Nmap ("Network Mapper") – это кросплатформенна утилита с открытым исходным кодом для **исследования различных сегментов сети и проверки ее безопасности**. Была она разработана товарищем Fyodor-ом (настоящее имя которого Gordon Lyon - http://insecure.org/fyodor/), а стала развиваться благодаря поддержке огромного количества поклонников этой незаменимой для администраторов вещи. Предназначается она для **быстрого сканирования локально-вычислительных сетей различного уровня**, отдельных локальных и удаленных хостов, определения состояния объектов сканируемой сети (портов и состояния соответствующих им служб). Первое упоминание этой великолепной программы относится к 8 февраля 1999 года. Программа была изначально реализована для **UNIX** систем, но постепенно появились ее реализации и для множества других операционных систем, таких как Microsoft Windows, Linux, Mac OS X и многих других.

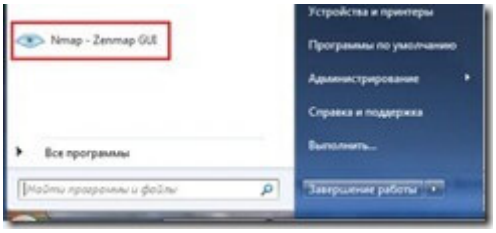
На момент написания данной статьи стала доступной версия Nmap 6.01 Released, о чем и было сообщено в вечерней рассылке. **Скачать** последнюю версия **сканера Nmap** можно указав в адресе браузера следующую ссылку: *http://nmap.org/download*.

Скачиваем увесистый файлик (25 Мб) и **запускаем на установку**. Вместе с собсвенно nmap-ом, который является обычным консольным сканером устанавливается и ряд дополнительных компонентов. Такие как **WinPcap и Zenmap**

WinPcap - это **библиотека для приложений в среде Microsoft Windows, позволяющая захватывать и передавать сетевые пакеты**, поступающие на сетевую карту компьютера, в обход стека протоколов. Благодаря широкому набору функций, WinPcap является средством для захвата и фильтрации пакетов, на котором основываются многие коммерческие, а также бесплатные **сетевые инструменты,**

включая анализаторы протоколов, сетевые мониторы, системы обнаружения сетевого вторжения, генераторы трафика, утилиты тестирования сети и другие подобные программы.

После установки в **Пуск**е появится следующий значок.



Запускаем программу.

Для пользователей **Windows** будет приятен тот факт, что сборка будет иметь графический интерфейс которым разработчики снабдили свое детище. Он как раз и называется оболочкой **Zenmap GUI** и выглядит следующим образом.

В следующем окне стоит обратить внимание на профиль сканирование.

В выпадающем списке “Профиль” нужно выбрать подходящий профиль сканирования из предложенных. Сразу стоит предупредить, что сканирование с использованием «**Intense scan**» может привести к зависанию некоторого сетевого оборудования такого как свитчи или маршрутизаторы. В случае возникновения такого печально события необходимо произвести **сброс через кнопку “reset”**, а при ее отсутствии – отключить питание устройства на несколько секунд.

Кроме того желающим проводить подобное сканирование из дома, через своего провайдера, могут запросто отрубить интернет или он сам отключится.

Итак продолжим. **Сканер Nmap** в семействе Windows поддерживает все использующиеся версии, основанные на платформе Windows NT: Windows 2000, Windows XP, Windows Vista, Windows 7, а также **Windows Server 2003/2003 R2 и Windows Server 2008/2008 R2**.

Что касается сканирования, то может быть получен следующий результат.

Немного теории…

Nmap использует множество различных методов сканирования, а именно UDP, TCP (connect), TCP SYN, FTP-proxy, Reverse-ident, ICMP (ping), FIN, ACK, Xmas tree, SYN- и NULL-сканирование. Утилита поддерживает также большой набор дополнительных возможностей таких как: определение операционной системы удалённого хоста с использованием отпечатков стека 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 RPC-сканирование, сканирование с использованием IP-фрагментации, а также произвольное указание IP-адресов и номеров портов сканируемых сетей.

