УДК 004

ОБЕСПЕЧЕНИЕ БАЗОВОЙ ЗАЩИТЫ VPS

Ткачёв Е.В.

магистрант 1 курса,

ФГБОУ ВО «Калужский государственный университет

им. К.Э. Циолковского»

Калуга, Россия

Белаш В.Ю.

к.пед.н., доцент,

ФГБОУ ВО «Калужский государственный университет

им. К.Э. Циолковского»

Калуга, Россия

Аннотация: Безопасность виртуальных частных серверов (VPS) является важнейшим аспектом их эксплуатации. В статье рассматриваются основные меры защиты, включая парольную политику, настройку подключения при помощи SSH-ключей, отключение удалённого доступа root, установку Fail2Ban, регулярное обновление программного обеспечения и резервное копирование. Приведены рекомендации по реализации каждой меры для оптимальной защиты сервера.

Ключевые слова: безопасность VPS, защита сервера, информационная безопасность, обновление, парольная политика, программное обеспечение, резервное копирование, SSH, Fail2Ban.

PROVIDING BASIC VPS PROTECTION

Tkachev E.V.

1st year Master's student,

Kaluga State University named after K. E. Tsiolkovsky

Kaluga, Russia

Belash V.Yu.
Ph.D., Associate Professor,
Kaluga State University named after K. E. Tsiolkovsky
Kaluga, Russia

Abstract: The security of virtual private servers (VPS) is an essential aspect of their operation. The article discusses the main security measures, including password policy, configuring connection using SSH keys, disabling remote root access, installing Fail2Ban, regular software updates and backups. Recommendations are given on how to implement each measure for optimal server protection.
Keywords: VPS security, server protection, information security, update, password policy, software, backup, SSH, Fail2Ban.

Любой ресурс, имеющий доступ к возможностям Интернета, неизбежно подвергается риску атак со стороны ботов, хакеров и других злоумышленников. Особенно это касается виртуальных и выделенных серверов (VPS/VDS). Хотя провайдеры могут предлагать базовый уровень защиты за дополнительную плату, такие как мониторинг и фильтрация трафика, но безопасность настроек самого сервера остается на ответственности пользователя.

Обеспечение безопасности бесплатно и требует минимальных временных вложений, если следовать базовым рекомендациям. Далее будут рассмотрены простые шаги по повышению безопасности VPS, а также более сложные методы, которые обеспечат дополнительную защиту. Все команды приведены для операционной системы Ubuntu.

При аренде сервера провайдер обычно выдаёт ip вашего сервера и сгенерируемый пароль, содержащий цифры и буквы разного регистра, который используется для подключения к VPS через root. Хотя такие пароли достаточно надежны, практика показывает, что пользователи нередко упрощают их, для простоты ввода и запоминания. Это приводит к созданию простых паролей,

которые не соответствуют минимальным требованиям безопасности. Более того, один и тот же пароль часто используется для нескольких серверов или сервисов, таких как электронная почта или социальные сети.

Для обеспечения безопасности необходимо следовать следующим требованиям:

– Необходимо менять пароль для VPS/VDS не реже одного раза в три месяца.

– Пароль должен содержать не менее 12 символов, включая в себя цифры, буквы верхнего и нижнего регистра, а также специальные символы.

– Для генерации случайного и надёжного пароля можно воспользоваться утилитой openssl. При помощи команды «openssl rand -base64 14» можно создать надёжный пароль, где «base64» - это система счисления, а «14» – это количество символов.

– Настроить вход по SSH-ключам и запретить вход по паролям для максимальной безопасности, что будет рассмотрено далее.

