# Практическое занятие: Программные средства для анализа сетевых устройств.

Целью занятия является формирование и закрепление навыков по использованию программных средств для анализа доступности сетевых устройств.

Задачи:

1. Изучить программные средства для анализа сетевых устройств.

2. Просканировать ПК в лаборатории при помощи сканера портов nmap.

**Необходимые теоретические сведения.**

Сервис – программа, запущенная на компьютере с целью обслуживания сторонних запросов на выполнение какой-либо работы. Порт - это уникальный числовой идентификатор, присвоенный операционной системой сетевому сервису, использующему в своей работе один из протоколов транспортного уровня (TCP или UDP). К сетевым сервисам относится любое ПО, предоставляющее возможность для обмена данными по сети. На одном порту каждого протокола может работать только один сервис. Номера портов до 5000 стандартизованы, а в диапазоне оставшихся значений вплоть до 65535 могут быть присвоены пользовательским процессам. Список всех стандартных сервисов и соответствующих им портов имеется в файле /etc/services. Например сервис HTTP работает на порту 80. Если порт открыт, то сервис работает и обменивается данными по сети с другими устройствами. Если порт закрыт, то сервис либо не работает, либо ОС запрещает ему сетевой обмен. Открыть или закрыть порт можно при помощи брандмауэра (firewall). Открытый порт может создать уязвимость в системе.

**Практическая часть**

Сканер портов nmap является основным средством для диагностики состояния ЛВС, тестирования безопасности, поиска уязвимостей. Злоумышленниками nmap может использоваться для подготовки к взлому сети. Сканер nmap позволяет не только определять сервисы и ОС, запущенные на целевом ПК, но и исследовать горизонтальную структуру сети при помощи PING-сканирования.

NMAP в режиме PING-сканирования позволяет исследовать горизонтальную структуру сети, то есть выяснить какие устройства и сколько включены в сеть. Чтобы воспользоваться им, нужно запустить nmap с параметром –sP и указать диапазон IP-адресов. Например nmap -sP 192.168.1.0/24 сканирует диапазон IP-адресов от 192.168.1.1 до 192.168.1.255 . Узлы, отвечающие на команду ping выводятся на экран. Через слэш указывается диапазон IP-адресов, относящийся к подсети, которую нужно просканировать. Как известно, весь IP-адрес имеет длину 32 бита. В нашем пример число 24 означает, что 24 бита относится к подсети, а 8-бит обозначают номер узла. То есть это соответствует маске подсети 255.255.255.0. Если nmap в режиме PING-сканирования запущен от имени администратора (root), то он кроме IP-адресов покажет MAC-адреса всех активных устройств в сети.

Если запустить NMAP без параметров и указать ему один IP-адрес, то он просканирует устройство, на этом адресе на наличие открытых портов и определит сервисы, которые работают на нём. Например, пусть имеется роутер с адресом 192.168.1.1, запускаем nmap: nmap 192.168.1.1. Если запустить nmap с параметром -sV, то можно узнать версию ПО и ОС. Например, запускаем: nmap -sV 192.168.1.1.

Zenmap - это графический интерфейс для nmap. Но его использовать можно не всегда, т.к. на серверах и встраиваемых устройствах графический сервер часто бывает недоступен. Запустить zenmap можно набрав в консоли zenmap или через главное меню. В главном окне программы (рис.2) можно выбрать объект сканирования, режим сканирования (Ping Scan, Regular Scan и т.п.). Zenmap позволяет строить карты топологии ЛВС.

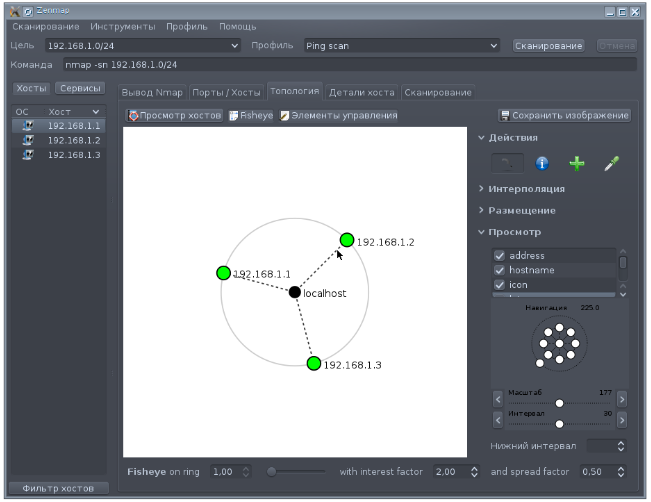


Рис. 2. Главное окно программы zenmap

Сервис SSH служит для удалённого управления ПК на Unix-like OC. На целевом ПК должен быть запущен SSH-сервер. Соединившись с ПК по SSH, мы получаем полный доступ к консоли ПК как если бы мы сидели за его клавиатурой и запустили терминал. Подключиться по SSH можно при помощи следующей команды:

ssh имя\_рользователя@IP-адрес

Вместо имени пользователя нужно подставить реальное имя пользователя на целевом ПК, IP-адрес которого нужно указать. Далее нужно ввести пароль. Теперь можно выполнять любые команды. Чтобы отсоединиться нужно набрать exit.

