Сетевые сканеры уязвимостей как самостоятельный класс ПО:

состав, функции, перспективы развития

Евгений НОВОСЕЛОВ,
ведущий инженер направления «Автоматизация ИБ», УЦСБ

Сетевые сканеры уязвимостей играют важную роль в обеспечении безопасности информационных систем и сетей. Они представляют собой специализированные инструменты, предназначенные для обнаружения и анализа потенциальных уязвимостей в компьютерных системах, сетевых устройствах и приложениях. В свете постоянно меняющихся угроз кибербезопасности эффективное использование сетевых сканеров уязвимостей стало неотъемлемой частью процесса защиты информации. В статье рассмотрим, какие прикладные функции выполняют сетевые сканеры и на какие критерии стоит ориентироваться при выборе решения, а также проведем краткий обзор самых популярных сетевых сканеров и проанализируем тенденции развития в этой сфере.

Основные функции и подходы к анализу результатов сканирования

Сетевые сканеры уязвимостей осуществляют сканирование сети или конкретных устройств с целью выявления потенциально слабых мест, которые могут быть использованы злоумышленниками для проведения атак. Эти инструменты осуществляют сканирование различных видов.

К ключевым компонентам сетевых сканеров уязвимостей относятся:

- движок сканирования. Ядро программного обеспечения, которое выполняет сканирование сети на предмет уязвимостей. Движок сканирования может включать в себя различные методы сканирования, такие как сканирование портов, анализ протоколов;
- база данных уязвимостей. Сетевые сканеры обычно используют базу данных уязвимостей для сравнения результатов сканирования с известными уязвимостями. Это позволяет определять, какие уязвимости могут присутствовать в обнаруженных сервисах и приложениях;
- интерфейс пользователя. Для взаимодействия с пользователем обычно предоставляется графический интерфейс или интерфейс командной строки, который позволяет настраивать параметры сканирования, анализировать результаты и принимать меры по устранению обнаруженных уязвимостей;
- механизмы безопасности. Защита от несанкционированного доступа, шифрование данных, аутентификация пользователей и другие меры безопасности для защиты сканера и его данных.

Среди основных функций и возможностей сетевых сканеров уязвимостей можно отметить следующие:

сканирование портов и служб. Сетевые сканеры могут проводить сканирование открытых портов и доступных служб на сетевых устройствах, выявляя потенциальные точки входа для злоумышленников;

обнаружение уязвимостей. Обнаруживают известные уязвимости в операционных системах, приложениях и сервисах, используя базы данных уязвимостей. Сканеры способны обнаруживать уязвимости в веб-приложениях, такие как SQL-инъекции, XSS-атаки и другие уязвимости, связанные с веб-технологиями;

анализ безопасности протоколов. Проверяют протоколы связи на наличие уязвимостей,

например, атаки на SSL/TLS, DNS-запросы и другие сетевые протоколы;
идентификация слабых паролей. Некоторые сканеры могут проводить анализ сложности паролей и находить слабые или уязвимые пароли в сети;
генерация отчетов. После завершения сканирования сканеры могут генерировать подробные отчеты о найденных уязвимостях – это помогает администраторам принимать меры по устранению обнаруженных проблем;
планирование и автоматизация сканирования. Предоставляют возможность планирования регулярных сканирований для автоматического обнаружения новых уязвимостей.

Анализ результатов сканирования уязвимостей включает в себя такие подходы, как:
приоритизация уязвимостей. После сканирования необходимо проанализировать результаты и определить, какие уязвимости представляют наибольшую угрозу для системы. Это позволит выявить, на какие уязвимости следует обратить особое внимание при их устранении;
классификация уязвимостей. Результаты сканирования могут быть классифицированы по типам уязвимостей. Это поможет лучше понять, где находятся основные проблемные зоны;
оценка потенциальных последствий. Анализ результатов сканирования также включает оценку потенциальных последствий эксплуатации обнаруженных уязвимостей. Это позволит определить, насколько критичными являются найденные проблемы;
сопоставление с известными эксплоитами. Проверка наличия известных эксплоитов для обнаруженных уязвимостей дает возможность оценить реальную угрозу для системы;
создание плана действий. На основе результатов сканирования разрабатывается план действий по устранению обнаруженных уязвимостей: определение приоритетов, временные рамки и ответственных лиц за исправление проблем;
мониторинг и повторное сканирование. После внесения изменений для устранения уязвимостей важно провести повторное сканирование, чтобы убедиться, что проблемы были успешно исправлены.

После внесения изменений для устранения уязвимостей важно провести повторное сканирование, чтобы убедиться, что проблемы были успешно исправлены.

