Важная информация

2. Перед началом работы

2.1 Использование поддерживаемой версии НАЙС.ОС Greenbone COMMUNITY EDITION

Для корректной работы **OPENVAS SCAN** следует использовать версию, официально поддерживаемую проектом **Greenbone** в составе **НАЙС.ОС Greenbone COMMUNITY EDITION**, включая актуальные патчи безопасности. Использование неподдерживаемой версии может привести к следующим последствиям:

- несовместимости с текущими обновлениями и базой тестов уязвимостей (feed);
- наличию неисправленных ошибок в системе;
- отсутствию критически важных функций, необходимых для стабильной работы тестов уязвимостей (VT);
- снижению полноты охвата при сканировании или пропуску уязвимостей;
- наличию неустранённых уязвимостей в используемых компонентах системы.

2.2 Влияние на исследуемую сетевую среду

OPENVAS SCAN включает полнофункциональный сканер уязвимостей. Несмотря на то, что он спроектирован с учётом минимизации влияния на сеть, процесс сканирования требует активного взаимодействия с целевыми системами.

Примечание

Основная задача **OPENVAS SCAN** — выявление уязвимостей, которые могут оставаться незамеченными. Для этого сканер частично имитирует поведение злоумышленников.

Рекомендуемые настройки по умолчанию минимизируют воздействие на инфраструктуру, однако побочные эффекты всё же возможны. При необходимости их

можно ограничить с помощью параметров конфигурации сканера.

Возможные побочные эффекты

- на целевых системах могут появляться записи в логах и уведомления о событиях;
- уведомления могут фиксироваться на сетевых устройствах, в системах мониторинга, межсетевых экранах и IPS/IDS;
- правила межсетевых экранов и сигнатуры систем защиты могут срабатывать на активность сканера;
- возможен рост сетевой задержки на целевых узлах и сегментах; в редких случаях — ситуации, схожие с DoS-атакой;
- нестабильные или уязвимые приложения могут аварийно завершаться;
- встроенные устройства с упрощёнными сетевыми стеками (например, IoT или OT) могут зависнуть или выйти из строя;
- выполняются пробные подключения (например, SSH, FTP) для сбора баннеров сервисов;
- выполняются проверки открытых портов по множеству протоколов (HTTP, FTP и др.);
- учётные записи могут блокироваться при тестировании стандартных комбинаций логин/пароль.

Поскольку подобное поведение является частью корректной процедуры тестирования, рекомендуется заранее добавить IP-адреса сканера в список разрешённых (allow list) целевых систем. Инструкции по созданию таких списков доступны в документации соответствующих сервисов.

Если система реагирует сбоями или блокировками при стандартных настройках, это означает, что злоумышленник сможет вызвать те же эффекты непреднамеренно — и именно раннее выявление подобных уязвимостей делает инфраструктуру устойчивее.

Хотя вероятность побочных эффектов минимальна при стандартных настройках, сканер позволяет включать более агрессивный режим проверки. Это увеличивает нагрузку и риск временного воздействия на целевую систему. Перед запуском убедитесь, что у вас есть официальное разрешение на проведение сканирования.

2.3 Сканирование через сетевое оборудование

2.3.1 Общие сведения

Рекомендуется избегать проведения сканирования через такие устройства, как IDS/IPS, WAF, прокси-серверы и межсетевые экраны. Подобное оборудование может искажать сетевой трафик, что приводит к непредсказуемым результатам:

- ложноположительным или ложноотрицательным результатам;
- замедлению процесса сканирования;
- некорректному определению открытых портов;
- потере пакетов при превышении лимитов TCP-сессий;
- чрезмерной нагрузке на системы логирования или, наоборот, образованию «слепых зон» при отключении журналов.

Примечание

Аналогичные эффекты могут наблюдаться, если ограничено максимальное число проверок на один хост.

2.3.2 Особенности при работе через межсетевые экраны

В зависимости от модели межсетевого экрана, он может включать дополнительные модули — глубокий анализ пакетов (Deep Packet Inspection) или защиту от DoS-атак. Эти модули часто имеют ограниченные настройки: например, включение/отключение на уровне интерфейса без возможности указания конкретных IP-адресов.

Некоторые функции могут быть скрыты или недоступны для конфигурации, из-за чего перечисленные выше побочные эффекты могут возникать неожиданно.

При интенсивном сканировании нагрузка на межсетевой экран существенно возрастает. В крайнем случае это может привести не только к разрыву соединений для сканера, но и к частичной потере работоспособности самого устройства, что эквивалентно отказу в обслуживании.