Захаров Андрей Иванович, аспирант
Научный руководитель: Лидский Эмануил Аркадьевич, проф., д-р техн. наук

ПРИНЦИПЫ РАЗРАБОТКИ СТРАТЕГИИ АТАКИ И ЗАЩИТЫ В КОМПЬЮТЕРНЫХ СЕТЯХ

Для создания эффективной политики безопасности важно уделить повышенное внимание оценке рисков или, другими словами, провести качественный анализ ситуации при использовании злоумышленником различных стратегий нападения.

Можно выделить три основных стратегии, которые может использовать атакующий для достижения поставленной им цели.

Первый вид стратегии подразумевает атаку "в лоб". Это означает, что злоумышленник будет пытаться осуществить атаку на представленные сетевые ресурсы, доступные в сетях общего пользования. При данном варианте развития событий злоумышленник будет вынужден провести информационную разведку с целью обнаружения, во-первых, доступных сетевых ресурсов на хосте потенциальной жертвы, во-вторых, оценить степень защиты на уровне сетевых протоколов. Следующим шагом будет поиск известных уязвимостей, присущих программному обеспечению, которое было выявлено в процессе разведки. Этот этап является критическим для данной стратегии нападения, поскольку именно наличие или отсутствие уязвимостей в сетевых ресурсах жертвы будет определять, возможно ли использовать брешь в защите для проникновения в систему. В случае обнаружения злоумышленником таких потенциально уязвимых мест на третьем этапе осуществляется попытка использовать найденные уязвимости. Здесь атакующий идет самым простым путем. Из всех найденных дыр выбирается именно та, использование которой позволит злоумышленнику получить максимальный уровень доступа после проникновения в систему. Тем не менее, иногда злоумышленник пытается эксплуатировать некоторые уязвимости наугад, поскольку невозможно со 100% вероятностью определить, присутствует ли та или иная уязвимость в системе.

Вторая стратегия основана на троянском проникновении. Здесь целью атаки являются клиентские программы, явно недоступные из внешней сети.

Речь идет не столько о компьютерных вирусах, сколько о специально подготовленных web-ресурсах с активным содержимым, на которые заманивается будущая жертва. Попадая на такой ресурс, на компьютере жертвы запускаются скрипты, специально созданные для эксплуатации конкретной уязвимости программы, которая выступила инициатором соединения. Обычно жертва, ничего не подозревая, загружает себе на компьютер программу, которая устанавливает скрытый канал соединения с "хозяином" и далее работает под его управлением. Этот вариант существенно труднее реализуем, но он и гораздо более опасен, поскольку предоставляет злоумышленнику практически полный доступ в локальную сеть.

Третья стратегия не всегда ставит целью непосредственное проникновение в систему. Зачастую могут решаться периферийные задачи, либо это может быть сопутствующим действием в процессе взлома. Этот тип атак называется "отказ в обслуживании". Проведение данной атаки позволяет злоумышленнику на время, либо полностью вывести атакуемый хост из рабочего состояния, тем самым саботировав работу сервисов, запущенных на хосте, либо допускает подмену реального сервера ложным. Данный тип атаки наиболее опасен не столько для информационных ресурсов, сколько для сетевых сервисов, предоставленных в общее пользование. Такая ситуация может возникнуть, например, у Интернет-банков.

Для того чтобы построить эффективную систему защиты, необходимо оценить те варианты нападения, которые представляют максимальную угрозу. Трем различным стратегиям злоумышленника защищаемый хост может противопоставить одну-единственную стратегию обороны. Под обороной здесь понимается не столько готовая инфраструктура, сколько концепция безопасности конечных информационных ресурсов – то есть программ. Типичное предприятие, сталкивающееся с проблемой безопасности, не имеет таких ресурсов, которыми, например, располагают банки, поэтому решение, связанное с полным перекрытием всех возможных путей атаки, видится нереализуемым.

Рациональный путь – перекрытие наиболее опасных для предприятия направлений атаки, которыми может воспользоваться злоумышленник.

Для решения этой задачи необходим стандарт, с помощью которого была бы возможность адресовать конкретные уязвимости в контексте воздействия атаки на защиту.

Наиболее удобным можно считать международный стандарт CVE – Common Vulnerabilities and Exposures и построенную на его основе базу данных по известным уязвимостям – ICAT. В базе ICAT каждой уязвимости сопоставлено множество характеристик ее проявления. Среди них можно выделить: условие атаки, тип потерь, тип уязвимости, затронутое программное обеспечение и т.д.

Используя эти характеристики, возможно описать стратегию нападения и защиты в терминах стандарта CVE. Поскольку три основные стратегии нападения основаны на различных целях, необходимо провести первичную декомпозицию базы данных, с целью разделения всех записей на три группы, каждая из которых будет содержать все возможные воплощения для каждой стратегии.

Дальнейшая декомпозиция каждой из трех выборок позволит нам выделять возможные реализации соответствующей стратегии.

Для первой стратегии поведение злоумышленника можно представить в виде дальнейшей декомпозиции соответствующей выборки, используя в качестве ключа группу параметров "Тип уязвимости". Для проведения атаки злоумышленник будет выбирать именно такие уязвимости, которые с одной стороны проще всего эксплуатировать, а с другой стороны, те, которые позволят получить максимальный уровень доступа в системе. Учитывая, что в настоящее время в Интернете можно без труда найти множество информации, посвященной взлому, злоумышленник с подавляющей вероятностью остановится на ва-

риантах, оптимально сочетающих оба фактора. На примере базы данных ICAT выбрать подходящую группу уязвимостей можно с помощью критерия LT_Security_protection и четырех критериев VT_Input_validation_error,VT_Buffer_overflow, VT_Boundary_condition_error и VT_Exceptional_condition_error, а также учитывая, что для данной стратегии возможна только удаленная атака, чему соответствует критерий AR_Launch_remotely.

Декомпозиция второй группы, соответствующей троянскому проникновению, будет осуществляться с использованием других критериев в качестве ключей. Ключом выступит, во-первых, "название программного обеспечения" – перечень очень мал, что позволит существенно сократить выборку. Затем критерий EC_Non_server_application и LT_Security_protection. Последний критерий указывает на то, что в обход системы безопасности на клиентской машине будет выполнено активное содержимое загруженного ресурса. Другим вариантом может стать использование критерия LT_Obtain_all_priv, что фактически будет означать мгновенное получение удаленного контроля над системой.

В третьей группе поведение злоумышленника, ставящего цель провести атаку отказа в обслуживании, можно предсказать, используя критерий LT_Availability в качестве ключа для дальнейшей декомпозиции.

Задачей защиты является выстраивание собственной стратегии обороны, эффективной против любой из трех стратегий нападения. Используя базу ICAT, защита может разработать комбинированную стратегию, целью которой является предсказание действий злоумышленника, наиболее опасных для конкретной защищаемой системы. Цель будет достигнута, если действия злоумышленника буду предсказаны с заданной точностью.

В процессе испытаний эффективность взаимодействия нападение-защита удобнее всего оценивать с помощью методов теории игр, что намечает путь дальнейшего исследования.