

7) The system according to claim 2, wherein the network configuration information includes network service information.

8) The system according to claim 2, wherein the network configuration information includes operating system information.

9) The system according to claim 2, wherein the domain knowledge includes exploit information.

10) The system according to claim 2, wherein the network database table includes more than one network database table.

11) The system according to claim 2, wherein the exploit table includes more than one exploit database table.

12) The system according to claim 2, wherein the result generation module is further configured to submit a query to a database management system.

13) The system according to claim 2, wherein the result is a metric.

14) The system according to claim 2, wherein the result is an attack path.

15) The system according to claim 2, wherein the result is part of an attack path.

16) The system according to claim 2, wherein the result is a collection of paths.

17) The system according to claim 2, wherein the result is an exploit.

18) The system according to claim 2, wherein the result is a condition-exploit pair.

19) The system according to claim 2, wherein the result is an exploit-condition pair.

20) The system according to claim 2, wherein the result is a table that describes an attack graph.

21) The system according to claim 2, wherein the network is reconfigured in response to the result.

22) The system according to claim 2, wherein at least part of the network database table and at least part of the exploit database table are stored in a common table.

23) A tangible computer readable medium containing a set of computer readable instructions that when executed by one or more processors, causes the one or more processors to perform a method for analyzing a network, the method comprising the steps of:

- a) inputting network configuration information that describes the configuration of a network;
- b) inputting domain knowledge for the network, the domain knowledge including knowledge about at least one exploit;
- c) storing the network configuration information in a network database table;
- d) storing the domain knowledge in an exploit database table,
- e) generating a result describing at least part of a network attack using the network database table and exploit database table.

* * * * *