Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Создание защищённой инфраструктуры для веб-приложений

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Шкребтана Максима Андреевича

Научный руководитель

доцент, к.п.н. _____ А. С. Гераськин

31.12.2016 г.

Заведующий кафедрой

профессор, к.ф.-м.н. _____ В. Н. Салий

31.12.2016 г.

Саратов 2017

ВВЕДЕНИЕ

Рынок хостинга развивается: всё больше поставщиков услуг хостинга предлагают своим клиентам аренду так называемых VPS (англ. Virtual Private Server — «виртуальный частный сервер»). Виртуальный частный сервер использует аппаратную виртуализацию и эмулирует работу отдельного физического сервера. VPS особенно популярны среди небольших компаний, которые не могут себе позволить или не хотят покупать физический сервер; это могут быть владельцы веб-приложений, интернет-магазинов, веб-порталов и других различных веб-сайтов. Стоимость аренды VPS существенно ниже, чем стоимость арены физического сервера. Более того, при аренде VPS отсутствует необходимость обслуживания аппаратной части сервера, так как этим занимается поставщик услуг VPS.

В 4-м квартале 2015 выручка компании Amazon Web Services — одного из крупнейших поставщиков услуг VPS — выросла на 69% по сравнению с аналогичным периодом 2014 года. Другая компания, DigitalOcean, в настоящее время занимает 2-е место среди поставщиков хостинг-услуг. В декабре 2012 года на арендованных виртуальных частных серверах (VPS) DigitalOcean работало чуть больше 100 веб-серверов, которые обслуживали около 200 веб-сайтов; в сентябре 2016 года на VPS DigitalOcean работало уже больше 283000 веб-серверов, обслуживающих больше 735000 веб-сайтов.

В отличие от виртуального хостинга (англ. shared hosting), при котором каждому веб-сайту выделяется отдельный раздел сервера и все сайты пользуются одним и тем же программным обеспечением (ПО), виртуальный сервер предоставляет администратору-владельцу полный и независимый контроль над всей операционной системой. Владелец виртуального частного сервера имеет возможность самостоятельно выбрать и установить операционную систему — как правило, дистрибутив GNU/Linux, FreeBSD или Windows.

В связи с этим отпадают искусственные ограничения, характерные для виртуального хостинга: количество создаваемых сайтов, баз данных, пользователей и т. д.

Как правило, пользователи, арендующие VPS, получают выделенный IP-адрес и гарантированный минимум вычислительных ресурсов (процессорного времени, оперативной памяти, постоянной памяти).

Недостатком VPS является необходимость администрирования системы, в том числе установка и конфигурирование программного обеспечения. Неправильная конфигурация программного обеспечения, используемого на сервере, предоставляет собой серьёзную уязвимость как для сервера, так и для отдельных веб-сайтов и приложений.

С учётом роста популярности виртуальных частных серверов становится всё более актуальной задача самостоятельного создания инфраструктуры для веб-приложений — установки и конфигурирования операционной системы, веб-сервера, СУБД, интерпретатора языка программирования, на котором реализовано веб-приложение. В данной работе описан процесс создания защищённой инфраструктуры для веб-приложений с использованием виртуализации на уровне операционной системы для лучшей изоляции компонентов инфраструктуры. Если злоумышленнику удастся эксплуатировать уязвимость одного из компонентов инфраструктуры, например веб-сервера, изоляция позволит обезопасить другие компоненты инфраструктуры.

Цель данной работы — создание защищённой, контролируемой и простой в управлении инфраструктуры для веб-приложений.

В задачи данной работы входят:

- создание виртуального сервера и конфигурирование серверного ПО;
- анализ уязвимостей конфигурации серверного ПО;
- изучение механизмов виртуализации на уровне ОС;
- построение инфраструктуры для веб-приложений с использованием виртуализации на уровне ОС;

- конфигурация и запуск существующего веб-приложения в рамках построенной инфраструктуры.

Дипломная работа состоит из введения, 3 глав, заключения, списка использованных источников и 4 приложений. Общий объем работы — 91 страница, из них 69 страниц — основное содержание, включая 14 рисунков и 2 таблицы, список использованных источников из 27 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В главе 1 описывается процесс создания и конфигурирования виртуального частного сервера. В разделе 1.1 описывается процесс конфигурирования сервера удалённого доступа OpenSSH для использования метода аутентификации с помощью инфраструктуры открытых ключей. Далее в разделе рассматриваются уязвимости конфигурации сервера OpenSSH. В разделе 1.2 описывается процесс создания учётной записи администратора сервера, имеющего возможность выполнять команды от имени пользователя root.

Глава 2 посвящена Docker — программному обеспечению для автоматизации развёртывания и управления приложениями в среде виртуализации на уровне операционной системы. Виртуализация на уровне ОС — метод виртуализации, при котором ядро ОС поддерживает несколько изолированных экземпляров пространства пользователя (так называемых контейнеров), вместо одного.

