РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2005 133 198** (13) **A**

(51) МПК
G06F 11/30 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21), (22) Заявка: **2005133198/09, 26.03.2004**

(30) Конвенционный приоритет:
28.03.2003 US 10/401,040

(43) Дата публикации заявки: **10.06.2006 Бюл. № 16**

(85) Дата перевода заявки PCT на национальную фазу: **28.10.2005**

(86) Заявка PCT:
US 2004/009500 (26.03.2004)

(87) Публикация PCT:
WO 2004/088477 (14.10.2004)

Адрес для переписки:
129010, Москва, ул. Б.Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры", пат.пов. Г.Б. Егоровой

(71) Заявитель(и):
ТРАСТВЭЙВ КОРПОРЕЙШН (US)

(72) Автор(ы):
ГРИН Кеннет (US),
ПАТАНЕЛЛА Джозеф (US),
СКЕТИНА Эрик (US),
ПРАТЕР Брайан (US)

(74) Патентный поверенный:
Егорова Галина Борисовна

(54) УСТРОЙСТВО И СПОСОБ ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВОЙ УЯЗВИМОСТИ И ОЦЕНКА СООТВЕТСТВИЯ

(57) Формула изобретения

1. Устройство для использования в качестве устройства сетевой защиты, содержащее модуль ввода сетевого параметра; первый модуль сканера сети, имеющий вход, соединенный с выходом указанного модуля ввода сетевого параметра; и модуль отчета, имеющий вход, соединенный с выходом указанного первого модуля сканера сети.

2. Устройство по п.1, дополнительно содержащее второй модуль сканера сети, имеющий вход, соединенный с выходом указанного модуля ввода сетевого параметра и имеющий выход, соединенный с входом указанного модуля отчета.

3. Устройство по п.1, в котором указанный модуль ввода сетевого параметра содержит данные, введенные пользователем.

4. Устройство по п.1, в котором указанный модуль ввода сетевого параметра содержит данные, предоставляемые в ответ на опрос.

5. Устройство по п.1, в котором указанный модуль ввода сетевого параметра содержит модуль проверки ошибок для оценки правильности предоставленных данных.

6. Устройство по п.1, в котором указанный модуль ввода сетевого параметра содержит базу данных сетевых адресов.

7. Устройство по п.1, в котором указанный модуль ввода сетевого параметра содержит базу данных имен пользователя.

8. Устройство по п.1, в котором указанный модуль ввода сетевого параметра содержит базу данных параметров настройки.

RU 2005133198 A

RU 2005133198 A

9. Устройство по п.8, в котором указанная база данных параметров настройки содержит данные, касающиеся, по меньшей мере, одного параметра, выбранного из группы, состоящей из сетевых адресов, MAC (управления доступом к среде) адресов, сетевых блоков, уязвимостей, представляющих интерес, инструментальных средств, которые должны использоваться для обнаружения уязвимости, максимальных допусков, доступности времени дня для выполнения программы, периодов пропуска сканирования, и частоты операций.

10. Устройство по п.1, в котором указанный первый модуль сканера сети содержит инструментальное средство сканирования сети, имеющее вход и выход.

11. Устройство по п.1, в котором указанный первый модуль сканера сети содержит, по меньшей мере, одно инструментальное средство, выбранное из группы, состоящей из nslookup, dig, whois, ping, traceroute, rpcinfo, nbtstat, net use, smbclient, nmblookup, nmap, nessus, whisker, nikto, onesixtyone, lantern, pptp_probe, Gbg, Wget, QTIP, DORIAN, Internet Security Systems Scanner, Cybercop Scanner, и Cisco Security Scanner.

12. Устройство по п.1, в котором указанный первый модуль сканера сети содержит модуль, приспособленный для создания списка сканирования, основываясь на данных от указанного модуля ввода сетевого параметра.

13. Устройство по п.1, в котором указанный первый модуль сканера сети содержит модуль, приспособленный для создания описи видимых систем в сети.

14. Устройство по п.1, в котором указанный первый модуль сканера сети содержит модуль, приспособленный для создания описи видимых систем в сети.

15. Устройство по п.1, в котором указанный первый модуль сканера сети содержит модуль, приспособленный для анализа результатов исследования сети.

16. Устройство по п.1, в котором указанный первый модуль сканера сети содержит модуль, приспособленный для исследования системы для определения состояния относительно опознаваемой уязвимости.

17. Устройство по п.1, в котором указанный модуль отчета содержит модуль гомогенизации, приспособленный для приема данных в одном или более форматах и представления их в однородном формате.

