Всем привет!

Сегодня наша лекция посвящена перехвату траффика в сети.

Чаще всего перехват траффика используется для шпионажа внутри сети компании, а так же для того, что бы достать все данные людей, подключенных к публичному Wi-Fi (в банке, гостинице, транспорте, кафе и т.д.)

Работать мы будем с программой Intercepter-NG.

Что такое Intercepter-NG

Intercepter-NG – это программа для выполнения атак человек-посередине. Имеется большое количество программ для таких атак, главной особенностью, выделяющей Intercepter-NG среди остальных, является то, что программа изначально была написана для Windows и прекрасно работает именно в этой операционной системе. Также к особенностям программы можно отнести графический интерфейс, в котором собраны многочисленные функции и опции, связанные с атакой человек-посередине, а также с некоторыми другими задачами пентестинга.

Благодаря графическому интерфейсу, использовать Intercepter-NG легко. Но большое количество опций и фрагментированная документация могут запутать начинающего пользователя. Надеюсь, что эта лекция научит вас всему и не оставит вопросов.

Что может Intercepter-NG

Главная задача Intercepter-NG – выполнение атаки человек-посередине. В практическом смысле, атака человек-посередине (её ещё называют атакой посредника) заключается в возможности просматривать передаваемые другими пользователями данные в локальной сети. Среди этих данных могут быть логины и пароли от сайтов. Также передаваемые данные можно не только анализировать и сохранять, но и изменять.

Чтобы описать техническую суть этой атаки, представьте себе локальную сеть. Такой локальной сетью могут быть несколько компьютеров в вашей квартире, которые подключены к роутеру. При этом неважно, подключены они по проводу или по Wi-Fi. Роутер получает запросы от компьютеров, перенаправляет их, например, в Интернет, а полученные ответы возвращает обратно компьютерам, отправившим запросы. В данной ситуации роутер является шлюзом.

Благодаря атаке, называемой ARP спуфингом, компьютер начинает считать шлюзом не роутер, а компьютер атакующего. Атакующий получает запросы от «жертвы» и передаёт их в пункт назначения (например, запрашивает содержимое веб-сайта в Интернете), получив ответ от пункта назначения, он направляет его «жертве». В этой ситуации атакующий становится посредником – отсюда другое название атаки человек-посередине – «атака посредника». Для реализации атаки ARP спуфинг необязательно понимать её детали.

Атакующий получает доступ к передаваемым данным и может, например, извлекать из этих данных пароли и сообщения. Процесс анализа передаваемых данных называется сниффингом. В процессе сниффинга Intercepter-NG умеет:

- Перехватывать логины и пароли для входа на веб-сайты
- Восстанавливать переданные данные (файлы)
- Перехватывать сообщения некоторых мессенджеров
- Показывать посещённые пользователем адреса

Кроме передачи данных, возможно их изменение, внедрение в код открываемых страниц JavaScript и принудительная загрузка пользователю файла.

Всё это прекрасно работает только для незашифрованных данных. Если данные зашифрованы (HTTPS), то их невозможно проанализировать без дополнительных действий.

Прежде чем подключиться к веб-сайту, компьютер обращается к DNS (серверу имён), чтобы узнать его IP адрес. Intercepter-NG умеет подменять ответы DNS (делать DNS спуфинг), что позволяет перенаправлять «жертву» на фальшивые копии сайтов для последующих атак.

Это далеко не все возможности программы. С другими возможностями мы познакомимся далее в этой лекции.

Где скачать Intercepter-NG

Официальным сайтом программы Intercepter-NG является sniff.su. Там же её можно скачать. Но некоторые браузеры помечают сайт как содержащий нежелательное ПО. Конечно, это не препятствует посещению сайта, но если вам не хочется нажимать несколько лишних кнопок, то ещё одни официальным сайтом, где можно скачать Intercepter-NG, является зеркало на Гитхабе: https://github.com/intercepter-ng/mirror. Там имеются все версии программы:

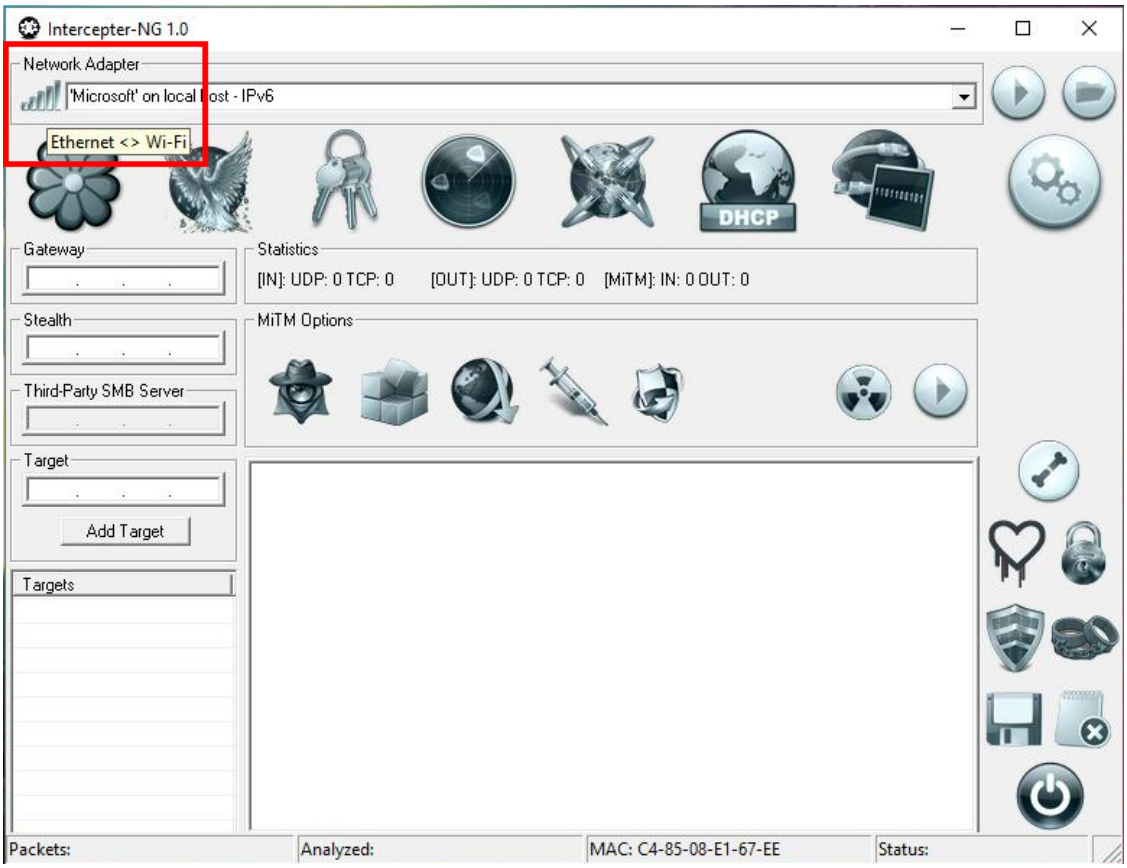
- файл с расширением **.apk** – это версия для Android (требует root прав)
- с буквами **CE** – консольная версия
- **Intercepter-NG.v*.zip** – основная версия для Windows

Скаченная программа не нуждается в установке – достаточно распаковать архив.

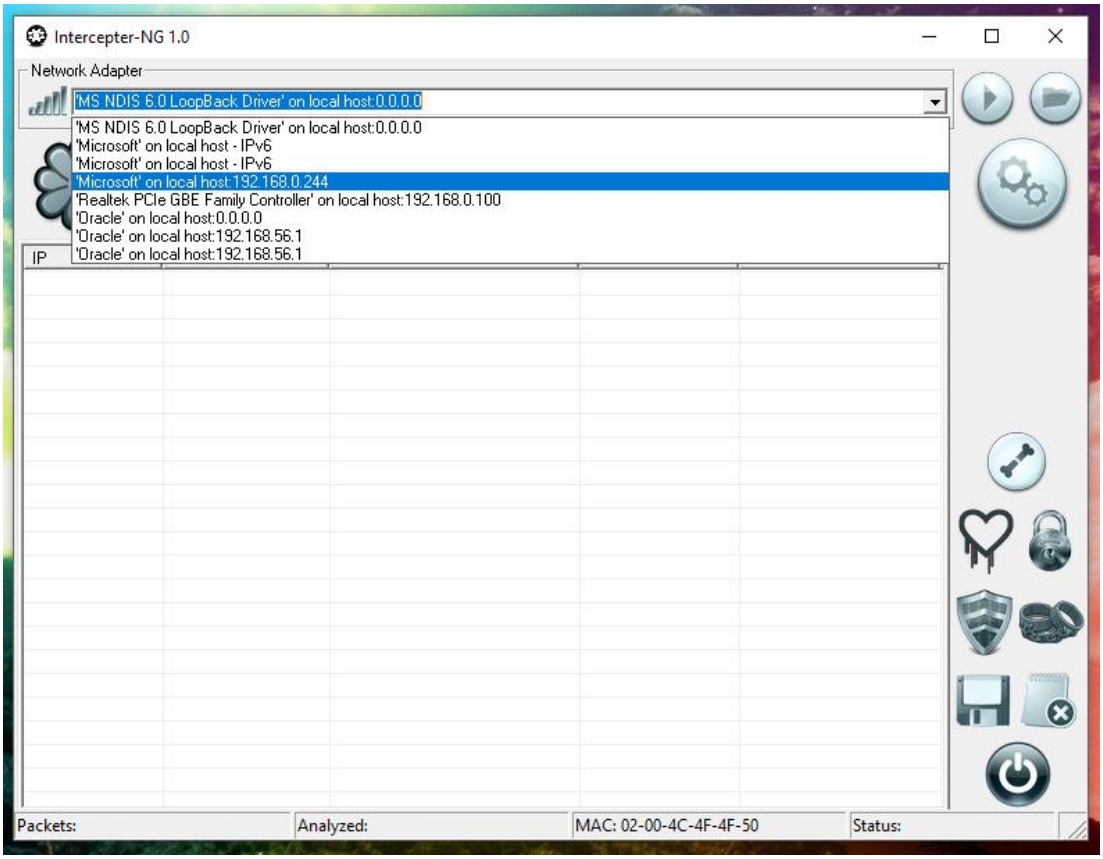
Атака человек-посередине в Intercepter-NG

Начнём с обычной атаки человек-посередине (атака посредника).

