(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102340485 A
(43)申请公布日 2012.02.01

(21)申请号 201010233950.0

(22)申请日 2010.07.19

(71)申请人 中国科学院计算技术研究所
地址 100080 北京市海淀区中关村科学院南路 6 号

(72)发明人 席荣荣 金舒原 吴进 董昭

(74)专利代理机构 北京律诚同业知识产权代理有限公司 11006
代理人 祁建国 梁挥

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

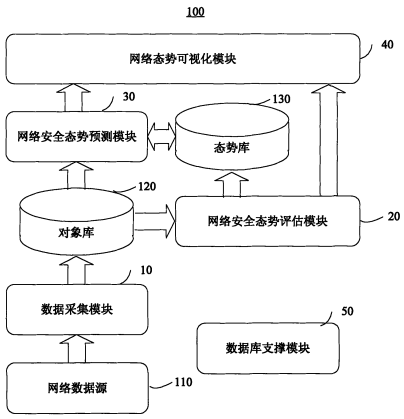
权利要求书 4 页 说明书 11 页 附图 5 页

(54)发明名称

基于信息关联的网络安全态势感知系统及其方法

(57)摘要

本发明有关于一种基于信息关联的网络安全态势感知系统及其方法，其中该系统包括：数据采集模块，用于获取网络基本信息；网络安全态势评估模块，用于利用网络基本信息，对网络的威胁性、脆弱性和稳定性进行量化分析，进而实现对当前的网络安全态势的分析；网络安全态势预测模块，用于根据网络安全态势的历史信息和当前状态对网络安全态势进行预测；网络态势可视化模块，用于根据网络安全态势的分析和预测结果，对网络安全指标进行可视化展现。本发明克服了现有的网络态势感知系统缺乏数据有效性验证，数据关联和定量分析的问题，从而使得网络安全态势感知更为准确。



CN 102340485 A

1. 一种基于信息关联的网络安全态势感知系统，其特征在于，包括：

数据采集模块，用于从网络中获取网络基本信息；

网络安全态势评估模块，连接所述数据采集模块，用于利用所述网络基本信息，对网络的威胁性、脆弱性和稳定性进行量化分析，进而实现对当前的网络安全态势的分析；

网络安全态势预测模块，连接所述数据采集模块、所述网络安全态势评估模块，用于根据所述网络安全态势的历史信息和当前状态对网络安全态势进行预测；

网络态势可视化模块，连接所述网络安全态势评估模块、所述网络安全态势预测模块，用于根据网络安全态势的分析和预测结果，对网络安全指标进行可视化展现。

2. 根据权利要求 1 所述的基于信息关联的网络安全态势感知系统，其特征在于，还包括：

数据库支撑模块，连接所述数据采集模块、所述网络安全态势评估模块、所述网络安全态势预测模块、所述网络态势可视化模块，用于设置数据库存储所述网络基本信息、进行网络安全态势分析和预测所需的数据信息、进行网络态势可视化显示所需的数据信息。

3. 根据权利要求 1 或 2 所述的基于信息关联的网络安全态势感知系统，其特征在于，

所述数据采集模块又包括：

入侵检测模块，用于获取用于感知威胁态势的信息；

主动扫描模块，用于获取网络基本信息和脆弱性信息；

流量监测模块，用于获取描述网络稳定性的网络流量信息。

4. 根据权利要求 3 所述的基于信息关联的网络安全态势感知系统，其特征在于，

所述网络安全态势评估模块又包括：

威胁性态势评估模块，连接所述入侵检测模块，用于将所述入侵检测模块产生的警报信息与所述脆弱性信息、网络拓扑信息进行数据关联，得到网络的威胁性态势；

脆弱性态势评估模块，连接所述主动扫描模块，用于将所述脆弱性信息与 CVSS 相关联，获取网络的脆弱性态势；

稳定性态势评估模块，连接所述流量监测模块，用于基于流量的变化获取网络的稳定性态势；

网络安全态势整体评估模块，连接所述威胁态势评估模块、所述脆弱性态势评估模块、所述稳定性态势评估模块，用于根据所述威胁性态势、所述脆弱性态势、所述稳定性态势，获取网络的整体安全态势值。

5. 根据权利要求 4 所述的基于信息关联的网络安全态势感知系统，其特征在于，

所述威胁性态势评估模块又包括：

标准化模块，用于将所述警报信息转化为统一的格式；

预处理模块，连接所述标准化模块，用于对具有相同源、目的和攻击类型的警报进行合并；

警报验证模块，连接所述预处理模块，用于通过判定攻击可能成功的概率，获取警报的完成度；

影响分析模块，连接所述预处理模块，用于量化评估每条警报的严重程度；

威胁识别模块，连接所述警报验证模块、所述影响分析模块，用于根据警报的完成度和严重程度，获取网络的威胁性态势。

6. 根据权利要求 5 所述的基于信息关联的网络安全态势感知系统，其特征在于，

所述威胁识别模块以如下公式获取用于评价网络的威胁性态势的网络威胁性指数：

$$TI = \frac{1}{n}\sum_{i=1}^{n}(C_i \times S_i)$$

其中：

TI 为网络的威胁性指数，n 表示单位时间内警报的数目，C_i 表示每条警报的完成度，S_i 表示每条警报的严重程度。

7. 根据权利要求 6 所述的基于信息关联的网络安全态势感知系统，其特征在于，

所述脆弱性态势评估模块以如下公式获取用于评价网络的脆弱性态势的网络脆弱性指数：

$$VI = \frac{1}{n}\sum_{i=1}^{n} v_i . CVSS$$

其中：

VI 为网络的脆弱性指数，n 表示网络中漏洞的数目，v_i。CVSS 表示每条漏洞在 CVSS 中的分值。

8. 根据权利要求 7 所述的基于信息关联的网络安全态势感知系统，其特征在于，

所述稳定性态势评估模块以如下公式获取用于评价网络的稳定性态势的流量的方差：

$$E = \frac{1}{n}\sum_{i=0}^{n} x_i$$

$$SI = \frac{1}{n}\sum_{i=0}^{n}(x_i - E)^2$$

其中：

SI 为网络的稳定性指数，由流量的方差表示，n 表示单位时间内流量的记录数，x_i 表示每条流量记录的输入和输出流量之和，E 表示单位时间内流量的期望值。

9. 根据权利要求 8 所述的基于信息关联的网络安全态势感知系统，其特征在于，

所述网络安全态势整体评估模块以如下公式获取网络的整体安全态势值：

$$ST = \alpha_1 TI + \alpha_2 SI + \alpha_3 VI$$

其中：

ST 为网络的整体安全态势值，α_1 表示威胁性指数在网络的整体安全态势中所占的比重，α_2 表示稳定性指数在网络的整体安全态势中所占的比重，α_3 表示脆弱性指数在网络的整体安全态势中所占的比重。

10. 根据权利要求 1、2、4-9 中任一所述的基于信息关联的网络安全态势感知系统，其特征在于，

所述网络安全态势预测模块以如下公式对网络安全态势进行预测：

$$P(S_j|S_i) = \frac{P(S_j|S_i)P(S_i)}{\sum_{j=0}^{n} P(S_i|S_j)P(S_j)}$$

其中：

n 表示网络安全状态的数目，S_i 表示网络处于的安全状态 i，$P(S_i)$ 表示网络处于 S_i 的概率，S_j 表示网络处于的安全状态 j，$P(S_j\ S_i)$ 表示网络在 τ-1 时刻出于 S_i，在 τ 时刻处于 S_j 的概率，$P(S_j|S_i)$ 表示网络在 τ 时刻处于 S_j，在 τ+1 时刻处于 S_j 的概率。

