**Бабаев Антон,Юрчик Максим группа 215**

**Тема 19. Сканеры сетевой безопасности  
Задание 1.** Вставьте пропущенные слова.

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.**

**Задание 2.** На решение каких задач направлены сетевые сканеры?

Сетевые сканеры направлены на решение следующих задач:  
– идентификация и анализ уязвимостей;  
– инвентаризация ресурсов, таких как операционная система, программное обеспечение и устройства сети;  
– формирование отчетов, содержащих описание уязвимостей и варианты их устранения.  
  
**Задание 3.** Заполните схему:

Механизмы работы сканеров

Зондирование

Сканирование

**Задание 4.** Опишите общий алгоритм работы сканеров.  
  
**В общем случае алгоритм работы сканеров следующий:**  
  
**– Проверка заголовков**. Самый простой и быстрый способ на основе сканирования, однако имеющий ряд недостатков. Так, вывод о «провале» делается лишь по результатам анализа заголовков. К примеру, проверяя FTP **–** сервер, сканер узнает версию обеспечения и на основе этой информации сообщает о возможных уязвимостях. Естественно, специалисты по сетевой безопасности осведомлены о ненадежности этого метода, однако как первый шаг сканирования — это оптимальное решение, не приводящее к нарушению работы сети.  
  
**– Активные зондирующие проверки**. Это сканирование, при котором не проверяется версия ПО, а сравнивается «цифровой слепок» фрагмента программы со «слепком» уязвимости. По тому же принципу действуют антивирусные программы, сравнивая ПО с имеющимися в базе сигнатурами вирусов. Тоже достаточно быстрый метод, хотя и медленнее первого, с большим коэффициентом надежности.  
  
**– Имитация атак**. Это зондирование, которое эксплуатирует дефекты в программном обеспечении. Таким образом подается своеобразный импульс некоторым уязвимостям, которые не заметны до определенного момента. Эффективный метод, однако применить его можно не всегда. Так, вероятна ситуация, когда даже имитируемая атака просто отключит проверяемый узел сети или уязвимость окажется негодна для реализации атаки.

**Задание 5.** По каким принципам работает большинство современных сканеров безопасности сети? Перечислите их.  
**–** сбор информации о сети, идентификация всех активных устройств и сервисов, запущенных на них;  
– обнаружение потенциальных уязвимостей;  
– подтверждение выбранных уязвимостей, для чего используются специфические методы и моделируются атаки;  
– формирование отчетов;  
– автоматическое устранение уязвимостей.  
  
**Задание 6.** Перечислите основные функции сетевых сканеров.  
– Среди основных функций необходимо отметить сканирование документации и передачу информации по электронным адресам;  
– Проверку раздробленной сети, что избавляет администратора от необходимости оценивать каждый узел в отдельности и несколько раз задавать параметры сканирования.  
– Экономию трафика и анализ «исторических» данных.  
  