Вид сканирования	Уязвимость	Устранение
Сканирование портов	Через открытые порты злоумышленники могут получить доступ к системам	Закрыть неиспользуемые порты в настройках брандмауэра. Настроить брандмауэр для фильтрации входящего трафика Использовать VPN для защищенного доступа к критически важным службам
Анализ уязвимостей операционной системы	Устаревшие или неподдерживаемые версии ОС могут иметь известные уязвимости	Регулярно обновлять операционные системы и устанавливать последние патчи. Настроить автоматические обновления для критически важных систем. Периодически проводить аудиты безопасности для выявления устаревших систем
Поиск необновленного программного обеспечения	Устаревшее программное обеспечение может содержать известные уязвимости	Регулярно проверять и обновлять все установленные программы и библиотеки. Использовать инструменты управления патчами для автоматизации процесса обновления. Удалять или заменять устаревшие приложения на поддерживаемые альтернативы
Сканирование на наличие сетевых устройств	Неизвестные или незащищенные устройства могут быть уязвимы	Внедрить управление доступом к сети (NAC) для контроля подключаемых устройств. Регулярно проводить инвентаризацию сетевых устройств и проверять их настройки безопасности. Настроить VLAN для изоляции устройств в зависимости от их роли в сети
Сканирование на наличие вредоносного ПО	Вредоносное ПО может скомпрометировать безопасность системы	Установить и регулярно обновлять антивирусное программное обеспечение. Регулярно проводить полные сканирования систем на наличие вредоносного ПО. Обучать пользователей распознавать фишинговые атаки и другие методы распространения вредоносного ПО

Требования к сетевым сканерам уязвимостей

В условиях постоянного роста киберугроз и усложнения векторов атаки выбор эффективного сетевого сканера уязвимостей становится критически важным для обеспечения безопасности информационных систем.

Основные функциональные требования к сетевым сканерам уязвимостей включают в себя следующие аспекты.

В условиях роста киберугроз выбор эффективного сетевого сканера уязвимостей становится критически важным для обеспечения безопасности информационных систем.

- **Сканирование сети и устройств**. Способность сканировать сеть и все подключенные устройства для обнаружения потенциальных уязвимостей является основой для выявления слабых мест в инфраструктуре. Если сканер обнаруживает незащищенное IoT-устройство, например, IP-камеру, администратор может принять меры для защиты этого устройства от атак.
- **Идентификация уязвимостей**. Возможность точно определять типы уязвимостей, такие как открытые порты, уязвимые сервисы, недостатки конфигурации и другие потенциальные проблемы. Сканер может выявить открытые порты на сервере и тем самым указать на потенциальные точки входа для злоумышленников.
- Оценка риска. Предоставление оценки уровня риска для каждой обнаруженной уязвимости позволяет администраторам определить приоритеты по исправлению проблем. Если сканер указывает, что уязвимость имеет высокий уровень риска из-за наличия эксплоита, администратор может сразу же принять меры по ее устранению.
- **Глубокий анализ уязвимостей**. Сканер должен иметь возможность проведения более глубокого анализа обнаруженных уязвимостей для выявления потенциальных последствий и определения способов эксплуатации.
- **Гибкие настройки сканирования**. Возможность настройки параметров сканирования в зависимости от требований и особенностей сети, включая выборочное сканирование и определение времени сканирования. Администратор может настроить сканирование на выходные, чтобы минимизировать влияние на производительность в рабочие часы.
- **Отчетность и визуализация результатов**. Генерация подробных отчетов о найденных уязвимостях, их степени критичности, а также возможность представления результатов сканирования в виде графиков или диаграмм для лучшего восприятия информации. График с количеством обнаруженных уязвимостей по категориям позволит руководству быстро оценить общую картину безопасности.
- **Интеграция с другими системами безопасности**. Возможность интеграции с другими системами мониторинга и безопасности для обеспечения более полного обзора состояния безопасности сети. Сканер может интегрироваться с SIEM-системой, что позволяет автоматически реагировать на обнаруженные уязвимости.

При выборе сканера уязвимостей необходимо обратить внимание и на то, как в нем реализованы следующие параметры безопасности:

- **защита данных** – обеспечение конфиденциальности и целостности данных, собираемых и передаваемых сканером, с целью предотвратить утечку чувствительной информации;
- **аутентификация и авторизация** – гарантия того, что только уполномоченные пользователи имеют доступ к функциям сканера, предоставление соответствующих прав доступа происходит на основе ролей и обязанностей;
- **защита от вредоносных атак** – реализация механизмов защиты от вредоносных атак, таких как инъекции кода, переполнение буфера, отказ в обслуживании и др.;
- **шифрование данных** – использование криптографических методов для защиты передаваемой информации между сканером и другими компонентами сети;
- **обновления и патчи** – регулярное обновление сканера с учетом последних обновлений безопасности для предотвращения использования известных уязвимостей;
- **логирование и мониторинг** – ведение журналов действий сканера для последующего анализа и мониторинга;
- **соблюдение стандартов безопасности** и руководящих принципов для обеспечения соответствия требованиям безопасности информационных систем.

