Бородин Г. А., Москаленко Н. А., Созина А. А.

**Обзор атак на DHCPv4. Методы защиты.**

УДК: 004.056.53

В данной статье рассмотрена специфика работы DHCPv4, исследованы инструменты настройки протокола и основные виды атак, а также приведены наиболее эффективные методы защиты. На практике, используя средства операционной системы «ALT Linux» и графического симулятора сети «GNS3», продемонстрирована их работа и представлены их особенности функционирования.

*Ключевые слова:* атаки на DHCPv4, методы защиты, ALT Linux, isc-dhcp-server, dnsmasq, Spoofing, Starvation, Rogue, DoS, Denial of Service, Yersinia, GNS.

**1. Введение**

DHCP (Dynamic Host Configuration Protocol) – протокол прикладного уровня, обеспечивающий автоматическую настройку IP-адресов и других сетевых параметров. Несмотря на свою простоту, он является незаменимым и актуальным инструментом в области сетевых инфраструктур, позволяя из одной точки эффективно управлять большим количеством устройств.Как и большинство других широко применяемых протоколов, DCHP не обошел стороной мир хакерских атак, изучению которых и посвящена данная работа. Для достижения поставленной цели, были решены следующие задачи:

– изучены теоретические основы и особенности работы с DHCP;

– рассмотрены и протестированы на практике инструменты для взаимодействия с протоколом;

– проанализированы существующие методы атак на DHCP;

– исследованы и смоделированы на практике наиболее эффективные методы борьбы с ними.

# 2. Анализ и применение инструментов работы с DHCP

Dynamic Host Configuration Protocol (DHCP) – протокол, благодаря которому устройства могут автоматически получать IP-адрес и другие необходимые параметры сети, такие как маска, адрес шлюза или DNS-сервера. IP-адрес, получаемый клиентом, выдается ему не навсегда, а на определенное время аренды, называемой «lease». Данный параметр будет зависеть от того, как долго клиенту DHCP-сервера будет требоваться соединение.

Для того, чтобы осуществить всю функциональность протокола, существует большое количество различных инструментов. Благодаря их разнообразию, администраторы могут выбрать подходящие решения в соответствии с потребностями своей сети и задачами, которые им предстоит выполнить. Для рассмотрения в данной работе были выбраны dhcp-server (isc-dhcpd-4.4.3-P1) и dnsmasq version 2.90 [1].[[1]](#footnote-1) Для тестирования инструментов будет использоваться, российская операционная система, ALT Linux 10.1, а также, графический симулятор сети, GNS3 2.2.34 совместно с программой для анализа сетевого трафика – Wireshark Version 4.2.0.

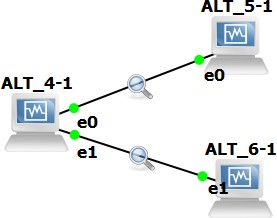


Рисунок 1 – Топология

В представленной на рисунке 1 топологии ALT\_4 является DHCP-сервером, а ALT\_5 (подсеть 192.168.50.0/24) и ALT\_6 (подсеть 172.16.50.0/24) – клиентами.

**2.1. isc-dhcp-server**

Для настройки DHCP-сервера в рамках isc-dhcp-server необходимо скачать пакет при помощи «apt-get install dhcp-server» и применить в конфигурационном файле /etc/dhcp/dhcpd следующие опции. «subnet» – сеть, для которой будет работать данная группа настроек. Она обязательно должна соответствовать используемой на одном из сетевых интерфейсов сервера. «range» – диапазон, из которого будут браться IP-адреса. «option subnet-mask» – маска сети. «option domain-name-servers» – через запятую перечисленные DNS-сервера. «option domain-name» – суффикс доменного имени. «option routers» – шлюз по умолчанию. «option broadcast-address» – адрес сети для широковещательных запросов. «default-lease-time» и «max-lease-time» – время и максимальное время в секундах, на которое клиент получит адрес, по его истечению будет выполнено продление срока [2].[[2]](#footnote-2)

После изучения основ можно переходить к заполнению конфигурационных файлов. Первым делом в /etc/sysconfig/dhcpd обозначим значение переменной «DHCPDARGS», которая устанавливает сетевой интерфейс, связанный с DHCP-сервером (в нашем случае enp0s3 и enp0s8).

