Nmap – (Network Mapper) сканнер уязвимостей сетей и сайтов с открытым исходным кодом. Истории создания посвещается.

Сетевой сканнер Nmap – удивительное творение свободной мысли когда то начинающего программиста Гордона Лиона (псевдоним Fyodor) создавшего фактически из расширенного сканера открытых портов (10 способов сканирования) полноценный хакерский инструмент, являющийся не только кроссплатформенным продуктом, но и имеющим в свободном доступе исходники на языке lua. Сканнер постоянно модернизируется свободными программистами, разрабатывающими скрипт команды (nse) и библиотеки данных. Фактически каждый знакомый с языком lua может внести вклад в его совершенствование или даже усовершенствовать исходник. Что касается выхода на профессиональный уровень, то это произошло как раз 10 лет назад когда версии 4.6 получили усовершенствованные конструктор команд и графический интерфейс трассировки маршрута. Начиная с этого времени ошибки в работе программы и в структуре интернет команд были устранены. Программа преобрела современный вид. (Он так и остался консервативным). Что делает честь разработчику, поскольку не отвлекает на бесполезные примочки. Конечно же набор скриптов в то время не превышал 50 экземпляров (сейчас 589), а библиотека интернет подходов 30 единиц (сейчас 132 основных). Единственным недостатком является разве что отсутствие привязки трассировки маршрута к географической карте, а также возможности задачи числа пропинговки звеньев маршрута как например в программе «Диагностика сайта». Но всё же это не столь важно для работы. Вот как всё начиналось:

ДЕНЬ РОЖДЕНИЯ СКАНЕРА NMAP, О КОТОРОМ ВПЕРВЫЕ БЫЛО РАССКАЗАНО В ЖУРНАЛЕ PHRACK.

Решающее для популярности nmap значение сыграла статья "Искусство сканирования" (The art of scanning), которую Fyodor написал в 1997 году для известного андеграунд-журнала Phrack. К статье прилагался исходный код сканера на языке C, что дало возможность каждому технически подкованному специалисту опробовать новый инструмент в действии. К тому моменту nmap поддерживал девять методов сканирования, в числе которых были и достаточно изысканные.

История проекта nmap (Network MAPper - составитель карты сети) достаточно долгая и не лишена увлекательности. Доказательством

популярности пакета может служить огромное количество загруженных с официального сайта (www.insecure.org/mnap/) копий программы. В пользу этого утверждения свидетельствует и тот факт, что код nmap, разрабатывавшийся для Unix-платформы, был впоследствии перенесен на платформу Windows, а интерфейс командной строки был удачно дополнен графическим интерфейсом (front-end).

Истоки

История проекта nmap началась более двадцати лет назад, когда хакер Fyodor Yarochkin занялся изучением свойств стека TCP/IP. Разумеется, практика - наилучший способ познать неизведанное, и в этом Fyodor преуспел. На момент начала проекта nmap в сетевом мире уже существовало с полдюжины различных сканеров портов. Все они обладали интересными свойствами и вполне успешно применялись специалистами. Но важнее всего было то, что каждая программа демонстрировала тот или иной подход к реализации концепции сканирования сети. Так, сканер pscan, созданный хакером Pluvius, показывал отличную производительность, а реализовать vanilla-scan (его еще называют TCP connect(), согласно ключевому признаку взаимодействия с сетью) сможет любой программист, начавший изучать сетевое программирование. Fyodor начал работу с того, что объединил известные на тот момент сканеры в единый пакет. Но к этому занятию он подошел творчески, то есть переписал практически весь код заново. Со временем путем экспериментов на собственной сети и благодаря постоянному обмену информацией с хакерами со всего мира Fyodor создал уникальный инструмент, позволяющий производить сканирование с помощью множества различных способов.

Пожалуй, решающее для популярности nmap значение сыграла статья "Искусство сканирования" (The art of scanning), которую Fyodor написал в 1997 году для известного андеграунд-журнала Phrack (www.phrack.org/show.php?p=51&a=11). К статье прилагался исходный код сканера на языке C, что дало возможность каждому технически подкованному специалисту опробовать новый инструмент в действии. К тому моменту nmap поддерживал девять методов сканирования, в числе которых были и достаточно изысканные.

