Руководство по защите zVirt 4.2 по методологии ХардкорИТ

Positive Technologies

Москва, 2024

1. Проблематика защиты zVirt

1.1. Покрытие рынка

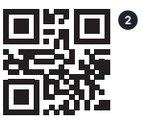
В 2024 году российские компании с государственным участием должны заменить зарубежное программное обеспечение на отечественное, в том числе средства виртуализации вычислительных ресурсов.

Платформа защищенной серверной виртуализации zVirt входит в реестр отечественного ПО, имеет заметную долю в количестве развернутых экземпляров (по данным Orion Soft[1], компании-производителя zVirt, на 40% замещенных узлов VMware vSphere в России установлено ПО zVirt), и в связи с реализацией государством политики импортозамещения эта доля будет увеличиваться.

Платформа виртуализации может быть привлекательной целью для хакеров: через нее могут быть атакованы и скомпрометированы сервисы, работающие в виртуальных машинах. Этот документ описывает типовые потенциальные проблемы безопасности платформы виртуализации на базе zVirt и дает рекомендации по повышению защищенности.

1.2. Статистика по уязвимостям

Компания Orion Soft активно занимается мониторингом и устранением критических уязвимостей в системе. Процесс управления уязвимостями включает регулярные обновления безопасности и применение патчей для защиты инфраструктуры клиентов. На текущий момент, пока не публикуется список существующих уязвимостей в продукте. Публикация реестра уязвимостей ПО zVirt в ближайших планах компании.



На данный момент, в открытом доступе, для платформы виртуализации oVirt, на базе которой были созданы первые версии ПО zVirt, в базе CVE[2] можно найти 56 записей об уязвимостях.

1.3. Архитектурные особенности

По умолчанию учетная запись пользователя root с паролем может быть использована для регистрации гипервизоров в платформе виртуализации через SSH. Диски виртуальных машин по умолчанию не шифруются, и при наличии доступа в операционную систему гипервизора можно подмонтировать диск виртуальной машины в файловую систему соответствующего гипервизора. Таким образом, платформа виртуализации может являться ключевой системой, что делает ее одной из целей для злоумышленника.

2. Недопустимые события с участием zVirt

Для примера рассмотрим в качестве недопустимых событий:

- утечку конфиденциальной информации;
- вынужденный простой в работе ИТ-систем.

Сценариями реализации недопустимых событий в таком случае могут быть:

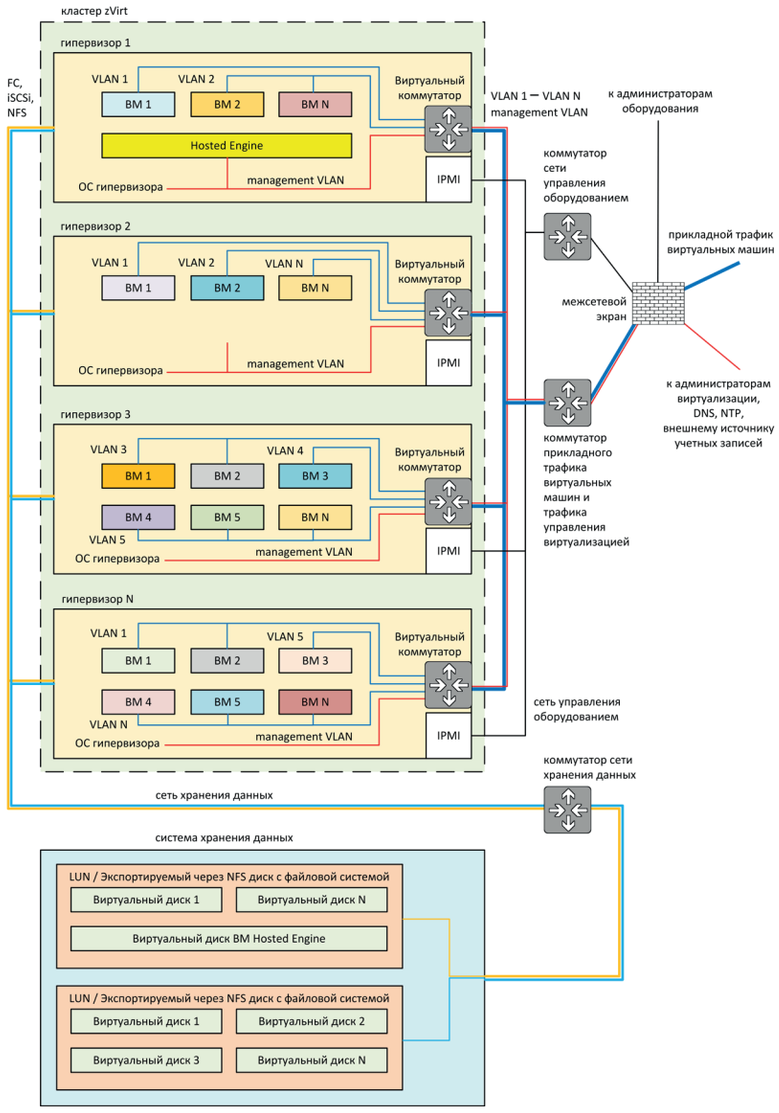
- доступ в блочное хранилище или хранилище общих дисков с файловой системой, на которых располагаются диски виртуальных машин;
- доступ в файловую систему диска виртуальной машины в обход виртуального оборудования;
- получение полномочий администратора, имеющего права на работу с диском определенной виртуальной машины, включая его удаление;
- несанкционированное подключение к консоли экрана виртуальной машины;
- получение полномочий администратора, имеющего права на изменение конфигурации определенной виртуальной машины и (или) управление ее виртуальным питанием;
- получение полномочий администратора, имеющего права на изменение конфигурации zVirt и (или) управление питанием гипервизоров.

