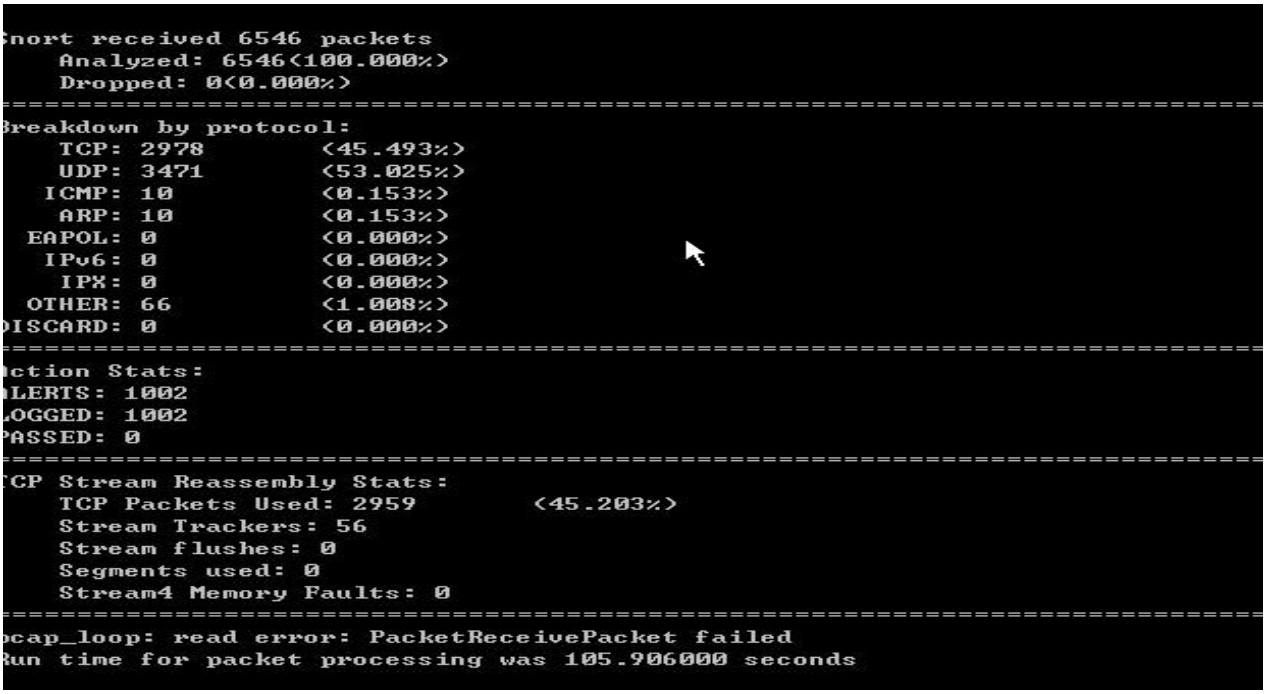
性能指标有准确性（Accuracy），处理性能（Performance），完备性（Completeness），容错性（Fault Tolerance），及时性（Timeliness）5 个因素。可以根据漏报率、误报率、资源占用率，以及特征库强度进行测试。

功能指标分为系统结构检测引擎和控制台。系统结构：集中/分布式结构、本地/远程管理模式、通讯安全；探测引擎：检测能力、事件响应、自身安全；控制台：策略灵活性、自定义事件、事件库更新、易用性、综合分析、事件数量

(三) 常用的未知攻击检测方法有哪些？

常见的未知攻击检测方法有统计分析、神经网络、数据挖掘等基于异常的检测方法。

(四) 课后练习：安装配置 Snort 系统，使用 NMAP 对系统进行扫描，观察 snort 是否能够检测出相关的扫描活动。


nort received 6546 packets
Analyzed: 6546(100.000%)
Dropped: 0(0.000%)
reakdown by protocol:
TCP: 2978 (45.493%)
UDP: 3471 (53.025%)
ICMP: 10 (0.153%)
ARP: 10 (0.153%)
EAPOL: 0 (0.000%)
IPv6: 0 (0.000%)
IPX: 0 (0.000%)
OTHER: 66 (1.008%)
ISCARD: 0 (0.000%)
ction Stats:
LERTS: 1002
OGGED: 1002
ASSED: 0
CP Stream Reassembly Stats:
TCP Packets Used: 2959 (45.203%)
Stream Trackers: 56
Stream flushes: 0
Segments used: 0
Stream4 Memory Faults: 0
cap_loop: read error: PacketReceivePacket failed
un time for packet processing was 105.906000 seconds