positive technologies

Руководство по защите Zabbix 7

Москва, 2024

Содержание

1. Введение

Наша команда состоит из экспертов в области построения защищенных ИТ-инфраструктур, и мы рады поделиться своим опытом с широким кругом специалистов.

ХардкорИТ — это подход, в основе которого лежит методология определения путей и времени атаки хакера с помощью анализа ИТ-инфраструктуры. Он позволяет быстро и эффективно оценить уровень защищенности конкретных ИТ-систем, критически важных для бизнеса, и сделать организацию киберустойчивой.

В условиях постоянного роста киберугроз и необходимости обеспечения надежной защиты данных критически важно оценить текущее состояние безопасности используемого программного обеспечения и его конфигураций. Наш подход во многом основан на харденинге.

Харденинг — это процесс повышения киберустойчивости, который означает способность организации продолжать свою деятельность и быстро восстанавливаться после кибератак. Харденинг включает в себя действия, направленные на укрепление защиты информационной системы, такие как:

- отключение неиспользуемых функций;
- изменение настроек по умолчанию;
- устранение уязвимостей;
- обновление компонентов.

Эти меры помогают уменьшить цепочку шагов для атакующих, замедлить продвижение, что в конечном итоге делает атаку очень дорогой для злоумышленника и снижает вероятность ее реализации.

Документ предназначен для специалистов в сферах ИТ и ИБ разного профиля: руководителей, архитекторов и инженеров.

Документ включает в себя:

- описание типовой архитектуры, наиболее популярной для компаний с менее чем 5000 узлов;
- описание механизмов повышения защищенности ПО без применения наложенных средств защиты;
- расчет метрики time to attack для настроек по умолчанию и рекомендованного профиля защиты;
- описание влияния параметров защиты на функциональность и производительность.

Документ не включает описаний использования наложенных средств защиты и харденинга на уровне операционной системы.

В качестве таксономии для действий по выявлению и предотвращению атак используется общепризнанный регулярно обновляемый источник — матрица тактик и техник злоумышленников MITRE ATT&CK Enterprise. В создании и обновлении справочника участвует большое международное сообщество экспертов и вендоров. Техники, описанные в матрице, легко

декомпозируются в гранулярные параметры проверки. Акцент сделан на использовании встроенных защитных механизмов ИТ-активов, построении сети и минимальном применении средств защиты информации.

2. Проблематика защиты Zabbix 7

2.1. Покрытие рынка

По данным с официального сайта система мониторинга Zabbix ежегодно скачивается более 4 млн раз в год.

2.2. Статистика по уязвимостям

Существует несколько источников об уязвимостях Zabbix.

Официальный портал Zabbix[1] 1 насчитывает 34 CVE (1 критически опасная* за 2023–2024 годы).

Портал NIST1[1] 2 содержит информацию о 32 CVE (1 критически опасная* за 2023–2024 годы).

Портал Mitre1[1] 3 содержит информацию о 26 CVE (1 критически опасная* за 2023–2024 годы).

2.3. Архитектурные особенности

Система мониторинга Zabbix имеет клиент-серверную архитектуру, поэтому одна из наиболее уязвимых особенностей Zabbix — возможность исполнения команд на узлах, имеющих доступ со стороны сервера, и более того —исполнение вредоносных команд на узлах, доступных через узлы с установленным Zabbix-агентом.

Система мониторинга Zabbix состоит из следующих компонентов:

- Zabbix Server,
- Zabbix Frontend[2],
- Zabbix Agent,
- Zabbix Proxy,
- Zabbix Java Gateway,
- Zabbix Web Service,
- СУБД[3].

[1] Оценка CVSS выше 9

[2] Zabbix Frontend не являются компонентом самой системы мониторинга, но необходим для ее работы.

[3] СУБД не являются компонентом самой системы мониторинга, но необходим для ее работы.

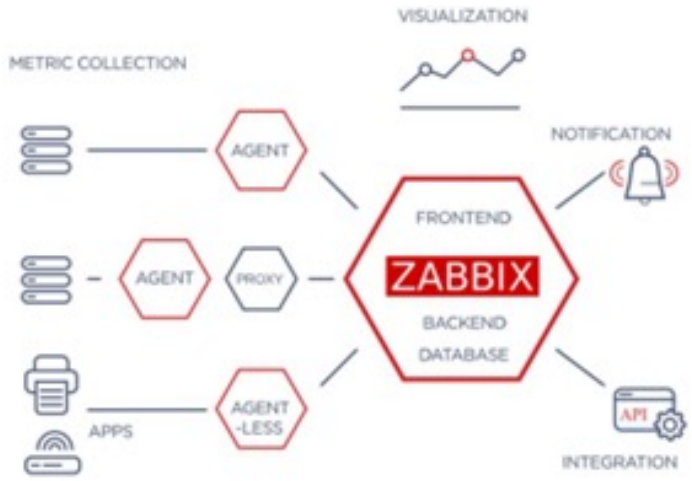

Рисунок 1. Система мониторинга Zabbix

Управление узлами происходит через веб-интерфейс или API, поэтому все перечисленные модули требуют особого внимания при настройке параметров безопасности.

3. Недопустимые события Zabbix 7

Zabbix не является целевой системой, но может быть ключевой системой для получения доступа к целевым.

Взлом Zabbix может привести к утечке информации об архитектуре сети и используемом оборудовании, что поможет злоумышленникам выявить уязвимости, позволяющие получить доступ к целевой системе.

4. Пример типовой инсталляции Zabbix 7

Zabbix предоставляет несколько вариантов установки системы мониторинга:

- установка из репозиториев на ОС Linux;
- контейнеры;
- образы для облачной инсталляции;
- готовые образы для локальной установки;
- сборка из исходного кода.

