(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102624696 B
(45)授权公告日 2014.11.05

(21)申请号 201110443114.X

(22)申请日 2011.12.27

(73)专利权人 中国航天科工集团第二研究院七〇六所
地址 100854 北京市海淀区永定路 51 号

(72)发明人 石波 王晓程 王斌 胡晴 陈志浩

(74)专利代理机构 北京思海天达知识产权代理有限公司 11203
代理人 张慧

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 1472916 A,2004.02.04,
CN 101436967 A,2009.05.20,
CN 101867498 A,2010.10.20,
CN 102148820 A,2011.08.10,
US 6535227 B1,2003.03.18,
谢巍 .《基于多源网络安全事件的态势评估研究与设计》.《中国优秀硕士学位论文全文数据库 信息科技辑》.2010,(第 4 期),全文 .
韦勇 .《网络安全态势评估模型研究》.《中国博士学位论文全文数据库 信息科技辑》.2009,(第 10 期),全文 .
崔孝林 .《网络安全评估系统的设计与实现》.《中国优秀硕士学位论文全文数据库 信息科技辑》.2010,(第 7 期),全文 .
Li Yu et al..《Research on Network Security Situation Awareness Based on Association Rule》.《Internet Technology and Applications,2010 International Conference on 》.2010,

审查员 张洁

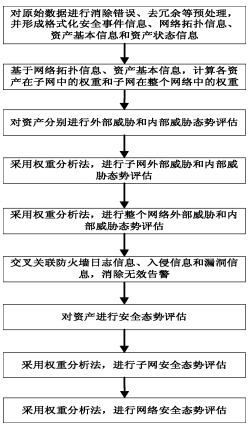
权利要求书2页 说明书7页 附图1页

(54)发明名称

一种网络安全态势评估方法

(57)摘要

一种网络安全态势评估方法,包括 :对原始数据进行预处理,计算各资产在子网中的权重和各子网在整个网络中的权重 ;对各资产进行外部威胁态势评估 ;对各资产进行内部威胁态势评估 ;采用权重分析法,进行各子网外部威胁态势评估和内部威胁态势评估 ;进行网络外部威胁态势评估和内部威胁态势评估 ;对防火墙日志信息、入侵信息和漏洞信息进行交叉关联,消除无效告警 ;综合评估各资产的安全态势 ;进行各子网安全态势评估 ;采用权重分析法,进行网络安全态势评估 ;本发明改变了现有技术中数据源单一的问题,使网络安全态势评估结果更加全面、精确 ;真实反映网络安全整体状况 ;评估结果直观实用,可以直接用于指导网络安全管理指挥、决策。



CN 102624696 B

1. 一种网络安全态势评估方法，其特征在于：包括以下步骤：

步骤 1：对原始数据进行预处理，消除重复信息和错误信息，生成格式化的安全事件信息、网络拓扑信息、资产基本信息和资产状态信息；

用于网络安全态势评估的数据来源包括防火墙、入侵检测系统、防病毒软件、漏洞扫描系统、拓扑发现工具、性能采集工具；经过去冗余、消除错误信息，再进行格式化，形成安全事件信息、网络拓扑信息、资产基本信息和资产状态信息；

步骤 2：基于网络拓扑信息、资产基本信息，计算各资产在子网中的权重和各子网在整个网络中的权重；

设定网络中有 n 个网络设备类资产 $ASSET_1$，$ASSET_2$，…，$ASSET_n$，每个网络设备类资产与其连接的终端类资产构成一个子网，根据网络拓扑信息，设定有 m 个终端类资产与网络设备类资产 $ASSET_k$($1 \leqslant k \leqslant n$) 相连接：$ASSET_{k1}$，$ASSET_{k2}$，…，$ASSET_{km}$；

计算网络设备类资产 $ASSET_k$ 的子网总资产值；

在计算权重时，设定权值为资产值的平方；

计算终端类资产 $ASSET_{kf}$ 在网络设备类资产 $ASSET_k$ 的子网中的权重；

计算网络设备类资产 $ASSET_k$ 在其子网中的权重；

计算网络设备类资产 $ASSET_k$ 的子网在整个网络中的权重；

步骤 3：基于入侵信息，对各资产进行外部威胁态势评估；基于病毒信息、漏洞信息，对各资产进行内部威胁态势评估；

在时间段 $[t_0, t_1]$ 内，无论入侵是否成功，对入侵信息进行统计，设定针对资产 $ASSET_w$ 的所有入侵信息为 IDS_1，IDS_2，…，IDS_p；

