DOI 10.37882/2223–2966.2022.07–2.07

# МЕТОДИКА ПОВЫШЕНИЯ ПРОИЗВОДИТЕЛЬНОСТИ ВИРТУАЛЬНЫХ СЕРВЕРОВ ПРИ ИСПОЛЬЗОВАНИИ СРЕДСТВ АНТИВИРУСНОЙ ЗАЩИТЫ

## A TECHNIQUE FOR IMPROVING THE PERFORMANCE OF VIRTUAL SERVERS WHEN USING ANTI-VIRUS PROTECTION TOOLS

***M. Kapustin***

*Summary.* Threats to information (computer) security are various actions that can lead to violations of the state of information protection. In other words, these are potentially possible events, processes or impacts that can harm information and computer systems. Information security threats can be divided into two types: natural and artificial. Natural phenomena include natural phenomena that are not dependent on humans, such as hurricanes, floods, fires, etc. artificial threats depend directly on the person and can be intentional and unintentional. Unintentional threats arise due to negligence, inattention and ignorance. An example of such threats can be the installation of applications that are not among the necessary ones for work and further disrupt the system, which leads to the loss of information. Intentional threats, unlike the previous ones, are created on purpose. These include attacks by intruders both from outside and from within the company. The result of the implementation of this type of threat is the loss of funds and intellectual property of the organization.

Unwanted content — malicious code, potentially dangerous programs and spam, that is, what is directly created to destroy or steal information.

Unauthorized access — viewing information by an employee who does not have permission to use it, by exceeding official authority. Unauthorized access leads to information leakage. Depending on what data and where it is stored, sources can be organized in different ways, namely through attacks on sites, hacking programs, intercepting data over the network, using unauthorized programs.

*Keywords:* virtual server, VPS, VDS, anti-virus protection.

***Капустин Михаил Николаевич***
*Руководитель инженерной группы, ООО «ЛАНИТ-ТЕХНОЛОГИИ»*
*White4spirit@yandex.ru*

*Аннотация.* Угрозы информационной (компьютерной) безопасности — это различные действия, которые могут привести к нарушениям состояния защиты информации. Другими словами, это-потенциально возможные события, процессы или воздействие, которые могут нанести вред информационным и компьютерным системам. Угрозы ИБ можно разделить на два типа: естественные и искусственные. К природным относятся природные явления, не зависящие от человека, например ураганы, наводнения, пожары и т.д. искусственные угрозы зависят непосредственно от человека и могут быть преднамеренными и непреднамеренными. Непреднамеренные угрозы возникают из-за неосторожности, невнимательности и незнания. Примером таких угроз может быть установка приложений, не входящие в число необходимых для работы и в дальнейшем нарушают работу системы, что и приводит к потере информации. Умышленные угрозы, в отличие от предыдущих, создаются специально. К ним можно отнести атаки злоумышленников как извне, так и изнутри компании. Результат реализации этого вида угроз-потери средств и интеллектуальной собственности организации.

Нежелательный контент — вредоносный код, потенциально опасные программы и спам, то есть то, что непосредственно создано для уничтожения или кражи информации.

Несанкционированный доступ-просмотр информации сотрудником, не имеющим разрешения пользоваться ею, путем превышения должностных полномочий. Несанкционированный доступ приводит к утечке информации. В зависимости от того, какие данные и где они хранятся, истоки могут организовываться разными способами, а именно через атаки на сайты, взлом программ, перехват данных по сети, использование несанкционированных программ.

*Ключевые слова:* виртуальный сервер, VPS, VDS, антивирусная защита.

В зависимости от различных способов классификации все возможные угрозы информационной безопасности можно разделить на следующие основные подгруппы:

- нежелательный контент;
- несанкционированный доступ;
- утечка информации;
- потеря данных;
- мошенничество;
- кибервойны;
- кибертерроризм.

При развертывании нового VPS-сервера существует выбор или доверить организацию системы защиты про-

вайдеру, или внедрять ее собственноручно. Далее представлен пример настройки сервера без участия технической поддержки хостинг-провайдера.

В таком случае предоставляется сервер с выбранной операционной системой, а все последующие действия по его настройке берет на себя предприятие "здоровье". Для начала следует выполнить несколько операций, которые позволят повысить его безопасность и функциональность.

Перед началом работы следует авторизоваться на сервере как пользователь root. Чтобы это сделать, нужен публичный IP-адрес сервера и пароль учетной записи администратора (root). Если они известны, в консоли вводится следующая команда, в которой следует заменить предложенный IP-адрес на адрес своего сервера:

ssh root@194.61.0.6.*
* IP-адрес приведен в качестве примера

Если появится предупреждение о проверке подлинности, следует принять его. Затем система запросит пароль или приватный ключ. Если вход осуществляется впервые с помощью пароля, система предложит задать новый.