Рекомендации не привязаны к конкретному способу инсталляции или к ОС и не зависят от значений параметров по умолчанию.

4.1. Описание типовой инсталляции

Zabbix-сервер является основным компонентом системы мониторинга Zabbix. Он отвечает за сбор данных от агентов Zabbix, за обработку и хранение данных, а также за выполнение различных административных функций.

Основные компоненты Zabbix-сервера:

- Zabbix Agent — отвечает за сбор данных;
- Zabbix Server — обрабатывает данные и выполняет различные административные функции;
- СУБД — хранит собранные данные и конфигурационные данные сервера;
- Zabbix Frontend — обеспечивает графическое представление данных и возможность управления сервером.

Управление Zabbix-сервером осуществляется через веб-интерфейс Zabbix, который предоставляет доступ к функциям настройки, мониторинга и управления агентами, узлами и трендами.

Агенты Zabbix являются программными компонентами, устанавливаемыми на отслеживаемые устройства или серверы. Они отвечают за сбор данных о состоянии и производительности устройств и отправку этих данных на Zabbix-сервер. Агенты Zabbix могут быть настроены для сбора различных типов данных, таких как данные об использовании ЦПУ, памяти, о загрузке сети, о состоянии служб и т. д.

Zabbix-сервер представляет собой мощный инструмент для мониторинга производительности и состояния сетевых устройств и серверов. Он позволяет получать информацию о работе инфраструктуры в реальном времени и реагировать на возникающие проблемы, а также проводить прогнозирование и планирование обслуживания.

5. Проблемы безопасности типовой инсталляции

Типовая инсталляция системы мониторинга зачастую обладает следующими проблемами с точки зрения безопасности:

- отключен TLS для доступа к веб-интерфейсу;
- используются типовые значения для доступа к СУБД;
- задан пароль администратора веб-интерфейса по умолчанию;
- не используется SSL для связи с агентами.

В типовом варианте инсталляции архитектуры выглядит подобным образом:

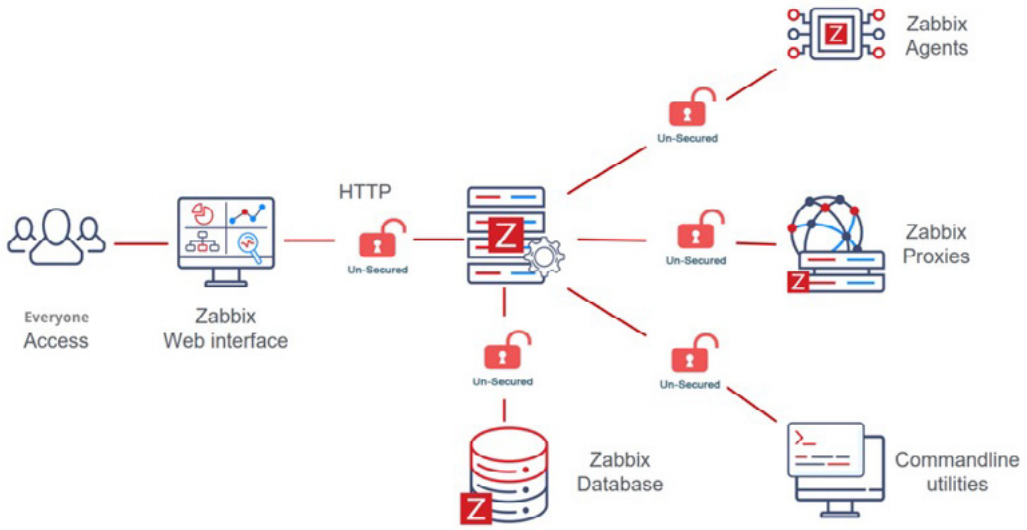

Рисунок 2. Архитектура безопасности типовой инсталяции.

Для атак на типовую инсталляцию системы мониторинга на базе Zabbix могут быть применены 14 тактик и более 160 техник из матрицы MITRE ATT&CK. Чтобы применить эти техники, атакующему достаточно обладать квалификациями киберхулигана или энтузиаста-одиночки.

6. Расчет времени проникновения для инсталляции с параметрами по умолчанию

При установленных параметрах по умолчанию злоумышленнику доступно более десяти маршрутов с минимальным временем атаки 14,69 часов.