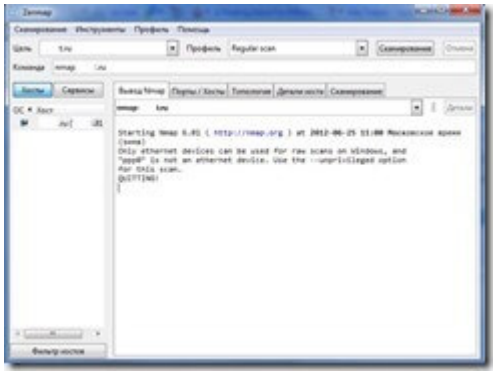
Результатом работы сетевого сканера Nmap является список сканированных портов удаленного хоста или группы хостов с указанием номера порта и его состояния, типа используемого протокола, названия службы, закрепленной за этим портом и другой информации.

Сетевой сканер Nmap обычно используется не только для проверки безопасности удаленных сегментов сети, но во много сетевые и системные администраторы

используют ее и для обычных задач, таких как контролирование структуры и функционирования сети, проверки корректного ответа сетевых служб и доступности различны сетевых устройств, как рабочих станций, так и серверов и другого сетевого оборудования..

Решение проблемы в работе сканера Nmap на Windows 7.

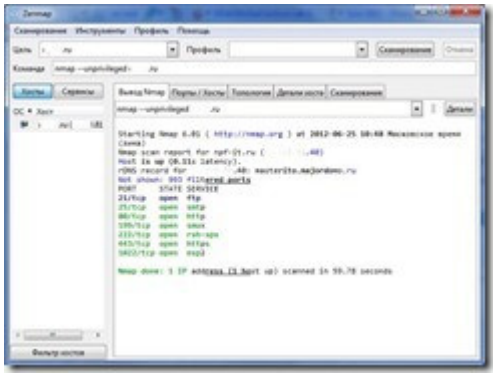
При запуске сканирования хостов из операционной системы Windows 7 возможно появления окна с ошибкой. Пример одной из таких ошибок показан ниже.



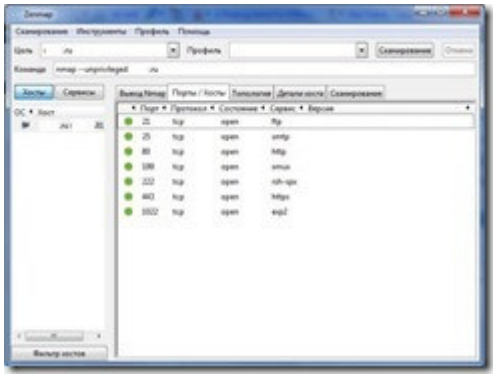
Возникновение подобного рода проблем связано с тем, что утилита, как правило, не работает напрямую через некоторые сетевые подключения (соединения) к сети интернет, такие как VPN, PPPoE или P2PT.

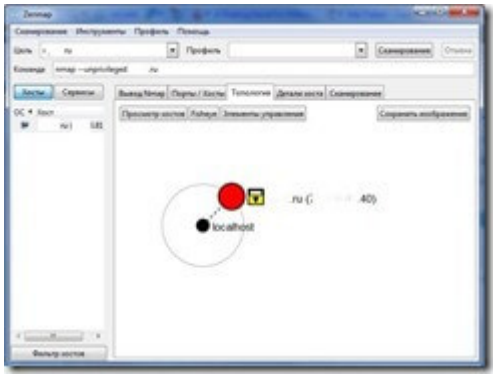
Вместе с тем существует как минимум 2 пути решения данной проблемы:

1. Прочитать внимательно сообщение об ошибке в окне вывода Nmap. он рекомендует использовать параметр *“--unprivileged”* в строке команды, что мы и делаем. Результат выполнения сканирования удаленного хоста с использование этой команды показан ниже.



Обратите внимание что другие ключи для команды сканирования не используются. Но этого вполне достаточно чтобы получить нужный результат.





2. Другой вариант решения возникшей проблемы – это установка между компьютером и кабелем провайдера **роутера (маршрутизатора, кто как его называет)**, чтобы утилита видела физический интерфейс ethernet, а не обращалась через виртуальное подключение. Я обычно для этого использую оборудование фирмы D-link, исключительно из соображения низкой цены. Вы можете рассмотреть такие изделия как **DI-804HV** или **DIR-120**.

На этом пока можно закончить.

И в завершении данного очень краткого обзора хочется сказать, что **сетевой сканер безопасности NMAP** является абсолютно бесплатным и имеет большое количество плагинов (http://sectools.org) на которые я бы советовал обратить особое внимание. Кстати русскую документацию, правда по консольной версии сканера, можно почитать здесь: http://nmap.org/man/ru/.

Так что скачивайте, изучайте и экспериментируйте!