# Краткое описание разрабатываемой системы

В процессе проведения тестирования на проникновение производится построение графа атак.

G = (V, A) – ориентированный граф, где V – непустое множество узлов, A – множество триплетов, называемых ребрами, вида , где – идентификатор уязвимости, присутствующей на узле . Направление дуги задаётся последовательностью следования узлов в записи.

Где – угроза попадания злоумышленником на узел , – узел графа, достижимый из , – критичность захвата узла , – подмножество достижимых узлов из .

Узел достижим из хотя бы 1 путь из в , *.*

Где – коэффициент зависящий от типа устройства. Можно использовать базу nmap классификации устройств (28 штук) и сопоставить каждому коэффициент по личным соображениям. Например, от 1 до 2. – критичность одного сервиса. Каждому сервису или типу сервисов можно сопоставить конкретную критичность компроментации, сервис узла .

Угроза компрометации системы на k-ом шаге поиска контрмер рассчитывается следующим образом:

Далее необходимо найти такую уязвимость , при удалении которой максимально снизится угроза компрометации системы, то есть:

Для подсчета необходимо в первую очередь определить множество . Для этого обойти граф (можно использовать любой алгоритм обхода, пока что используется обход в ширину (DFS)), начиная от узла , и пометить все достижимые узлы. Сложность алгоритма обхода Таким образом, сложность подсчета в худшем случае равняется

Данный алгоритм можно оптимизировать следующим образом. Представим, что каждый узел исходного графа принадлежит подграфу одного из двух типов – компоненте сильной связности или N-арному дереву.

Ориентированный граф называется сильно связным, если любые два его узла сильно связны. Два узла и любого графа сильно связны, если существует ориентированный путь из в и ориентированный путь из в . Компонентами сильной связности орграфа называются его максимальные по включению сильно связные подграфы. Областью сильной связности называется множество узлов компоненты сильной связности.

Осуществим поиск областей сильной связности (обозначим их , например, с помощью алгоритма Косарайю, который использует двойной обход в глубину, следовательно его сложность O(2|V| + 2|A|).

Ориентированное N-арное дерево — ацикличный орграф (ориентированный граф, не содержащий циклов), в котором только один узел имеет нулевую степень захода (в него не ведут дуги), а все остальные узлы имеют степень захода не больше N. Узел с нулевой степенью захода называется корнем дерева, узлы с нулевой степенью исхода (из которых не исходит ни одна дуга) называются концевыми узлами или листьями. Обозначим их . Значение N может отличаться от дерева к дереву.

При этом в N-арное дерево включаются только те узлы, входящие дуги которых направлены от узлов того же дерева. Исключение может составлять только корневой узел. (доп условие)

В первую очередь производится поиск всех компонент сильной связности и соответствующих им областей сильной связности. Проиллюстрируем данный щаг на примере. Считаем, что все узлы имеют по 1 уязвимости, вследствие чего дуги не подписаны (рисунок Х).



Рисунок Х – Пример ориентированного графа

Обозначим на графе компоненты сильной связности и N-арные деревья (рисунок Х). Компоненты сильной связности обозначены зеленым цветом, N-арные деревья – оранжевым.



Рисунок Х – Иллюстрация поиска подграфов двух типов

Рассмотрим некоторые свойства полученных подграфов:

* Из определения компоненты сильной связности следует, что в ней существуют маршруты из любого узла компоненты в любой другой. Отсюда:

– k-ая область сильной связности

Следовательно, для каждой области сильной связности достаточно посчитать единственный раз.

* Из определения компоненты сильной связности и N-арного дерева следует, что попав в любую из данных компонент гарантируется прохождение по всем узлам подграфа. При этом в N-арном дереве существует только один корневой узел, следовательно вход в данный подграф возможен исключительно через него, что позволит пройти по всем узлам данного дерева. Следовательно при достижении корневого узла такого дерева нет необходимости в пересчете критичности его узлов. Достаточно сделать это один раз:

– критичность захвата подграфа

* Ребра исходного графа распределяются на 3 категории:
  + Ребра, принадлежащие компонентам сильной связности;
  + Ребра, принадлежащие N-арным деревьям;
  + Ребра, связывающие различные подграфы.

В связи с этим при удалении ребер возможны 3 ситуации:

1. Если ребро находилось в компоненте сильной связности или N-арном дереве, необходимо осуществить перераспределение узлов данной компоненты по новым подграфам сильной связности и N-арным деревьям. Также необходимо осуществить новые расчёты параметров и
2. Если ребро соединяло две компоненты, нет необходимости в пересчете параметров подграфов.

Исходя из вышеописанных свойств можно провести следующее преобразование: представим все компоненты сильной связности и N-арные деревья как узлы нового графа, которые включают в себя все входящие и все исходящие дуги исходного подграфа. При этом новое значение критичности узла высчитывается по формуле:

А новое значение угрозы попадания на узел

Где – k-ая область сильной связности

Таким образом, при определении значения угрозы компрометации системы можно будет воспользоваться результатами расчетов, полученных в процессе вычисления угрозы компрометации системы что весьма критично, так рассматриваемая структура сетевой организации очень часто выглядит так, что . Следовательно перебор всех возможных решений займет продолжительное время.

(ОЦЕНИТЬ СЛОЖНОСТЬ)