# Практическая работа № 21

Усик Степан

**Тема** Выполнение установки сетевого сканера. Определение списка открытых портов в операционной системе Windows при помощи сетевого сканера

**Цель** научиться устанавливать сетевой сканер и работать с ним

**Теоретические сведения**

Сканер портов относится к программному приложению, которое сканирует сервер на наличие открытых портов. Он позволяет аудиторам и сетевым администраторам проверять сетевую безопасность, в то время как злоумышленники и хакеры используют ее для определения открытых портов для использования или запуска вредоносных служб на компьютере или сервере.

Сканирование портов представляет собой способ определения, какие порты в сети открыты. Поскольку порты на компьютере — это место, где информация отправляется и принимается, сканирование портов аналогично стуку в дверь, чтобы увидеть, находится ли кто-то дома.

Выполнение сканирования портов в локальной сети или на сервере позволяет определить, какие порты открыты и находятся в режиме прослушивания (**listening**) (получения информации), а также выявить наличие таких устройств безопасности, как межсетевые экраны, которые находятся между отправителем и целью. Этот метод известен как дактилоскопия (**fingerprinting**). Это также полезно для тестирования сетевой безопасности и надежности брандмауэра системы. Благодаря этой функциональности, это также популярный инструмент разведки для злоумышленников, ищущих слабую точку доступа для проникновения в компьютер или сервер.

Порты различаются по своим назначениям. Они пронумерованы **от 0 до 65535**, но определенные диапазоны используются чаще. Порты с 0 по 1023 идентифицируются как «общеизвестные порты» или стандартные порты и были назначены для определенных служб, агентством по присвоению номеров в Интернете (IANA). Некоторые из наиболее известных портов и назначенных им служб включают в себя:

* Порт 20 (UDP) - протокол передачи файлов ([FTP](http://pyatilistnik.org/spisok-standartnyih-komand-ftp/)) для передачи данных
* Порт 22 (tcp) - протокол Secure Shell ([SSH](http://pyatilistnik.org/ssh-esxi-shell-vmware-esxi-5/)) для безопасного входа, FTP и переадресации портов
* Порт 23 (tcp) - протокол [Telnet](http://pyatilistnik.org/kak-ustanovit-telnet-klienta-v-windows-server-2012r2/" \t "_blank) для не зашифрованных текстовых коммутаций
* Порт 53 (UDP) - Система доменных имен ([DNS](http://pyatilistnik.org/chto-takoe-dns/)) переводит имена всех компьютеров в Интернете в [IP-адреса](http://pyatilistnik.org/konflikt-ip-adresov-windows-reshaem-za-minutu/)
* [Порт 80](http://pyatilistnik.org/how-to-open-port-443-in-windows/) (tcp) - Всемирная паутина HTTP

Сканирование портов отправляет тщательно подготовленный пакет на каждый номер порта назначения. Основные методы, которые может использовать программное обеспечение для сканирования портов:

* **Ваниль (Vanilla)** - самый простой скан; попытка подключиться ко всем 65 536 портам по по очереди. Ванильное сканирование — это полное сканирование соединения, то есть оно отправляет флаг SYN (запрос на подключение) и после получения ответа SYN-ACK (подтверждение подключения) отправляет обратно флаг ACK. Этот обмен SYN, SYN-ACK, ACK включает квитирование TCP. Полное сканирование подключений является точным, но очень легко обнаруживается, поскольку все подключения всегда регистрируются брандмауэрами.
* **Сканирование SYN (SYN Scan)** - также называется полуоткрытым сканированием, оно только отправляет SYN и ожидает ответа SYN-ACK от цели. Если ответ получен, сканер никогда не отвечает. Так как соединение TCP не было установлено, система не регистрирует взаимодействие, но отправитель узнал, открыт порт или нет.
* **Сканирование XMAS и FIN (XMAS and FIN Scans)** - набор сканирований, используемых для сбора информации без регистрации в целевой системе. При сканировании FIN незапрошенный флаг FIN (обычно используемый для завершения установленного сеанса) будет отправлен на порт. Ответ системы на этот случайный флаг может показать состояние порта или брандмауэр. Например, закрытый порт, который получает незапрошенный пакет FIN, ответит пакетом RST (мгновенный прерывание), но открытый порт проигнорирует его. Сканирование XMAS просто отправляет набор всех флагов, создавая бессмысленное взаимодействие. Ответ системы может быть интерпретирован для лучшего понимания портов системы и брандмауэра.
* **Сканирование отказов FTP (FTP Bounce Scan)** - позволяет замаскировать местоположение отправителя путем пересылки пакета через FTP-сервер. Это также предназначено для отправителя, чтобы остаться незамеченным.
* **Сканирование развертки (Sweep scan)** - пингует один и тот же порт на нескольких компьютерах, чтобы определить, какие компьютеры в сети активны. Это не раскрывает информацию о состоянии порта, а сообщает отправителю, какие системы в сети активны. Таким образом, его можно использовать как предварительное сканирование.