11. 一种基于信息关联的网络安全态势感知方法，其特征在于，包括：

步骤 A，从网络中获取网络基本信息；

步骤 B，利用所述网络基本信息，对网络的威胁性，脆弱性和稳定性进行量化分析，进而实现对当前的网络安全态势的分析；

步骤 C，根据所述网络安全态势的历史信息和当前状态对网络安全态势进行预测；

步骤 D，根据网络安全态势的分析和预测结果，对网络安全指标进行可视化展现。

12. 根据权利要求 11 所述的基于信息关联的网络安全态势感知方法，其特征在于，还包括：

步骤 E，设置数据库存储所述网络基本信息、进行网络安全态势分析和预测所需的数据信息、进行网络态势可视化显示所需的数据信息。

13. 根据权利要求 11 或 12 所述的基于信息关联的网络安全态势感知方法，其特征在于，所述 A 步骤进一步包括：

A1、获取用于感知威胁态势的信息；

A2、获取网络基本信息和脆弱性信息；

A3、获取描述网络稳定性的网络流量信息。

14. 根据权利要求 13 所述的基于信息关联的网络安全态势感知方法，其特征在于，所述 B 步骤进一步包括：

B1、将所述入侵检测模块产生的警报信息与所述脆弱性信息、网络拓扑信息进行数据关联，得到网络的威胁性态势；

B2、将所述脆弱性信息与 CVSS 相关联，获取网络的脆弱性态势；

B3、基于流量的变化获取网络的稳定性态势；

B4、根据所述威胁性态势、所述脆弱性态势、所述稳定性态势，获取网络的整体安全态势值。

15. 根据权利要求 14 所述的基于信息关联的网络安全态势感知方法，其特征在于，

所述 B1 步骤进一步包括：

B11、将所述警报信息转化为统一的格式；

B12、对具有相同源、目的和攻击类型的警报进行合并；

B13、通过判定攻击可能成功的概率，获取攻击的完成度；

B14、量化评估每条警报的严重程度；

B15、根据警报的完成度和严重程度，获取网络的威胁性态势。

16. 根据权利要求 15 所述的基于信息关联的网络安全态势感知方法，其特征在于，

所述 B15 步骤进一步包括：以如下公式获取用于评价网络的威胁性态势的网络威胁性指数：

$$TI = \frac{1}{n}\sum_{i=1}^{n}(C_i \times S_i)$$

其中：

TI 为网络的威胁性指数，n 代表单位时间内警报的数目，C_i 表示每条警报的完成度，S_i 表示每条警报的严重程度。

17. 根据权利要求 16 所述的基于信息关联的网络安全态势感知方法，其特征在于，

所述 B2 步骤进一步包括：以如下公式获取用于评价网络的脆弱性态势的网络脆弱性指数：

$$VI= \frac{1}{n}\sum_{i=1}^{n} v_i . CVSS$$

其中：

VI 为网络的脆弱性指数，n 表示网络中漏洞的数目，v_i。CVSS 表示每条漏洞在 CVSS 中的分值。

18. 根据权利要求 17 所述的基于信息关联的网络安全态势感知方法，其特征在于，

所述 B3 步骤进一步包括：以如下公式获取用于评价网络的稳定性态势的流量的方差：

$$E = \frac{1}{n}\sum_{i=0}^{n} x_i$$

$$SI = \frac{1}{n}\sum_{i=0}^{n}(x_i - E)^2$$

其中：

SI 为网络的稳定性指数，由流量的方差表示，n 表示单位时间内流量的记录数，x_i 表示每条流量记录的输入和输出流量之和，E 表示单位时间内流量的期望值。

19. 根据权利要求 18 所述的基于信息关联的网络安全态势感知方法，其特征在于，

所述 B4 步骤进一步包括：以如下公式获取网络的整体安全态势值：

$$ST = \alpha_1 TI + \alpha_2 SI + \alpha_3 VI$$

其中：

ST 为网络的整体安全态势值，α_1 表示威胁性指数在网络的整体安全态势中所占的比重，α_2 表示稳定性指数在网络的整体安全态势中所占的比重，α_3 表示脆弱性指数在网络的整体安全态势中所占的比重。

20. 根据权利要求 11、12、14-19 中任一所述的基于信息关联的网络安全态势感知方法，其特征在于，

所述 C 步骤进一步包括：以如下公式对网络安全态势进行预测：

$$P(S_j|S_i) = \frac{P(S_j|S_i)P(S_i)}{\sum_{j=0}^{n} P(S_i|S_j)P(S_j)}$$

其中：

n 表示网络安全状态的数目，S_i 表示网络处于的安全状态 i，$P(S_i)$ 表示网络处于 S_i 的概率，S_j 表示网络处于的安全状态 j，$P(S_j\ S_i)$ 表示网络在 $\tau-1$ 时刻出于 S_i，在 τ 时刻处于 S_j 的概率，$P(S_j|S_i)$ 表示网络在 τ 时刻处于 S_j，在 $\tau+1$ 时刻处于 S_j 的概率。

基于信息关联的网络安全态势感知系统及其方法

技术领域

[0001] 本发明涉及信息安全领域，尤涉及一种基于信息关联的网络安全态势感知系统及其方法。

背景技术

[0002] 目前有很多科研机构正在进行网络态势感知工具的研发，并取得了一定的进展。CERT NetSA(Network Situational Awareness Team) 开发的 SiLK 是一款流量分析工具。它可以在大规模网络中进行安全分析，支持高效的网络流数据的收集、存储和分析，使得网络安全分析员可以从大量历史数据集中快速查询相关信息，根据查询结果对网络安全态势进行评估。Silk 由收集系统和分析系统两部分构成。收集系统负责接收 Netflow，并且将其转化为更合理的格式，将这些包存入特定服务的二进制文件中；分析系统负责读取文件、执行各种查询操作，过滤，统计相关信息。

[0003] NCASSR(National Center for Advanced Secure System Research) 开发的 NVisionIP 和 NFlowConnect-IP 侧重于研究网络安全态势的可视化。NVisionIP 和 NFlowConnect-IP 分别从网络流量信息和网络连接信息的角度对网络安全态势进行感知，并在一个屏幕中显示整个网络的安全态势。NVisionIP 主要是对网络流量信息进行数据挖掘，从网络流量信息的角度对网络的态势进行感知，它利用路由等设备提供的流量信息，依据相关攻击的流量特性，对网络的攻击态势从流量的角度进行分析，并进行可视化展示。NFlowConnect-IP 主要从网络连接的角度对网络态势进行感知，它利用网络中主机的连接情况，结合相关攻击的连接特性，对网络的攻击态势从连接的角度进行分析。并进行可视化展示。

[0004] Sourcefire 公司开发的 3D System 是进行高效的网络安全管理的智能化基础设施。其中的 3D Sensor 负责监测和收集各种网络信息，并对网络信息进行控制管理的网络态势感知工具。3D Sensor 由 IPS、RNA、RUA 和 Netflow Analysis 四部分组成。IPS(Intrusion Detection System，入侵检测系统）提供入侵检测和保护，RNA(Real-time Network Awareness，实时网络识别）监测和收集网络信息；RUA(Real-time User Awareness，实时用户识别）监测和收集网络用户信息；Netflow Analysis（流量分析）收集并监测网络流量信息。

[0005] 信息安全国家重点实验室开发的信息系统安全态势评估工具，是一套采集与处理信息系统多源数据，并进行安全态势分析与预测的综合性工具。该工具以信息系统的资产信息、脆弱性信息和威胁信息三方面为基础，通过网络拓扑自动发现技术、脆弱性扫描技术和多源日志采集与分析技术获取相应信息，实现辅助型信息资产的安全审核、安全管理制度的执行检查以及面向海量日志的安全事件分析，最后综合分析信息系统安全态势并进行预测。

[0006] 西安交通大学的陈秀真等提出的层次化网络安全威胁态势量化评估方法，在报警发生频率、报警严重性及其网络带宽耗用率的统计基础上，对服务、主机本身的重要性因子

