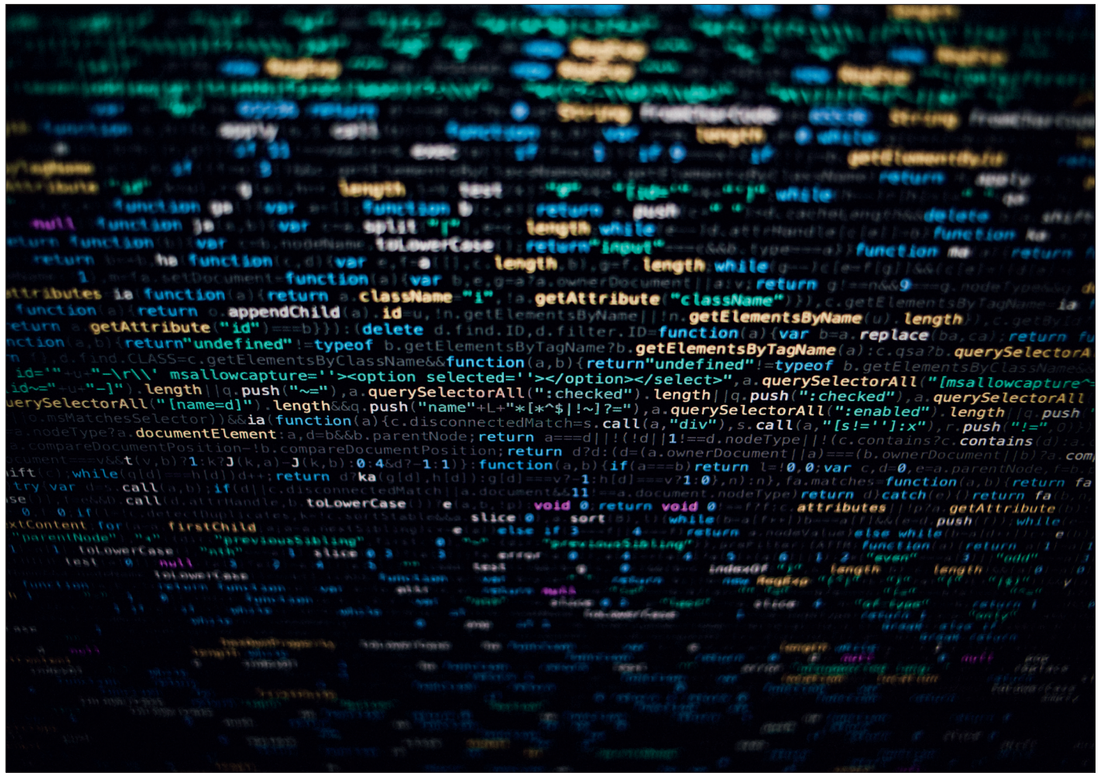
Виктор СЕРДЮК
генеральный директор
АО «ДиалогНаука»

Роман ВАНЕРКЕ
технический директор
АО «ДиалогНаука»

ВНИМАНИЕ, РОБОТ-ПЕНТЕСТЕР!

BAS — НОВЫЙ ИНСТРУМЕНТ ДЛЯ АВТОМАТИЗАЦИИ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ



В эпоху цифровой трансформации компаниям приходится заниматься защитой своих цифровых активов. Однако, как можно гарантировать, что злоумышленники не доберутся до наиболее ценных ресурсов цифрового бизнеса? Необходимо регулярно проводить оценку защищённости своих информационных систем. До недавнего времени для этого использовали либо автоматические сканеры уязвимостей, либо услуги внешних специализированных организаций, которые имитировали проникновение в корпоративную сеть — так называемые пентесты. Не так давно на рынке информационной безопасности появился новый класс решений — BAS (Breach and Attack Simulation), который и будет рассмотрен в данной статье.

ПЕНТЕСТ VS САМООЦЕНКА

Внутренний аудит с помощью сканера уязвимостей имеет свои преимущества в том, что служба безопасности контролирует этот процесс и не допустит нарушения работоспособности системы во время проведения тестирования. Процесс поиска уязвимостей обычно запускается во время, когда возможный сбой в информационных системах принесёт минимальный ущерб. Впрочем, современные средства поиска уязвимостей работают достаточно эффективно и не создают чрезмерной нагрузки на сеть и проверяемые узлы, как это было на начальных этапах развития этого класса продуктов. Однако не стоит забывать, что сканеры проверяют только технические уязвимости, не тестируя уязвимости в архитектуре, а также не используют так называемую социальную инженерию. Кроме того, результаты сканирования оценивают те же люди, что и создавали систему, и они не всегда могут адекватно оценить опасность тех или иных уязвимостей.

