# СИСТЕМА ХАНИПОТОВ T-POT

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*
*Грицкевич В.И.*

*Петров С.Н. – канд. тех. наук*

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..

Целью создания и использования 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 [1].

Среди огромного количества различных ханипотов стоит обратить внимание на такую систему как T-Pot. 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 [2].

T-Pot является совокупностью docker-версий следующих ханипотов [3]:

– adbhoney (ханипот слабого взаимодействия для Android Debug Bridg, универсальный интерфейс доступа к устройствам Android с персонального компьютера);

– ciscoasa (ханипот слабого взаимодействия для Cisco ASA, способный обнаруживать CVE-2018-0101, атаки типа отказ в обслуживании и попытки удаленного исполнения команд);

– citrixhoneypot (обнаруживает и логгирует попытки сканирования и эксплуатации CVE-2019-19781);

– conpot (ханипот слабого взаимодействия эмулирующий комплекс инфраструктур, которые заставляют злоумышленника подумать, что он обнаружил большой промышленный комплес);

– cowrie (SSH и Telnet ханипот среднего взаимодействия, логгирующий брутфорс-атаки и команды, выполняемые злоумышленником);

– dionaea (сборник ханипотов, работающий на таких протоколах, как http, ftp, mysql и т.д.);

– elasticpot (ханипот Elastic Search);

– glutton (работает как MITM между злоумышленником и сервером, логгируя все действия);

– heralding (собирает авторизационные данные с протоколов ssh, telnet, ftp, rdp, http, https, pop3, pop3s, imap, imaps, smtp, vnc, postgresql, socks5);

– honeypy (плагины, эмулирующие UDP и TCP сервисы);

– honeytrap (динамически запускает серверные процессы на портах, к которым происходит обращение);

– mailoney (SMTP ханипот);

– rdpy (ханипот удаленного рабочего стола);

– snare+tanner (веб-ханипот).

Далее представлены результаты работы системы T-Pot за декабрь 2019 года.

Наибольшее количество атак пришлось на следующие модули системы T-Pot:

– dionaea (20843332 атаки, большая часть из которых пришлась на модуль эмулирующий SQL-сервер);

– honeytrap (716538);

– heralding (233784);

– rdpy (169583);
– mailoney (23765).

Если рассматривать статистику со всей системы T-Pot, то наиболее активными странами с точки зрения количества попыток несанкционированного доступа являются:

– Российская Федерация (4619164);
– Индия (1907802);
– Вьетнам (1402678);
– Армения (1050582);
– Индонезия (953348).

Если же рассматривать статистику несанкционированных попыток доступа к веб-серверу, то ситуация нескол

– Китай (3497);
– Гонгконг (865);
– США (574);
– Италия (473);
– Франция (321).

Безусловно, эти данные не отражают реальной картины, так как подавляющее большинство злоумышленников используют средства анонимизации в сети Интернет, однако их можно использовать для составления общей картины в целом.

Помимо этого, были собраны данные по наиболее часто используемым именам пользователей (рисунок 1) и паролям (рисунок 2).

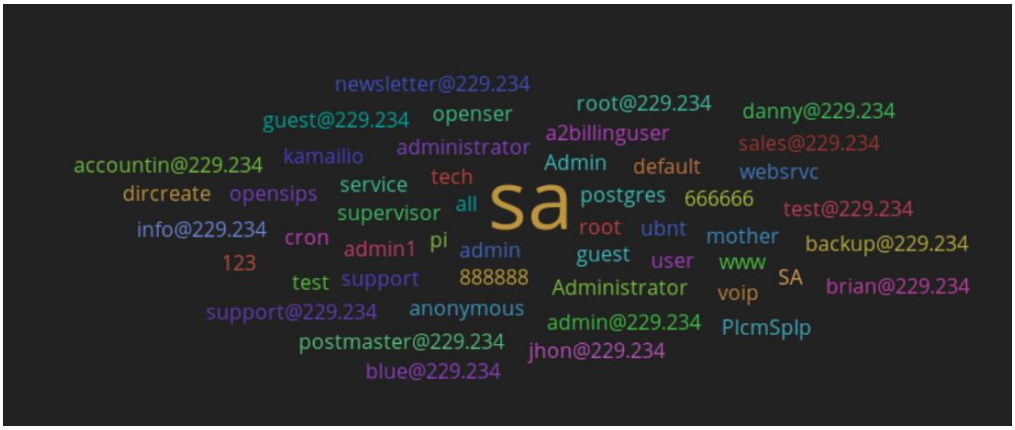


Рисунок 1 – Наиболее часто используемые имена пользователей

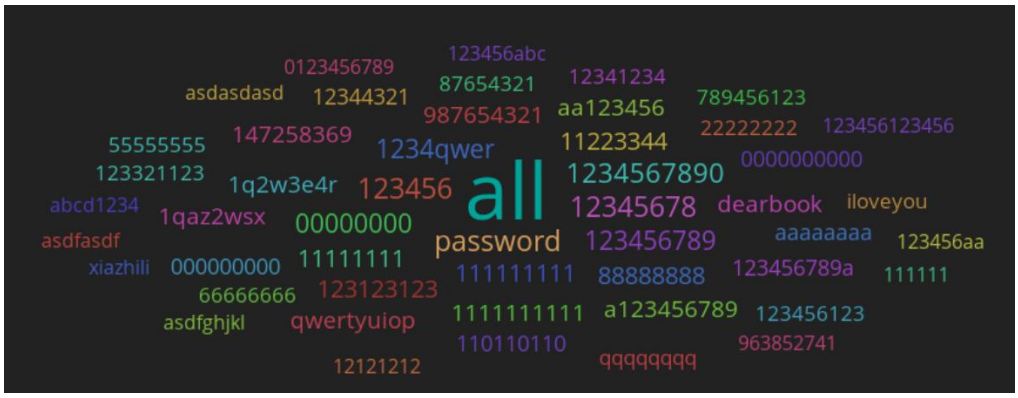


Рисунок 2 – Наиболее часто используемые пароли

Таким образом, можно сделать вывод о том, что ханипоты предоставляют информацию, которую можно использовать для анализа активности потенциальных злоумышленников, и с учетом этого повышать уровень защищенности информационных систем..

Список использованных источников:

1. Ханипот (Honeypot) [Электронный ресурс]. – Режим доступа: https://encyclopedia.kaspersky.ru/glossary/honeypot/.
2. 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/.
3. Концепция системы T-Pot [Электронный ресурс]. – Режим доступа: https://github.com/dtag-dev-sec/tpotce#concept.