进行加权，层次化计算服务、主机以及整个网络系统的威胁指数，进而分析网络的安全态势。该方法侧重于从服务、主机和网络受到威胁的角度层次化的评估网络的安全态势。

[0007] 西安电子科技大学的李伟生等根据网络安全态势和安全事件之间的不同的关联性建立态势评估的贝叶斯网络模型，并给出相应的信息传播算法，以安全事件的发生为触发点，根据相应的信息传播算法评估网络的安全态势，该方法从以安全事件为代表的网络威胁的角度评估网络的安全态势。

[0008] 哈尔滨工程大学的王惠强等将多种理论与态势感知相结合，提出了多种态势感知模型。基于简单加权法和灰色理论的网络态势感知模型，利用简单加权法评估网络态势的安全性，并利用灰色理论预测网络安全的发展趋势。基于粗糙集的态势感知算法，将网络攻击行为作为安全要素，利用粗糙集理论处理海量网络安全数据，并且通过具有攻击行为、网络服务和安全态势三个层次的感知模型进行网络态势感知。基于 Netfolw 的安全态势感知系统，通过 NetFlow 流数据采集器进行数据采集，并且在此基础上进行数据预处理、事件关联与目标识别、态势评估、威胁评估、响应与预警、态势可视化显示等操作，从而对网络的安全态势进行监控和应急响应。

[0009] 综上所述，现有的网络安全态势感知系统存在以下不足 ：

[0010] 1) 缺乏数据有效性的验证

[0011] 从网络中直接采集的数据可能是由网络安全设备误报产生的，对这样的数据进行加工取得的结果，准确性值得商讨。

[0012] 2) 缺乏数据关联

[0013] 现有的网络安全态势感知系统倾向于获取多源数据信息，但缺乏对数据信息之间关联性的分析。

[0014] 3) 缺乏定量分析

[0015] 目前网络安全评估一般都采用定性的或者等级分类的方式描述网络的安全状态，缺乏更为准确的，与国际标准一致的定量分析。

发明内容

[0016] 本发明的一目的在于提供一种基于信息关联的网络安全态势感知系统及其方法，用于克服现有的网络态势感知系统缺乏数据有效性验证，数据关联和定量分析的问题，从而使得网络安全态势感知更为准确。

[0017] 为了实现上述目的，本发明提供一种基于信息关联的网络安全态势感知系统，其特征在于，包括 ：

[0018] 数据采集模块，用于从网络中获取网络基本信息 ；

[0019] 网络安全态势评估模块，连接所述数据采集模块，用于利用所述网络基本信息，对网络的威胁性、脆弱性和稳定性进行量化分析，进而实现对当前的网络安全态势的分析 ；

[0020] 网络安全态势预测模块，连接所述数据采集模块、所述网络安全态势评估模块，用于根据所述网络安全态势的历史信息和当前状态对网络安全态势进行预测 ；

[0021] 网络态势可视化模块，连接所述网络安全态势评估模块、所述网络安全态势预测模块，用于根据网络安全态势的分析和预测结果，对网络安全指标进行可视化展现。

[0022] 所述的基于信息关联的网络安全态势感知系统，其中，还包括 ：

[0023] 数据库支撑模块，连接所述数据采集模块、所述网络安全态势评估模块、所述网络安全态势预测模块、所述网络态势可视化模块，用于设置数据库存储所述网络基本信息、进行网络安全态势分析和预测所需的数据信息、进行网络态势可视化显示所需的数据信息。

[0024] 所述的基于信息关联的网络安全态势感知系统，其中，

[0025] 所述数据采集模块又包括：

[0026] 入侵检测模块，用于获取用于感知威胁态势的信息；

[0027] 主动扫描模块，用于获取网络基本信息和脆弱性信息；

[0028] 流量监测模块，用于获取描述网络稳定性的网络流量信息。

[0029] 所述的基于信息关联的网络安全态势感知系统，其中，

[0030] 所述网络安全态势评估模块又包括：

[0031] 威胁性态势评估模块，连接所述入侵检测模块，用于将所述入侵检测模块产生的警报信息与所述脆弱性信息、网络拓扑信息进行数据关联，得到网络的威胁性态势；

[0032] 脆弱性态势评估模块，连接所述主动扫描模块，用于将所述脆弱性信息与 CVSS 相关联，获取网络的脆弱性态势；

[0033] 稳定性态势评估模块，连接所述流量监测模块，用于基于流量的变化获取网络的稳定性态势；

[0034] 网络安全态势整体评估模块，连接所述威胁态势评估模块、所述脆弱性态势评估模块、所述稳定性态势评估模块，用于根据所述威胁性态势、所述脆弱性态势、所述稳定性态势，获取网络的整体安全态势值。

[0035] 所述的基于信息关联的网络安全态势感知系统，其中，

[0036] 所述威胁性态势评估模块又包括：

[0037] 标准化模块，用于将所述警报信息转化为统一的格式；

[0038] 预处理模块，连接所述标准化模块，用于对具有相同源、目的和攻击类型的警报进行合并；

[0039] 警报验证模块，连接所述预处理模块，用于通过判定攻击可能成功的概率，获取警报的完成度；

[0040] 影响分析模块，连接所述预处理模块，用于量化评估每条警报的严重程度；

[0041] 威胁识别模块，连接所述警报验证模块、所述影响分析模块，用于根据警报的完成度和严重程度，获取网络的威胁性态势。

[0042] 所述的基于信息关联的网络安全态势感知系统，其中，

[0043] 所述威胁识别模块以如下公式获取用于评价网络的威胁性态势的网络威胁性指数：

[0044] $$TI = \frac{1}{n}\sum_{i=1}^{n}(C_i \times S_i)$$

[0045] 其中：

[0046] TI 为网络的威胁性指数，n 表示单位时间内警报的数目，C_i 表示每条警报的完成度，S_i 表示每条警报的严重程度。

[0047] 所述的基于信息关联的网络安全态势感知系统，其中，

[0048] 所述脆弱性态势评估模块以如下公式获取用于评价网络的脆弱性态势的网络脆弱性指数：

[0049] $$VI=\frac{1}{n}\sum_{i=1}^{n}v_i.CVSS$$

[0050] 其中：

[0051] VI 为网络的脆弱性指数，n 表示网络中漏洞的数目，v_i。CVSS 表示每条漏洞在 CVSS 中的分值。

[0052] 所述的基于信息关联的网络安全态势感知系统，其中，

[0053] 所述稳定性态势评估模块以如下公式获取用于评价网络的稳定性态势的流量的方差：

[0054] $$E=\frac{1}{n}\sum_{i=0}^{n}x_i$$

[0055] $$SI=\frac{1}{n}\sum_{i=0}^{n}(x_i-E)^2$$

[0056] 其中：

[0057] SI 为网络的稳定性指数，由流量的方差表示，n 表示单位时间内流量的记录数，x_i 表示每条流量记录的输入和输出流量之和，E 表示单位时间内流量的期望值。

[0058] 所述的基于信息关联的网络安全态势感知系统，其中，

[0059] 所述网络安全态势整体评估模块以如下公式获取网络的整体安全态势值：

[0060] $ST = \alpha_1 TI + \alpha_2 SI + \alpha_3 VI$

[0061] 其中：

[0062] ST 为网络的整体安全态势值，α_1 表示威胁性指数在网络的整体安全态势中所占的比重，α_2 表示稳定性指数在网络的整体安全态势中所占的比重，α_3 表示脆弱性指数在网络的整体安全态势中所占的比重。

[0063] 所述的基于信息关联的网络安全态势感知系统，其中，

[0064] 所述网络安全态势预测模块以如下公式对网络安全态势进行预测：

[0065] $$P(S_j|S_i)=\frac{P(SjSi)P(Si)}{\sum_{j=0}^{n}P(Si|Sj)P(Sj)}$$

[0066] 其中：

[0067] n 表示网络安全状态的数目，S_i 表示网络处于的安全状态 i，$P(S_i)$ 表示网络处于 S_i 的概率，S_j 表示网络处于的安全状态 j，$P(S_j\ S_i)$ 表示网络在 τ-1 时刻出于 S_i，在 τ 时刻处于 S_j 的概率，$P(S_j|S_i)$ 表示网络在 τ 时刻处于 S_j，在 τ+1 时刻处于 S_j 的概率。