Внешние пентестеры могут использовать более широкий спектр векторов атак и методов проникновения. Они проверяют не только технические уязвимости, но также могут выявить и архитектурные проблемы, и неправильную работу персонала с внешними обращениями. Пентестеры имитируют деятельность хакеров, что позволяет более адекватно оценить защищенность информационных систем во время реальных атак. При этом пентестеры вынуждены скрываться от систем обнаружения, что позволяет проверить, в том числе, и эффективность работы средств защиты при обнаружении постороннего присутствия — работу сканеров они фиксируют достаточно быстро.

Впрочем, самое главное преимущество пентеста в том, что внешней команде исследователей приходится проходить все те же этапы проникновения, что и реальным злоумышленникам. Им также приходится собирать информацию об используемых программных устройствах, сервисах и базовых компонентах, искать уязвимости в этих компонентах и разрабатывать эксплойты для проникновения с учётом используемых в компании средств защиты. Если первичное проникновение прошло успешно, они, также как и реальные хакеры, изучают внутреннюю сеть компании и стараются получить доступ к ценной информации внутри сети. Полная цепочка действий от изучения до вывода ценной информации получила название Kill chain. Внутренние тестировщики останавливаются на первых двух этапах исследования и проникновения, не тестируя сам процесс реагирования системы защиты на реальную атаку.

В то же время большинство экспертов в безопасности уже говорят о том, что защититься от проникновения невозможно — рано или поздно будет обнаружена уязвимость, которая не учитывалась при самооценке и которую хакеры смогут проэксплуатировать. Поэтому при построении системы защиты не стоит забывать о таких важных элементах системы, как обнаружение вторжений, блокирование утечки конфиденциальной информации, проведение расследования инцидентов и совершенствование системы защиты. Именно эти элементы и может протестировать команда пентестеров. А главное, группа специалистов по безопасности сможет получить ценный опыт предотвращения проникновения, реагирования на атаку и проведения расследования — поучаствовать в своеобразных киберучениях.

В принципе, альтернативой внешним пентестерам может являться собственная команда аудиторов, получившая наименование Red Team. Она должна быть независимой и работать по тем же принципам, что и внешние пентестеры, однако в реальности и эта команда нарабатывает собственные приёмы, которые могут оказаться недостаточно универсальными. Поэтому и такая независимая самооценка может дать недостаточно точный результат. Необходимо также отметить, что использование собственной команды пентестеров, требует значительных финансовых затрат, что могут позволить себе только компании со значительными бюджетами на обеспечение информационной безопасности.

BAS-АВТОМАТИЗАЦИЯ

Для автоматизации работы пентестеров начали появляться инструменты, которые позволяют роботизировать все этапы проведения теста на проникновение, точнее, всей цепочки kill chain. Эти инструменты получили наименование Breach and Attack Simulation (BAS). От сервисов удалённого тестирования на уязвимости — так называемых облачных сканеров — данные решения отличаются тем, что так же как и при пентесте проверяют все вектора возможной атаки и позволяют службам ИБ предприятия на регулярной основе проверять эффективность применяемых средств защиты информации.

Предполагается, что BAS-платформы выполняют следующие функции:

- исследование / рекогносцировка. BAS-решение симулирует все методы получения первичной информации для проникновения, которые используют хакеры. Как правило, для этого используется сканирование внешнего периметра компании для выявления всех возможных узлов и сервисов, через которые потенциально может быть реализована атака.
- Проникновение. На этапе проникновения сканеры тестируют периметр на уязвимости, как это делают и другие средства поиска уязвимостей. Однако BAS-решения проводят также и имитационные тесты, например, с помощью специальных фишинговых рассылок с вредоносным кодом. Этот этап позволяет оценить не только уровень осведомлённости сотрудников компании, но и эффективность работы шлюзов безопасности, которые должны обнаружить вредоносный код. Аналогичным

