Содержание

L Traffic analysis	3
Оборудование	3
Раздел	3
Задачи	3
Файлы	4
Результаты разбора	6
Логи разбора трафика	1

1 Traffic analysis

Оборудование

Для настройки корректной работы раздела Разбора трафика необходимо добавить оборудование типа "Сервер разбора Рсар" в раздел Управления списка оборудования.

Конфигурация оборудования для разбора трафика:

- 1. Процессор (СРU) 2.5 ГГц, 2 шт
- 2. Оперативная память (RAM) от 4 Гб
- 3. Жесткий диск (HDD) от 100 Гб
- 4. Операционная система Ubuntu 20.04

Для установки необходимых для работы утилит необходимо выполнить следующую команду:

apt install wireshark tshark sox

Раздел

Для перехода в раздел разбора траффика в меню перейдите в раздел "Законный перехват"→"Разбор трафика"→"Разбора трафика".

Раздел Разбора трафика выглядит как на рисунке ниже.

Задачи

Задачи для Разбора трафика находятся в левой части страницы Разбора трафика.

Создание задачи

Для создания новой задачи Разбора трафика нажмите на кнопку "+" в туллбаре над списком существующих задач.

×

В открывшейся форме создания задачи введите:

- Название задачи
- Описание задачи

.....

×

×

Нажмите кнопку "Сохранить".

Редактирование задачи

Для редактирования задачи нажмите на кнопку редактирования напротив существующей задачи.

×

В открывшейся форме редактирования задачи измените:

- Название задачи
- Описание задачи

Нажмите кнопку "Сохранить".

Удаление задачи

Для удаления задачи нажмите на кнопку "Удалить" напротив существующей задачи и подтвердите либо отмените действие.

Файлы

Файлы для Разбора трафика находятся в центральной части страницы Разбора трафика.

×

Добавление файла

Для добавления нового файла для Разбора трафика нажмите на кнопку "+" в туллбаре над списком добавленных файлов.

×

В открывшейся форме добавления файла:

- Загрузите или перетащите рсар-файл;
- При необходимости задайте отображаемое название и описание для файла;
- Укажите необходимые типы разбора трафика (Web,Dns,Mail,Voip,Ftp);

Нажмите кнопку "Сохранить".

Редактирование файла

Для редактирования файла для Разбора трафика нажмите на кнопку редактирования напротив существующего файла.

×

В открывшейся форме редактирования файла можно изменить:

- Отображаемое название файла;
- Описание файла;
- Типы разбора трафика (Web,Dns,Mail,Voip,Ftp);

Нажмите кнопку "Сохранить".

В случае, если были внесены изменения в типы разбора трафика - на экране появится форма подтверждения перезапуска разбора трафика для этого файла.

Удаление файла

Для удаления файла нажмите на кнопку "Удалить" напротив существующего файла и подтвердите либо отмените действие.

×

Перезапуск разбора файла

Для перезапуска разбора файла:

- 1. Выберите необходимый файл из списка;
- 2. Нажмите на кнопку перезапуска разбора в тулбаре;
- 3. Подтвердите либо отмените действие.

×

Импорт файлов из раздела захвата трафика

Файлы для разбора трафика можно импортировать из раздела "Захват трафика".

Перейдите в раздел "Законный перехват"→"Захват трафика".

×

В списке файлов выберите файлы, которые необходимо разобрать и нажмите кнопку разбора.

×

В открывшейся форме:

- Выберите задачу Разбора трафика, в которую будут импортированы файлы.
- В случае выбора "Новой задачи" введите имя задачи, которая будет создана при импорте.
- Типы разбора для импортируемых файлов (Web,Dns,Mail,Voip,Ftp).

Нажмите на кнопку "Применить". После завершения процесса импорта файлов появится окно с предложением о переходе в раздел "Разбор трафика".

×

Результаты разбора

Результаты разбора находятся в правой части страницы Разбора трафика.

Web

На вкладке результатов разбора Web отображаются HTTP-запросы.

Запросы

На вкладке "Запросы" отображаются "сырые" данные о запросах.

