# АВТОМАТИЗАЦИЯ ТЕСТОВ НА ПРОНИКНОВЕНИЕ

## ВОЗМОЖНОСТИ И ПРЕИМУЩЕСТВА

**Максим ПЯТАКОВ**
заместитель генерального директора, сооснователь CtrlHack

**Виктор СЕРДЮК**
генеральный директор АО «ДиалогНаука»

### ЧТО ЗАКАЗЧИК ХОЧЕТ ОТ ТЕСТА НА ПРОНИКНОВЕНИЕ?

За последние годы многие владельцы информационных систем поняли, что наиболее результативным методом оценки защищенности является проведение тестов на проникновение. Такие тесты позволяют посмотреть на свою сеть глазами хакера, выявить недостатки в системе защиты и подготовиться к возможным реальным кибератакам. Да и регуляторы все чаще выдвигают требования о необходимости проведения тестирований на проникновение на регулярной основе. Поэтому многие покупают услуги по проведению пентестов, а часть компаний создают свои внутренние команды по проведению тестов на проникновение или команды red team.

Основная цель, которая преследуется заказчиками при планировании таких работ — это имитация действий хакеров для оценки уровня реальной защищенности системы. При этом предполагается, что во время таких работ будет покрыта максимально возможная часть инфраструктуры. Хакеру же нельзя указать, в какой части инфраструктуры ему начинать и развивать атаку, а в какой нет. В крупных инфраструктурах, особенно территориально-распределенных, настройки могут отличаться настолько, что в одном месте какие-то из хакерских действий невыполнимы, а в другой части инфраструктуры эти же действия вполне могут иметь успех.

Однако в рамках выделенного времени и стоимости работ ни одна команда не сможет охватить всю инфраструктуру и проверить возможность выполнения максимального количества хакерских техник. В результате команды вынужденно фокусируются на действиях, которые можно выполнить достаточно быстро и которые чаще всего дают необходимый результат (конечно, исходя из опыта работ каждой такой команды).

### ПРОБЛЕМЫ «РУЧНЫХ» ТЕСТОВ НА ПРОНИКНОВЕНИЕ?

Рынок услуг по проведению тестов на проникновение хорошо развит. Есть большое количество компаний, готовых оказывать такие услуги. Однако у таких услуг есть свои минусы и ограничения. Если мы говорим о внешней команде, то каждый цикл работ это закупочные процедуры, заключение договоров, согласование ТЗ, приемка работ. Т.е. долго, сложно. Поэтому такие работы обычно выполняются один или два раза в год.

При этом практически невозможно гарантировать высокую квалификацию команды во время выполнения ручного теста на проникновение. Кроме того, фактически внешние люди получают доступ к информации о возможных уязвимостях тестируемой инфраструктуры с соответствующими рисками утечки такой чувствительной информации.

Что же с технической стороной выполнения тестов на проникновение? В связи с ограниченным временем выполнения работ команда обычно успевает проверить ограниченный набор техник для получения результата. При этом хакер не имеет таких ограничений. Если посмотреть на общую картину, то на данный момент известно и описано несколько сотен реализаций различных техник на разных шагах выполнения кибератак. Понятно, что ни одна из команд физически не сможет проверить даже 10–15% таких техник. Да в большинстве случаев для достижения результата им это и не нужно. Если в ходе работ команда смогла найти один