3. Пример типовой инсталляции платформы

3.1. Архитектурная схема типовой инсталляции

Архитектурная схема типовой инсталляции платформы виртуализации на базе zVirt 4.2 приведена на рисунке 1 (это не единственно возможная схема развертывания zVirt, например возможно развертывание, при котором управляющий сервер не находится в виртуальной машине zVirt, или развертывание с SDS).

Рисунок 1. Архитектурная схема типовой инсталляции zVirt



3.2. Описание типовой инсталляции

Приведенная выше распространенная типовая схема установки zVirt включает в себя несколько гипервизоров, к которым по протоколам FC или iSCSI подключены блочные устройства (LUN), либо по протоколу NFS3 (или NFS4) подключены диски с файловой системой. Гипервизоры, которым доступен идентичный набор блочных устройств и дисков с файловой системой (на этих наборах находятся виртуальные диски виртуальных машин), могут быть объединены в кластер, что является необходимым (но недостаточным) условием для живой миграции виртуальных машин между гипервизорами и для работы службы High Availability. Каждый гипервизор имеет одно или

несколько сетевых подключений с разделением сетей по VLAN. В гипервизорах к виртуальным машинам подключается один или несколько виртуальных сетевых адаптеров, к каждому адаптеру привязывается определенная VLAN внешней сети.

Управляющий виртуализацией сервер на этой схеме находится в виртуальной машине, так называемой HostedEngine. Для того, чтобы эта виртуальная машина могла работать на определенном гипервизоре, должна быть выполнена специальная настройка гипервизора (то есть, в общем случае виртуальная машина HostedEngine может быть запущена не на любом гипервизоре).

Управляющий сервер и каждый гипервизор постоянно связываются друг с другом через сеть, называемую на схеме management VLAN. Управление виртуализацией выполняется через web-консоль, сервис которой работает на управляющем сервере. Для аутентификации и авторизации могут быть использованы как локальные учетные записи и группы, так и внешние LDAP, Active Directory, Free IPA и др.

4. Проблемы безопасности типовой инсталляции

В этом разделе приведены проблемы безопасности типовой инсталляции платформы виртуализации zVirt.

Типовая инсталляция платформы виртуализации зачастую обладает следующими проблемами с точки зрения безопасности:

- Для доступа через SSH в ОС гипервизоров используется учетная запись root с паролем.
- Для доступа в ОС гипервизоров используются неперсонифицированные учетные записи.
- Игнорируются выпущенные производителем обновления zVirt.
- Несколько пользователей платформы виртуализации могут одновременно подключаться к одной консоли с экраном виртуальной машины, при этом один пользователь не получает уведомления о подключении другого.
- Неверно настроенное зонирование для блочных устройств или неверно настроенный экспорт NFS для общих дисков с файловой системой, а также неверно настроенный межсетевой экран позволяют подключать блочные устройства и (или) диски не только к гипервизорам кластера zVirt (не является проблемой безопасности именно zVirt, но это связанная с zVirt проблема).
- Администраторы, работающие в консоли с экраном виртуальной машины, зачастую закрывают консоль, не завершив сеанс пользователя ОС в виртуальной машине, и если ОС с графическим интерфейсом автоматически блокируют через некоторое время сессию, то в ОС, в которых нет графического интерфейса, сессия пользователя ОС сервера в виртуальной машине остается открытой неограниченно долго (не является проблемой безопасности именно zVirt, но это связанная с zVirt проблема).
- Есть возможность установить RPM-пакеты из файловой системы посредством DNF или RPM без проверки цифровой подписи пакета.