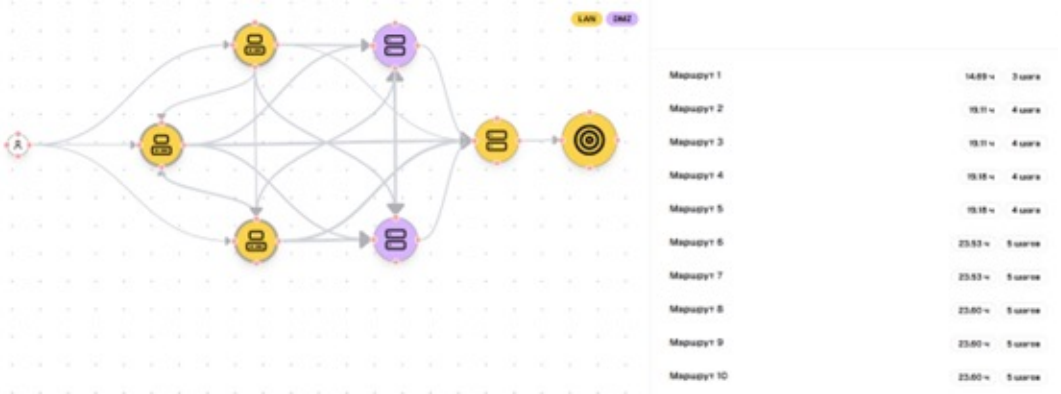

Рисунок 3. Путь атакующего до применения рекомендаций по защищённости

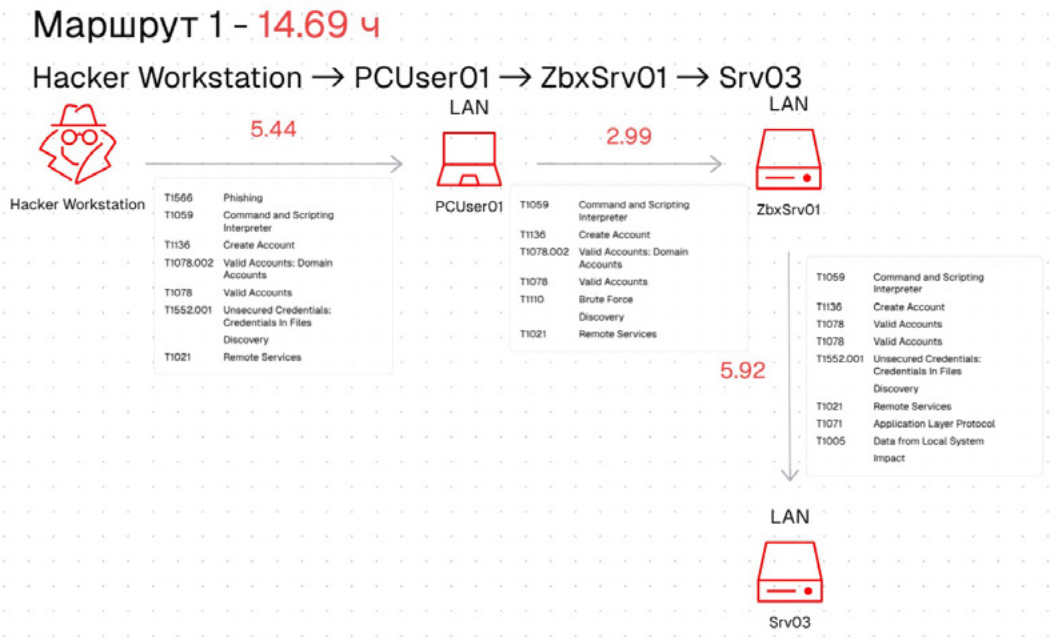

Рисунок 4. Путь атакующего до применения рекомендаций по защищённости с детализацией по техникам

7. Рекомендации по повышению защищенности

Повышение защищенности означает увеличение времени и/или количества шагов, необходимых для проведения атаки на систему.

Рекомендация	**Защитные меры из матрицы MITRE ATT&CK**
Использовать TLS для связи с Zabbix-сервером	M1041 Encrypt Sensitive Information
Использовать LDAPS для авторизации пользователей в веб-интерфейсе	
Использовать TLS для доступа к веб-интерфейсу[1]	
Не использовать связку логин-пароль по умолчанию для авторизации в веб-интерфейсе и для подключения к СУБД	M1026 Privileged Account Management
Запускать агент от имени непривилегированного пользователя	
Запретить выполнение скриптов на узле через Zabbix, если этого не требуется для шаблонов мониторинга	

[1] Настройка производится на стороне веб-сервера, не являющегося компонентом системы мониторинга Zabbix, но напрямую влияет на безопасность системы.

Рекомендация	Защитные меры из матрицы MITRE ATT&CK
Ограничить доступ к базе данных по IP-адресу Zabbix-сервера, если база расположена на другом узле, или только локальным адресом, если она расположена на локальном узле[2]	M1037 Filter Network Traffic
Ограничить доступ к веб-интерфейсу и API Zabbix-сервера по IP-адресам устройств администраторов1	
Использовать LDAPS для авторизации пользователей в веб-интерфейсе	M1036 Account Use Policies
Проводить регулярные обновления Zabbix-сервера и Zabbix-агентов	M1051 Update Software
Настроить MFA для авторизации пользователей Zabbix в веб-интерфейсе	M1032 Multi-factor Authentication
Использовать Zabbix-прокси в сегментах сети с повышенной угрозой (DMZ) в режиме passive	M1031 Network Intrusion Prevention M1030 Network Segmentation
Использовать HashiCorp Vault или CyberArk Vault CV12 для хранения паролей[3]	M1043 Credential Access Protection
Отправлять журналы на удаленный узел для дальнейшего анализа	M1029 Remote data storage
Запретить запуск произвольных скриптов при помощи AlertScripts	M1038 Execution Prevention M1042 Disable or Remove Feature or Program
Проверить права на бинарные и конфигурационные файлы Zabbix-сервера, Zabbix-агента и Zabbix-прокси	M1022 Restrict File and Directory Permissions

Таблица 1. Соответствие рекомендаций защитным мерам из матрицы MITRE ATT&CK

7.1. Использование TLS для связи с Zabbix-сервером

Zabbix поддерживает шифрование соединений между Zabbix-сервером, Zabbix-прокси, Zabbix-агентом, утилитами zabbix_sender и zabbix_get с использованием протокола TLS 1.2. Использование шифрования позволит избежать перехвата и подмены данных. Кроме того, поддерживается работа с защищенными каналами связи с СУБД.

Исходящие соединения (пассивные) могут быть зашифрованы одним из способов на выбор. Для входящих соединений доступны любые варианты: без шифрования, PSK или сертификат.

Utilities Encryption (Zabbix Documentation) 4

Mysql Encryption (Zabbix Documentation) 5

PostgreSQL Encryption (Zabbix Documentation) 6

[2] Настройка производится на стороне СУБД MySQL или PostgreSQL, не являющегося компонентом системы мониторинга Zabbix, но напрямую влияет на безопасность системы.

