МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ / METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

DOI: https://doi.org/10.60797/itech.2025.5.2

СЕТЕВЫЕ АТАКИ НА УРОВНЕ СЕТЕВОГО ДОСТУПА МОДЕЛИ *TCP/IP*

Научная статья

Иванов Ю.Б.[1], Чубуткин И.А.[2,] *

[1, 2] Академия Федеральной службы охраны Российской Федерации, Орёл, Российская Федерация

* Корреспондирующий автор (chuba41[at]mail.ru)

Аннотация

В современных мультисервисных сетях связи передается большое количество данных, которые носят конфиденциальный характер. Как правило, для защиты этих данных используются методы и средства, работающие на прикладном, транспортном или сетевом уровнях модели *TCP/IP*. Защите информации на уровне сетевого доступа модели *TCP/IP* уделяется меньше внимания, несмотря на то что он также позволяет злоумышленнику получить доступ к конфиденциальной информации. Для обеспечения безопасности информации на уровне сетевого доступа модели *TCP/IP* необходимо рассмотреть уязвимости, которые может использовать злоумышленник. В статье рассмотрены сетевые атаки, которые может совершить злоумышленник на уровне сетевого доступа модели *TCP/IP*. Проведенный анализ атак позволяет сделать вывод о необходимости обеспечения защиты данных на нижнем уровне модели *TCP/IP*.

Ключевые слова: модель TCP/IP, сетевые атаки, уровень сетевого доступа модели TCP/IP, информационная безопасность.

NETWORK ATTACKS AT THE NETWORK ACCESS LAYER OF THE *TCP/IP* MODEL

Research article

Ivanov Y.B.[1], Chubutkin I.A.[2,] *

[1, 2] Academy of the Federal Security Service of the Russian Federation, Orel, Russian Federation

* Corresponding author (chuba41[at]mail.ru)

Abstract

In modern multiservice communication networks, a large amount of data of a confidential nature is transmitted. As a rule, methods and tools operating at the application, transport or network layers of the *TCP/IP* model are used to protect this data. Protection of the information on a network access level of *TCP/IP* model is given less attention, in spite of the fact that it also allows the attacker to get access to confidential information. To ensure the security of information on the network access layer of *TCP/IP* model, it is necessary to examine the vulnerabilities that can be used by an attacker. The article discusses network attacks that can be committed by an attacker at the network access level of *TCP/IP* model. The analysis of attacks allows to conclude that it is necessary to ensure data protection at the lower level of the *TCP/IP* model.

Keywords: TCP/IP model, network attacks, TCP/IP model network access layer, information security.

Введение

Современные мультисервисные сети связи позволяют обмениваться различными данными, достаточно большая часть которых носит конфиденциальный характер. Эти данные могут иметь интерес для злоумышленников, которые всеми возможными способами пытаются завладеть ими. Для защиты конфиденциальных данных используются различные методы и средства защиты информации, которые постоянно совершенствуются. Нарушителю становится сложнее получить конфиденциальные данные, передаваемые по сети связи. В связи с этим ему необходимо получить сетевую служебную информацию, которая циркулирует на уровне сетевого доступа модели *TCP/IP*, позволяющую сделать определенные выводы о сети связи и организовать более сложную атаку, а в некоторых случаях получить конфиденциальные данные (логины, незашифрованные пароли, и др.).

В [1, С. 48] рассмотрены актуальные угрозы безопасности информации для протоколов уровня сетевого доступа модели *TCP/IP*. Данные угрозы могут быть реализованы злоумышленниками при проведении различных атак на сеть связи. Рассмотрим сетевые атаки, которые могут быть совершены на сеть связи на уровне сетевого доступа модели *TCP/IP*.

Сетевой атакой называется компьютерная атака с использованием протоколов межсетевого взаимодействия. В свою очередь компьютерной атакой называется целенаправленное несанкционированное воздействие на информацию, на ресурс информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств [2, С. 3].

Условно уровень сетевого доступа модели *TCP/IP* соответствует канальному и физическому уровням модели *OSI* (см. рис. 1) [3, С. 58].

