О необходимости применения сканеров уязвимостей для обеспечения информационной безопасности

Крутофал Глеб Евгеньевич
курсант КВВУ им. С.М. Штеменко,
г. Краснодар, РФ

Аннотация

В статье рассматриваются задачи, предназначение и механизмы работы сканеров уязвимостей, необходимых для обнаружения проблем безопасности в информационных системах, оказания помощи в их устранении, а также для повышения эффективности защиты информации.

Ключевые слова

Сканер уязвимостей, уязвимость, информационная безопасность

В настоящее время информационная инфраструктура играет важнейшую роль в обеспечении процесса функционирования государственных и военных структур. Использование вычислительных систем для хранения, обработки и передачи информации создаёт необходимость их надёжной защиты, что особенно актуально, учитывая глобальную тенденцию к росту числа информационных угроз.

В интернете существует большое количество компьютерных вирусов, которые могут реализовывать несанкционированный доступ в систему и вредить ценным данным.
А широкое наличие уязвимостей в информационных системах и элементах комплексов защиты информации является большой проблемой для специалистов обеспечения информационной безопасности. Кроме этого, часто хакеры используют направленные атаки на организации, чтобы украсть конфиденциальные данные для последующей перепродажи конкурентам, или навредить, остановив работу на неопределённое время.

Под уязвимостью информационной системы понимается такое её свойство (недостаток), которое может быть использовано злоумышленником для реализации угроз безопасности информации.

Поиском брешей в системе можно заниматься вручную, но это будет крайне трудозатратный процесс, который занимает много времени, при высокой вероятности что-нибудь не заметить. Поэтому лучше всего использовать автоматические средства для поиска уязвимостей и слабых мест в информационной инфраструктуре организации. Для этого специалистам по информационной безопасности рекомендуется регулярно пользоваться сканерами уязвимостей.

Сканеры уязвимостей — это программные или программно-аппаратные средства, служащие для осуществления диагностики и мониторинга, позволяющие сканировать сети, компьютеры, операционные системы, службы и приложения на предмет обнаружения возможных проблем в системе безопасности, оценивать и устранять уязвимости.

Сканеры уязвимостей позволяют проверить разнообразные приложения в системе на предмет наличия «дыр», которыми могут воспользоваться злоумышленники, отследить всю сетевую активность [1]. Кроме того, могут быть использованы низкоуровневые средства, такие как сканеры портов, для выявления и анализа возможно установленных нежелательных протоколов в системе. Такие сканеры имеют особое значение для тех организаций, в сферу деятельности которых входит обработка и хранение ценных архивов и конфиденциальных сведений. Данные программы

требуются компаниям, занимающимся научными исследованиями, медициной, торговлей, информационными технологиями, рекламой, финансами и выполнением других задач, которым может помешать утечка информации.

Таким образом, сканеры направлены на решение следующих задач:

— идентификация и анализ уязвимостей, поиск попавшего на компьютер вредоносного кода;

— инвентаризация ресурсов, таких как операционная система, программное обеспечение и устройства сети;

— формирование отчётов, содержащих описание уязвимостей и варианты их устранения.

Также можно провести сканирование сети, составить её карту и определить, какие именно сетевые устройства в инфраструктуре организации используются. Будут также определены все поддомены. Сразу же можно выявить открытые порты, запущенные сетевые сервисы, которые представляют угрозу для безопасности. На сетевых устройствах будет произведён поиск уязвимостей, которые можно будет закрыть установкой патчей, обновлением или изменением конфигураций. Кроме того, сканер позволяет проверить на стойкость используемые пароли на сервисах с доступной авторизацией, и при этом выявлять пароли, установленные по умолчанию. Будет произведён и «брутфорс» (полный перебор возможных вариантов) с использованием актуальной базы паролей [1].

Сканеры уязвимостей позволяют также сканировать средства защиты информации и определять, когда можно установить новые патчи, обновить программное обеспечение, изменить конфигурацию и настройки, а также проверить актуальность баз сигнатур. Современные сканеры поддерживают практически все современные операционные системы, а также большое количество сетевого оборудования и прочих объектов. Также всё большую популярность начинают набирать облачные решения такого рода.

Сканеры уязвимостей при своей работе используют два основных механизма:

а) первый — зондирование. Не слишком оперативен, но точен. Это механизм активного анализа, который запускает имитации атак, тем самым проверяя реакцию системы. При зондировании применяются методы реализации атак, которые помогают подтвердить наличие уязвимости и обнаружить ранее не выявленные «провалы»;

б) второй механизм — сканирование. Это более быстрый механизм, но даёт менее точные результаты. Это пассивный анализ, при котором сканер ищет уязвимость без подтверждения её наличия, используя косвенные признаки. С помощью сканирования определяются открытые порты и собираются связанные с ними заголовки. [5]

Они в дальнейшем сравниваются с таблицей правил определения сетевых устройств, требованиями к операционным системам и актуальными недоработками программного обеспечения. После сравнения сетевой сканер безопасности сообщает о наличии или отсутствии уязвимостей.