[3] Zabbix не предоставляет компоненты для безопасного хранения «секретов», поэтому, согласно официальной документации, рекомендуется использование сторонних средств.

Примеры конфигурации в режиме PSK:

Для настройки Zabbix-агента измените конфигурационный файл следующим образом.

В случае использования Zabbix-прокси измените конфигурационный файл следующим образом.

Активный режим работы прокси:

```
TLSConnect=psk
TLSAccept=psk
TLSPSKIdentity=PSK_Number
TLSPSKFile=/path/to/file_with_psk.psk
```

Пассивный режим работы прокси:

```
TLSConnect=psk
TLSPSKIdentity=PSK_Name
TLSPSKFile=/path/to/file_with_psk.psk
```

Для использования zabbix_sender и zabbix_get TLS будет выглядеть так:

```
TLSAccept=psk
TLSPSKIdentity=PSK_Name
TLSPSKFile=/path/to/file_with_psk.psk
```

```
zabbix_sender -z 127.0.0.1 -s zabbix02 -k Encrypt -o 18 –tls-connect psk –tls-psk-identity «PSK_Name» –tls-psk-file /path/to/file_with_psk.psk

zabbix_get -s 127.0.0.1 -k agent.version \

–tls-connect psk –tls-psk-identity «PSK_Name» –tls-psk-file /path/to/file_with_psk.psk
```

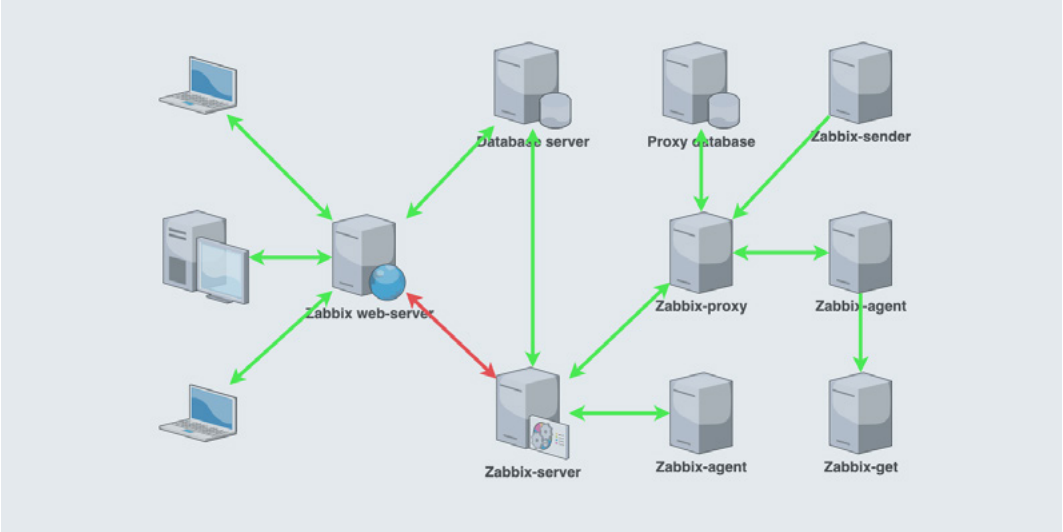

Рисунок 5. Информационные потоки, которые подлежат шифрованию (обозначены зелёным цветом).

Известные проблемы: нет

Снижение производительности: при большом количестве данных может возникать дополнительная нагрузка на ЦПУ.

7.2. Использование LDAPS для авторизации пользователей в веб-интерфейсе

LDAPS обеспечивает шифрование данных между клиентом и сервером, что защищает конфиденциальную информацию от потенциальных злоумышленников. Данные передаются в виде зашифрованных пакетов. Это делает их недоступными для перехвата и анализа — в отличие от LDAP, где пакеты передаются в открытом виде.тоздесь

Помимо шифрования LDAPS позволяет клиенту проверять подлинность сервера LDAP перед передачей конфиденциальной информации. Это обеспечивает обращение к правильному серверу и защиту от атак «человек посередине».

Известные проблемы: нет

Снижение производительности: нет

7.3. Использование TLS для доступа к веб-интерфейсу спользование выделенного хранилища под резервные копии

Для настроек веб-сервера nginx обратитесь к официальной документации на сайте nginx [7].

Выпустите или получите заранее выпущенный SSL-сертификат. Укажите путь до файла сертификата и приватного ключа в секции server необходимого домена:

```
server {
...
    ssl_certificate     www.example.com.crt;
ssl_certificate_key www.example.com.key;
```

Измените значение директивы listen с порта 80 на порт 443 и при необходимости укажите принудительное использование SSL.

```
server {
    listen          443 ssl;
...
```

Настройте redirect с HTTP на HTTPS для необходимого домена.

```
server {
listen 80;
...
    return 301 https://$host$request_uri;
}
```

Apache Documentation [8]

Если в качестве веб-сервера используется Apache, то конфигурация должна содержать следующие настройки.

```
<VirtualHost ...>
  <Location />
  Order deny,allow
  Deny from all
  Allow from xxx.xxx.xxx.xxx
  </Location>
  ...
</VirtualHost>
```

Известные проблемы: нет

Снижение производительности: использование TLS может привести к дополнительной нагрузке на ЦПУ, однако веб-интерфейс Zabbix — не настолько интенсивно используемая часть системы, чтобы включение TLS смогло существенно повлиять на производительность

.

7.4. Запрет на использование связки логин-пароль по умолчанию для авторизации в веб-интерфейсе и для подключения к СУБД

Имя базы и логин для доступа к ней имеют стандартное значение при типовой установке. Стандартные значения могут быть легко угаданы злоумышленниками, что может привести к уменьшению времени, необходимого для взлома системы.