После ввода пароля авторизация пройдет успешно, позволяя настроить сервер на CentOS.[9]

Пользователь root в дистрибутивах Linux имеет неограниченные права. Однако, не стоит работать под ним постоянно. При наличии больших возможностей достаточно совершить одно неверное действие, которое приведет к необратимым последствиям. Поэтому стоит создать дополнительный профиль пользователя, для которого можно установить некоторые ограничения.

Для начала создадим новый профиль пользователя с именем "demo":
adduser demo

Назначим для него пароль:
passwd 123

Далее вводим новый пароль и повторяем его после следующего запроса. Новый созданный аккаунт "demo" получил стандартные права. В то же время, при настройке сервера нужно будет провести глубокую настройку VPS-серверу, для чего понадобятся root-права.

Для того, чтобы не менять постоянно стандартный аккаунт на профиль администратора, можно сделать из demo "суперпользователя". Для того, чтобы запускать команды с правами администратора, перед ними достаточно дописать команду sudo.

Далее-добавляем профиль demo к группе «wheel». В CentOS пользователи данной группы могут использовать команду sudo. Для этого используем следующую команду:

# gpasswd-a demo wheel

Чтобы улучшить защиту сервера, можно добавить аутентификацию пользователей с помощью открытого ключа. Это на порядок увеличивает безопасность сервера, поскольку позволяет выполнять авторизацию путем ввода ключа

SSH. Для создания новой пары ключей SSH достаточно ввода команды:

ssh-keygen

Подтверждаем нажатием кнопки Enter принятие этого имени файла и пути к нему. Система предложит задать пароль для защиты ключа. Впрочем, этот шаг необязателен и можно обойтись без пароля. Эта процедура сгенерирует закрытый ключ id_rsa и открытый ключ id_rsa.pub во внутреннем каталоге.ssh.

Когда пара SSH-ключей будет успешно сгенерирована, понадобится скопировать на новый сервер открытый ключ. Сделать это можно с помощью скрипта ssh-copy-id, который нужно предварительно установить на CentOS7. Он поможет установить открытый ключ каждому авторизованному пользователю.

Для этого вписываем в консоль команду:

ssh-copy-id

После ее выполнения вводится имя пользователя и IP-адрес сервера, на который добаваестья ключ:

ssh-copy-id demo@194.61.0.6

Когда пароль будет введен, открытый ключ добавится в файл удаленного пользователя по пути.ssh / authorized_keys. Соответствующий закрытый ключ будет использоваться для входа на сервер.

После применения изменений необходимо выполнить перезагрузку SSH, чтобы система начала работать с новой конфигурацией. Для этого используем следующую команду, чтобы перезапустить демон SSH:

systemctl reload sshd

Перед тем, как покинуть сервер, рекомендуется проверить, правильно ли он настроен. Далее следует закрыть и открыть терминал, чтобы в нем создать новое соединение с нашим сервером. Однако, в данном случае вместо входа в профиль «root», используется уже созданный «demo».

К настроенному удаленному серверу можно подключиться командой: ssh demo@194.61.0.6.

Для установки на сервере организации выбраны следующие программные решения:

- межсетевой экран ConfigServer Security and Firewall(CSF);
- система предупреждения вторжений fail2ban;
- антивирусное программное обеспечение Maldet.

Установка межсетевого экрана. По сравнению с другими аналогичными решениями, Configserver Security and Firewall (CSF) — это бесплатное программное обеспечение брандмауэра с открытым исходным кодом с широким спектром функций. CSF также интегрирован в панели управления хостингом VDS, такие как cPanel и Directadmin. Следовательно, после установки CSF можно настраивать непосредственно из этих панелей управления.

Первым образом для установки CSF нужно подключиться по SSH с правами суперпользователя (root). Для работы CSF необходим Perl, а также библиотека Time / HiRes. Если эти пакеты не установлены, установщик CSF выведет ошибку. Для установки этих пакетов нужно ввести следующие команды:

yum install perl-libwww-perl yum install perl-Time-HiRes

Для того, чтобы установить этот фаервол, необходимо скачать установочный архив CSF, распаковать его и запустить исполняемый файл. Для этого нужны команды:

rm -fv csf.tgz //Удаляем файл csf.tgz, если таковой имеется wget https://download.configserver.com / csf.tgz //Загружаем архив tar -xzf csf.tgz //Распаковываем архив cd csf //Переходим в распакованную директорию sh install.sh //Выполняем установочный скрипт

Установка происходит в автоматическом режиме. После ее завершения необходимо проверить, есть ли на VPS необходимые модули IPTables:

perl /etc/csf/csftest.pl

Результат выполнения команды должен быть примерно таким:

Testing ip_tables / iptable_filter…OK
Testing ipt_LOG…OK
Testing ipt_multiport / xt_multiport…OK
Testing ipt_limit/xt_limit…OK
Testing iptable_nat / ipt_redirect…OK
RESULT: csf should functionn op this server

Как правило, указанные в заключении модули установлены на VPS по умолчанию. Если какой-либо из нужных модулей отсутствует, результаты теста об этом сообщат, после чего необходимо будет произвести установку указанных модулей, чтобы функциональность CSF была ограничена.