[0068] 为了实现上述目的，本发明提供一种基于信息关联的网络安全态势感知方法，其特征在于，包括：

[0069] 步骤 A，从网络中获取网络基本信息；

[0070] 步骤 B，利用所述网络基本信息，对网络的威胁性，脆弱性和稳定性进行量化分析，进而实现对当前的网络安全态势的分析；

[0071] 步骤 C，根据所述网络安全态势的历史信息和当前状态对网络安全态势进行预测；

[0072] 步骤 D，根据网络安全态势的分析和预测结果，对网络安全指标进行可视化展现。

[0073] 所述的基于信息关联的网络安全态势感知方法，其中，还包括：

[0074] 步骤 E，设置数据库存储所述网络基本信息、进行网络安全态势分析和预测所需的数据信息、进行网络态势可视化显示所需的数据信息。

[0075] 所述的基于信息关联的网络安全态势感知方法，其中，所述 A 步骤进一步包括：

[0076] A1、获取用于感知威胁态势的信息；

[0077] A2、获取网络基本信息和脆弱性信息；

[0078] A3、获取描述网络稳定性的网络流量信息。

[0079] 所述的基于信息关联的网络安全态势感知方法，其中，所述 B 步骤进一步包括：

[0080] B1、将所述入侵检测模块产生的警报信息与所述脆弱性信息、网络拓扑信息进行数据关联，得到网络的威胁性态势；

[0081] B2、将所述脆弱性信息与 CVSS 相关联，获取网络的脆弱性态势；

[0082] B3、基于流量的变化获取网络的稳定性态势；

[0083] B4、根据所述威胁性态势、所述脆弱性态势、所述稳定性态势，获取网络的整体安全态势值。

[0084] 所述的基于信息关联的网络安全态势感知方法，其中，

[0085] 所述 B1 步骤进一步包括：

[0086] B11、将所述警报信息转化为统一的格式；

[0087] B12、对具有相同源、目的和攻击类型的警报进行合并；

[0088] B13、通过判定攻击可能成功的概率，获取攻击的完成度；

[0089] B14、量化评估每条警报的严重程度；

[0090] B15、根据警报的完成度和严重程度，获取网络的威胁性态势。

[0091] 所述的基于信息关联的网络安全态势感知方法，其中，

[0092] 所述 B15 步骤进一步包括：以如下公式获取用于评价网络的威胁性态势的网络威胁性指数：

[0093] $$TI = \frac{1}{n}\sum_{i=1}^{n}(C_i \times S_i)$$

[0094] 其中：

[0095] TI 为网络的威胁性指数，n 代表单位时间内警报的数目，C_i 表示每条警报的完成度，S_i 表示每条警报的严重程度。

[0096] 所述的基于信息关联的网络安全态势感知方法，其中，

[0097] 所述 B2 步骤进一步包括：以如下公式获取用于评价网络的脆弱性态势的网络脆弱性指数：

[0098] $$VI = \frac{1}{n}\sum_{i=1}^{n} v_i \cdot CVSS$$

[0099] 其中：

[0100] VI 为网络的脆弱性指数，n 表示网络中漏洞的数目，v_i。CVSS 表示每条漏洞在 CVSS 中的分值。

[0101] 所述的基于信息关联的网络安全态势感知方法，其中，

[0102] 所述 B3 步骤进一步包括：以如下公式获取用于评价网络的稳定性态势的流量的方差：

[0103] $$E = \frac{1}{n}\sum_{i=0}^{n} x_i$$

[0104] $$SI = \frac{1}{n}\sum_{i=0}^{n}(x_i - E)^2$$

[0105] 其中：

[0106] SI 为网络的稳定性指数，由流量的方差表示，n 表示单位时间内流量的记录数，x_i 表示每条流量记录的输入和输出流量之和，E 表示单位时间内流量的期望值。

[0107] 所述的基于信息关联的网络安全态势感知方法，其中，

[0108] 所述 B4 步骤进一步包括：以如下公式获取网络的整体安全态势值：

[0109] $ST = \alpha_1 TI + \alpha_2 SI + \alpha_3 VI$

[0110] 其中：

[0111] ST 为网络的整体安全态势值，α_1 表示威胁性指数在网络的整体安全态势中所占的比重，α_2 表示稳定性指数在网络的整体安全态势中所占的比重，α_3 表示脆弱性指数在网络的整体安全态势中所占的比重。

[0112] 所述的基于信息关联的网络安全态势感知方法，其中，

[0113] 所述 C 步骤进一步包括：以如下公式对网络安全态势进行预测：

[0114] $$P(S_j|S_i) = \frac{P(S_j S_i)P(S_i)}{\sum_{j=0}^{n} P(S_i|S_j)P(S_j)}$$

[0115] 其中：

[0116] n 表示网络安全状态的数目，S_i 表示网络处于的安全状态 i，$P(S_i)$ 表示网络处于 S_i 的概率，S_j 表示网络处于的安全状态 j，$P(S_j\ S_i)$ 表示网络在 $\tau-1$ 时刻出于 S_i，在 τ 时刻处于 S_j 的概率，$P(S_j|S_i)$ 表示网络在 τ 时刻处于 S_j，在 $\tau+1$ 时刻处于 S_j 的概率。

[0117] 本发明与现有的网络安全态势感知系统相比，具有以下优点：

[0118] 1) 本发明通过警报验证提高数据的有效性，主要来判定攻击成功的概率，即攻击的完成度；对于不可能成功的攻击直接过滤，从而提高数据信息的有效性；

[0119] 2) 本发明的警报验证模块和影响分析模块都涉及到数据的关联，警报验证通过匹配攻击的需求信息与网络的基本配置信息，实现了网络威胁性信息与网络拓扑信息的关联，影响分析模块通过警报的 CVE-id(Common Vulnerabilites and Exposure-id，通用脆弱性标识符）实现了威胁性信息和脆弱性信息的关联，从而很好的实现了网络中各种数据信息的关联分析；

[0120] 3) 本发明依据 CVSS(Common Vulnerability Scoring System，通用弱点评价体系）量化评估每条警报以及每个漏洞的严重程度，另外通过流量的方差来描述网络的稳定性，从而实现了采用与国际评分标准一致的方法定量分析网络的安全态势。

附图说明

[0121] 图 1 是本发明基于信息关联的网络安全态势感知系统结构图；

[0122] 图 2 是本发明数据采集模块与网络安全态势评估模块的结构图；

[0123] 图 3 是本发明基于信息关联的网络安全态势感知方法流程图；

[0124] 图 4 是本发明网络脆弱性的柱状图展示；

[0125] 图 5 是本发明网络脆弱性的饼状图展示；

[0126] 图 6 是本发明网络威胁性的曲线图展示；

[0127] 图 7 是本发明网络流量的曲线图展示；

[0128] 图 8 是本发明网络整体安全状态的柱状图展示；

[0129] 图 9 是本发明网络安全状态预测值与真实值曲线比较展示。

具体实施方式

[0130] 以下结合附图和具体实施例对本发明进行详细描述，但不作为对本发明的限定。

[0131] 如图 1 所示，是本发明基于信息关联的网络安全态势感知系统结构图，图 2 是本发明数据采集模块与网络安全态势评估模块的结构图。

[0132] 该系统 100 包括如下模块：

[0133] 数据采集模块 10，用于从网络（即网络数据源 110）中获取网络基本信息，通过拓扑自发现技术获取网络的拓扑信息；通过主动扫描和被动嗅探相结合的方式获取网络的脆弱性信息、状态信息和运行信息等基本的网络安全信息；通过对各种防护措施日志的采集和分析技术来获取威胁信息等。

[0134] 网络安全态势评估模块 20，连接数据采集模块 10，用于利用获取的网络基本信息，对网络的威胁性、脆弱性和稳定性分别进行量化分析，进而实现对当前的网络安全态势的分析。