Сканеры открытых портов

1. Advanced Port Scanner
2. Angry IP Scanner
3. Nmap

**Методические указания**

1. Для поиска воспользуйтесь программой AngryIp scanner (скачать можно с официального сайта по адресу www.angryip.org). Приложение осуществляет сканирование портов. *(Можете воспользоваться любой другой на ваш выбор.)*
2. Запустите утилиту на компьютере. Перед вами откроется окно. Можете выполнить настройки программы. Зайдите в раздел Tools и потом нажмите на Preferences. Поставьте обязательно галочку на вкладке Scan dead hosts which dont reply to ping.

Это позволит выполнять сканирование более медленно и при этом находить больше прокси. В опции Ports указывайте порты. В поле P Range введите диапазоны поиска. Потом нажимайте кнопочку Start. Процесс поиска запущен. Осталось только некоторое время подождать и посмотреть результаты. Перед вами будет целый список компьютеров.

1. Также удобная программа для поиска – NetSearch.

Скачайте и установите себе на компьютер и запустите программу (скачать можно с портала www.softportal.com). Перед вами откроется окно. Чтобы начать поиск, найдите вкладку «Сканирование сети». Далее нажмите кнопку «Старт» и подождите результат. Кроме того, вы можете задать параметры поиска. У вас будет возможность отправить сообщение пользователю найденного компьютера.

В настройках программы можно сделать так, что программа NetSearch будет запускаться автоматически. Для этого установите параметры на NetSearch.exe auto.

1. NetView – программа, осуществляющая поиск IP-адресов, имена компьютеров. Официального сайта у программы нет, однако ее можно скачать на софт-портале www.soft.oszone.net. Установите любой удобный для вас язык интерфейса. Это можно сделать в настройках.

Чтобы начать сканирование, достаточно нажать на кнопку «Сканер сети» в разделе «Инструменты» или «Запустить сканер». Результат появится в центре рабочего окна. Если вы нажмете на одном из названий компьютера, сможете произвести редактирование. Пользователь может также ввести те IP-адреса, которые он хочет найти. Программа NetView просканирует сеть и выдаст вам результат. Для работы можно использовать любую из перечисленных программ.

**Контрольные вопросы:**

**1. 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

2.GFI LanGuard

Одна из компаний-лидеров на рынке информационной безопасности — GFI Software. Компания работает с 1992 года и за это время заслужила репутацию надежной организации, производящей профессиональные продукты для решения широкого спектра ИТ-задач.

Nessus

Проект был запущен еще в 1998 году, а в 2003 разработчик Tenable Network Security сделал сетевой сканер безопасности коммерческим. Но популярность продукта не упала. Согласно статистике более 17% пользователей предпочитают именно Nessus. Регулярно обновляемая база уязвимостей, простота в установке и использовании, высокий уровень точности — его преимущества перед конкурентами. А ключевой особенностью является использование плагинов. То есть любой тест на проникновение не зашивается наглухо внутрь программы, а оформляется в виде подключаемого плагина. Аддоны распределяются на 42 различных типа: чтобы провести пентест, можно активировать как отдельные плагины, так и все плагины определенного типа — например, для выполнения всех локальных проверок на Ubuntu-системе. Интересный момент — пользователи смогут написать собственные тесты с помощью специального скриптового языка.