- Есть возможность модификации конфигурации загрузки ОС в интерфейсе GRUB 2 без запроса пароля.
- Пользователь root может получить доступ из ОС гипервизора к содержимому дисков виртуальных машин, которые работают на этом гипервизоре.
- Сессия SSH не завершается при бездействии пользователя. При использовании «сервера подскока» (jump server) для доступа в ОС гипервизоров и сервера управления администраторы зачастую не завершают сеанс пользователя после выполнения задачи, а отключаются от него, не закрывая сессии SSH, которые остаются открытыми неограниченно долго.
- В настройках SSH-сервера на гипервизорах и сервере управления виртуализацией, по умолчанию, разрешена аутентификация по GSSAPI, даже если используются только локальные учетные записи.
- По умолчанию разрешен доступ пользователям с пустым паролем.

Гипервизоры и управляющая виртуализацией виртуальная машина — это, прежде всего, узлы с установленной ОС семейства Linux, и для них могут быть применены тактики и техники для Linux из матрицы MITRE ATT&CK. Кроме того, в матрице указаны и специфичные именно для zVirt тактики и техники.

Для типовой инсталляции платформы виртуализации на базе zVirt могут быть применены **14 тактик** и **более 140 техник** из матрицы MITRE ATT&CK. Для их применения достаточно **низкой квалификации атакующего** (условно ее можно обозначить как «киберхулиган» или «энтузиаст-одиночка»).

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:

- 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;
- 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;
- T1547 Автозапуск при загрузке или входе в систему;
- T1574 Перехват потока исполнения.

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

- T1014 Руткит;
- T1027 Обфусцированные файлы или данные;
- T1036 Маскировка;
- T1055 Внедрение кода в процессы;
- T1070 Устранение индикаторов;
- T1078 Существующие учетные записи;
- T1140 Деобфускация/декодирование файлов или данных;
- T1205 Передача управляющих сигналов в трафике;
- T1211 Эксплуатация уязвимостей для предотвращения обнаружения;
- T1218 Выполнение с помощью системных бинарных файлов;
- T1222 Изменение разрешений для файлов и каталогов;
- T1480 Ограничения на исполнение;
- 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;

- T1212 Эксплуатация уязвимостей для получения учетных данных;
- 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;
- 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;
- T1518 Изучение установленного ПО;
- 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.

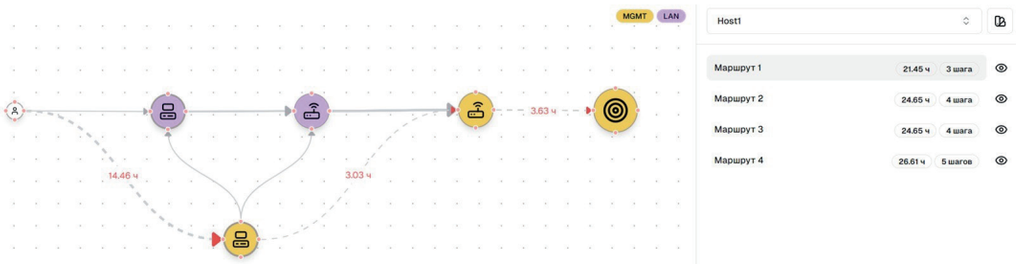
В рамках тактики «Деструктивное воздействие» могут быть применены следующие техники:

- 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.

5. Расчет времени проникновения для инсталляции с параметрами по умолчанию

При параметрах настройки по умолчанию только 2 из 43 превентивных контролей были реализованы, что значительно облегчает реализацию недопустимых событий злоумышленнику. На это ему может потребоваться всего 3 шага и около 22 часов (см. рисунок 2).

Рисунок 2. Путь атакующего до повышения защищенности



6. Рекомендации по повышению защищенности

При развертывании zVirt автоматически применяются параметры безопасности «по умолчанию». В этом разделе приведены рекомендации по повышению защищенности типовой установки zVirt, связанные с планированием схемы установки и эксплуатацией zVirt.

Соответствие рекомендаций защитным мерам из матрицы MITRE ATT&CK указано в таблице. Подробное описание рекомендаций приведено в подразделах ниже.

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

Рекомендация	**Защитные меры из матрицы MITRE ATT&CK**
Установка последних обновлений zVirt	M1051 Update Software
Создание персональных учетных записей для администраторов zVirt	M1026 Privileged Account Management
Настройка доступа администраторов с персональными учетными записями через SSH в ОС гипервизоров и управляющего сервера по SSH-ключу с парольной фразой; запрет доступа только по паролю	M1036 Account Use Policies M1043 Credential Access Protection M1032 Multi-factor Authentication
Усиление парольной политики для учетных записей	M1027 Password Policies
Изменение конфигурации протоколов SSL и TLS	M1041 Encrypt Sensitive Information
Отключение неиспользуемых сервисов	M1042 Disable or Remove Feature or Program
Использование средств контроля целостности	M1049 Antivirus/Antimalware
Выделение управляющей сети zVirt в отдельный сегмент	M1030 Network Segmentation
Установка пароля для доступа к модификации конфигурации загрузки ОС в интерфейсе GRUB2	M1046 Boot Integrity
Выполнений действий по защите внешнего источника учетных записей zVirt	M1018 User Account Management
Отключение возможности аутентификации в ОС учетной записи с пустым паролем	M1027 Password Policies
Запрет установки RPM-пакетов, находящихся в файловой системе сервера, без проверки цифровой подписи	M1045 Code Signing M1033 Limit Software Installation
Шифрование дисков виртуальных машин	M1041 Encrypt Sensitive Information
Ограничение длительности сессии SSH до гипервизора или сервера управления виртуализацией при бездействии пользователя	M1036 Account Use Policies
Отключение неиспользуемых методов аутентификации, в частности, в параметрах SSH-сервера метод GSSAPI Authentication, который включен по умолчанию	M1042 Disable or Remove Feature or Program
Использование двухфакторной аутентификации на административном и пользовательском порталах	M1032 Multi-factor Authentication

