УДК 004.056.53

С. В. Поршнев, О. А. Пономарева, Э. В. Соломаха

ОБЛАЧНЫЙ СЕРВИС АНАЛИЗА ОПЕРАЦИОННЫХ СИСТЕМ И ПРИЛОЖЕНИЙ

Большое число уязвимостей в современных операционных системах и программном обеспечении, представляющих угрозы безопасности информации, определяет необходимость их изучения при подготовке специалистов в области информационной безопасности. В статье обсуждаются принципы построения программно-аппаратного комплекса, основанного на совместном использовании облачных технологий и технологий виртуализации; описана методика сборки операционной системы OpenStarck; приведены примеры, подтверждающие работоспособность выбранного подхода.

The presence of a large number of vulnerabilities in modern operating systems and software that pose a threat to information security determines the need to study them when training specialists in the field of information security. The article discusses the principles of building a software and hardware complex based on the joint use of cloud and virtualization technologies; describes the assembly method of the OpenStarck operating system; examples are given that confirm the operability of the chosen approach.

Ключевые слова: операционная система, программное обеспечение, уязвимость, облачные технологии, виртуализация.

Keywords: operating system, software, vulnerability, cloud technology, virtualization.

Введение

Федеральные государственные образовательные стандарты направлений подготовки и специальностей группы 10.00.00 «Информационная безопасность» предусматривают изучение вредоносного программного обеспечения и уязвимостей операционных систем (ОС).

Современный перечень вредоносных программ и уязвимостей ОС и работающего под их управлением программного обеспечения (ПО) весьма велик — например, в Банке данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю Российской Федерации [1] представлено описание 213 угроз безопасности, которые могут быть использованы вредоносным ПО. Поэтому разработка облачного сервиса анализа операционных систем и приложений для изучения уязвимостей ОС и ПО является актуальной.

Также в современных условиях многообразия ОС и ПО оказываются востребованными универсальные сервисы, которые обеспечивают одновременную работу большого числа пользователей с различными типами ОС и ПО. В статье описывается разработанный на основе совместного использования облачных технологий и технологий виртуализации сервис, удовлетворяющий данному требованию.

Вестник Балтийского федерального университета им. И. Канта.
Сер.: Физико-математические и технические науки. 2019. № 4. С. 76 – 80.

Обоснование выбора облачной технологии

Для создания облачной вычислительной структуры была выбрана облачная ОС *OpenStack* [2; 3], представляющая собой комплекс проектов свободного ПО, предназначенный для создания инфраструктурных облачных сервисов и облачных хранилищ. Напомним, что основными компонентами ОС *OpenStack* являются:

— Nova — контроллер вычислительных ресурсов;

— Neutron (в первых версиях ОС — Quantum) — сервис «подключение к сети как услуга» между интерфейсами устройств (vNIC), которые управляются другими сервисами *OpenStack*;

— Keystone — сервис идентификации;

— Glance — библиотека образов виртуальных машин, позволяющая использовать шаблоны для запуска виртуальных машин и производить резервное копирование;

— Cinder — служба работы с блочными устройствами хранения данных виртуальных машин;

— Swift — облачное файловое хранилище, используемое для хранения пользовательских статических файлов, например образов виртуальных машин и их резервных копий;

— Ceilometer — средства сбора, нормализации и трансформации данных, предоставляемых сервисами *OpenStack*, которые используются для реализации различных сценариев реагирования на события;

— Horizon — графический интерфейс для администрирования облака через web-приложение.

Выбор данной ОС обусловлен тем, что открытая архитектура ОС, которая при ее полной установке оказывается весьма требовательна к техническим характеристикам используемых вычислительных, обеспечивает возможность сборки конфигурации ОС, функционирующей на обычном персональном компьютере с относительно невысокими техническими характеристиками.

Развертывание ОС *OpenStack*

Развертывание ОС *OpenStack* на ноутбуке с двухъядерным процессором, 8 Гб оперативной памяти, 500 Гб емкости жесткого диска с ОС *Linux*, установленной из дистрибутива CentOS, производилось выполнением следующей последовательности действий:

1) копирование репозитариев дистрибутива ОС *OpenStack* на жесткий диск используемого ноутбука, отключение сетевого менеджера ОС *Linux*, установка статического адреса ОС *OpenStack*;

2) установка брокера сообщений *RabbitMQ*;

3) установка и настройка компонента Keystone (создание и наполнение с помощью криптографической библиотеки OpenSSL базы данных, содержащей ключи и сертификаты, настройка точки входа, пользователей и ролей);

4) развертывание компонентов Glance, Cinder, Swift, Nova;
5) установка и настройка компонента Neutron;
6) установка компонента Horizot.

Проверка работоспособности ОС *OpenStack*

Для проверки работоспособности развернутой облачной системы виртуализации с помощью стандартных средств ОС *OpenStack* была создана виртуальная машина CirrOS [4] и произведен успешный запуск консоли с одновременно подключенных к ней ноутбука (рис. 1) и смартфона (рис. 2).

