СЕТЕВЫЕ УГРОЗЫ

Гладкая В. С., Гельдымурадов С., Дроздов В. С.

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

Розум Г. А. – м-р техники и технологии,
ассист. каф ИПиЭ,

Рассмотрены сетевые угрозы, методы анализа и технологии обнаружения сетевых атак.

Удалённая сетевая атака — информационное разрушающее воздействие на распределённую вычислительную систему (РВС), осуществляемое программно по каналам связи.

Для организации коммуникаций в неоднородной сетевой среде применяются протоколы TCP/IP, обеспечивая совместимость между компьютерами разных типов. Данный набор протоколов завоевал популярность благодаря совместимости и предоставлению доступа к ресурсам глобальной сети Интернет и стал стандартом для межсетевого взаимодействия. Однако повсеместное распространение стека протоколов TCP/IP обнажило и его слабые стороны. В особенности из-за этого удалённым атакам подвержены распределённые системы, поскольку их компоненты обычно используют открытые каналы передачи данных, и нарушитель может не только проводить пассивное прослушивание передаваемой информации, но и модифицировать передаваемый трафик.

Трудность выявления проведения удалённой атаки и относительная простота проведения(из-за избыточной функциональности современных систем) выводит этот вид неправомерных действий на первое место по степени опасности и препятствует своевременному реагированию на осуществлённую угрозу, в результате чего у нарушителя увеличиваются шансы успешной реализации атаки. Пассивное воздействие на распределённую вычислительную систему (РВС) представляет собой некоторое воздействие, не оказывающее прямого влияния на работу системы, но в то же время способное нарушить её политику безопасности. Отсутствие прямого влияния на работу РВС приводит именно к тому, что пассивное удалённое воздействие (ПУВ) трудно обнаружить. Возможным примером типового ПУВ в РВС служит прослушивание канала связи в сети.

Активное воздействие на РВС — воздействие, оказывающее прямое влияние на работу самой системы (нарушение работоспособности, изменение конфигурации РВС и т. д.), которое нарушает политику безопасности, принятую в ней. Активными воздействиями являются почти все типы удалённых атак: в саму природу наносящего ущерб воздействия включается активное начало. Явное отличие активного воздействия от пассивного — принципиальная возможность его обнаружения, так как в результате его осуществления в системе происходят некоторые изменения. При пассивном же воздействии, не остается совершенно никаких следов (из-за того, что атакующий просмотрит чужое сообщение в системе, в тот же момент не изменится собственно ничего).

Этот признак, по которому производится классификация, по сути есть прямая проекция трех базовых разновидностей угроз — отказа в обслуживании, раскрытия и нарушения целостности.

Главная цель при любой атаке — получение несанкционированного доступа к информации. Существуют два принципиальных варианта получения информации: искажение и перехват. Вариант перехвата информации означает получение к ней доступа без возможности её изменения. Перехват информации приводит, следовательно, к нарушению её конфиденциальности. Прослушивание канала в сети — пример перехвата информации. В этом случае имеется нелегитимный доступ к информации без возможных вариантов её подмены. Очевидно, что нарушение конфиденциальности информации относится к пассивным воздействиям.

Возможность подмены информации следует понимать либо как полный контроль над потоком информации между объектами системы, либо возможность передачи различных сообщений от чужого имени. Следовательно, понятно, что подмена информации приводит к нарушению её целостности. Такое информационное разрушающее воздействие есть характерный пример активного воздействия. Примером же удалённой атаки, предназначенной для нарушения целостности информации, может послужить удалённая атака (УА) «Ложный объект РВС».

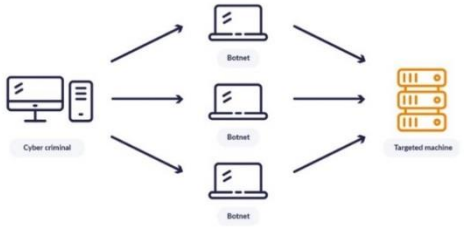

Рисунок 1 – иллюстрация схемы DDOS атаки на компьютер жертвы

Список использованных источников:

1. Медведовский И. Д., Семьянов П. В., Платонов В. В. АТАКА ЧЕРЕЗ INTERNET
2. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей.
3. Семенов Ю. А. Протоколы и ресурсы Internet. — М.: Радио и связь,