18. Устройство по п.1, в котором указанный модуль отчета содержит базу данных окружения клиента.

19. Устройство по п.18, в котором указанная база данных окружения клиента содержит данные, соответствующие, по меньшей мере, одним из группы, состоящей из параметров сканирования, используемых при сканировании, операционных систем, системном реестре IP, уязвимости, времени сканирования, последней дате сканирования, следующей дате сканирования, состоянии сети, обнаруженного MAC адреса, журнала активности сканирования, видимых систем, видимых служб, сканированных имен домена, сканированных IP, обнаруженных IP и приложений, используемых при сканировании.

20. Устройство по п.1, в котором указанный модуль ввода сетевого параметра приспособлен для вывода параметров тестирования сети, основываясь на режиме соответствия, введенном пользователем.

21. Устройство по п.20, в котором указанный режим соответствия выбирается из группы, состоящей из промышленного стандарта, корпоративного регулирования и правительственного регулирования.

22. Способ для защиты сети, содержащий этапы: ввод данных в модуль сканирования; первый этап сканирования сети первым инструментальным средством указанного модуля сканирования; и представление результатов указанного первого этапа сканирования.

23. Способ по п.22, дополнительно содержащий второй этап сканирования сети вторым инструментальным средством указанного модуля сканирования.

24. Способ по п.22, в котором указанный этап ввода данных содержит ввод данных пользователя.

25. Способ по п.22, в котором указанный этап ввода данных содержит ответ на опрос.

26. Способ по п.22, в котором указанный этап ввода данных содержит проверку

RU 2005133198 A

RU 2005133198 A

указанных данных на ошибки.

27. Способ по п.22, в котором указанный этап ввода данных содержит предоставление базы данных сетевых адресов.

28. Способ по п.22, в котором указанный этап ввода данных содержит предоставление базы данных имен пользователя.

29. Способ по п.22, в котором указанный этап ввода данных содержит предоставление базы данных параметров настройки.

30. Способ по п.29, в котором указанная база данных параметров настройки содержит данные, касающиеся, по меньшей мере, одного или параметра, выбранного из группы, состоящей из сетевого адреса, MAC адреса, сетевых блоков, уязвимостей, представляющих интерес, инструментальных средств, которые должны использоваться для обнаружения уязвимости, максимальных допусков, доступности времени дня для выполнения программы, периодов пропуска сканирования и частоты операций.

31. Способ по п.22, в котором указанное первое инструментальное средство содержит инструментальное средство сканирования сети, имеющее вход и выход.

32. Способ по п.22, в котором указанное инструментальное средство сканирования сети содержит, по меньшей мере, одно инструментальное средство, выбранное из группы, состоящей из nslookup, dig, whois, ping, traceroute, rpcinfo, nbtstat, net use, smbclient, nmblookup, nmap, nessus, whisker, nikto, onesixtyone, lantern, pptp_probe, Gbg, Wget, QTIP, DORIAN, Internet Security Systems Scanner, Cybercop Scanner и Cisco Security Scanner.

33. Способ по п.22, в котором указанный первый этап сканирования содержит создание списка сканирования, основываясь на данных от указанного модуля ввода сетевого параметра.

34. Способ по п.22, в котором указанный первый этап сканирования содержит создание описи видимых систем в сети.

35. Способ по п.22, в котором указанный первый этап сканирования содержит создание описи видимых служб в сети.

36. Способ по п.22, в котором указанный первый этап сканирования содержит результаты анализа исследования сети.

37. Способ по п.22, в котором указанный первый этап сканирования содержит исследование системы для определения состояния относительно опознаваемой уязвимости.

38. Способ по п.22, в котором указанный этап представления результатов содержит данные гомогенизации в одном или более форматах в однородный формат.

39. Способ по п.22, в котором указанный этап представления результатов содержит генерацию базы данных окружения клиента.

40. Способ по п.39, в котором указанная база данных окружения клиента содержит данные, соответствующие, по меньшей мере, одним из группы, состоящей из параметров сканирования, используемых при сканировании, операционных систем, реестре IP, уязвимости, времени сканирования, последней дате сканирования, дате следующего сканирования, состоянии сети, обнаруженном MAC адресе, журнале активности сканирования, видимых систем, видимых служб, сканированных имен домена, сканированных IP, обнаруженных IP и приложений, используемых при сканировании.

41. Способ по п.22, в котором указанный этап ввода данных содержит проведение теста сетевого параметров, основываясь на режиме соответствия, введенном пользователем.