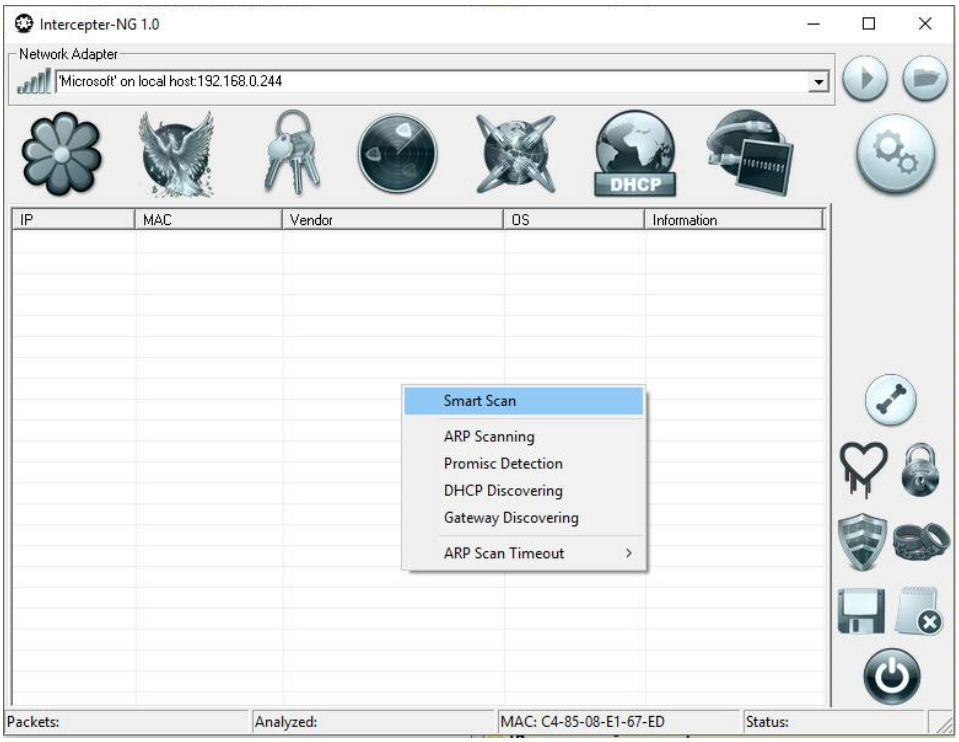
Сделаем небольшие настройки. В зависимости от того, подключены вы по Wi-Fi или по Ethernet (проводу), кликая на выделенную иконку перейдите в нужный режим (если соединены по проводу – выберите изображение сетевой карты, если по беспроводной сети, то выберите изображение с уровнем сигнала):



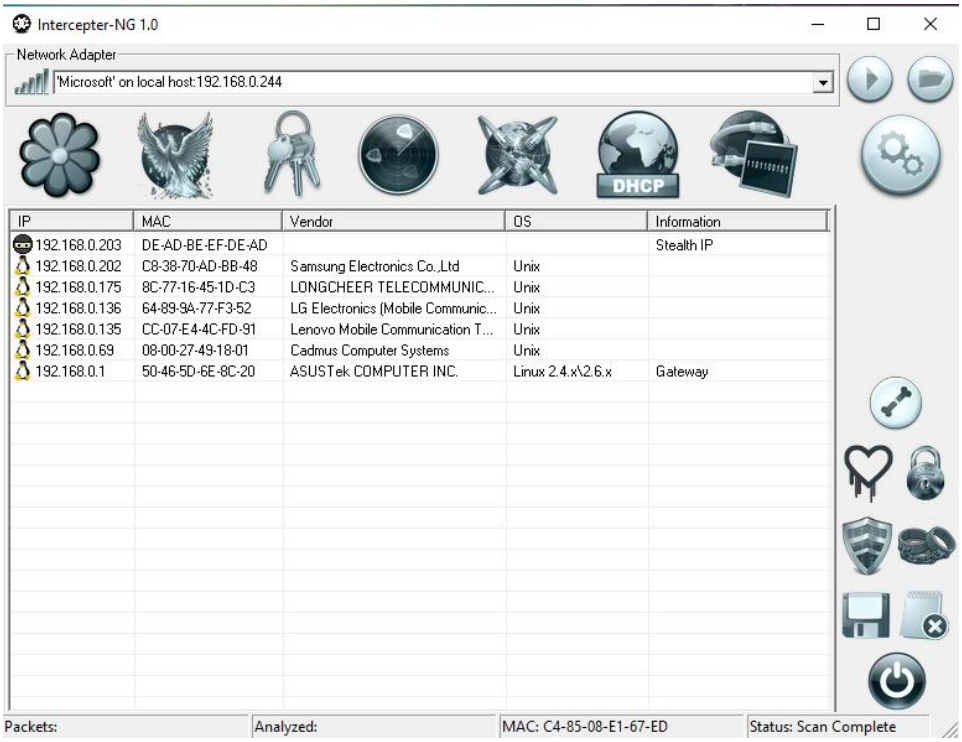
Также откройте выпадающий список сетевых адаптеров (**Network Adapter**). У меня всё работает, когда я выбираю вариант со своим IP адресом (т.е. 'Microsoft' on local host: 192.168.0.244):



