СӘТБАЕВ УНИВЕРСИТЕТІ SATBAYEV UNIVERSITY

Дисциплина «Этичный хакинг и противодействие взлому»

Лекция 3

Сканирование сети

Преподаватель: **Батыргалиев Асхат Болатканович, PhD, ассоц.проф. кафедры «Кибербезопасность, обработка и хранение информации»**

askhat.b.b@gmail.com

Содержание

1. Обзор возможностей сканирования сети
2. Варианты сканирования сети
3. Сканирование IP-адресов
4. Сканирование портов
5. Инструменты сканирования сети

По завершению урока Вы будете знать:

1. Возможности сканирования сети
2. Варианты сканирования сети
3. Возможности сканирования IP-адресов
4. Возможности сканирование портов
5. Инструменты сканирования сети

Обзор возможностей сканирования сети

Сканирование является основным способом сбора данных в сети и позволяет без знания топологии собрать актуальные данные, а также произвести поиск сервисов, работающий на хостах. Оно базируется на знании особенностей поведения хостов и протоколов при нарушении стандартных алгоритмов взаимодействия.

Каждый протокол, который может использоваться для передачи информации, хранит данные в двух частях. Первая - заголовок, на основании которого работают служебные алгоритмы протокола. Здесь могут быть перечислены настройки соединения, описаны основные правила для обработки и передачи информации. Вторач часть – данные.

Самый распространенный протокол, который позволяет производить сканирование и может быть обнаружен практически во всех современных сетях, это протокол TCP. Протокол является одним из основополагающих протоколов самой популярной модели TCP/IP. Протокол позволяет настраивать соединение и контролировать соединение на протяжении всего взаимодействия. Именно данный механизм контроля состояния соединения используется большинством способов сканирования.

Варианты сканирования сети

На сегодняшний день известны следующие варианты сканирования с помощью TCP протокола в порядке убывания эффективности:

- **Connect Scan** - обычный алгоритм настройки соединения, реализуется сетевыми функциями операционной системы;
- **SYN Scan** - сканирование, которое основано на отправке пакетов, содержащих только один установленный флаг контроля соединения - SYN;
- **ACK Scan** - сканирование, которое основано на отправке пакетов, содержащих только один установленный флаг контроля соединения - ACK;
- **Maimon** - сканирование, которое основано на отправке пакетов, содержащих несколько установленных флагов контроля соединения - FIN/ACK;
- **Null scan** - сканирование, которое основано на отправке пакетов не содержащих ни одного флага, который отвечает за контроль соединения;
- **FIN scan** - сканирование, которое основано на отправке пакетов, содержащих только один установленный флаг контроля соединения - FIN;
- **Xmas Scan** - сканирование, которое основано на отправке пакетов, содержащих на каждый запрос разные флаги из всех доступных для контроля соединения.

Сканирование IP-адресов

Если говорить о механизмах, которые используются в утилитах сканирования IP-адресов, то, как правило, речь идет о рассылке широковещательных пакетов ICMP. Утилиты отправляют пакеты типа ICMP ECHO по указанному IP-адресу и ожидают ответного пакета ICMP ECHO_REPLY. Получение такого пакета означает, что в данный момент компьютер подключен к сети по указанному IP-адресу.

Рассматривая возможности протокола ICMP для сбора информации о сети, следует отметить, что прослушивание при помощи утилиты ping и ей подобных - это всего лишь верхушка айсберга. Обмениваясь ICMP-пакетами с каким-либо узлом сети, можно получить куда более ценную информацию о сети, нежели констатация факта подключения узла к сети по заданному IP-адресу.

Для защиты от такого рода сканирования блокируются ответы на ICMP-запросы. Именно такой подход зачастую используется системными администраторами, которые заботятся о безопасности своих сетей. Однако, несмотря на блокировку пакетов ICMP, существуют и другие методы, позволяющие определить, подключен ли данный узел к сети.

В тех случаях, когда обмен данными по протоколу ICMP заблокирован, используется метод сканирования портов (port scanning). Просканировав стандартные порты каждого потенциального IP-адреса сети, можно определить, какие узлы подключены к сети. Если порт открыт (opened port) или находится в режиме ожидания (listening mode), это значит, что по данному IP-адресу имеется компьютер, подключенный к сети.

Прослушивание сети методом сканирования портов относится к разряду так называемого TCP-прослушивания.

Сканирование портов

Механизм сканирования портов основан на попытке пробного подключения к портам TCP и UDP исследуемого компьютера с целью определения запущенных служб и соответствующих им портов. Обслуживаемые порты могут находиться в открытом состоянии или в режиме ожидания запроса. Определение портов, находящихся в режиме ожидания, позволяет выяснить тип используемой операционной системы, а также запущенные на компьютере приложения.

Существует сравнительно много способов сканирования портов, для систем Windows наиболее часто встречаются следующие:

TCP-сканирование подключением (TCP connect scan);

TCP-сканирование с помощью сообщений SYN (TCP SYN scan);

TCP нуль-сканирование (TCP Null scan);

TCP-сканирование с помощью сообщений ACK (TCP ACK scan);

UDP-сканирование (UDP scan).