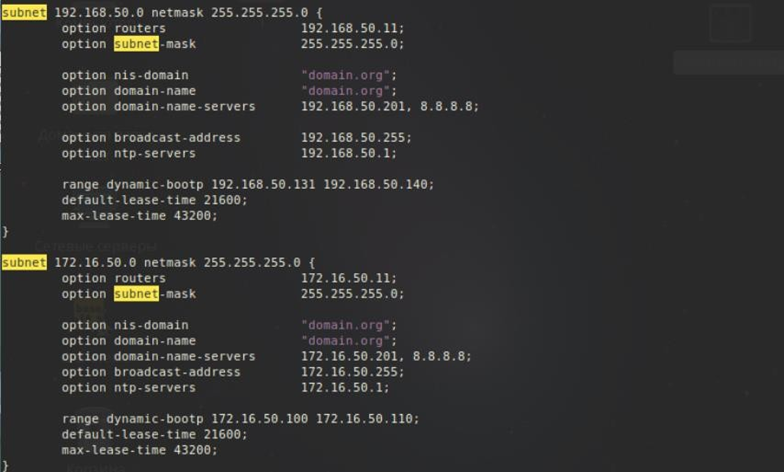


Рисунок 2 – Конфигурация /etc/dhcp/dhcpd.conf

Следующим шагом редактируем файл /etc/dhcp/dhcpd.conf. В приведенной на рисунке 2 конфигурации можно выделить настройки для двух используемых подсетей. Каждая из них начинается с subnet <сеть>, чтобы обозначить сеть, для которой будет работать данная группа настроек. Проверить корректность заполнения файла можно при помощи команды «dhcpd –t» [3].[[3]](#footnote-3)

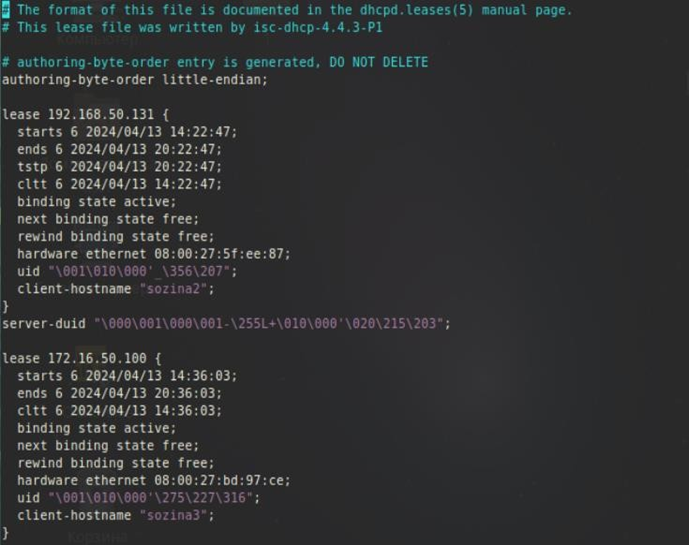


Рисунок 3 – Содержимое файла /var/lib/dhcp/dhcpd/state/dhcpd.leases

Теперь выполняем команды «systemctl start dhcp-server» и «systemctl status dhcp-server», для запуска и проверки корректности конфигурации. Включаем машины ALT\_5 и ALT\_6. Как видно из рисунка 3, после этого в файле /var/lib/dhcp/dhcpd/state/dhcpd.leases появятся соответствующие записи, демонстрирующие, что сервер работает и выдает адреса в аренду [4].[[4]](#footnote-4) Также удостовериться в этом можно проверив IP-адреса на машинах при помощи «ip –br a»: ALT\_5 займет 192.168.50.131/24 – первый адрес, из предоставленного для нее диапазона, а ALT\_6 –172.16.50.100/24

**2.2. dnsmasq**

Как и в предыдущем пункте для настройки dnsmasq произведем скачивание советующего пакета, используя команду «apt-get install dnsmasq». Все настройки будут производиться в файле /etc/dnsmasq.conf [5].[[5]](#footnote-5)

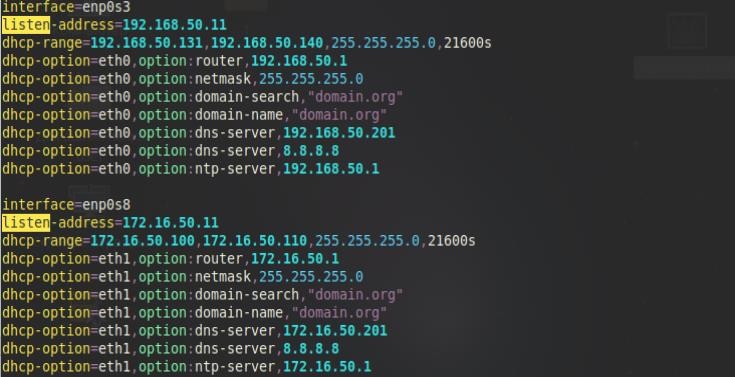


Рисунок 4 – Конфигурация /etc/dnsmasq.conf

Для демонстрации работы данного инструмента была взята первая конфигурация и синтаксически изменена под стандарты dnsmasq. После редактирования файла, рисунок 4, сервис был успешно запушен вместе с двумя оставшимися машинками. В результате применения настройки ip-адрес на ALT\_5 станет 192.168.50.140/24, а на ALT\_6 – 192.168.50.140/24. Однако необходимо обратить внимание на то, что машине ALT\_5 присвоилось значение не из начала, а из конца диапазона. Произойти это могло по той причине, что при работе DHCP-сервера порядок выдачи адресов может не всегда совпадать с последовательностью в диапазоне. DHCP клиенты могут запрашивать адреса в несколько другом порядке и в разных интервалах, что может привести к различиям в полученных адресах.