Большинство современных сканеров безопасности сети работает по принципам:

1) сбор информации о сети, идентификация всех активных устройств и сервисов, запущенных на них;

2) обнаружение потенциальных уязвимостей;

3) подтверждение выбранных уязвимостей, для чего используются специфические методы и моделируются атаки;

4) формирование отчётов;

5) автоматическое устранение уязвимостей. Не всегда данный этап реализуется в сетевых сканерах безопасности, но часто встречается в системных сканерах.

Программа, выполняющая сканирование на уязвимости, работает следующим образом:

1. Собирает о сети всю необходимую информацию, сначала определяя все активные устройства в системе и работающее на них программное обеспечение. Если анализ проводится только на уровне одного ПК с уже установленным на нём сканером, этот шаг пропускают.

2. Пытается найти потенциальные уязвимости, применяя специальные базы данных, для того чтобы сравнить полученную информацию с уже известными видами «дыр» в безопасности. Сравнение выполняется с помощью активного зондирования или проверки заголовков.

3. Подтверждает найденные уязвимости, применяя специальные методики — имитацию определённого типа атак, способных доказать факт наличия или отсутствия угрозы.

4. Генерирует отчёты на базе собранных при сканировании сведений, описывая уязвимости.

Завершающий этап сканирования предполагает собой автоматическое исправление для устранения проблем или выдача соответствующих рекомендаций для администратора безопасности. Эта функция есть практически в каждом системном сканере, и отсутствует у большинства сетевых приложений для проверки [3].

Современные сканирующие программы имеют интуитивно понятное меню и достаточно легко настраиваются для работы в соответствии с выполняемыми задачами.

После получения отчётов сканер позволяет администратору запускать исправление угроз. Ещё одна важная функция предполагает сохранение истории прошлых проверок, что позволяет оценить работу узлов в определённых временных интервалах и оценить риски появления новых проблем с безопасностью.

Наиболее заметными на российском рынке сканеров являются следующие продукты:

— RedCheck («АЛТЭКС-СОФТ»);

— ScanOVAL (ФСТЭК России);

— «SCADA-Аудитор» (НТЦ «Станкоинформзащита»);

— XSpider (Positive Technologies);

— Nessus («Tenable Network Security»);

— Ревизор сети («ЦБИ-Сервис»);

— Сканер-ВС (НПО «Эшелон»);

— MaxPatrol 8 (Positive Technologies) [4].

Современные сканеры безопасности информации должны предоставлять надёжный инструментарий, способный эффективно обеспечить сложный процесс мониторинга безопасности при минимальном вмешательстве специалиста в рутинные задачи сканирования.

С практической точки зрения особо важным преимуществом любого средства обеспечения безопасности информации является наличие сертификата уполномоченного органа государственной власти.

Вывод: с учётом широкого ассортимента приложений для сканирования сети и её узлов на уязвимости, существенно облегчается работа администратора. Теперь от него не требуется самостоятельно запускать все механизмы сканирования вручную — достаточно просто найти подходящее приложение, выбрать способ проверки, настроить и воспользоваться рекомендациями

полученного отчёта.

Выбирать подходящий сканер следует по функциональности приложения, эффективности поиска угроз и, что тоже достаточно важно, по цене, которая должна быть сопоставима с ценностью защищаемой информации. Необходимо отметить, что данный тип средств защиты стремительно развивается, постепенно сканеры превращаются в более масштабные системы, решающие большее количество задач.

Литература

1. «Сканеры уязвимостей». — Текст : электронный // Википедия : [сайт]. — URL: https://ru.wikipedia.org/wiki/Сканеры_уязвимостей.

2. Чекулаева, Е. Н. Управление информационной безопасностью : учебное пособие / Е. Н. Чекулаева. — Йошкар-Ола : Поволжский государственный технологический университет, 2020. — 153 с. — Текст : непосредственный.

3. Сканирование на уязвимости: как проверить устройство и обезопасить себя от потенциальных угроз. — Текст : электронный // Портал полезных знаний : [сайт]. — URL: https://actualvape.ru/skanirovanie-na-uyazvimosti-kak-proverit-ustroistvo-i-obezopasit/.

4. Обзор отечественных сканеров уязвимостей. — Текст : электронный // Штирлиц : [сайт]. — URL: https://schtirlitz.ru/raznoe-2/nessus-skaner-uyazvimostej-skaner-uyazvimostej-nessus-vulnerability-scanner-ot-tenable-instrukciya-po-primeneniyu.html#i-9.

5. Черемых, В. Сканеры уязвимостей / В. Черемых. — Текст : электронный // IT-black : [сайт]. — URL: https://it-black.ru/skanery-uyazvimostey/.