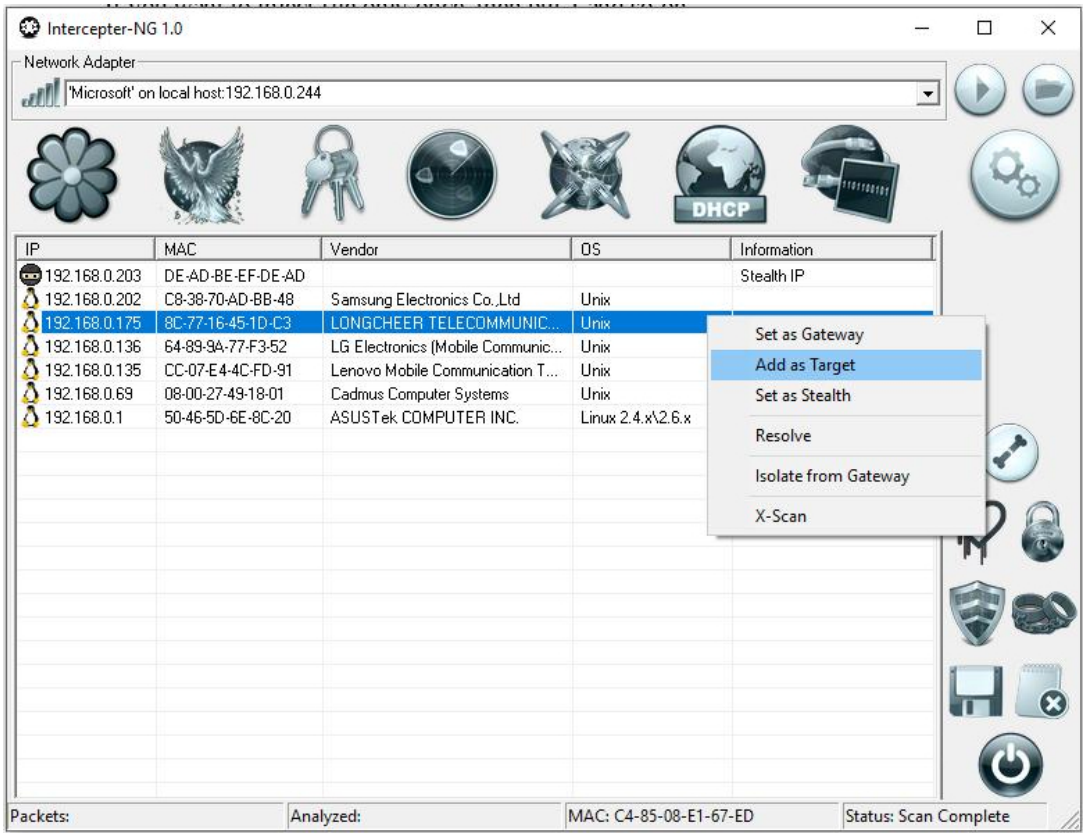
Кликните правой кнопкой по пустой таблице и выберите **Smart Scan**:



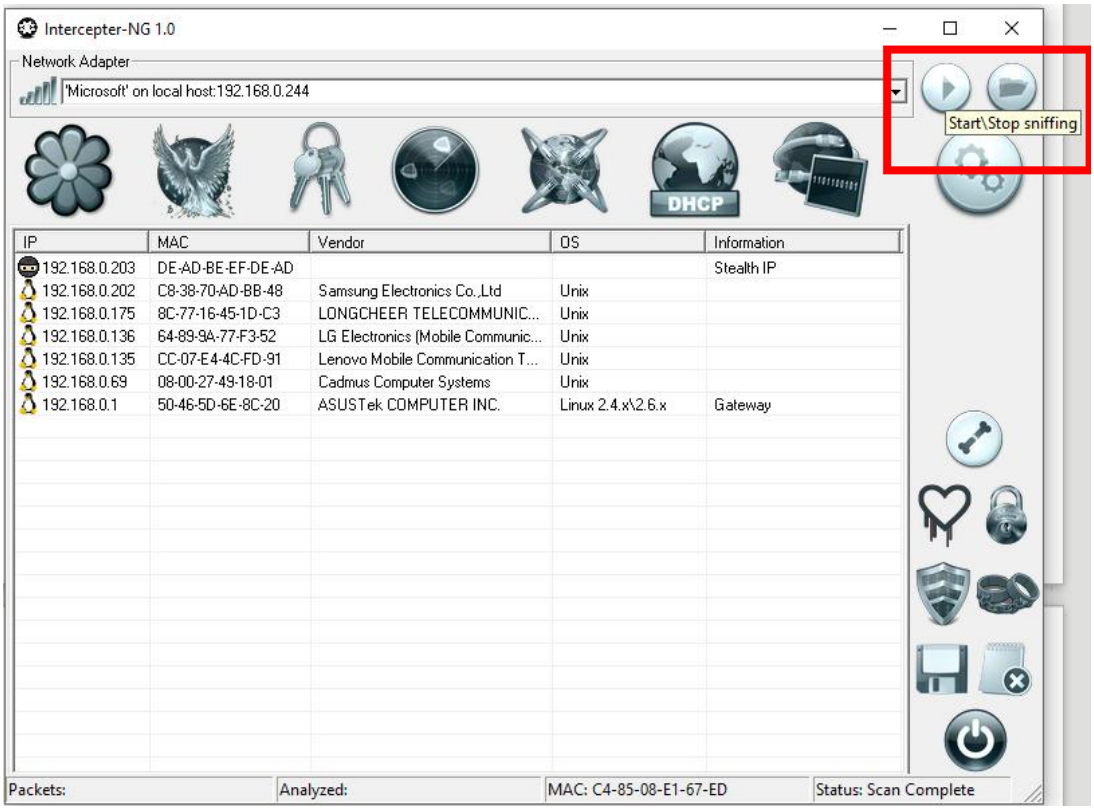
Будет отображён список целей:



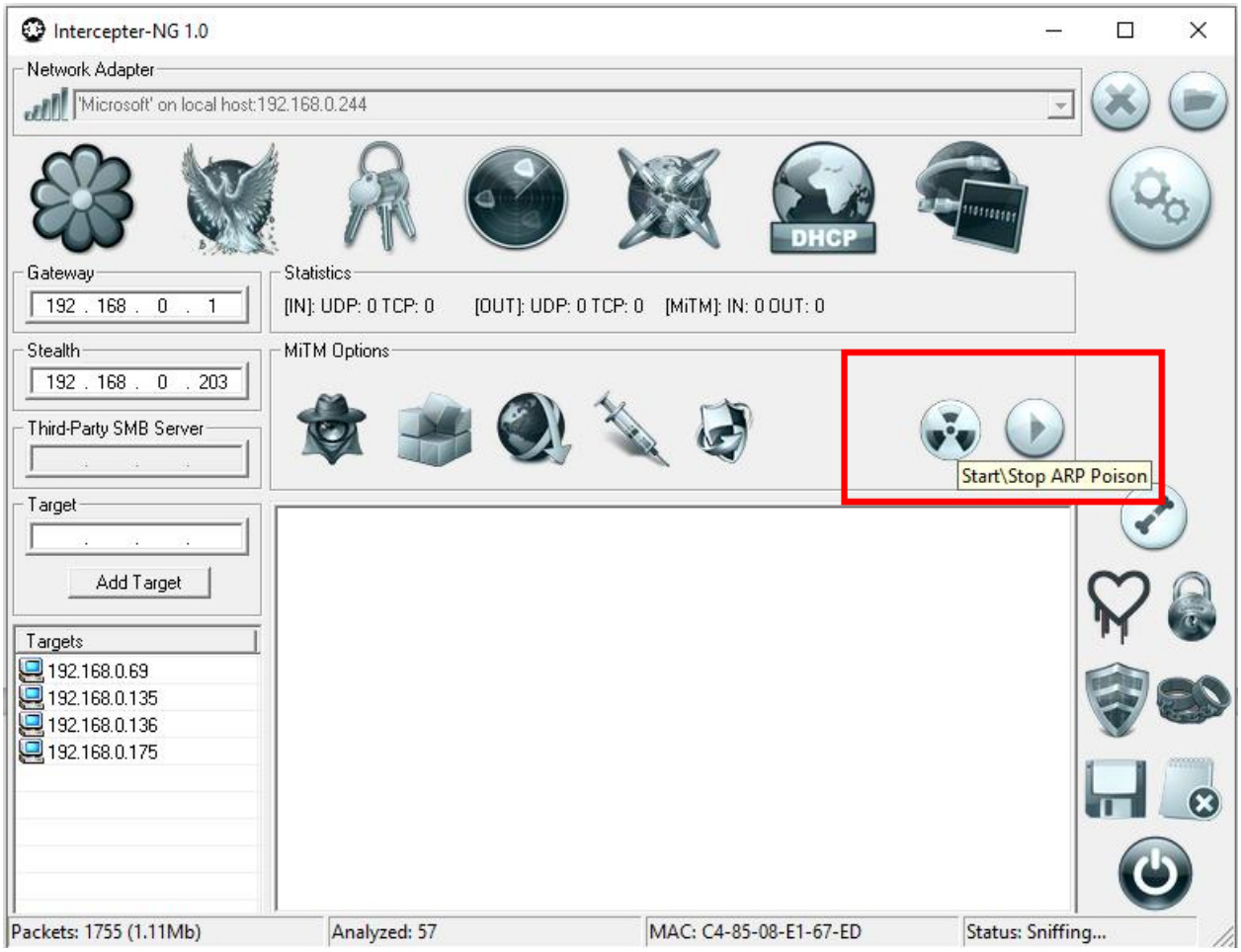
Добавьте нужные в качестве целей (**Add as Target**):