Рекомендация	Защитные меры из матрицы MITRE ATT&CK
Выделение для работы виртуальной машины с Hosted Engine отдельного кластера виртуализации и отдельного LUN или диска СХД, доступного только на гипервизорах этого кластера	M1048 Application Isolation and Sandboxing M1037 Filter Network Traffic M1035 Limit Access to Resource Over Network M1030 Network Segmentation

6.1. Установка последних обновлений zVirt

Используйте только поддерживаемые производителем версии ПО, а также следите за выпуском новых версий обновлений. Эти обновления содержат исправления программных ошибок и закрывают уязвимости, которые были обнаружены в ходе эксплуатации. Подробнее о построении процесса управления уязвимостями можно узнать на курсе-практикуме[3].

6.2. Создание персональных учетных записей для администраторов zVirt

Запретите выполнять рутинные операции в ОС гипервизоров и управляющего сервера под учетной записью root. Запретите выполнение рутинных операций в web-консоли zVirt под учетной записью admin. Создайте персональные учетные записи для администраторов zVirt.

6.3. Настройка доступа администраторов с персональными учетными записями через SSH в ОС гипервизоров и управляющего сервера по SSH-ключу с парольной фразой; запрет доступа по паролю без SSH-ключа

Доступ администраторов в ОС гипервизоров и управляющего сервера через SSH должен выполняться по SSH-ключу с парольной фразой, при этом доступ по паролю без SSH-ключа необходимо отключить.

Для доступа администратора под учетной записи root на гипервизорах не стоит использовать SSH-ключ, который используется для доступа с использованием сервисов управляющего сервера в ОС гипервизора, — необходимо сгенерировать отдельный SSH-ключ с парольной фразой.

6.4. Усиление парольной политики для учетных записей

Используйте парольные политики для определения требований к сложности паролей, частоте смены паролей и параметрам блокировки учетной записи. Рекомендуемая минимальная длина пароля — 12 знаков. В пароле должны быть как минимум три из четырех групп знаков.

Нет однозначного мнения о том, каким должен быть максимальный срок действия пароля. При слишком коротком сроке действия повышается нагрузка на подразделение, занимающееся поддержкой ИТ-инфраструктуры. При слишком большом сроке увеличивается вероятность использования злоумышленниками паролей, полученных в результате публичных утечек. Чаще всего, устанавливается срок действия пароля от 40 до 180 дней. Решение о максимальном сроке действия пароля предлагается принимать исходя из условий и особенностей деятельности конкретной организации.

Количество неудачных попыток аутентификации, предшествующее блокировке, рекомендуется устанавливать индивидуально в каждой организации, ориентируясь на количество запросов пользователей в техническую поддержку по поводу блокировки учетной записи. Рекомендуемый диапазон — от пяти до десяти неудачных попыток аутентификации.

Настройка парольной политики для учетных записей в zVirt 4.1 и более ранних, а также в zVirt 4.2, использующем провайдер аутентификации AAA JDBC, описана в wiki Orion Soft[4].

Для zVirt 4.2, использующем в качестве провайдера аутентификации Keycloak, настройка парольной политики для учетных записей описана в разделе 1.2.4. «Настройка политик» здесь[5].

6.5. Изменение конфигурации протоколов SSL и TLS

Используйте RSA-2048 при создании новых ключей сертификатов. При обновлении или создании новых запросов на подпись сертификатов рекомендуется отдавать предпочтение алгоритму SHA-256 или более безопасным.

Статья о создании сертификата для zVirt находится в wiki Orion Soft[6].

6.6. Отключение неиспользуемых сервисов

По умолчанию, на гипервизорах и управляющем виртуализацией сервере запускается предопределенный набор сервисов. В конкретной установке zVirt не все сервисы могут быть необходимы для функционирования системы. Такие сервисы необходимо выключить, если это сделать невозможно — закрыть прослушиваемый сетевой порт локальным сетевым экраном.

6.7. Использование средств контроля целостности

На гипервизорах и управляющем виртуализацией сервере следует использовать средства контроля целостности, например aide или rkhunter.

