**УДК 004.056.53**

# ТЕСТИРОВАНИЕ ЗАЩИЩЕННОСТИ ПРОТОКОЛА DHCP В СЕГМЕНТЕ КОРПОРАТИВНОЙ СЕТИ

***Веревкин Сергей Александрович, Бурлов Вячеслав Георгиевич, Краева Екатерина Витальевна, Мартын Ирма Андреевна***
*ФГБОУ ВО «Российский государственный гидрометеорологический университет», г. Санкт-Петербург, Россия*

*Аннотация.* В статье рассматривается процесс тестирования защищенности протокола DHCP посредством реализации действий, направленных на нарушение работоспособности DHCP-сервера, либо на его компрометацию с целью получения злоумышленником потенциала для проведения иных сетевых атак в корпоративной сети.
*Ключевые слова*: корпоративная сеть, уязвимость, DHCP-starvation, защита информации.

# TESTING THE SECURITY OF THE DHCP PROTOCOL IN THE CORPORATE NETWORK SEGMENT

***Verevkin Sergey, Burlov Vyacheslav, Kraeva Ekaterina, Martyn Irma***
*Russian State Hydrometeorological University,*
*Saint Petersburg, Russia*

*Abstract*. The article discusses the process of testing the security of the DHCP protocol by implementing actions aimed at disrupting the performance of the DHCP server, or compromising it in order to obtain the potential for an attacker to conduct other network attacks in the corporate network.
*Keywords*: corporate network, vulnerability, DHCP-starvation, information security.

С каждым годом, современное общество все сильнее зависит от информационных систем сетевых технологий, играющих важнейшую роль не только в функционировании отдельных организаций, но и обеспечивающих функционирование крупнейших объектов инфраструктуры.

Возможность эксплуатации уязвимостей подобных систем, является мощным механизмом воздействия как на интересы отдельно взятых корпораций, так и на крупные государственные организации. По этой причине возникает необходимость обеспечения защищенности информации, обрабатываемой в информационных системах организаций [1].

Зачастую, уязвимости связанны с недостатками программных и аппаратных сетевых решений, требующих дополнительной настройки для противодействия потенциальным атакам.

В качестве примера, рассмотрим оценку состояния защищенности сегмента корпоративной сети организации в случае атаки на протокол прикладного уровня – DHCP [2].

Создание макета, выполним на базе бесплатного средства виртуализации VirtualBox, позволяющего реализовать виртуальный сегмент сети, что позволяет оградить используемые в основной сети устройства от негативного воздействия [3].

Для реализации атак на протокол DHCP, воспользуемся популярным средством для тестирования на проникновение – Yersinia, являющегося многофункциональным инструментом с открытым исходным кодом, предназначенным для проведения атак на канальном уровне модели оси. Инструмент позволяет проводить атаки и компрометировать работу таких протоколов и служб как: STP, DHCP, CDP, DTP и многие другие [4].

DHCP Starvation.

Первым шагом, требуется вывести из строя используемый в сети DHCP сервер, для чего используем атаку DHCP Starvation [2]. Суть атаки заключается в исчерпании пула IP-адресов сети, для чего первым шагом устанавливается адрес существующего DHCP-сервера, после чего выполняется циклический запрос IP-адресов DHCP сервера для не существующих клиентов.

Для реализации DHCP-starvation выполним запуск графического режима утилиты yersinia с помощью команды:

*yersinia –G*

Затем выберем протокол DHCP и начнем проведение атаки, выбрав пункт «Sending DISCOVER packet», в результате чего будет выведен из строя активный DHCP-сервер, после чего следует приступать к следующей атаке, заключающейся в его подмене. Результат проведения атаки на DHCP-сервер представлен на Рисунке 1.

