Теория ping

Команда ping служит для принудительного вызова ответа конкретной машины. Для этого используется дейтаграмма ECHO_REQUEST протокола ICMP. Это протокол низкого уровня, который не требует наличия серверных процессов на зондируемой машине; это хороший способ убедится в том, что питание машины включено и IP находится в поднятом состоянии. Успешный результат использования команды ping вовсе не обязательно означает, что выполняются какие-то сервисные программы высокого уровня.

Ping - хорошее средство проверки правильности конфигурации сети, поскольку в выполнении этой команды участвуют система маршрутизации, схемы разрешения адресов и сетевые шлюзы. Если данная команда не работает - можете быть совершенно уверены, что более сложные средства тем более не функционируют. Несмотря на свою простоту, ping - одна из главных рабочих лошадок, использующихся при отладке сетей.

Безопасность. Что можно узнать по IP.

В этой небольшой статье вы узнаете, какие данные можно узнать о компьютере, зная только его уникальный! ip адрес.

Что такое ip адрес
В сети интернет у каждого компьютера есть свой уникальный ip - адрес. Он состоит из 4 цифр, каждая цифра может быть от 0 до 255. Весь адрес состоит из идентификатора сети и идентификатора хоста.
Существуют 5 классов ip - адресов, отличающиеся количеством бит в сетевом номере и хост - номере. Класс адреса определяется значением его первого октета.
Класс
a
b
c
d
e

Диапазон значений первого октета
1 - 126
128 - 191
192 - 223
224 - 239
240 - 247

Возможное количество сетей
126
16382
2097150

Возможное количество узлов
16777214
65534
254
268435456

134217728

Адреса класса a - предназначены для использования в больших сетях общего пользования. Они допускают большое количество номеров узлов.

Адреса класса b - используются в сетях среднего размера, например, сетях университетов и крупных компаний.

Адреса класса c - используются в сетях с небольшим числом компьютеров.

Адреса класса d - используются при обращениях к группам машин.

Адреса класса e - зарезервированы на будущее.

Стоит сразу отметить, что свой ip в интеренете имеет каждый компьютер. Будь то какой либо сайт или пользователь. Но есть и одно отличие: Каждый сайт имеет свой ip адрес. Т.е. по ip адресу находят сервер где находится сайт и сам сайт. Пользователи же обычно имеют динамически выделяемые ip адреса. То есть при дозвоне провайдеру, человеку выделяется один из свободных ip адресов, который принадлежат провайдеру. Провайдер же их берет в аренду и платит за это деньги, поэтому информацию о том, кому принадлежит какой либо диапазон ip адресов можно узнать вплоть до телефона владельца этого диапазона.
Иногда пользователь может иметь статический ip адрес по которому его всегда можно найти, но это редко, и за такую услугу провайдер обычно берет плату.
Как узнать свой собственный ip адрес.
В wnndows входит специальная программы winipcfg, с ее помощью можно узнать некоторую интересную информацию, в том числе и свой ip адрес. Просто наберите в командной строке winipcfg и перед вами появится окошко с вашим ip адресом

Надо еще отметить, что изначально (т.е. пока вы не подключены ни к какой сети и вам не выдан ip адрес) ваш компьютер имеет адрес - 127.0.0.1

Что можно узнать по ip
Сперва объясню зачем это нужно и для чего может пригодиться:
Например Вы администратор какого-либо сайта, чата, форума,: Допустим такую ситуацию: к вам приходит продвинутый юзер или чем хуже "хакер" и начинает издеваться над вашим ресурсом (имеется ввиду: получать доступ через открытые вами дыры, это и не мудрено, ведь не каждый из нас специалист по безопасности). Как в этом случае поступить? Попытаться закрыть этому пользователю доступ к ресурсу, хм: - это наверняка не получится, постоянно восстанавливать данные, которые мог попортить атакующий, тоже не выход. Единственно, что можно посоветовать - службы определения по ip или hostname имя провайдера, его географическое расположение и т.д.
Что это нам даст?
В идеальном случае - местонахождение нашего "хакера", его телефон, ну и соответственно фамилии людей проживающих по этому адресу.

