

Хакерские утилиты и защита от них

СЕТЕВЫЕ АТАКИ

Сетевые атаки - направленные действия на удаленные сервера для создания затруднений в работе или утери данных

Сетевые атаки на удаленные серверы реализуются с помощью **специальных программ**, которые посылают на них специфические запросы. Это приводит к отказу в обслуживании (**«зависанию»** сервера), если ресурсы атакуемого сервера недостаточны для обработки всех поступающих запросов.



СЕТЕВЫЕ АТАКИ

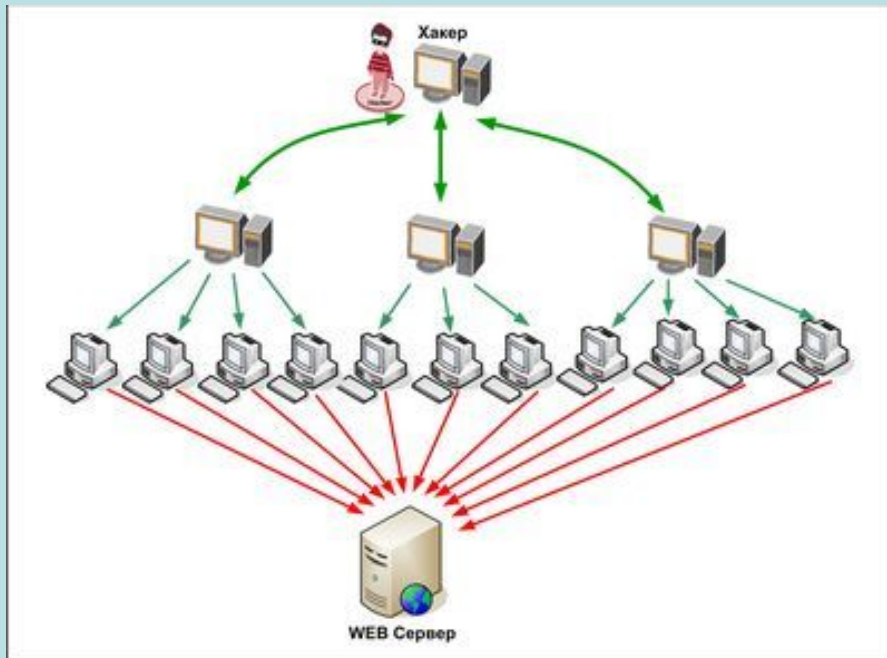


DoS-программы (от англ. Denial of Service – отказ в обслуживании) реализуют атаку с одного компьютера с ведома пользователя.

DoS-программы обычно наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера.

Некоторые сетевые черви содержат в себе DoS-процедуры, атакующие конкретные сайты. Так, червь «Codedred» 20 августа 2001 года организовал успешную атаку на официальный сайт президента США, а червь «Mydoom» 1 февраля 2004 года «выключил» сайт компании – производителя дистрибутивов UNIX.

СЕТЕВЫЕ АТАКИ



Чаще всего при проведении DDoS-атак злоумышленники используют трехуровневую архитектуру

DDoS-программы (*от англ. Distributed DoS – распределенный DoS*) реализуют распределенные атаки с разных компьютеров, причем без ведома пользователей зараженных компьютеров.

Для этого DDoS-программа засылается на компьютеры «жертв-посредников» и после запуска в зависимости от текущей даты или по команде от **хакера** начинает сетевую атаку на указанный сервер в сети.

Некоторые хакерские утилиты реализуют **фатальные сетевые атаки**. Такие утилиты используют уязвимости в операционных системах и приложениях и отправляют специально оформленные запросы на атакуемые компьютеры в сети. В результате сетевой запрос специального вида вызывает **критическую ошибку** в атакуемом приложении, и система прекращает работу.