На гипервизорах и управляющем виртуализацией сервере установлен по умолчанию пакет aide, но не выполнена настройка для регулярного контроля целостности системных файлов и каталогов. Необходимо выполнить такую настройку.

Для справки по настройке aide можно использовать статью[7].

6.8. Выделение управляющей сети zVirt в отдельный сегмент

Управляющая сеть zVirt используется для связи управляющего виртуализацией сервера с гипервизорами. Доступ в эту сеть должен быть ограничен и предоставляться только администраторам zVirt.

Изменение сетевых параметров сети управления описано в статье[8].

6.9. Установка пароля для доступа к модификации конфигурации загрузки ОС в интерфейсе GRUB 2

В среде zVirt по умолчанию в качестве загрузчика ОС используется GRUB2 и во время загрузки возможно изменить конфигурацию загрузки ОС в интерфейсе GRUB2 без ввода пароля. Модификация конфигурации загрузчика может позволить злоумышленнику изменить строку параметров ядра Linux, поэтому необходимо установить пароль для доступа к модификации конфигурации загрузки ОС в интерфейсе GRUB2, для установки пароля можно руководствоваться статьёй[9].

6.10. Выполнение действий по защите внешнего источника учетных записей zVirt

В качестве источника учетных записей zVirt может использоваться Miscrosoft Active Directory, LDAP-каталог, FreeIPA и другие сервисы. Каждый из них может быть объектом атаки для получения учетных данных, которые позволят пройти аутентификацию и авторизацию в zVirt, и получить доступ к целевым виртуальным машинам. Необходимо выполнить действия по защите этих сервисов.

6.11. Отключение возможности аутентификации в ОС учетной записи с пустым паролем

По умолчанию, в ОС гипервизоров и управляющего сервера zVirt разрешена аутентификация пользователей с пустым паролем. Следует запретить аутентификацию с пустым паролем.

Есть различные способы сделать это, но предпочтительным, с точки зрения исключения побочных эффектов, является использование утилиты authselect, работа с которой описана[10].

При её запуске, для достижения результата, следует указать параметр профиля without-.

6.12. Запрет установки RPM-пакетов, находящихся в файловой системе сервера, без проверки цифровой подписи

По умолчанию, в ОС гипервизоров и управляющего сервера zVirt выполняется установка RPM-пакетов из локальной файловой системы, посредством DNF или RPM, без проверки цифровой подписи пакета. Требуется запретить установку RPM-пакетов без проверки цифровой подписи пакета.

Настройки для dnf находятся в файле /etc/dnf/dnf.conf. За проверку подписи пакетов, устанавливающихся из локальной файловой системы, отвечает параметр localpkg_gpgcheck, по умолчанию отсутствующий в конфигурационном файле. Необходимо добавить этот параметр в конфигурационный файл со значением True.

Настройки для rpm находятся в файле /usr/lib/rpm/macros. За проверку подписи отвечает параметр %_pkgverify_level, которому необходимо выставить значение all.

6.13. Шифрование дисков виртуальных машин

При наличии полномочий root пользователь может получить доступ из ОС гипервизора к содержимому дисков виртуальных машин, которые могут работать на этом гипервизоре. Для предотвращения просмотра или копирования информации, находящейся на виртуальном диске, необходимо использовать шифрование виртуальных дисков виртуальных машин.

В базе знаний Orion Soft имеется статься, посвященная шифрованию дисков виртуальных машин[11].

6.14. Ограничение длительности сессии SSH до гипервизора или сервера управления виртуализацией при бездействии пользователя

По умолчанию на SSH-сервере на гипервизорах и сервере управления виртуализацией не ограничена длительность сессии при бездействии пользователя. При использовании «сервера подскока» для доступа в ОС гипервизоров и сервера управления администраторы, зачастую, не завершают сеанс пользователя после выполнения задачи, а отключаются, не закрывая сессии SSH, которые остаются открытыми неограниченно долго.

Необходимо выполнить настройку SSH-сервера на гипервизорах и сервере управления виртуализацией для ограничения длительности сессии при бездействии пользователя.

В zvirt используется сервер openssh версии 8, который не имеет своих средств контроля длительности сессии пользователя. Более того, установленная версия openssh не устанавливает переменные в секции match в конфигурационном файле /etc/ssh/sshd_config, что не позволяет исключить root из ограничений на длительность сессии. Поэтому, ограничение сессии пользователя следует сделать иными средствами, например, добавив в конец файла .bash_profile в домашнем каталоге пользователя на гипервизорах и управляющем виртуализацией сервере строку export TMOUT="3600", где 3600 – максимальная длительность сессии пользователя в секундах (можно указать любую приемлемую длительность сессии).

6.15. Отключение неиспользуемых методов аутентификации, в частности, в параметрах SSH-сервера метод GSSAPI Authentication, который включен по умолчанию

В параметрах SSH-сервера на гипервизорах и сервере управления виртуализацией по умолчанию разрешен метод аутентификации GSSAPI Authentication, даже если используются только локальные учетные записи.