计算资产 $ASSET_w$ 的外部威胁态势值；

计算资产 $ASSET_w$ 的内部威胁态势值；

步骤 4：基于各资产在子网中的权重，采用权重分析法，进行各子网外部威胁态势评估和内部威胁态势评估；

网络设备类资产的子网外部威胁态势值就是该子网内所有资产的外部威胁态势值的加权和；

网络设备类资产的子网内部威胁态势值就是该子网内所有资产的内部威胁态势值的加权和；

步骤 5：基于各子网在整个网络中的权重，采用权重分析法，进行网络外部威胁态势评估和内部威胁态势评估；

网络外部威胁态势值就是所有子网的外部威胁态势值的加权和；

网络内部威胁态势值就是所有子网的内部威胁态势值的加权和；

步骤 6：对防火墙日志信息、入侵信息和漏洞信息进行交叉关联，消除无效告警；

针对资产 $ASSET_w$ 的入侵信息，若资产 $ASSET_w$ 上不存在入侵针对的漏洞，则该入侵无效，不会对网络安全产生危害，最终筛选得到针对资产 $ASSET_w$ 的所有有效入侵信息 IDS_1，IDS_2，…，IDS_s；

步骤 7：基于交叉关联后的各类信息，综合评估各资产的安全态势；

在时间段 $[t_0, t_1]$ 内，对资产状态信息进行统计，设定资产 $ASSET_w$ 的所有状态信息为 $STATE_{t0}$，$STATE_1$，$STATE_2$，…，$STATE_t$，$STATE_{t1}$；

计算资产 $ASSET_w$ 的单位时间流量；

资产的单位时间流量就是某时间段内总流量的平均值；

处理器平均使用率就是某时间段内所有采集的处理器使用率的算术平均值；

内存平均占用率就是某时间段内所有采集的内存占用率的算术平均值；

基于资产 $ASSET_w$ 的有效入侵信息、病毒信息、状态信息，计算资产 $ASSET_w$ 的安全态势值；

资产的安全态势值通过对单位时间流量、处理器平均使用率、内存平均占用率、有效入侵的严重等级、病毒严重等级的数学计算得到；

步骤 8：基于各资产在子网中的权重，采用权重分析法，进行各子网安全态势评估；

采用权重分析法，计算网络设备类资产 $ASSET_k$ 的子网综合安全态势值；

网络设备类资产的子网综合安全态势值就是该子网内所有资产的安全态势值的加权和；

步骤 9：基于各子网在整个网络中的权重，采用权重分析法，进行网络安全态势评估；

采用权重分析法，计算综合网络安全态势值；

综合网络安全态势值就是所有子网的综合安全态势值的加权和。

2. 根据权利要求 1 所述的一种网络安全态势评估方法，其特征在于：所述的安全事件信息分为防火墙日志信息、入侵信息、病毒信息、漏洞信息；防火墙日志信息 FW 包含：源地址、目的地址、源端口、目的端口、协议、处理方式；入侵信息 IDS 包含：目的地址、入侵类型、入侵针对的漏洞、入侵严重等级；病毒信息 VIRUS 包含：资产地址、病毒类型、病毒严重等级；漏洞信息 VUL 包含：资产地址、漏洞类型、漏洞严重等级。

3. 根据权利要求 1 所述的一种网络安全态势评估方法，其特征在于：所述的网络拓扑信息包括：资产标识、资产连接关系。

4. 根据权利要求 1 所述的一种网络安全态势评估方法，其特征在于：所述的资产基本信息 ASSET 包括：资产标识、资产类型、资产值、子网总资产值；资产基本信息分为两类：终端类和网络设备类，终端类资产的子网总资产值为 0，网络设备类资产的子网总资产值为该网络设备子网内所有资产的资产值总和。

5. 根据权利要求 1 所述的一种网络安全态势评估方法，其特征在于：所述资产状态信息包括：资产标识、时间、总流量、处理器使用率、内存占用率。

一种网络安全态势评估方法

技术领域

[0001] 本发明属于网络安全技术领域，特别是一种网络安全态势评估方法。

技术背景

[0002] 网络是信息时代的产物，目前几乎覆盖了世界上所有重要领域。随着网络规模不断扩大，网络攻击和破坏行为日益频繁，网络安全形势日趋严峻。为形成网络安全主动防护能力，首先需要了解网络的内外部威胁和整体安全状态。

[0003] 网络安全态势评估技术通过对网络中影响安全的因素进行深层次综合处理分析，对网络整体安全状况进行实时评估，为网络安全管理指挥、决策提供指导。

[0004] 目前用于网络安全态势评估的方法主要分为 3 类：基于数学模型的方法、基于知识推理的方法和基于模式识别的方法。但从应用的角度看，目前的研究还存在以下不足：