УТИЛИТЫ «ВЗЛОМА» УДАЛЁННЫХ КОМПЬЮТЕРОВ

Утилиты «взлома» удаленных компьютеров предназначены для проникновения в удаленные компьютеры с целью дальнейшего управления ими (используя методы троянских программ типа утилит удаленного администрирования) или для внедрения во «взломанную» систему других вредоносных программ

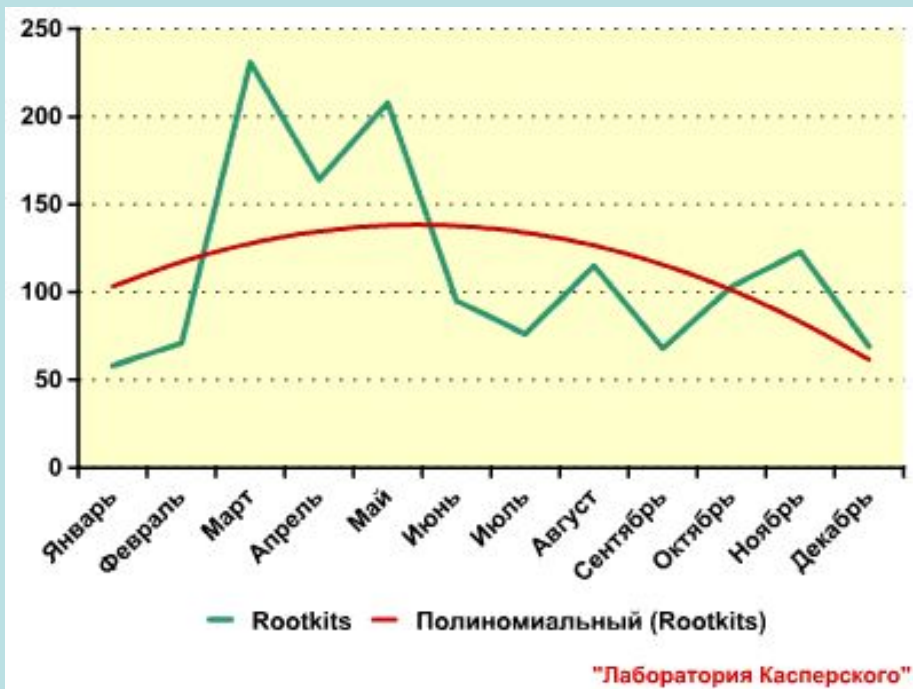


Утилиты «взлома» удаленных компьютеров обычно используют уязвимости в операционных системах или приложениях, установленных на атакуемом компьютере.

Профилактическая защита от «взлома» состоит в своевременной загрузке из Интернета обновлений системы безопасности операционной системы и приложений.

РУТКИТЫ

Руткит (от англ. *root kit* - «набор для получения прав root») - программа или набор программ для скрытного взятия под контроль «взломанной» системы.



Количество новых руткитов, обнаруженных аналитиками «Лаборатории Касперского» в 2007 году

В операционной системы UNIX под термином **«rootkit»** понимается набор утилит, которые хакер устанавливает на «взломанном» им компьютере после получения первоначального доступа.

В операционной системе Windows под **rootkit** принято подразумевать программу, которая внедряется в систему и перехватывает системные функции.

Многие rootkit устанавливают в систему свои драйверы и службы (они также являются «невидимыми»).

ЗАЩИТА ОТ ХАКЕРСКИХ АТАК И СЕТЕВЫХ ЧЕРВЕЙ

Защита компьютерных сетей или отдельных компьютеров от несанкционированного доступа может осуществляться с помощью **межсетевого экрана**, или **брандмауэра** (от англ. firewall).

Межсетевой экран позволяет:

- *блокировать хакерские DoS-атаки, не пропуская на защищаемый компьютер сетевые пакеты с определенных серверов (определенных IP-адресов или доменных имен);*
- *не допускать проникновение на защищаемый компьютер сетевых червей (почтовых, Web и др.);*
- *препятствовать троянским программам отправлять конфиденциальную информацию о пользователе и компьютере.*



Межсетевые экраны ZyXEL - защита сети от вирусов, спама, **сетевых атак**.

Межсетевой экран может быть реализован как **аппаратно**, так и **программно**.

Настройка Центра безопасности Windows

