Министерство образования Республики Беларусь

ПОЛОЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Кафедра вычислительных систем и сетей

**Методические указания по выполнению лабораторной работы № 1 по курсу «Защита информационных ресурсов компьютерных систем и сетей»**

Сетевой сканер уязвимостей хоста

Доцент,

кандидат технических наук,

Раханов Константин Яковлевич

**Полоцк, 2015**

**Содержание**

[Теоретические сведения 3](#_Toc397592311)

[Сканирование портов 5](#_Toc397592312)

[Сканирование протокола TCP/IP 5](#_Toc397592313)

[Типы сканирования 6](#_Toc397592314)

[Скорость сканирования 8](#_Toc397592315)

[Применение пула потоков 9](#_Toc397592316)

[Цель работы 9](#_Toc397592317)

[Требования, предъявляемые к лабораторной работе 9](#_Toc397592318)

[Ход выполнения работы 10](#_Toc397592319)

[Содержание отчета 10](#_Toc397592320)

**Теоретические сведения**

Основным фактором, определяющим защищенность автоматизированной системы (АС) от угроз безопасности, является наличие в АС уязвимостей защиты. Уязвимости защиты могут быть обусловлены как ошибками в конфигурации компонентов АС, так и другими причинами, в число которых входят ошибки и программные закладки в коде ПО, отсутствие механизмов безопасности, их неправильное использование, либо их неадекватность существующим рискам, а также уязвимости, обусловленные человеческим фактором. Наличие уязвимостей в системе защиты АС, в конечном счете, приводит к успешному осуществлению атак, использующих эти уязвимости.

Сканеры уязвимостей являются, пожалуй, наиболее доступными и широко используемыми средствами анализа защищенности. Основной принцип их функционирования заключается в эмуляции действий потенциального злоумышленника по осуществлению сетевых атак. Поиск уязвимостей путем имитации возможных атак является одним из наиболее эффективных способов анализа защищенности АС, который дополняет результаты анализа конфигурации по шаблонам, выполняемый локально с использованием шаблонов (списков проверки). Сканер является необходимым инструментом в арсенале любого администратора либо аудитора безопасности АС.

**Сканеры уязвимостей** — это программные или аппаратные средства, служащие для осуществления диагностики и мониторинга сетевых компьютеров, позволяющее сканировать сети, компьютеры и приложения на предмет обнаружения возможных проблем в системе безопасности, оценивать и устранять уязвимости.

Сканеры уязвимостей позволяют проверить различные приложения в системе на предмет наличия «дыр», которыми могут воспользоваться злоумышленники. Также могут быть использованы низкоуровневые средства, такие как сканер портов, для выявления и анализа возможных приложений и протоколов, выполняющихся в системе.

Современные сканеры способны обнаруживать сотни уязвимостей сетевых ресурсов, предоставляющих те или иные виды сетевых сервисов. Их предшественниками считаются сканеры телефонных номеров (war dialers), использовавшиеся с начала 80-х и не потерявшие актуальности по сей день. Первые сетевые сканеры представляли собой простейшие сценарии на языке Shell, сканировавшие различные TCP-порты. Сегодня они превратились в зрелые программные продукты, реализующие множество различных сценариев сканирования.

Современный сетевой сканер выполняет четыре основные задачи:

* Идентификацию доступных сетевых ресурсов;
* Идентификацию доступных сетевых сервисов;
* Идентификацию имеющихся уязвимостей сетевых сервисов;
* Выдачу рекомендаций по устранению уязвимостей.

В функциональность сетевого сканера не входит выдача рекомендаций по использованию найденных уязвимостей для реализации атак на сетевые ресурсы. Возможности сканера по анализу уязвимостей ограничены той информацией, которую могут предоставить ему доступные сетевые сервисы.

Принцип работы сканера заключается в моделировании действий злоумышленника, производящего анализ сети при помощи стандартных сетевых утилит. При этом используются известные уязвимости сетевых сервисов, сетевых протоколов и ОС для осуществления удаленных атак на системные ресурсы и осуществляется документирование удачных попыток.