[0005] 1、数据源单一：用于网络安全态势评估的基础数据来源偏少，导致网络安全态势评估结果存在片面性，无法全面反映网络安全整体状况；

[0006] 2、评估结果不够精确：网络安全态势评估算法设计不合理，导致评估结果不够精确，无法真实反映网络安全整体状况；

[0007] 3、评估结果难于理解：评估结果仅仅是网络安全一个方面的数值或者等级，很难直接用于指导网络安全管理指挥、决策。

发明内容

[0008] 本发明的目的在于，通过提供一种网络安全态势评估方法，对网络中影响网络安全的因素进行综合处理分析，对外部和内部威胁态势分别进行评估，再对网络安全态势进行综合评估。

[0009] 本发明是采用以下技术手段实现的：

[0010] 一种网络安全态势评估方法，包括：安全事件信息、网络拓扑信息、资产基本信息和资产状态信息；包括以下步骤：

[0011] 步骤 1：对原始数据进行预处理，消除重复信息和错误信息，生成格式化的安全事件信息、网络拓扑信息、资产基本信息和资产状态信息；

[0012] 用于网络安全态势评估的数据来源包括防火墙、入侵检测系统、防病毒软件、漏洞扫描系统、拓扑发现工具、性能采集工具；经过去冗余、消除错误信息，再进行格式化，形成安全事件信息、网络拓扑信息、资产基本信息和资产状态信息。

[0013] 步骤 2：基于网络拓扑信息、资产基本信息，计算各资产在子网中的权重和各子网在整个网络中的权重；

[0014] 设定网络中有 n 个网络设备类资产 $ASSET_1$，$ASSET_2$，...，$ASSET_n$，每个网络设备类资产与其连接的终端类资产构成一个子网，根据网络拓扑信息，设定有 m 个终端类资产与网络设备类资产 $ASSET_k$($1 \leqslant k \leqslant n$) 相连接：$ASSET_{k1}$，$ASSET_{k2}$，...，$ASSET_{km}$；

[0015] 计算网络设备类资产 $ASSET_k$ 的子网总资产值；

[0016] 在计算权重时，设定权值为资产值的平方；

[0017] 计算终端类资产 $ASSET_{kf}$ 在网络设备类资产 $ASSET_k$ 的子网中的权重；

[0018] 计算网络设备类资产 $ASSET_k$ 在其子网中的权重；

[0019] 计算网络设备类资产 $ASSET_k$ 的子网在整个网络中的权重。

[0020] 步骤 3：基于入侵信息，对各资产进行外部威胁态势评估；基于病毒信息、漏洞信息，对各资产进行内部威胁态势评估；

[0021] 在时间段 $[t_0, t_1]$ 内，无论入侵是否成功，对入侵信息进行统计，设定针对资产 $ASSET_w$ 的所有入侵信息为 $IDS_1, IDS_2, \ldots, IDS_p$；

[0022] 计算资产 $ASSET_w$ 的外部威胁态势值；

[0023] 计算资产 $ASSET_w$ 的内部威胁态势值。

[0024] 步骤 4：基于各资产在子网中的权重，采用权重分析法，进行各子网外部威胁态势评估和内部威胁态势评估；

[0025] 网络设备类资产的子网外部威胁态势值就是该子网内所有资产的外部威胁态势值的加权和；

[0026] 网络设备类资产的子网内部威胁态势值就是该子网内所有资产的内部威胁态势值的加权和。

[0027] 步骤 5：基于各子网在整个网络中的权重，采用权重分析法，进行网络外部威胁态势评估和内部威胁态势评估；

[0028] 网络外部威胁态势值就是所有子网的外部威胁态势值的加权和；

[0029] 网络内部威胁态势值就是所有子网的内部威胁态势值的加权和。

[0030] 步骤 6：对防火墙日志信息、入侵信息和漏洞信息进行交叉关联，消除无效告警；

[0031] 针对资产 $ASSET_w$ 的入侵信息，若资产 $ASSET_w$ 上不存在入侵针对的漏洞，则该入侵无效，不会对网络安全产生危害，最终筛选得到针对资产 $ASSET_w$ 的所有有效入侵信息 $IDS_1, IDS_2, \ldots, IDS_s$。

[0032] 步骤 7：基于交叉关联后的各类信息，综合评估各资产的安全态势；

[0033] 在时间段 $[t_0, t_1]$ 内，对资产状态信息进行统计，设定资产 $ASSET_w$ 的所有状态信息为 $STATE_{t0}, STATE_1, STATE_2, \ldots, STATE_t, STATE_{t1}$。