В разделах 2.1 и 2.2 описываются механизмы, используемые Docker: namespaces и cgroups. Механизм namespaces обеспечивает изоляцию процессов, а механизм cgroups ограничивает и изолирует вычислительные ресурсы для групп процессов.

Далее в разделе 2.3 описывается клиент-серверная архитектура Docker и метод взаимодействия между клиентом docker и сервером dockerd.

Раздел 2.4 раскрывает суть понятий «образ» и «контейнер», используемых в рамках ПО Docker. Описывается внутренняя структура и процесс создания образов, а также процесс запуска контейнеров.

В разделе 2.5 поясняется устройство «томов данных», используемых для постоянного хранения данных независимо от жизненного цикла контейнера.

В разделе 2.6 рассказывается о сетевых возможностях Docker, таких как построение новых сетей и создание правил маршрутизации.

В главе 3 описывается процесс создания защищённой инфраструктуры для веб-приложений с использованием Docker-контейнеров. В разделе 3.1

описывается создание образа и запуск контейнера для изоляции веб-сервера Nginx; также в данном разделе рассматриваются уязвимости конфигурации Nginx.

В разделе 3.2 описывается процесс получения сертификата X.509 и конфигурация HTTPS-сервера. В этом разделе описывается протокол автоматического управления сертификатами ACME с участием агента удостоверяющего центра Let’s Encrypt. Далее рассматривается процесс конфигурирования веб-сервера Nginx для работы с агентом Let’s Encrypt и процесс получения сертификата. Далее описывается процесс конфигурирования HTTPS-сервера, который должен использовать полученный сертификат.

В разделе 3.3 описывается создание образа и запуск контейнера для изоляции СУБД. В разделе 3.4 описывается создание образа и запуск контейнера для изоляции веб-приложения на примере WordPress.

ЗАКЛЮЧЕНИЕ

В данной работе были описаны механизмы контейнеризации и возможности программного обеспечения Docker. Была описана конфигурация серверного ПО, а также процессы создания контейнеров для веб-сервера, СУБД и веб-приложения.

В данной работе был описан процесс получения сертификата открытого ключа сервера стандарта X.509 по протоколу ACME и процесс конфигурирования HTTPS-сервера для обеспечения безопасных соединений между веб-сервером и клиентом.

Таким образом в ходе данной работы была описана и создана защищённая, контролируемая и простая в управлении инфраструктура для веб-приложений с использованием механизмов контейнеризации.

С ростом популярности виртуальных частных серверов задача самостоятельного создания инфраструктуры для веб-приложений становится всё более актуальной. Использование контейнеризации и таких инструментов как Docker и Docker Compose позволяет не только упростить эту задачу, но и повысить уровень защищённости и надёжности инфраструктуры.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Novet J. Amazon Web Services brings in $2.4B in revenue in Q4 2015, up 69% over last year [Электронный ресурс]: тематический портал // VentureBeat. 2016. URL: http://venturebeat.com/2016/01/28/amazon-web-services-brings-in-2-4b-in-revenue-in-q4-2015-up-69-over-last-year/ (дата обращения: 23.12.2016). Загл. с экр. Яз. англ.
2. DigitalOcean - Growth [Электронный ресурс]: тематический портал // Netcraft. URL: http://trends.netcraft.com/www.digitalocean.com (дата обращения: 23.12.2016). Загл. с экр. Яз. англ.
3. Tholeti B. Hypervisors, virtualization, and the cloud: Dive into the KVM hypervisor [Электронный ресурс]: тематический портал // IBM developerWorks. 2011. URL: http://www.ibm.com/developerworks/cloud/library/cl-hypervisorcompare-kvm/index.html (дата обращения: 23.12.2016). Загл. с экр. Яз. англ.
4. SSH usage profiling [Электронный ресурс]: офиц. сайт // OpenSSH. URL: http://www.openssh.com/usage/graphs.html (дата обращения: 23.12.2016). Загл. с экр. Яз. англ.
5. Nemeth E. и др. Unix® and Linux® System Administration Handbook. 4th Edition. Prentice Hall, 2010. 1344 с.
6. Механизмы контейнеризации: namespaces [Электронный ресурс]: тематический портал // Блог компании Селектел. 2016. URL: https://blog.selectel.ru/mexanizmy-kontejnerizacii-namespaces/ (дата обращения: 23.12.2016). Загл. с экр. Яз. рус.
7. Механизмы контейнеризации: cgroups [Электронный ресурс]: тематический портал // Блог компании Селектел. 2016. URL: https://blog.selectel.ru/mexanizmy-kontejnerizacii-cgroups/ (дата обращения: 23.12.2016). Загл. с экр. Яз. рус.
8. Kleen A. UNIX - sockets for local interprocess communication [Электронный ресурс]: офиц. сайт // The Linux man-pages project. 2016. URL: http://man7.org/linux/man-pages/man7/unix.7.html (дата обращения: 24.12.2016). Загл. с экрана. Яз. англ.

