УДК 004

СЕТЕВЫЕ УДАЛЕННЫЕ АТАКИ

Асхатова Ляйсан Ильдаровна
канд. экон. наук
Казанский федеральный университет, Казань

Галимов Эдвард Раифович
студент

Габдуллин Ильдар Масхутович
студент
Казанский национальный исследовательский технический университет им. А.Н. Туполева, Казань

author@apriori-journal.ru

Аннотация. Рассматривается классификация сетевых удаленных атак.

Ключевые слова: атака; сегмент; сеть.

NETWORK REMOTE ATTACKS

Askhatova Laysan Ildarovna
candidate of economical sciences
Kazan Federal University, Kazan

Galimov Edward Raifovich
student

Gabdullin Ildar Maskhutovich
student
Kazan National Research Technical University, Kazan

Abstract. The classification of network remote attacks.

Key words: attack; segment; the network.

В настоящее время создаются транснациональные корпорации, успех которых зависит от скорости обмена информацией между филиалами. Проблема скорости передачи информации практически решена, но здесь возникает проблема безопасности передаваемых данных.

Основная цель любой классификации состоит в том, чтобы предложить такие классификационные признаки, используя которые можно наиболее точно описать классифицируемые явления или объекты. Классификация сетевых удаленных атак представлена на рис. 1.

1. По характеру воздействия:

- пассивное (класс 1.1).
- активное (класс 1.2).

Пассивным воздействием на распределенную вычислительную систему называется воздействие, которое не оказывает непосредственного влияния на работу системы, но может нарушать ее политику безопасности. Именно отсутствие непосредственного влияния на работу распределенной ВС приводит к тому, что пассивное удаленное воздействие практически невозможно обнаружить. Примером пассивного типового удаленного воздействия в РВС служит прослушивание канала связи в сети.

Под активным воздействием на распределенную ВС понимается воздействие, оказывающее непосредственное влияние на работу системы (изменение конфигурации РВС, нарушение работоспособности и т. д.) и нарушающее принятую в ней политику безопасности [2]. Практически все типы удаленных атак являются активными воздействиями. Это связано с тем, что в самой природе разрушающего воздействия содержится активное начало. Очевидной особенностью активного воздействия по сравнению с пассивным является принципиальная возможность его обнаружения (естественно, с большей или меньшей степенью сложности), так как в результате его осуществления в системе происходят определенные изменения.