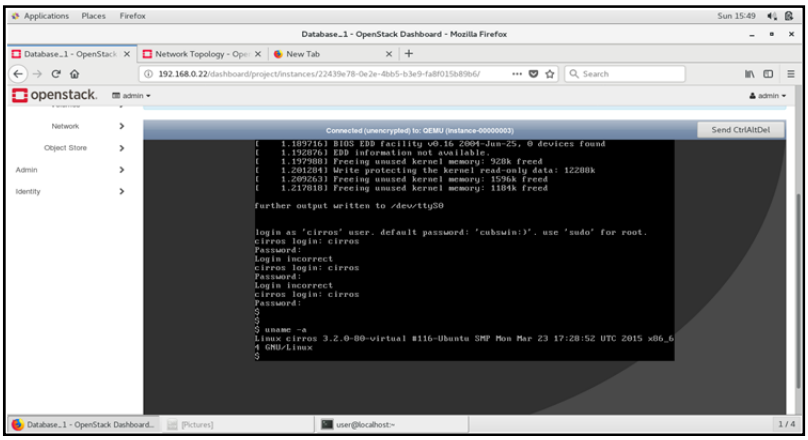

Рис. 1. Окно консоли, запущенной с ноутбука

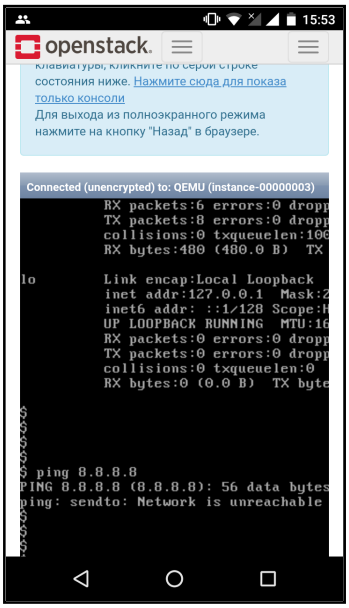

Рис. 2. Окно консоли, запущенной со смартфона

Еще одним подтверждением работоспособности выбранного подхода стали результаты исследования известных уязвимостей ОС *CrackOS*, к которым можно получить доступ как удаленно (внешние уязвимости), так и со стороны одной из учетных записей (внутренние уязвимости).

Для этого в облачной инфраструктуре *OpenStack* была эмулирована виртуальная машина, функционирующая под управлением ОС *CrackOS*. Ее структурная схема представлена на рисунке 3.

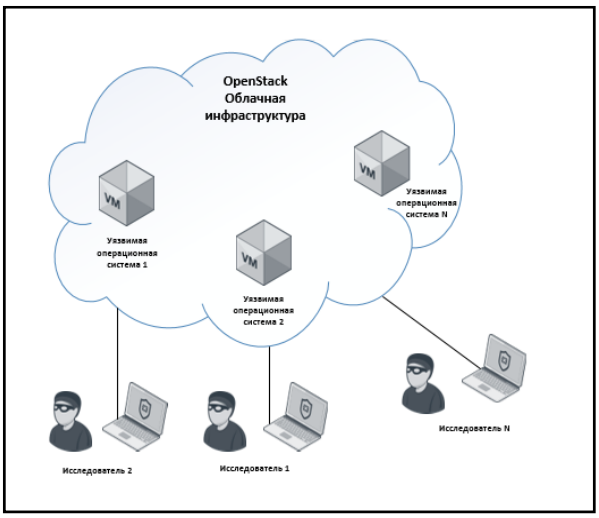

Рис. 3. Облачная инфраструктура *OpenStack*

Разработанный облачный сервис позволяет производить тестирование на наличие уязвимостей широкого круга операционных систем и приложений с использованием разных наборов инструментов.

Заключение

Разработанный сервис представляет собой инструмент для обучения и исследования уязвимостей операционных систем и приложений, позволяющий получить практические навыки:

— в определении сценариев атак злоумышленников на информационные системы;

— эксплуатации известных уязвимостей и поиске новых;

— проектировании информационных систем, в том числе ресурсов, представляющих собой приманку для злоумышленников (так называемые honeypot);

— определении необходимых действий для предотвращения атак злоумышленников на информационные системы;

— администрировании информационных систем;

— тестировании на проникновение приложений и операционных систем.

Список литературы

1. *Банк* данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю Российской Федерации : [сайт]. URL: https://bdu.fstec.ru/threat (дата обращения: 02.09.2019).

2. *OpenStack.* Open source software for creating private and public clouds. URL: https://www.openstack.org/ (дата обращения: 02.09.2019).

3. *Маркелов А.А.* OpenStack. Практическое знакомство с облачной операционной системой. М., 2017.

4. *OpenStack.* Get images. URL: https://docs.openstack.org/image-guide/obtain-images.html (дата обращения: 02.09.2019).

Об авторах

Сергей Владимирович Поршнев — д-р техн. наук, проф., Уральский федеральный университет им. первого Президента России Б.Н. Ельцина; ведущий научный сотрудник, Институт математики и механики им. Н.Н. Красовского Уральского отделения РАН, Россия.

E-mail: s.v.porshnev@urfu.ru

Ольга Алексеевна Пономарева — ст. преп., Уральский федеральный университет им. первого Президента России Б.Н. Ельцина, Россия.

E-mail: o.a.ponomareva@urfu.ru

Эдуард Викторович Соломаха — ассист., Уральский федеральный университет им. первого Президента России Б.Н. Ельцина, Россия.

E-mail: o.a.ponomareva@urfu.ru

The authors

Prof. Sergey V. Porshnev, Ural Federal University named after First President of Russia B.N. Yeltsin; Leading Researcher, N.N. Krasovsky Institute of Mathematics and Mechanics of the Ural Branch of the Russian Academy of Sciences, Russia.

E-mail: s.v.porshnev@urfu.ru

Olga A. Ponomareva, Assistant Professor, Ural Federal University named after First President of Russia B.N. Yeltsin, Russia.

E-mail: o.a.ponomareva@urfu.ru

Eduard V. Solomaha, Assistant, Ural Federal University named after First President of Russia B.N. Yeltsin, Russia.

E-mail: o.a.ponomareva@urfu.ru