Зачем автоматизировать пентест

Максим Пятаков, *заместитель генерального директора/сооснователь CtrlHack*
Виктор Сердюк, *генеральный директор АО "ДиалогНаука"*


Фото: CtrlHack


Фото: ДиалогНаука

Тесты на проникновение стали неотъемлемой частью работ по оценке защищенности информационных систем. Многие компании осознают, что такой тест является одним из наиболее действенных способов проверить инфраструктуру и подготовиться к возможным киберугрозам.

Цели пентеста на стороне заказчика

Некоторые компании создают свои внутренние команды для проведения тестов на проникновение, или команды red team, но большинство покупают услуги по проведению пентестов у внешних подрядчиков.

Оба варианта подразумевают проведение имитации атаки с максимальным покрытием на информационные системы заказчика, чтобы определить уровень защиты компании, а также имеющиеся уязвимости. Обычно для этих целей предоставляется максимальная свобода действий "белому" пентестеру, так как нет какого-то определенного "кодекса" хакера, который будет ограничивать выбранные векторы атаки. Но мы знаем, что любая команда все равно ограничена в ресурсах и вынуждена применять инструментарий, который с профессиональной точки зрения способен дать нужный эффект наиболее оперативно.

Сложности ручного пентеста

На рынке информационной безопасности за несколько десятков лет, по мере его развития, появилось много разных компаний и специалистов, которые вполне успешно и профессионально оказывают услуги по проведению тестов на проникновение. Но, как обычно, есть нюансы: у собственных специалистов компании может быть высокая загрузка, не до конца отлаженные внутренние рабочие процессы и т.д., а при обращении ко внешним исполнителям нельзя до конца быть уверенными в квалификации команды, кроме того есть обязательные циклы согласования ПЗ, КП, ТЗ, договора, закупки, приемки работ и прочие действия. Это все требует большого количества времени, из-за чего пентест возможно выполнить не чаще 1–2 раз за год. Продолжая мысль о внешних специалистах: они могут получить (и наверняка получат) чувствительную информацию, нежелательную для распространения, неаккуратное обращение с которой (или злой умысел) могут привести к утечке и неблагоприятным последствиям для заказчика.

Еще одной проблемой является то, что заказчик перед выполнением работ не имеет представления о методах и техниках, которые будет применять внешняя команда пентестеров, и не может влиять на набор таких методов. В результате в итоговом отчете о проведенном пентесте заказчик может и не увидеть описание части методик, которые, например, не привели к получению какого-либо результата при выполнении работ. А эта информация является важной, потому что показывает заказчику, от каких методов та часть его инфраструктуры, в которой проводились работы, защищена, и, соответственно, не позволяет ему самому проверить эти же методы в других частях инфраструктуры.

В силу различных ограничений не все технические средства и методики доступны для реализации на стороне пентестеров, что вынуждает команду использовать наиболее вероятные с точки зрения успешной реализации инструменты для проведения успешной атаки. Но все желаемые и вероятные варианты реализовать не получится. В лучшем случае это будет десятая часть из всех возможных, а успешная реализация взлома часто приводит к тому, что остальные варианты уже не рассматриваются. Потенциальный злоумышленник не имеет большого количества ограничений и может успешно провести атаку с нескольких векторов, непроверенные способы ее исполнения останутся за скобками.

Сроки и ограничения по трудозатратам приводят к тому, что проверками в рамках теста покрывается только часть инфраструктуры. Даже на первичном этапе внутреннего сканирования затрагивается обычно только небольшая часть машин, а дальше атака в рамках теста распространяется только по некоторому участку инфраструктуры. Ни одна команда не сможет покрыть тестами большую часть машин в крупной сети, в которой может насчитываться несколько тысяч или даже десятков тысяч узлов. 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 дороже.

После окончания теста на проникновение исполнитель готовит отчет с описанием выявленных уязвимостей и несоответствий, а 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. В результате – оценка защищенности только раз в полгода или год, по ограниченному набору векторов атак и только для части инфраструктуры.

Индивидуальный подход или стандартные практики?