[0034] 计算资产 $ASSET_w$ 的单位时间流量；

[0035] 资产的单位时间流量就是某时间段内总流量的平均值；

[0036] 处理器平均使用率就是某时间段内所有采集的处理器使用率的算术平均值；

[0037] 内存平均占用率就是某时间段内所有采集的内存占用率的算术平均值；

[0038] 基于资产 $ASSET_w$ 的有效入侵信息、病毒信息、状态信息，计算资产 $ASSET_w$ 的安全态势值；

[0039] 资产的安全态势值通过对流量、处理器平均使用率、内存平均占用率、有效入侵的严重等级、病毒严重等级的数学计算得到。

[0040] 步骤 8：基于各资产在子网中的权重，采用权重分析法，进行各子网安全态势评估；

[0041] 采用权重分析法，计算网络设备类资产 $ASSET_k$ 的子网综合安全态势值；

[0042] 网络设备类资产的子网综合安全态势值就是该子网内所有资产的安全态势值的

加权和。

[0043] 步骤 9 :基于各子网在整个网络中的权重,采用权重分析法,进行网络安全态势评估 ;

[0044] 采用权重分析法,计算综合网络安全态势值 ;

[0045] 综合网络安全态势值就是所有子网的综合安全态势值的加权和。

[0046] 前述的安全事件信息分为防火墙日志信息、入侵信息、病毒信息、漏洞信息 ;防火墙日志信息 FW 包含 :源地址、目的地址、源端口、目的端口、协议、处理方式 ;入侵信息 IDS 包含 :目的地址、入侵类型、入侵针对的漏洞、入侵严重等级 ;病毒信息 VIRUS 包含 :资产地址、病毒类型、病毒严重等级 ;漏洞信息 VUL 包含 :资产地址、漏洞类型、漏洞严重等级。

[0047] 前述的网络拓扑信息包括 :资产标识、资产连接关系。

[0048] 前述的资产基本信息 ASSET 包括 :资产标识、资产类型、资产值、子网总资产值 ;资产基本信息分为两类 :终端类和网络设备类,终端类资产的子网总资产值为 0,网络设备类资产的子网总资产值为该网络设备子网内所有资产的资产值总和。

[0049] 前述的资产状态信息包括 :资产标识、时间、总流量、处理器使用率、内存占用率。

[0050] 本发明一种网络安全态势评估方法,与现有技术相比,具有以下明显的优势和有益效果 :

[0051] 本发明一种网络安全态势评估方法,改变了现有技术中数据源单一的 :问题,使网络安全态势评估结果更加全面,客观的反映了网络安全整体状况 ;评估结果精确,真实反映网络安全整体状况 ;评估结果直观实用,可以直接用于指导网络安全管理指挥、决策。

附图说明

[0052] 图 1 为本发明网络安全态势评估方法的流程图。

具体实施方式

[0053] 下面结合流程图,对优选实施例作详细说明,应该强调的是,下述说明仅仅是示例性的,而不是为了限制本发明的范围及其应用。

[0054] 步骤 1 :对原始数据进行预处理,消除重复信息和错误信息,生成格式化的安全事件信息、网络拓扑信息、资产基本信息和资产状态信息。

[0055] 用于网络安全态势评估的数据来源包括防火墙、入侵检测系统、防病毒软件、漏洞扫描系统、拓扑发现工具、性能采集工具等。经过去冗余、消除错误信息,再进行格式化,形成安全事件信息、网络拓扑信息、资产基本信息和资产状态信息。

[0056] 安全事件信息主要分为防火墙日志信息、入侵信息、病毒信息、漏洞信息。防火墙日志信息 FW 主要包含 :源地址、目的地址、源端口、目的端口、协议、处理方式 ;入侵信息 IDS 主要包含 :目的地址、入侵类型、入侵针对的漏洞、入侵严重等级 ;病毒信息 VIRUS 主要包含 :资产地址、病毒类型、病毒严重等级 ;漏洞信息 VUL 主要包含 :资产地址、漏洞类型、漏洞严重等级。

[0057] 网络拓扑信息主要包含 :资产标识、资产连接关系。

[0058] 资产基本信息 ASSET 主要包含 :资产标识、资产类型、资产值、子网总资产值。资产基本信息主要分为两类 :终端类和网络设备类,终端类资产的子网总资产值为 0,网络设备

类资产的子网总资产值为该网络设备子网内所有资产（包括终端类和网络设备类）的资产值总和。

[0059] 资产状态信息 STATE 主要包含：资产标识、时间、总流量、处理器使用率、内存占用率。

[0060] 步骤 2：基于网络拓扑信息、资产基本信息，计算各资产在子网中的权重和各子网在整个网络中的权重。

[0061] 设定网络中有 n 个网络设备类资产 $ASSET_1$，$ASSET_2$，...，$ASSET_n$，每个网络设备类资产与其连接的终端类资产构成一个子网，根据网络拓扑信息，设定有 m 个终端类资产与网络设备类资产 $ASSET_k$（$1 \leqslant k \leqslant n$）相连接：$ASSET_{k1}$，$ASSET_{k2}$，...，$ASSET_{km}$。