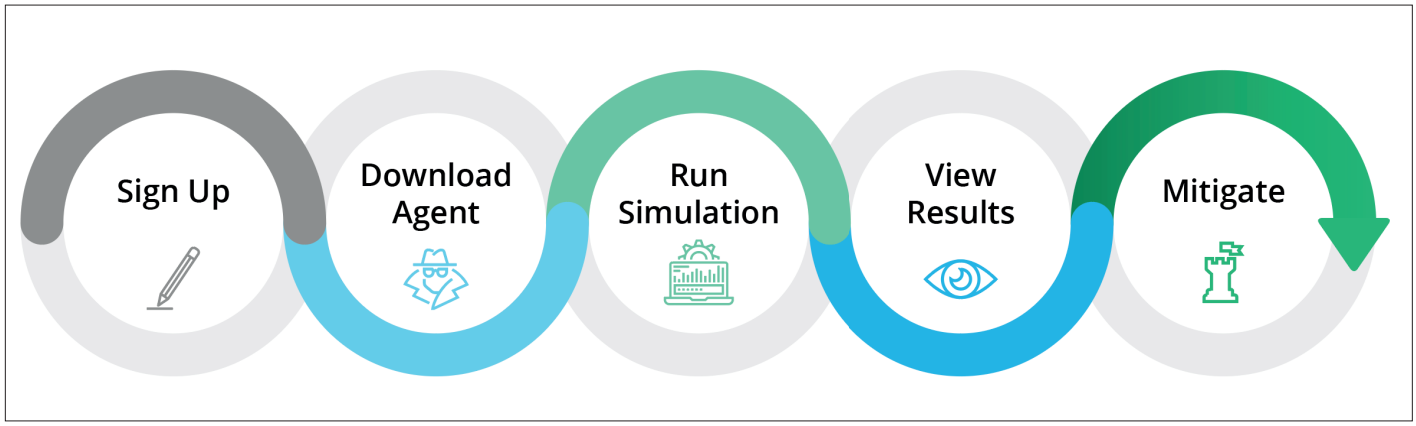


Схема работы сервиса Cymulate. Источник: https://cymulate.com/how-it-works/

образом тестируется и использование веб-браузеров на возможность проникновения. С помощью ссылок на специальным образом скомпрометированные сайты BAS-решение проверяет уязвимости в веб-браузерах, а также шлюзовых систем безопасности.

◆ Внутреннее исследование. Следующим этапом проникновения является закрепление в системе, для чего хакеры взламывают рабочие станции и сервера, устанавливая в них модули для удалённого управления. BAS-решение тестирует защиту конечных точек — антивирусов и EDR, имитируя при этом действия злоумышленников для перемещения внутри корпоративной сети с использованием стандартных средств удалённого администрирования, входящих в состав операционных систем. Для этого могут использоваться специальные программные агенты, устанавливаемые на рабочие станции пользователей.

◆ Кража конфиденциальной информации. Заключительным этапом хакерской атаки обычно является вывод конфиденциальной информации за пределы корпоративной сети. Поэтому BAS-решения также пытаются передать вовне корпоративной сети обнаруженную информацию, на которую DLP должна среагировать. Таким образом, в этом случае тестируется эффективность DLP-систем в части обнаружения и блокирования попыток утечки конфиденциальной информации. Причём в качестве каналов утечки используются не только стандартные векторы, такие как Web-почта или HTTP, но и скрытые, типа DNS- или ICMP-VPN.

Таким образом, BAS-решения автоматизируют проверку не только уязвимостей в используемом компанией ПО и оборудовании, но и организует своеобразные учения для служб информационной безопасности, в рамках которых появляется возможность отработать процедуры реагирования на различные этапы хакерских действий со стороны сотрудников службы информационной безопасности.

На сегодняшний день на рынке уже представлен целый ряд продуктов, относящихся к категории BAS-решений. Одним из примеров такого решения является сервис Cymulate, который позволяет реализовать каждую из перечисленных выше проверок через сеть Интернет. При этом часть проверок осуществляется удалённо, а для некоторых тестов требуется установка агента в корпоративной сети компании. Результаты работы сервиса предоставляются клиентам в виде отчётов, которые можно использовать для совершенствования своей системы защиты.

Сервис Cymulate включает в себя следующие вектора атак для тестирования системы защиты организации:

◆ Immediate threat alert assessment — регулярно тестирует периметр корпоративной сети с использованием актуальных на момент тестирования угроз;

◆ Email security assessment — проверяет работу средств защиты, контролирующих электронную почту;

◆ Web gateway assessment — тест веб-фильтра и других компонентов защиты, контролирующих протокол HTTP/HTTPS;

◆ Lateral movement assessment — тестирование внутренних средств сегментирования и межсетевого экранирования корпоративных сетей;

◆ Endpoint assessment — проверка работы средств защиты, установленных на рабочих станциях и серверах;

◆ Data exfiltration assessment — проверка для систем DLP;

◆ Phishing assessment — проверяет реагирование сотрудников компании на фишинговые сообщения, а почтовые шлюзы — на защиту от массовых рассылок подозрительной корреспонденции;

◆ SOC/SIEM simulation — комплексное тестирование на проверку и отработку действий сотрудников служб реагирования на инциденты.

Таким образом, сервис Cymulate предлагает полный спектр проверок, относящихся к категории BAS, причём без покупки дополнительного оборудования и программного обеспечения. Сервисы предоставляются по модели подписки через Интернет с помощью бесплатного агента для управления процессом тестирования.

***

Аналитики компании Gartner, которые ввели в обиход термин BAS, надеются, что инструменты данного класса постепенно дополнят услуги «ручных» тестов на проникновение, которые часто не дают общей картины защищённости корпоративной сети. Использование инструментов данного класса позволит на регулярной основе получать информацию о реальном уровне защищённости организации от внешних и внутренних угроз.