ДОКУМЕНТАЦИЯ

NetTrap

Технология Deception

Авторство:
Группа ББСО-02-20
Бочкарёв Марк
Валеева Рената
Левина Анна
Онищенко Евгений
Пыхов Степан
Редькин Павел
Шамрай Максим

Москва, 2024

Руководство Администратора

Установка:

Чтобы софт был корректно установлен, необходимо совершать все шаги с правами аднминистратора.

0. Перед началом установки необходимо убедиться, что компьютер подключён к сети интернет, на вашей системе установлен Git, Docker, Docker Compose и выключен сервис SSH, FTP, программы, работающие на порту TCP/8000.
1. Выберите директорию, куда будет произведена установка. Выполните копирование репозитория с GitHub https://github.com/Pavel-Alze/Deception. На Linux дистрибутивах, выполните команду «`git clone https://github.com/Pavel-Alze/Deception.git`»и дождитесь окончания загрузки.
2. У вас появилась директория Deception/ . Перейдите в неё и запустите установочный файл install.sh . На Linux дистрибутивах, выполните команду «`./install.sh`» дождитесь полной установки.
3. Для корректной работы необходимо либо создать, либо добавить уже существующего бота в ваш чат/канал в соц.сети «Telegram». Далее в файле main.py необходимо изменить следущие поля: «token» если вы будете использовать своего бота и поле «chat_id» для того, чтобы бот мог корректно отправлять сообщения. Также стоит заметить, что при использовании бота его необходимо предварительно добавить в ваш чат/канал как администратора.
4. После установки на вашем компьютере будет развёрнута система из трёх ловушек и программы оповещения в тг-канал. Софт будет запущен автоматически после установки и будет запускаться после каждой перезагрузки операционной системы.

Эксплуатация:

После установки софт, не требует никаких дальнейших действий для его эксплуатации. В целях исключения сбоя в работе софта необходимо следить, чтобы к устройству был доступ по протоколу TCP и портам 22(SSH),21(FTP),443(HTTPS),8000, а так же возможность установления TCP соединения с ip-адресом 149.167.67.220 – необходимо для работы тг-бота. Остальные ограничения на трафик определяются администратором.

Софт включает в себя три ловушки:

-SSH
-FTP
-WEB

Каждая из них работает независимо от другой.

username – указание пользователя; ***password*** – пароль пользователя; ***ip-адрес*** – адрес устройства, на котором развёрнут продукт.

-SSH

При взаимодействии злоумышленника с SSH-ловушкой в логах можно будет найти такие данные как: ip с которого злоумышленник проивёл соединение; команда, выполенная злоумышленником.
Функциональный набор ловушки – `pwd, ls, cat, sudo`
Подключение производится по команде «`ssh` ***`username`***`@`***`ip-адрес`*** `-p 22`»
Сработает только пара значений ***username:password*** *admin:admin*, в остальных случаях доступ будет заблокирован.

-FTP

При взаимодействии злоумышленника с FTP-ловушкой в логах можно будет найти такие данные как: ip с которого злоумышленник проивёл соединение; команда, выполенная злоумышленнком вместе с параметрами
Функциональный набор ловушки – `pwd, user, pass, list, type, cwd`
Подключение производится по команде «`ftp open` ***`ip-адрес`***», далее указываются ***username*** и ***password***
Подключение доустпно по любой паре значений ***username:password***

-WEB

При взаимодействии злоумышленника с WEB-ловушкой в логах можно будет найти такие данные как: ip с которого злоумышленник проивёл соединение;запрос, выполенный злоумышленнком и ответ сервера
Запросы доступные при обращении к ловушке – / , /main , /login , /admin
Обращение к ловушке по команде «curl http://***ip-адрес***:8000/» или указание адреса в адресной строке браузера
Ответом сервера будет код 404 и страница ошибки

Система оповещения сообщит о факте взаимодействия с ловушкой

Руководство Пользователя

Эксплуатация:

Софт работает в автономном режиме. Пользователь самолично не должен взаимодействовать с софтом. Также пользователь должен исключить попытки подключения к рабочему устройству по SSH, FTP, а так же взаимодействии с сервером на порту 8000 – это приведёт к ложному срабатыванию системы оповещения. В случае возникновения проблем или вопросов – обратиться к администратору.

Пример:

1. SSH-ловушка
   Атака. Проникновение на SSH сервер и чтение данных с него (Рис.1)

```
C:\Users\lycey>ssh admin@192.168.25.130
admin@192.168.25.130's password:
Welcome to SSHHostServer

mirea@admin$pwd
/home/admin
mirea@admin$ls
README.txt
mirea@admin$exit
Connection to 192.168.25.130 closed.
```

Рис.1

Логи SSH сервера во время атаки. Выявлен ip-адрес злоумышленника и его действия на сервере (Рис.2)

```
sshpot | Listening for connection on port 22 ...
sshpot | New connection is here from: 192.168.25.1
sshpot | INFO SSH  Command receied (192.168.25.1): pwd
sshpot | INFO SSH  Command receied (192.168.25.1): ls
sshpot | INFO SSH  Command receied (192.168.25.1): exit
```

Рис.2

2. FTP-ловушка
   Атака. Проникновение на FTP сервер (Рис.3)

```
ftp> open 192.168.25.130
Connected to 192.168.25.130.
220 Welcome to FTP Honeypot!
502 Command not implemented.
User (192.168.25.130:(none)): admin
331 User name okay, need password.
Password:
230 User logged in, proceed.
ftp> user
Username admin
331 User name okay, need password.
Password:
230 User logged in, proceed.
```

Рис.3

Логи FTP сервера во время атаки. Выявлен ip-адрес злоумышленника и авторизационные данные, которые он применил. (Рис.4)

```
ftppot | INFO FTP  ('192.168.25.1', 60774) OPTS UTF8
ftppot | INFO FTP  ('192.168.25.1', 60774) USER admin
ftppot | INFO FTP  ('192.168.25.1', 60774) PASS admin
ftppot | INFO FTP  ('192.168.25.1', 60774) USER admin
ftppot | INFO FTP  ('192.168.25.1', 60774) PASS admin
```

Рис.4

3. WEB-ловушка
   Атака. Взаимодействие с Web сервером через браузер (Рис.5)

Рис.5

   Логи Web сервера во время атаки. Выявлен ip-адрес злоумышленника, его действия и ответ сервера (Рис.6)

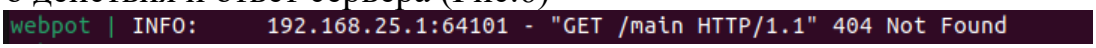

Рис.6

4. Система оповещения. Оповещение в тг-канал сразу после появления логов микросервисов о взаимодействии с ними (Рис.7)

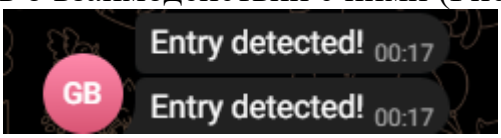

Рис.7