Если метод GSSAPI Authentication не требуется для подключения через SSH к гипервизорам и серверу управления виртуализацией, необходимо отключить этот тип аутентификации, как потенциальную уязвимость. Для этого, на гипервизорах и управляющем сервере в конфигурационном файле /etc/ssh/sshd_config следует указать параметр GSSAPIAuthentication со значением no и перезапустить сервис sshd.

6.16. Использование двухфакторной аутентификации на административном и пользовательском порталах

В zVirt версии 4.2 появилась возможность двухфакторной аутентификации в административном и пользовательском порталах. Следует использовать эту возможность.

Настройка двухфакторной аутентификации описана в wiki Orion Soft[12].

6.17. Выделение для работы виртуальной машины с HostedEngine отдельного кластера и отдельного LUN или диска СХД, доступного только на гипервизорах этого кластера

При компрометации гипервизора и получении злоумышленником полномочий root, ему становятся доступны виртуальные диски виртуальных машин, которые могут работать на этом гипервизоре. Компрометация может быть, в том числе, результатом эксплуатации возможной уязвимости платформы виртуализации, позволяющей злоумышленнику попасть из ОС виртуальной машины в ОС гипервизора.

Для предотвращения получения доступа к виртуальному диску управляющей виртуализацией виртуальной машины (HostedEngine) в результате такой атаки, необходимо уменьшить количество гипервизоров, к которым подключен LUN или диск СХД с виртуальным диском Hosted Engine, — то есть создать отдельный кластер виртуализации именно для работы Hosted Engine и подключить LUN или диск СХД только к гипервизорам этого кластера.

От используемой технологии подключения СХД к гипервизорам зависит реализация рекомендации.

На рисунке 3 представлена схема сценария, при котором для подключения СХД используется FC или iSCSi. В этом случае может использоваться общая для всех гипервизоров сеть хранения данных, при этом, запрет доступа к конкретным LUN реализуется за счет зонирования для FC и ограничения списка инициаторов для iSCSI.

В случае, если используется NFS — при общей сети хранения данных для всех гипервизоров —контроль доступа гипервизоров к экспортируемой через NFS файловой системе может быть реализован только на базе IP-адресов гипервизоров, что не очень безопасно. Поэтому необходимо отделить физически сеть хранения данных ВМ Hosted Engine от сети хранения данных остальных ВМ, как это показано на рисунке 4.

Для отказоустойчивости в кластере, выделенном для работы Hosted Engine, должно быть не менее двух гипервизоров. Мощности даже не очень современного оборудования, которое может быть использовано для работы в качестве гипервизора, могут быть избыточными, если на них будет работать только Hosted Engine. Поэтому, скорее всего, в этот кластер будут «подселены» другие виртуальные машины, тем не менее, вероятность описанной выше атаки будет снижена — ввиду меньшего количества виртуальных машин в кластере.

При планировании архитектуры платформы виртуализации следует учесть выделение отдельных ресурсов для Hosted Engine, как описано выше. Если же платформа виртуализации уже развернута без учета этой рекомендации, то можно воспользоваться процедурой перемещения виртуальной машины Hosted Engine в другое хранилище, которая описана в статье[13].

Рисунок 3. Схема установки zVirt с отдельным кластером для Hosted Engine и сетью данных, построенной на FC или iSCSI