Метод TCP-сканирования подключением (TCP connect scan) заключается в попытке подключения по протоколу TCP к нужному порту с прохождением полной процедуры согласования параметров соединения (процедура handshake), заключающейся в обмене служебными сообщениями (SYN, SYN/ACK, ACK) между узлами сети.

Сканирование портов

В методе TCP-сканирования с помощью сообщений SYN (TCP SYN scan) полного подключения к порту не происходит. Исследуемому порту посылается сообщение SYN, и если в ответ приходит сообщение SYN/ACK, то это означает, что порт находится в режиме прослушивания. Данный метод сканирования портов является более скрытым в сравнении с методом сканирования с полным подключением.

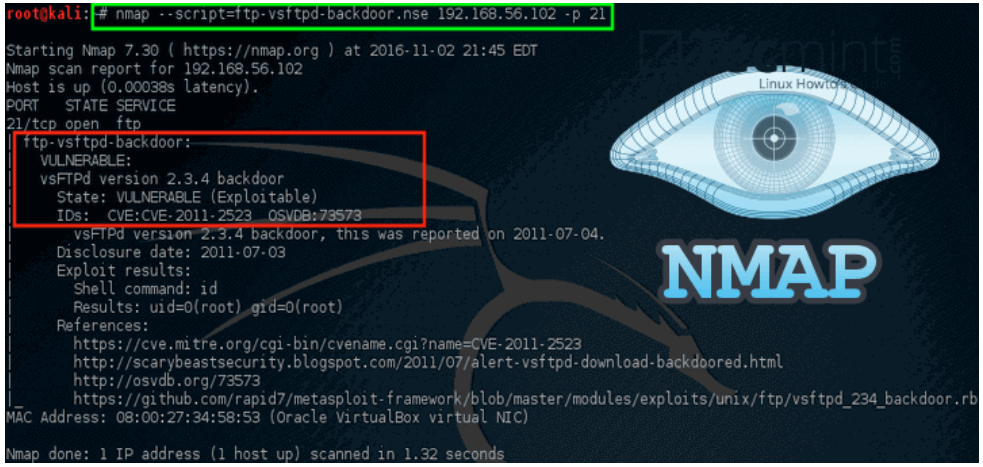
В методе TCP-нуль-сканирования (TCP Null scan) осуществляется отправка пакетов с отключенными флагами. Исследуемый узел в ответ должен отправить сообщение RST для всех закрытых портов.

Метод TCP-сканирования с помощью сообщений ACK (TCP ACK scan) позволяет установить набор правил, используемых брандмауэром, и выяснить, выполняет ли брандмауэр расширенную фильтрацию пакетов.

Метод UDP-сканирования заключается в отправке пакетов по протоколу UDP. Если в ответ поступает сообщение, что порт недоступен, то это значит, что порт закрыт. При отсутствии такого ответа можно предположить, что порт открыт. Стоит отметить, что протокол UDP не гарантирует доставки сообщений, поэтому данный метод сканирования не очень надежен. Кроме того, UDP-сканирование - процесс очень медленный, в связи с чем к такого рода сканированию прибегают крайне редко.

Инструменты сканирования сети

Nmap уже долгое время считается надёжным инструментом информационной безопасности, он используется инженерами и сотрудниками служб безопасности. Это кроссплатформенная утилита, имеющая широкий спектр функцию, не ограничивающихся простым сканированием сетей.

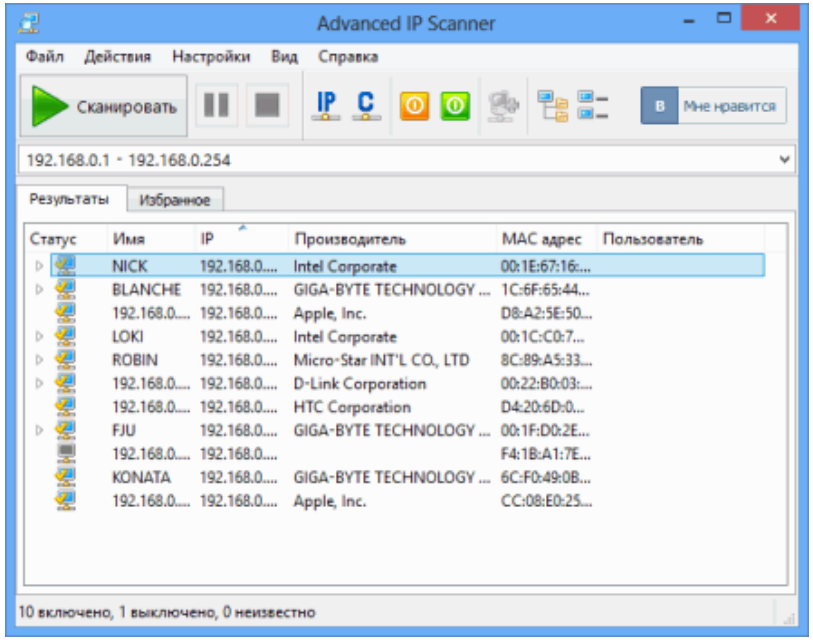


Она содержит утилиты сканирования сетей, используемые для исследования сетей, и предоставляет множество утилит для аудита безопасности. Она позволяет выполнять глубокое изучение IP-пакетов, в том числе содержащих информацию о сервисах, приложениях, идентификации ОС и других характеристиках удалённого хоста. В ней есть опции «интересных портов», помогающие быстро находить порты удалённых хостов, которые часто бывают открытыми.

