УДК 004.777

СИСТЕМА И СРЕДСТВА МОНИТОРИНГА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Чаган Н.Ф.

гр.267241

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

Научный руководитель: Борботько Т.В. – доктор технических наук, профессор кафедры ЗИ

Аннотация. В материалах доклада рассматривается система мониторинга событий информационной безопасности, построенная на основе ханипотов, предназначенная для своевременного и точного обнаружения нарушителя в информационной сети организации, а также для использования на оборудовании или в системах (например, АСУ ТП), где использование традиционных систем, таких как EDR, AVP, DLP и т.д., не представляется возможным.

Ключевые слова: система мониторинга, ханипот, DDP

Введение. Нарушители рано или поздно находят способ проникнуть в периметр сети организации. Затем начинается период скрытого распространения, который может продолжаться до года, в зависимости от размера сети. В настоящее время атакующие стараются не применять «шумные» инструменты – активное сетевое сканирование, взлом паролей методом перебора и т.п. Они стремятся максимально использовать информацию, которую могут собрать на скомпрометированных рабочих станциях (роли, сетевое окружение, закладки, файлы, пользователи и конфигурация систем). При этом исходят из того, что эта информация является подлинной. В качестве одного из путей совершенствования систем информационной безопасности является применение

технологии обмана, позволяющей как можно раньше обнаружить факт проникновения в инфраструктуру, переключить внимание нарушителя от критически важных элементов информационно-коммутационной сети и задержать его активные действия. В основе данной технологии лежит четкое понимание того, что любая система защиты может быть преодолена.

В настоящее время существуют современные технологии обмана нарушителей, такие как платформы для создания распределенной инфраструктуры ложных целей (Distributed Deception Platform – DDP), которые являются развитием идеи ханипотов (Honeypots) – отдельных хостов для привлечения нарушителя. Отличительной чертой данных систем является имитация не только серверов и конечных станций, но и сетевой инфраструктуры, а также автоматизация и централизованное управление. Данные платформы можно считать последним рубежом обороны, т.к. нарушитель уже находится внутри сети. Хотелось бы отметить, что технологии обмана не заменяют существующих систем управления событиями (SIEM-систем), системы защиты конечных станций (endpoint protection platform), а лишь дополняют их.

Основная часть. Систему мониторинга событий информационной безопасности в части технологий обмана нарушителей представляется целесообразным строить на основе таких средств, как ханипоты, они же пассивные ловушки, которые всегда имеют дело с действиями нарушителей. Если говорить о таких системах, как EDR, то они не способны определить, использует ли внутренний инсайдер легитимную учетную запись со злым умыслом или у него есть законное право на доступ к активам. SIEM настроены на обнаружение вредоносной активности с помощью заданных корреляционных правил, которые могут быть недостаточно точными и разрабатываются вручную, что делает этот процесс особенно трудоемким. В то же время это не делает EDR, SIEM и другие системы менее значимыми. Ханипоты в свою очередь способны обнаружить попытку атаки с минимальным количеством ложноположительных срабатываний. Это главное отличие и преимущество данного класса решений. Также следует отметить, что они позволяют настроить мониторинг хакерской активности в тех «средах», где установить другие классы решений (например, EDR) зачастую технически невозможно. В последнее время направление атак нарушителей сконцентрировано больше на нетрадиционных поверхностях IT-атак в таких сферах, как здравоохранение или промышленность, так как используемое оборудование или системы (например, АСУ ТП) не поддерживают подобное ПО. Чтобы размыть поверхность атаки, создается эмуляция программируемых логических контроллеров (ПЛК), медицинского оборудования, банковских систем и т.д., в зависимости от конкретной организации, где применяются ловушки. Столкнувшись с одной из них, злоумышленник не поймет, где настоящие активы, а где приманки. С большой долей вероятности он ошибется, и его активность будет зафиксирована.

Обманные технологии в системе мониторинга могут применяться на 3 уровнях.

1-й уровень – конечных устройств. В данном случае требуется использование приманки, так называемые хлебные крошки. К ним относятся имитация cookies, txt-файл с паролями, кэш браузера с чувствительной информацией – все, что привлекает внимание атакующего.

2-й уровень – сетевой. На данном уровне используются ловушки – ложные цели атаки, замаскированные под такие ресурсы, как серверы, рабочие станции, маршрутизаторы. Некоторые сегодняшние решения позволяют эмулировать банкоматы, медицинское оборудование и IoT.