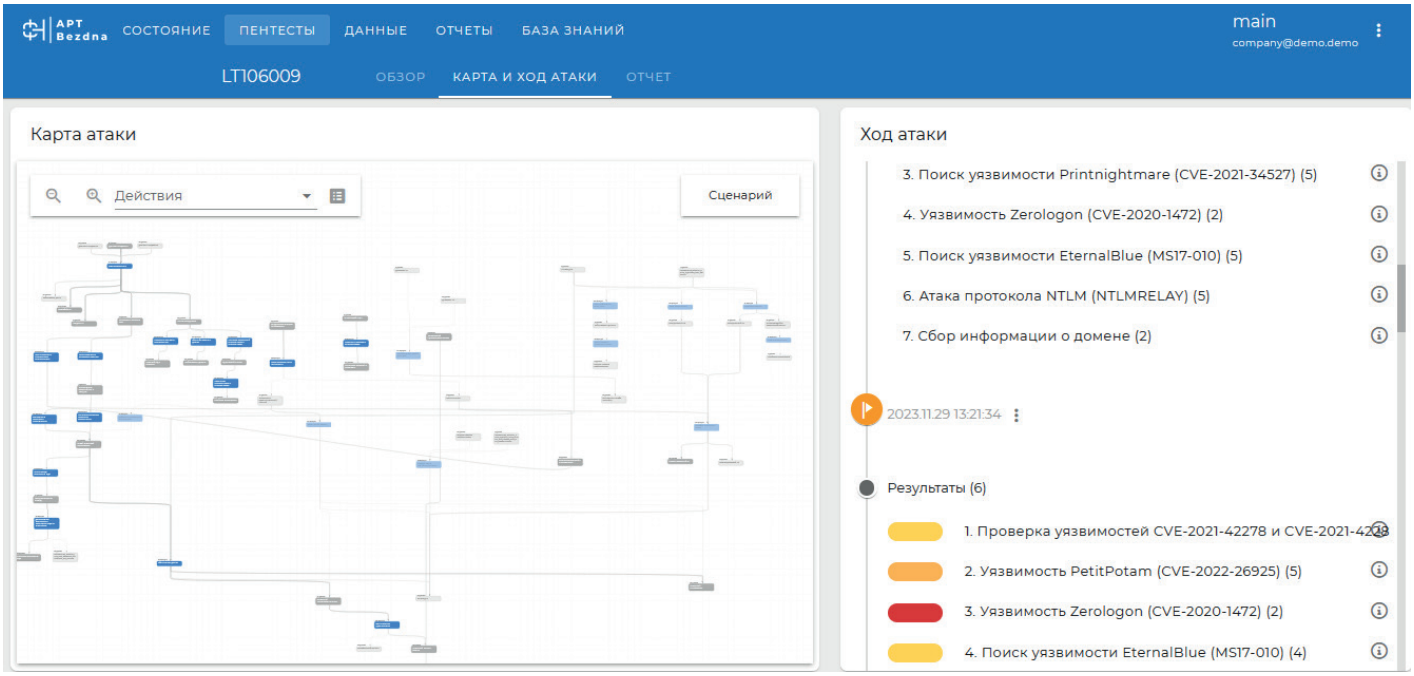


**Рисунок 1.** Сценарий атаки комплекса автоматического тестирования на проникновение CtrlHack APT Bezdna

вектор атаки, который успешно выполнился, то в большинстве случаев остальные возможные вектора не проверяются.

Сроки и ограничения по трудозатратам приводят также к тому, что проверками в рамках теста покрывается только часть инфраструктуры. Даже на первичном этапе внутреннего сканирования затрагивается обычно только небольшая часть машин и соответственно дальше атака в рамках теста распространяется также только по некоторому участку инфраструктуры. Также ни одна команда не сможет покрыть тестами большую часть машин в крупной сети (в которой может насчитываться несколько тысяч или даже десятков тысяч узлов). Как один из вариантов выхода из этой ситуации — заказывать работы, которые включают в себя выполнение тестов одновременно в разных сегментах сети. Но такие работы будут стоить значительно больших денег.

После окончания теста на проникновение исполнитель готовит отчет с описанием выявленных уязвимостей и несоответствий, и заказчик запускает процесс исправления выявленных недостатков. Но как проверить потом, что действительно ВСЕ недостатки исправлены? В большинстве случаев такие проверки откладываются до следующего запланированного теста. И во многих случаях выясняется, что не все было корректно исправлено. К сожалению, оперативно проверить качество устранения недостатков практически невозможно.