После установки ConfigServer Security and Firewall работает в тестовом режиме, который рекомендуется отключать только после того как будет отредактированный конфигурационный файл /etc/csf/csf.conf для нужд предприятия.

В файле конфигурации необходимо как минимум убедиться в том, что все необходимые для работы TCP и UDP порты открыты. Пример таких параметров в файле конфигурации может быть следующим:

# Allow iincoming TCP ports
TCP_IN = «20,21,22,25,53,80,110,143,443,465,587,993,995»
# Allow outgoing TCP ports
TCP_OUT = “20,21,22,25,53,80,110,113,443”
# Allow incoming UDP ports
UDP_IN = “20,21,53”
# Allow outgoing UDP ports
# To allow outgoing traceroute add 33434:33523 to this list UDP_OUT = “20,21,53,113,123”

Отключение тестового режима выполняется путем изменения значения параметра Testing в файле конфигурации, а именно необходимо значение 1 изменить на 0. После этого можно сохранить изменения.

Система предупреждения вторжений. Для установки выбрана система Fail2ban. Это-фреймворк для предотвращения проникновения, предназначенный для блокировки неизвестных IP-адресов, которые пытаются проникнуть во внутреннюю систему. Этот пакет программ важен для защиты от любых атак грубой силы на сервисы.

Чтобы установить пакет используется такая команда:

apt-get install fail2ban

После установки программного пакета необходимо изменить файл конфигурации, чтобы настроить его в со-

ответствии с потребностями. Прежде чем вносить изменения, рекомендуется создать резервную копию файла конфигурации, введя следующую команду:

cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.conf.backup

Затем открываем файл: папка / etc/fail2ban / jail.conf

После выполнения изменений, следует перезагрузить сервис, используя следующую команду:

/ etc / init.d/fail2ban restart

Установка утилиты для сканирования maldetect для сканирования Linux сервера. MalDetect может использовать данные от систем обнаружения атак чтобы обнаруживать вредоносный код (malware). Также может использовать антивирусную базу других сканеров, таких как ClamAV.

MalDetect не доступен в репозиториях ПО, поэтому загрузить и установить его нужно вручную:

cd / usr / local / src; wget http://www.rfxn.com/downloads/maldetect-

current.tar; cd maldetect-* sh ./install.sh; cd ./ rm -rf maldetect-*

После установки обновляем:

maldet-Update-ver maldet-Update

Сканирование происходит следующим образом:

maldet -a /home?/?/ public_html

Каждой проверке присваивается уникальный ID.

MalDetect не удаляет файлы во время сканирования. По окончанию каждого сканирование будет предложено команду, с помощью которой можно просмотреть лог сканирования.

maldet-report% report.ID%

Для удаления найденных файлов нужно выполнить следующую команду: maldet -q%report.ID%

После перечисленных средств можно переходить к установке демонов для работы сайта и электронной почты. Сервер базы данных MySQL по умолчанию. Для работы веб-сайта нужно установить веб-сервер. Выбирая среди таких популярных серверов как nginx, Apache Tomcat, Node.js, Apache HTTP Server, выбор падает на последний, так как он является наиболее часто используемым.

Безопасность бизнеса чрезвычайно важна, но для компании может быть сложным вопросом. Независимо от того, является ли целью предотвращение взлома, защита своих ценных данных, предупреждение краж, стоит пристально следить за своим персоналом, есть много вещей, которые стоит продумать, чтобы ваша безопасность соответствовала потребностям компании.

Каждый бизнес имеет свои особенности, а это значит, что меры безопасности, подходящие одной компании, не обязательно будут удовлетворять потребности другой.

Важно сначала проанализировать потребности в безопасности, то есть, что лучше всего подойдет для конкретного предприятия и что оно может себе позволить. Это включает ряд таких вопросов, как:

- Нужно ли применять меры безопасности в помещении, на открытом воздухе, или в обоих случаях?
- Нужно ли будет покрывать большую площадь или малую?
- Необходимо ли, чтобы система работала круглосуточно, или только тогда, когда бизнес работает?
- Уместно ли внедрение выбранных средств защиты?