Инструменты сканирования сети

Advanced IP Scanner. Этот инструмент обеспечивает возможность быстрого сканирования сетей. Advanced IP Scanner - бесплатная утилита, которая быстро скачивается. Мощная и одновременно простая в использовании программа для сканирования локальных сетей и удаленных веб-серверов с целью обнаружения доступных для подключения к ним сетевых протоколов. Также утилита предлагает функции для удаленного управления компьютером.

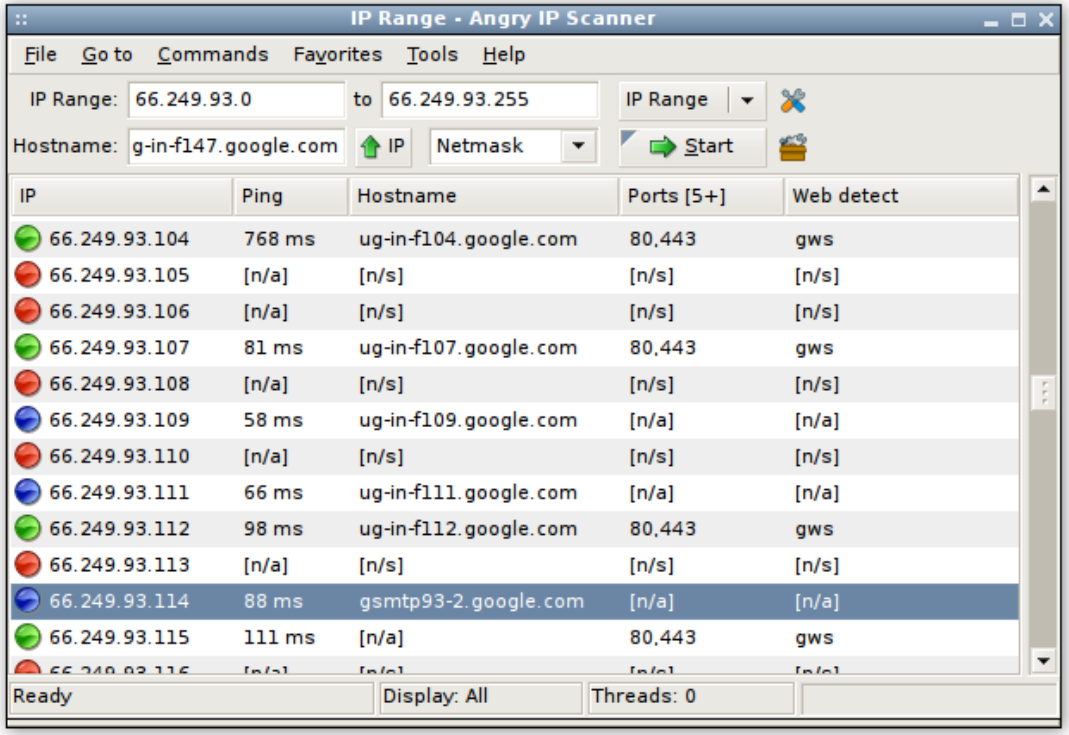
Этот инструмент, совместимый только с Windows, предоставляет множество базовых функций сканирования, в том числе определение имён устройств, IP-адресов и MAC-адресов при помощи OUI lookups для распознавания производителей устройств. Результаты работы утилиты можно экспортировать в файл CSV для дальнейшего исследования устройств в других инструментах и документации. Также она может взаимодействовать с функциональностью Wake-On-LAN найденных удалённых хостов и позволяет удобно обмениваться данными с устройствами, с поддержкой RDP.



Инструменты сканирования сети

Angry IP Scanner – кроссплатформенный сканер, поддерживает Windows, Mac и Linux. Angry IP Scanner сканирует сетевые порты и IP-адреса.