[0062] 计算网络设备类资产 $ASSET_k$ 的子网总资产值：

[0063] $$TOTAL\_VALUE_k = VALUE_k + \sum_{i=1}^{m} VALUE_{ki}$$（网络设备类资产的子网总资产值就是该子网内所有资产的资产值之和）

[0064] 其中，$TOTAL\_VALUE_k$ 为网络设备类资产 $ASSET_k$ 的子网总资产值，$VALUE_k$ 为网络设备类资产 $ASSET_k$ 的资产值，$\sum_{i=1}^{m} VALUE_{ki}$ 为与网络设备类资产 $ASSET_k$ 相连接的 m 个终端类资产的资产值之和，$1 \leqslant k \leqslant n$。

[0065] 在计算权重时，为突出资产值高的资产的重要性，设定权值为资产值的平方。

[0066] 计算终端类资产 $ASSET_{kf}$ 在网络设备类资产 $ASSET_k$ 的子网中的权重：

[0067] $$P_{kf} = \frac{VALUE_{kf}^{\ 2}}{VALUE_k^{\ 2} + \sum_{i=1}^{m} VALUE_{ki}^{\ 2}}$$（终端类资产的权重就是该资产的权值在子网的总权值中所占的比重）

[0068] 其中，P_{kf} 为终端类资产 $ASSET_{kf}$ 在网络设备类资产 $ASSET_k$ 的子网中的权重，$VALUE_{kf}^{\ 2}$ 为终端类资产 $ASSET_{kf}$ 的权值，$VALUE_k^{\ 2} + \sum_{i=1}^{m} VALUE_{ki}^{\ 2}$ 为网络设备类资产 $ASSET_k$ 的子网中所有资产的权值和，$1 \leqslant k \leqslant n$，$1 \leqslant f \leqslant m$。

[0069] 计算网络设备类资产 $ASSET_k$ 在其子网中的权重：

[0070] $$P_k = \frac{VALUE_k^{\ 2}}{VALUE_k^{\ 2} + \sum_{i=1}^{m} VALUE_{ki}^{\ 2}}$$（网络设备类资产的权重就是该资产的权值在子网的总权值中所占的比重）

[0071] 其中，P_k 为网络设备类资产 $ASSET_k$ 在其子网中的权重，$VALUE_k^{\ 2}$ 为网络设备类资产 $ASSET_k$ 的权值，$VALUE_k^{\ 2} + \sum_{i=1}^{m} VALUE_{ki}^{\ 2}$ 为网络设备类资产 $ASSET_k$ 的子网中所有资产的权值和，$1 \leqslant k \leqslant n$。

[0072] 计算网络设备类资产 $ASSET_k$ 的子网在整个网络中的权重

[0073] $$T\_P_k = \frac{TOTAL\_VALUE_k^{\ 2}}{\sum_{i=1}^{n} TOTAL\_VALUE_i^{\ 2}}$$（子网的权值就是子网的权值在整个网络的总权值

中所占的比重）

[0074] 其中，T_P_k 为网络设备类资产 $ASSET_k$ 的子网在整个网络中的权重，$TOTAL\_VALUE_k^2$ 为网络设备类资产 $ASSET_k$ 的子网的权值，$\sum_{i=1}^{n} TOTAL\_VALUE_i^2$ 为整个网络中所有子网的权值和，$1 \leqslant k \leqslant n$。

[0075] 步骤 3：基于入侵信息，对各资产进行外部威胁态势评估；基于病毒信息、漏洞信息，对各资产进行内部威胁态势评估。

[0076] 在时间段 $[t_0, t_1]$ 内，无论入侵是否成功，对入侵信息进行统计，设定针对资产 $ASSET_w$ 的所有入侵信息为 $IDS_1, IDS_2, \ldots, IDS_p$。

[0077] 计算资产 $ASSET_w$ 的外部威胁态势值

[0078] $$ATT_w = \sqrt[3]{\sum_{i=1}^{p} IDS\_LEV_i^3}$$（资产的外部威胁态势由资产外部的因素决定，主要为入侵，资产的外部威胁态势值通过对所有入侵的严重等级的数学计算得到）