Усовершенствования включали внедрение операционной системы дактилоскопии, дактилоскопического обслуживания, переписанный код (с языка C на C++), дополнительные виды сканирования, поддержка протокола (например, IPv6, протокол SCTP) и новые программы, которые дополняют основные функции сканирования. Изменения включали в себя:

 12 декабря 1998—Выпущена Nmap 2.00, включая операционную систему сканирования отпечатков пальцев

 11 апреля 1999—NmapFE, передняя часть GTK+, в комплекте с

Nmap
 7 декабря 2000—порт Windows
 28 августа 2002—переписка с языка C на C++ (язык программирования)
 16 сентября 2003—первый публичный выпуск, включающий обнаружение служебной версии
 31 августа 2004—ядро сканирования переписано для версии 3.70, новый движок называется ultra_scan
Лето 2005-Nmap выбран для участия в Google Summer of Code. Добавлены возможности Zenmap, который использует скриптовый движок (HCE), Netcat [9] , и операционная система 2-го поколения.
 13 декабря 2007—был выпущен Nmap 4.50, 10-летие издания. Включены Zenmap, операционная система 2-го поколения, и nmap, использующий скриптовый движок.
 30 марта 2009 года—аварийный релиз Nmap 4.85BETA5, использование Nmap Scripting Engine (NSE) для выявления вирусные инфекции
 16 2009—5 июля.00 в комплекте с netcat-замена и Ndiff сканирования сравнение инструментов.
 28 января 2011—5.50 включена генерация Netcat пакетов Nping
 21 мая 2012—6.00 выпущен с полной поддержкой IPv6.
 9 ноября 2015—Nmap 7.00
 20 декабря 2016—Nmap 7.
"Changelog" nmap фиксирует все изменения.
На мой взгляд, весьма важным и прогрессивным является так называемый Idle scan, предложенный хакером Antirez. Эта технология до сих пор используется редко даже хакерами, многие компании не предпринимают мер по предотвращению подобных атак, а производители сетевых средств просто игнорируют данную проблему (и это несмотря на то, что о ней известно с 1998 года, а разработчики технологии выпустили документ, подробно описывающий технику сканирования, возможные последствия атаки и даже меры, которые необходимо предпринять, чтобы защитить свою сеть).
Было бы естественно ожидать, что со временем проект nmap постепенно "затухнет". Это обычное явление для подобных проектов: со временем изменения выходят все реже, так как большая часть функций уже реализована создателями, а команда разработчиков переключается на другие проекты. Но nmap удалось избежать этой участи.
Во-первых, в 2000 году Fyodor создал web-серверwww.insecure.org, посвященный исследованию вопросов сетевой безопасности. Конечно, этот проект преследовал цель популяризации nmap: на сайте всегда можно найти новости, касающиеся программы, подробное описание методик сканирования для начинающих и самые новые версии программы для всех поддерживаемых платформ.

Подробнее: https://www.securitylab.ru/informer/240621.php
Однако все это - привычные атрибуты большинства современных web-серверов. Fyodor пошел намного дальше, создав сообщество хакеров, которых объединяла полезная программа и желание совершенствовать свои познания в области взаимодействия сетей. Во-первых, создание электронного списка рассылки (который впоследствии разделился на несколько, в соответствии с интересами участников) позволило ускорить развитие пакета nmap, ибо в число активных разработчиков вошло немало квалифицированных хакеров. Во-вторых, с течением времени Insecure.org стал местом, где специалисты стали обмениваться свежими идеями и результатами экспериментов. В общем, посещение этого web-узла вошло в привычку как у хакеров, так и у сотрудников подразделений информационной безопасности спецслужб.
А что же nmap? Пакет продолжил свое развитие в новом направлении. На этот раз Fyodor уделил внимание технологии активного распознавания операционной системы на удаленном узле по отпечатку TCP/IP. Это - достаточно интересная задача, поэтому в проект были вовлечены лучшие специалисты. Объединенные усилия дали поразительный результат: nmap смог определять с большой долей вероятности многие ОС как удаленных узлов, так и интеллектуальных сетевых устройств (маршрутизаторов, межсетевых экранов). Впоследствии программа пополнилась уникальным средством сбора неизвестных "отпечатков" ОС. Каждый пользователь nmap мог без лишних усилий пополнить общую базу знаний новыми данными, отправив их по Интернет. Благодаря этому техническому решению система стала очень быстро наполняться за счет данных, приходящих от тысяч хакеров, использующих в своей практике этот инструмент. Сейчас в базе свыше тысячи "отпечатков". При этом система опознает не только маршрутизаторы, но и такие "экзотические" сетевые устройства, как игровые консоли, телефоны, управленческие АТС, наладонные компьютеры и даже web-камеры. Fyodor тем временем выпустил новую статью - "Определение удаленной ОС с помощью отпечатка стека TCP/IP" (Remote OS detection via TCP/IP Stack FingerPrinting), которая была опубликована в 54-м выпуске журнала "Phrack"
(http://www.phrack.org/show.php?p=54&a=9) и вызвала новую волну интереса к nmap.

Новая история.