Как результат — оценка защищенности только раз в полгода или год, по ограниченному набору векторов атак и только для части инфраструктуры.

## ВНУТРЕННЯЯ КУХНЯ ТЕСТОВ НА ПРОНИКНОВЕНИЕ

Если мы говорим о «внутренних» тестах на проникновение, то такой тест (также как и реальная атака) состоит из набора шагов, которые позволяют выполнить закрепление, повышение привилегий, разведку, распространение в сети и т.д.

При этом большинство действий на этих шагах известны и описаны. А многие из этих действий не являются уникальными для каждого теста и могут использоваться без существенных изменений в разных сетях заказчиков. Некоторые операции могут быть уникальны, разрабатываться под конкретную сеть или требовать анализа человека. Но большинство операций рутинны и повторяются без существенных изменений из теста в тест. Команды, которые выполняют большое количество тестов на проникновение, для сокращения трудозатрат используют специальные скрипты или разрабатывают свои скрипты для автоматизации таких действий. Более того, часть векторов атак, например, связанных с атаками на контроллер домена с целью его захвата, могут выполняться в автоматическом режиме практически без участия человека.

## ПОМОЖЕТ ЛИ АВТОМАТИЗАЦИЯ?

Так как часть операций в рамках теста на проникновение можно автоматизировать, то возникает вопрос, а можно ли вообще выполнять такие тесты в автоматическом режиме и без привлечения специалистов из внешних команд? Ответ на него дали израильские разработчики, создавшие первую платформу автоматического тестирования на проникновение. Она позволила в автоматическом режиме выполнять ряд сценариев, выполняемых в рамках «внутреннего» теста на проникновение.

Такие системы позволяют устранить ряд недостатков «ручных» тестов:

- автоматизация поможет максимально покрыть инфраструктуру;

