ИНТЕЛЛЕКТУАЛЬНЫЕ МЕТОДЫ В ЗАДАЧАХ ЗАЩИТЫ ОТ КИБЕРУГРОЗ

ЛАБОРАТОРНАЯ РАБОТА № 4
SIEM-системы.

Выполнил:
Мосолков Е.Н.
Преподаватель:
Исхаков А.Ю.

Москва 2021 г.

ЦЕЛЬ РАБОТЫ

Изучение механизмов работы систем класса SIEM

ЗАДАЧА ПРАКТИЧЕСКОЙ РАБОТЫ

Необходимо автоматизировать выявление данных из дампа журнала событий (файл small_log на Google диске) и ответить на следующие вопросы:

- Количество разных источников сообщений. Предоставить перечень.
- Количество разных типов сообщений от Cisco ASA, встречающихся в дампе. Предоставить перечень.
- Перечень различных IP-адресов, встретившихся в сообщениях Cisco ASA.

Автоматизацию можно выполнить с помощью любого инструментария. По результатам помимо ответов на вопросы можно предоставить исходный код и работающий прототип. В случае невозможности автоматизации необходимо предоставить без кода ответы на вышеуказанные вопросы.

ОТВЕТЫ НА ВОПРОСЫ, ПОЯСНЕНИЯ И ОБЗОР ФУНКЦИОНАЛА КОДА

1. Количество разных источников сообщений

Ответ: 3

Список источников: файл HOSTS.txt

2. Количество разных типов сообщений

Ответ: 22

Список сообщений: файл MESSAGES.txt

3. Количество разных IP-адресов, встретившихся в сообщениях Cisco ASA

Ответ: 339

Список ip адресов: файл IPS.txt

Как были получены ответы на вопросы:

С помощью Jupyter Notebook и python, а также использования регулярных выражений, был считан файл с логами, затем обработан 3 раза, на выходе были получены списки с ответами на вопросы.

Для ответа на первый вопрос – программа проходила по всем строкам логов и искалаимя хоста (находится сразу после поля timestamp), затем из полученного списка хостов составлялся набор уникальных хостов – их нашлось 3

Для ответа на второй вопрос – программа проходилась по всем строкам отбирая только те в которых присутствовало регулярное выражения, соответствующее сообщению Cisco ASA, затем программа составляла коллекцию уникальных ошибок – их нашлось 22

Для ответа на 3й вопрос – программа проходилась по всем строкам отбирая только те, в которых появлялась сообщение Cisco ASA, затем находила в такой строке все ip адреса, после чего составлялась коллекция уникальных ip. После составления коллекции ip вычитались ip адреса, принадлежащие хосту – итого получилось 339 уникальных ip адресов

Что пытался сделать злоумышленник:

Злоумышленник пытался провести DoS атаку, а именно пытался заставить машину бесконечно отправлять и принимать пакеты от самой себя, т.е. зациклиться.

Что в этом файле показалось странным

Странным в этом файле показалось то, что в нем есть ip адреса некорректного формата. Пример: 192.168.101.22832

А также большие значения маски подсети

Пример: 10.156.148.2167/5666

Как можно объяснить эту странность:

Вероятно, это сделано для того, чтобы злоумышленника было не просто отследить по ip адресу

КОД

```
import re

ip_reg = r'\d{1,5}\.\d{1,5}\.\d{1,5}\.\d{1,5}'

with open('small_log.crash', 'r') as file:
    data = file.readlines()

# 1. Источники собщений
hosts = set([s.split(' ')[3] for s in data])
host_ips = [re.match(ip_reg, h).group(0) for h in hosts if re.match(ip_reg, h)]
for e in hosts:
    print(e)

print(host_ips)

# 2. Ошибки Cisco ASA
err_set = set([re.search(r'%ASA-\d{1}-\d{6}', e).group(0) for e in data if
re.search(r'%ASA-\d{1}-\d{6}', e)])
for err in sorted(err_set):
    print(err)

print(f'Итого {len(err_set)} различных ошибок Cisco ASA')

# 3. IP адреса

ips = set([i for j in [re.findall(ip_reg, s) for s in data if re.search(r'%ASA-\d{1}-
\d{6}', s)] for i in j]) - set(host_ips)

for i in ips:

    print(i)


print(f'Итого {len(ips)} ip адреса в сообщениях Cisco ASA')
```

ВЫВОД

Я изучил механизмы работы систем класса SIEM