SYSTEM AND METHOD FOR NETWORK PENETRATION TESTING

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This patent application is related to and claims the benefit of priority of U.S. provisional patent application no. 63/357,052, filed on June 30, 2022, the entire contents of which is incorporated by reference.

FIELD

[0002] Embodiments relate to systems and methods for network penetration testing and evaluation.

BACKGROUND INFORMATION

[0003] Known systems and methods for network penetration testing and evaluation typically require large computational resources, fail to effectively correlate penetration vulnerability to a network function inside a core network of the network, and may not facilitate access to security modules for operating on the network via a single access point due to disparate languages used for each security module.

SUMMARY

[0003a] In an aspect, the present disclosure refers to a system for network penetration testing, the system comprising:

a processor;

computer memory having instructions stored thereon that when executed will cause the processor to:

receive a first configuration file including network configuration information pertaining to defining a network, and define log gathering procedures based on the network configuration information;

locate a second configuration file including security module information pertaining to a security module, and define a test case based on the security module information, the test case including a test data package;
parse data from the first configuration file and the second configuration file to generate a data object;
activate the security module to evaluate a security of the network, and produce a vulnerability output;
execute within the security module, based on the data object, the test data package and the test case to identify a penetration vulnerability associated with the vulnerability output of the network; and
output, via a user interface, the penetration vulnerability of the network.

[0003b] In an aspect, the present disclosure refers to a method for penetration testing a network, the method comprising:
using a configuration file to treat a security module as an operating module that is external to a system executing the method by defining a data object from the configuration file;
activating the security module;
executing, based on the data object, a test data package and a test case to identify a penetration vulnerability of the network.

[0003c] In an aspect, the present disclosure refers to a method for penetration testing a network, the method comprising:
receiving a first configuration file including network configuration information pertaining to defining a network, and defining log gathering procedures based on the network configuration information;
locating a second configuration file including security module information pertaining to a security module, and defining a test case based on the security module information, the test case including a test data package;
parsing data from the first configuration file and the second configuration file to generate a data object;
activating the security module to evaluate a security of the network, and produce a vulnerability output;
executing within the security module, based on the data object, the test data package and the test case to identify a penetration vulnerability associated with the vulnerability output of the network; and
outputting, via a user interface, the penetration vulnerability of the network.

[0004] Examples relate to a system for network penetration testing. The system can include a processor. The system can include a computer memory having instructions stored thereon that when executed will cause the processor to execute functions. The instruction can cause the processor to receive a first configuration file including network configuration information pertaining to defining a network, and define log gathering procedures based on the network configuration information. The instruction can cause the processor to locate a second configuration file including security module information pertaining to a security module, and define a test case based on the security module information, the test case including a test data package. The instruction can cause the processor to parse data from the first configuration file and the second configuration file to generate a data object. The instruction can cause the processor to activate the security module to evaluate a security of the

network, and produce a vulnerability output. The instruction can cause the processor to execute within the security module, based on the data object, the test data package and the test case to identify a penetration vulnerability associated with the vulnerability output of the network. The instruction can cause the processor to output, via a user interface, the penetration vulnerability of the network.

[0005] Examples relate to a method for penetration testing a network. The method can involve using a configuration file to treat a security module as an operating module that is external to a system executing the method by defining a data object from the configuration file. The method can involve activating the security module. The method can involve executing, based on the data object, a test data package and a test case to identify a penetration vulnerability of the network.

[0006] Examples relate to a method for penetration testing a network. The method can involve receiving a first configuration file including network configuration information pertaining to defining a network, and defining log gathering procedures based on the network configuration information. The method can involve locating a second configuration file including security module information pertaining to a security module, and defining a test case based on the security module information, the test case including a test data package. The method can involve parsing data from the first configuration file and the second configuration file to generate a data object. The method can involve activating the security module to evaluate a security of the network, and produce a vulnerability output. The method can involve executing within the security module, based on the data object, the test data package and the test case to identify a penetration vulnerability associated with the vulnerability output of the network. The method can involve outputting, via a user interface, the penetration vulnerability of the network.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] Other features and advantages of the present disclosure will become more apparent upon reading the following detailed description in conjunction with the accompanying drawings, wherein like elements are designated by like numerals, and wherein:

[0008] FIG. 1 shows an exemplary system flow diagram;

[0009] FIG. 2 shows an exemplary system architecture diagram;

[0010] FIG. 3 shows an exemplary authenticator module flow diagram for executing server initiation;