ТЕОРЕТИКО-ИГРОВОЙ ПОДХОД К РЕШЕНИЮ ЗАДАЧИ ОПТИМАЛЬНОГО РАЗМЕЩЕНИЯ ЛОЖНЫХ ЦЕЛЕЙ В КОМПЬЮТЕРНОЙ СЕТИ ДЛЯ ОБНАРУЖЕНИЯ НАПРАВЛЕННЫХ АТАК

Ю.В. Алейнов

Самарский государственный аэрокосмический университет имени академика С.П. Королёва (национальный исследовательский университет), Самара, Россия

В статье поставлена и рассмотрена задача оптимального размещения ложных целей в компьютерной сети для обнаружения атак направленного типа (*APT*). Предложена теоретико-игровая модель конфликта атакующего и системы защиты. Определены способы представления множеств стратегий игроков и функции выигрыша, предложен критерий оптимальности стратегий.

Ключевые слова: *APT*, *Honeypot*, направленные атаки, обнаружение вторжений, оптимальное размещение ложных целей, теория игр.

Введение

В настоящее время проблема обнаружения направленных сетевых атак (APT) становится все более актуальной. Традиционные средства обнаружения вторжений (ОВ) малоэффективны в условиях направленных атак из-за высокой степени вариативности поведения злоумышленника, не позволяющей достоверно распознавать его активность [1].

Наряду с традиционными способами ОВ, перспективным является способ, основанный на внедрении в компьютерную сеть специальных ложных объектов (Honeypot). Такие объекты с точки зрения нарушителя не отличаются от других объектов сети, но их участие в нормальных производственных процессах исключено. Это позволяет более эффективно обнаруживать атаки, затрагивающие подобные приманки [2].

Одной из главных проблем данного способа ОВ является его пассивность, которая проявляется в том, что нарушитель не может быть обнаружен до тех пор, пока он не атакует приманку [2,3]. Считая, что выбор цели из множества однотипных сетевых объектов совершается случайным образом, можно говорить о вероятности атаки на ложную цель как о показателе эффективности ОВ данным способом. Эта вероятность, очевидно, зависит от многих факторов, среди которых в условиях направленной атаки можно особо выделить расположение ложных целей в защищаемой сети.

Таким образом, актуальной является задача наилучшего, с точки зрения вероятности обнаружения, расположения ложных целей в сети в условиях противоборства нарушителя, осуществляющего направленную атаку, и системы защиты сети. В данной статье для решения этой задачи предлагается использовать методы теории игр.

1. Задача оптимального размещения ложных целей

Под расположением ложных целей в сети предлагается понимать, прежде всего, их размещение относительно границ зон межсетевого экрана (МЭ). Работающий в сети МЭ влияет на доступность одних сетевых узлов относительно других и относительно внешнего нарушителя. В зависимости от того, к каким элементам сети имеет доступ потенциальный нарушитель, ему доступны для атаки различные подмножества сетевых узлов. В ходе атаки злоумышленник может захватывать контроль над новыми узлами сети, тем самым расширяя подмножество доступных ему для атаки целей [1,4].

Сеть, разделенную на зоны межсетевого экрана, удобно представлять в виде графа, вершины которого соответствуют зонам межсетевого экрана, а ребра проводятся между вершинами в том случае, если существует возможность передачи данных между узлами в соответствующих зонах (рис. 1).

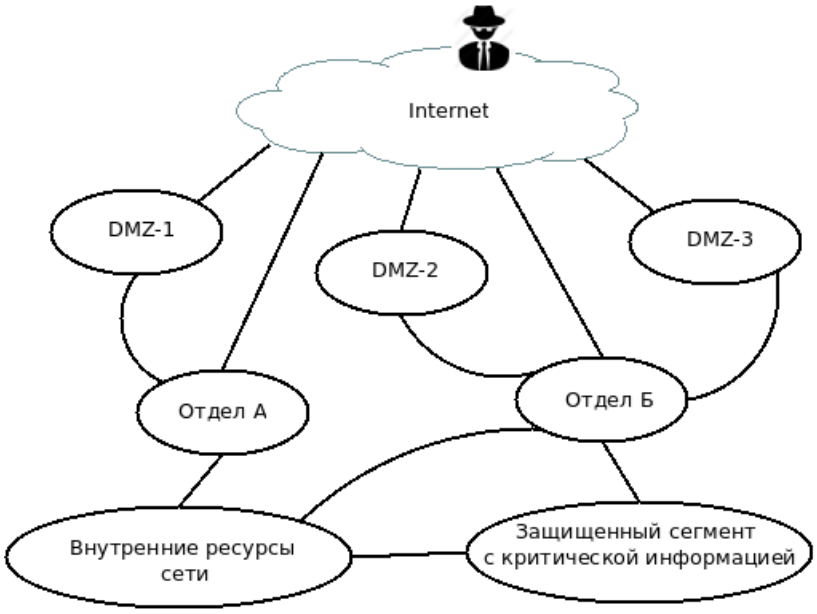

Рис.1. Граф, изображающий отношения доступности между зонами МЭ.