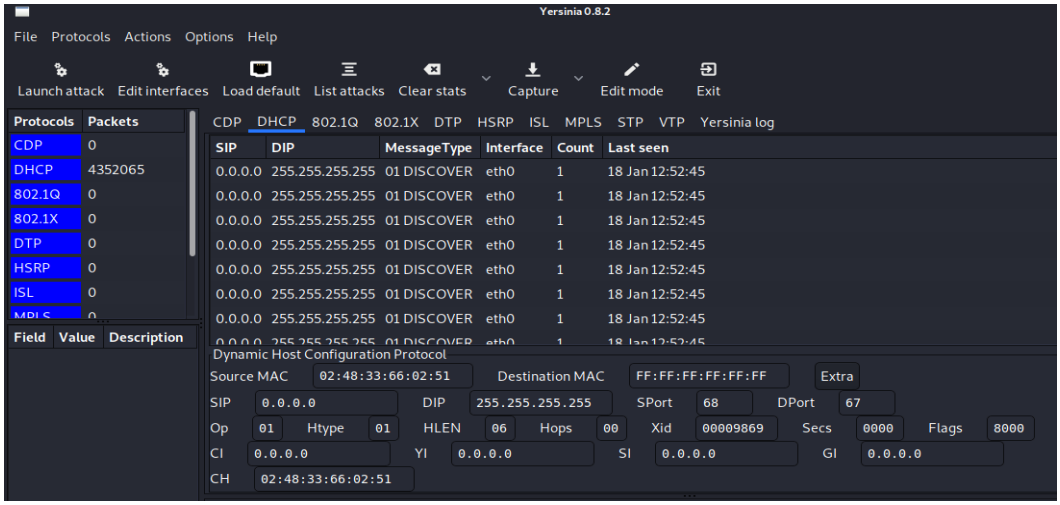


Рисунок 1 - Проведение атаки DHCP-starvation

В случае успешной атаки, продолжим развитие атаки и выполним подмену DHCP-сервера [3]. Реализация атаки, заключающейся в создании собственного DHCP-сервера может также реализовываться посредством настройки

параметров системы, однако в данной работе, рассмотрим процесс создания поддельного DHCP с помощью использованной ранее утилиты yersinia.

Алгоритм работы протокола DHCP, состоит из 4-х этапов [5]:

1. discover – опрос сети на наличие DCHP-серверов;
2. offer – получение ответа от DHCP-серверов;
3. request – запрос IP-адреса у выбранного сервера;
4. acknoledgement – получение от DHCP-сервера подтверждение аренды IP-адреса.

Выбрав DHCP протокол, выберем Creating DHCP rouge server, выполним настройку параметров создаваемого сервера, а именно:

– Server ID – адрес сервера, от имени которого будут формироваться DHCP ответы (192.168.1.1);

– Start IP/End IP – начальный и конечный IP-адреса пула DHCP сервера (192.168.1.2 и 192.168.1.40;

– Lease Time - время, на которое выделяется IP-адрес (3600 сек.);

– Renew Time - время продления занимаемого IP-адреса клиентом (3600 сек.);

– Subnet Mask – маска подсети (255.255.255.0);

– Router – адрес маршрутизатора, выдаваемы клиентам (192.168.1.10);

– DNS Server – выдаваемые клиентам DNS сервера (192.168.1.10);

– Domain – имя домена в локальной сети.

По завершении настройки выполним запуск поддельного DHCP-сервера в сегменте корпоративной сети, который может стать серьезной проблемой, поскольку с его помощью можно не только перехватывать, но и модифицировать пользовательский трафик. Результат создания поддельного DHCP-сервера представлен на Рисунке 2.

В дальнейшем, при подключении устройств к сегменту корпоративной сети, устройства будут обращаться к созданному злоумышленником DHCP-серверу, что позволит в дальнейшем не только производить сниффинг сети, но и получить сведения об оборудовании, используемом в организации.

В статье рассмотрен процесс эксплуатации уязвимостей протокола DHCP. В ходе работы были произведены атаки, на DHCP-сервер виртуального сегмента сети с целью его выведения из строя и подмены на собственный сервер [6]. Рассмотренный пример является наглядной демонстрацией эксплуатации уязвимостей, устраняемых посредством настройки работы конкретного протокола.