[0135] 网络安全态势预测模块 30，连接网络安全态势评估模块 20，用于根据网络安全态势的历史信息和当前状态对网络安全态势（网络未来一段时间的发展趋势）进行预测。

[0136] 网络态势可视化模块 40，连接网络安全态势评估模块 20、网络安全态势预测模块 30，用于根据网络安全态势的分析和预测结果，以多种展现方式（直方图、饼图等）、多角度（威胁的种类、漏洞的类型、流量的变化等）对网络安全指标进行可视化展现。实时反映被监控网络运行状况的态势系统，让网络管理员能直观，快捷的获得网络运行信息，发现网络恶意行为，采取有效措施。

[0137] 在图 4 中，网络态势可视化模块 40 是以柱状图形式展示网络的脆弱性；在图 5 中，网络态势可视化模块 40 是以饼状图形式展示网络的脆弱性；在图 6 中，网络态势可视化模块 40 是以曲线图形式展示网络的威胁性；在图 7 中，网络态势可视化模块 40 是以曲线图形式展示网络的流量；在图 8 中，网络态势可视化模块 40 是以柱状图形式展示网络整体安全状态；在图 9 中，网络态势可视化模块 40 是以网络安全状态预测值与真实值曲线对比进行展示。

[0138] 数据库支撑模块 50，连接数据采集模块 10、网络安全态势评估模块 20、网络安全态势预测模块 30、网络态势可视化模块 40，用于设计合理的数据库，以用于网络基本信息的存储，为态势分析，预测和可视化子系统提供分析和显示的数据信息。

[0139] 其中，数据采集模块 10 根据获取信息的不同，又可以进一步分为：

[0140] 入侵检测模块 11，用于获取用于感知威胁态势的信息；

[0141] 主动扫描模块 12，用于获取网络基本信息和脆弱性信息；

[0142] 流量监测模块 13，用于获取描述网络稳定性的流量信息。

[0143] 其中，网络安全态势评估模块 20 从不同的角度，可以进一步分为：

[0144] 威胁性态势评估模块 21，用于将入侵检测模块 11 产生的警报信息与脆弱性信息，网络拓扑信息进行数据关联，得到网络的威胁性态势；

[0145] 脆弱性态势评估模块 22，用于将主动扫描模块 12 产生的脆弱性信息与 CVSS 相关联，获取网络的脆弱性态势；

[0146] 稳定性态势评估模块 23，用于利用流量监测模块 13 获取网络流量信息，并基于流量的变化获取网络的稳定性态势。

[0147] 网络安全态势整体评估模块 24，连接威胁态势评估模块 21、脆弱性态势评估模块 22、稳定性态势评估模块 23，用于根据上述模块从三个角度进行评估得到的评估结果，获取网络的整体安全态势值。

[0148] 其中，威胁态势评估模块 21 根据数据处理的流程，可以进一步分为 ：

[0149] 标准化模块 211，用于将入侵检测模块 11 产生的警报信息，结合 IDMEF 格式，转化为统一的格式，使得各模块之间便于交互 ；

[0150] 预处理模块 212，连接标准化模块 211，用于对具有相同源、目的和攻击类型的警报进行合并，从而减少警报的数量，提高性能 ；

[0151] 警报验证模块 213，连接预处理模块 212，用于通过匹配攻击的需求信息与网络的基本配置信息，判定攻击可能成功的概率，获取攻击的完成度 ；

[0152] 影响分析模块 214，连接预处理模块 212，用于依据 CVSS，量化评估每条警报的严重程度 ；

[0153] 威胁识别模块 215，连接警报验证模块 213、影响分析模块 214，用于根据警报的完成度和严重程度，获取网络的威胁性态势。

[0154] 其中，数据库支撑模块 50 设置的数据库包括对象库 120、态势库 130。对象库 120 用于存储网络基本信息，态势库 130 用于存储为态势分析、预测提供分析和显示的数据信息 ；对象库 120 和态势库 130 同时为可视化子系统提供分析和显示的数据信息。

[0155] 如图 3 所示，是本发明基于信息关联的网络安全态势感知方法流程图。结合图 1、2，对基于信息关联的网络安全态势感知方法进行描述，该方法包括以下步骤 ：

[0156] 步骤 A ：数据采集，从网络中获取网络基本信息，威胁性信息，脆弱性信息以及流量信息。通过拓扑自发现技术获取网络的拓扑信息 ；通过主动扫描和被动嗅探相结合的方式获取网络的脆弱性信息、状态信息和运行信息等基本的网络安全信息 ；通过入侵检测模块 11 产生警报信息来获取威胁性信息 ；通过流量监测模块 13 获取描述网络稳定性的流量信息。

[0157] 其中，步骤 A 根据获取信息的不同，又可以进一步分为 ：

[0158] A1，获取脆弱性信息的入侵检测步骤 ；

[0159] A2，获取脆弱性信息和网络基本信息的主动扫描步骤 ；

[0160] A3，获取流量信息的流量监测步骤。

[0161] A1-A3 各步骤获取的数据内容格式如下 ：

[0162] 威胁性信息表 ：警报 ID，检测时间，警报名，警报类型，警报严重程度，协议，源主机，目的主机，源端口，目的端口 ；

[0163] 脆弱性信息 ：漏洞 ID，扫描时间，CVE-ID，主机 IP，端口，安全类型，风险级别 ；

[0164] 主机信息表 ：主机 ID，主机名，主机状态，开放端口，端口状态，服务，协议，主机 IP，操作系统，扫描时间 ；

[0165] 路由信息表 ：表项 ID，源主机 IP，目的主机 IP，距离，路由路径 ；

[0166] 流量信息表 ：流量 ID，开始时间，运行时间，输入数据包，输出数据包，输入字节数，输出字节数，Tcp 数据包，Udp 数据包，Icmp 数据包，其他 IP 数据包，非 IP 数据包，广播

数据包；

[0167] 步骤 B：网络态势评估，利用数据采集模块 10 获取的网络基本信息，对网络的威胁性，脆弱性和稳定性分别进行量化分析，进而实现对当前的网络安全态势的分析。具体包括：

[0168] B1，威胁性态势评估步骤；

[0169] B2，脆弱性态势评估步骤；

[0170] B3，稳定性态势评估步骤；以及

[0171] B4，网络安全态势整体评估步骤。

[0172] 其中步骤 B1：威胁性态势评估步骤，是以入侵检测模块 11 产生的警报信息作为原始数据信息，经过一系列处理获取网络的威胁性指数。该步骤又可以进一步分为：

[0173] B11，标准化；

[0174] B12，预处理；

[0175] B13，警报验证；

[0176] B14，影响分析；以及

[0177] B15，威胁识别。

[0178] 步骤 B11：参考 IDMEF 中 Impact Class 的格式，将原始数据信息转化为统一的格式，使得各模块之间便于交互信息。标准化处理之后的威胁信息数据格式如下：

[0179] 警报信息表：检测时间，警报名称，源 IP，源端口，目的 IP，目的端口，分类，完成度，严重度。

[0180] 其中，前六项由原始信息拷贝获取，分类通过匹配 Snort 规则库获取，完成度由警报验证模块 213 获取，严重度由影响分析模块 214 获取。

[0181] 步骤 B12：对具有相同源，目的和攻击类型的警报进行合并，从而减少警报的数量，提高性能。

[0182] 步骤 B13：判定攻击可能成功的概率。通过匹配攻击的需求信息与网络的基本配置信息完成。根据网络配置信息的获取方式可以分为被动验证和主动验证。警报验证模块 213 采用被动验证和主动验证相结合的方式获取网络配置信息。警报验证模块 213 利用主动扫描模块 12 获取网络基本信息作为配置信息的基本数据库，当警报验证模块 213 接收到某个警报时，首先在基本数据库中进行匹配，根据匹配结果判定攻击可能成功的概率；若在基本数据库中没有警报对应的网络基本信息，则利用主动验证的方式判定攻击可能成功的概率，过程如下：首先从警报中提取对应的 CVE-ID，根据 CVE-ID 查找相应的 NASL 脚本并执行，然后根据脚本的返回值判定攻击成功的概率。对于没有相应的 NASL 脚本的警报，其成功概率赋值为不可判定。通过警报验证可以确定每条警报的完成度，其参考值为成功 100％，不成功 0％，不可判定 50％。

[0183] 步骤 B14：判定警报对网络所造成的影响。处理过程如下：首先从警报中提取对应的 CVE-ID，然后根据 CVE-ID 在 CVSS 中获取相应的分值，利用该值来表示警报的影响程度。对于没有对应 CVE-ID 的警报信息，根据警报分类查找缺省值。缺省值通过计算某类警报信息的 CVSS 分值的平均值获取。通过影响分析可以确定警报的严重度，其参考值范围为 0.0-10.0.