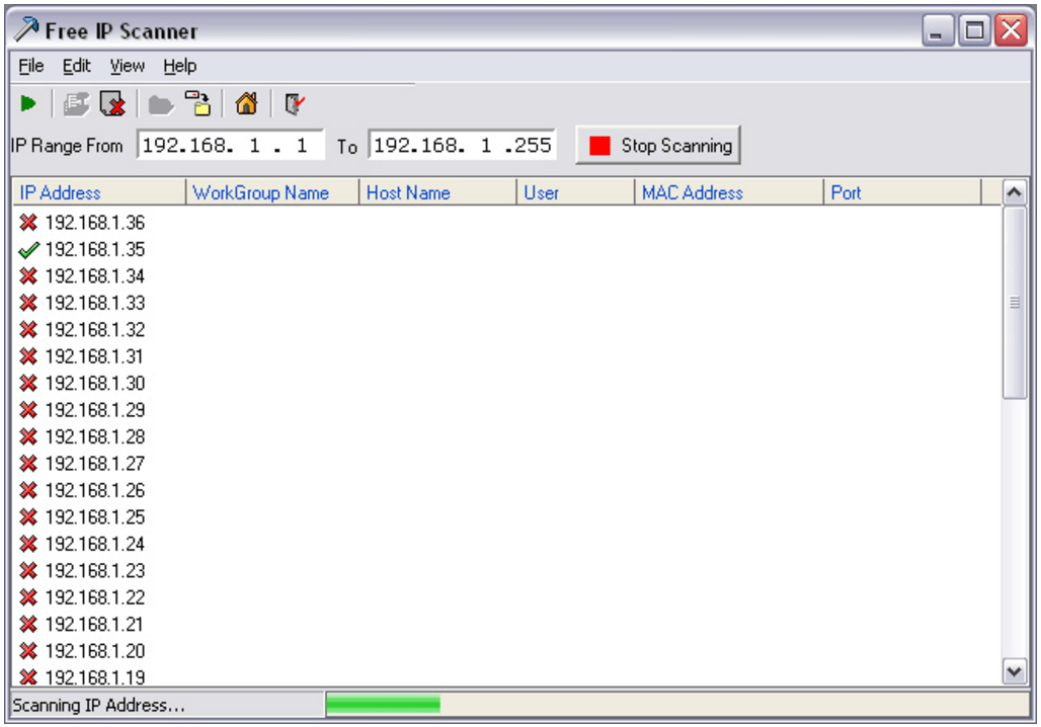
Он пингует адреса и резолвит имена хостов из DNS. Также он определяет MAC-адреса устройств для OUI lookup, а его возможности можно легко расширить при помощи опенсорсных плагинов, написанных на Java. Он имеет множество других функций, например, получение имени NetBIOS, рабочей группы, подключенных пользователей Windows, определение веб-серверов и многое другое. Инструмент позволяет экспортировать результаты в CSV, TXT, XML или в файлы списков IP-портов.



Инструменты сканирования сети

Free IP scanner - это простая утилита IP-сканирования, имеющая множество отличных функций. Это быстрый сканер, для обеспечения производительности использующий технологию многопоточности. Пользователь может настраивать уровни приоритетов процесса сканирования и максимальное количество потоков. Разработчик утверждает, что инструмент может сканировать сотни компьютеров в секунду.

Для поиска находящихся онлайн-хостов он использует пинг. Опционально он может резолвить имена хостов, находить открытые порты и использовать другие функции в случае нахождения онлайн-хостов. Как и другие сканеры, он может получать информацию NetBIOS, в том числе имя хоста, рабочую группу, подключенного пользователя и MAC-адрес. Результаты сканирования можно сохранять в простой текстовый файл.



Инструменты сканирования сети

Встроенная командная строка и PowerShell. Также для нахождения хостов в сети можно использовать встроенные командные среды, в том числе командную строку и PowerShell. Например, можно выполнить простую однострочную команду для быстрого пинга и возврата всех онлайн-хостов в конкретной подсети:

```
for /l %i in (1,1,255) do @ping 10.1.149.%i -w 1 -n 1|find /i "ttl=«
```

Кроме того, компания Microsoft предоставляет множество превосходных бесплатных примеров кода для различных ping-утилит, встроенных в галерею PowerShell.

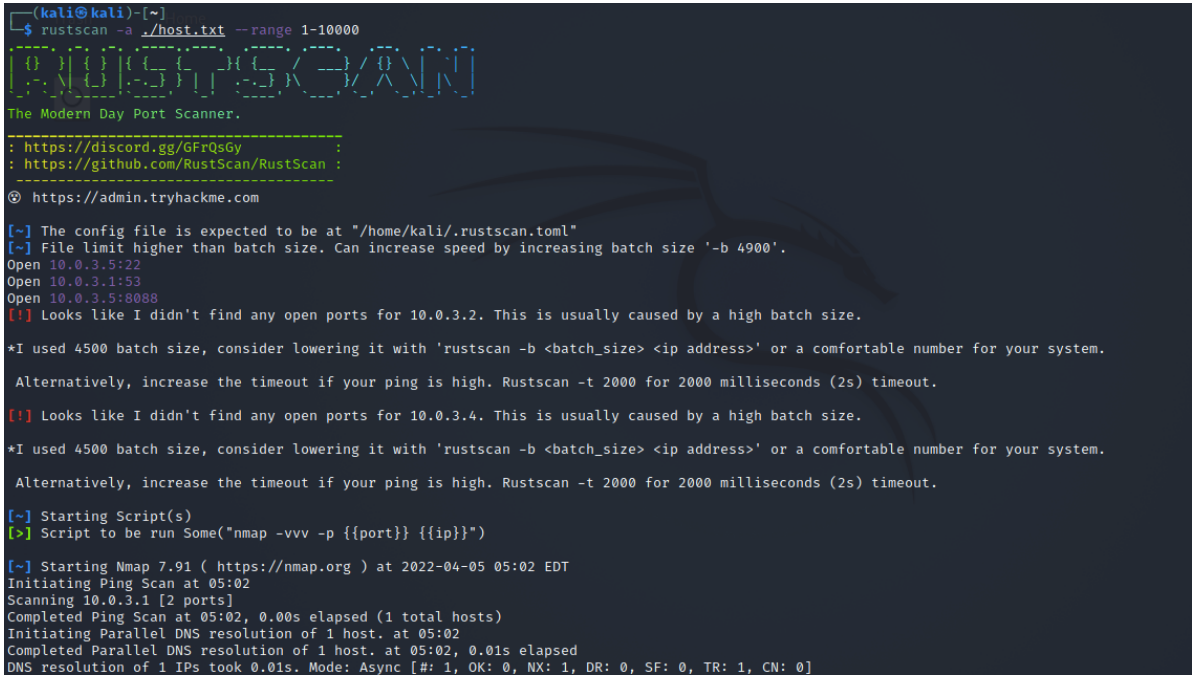
```
PS C:\Users\devadmin> ping-addressrange

cmdlet Ping-AddressRange at command pipeline position 1
Supply values for the following parameters:
NetIP: 10.1.149.1-10
interface: Ethernet0

Name                           Value
----                           -----
Localhost
Num_alive_host                 9
Host_scanned                   9
Host_alive                     {10.1.149.5, 10.1.149.4, 10.1.149.7, 10.1.149.6…}

PS C:\Users\devadmin>
```

