ОБНАРУЖЕНИЕ СЕТЕВЫХ АТАК С ПОМОЩЬЮ HONEYPOT

Грицкевич В.И., Петров С.Н.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Петров С.Н. – к.т.н., доцент

В работе приводится описание полуавтоматического подхода к обнаружению атак с помощью ханипота совместно с человеческими возможностями принятия решения.

В современном мире для любой организации очень важно защитить свои активы от нападения злоумышленников. Чтобы осуществить мечту о полной безопасности, нужно быть на шаг впереди злоумышленников, или необходимо определить возможную атаку, прежде чем она будет осуществлена. Одним из таких инструментов для мониторинга поведения злоумышленников является ханипот.

Ханипот (от англ. honeypot, горшочек с медом) – приманка, используемая для привлечения внимания злоумышленников, для которых она может выглядеть, например, как обыкновенный фрагмент компьютерной системы. Ханипоты предоставляют собой средство отвлечения злоумышленников от реальной сети или наблюдения за их деятельностью. Другими словами, ханипот – это сетевая система для определения несанкционированного использования информационной системы путем анализа поведения злоумышленника в изолированной и контролируемой среде. Именно потому, что зачастую невозможно различить легитимный и вредоносный запрос, были созданы такие инструменты, как ханипоты. Ханипот – это информационная система, которая предназначена для мониторинга и обнаружения возможных атак, путем имитации уязвимой системы [1].

Целью ханипотов является регистрация всех возможных злонамеренных действий злоумышленника в зависимости от типа ханипота, реализованного в рамках инфраструктуры. Системы ханипот могут использоваться для идентификации различных типов вредоносных действий, такие как атаки веб-приложений, известные эксплуатация уязвимостей, эксплуатация устаревших программ/систем и автоматические атаки вредоносных ботов. Помимо обнаружения различных типов атак, хорошо внедренная система может также использоваться для обнаружения атак эскалации привилегий и их возможных причин. Логика выявления разных атак на повышение привилегий вращается вокруг реализации инфраструктуры с уязвимыми системами и слабыми конфигурациями. Когда злоумышленник использует любую из этих слабых конфигураций или учетные данные из этих намеренно уязвимых систем, ханипот может обнаружить, что злоумышленник скомпрометировал одну из преднамеренно уязвимых систем и пытается произвести атаку повышения привилегий.

Современный ханипот может включать в себе такие функции, как обнаружение фактов сканирования сети, мониторинг производительности, анализ журнала и т. д. для эффективного анализа поведения злоумышленника и принятия определенных решений, например, разрешить или заблокировать активность злоумышленника.

Архитектура рассматриваемой системы (рисунок 1) состоит из четырех различных компонентов, а именно: внешний брандмауэр, ханипот (виртуальная машина), база данных и специальная группа SOC (Security operating center, центр реагирования на инциденты информационной безопасности) для ручного анализа журналов. В ней присутствуют различные модули для определения наиболее точных результатов, которые помогут администратору принимать решения на основе генерируемых журналов. Данная архитектура состоит из следующих модулей: межсетевой экран, виртуальная машина (ханипот), база знаний, анализ IP, свод правил, группа SOC (центр реагирования на инциденты информационной безопасности) [2]. Внутреннее устройство ханипота представлено на рисунке 2.

Группа SOC (Security Operation Center) – это группа лиц, которые вручную анализируют данные из различных источников и подводят итоги для какого-либо действия или события с точки зрения уровня серьезности. Основным преимуществом команды SOC является следование полуавтоматическому подходу, заключающемуся в комбинировании автоматического и глубокого ручного анализа любого злонамеренного инцидента и приближении к нулевой вероятности ложных срабатываний.

Правило – это, по сути, протокол, которому будет следовать межсетевой экран для подавления злонамеренных действий. Свод правил – это набор как стандартных, так и настраиваемых правил, которые межсетевой экран будет автоматически извлекать через определенные промежутки времени. Помимо стандартных правил, которые брандмауэр будет вставлять на этапе инициализации, команда SOC также может обновлять правила на основе различных сценариев.

Система использует два типа межсетевых экранов, а именно: сетевой межсетевой экран и хостовой межсетевой экран (iptables), которые отвечают за обработку таких задач, как фильтрация

пакетов, сегрегация сети и предотвращение вторжений. Сетевой брандмауэр используется для сегрегации сети, разделяющей ханипот, SOC и сеть базы данных [2].