Таким образом, задача оптимального расположения ложных целей в сети сводится к задаче размещения заданного числа ложных целей по вершинам графа, изображающего сеть, так, чтобы вероятность обнаружения была максимальной.

2. Теоретико-игровой подход к решению задачи размещения ложных целей

Конфликт, в котором принимают участие рациональные стороны, способные учитывать влияние собственных действий на действия противника, целесообразно анализировать методами теории игр [5].

Противоборство нарушителя и системы защиты сети в ходе направленной атаки на сеть – это, очевидно, конфликтная ситуация, в которой участвуют две стороны. Цель нарушителя – построить такой маршрут в графе, изображающем сеть, чтобы вероятность его обнаружения при движении по этому маршруту была минимальной. Система защиты, путем распределения ложных целей по зонам межсетевого экрана, старается достичь про-

тивоположной цели. Таким образом, противоборство нарушителя и системы защиты представляет собой антагонистический конфликт двух игроков, который хорошо описывается с помощью аппарата теории игр [5].

Формально, пусть $Z_1, Z_2, \ldots, Z_k$ – зоны межсетевого экрана. Пусть целью нарушителя является компрометация какого-либо сетевого узла из зоны межсетевого экрана Z_T, а начальное положение нарушителя таково, что он может атаковать только узлы, находящиеся в зоне Z_0. Тогда множество стратегий нарушителя A представляет собой все возможные пути из вершины, соответствующей зоне Z_0 в вершину, соответствующую зоне Z_T.

Стратегии стороны защиты могут быть определены следующим образом. Рассмотрим вектор $\vec{h} = (h_1, h_2, \ldots, h_k)$, каждая координата которого соответствует одной из зон межсетевого экрана по следующему правилу: $h_i = |Z_i|_{HP}$, где $|Z_i|_{HP}$ – количество ложных целей в зоне Z_i, $i = 1..k$. Пусть имеющихся ресурсов в сети достаточно для обеспечения работы N ложных целей. Тогда множество D стратегий системы защиты совпадает с множеством всех векторов h ∈ ℤk, таких, что $\sum_{i=1}^{k} h_i = N$. В качестве платежной функции предлагается использовать значение $P_{Обн} = P_{Обн}(a, d)$ вероятности обнаружения атаки при фиксированных маршруте нарушителя a ∈ A и размещении d ∈ D ложных целей стороной защиты.

В качестве решения матричной игры $G = \langle A, D, P_{Обн}(a, d) \rangle$ с точки зрения системы защиты предлагается использовать осторожную (минимаксную) стратегию. Такая стратегия является оптимальной с точки зрения критерия Вальда (критерий крайнего пессимизма), который уместно применять в условиях полного отсутствия информации о стратегии противника в антагонистическом конфликте [5]. Очевидно, в общем случае сторона защиты не имеет достоверной информации о нарушителе и доступных ему для атаки целях. Применение осторожной стратегии гарантирует системе защиты обнаружение вторжения с вероятностью не ниже некоторого заранее заданного предела, что может быть использовано для количественной оценки эффективности обнаружения вторжений системой ложных целей.

Заключение

В данной статье предложена схема теоретико-игровой модели для решения задачи оптимального размещения ложных сетевых объектов с целью обнаружения атак направленного типа. Предложены способы представления стратегий нарушителя и системы защиты, а также функции выигрыша.

Дальнейшее исследование рассмотренного вопроса должно включать построение модели, учитывающей возможность наличия в сети нескольких категорий ресурсов, представляющих различный интерес для злоумышленника, а также возможность наличия нескольких неравноправных точек ввода нарушителя в сеть.

Литература

1. Sood, A.K., Enbody, R.J. Targeted Cyberattacks: A Superset of Advanced Persistent Threats // Security & Privacy, IEEE (Volume:11 , Issue: 1) . IEEE, 2013.
2. Медведовский И. Д., Семьянов П. В., Леонов Д. Г. Атака на Internet" ДМК Пресс" Издательство:- 2006. 2-ое, перераб. и доп //Издание:-336 с.
3. Bringer M.L., Chelmecki, C.A., Fujinoki H A Survey: Recent Advances and Future Trends in Honeypot Research. // International Journal of Computer Network & Information Security. 2012. №4.
4. Piggin R. Cyber security trends: What should keep CEOs awake at night //International Journal of Critical Infrastructure Protection. – 2016.
5. Мазалов В. В. и др. Математическая теория игр и её приложения //СПб.: Лань. – 2010.