Известные проблемы: нет

Снижение производительности: нет

7.5. Запуск агента от имени непривилегированного пользователя

Не запускайте Zabbix-агент под суперпользователем. Рекомендуем использовать иного пользователя с минимально необходимыми правами в соответствии с требованиями шаблонов

мониторинга для конкретного узла. В случае недостатка прав для выполнения сбора данных выдавайте возможность повышения прав точечно, например при помощи настройки sudoers.

Известные проблемы: если у непривилегированного пользователя недостаточно прав для выполнения команды или доступа к файлу, то эта рекомендация может вызывать ограничение функциональности.

Снижение производительности: нет

7.6. Запрет на выполнение комманд на узле через Zabbix, если этого не требуется для шаблонов мониторинга

В zabbix_agentd.conf присвойте параметру EnableRemoteCommands значение 0. Параметру UnsafeUserParameters в явном виде также необходимо присвоить значение 0.

EnableRemoteCommands (Zabbix Documentaion) [9]

UnsafeUserParamaters (Zabbix Documentation) [10]

Известные проблемы: в случае использования шаблонов, которые требуют запуск сторонних скриптов, могут возникнуть ограничения функциональности.

Снижение производительности: нет

7.7. Ограничение доступа к базе данных по IP-адресу Zabbix-сервера, если она расположена на другом узле, или только локальным адресом, если она расположена на локальном узле

Установите фильтрацию для доступа к базе данных, как минимум со стороны СУБД. Ограничьте возможность подключения только со стороны Zabbix-сервера. В случае установки на локальном ПК разрешите подключение только с локального узла или через сокет.

В случае использования MySQL необходимо указать IP-адрес в формате ‘имя пользователя’@’IP-адрес Zabbix сервера’, используя оператор CREATE при создании нового пользователя или ALTER при изменении существующего.

```
CREATE USER ‘newuser’@’localhost’

ALTER USER ‘olduser’@’%’
```

Если используется PostgreSQL, то необходимо отредактировать файл pg_hba.conf в следующем формате:

```
host database newuser IP_ADDRESS/32 md5
```

Для доступа к MySQL только при помощи сокета необходимо указать путь до него в параметре bind-address файла my.cnf:

```
bind-address = IP_ADDRESS//var/lib/mysql/mysql.sock
```

Аналогично для PostgreSQL, но название параметра — listen_addresses, а файла — postgresql.conf:

```
listen_addresses = '/var/run/postgresql'
```

Известные проблемы: в случае использования базы Zabbix сторонними ресурсами в качестве источника их работоспособность может быть нарушена.

Снижение производительности: нет

7.8. Ограничение доступа к веб-интерфейсу и API Zabbix-сервера по IP-адресам устройств администраторов

Установите фильтрацию со стороны веб-сервера для доступа к веб-интерфейсу и API. Разрешите подсети или точечные адреса, где находятся рабочие станции потенциальных пользователей системы мониторинга.

При использовании nginx необходимо задействовать модуль ngx_http_access_module, а именно директоры allow и deny, следующим образом.

```
    ...
location / {
    allow 192.168.1.0/24;
    allow 10.10.0.186/32;
    deny  all;
}
    ...
```

Если используется Apache, потребуются модуль mod_authz_host и директива Require. Пример конфигурации приведен ниже.

```
...

Require ip 192.168.1.0/24 10.10.0.186

...
```

Nginx Documentation [11]

Apache Documentation [12]

Известные проблемы: при необходимости доступа к API со сторонних ресурсов следует указать адреса этих ресурсов в списке разрешенных, иначе их работа будет нарушена.

Снижение производительности: нет

7.9. Регулярное обновление Zabbix-сервера и Zabbix-агентов

В системе мониторинга Zabbix регулярно обнаруживаются новые уязвимости, которые чаще всего очень быстро исправляются разработчиками. Регулярное обновление системы позволяет избежать появления уязвимостей, которые могли бы использоваться злоумышленником для взлома.

Известные проблемы: нет

Снижение производительности: нет

7.10. Настройка MFA для авторизации пользователей Zabbix в веб-интерфейсе

Начиная с версии 7.0 Zabbix предоставляет нативные средства для проведения двухфакторной аутентификации пользователей. Рекомендуется включить ее независимо от наличия второго фактора от сторонних поставщиков.

Алгоритм хеширования SHA-1 считается уязвимым. Рекомендуется использовать SHA-256 или SHA-512 для хеширования токена.

Zabbix Documentation [13]

Известные проблемы: требуется возможность использовать OTP или TOTP на устройстве пользователя системы

Снижение производительности: нет

7.11. Использование Zabbix-прокси в сегментах сети с повышенной угрозой (DMZ) в режиме passive

Zabbix-прокси может работать в двух режимах: active и passive.

В активном режиме прокси будет подключаться к серверу Zabbix и запрашивать данные конфигурации.

В пассивном к прокси будет подключаться сервер Zabbix.

Обратите внимание, что при использовании активного прокси данные конфигурации могут стать доступны лицам, имеющим доступ к порту траппера Zabbix-сервера. Такое возможно, потому что кто угодно может представиться активным прокси и запросить данные конфигурации, если аутентификация не выполняется или адреса прокси не ограничены в поле Адрес прокси.

Zabbix Proxy Documentation [14]

Известные проблемы: нет

Снижение производительности: возможно увеличение нагрузки на Zabbix-сервер, так как в таком варианте использования существенная часть работы переносится с прокси на сервер.

