УДК 004.056.53 **Информационные технологии**

Логинов Олег Андреевич, *студент ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова»*

e-mail: neon2721@gmail.com

Баранкова Инна Ильинична, *научный руководитель****,*** *доктор технических наук, заведующая кафедрой информатики и информационной безопасности ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова»*

ПРИМЕНЕНИЕ HONEYPOT-ЛОВУШЕК ДЛЯ СБОРА ДАННЫХ О КИБЕРАТАКАХ НА ПРОМЫШЛЕННЫЕ СЕТИ

Аннотация: В данной рассмотрено исследование метода сбора данных о кибератаках на промышленные сети с помощью honeypot. Приведен краткий обзор существующих honeypot-решений для промышленных сетей. Также описывается процесс установки и настройки выбранного решения. В заключении подводится итог исследования, обсуждается его ограничения и перспективы дальнейшего развития.

Ключевые слова: honeypot, промышленные сети, кибератаки, сбор данных, настройка, сравнение, информационная безопасность, кибербезопасность.

Abstract: This article presents a study of the method for collecting data on cyber-attacks on industrial networks using a Honeypot solution. A comparison of existing Honeypot solutions for industrial networks is conducted, and the process of installing and configuring the selected solution is described. The study includes the results of analyzing attack data collected by the honeypot, including the nature of the attacks and the tools used, as well as an analysis of the effectiveness of the honeypot solution. In conclusion, the findings of the study are summarized, its limitations are

discussed, and prospects for future research are outlined.

Keywords: honeypot, industrial networks, cyberattacks, data collection, configuration, comparison, information security, cybersecurity.

Введение: В современном мире информационные технологии играют огромную роль в различных сферах жизни, включая промышленность. Однако, как и любые технологии, они могут стать объектом кибератак, которые могут нанести значительный ущерб предприятию. Поэтому вопросы информационной безопасности, особенно в промышленных системах, остаются актуальными. Одним из наиболее интересных и инновационных методов защиты информарции является – сбор информации о кибератаках при помощи honeypot.

Что такое Honeypot?

Honeypot (англ. – горшочек с медом) («лову́шка») – ресурс, представляющий собой приманку для злоумышленников. Ее основная цель - привлечь злоумышленников и предоставить информацию об их действиях и методах атаки [1].

Принцип работы Honeypot заключается в том, что система, созданная в качестве ловушки, выглядит как настоящая система, которая может привлечь к себе злоумышленников. При попытке злоумышленника проникнуть в систему ловушка фиксирует все его действия и передает информацию об атаке администратору, который может использовать эту информацию для повышения безопасности настоящей системы.

Основные виды Honeypot

Существует три основных типа Honeypot:

- слабого взаимодействия
- среднего взаимодействия
- сильного взаимодействия.

Honeypot слабого взаимодействия является наиболее пассивным типом Он используется для сбора информации о потенциальных атаках, но не предоставляет реальной среды для взаимодействия злоумышленника с системой.

Этот тип обычно используется для мониторинга внешних атак, таких как сканирование портов или попытки взлома.

Honeypot среднего взаимодействия имеет более активную роль в симуляции реальной среды. Он может имитировать различные сервисы и протоколы, что позволяет злоумышленнику взаимодействовать с системой на более высоком уровне. Этот тип обычно используется для привлечения злоумышленников, которые уже проникли в систему и пытаются получить доступ к важным ресурсам.

Honeypot сильного взаимодействия обеспечивает полную имитацию реальной среды и предоставляет злоумышленнику доступ к полному набору сервисов и протоколов, которые доступны в реальной системе. Этот тип обычно используется для анализа поведения злоумышленников и определения их методов атаки [2].

Существующие Honeypot для промышленных сетей

В таблице приведен краткий обзор существующих open-source honeypot-решений, которые могут использоваться в промышленных сетях

Таблица 1 – Обзор Honeypot для промышленных сетей

Название	Год	Взаимодействие	Масштабируемость	Эмулируемые сервисы
Conpot	2013	Низкое	+	IEC 60870-5-104, BACnet, EtherNet/IP, Guardian AST, Kamstrup, Modbus, S7comm, HTTP, FTP, SNMP, IPMI, TFT
GasPot	2015	Низкое	-	Guardian AST
SCADA Honeynet	2004	Низкой	+	S7 Mpi, S7 Ppi, Profinet, Modbus Rtu/Tcp Ip, Host-Link (Omron), Fins Ethernet(Omron), Mewtocol(Panasonic), SQL Server, E-mail, SMS(Gsm Message)
HoneyPLC	2020	Высокое	-	S7Comm, SNMP, HTTP

Установка и настройка Honeypot

Для исследования было выбрано Honeypot-решение Conpot. Данный

продукт достаточно прост в установке и настройке, так же он эмулирует большинство используемых в промышленных сетях сервисов.