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.

XSpider

Компания Positive Technologies работает на рынке более 10-ти лет и обладает одним из крупнейших исследовательских центров безопасности. У этой корпорации тоже есть свой сетевой сканер — программа XSpider, которая, по заявлению разработчика, может выявить треть уязвимостей завтрашнего дня. Ключевой особенностью этого сканера является возможность обнаружения максимального количества «провалов» в сети еще до того, как их увидят хакеры. При этом сканер работает удаленно, не требуя установки дополнительного ПО. Отработав, сканер отправляет специалисту по безопасности полный отчет и советы по устранению «дыр».

QualysGuard

Многофункциональный сканер уязвимостей. Он предоставляет обширные отчеты, которые включают:

оценку уровня критичности уязвимостей;

оценку времени, необходимого для их устранения;

проверку степени их воздействия на бизнес;

анализ тенденций в области проблем безопасности.

Фирма-разработчик продукта, Qualys, Inc., широко известна в мировой среде ИТ-специалистов, у которых этот сканер пользуется доверием. Достаточно сказать, что около 50-ти компаний из списка Forbes «Global 100» используют данный продукт.

3.ISS Internet Scanner в описании не нуждается. Он показал себя как всегда на высоком уровне, правда на этот раз уступив пальму первенства XSpider-у.

XSpider оказался бесспорным лидером, сильно оторвавшись от конкурентов особенно при поиске уязвимостей в Windows и Solaris, что особенно приятно при его небольшом размере и бесплатном распространении. Есть большой минус: очень мало выводится информации при выдаче списка уязвимостей, что предполагает высокий уровень знаний и профессионализма у специалиста использующего эту программу.

LanGuard с натяжкой можно назвать сканером безопасности. Он очень хорошо работает с NetBios, выдавая список ресурсов, сервисов и пользователей. Эта способность сильно отличает сканер от остальных, но вот именно только эта. На этом преимущества LanGuard заканчиваются.

ShadowSecurityScanner практически не отстал от ISS. И это при столь большой разнице в их цене. У программы простой интерфейс похожий на интерфейс сканера Retina. Подробные советы и рекомендации по устранению уязвимостей легко позволяют справиться с проблемами. Минусы: небольшое количество распознаваемых уязвимостей, гораздо большее потребление системных ресурсов при работе по сравнении с другими сканерами.

X-Scan бесплатный сканер по возможностям похожий на LanGuard, но немного его превосходящий. Минусы: не очень читабельный интерфейс программы, отсутствие каких-либо комментариев про найденные уязвимости.

4.(TCP SYN сканирование)

SYN это используемый по умолчанию и наиболее популярный тип сканирования. На то есть несколько причин. Он может быть быстро запущен, он способен сканировать тысячи портов в секунду при быстром соединении, его работе не препятствуют ограничивающие бранмауэры. Этот тип сканирования относительно ненавящив и незаметен, т.к. при таком сканировании TCP соединение никогда не устанавливается до конца. Он работает с любым TCP стеком, не завися от каки-либо особенностей специфичной платформы, как это происходит при сканированиях типа FIN/NULL/Xmas, Maimon и idle сканировании. Он также предоставляет ясную и достоверную дифференциацию между состояниями открыт, закрыт и фильтруется.

Эту технику часто называют сканированием с использованием полуотрытых соединений, т.к. вы не открываете полного TCP соединения. Вы посылаете SYN пакет, как если бы вы хотели установить реальное соединение и ждете. Ответы SYN/ACK указывают на то, что порт прослушивается (открыт), а RST (сброс) на то, что не прослушивается. Если после нескольких запросов не приходит никакого ответа, то порт помечается как фильтруемый. Порт также помечается как фильтруемый, если в ответ приходит ICMP сообщение об ошибке недостижимости (тип 3, код 1,2, 3, 9, 10 или 13).

