ВИДЫ СЕТЕВЫХ АТАК, ОСУЩЕСТВЛЯЕМЫХ НА ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Чопик К. В.

Алефиренко В. М. – канд.техн.наук.,доцент

В статье рассмотрены основные виды сетевых атак. Проведено детальное рассмотрение каждой из атак. Приведена классификация атак, наиболее часто осуществляемых злоумышленниками.

На сегодняшний день с ростом популярности Интернета возникает беспрецедентная опасность разглашения персональных данных, критически важных корпоративных ресурсов и государственных тайн. Каждый день злоумышленники подвергают угрозе эти ресурсы, пытаясь получить к ним доступ при помощи специальных атак, которые постепенно становятся более изощренными. Чтобы своевременно обеспечить безопасность компьютера, важно знать, какого рода сетевые атаки могут ему угрожать.

Сетевые атаки делятся на две большие группы:

– пассивные;

– активные.

Активной называется такая атака, при которой противник имеет возможность модифицировать передаваемые сообщения и вставлять свои сообщения [1].

Активные атаки, в свою очередь, разделяются на следующие типы:

– атака Man In The Middle;

– DoS-атака;

– Reply-атака.

Атака Man In The Middle – это такой вид сетевой атаки, при которой злоумышленник тайно ретранслирует и при необходимости изменяет связь между двумя сторонами, которые считают, что они непосредственно общаются друг с другом [2].

Одним из примеров атаки Man In The Middle является активное прослушивание, при котором злоумышленник устанавливает независимые связи с жертвами и передаёт сообщения между ними. Тем самым он заставляет жертв поверить, что они разговаривают непосредственно друг с другом через частную связь, фактически же весь разговор управляется злоумышленником.

Существует несколько способов проведения атаки Man In The Middle. К ним относятся:

– создание двойника выходной точки, то есть при создании точной копии точки доступа, злоумышленник может получить доступ к каналу передачи данных;

– ARP-spoofing – атака основана на том, что протокол ARP не проверяет подлинности ARP-запросов и ARP-ответов, таким образом сетевое оборудование будет обрабатывать ARP-ответ без запроса [3];

– подмена DHCP-сервера основана на том, что у клиента нет возможности аутентифицировать DHCP-сервер.

DoS-атака существенно отличается от других видов атак. В данном случае цель злоумышленника не состоит в получении доступа к сети, а состоит в том, чтобы сеть стала недоступной для обычного использования за счет превышения допустимых пределов функционирования сети [4]. Реализация DoS-атак может быть проведена следующими способами:

– HTTP-флуд – представляет собой генерирование большого количества HTTP-запросов к серверу жертвы;

– SYN-флуд – принцип атаки заключается в том, что злоумышленник, посылая SYN-запросы, переполняет на сервере жертвы очередь на подключения;

– UDP-флуд – принцип атаки заключается в отправке множества UDP-пакетов на определённые или случайные номера портов удалённого сервера жертвы, который для каждого полученного пакета должен определить соответствующее приложение;

– ICMP-флуд – принцип атаки заключается в том, что компьютер-жертва получает особым образом подделанный эхо-запрос, после которого он перестает отвечать на запросы вовсе;

– MAC-флуд – принцип атаки заключается в отправке множества пустых Ethernet-фреймов с различными MAC-адресами, которыми заполняется память коммутатора.

Replay-атака – это пассивный захват данных с последующей их пересылкой для получения несанкционированного доступа. На самом деле Replay-атака является одним из вариантов фальсификации, но в силу того, что это один из наиболее распространенных вариантов атаки для получения несанкционированного доступа, его часто рассматривают как отдельный тип атаки [1].

Пассивной называется такая атака, при которой противник не имеет возможности модифицировать передаваемые сообщения и вставлять в информационный канал между отправителем и получателем свои сообщения. Целью пассивной атаки может быть только прослушивание передаваемых сообщений и анализ трафика [1].

Пассивные атаки могут быть следующие:

– Snooping (подслушивание);

– парольная атака;

– скомпрометированный ключ атаки.

Snooping означает подслушивание, то есть злоумышленник будет слышать разговор который происходит между двумя компьютерами в сети. Это может произойти в закрытой системе, а также через Интернет. При подслушивании конфиденциальные данные, передаваемые по сети, могут быть доступны для других пользователей.

При совершении парольных атак злоумышленник получает доступ к компьютеру и ресурсам сети путем получения пароля управления системой. Часто можно увидеть, что злоумышленник изменил сервер и конфигурацию сети и в некоторых случаях даже может удалить данные. Кроме того, данные могут передаваться в разные сети.