[0184] 步骤 B15：获取网络的威胁性指数。

[0185] 安全事件的影响＝安全事件成功的概率 X 安全事件的严重程度

[0186] 其中，成功的概率由警报验证过程获取，严重程度由影响分析过程获取。这样就可以获取一个量化的网络威胁性指数，用于评价网络的威胁性态势，威胁识别模块 215 利用下面公式实现网络威胁性指数的获取：

[0187] $$TI = \frac{1}{n}\sum_{i=1}^{n}(C_i \times S_i)$$

[0188] 其中：

[0189] TI 为网络的威胁性指数，n 代表单位时间内警报的数目，C_i 表示每条警报的完成度，即警报所代表攻击的成功概率，S_i 表示每条警报的严重程度。

[0190] 步骤 B2：脆弱性态势评估，脆弱性态势评估模块 22 依据 CVSS 对网络的脆弱性信息进行定量分析，从而获取每个脆弱性信息的量化值，进而获取网络脆弱性指数的量化值，网络脆弱性指数用于评价网络的脆弱性态势，公式如下：

[0191] $$VI = \frac{1}{n}\sum_{i=1}^{n} v_i.CVSS$$

[0192] 其中：

[0193] VI 为网络的脆弱性指数，n 表示网络中脆弱性（即漏洞）的数目，v_i.CVSS 表示每条漏洞在 CVSS 中的分值。

[0194] 步骤 B3：稳定性态势评估，方差可以描述事物的变化情况，稳定性态势评估模块 23 利用流量的方差来刻画 / 评价网络的稳定性态势，并且对其进行量化，公式如下：

[0195] $$E = \frac{1}{n}\sum_{i=0}^{n} x_i$$

[0196] $$SI = \frac{1}{n}\sum_{i=0}^{n}(x_i - E)^2$$

[0197] 其中：

[0198] SI 为网络的稳定性指数，由流量的方差表示，n 表示单位时间内流量的记录数，x_i 表示每条流量记录的输入和输出流量之和，E 表示单位时间内流量的期望值。

[0199] 步骤 B4：网络安全态势整体评估，由网络安全态势整体评估模块 24 利用前面三个角度对网络安全性的评估，获取整体的网络安全态势量化值，具体操作如下：

[0200] $ST = \alpha_1 TI + \alpha_2 SI + \alpha_3 VI$

[0201] 其中：

[0202] ST 是网络安全态势量化值，α_1 表示威胁性指数在网络的整体安全态势中所占的比重，即威胁性指数的权值，α_2 表示稳定性指数在网络的整体安全态势中所占的比重，即稳定性指数的权值，α_3 表示脆弱性指数在网络的整体安全态势中所占的比重，即脆弱性指数的权值。

[0203] 步骤 C：对网络的安全态势进行预测，网络安全态势预测模块 30 采用贝叶斯推理过程，即

[0204] $$P(S_j|S_i) = \frac{P(S_j|S_i)P(S_i)}{\sum_{j=0}^{n} P(S_i|S_j)P(S_j)}$$

[0205] 其中：

[0206] n 表示网络安全状态的数目，S_i 表示网络处于的安全状态 i，$P(S_i)$ 表示网络处于 S_i 的概率，S_j 表示网络处于的安全状态 j，$P(S_j)$ 表示网络处于 S_j 的概率，$P(S_j\ S_i)$ 表示网络在 $\tau-1$ 时刻处于 S_i，在 τ 时刻处于 S_j 的概率，$P(S_j|S_i)$ 表示网络在 τ 时刻处于 S_j，在

$\tau+1$ 时刻处于 S_j 的概率。

[0207] 将网络的安全态势分为安全，一般，危险和高危险四种状态 Si，公式中的先验概率由自学习方法获取，通过实时统计网络状态信息获取。

[0208] 通过上述步骤可以获取网络的总体安全态势值，并对其发展趋势进行预测。同时该系统提供对原始网络基本信息，威胁性信息，脆弱性信息和流量信息，以及威胁性态势，脆弱性态势和稳定性态势的查询和统计显示功能。

[0209] 本发明提供了一种基于信息关联的网络安全态势感知系统及其方法，克服现有的网络态势感知系统缺乏数据有效性验证，数据关联和定量分析的问题，从而使得网络安全态势感知更为准确。

[0210] 当然，本发明还可有其它多种实施例，在不背离本发明精神及其实质的情况下，熟悉本领域的技术人员当可根据本发明做出各种相应的改变和变形，但这些相应的改变和变形都应属于本发明所附的权利要求的保护范围。