Инструменты сканирования сети

rustscan. Сканер написанный на языке программирования Rust, сканер - обертка над nmap. Возможности: сканирование всех портов за 3 секунды; поддержка движка для автоматизации процесса сканирования, возможность перенапрявлять результаты в Nmap; адаптивное обучение для улучшения процесса сканирования; раба с адресами введенными в различных форматах IPv6, CIDR и т.д.

Недостатки ограничение пулами и CIDR сканировать с помощью этого инструмента не получится.

Сканер можно установить различными способами, как готовый пакет или как Docker image.



Инструменты сканирования сети

masscan. Сканер, который можно использовать для очень большого количества хостов и просканировать чуть ли не весь интернет за считанные минуты. Возможно, это в первую очередь из-за собственного сетевого стека, который в обход стека операционной системы самостоятельно отправляет запросы в сеть и занимается его обработкой.

```
┌──(kali㉿kali)-[~/mass/masscan-1.3.0]
└─$ sudo masscan -p1-1024 10.0.3.0/24 --rate=1000

Starting masscan 1.3.0 (http://bit.ly/14GZzcT) at 2022-04-05 10:06:22 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 256 hosts [1024 ports/host]
Rate:  0.98-kpps,  9.15% done,   0:03:59 remaining, found=0
```

Naabu. Сканер, написанный на языке программирования Go. Упрощает процесс сканирования и по сути использует только один тип сканирования - SYN Scan.

```
┌──(kali㉿kali)-[~/go/bin]
└─$ sudo ./naabu -host 10.0.3.5

                 __
 ___  ___  ___  / /  __ __
/ _ \/ _ \/ _ \/ _ \/ // /
/_//_/\_,_/\_,_/_.__/\_,_/ v2.0.6

                projectdiscovery.io

Use with caution. You are responsible for your actions
Developers assume no liability and are not responsible for any misuse or damage.
[INF] Running SYN scan with CAP_NET_RAW privileges
[INF] Found 2 ports on host 10.0.3.5 (10.0.3.5)
10.0.3.5:22
10.0.3.5:49153
```

Инструменты сканирования сети

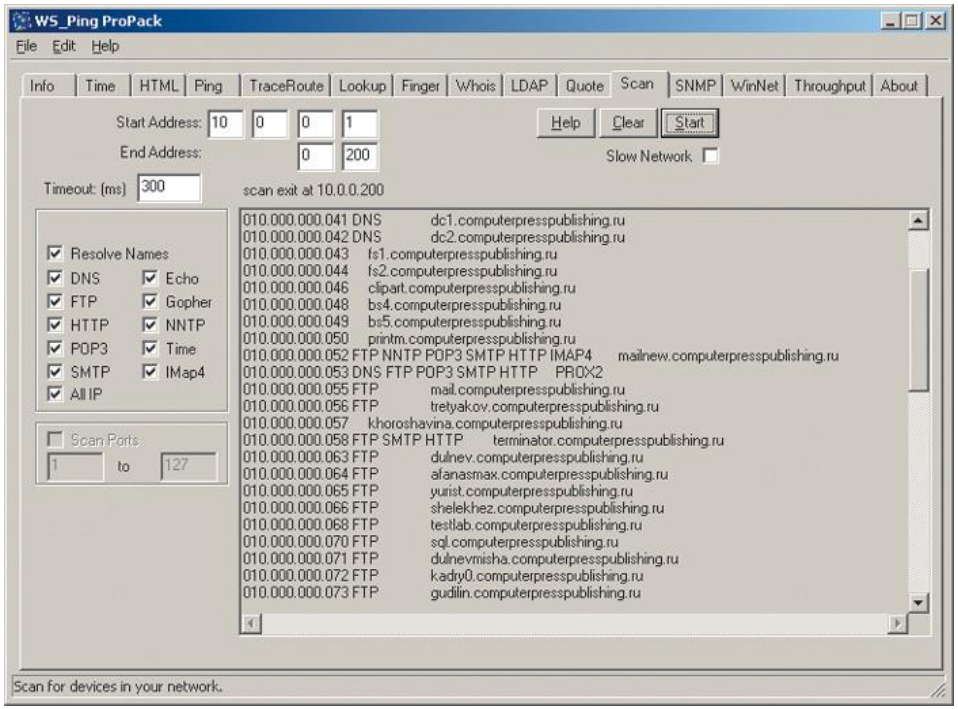
Сканер **WS PingPro** позволяет определить список всех IP-адресов, по которым имеются подключенные к сети узлы, а также выяснить их сетевые имена. Кроме того, сканер WS PingPro определяет запущенные на компьютере службы и дает возможность просканировать порты сетевого компьютера в заданном диапазоне (в демо-версии программы данная возможность заблокирована). Для настройки на различные по производительности сети сканер WS PingPro позволяет задавать время, в течение которого ожидается ответ от хоста сети (по умолчанию - 300 мс). В дополнение к сетевому сканеру пакет WS PingPro предоставляет в распоряжение пользователя такие утилиты, как SNMP tool, WinNet, Time tool, Throughput, Info tool, и др.