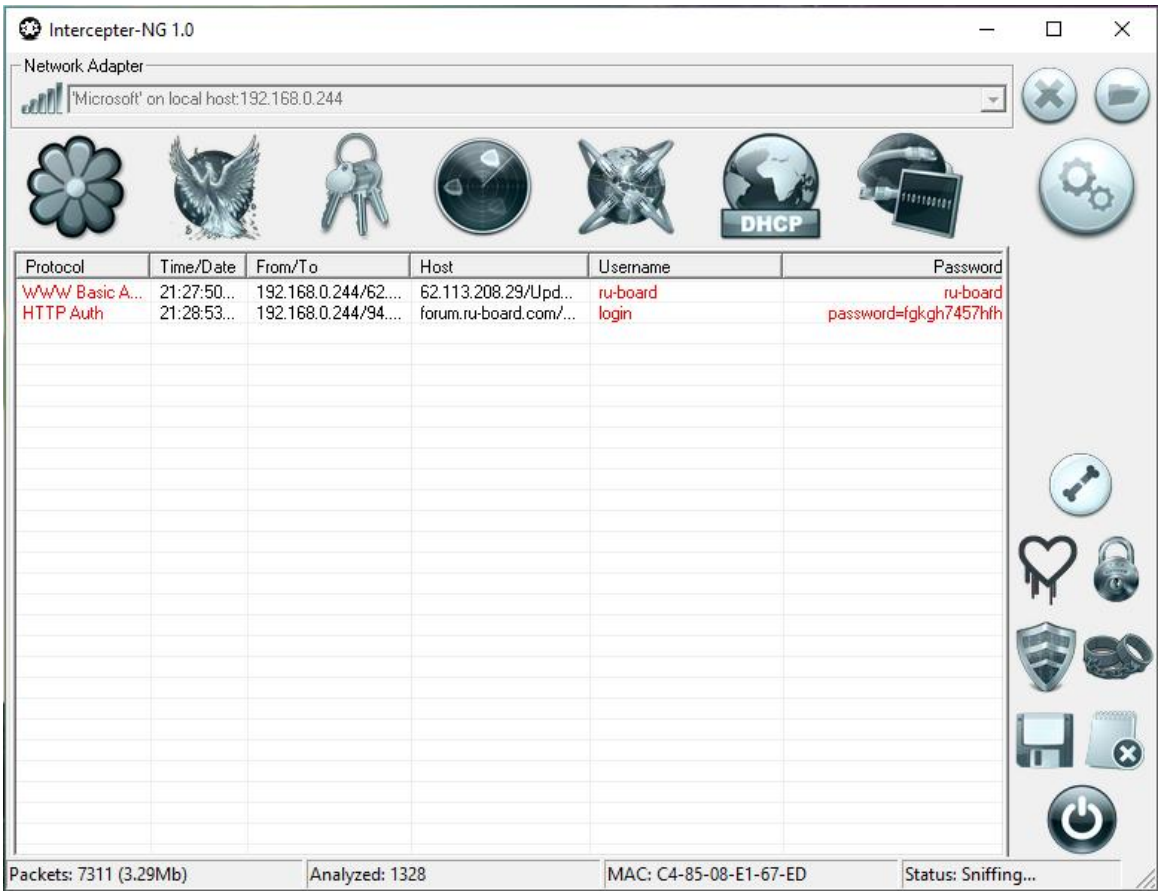
Для начала сниффинга нажмите соответствующую иконку:



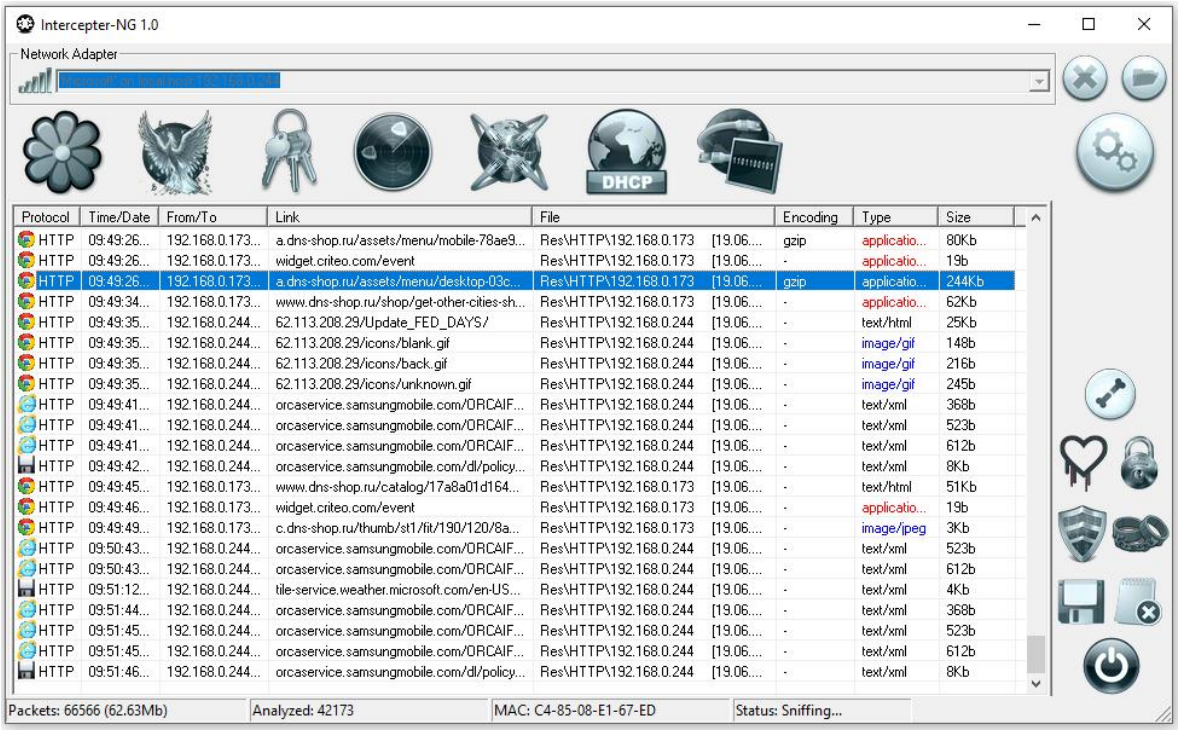
Перейдите на вкладку **MiTM mode** (это глобус с патч-кордами) и нажмите иконку **ARP Poison** (символ радиационной опасности):