Существует два основных механизма, при помощи которых сканер безопасности проверяет наличие уязвимости - сканирование (scan) и зондирование (probe).

Сканирование - механизм пассивного анализа, с помощью которого сканер пытается определить наличие уязвимости без фактического подтверждения ее наличия - по косвенным признакам. 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.

Зондирование - механизм активного анализа, который позволяет убедиться, присутствует или нет на анализируемом узле уязвимость. Зондирование выполняется путем имитации атаки, использующей проверяемую уязвимость. 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").

Работу сканера уязвимостей делится на 4 этапа:

1. Обнаружение активных IP-адресов, открытых портов, запущенных операционных систем и приложений.
2. Составление отчёта о защищенности (необязательный шаг).
3. Определение уровня возможного вмешательства в операционную систему или приложения (может повлечь сбой).
4. На заключительном этапе сканер может воспользоваться уязвимостью, вызвав сбой операционной системы или приложения.

Сканеры могут быть вредоносными или «дружественными». Дружественные выполняют этап 1, 2 или 3, но никогда не доходят до этапа 4.

Среди сканеров уязвимостей можно выделить:

* сканер портов;
* сканеры, исследующие топологию компьютерной сети;
* сканеры, исследующие уязвимости сетевых служб;
* сетевые черви;
* CGI-сканеры ("дружественные" — помогают найти уязвимые скрипты).

**Сканирование портов**

Сканер портов — программное средство, разработанное для поиска хостов сети, в которых открыты нужные порты. Эти программы обычно используются системными администраторами для проверки безопасности их сетей и злоумышленниками для взлома сети. Может производиться поиск как ряда открытых портов на одном хосте, так и одного определённого порта на многих хостах. Последнее характерно для деятельности сетевых червей.

Сам процесс *называется сканированием портов* или (в случае, когда осуществляется проверка многих хостов) *сканированием сети*. Сканирование портов может являться первым шагом в процессе взлома или предупреждения взлома, помогая определить потенциальные цели атаки (уязвимости). Путем отправления пакетов данных и анализа ответов могут быть исследованы работающие на машине службы (Web-сервер, FTP-сервер, mail-сервер, и т. д.), установлены номера их версий и используемая операционная система.

**Сканирование протокола TCP/IP**

Самым распространённым в сети Интернет стеком протоколов является TCP/IP. Службы, находящиеся на хостах, адресуются двумя идентификаторами: IP-адресом и номером порта. Существует 65536 возможных номеров портов. Большинство сервисов используют ограниченный набор номеров портов, номера которых закрепляются организацией IANA для значимым сервисов. Список закрепленных портов представлен на официальном сайте IANA по адресу: <http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>.

Некоторые сканеры портов ищут только наиболее часто используемые, или наиболее уязвимые порты определённого хоста, набора хостов.

Результат сканирования порта обычно подпадает под одну из трёх категорий:

* *открыт, или соединение принято* (open): хост послал ответ, подтверждающий, что хост «слушает» — принимает соединения на данный порт;
* *закрыт, запрещено, не слушает* (closed): хост послал ответ, информирующий, что соединения на данный порт будут отвергнуты;
* заблокирован, отфильтрован (filtered, firewalled): от хоста не поступило ответа.

Основную угрозу уязвимостей представляют открытые порты, которые влияют на безопасность и стабильной работы программ, служб и операционных систем. Закрытые порты могут представлять опасность только для операционных систем. Заблокированные порты, в настоящее время, реальной опасности не представляют

**Типы сканирования**

**Проверка онлайн.** В ряде случаев, перед сканированием полезно проверить наличие работающей системы на целевом IP-адресе. Эта задача может быть решена путём посылки Echo-сообщений протокола ICMP с помощью утилиты ping c последовательным перебором всех адресов сети или отправкой Echo-сообщения по широковещательному адресу.