Если пароль вполне возможно подобрать (особенно простой), то с SSH-ключом такое почти невозможно [2], поэтому, если имеется такая возможность, использовать именно этот способ подключения к серверу. Использование SSH-ключей также избавляет от необходимости запоминания сложных паролей и упрощает автоматизацию задач, так как SSH-ключ хранится на компьютере. Пример созданного публичного и закрытого ключа представлен ниже (рис. 1). Кроме того, SSH обеспечивает шифрование всего трафика, позволяя выбрать алгоритм шифрования, что значительно повышает уровень безопасности.

```
Private Key:
-----BEGIN EC PRIVATE KEY-----
MIHcAgEBBEIAemR/zfAT2rWmG9A4wXzdTsjdDOH9Kn7XsgDVtE4qCDUZlYoFSKaF
2pruEUUOFpy82mnw5Tcu1hDQ1O1CAgfLPe+gBwYFK4EEACOhgYkDgYYABADxHzLW
hxOxHiY9xG3ZFZW3QOocFduShElluTKmvMT8yvc44gNAh7AffqCFnJlirKOOG15V
Cr+rPKDJBzzbZDXDNwCIyVF96VI4tZj4nCcdV16HXVTS6c35HFAFsQnV8+qkdWyL
BqAmz9FpA48AeYUs4GSKkeMRHkHcRu3uUR1sL3nnSg==
-----END EC PRIVATE KEY-----

Public Key:
ecdsa-sha2-nistp521
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAAIbmlzdHA1MjEAAACFBADxHzLWhxOxHiY9xG3ZFZW3QOocFduShEllu
TKmvMT8yvc44gNAh7AffqCFnJlirKOOG15VCr
+rPKDJBzzbZDXDNwCIyVF96VI4tZj4nCcdV16HXVTS6c35HFAFsQnV8+qkdWyLBqAmz9FpA48AeYUs4GSKkeMRHkH
cRu3uUR1sL3nnSg==
```

Рис. 1. Пример приватного и публичного ключа SSH

SSH-ключ представляет собой связку из публичного и приватного ключей (длиной до 4096 бит). Публичный ключ хранится на удаленном сервере, а приватный — на локальной машине пользователя. При попытке подключения сервер генерирует случайную строку и шифрует её с использованием публичного ключа, после чего отправляет обратно клиенту. Расшифровать её можно только используя приватный ключ.

Для того чтобы сгенерировать новый SSH- ключ необходимо ввести команду «ssh-keygen -t rsa», после чего можно ввести имя ключа и passphrase (дополнительная защита ключа паролем). При завершении генерации на компьютере появятся 2 файла: id_rsa - приватный ключ (хранится у пользователя локально) и id_rsa.pub — публичный ключ, который необходимо отправить на сервер. После передачи ключа можно подключаться к серверу по SSH без использования пароля, выполнив команду «ssh root@<IP-адрес сервера> -p <номер порта SSH>».

По умолчанию SSH использует порт 22, но для защиты от ботов (которые в основном ориентированы на стандартные порты) рекомендуется сменить номер порта на любой другой не занятый. Дополнительно следует отключить все

неиспользуемые порты, чтобы минимизировать потенциальные точки для атак на сервер.

Ещё одной важной мерой базовой защиты (в том числе от ботов) является отключение возможности входа под учетной записью root. Так как root-пользователь присутствует на большинстве серверов и обладает максимальными правами в системе — это делает его основной целью для многих атак. Важно помнить, что перед перед отключением доступа к root необходимо создать пользователя с достаточными привилегиями для управления сервером, иначе после завершения операции доступ к серверу будет невозможен. Для отключения необходимо отрыть файл конфигурации SSH для редактирования: «nano /etc/ssh/sshd_config» и изменить параметр PermitRootLogin на «no», после чего необходимо перезапустить SSH командой «service ssh restart». Стоит учесть, что что отключение удаленного доступа к root касается исключительно подключения по протоколу SSH, что даёт возможность добавить другого пользователя в группу sudo и при необходимости использовать команду «sudo su» для выполнения задач от имени root.