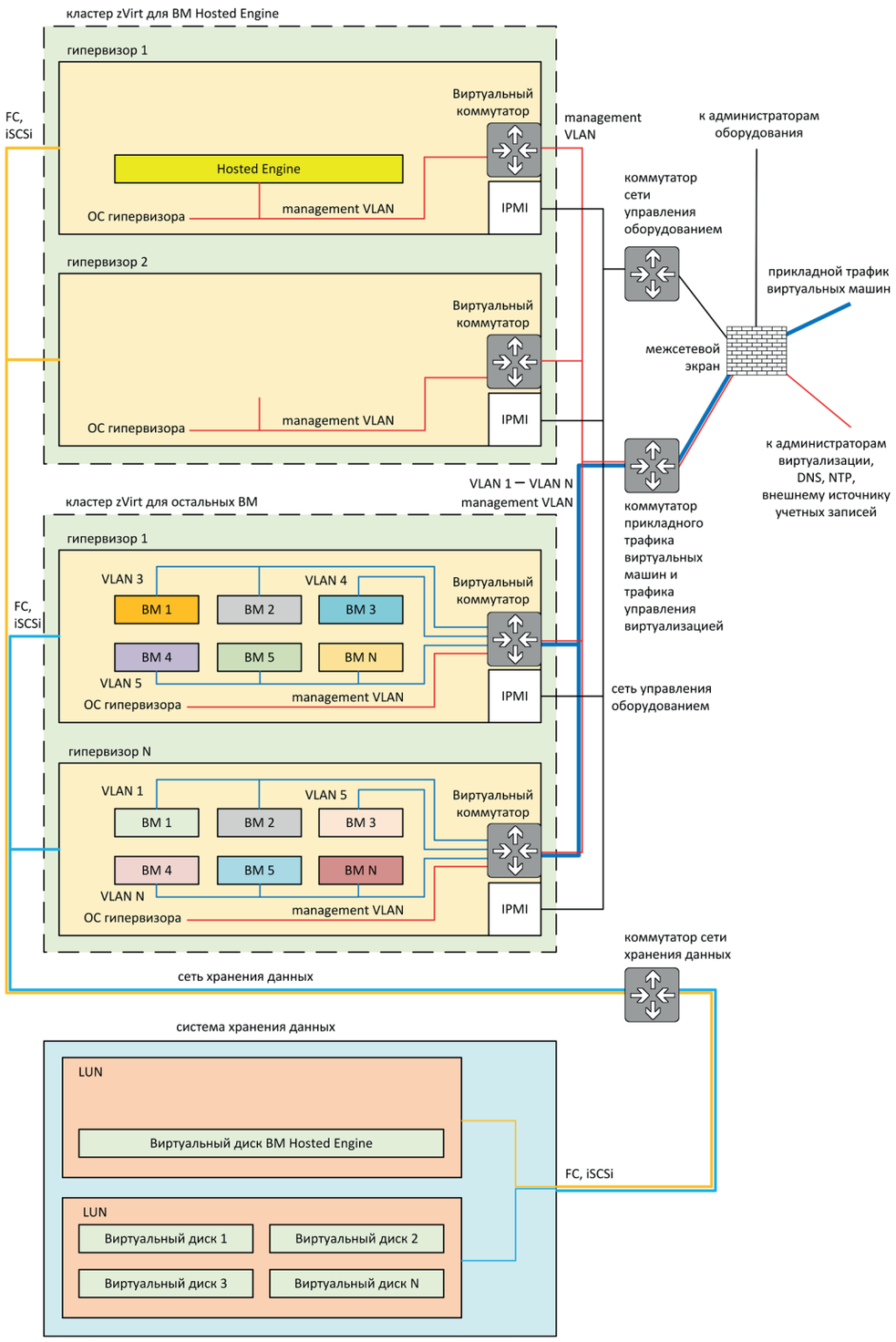
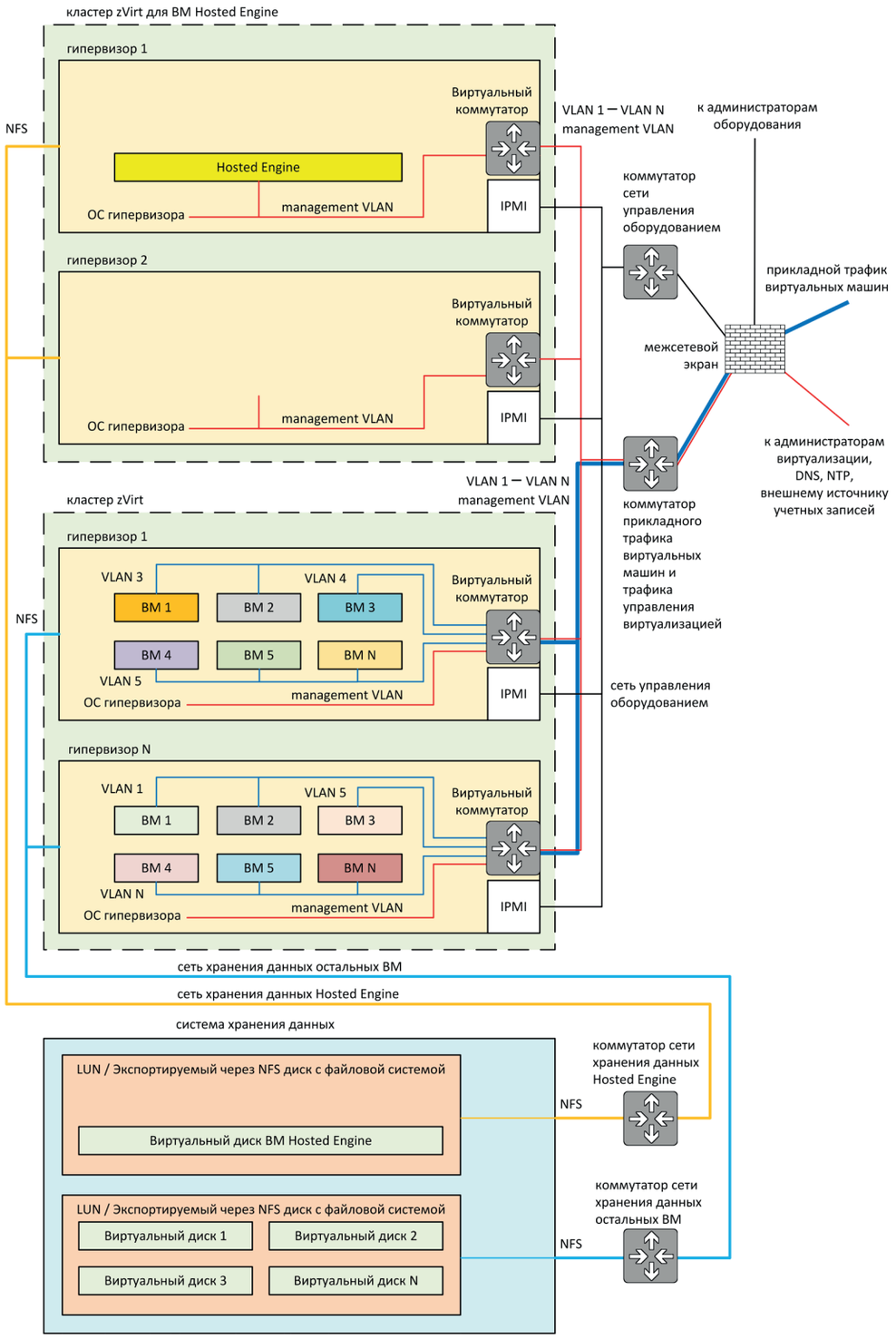