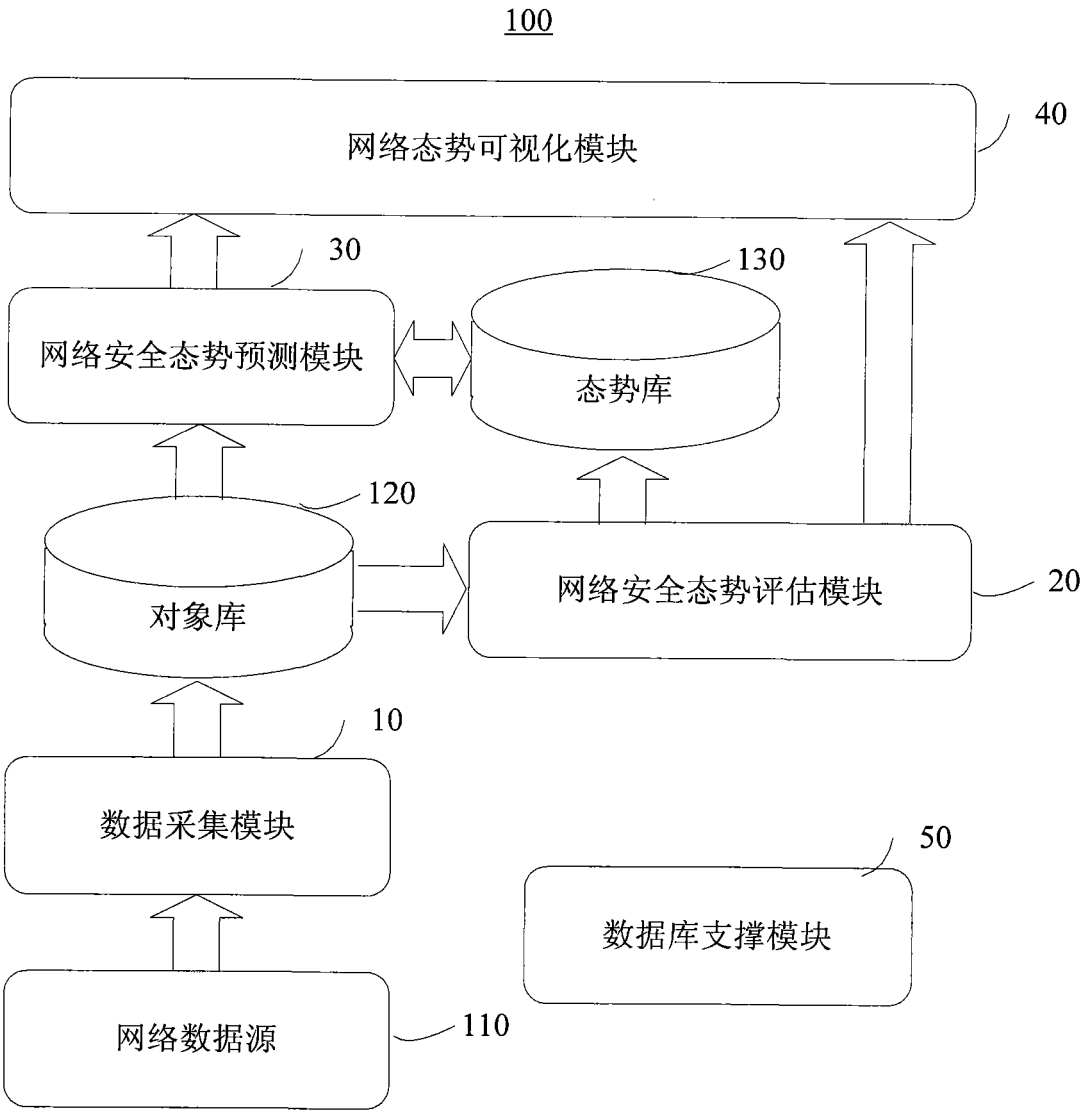

100
网络态势可视化模块
40
30
130
网络安全态势预测模块
态势库
120
对象库
网络安全态势评估模块
20
10
数据采集模块
50
数据库支撑模块
网络数据源
110

图 1

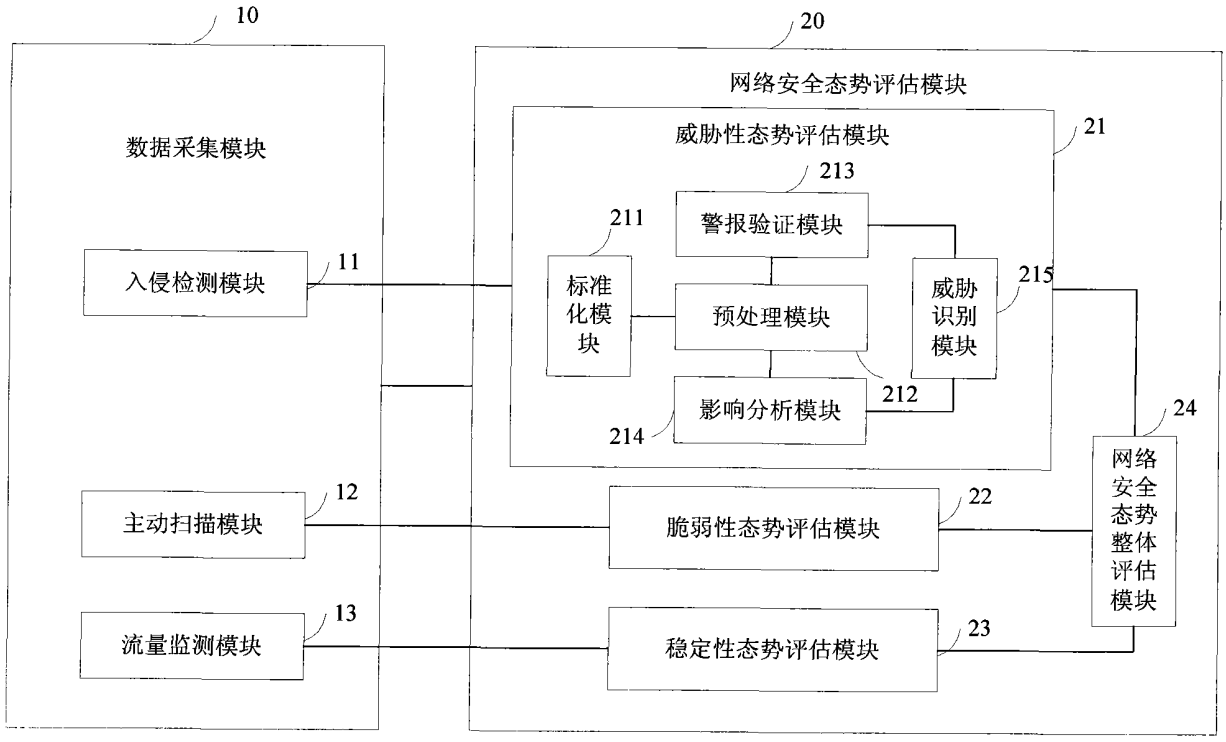

10
数据采集模块
入侵检测模块
11
主动扫描模块
12
流量监测模块
13
20
网络安全态势评估模块
威胁性态势评估模块
21
213
警报验证模块
211
标准化模块
预处理模块
威胁识别模块
215
212
影响分析模块
214
24
网络安全态势整体评估模块
脆弱性态势评估模块
22
稳定性态势评估模块
23

图 2

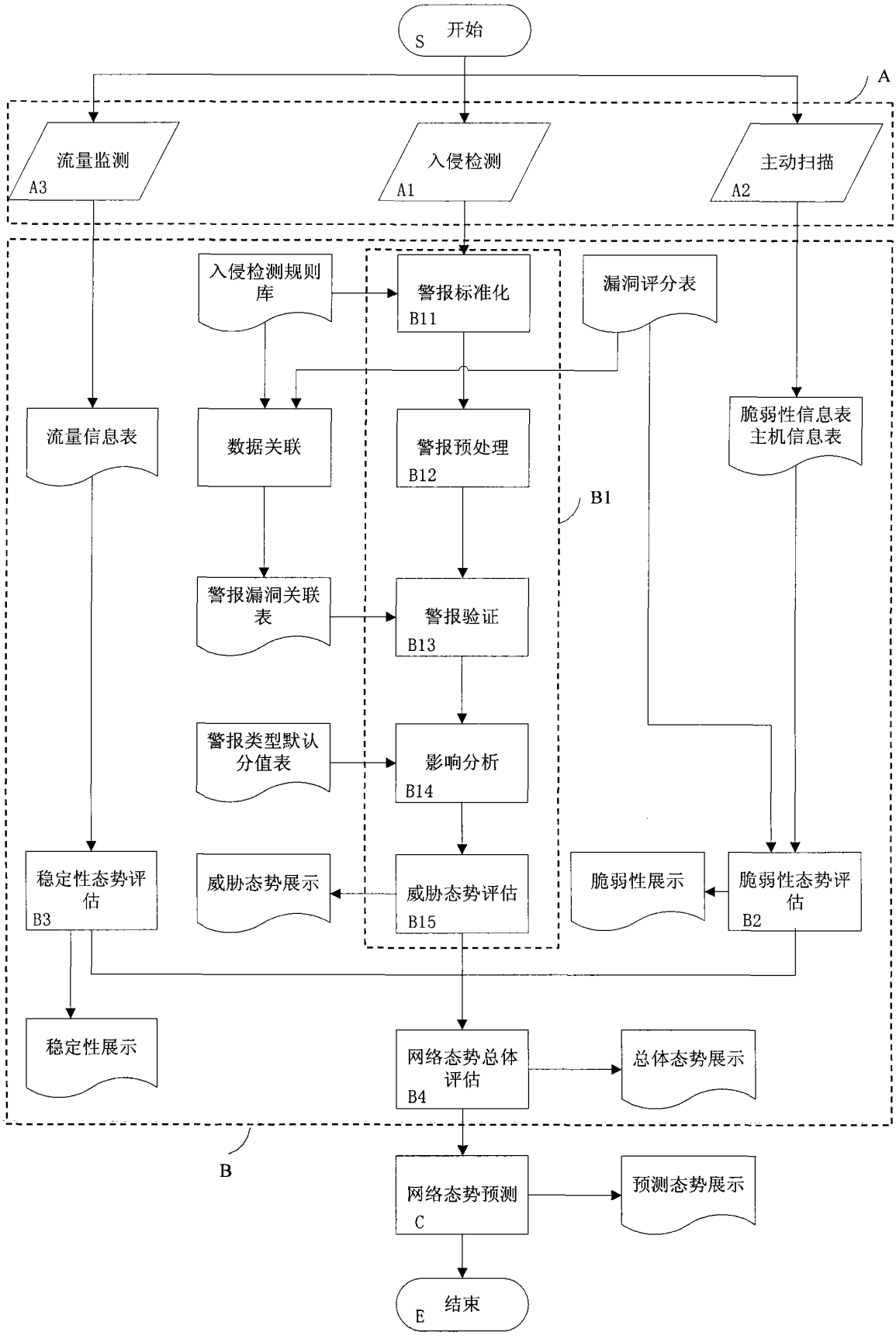

开始
S
A
流量监测
A3
入侵检测
A1
主动扫描
A2
入侵检测规则库
警报标准化
B11
漏洞评分表
流量信息表
数据关联
警报预处理
B12
脆弱性信息表
主机信息表
B1
警报漏洞关联表
警报验证
B13
警报类型默认分值表
影响分析
B14
稳定性态势评估
B3
威胁态势展示
威胁态势评估
B15
脆弱性展示
脆弱性态势评估
B2
稳定性展示
网络态势总体评估
B4
总体态势展示
B
网络态势预测
C
预测态势展示
结束
E

