ITD GROUP

Vulnerability Scanners, Pentests и Red Teaming vs Breach Attack Simulation (BAS)

CTRLHACK

Сканирование уязвимостей и пентесты полезны для получения представления о состоянии безопасности организации в определенный момент времени. Однако они не дают полной картины состояния; особенно, когда речь идет о более изощренных атаках.

Наиболее эффективный способ для организации проверить свою устойчивость к растущей волне киберпреступности — выбрать целевые симуляции атак, в которых используются различные многовекторные атаки с применением широкого спектра техник.

Именно к этому виду проверок относятся решения симуляции взлома и атаки (BAS). Инструменты BAS помогают сделать меры безопасности более последовательными и автоматизированными.

Vulnerability Scanners

Сканирование уязвимостей выполняется приложением, которое может быть проприетарным или с открытым исходным кодом.

Это приложение проверяет уязвимости, которые уже известны поставщикам и отрасли, или слабые места, которые уже использовались киберпреступниками.

Сканируются тысячи различных уязвимостей в сетях или системах, таких как программные ошибки, отсутствующие патчи ОС, уязвимые службы, небезопасные настройки по умолчанию и уязвимости веб-приложений.

Сканирование используется для помощи в автоматизации процесса аудита безопасности ИТ организации. Сканируя сети и веб-сайты на наличие тысяч различных угроз безопасности, подобная система, как правило, становится в определенной мере центральной частью кибербеза организации.

Плюсы:

- Автоматизируется, можно планировать, относительно просто в использовании
- Обнаруживает известные уязвимости
- Относительно быстро (в среднем по мировому рынку), может дать результат в течение нескольких часов
- Не требует специальных знаний
- Дает информацию по последним эксплойтам
- Может быть более экономичным, чем традиционный пентест
- Возможность выполнения нескольких сканирований одновременно

Слабые места:

- Отсутствие обзора процесса. Сканер предоставляет только некоторый снимок и зачастую не дает существенного понимания и конкретики.
- Невозможно обнаружить уязвимости, которые еще не были сопоставлены в рамках сканирования или обновления (при пассивном скане). Время между обновлениями подвергает организации риску.
- Дает относительно высокий уровень ложных срабатываний (по средним оценкам, 30–60 %).
- Зачастую отсутствует соответствующий сценарий угрозы модели противника.
- Требуется постоянная и частая актуализация баз.
- Предназначен для некритичных систем; гораздо реже в реальности применяется для критических систем реального времени.
- Может создать нагрузку на продуктивную систему, что может привести к простою.

Резюме

Сканирование уязвимостей может найти только известную уязвимость или угрозу. Поскольку процесс дальнейшей обработки полученных сканом данных влечет за собой только обновление и/или исправление системы, неправильная конфигурация или неправильное использование инфраструктуры и решений безопасности не будут устранены.

Pentests

Ручной пентест проводится силами специалистов, которые пытаются оценить безопасность инфраструктуры, работая с уязвимостями.

Эти уязвимости могут присутствовать в ОС, службах или приложениях из-за неправильной конфигурации или из-за специфического поведения конечного пользователя.

Другими словами, корпоративная сеть, приложения, устройства и/или люди подвергаются атаке, чтобы проверить, сможет ли хакер проникнуть в организацию.

Тесты также показывают, насколько глубоко может проникнуть злоумышленник и сколько данных может быть украдено или использовано.

Слабые места:

- Успех зависит от навыков и опыта каждого отдельного пентестера.
- Не выявляет все слабые места, которыми пользуются злоумышленники из-за ограниченной области пентеста (слабые возможности масштабирования).
- Тестер зачастую не может использовать все методы атаки, которые он изучил за предыдущие годы.
- Получение отчета об оценке занимает много времени (недели).
- Не обеспечивает всестороннего понимания, поскольку ручное тестирование не может проверять все аспекты системы (например, строки кода, декомпилированную сборку, веб-страницы и параметры, веб-сервисы и т. д.), в отличие от автоматизированных инструментов
- Результаты ручных пентестов отражают конкретный момент времени. Они не выполняются с высокой частотой из-за больших затрат.

Плюсы:

- Выявляет слабые места, которые не обнаруживаются при сканировании уязвимостей
- Выявляет выбранные слабые места с высоким риском
- Пентестер может узнать о новых угрозах раньше
- Отчет об оценке может быть использован для устранения недостатков инфраструктуры
- Предоставляет возможность тренинга для сетевой безопасности

Резюме

Пентест позволяет осуществлять «узкие» проверки, на которых не фокусируются сканеры или BAS. Например, поиск файлов с паролями. В пентестах больше связанного с человеческим фактором. Они позволяют отследить, как работают сотрудники, насколько соблюдаются регламенты.

