СКАНЕР УЯЗВИМОСТИ СЕТИ КАК НОВЫЙ МЕТОД ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ДАННЫХ

Гиро К.Ю.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Федоренко В.А.

Аннотация. Чтобы выявить уязвимость сети есть множество устройств и подходов. Одним из них является сканер уязвимости сети. Грамотно его используя, специалист может значительно усилить сетевую безопасность.

Принцип работы сканеров - проверка используемых приложений, поиск «дыр», которыми могли бы воспользоваться хакеры, и предупреждение администратора о зонах риска системы.

Таким образом, сетевые сканеры 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, ОС 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 используемых источников:

1. https://roi4cio.com/categories/category/skaner-ujazvimostei
2. Таненбаум Э. С., Уэзеролл Д. Компьютерные сети пятое издание Изд-во Питер, 2020. С – 857-906.