Для хранения конфиденциальных данных, может быть использован секретный ключ. Когда ключ находится в распоряжении злоумышленника, такой ключ становится скомпрометированным. Злоумышленник теперь будет иметь доступ к конфиденциальным данным и может внести изменения в данные. Однако, существует также вероятность того, что злоумышленник будет пробовать различные перестановки и комбинации ключа для доступа к другим наборам конфиденциальных данных [5].

Проведенная классификация сетевых атак представлена на рисунке 1.

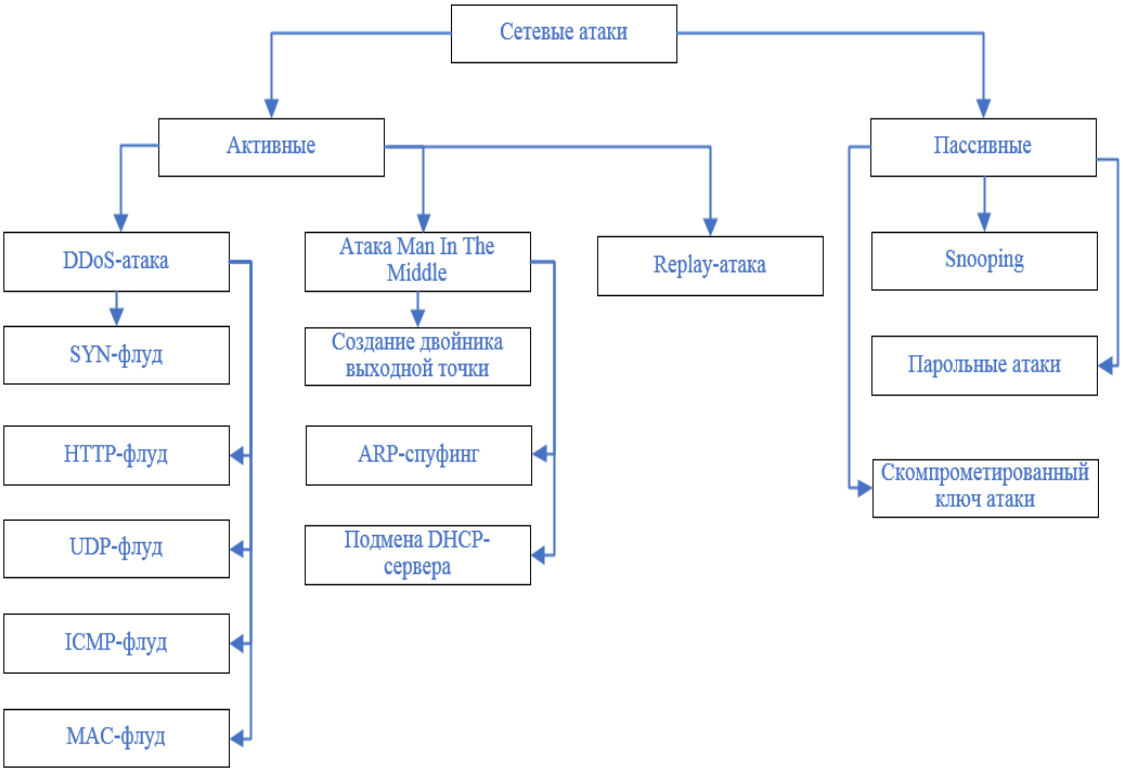

Рисунок 1 – Классификация сетевых атак

В заключение можно отметить, что такая классификация сетевых атак на информационную инфраструктуру достаточно полно отражает представление об имеющихся их видах, что позволяет более оперативно обнаруживать и предотвращать нарушения безопасности информационной инфраструктуры.

Список использованных источников:

1. Классификация сетевых атак [Электронный ресурс]. – Режим доступа: https://helpiks.org/8-55790.html.

2. Атака «man in the middle» [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/.

3. Атака канального уровня ARP-spoofing и как защитить коммутатор Cisco [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/192022/.

4. Классификация сетевых атак [Электронный ресурс]. – Режим доступа: https://studbooks.net/2261861/informatika/klassifikatsiya_setevyh_atak.

5. Виды компьютерных атак [Электронный ресурс]. – Режим доступа: https://kompkimi.ru/programms-2/sistemnye-programmy/zashhita-pk/vidy-kompyuternyx-atak#i.