Выступление

1. Актуальность

Сетевая инфраструктура практически любой организации представляет собой сложную структуру, состоящую из множества различных сервисов, направленных на поддержание функционирования компании. Данная структура очень динамична: добавляются новые сервисы, меняются конфигурации существующих, создаются новые связи между сервисами.

Появление новых сущностей зачастую сопровождается появлением новых уязвимостей, которые становятся причиной нарушения информационной безопасности системы.

Для выявления недостатков компонентов системы, а также поиска уязвимостей и потенциальных векторов атак на информационные ресурсы, проводится анализ защищенности сети. Одним из наиболее эффективных методов анализа является тестирование на проникновение, в ходе которого осуществляется моделирование атак реальных злоумышленников.

В результате проведения анализа защищенности посредством тестирования на проникновение проводится описание основных обнаруженных уязвимостей, а также способов их устранения. Однако в крупных компаниях, как и в большинстве рассмотренных методик, существует практика устранения только тех уязвимостей, эксплуатация которых приводит к проникновению во внутреннюю сеть организации или компрометации наиболее критически важных узлов системы. Из-за сложности сетевой инфраструктуры устранение всех прочих уязвимостей затягивается на неопределенный срок, что создаёт опасную ситуацию, в которой злоумышленник, обнаружив новую точку входа, может воспользоваться существующими цепочками уязвимостей для компрометации сети.

Необходимо не только защитить сеть от проникновения извне, но и обеспечить должный уровень защищенности внутренней сети. Так, по данным Positive Technologies за 2019 год [1] при проведении внешнего тестирования на проникновение экспертам удалось преодолеть сетевой периметр 92% организаций, тогда как от лица внутреннего нарушителя был получен полный контроль над инфраструктурой во всех исследуемых системах.

(ЗДЕСЬ СТАТИСТИКА)

1. Цель работы. Задачи.

Для оценки уровня защищенности системы в данной работе предлагается использовать подход, основанный на анализе графа потенциальных атак с составлением метрик защищенности узлов и сети в целом для определения наиболее эффективных мер защиты. Рассмотренный подход позволяет оценить уровень риска системы при проникновении нарушителя на любой из узлов сетевой инфраструктуры, включенных в граф атак, и, следовательно, снизить риск компрометации системы с любого из узлов графа.

Цель данной работы – разработать автоматизированную систему оценки уровня защищенности сетевой инфраструктуры и выбора защитных мер на основе графов потенциальных атак.

Для достижения поставленной цели определены следующие задачи:

* Определить основные способы идентификации уязвимостей и узлов сети в процессе тестирования на проникновение;
* Проанализировать применимость графов атак в задачах оценки защищенности сети и существующие методики оценки защищенности сети и выбора защитных мер;
* Разработать методики оценки защищенности сетевой инфраструктуры и выбора защитных мер на основе анализа графа атак;
* Реализовать автоматизированную систему анализа защищенности сетевой инфраструктуры на основе анализа графа атак;

1. Концепция тестирования на проникновение. Подходы и этапы.

Тестирование на проникновение – это услуга в сфере информационной безопасности, суть которой заключается в санкционированной попытке проникнуть в информационную систему и обойти существующий комплекс средств ее защиты.

Существует несколько подходов к проведению тестирования на проникновение:

* Метод белого ящика – подход, при котором тестировщик имеет полный доступ к глубоким знаниям о функционировании и основных атрибутах системы. Это тестирование очень эффективно, так как понимание каждого аспекта системы очень полезно при проведении обширных испытаний на проникновение;
* Метод серого ящика – подход, при котором тестировщик получает ограниченную информацию о системе (например, знания алгоритма, архитектуры, внутренних состояний) для имитации внешней атаки на систему;
* Метод черного ящика – подход, при котором тестировщику предоставляется только высокоуровневая информация (например, URL или IP-адрес организации) для проведения тестирования на проникновение. Это весьма трудоемкий подход, так как тестировщику требуется значительное количество времени для изучения свойств и деталей системы; кроме того, высока вероятность пропустить часть областей из-за недостатка времени и информации. Также значительно усложняется оценка рисков, ввиду отсутствия знаний о бизнес-логике организации.



