Лекция 3.4. Сканирование портов и уязвимостей

В данной лекции будут рассмотрены следующие вопросы:  
1. Сканер уязвимости сети.  
2.  Задачи сетевых сканеров.  
3. Механизмы и принципы работы сетевого сканера локальной сети.

Глава 1. Сканирование портов и уязвимостей

1. Сканер уязвимости сети.  
2. Механизмы работы сетевого сканера локальной сети.  
3. Возможности современных программных решений.  
4. Сравнение сканеров уязвимостей сети.  
Сканер уязвимости сети  
Одним из важнейших этапов обеспечения информационной безопасности является идентификация потенциальных рисков. Большинство ИТ-специалистов знают, насколько может быть опасна «брешь» в ОС и приложениях. И чрезвычайно важно найти эти «дыры», или на языке профессионалов — уязвимости прежде, чем ими смогут воспользоваться недоброжелатели. Для этой цели и были созданы сканеры безопасности.  
Продвинутые специалисты по IT-безопасности используют в своей работе специализированное аппаратное или программное обеспечение, сканирующее сеть и её устройства на предмет обнаружения слабых мест в системе безопасности. Это и есть сканеры уязвимости, или по-другому — безопасности, сети. Они проверяют используемые приложения, ищут «дыры», которыми могли бы воспользоваться хакеры, и предупреждают администратора о зонах риска системы. Грамотно используя сканер уязвимости сети, специалист может значительно усилить сетевую безопасность.  
**Сканер уязвимости сети** — автоматизированное решение для проведения полного сканирование портов, контроля необходимых обновлений ПО для защиты сети, а также проверки программного и аппаратного обеспечения. Таким образом, сетевые сканеры направлены на решение следующих задач:  
1. Идентификация и анализ уязвимостей.  
2. Инвентаризация ресурсов, таких как операционная система, программное обеспечение и устройства сети.  
3. Формирование отчётов, содержащих описание уязвимостей и варианты их устранения.

Глава 2. Сканирование портов и уязвимостей

Механизмы работы сетевого сканера локальной сети  
Сканеры уязвимостей сети при своей работе используют два основных механизма.  
1. 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».  
2. Сканирование. Более быстрый, 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. 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.  
Большинство современных сканеров безопасности сети работает по нижеперечисленным 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; формирование отчётов.  
4.  автоматическое устранение уязвимостей.  
Не всегда данный этап реализуется в сетевых сканерах безопасности, но часто встречается в сканерах системных. Существует возможность создания резервного сценария, который может отменить произведённые изменения, например, если после устранения уязвимости будет нарушено полноценное функционирование сети.  
Тем не менее каждый сканер из множества представленных сейчас на рынке выделяется своими функциями и возможностями.

1. Какую задачу не выполняют сетевые сканеры?
   1. Шифрование данных
   2. Анализ системных служб и протоколов
   3. Определение открытых портов и сервисов
   4. Обнаружение уязвимостей
2. В рамках какой из задач сканирования сканер может обнаружить, что порт 80 открыт, и на нём работает веб-сервер?
   1. Анализ системных служб и протоколов
   2. Определение открытых портов и сервисов
   3. Обнаружение уязвимостей
3. В рамках решения какой задачи сканер может обнаружить уязвимость в версии программного обеспечения на открытом порту и предупредить о возможной атаке через эту уязвимость?
   1. Анализ системных служб и протоколов
   2. Определение открытых портов и сервисов
   3. Обнаружение уязвимостей
4. В рамках решения какой задачи сканер может обнаружить, что протокол Telnet используется без шифрования, что может привести к потенциальному компрометации паролей?
   1. Анализ системных служб и протоколов
   2. Определение открытых портов и сервисов
   3. Обнаружение уязвимостей
5. Какой сетевой сканер специализируется на сканировании сетевых хостов, определении открытых портов, обнаружении операционных систем, анализе сервисов?
   1. Nmap
   2. Nikto
   3. Оба сканера
6. Какой сетевой сканер специализируется на обнаружении известных уязвимостей: настройке безопасности, настройке уязвимых скриптов и конфигурационных ошибок?
   1. Nmap
   2. Nikto
   3. Оба сканера
7. Что входит в понятие «соблюдение этичности и законности при сканировании уязвимостей»?
   1. Получение согласия, соблюдение конфиденциальности, ограничение использования сканирования только легитимными целями
   2. Соблюдение конфиденциальности, ограничение использования сканирования только легитимными целями, шифрование паролей и логинов
   3. Получение согласия, использование официальных версий сетевых сканеров, соблюдение конфиденциальности