Примеры распространенных продуктов

Рассмотрим наиболее популярные сетевые сканеры уязвимостей.

Nessus. Один из самых известных и широко используемых сетевых сканеров уязвимостей. Он предлагает обширные возможности сканирования и анализа уязвимостей в сетях и приложениях.

OpenVAS. Бесплатный и открытый сканер уязвимостей, который предоставляет широкий набор функций для обнаружения и анализа уязвимостей.

MaxPatrol 8. Комплексная платформа для поиска угроз и реагирования на инциденты, которая обнаруживает и реагирует на сложные угрозы в режиме реального времени с помощью машинного обучения и поведенческого анализа. Предназначена для помощи организациям в обнаружении и реагировании на сложные угрозы, включая APT, атаки нулевого дня и программы-вымогатели.

RedCheck. Сканер уязвимостей для комплексного анализа защищенности инфраструктуры предприятия. Он обнаруживает уязвимости в операционных системах, прикладном ПО, сетевом оборудовании, веб-серверах, СУБД, средствах виртуализации и других компонентах, а также проводит аудит парольной политики, конфигураций и соответствия политикам и стандартам безопасности. RedCheck помогает выявить и устранить уязвимости, улучшить безопасность и соответствие требованиям нормативных документов.

Выбор подходящего сканера уязвимостей зависит от специфики организации, требований к безопасности и бюджета. Nessus и OpenVAS подходят для широкого применения, тогда как MaxPatrol 8 и RedCheck ориентированы на сложные угрозы и работу в развитых корпоративных средах. Сканеры с сертификатами ФСТЭК, например, MaxPatrol 8 и RedCheck, обеспечивают высокий уровень безопасности и подходят для организаций, работающих с конфиденциальной информацией и в условиях строгого регулирования.

Перспективы использования искусственного интеллекта

Роль искусственного интеллекта (ИИ) в развитии сетевых сканеров уязвимостей в ближайшем будущем может стать критически важной для обеспечения безопасности информационных систем. Рассмотрим несколько возможных перспектив и примеров использования ИИ в этой области.

Автоматизация процесса обнаружения уязвимостей: с помощью ИИ можно разрабатывать алгоритмы, способные автоматически сканировать сети и обнаруживать потенциальные уязвимости. Использование машинного обучения позволяет создавать модели, способные выявлять необычные или подозрительные паттерны в сетевом трафике.

Прогнозирование уязвимостей: ИИ позволяет выявлять потенциальные уязвимости на основе данных о предыдущих атаках и известных уязвимостях, что обеспечивает возможность организациям принимать своевременные меры для предотвращения вероятных угроз.

Анализ больших объемов данных: ИИ может помочь в обработке и анализе постоянно увеличивающегося объема данных, выявляя скрытые угрозы и паттерны, которые могли быть упущены специалистами.

Разработка адаптивных систем защиты: используя ИИ, можно разрабатывать системы защиты, способные адаптироваться к новым видам угроз и изменяющейся сетевой среде. Это помогает повысить эффективность защиты от новых и неизвестных атак.

Таким образом, основные тенденции использования искусственного интеллекта в развитии сетевых сканеров уязвимостей связаны с автоматизацией процессов обнаружения уязвимостей, анализом данных и разработкой более адаптивных систем защиты.

Заключение

Роль сканеров заключается в помощи специалистам по информационной безопасности и системным администраторам заблаговременно обнаруживать и исправлять проблемы в защищенности сети.

> Роль искусственного интеллекта (ИИ) в развитии сетевых сканеров уязвимостей в ближайшем будущем может стать критически важной для обеспечения безопасности информационных систем.

Ключевые задачи, с которыми могут справиться сканеры уязвимостей, – обнаружение потенциальных угроз и слабых мест в защищенности сети или конкретных устройств, оценка рисков и формирование стратегии по обеспечению безопасности. Регулярное использование сетевых сканеров уязвимостей способствует повышению общего уровня кибербезопасности защищаемой системы.

Основные направления развития сетевых сканеров включают в себя повышение точности обнаружения уязвимостей, автоматизацию процесса анализа и реагирования на угрозы, а также разработку гибких систем, способных адаптироваться к новым видам кибератак. Интеграция ИИ в сетевые сканеры уязвимостей позволит создать более надежные и защищенные информационные системы, способные оперативно реагировать на угрозы и предотвращать потенциальные атаки. ■