3-й уровень – интерактивных ловушек FullOS. Они занимают физические IT-ресурсы, как и настоящие пользователи.

Реализуется это следующим образом. Нарушитель, который не обладает данными о сети, в процессе разведки находит приманки и начинает с ними взаимодействовать. Когда его заинтересует определенная база данных, он попытается подключиться к операционной системе и взаимодействовать с ней как с активом, не предполагая, что это эмуляция. Легитимные пользователи не знают о существовании таких ловушек, и им нет смысла к ним подключаться. Следовательно, фиксирование попытки подключения, достоверно свидетельствует о том, что данные действия связаны с действиями нарушителя. Таким образом, одним из главных достоинств таких ловушек является то, что они практически единственный класс средств защиты с нулевым процентом ложноположительных срабатываний, в отличие от систем класса DLP, EDR, AntiAPT и т.п. Данные средства являются очень удобными в плане администрирования, так как любые срабатывания в системе автоматически указывают на попытки вредоносной активности. Система мониторинга событий информационной безопасности на основе ханипотов работает на стадии горизонтального распространения атаки в сети (рисунок 1).

Рисунок 1 – Модель действия нарушителя

Представляется целесообразным применение возможности интеграции с внешними сервисами, например с SIEM. При внедрении ловушек важнейшим этапом для администратора является сбор сведений о том, кто именно и в какую ловушку попался. Администратору необходимо зафиксировать попытку аутентификации с ловушкой. Ханипоты умеют «читать» логи из интегрированных систем о неудачных попытках подключения с подставными учетными данными. В случае с SIEM путем создания правил корреляции событий можно фиксировать факты использования информационных токенов злоумышленником. Это позволит максимально точно и практически мгновенно определить развивающуюся атаку.

Современные системы ханипотов уже значительно продвинулись в развитии по сравнению с их первоначальными версиями, приобрели множество интересных возможностей. Самые первые ловушки могли только эмулировать сервисы, а в настоящее время ханипоты автоматически маскируются под активы, применяемые в каждой конкретной организации. Хороший пример – учетные записи пользователей. В каждой организации есть служба каталогов, в которой зачастую применяется шаблон для формирования имени пользователя для сотрудника. Например, все пользователи домена созданы по шаблону с использованием имени и фамилии. В этом случае будет применяться единый шаблон адреса электронной почты, например с использованием первой буквы имени, точки, фамилии, @ и домена. Система ханипотов анализирует эти паттерны и при

составлении приманок также их придерживается, то есть фейковые пользователи, созданные системой приманок, будут очень похожи на те, что используются в домене компании [2].

Заключение. Ханипоты – один из самых надежных классов решений. Они практически безотказны и помогают предотвратить или остановить атаку в самом начале, минимизируя риски утечки данных и связанные с ними убытки. Они просты в настройке и работают фактически автономно, что делает их подходящими практически любой компании. Таким образом, система мониторинга событий информационной безопасности, построенная на технологии обмана нарушителя с использованием ханипотов, позволит своевременно получить достоверные данные о нахождении нарушителя в информационной сети предприятия, а также экономить финансовые, временные и человеческие ресурсы при технической поддержке и сопровождении данного решения.

Список литературы

1. Rahul Koul, Bakal J.W. Modern attack detection using intelligent honeypot // International research journal of engineering and technology. 2017. № 4. P. 2866–2869.

2. CISOCLUB – информационный портал и профессиональное сообщество специалистов по информационной безопасности. https://cisoclub.ru/ [Электронный ресурс]. – Режим доступа : https://cisoclub.ru/hanipoty-zashhishhaem-sistemy-hitrostju/. – Дата доступа : 10.02.2024.

UDC 004.777

INFORMATION SECURITY EVENT MONITORING SYSTEM AND TOOLS

Chagan N.E.

gr.267241

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Borbotko T.V. – Dr. of Sci. (Tech.), professor at the department of IS

Annotation. The materials of the report consider an information security event monitoring system based on honeypots, designed for timely and accurate detection of an intruder in the organization's information network. Also for use on equipment or systems (for example, automated control systems), where the use of traditional systems such as EDR, AVP, DLP, etc. is not possible.

Keywords: monitoring system, Honeypots, DDP