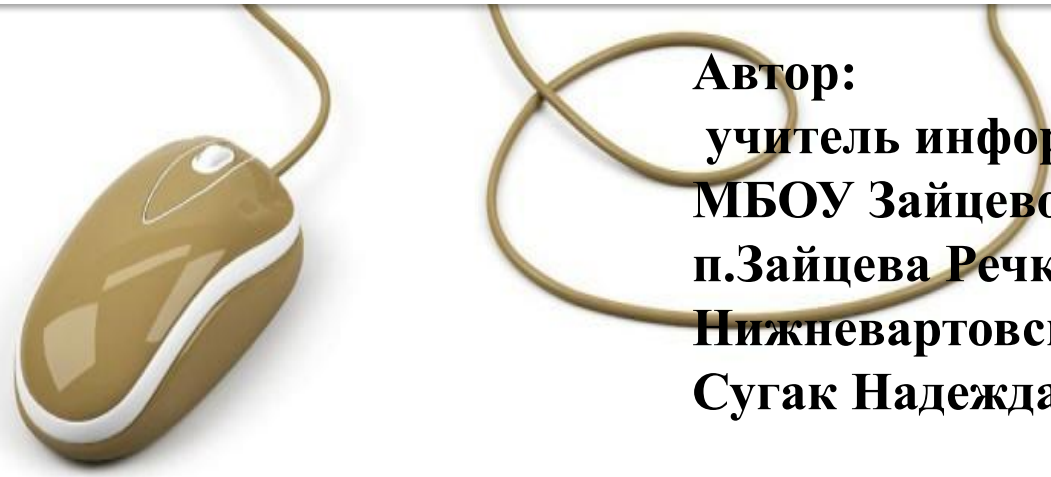
Основные виды и приемы хакерских атак



Автор:
учитель информатики
МБОУ Зайцевореченская ОСШ
п.Зайцева Речка,
Нижневартовский район
Сугак Надежда Александровна

Хакерская атака – это покушение на систему безопасности, для захвата контроля над удаленной или локальной вычислительной системой, либо для ее дестабилизации, либо отказа в обслуживании

Для осуществления хакерской атаки хакеры часто используют уязвимости в программном обеспечении для внедрения в компьютерную систему

Целью таких атак являются кража конфиденциальной информации или установка вредоносных программ. Помимо этого, хакеры также могут использовать взломанные персональные компьютеры для рассылки спама

Наиболее распространенными хакерскими атаками являются: mailbombing, переполнение буфера, внедрение вирусов, троянов, атаки на отказ в обслуживании и пр.

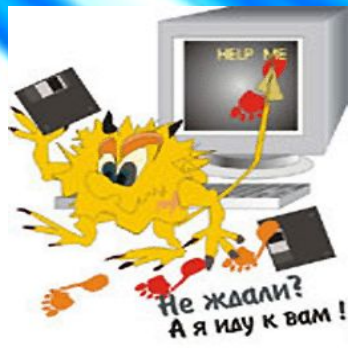
Mailbombing

Считается самым старым методом атак, хотя суть его проста и примитивна: большое количество почтовых сообщений делают невозможными работу с почтовыми ящиками, а иногда и с целыми почтовыми серверами

Для этой цели было разработано множество программ, и даже неопытный пользователь штурма мог совершить атаку, указав всего лишь e-mail жертвы, текст сообщения, и количество необходимых сообщений

Многие такие программы позволяли прятать реальный IP-адрес отправителя, используя для рассылки анонимный почтовый сервер

Эту атаку сложно предотвратить, так как даже почтовые фильтры провайдеров не могут определить реального отправителя спама. Провайдер может ограничить количество писем от одного отправителя, но адрес отправителя и тема зачастую генерируются случайным образом



Переполнение буфера

Пожалуй, один из самых распространенных типов атак в Интернете. Принцип данной атаки построен на использовании программных ошибок, позволяющих вызвать нарушение границ памяти и аварийно завершить приложение или выполнить произвольный бинарный код от имени пользователя, под которым работала уязвимая программа

Если программа работает под учётной записью администратора системы, то данная атака позволит получить полный контроль над компьютером жертвы, поэтому рекомендуется работать под учётной записью рядового пользователя, имеющего ограниченные права на системе, а под учётной записью администратора системы выполнять только операции, требующие административные права

Вирусы, троянские программы, почтовые черви, Rootkit-ы и другие специальные программы

Следующий вид атаки представляет собой более изощрённый метод получения доступа к закрытой информации — использование специальных программ для ведения работы на компьютере жертвы, а также дальнейшего распространения (это вирусы и черви)

Такие программы предназначены для поиска и передачи своему владельцу секретной информации, либо просто для нанесения вреда системе безопасности и работоспособности компьютера жертвы

Man-in-the-Middle

Вид атаки, когда злоумышленник перехватывает канал связи между двумя системами, и получает доступ ко всей передаваемой информации.

При получении доступа на таком уровне злоумышленник может модифицировать информацию нужным ему образом, чтобы достичь своих целей.

