УДК 004.56

СКАНЕР УЯЗВИМОСТИ СЕТИ КАК СРЕДСТВО ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ДАННЫХ

М.И. Тихонович
Государственное предприятие «НИИ ТЗИ», Минск, Беларусь

Аннотация. Чтобы выявить уязвимость сети есть множество устройств и подходов. Одним из них является сканер уязвимости сети. Грамотно его используя, специалисты по информационной безопасности могут значительно усилить сетевую безопасность организации. Рассмотрены вопросы, связанные с анализом существующих механизмов поиска уязвимостей. Актуальность данной темы обосновывается возрастающим числом кибератак и инцидентов по утечке данных, которые представляют серьезную угрозу для конфиденциальности и целостности информации. С развитием средств автоматизации проектирования и разработки операционных систем, программного обеспечения и повышения уровня развития технологий злоумышленники все чаще находят «дыры» в корпоративной сети, которые в последствии могут быть использованы для несанкционированного доступа, изменения данных или нарушения нормальной работы локально вычислительной сети организации.
Ключевые слова: сканер; сканер уязвимости; угроза; анализ уязвимостей; корпоративная сеть; уязвимость; оптимизация; сеть; сетевая безопасность; ИТ-инфраструктура.

NETWORK VULNERABILITY SCANNER AS A MEAN OF ENSURING DATA PROTECTION

M.I. Tikhonovich
State Enterprise "NII TZI", Minsk, Belarus

Abstract. To identify network vulnerability there are many devices and approaches. One of them is a network vulnerability scanner. Properly using it, information security specialists can significantly strengthen the network security of the organization. The questions related to the analysis of existing vulnerability scanning mechanisms are considered. The relevance of this topic is justified by the increasing number of cyberattacks and data leakage incidents, which pose a serious threat to the confidentiality and integrity of information. With the development of automation design and development of operating systems, software and increasing the level of technology, attackers are increasingly finding "holes" in the corporate network, which can then be used for unauthorized access, data modification or disruption of the normal operation of the local area network of the organization.
Keywords: scanner; vulnerability scanner; threat; vulnerability analysis; corporate network; vulnerability; optimization; network; network security; IT infrastructure.

Введение

Сканеры уязвимостей – это программные инструменты, предназначенные для поиска слабых мест в информационной инфраструктуре. Они позволяют обнаруживать уязвимости в сетевых ресурсах, операционных системах, приложениях и веб-сервисах, что крайне важно для обеспечения кибербезопасности. Современные сканеры способны анализировать как внутренние, так и внешние угрозы, предоставляя отчеты с детальными рекомендациями по устранению обнаруженных проблем.

Главная задача сканеров уязвимостей – предотвращение потенциальных атак. Они помогают выявить слабые места до того, как злоумышленники смогут их использовать. Использование этих инструментов позволяет поддерживать высокий уровень информационной безопасности, защищая данные компании и пользователей от утечек и несанкционированного доступа. Сканеры автоматизируют процесс поиска уязвимостей, значительно сокращая время на проверку и улучшая точность.

Основная часть

Принцип работы сканеров – проверка используемых операционных систем, приложений, средств защиты информации, поиск «дыр», которыми могли бы воспользоваться хакеры, и предупреждение администратора о зонах риска системы.

Таким образом, сканеры уязвимостей направлены на решение следующих задач:

– идентификация и анализ уязвимостей;

– инвентаризация ресурсов;

– формирование отчетов.

Сканеры уязвимостей сети при своей работе используют два основных механизма: зондирование, сканирование. Зондирование – не слишком оперативен, но точен. Это механизм активного анализа, который запускает имитации атак, тем самым проверяя уязвимость. При зондировании применяются методы реализации атак, которые помогают подтвердить наличие уязвимости и обнаружить ранее не выявленные «провалы». Этот метод более медленный, чем «сканирование», но почти всегда гораздо более точный, чем он. В терминах компании ISS данный метод получил название «подтверждение» (verification). Согласно компании, Cisco этот процесс использует информацию, полученную в процессе сканирования («логического вывода»), для детального анализа каждого сетевого устройства. Этот процесс также использует известные методы реализации атак для того, чтобы полностью подтвердить предполагаемые уязвимости и обнаружить другие уязвимости, которые не могут быть обнаружены пассивными методами, например, подверженность атакам типа «отказ в обслуживании» («denial of service»).

