Как защитить сервер: 6 практических методов

Любая IT-инфраструктура нуждается в надежной защите. Информационная безопасность — это тема, которую не охватить за пару уроков. Однако существует некоторый минимум, который поможет защититься от атак непрофессиональных хакеров и ботов. В этой статье рассмотрим, как защитить сервер, используя 6 несложных методов.

Инструменты и методы защиты

Обеспечение защиты сервера от взлома всегда включает комплекс различных мер. Условно методы можно разделить на следующие направления:

- Защита каналов связи, через которые осуществляется администрирование и использование системы.
- Организация нескольких уровней безопасности системы.
- Разграничение доступа к ресурсам инфраструктуры.
- Мониторинг и аудит систем.
- Резервное копирование.
- Своевременные обновления (или откаты) ПО.
- Антивирусная защита серверов.

Далее рассмотрим 6 практических методов, позволяющих получить уровень защиты, который не по зубам непрофессиональным взломщикам и ботам.

Разграничение привилегий

При организации доступа к ресурсам следуйте универсальному правилу — процессы и пользователи должны иметь доступ только к тем ресурсам, которые минимально необходимы для работы. Особенно это касается баз данных и операционных систем. Принцип наименьших привилегий поможет наладить защиту сервера от несанкционированного доступа извне, минимизировав ущерб, а также от внутренних угроз.

Для каждого администратора лучше всего создать отдельную учетную запись, а операции, не требующих повышенных прав, нужно выполнять с непривилегированных аккаунтов. При использовании среды Microsoft Active Directory периодически проводите проверки и конфигурирование групповых политик, так как такой механизм в руках злонамеренного администратора или хакера может привести к серьезным нарушениям безопасности.

При работе с *nix системами не следует постоянно работать под учетной записью `root`. Лучше всего ее отключить и использовать программу `sudo`. Настройки `sudo` можно изменить в файле `/etc/sudoers` или командой `visudo`. Приведем две полезные директивы `defaults`, которые помогут следить за тем, кто что делает через `sudo`.

По умолчанию лог пишется в `syslog`. Следующая настройка (файл `/etc/sudoers`) аккумулирует записи в отдельный файл для удобства:

```
Defaults log_host, log_year, logfile="/var/log/sudo.log"
```

Этот параметр заставляет sudo записывать текст сеанса работы (лог команд, сообщения `stdin`, `stderr`, `stdout` и лог с `tty/pty`) в директорию `/var/log/sudo-io`:

```
Defaults log_host, log_year, logfile="/var/log/sudo.log"
```

Мандатное управление доступом

Следующий совет касается Linux-систем и связан с предыдущим. Многие linux-админы довольствуются дискреционными механизмами разграничения доступа, которые являются основными и всегда активны. Между тем во многих дистрибутивах (AppArmor в Ubuntu, SELinux в RHEL-based системах) имеются механизмы мандатного управления. Они требуют более сложной настройки ОС и сервисов, зато позволяют детально разграничить доступ к объектам файловой системы, обеспечивая более надежную программную защиту сервера.

Удаленное администрирование ОС

При удаленном администрировании операционной системы используйте безопасные протоколы. Для Windows таким считается RDP, в Linux — SSH. Хоть эти протоколы и являются надежными, можно дополнительно усилить защиту.

Для RDP желательно заблокировать подключения учетных записей с пустым паролем. Сделать это можно через «Локальные политики безопасности» и параметр «Учетные записи:

Разрешить использование пустых паролей только при консольном входе». Если не используется VPN, RDP-сессии можно защитить безопасным транспортным протоколом TLS, речь о котором пойдет чуть позже.

По умолчанию, проверка личности пользователя в SSH происходит по паролю. Установив аутентификацию по SSH-ключам, вы повысите защиту сервера, так как длинный ключ значительно сложнее подобрать, к тому же не придется вводить пароль (ключ хранится на сервере). Настройка ключей требует всего несколько простых шагов:

Генерация пары ключей на локальной машине:

```
ssh-keygen -t rsa
```

Размещение ключей на удаленной станции:

```
ssh-copy-id логин@адрес
```

Если не хотите использовать ключи, присмотритесь к программе Fail2ban, которая ограничивает число попыток ввода пароля и блокирует IP-адреса. Также же не лишним будет поменять порты по умолчанию: 22/tcp для SSH, 3389/tcp для RDP.

Настройка фаервола

Правильная система безопасности состоит из уровней. Не стоит надеяться только на механизмы разграничения доступа. Логичней контролировать сетевые соединения до того, как они доберутся до сервисов. Для этого существуют файрволы.

Межсетевой экран (брандмауэр или файрвол) обеспечивает контроль доступа на уровне сети к участкам инфраструктуры. Руководствуясь определенным набором разрешающих правил, файрвол определяет, какой трафик пропускать через периметр. Все, что под правила не попадает, блокируется. Следует заметить, что в Linux, брандмауэр является частью ядра (netfilter), поэтому для работы в пользовательском пространстве необходимо установить фронтенд: nftables, iptables, ufw или firewalld.

