ОПРЕДЕЛЕНИЕ И ЦЕЛИ ОСНОВНЫХ УГРОЗ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Калмухамедова Альбина Бакыткельдиевна

студент, кафедра пожарной безопасности Уфимского государственного технического авиационного университета, РФ, г. Уфа

Цыпышева Марина Викторовна

студент, кафедра пожарной безопасности Уфимского государственного технического авиационного университета, РФ, г. Уфа

Миниахметов Рамазан Маратович

студент, кафедра вычислительной техники и защиты информации Уфимского государственного технического авиационного университета, РФ, г. Уфа

Основными категориями угроз информационной безопасности являются:

1. Вторжение или взлом;

2. Вирусы и черви;

3. Троянский конь;

4. Spoofing;

5. Sniffing;

6. Отказ в обслуживании (DoS).

Взлом - это не что иное, как получение доступа к компьютерной системе без ведома ее владельца. Люди, которые совершают подобные незаконные действия, называются хакерами. Как только они получат доступ к целевым системам, они могут изменять данные, имеющиеся в этих системах, или украсть личную информацию, например, связанную с банковскими и кредитными карточными счетами. Большинство целевых систем для хакеров - это сайты электронной коммерции, отдельные машины, а иногда и банковские веб-сайты. Целевые системы взлома зависят от хакеров и их интересов. Некоторые люди будут взломать только для удовольствия и любопытства. Для взлома хакеру необходимо просканировать целевые системы на наличие слабостей, собрать информацию об используемых операционных системах, незащищенных папках, конфигурационных файлах и т. д. Он собирает все эти данные и анализирует, как можно компрометировать целевой сайт или систему. Как только хакеру удастся найти этот способ, начнется незамедлительная атака на систему. Чтобы предотвратить подобные атаки, большинство веб-сайтов электронной коммерции и даже отдельные пользователи начали использовать хорошие системы брандмауэра. Всякий раз, когда происходит атака, системы брандмауэра сразу сообщают об угрозе, а иногда и помогают отслеживать атаку.

Вирусы и черви - это компьютерные программы, которые не позволяют работать с компьютерными системами. Существует тонкая граница между ними. Оба могут клонировать себя, но, путешествуя по сети, вирусу нужен файл-носитель. Он не может путешествовать

самостоятельно там, где черви могут путешествовать без каких-либо проблем. Им не нужен зараженный файл. Конечная цель этих вирусов и червей подвергнуть сбою хорошую рабочую систему, а иногда черви могут украсть личную информацию, чтобы отправить ее своему создателю. Лучшим способом избежать вирусов является установка антивирусных программ для всех систем. Некоторые новые вирусы могут попытаться обойти антивирусное программное обеспечение. Поэтому очень важно постоянно обновлять базу данных вирусов. Помимо этого, пользователи должны быть очень осторожны при загрузке файлов с различных сайтов или почты, поскольку загруженный документ может содержать вредоносный вирус.

Программы Trojan Horse (троянский конь) изначально использовались для системного администрирования. Эти программы состоят из двух частей. Одна работает как сервер, а другая - как клиент. Сервер устанавливается на рабочих станциях, а клиент - на машинах администраторов. Хакеры могут использовать эти программы в своих целях, чтобы получить контроль над целевыми машинами и украсть конфиденциальную информацию.

Spoofing - это тип мошенничества, когда злоумышленник пытается получить несанкционированный доступ к системе или информации пользователя, делая вид, что является пользователем. Основная цель заключается в том, чтобы обмануть пользователя и получить доступ к банковскому счету, компьютерной системе или украсть личную информацию.

Sniffing - обнюхивание (с англ. sniffing) пакетов позволяет отдельным пользователям захватывать данные по мере их передачи по сети. Этот метод используется сетевыми специалистами для диагностики сетевых проблем, а также злоумышленниками для захвата незашифрованных данных, таких как пароли и имена пользователей. Если вы хотите сохранить конфиденциальность информации, работайте с зашифрованными протоколами и зашифровывайте все конфиденциальные данные, отправляемые через Интернет (например, электронные письма).

Отказ в обслуживании (DoS – атака) – основная цель этой атаки – перегрузить и в дальнейшем обрушить работу ресурса и сделать невозможным доступ для обычных пользователей. Для совершения DoS-атаки, злоумышленнику не нужно быть экспертом. Ее возможно осуществить с помощью простой команды ping. Обычно, когда опытные хакеры атакуют сайт с помощью DoS, они это делают не со своей машины, а устанавливают небольшие программы под названием «зомби» на некоторых компьютерах, которые находятся на промежуточном уровне в сетях. Во время атаки, они будут запускать эти программы удаленно и заставят промежуточные компьютеры атаковать одновременно.

Список литературы:

1. Чипига А.Ф. Информационная безопасность автоматизированных систем — М.: Гелиос АРВ, 2010. — 336 с.

2. Ярочкин В.И. Информационная безопасность: Учебник для вузов / В.И. Ярочкин. — М.: Акад. Проект, 2008. — 544 с.