# 3. Виды атак на DHCP

Несмотря на то, что представленные ниже атаки является классическими и базовыми, они не перестают быть актуальными и востребованными, в первую очередь, потому что подобные атаки до сих пор являются эффективными и относительно легкими в исполнении даже для злоумышленников с небольшими навыками. Кроме того, это связано с недостаточным уровнем защиты. Многие компании могут уделять меньше внимания безопасности DHCP, в сравнении с другими уровнями защиты, что делает их подверженными рискам [6].[[6]](#footnote-6)

DHCP Spoofing – злоумышленник выдает себя за DHCP-сервер и отправляет ложные ответы клиентам, представляясь как шлюз по умолчанию или DNS-сервер, тем самым начиная посредническую атаку[[7]](#footnote-7)[7]. Таким образом пользовательский трафик может быть перехвачен прежде, чем выполнится пересылка на верифицированный шлюз, или же выполнится DoS-атака, по окончании которой настоящий DHCP-сервер будет заполнен запросами к ресурсам стека IP-адресов. Основные функции, которые реализует DHCP-Snooping:

– защищает клиентов внутри сети от получения адреса от DHCP-сервера, не прошедшего процесс авторизации;

– устанавливает, какие пакеты сообщений протокола DHCP требуется отфильтровать, какие и куда конкретно перенаправить с уточнением портов;

– взаимодействует с базой данных привязки портов, внутри которой содержится большой объём информации касательно надёжности хостов, с развёрнутым описанием тех, которым не стоит доверять.

DHCP Starvation (истощение ресурсов DHCP), как правило, направлена на глобальные DHCP-серверы с единственной задачей: переполнить сообщениями вида DHCP REQUEST ранее авторизованный в системе DHCP-сервер, сделав это при помощи поддельных MAC-адресов источника. Системный DHCP будет работать в штатном режиме, отвечая на все приходящие запросы, однако вскоре данная атака с истощением DHCP истощит пул DHCP, назначая на каждый из запросов доступные в системе IP-адреса[[8]](#footnote-8)[8]. При атаке DHCP Starvation происходят следующие процессы:

– Подмена DHCP-запросов: злоумышленник осуществляет отправку DHCP-запросов, в которых непосредственно используются поддельные MAC-адреса, а также идентификаторы устройств в сети. Такие запросы запрашивают у DHCP-сервера распределение IP-адреса на указанный список устройств.

– Перенасыщение DHCP-пула: IP-адреса, выданные DHCP-сервером согласно ложным запросам, истощают общий пул, и по мере увеличения ложных запросов, доступные адреса в DHCP-пуле заканчиваются.

– Последствия истощения пула: плановые устройства, для которых необходимо получить IP-адрес при помощи DHCP, отрезаны от возможности получения доступа к списку свободных адресов, ведь они все уже ранее были выделены ложным устройствам.

– Отказ в возможности доступа к сети: различные устройства, которым не удалось получить IP-адрес, не могут выполнить конкретную конфигурацию для дальнейшей работы в сети. Это приводит к ограничению их доступа в сетевые ресурсы.

DHCP Rogue - злоумышленник устанавливает фальшивый DHCP сервер в сети для осуществления подмены при выдаче различных сетевых параметров, в том числе, и ложных IP-адресов[[9]](#footnote-9)[9].

Такая угроза зачастую приводит к перехвату сетевого трафика и другим видам атак. Вскоре, после успешного подключения в сеть благодаря физическому доступу к сети или путем получения доступа к устройству, которое ранее находилось внутри сети, DHCP-сервер злоумышленника запускает процесс выдачи ложных IP-адресов, установки шлюзов по умолчанию, серверов DNS и других сетевых параметров, направленный на устройства в сети. Обыкновенные устройства, ранее подключенные в сеть, начинают автоматически получать весь перечень ложных параметров.

Таким образом злоумышленник имеет возможность к манипулированию всем сетевым трафиком, который проходит через DHCP-сервер, принадлежащий ему. Процесс работы с сетевым трафиком может включать в себя получение паролей, данных о сеансах пользователей и любой другой конфиденциальной информации[[10]](#footnote-10)[10].

Основное отличие описываемого метода DHCP Rogue от DHCP Spoofing в том, что в Spoofing атакующий отправляет ложные ответы от своего реального IP адреса, тогда как в случае Rogue он создает фальшивый DHCP сервер с другим IP адресом в сети.

DHCP Denial of Service (DoS) - злоумышленник перегружает DHCP-сервер запросами или фальшивыми пакетами, что зачастую приводит к отказу обслуживания внутренних клиентов, невозможности получить IP адрес и общему нарушению работы сети.

Отказ в обслуживании (DoS). Такое может происходить, когда DHCP-сервер исчерпал список доступных IP-адресов. Исчерпания списка приводит к отсутствию возможности получения доступа к сети новым устройствам. Таким образом, взаимодействие этих устройств с сетью становится нереализуемым[[11]](#footnote-11)[11].