-sT (TCP сканирование с использованием системного вызова connect)

Это используемый по умолчанию тип TCP сканирования, когда недоступно SYN сканирование. Это происходит в случае, когда у пользователя нет привилегий для использования сырых пакетов или при сканировании IPv6 сетей. Вместо того, чтобы использовать сырые пакеты, как это происходит при большинстве других типов сканирования, Nmap "просит" операционную систему установить соединение с целевой машиной по указанному порту путем системного вызова connect. Это такой же высокоуровневый системный вызов, используемый браузерами, P2P клиентами и другими приложениями для установки соединения. Этот вызов является частью программируемого интерфейса, известного как Berkeley Sockets API. Вместо того, чтобы считывать ответы в форме сырых пакетов, Nmap использует этот API для получения информации о статусе каждой попытки соединения.

При доступности SYN сканирования, оно, безусловно, будет являться лучшм выбором. У Nmap имеется меньше возможностей контролирования высокоуровнего вызова connect по сравнению с сырыми пакетами, что делает его менее эффективным. Системный вызов завершает соединения по открытым портам, вместо того, чтобы использовать полуоткрытые соединения, как в случае с SYN сканированием. Таким образом на получение той же самой информации потребуется больше времени и пакетов, да к тому же целевые машины скорее всего запишут это соединение в свои логи. То же самое сделает и порядочная IDS, хотя большинство машин не имеют такой системы защиты. Многие службы на вашей Unix системе будут добавлять запись в системный лог (syslog), а также сообщение об ошибке, когда Nmap будет устанавливать и закрывать соединение без отправления данных. Некоторые службы даже аварийно завершают свою работу, когда это происходит, хотя это не является обычной ситуацией. Администратор, который увидит в логах группу записей о попытке установки соединения от одной и той же системы, должен знать, что его машина подверглась такому типу сканирования.

-sU (Различные типы UDP сканирования)

В то время как большинство сервисов Интернета используют TCP протокол, UDP службы также широко распространены. Тремя наиболее популярными являются DNS, SNMP и DHCP (используют порты 53, 161/162 и 67/68). Т.к. UDP сканирование в общем случае медленнее и сложнее TCP, то многие специалисты по безопасности игнорируют эти порты. Это является ошибкой, т.к. существуют UDP службы, которые используются атакующими. К счастью, Nmap позволяет инвентаризировать UDP порты.

UDP сканирование запускается опцией -sU. Оно может быть скомбинировано с каким-либо типом TCP сканирования, например SYN сканирование (-sS), чтобы использовать оба протокола за один проход.

UDP сканирование работает путем посылки пустого (без данных) UDP заголовка на каждый целевой порт. Если в ответ приходит ICMP ошибка о недостижимости порта (тип 3, код 3), значит порт закрыт. Другие ICMP ошибки недостижимости (тип 3, коды 1, 2, 9, 10 или 13) указывают на то, что порт фильтруется. Иногда, служба будет отвечать UDP пакетом, указывая на то, что порт открыт. Если после нескольких попыток не было получено никакого ответа, то порт классифицируется как открыт|фильтруется. Это означает, что порт может быть открыт, или, возможно, пакетный фильтр блокирует его. Функция определения версии (-sV) может быть полезна для дифференциации действительно открытых портов и фильтруемых.

Большой проблемой при UDP сканировании является его медленная скорость работы. Открытые и фильтруемые порты редко посылают какие-либо ответы, заставляя Nmap отправлять повторные запросы, на случай если пакеты были утеряны. Закрытые порты часто оказываются еще большей проблемой. Обычно они в ответ возвращают ICMP ошибку о недостижимости порта. Но в отличии от RST пакетов отсылаемых закрытыми TCP портами в ответ на SYN или сканирование с установкой соединения, многие хосты ограничивают лимит ICMP сообщений о недостижимости порта по умолчанию. Linux и Solaris особенно строги в этом плане. Например, ядро Linux 2.4.20 огранивает количество таких сообщений до одного в секунду (в net/ipv4/icmp.c).