Второй механизм – сканирование – более быстрый, но дает менее точные результаты. Это пассивный анализ, при котором сканер ищет уязвимость без подтверждения ее наличия, используя косвенные признаки. С помощью сканирования определяются открытые порты и собираются связанные с ними заголовки. Они в дальнейшем сравниваются с таблицей правил определения сетевых устройств, операционных систем и возможных «дыр». После сравнения сетевой сканер безопасности сообщает о наличии или отсутствии уязвимости. Этот метод является наиболее быстрым и простым для реализации. В терминах компании ISS данный метод получил название «логический вывод» (inference). Согласно компании, Cisco этот процесс идентифицирует открытые порты, найденные на каждом сетевом устройстве, и собирает связанные с портами заголовки (banner), найденные при сканировании каждого порта. Каждый полученный заголовок сравнивается с таблицей правил определения сетевых устройств, операционных систем и потенциальных уязвимостей. На основе проведенного сравнения делается вывод о наличии или отсутствии уязвимости.

На практике указанные механизмы реализуются следующими несколькими методами: «Проверка заголовков» (banner check), «Активные зондирующие проверки» (active probing check), «Имитация атак» (exploit check).

Большинство современных сканеров безопасности сети работает по следующим шагам: сбор информации о сети, обнаружение потенциальных уязвимостей,

подтверждение выбранных уязвимостей, формирование отчетов, автоматическое устранение уязвимостей.

Виды сканирования: WhiteBox – Сканер запускается внутри исследуемой сети, BlackBox – Сканер запускается извне исследуемой сети, Сканер локальной сети – жизненно необходимое средство для компаний, чья деятельность напрямую связана с хранением и обработкой уникальных баз данных, конфиденциальной информации, ценных архивов. Без сомнения, сканеры сети необходимы организациям в сфере обороны и других служб – словом, везде, где нежелательна или даже опасна утечка накопленной информации, имеются базы персональных данных клиентов.

Список использованных источников

1. Крутофал Г. Е. О необходимости применения сканеров уязвимостей для обеспечения информационной безопасности / Г.Е. Крутофал – Текст: электронный // Евразийский научный журнал. – 2022. – №. 4. – URL: https://cyberleninka.ru/article/n/o-neobhodimosti-primeneniya-skanerovuyazvimostey-dlya-obespecheniya-informatsionnoy-bezopasnosti/viewer (дата обращения: 28.02.2025).

2. Долгин А. А. Разработка сканера уязвимостей компьютерных систем на основе защищенных версий ОС Windows / А. А. Долгин, П. Б. Хорев // Труды международной научно-технической конференции «Информационные средства и технологии. – 2005. – URL: https://networkjournal.mpei.ac.ru/cgi-bin/main.pl?l=ru&n=7&pa=14&ar=6 (дата обращения: 25.02.2025).

3. Сирсен, Р., Хаббард, Д.У. Как оценить риски в кибербезопасности. Лучшие инструменты и практики / Ричард Сирсен. Дуглас У. Хаббард. – М. : «Бомбора», 2023 – 464 с.

References

1. Krutofal G. E. On the need to use vulnerability scanners to ensure information security / G.E. Krutofal – Text: electronic // Eurasian Scientific Journal. - 2022. - №. 4. - URL: https://cyberleninka.ru/article/n/o-neobhodimosti-primeneniya-skanerovuyazvimostey-dlya-obespecheniya-informatsionnoy-bezopasnosti/viewer (date of reference: 28.02.2025).

2. Dolgin, A. A. A. Development of a vulnerability scanner of computer systems based on protected versions of Windows OS / A. A. Dolgin, P. B. Khorev // Proceedings of the international scientific and technical conference "Information means and technologies. - 2005. - URL: https://networkjournal.mpei.ac.ru/cgi-bin/main.pl?l=ru&n=7&pa=14&ar=6 (date of reference: 25.02.2025).

3. Sirsen, R., Hubbard, D.W. How to assess risks in cybersecurity. Best tools and practices / Richard Sirsen, Douglas W. Hubbard. - Moscow : "Bombora", 2023 - 464 p.

Сведения об авторе

Тихонович М.И., магистрант кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», инженер сектора систем защиты информации Государственного предприятия «НИИ ТЗИ». mtikh@niitzi.by.

Information about the author

Tikhonovich M.I., Master's Student. Information Protection Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", engineer of the information protection systems sector of the State Enterprise "NII TZI". mtikh@niitzi.by.