Хакерские утилиты и защита от них

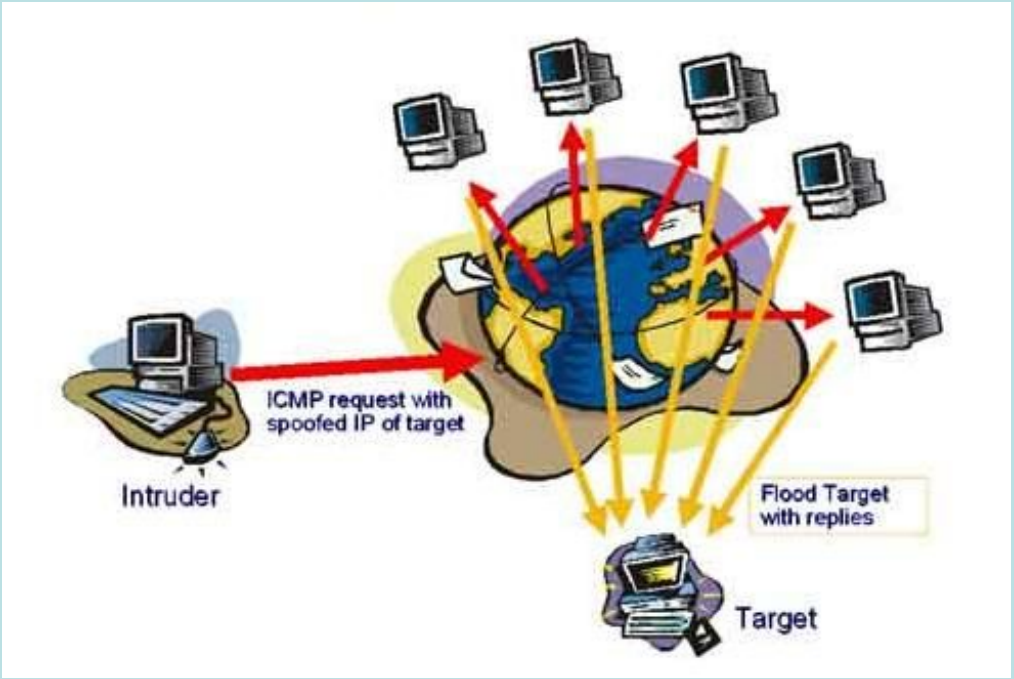
11 класс

СЕТЕВЫЕ АТАКИ

Сетевые атаки – направленные действия на удалённые сервера для создания затруднений в работе или утери данных.

Сетевые атаки на удалённые 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

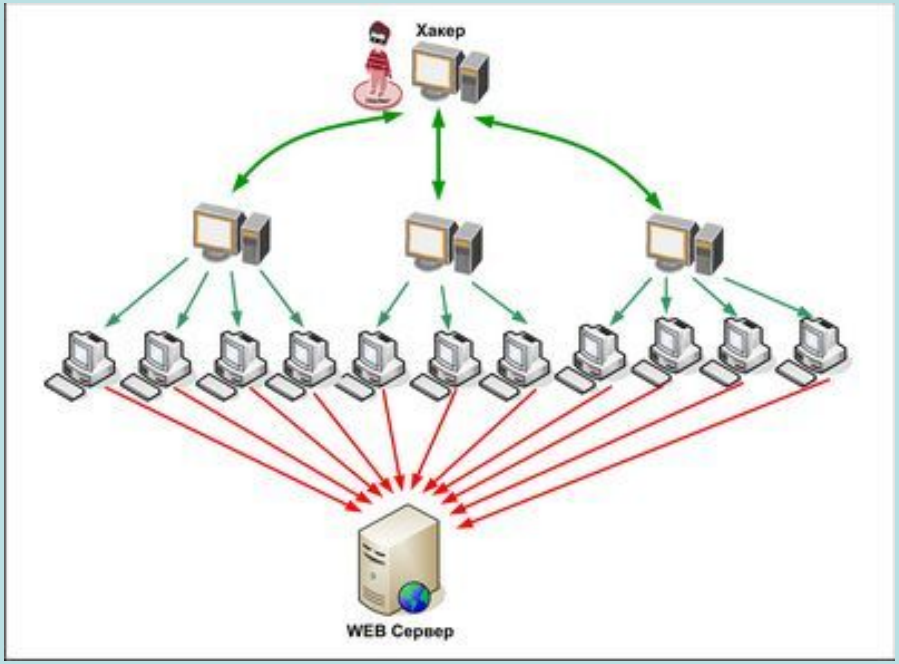


DoS-программы (от англ. Denial of Service – отказ в обслуживании) реализуют атаку с одного компьютера с ведома пользователя.

DoS-программы обычно наносят ущерб удалённым компьютерам и сетям, не нарушая работоспособность заражённого компьютера.

Некоторые сетевые черви содержат в себе DoS-процедуры, атакующие конкретные сайты. Так, червь «Codered» 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 – распределённый DoS)* реализуют распределённые атаки с разных компьютеров, причём без ведома пользователей заражённых 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.