Теперь Fyodor'у пришлось не только развивать nmap или создавать сообщество хакеров, но и управлять их творческой энергией. Со временем необходимость применения nmap при настройке сети осознали многие системные администраторы. Логика проста: лучше самостоятельно узнать об уязвимостях своей сети и устранить их, чем восстанавливать инфраструктуру после вторжения извне. Так nmap

открыл себе путь во все ключевые дистрибутивы Linux. Он стал обязательным пакетом даже во многих "урезанных" дистрибутивных версиях, так как предоставлял множество полезных диагностических функций и мог с успехом заменить такие программы, как ping.
Настоящий триумф среди представителей компьютерного андеграунда ждал nmap летом 2003 года, когда на экраны кинотеатров вышел фильм The Matrix Reloaded. В нашумевшем блокбастере есть сцена реального взлома, когда Trinity использует nmap версии 2.54 Beta, чтобы найти уязвимый SSH-сервер, а затем взламывает его.
На протяжении первой половины 2003 года Fyodor выпускал лишь незначительные дополнения к своему пакету. Складывалось впечатление, что проект теряет динамику - ничего кардинально нового уже не появлялось. Однако в самом начале сентября автор программы распространил сообщение, в котором призывал сообщество пользователей загрузить новую версию nmap и широко тестировать новую возможность пакета - автоматическое определение версий сервисов удаленного узла. Это была настоящая революция! Из простого диагностического средства nmap вдруг превратился в инструмент подготовки сетевых атак.
Новая функциональность nmap пришлась по вкусу многим, ведь она избавляет от многих рутинных операций. Раньше хакеру для проведения атаки было нужно выполнить множество подготовительных операций, а уверенности в правильности сделанных шагов не было ни у кого. Сначала нужно было просканировать сеть, чтобы узнать, какие сервисы доступны на каждом узле. Затем желательно определить ОС и ее версию, чтобы сориентироваться, с какими уязвимостями он будет иметь дело. Наконец, необходимо выяснить, какая служба работает на каждом из активных портов (в последнее время системные администраторы в целях повышения безопасности стали запускать традиционные сервисы на непривычных портах). Только после этого хакер мог хотя бы приблизительно представить себе метод проникновения в систему. Теперь все шаги nmap выполняет автоматически (сканирование портов множеством методов, определение ОС и степень ее уязвимости), а сейчас еще и идентифицирует запущенные сервисы и даже их версии! В качестве бесплатного "бонуса" - способность nmap взаимодействовать с портами узлов по защищенным SSL-соединениям, так что даже шифрование канала уже не эффективно.
Учитывая то, что для сбора "отпечатков" служб используется уже опробованная методика электронной отсылки сообщений, можно признать, что база знаний nmap пополняется сегодня стремительно. Новые релизы появляются регулярно, и это дает возможность опознавать самые новые ОС и сетевые устройства. Для тех, кто

только начинает познавать азы сетевого взаимодействия, Fyodor выпустил документ, подробно описывающий ключевые особенности распознавания сервисов удаленного узла, а также как этими возможностями воспользоваться в конкретных ситуациях. Благодаря такой информационной поддержке nmap пользуется популярностью даже среди новичков.

Чего нет в nmap?

Казалось бы, nmap имеет шансы стать универсальным средством проникновения... Но не все так просто, и помимо этого пакета есть еще сотни не менее полезных программ, решающих другие задачи. Да и nmap нельзя считать абсолютно универсальным сетевым сканером. Чего нет в nmap, так это высокоуровневых средств сканирования в локальных сетях. Все возможности пакета основаны на свойствах стека TCP/IP. А ведь в корпоративных сетях есть еще немало протоколов, которыми можно воспользоваться для локализации ресурсов, - например, протокол NetBIOS. В то же время в TCP/IP есть свои средства взаимодействия на уровне Data link - к примеру, протокол ARP. Таким образом, если Fyodor когда-нибудь решит создать сетевой сканер для локальных сетей, у него будет широкое поле деятельности, так как существующие на сегодняшний день разработки разрознены, не обладают достаточной степенью унификации и не имеют такой технологической базы, какую заложили в nmap его создатели.

КАК РАБОТАЕТ NMAP?

В компьютерных сетях все подключенные устройства имеют свой ip адрес. Каждый компьютер поддерживает протокол ping, с помощью которого можно определить подключен ли он к сети. Мы просто отправляем ping запрос компьютеру, и если он отзывается, то считаем, что он подключен. Nmap использует немного иной подход. Компьютеры также определенным образом реагируют на те или иные сетевые пакеты, утилита просто отправляет нужные пакеты и смотрит какие хосты прислали ответ.

Но об этом вы, наверное, уже знаете. Более интересно то как Nmap узнает какие сервисы запущены на машине. Суть работы всех сетевых программ основана на портах. Чтобы получить сообщение из сети, программа должна открыть порт на вашем компьютере и ждать входящих соединений. А для отправки сообщения по сети нужно подключиться к уже другой программой (адресатом) порту. Затем программе необходимо будет открыть порт, на котором она будет ждать ответа.