Анализируя трафик и отслеживая Echo-сообщения, посылаемые за короткий промежуток времени всем узлам, можно выявить попытки сканирования. Вместо Echo-сообщений могут применяться TCP-сегменты с code bit RST, ответы на несуществующие DNS-запросы. Если сканер получит в ответ ICMP Destination Unreachable пакет с кодом 1 (host unreachable), то значит, тестируемый узел выключен или не подключен к сети.

Следует иметь в виду, что (на практике) неполучение ответа на запросы не гарантирует несуществование хоста, поскольку многие системные администраторы ради «безопасности» идут на нарушение сетевых стандартов и закрывают работу ICMP протокола.

**SYN-сканирование.** Данный тип сканирования является наиболее популярным. Вместо использования сетевых функций операционной системы, сканер портов сам генерирует IP пакеты, и отслеживает ответы на них. Эту технику часто называют сканированием с использованием полуоткрытых соединений, поскольку полное соединение TCP/IP никогда не открывается. Сканер портов генерирует пакет SYN. Если порт на целевом хосте открыт, с него придёт пакет SYN-ACK. Хост сканера отвечает пакетом RST, закрывая тем самым соединение до того, как процесс установления соединения завершился.

Использование самостоятельно сформированных сетевых пакетов имеет ряд преимуществ, давая сканирующей программе полный контроль над посылаемыми пакетами и ответами на них, задержками ответов, и позволяя получить детальные результаты сканирования.

Мнения по поводу потенциального вреда, наносимого сканируемому хосту, неоднозначны. С одной стороны, SYN-сканирование имеет то преимущество, что отдельные приложения никогда не получают входящее соединение (оно обрывается на этапе установки), с другой, отправка пакета RST во время установления соединения может вызывать проблемы у некоторых сетевых устройств, особенно простых, таких как сетевые принтеры.

**TCP-сканирование.** Данный более простой метод использует сетевые функции операционной системы, и применяется, когда SYN-сканирование по тем или иным причинам неосуществимо. Сканер, в случае, если порт открыт, завершает трёхэтапную процедуру установления соединения, и затем сразу закрывает соединение. В противном случае, возвращается код ошибки. Преимуществом данного метода является то, что он не требует от пользователя специальных прав доступа. Тем не менее, использование сетевых функций операционной системы не позволяет производить низкоуровневый контроль, поэтому данный тип используется не столь широко.

Главным недостатком данного метода является большое количество открытых и сразу прерванных соединений, создающее нагрузку на сканируемую систему и позволяющее просто обнаружить активность сканера портов.

**UDP-сканирование.** Сканирование с помощью пакетов UDP также возможно, хотя имеет ряд особенностей. Для UDP отсутствует понятие соединения, и нет эквивалента TCP-пакету SYN. Тем не менее, если послать UDP-пакет на закрытый порт, система ответит сообщением ICMP «порт недоступен». Отсутствие такого сообщения истолковывается как сигнал того, что порт открыт. Однако, если порт блокируется брандмауэром, метод неверно покажет, что порт открыт. Если заблокированы ICMP-сообщения о недоступности порта, все порты будут казаться открытыми. Также, может быть установлено ограничение на частоту использования ICMP-пакетов, что также влияет на результаты, даваемые методом.

Альтернативным подходом является отправка UDP-пакетов, специфичных для приложения, в расчёте на получения ответа с уровня приложения. Например, отправка запроса DNS на порт 53 приведёт к ответу, если по запрашиваемому адресу имеется DNS-сервер. Проблема в данном случае состоит в наличии соответствующего «пробного» пакета для каждого из портов. В некоторых случаях, сервис может присутствовать, но быть сконфигурирован таким образом, чтобы не отвечать на известные «пробные» пакеты.

Также возможен комбинированный подход, сочетающий в себе оба вышеуказанных метода. Так, сканирование может начинаться отправкой UDP-пакета для проверки на ICMP-ответ «порт недоступен», а затем порты с неопределённым результатом «открыт или заблокирован» могут повторно проверяться на ответы, специфичные для приложения.