7.12. Использование HashiCorp Vault или CyberArk Vault CV12 для хранения «секретов»

На Zabbix-сервере можно зашифровать различные виды данных:

- учетные данные для доступа к внешним ресурсам (база данных, LDAP, active directory);
- ключи доступа к внешним сервисам (API-ключи, токены);
- конфиденциальные параметры конфигурации (например, SSL-сертификаты, ключи шифрования).

По умолчанию все данные в конфигурационных файлах Zabbix-сервера хранятся в формате plain text.

Zabbix CyberAck Documentation [15]

Zabbix HashiCorp Documentation [16]

Известные проблемы: нет

Снижение производительности: нет

7.13. Отправка журналов на удаленный узел для дальнейшего анализа

Передавайте журналы работы сервера Zabbix и веб-сервера на сторонний узел для дальнейшего анализа. Это поможет выявить несанкционированную авторизацию в веб-интерфейсе или API Zabbix-сервера, а также выполнение скриптов и команд не из списка утвержденных.

Известные проблемы: нет

Снижение производительности: эта рекомендация может увеличить нагрузку на сетевой стек и процессор из-за увеличения сетевого трафика.

7.14. Запрет на запуск произвольных скриптов при помощи AlertScripts или ExternalScripts

В Zabbix предусмотрен механизм подключения собственных систем оповещения через запуск скриптов — AlertScripts.

ExternalScripts в Zabbix позволяет добавлять пользовательские скрипты для выполнения различных задач. Этот механизм применяется для захвата узла при наличии уязвимого нотификатора, а также служит одним из способов закрепления в системе.

В zabbix_agentd.conf присвойте параметру AllowRoot значение 0, если установлено иное.

Известные проблемы: при наличии средств оповещения, отличных от стандартных, их работа может быть нарушена.

Снижение производительности: нет

7.15. Проверка прав на бинарные и конфигурационные файлы Zabbix-сервера, Zabbix-агента и Zabbix-прокси

Необходимо регулярно проводить проверку соответсвия прав и владельцев файлов и директорий на соответствие с необходимыми.

Zabbix-агент:

```
/etc/zabbix/zabbix_agentd.conf

/etc/zabbix/zabbix_agentd.d

/usr/sbin/zabbix_agentd

/var/run/zabbix
```

Zabbix-сервер:

```
/etc/zabbix/zabbix_server.conf
/usr/lib/systemd/system/zabbix-server.service
/usr/lib/zabbix/alertscripts
/usr/lib/zabbix/externalscripts
/usr/sbin/zabbix_server_mysql
/var/run/zabbix
```

Zabbix-прокси:

```
/etc/zabbix/zabbix_proxy.conf
/usr/lib/systemd/system/zabbix-proxy.service
/usr/lib/zabbix/externalscripts
/usr/sbin/zabbix_proxy_sqlite3
/var/run/zabbix
```

Zabbix-веб:

```
/usr/share/zabbix/*
/etc/zabbix/web
/etc/zabbix/web/maintenance.inc.php
/etc/zabbix/web/zabbix.conf.php
```

zabbix-sql-scripts.noarch:

```
/usr/share/zabbix-sql-scripts/*
```

Известные проблемы: нет

Снижение производительности: нет

8. 8. Расчет времени проникновения (TTA) после применения рекомендаций

После применения рекомендаций минимальное количество реализованных превентивных мер возросло до 16 из 43, а на некоторых узлах до 21 из 43. Благодаря этому расчетное TTA увеличилось более чем на 50% — до 22,99 часов (рисунки 6 и 7)

