Автоматизация пентеста: на шаг впереди хакера

Валерий Филин, *технический директор CITUM*
Павел Стеблянко, *генеральный директор CITUM*
Виктор Сердюк, *генеральный директор АО "ДиалогНаука"*

Эффективная защита от угроз информационной безопасности возможна только при комплексном подходе. Одним из его ключевых элементов является своевременное обнаружение и устранение уязвимостей. Традиционно решение этих задач осуществляется двумя способами: с использованием специализированных средств для сканирования уязвимостей (так называемых сканеров безопасности) или посредством тестирования на проникновение (пентеста) с привлечением высококвалифицированных специалистов, которые могут взглянуть на систему защиты организации "глазами хакеров". Однако, помимо очевидных преимуществ, традиционные методы имеют и ряд ограничений.

Сканеры безопасности, например, обычно генерируют отчеты, насчитывающие сотни страниц с информацией о выявленных уязвимостях, среди которых практически невозможно выделить те, которые действительно представляют наибольшую опасность для организации. Услуги по тестированию на проникновение обычно занимают много времени и дорого стоят. При этом они дают заказчику "текущий срез", актуальный только в один момент времени.

Для устранения ограничений традиционных методов анализа защищенности на рынке информационной безопасности появился новый класс решений для автоматизации тестирования на проникновение. В этой статье мы детально раскроем описанные проблемы и расскажем о платформе автоматизации пентеста – Pcysys PenTera.

Установка патчей – не панацея от угроз

Вслед за тем как компании внедряют новые информационные системы, количество потенциальных уязвимостей, которым они подвержены, растет с экспоненциальной скоростью. Беглый взгляд на базу данных уязвимостей National Vulnerability Database[1] показывает, что в последние годы произошел резкий всплеск их количества, особенно в приложениях с открытым исходным кодом. Публично доступные эксплойты для этих уязвимостей – лишь наиболее простые из инструментов хакера.

Приоритизация и закрытие уязвимостей для крупной компании может оказаться титанически сложной задачей. В организациях, где серьезно относятся к вопросам ИБ, обычно есть выделенная команда, специализирующаяся на выявлении и устранении уязвимостей, однако высоки шансы того, что сотрудники не успеют охватить их все. Установка патчей, как правило, приоритизирована: большинство организаций фокусируют внимание на устранении уязвимостей, имеющих наивысший теоретический уровень критичности. Даже если вы успеваете ликвидировать уязвимости с уровнем опасности "критичная" и "высокая", скорее всего вы отталкиваетесь от статистической шкалы CVSS (Common Vulnerability Scoring System[2]). Эта универсальная шкала по умолчанию не учитывает контекст вашей сети, приложений и массивов данных, поэтому оценка степени критичности статичных уязвимостей на основе CVSS, как правило, не является полностью релевантной для конкретного окружения и носит теоретический характер.

Нет сомнений, что обнаружение уязвимостей и установка патчей – жизненно необходимые задачи для сокращения поверхности атаки. Но даже после установки всех обновлений вы все еще можете быть взломаны.

Неочевидные точки входа

Существует ряд значимых аспектов, которые остаются без внимания систем управления уязвимостями. К ним относятся так называемые динамические уязвимости, связанные с небезопасным пользовательским поведением, небезопасной конфигурацией инфраструктуры, ошибками в настройках внедренных средств защиты, нестойкими паролями и недостаточным контролем за привилегированным доступом.

Как правило, хакерская атака начинается через эксплуатацию динамических уязвимостей. Точкой входа в сеть может служить рабочая станция, куда злоумышленник успешно проникает, например, с использованием техник социальной инженерии. Попав внутрь сети, атакующий изучает и оценивает ее, выполняет горизонтальное продвижение, используя доступные средства для достижения конечной цели своей атаки.

Для борьбы с наиболее сложными целенаправленными атаками целесообразно прибегать к методу оценки эффективности применяемых средств защиты

[1] *https://nvd.nist.gov/*
[2] *https://www.first.org/cvss/*

с позиции злоумышленника. Во время атаки необязательно использовать критические уязвимости, выявляемые сканерами. Терпеливо изучив сеть и средства защиты, злоумышленники могут прибегнуть к инструментам, специально разработанным для эксплуатации уязвимостей со средней или даже низкой критичностью по шкале CVSS.

Важно отметить, что возможности атакующих довольно обширны: наиболее известная отраслевая база знаний по техникам атак MITRE ATT&CK Matrix[3] описывает сотни различных приемов, сгруппированные в 12 категорий.

Атакующие постоянно совершенствуют и развивают свои навыки и пополняют арсенал используемых средств. Как только становится известно о новых эффективных техниках реализации атак, они мгновенно получают распространение через "теневой Интернет" (Dark Web[4]) и специализированные хакерские сообщества.

Зачем автоматизировать пентест?

Попытка защитить себя без понимания точки зрения злоумышленника – невероятно сложная задача. Традиционный подход к тестированию на проникновение дает вам статичный снимок того, как атакующий может взломать сеть в конкретный момент времени. В большинстве случаев пентест – это недостаточно регулярная процедура, выполняемая один или два раза в год. Современные сети меняются динамично, из-за чего результаты пентеста устаревают за считанные дни.

Ответить на этот вызов позволяет машинный пентест, который обходит названные ограничения и дает вам возможность круглосуточного наблюдения за состоянием защиты, предоставляя выводы и рекомендации, релевантные именно вашим информационным системам.