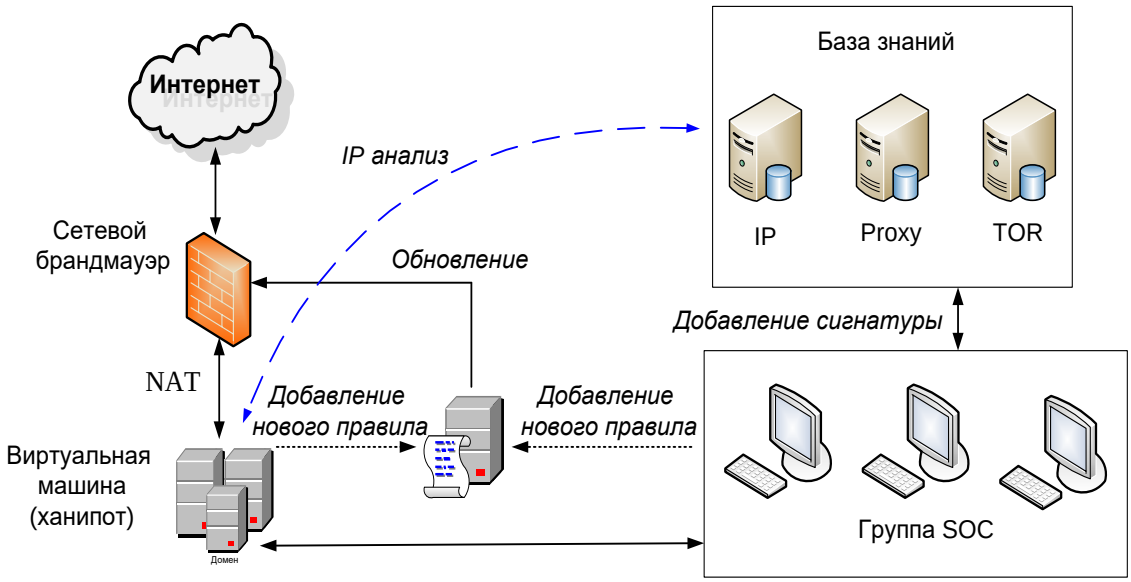

Рисунок 1 – Архитектура рассматриваемой системы

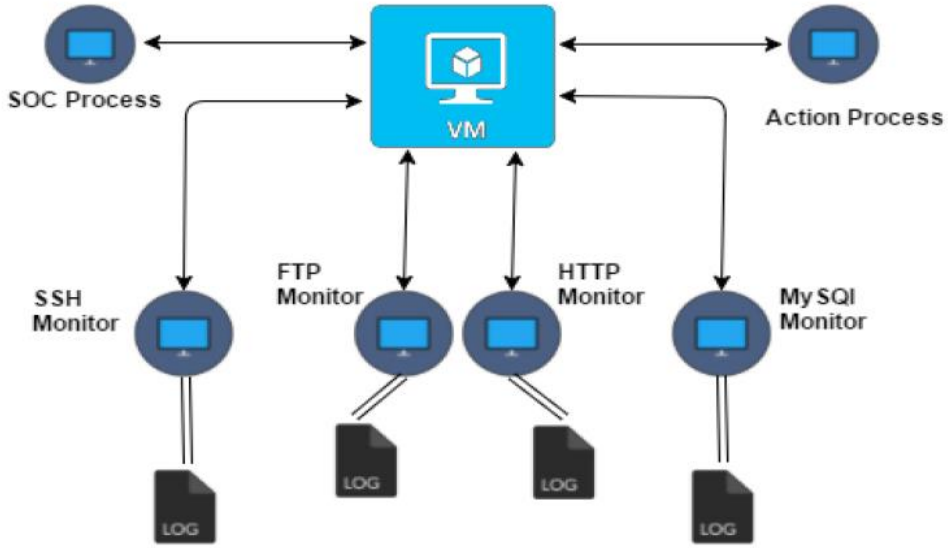

Рисунок 2 – Внутреннее устройство ханипота

Таким образом, основная цель заключается в создании самодостаточной децентрализованной системы для наблюдения за поведением злоумышленника с использованием полуавтоматического подхода. Предлагаемая система может преодолеть проблемы, имеющиеся в предыдущих реализациях, а именно минимизировать ложные срабатывания, путем выполнения ручного анализа. Система включает в себя логику для выполнения базового анализа поведения путем мониторинга различных путей к файлам и типов запросов в течение определенного периодического интервала, чтобы различать обычные и вредоносные действия конечного пользователя. Система также включает в себя взаимодействие с человеком и проверку данных с различных онлайн-ресурсов для получения наиболее точных результатов.

Список использованных источников:

1. Ханипот (Honeypot). [Электронный ресурс]. – Режим доступа: https://encyclopedia.kaspersky.ru/glossary/honeypot/.

2. Rahul koul, J. W. Bakal, Modern attack detection using intelligent honeypot, журнал «International research journal of engineering and technology», 2017, №4, p. 2866 – 2869.