Процесс тестирования на проникновение в общем случае состоит из 4 этапов:

* Планирование – на котором определяются требования, ограничения и цели тестирования;
* Сбор информации о системе;
* Проникновение на целевой узел (атака);
* Составление отчёта.

1. Тестирование на проникновение. Этап сбора информации.

Разнообразие приложений, протоколов, операционных систем и прошивок оборудования ставит перед тестировщиком задачу по точной идентификации как самого сетевого устройства, так и установленного на нем программного обеспечения и других важных для этапа проникновения параметров.

На этапе сбора информации о системе осуществляется:

• Определение всех доступных узлов системы;

• Определение имен хостов;

• Определение контактной информации сотрудников организации;

• Определение типа узлов;

• Определение типа и версии операционных систем;

• Получение баннеров с обнаруженных портов;

• Определение типа и версий определенных сервисов;

• Определение разделяемых ресурсов;

• Определение пользователей и групп сервисов;

• Идентификация средств защиты;

• Получение списка актуальных уязвимостей;

• Получение списка доступных эксплойтов.

1. Тестирование на проникновение. Этап проникновения.

На данном этапе осуществляется проверка ранее обнаруженных уязвимостей и недостатков системы путем их эксплуатации. Таким образом, подтверждается или опровергается факт наличия той или иной уязвимости и определяется её влияние на информационную безопасность сетевой инфраструктуры организации.

В результате проникновения на очередной узел тестировщик может получить: информацию об учетных записях пользователей системы и сервисов (Системы Управления Базами Данных (СУБД), почты, Системы контроля версий, и т.п.); исходные коды различных проектов; доступ к ранее недоступным узлам или новой сети и т.д.

Полученный в результате проникновения доступ к узлам системы и новым сетям используется на этапе сбора информации для расширения покрытия сети тестировщиком.

Информация, полученная на этапе сбора сведений об узлах сети, может быть отфильтрована и использована в качестве метрики риска компрометации для каждого узла. Такой способ не требует наличия дополнительной информации о системе, предоставить которую может только заказчик, и, как следствие, отлично подходит для использования в автоматизированной системе оценки защищенности.

1. Методики оценки защищенности.

Оценка защищенности компьютерной сети – это процесс выявления уязвимостей, угроз и рисков, связанных с активами организации и мер защиты, которые могут смягчить эти риски.

Существует три основных подхода к оценке защищенности:

* Качественный – методики данного подхода используют опыт и суждения экспертов, аккумулированные в базе знаний. Они могут использовать опросные листы для определения уровня угрозы и ожидаемых рисков. Такие методики не позволяют определить численную величину риска. К таким методикам относятся: COBRA, OCTAVE, FRAP.
* Количественный – данные методики описывают возможные риски в денежном или частотном эквиваленте. На основе полученных значений и стоимости реализации мер защиты риски сравниваются для принятия оптимальных мер защиты. В данной работе были рассмотрены RiskWatch и ГРИФ.
* Смешанный – данные методики сопоставляют качественному уровню определенный количественный диапазон. К таким методикам относится CRAMM и методика на основе графов атак, использующая значение CVSS, обнаруженных уязвимостей.

1. Концепция графа атак.

Существует множество работ по применимости графов атак в задаче оценки защищенности сетевой инфраструктуры. Они отлично подходят для иллюстрации того, каким образом может развиваться атака внутри сети организации.

Граф атак можно представить как последовательность всех возможных действий злоумышленника для реализации угроз, так называемых трасс атак.

Общепринятые типы 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. Как следствие такие графы строятся намного быстрее, чем полные, но тем не менее всё ещё содержат лишние структуры.
* 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.

Основные проблемы при работе с графами атак:

* Обработка циклов;
* Значительное время обработки.

Для решения данных проблем применяются различные предположения, такие как: свойство монотонности графа и отказ от повторного посещения узлов; выделяются различные типы циклов графа и производятся расчеты вероятностей применения атакующих действий в зависимости от вида цикла.