Оспанова А. Б., Уалиханов Г. С., Жаркимбекова А. Т.

Евразийский национальный университет им. Л. Н. Гумилева, г. Астана

o.ademi111@gmail.com, [vip.galimkhan@mail.ru](mailto:vip.galimkhan@mail.ru), aighan@mail.ru

Управление утилитами Kali Linux

*В работе исследован кроссплатформенный инструментарий разработки приложений с графическим интерфейсом пользователя для операционной системы Kali Linux. С помощью библиотеки Qt и пакета PyQt для Python выполнена графическая программа, реализующая функциональные возможности некоторых утилит дистрибутива Kali Linux с обработкой результатов.*

Пакет PyQt ([1]) для популярного скриптового языка Python позволяет использовать практически все широкие возможности библиотеки Qt ([2]), а также вместе с ним доступна среда Qt Designer. За счет относительной легкости использования, применимости в различных сферах программирования и имеющегося большого количества качественных и доступных обучающих материалов связка Qt+Python (PyQt), также обеспечивающая кроссплатформенность получаемых приложений, достаточно популярна среди разработчиков. Отметим, что приложения работают на всех платформах, поддерживаемых Qt (Linux и другие UNIX-подобные ОС, Mac OS X и Windows). Существует две версии библиотеки PyQt: PyQt5, поддерживающая Qt 5, и PyQt4, совместимая с Qt 4; обе версии поддерживают Python 2.x и Python 3.x. Все варианты достаточно успешно сосуществуют, Python 2.7.14 широко популярен и поддерживается, имеет множество развивающихся библиотек, а также функционирует множество известных программ, написанных на нем, с обширной, в том числе коммерческой, пользовательской базой.

Дистрибутив Kali Linux предназначен для тестирования информационной безопасности, для этих целей есть большое множество инструментов, многие из которых обладают мощными возможностями. Операционная система и инструментарий обеспечены широкой поддержкой, регулярно обновляются. На сегодняшний день последняя версия дистрибутива Kali Linux 2018.1, обновлено ядро до версии 4.14.12. Далее в таблице 1 приведена некоторая классификация инструментария Kali Linux по разделам информационной безопасности.

Таблица 1. Инструменты Kali Linux по разделам информационной безопасности

|  |
| --- |
| Категории инструментов Kali Linux |
| Инструменты сканирования и сбора информации (автоматизированное тестирование сетей, оборудования) |
| Анализ уязвимостей (автоматизированное тестирование на проникновение, инъекции в базы данных sql и т. п.) |
| Аудит и атаки на беспроводные сети (атаки клиентов, обнаружение устройств и другое) |
| Тестирование и атаки Web-приложений (поиск, автоматическое обнаружение сайтов с уязвимостями, эксплуатация уязвимостей, захват рендеринга Web-страниц) |
| Компьютерная криминалистика (сканирование серверов, поиск уязвимостей, цифровые расследования, реагирование на инциденты, выявление атак, снятие отпечатков трафика, исследование образов дисков, идентификация типов файлов) |
| Эксплуатация уязвимостей (генерация нагрузок на сервер, автоматизированное тестирование на проникновение, массовое сканирование и другое) |
| Стресс-тестирование (эксплуатирование уязвимостей протоколов беспроводной связи, тестирование на проникновения, атаки на WPS (Wifi Protected Setup), заглушка wi-fi клиентов и точек доступа и другое) |
| Sniffing и Spoofing (сетевые атаки и мониторинг, перехват и перенаправление пакетов в сетях, поиск и эксплуатация уязвимостей, атаки, использующие уязвимости DNS, захват изображений из сетевого трафика и другое) |
| Атаки на пароли (атаки по словарю, взлом с использованием графических ядер и радужных таблиц, генератор словарей с паролями, генерация списка паролей по данным атакуемого пользователя) |
| Доступ к защищенным программам и устройствам (добавления бэкдоров в приложения, скрытые интерактивные подключения через HTTP, изощренные атаки на заблокированный/защищённый паролем компьютер (требует подключения дополнительного аппарата (Raspberry Pi Zero [3]), веб-шеллы на различных языках) |
| Реверс инжиниринг (инжиниринг двоичных файлов, исследование вредоносного программного обеспечения) |
| Взлом оборудования (атаки на сетевое оборудование, взлом паролей) |
| Приложения для тренировки (небезопасные Web-приложения, уязвимые рабочие окружения для тестирования, специальным образом настроенные виртуальные машины) |
| Инструменты по составлению отчётов (анализ, визуальное представление информации, выявление связей, хранение, форматирование и другие возможности обработки, захват рендеринга Web-страниц, подготовка сетевых атак) |
| Анонимность (автоматическое подключение к случайному VPN, Web-прокси с возможностями фильтрации, модификации данных Web-страницы и HTTP заголовков, контролем доступа, защита от анализа трафика, анонимайзеры, перенаправляющие службы и трафик) |
| Шифрование данных и антикриминалистика (безопасное очищение файлов, дисков, разделов подкачки и памяти, переписывание несколько раз файлов) |
| Социальная инженерия |