Для защиты сервера от атак типа «Brute Force» или «Denial of Service» следует установить программный пакет Fail2Ban [1]. Утилита осуществляет мониторинг журнала авторизации, благодаря чему выявляет ip-адреса, с которых осуществляется большое количество неудачных попыток входа на сервер. При обнаружении таких действий утилита автоматически создаёт правило для брандмауэра, блокирующее трафик подозрительного IP-адреса, добавляя его в чёрный список. Для установки Fail2Ban необходимо выполнить команду: «sudo apt install fail2ban». Утилита обладает широкими возможностями для настройки параметров, которые реализуются через конфигурационные файлы, расположенные в каталоге /etc/fail2ban. Перед внесением изменений в конфигурацию рекомендуется создать копию основного конфигурационного файла, а все изменения вносить в созданную копию, избегая прямой модификации исходного файла. Это обеспечит возможность отката к исходным

настройкам в случае ошибки. Для применения изменений необходимо перезапустить Fail2Ban. Это можно сделать с помощью команды: «/etc/init.d/fail2ban restart».

Для поддержания безопасности VPS важно своевременно обновлять программное обеспечение на сервере, так как обновления и патчи обычно выпускаются специально для устранения выявленных уязвимостей. Актуальная версия ПО значительно усложняет возможность реализации атак и эксплоитов злоумышленником.

Для сервера на основе операционной системы Ubuntu обновление осуществляется выполнением всего двух команд: «sudo apt update» и «sudo apt update» [3], первая актуализирует список пакетов ПО, а вторая запустит процесс их установки.

Пользователи делятся на два типа: те, которые делает бэкапы и те, которые уже делает бэкапы. Резервное копирование (бэкап) является важным элементом защиты и обеспечения стабильной работы VPS, так как оно необходимо для предотвращения потери данных, которая может произойти из-за аппаратных или программных сбоев, кибератак, ошибок, вызванных человеческим фактором. Процесс резервного копирования включает создание копий данных, их сохранении в безопасных местах (локальные носители, облачные хранилища или другие удалённые серверы) и возможность их восстановления в случае необходимости [4].

Существует два глобальных подхода при организации резервного копирования:

1. Настройка создания бэкапов всей системы или критической её части через панель управления. Метод позволяет хранить резервную копию непосредственно на сервере или в облачных хранилищах (рекомендуется хранить одновременно в нескольких местах). Он прост в реализации и почти не требует финансовых вложений, однако необходимо периодически

контролировать свободное пространство на диске, необходимое для создания очередной копии.

2. Покупка услуги резервного копирования у провайдера. Данная услуга обычно стоит около 500 рублей в месяц за ежедневное резервное копирование, при этом вся ответственность за копирование и хранение данных возлагается на провайдера.

Также стоит обратить внимание что описанные подходы можно и нужно комбинировать для получения максимальной надёжности системы.

Оптимизация парольной политики, использование SSH-ключей вместо паролей и внедрение утилиты Fail2Ban значительно снижают вероятность успешных атак. Регулярное обновление программного обеспечения и создание резервных копий обеспечивают дополнительный уровень защиты и готовность к нештатным ситуациям. Комбинирование перечисленных методов позволяет создать устойчивую и надёжную систему, минимизирующую риски и обеспечивающую стабильную работу серверной инфраструктуры.

Библиографический список

1. Fail2Ban Documentation. Официальная документация Fail2Ban [Электронный ресурс]. Режим доступа: https://www.fail2ban.org/ (дата обращения: 25.01.2025).

2. OpenSSH Project. Руководство по SSH и настройке ключей [Электронный ресурс]. Режим доступа: https://www.openssh.com/ (дата обращения: 17.01.2025).

3. Ubuntu Documentation. Ubuntu Server documentation [Электронный ресурс]. Режим доступа: https://ubuntu.com/server/docs (дата обращения: 12.01.2025).

4. Резниченко О. С., Клименко Н. А. Разработка рекомендаций для реализации мер по обеспечению информационной безопасности веб-интерфейсов пользователей для систем поддержки принятия решений // Управление в XXI веке : сб. статей по материалам Междунар. науч.-практ. конф., НИУ «БелГУ», 23 окт. 2015 г. НИУ «БелГУ»: Издательский дом «Белгород», 2015. – С. 379–382.

Оригинальность 77%