# 4. Экспериментальное исследование

Для тестирования атак будут использоваться, как и предыдущем пункте, российская операционная система, ALT Linux 10.1, графический симулятор сети, GNS3 2.2.34 и встроенная в него реализация коммутаторов, а также Wireshark Version 4.2.0 [12].[[12]](#footnote-12)

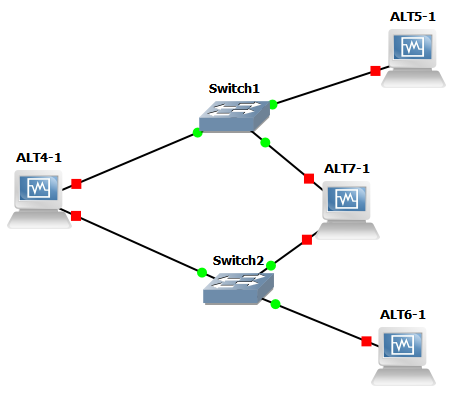


Рисунок 5 – Топология, используемая для проведения атак

Методика проведения атак на DHCP сервер, реализованный по средствам вышеописанных инструментов имеет одинаковую последовательность и способы реализация, злоумышленник подключается к коммутатору и посредствам вредоносного ПО осуществляет ниже описанные действия.

Осуществление атак типа DHCP Starvation и DoS выполняется одним способом, но перед тем как начать реализацию, разберемся в ее механизме. DHCP-сервер управляет таблицей соответствия, где каждому IP-адресу сопоставлен определенный MAC-адрес клиента. Это предотвращает возможность выдачи одного и того же IP-адреса разным клиентам. Суть атаки на DHCP заключается в исчерпании ресурсов сервера: отправляются фальшивые запросы DHCP-Discover с произвольными MAC-адресами. В ответ на каждый такой запрос сервер резервирует один из своих IP-адресов, что в итоге приводит к его невозможности обслуживать запросы легитимных пользователей на протяжении времени проведения атаки. Для начала атаки выбираем использование протокола DHCP с опцией «отправка обнаруженных пакетов», после чего начинаем транслировать поддельные пакеты DHCP-DISCOVER.