Для начала поговорим о том, как узнать сам ip человека.
Способов может быть множество.
Например вам нужно узнать ip адрес человека, побывавшего на вашем сайте. Начнем с того, что при обращении к какому либо серверу (в нашем случае - серверу предоставляющему хостинг этому сайту), в логах сервера всегда фиксируется с какого ip

адреса поступил запрос. Ниже приведу часть лога программы small http server:

!->18/09 13:19:40 [194.29.16.182:>80] (t1 23) дата, время, ip адрес и порт, номер запроса
head /images/pic.g**if** http/1.1 Что запрашивается, протокол
connection: close
from: admin@provider.com E-mail адрес для связи
host: 195.232.27.17 кому был послан запрос
referer: http:// mpeg4.nightmail.ru /index. htm откуда поступил запрос
accept-language: ru язык сделавшего запрос
accept-encoding: gzip, deflate кодирование
user-agent: mozilla/4.0 (compatible; msie 5.01; windows 98; myie2 0.3) информация о программе сделавшей запрос
connection: keep-alive связь: проложить соединение
Из этого видно , что при запросе любого документа сервер фиксирует обращение даже к каждой картинке входящей в этот документ, иначе как бы он узнал, что и куда отправлять. Поэтому можно составить полную картину обмена информацией между пользователем и сервером, и узнать ip адрес не составляет труда. Труда может стоить получение этой информации с сервера, но такой метод возможен.
Конечно иногда бывает все гораздо проще. Часто сервер, предоставляющий хостинг сам ведет статистику, и вы как пользователь их услуг, получить эту информацию можете. Но многие пользуются услугами сервисов бесплатного хостинга, порой таких услуг не предоставляющих. Тогда, если на сайте установлен какой-нибудь счетчик посетителей (ramblertop100, hotlog и т.д.) вы легко можете узнать ip адрес посетителя и время визита из его отчета.
Также, почти всегда при создании сообщений в гостевых книгах и форумах фиксируется и ip адрес отправителя, который обычно доступен только администраторам этого форума. Если администратор - вы, вам не составит труда его узнать. Если нет, вы можете обратиться за помощью к администратору.
Иногда бывает необходимо узнать ip адрес отправителя письма. Узнать его можно из его служебного заголовка.
Существуют также программы и методы чтобы узнать ip адрес человека в чате или по icq. Например, есть множество программ, с помощью которых можно зная uin icq человека узнать его ip адрес.

Перейдём к самому интересному, а именно как
получить данные о "владельце" ip:
Итак, если вам известен ip адрес, вы можете узнать много полезной информации о его владельце. Для этих целей нужно воспользоваться специальным сервисом - whois . Начало формы

Подобных сервисов в интеренете много:
http://www.whoisin**form**.ru

http://www.web-tools.ru
http://www.iontail.com/?p=utils
http://www.all-nettools.com

С помощью такого сервиса можно узнать имя человека на которого зарегистрирован данный ip адрес, его e-mail, телефон и даже адрес. Также можно узнать когда был арендован данный диапазон, на какой срок. и для какой организации.
Если владелец ip адреса в данный момент находится в on-line, то можно посмотреть, какие порты открыты на этом компьютере. Это тоже может дать некоторую информацию о

