

NOVEDAD DE LA INVENCION

Habiendo descrito la presente invención, se considera como novedad, y por lo tanto se reclama como propiedad lo contenido en las siguientes:

5

REIVINDICACIONES

1. Un método implementado por computadora, caracterizado porque comprende:

recolectar, por un sistema de computadora, datos de una
10 pluralidad de diferentes tipos de fuentes, en donde los datos recolectados incluyen datos de la red y datos de recurso;

identificar, por el sistema de computadora con base en los datos de la red en los datos recolectados, un evento de tráfico de la red y una pluralidad de recursos de la red
15 relacionados con el evento de tráfico de la red;

identificar, por el sistema de computadora con base en los datos de recurso en los datos recolectados, conexiones entre la pluralidad de recursos de la red;

generar, por el sistema de computadora, una gráfica de
20 información de flujo que representa la pluralidad de recursos de la red y las conexiones entre la pluralidad de recursos de la red, en donde la gráfica de información de flujo representa el tráfico de la red que se permite entre los recursos de la red y el tráfico de la red se bloquea entre

los recursos de la red; y

presentar la gráfica de información de flujo a través de una pantalla de una interfaz de usuario en comunicación con el sistema de computadora.

5 2. El método de conformidad con la reivindicación 0, caracterizado porque los datos recolectados se obtienen de una fuente seleccionada del grupo que consiste de: un enrutador, un conmutador, un servidor de seguridad, un sistema de detección de intrusión, un sistema de protección
10 de intrusión y combinaciones de los mismos.

3. El método de conformidad con la reivindicación 0, caracterizado además porque comprende filtrar la información duplicada de los datos recolectados.

4. El método de conformidad con la reivindicación 0,
15 caracterizado porque uno o más de: una característica de una conexión entre recursos de la red y una característica de un recurso de la red se identifica con base al menos parcialmente en un atributo seleccionado de los datos recolectados.

20 5. El método de conformidad con la reivindicación 0, caracterizado porque el atributo se selecciona por un usuario a través de la interfaz de usuario.

6. El método de conformidad con la reivindicación 0, caracterizado porque el atributo se selecciona

automáticamente por el sistema de computadora.

7. El método de conformidad con la reivindicación 0, caracterizado porque la una o más de las características de una conexión entre los recursos de la red y la característica
5 de un recurso de la red se indica visualmente en la gráfica de información de flujo.

8. El método de conformidad con la reivindicación 0, caracterizado porque la gráfica de información de flujo representa conexiones entre los recursos de la red usando las
10 líneas de flujo direccionales seleccionables.

9. El método de conformidad con la reivindicación 0, caracterizado porque las líneas de flujo indican un tipo de la fuente de los datos recolectados usados para identificar la conexión.

15 10. El método de conformidad con la reivindicación 0, caracterizado además porque comprende:

identificar características de las conexiones entre los recursos de la red; y

en respuesta a la selección, por un usuario a través de
20 la interfaz de usuario, de una línea de flujo respectiva asociada con una conexión de la pluralidad de conexiones, que muestra las características de la conexión seleccionada.

11. El método de conformidad con la reivindicación 0, caracterizado porque la muestra de las características de la

conexión seleccionada incluye mostrar las reglas para permitir y bloquear el tráfico sobre la conexión seleccionada.

12. El método de conformidad con la reivindicación 0,
5 caracterizado además porque comprende:

recibir ediciones, del usuario a través de la interfaz de usuario, a las reglas mostradas para permitir y bloquear el tráfico sobre la conexión seleccionada; y

aplicar las reglas editadas a la conexión seleccionada.

10 13. El método de conformidad con la reivindicación 0, caracterizado porque la generación de la gráfica de información de flujo incluye:

identificar un recurso asociado con un tipo de vulnerabilidad de seguridad; e

15 indicar visualmente el recurso identificado que se asocia con la vulnerabilidad de seguridad en la gráfica de información de flujo.

14. El método de conformidad con la reivindicación 0, caracterizado porque la gráfica de información de flujo
20 representa la información en un recurso y uno o más de: los datos de la red asociados con el recurso, y un atributo operacional del sistema asociado con el recurso.

15. El método de conformidad con la reivindicación 0, caracterizado además porque comprende:

recolectar los datos actualizados;
actualizar la gráfica de información de flujo basada en
los datos actualizados; y
presentar la gráfica de información de flujo actualizada
5 a través de la pantalla de la interfaz de usuario.

16. El método de conformidad con la reivindicación 0,
caracterizado además porque comprende almacenar datos
relacionados con la gráfica de información de flujo en
respuesta a la entrada del usuario a través de la interfaz de
10 usuario.

17. El método de conformidad con la reivindicación 0,
caracterizado porque los datos relacionados con la gráfica de
información de flujo incluye uno o más de: los datos
recolectados usados para generar la gráfica de información de
15 flujo, y la gráfica de información de flujo misma.

18. El método de conformidad con la reivindicación 0,
caracterizado además porque comprende:
analizar los datos recolectados; y
generar una alerta en respuesta al análisis de los datos
20 recolectados.

19. El método de conformidad con la reivindicación 0,
caracterizado porque el análisis de los datos recolectados
incluye comparar los datos recolectados a uno o más de: una
póliza de seguridad, una póliza de conformidad de normas y

una norma de desempeño.

20. El método de conformidad con la reivindicación 0, caracterizado además porque comprende generar un reporte con base en los datos recolectados.

5 21. El método de conformidad con la reivindicación 0, además comprende exportar al menos una porción de los datos recolectados a terceros a través de una corriente de datos.

22. Un medio legible por computadora no transitorio, tangible, caracterizado porque almacena instrucciones que,
10 cuando se ejecutan, provocan que un sistema de computadora:

recolecte datos de una pluralidad de diferentes tipos de fuentes, en donde los datos recolectados incluyen datos de la red y datos de recursos;

identifique, con base en los datos de la red en los
15 datos recolectados, un evento de tráfico de la red y una pluralidad de recursos de la red relacionados con el evento del tráfico de la red;

identifique, con base en los datos de recursos en los datos recolectados, conexiones entre la pluralidad de
20 recursos de la red;

genere una gráfica de información de flujo que representa la pluralidad de recursos de la red y las conexiones entre la pluralidad de recursos de la red, en donde la gráfica de información de flujo representa el

tráfico de la red que se permite entre los recursos de la red y el tráfico de la red que se bloquea entre los recursos de la red; y

5 presente la gráfica de información de flujo a través de la pantalla de una interfaz de usuario en comunicación con el sistema de computadora.

23. Un sistema de computadora, caracterizado porque comprende:

un procesador; y
10 memoria en comunicación con el procesador y las instrucciones de almacenamiento que, cuando se ejecutan por el procesador, provocan que el sistema de computadora:

recolecte datos de una pluralidad de diferentes tipos de fuentes, en donde los datos recolectados incluyen datos de la
15 red y datos de recursos;

identifique, con base en los datos de la red en los datos recolectados, un evento de tráfico de la red y una pluralidad de recursos de la red relacionados con el evento de tráfico de la red;

20 identifique, con base en los datos de recursos en los datos recolectados, conexiones entre la pluralidad de recursos de la red;

genere una gráfica de información de flujo que representa la pluralidad de recursos de la red y las

conexiones entre la pluralidad de recursos de la red, en donde la gráfica de información de flujo representa el tráfico de la red que se permite entre los recursos de la red y el tráfico de la red que se bloquea entre los recursos de la red; y

presente la gráfica de información de flujo a través de una pantalla de una interfaz de usuario en comunicación con el sistema de computadora.

10

15

20