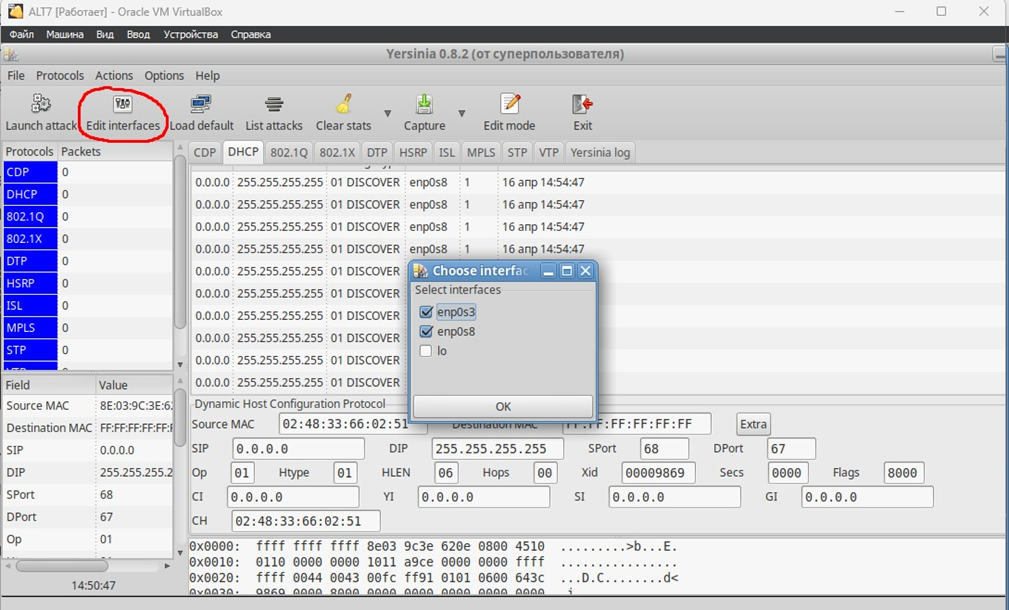


Рисунок 6 – Включение отправки на порты enp0s3 и enp0s8

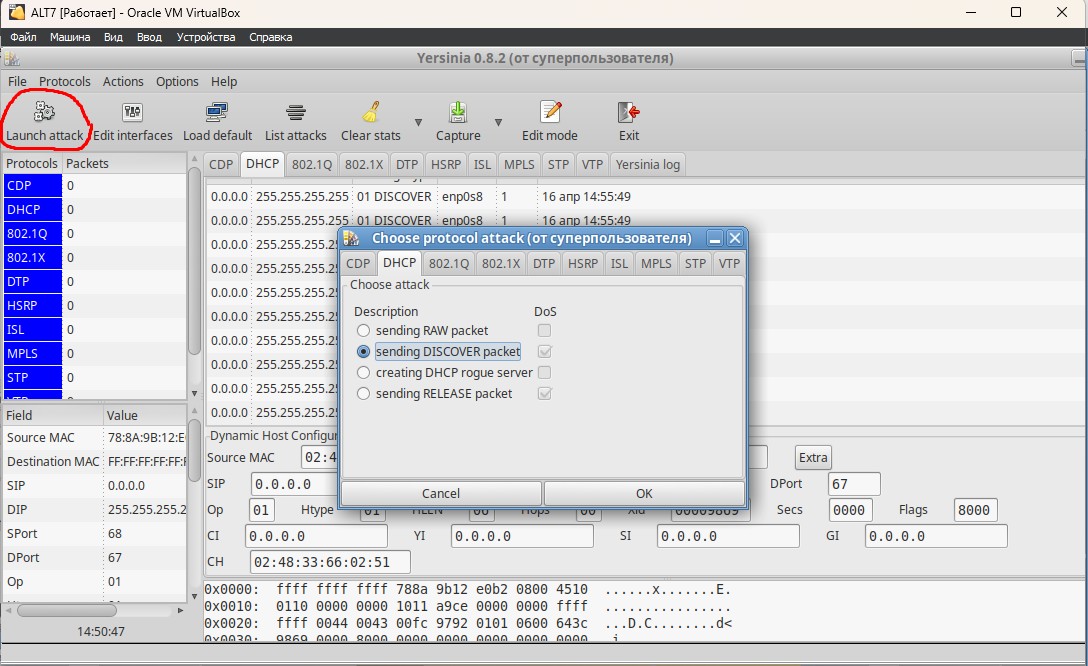


Рисунок 7 – Запуск трансляции поддельных пакетов

Пока сервер заполняется поддельными пакетами, давайте рассмотрим пул адресов DHCP. Весь диапазон адресов от 192.168.1.2 до 192.168.1.254 уже занят на DHCP-сервере. Во время активного «флуда» сервер не способен выделять IP-адреса из своего пула новым клиентам, так как его ресурсы полностью исчерпаны. Кроме того, такой «флуд» может привести к сбоям в работе DHCP-сервера из-за перегрузки. Оценим, как это повлияло на загрузку процессора маршрутизатора (введем команду htop).

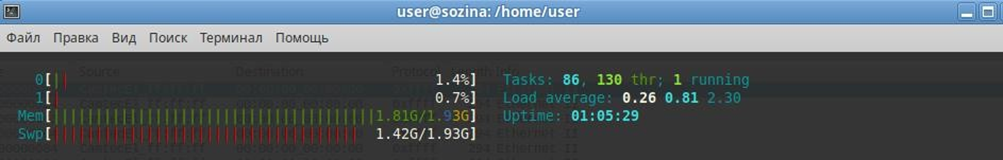


Рисунок 8 – Показатель загруженности оперативной памяти и пространства подкачки

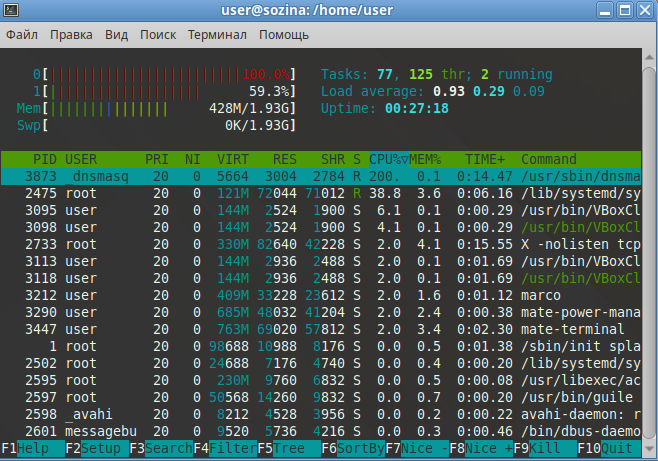


Рисунок 9 – Таблица запущенных процессов ALT4 с настройкой dnsmasq (DHCP сервер)

Как видно на рисунке 9, текущая загрузка процессора составляет 100%. При достижении максимальной нагрузки, существует риск, что DHCP-сервер может перестать функционировать на период до 12 часов [13].[[13]](#footnote-13)

Для атак DHCP Spoofing и Rogue, выполняющихся одинаково, необходимо установить мошеннический DHCP-сервер. Этот сервер будет использоваться для распространения фальсифицированных сетевых настроек (включая адрес шлюза по умолчанию) для выполнения атак типа «человек посередине» (MITM). Для злоумышленника оптимальный сценарий начинается с деактивации легитимного DHCP-сервера, что в данном случае уже осуществлено. В инструментарии Yersinia присутствует функционал под названием «создание DHCP Rogue сервера». Для его активации необходимо настроить несколько параметров: адрес поддельного сервера, чтобы он мог выдавать сетевые параметры от своего имени, диапазон выдаваемых IP-адресов, продолжительность аренды IP-адреса (чем дольше, тем лучше), маска подсети и, что наиболее важно, адрес шлюза по умолчанию — устройство, которое будет перехватывать трафик пользователей [14].[[14]](#footnote-14)