компьютере. Сделать это можно любым сканером. Некоторые из таких сканеров сами могут вам сообщить и о назначении каждого открытого порта. К примеру на компьютере оказались открыты следующие порты: 139 (netbios), 11476 (icq).
Есть вероятность, что на компьютере обнаружатся открытые порты известных троянов (т.е. можно взять клиента и подключиться к удаленному компьютеру), хотя во многих троянах появилась возможность устанавливать пароль на подключение к серверу и произвольный порт (что затрудняет определение "троянского коня"). В таком случае можно просканировать все порты определенного ip. Могие порты открыты стандартными сервисами, а к подозрительным портам можно попробовать подключиться например с помощью утилиты rawtcp входящей в состав essential net tools 3.0 885kb . Тогда при определении подключения к порту троян на другом конце просто может "представиться" как это делает например netbus (посылает сообщение вида netbus v1.7)
А еще, раз уж речь зашла о работе троянских программ, хочу предупредить тех кто использует такие программы в благих целях (например для контроля своей локальной сети и.т.п.) Даже установка пароля на подключение к серверу наверняка не сможет защитить от несанкционированного подключения. Например в internet'e без труда можно найти программу rat cracker с помощью которой легко обойти парольную защиту самых распространенных троянов.
сейчас много домашних компьютеров объединены в локальные сети и некоторые на своем компьютере открывают папки или диски для совместного доступа. При подключении этого человека к интернету в эти папки можно заглянуть, если они не запаролены Для этого надо воспользоваться любой программой для поиска расшаренных данных (legion, ess nettools, shared resource scanner 6.2) И в этом случае установленный пароль не даст надежной защиты вашему компьютеру. Для взлома паролей к таким ресурсам существует множество эффективных программ. Например xintruder

Анонимность электронной почты

Для того, чтобы узнать ip, надо получить письмо любым почтовым клиентом: ms outlook, the bat!....Как настроить ms outlook читай ниже. Когда получили письмо надо просто посмотреть код письма. Там в заголовке письма указан ip отправителя. В outlook открываем письмо и жмем Файл, затем Свойства и выбираем закладку Подробности. В the bat! делается так: Открываем письмо, жмём Просмотр и выбираем Служебная информация после этого вверху прибавляется заголовок письма. Во многих почтовых системах с web-интерфейсом тоже есть возможность посмотреть заголовок письма.
Пример (заголовок)
from vasyap@mail.ru sat mar 27 12:16:35 2000.....от кого и дата
envelope-to: xxx@mail.ru.
delivery-date: sat, 27 mar 2000 12:16:35 +0300.....дата и время
received: from mail by f8.mail.ru with local (exim 3.14 #43)
id Рк4еК5е-0554нq7-00
for xxxx@mail.ru; sat, 27 mar 2000 12:16:35 +0300.....это наш адрес
received: from [208.46.44.12] by koi.mail.port.ru with http;
sat, 27 mar 2000 09:16:35 +0000 (gmt)
from: "vasya pupkin" ..
to: xxx@mail.ru.....кому
subject: hi beavis.....Тема письма
mime-version: 1.0
x-mailer: the but!.....прога которой посылали
x-originating-ip: unknown via proxy [xxx.yyy.zzz.xxx].....ip отправителя
reply-to: "vasya pupkin" .....кому ответить(от кого)
content-type: text/plain; charset=koi8-r.....кодировка письма

content-transfer-encoding: 8bit
message-id:
date: sat, 27 mar 2000 12:16:35 +0300

Важно

В письме может быть несколько ip, самый нижний и есть ip, отправителя
Скрытие своего ip-адреса
О том как скрыть свой ip отправляя письмо, читайте в статье "Отправка анонимной почты"
Настрройка ms outlook
Отправлять письма можно не только при помощи броузеров (ie , nn), но и любой почтовой программой, просто надо указать ваше имя (например pupkin) и адрес pop сервера (в нашем случае www.mail.ru). Это можно делать программой outlook express, чтобы получить почту достаточно нажать "получить". Настраивается она следующим образом: Запускаете outlook express заходите в сервис / учетные записи нажимаете кнопку добавить, выбираете почту вводите ваш электронный адрес pupkin@mail.ru , нажимаете далее, в поле сервер входящей почты пишите www.mail.ru или другой а во втором поле адрес smtp сервера (отправка сообщений) далее надо вроде ввести ваше имя и пароль. Теперь просто нажмите получить почту или что-то в этом роде...(Про адреса pop и smtp серверов почитайте на сайте где у вас почта)
Источник:
hack zone.