Red Teaming

Целевые смоделированные атаки (или Red Teaming) позволяют использовать упреждающий подход, помимо выявления слабых мест в системе безопасности организации, они также могут предоставить ценную информацию о способности организации выявлять текущие атаки и устранять их из среды.

Многоэтапные атаки используются для имитации различных типов злоумышленников, а также для выявления пробелов в средствах управления информационной безопасностью с помощью оптимизации имитации.

Слабые места:

- Моделирование должно проводиться регулярно
- Требуется внутренняя или внешняя экспертиза (довольно серьезная)
- Требуется последующая деятельность для снижения рисков (плотная работа по интерпретации результатов, выстраиванию процессов по их обработке и контролю изменений, в том же ручном формате)
- Необходимо соблюдать политику безопасности организации в соответствии с различными нормативными актами (усложняет процесс интерпретации и обработки).
- Директорам по информационной безопасности и ИТ-командам может быть трудно оценить степень эффективности.

Плюсы:

- Имитирует тактики, техники и процедуры (TTP), применяемые реальными злоумышленниками.
- Готовит организацию к кибератакам в реальном мире, выполняя смоделированные атаки для заданных сценариев угроз.
- Проактивный подход.
- В какой-то мере это может быть более экономично, чем ручные пентесты.
- Обнаруживает неизвестные проблемы в неочевидных местах инфраструктуры
- Позволяет оценивать операции по обеспечению безопасности/возможности мониторинга.

Резюме

Задача Red Team — пройти из точки А в точку Б за определённое количество времени. При этом удается использовать сильно ограниченный ряд известных хакерских техник.

Результатом, как правило, является определение возможного вектора атаки: с конкретного компьютера до конкретного сервера через конкретные 15–20 машин с используются 10–20 реализаций конкретных техник. В таких условиях остается неизвестным, как отреагируют системы защиты на остальной части инфраструктуры.

CtrlHack: BAS

Платформа выполняет симуляцию этапов целевых атак, измеряя реальную готовность организации эффективно справляться с угрозами кибербезопасности.

Используя наступательный подход, CtrlHack выявляет критические угрозы, моделируя широкий спектр многовекторных атак с точки зрения злоумышленника.

Симуляции можно запускать по запросу в любое время и из любого места (точки выполнения атаки контролируются посредством расстановки агентов в сети), не затрагивая пользователей или инфраструктуру (не нарушая работу, не перегружая какие-то критичные объекты).

Благодаря возможностям по работе с SIEM, компании могут привести в порядок процесс обнаружения нежелательных активностей и оптимизировать работу команды реагирования на инциденты ИБ.

Организации могут постоянно проверять уровень обнаружения тех или иных методов, применяемых в современных атаках, сопоставляя это со структурой матрицы MITRE.

С одной стороны, компания получает большее понимание имеющиеся недостатков как в системах защиты, так и в методах обнаружения техник атакующих, которые не обнаруживаются, и при этом никак не будут заблокированы другими средствами, поскольку представляют под собой зачастую набор разрешенных различными политиками действий.

С другой стороны, для сотрудников отделов ИБ CtrlHack становится дополнительным инструментом повышения уровня знаний в обнаружении киберугроз и реагировании на них.

Имитируя множество стратегий (>200), применяемых хакерами, CtrlHack позволяет компаниям оценить свою реальную готовность эффективно справляться с угрозами кибербезопасности.

Важно понимать, что указанные выше методы не являются полностью взаимозаменяемы-ми. Каждый из них решает свои конкретные задачи и несёт отдельную ценность для организациям.

Использование BAS сильно повышает эффективность работы пентестеров и Red Team. Сам продукт — не их рабочий инструмент, но если его применять в SIEM, то список техник, которые должна опробовать Red Team, уменьшается в разы. Ведь из отчётов BAS и SOC видно, что уже детектируется, а благодаря этому достигается заметная экономия времени и ресурсов.

CTRLHACK

Непрерывная объективная оценка
уровня защищенности и повышение
эффективности системы защиты

ITD GROUP

Эксклюзивный дистрибьютор – компания ITD Group

123557, Москва, Большой Тишинский переулок, д. 19, стр. 3

+7 (499) 502-13-75
info@iitdgroup.ru