Простейшими средствами защиты является настройка коммутационного оборудования с функцией DHCP snooping, подразделяющий порты оборудования на «доверенные» и «недоверенные», ограничивая тем самым физическую область подключения DHCP-сервера, а также позволяющую ограничить количество DHCP пакетов на каждый порт оборудования, а в случае превышения заданного лимита позволит отследить атакующее устройство.

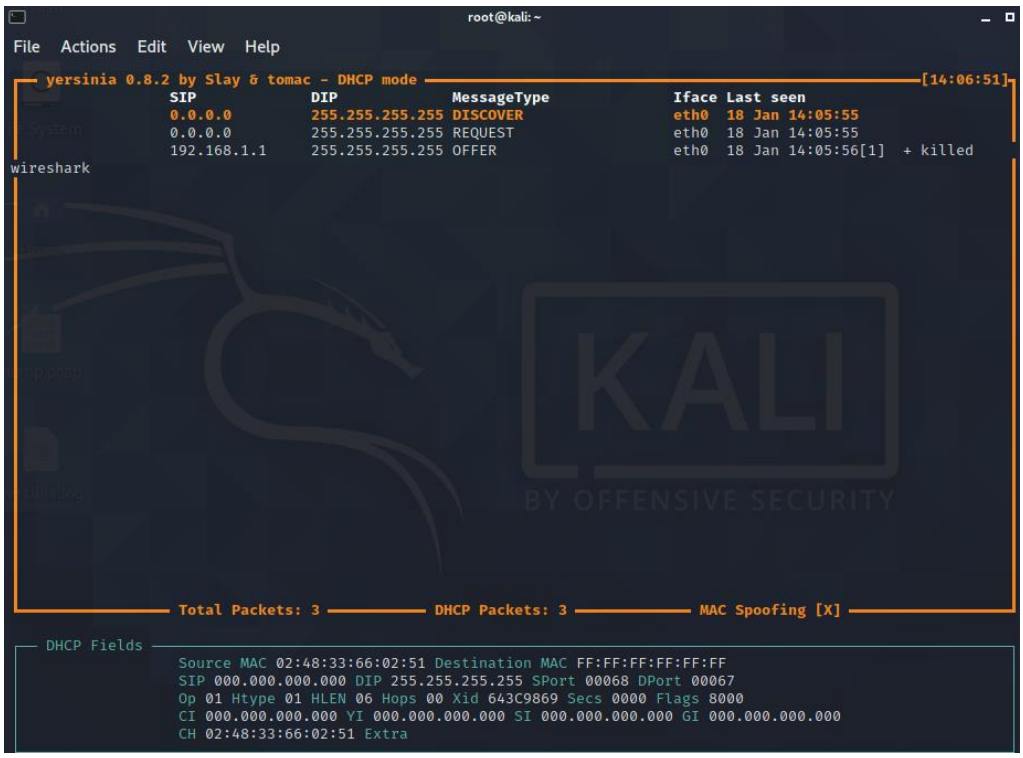

Рисунок 2 - Создание поддельного DHCP-сервера

Еще одним способом защиты от атак на DHCP, является ограничение количества MAC-адресов на порт коммутационного оборудования, таким образом данная настройка позволит избежать несанкционированного подключения оборудования со стороны злоумышленника.

## Список использованной литературы

1. Скабцов Н. «Аудит безопасности информационных систем», СПб.: Питер, 2018.

2. Сандерс К. Анализ пакетов. Практическое руководство по использованию Wireshark и tcpdump для решения реальных проблем в локальных сетях. М.: Вильямс, 2019.

3. Татарникова Т.М., Елизаров М.А. Имитационная модель виртуального канала // Научно-технический вестник информационных технологий, механики и оптики. 2016. Т. 16. № 6. С. 1120-1127.

4. Forshaw J. Attacking Network Protocols. William Pollock Publ., 2018

5. Солдатов А., Бороган И. Анонимность в Сети. Как защитить себя от Большого Брата. М.: Сахаровский центр, 2014.

6. Ali S., Heriyanto T. BackTrack 4: Assuring Security by Penetration Testing, Birmingham – Mumbai: Pckt Publ., 2011.