Содержание:

Введение

Атаки, которым вы можете подвергнуться в Сети, весьма разнообразны, но можно выделить два основных типа: отказ в обслуживании (DoS-атаки) и несанкционированный доступ. Отказ в обслуживании - это атаки, направленные на нарушение нормальной работы (как правило, их целью является перезагрузка или зависание вашего компьютера). Получение несанкционированного доступа - гораздо более опасный вид атаки. В этом случае злоумышленник получает доступ файлам на вашем жестком диске а иногда и возможность выполнять произвольные программы, что дает ему возможность украсть какую-либо важную информацию (например, пароль к почтовому ящику, сайту, красивый номер ICQ UIN, сертификат WebMoney) или использовать ваш компьютер для атаки на другие объекты.

Наиболее распространенные виды атак,

с которыми можно столкнуться в Сети:

Nuke (нюк) - использование уязвимостей операционной системы с целью вызывать перезагрузку компьютера. Нюки были очень распространены для ранних версий Windows 9X, которые содержали ошибки в реализации протокола TCP/IP, используемого в Сети.

Ping Flood (иногда также называется Dead Link) - забрасывание атакуемого ICMP-пакетами, которые обычно используются для проверки связи, в результате чего он не может принимать/передавать какую-либо информацию. Такая атака может быть успешно реализована либо с более быстрого канала связи, чем у атакуемого, либо распределенно, с нескольких компьютеров сразу.

SYN Flood - во многом похож на ping flood, но посылаются SYN-пакеты, которые устанавливают неиспользуемые соединения, что приводит к бессмысленному использованию ресурсов компьютера, из-за чего работа сначала просто замедляется, а затем компьютер либо не может установить соединение, либо просто зависает. Для того, чтобы эта атака стала возможной, на компьютере должен быть открыт хоть какой-нибудь порт.

Virus (вирус) - программа, способная самопроизвольно размножаться, т.е. создавать и рассылать собственные копии, а иногда приносить какой-либо вред компьютеру, начиная от простых шуток над пользователем, и кончая полным уничтожением данных на диске (а иногда и перепрошивкой BIOS'а). В последнее время наиболее распространены почтовые вирусы (приходят по e-mail) и macro-вирусы (распространяются в виде макросов в файлах, созданных в MS-Office).

Атаки, направленные на получение доступа:

NetBios-атаки - попытка получить доступ к файлам, используя сетевой протокол NetBios и ресурсы, сделанные общедоступными без пароля. Один из самых распространенных типов атак, так как наиболее просто реализуем.

Trojan (троян) - установка на компьютер программы, которая работает незаметно для пользователя и позволяет атакующему производить какие-либо действия на чужом компьютере, например получить доступ к его файлам или удаленное управление. Очень часто троян посылают пользователю, маскируя под какую-либо полезную программу.

Cross Site Scripting (XSS) - внедрение в страницу кода JavaScript, который осуществит перехват каких-либо данных пользователя (как правило, cookies или идентификатора сессии в URL) и передаст их сайту зломышленника. Используется для получения доступа от имени атакуемого пользователя к чатам, форумам или другими Web-ресурсам.

Страницы с ошибками - страницы, в которых используются уязвимости браузеров для того, чтобы вызвать сбой в системе (хотя иногда с помощью этих ошибок можно получить доступ и к файлам, и даже выполнить произвольный код).

Также возможна любая комбинация различных способов атаки, в зависимости от цели атакующего. Например, атакующий может получить доступ через NetBios, положить троян в "Автозагрузку" и затем применить Nuke для того, чтобы заставить пользователя перезагрузиться и запустить троян.