42. Способ по п.41, в котором указанный режим соответствия выбирается из группы, состоящей из промышленного стандарта, корпоративного регулирования, и правительственного регулирования.

43. Способ оценки соответствия компьютерной сети, содержащий этапы на которых генерируют первый набор задач, содержащий первое множество команд; генерируют задачи сканирования для анализа компьютерной сети; выбирают заранее определенные сгенерированные задачи сканирования в соответствии с первым множеством команд; генерируют второй набор задач, содержащий выбранные задачи сканирования;

RU 2005133198 A

RU 2005133198 A

генерируют, по меньшей мере, одно назначение задачи, содержащее часть второго набора задач; анализируют компьютерную сеть, используя, по меньшей мере, одно назначение задачи; и создают отчет о результатах анализа компьютерной сети.

44. Способ по п.43, в котором этап генерации первого набора задач содержит этапы, на которых вводят данные относительно компьютерной сети; и генерируют первое множество команд, основываясь на введенных данных.

45. Способ по п.43, в котором этап генерации второго набора задач содержит этап, на котором добавляют, по меньшей мере, одну дополнительную задачу сканирования, требуемую для анализа компьютерной сети.

46. Способ по п.45, в котором, по меньшей мере, одна дополнительная задача содержит команду для прослушивания пакетов в компьютерной сети.

47. Способ по п.43, в котором этап генерации второго набора задач содержит этап расположения по приоритетам выбранных задач сканирования.

48. Способ по п.43, в котором этап генерации второго набора задач содержит этап добавления, по меньшей мере, одной задачи, основываясь на результатах анализа компьютерной сети.

49. Способ по п.43, в котором этап анализа содержит этапы, на которых выбирают, по меньшей мере, одно инструментальное средство сканирования из библиотеки инструментальных средств; и применяют выбранное инструментальное средство сканирования к компьютерной сети.

50. Способ по п.49, в котором этап выбора, по меньшей мере, одного инструментального средства сканирования содержит одновременно выбор множества инструментальных средств сканирования.

51. Способ по п.49, в котором этап выбора, по меньшей мере, одного инструментального средства сканирования содержит последовательный выбор множества инструментальных средств сканирования.

52. Способ по п.43, в котором этап анализа содержит предоставление, по меньшей мере, одного инструментального средства сканирования, где, по меньшей мере, одно инструментальное средство сканирования реагирует на команды в, по меньшей мере, одной назначенной задаче.

53. Способ по п.52, в котором этап анализа содержит предоставление множества инструментальных средств сканирования, где, по меньшей мере, два из множества инструментальных средств сканирования работают на различных операционных системах.

54. Способ по п.52, в котором этап анализа дополнительно содержит перевод команд в пределах, по меньшей мере, одной назначенной задачи в, по меньшей мере, один из языка и формата, требуемого, по меньшей мере, одним инструментальным средством сканирования.

55. Способ по п.43, в котором этап анализа содержит определение, может ли компьютерная сеть быть проанализирована, причем компьютерная сеть анализируется, если определено, что компьютерная сеть может быть проанализирована.

56. Способ по п.43, в котором этап создания отчета содержит генерацию собственного вывода, основываясь на анализе компьютерной сети, где собственный вывод содержит результаты анализа компьютерной сети.

57. Способ по п.56, в котором этап создания отчета дополнительно содержит перевод сгенерированного собственного вывода в, по меньшей мере, одно из общего языка и общего формата.

58. Система для сканирования компьютерной системы, содержащая модуль управления задачами для генерации, по меньшей мере, одного назначения задачи, причем, по меньшей мере, одно назначение задачи содержит команды для сканирования, по меньшей мере, одной компьютерной сети; и по меньшей мере один модуль сканирования для приема, по меньшей мере, одного назначения задачи и для сканирования, по меньшей мере, одной компьютерной сети в соответствии с командами.

59. Система по п.58, в котором по меньшей мере один модуль сканирования содержит множество модулей сканирования.

RU 2005133198 A

RU 2005133198 A

60. Система по п.58, в котором по меньшей мере один модуль сканирования содержит, по меньшей мере, одно инструментальное средство для сканирования по меньшей мере одной компьютерной сети.

61. Система по п.60, в котором по меньшей мере один модуль сканирования содержит множество модулей сканирования.

62. Система по п.58, в котором по меньшей мере одно назначение задачи содержит команды, основанные на данных, введенных пользователем.

63. Система по п.58, в котором по меньшей мере одно назначение задачи содержит команды, основанные на результате сканирования по меньшей мере одним модулем сканирования.

RU 2005133198 A