Nmap обнаруживает такого рода ограничения и соответственно сокращает количество запросов, чтобы не забивать сеть бесполезными пакетами, которые все равно будут отброшены целевой машиной. К сожалению, при ограничении в стиле Linux (один пакет в секунду) сканирование 65,536 портов займет более 18 часов. К способам увеличения скорости UDP сканирования относятся: параллельное сканирование нескольких хостов, сканирование в первую очередь только наиболее популярных портов, сканирование из-за брандмауэра и использование --host-timeout дял пропуска медленных хостов.

-sN; -sF; -sX (TCP NULL, FIN и Xmas сканирования)

Эти три типа сканирования используют (другие типы сканирования доступны с использованием опции --scanflags описанной в другой секции) незаметную лазейку в TCP RFC, чтобы разделять порты на открытые и закрытые. На странице 65 RFC 793 говорится, что «если порт назначения ЗАКРЫТ .... входящий сегмент не содержащий RST повлечет за собой отправку RST в ответ.» На следующей странице, где обсуждается отправка пакетов без установленных битов SYN, RST или ACK, утверждается что: «вы вряд ли с этим столкнетесь, но если столкнетесь, то сбросьте сегменти и вернитесь к исходному состоянию.»

Когда сканируется система отвечающая требованиям RFC, любой пакет, не содержащий установленного бита SYN, RST или ACK, повлечет за собой отправку RST в ответ в случае, если порт закрыт, или не повлечет никакого ответа, если порт открыт. Т.к. ни один из этих битов не установлен, то любая комбинация трех оставшихся (FIN, PSH и URG) будет являться правильной. Nmap использует это в трех типах сканирования:

Null сканирование (-sN)

Не устанавливаются никакие биты (Флагов в TCP заголовоке 0)

FIN сканирование (-sF)

Устанавливается только TCP FIN бит.

Xmas сканирование (-sX)

Устанавливаются FIN, PSH и URG флаги.

-sA (TCP ACK сканирование)

Этот тип сканирования сильно отличается от всех других тем, что он не способен определить открый порт open (или даже открытый|фильтруемый). Он используются для выявления правил брандмауэров, определения учитывают ли он состояние или нет, а также для определения фильтруемых ими портов.

Пакет запроса при таком типе сканирования содержит установленным только ACK флаг (если не используется --scanflags). При сканировании нефильтруемых систем, открытые и закрытые порты оба будут возвращать в ответ RST пакет. Nmap помечает их как не фильтруемые, имея ввиду, что они достижимы для ACK пакетов, но неизвестно открыты они или закрыты. Порты, которые не отвечают или посылают в ответ ICMP сообщение об ошибке (тип 3, код 1, 2, 3, 9, 10 или 13), помечаются как фильтруемые.

-sW (TCP Window сканирование)

Этот тип сканирования практически то же самое, что и ACK сканирование, за исключением того, что он использует особенности реализации различных систем для разделения портов на открытые и закрытые, вместо того, чтобы всегда при получении RST пакета выводить не фильтруется. Это осуществляется путем анализа TCP Window поля полученного в ответ RST пакета. В некоторых системах открытые порты используют положительное значение этого поля (даже в RST пакетах), а закрытые - нулевое. Поэтому вместо того, что все время при получении RST пакета в ответ помечать порты как не фильтруемые, при Window сканировании порты помечаются как открытые или закрытые, если значение поля TCP Window положительно или равно нулю соответственно.

Этот тип сканирования основывается на особенностях реализации меньшинства систем в Интернете, поэтому вы не можете все время доверять ему. В общем случае в системах, не имеющих таких особенностей, все порты будут помечаться как закрытые. Конечно, это возможно, что у машины действительно нет открытых портов. Если большинство просканированных портов закрыты, и лишь несколько распространненых портов (таких как 22, 25, 53) фильтруются, то скорее всего результатам сканирования можно доверять. Иногда, системы будут вести себя прямо противоположным образом. Если в результате сканирования будет найдено 1000 открытых портов и 3 закрытых или фильтруемых, то как раз эти 3 могут оказаться действительно открытыми.

