УДК 004.852

СПОСОБ ПОСТРОЕНИЯ ДИНАМИЧЕСКОГО ЛОЖНОГО СЛОЯ СЕТИ НА ОСНОВЕ ДЕЙСТВИЙ ЗЛОУМЫШЛЕННИКА

Саулин М.А.[1], Мишуков О.А.[1]
Научный руководитель – кандидат технических наук, Мишуков О.А.[1]
1 – Военно-космическая академия имени А.Ф. Можайского
e-mail: vka@mil.ru

Введение. В условиях роста кибератак, ложные сетевые слои, имитирующие реальные сетевые ресурсы, играют важную роль в обнаружении и анализе злоумышленников. Однако, статичные honeypot-системы становятся предсказуемыми, что снижает их реалистичность. Актуальность работы заключается в необходимости разработки динамических honeypot-систем, способных адаптироваться к действиям атакующего и обеспечивать реалистичную имитацию сетевой среды.

Основная часть. Данный подход повышает реалистичность имитации ложного слоя сети. Статические honeypot системы демонстрируют предсказуемое поведение, всегда одинаково отвечая на запросы и поддерживая фиксированный набор сервисов. Динамические honeypot, напротив, автономно анализируют сетевую среду, адаптируя свою архитектуру и имитируя актуальное поведение узлов. Они автоматически развертывают соответствующие узлы при обращении злоумышленника и деактивируют их при прекращении взаимодействия. В отличие от статических систем, которые требуют постоянного контроля и ручной настройки динамические honeypot нуждаются лишь в первоначальном запуске, далее самостоятельно развертывают необходимые устройства, устанавливают связи и запускают сервисы. Для поддержания актуальной конфигурации динамическая ловушка самостоятельно собирает информацию о сетевом окружении с помощью модуля анализа операционной системы.[1] Ручное создание устройств с различными сервисами в honeypot приводит к предсказуемости. Для автоматизации данного процесса предлагается использовать скрытые марковские модели (СММ). СММ – представляет собой статистическая модель, в которой система, которую моделируют, имеет скрытые состояния, которые можно наблюдать только через связанные с ними наблюдаемые состояния. В контексте honeypot, скрытое состояние представляет собой уровень активности пользователей в определённое время суток и действия злоумышленника, а наблюдаемые состояния - это выбор операционной системы и сервиса для запуска.[2]

Для создания СММ необходим корпус данных, определяющий вероятности переходов между скрытыми состояниями (например, разный уровень активности пользователей в определенное время суток) и вероятности эмиссий, то есть вероятности выбора определенных сервисов при заданном уровне активности. СММ начинается с наблюдения текущего времени суток, далее алгоритм определяет наиболее вероятный уровень активности и, на основе этого, выбирает сервис для имитации. Процесс продолжается, пока не будет достигнуто ограничение на количество сервисов, определяемое заданным значением P. Таким образом, СММ позволяет генерировать разнообразные и непредсказуемые конфигурации устройств в honeypot, учитывая динамику активности пользователей и используя вероятности, основанные на корпусе данных.

Алгоритм работы системы включает следующие этапы:

1. Сбор Данных: Чтобы наша динамическая система работала эффективно, мы должны постоянно следить за тем, что происходит в сети, и быстро реагировать на любые изменения. Сначала система непрерывно собирает информацию о сетевом трафике, включая время, используемые порты, попытки взлома и IP-адреса атакующих. Затем

эта информация анализируется, чтобы обнаружить атаки и понять, какие типы запросов отправляются и как часто.

2. Определение Активности: Затем эта информация анализируется, чтобы обнаружить атаки и понять, какие типы запросов отправляются и как часто.
3. Обновление Наблюдаемых Состояний: Далее система обновляет свое представление о происходящем, добавляя информацию об обнаруженных атаках к обычным данным о сетевой активности.Наблюдаемые состояния для CMM теперь включают:
   - Нормальные Данные: Время суток и другие параметры «нормальной» активности.
   - Данные об Атаках: Тип атак, использованные порты, и другие характеристики атак.
4. Определение Скрытого Состояния: После этого, используя скрытые марковские модели, система определяет, в каком состоянии она находится — в нрмальном состоянии или под атакой.
   - Нормальное Состояние: Если атак нет или они незначительны, то скрытое состояние отражает «нормальную» активность.
   - Состояние Атаки: Если обнаружена атака, скрытое состояние переходит в состояние, соответствующее типу атаки (например, «активный SSH-скан», «попытка веб-эксплуатации» и т.д.).
5. Выбор Сервисов: В зависимости от этого состояния система выбирает, какие сервисы запускать в honeypot. Если обнаружена атака, приоритет отдается тем сервисам, которые, скорее всего, заинтересуют злоумышленника. При этом система также стремится создать разнообразную и непредсказуемую конфигурацию, чтобы не стать легкой мишенью. Этот процесс повторяется непрерывно, позволяя системе динамически адаптироваться к текущей ситуации и эффективно привлекать и анализировать действия злоумышленников.[3]

Выводы: Предложенная динамическая система адаптируется к действиям злоумышленника, обеспечивая более реалистичную имитацию сетевой среды и повышая непредсказуемость системы, что способствует более тщательному изучению злоумышленника. Дальнейшие исследования должны сосредоточиться на оптимизации CMM, а также на интеграции с другими системами защиты для противодействия современным кибератакам.

Литература:

1. Противодействие Honeypots: Системные вопросы, часть первая [Электронный ресурс].
   URL: https://www.securitylab.ru/analytics/216392.php.
2. Что такое скрытые модели Маркова / Хабр [Электронный ресурс].
   URL: https://habr.com/ru/articles/135281/
3. Rabiner, L. R. (1989). A tutorial on hidden Markov models and selected applications in speech recognition.Proceedings of the IEEE, 77(2), 257-286 [Электронный ресурс].
   URL: https://web.mit.edu/6.435/www/Rabiner89.pdf