Утилита SNMP tool позволяет получить информацию о сетевом узле (как правило, речь идет о коммутаторах и маршрутизаторах), поддерживающем протокол SNMP.

Утилита WinNet позволяет просканировать локальную сеть и отобразить NetBEUI-имена всех узлов сети, доменов и разделяемых ресурсов.

Утилита Time tool синхронизирует время локального компьютера с временем ближайшего сервера времени.

Throughput - диагностическая утилита, позволяющая протестировать скорость соединения пользователя с удаленным узлом сети.



Инструменты сканирования сети

Advanced LAN Scanner - утилита, позволяющая сканировать IP-адреса. В сравнении с Advanced IP Scanner данная утилита представляет собой сочетание IP-сканера и сканера портов и позволяет не только определять IP-адреса, но и собирать подробную информацию о сетевых именах компьютеров, об установленной на них операционной системе, об открытых портах, о принадлежности пользователя к той или иной группе, о пользователях, которые имеют санкционированный доступ к компьютеру, и массу другой информации.

Кроме того, данный сканер имеет широкие возможности настройки и позволяет задавать количество одновременно выполняемых потоков, диапазон сканируемых портов, а также управлять временем ожидания ответа на запрос. В заключение отметим, что данный сканер позволяет подключаться к выбранному узлу либо используя текущую учетную запись пользователя, либо задавая имя пользователя и пароль.

Инструменты сканирования сети

Пакет IP-Tools представляет собой набор из 19 сетевых утилит, объединенных общим интерфейсом.

В состав пакета IP-Tools входят:

Local Info - утилита, отображающая информацию о локальном компьютере (тип процессора, память и т.д.);

Connection Monitor - утилита, отображающая информацию о текущих TCP- и UDP-соединениях;

NetBIOS Info - утилита, отображающая информацию о NetBIOS-интерфейсах локального и удаленного компьютера;

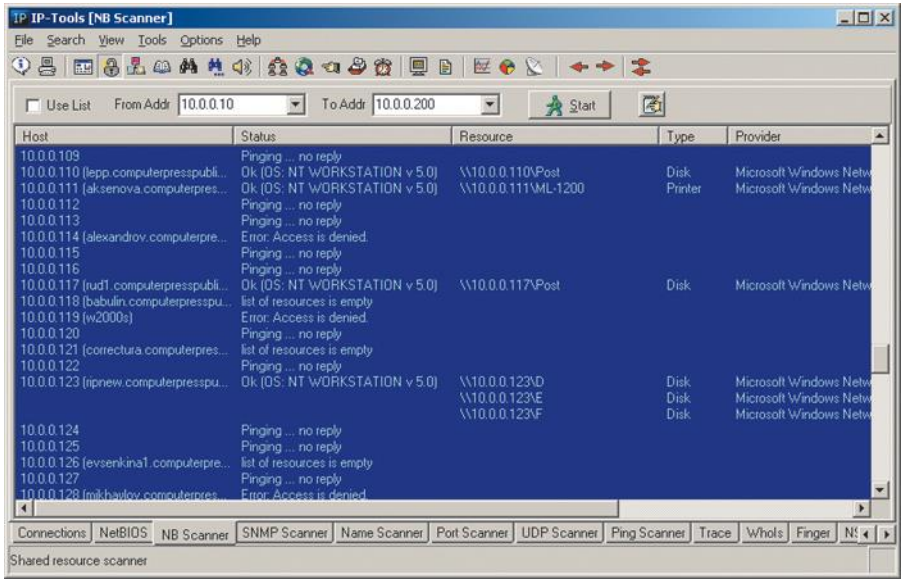
NB Scanner - сканер разделяемых сетевых ресурсов;

SNMP Scanner - сканер SNMP-устройств в сети;

Name Scanner - сканер сетевых имен компьютеров;

Port Scanner - TCP-сканер портов;

UDP Scanner - UDP-сканер портов;



Инструменты сканирования сети

Ping Scanner - IP-сканер с использованием процедуры пингования;

Trace - утилита для отслеживания маршрута прохождения пакетов;

WhoIs - утилита, позволяющая собирать информацию об узлах в Интернете;

Finger - утилита, собирающая и предоставляющая информацию о пользователях удаленного ПК по протоколу Finger;

NS LookUp - утилита, позволяющая поставить в соответствие IP-адрес и имя домена;

GetTime - утилита, позволяющая синхронизировать время локального ПК и заданного сервера времени;

Telnet - утилита для поиска клиентов сети, у которых установлена служба Telnet;

HTTP - утилита для поиска клиентов сети, у которых установлена служба HTTP;

IP-Monitor - утилита для отображения IP-трафика в реальном времени;

Host Monitor - утилита для отслеживания состояния узлов сети (подключен/отключен).