Векторы атак на корпоративные инфраструктуры обычно базируются на использовании известных уязвимостей и недостатков в подобных системах, для устранения которых, как правило, достаточно применить базовые принципы обеспечения информационной безопасности:

- ограничить число интерфейсов сетевых служб, доступных для подключения на сетевом периметре;
- регулярное обновление программного обеспечения и установка обновлений безопасности операционной системы;
- использование SIEM-системы для своевременного обнаружения атак;
- для защиты веб-сайтов от атак ботов использовать капчи;
- проводить регулярные лекции с целью повышения осведомленности работников в вопросах информационной безопасности (важно оценивать эффективность таких лекций);
- регулярно проводить тестирование на проникновение чтобы своевременно выявлять новые векторы атак и проверки принятых мер защиты на практике;
- использовать специализированные антивирусные программы для защиты от вредоносного ПО,

распространяемого с помощью социальной инженерии;
- защищать или отключать в локальной вычислительной сети протоколы канального или сетевого уровня, которые не используются и разделять сеть на сегменты;
- минимизировать привилегии пользователей и служб, использовать строгую политику в отношении паролей;
- защищать учетные записи, имеющие повышенный доступ;
- не хранить конфиденциальную информацию в общедоступном виде или в публичном доступе.

ЛИТЕРАТУРА


1. Денисенко В.В. Компьютерное управление технологическим процессом, экспериментом, оборудованием / В.В. Денисенко.— М.: Горячая линия — Телеком, 2009. -с.105–110
2. Нургалиев Р.К. Лабораторный стенд для изучения систем автоматизации узлов коммерческого учета жидких продуктов / Р.К. Нургалиев, В.В. Кузьмин, Ю.А. Куликов, А.В. Чупаев, Р.Р. Галямов, А.А. Гайнуллина // Вестник Казан.технол.ун-та.—2013. -Т. 16, № 1.— С. 67–70.
3. Нургалиев Р.К. Промышленные сети передачи данных / Р.К. Нургалиев, Р.Н. Зарипов, Д.Б. Флакс, Э.У. Даутова // Вестник Казан.технол.ун-та.—2013. -Т. 16, № 1.— С. 252–255.
4. Gu L., Zeng D., Guo S., et al. Cost Efficient Resource Management in Fog Computing Supported Medical Cyber-Physical System // IEEE Transactions on Emerging Topics in Computing. 2017. Vol. 5, no. 1. P. 108–119. DOI: 10.1109/TETC.2015.2508382.
5. Guth J., Breitenbucher U., Falkenthal M., et al. Comparison of IoT Platform Architectures: A Field Study Based on a Reference Architecture // 2016 Cloudification of the Internet of Things, CIoT 2016, 2017. Institute of Electrical and Electronics Engineers Inc., 2017. DOI: 10.1109/CIOT.2016.7872918.
6. Hagiu A., Wright J. When Data Creates Competitive Advantage. . . And When It Doesn't // Harvard Business Review. 2020. Vol. 98, no. 1. P. 94–101.
7. Iorga M., Feldman L., Barton R., et al. Fog Computing Conceptual Model. Gaithersburg, MD, 2018.
8. Jalali F., Hinton K., Ayre R., et al. Fog Computing May Help to Save Energy in Cloud Computing // IEEE Journal on Selected Areas in Communications. 2016. Vol. 34, no. 5. P. 1728–1739. DOI: 10.1109/JSAC.2016.2545559.
9. Kakakhel S.R.U., Mukkala L., Westerlund T., et al. Virtualization at the Network Edge: A Technology Perspective // 2018 3rd International Conference on Fog and Mobile Edge Computing, FMEC2018 (Barcelona, Spain, April, 23–26, 2018). Institute of Electrical and Electronics Engineers Inc., 2018. P. 87–92. DOI: 10.1109/FMEC.2018.8364049.
10. Lee J. A View of Cloud Computing // International Journal of Networked and Distributed Computing. 2013. Vol. 1, no. 1. P. 2–8. DOI: 10.2991/ijndc.2013.1.1.2.
11. Madsen H., Albeanu G., Burtschy B., et al. Reliability in the Utility Computing Era: Towards Reliable Fog Computing // International Conference on Systems, Signals, and Image Processing (Rio de Janeiro, Brazil, June, 3–5, 2013). IEEE Computer Society, 2013. P. 43–46. DOI: 10.1109/IWSSIP.2013.6623445.
12. Mahmood Z., Ramachandran M. Fog Computing: Concepts, Principles and Related Paradigms // Springer International Publishing, 2018. P. 3–21. DOI: 10.1007/978–3–319–94890–4_1.




Журнал «Современная наука: актуальные проблемы теории и практики»