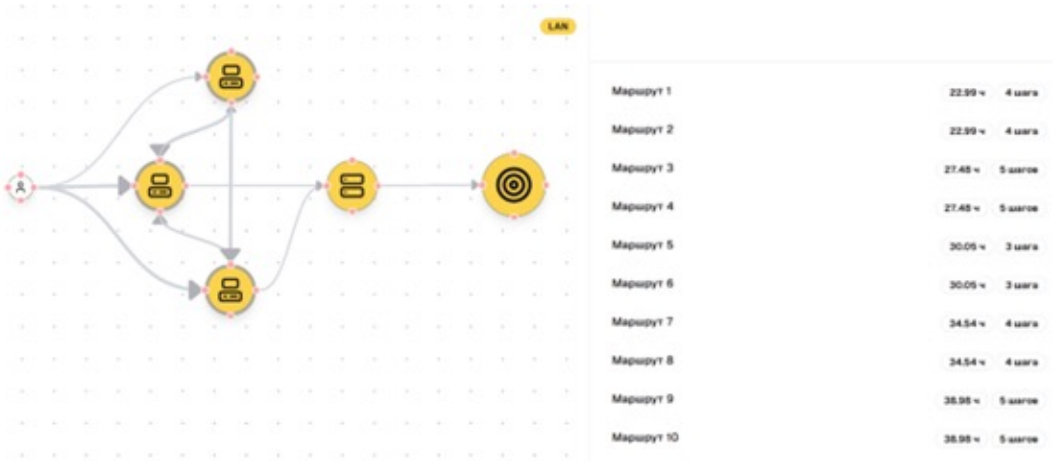

Рисунок 6. Путь атакующего после применения рекомендаций

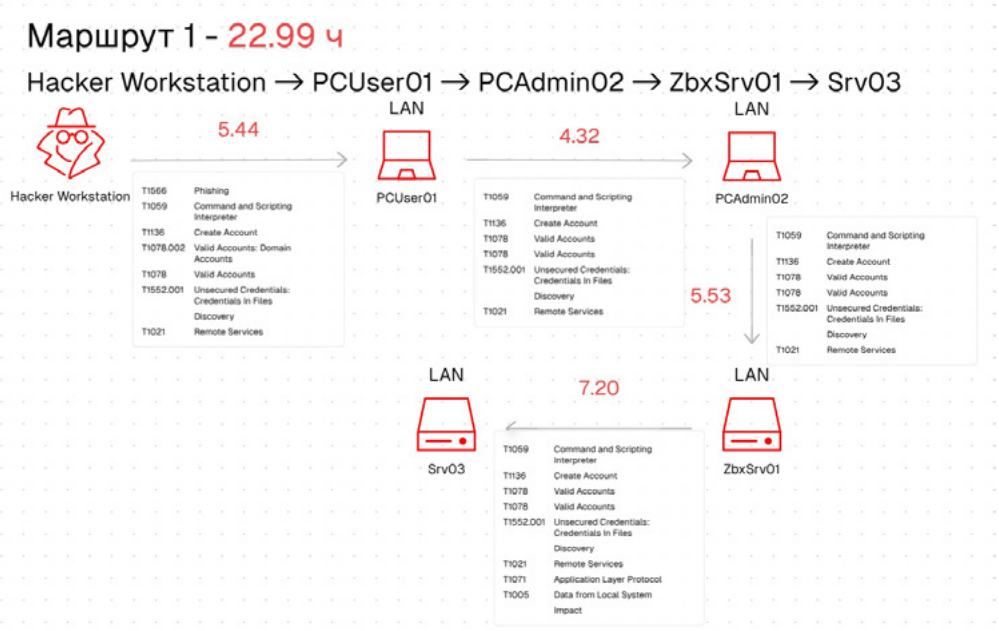

Рисунок 7. Путь атакующего после применения рекомендаций с детализацией по техникам

9. Заключение

Усложнение доступа к интерфейсу администратора может значительно увеличить время и сложность атаки, что предоставит команде мониторинга и реагирования намного больше времени на выявление и локализацию действий злоумышленника.

Помимо увеличения времени и сложности атаки, правильно настроенные агенты с минимально возможными привилегиями сводят к минимуму возможность нанесения ущерба средствам системы мониторинга.

9.1. Целевое состояние системы

После проведения всех мероприятий по харденингу архитектура системы мониторинга будет выглядеть следующим образом (рисунок 8):

Рисунок 8. Целевое состояние системы.

Потенциально уязвимые сегменты взаимодействуют с сервером через Zabbix-прокси в режиме passive. Только ПК пользователей Zabbix-сервера имеют доступ к Zabbix-фронтенду. Все потоки данных, которые возможно зашифровать, используют TLS. (Нужно исправить схему, сейчас https не в том месте) Интегрированы HashiCorp Vault или CyberArk Vault CV12 для хранения «секретов».

Приложение 1

Применимые тактики и техники из матрицы MITRE ATT&CK

В рамках тактики «Разведка» могут быть применены следующие техники:

- T1589 — сбор информации об атакуемых пользователях;
- T1590 — сбор информации об атакуемой сетевой инфраструктуре;
- T1591 — сбор бизнес-информации об атакуемой организации;
- T1592 — сбор информации об атакуемых узлах;
- T1593 — поиск на общедоступных сайтах;
- T1594 — поиск на сайтах атакуемой организации;
- T1595 — активное сканирование;
- T1596 — поиск технической информации в общедоступных источниках;
- T1597 — поиск в закрытых источниках;
- T1598 — фишинг с целью сбора сведений.

В рамках тактики «Подготовка ресурсов» могут быть применены следующие техники:

- T1583 — приобретение инфраструктуры;
- T1584 — компрометация сторонней инфраструктуры;
- T1585 — создание учетных записей;
- T1586 — компрометация учетных записей;
- T1587 — разработка собственных средств;
- T1588 — подготовка необходимых средств;
- T1608 — размещение средств;
- T1650 — приобретение доступа.

В рамках тактики «Первоначальный доступ» могут быть применены следующие техники:

- T1078 — существующие учетные записи;
- T1091 — распространение через съемные носители;
- T1190 — недостатки в общедоступном приложении;
- T1195 — компрометация цепочки поставок;
- T1199 — доверительные отношения;
- T1566 — фишинг.

В рамках тактики «Выполнение» могут быть применены следующие техники:

- T1047 Инструментарий управления Windows;
- T1053 — запланированная задача (задание);
- T1059 — интерпретаторы командной строки и сценариев;
- T1072 — средства развертывания ПО;
- T1106 — нативный API;
- T1129 — общие модули;
- T1203 — эксплуатация уязвимостей в клиентском ПО;
- T1204 — выполнение с участием пользователя;
- T1569 — системные службы.

В рамках тактики «Закрепление» могут быть применены следующие техники:

- T1037 — сценарии инициализации при загрузке или входе в систему;
- T1053 — запланированная задача (задание);
- T1078 — существующие учетные записи;
- T1098 — манипуляции с учетной записью;
- T1136 — создание учетной записи;
- T1197 Задания BITS
- T1205 — передача управляющих сигналов в трафике;
- T1505 — компонент серверного ПО;
- T1547 — автозапуск при загрузке или входе в систему;
- T1556 — изменение процесса аутентификации;
- T1574 — перехват потока исполнения.

В рамках тактики «Повышение привилегий» могут быть применены следующие техники:

- T1037 — сценарии инициализации при загрузке или входе в систему;
- T1053 — запланированная задача (задание);
- T1055 — внедрение кода в процессы;
- T1068 — эксплуатация уязвимостей для повышения привилегий;
- T1078 — существующие учетные записи;
- T1134 Манипуляции с токенами доступа;
- T1484 Изменение доменной политики;
- T1547 — автозапуск при загрузке или входе в систему;
- T1548 Обход механизмов контроля привилегий;
- T1574 — перехват потока исполнения.