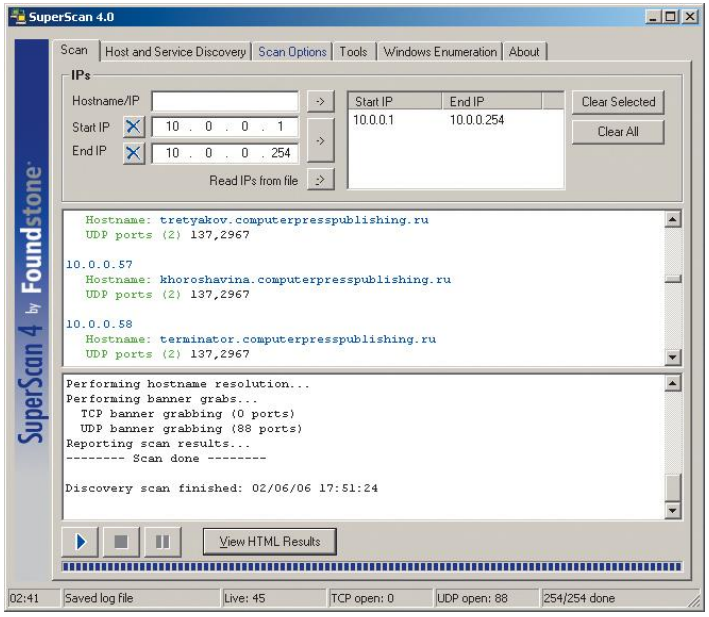
Инструменты сканирования сети

Утилита **SuperScan 4** представляет собой быстрый и гибкий сканер IP-адресов и портов. Утилита позволяет гибко задавать перечень IP-адресов исследуемых узлов и сканируемых портов.

При работе со сканером SuperScan 4 возможен как ручной ввод IP-адресов сканирования, так и экспорт адресов из файла. Поддерживается ввод одиночных адресов, диапазона адресов и диапазона в формате CIDR (10.0.0.1/255). Кроме того, IP-адреса можно вставлять непосредственно из буфера обмена.

При помощи настроек сканера можно назначить исследование только тех хостов сети, которые отвечают на запрос и определяются как присутствующие в сети. В то же время можно обязать сканер исследовать все узлы сети независимо от того, отвечают они на ICMP-запросы или нет.

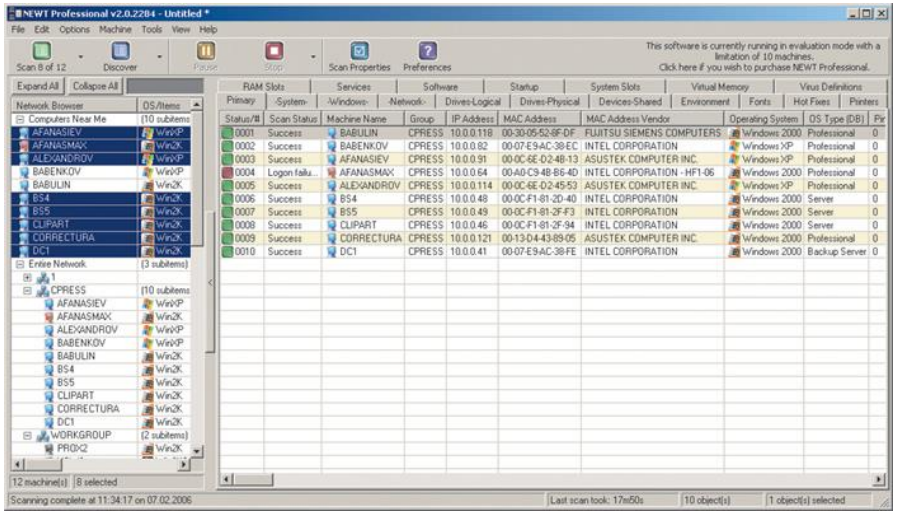
SuperScan 4 имеет встроенный UDP-сканер, поддерживающий два типа сканирования: Data и Data+ICMP. В методе Data исследуемому узлу посылаются пакеты данных UDP, которые требуют ответов от сервисов, использующих хорошо известные порты. В методе Data+ICMP применяется аналогичный метод сканирования. Если порт не отвечает сообщением «ICMP Destination Port Unreachable», то он рассматривается как открытый. Далее используется сканирование известных закрытых портов на предмет генерации ими ответных сообщений. Отметим, что данный метод может иногда приводить к ложным результатам, особенно если ответы на ICMP-запросы заблокированы.

