(1 слайд – титульник)

(2 слайд – Актуальность)

Сетевая инфраструктура организации – это почти всегда высокодинамичная структура, состоящая из множества узлов и сервисов, связанных между собой.

Для анализа защищенности сетевой инфраструктуры чаще всего используется тестирование на проникновение.

Формируемые в результате тистирования описания уязвимостей и способы их устранения используются организациями для сокращения своих рисков.

Однако на практике чаще всего устраняют только те уязвимости, которые способствуют проникновению злоумышленника в сеть, либо компрометации наиболее значимых узлов, оставляя тем самым внутри сети цепочки уязвимостей, которыми может воспользоваться любой вновь папавший в сеть.

Подобная ситуация объясняется сложностью методик и недостатком сведений о системе для проведения должного ранжирования рисков. В данной работе предлагается новый подход, основанный на предположении, что любой из узлов системы в дальнейшем может стать новой точкой входа.

(3 слайд – цели и задачи)

Цель работы – разработать методики оценки защищенности сетевой инфраструктуры и выбора защитных мер на основе графов атак

Задачи:

-Определить способы идентификации узлов и узявимостей;

-Проанализировать применимость графов атак в задаче оценки защищенности;

-Разработать методики

-Реализовать методики

-Оценить их эффективность

(4 слайд – этапы тестирования на проникновение)

Тестирование на проникновение состоит из 4 основных этапов:

-Планирование;

-Сбор информации;

-Проникновение;

-Составление отчёта;

На этапе планирования выбираются цели тестирования, определяются основные ограничения и требования;

На этапе сбора информации проводится поиск узлов системы, сбор информации об основном управляющем персонале, детальный анализ обнаруженных узлов, включающий: определение версии ОС, типов и версии запущенных сервисов, типа самого узла, описывающего его место в системе и многое другое. Полученные на данном этапе сведения, могут быть использованы тестировщиком в процессе оценки защищенности системы. Подобный подход позволяет избежать временных задержек, которые требуются для получения дополнительной информации о системе, которую тестировщик чаще всего получить не может.

На этапе проникновения строятся и апробируются потенциальные веторы атак, на основании информации, полученной на этапе сбора информации. В результате эксплуатации уязвимостей может быть получена информация об учетных записях пользователей, сервисов, исходные коды проектов организации, в которых также могут находиться записи об учётных записях и различные ключи доступа, а также, что немаловажно, доступ к другим подсетям организации.

Этап составления отчётности включает в себя документационную работу по мероприятиям, проводимым на всех упомянутых этапах. Кроме того, она может описывать различные риски, выявленные проблемы, уязвимые области (использованные или нет) и предлагаемые для устранения недостатков решения.

Этапы 2 и 3 выполняются циклично, в основном после получения дополнительной информации, полученной после апробации очередной уязвимости.

(5 слайд – Методики оценки защищенности сетевой инфраструктуры)

Методики оценки защищенности позволяют представить уровень защищенности системы в форме показателей защищенности. Показатель – мера измерения, дающая качественную или количественную оценку определенных атрибутов.

Количественные методики оценки защищенности позволяют измерить риск в терминах частоты нежелательных событий или денежных единиц, в то время как качественные показатели позволяют ранжировать риски относительно друг друга на основе уязвимостей, угроз и защитных мер в терминах словесного описания уровня риска (низкий, средний, высокий и т.д.).

Существует также и третий тип методик – смешанные. Данные методики сопоставляют любому качественному уровню определенный числовой диапазон.

К качественным методикам относятся: COBRA, OCTAVE, FRAP

К количественным: RiskWatch, ГРИФ, MSAT;

К смешанным можно отнести: CRAMM и методики, основанные на графах атак.

(6 слайд – Графы атак)

Графы атак применяются для анализа того, каким образом может развиваться атака внутри сети организации посредством эксплуатации обнаруженных в системе уязвимостей. Графы отражают все возможные пути атак, и могут также быть использованы для отображения состояний системы в соответствии с использованными уязвимостями.

Можно выделить следующие виды графов атак:

- Полный граф атак – узлы такого графа представляют собой состояния, а ребра – уязвимости. Такие графы иллюстрируют каждую возможную трассу атак, которую может реализовать нарушитель. Они имеют сложность O(n!), что негативно сказывается на их размере и, следовательно, на скорости вычислений.

- Граф предсказаний – узлы и ребра представляют собой те же сущности, что и в полном графе. Каждый узел попадает в граф предсказаний, если ни один его предок не использует ту же уязвимость для попадания в то же состояние. Данные графы не имеют недостатка полного графа по скорости построения и могут правильно прогнозировать влияние удаления любой из уязвимостей в сети.

- MP-граф (граф со множеством предусловий) – содержит три типа узлов: уязвимости, состояния и предусловия. Для отображения связей с уже существующими узлами добавляются дополнительные циклические дуги. Данный граф строится быстро и может быть преобразован в полный граф или граф предсказаний.

Однако при работе с графами появляется несколько проблем: обработка циклов и значительное время обработки;

В данной работе данные проблемы решаются с помощью оптимизаций, о которых будет рассказано чуть позже.