图 3

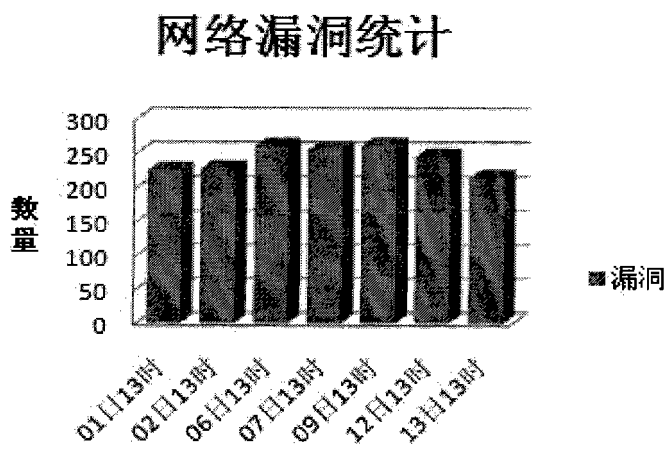

网络漏洞统计
数量
300
250
200
150
100
50
0
01日13时
02日13时
06日13时
07日13时
09日13时
12日13时
13日13时
漏洞

图 4

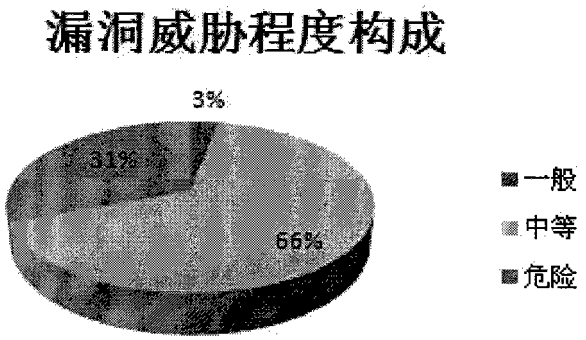

漏洞威胁程度构成
3%
31%
66%
一般
中等
危险

图 5

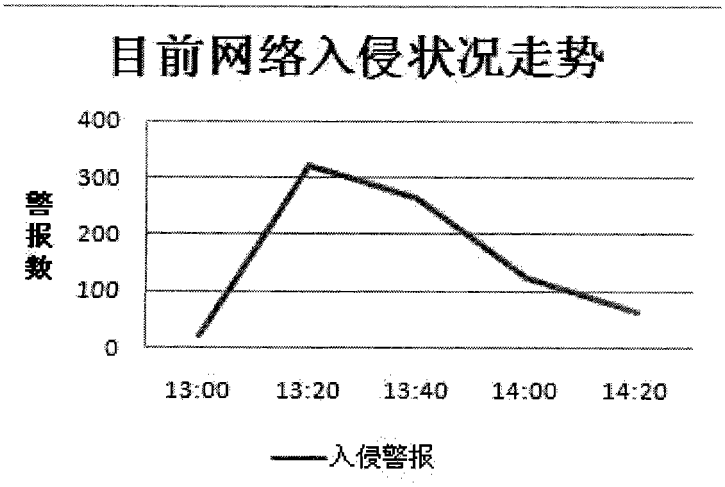

目前网络入侵状况走势
警报数
400
300
200
100
0
13:00
13:20
13:40
14:00
14:20
入侵警报

图 6

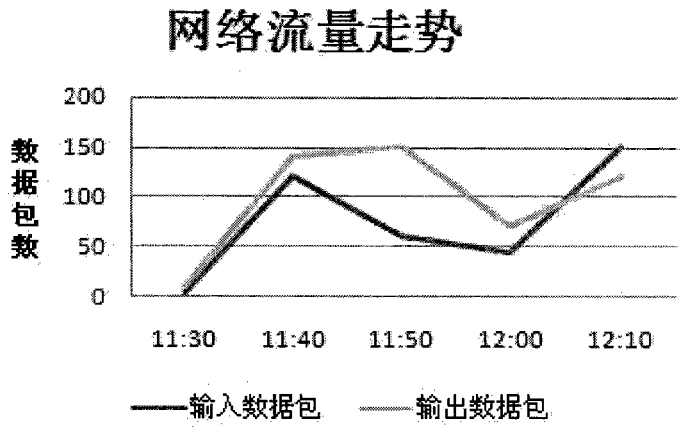

网络流量走势
数据包数
200
150
100
50
0
11:30
11:40
11:50
12:00
12:10
输入数据包
输出数据包

图 7

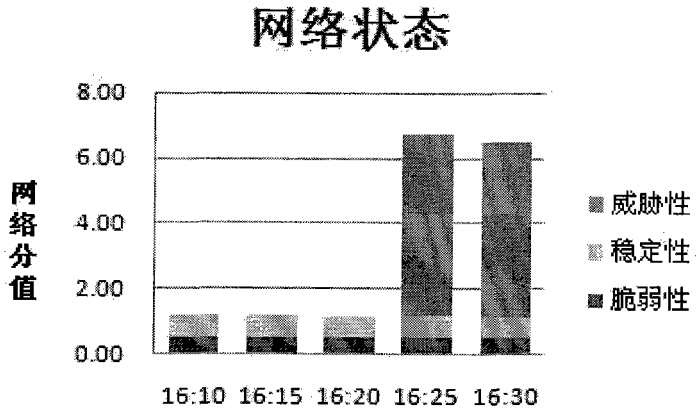

网络状态
网络分值
8.00
6.00
4.00
2.00
0.00
16:10
16:15
16:20
16:25
16:30
威胁性
稳定性
脆弱性

图 8

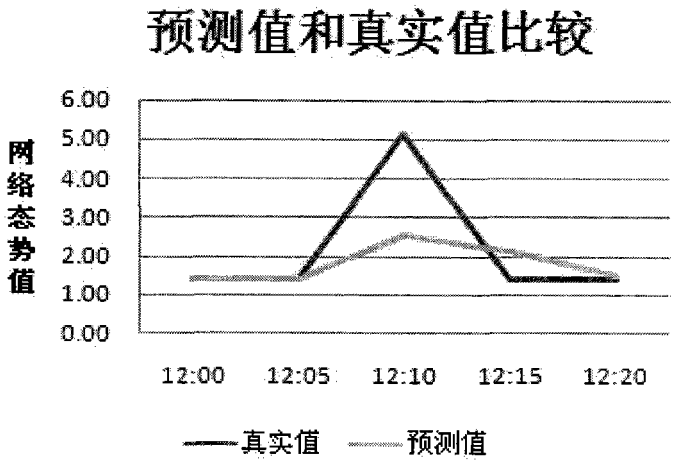

预测值和真实值比较
网络态势值
6.00
5.00
4.00
3.00
2.00
1.00
0.00
12:00
12:05
12:10
12:15
12:20
真实值
预测值

图 9