В таблице доступны следующие данные:

- Дата и время запроса
- Адрес запроса
- Размер ответа в байтах
- Метод

×

При нажатии на кнопку "Дополнительная информация о запросе"(?) откроется попап с дополнительной информацией о запросе:

- Агент
- Хост
- Урл
- Тип содержимого
- Кодировка
- Метод запроса
- Код ответа
- Размер ответа в байтах
- Порт отправителя
- Порт получателя
- Время ТСР

- Протокол IP
- Версия IP
- IP отправителя
- ІР получателся
- Тип Eth
- Eth отправителя
- Eth получателя
- Идентификатор файла для разбора
- Имя файла для разбора
- Имя файла с содержимым ответа

×

Изображения

На вкладке "Изображения" отображаются запросы, в в ответ на которые возращались изображения.

DNS

На вкладке результатов разбора DNS отображаются хосты.

В таблице доступны следующие данные:

- Дата и время запроса
- Хост

×

Дополнительная информация

При нажатии на кнопку "Дополнительная информация о запросе"(?) откроется попап с дополнительной информацией о запросе:

- Список хостов
- Список адресов
- Список сертификатов
- Дата запроса
- Время ответа
- Порт отправителя
- Порт получателя
- Протокол IP
- Версия ІР
- ІР отправителя
- ІР получателя
- Тип Eth

- Eth отправителя
- Eth получателя
- Идентификатор заприси
- Идентификатор файла для разбора
- Имя файла для разбора

Mail

На вкладке результатов разбора MAIL отправленные/полученные Email-ы.

В таблице доступны следующие данные:

- Дата и время отправки/получения;
- Отправитель
- Получатель
- Тема письма

×

Содержимое

При нажатии на кнопку Содержимого письма откроется попап в котором доступны:

- Отправитель
- Получатель
- Тема письма
- Текст письма
- Список приложенных файлов к письму (можно скачать)

×

Дополнительная информация

При нажатии на кнопку Дополнительной информации(?) откроется попап с дополнительной информацией о письме:

- Порт отправителя
- Порт получателя
- Протокол IP
- Версия ІР
- ІР отправителя
- ІР получателя
- Тип Eth
- Eth отправителя
- Eth получателя
- Отправитель

- Получатель
- Тема
- Идентификатор письма
- Агент пользователя
- Версия МІМЕ
- Тип содержимого
- Язык
- Составной тип
- Тип составного содержимого
- Кодировка составного содержимого
- Диспозиция составного содержимого
- Идентификатор заприси
- Идентификатор файла для разбора
- Имя Eml-файла

Voip

На вкладке результатов разбора Voip информация о совершенных Voip-сессиях.

В таблице доступны следующие данные:

- Дата и время сессии
- Продолжительность сессии
- Вызывающий
- Вызываемый

×

Аудиозапись

При нажатии на кнопку Записи откроется попап, в котором можно прослушать аудиозаписи:

- Вызывающего
- Вызываемого
- Комбинированную

Логи запросов

При нажатии на кнопку Логи запросов откроется попап с логами всех запросов сессии.

×

×

Дополнительная информация

При нажатии на кнопку "Дополнительная информация"(?) откроется попап с дополнительной информацией о сессии:

- Порт отправителя
- Порт получателя
- Протокол IP
- Версия IP
- IP отправителя
- ІР получателя
- Тип Eth
- Eth отправителя
- Eth получателя
- Продолжительность сессии
- Вызывающий
- Вызываемый
- Идентификатор звонка
- Ssrc исходящий
- Ssrc входящий
- Названия файлов аудиозаписей
- Идентификатор файла для разбора

×

Ftp

На вкладке результатов разбора FTP отображаются файлы отправленные/полученые посредством FTP.

В таблице доступны следующие данные:

- Дата и время запроса
- Имя файла
- Направление (Скачивание/Загрузка)
- Размер файла в байтах
- Адрес клиента
- Адрес сервера

×

Дополнительная информация

При нажатии на кнопку "Дополнительная информация"(?) откроется попап с дополнительной информацией о запросе:

- Порт отправителя
- Порт получателя
- Протокол IP

- Версия IP
- ІР отправителя
- ІР получателя
- Тип Eth
- Eth отправителя
- Eth получателя
- Имя файла
- Директория Ftp
- Размер файла в байтах
- Направление
- Идентификатор файла для разбора
- Файл ответа

Логи разбора трафика

Для перехода в раздел логов разбора траффика в меню перейдите в раздел "Законный перехват"→"Разбор трафика"→"Логи разбора трафика".

×

×

Раздел Логов разбора трафика выглядит как на рисунке ниже.