Рисунок 4. Схема установки zVirt с отдельным кластером для Hosted Engine и сетью данных, построенной на NFS



7. Расчет времени проникновения (TTA) после применения рекомендаций

После применения рекомендаций количество реализованных превентивных контролей возросло до 15 из 43. Благодаря этому расчетное TTA увеличилось до 24 часов (см. рисунки 5 и 6).

Рисунок 5. Путь атакующего после применения рекомендаций

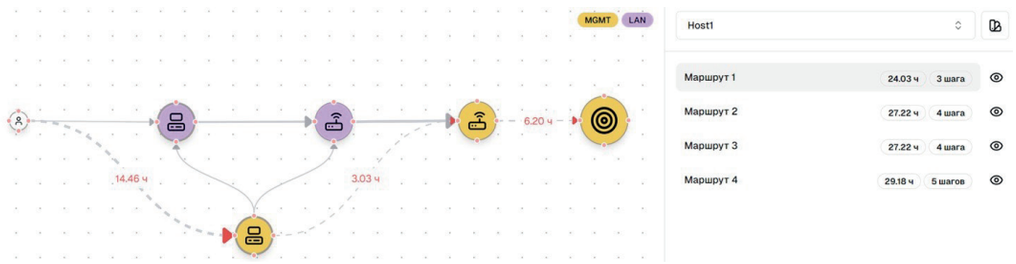
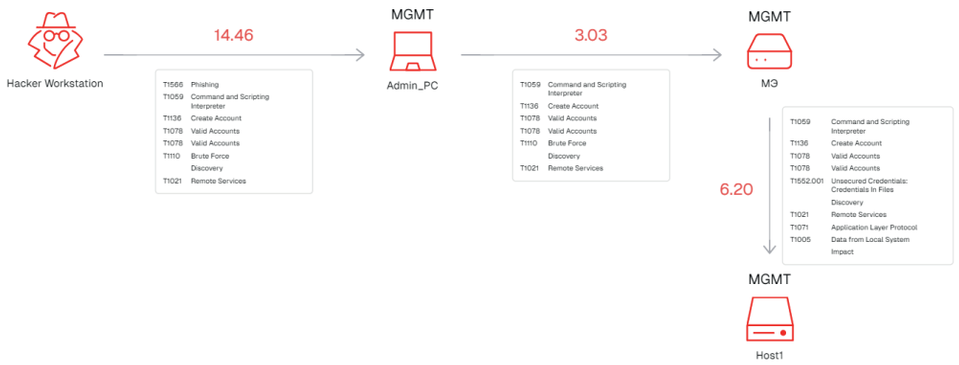


Рисунок 6. Путь атакующего с детализацией по техникам

Маршрут 1 - 24.03 ч

Hacker Workstation → Admin_PC → МЭ → Host1



8. Заключение

Несмотря на то, что проведенный харденинг не увеличивает количество узлов на пути злоумышленника, выполнение каждого шага занимает больше времени, и у команды мониторинга и реагирования появляется больше времени на детектирование и локализацию действий злоумышленника. При этом реализация контролей не требует дополнительных затрат на внедрение новых средств защиты, большинство из них может быть применено в течение нескольких часов.

ptsecurity.com
pr@ptsecurity.com

Positive Technologies — лидер в области результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют более 4000 организаций по всему миру.

Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 205 тысяч акционеров.

Следите за нами в соцсетях (Telegram, ВКонтакте, Twitter, Хабр) и в разделе «Новости» на сайте ptsecurity.com, а также подписывайтесь на телеграм-канал IT's positive investing.