**Задание 7.** Заполните таблицу:

|  |  |  |  |
| --- | --- | --- | --- |
| **Название сканера** | **Функции** | **Достоинства** | **Недостатки** |
| GFI LanGuard | – функция инвентаризации ПО; – сканер портов; – обновления и патчи; – аудит узлов; – самые свежие сведения об угрозах; – автоматическое исправление; – поддержка популярных ОС; – экономия трафика; – поддержка виртуальных платформ; – контроль установленного ПО. | – Помимо обнаружения открытых портов, небезопасных настроек и запрещенного к установке ПО, он проверяет обновления и патчи не только ОС (десктопных и мобильных, физических и виртуальных), но и установленного ПО.   – Сканер уязвимости проверяет все: от серверов до сетевого аппаратного обеспечения, от виртуальных машин до смартфонов. | – Ориентирован именно на работу с патчами – некоторые администраторы отмечают в нем отсутствие некоторых сложных проверок (например, CGI–скриптов на Web–серверах) и невозможность определять собственные форматы отчетов. |
| Nessus | – сканер уязвимостей для небольших организаций, включающих в себя до 50 рабочих машин, а также для аудиторов, осуществляющих анализ безопасности своих заказчиков.   – Продукт позволяет оценивать конфигурации, находить уязвимости и, в случае обнаружения проблем при настройке инфраструктуры, предотвращать сетевые атаки. | – Постоянно актуальная база всевозможных эксплуатируемых угроз, на наличие которых он легко проверит необходимую сеть.  – Использование плагинов. – Простота в установке и использовании. – Высокий уровень точности. | – При отключенной опции «safe checks» некоторые тесты на уязвимости могут привести к нарушениям в работе сканируемых систем.  – Цена. Годовая лицензия может вам обойтись в 114 тысяч рублей. |
| Symantec  Security Check | – обнаружение вирусов и троянов, интернет-червей, вредоносных программ, поиск уязвимостей в локальной сети. | – состоит из двух частей: Security Scan, которая проверяет безопасность системы, и Virus Detection, выполняющей полную проверку компьютера на вирусы. Устанавливается быстро и просто, работает через браузер. | – уступает большинству конкурентов, хотя все свои основные функции выполняет |
| XSpider | – сканирование портов идентификация активных сетевых сервисов анализ уязвимостей сканирование по расписанию генерация отчетов. | – возможность обнаружения максимального количества «провалов» в сети еще до того, как их увидят хакеры.  – работает удаленно, не требуя установки дополнительного ПО.  Отработав, сканер отправляет специалисту по безопасности полный отчет и советы по устранению «дыр». | – долгая установка; – возможен конфликт со стандартом брандмауэром; – для получения доступа ко всем возможностям требуется покупка лицензии |
| QualysGuard | – оценку уровня критичности уязвимостей; – оценку времени, необходимого для их устранения; – проверку степени их воздействия на бизнес; – анализ тенденций в области проблем безопасности. | – Облачная платформа QualysGuard и встроенный набор приложений позволяют предприятиям упростить процесс обеспечения безопасности и снизить затраты на соответствие различным требованиям, при этом предоставляя важную информацию о безопасности и автоматизируя весь спектр задач аудита, комплекс-контроля и защиту ИТ-систем и веб-приложений. – | – Однако, несмотря на все технологические преимущества, круг заказчиков Qualys был ограничен тем, что многие компании не готовы отдавать данные сканирований в зарубежное облако. |

**Задание 8.** Опишите общий алгоритм работы сканеров.  
**В общем случае алгоритм работы сканеров следующий:**  
  
**– Проверка заголовков**. Самый простой и быстрый способ на основе сканирования, однако имеющий ряд недостатков. Так, вывод о «провале» делается лишь по результатам анализа заголовков. К примеру, проверяя FTP-сервер, сканер узнает версию обеспечения и на основе этой информации сообщает о возможных уязвимостях. Естественно, специалисты по сетевой безопасности осведомлены о ненадежности этого метода, однако как первый шаг сканирования — это оптимальное решение, не приводящее к нарушению работы сети.  
  
**– Активные зондирующие проверки**. Это сканирование, при котором не проверяется версия ПО, а сравнивается «цифровой слепок» фрагмента программы со «слепком» уязвимости. По тому же принципу действуют антивирусные программы, сравнивая ПО с имеющимися в базе сигнатурами вирусов. Тоже достаточно быстрый метод, хотя и медленнее первого, с большим коэффициентом надежности.  
  
**– Имитация атак**. Это зондирование, которое эксплуатирует дефекты в программном обеспечении. Таким образом подается своеобразный импульс некоторым уязвимостям, которые не заметны до определенного момента. Эффективный метод, однако применить его можно не всегда. Так, вероятна ситуация, когда даже имитируемая атака просто отключит проверяемый узел сети или уязвимость окажется негодна для реализации атаки.  
  