Преобразование пентеста в доступный ежедневный метод проверки позволяет защищающейся стороне первой узнавать об эксплуатируемых уязвимостях и исправлять их до того, как злоумышленник сможет найти и использовать их в атаке. Кроме того, автоматизированный пентест дает возможность сфокусироваться на исправлении именно тех уязвимостей, которые в реальной жизни могут эксплуатировать хакеры.

Злоумышленники уже давно автоматизируют свою деятельность и применяют для атак специализированные комплексные решения. Команды безопасности в организациях продолжают использовать классический набор отдельных инструментов для ручного тестирования защиты, который зачастую отстает от соответствующего инструментария хакеров. Таким образом, автоматизация пентеста дает возможность существенно упростить и повысить эффективность предотвращения атак.

5 преимуществ автоматизации пентеста

Автоматизация пентестов дает службе ИБ множество уникальных преимуществ:

1. Позволяет выполнять тестирование на проникновение с беспрецедентной скоростью, демонстрируя общую картину реальных рисков в течение нескольких часов вместо дней или даже недель.

2. Благодаря высокой скорости работы тестирование защищенности можно выполнять в полном масштабе инфраструктуры.

3. Вы можете проверять свою сеть как угодно часто – ежемесячно, еженедельно или даже ежедневно, получая непрерывную оценку, недостижимую в случае ручного пентеста.

4. Непрерывный анализ защищенности позволяет выявлять редкие или "плавающие" уязвимости, равно как векторы атак, доступные в течение непродолжительного времени.

5. Автоматизация позволяет протестировать сценарий скрытного терпеливого злоумышленника, который неделями находится в сети, никак себя не обнаруживает и ждет удачного момента для взлома. Такой сценарий практически невозможно воспроизвести по запросу в рамках обычного пентеста, выполняемого приглашенным подрядчиком.

PCYSYS PenTera – новый подход к кибербезопасности

Большинство служб информационной безопасности сталкиваются с проблемами наличия бюджета и квалифицированных кадров. Именно поэтому для оптимизации затрат и повышения эффективности работы автоматизируются процессы кибербезопасности, включая оценку рисков, установку обновлений, обнаружение и предотвращение вторжений и др. В сфере автоматизации процессов тестирования на проникновение лидирует компания Pcysys.

Автоматизированный пентест дает глубокое понимание контекста слабых мест и уязвимостей в сети, а также позволяет оптимизировать процесс установки патчей. Вместо применения традиционного подхода к устранению уязвимостей на основе шкалы CVSS вы можете начать с исправления того, что действительно несет максимальный риск для вашей организации. После устранения наиболее критичных проблем можно немедленно запустить повторную проверку сценария атаки, чтобы убедиться в эффективности принятых мер. Таким образом, вы всегда остаетесь на шаг впереди атакующего.

Анализ защищенности со всех сторон

Pcysys PenTera – это программная платформа, предназначенная для автоматизации пентеста. Простым нажатием кнопки вы сможете проверить, защищена ли ваша ИТ-инфраструктура, и выявить проблемы разной степени критичности, которые необходимо устранить для предотвращения потенциального взлома сети.

Эта система имеет целый ряд плюсов:

1. Pcysys PenTera может непрерывно выполнять оценку защищенности сети. Вместо ежеквартального или ежегодного пентеста вы можете оценивать уровень защищенности постоянно, и все это без дополнительных инвестиций или существенных затрат ресурсов. Вы можете запустить задачу проверки и заняться повседневными делами, а по завершении тестирования получить от системы отчет с рекомендациями по устранению слабых мест.

2. PenTera показывает модель реального хакера. Это не симуляция, а реальный взлом организации, выполняемый безопасным способом с применением этических вредоносных инъекций и хакерских приемов. Система покажет объективную оценку защищенности сети организации в условиях, максимально близких к реальному взлому, и продемонстрирует пошаговые векторы атак с подробным описанием каждого этапа. При этом эксплуатация выполняется безопасным образом, не приводя к прерыванию критичных сервисов и бизнес-процессов.

3. PenTera помогает приоритизировать устранение уязвимостей и слабых мест в сети организации, выводя процесс на новый, экономически эффективный уровень. Сканеры анализа защищенности показывают десятки тысяч уязвимостей (есть даже сети с более чем миллионом уязвимостей), что сильно усложняет процесс их устранения. PenTera фокусирует процесс устранения в первую очередь на фактически подтвержденных и опасных векторах атак.

Эффективное решение для любой отрасли

Технология Pcysys PenTera не привязана к какой-либо конкретной отрасли. Сеть – везде сеть, будь то в финансовой, производственной или другой организации. В числе заказчиков Pcysys есть банки, фонды, инвестиционные и страховые компании, телеком-операторы, ИТ-компании, юридические организации, ритейл, образовательные учреждения, организации из сферы здравоохранения и др.

Pcysys PenTera позволяет существенно повысить уровень защищенности компании за счет обеспечения непрерывной оценки текущего уровня безопасности с позиции реального злоумышленника. Система дополняет существующие средства защиты, такие как SIEM или решения по управлению привилегиями, и успешно интегрируется с ними.

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

[3] https://attack.mitre.org/matrices/enterprise/
[4] https://en.wikipedia.org/wiki/Dark_web