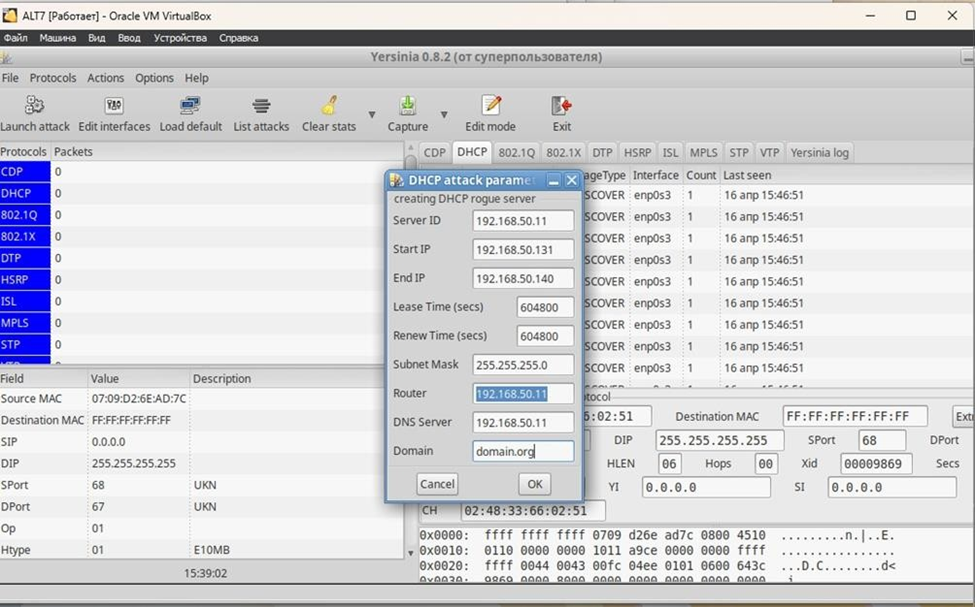


Рисунок 10 – настройка ALT7 (злоумышленник) в качестве подменного DHCP сервера

Переведем сетевой интерфейс компьютера, используемого для перехвата данных, в режим маршрутизации. В результате, клиентские устройства, настроенные на автоматическое получение IP-адресов, начнут отправлять широковещательные запросы DHCP-Discover и, как следствие, будут получать сетевые настройки от нашего мошеннического DHCP-сервера.

Таблица 1. Выводы по результатам проведения атак

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование атаки на сервер DHCP | Суть атаки | Опасность проведенной атаки для сети | Методы защиты |
| Spoofing (Rogue) | Подмена основного сервера до приостановки проведения DoS атаки. | Перехват любых данных, отправляющихся с клиентских компьютеров. | Подключение технологии DHCP Snooping на коммутаторах: указание для каких VLAN необходимо обрабатывать DHCP-пакеты и каким порттам можно «доверять». |
| Starvation (DoS) | DHCPD: | | Активации режима port-security на портах коммутаторов (ограничение числа MAC-адресов) и указание вида реагирования при превышении заданного порога. Также эффективным способом является ограничение скорости обработки пакетов. |
| Прекращение приема спам пакетов при продолжительной отправке. | Большая нагрузка на процессор и оперативную память сервера. |
| DNSMASQ: | |
| Прекращение приема спам пакетов осуществляется только посредствам дополнительных инструментов защиты. | Нагрузка на процессор еще больше, чем для сервера настроенным dhcpd, но меньшая нагрузка на оперативную память. |

В таблице 1 были подведены итоги практического исследования, содержащие информацию о успешности проведения атак, их опасности для сети, а также методах защиты.

# 5. Методы защиты от атак на DHCP

Рассмотрим технологии безопасности, предотвращающие DHCP-атаки. Условно их можно разделить на два направления: защита от «истощения» DHCP и от подмены DHCP. В большинстве случаев атаки на протокол DHCP нейтрализуются при помощи технологии DHCP Snooping, которую следует использовать в сочетании с защитой портов. Каждая из технологий реализована на коммутаторах. Также концепция надёжных портов решает проблему, связанную с незапланированным внедрением в сеть DHCP-серверов, которые не прошли процесс авторизации. Доверенные системные порты позволяют пересылать DHCP-сообщения с сервера. Надежные порты подключены к DHCP-серверу. Значит, остальные порты являются ненадежными. Когда в системе включается отслеживание DHCP, по умолчанию весь перечень портов становятся ненадежным. Поэтому необходимо указать надежный порт для коммутатора. Однако, до этого обязательно включить глобальное отслеживание DHCP, а также указать VLAN, в которой он будет работать.