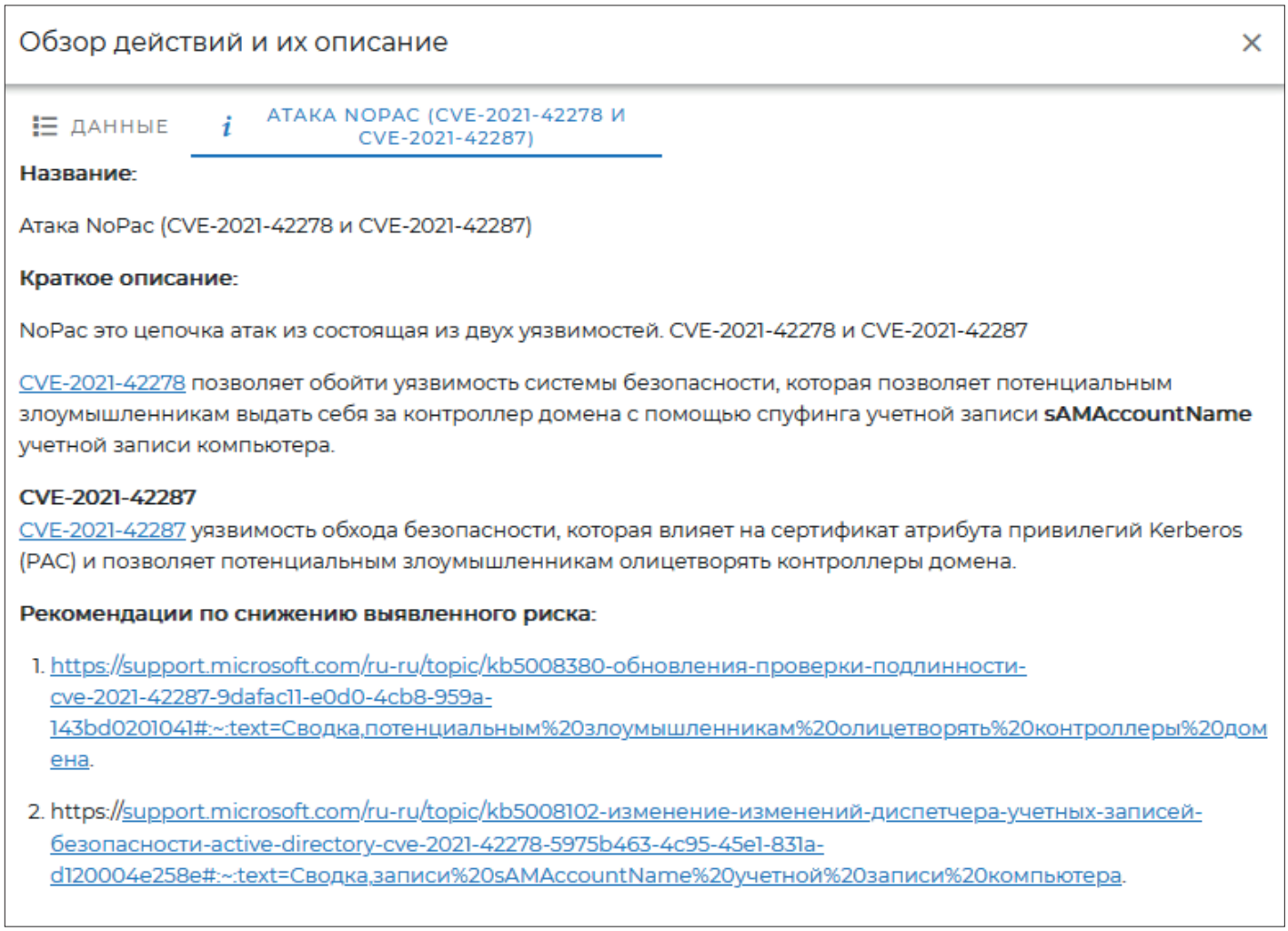


**Рисунок 2.** Описание найденных уязвимостей и рекомендации по устранению выявленных недостатков в платформе симуляции кибератак CtrlHack APT Bezdna

- автоматические сценарии могут использовать больше техник, чем человек в рамках своих работ;
- можно полностью повторить выполненный тест для проверки исправлений недостатков;
- можно делать тест на проникновение намного чаще и в то время, когда вам это нужно без привлечения внешних команд.

Как результат появляется возможность проводить постоянную оценку защищенности всей инфраструктуры компании (рис.1).

Безусловно, системы автоматического тестирования на проникновение не могут полностью заменить человека, и место для «ручного» теста на проникновение все равно остается, ведь нетривиальные действия автомат не сможет выполнить. Но при этом автоматизация основных и наиболее часто использующихся техник позволит существенно повысить защищенность инфраструктуры и на постоянной основе отслеживать возможные проблемы и недостатки с точки зрения безопасности сети. А для специалистов по тестам на проникновение остаются более сложные сценарии. В случае же наличия внутренней команды по тестам на проникновение автоматизация позволяет существенно повысить эффективность таких команд и избавить их от выполнения рутинных операций.

## ПЕРВАЯ РОССИЙСКАЯ ПЛАТФОРМА АВТОМАТИЧЕСКОГО ТЕСТА НА ПРОНИКНОВЕНИЕ

Российский разработчик платформ симуляции кибератак компания CtrlHack представила свой новый продукт — CtrlHack APT Bezdna. APT Bezdna — это комплекс автоматического тестирования на проникновение. Продукт предназначен для проведения тестов внутренней инфраструктуры. В разработке принимает участие команда «пентестеров» с большим опытом выполнения тестов у крупных корпоративных заказчиков. Свой опыт и глубокую экспертизу они переносят в сценарии, которые выполняются в рамках автоматических тестов. Комплекс позволяет одним кликом запустить тест с максимальным покрытием задач. По итогам выполнения теста предоставляется детальный отчет с рекомендациями по устранению выявленных недостатков (рис. 2). Результаты выполненного теста можно использовать для проведения последующих тестов и для приоритизации выявленных уязвимостей.