ПРИМЕНЕНИЕ СИСТЕМЫ T-POT ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

В.И. Грицкевич

Система T-Pot – это коллекция различных ханипотов, собранных компанией T-Mobile. Он представляет реализацию стека ELK (Elastic Search, Logstash, Kibana) для визуализации всех событий, захваченных различными ханипотами и некоторыми другими инструментами. Все ханипоты в T-Pot работают, используя docker (виртуальный контейнер), что значительно упрощает управление всеми настройками. Сам по себе ханипот не является средством обеспечения информационной безопасности. Это лишь приманка, ловушка для злоумышленника, целью которой является заставить его поверить в легитимность сервисов, которые имитирует ханипот. Однако такие приманки позволяют получить и проанализировать огромное количество информации, которая может оказаться полезной при планировании мероприятий повышения уровня информационной безопасности организаций. В частности, данная система содержит SSH и Telnet ханипоты, веб-ханипоты (эмулируют такие сервисы, как Redmine, Tomcat, Gitlab), ханипот, эмулирующий промышленный комплекс, SMTP-ханипот и многие другие. Система собирает информацию о методах, применяемых злоумышленниками, для проведения атак, что позволяет предотвратить атаку еще до попытки ее реализации. Помимо этого, появляется возможность оценить с каких территорий производятся атаки. Таким образом, система ханипотов T-Pot предоставляет информацию, с помощью которой можно значительно повысить уровень защищенности информационных систем.

Литература

1. Introduction to T-Pot - The all in one honeypot [Электронный ресурс]. – Режим доступа: https://northsec.tech/introduction-to-t-pot-the-all-in-one-honeypot/. – Дата доступа: 10.05.2020.