(7 слайд – Показатели защищенности)

Оценка защищенности невозможна без определения показателей защищенности.

Существует 2 типа показателей защищенности:

- Базовые показатели - показатели защищенности, непосредственно характеризующие элементы конфигурации и безопасности анализируемой системы, такие как: запущенные на узлах сервисы; уязвимости; источники угроз; атакующие действия; защитные меры.

- Интегральные показатели - показатели, непосредственно характеризующие безопасность всей сетевой инфраструктуры. Введение отдельных мер защиты приводит к необходимости повторного вычисления данных показателей.

На слайде представлено множество возможных показателей защищенности на графах атак, сгруппированные в зависимости от области действия показателей.

В данной работе в качестве базового показателя защищенности предлагается использовать риск компрометации каждого узла, который описывает предполагаемую ценность узла на основании сведений, полученных на этапе сбора о системе, а также топологический показатель нисходящего риска, рассчитанный как сумма показателей риска компрометации каждого узла, достижимого из текущего. Данный показатель позволит получить точное представление о возможностях нарушителя при попадании на конкретный узел графа.

В качестве интегрального показателя предлагается использовать уровень риска системы, представляющий собой сумму нисходящих рисков всех узлов.

(8 слайд – Методики выбора защитных мер)

В процессе оценки защищенности сетевой инфраструктуры, на этапе выбора защитных мер, необходимо провести приоритизацию и применение соответствующих защитных мер, способствующих понижению уровня риска системы.

Задача поиска оптимальных защитных мер на графе атак зачастую является нетривиальной ввиду описанных раньше проблем.

Большинство рассмотренных методик, применимых к графам атак пытаются ограничить доступ злоумышленника к узлам внутренней сети от существующей точки входа. Под точкой входа понимается любой узел, через который злоумышленник может попасть во внутреннюю сеть организации.

При этом данные методики используют либо сильно ограниченный набор сведений о системе, такой как количество узлов системы, количество компрометированных узлов с целевого узла и тому подобные, либо дополнительные сведения, которые можно получить только от владельца системы, такие как затраты на реализацию контрмер и ущерб от атаки.

(9 слайд – Требования к методикам)

Ввиду всех вышеописанных проблем выдвигаются следующие требования к разрабатываемым методикам:

1. Активы организации представляют собой сетевые узлы;

2. Проверяющий должен быть способен провести оценку защищенности сетевой инфраструктуры, опираясь исключительно на те сведения о системе, которые может получить самостоятельно.

3. Ценность узлов должна вычисляться на основании общедоступной информации, полученной на этапе сбора информации в процессе проведения тестирования на проникновение и определяться целочисленным значением;

4. Ценность узла должна напрямую зависеть от запущенных на нем сервисов;

5. Ценность узла должна зависеть от его типа;

6. В качестве базового показателя защищенности должен быть использован параметр нисходящего риска, вычисление которого основано на ценности достижимых из текущего узла хостов.

7. В качестве интегрального показателя должен выступать уровень риска системы, вычисляющийся как сумма параметров нисходящего риска каждого из узлов графа;

8. Алгоритм выбора защитных мер должен обеспечивать отсутствие циклов и оптимизацию этапа перестройки графа атак;

9. Выбор защитных мер должен осуществляться с целью минимизации уровня риска всей сетевой инфраструктуры.

(10 слайд – Разработка методик. Структура графа атак)

Оценка защищенности производится по ориентированному графу с собственной идентификацией дуг (орграфу с идентификацией):

Для описания орграфа используются следующие сущности:

* V – непустое множество вершин графа;
* A – множество дуг графа;
* C – множество успешно проэксплуатированных уязвимостей;
* – отображение множества уязвимостей на множество дуг. Данное отображение сюръективно, то есть для любой уязвимости существует отображение на дугу графа. При этом несколько уязвимостей могут иметь один образ.

Таким образом, множество отображает возможность компрометации узла из узла , а отображение определяет набор уязвимостей, позволяющих осуществить компрометацию.

(11 слайд – Разработка методик. Методика оценки защищенности)

Как уже говорилось, для проведения оценки защищенности системы в данной работе используется показатель риска компрометации узла. Значение риска компрометации вычисляется на основании типа узла и запущенных на нем сервисов.

Формула (1) используется для оценки риска компрометации узла:

здесь device\_type\_coef(x) – коэффициент критичности узла, зависящий от типа узла x, представленный в таблице 3.1, а service\_cost – риск компрометации сервиса, зависящий от принадлежности сервиса к одной из групп, определенных в таблице 3.2, S(x) – множество сервисов узла x. Значения в таблицах сформированы в зависимости от значимости того или иного типа узла или группы сервисов.

Второй показатель защищенности – уровень нисходящего риска, вычисляется как сумма риска компрометации всех узлов, достижимых из текущего.

Здесь W(x) множество узлов, достижимых из x.

В качестве интегрального показателя защищенности используется уровень риска системы, который вычисляется как сумма нисходящих рисков всех узлов системы.