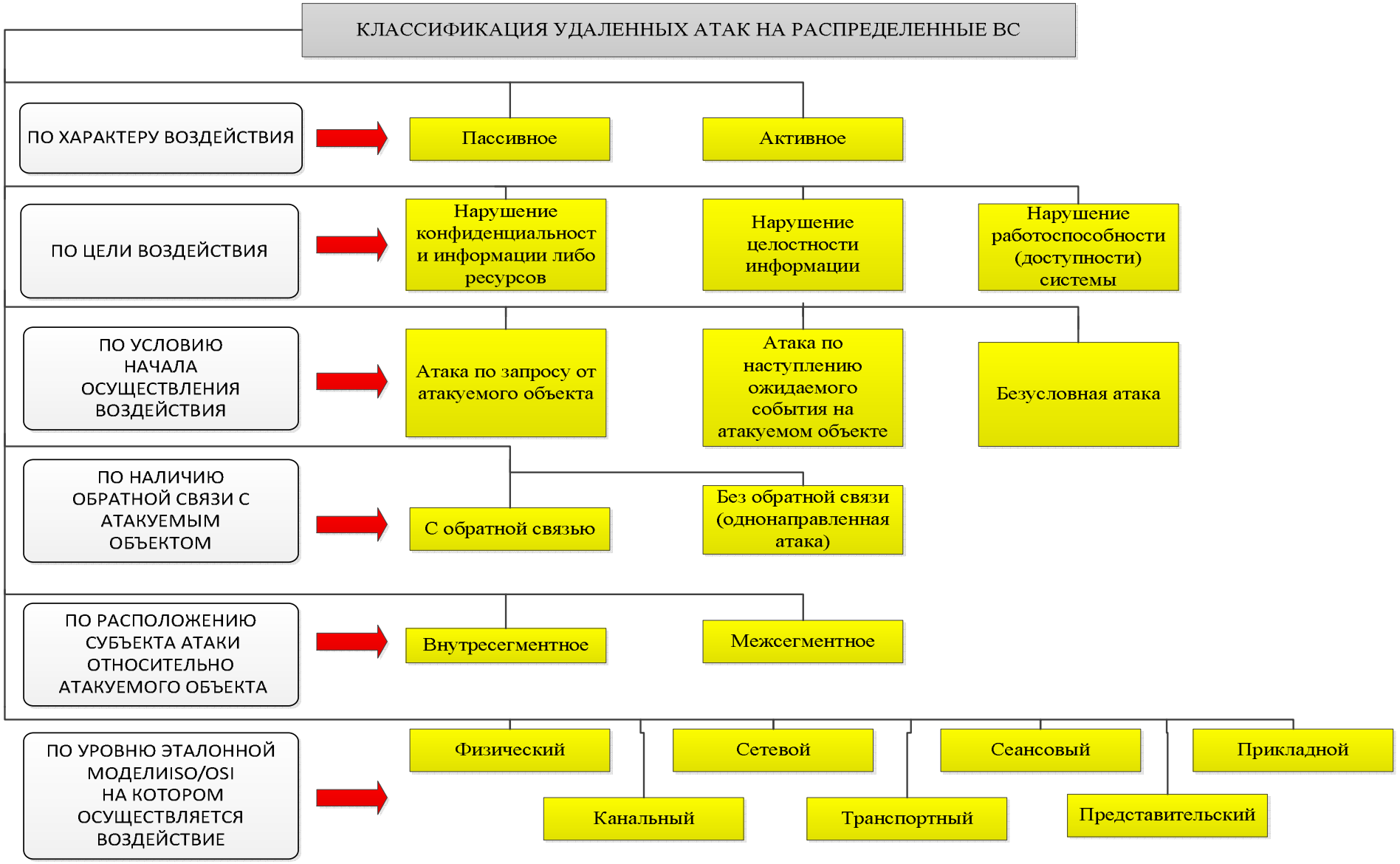

Рис. 1. Классификация сетевых удаленных атак

2. По цели воздействия:

- нарушение конфиденциальности информации либо ресурсов системы (класс 2.1).
- нарушение целостности информации (класс 2.2).
- нарушение работоспособности (доступности) системы (класс 2.3).

Основная цель практически любой атаки - получить несанкционированный доступ к информации. Существуют две принципиальные возможности доступа к информации: перехват и искажение. Возможность перехвата информации означает получение к ней доступа, но невозможность ее модификации. Следовательно, перехват информации ведет к нарушению ее конфиденциальности. Примером перехвата информации может служить прослушивание канала в сети. Очевидно также, что нарушение конфиденциальности информации является пассивным воздействием.

Возможность искажения информации означает либо полный контроль над информационным потоком между объектами системы, либо возможность передачи сообщений от имени другого объекта. Таким образом, очевидно, что искажение информации ведет к нарушению ее целостности. Данное информационное разрушающее воздействие представляет собой яркий пример активного воздействия. Примером удаленной атаки, цель которой нарушение целостности информации, может служить типовая удаленная атака «Ложный объект РВС».

3. По условию начала осуществления воздействия.

Удаленное воздействие, также как и любое другое, может начать осуществляться только при определенных условиях. В распределенных ВС существуют три вида условий начала осуществления удаленной атаки:

- Атака по запросу от атакуемого объекта (класс 3.1).

В этом случае атакующий ожидает передачи от потенциальной цели атаки запроса определенного типа, который и будет условием начала осуществления воздействия.

- Атака по наступлению ожидаемого события на атакуемом объекте (класс 3.2).

В этом случае атакующий осуществляет постоянное наблюдение за состоянием операционной системы удаленной цели атаки и при возникновении определенного события в этой системе начинает воздействие.

- Безусловная атака (класс 3.3).

В этом случае начало осуществления атаки безусловно по отношению к цели атаки, то есть атака осуществляется немедленно и безотносительно к состоянию системы и атакуемого объекта.

4. По наличию обратной связи с атакуемым объектом:

- с обратной связью (класс 4.1).
- без обратной связи (однонаправленная атака) (класс 4.2).

Атаки без обратной связи обычно осуществляются передачей на атакуемый объект одиночных запросов, ответы на которые атакующему не нужны. Примером однонаправленных атак является типовая УА «Отказ в обслуживании».

5. По расположению субъекта атаки относительно атакуемого объекта:

- внутрисегментное (класс 5.1).
- межсегментное (класс 5.2).

Рассмотрим ряд определений:

Субъект атаки (или источник атаки) – это атакующая программа или оператор, непосредственно осуществляющие воздействие.

Сегмент сети – физическое объединение хостов. Например, сегмент сети образуют совокупность хостов, подключенных к серверу по схеме «общая шина». При такой схеме подключения каждый хост имеет возможность подвергать анализу любой пакет в своем сегменте.

6. По уровню эталонной модели ISO/OSI, на котором осуществляется воздействие:

- физический (класс 6.1).
- канальный (класс 6.2).
- сетевой (класс 6.3).
- транспортный (класс 6.4).
- сеансовый (класс 6.5).
- представительный (класс 6.6).
- прикладной (класс 6.7).