Ограничение скорости – очередная полезная функция отслеживания DHCP, позволяющая ограничить количество DHCP-пакетов, передаваемых внутри порта коммутатора в единицу времени (секунду). Для включения этой функции, необходимо выбрать общий диапазон ненадёжных портов и наложить ограничение, сопоставимое с расчётной нагрузкой вашей системы. Ограничение скорости позволяет ограничить доступ злоумышленнику к возможности исчерпания пула адресов из-за большого количества DHCP- запросов.

Сопоставление MAC-адресов. В составе заголовка DHCP и MAC- адреса источника, а также в заголовке Ethernet, поле CHADDR: если корректно выстроено клиент-серверное взаимодействие, то значения этих полей должны быть идентичными. Когда включена функция, позволяющая проверить корректность MAC-адреса, коммутатор сравнивает два установленных поля: если они содержат разные MAC-адреса, коммутатор удаляет их [15].[[15]](#footnote-15)

Охрана порта. Это функция безопасности коммутатора, которая не имеет ничего общего с технологией отслеживания DHCP, но играет важную роль в защите сети от DHCP-атак. Защита портов позволяет указать MAC-адреса хостов, которым разрешено передавать данные через данный порт. MAC-адрес источника в заголовке Ethernet используется для проверки; на основании ее результатов принимается решение о разрешении передачи данных через порт.

**6. Заключение**

В результате выполнения работы были изучены теоретические основы и особенности работы с DHCP, рассмотрены и протестированы на практике инструменты для взаимодействия с протоколом, проанализированы существующие методы атак на DHCP, исследованы и смоделированы на практике наиболее эффективные методы борьбы с ними.

Атаки на DHCP являются серьезной угрозой для безопасности сетей передачи информации и операционных сетей, поскольку могут привести к несанкционированному получению IP-адресов, перехвату сетевого трафика, и выполнению различных сетевых атак. Однако, существуют эффективные методы защиты от таких атак, которые могут быть реализованы администраторами сетей. Основные методы защиты включают в себя использование аутентификации DHCP, блокирование нежелательного трафика, мониторинг сетевой активности, использование защищенных протоколов, регулярные обновления и организация корректной системы аппаратного обеспечения. Реализация данных методов позволит минимизировать риски атак на DHCP и обеспечить безопасность информационных систем и сетей передачи информации.

**Литература**

1. DNSMasq As DHCP Server [сайт]. [2023]. URL: <https://wiki.dd-wrt.com/wiki/index.php/DNSMasq_as_DHCP_server> (дата обращения: 16.04.2024)

2. Зачем нужен протокол DHCP? Что такое DHCP опции (DHCP options) и зачем они нужны [сайт.]? [2023]. URL: <https://zametkinapolyah.ru/kompyuternye-seti/9-1-zachem-nuzhen-protokol-dhcp-chto-takoe-dhcp-opcii-dhcp-options-i-zachem-oni-nuzhny.html> (дата обращения: 16.04.2024)

3. DHCP сервер [сайт.]. [2022]. URL: <https://www.altlinux.org/DHCP_сервер> (дата обращения: 17.04.2024)

4. *Курячий Г.* Автоматическая настройка сети (RARP и DHCP) [Электронный ресурс]. URL: <http://ftp.altlinux.com/pub/docs/Heap/modules/dhcp.kirill/index.html> (дата обращения: 16.04.2024)

5. Настройка dnsmasq: DHCP и DNS [сайт.]. [2014]. URL: <https://mnorin.com/nastrojka-dnsmasq-dhcp-dns.html> (дата обращения: 17.04.2024)

6. *Иванов В.* Атаки DHCP [Электронный ресурс]. – URL: <https://habr.com/ru/companies/dsec/articles/333978/> (дата обращения: 20.04.2024)

7. *Михайлов А.* Атаки на DHCP. Разбираем техники DHCP Starvation и DHCP Spoofing и защиту от них [Электронный ресурс]. URL: <https://xakep.ru/2022/11/25/dhcp-hacking/> (дата обращения: 20.04.2024)

8. Атака истощения DHCP (DHCP Starvation) [сайт.]. URL: <https://service.securitm.ru/vulns/5029b549-1f7d-41be-a6dc-1b2ca6a8f523> (дата обращения: 21.04.2024)

9. DHCP. Кибрарий [сайт.]. URL: http://www.sberbank.ru/ru/person/kibrary/vocabulary/dhcp (дата обращения: 21.04.2024)

10. *Ю. Л. Конева, Н. В. Дворцов* Типовые атаки на DHCP // Молодой ученый. 2023. № 51 (498). С. 7-8.

11. Атаки канального уровня [сайт.]. [2023]. URL: <https://ru.wikipedia.org/wiki/Атаки_канального_уровня> (дата обращения: 21.04.2024)

12. *Уймин, А. Г.* Обзор систем моделирования: анализ эффективности на примере чемпионата AtomSkills-2023 // Автоматизация и информатизация ТЭК. 2023. № 11(604). С. 25-34.