(12 слайд – Разработка методик. Методика выбора защитных мер)

Методика выбора защитных мер заключается в поиске такой уязвимости, при устранении которой произойдет максимально возможное снижение уровня риска системы.

При устранении уязвимости удаляются все дуги графа, направленные к уязвимому узлу, если они используются для эксплуатации только ДАННОЙ уязвимости.

Использование данного подхода позволит максимально снизить риск компрометации сети с любого из узлов системы, присутствующего в графе атак.

Проблемы циклов и длительной обработки на графах атак решаются с помощью определения всех узлов к подграфам одного из двух типов: компоненте сильной связности или модифицированному N-арному дереву.

Компонентой сильной связности является любой подграф, содержащий цикл. Преимущества (+) данного подграфа состоит в том, что:

* Нисходящие риски всех узлов данной компоненты равны;
* Гарантируется прохождение по всем узлам подграфа;
* Если устраняемая уязвимость принадлежит узлу компоненты сильной связности, которая и после устранения уязвимости остаётся сильно связанной, уровень риска системы не изменяется.

N-арное дерево представляет собой дерево, в котором степени вершин не превосходят N+1. Под степенью вершины понимается сумма входящих и исходящих дуг вершины.

Для использования N-арных деревьев в качестве подграфов графа атак необходимо ввести несколько дополнительных условий

* В данный подграф включаются только те узлы, входящие дуги которых направлены от узлов того же дерева;
* Только корень может иметь входящие дуги, направленные из других подграфов графа атак;
* При удалении всех исходящих дуг данного подграфа, направленных на узлы, расположенные вне данного подграфа, корень является шарниром, то есть узлом, при удалении которого возрастет число компонент связности исходного графа

К преимуществам (+) данного вида подграфов относится:

* Попадание в подграф возможно только через корневой узел => обеспечивается прохождение по всем узлам подграфа.

Гарантия прохождения через все узлы подграфа позволяет ввести понятие риска компрометации подграфа, который складывается из рисков компрометации всех его узлов.

Фактически, все подграфы, количество узлов в которых больше 1 представляют собой псевдо-узлы, входящие и исходящие дуги которых – это соответствующие дуги исходных подграфов

(13 слайд – Процесс оценки защищенности и выбора защитных мер)

1. Вычисляется риск компрометации каждого узла системы;
2. Осуществляется поиск НОВЫХ компонент сильной связности и выполняются предварительные расчёты их риска компрометации и нисходящего риска;
3. Осуществляется поиск НОВЫХ модифицированных N-арных деревьев и выполняются предварительные расчёты их риска компрометации.
4. Проводится сравнительная оценка рисков;
5. Осуществляется выбор очередной защитной меры, после чего повторяются шаги 2-5.
6. По окончании проверки всех возможных контрмер, предлагается мера, приводящая к максимальному снижению уровня риска системы.

Таким образом, разработанные методики позволяют определить последовательность контрмер, которые необходимо устранить владельцу оцениваемой системы.

(14 слайд – Программная реализация разработанных методик)

Для реализации разработанных методик был использован язык Python ввиду его кросплатформенности и простоты интегрируемости в другие приложения. Разработанная система состоит из 4 компонентов:

* Компонента обработки данных;
* Компонента оценки защищенности;
* Компонентавыбора контрмер;
* Компонента визуализации.

Компонент обработки данных отвечает за преобразование входных данных и данных, поступающих с компонента выбора контрмер, в набор классов, реализующих операции над графом атак.

Компонент оценки защищенности производит вычисление основных показателей риска и производит сравнительную оценку текущего состояния и состояния, которому предшествовало удаление одной из существующих уязвимостей.

В компоненте выбора контрмер реализуются алгоритмы поиска уязвимости, при удалении которой максимально снизится уровень риска системы.

Компонент визуализации осуществляет отправку данных о графе атак на сервис 3vis, разработанный компанией NeoBIT для полноценной визуализации графа атак.

Разработанная система осуществляет итеративный поиск оптимальных контрмер. Это значит, что на вход подаётся количество уязвимостей, которые необходимо удалить, данные, имитирующие граф атак, а на выходе имеется набор пар (целевой узел, уязвимость), упорядоченные по приоритету устранения.

(15 слайд – Оценка эффективности разработанных методик)

Разработанная система всегда выбирает наиболее критичную уязвимость с точки зрения методики, поэтому для оценки её эффективности используется временной показатель.

Эксперименты проводились на сгенерированных графах атак различного размера для двух реализаций разработанных методик: наивной, то есть не учитывающей оптимизаций, основанных на разбиении исходного графа атак на 2 типа подграфов и полной, включающей оптимизации.

Результаты проведенных экспериментов приведены на рис. Х. Исходные данные представлены в табл …

(16 слайд – Сравнение с другими методиками)

В табл.Х представлен сравнительный анализ наиболее популярных на сегодняшний день методик, а также методики, предложенной в данной работе.

Разработанная методика может быть использована в качестве дополнительного модуля в любой системе анализа защищенности, на неё не накладываются никакие ограничения об информированности оценщика и она полностью подлежит автоматизации.