[0079] 其中，ATT_w 为资产 $ASSET_w$ 的外部威胁态势值，IDS_LEV_i 为入侵信息 IDS_i 的入侵严重等级。

[0080] 在时间段 $[t_0, t_1]$ 内，对病毒信息进行统计，设定资产 $ASSET_w$ 感染的所有病毒信息 $VIRUS_1, VIRUS_2, \ldots, VIRUS_q$。

[0081] 在时间段 $[t_0, t_1]$ 内，对漏洞信息进行统计，设定资产 $ASSET_w$ 的所有漏洞信息 $VUL_1, VUL_2, \ldots, VUL_r$。

[0082] 计算资产 $ASSET_w$ 的内部威胁态势值

[0083] $$DEF_w = \sqrt[3]{\sum_{i=1}^{q} VIRUS\_LEV_i^3} + \sqrt[3]{\sum_{i=1}^{p} VUL\_LEV_i^3}$$（资产的内部威胁态势由资产内部的因素决定，主要包含病毒和漏洞，资产的内部威胁态势值通过对资产的所有病毒和漏洞的严重等级的数学计算得到）

[0084] 其中，DEF_w 为资产 $ASSET_w$ 的内部威胁态势值，$VIRUS\_LEV_i$ 为病毒信息 $VIRUS_i$ 的病毒严重等级，VUL_LEV_i 为漏洞信息 VUL_i 的漏洞严重等级。

[0085] 步骤 4：基于各资产在子网中的权重，采用权重分析法，进行各子网外部威胁态势评估和内部威胁态势评估。

[0086] 采用权重分析法，计算网络设备类资产 $ASSET_k$ 的子网外部威胁态势值和内部威胁态势值

[0087] $$ATT\_SA_k = P_k \times ATT_k + \sum_{i=1}^{m} \left(P_{ki} \times ATT_{ki}\right)$$（网络设备类资产的子网外部威胁态势值就是该子网内所有资产的外部威胁态势值的加权和）

[0088] $$DEF\_SA_k = P_k \times DEF_k + \sum_{i=1}^{m} \left(P_{ki} \times DEF_{ki}\right)$$（网络设备类资产的子网内部威胁态势值就是该子网内所有资产的内部威胁态势值的加权和）

[0089] 其中，ATT_SA_k 为网络设备类资产 $ASSET_k$ 的子网外部威胁态势值，DEF_SA_k 为网络设备类资产 $ASSET_k$ 的子网内部威胁态势值，P_k 为网络设备类资产 $ASSET_k$ 在其子网中的权重，P_{ki} 为终端类资产 $ASSET_{ki}$ 在网络设备类资产 $ASSET_k$ 的子网中的权重，ATT_k 为网络设备

类资产 $ASSET_k$ 的外部威胁态势值，DEF_k 为网络设备类资产 $ASSET_k$ 的内部威胁态势值，ATT_{ki} 为终端类资产 $ASSET_{ki}$ 的外部威胁态势值，DEF_{ki} 为终端类资产 $ASSET_{ki}$ 的内部威胁态势值，$1 \leqslant k \leqslant n$。

[0090] 步骤 5：基于各子网在整个网络中的权重，采用权重分析法，进行网络外部威胁态势评估和内部威胁态势评估；

[0091] 采用权重分析法，计算网络外部威胁态势值和内部威胁态势值

[0092] $TOTAL\_ATT = \sum_{i=1}^{n}(T\_P_i \times ATT\_SA_i)$（网络外部威胁态势值就是所有子网的外部威胁态势值的加权和）

[0093] $TOTAL\_DEF = \sum_{i=1}^{n}(T\_P_i \times DEF\_SA_i)$（网络内部威胁态势值就是所有子网的内部威胁态势值的加权和）

[0094] 其中，TOTAL_ATT 为网络外部威胁态势值，TOTAL_DEF 为网络内部威胁态势值，T_P_i 为网络设备类资产 $ASSET_i$ 的子网在整个网络中的权重，ATT_SA_i 为网络设备类资产 $ASSET_i$ 的子网外部威胁态势值，DEF_SA_i 为网络设备类资产 $ASSET_i$ 的子网内部威胁态势值。

[0095] 步骤 6：对防火墙日志信息、入侵信息和漏洞信息进行交叉关联，消除无效告警。

[0096] 针对资产 $ASSET_w$ 的入侵信息，若资产 $ASSET_w$ 上不存在入侵针对的漏洞，则该入侵无效，不会对网络安全产生危害，最终筛选得到针对资产 $ASSET_w$ 的所有有效入侵信息 IDS_1，IDS_2，...，IDS_s。

[0097] 步骤 7：基于交叉关联后的各类信息，综合评估各资产的安全态势。

[0098] 在时间段 $[t_0, t_1]$ 内，对资产状态信息进行统计，设定资产 $ASSET_w$ 的所有状态信息为 $STATEt_0$，$STATE_1$，$STATE_2$，...，$STATE_t$，$STATE_{t1}$。

