KALI LINUX В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Михейчик А.Д.

Хацкевич О.А. – к. т. н., доцент

В работе рассмотрен один из самых известных инструментов, служащий для проведения тестирования на проникновение, - дистрибутив Kali Linux. Продемонстрированы его недостатки, а также известные инструменты, с помощью которых специалисты по защите информации могут проводить испытания.

На сегодняшний день использование новейших сервисов и технологий приводит к эффективному функционированию информационной среды. Но, к сожалению, данные сервисы и технологии могут быть уязвимы для кибератак, что может привести к серьезным последствиям. К таким последствиям можно отнести: осуществление DDoS-атак; кража конфиденциальной информации; проникновение вредоносных программ, которые могут непосредственно повлиять на работу компании и т.д.

Для решения проблем, связанных с информационной безопасностью, многие компании устанавливают антивирусные программные средства, межсетевые экраны, системы обнаружения и предотвращения вторжений, DLP-системы и т.п. В последнее время набирает популярность тестирование на проникновение (пентестинг).

Пентестинг представляет из себя инструмент, с помощью которого осуществляется серия тестов на проникновение, которые основаны на атаках информационной системы для того, чтобы обнаружить недостатки и слабые места данной системы и в последствии их устранить [1]. Следует учитывать, что данные тесты не наносят вред информационной системе.

На данный момент существует большое разнообразие инструментов, с помощью которых можно выполнить тестирование на проникновение. Благодаря тому, что многие инструменты используются отдельно, возник вопрос о том, чтобы их объединить в одну систему. К такой системе можно отнести и известный дистрибутив Linux – Kali Linux.

Данный дистрибутив служит для специалистов по защите информации, чтобы тестировать систему на безопасность. В виду того, что для работы с инструментами, которые встроены в Kali, нужно иметь права суперпользователя, то уровень пользователя по умолчанию является root. Следовательно, это одна из веских причин, почему не стоит использовать данный дистрибутив для обычного пользования.

Как уже отмечалось выше, Kali Linux используется только для осуществления пентестинга, поэтому все программы, которые встроены в данный дистрибутив, служат только для тестирования безопасности. В нем отсутствуют обычные офисные программы, читалки и т.п. Инструменты, которые могут быть использованы, представлены на рисунке 1 [2].

Рисунок 1 – Инструменты Kali Linux

Ниже будет дана краткая характеристика пяти известных инструментов, которые установлены по умолчанию в дистрибутиве Kali [3]:

1) Jhon The Ripper – инструмент, который используется специалистами для взлома паролей методом перебора;

2) Aircrack-ng – эта программа предназначена для взлома и тестирования безопасности Wi-Fi сетей;

3) Burp Suite – инструмент служит для обнаружения уязвимостей на сайтах Интернета и веб-приложений, которые работают по HTTP и HTTPS протоколам;

4) Wireshark – один из самых известных инструментов, служащий для проведения анализа сетевых пакетов, приложений;

5) Metasploit – платформа для разработки, тестирования и использования кодов эксплойтов.

В статье рассмотрены проблемы информационной безопасности. Предложено использовать известный дистрибутив Kali Linux для проведения тестирования информационной системы на проникновение. Продемонстрированы известные инструменты, которые входят в состав Kali, используемые специалистами для проведения испытаний.

Список использованных источников:

1. Пентестинг [Электронный ресурс] – Режим доступа: http://www.tadviser.ru (Дата обращения: 17.03.2019).

2. Kali Linux [Электронный ресурс] – Режим доступа: https://losst.ru/obzor-kali-linux (Дата обращения: 18.03.2019).

3. Инструменты Kali Linux [Электронный ресурс] – Режим доступа: https://losst.ru/luchshie-instrumenty-kali-linux (Дата обращения: 19.03.2019).