БОТНЕТ

Ботнет (англ. botnet, произошло от слов robot и network) – это компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами – автономным программным обеспечением. Чаще всего бот в составе ботнета является программой, скрытно устанавливаемой на устройство жертвы и позволяющей злоумышленнику выполнять некие действия с использованием ресурсов заражённого компьютера. Обычно используются для нелегальной или неодобряемой деятельности – рассылки спама, перебора паролей на удалённой системе, атак на отказ в обслуживании.

Управление обычно получают в результате установки на компьютер невидимого необнаруживаемого пользователем в ежедневной работе программного обеспечения без ведома пользователя. Происходит обычно через:

- Заражение компьютера вирусом через уязвимость в ПО (ошибки в браузерах, почтовых клиентах, программах просмотра документов, изображений, видео).
- Использование неопытности или невнимательности пользователя – маскировка под «полезное содержимое».
- Использование санкционированного доступа к компьютеру (редко).
- Перебор вариантов администраторского пароля к сетевым разделяемым ресурсам (в частности, к ADMIN$, позволяющей выполнить удалённо программу) – преимущественно в локальных сетях.

Наиболее заметной из всех видов деятельности ботнета является DDoS-атака. **Среди успешных (и почти успешных) атак:**

- DDoS-атака на сайт Microsoft.com (вирус MSBlast, в один день начавший со всех заражённых машин посылать запросы на microsoft.com, привёл к простою сайта);
- Серия DDoS-атак на «Живой журнал» весной – летом 2011 года.

УТИЛИТЫ «ВЗЛОМА» УДАЛЁНЫХ КОМПЬЮТЕРОВ

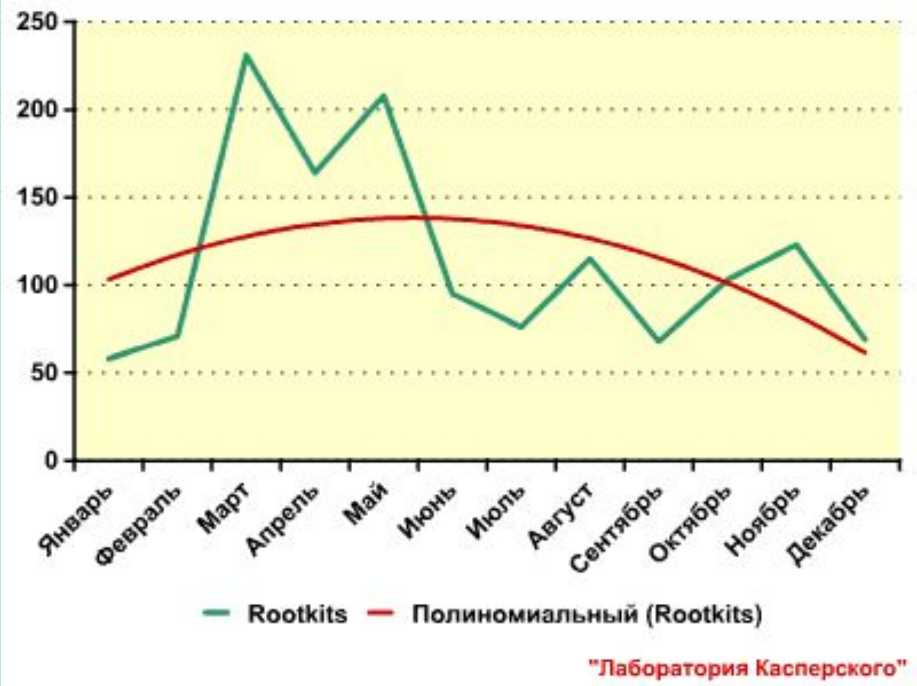
Утилиты «взлома» удалённых компьютеров предназначены для проникновения в удалённые компьютеры с целью дальнейшего управления ими (используя методы троянских программ типа утилит удалённого администрирования) или для внедрения во «взломанную» систему других вредоносных программ.

Утилиты «взлома» удалённых 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 системе 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 определённых серверов (определённых IP-адресов или доменных имён);*
- *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.

Межсетевые экраны Cisco ASA 5500 нового поколения

Межсетевые экраны Cisco ASA 5500 нового поколения

Межсетевой экран Cisco ASA серии 5500 помогает организациям найти оптимальный баланс между безопасностью и производительностью. Он сочетает в себе наиболее широко применяемый в отрасли межсетевой экран с контролем состояния соединений и обширный набор служб обеспечения безопасности сети нового поколения, включая:

- детальный контроль и управление приложениями и микроприложениями с инструментами управления на основе поведения;
- надёжную защиту от интернет-угроз;
- расширенную защиту от угроз с помощью высокоэффективной многофункциональной системы предотвращения вторжений (IPS);
- надежно защищённый удаленный доступ;
- защиту от ботнетов;
- превентивную защиту от интернет-угроз практически в реальном времени.

Все межсетевые экраны Cisco ASA серии 5500 нового поколения работают под управлением программного обеспечения Cisco Adaptive Security Appliance (ASA) и поддерживают функции контроля состояния соединений корпоративного класса, а также возможности межсетевых экранов нового поколения.

КОМПЬЮТЕРНЫЙ ПРАКТИКУМ

Настройка Центра безопасности Windows