[0099] 计算资产 $ASSET_w$ 的单位时间流量

[0100] $PER_w = \frac{FLEX_{t1} - FLEX_{t0}}{t_1 - t_0}$（资产的单位时间流量就是某时间段内总流量的平均值）

[0101] 其中，PER_w 为时间段 $[t_0, t_1]$ 内资产 $ASSET_w$ 单位时间流量，$FLEX_{t1}$-$FLEX_{t0}$ 为时间段 $[t_0, t_1]$ 内资产 $ASSET_w$ 的总流量，t_1-t_0 为时间段 $[t_0, t_1]$ 内的总时间。

[0102] 处理器平均使用率

[0103] $CPU\_AVG_w = \frac{CPU_{t0} + \sum_{i=1}^{t} CPU_i + CPU_{t1}}{t+2}$（处理器平均使用率就是某时间段内所有采集的处理器使用率的算术平均值）

[0104] 其中，CPU_AVG_w 为时间段 $[t_0, t_1]$ 内处理器平均使用率，$CPU_{t0} + \sum_{i=1}^{t} CPU_i + CPU_{t1}$ 为时间段 $[t_0, t_1]$ 内采集的所有资产状态信息的处理器使用率之和，t+2 为采集的资产状态信息总数，$0 \leqslant CPU_i \leqslant 1$。

[0105] 内存平均占用率

[0106] $$PF\_AVG_w = \frac{PF_{t0} + \sum_{i=1}^{t} PF_i + PF_{t1}}{t+2}$$（内存平均占用率就是某时间段内所有采集的内存占用率的算术平均值）

[0107] 其中，PF_AVG_w 为时间段 $[t_0, t_1]$ 内内存平均占用率，$PF_{t0} + \sum_{i=1}^{t} PF_i + PF_{t1}$ 为时间段 $[t_0, t_1]$ 内采集的所有资产状态信息的内存占用率之和，t+2 为采集的资产状态信息总数，$0 \leqslant PF_i \leqslant 1$。

[0108] 基于资产 $ASSET_w$ 的有效入侵信息、病毒信息、状态信息，计算资产 $ASSET_w$ 的安全态势值

[0109]

$$SEC_w = \sqrt{\frac{\left(\frac{PER_w}{PER_{w\_\max}}\right)^2 + CPU\_AVG_w^{\,2} + PF\_AVG_w^{\,2}}{3}} \times \left(\sqrt[3]{\sum_{i=1}^{s} IDS\_LEV_i^3} + \sqrt[3]{\sum_{i=1}^{q} VIRUS\_LEV_i^3} \right)$$

[0110] （资产的安全态势值通过对流量、处理器平均使用率、内存平均占用率、有效入侵的严重等级、病毒严重等级的数学计算得到）

[0111] 其中 PER_{w_max} 为资产 $ASSET_w$ 单位时间最大流量，IDS_LEV_i 为入侵信息 IDS_i 的入侵严重等级，$VIRUS\_LEV_i$ 为病毒信息 $VIRUS_i$ 的病毒严重等级。

[0112] 步骤 8：基于各资产在子网中的权重，采用权重分析法，进行各子网安全态势评估；

[0113] 采用权重分析法，计算网络设备类资产 $ASSET_k$ 的子网综合安全态势值

[0114] $$SEC\_SA_k = P_k \times SEC_k + \sum_{i=1}^{m} \left(P_{ki} \times SEC_{ki} \right)$$（网络设备类资产的子网综合安全态势值就是该子网内所有资产的安全态势值的加权和）

[0115] 其中，SEC_SA_k 为网络设备类资产 $ASSET_k$ 的子网综合安全态势值，P_k 为网络设备类资产 $ASSET_k$ 在其子网中的权重，P_{ki} 为终端类资产 $ASSET_{ki}$ 在网络设备类资产 $ASSET_k$ 的子网中的权重，SEC_k 为网络设备类资产 $ASSET_k$ 的安全态势值，SEC_{ki} 为终端类资产 $ASSET_{ki}$ 的安全态势值，$1 \leqslant k \leqslant n$。

[0116] 步骤 9：基于各子网在整个网络中的权重，采用权重分析法，进行网络安全态势评估。

[0117] 采用权重分析法，计算综合网络安全态势值

[0118] $$TOTAL\_SEC = \sum_{i=1}^{n} \left(T\_P_i \times SEC\_SA_i \right)$$（综合网络安全态势值就是所有子网的综合安全态势值的加权和）