Цель такой атаки — кража или фальсифицирование передаваемой информации, или же получение доступа к ресурсам сети. Такие атаки крайне сложно отследить

Сниффинг пакетов

Также довольно распространённый вид атаки, основанный на работе сетевой карты в режиме promiscuous mode, а также monitor mode для сетей Wi-Fi. В таком режиме все пакеты, полученные сетевой картой, пересылаются на обработку специальному приложению, называемому снифферо́м.

В результате злоумышленник может получить большое количество служебной информации: кто, откуда и куда передавал пакеты, через какие адреса эти пакеты проходили.

Самой большой опасностью такой атаки является получение самой информации, например логинов и паролей сотрудников, которые можно использовать для незаконного проникновения в систему под видом обычного сотрудника компании.

Инъекция

Атака, связанная с различного рода инъекциями, подразумевает внедрение сторонних команд или данных в работающую систему с целью изменения хода работы системы, а в результате — получение доступа к закрытым функциям и информации, либо дестабилизации работы системы в целом.

Наиболее популярна такая атака в сети Интернет, но также может быть проведена через командную строку системы

PHP-инъекция

Один из способов взлома веб-сайтов, работающих на PHP. Он заключается в том, чтобы внедрить специально сформированный злонамеренный сценарий в код веб-приложения на серверной стороне сайта, что приводит к выполнению произвольных команд

Известно, что во многих распространённых в интернете бесплатных движках и форумах, работающих на PHP (чаще всего это устаревшие версии) есть непродуманные модули или отдельные конструкции с уязвимостями. Хакеры анализируют такие уязвимости, как неэкранированные переменные, получающие внешние значения, например старая уязвимость

DoS-атака

от англ. Denial of Service — Отказ в обслуживании — атака, имеющая своей целью заставить сервер не отвечать на запросы. Такой вид атаки не подразумевает получение некоторой секретной информации, но иногда бывает подспорьем в инициализации других атак. Например, некоторые программы из-за ошибок в своём коде могут вызывать исключительные ситуации, и при отключении сервисов способны исполнять код, предоставленный злоумышленником или атаки лавинного типа, когда сервер не может обработать огромное количество входящих пакетов

DDoS (от англ. Distributed Denial of Service — Распределенная DoS) — подтип DoS атаки, имеющий ту же цель что и DoS, но производимой не с одного компьютера, а с нескольких компьютеров в сети. В данных типах атак используется либо возникновение ошибок, приводящих к отказу сервиса, либо срабатывание защиты, приводящей к блокированию работы сервиса, а в результате также к отказу в обслуживании. DDoS используется там, где обычный DoS неэффективен. Для этого несколько компьютеров объединяются, и каждый производит DoS атаку на систему

Физкульминутка

Упражнение первое:

резко зажмурить глаза на 3 секунды: и широко открыть на 3 секунды, повторить упражнение 10 раз.

Упражнение второе:

поднять глаза вверх, при этом голова остается в одном положении, задержать взгляд на 3 секунды, затем опустить глаза вниз и задержать взгляд на 3 секунды повторить упражнение 10 раз

Упражнение третье:

часто-часто моргать глазами, повторить 10 раз.

Организация эффективной защиты от хакеров

Даже если ты используешь свой компьютер в основном лишь для скачивания фильмов и музыки или общения с друзьями в соцсетях знания, как защититься от хакеров, тебе тоже будут полезны

Вот несколько простых советов, как не заразиться «электронным зверинцем»:

- ✔ Не доверяйте спаму! Большинство червей распространяются через электронную почту, а точнее через спам. Поэтому удаляйте все спамерские послания, не вникая особо в подробности написанного;
- ✔ Используйте брандмауэр, хотя бы встроенный в систему, и внимательно анализируйте его сообщения и логи;
- ✔ Крайне аккуратно работайте с почтой, а также программами для обмена сообщениями и работы с файлообменными сетями, например, следует отключить использование HTML в принимаемых письмах;
- ✔ Никогда не запускайте программы сомнительного происхождения, даже полученные из заслуживающих доверия источников, например, из присланного другом письма;
- ✔ Ни при каких условиях не передавайте по телефону или по почте свои персональные данные, особенно пароли;
- ✔ Регулярно создавайте резервные копии критических данных

✔ Обновляйте программное обеспечение. Частенько хакерами используются дыры во всяких браузерах или офисах. Компания, писавшая программу спешно выпускает обновления, в котором уязвимость закрывается. Но есть пользователи, которые не очень-то заботятся о скачивании обновлений, поэтому хакеры успешно используют их для своих атак

✔ Не посещайте сомнительные сайты

Очень часто сайты с сомнительным содержанием таят в коде своих страниц червя, который с удовольствием перетечёт к вам на компьютер

✔ Будьте осторожны с тем, что попадает на ваш компьютер. Не желательно без обновлённого хорошего антивируса подключать к своему компьютеру устройства хранения информации.

Чаще всего вирусы переносятся вместе с дискетами, на которых хранятся текстовые файлы, на флешках и на винчестерах.

НИКТО не может гарантировать,
что если правила безопасности соблюдаете ВЫ,
ваш знакомый тоже соблюдает эти правила!


СПАСИБО ЗА
ВНИМАНИЕ!