Утилита nmap в процессе сканирования сети перебирает доступный диапазон портов и пытается подключиться к каждому из них. Если подключение удалось, в большинстве случаев, передав несколько пакетов программа может даже узнать версию программного обеспечения, которые ожидает подключений к этому порту. Теперь,

после того, как мы рассмотрели основы, рассмотрим как пользоваться nmap для сканирования портов и сети.

СИНТАКСИС NMAP

Команда запуска Nmap очень проста для этого достаточно передать ей в параметрах целевой IP адрес или сеть, а также указать опции при необходимости:

$ nmap опции адрес

Теперь давайте рассмотрим основные опции, которые понадобятся нам в этой статье.

 -sL — просто создать список работающих хостов, но не сканировать порты nmap;
 -sP — только проверять доступен ли хост с помощью ping;
 -PN — считать все хосты доступными, даже если они не отвечают на ping;
 -sS/sT/sA/sW/sM — TCP сканирование;
 -sU — UDP сканирование nmap;
 -sN/sF/sX — TCP NULL и FIN сканирование;
 -sC — запускать скрипт по умолчанию;
 -sI — ленивое Indle сканирование;
 -p — указать диапазон портов для проверки;
 -sV — детальное исследование портов для определения версий служб;
 -O — определять операционную систему;
 -T[0-5] — скорость сканирования, чем больше, тем быстрее;
 -D — маскировать сканирование с помощью фиктивных IP;
 -S — изменить свой IP адрес на указанный;
 -e — использовать определенный интерфейс;
 —spoof-mac — установить свой MAC адрес;
 -A — определение операционной системы с помощью скриптов.

Описание

Nmap использует множество различных методов сканирования, таких как UDP [10] , TCP (connect) [11] , TCP SYN (полуоткрытое), FTP-proxy (прорыв через ftp) [12] , Reverse-ident, ICMP [13] (ping) [14] , FIN [15] , ACK [16] ,
Xmas tree [17] , SYN- и NULL-сканирование [18] . Nmap также поддерживает
большой набор дополнительных возможностей, а именно: определение операционной системы удалѐнного хоста с использованием отпечатков стека [19] TCP/IP, «невидимое» сканирование, динамическое вычисление времени задержки и повтор передачи пакетов, параллельное сканирование, определение неактивных хостов методом параллельного ping-опроса, сканирование с использованием ложных хостов, определение наличия пакетных фильтров, прямое (без использования portmapper) RPC-

сканирование [20] , сканирование с использованием IP-фрагментации, а также произвольное указание IP-адресов и номеров портов сканируемых сетей. В последних версиях добавлена возможность написания произвольных сценариев (скриптов) на языке программирования Lua [21] . Существуют графические интерфейсы, упрощающие выполнение задач сканирования:
 Nmap Front End (Qt) [22] ;
 zenmap (GTK, Linux). [Источник 2]

Особенности Функции Nmap включают:

1. Обнаружение сети и узлов в сети. Например, перечисление узлов, которые отвечают на запросы TCP (Transmission Control Protocol) и/или ICMP (Internet Control Messaging Protocol) или имеют определенный открытый порт.
2. Сканирование портов, перечисление открытых портов на целевых узлах.
3. Обнаружение версий, опрос сетевых служб на удаленных устройствах для определения имени приложения и номера его версии.
4. Обнаружение ОС, определение операционной системы и аппаратных характеристик сетевых устройств.
5. Взаимодействие с целевой программой с помощью Nmap Scripting Engine (NSE) и языка программированияLua.
6. Nmap может предоставить дополнительную информацию о целевых объектах, включая обратные DNS-имена, типы устройств и MAC-адреса.

Типичные области применения:

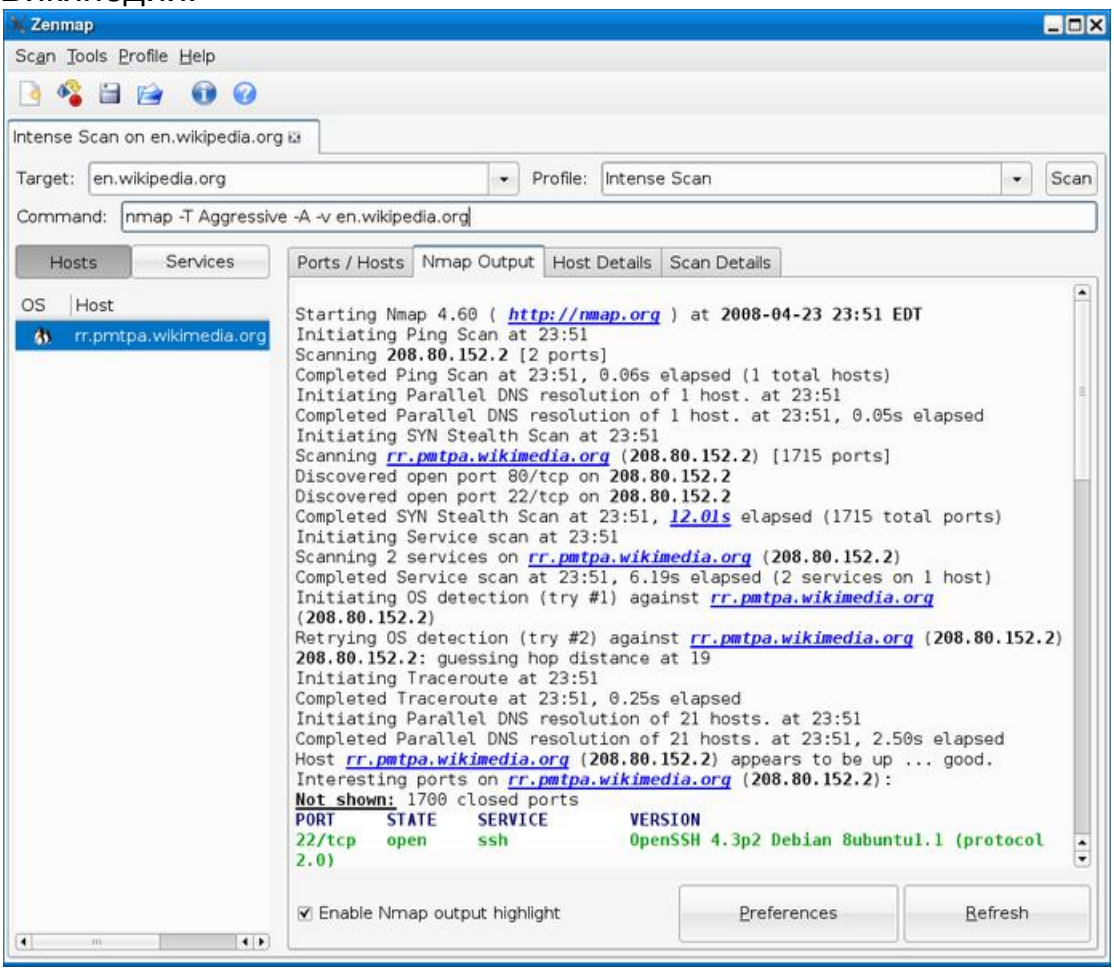
1. Аудит безопасности устройства или брандмауэра путем определения сетевых подключений, которые могут быть сделаны, или через него.
2. Определение открытых портов на целевом узле при подготовке к аудиту.
3. Инвентаризация сети, составление карты сети (картирование сети) [23] , обслуживание и управление активами.
4. Аудит безопасности сети путем выявления новых серверов.
5. Создание трафика для хостов в сети, анализ ответов и измерение времени отклика.
6. Поиск и использование уязвимостей в сети.

Графический интерфейс.

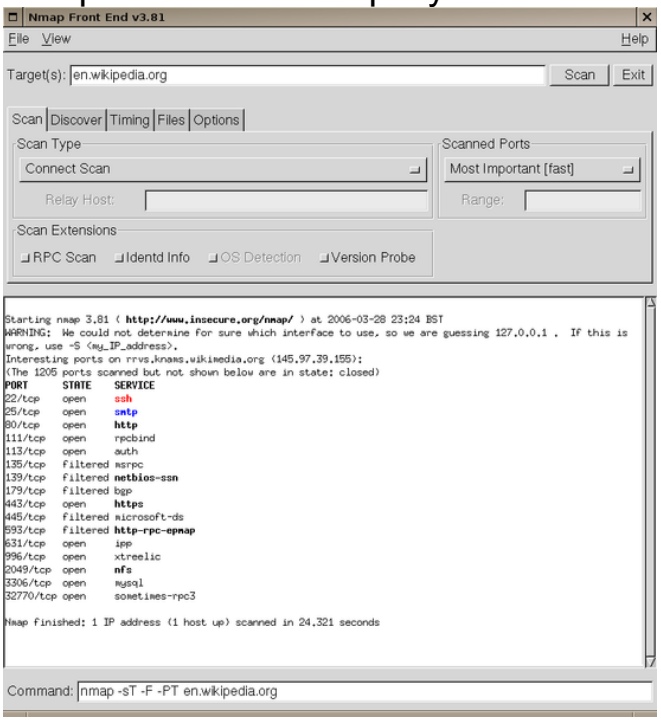
Программное обеспечение предоставляет ряд функций для проверки компьютерных сетей, включая обнаружение хостов и сервис обнаружения операционных систем. Эти функции расширяются скриптами, обеспечивающими более совершенное обнаружение службы, обнаружение уязвимостей, и другими функциями. Nmap может адаптироваться к условиям сети, включая задержки и перегрузки во время сканирования. Сообщество пользователей Nmap

продолжает разрабатывать и совершенствовать этот инструмент.