На практике многие действия злоумышленников хорошо изучены и в основе своей не сильно меняются, поэтому пентестеры знают множество вариаций стандартных сценариев проведения атаки на объект и, исходя из своей практики, делают проверку устойчивости компании именно к данным типам взлома. Пишутся и исполняются рутинные пошаговые скрипты для исполнения действий возможного нарушителя, проверяются известные методики проникно-

вения в информационные системы и реализуются другие шаблоны поведения потенциального злоумышленника.

Для большинства компаний этих методов будет достаточно, чтобы выявить потенциальные угрозы для организации. Бывают редкие случаи, когда заказчики могут (или готовы) позволить себе повышение трудозатрат на пентест либо под инфраструктуру компании требуется уникальный инструментарий или нестандартные методики, но в большинстве случаев действия пентестеров достаточно консервативны.

Непрерывность пентеста

"Ручной" пентест может выполняться достаточно редко, в большинстве случаев это один раз в полгода или год. Но в реальности такие работы нужно проводить постоянно. Причин для этого несколько:

1. Постоянные изменения в инфраструктуре и настройках информационных систем. Иногда применение новых настроек может привести к тому, что хакерская техника, которая при прошлом пентесте не выполнялась, теперь стала выполняться.

2. Частое появление новых уязвимостей, которые появляются не один раз в полгода. Кроме выявления потенциальных уязвимостей в сети (можно сделать сканером уязвимостей), нужно проверить, возможна ли эксплуатация данной уязвимости и возможно ли в результате этой эксплуатации развить атаку дальше в инфраструктуре. Опыт подсказывает, что новые уязвимости после выхода эксплойта начинают активно эксплуатироваться в атаках в первый же месяц.

3. На некоторых шагах пентеста могут выявляться "слабые" пароли учетных записей или повышенные привилегии для отдельных учетных записей. Так как эти ситуации могут возникать в любой момент времени, такие проверки также нужно проводить на постоянной основе.

Все проверки, описанные выше, нужно выполнять на постоянной основе. То есть должна быть возможность выполнять фактически непрерывный пентест инфраструктуры. Задача хорошая, но не решаемая без средств автоматизации.

Вопрос автоматизации

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? Полностью исключить выполнение "ручных" работ не получится, но выполнять большинство действий в автоматическом режиме сейчас вполне возможно. На рынке есть решения, которые позволяют выполнять пентест в автоматическом режиме и покрывают большинство повторяющихся и рутинных операций, выполняемых командами пентеста.

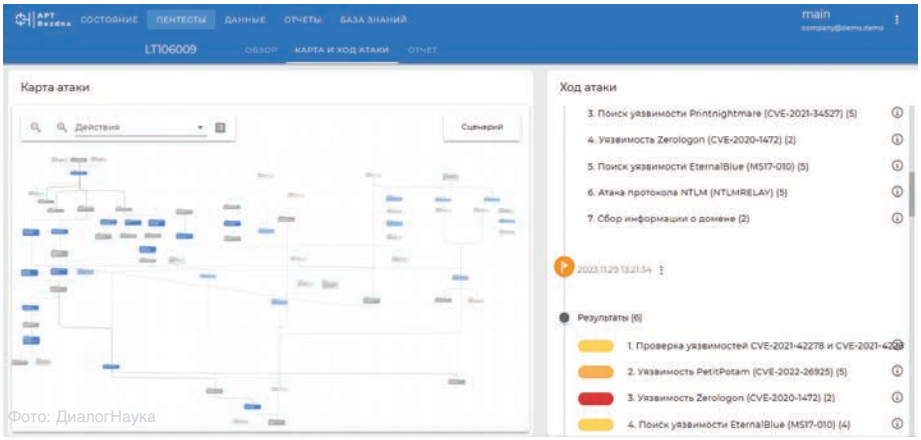

Рис. 1. Карта атаки при пентесте от CtrlHack APT Bezdna

До недавнего времени на российском рынке было представлено израильское, а в этом году российские разработчики представили и отечественное решение данного класса.

Эти решения позволяют 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;
- 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, и фактически решить задачу непрерывного пентеста.

Как результат появляется возможность проводить постоянную оценку защищенности всей инфраструктуры компании (см. 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 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.

Рис. 2. Обнаруженные уязвимости и рекомендации по их устранению в интерфейсе CtrlHack APT Bezdna

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 (см. рис. 2). Результаты выполненного теста можно использовать для проведения последующих тестов и для приоритизации выявленных уязвимостей. ●