9. Docker security [Электронный ресурс]: офиц. сайт // Docker.com. 2016. URL: https://docs.docker.com/engine/security/security/ (дата обращения: 23.12.2016). Загл. с экр. Яз. англ.
10. Understand images, containers, and storage drivers [Электронный ресурс]: офиц. сайт // Docker.com. 2016. URL: https://docs.docker.com/engine/userguide/storagedriver/imagesandcontainers/ (дата обращения: 23.12.2016). Загл. с экр. Яз. англ.
11. Docker Image Specification v1.2.0 [Электронный ресурс]: Хостинг проектов // GitHub.com. URL: https://github.com/docker/docker/blob/v1.12.5/image/spec/v1.2.md (дата обращения: 23.12.2016). Загл. с экр. Яз. англ.
12. Docker and AUFS in practice [Электронный ресурс]: офиц. сайт // Docker.com. 2016. URL: https://docs.docker.com/engine/userguide/storagedriver/aufs-driver/ (дата обращения: 23.12.2016). Загл. с экр. Яз. англ.
13. Kuznets T. Docker Security Scanning safeguards the container content lifecycle [Электронный ресурс]: тематический портал // Docker Blog. 2016. URL: http://dockr.ly/2fkthS5 (дата обращения: 23.12.2016). Загл. с экр. Яз. англ.
14. Бикманс Ж. Монтирование и заполнение каталога /dev // Linux с нуля / пер. Ромоданов Н.А. М.: ДМК Пресс, 2014. С. 120.
15. Linux Bridge [Электронный ресурс]: тематический портал // Xgu.ru / пер. Чубин И. 2013. URL: http://xgu.ru/wiki/Linux_Bridge (дата обращения: 23.12.2016). Загл. с экрана. Яз. рус.
16. Емельянов П. Virtual ethernet device (tunnel) [Электронный ресурс]: тематический портал // LWN.net. 2007. URL: https://lwn.net/Articles/232688/ (дата обращения: 23.12.2016). Загл. с экр. Яз. англ.
17. Usage Statistics and Market Share of Web Servers for Websites, December 2016 [Электронный ресурс]: тематический портал // W3Techs. 2016. URL: https://w3techs.com/technologies/overview/web_server/all (дата обращения: 23.12.2016). Загл. с экр. Яз. англ.

18. Historical yearly trends in the usage of web servers, December 2016 [Электронный ресурс]: тематический портал // W3Techs. 2016. URL: https://w3techs.com/technologies/history_overview/web_server/ms/y (дата обращения: 23.12.2016). Загл. с экр. Яз. англ.
19. Garrett O. NGINX vs. Apache: Our View of a Decade-Old Question [Электронный ресурс]: офиц. сайт // nginx.com. 2015. URL: https://www.nginx.com/blog/nginx-vs-apache-our-view/ (дата обращения: 23.12.2016).
20. nginx: документация [Электронный ресурс]: офиц. сайт // nginx.org. URL: http://nginx.org/ru/docs/ (дата обращения: 23.12.2016). Загл. с экр. Яз. рус.
21. OWASP Secure Headers Project [Электронный ресурс]: офиц. сайт // OWASP. URL: https://www.owasp.org/index.php/List_of_useful_HTTP_headers (дата обращения: 23.12.2016). Загл. с экр. Яз. англ.
22. Love R. Everything you Need to Know about HTTP Public Key Pinning (HPKP) [Электронный ресурс]: персональный сайт // Robert Love - Blog. 2015. URL: http://blog.rlove.org/2015/01/public-key-pinning-hpkp.html (дата обращения: 23.12.2016). Загл. с экр. Яз. англ.
23. Атака Clickjacking и защита от неё [Электронный ресурс]: тематический портал // Современный учебник Javascript. URL: https://learn.javascript.ru/clickjacking (дата обращения: 23.12.2016). Загл. с экр. Яз. рус.
24. How It Works - Let’s Encrypt - Free SSL/TLS Certificates [Электронный ресурс]: офиц. сайт // Let’s Encrypt. URL: https://letsencrypt.org/how-it-works/ (дата обращения: 23.12.2016). Загл. с экр. Яз. англ.
25. Certbot Documentation [Электронный ресурс]: офиц. сайт // Electronic Frontier Foundation. URL: https://certbot.eff.org/docs/ (дата обращения: 23.12.2016). Загл. с экр. Яз. англ.
26. Security/Server Side TLS [Электронный ресурс]: тематический портал // MozillaWiki. URL: https://wiki.mozilla.org/Security/Server_Side_TLS (дата обращения: 23.12.2016). Загл. с экр. Яз. англ.

27. An implementation of the TCP/IP protocol suite for the LINUX operating system [Электронный ресурс] // Linux Cross Reference. URL: http://lxr.free-electrons.com/source/include/uapi/linux/if.h#L28 (дата обращения: 23.12.2016). Загл. с экр. Яз. англ.