[0119] 其中，TOTAL_SEC 为综合网络安全态势值，T_P_i 为网络设备类资产 $ASSET_i$ 的子网在整个网络中的权重，SEC_SA_i 为网络设备类资产 $ASSET_i$ 的子网综合安全态势值。

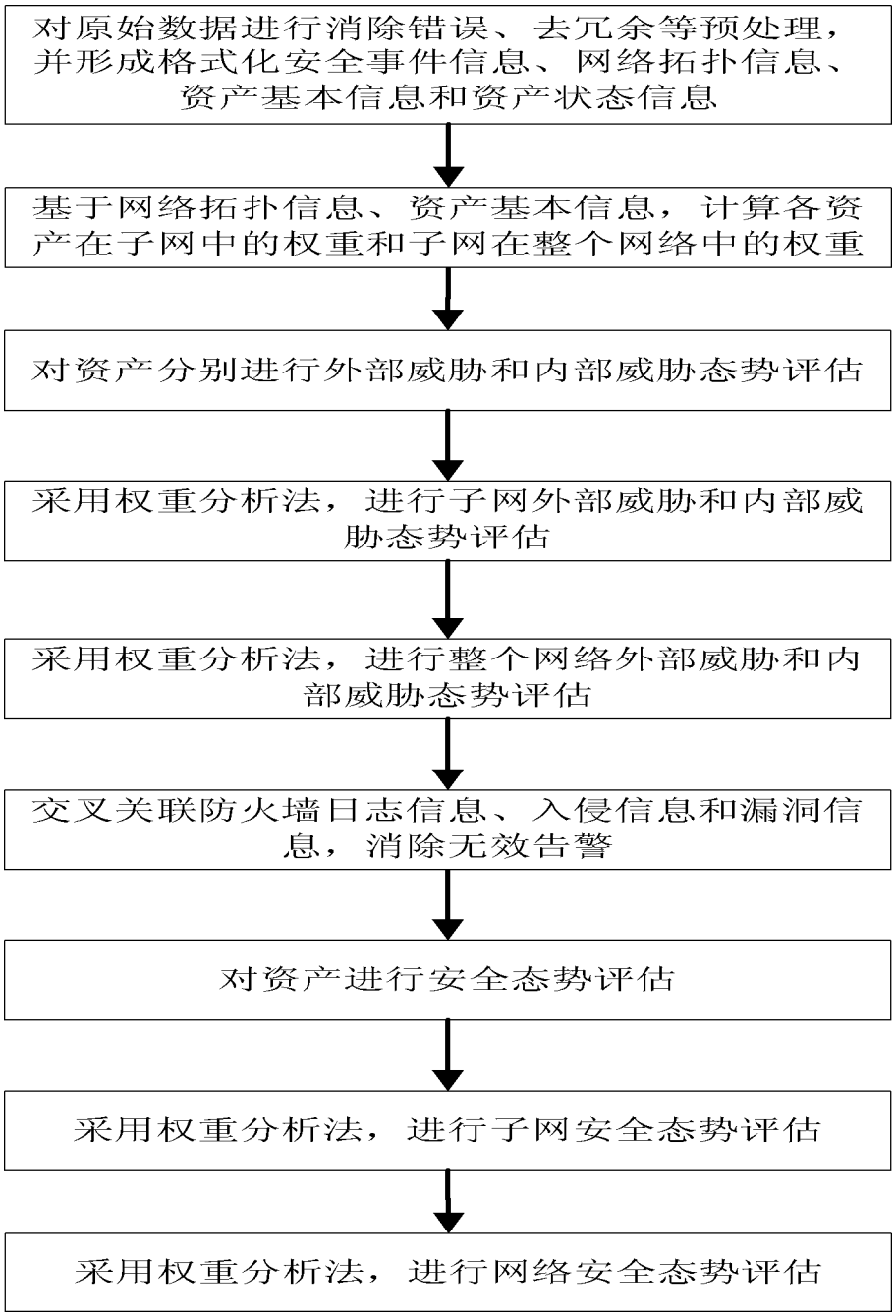

对原始数据进行消除错误、去冗余等预处理，并形成格式化安全事件信息、网络拓扑信息、资产基本信息和资产状态信息
基于网络拓扑信息、资产基本信息，计算各资产在子网中的权重和子网在整个网络中的权重
对资产分别进行外部威胁和内部威胁态势评估
采用权重分析法，进行子网外部威胁和内部威胁态势评估
采用权重分析法，进行整个网络外部威胁和内部威胁态势评估
交叉关联防火墙日志信息、入侵信息和漏洞信息，消除无效告警
对资产进行安全态势评估
采用权重分析法，进行子网安全态势评估
采用权重分析法，进行网络安全态势评估

图 1