Методики сканирования портов: назначения, преимущества, недостатки.

Введение

Сканирование портов, полезный инструмент администратора компьютерных сетей позволяющий своевременно находить уязвимые места в сетевом экране и конфигурациях программного обеспечения сетевого оборудования. Существуют различные методы сканирования портов, каждый из которых имеет свои преимущества и недостатки, а так же особенности в получаемой при сканировании информации.

Сканирование портов (сканер портов)

Сканирование портов - сканирование хоста или сети на наличие открытых портов. ПО для сканирование портов называется **сканером портов**. Так как программное обеспечение работающее по тому или иному порту может иметь уязвимости, такой открытый порт может являться серьезной угрозой информационной безопасности. В связи с этим сканерами портов пользуются или системные администраторы для предотвращения атак или злоумышленники для поиска точек входа в систему. [2] Результаты сканирования сети классифицируются следующим образом:

- открытый порт - сканером получен ответ, хост принимает соединения на данный порт.
- закрытый порт - сканером получен ответ, хост не принимает соединения на данный порт.
- заблокированный порт - сканер не получил ответ.

Методы сканирования портов

Перед сканированием любого типа обычно проводится проверка на наличие указанного хоста в сети. При помощи протокола ICMP отправляются echo сообщения на все сканируемые адреса, но отсутствие ответа на echo запрос не всегда означает отсутствие хоста в сети, так как системные администраторы зачастую запрещают работу ICMP в целях безопасности. Такой тип сканирования иногда называют **ping-сканированием**.

- **SYN сканирование** - самый распространенный тип сканирования. Сканер портов генерирует IP пакеты напрямую без использования сетевых функций ОС предназначенных для установки TCP соединения. Это все необходимо для того чтобы напрямую управлять содержимым заголовка TCP и позволяет не создавать полностью открытое соединение. Принцип работы SYN сканирования таков.

1. Сканер создает пакет с установленным флагом SYN и отправляет его на указанный адрес (диапазон адресов).
2. Если порт на целевом хосте открыт то в ответ сканеру придет пакет SYN-ACK и это означает что порт открыт. Если хост не отвечает значит SYN сканирование скорее всего заблокировано на уровне правил межсетевого экрана.
3. Сканер отвечает пакетом RST и закрывает соединение до завершение его установки.

Этот способ сканирования позволяет одновременно сканировать большое количество адресов и портов не создавая большой нагрузки на хост и сеть созданием и закрытием множества TCP соединений. Но для работы такого сканера потребуются повышенные привилегии и стороннее ПО для генерации IP пакетов в обход TCP стека операционной системы.

- **TCP сканирование** - самый простой способ сканирования портов. Используя сетевые функции операционной системы осуществляется попытка создать TCP соединение с хостом. При условии что порт открыт соединение будет установлено, иначе порт закрыт. Такой тип сканирования не требует специальный драйверов сетевых устройств и повышенных привилегий для сканирования сети, но сильно нагружает сканируемый хост.

- **ACK сканирование** - этот тип сканирования используется для проверки наличия межсетевого экрана и определения сложности его правил фильтрации. На хост отправляются пакеты с установленным флагом ACK, который устанавливается только при установленном соединении. Если в межсетевом экране используются простые правила фильтрации то экран пропустит этот пакет, более сложные правила учитывают и блокируют такой тип сканирования.

- **FIN сканирование** - данный тип сканирования использует особенность спецификации TCP (RFC 793), в которой описано что на пакет FIN отправленный на закрытый порт, сервер должен ответить пакетом с флагом RST, если порт открыт то сервер игнорирует такой пакет. Такое сканирование применяется если сервер умеет распознавать другие типы сканирования, но не все разработчики ПО придерживаются спецификаций RFC, поэтому FIN сканирование может не дать результатов.

В протоколе UDP отсутствует понятие соединение, поэтому мы не можем определить силами протокола был получен отправленный пакет или нет. Сканирование UDP порта имеет ряд особенностей. При отправке UDP пакета на закрытый порт при включенном протоколе ICMP, сканер получит ответ “порт закрыт”, если же системный администратор отключил ICMP то компьютерам извне будет казаться что все порты открыты.

Для того чтобы обойти отключение ICMP или межсетевой экран можно формировать UDP пакет специфичный для ПО работающего с данным портом. Таким образом при открытом порте мы получим ответ уровня приложения. Но подготавливать тестовые пакеты для всего сетевого ПО, работающего по UDP - невозможная задача. Поэтому может использоваться комбинированное сканирование - сначала сканируются все порты UDP отправкой пустого пакета, а далее используются специализированные пакеты для выбранных портов, если они поддерживаются ПО для сканирования.

Выводы

Существуют различные методы сканирования портов, с своими особенностями и выбирать метод сканирования необходимо исходя из множества факторов таких как : программное и аппаратное обеспечение сканируемых устройств, настройки сетевых экранов, особенности ПО на сканирующем хосте и другие.

Список литературы

[1] Интернет-ресурс *Port scanning techniques* URL: https://nmap.org/book/man-port-scanning-techniques.html

[2] Интернет-ресурс *Википедия. Сканер портов.* URL: https://ru.wikipedia.org/wiki/Сканирование_портов