Практическое задание 07

Используйте командную строку вашей операционной системы.

В Windows запустите Win-X Powershell (администратор) или Win-R и введите **cmd**.

В GNU Linux или Mac OS используйте terminal (bash).

Запустите **netstat --help** либо **netstat --help|more** чтобы узнать перечень ключей.

В UNIX-подобных системах (GNU/Linux или Mac OS) можно использовать также **netstat --help|less** или **man netstat**.

Используйте разные варианты ключей, чтобы определить, какие у вас имеются открытые порты (TCP и UDP), какие имеются прослушивающие TCP-сокеты, установленные TCP-соединения (как исходящие, так и входящие). Выберите 10 произвольных строк и проанализируйте, какой протокол прослушивает этот сокет или установленное соединение (входящее либо исходящее). Если порт нестандартный или не зарезервирован за каким-либо протоколом, попробуйте узнать имя процесса или идентификатор процесса (чтобы узнать его в списке процессов или диспетчере задач). Узнайте, что это за сервис, и зачем ему нужны соединения. Можно искать в Интернете информацию о сервисе.

Данная задача может быть полезной на практике при поиске вредоносного ПО. Если программа запущена из домашней директории или /tmp, если она соединяется с неизвестным вам адресом, и это не используемый вами сервис, возможно, это троян или вирус.

Отчет должен содержать подробное описание 10 произвольных строк:

- что это за сокет;
- какой протокол, в каком состоянии соединение;
- какой сервис или программа его использует;
- зачем.

Отчет должен быть подготовлен в формате .docx или .pdf и сдан в качестве домашнего задания. Отчет может содержать скриншоты, но не должен состоять из одного скриншота вывода **netstat** без каких-либо пояснений.

Дополнительное усложненное задание: выбрать из приведенных примеров эхо-сервера (либо написать самостоятельно на выбранном вами языке, либо найти в Интернете), запустить на машине (можно виртуальной, или VDS, если используете).

Доступны примеры эхо-сервера:

- echo7.c – пример на Си;
- phpecho.php – пример на PHP;
- pyecho.py и pyecho2.php – примеры на Python.

Также доступны примеры на Java от нашего преподавателя **Алексея Степченко**: простой пример эхо-сервера и клиента в архиве samples.zip, более сложный — в simple_server.zip.

Используя Telnet либо PuTTY (в Windows), либо написав собственный клиент, установить одно, затем два, затем три соединения с сервером, отследить с помощью **netstat** поведение и точно также добавить в отчет.

Облегченная версия дополнительного усложненного задания: вместо эхо-сервера использовать установленный на виртуальной машине (Ubuntu) либо VDS OpenSSH-server и соединяться с ним с помощью SSH-клиента или PuTTY. Задокументировать, что происходит с сокетами при одном, двум, трех одновременных подключениях.