Для установки данной ловушки была выбран облачный сервер. Характеристики сервера:

Операционная система: Ubuntu 20.04

Процессор: 1x2.8 ГГц

Оперативная память: 1 Гб

Для хранения данных использовался SSD на 15 Гб.

Данных характеристик хватает для стабильной работы Conpot.

Шаги установки «ловушки»:

1. Необходимо обновить и установить необходимые пакеты:

$ sudo apt update

$ sudo apt-get install git libsmi2ldbl smistrip libxslt1-dev python3.8-dev libevent-dev default-libmysqlclient-dev

$ sudo apt-get install python3-pip

$ sudo pip3 install virtualenv

$ sudo pip install --upgrade pip

$ sudo pip install --upgrade setuptools

$ sudo pip install cffi==1.14.0

2. Далее необходимо клонировать github-репозиторий и перейти в папку conpot:

$ git clone https://github.com/mushorg/conpot

3. Финальным шагом будет установка пакета командой:

$ sudo python3 setup.py install

Теперь можно запустить «ловушку» командой:

$ sudo conpot -f -t default

В качестве шаблона был выбран стандартный шаблон «default» эмулирующий PLC Siemens S7-200.

По умолчанию сервисы эмулируются на не стандартных портах.

Например, HTTP сервер запускается на порте 8800 вместо 80, FTP сервер

на 2121 вместо 21.

Для того чтобы дать возможность conpot запускаться на стандартых портах необходимо воспользоваться утилитой authbind, а также изменять в шаблонах порты, используемые при запуске серверов, эмулирующих различные сервисы.

После удачного запуска honeypot начнёт фиксировать подключения к нему с использованием различных протоколов и выводить в командную строку информацию об этих подключениях. Пример вывода информации представлен на рисунке 1.

Рисунок 1 - Вывод информации о подключениях

Результаты

Для проведения исследования Conpot был запущен на облачном сервере. Сбор данных проводился в течение 7 дней. Количество запросов, сгруппированных по протоколам представлено на рисунке 2.

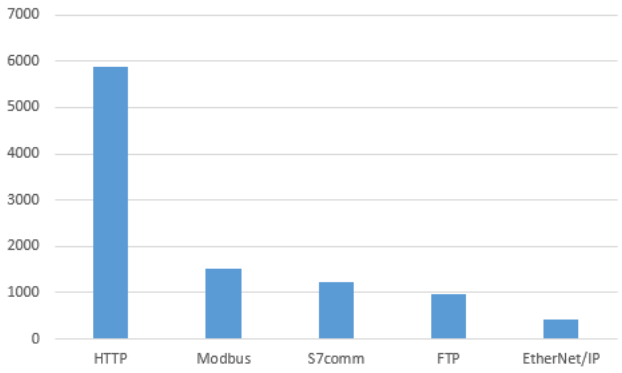

Рисунок 2 - Количество подключения по протоколам

На основе собранных данных можно сделать выводы о том какой протокол

чаще всего подвергается атакам, а также какими методами пользуется злоумышленник при атаке нашей системы.

Заключение

В данной статье было исследовано использование honeypot для сбора данных об атаках на промышленные сети. Были рассмотрены различные типы «ловушек» и приведен обзор существующих решений для промышленных систем. Также был описан процесс установки и настройки honeypot Conpot.

Использование honeypot может быть очень полезным для обнаружения и анализа кибератак в промышленных сетях. Honeypot может собирать информацию о способах атак, использованных уязвимостях и используемых инструментах. Эта информация может быть использована для улучшения систем защиты.

Библиографический список:

1. Авдошин А.С., Шатунов П.П. Honeypot как метод защиты информационных образовательных ресурсов / А.С. Авдошин, П.П. Шатунов // Известия Волгоградского государственного технического университета. Серия: Новые образовательные системы и технологии обучения в ВУЗе. 2010. № 8. С.16-18.

2. SecurityLab [Электронный ресурс]: Технология Honeypot. Часть 2: Классификация Honeypot, URL: https://www.securitylab.ru/analytics/275775.php (дата обращения 20.03.2023).