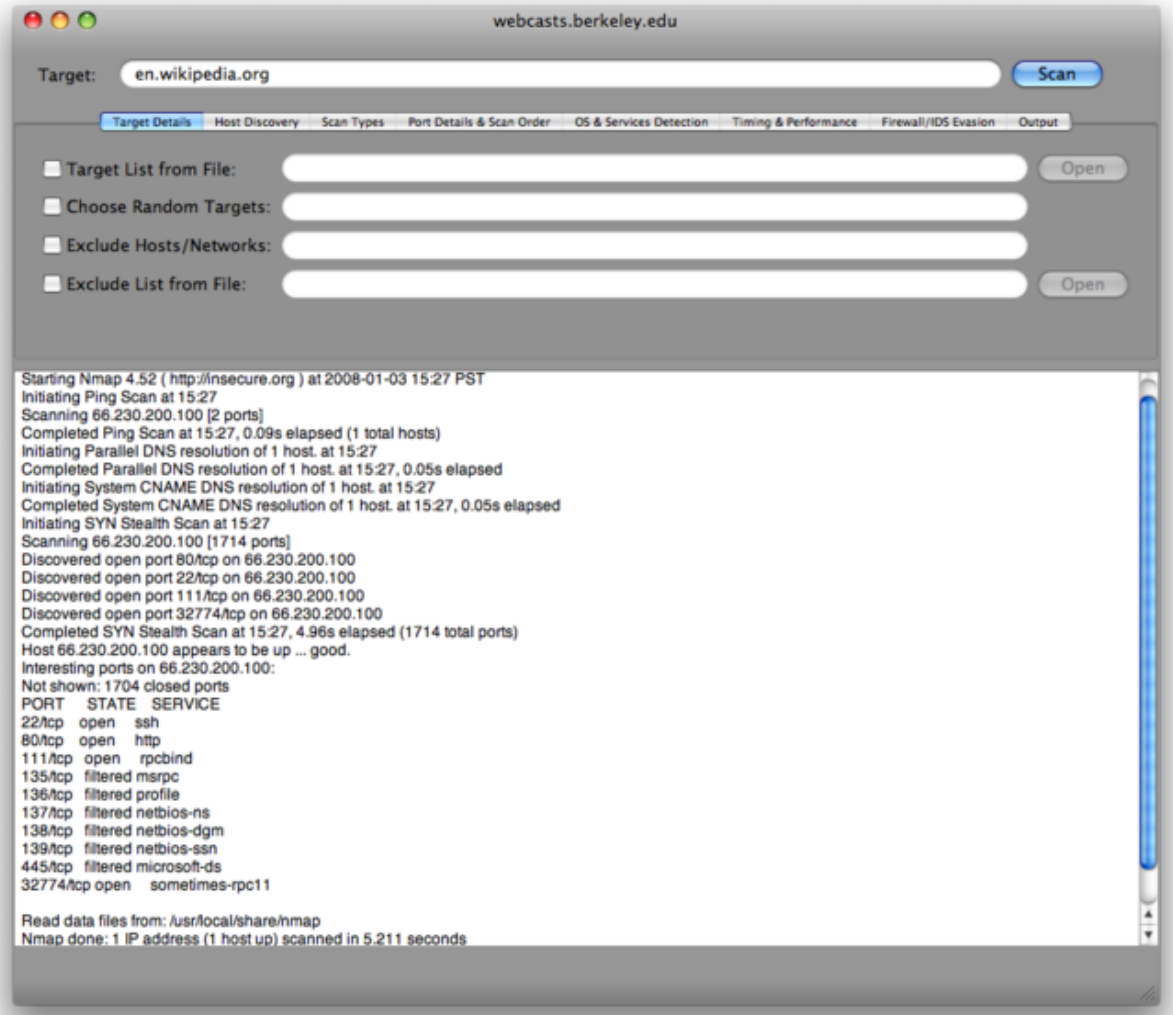
Zenmap показывает результаты сканирования портов для Википедии:



NmapFE показывает результаты сканирования портов для Wikipedia:



XNmap: Mac OS и GUI:



GUI Nmap — Zenmap

Также nmap имеет GUI [24] , который можно использовать для построения и выполнения команд, и это — Zenmap. Он позволит выбрать цель, запустить сканирование, отобразить результаты, а также сохранить их и сравнить с другими результатами. GUI Zenmap это хороший способ познакомиться с Nmap, но лучше знать как использовать Nmap в командной строке, если вы собираетесь работать с ним часто. [Источник 3]

Принцип работы

Как было отмечено ранее Nmap был разаработан для быстрого сканирования больших сетей, хотя прекрасно справляется и с единичными целями. Nmap использует сырые IP пакеты оригинальными способами, чтобы определить какие хосты доступны в сети, какие службы (название приложения и версию) они предлагают, какие операционные системы (и версии ОС) они используют, какие типы пакетных фильтров/брандмауэров используются и еще дюжины других характеристик. В тот время как Nmap обычно используется для проверки безопасности, многие сетевые и системные администраторы

находят ее полезной для обычных задач, таких как контролирование структуры сети, управление расписаниями запуска служб и учет времени работы хоста или службы.
Выходные данные Nmap это список просканированных целей с дополнительной информацией по каждой в зависимости от заданных опций. Ключевой информацией является «таблица важных портов». Эта таблица содержит номер порта, протокол, имя службы и состояние. Состояние может иметь значение open (открыт), filtered (фильтруется), closed (закрыт) или unfiltered (не фильтруется). Открыт означает, что приложение на целевой машине готово для установки соединения/принятия пакетов на этот порт. Фильтруется означает, что брандмауэр, сетевой фильт или какая-то другая помеха в сети блокирует порт, и Nmap не может установить открыт этот порт или закрыт. Закрытые порты не связаны ни с каким приложение, так что они могут быть открыты в любой момент. Порты расцениваются как не фильтрованные, когда они отвечают на запросы Nmap, но Nmap не может определить открыты они или закрыты. Nmap выдает комбинации «открыт/фильтруется» и «закрыт/фильтруется», когда не может определить, какое из этих двух состояний описывает порт. Эта таблица также может предоставлять детали о версии программного обеспечения, если это было запрошено. Когда осуществляется сканирование по IP протоколу (-sO), Nmap предоставляет информацию о поддерживаемых IP протоколах, а не об открытых портах. В дополнение к таблице важных портов Nmap может предоставлять дальнейшую информацию о целях: преобразованные DNS имена, предположение о используемой операционной системе, типы устройств и MAC адреса.
Немного о будущем
Было бы интересно заглянуть в будущее и узнать о дальнейшей судьбе проекта nmap.
Недавно Fyodor раскрыл свои планы относительно развития продукта. В первую очередь он отметил, что не хочет делать из nmap "универсального средства взлома". Поэтому продукт не будет развиваться по принципу поглощения все новых технологий. Из-за этого пришлось бы пожертвовать одним из ключевых архитектурных принципов Unix, согласно которому задачи решаются с помощью набора гибких, специализированных приложений.
Одной из важнейших задач Fyodor считает сейчас повышение производительности программы. По своему опыту могу сказать, что задействование одновременно нескольких полезных свойств программы заставляет ее "задумываться" на продолжительное время. Для ускорения работы Fyodor планирует переписать наиболее критичные участки кода nmap заново. Кроме того, предстоит много работы, связанной с наращиванием базы знаний nmap.
Что касается новых возможностей, то тут путь развития nmap

решается коллегиально - путем голосования на сайте всех заинтересованных участников проекта.
Кстати, сайт insecure.org также не прекратил своего развития. Со временем он стал одним из центров распространения технической информации о функционировании компьютерных сетей. С ростом популярности web-проекта росло и количество постоянных посетителей. Благодаря сформировавшемуся сообществу единомышленников группа разработки nmap смогла быстро решать возникающие технические проблемы. Со временем влиятельность сообщества Insecure.org должны были признать многие организации, профессионально занимающиеся защитой информации (например, проект MITRE).
Очередным этапом в развитии Insecure.org стало создание раздела списков рассылки, посвященных тематике информационной безопасности. Здесь можно найти информацию из самых авторитетных списков рассылки, посвященных компьютерной безопасности, - Bugtraq, Full Disclisure, Vuln Watch и другие. Впоследствии архив списков рассылки был перемещен на отдельный сервер -www.seclists.org, однако это по-прежнему составная часть проекта Insecure.org. Что касается самого Fyodor, то он помимо разработки nmap принимает активное участие в другом проекте, связанном с ИТ-безопасностью, - honeynet. Эта разработка позволяет защищать сети от хакерских атак, отвлекая внимание нарушителя на "более интересные" цели. Кроме того, honeynet позволяет наблюдать хакерскую технику взлома сетей "в реальном времени".
Fyodor Yarochkin помимо работы над программами много путешествует, выступая с докладами на тематических конференциях. Одно из таких мероприятий проходило в феврале в Германии. А сейчас Fyodor работает над книгой, которая будет посвящена nmap и методикам исследования сетей с помощью необычных сетевых пакетов.