**Ответы на вопросы:**1. Охарактеризуйте сканеры безопасности сети.  
**Сканер уязвимости сети** – автоматизированное решение для проведения полного сканирование портов, контроля необходимых обновлений ПО для защиты сети, а также проверки программного и аппаратного обеспечения.  
  
Сканеры 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.  
  
2. На решение каких задач направлены сетевые сканеры.  
Сетевые сканеры направлены на решение следующих задач:  
– идентификация и анализ уязвимостей;  
– инвентаризация ресурсов, таких как операционная система, программное обеспечение и устройства сети;  
– формирование отчетов, содержащих описание уязвимостей и варианты их устранения.  
  
3. Опишите основные механизмы работы сканеров уязвимости сетей.  
  
**Сканеры уязвимостей сети при своей работе используют два основных механизма:**  
  
**Первый** **механизм** **–** *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».  
  
**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.  
  
4. Опишите общий алгоритм работы сканеров.  
 **В общем случае алгоритм работы сканеров следующий:**  
  
**– Проверка заголовков**. Самый простой и быстрый способ на основе сканирования, однако имеющий ряд недостатков. Так, вывод о «провале» делается лишь по результатам анализа заголовков. К примеру, проверяя FTP-сервер, сканер узнает версию обеспечения и на основе этой информации сообщает о возможных уязвимостях. Естественно, специалисты по сетевой безопасности осведомлены о ненадежности этого метода, однако как первый шаг сканирования — это оптимальное решение, не приводящее к нарушению работы сети.  
  
**– Активные зондирующие проверки**. Это сканирование, при котором не проверяется версия ПО, а сравнивается «цифровой слепок» фрагмента программы со «слепком» уязвимости. По тому же принципу действуют антивирусные программы, сравнивая ПО с имеющимися в базе сигнатурами вирусов. Тоже достаточно быстрый метод, хотя и медленнее первого, с большим коэффициентом надежности.  
  
**– Имитация атак**. Это зондирование, которое эксплуатирует дефекты в программном обеспечении. Таким образом подается своеобразный импульс некоторым уязвимостям, которые не заметны до определенного момента. Эффективный метод, однако применить его можно не всегда. Так, вероятна ситуация, когда даже имитируемая атака просто отключит проверяемый узел сети или уязвимость окажется негодна для реализации атаки.  
  
5. По каким принципам работает большинство современных сканеров безопасности сети?   
 Перечислите их.  
**–** сбор информации о сети, идентификация всех активных устройств и сервисов, запущенных на них;  
– обнаружение потенциальных уязвимостей;  
– подтверждение выбранных уязвимостей, для чего используются специфические методы и моделируются атаки;  
– формирование отчетов;  
– автоматическое устранение уязвимостей.  
  
6. Перечислите основные функции сетевых сканеров.  
– Среди основных функций необходимо отметить сканирование документации и передачу информации по электронным адресам;  
– Проверку раздробленной сети, что избавляет администратора от необходимости оценивать каждый узел в отдельности и несколько раз задавать параметры сканирования.  
– Экономию трафика и анализ «исторических» данных.  
  
7. Опишите любой конкретный программный продукт (любой сетевой сканер   
 безопасности).  
**Symantec Security Check**  
Бесплатный сканер одноименного производителя.   
– Основные функции – обнаружение вирусов и троянов, интернет-червей, вредоносных программ, поиск уязвимостей в локальной сети.   
  
– Это онлайн-продукт, состоящий из двух частей: Security Scan, которая проверяет безопасность системы, и Virus Detection, выполняющей полную проверку компьютера на вирусы. Устанавливается быстро и просто, работает через браузер.   
  
– К сожалению, по итогам многих тестов уступает большинству конкурентов, хотя все свои основные функции выполняет. Согласно последним отзывам, этот сканер сети лучше использовать для дополнительной проверки.

**Отметка \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Подпись преподавателя \_\_\_\_\_\_\_\_\_\_\_\_ / А.И. Недера**