-sM (TCP сканирование Мэймона (Maimon))

Этот тип сканирования носит имя своего первооткрывателя, Уриела Мэймона (Uriel Maimon). Он описал эту технику в журнале Phrack Magazine, выпуск #49 (Ноябрь 1996). Версия Nmap с поддержкой этого типа сканирования была выпущена через два номера. Техника практически такая же как и при NULL, FIN и Xmas сканированиях, только в качестве запросов используются запросы FIN/ACK. Согласно RFC 793 (TCP), в ответ на такой запрос должен быть сгенерирован RST пакет, если порт открыт или закрыт. Тем не менее, Уриел заметил, что многие BSD системы просто отбрасывают пакет, если порт открыт.

--scanflags (Заказное TCP сканирование)

Действительно продвинутым пользователям Nmap не нужды ограничивать себя заранее приготовленными типами сканирования. С помощью опции --scanflags вы можете разработать свой тип сканирования путем задания специфичных TCP флагов. Используйте свое воображение, обходя системы обнаружения вторжений, чьи производители просто просмотрели справочное руководство Nmap, путем задания собственных правил!

Аргументом опции --scanflags может быть числовое значение, например, 9 (PSH и FIN флаги), но использование символьных имен намного проще. Используйте любые комбинации URG, ACK, PSH, RST, SYN и FIN. Например, опцией --scanflags URGACKPSHRSTSYNFIN будут установлены все флаги, хотя это и не очень полезно для сканирования. Порядок задания флагов не имеет значения.

В добавлении к заданию желаемых флагов, вы также можете задать тип TCP сканирования (например, -sA или -sF). Это укажет Nmap на то, как необходимо интерпретировать ответы. Например, при SYN сканировании отсутствие ответа указывает на фильтруемый порт, тогда как при FIN сканировании - на открытый|фильтруемый. Nmap будет осуществлять заданный тип сканирования, но используя указанные вами TCP флаги вместо стандартных. Если вы не указываете тип сканирования, то по умолчанию будет использоваться SYN.

5. Сетевая атака в большинстве случаев представляет собой атаку на какой-либо доступный из сети сервис на вашем компьютере. Если такого сервиса у Вас нет — можно не беспокоиться, что кто-то Вас «взломает». В этом случае опасаться следует других угроз — вирусы, malware (нежелательные программы), и другие внутренние воздействия. Рекомендации по предотвращению — стандартны и описаны много раз. Установите антивирус, регулярно его обновляйте, регулярно устанавливайте обновления операционной системы, не запускайте неизвестные Вам программы и так далее. Но даже и в этом случае наличие персонального файрвола на компьютере может помочь Вам в случае, когда антивирус или обновления операционной системы ещё не в состоянии блокировать новые угрозы. Просто всегда внимательно читайте, что именно предлагает Вам сделать та или иная программа, и старайтесь понять, а нужно ли, чтобы это действие действительно было выполнено.

Хотим отметить, что по умолчанию в настройках Windows систем для работы с приложениями в локальной сети, есть открытые для внешнего доступа «серверные» сервисы, то есть те к которым можно обратится с другого компьютера. Поэтому не стоит отключать встроенный брандмауэр (файрвол), либо не пренебрегайте установкой сторонних продуктов подобной функциональности.

6.Принцип работы заключается в том, что сканирующий комп использует так называемое полусоединение, то есть, получив SYN-ACK от сканируемого устройства, сканер завершает свою работу. Выглядит это так: Порт открыт.

7.Закрытые порты не дают 100% гарантии, что Ваш компьютер будет полностью защищен от вирусов. Самая лучшая защита - это здравый смысл. Устанавливайте обновления операционной системы, не переходите по подозрительным ссылкам в интернете и не устанавливайте программы из неофициальных источников. Для более полной уверенности, в том, что Вы полностью защищены, необходимо купить VPN. Это позволит обезопасить себя от перехвата Вашего трафика хакерами.

8.Атака со сканированием портов или Сканирование портов это незаконная деятельность, при которой порты компьютера автоматически сканируются или любой другой компьютер, подключенный к сети. Цель этого — проверить, какие порты открыты, закрыты или у какого из них есть протокол безопасности.



Я сканировал программой spotlight.