УДК 004.056

РАЗРАБОТКА HONEYPOT-ЛОВУШКИ СЕТЕВЫХ СЛУЖБ С ПОВЫШЕННОЙ ДОСТОВЕРНОСТЬЮ ИМИТАЦИИ ЗА СЧЕТ ДИНАМИЧЕСКОЙ ГЕНЕРАЦИИ КОНТЕНТА

Нигоматулин А.А. (Университет ИТМО)
Научный руководитель – доцент, кандидат технических наук Менщиков А.А.
(Университет ИТМО)

Введение. В современном мире, несмотря на распространенность и разнообразие средств и технологий защиты в телекоммуникационных сетях, наблюдается рост результативных атак на компьютерные системы. Стандартных мер защиты недостаточно для обеспечения безопасности, в результате чего начинают набирать популярность решения на основе honeypot [1]. Являясь средством введения в заблуждение атакующего, honeypot должен с максимально возможной достоверностью имитировать реальную информационную систему с целью удержания внимания злоумышленника как можно более продолжительное время. Полностью достоверной имитацией может стать только полная копия реальной системы, что трудно реализуемо ввиду затрат значительных ресурсов на поддержание функционирования. Ввиду этого существующие на сегодняшний день реализации honeypot, являются компромиссом достоверности и ресурсоемкости. В текущей работе предлагается концепт компонента honeypot-решения, позволяющего повысить достоверность имитации ловушки сетевых служб за счет динамической генерации контента без значительного увеличения потребляемых ресурсов.

Основная часть. В качестве основы рассматривается модульное, масштабируемое honeypot решение [1,2,3], имеющее реализованные honeypot-модули, имитирующие рабочие станции или сервера с веб-приложениями.

В работе предлагается объединение honeypot-хостов в эмулируемую локальную сеть, путем добавления модуля-роутера. Доступ в нее может быть получен атакующим в результате успешного захвата одного из honeypot-хостов, находящихся на периметре сети.

В модуле-роутера предлагается реализация следующего функционала:

1) Непосредственная маршрутизация трафика между honeypot-хостами.
2) Имитация сетевого доступа от захваченного атакующим хоста к большему количеству клиентов сети, чем реально развернутым honeypot-хостам.
3) Модификация пакетов реальных honeypot-хостов с целью увеличения числа сетевых отпечатков, доступных атакующему.
4) Генерация широковещательного трафика, характерного для данного типа сетей, в том числе от несуществующих хостов.
5) Расширение поверхности атаки злоумышленника за счет поддержки проведения последних на уровне протоколов [4].
6) Взаимодействие с контроллером honeypot-сети с целью развертывания целевых honeypot-хостов [5], с которыми атакующий начинает активное взаимодействие.

Описанный функционал направлен на повышение достоверности honeypot-системы, а счет внедрения возможности сетевого взаимодействия с динамической генерацией трафика, доступного злоумышленнику и, как результат, увеличение поверхности атаки.

Предлагаемый функционал динамической маршрутизации позволяет при незначительном росте потребления ресурсов honeypot-системы увеличить количество виртуальных целей для атакующего, а также сымитировать их сетевое взаимодействие, повышающее достоверность эмуляции сети и системы в целом.

Выводы. В текущей работе представлен подход к повышению достоверности honeypot-ловушки сетевых служб за счет расширения поверхности для возможных атак. В дальнейшей

работе предполагается совершенствование механизмов виртуальной маршрутизации [6], а также внедрение системы генерации более достоверного виртуального сетевого трафика [7].

Список использованных источников:

1. Красов А.В., Петрив Р.Б., Сахаров Д.В., Сторожук Н.Л., Ушаков И.А. МАСШТАБИРУЕМОЕ HONEYPOT-РЕШЕНИЕ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В КОРПОРАТИВНЫХ СЕТЯХ // Труды учебных заведений связи. 2019. №3. URL: https://cyberleninka.ru/article/n/masshtabiruemoe-honeypot-reshenie-dlya-obespecheniya-bezopasnosti-v-korporativnyh-setyah (дата обращения: 24.02.2023).
2. J. Buzzio-Garcia, "Creation of a High-Interaction Honeypot System based-on Docker containers," _2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4)_, London, United Kingdom, 2021, pp. 146-151, doi: 10.1109/WorldS451998.2021.9514022.
3. Sivamohan, S., Sridhar, S.S., Krishnaveni, S. (2022). Efficient Multi-platform Honeypot for Capturing Real-time Cyber Attacks. In: Hemanth, D.J., Pelusi, D., Vuppalapati, C. (eds) Intelligent Data Communication Technologies and Internet of Things. Lecture Notes on Data Engineering and Communications Technologies, vol 101. Springer, Singapore. https://doi.org/10.1007/978-981-16-7610-9_21
4. Forshaw, James. _Attacking Network Protocols : A Hacker’s Guide to Capture, Analysis, and Exploitation_. 1st ed., San Francisco, No Starch Press, 2018.
5. B. Park, S. P. Dang, S. Noh, J. Yi and M. Park, "Dynamic Virtual Network Honeypot," _2019 International Conference on Information and Communication Technology Convergence (ICTC)_, Jeju, Korea (South), 2019, pp. 375-377, doi: 10.1109/ICTC46691.2019.8939791.
6. J. M. Ceron, C. Scholten, A. Pras and J. Santanna, "MikroTik Devices Landscape, Realistic Honeypots, and Automated Attack Classification," _NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium_, Budapest, Hungary, 2020, pp. 1-9, doi: 10.1109/NOMS47738.2020.9110336.
7. A. Cheng, "PAC-GAN: Packet Generation of Network Traffic using Generative Adversarial Networks," _2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)_, Vancouver, BC, Canada, 2019, pp. 0728-0734, doi: 10.1109/IEMCON.2019.8936224.

Нигоматулин А.А. Подпись

Менщиков А.А. (научный руководитель) Подпись