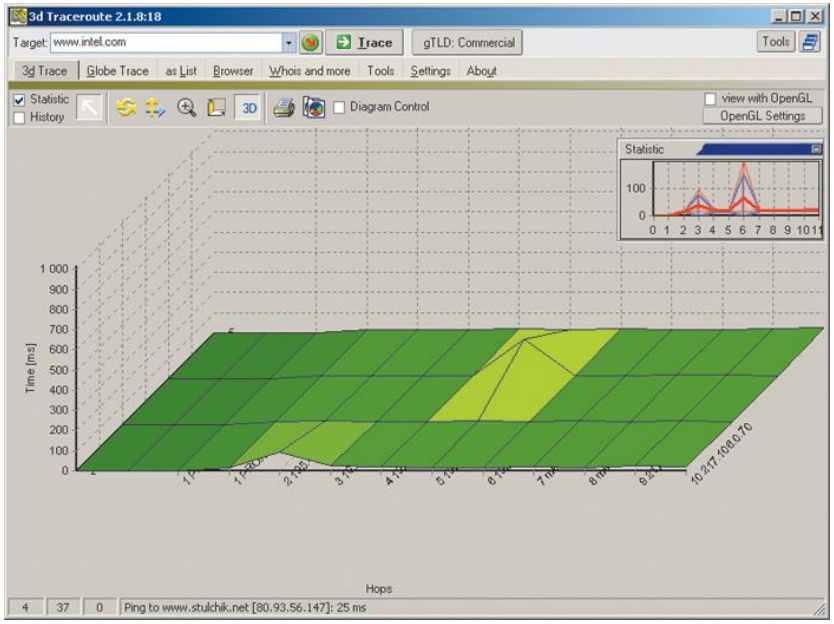


Утилита поддерживает два типа TCP-сканирования портов: TCP-connect и TCP SYN. Настройки сканера позволяют выбрать тип TCP-сканирования. Из возможностей настройки сканера SuperScan 4 можно отметить управление скоростью сканирования (скорость, с которой сканер посылает в сеть пакеты).

Инструменты сканирования сети

NEWT Professional v.2.0 - это комплексный сетевой сканер, позволяющий автоматизировать сбор информации о компьютерах локальной сети. Для системных администраторов, которым время от времени приходится заниматься инвентаризацией сети, он будет незаменимым инструментом.



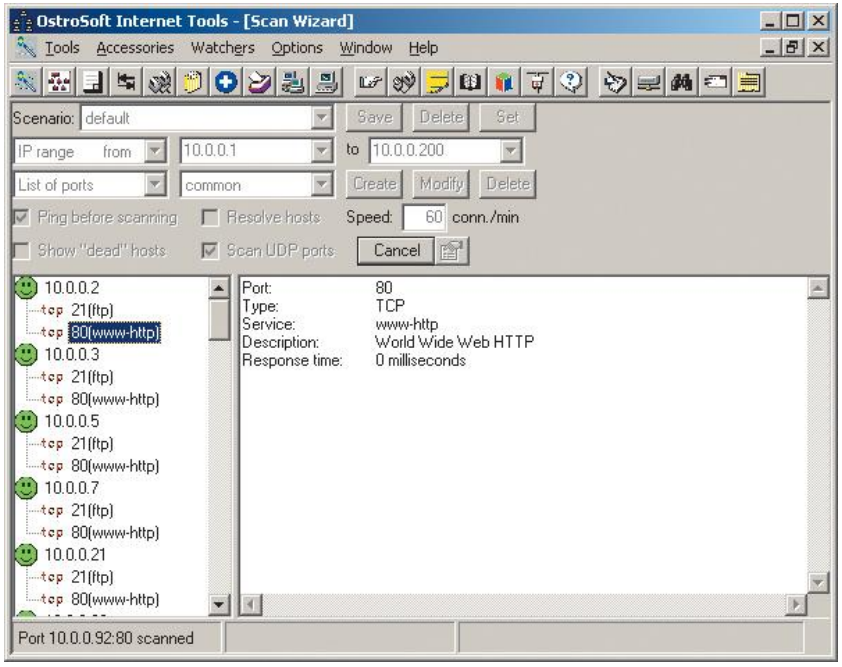


www.d3tr.co предназначен для отслеживания маршрутов прохождения пакетов между узлами в сети. При этом особенность данной утилиты заключается в том, что она позволяет строить трехмерный график задержек по всему маршруту.

Инструменты сканирования сети

Утилита **OstroSoft Internet Tools v.5.1** представляет собой комплексный сетевой сканер, включающий 22 утилиты: Scan Wizard, Domain Scanner, Port Scanner, Netstat, Ping, Traceroute, Host Resolver, NS Lookup, Network Info, Local Info, Finger, FTP, HTML Viewer, Ph, Simple Services, TCP Clients, WhoIs, Connection Watcher, Host Watcher, Service Watcher, Mail Watcher, HTML Watcher.

По сути, Scan Wizard представляет собой одновременно IP-сканер и сканер портов. В частности, можно задавать скорость сканирования, вводить диапазон IP-адресов, задавать диапазон сканируемых портов, выбирать тип сканирования портов. Результаты сканирования можно сохранять. Стоит отметить, что по своим скоростным характеристикам данный сканер не отличается выдающимися возможностями, так что исследование сети класса C может занять у него очень много времени.



Утилита Domain Scanner позволяет определить те хосты внутри сетевого домена, которые используют ту или иную службу. К примеру, задав адрес домена, можно выяснить, на каких компьютерах установлен Web-сервер, Mail-сервер, FTP-сервер и т.д.