**ACK-сканирование.** Данное сканирование применяется для определения, фильтруется данный порт или нет, и особенно эффективен для определения наличия брандмауэров и выяснения их правил. Простая фильтрация пакетов разрешит прохождение пакетов с установленным битом ACK (используемые для уже установленных соединений), тогда как более сложные брандмауэры — нет.

**FIN-сканирование.** Некоторые серверы способны отследить попытку SYN-сканирования их портов. Например, попытка SYN-сканирования может быть распознана по поступлению «поддельных» SYN-пакетов на закрытые порты защищаемого сервера, и в случае опроса нескольких портов сервер разрывает соединение для защиты от сканирования.

Сканирование с использованием FIN-пакетов позволяет обойти подобные средства защиты. Согласно RFC 793, на прибывший FIN-пакет на закрытый порт сервер должен ответить пакетом RST. FIN-пакеты на открытые порты должны игнорироваться сервером. По этому различию становится возможным отличить закрытый порт от открытого.

Указанной рекомендации RFC 793 придерживаются не все операционные системы. Например, реакция Windows семейства 95/98/NT на приходящий FIN-пакет не различается для открытого и закрытого порта.

**Скорость сканирования**

Скорость сканирования зависит от таких факторов как количество проверяемых портов, склонности сканируемых систем к ICMP-ответам, избранного способа сканирования, количества проверяемых хостов и их склонности отвечать на запросы, а также от того, насколько осуществляющая сканирование сторона озабочена незаметностью своей деятельности. Чтобы не дать себя раскрыть, сканер портов может растянуть отправку сообщений во времени. С другой стороны, при большом количестве проверяемых хостов их сканирование может осуществляться параллельно так, что нагрузка на каждый конкретный хост будет весьма низка.

**Применение пула потоков**

Большое количество потоков сканера требуют от операционной системы большого объема работы, связанной с учетом использования системных ресурсов, поэтому создавать и уничтожать их — не самое лучшее решение. Создание и уничтожение потоков влечет за собой увеличение ресурсов системы.

Вместо этого для всех потребностей программы в потоках лучше использовать существующий набор потоков, применяемых повторно по мере необходимости. Такой подход называют пулом потоков. Используя пул потоков, можно избавится от необходимости самостоятельно создавать, уничтожать и контролировать потоки — все это делается пулом потоков.

Можно разработать собственный пул потоков или использовать предоставляемый операционной системой (платформой). Преимущество использования пула потоков вместо создания собственных потоков заключается в том, что операционная система берет на себя планирование задач — задачей программиста является своевременная отправка исполняемых функций в пул потоков, чтобы операционная система могла нагрузить все аппаратные мощности. Приложение должно выдавать задачи пулу потоков, где эти задачи помещаются в очередь потоков и в конечном счете планируются к выполнению в аппаратных потоках, а все остальное программисту неподвластно.

**Цель работы**

Разработать приложение для сканирования открытых портов на сетевом хосте.

**Требования, предъявляемые к лабораторной работе**

Язык программирования: определяется студентом.

Метод сканирования: определяется студентом.

Функциональность сканера портов:

* использование пула потоков, с возможностью корректировки (выставления) количества потоков в пуле;
* вывод информации по времени сканирования для различного количества потоков в пуле;
* вывод статистики по обнаруженным уязвимостям.

**Ход выполнения работы**

1. Изучить теоретические сведения, ознакомиться с походами к поиску уязвимостей на хостах, методами сканирования портов.
2. Выбрать технологию разработки, метод сканирования
3. Разработать приложение для сканирования открытых портов на сетевом хосте
4. Написать отчет о проделанной работе.
5. Защитить отчет.
6. Предоставить отчет и исходные коды приложения в архиве (формат архива: «ZIRKSiS\_Lab\_1\_IT-1\_Фамилия\_на\_транслите.zip»).

**Содержание отчета**

1. Титульный лист, содержащий пункты «Разработал», «Проверил».
2. Описания реализации приложения с листингом основных функций, скриншотами, демонстрирующими работу приложения.
3. Вывод о функционировании полученного приложения, содержащий СОБСТВЕННОЕ заключение о результатах работы приложения.