В рамках тактики «Предотвращение обнаружения» могут быть применены следующие техники:

- T1006 Прямой доступ к тому;
- T1014 Руткит;
- T1027 Обфусцированные файлы или данные;
- T1036 Маскировка;
- T1055 Внедрение кода в процессы;
- T1070 Устранение индикаторов;
- T1078 Существующие учетные записи;
- T1112 Изменение реестра;
- T1127 Выполнение через доверенные утилиты разработчика;
- T1134 Манипуляции с токенами доступа;
- T1140 Деобфускация/декодирование файлов или данных;
- T1197 Задания BITS;
- T1202 Непрямое выполнение команд;
- T1205 Передача управляющих сигналов в трафике;
- T1207 Поддельный контроллер домена;
- T1211 Эксплуатация уязвимостей для предотвращения обнаружения;
- T1216 Выполнение через системный сценарий;
- T1218 Выполнение с помощью системных бинарных файлов;
- T1222 Изменение разрешений для файлов и каталогов;
- T1480 Ограничения на исполнение;
- T1484 Изменение доменной политики;
- T1548 Обход механизмов контроля привилегий;
- T1550 Использование альтернативных сущностей для аутентификации;
- T1553 Нарушение работы средств контроля доверия;
- T1556 Изменение процесса аутентификации;
- T1562 Ослабление защиты;
- T1564 Сокрытие артефактов;
- T1574 Перехват потока исполнения;
- T1599 Преодоление границ сети;
- T1600 Понижение надежности шифрования;
- T1622 Предотвращение отладки.

В рамках тактики «Получение учетных данных» могут быть применены следующие техники:

- T1003 Получение дампа учетных данных;
- T1040 Прослушивание сетевого трафика;

- T1056 Перехват вводимых данных;
- T1110 Метод перебора;
- T1187 Принудительная аутентификация;
- T1212 Эксплуатация уязвимостей для получения учетных данных;
- T1528 Кража токена доступа к приложению;
- T1539 Кража сессионных куки;
- T1552 Незащищенные учетные данные;
- T1555 Учетные данные из хранилищ паролей;
- T1556 Изменение процесса аутентификации;
- T1557 «Злоумышленник посередине»;
- T1558 Кража или подделка билетов Kerberos;
- T1606 Подделка учетных данных для веб-ресурсов.

В рамках тактики «Изучение» могут быть применены следующие техники:

- T1007 Изучение системных служб;
- T1010 Изучение открытых приложений;
- T1012 Запросы к реестру;
- T1016 Изучение конфигурации сети;
- T1018 Изучение удаленных систем;
- T1033 Изучение владельца или пользователей системы;
- T1040 Прослушивание сетевого трафика;
- T1046 Изучение сетевых служб;
- T1049 Изучение сетевых подключений;
- T1057 Изучение процессов;
- T1069 Изучение групп разрешений;
- T1082 Изучение системы;
- T1083 Изучение файлов и каталогов;
- T1087 Изучение учетных записей;
- T1124 Изучение системного времени;
- T1135 Изучение общих сетевых ресурсов;
- T1201 Изучение парольной политики;
- T1482 Изучение доверительных отношений между доменами;
- T1518 Изучение установленного ПО;
- T1615 Изучение групповой политики;
- T1622 Предотвращение отладки;
- T1652 Изучение драйверов устройств.

В рамках тактики «Перемещение внутри периметра» могут быть применены следующие техники:

- T1080 — заражение общего содержимого;
- T1210 — эксплуатация уязвимостей в удаленных службах;
- T1534 — внутренний целевой фишинг;
- T1570 — передача инструментов внутри периметра.

В рамках тактики «Сбор данных» могут быть применены следующие техники:

- T1005 — данные из локальной системы;
- T1039 — данные с общих сетевых дисков;
- T1056 — перехват вводимых данных;
- T1074 — промежуточное хранение данных;
- T1119 — автоматизированный сбор данных;
- T1557 — «злоумышленник посередине»;
- T1560 — архивация собранных данных.

В рамках тактики «Организация управления» могут быть применены следующие техники:

- T1001 Обфускация данных;
- T1008 Резервные каналы;
- T1071 Протокол прикладного уровня;
- T1090 Прокси-сервер;
- T1095 Протоколы (кроме прикладного уровня);
- T1102 Веб-служба;
- T1104 Отдельный канал для каждого этапа;
- T1105 Передача инструментов из внешней сети;
- T1132 Кодирование данных;
- T1205 Передача управляющих сигналов в трафике;
- T1219 ПО для удаленного доступа;
- T1568 Динамическое разрешение;
- T1571 Нестандартный порт;
- T1572 Туннелирование протокола;
- T1573 Зашифрованный канал.

В рамках тактики «Эксфильтрация данных» могут быть применены следующие техники:

- T1011 Эксфильтрация через альтернативную сетевую среду;
- T1020 Автоматизированная эксфильтрация;

- T1029 Передача по расписанию;
- T1030 Ограничение размера передаваемых блоков данных;
- T1041 Эксфильтрация по каналу управления;
- T1048 Эксфильтрация по альтернативному протоколу;
- T1567 Эксфильтрация через веб-службу.

В рамках тактики «Деструктивное воздействие» могут быть применены следующие техники:

- T1485 Уничтожение данных;
- T1486 Шифрование данных;
- T1489 Остановка службы;
- T1490 Препятствование восстановлению системы;
- T1496 Несанкционированное использование ресурсов;
- T1498 Сетевой отказ в обслуживании;
- T1499 Точечный отказ в обслуживании;
- T1529 Завершение работы или перезагрузка системы;
- T1531 Прекращение доступа к учетной записи;
- T1561 Уничтожение диска;
- T1565 Манипуляции с данными.