13. Истощение и подмена DHCP-сервера [сайт.]. <URL:https://spy-soft.net/dhcp-starvation-dhcp-spoofing/> (дата обращения: 22.04.2024)

14. Сетевые атаки и защита от них [сайт.]. [2024]. <URL:https://tech-geek.ru/network-attacks/> (дата обращения: 22.04.2024)

**Бородин Гавриил Андреевич**

студент 3-го курса РГУ нефти и газа (НИУ) имени И.М. Губкина (119991, Москва, Ленинский пр-т., д.65), тел. +7 (499) 507-88-88, e-mail: bga9104@gmail.com.

**Москаленко Никита Алексеевич**

студент 3-го курса РГУ нефти и газа (НИУ) имени И.М. Губкина (119991, Москва, Ленинский пр-т., д.65), тел. +7 (499) 507-88-88, e-mail: nikitamoskalenko226@gmail.com.

**Созина Анастасия Алексеевна**

студентка 3-го курса РГУ нефти и газа (НИУ) имени И.М. Губкина (119991, Москва, Ленинский пр-т., д.65), тел. +7 (499) 507-88-88, e-mail: sosnaza@mail.ru.

**Overview of attacks on DHCPv4. Methods of protection.**

**Borodin G. A., Moskalenko N. A., Sozina A. A.**

This article examines the specifics of DHCPv4, examines the protocol configuration tools and the main types of attacks, and provides the most effective methods of protection. In practice, using the tools of the ALT Linux operating system and the GNS3 graphical network simulator, their work is demonstrated and their functioning features are presented.

*Keywords:* attacks on DHCPv4, protection methods, ALT Linux, isc-dhcp-server, dnsmasq, Spoofing, Starvation, Rogue, DoS, Denial of Service, Yersinia, GNS.

1. DNSMasq As DHCP Server [сайт]. URL: https://wiki.dd-wrt.com/wiki/index.php/DNSMasq\_as\_DHCP\_server [↑](#footnote-ref-1)
2. Зачем нужен протокол DHCP? Что такое DHCP опции (DHCP options) и зачем они нужны [сайт.]? [2023]. URL: https://zametkinapolyah.ru/kompyuternye-seti/9-1-zachem-nuzhen-protokol-dhcp-chto-takoe-dhcp-opcii-dhcp-options-i-zachem-oni-nuzhny.html [↑](#footnote-ref-2)
3. DHCP сервер [сайт.]. [2022]. URL: https://www.altlinux.org/DHCP\_сервер [↑](#footnote-ref-3)
4. Курячий Г. Автоматическая настройка сети (RARP и DHCP) [Электронный ресурс]. URL: http://ftp.altlinux.com/pub/docs/Heap/modules/dhcp.kirill/index.html [↑](#footnote-ref-4)
5. Настройка dnsmasq: DHCP и DNS [сайт.]. [2014]. URL: https://mnorin.com/nastrojka-dnsmasq-dhcp-dns.html [↑](#footnote-ref-5)
6. Иванов В. Атаки DHCP [Электронный ресурс]. – URL: https://habr.com/ru/companies/dsec/articles/333978/ [↑](#footnote-ref-6)
7. Михайлов А. Атаки на DHCP. Разбираем техники DHCP Starvation и DHCP Spoofing и защиту от них [Электронный ресурс]. URL: https://xakep.ru/2022/11/25/dhcp-hacking/ [↑](#footnote-ref-7)
8. Атака истощения DHCP (DHCP Starvation) [сайт.]. URL: https://service.securitm.ru/vulns/5029b549-1f7d-41be-a6dc-1b2ca6a8f523 [↑](#footnote-ref-8)
9. DHCP. Кибрарий [сайт.]. URL: http://www.sberbank.ru/ru/person/kibrary/vocabulary/dhcp [↑](#footnote-ref-9)
10. Ю. Л. Конева, Н. В. Дворцов Типовые атаки на DHCP // Молодой ученый. 2023. № 51 (498). С. 7-8. [↑](#footnote-ref-10)
11. Атаки канального уровня [сайт.]. [2023]. URL: https://ru.wikipedia.org/wiki/Атаки\_канального\_уровня [↑](#footnote-ref-11)
12. Уймин, А. Г. Обзор систем моделирования: анализ эффективности на примере чемпионата AtomSkills-2023 // Автоматизация и информатизация ТЭК. 2023. № 11(604). С. 25-34. [↑](#footnote-ref-12)
13. Михайлов А. Атаки на DHCP. Разбираем техники DHCP Starvation и DHCP Spoofing и защиту от них [Электронный ресурс]. URL: https://xakep.ru/2022/11/25/dhcp-hacking/ [↑](#footnote-ref-13)
14. Истощение и подмена DHCP-сервера [сайт.]. URL:https://spy-soft.net/dhcp-starvation-dhcp-spoofing/ [↑](#footnote-ref-14)
15. Сетевые атаки и защита от них [сайт.]. [2024]. URL:https://tech-geek.ru/network-attacks/ [↑](#footnote-ref-15)