Команда

ssh rpd@192.168.1.1

выполняет удалённый вход на ПК с адресом 192.168.1.1 под пользователем rpd.

Утилита netstat выводит информацию о локальной сети и средствах TCP/IP. Именно к ней чаще всего обращаются администраторы, чтобы быстро отыскать причину неисправности в сети TCP/IP. Содержание и форма выходной информации зависят от операционной системы, но обычно выводятся следующие данные: список соединений, статистика сетевых интерфейсов, информация по буферам данных, содержание таблицы маршрутизации, статистика работы протокола. Характер выводимой информации можно выбирать с помощью опции командной строки. Запуск netstat –t показывает список серверов, с которыми в настоящий момент установлено соединение.

Netcat позволяет сканировать порты, передавать файлы, прослушивать порты. Запускается netcat при помощи команды nc в терминале. В зависимости от набора переданных параметров Netcat может передавать или принимать данные по сети. Netcat может быть использован в качестве сервера. Если Вы запустите его, как указано ниже, он будет слушать на порту 12345 (на всех интерфейсах):

nc -l -p 12345

За параметром –p следует десятичное число - номер порта, который можно выбрать произвольно, но больше чем 5000. Номер порта должен быть не занят другим сервисом. Теперь можно подключиться к компьютеру, на котором запущен Netcat с любого компьютера в сети. Для этого на удалённом компьютере нужно набрать команду:

nc –n 10.10.10.10 12345, где вместо 10.10.10.10 следует указать адрес компьютера на котором запущен Netcat. Теперь установлен двухсторонний обмен данными по сети. Любая строка, которая вводится с клавиатуры на клиенте отображается на сервере, и наоборот. Остановить сервер или клиент можно нажав Ctrl+C Если сервер остановлен, то все клиенты автоматически останавливаются и отключаются. Применяя конвейеры и перенаправление ввода-вывода, можно комбинировать netcat с любыми другими программами и передавать таким образом по сети файлы и текстовые и двоичные данные, вырабатываемые любой другой программой. В основном данный режим используется для передачи нестандартных данных. Можно также реализовать фильтрацию сетевого обмена. Для того, чтобы протестировать netcat в пределах одного компьютера нужно указать IP-адрес петлевого интерфейса 127.0.0.1. Этот IP-адрес (localhost) обозначает соединение компьютера самого с собой. С него разрешены соединения на любой порт, тогда как на внешних интерфейсах (Ethernet) часть портов может быть закрыта через firewall. Протестировать сетевой сервис с другого компьютера, если нет к нему физического доступа можно при помощи ssh. Можно зайти через SSH на другой компьютер.

Netcat может запустить любую программу как сетевой сервис. При этом программа может получать команды не с клавиатуры, а через сеть. Для этого служит параметр -e. Например:

nc -l -p 8888 -e /bin/bash

запускает интерпретатор командной строки bash в режиме сервера на порту 8888. Если теперь соединиться с ним с другой консоли, или с другой машины, то на клиенте можно выполнять стандартные команды командной строки.

# Задание для закрепления практических навыков:

1. Открыть файл /etc/services , например при помощи текстового редактора gedit или консольного текстового редактора mcedit (запускается отдельно или встроен в файловый менеджер mc). Изучить структуру данного файла. Найти номера портов, соответствующих сервисам HTTPS, FTP, SSH, TELNET.

2. Узнать свой IP-адрес и маску подсети. Например при помощи команды ifconfig. Исследовать структуру сети в лаборатории при помощи nmap, просканировав свою подсеть (в которую входит IP-адрес своей машины). Сделать выводы по результатам сканирования.

3. При помощи nmap узнать, какие сервисы работают и какая ОС установлена на своём ПК, на роутере в лаборатории, и на соседнем ПК.

4. Подключиться к одному из соседних ПК при помощи SSH, узнать содержимое домашнего каталога ~, отсоединиться от ПК.

5. Запустить netstat –t и вывести список активных соединений. Запустить браузер Firefox и соединиться с любым сайтом. Повторить вызов netsat и проанализировать изменения.

6. Запустить netcat в режиме сервера. Соединиться с ним с той же машины, использую петлевой интерфейс (адрес 127.0.0.1). Убедиться, что есть обмен данными. Остановить клиент.

7. Запустить при помощи netcat интерпретатор командной строки как сетевой сервис. Соединиться с ним, запустив netcat в режиме клиента, выполниь несколько стандартных Linux-команд (например ls, cd).