Во вкладке **Password Mode** (символ — связка ключей), будут появляться захваченные учётные данные:



На вкладке **Resurrection** (кнопка с птицей Феникс) вы можете видеть, какие файлы были переданы:



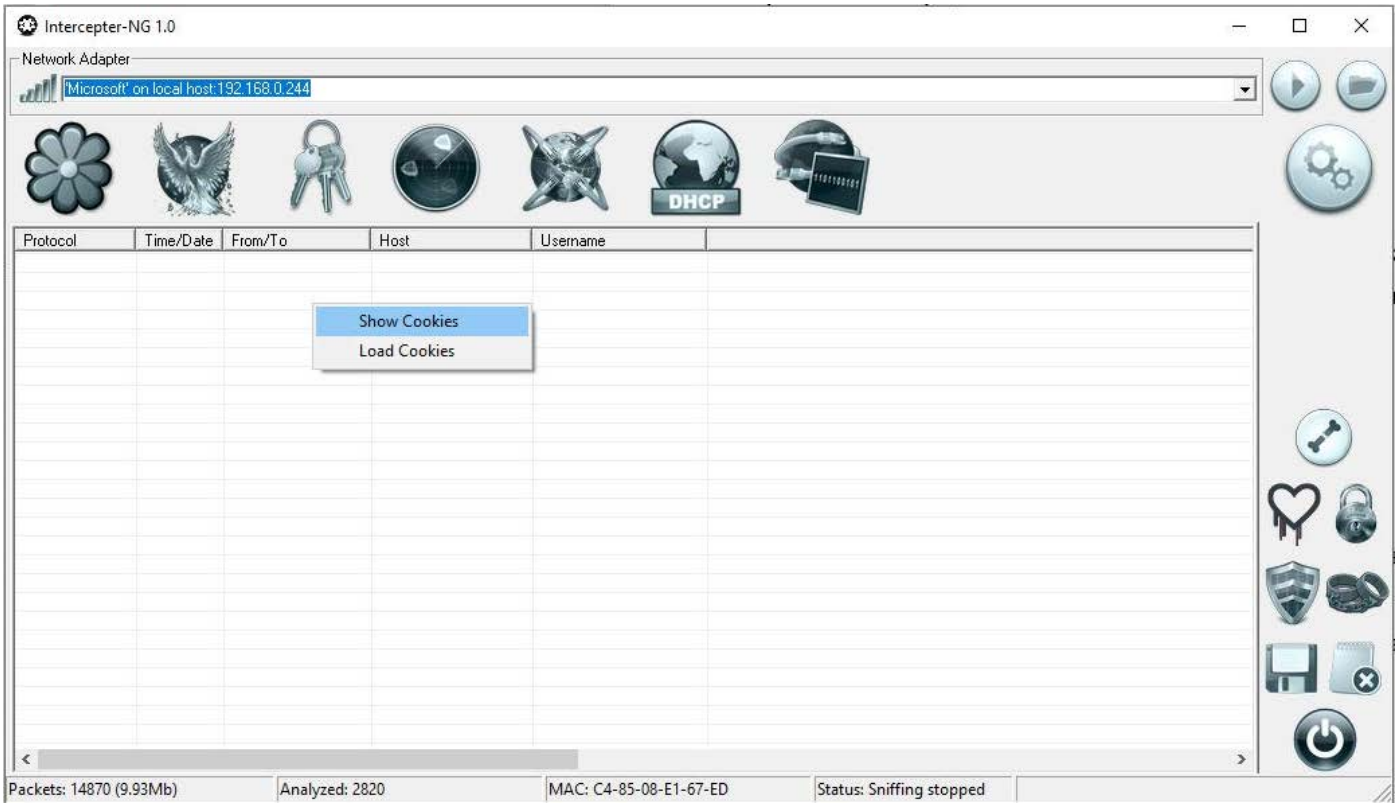
Была рассмотрена базовая атака, позволяющая:

- перехватывать логины и пароли;
- видеть, какие сайты посещает пользователь и какие файлы скачивает.