Немного о практических задачах.

Nmap (Network Mapper) — свободная утилита с открытым исходным кодом, предназначенная для сканирования сетей и аудита сетевой безопасности. Nmap использует множество различных методов сканирования (UDP, TCP, TCP SYN, FTP, ICMP и т.д.), а также поддерживает большой набор дополнительных возможностей.

Ниже описаны некоторые полезные возможности этой замечательной утилиты.

Для выполнения большинства операций nmap требуются полномочия пользователя root. При запуске nmap от имени обычного пользователя значительная часть функций будет не доступна.

1. Получение информации об удаленном хосте и определение операционной системы

Nmap используются в следующем виде:

```
$ sudo nmap -sS -P0 -sV -O <target>
```

где:

- < target > — IP, хост или подсеть
- **-sS** — TCP SYN сканирование (полуоткрытое)
- **-P0** — отключение ICMP сканирования.
- **-sV** — определение закрытых и фильтруемых портов
- **-O** — определение версии операционной системы
  Еще опции:

- **-A** — включает определение «отпечатка» и версии операционной системы
- **-v|-vv** — уровень вывода диагностических сообщений
  Используя дополнительные опции, команда выглядит следующим образом:

```
$ sudo nmap -sS -P0 -A -v < target >
```

2. Определение списка серверов с открытым портом

Nmap используются в следующем виде:

```
$ sudo nmap -sT -p 22 -oG - 192.168.1.* | grep open
```

Номер порта указывается после опции «-p». В данном примере, выполняется поиск машин, для которых возможен вход по ssh (если, конечно, не изменен порт по умолчанию для ssh).

3. Поиск активных IP адресов в сети

Nmap используются в следующем виде:

```
$ sudo nmap -sP 192.168.0.*
```

Чтобы опросить конкретную подсеть, можно использовать следующие параметры:

```
$ sudo nmap -sP 192.168.0.0/24
```

4. Опросить (пропинговать) диапазон адресов

Nmap используются в следующем виде:

```
$ sudo nmap -sP 192.168.1.100-254
```

Nmap понимает много натаций IP адресов.

5. Поиск неиспользуемых IP адресов в подсети

Nmap используются в следующем виде:

```
$ sudo nmap -T4 -sP 192.168.2.0/24 && egrep "00:00:00:00:00:00" /proc/net/arp
```

6. Поиск вируса Conficker в подсети

Nmap используются в следующем виде:

```
$ sudo nmap -PN -T4 -p139,445 -n -v \
    -script=smb-check-vulns \
    -script-args \
    safe=1 192.168.0.1-254
```

Чтобы скорректировать список IP адресов, заменить «192.168.0.1-256» на свой вариант.

7. Поиск в сети мошеннических точек доступа (AP)

Nmap используются в следующем виде:

```
$ sudo nmap -A -p1-85,113,443,8080-8100 \
```

```
-T4 -min-hostgroup 50 \
-max-rtt-timeout 2000 \
-initial-rtt-timeout 300 \
-max-retries 3 \
-host-timeout 20m \
-max-scan-delay 1000 \
-oA wapscan 10.0.0.0/8
```

8. Декорирование истинного IP адреса при сканировании сети

Nmap используются в следующем виде:

```
$ sudo nmap -sS 192.168.0.10 -D 192.168.0.2
```

В данном примере выполняется поиск открытых портов на машине 192.168.0.10, в качестве адреса, откуда ведется сканирование указывается адрес 192.168.0.2. Таким образом, в логах машины 192.168.0.10 будет отображен не истинный IP адрес, с которой ведется сканирование, а указанный — 192.168.0.2.

9. Список обратных DNS записей для подсети

Nmap используются в следующем виде:

```
$ sudo nmap -R -sL 209.85.229.99/27 | \
    awk '{if($3=="not")print"(" $2 ") no PTR";else print $3 " is "$2}' | \
    grep `(`
```

В этом примере, nmap выполняет поиск обратных DNS записей для подсети. Результатом поиска будет список IP адресов с соответствующими PTR записями для подсети. Чтобы выполнить запрос через конкретный DNS сервер, необходимо добавить «-dns-servers x.x.x.x» после опции «-sL».

10. Подсчет Linux/Windows машин в сети

Nmap используются в следующем виде:

```
$ sudo nmap -F -O 192.168.0.1-255 | \
    grep "Running: " > /tmp/os; \
    echo "$(cat /tmp/os | grep Linux | wc -l) Linux device(s)"; \
  echo "$(cat /tmp/os | grep Windows | wc -l) Window(s) devices"
```