Такое разнообразие утилит Kali Linux, которые, к тому же, имеют множество служб и параметров вызова, выдающих большие объемы информации, обусловило, отчасти, создание представляемого в работе приложения. Это программа с графическим интерфейсом (рис. 1), где реализованы некоторые наиболее употребимые для экспресс-тестирования режимы вызова утилит для тестирования сетевой безопасности, с возможностью работы с данными из файла (инструменты типа nmap, ifconfig с различными параметрами).

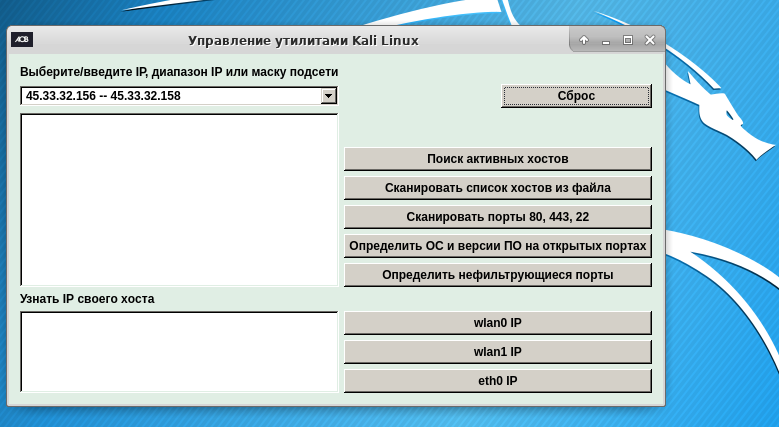


Рисунок 1. Интерфейс программы

Кроме того, реализован анализ и обработка текстов сообщений вызываемых утилит, результаты работы фильтруются и выводятся в форматированном виде, для чего, в частности, применялась утилита grep (рис. 2-3). На рисунке 2 приведены результаты поиска портов, не защищенных сетевыми экранами, поиска активных портов, а также сканирования списка хостов из файла. На рисунке 3 с помощью программы найдены версии программного обеспечения, работающего на открытых портах хостов 45.33.32.250-45.33.32.251, получены результаты сканирования портов 80, 22 и 443 на тех же хостах, а также IP беспроводного сетевого интерфейса в локальной сети.

Использован shell-код, выполненный на Python и bash, что не привело практически к увеличению времени обработки запросов.

Программа написана на Python 2.7.14+PyQt4 4.11.4.

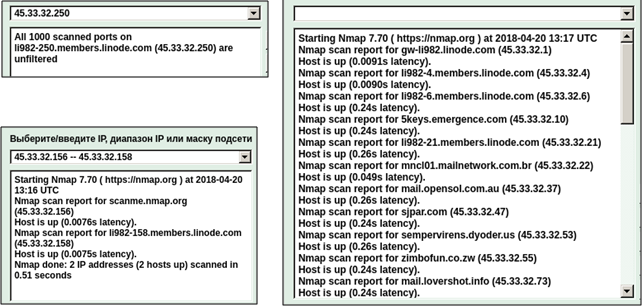


Рисунок 2. Вывод фильтрованной информации 1

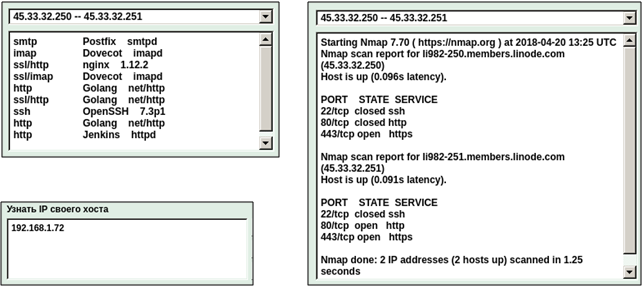


Рисунок 3. Вывод фильтрованной информации 2

Данная работа является перспективной предпосылкой к планируемой авторами разработке кроссплатформенной автоматизированной системы для тестирования безопасности сетей с интеллектуальным анализом данных, формированием отчетов и рекомендаций по принятию мер защиты; работа с данной системой будет доступна пользователям, не являющимся специалистами в области информационной безопасности и не владеющими профессиональным программным инструментарием.

Список использованных источников

1. PyQt4 4.11.4 – pypi.org/project/PyQt4/.

2. Qt – www1.qt.io/ru/.

3. Официальный сайт Raspberry Pi – <https://www.raspberrypi.org/>.