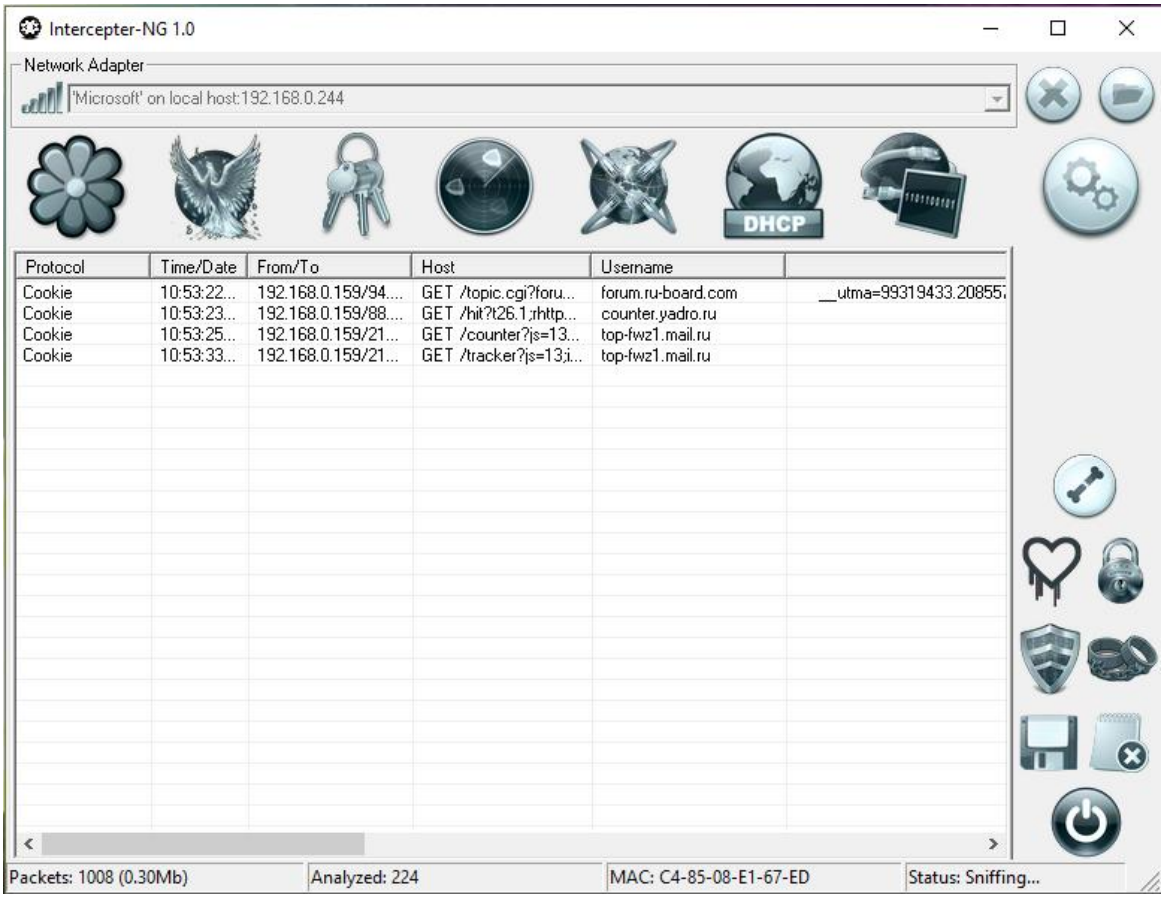
Базовая атака включает в себя сканирование локальной сети, выбор целей, запуск сниффинга и запуск ARP-травления. С этих действий начинается и ряд других, более сложных атак.

Вход на сайт с перехваченными куки

Программа может перехватывать не только учётные данные и файлы. Также перехватываются cookies. Используя эти куки можно войти под тем же пользователем, что и жертва на сайт без ввода пароля. Начните базовую атаку. Перейдите во вкладку **Паролей** (на иконке связка ключей), кликните правой кнопкой пустом поле таблицы и поставьте галочку **Show Cookies**:



Вы увидите перехваченную куки:



Кликните по записи правой кнопкой мыши и выберите **Open in browser** – откроется посещённая пользователем страница, при этом вы будете залогинены под пользователем, которому принадлежит куки.

Обнуление куки для провоцирования ввода логина и пароля

Куки могут со временем быть обновлены, и мы не сможем вновь зайти со старыми куки на сайт. Поэтому нам хотелось бы получить логин и пароль. Но пока куки действуют, пользователю не нужно вводить учётные данные каждый раз, поэтому хотя «жертва» и заходит на сайт, мы не можем их перехватить.

Чтобы не ждать, пока истечёт срок действия куки и на целевом компьютере понадобиться ввести учётные данные, мы можем ускорить этот процесс – обнулить куки. Для этого имеется специальная опция: Cookie Killer.

Cookie Killer — обнуляет кукиз, тем самым принуждая пользователя повторно авторизоваться — ввести логин и пароль, чтобы атакующий мог их перехватить. Функция Cookie Killer работает и для SSL соединений. Имеются черные (misc\ssl_bl.txt) и белые списки (misc\ssl_wl.txt). В них можно исключить или напротив жестко указать IP адреса или домены, к которым следует или не следует применять SSL MiTM. При указании extra ssl port нет необходимости указывать тип read\write, достаточно указать номер порта. Весь трафик пишется в ssl_log.txt.