Первое, что нужно сделать при настройке фаервола — закрыть неиспользуемые порты и оставить только те, к которым предполагается доступ извне. Например, для веб-сервера это порт 80 (http) и 443 (https). Ничего кардинально опасного в открытом порту нет (угроза может быть в программе, стоящем за портом), но все же лучше убрать лишнее.

Помимо обеспечения внешнего периметра безопасности, межсетевые экраны помогают разделить инфраструктуру на сегменты и контролировать трафик между ними. Если у вас имеются общедоступные сервисы, подумайте, можно ли их изолировать от внутренних ресурсов (DMZ). Также советуем присмотреться к системам обнаружения и предотвращения

вторжений (IDS/IPS). Этот вид решений работает по обратному принципу — заблокировать проблему безопасности, все остальное пропустить.

Виртуальные частные сети

До этого мы рассматривали, как защитить сервер от взлома. Теперь рассмотрим защиту нескольких серверов. Сейчас виртуальные частные сети (VPN) чаще всего применяют в качестве анонимайзера и инструмента доступа к недоступным ресурсам. Однако основное их назначение – безопасное объединение сетей филиалов организаций. В своей сути VPN представляет собой логическую сеть поверх другой сети (например, Интернет). Безопасность обеспечивается средствами криптографии, поэтому защищенность соединений не зависит от безопасности базовой сети.

Существует множество VPN-протоколов. Выбор зависит от размеров организации, сети и требуемого уровня безопасности. Для маленькой фирмы и домашней локальной сети подойдет классический PPTP: почти на любом роутере или телефоне есть возможность настроить pptp. Из недостатков можно отметить устаревшие методы шифрования. Для высокого уровня защищенности и соединений типа сеть-сеть подходящим будут протоколы IPsec, для соединений сеть-узел — OpenVPN и WireGuard Однако они требуют более тонкой настройки, в отличие от PPTP.

TLS и инфраструктура открытых ключей

Многие протоколы прикладного уровня разрабатывались во времена, когда сети не выходили за пределы институтов и военных учреждений, а web еще не изобрели. HTTP, FTP, SMTP и другие популярные протоколы передают данные в виде обычного текста. Если хотите обеспечить защиту сайта, веб-панели управления внутренним сервисом или почты, используйте TLS.

TLS — это протокол защиты транспортного уровня, предназначенный для безопасной передачи данных в небезопасной сети. Хоть вместе с TLS часто встречается название SSL (SSL-сертификат, пакет OpenSSL), учитывайте, что современной версией протокола является TLS 1.2/1.3. Ранние версии TLS и протокол-предшественник SSL считаются устаревшими.

TLS позволяет обеспечить приватность, целостность данных и аутентификацию ресурса. Последнее достигается с помощью цифровой подписи и инфраструктуры открытых ключей (PKI). PKI работает следующим образом: подлинность сервера определяется SSL-сертификатом, который подписывается удостоверяющим центром (CA). Сертификат центра

в свою очередь подписывается вышестоящим CA и так далее по цепочке. Сертификаты корневого центра являются самоподписанными, то есть доверие к ним подразумевается по умолчанию.

TLS также можно использовать вместе с VPN, например настроить авторизацию клиентов по SSL-сертификатам или TLS handshake. В таком случае необходимо внутри локальной сети самостоятельно организовать инфраструктуру открытых ключей (сервер CA, ключи и сертификаты узлов).

Чем опасны взломщики?

Степень опасности угрозы зависит от ее вида. Атаки условно делятся на несколько видов.

Первый вид связан с проникновением за периметр безопасности. В этом случае злоумышленник получает доступ к учетной записи авторизованного пользователя сервиса или системы, например базы-данных. Угрозу представляют взломы привилегированных аккаунтов, так как в руки хакера попадают средства просмотра секретной информации и изменения параметров системы. Критически опасная разновидность «проникновения» — несанкционированный доступ к учетной записи суперпользователя операционной системы. В подобной ситуации под удар попадает большая часть инфраструктуры.

Другой вид атак нацелен на вывод системы из строя. Подобные угрозы не подразумевают утечек данных, но это не делает их менее опасными. Самая показательная атака такого рода — DoS и DDoS. Их суть заключается в том, что злоумышленники нагружают сервер лавиной обращений. Рабочий сервер не справляется с нагрузкой и перестает отвечать на запросы пользователей. Иногда DoS бывает подспорьем для осуществления других атак.

Результатами атак часто становится утечки данных, финансовый и репутационный ущерб, поэтому при налаживании IT-инфраструктуры важно продумать хотя бы минимальный уровень безопасности.

Revision #1
Created 2023-10-24 18:15:59 UTC by odiljonov
Updated 2023-10-24 18:16:24 UTC by odiljonov