Модель *OSI*	Модель *TCP/IP*
Уровень приложений	Уровень приложений
Уровень представления	
Сеансовый уровень	
Транспортный уровень	Транспортный уровень
Сетевой уровень	Межсетевой уровень
Канальный уровень	Уровень сетевого доступа
Физический уровень	

Рисунок 1 - Условное соответствие уровней моделей *OSI* и *TCP/IP*
DOI: https://doi.org/10.60797/itech.2025.5.2.1

Атаки, реализуемые на уровне сетевого доступа модели TCP/IP

Рассмотрим атаки, реализуемые на физическом уровне. К данным атакам относятся *RJ*-45 *Sniffing*, установка в разрыв, подключение к концентратору [4, С. 33-41].

RJ-45 *Sniffing* заключается в полудуплексном прослушивании трафика, передаваемого по витой паре. Атака заключается в подключении к *TX*- или *RX*-паре специального кабеля, с одной стороны которого расположены зажимы типа «крокодил», с другой – коннектор *RJ*-45. При этом важно, чтобы в коннекторе провода, к которым присоединены зажимы, соответствовали *RX*-паре. Коннектор *RJ*-45 специального кабеля необходимо подключить к сетевой карте атакующего устройства (см. рис. 2). Для прослушивания проходящего трафика необходимо также специальное программное обеспечение, позволяющее представлять снимаемые сигналы в удобном для понимания виде. В качестве атакующего устройства возможно использование одноплатного компьютера или смартфона, что позволяет сделать такую атаку менее заметной. Таким образом, устройство негласного приема информации может быть оставлено на достаточно большой промежуток времени для сбора большого количества информации.

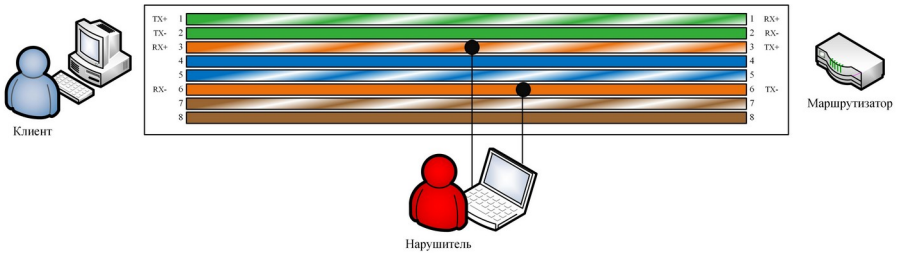

Рисунок 2 - Схема подключения нарушителя при атаке *RJ-45 Sniffing*
DOI: https://doi.org/10.60797/itech.2025.5.2.2

Атака установкой в разрыв предполагает установку атакующего устройства злоумышленника таким образом, чтобы сетевой кабель от отправителя подключался к одному порту устройства, а кабель, идущий к получателю, – к другому порту. Данная атака является атакой типа «человек посередине». Задача злоумышленника направить трафик между получателем и отправителем через контролируемый им узел. Для этого необходимо предварительно настроить перенаправление трафика и маршрутизацию.

При подключении к концентратору у злоумышленника для реализации атака нет необходимости в предварительной настройке оборудования. Концентратор, получая пакет на одном из своих портов, ретранслирует его на все остальные, при этом все устройства, подключенные к концентратору, получают отправленные пакеты. Для того чтобы прослушать весь трафик, который проходит через концентратор, злоумышленнику достаточно запустить на своем устройстве программное обеспечение, позволяющее анализировать трафик.

На канальном уровне злоумышленник может совершить следующие типы атак [5, С. 41]:

- переполнение *CAM*-таблиц;
- *VLAN Hopping*;
- атака на *PVLAN*;
- атака на *STP*;
- *MAC-Spoofing*;
- *ARP-Spoofing*;
- атака на *DHCP*.

Атака переполнения *CAM*-таблиц коммутаторов, в которых содержаться записи о соответствии физических портов *MAC*-адресам, реализуется следующим образом. В *CAM*-таблице количество записей, которые могут храниться в памяти коммутатора, ограничено. Когда *CAM*-таблиц заполнена, новые записи в нее не добавляются, а весь трафик, проходящий через коммутатор, транслируется на все порты как в концентраторе. Поэтому весь трафик, проходящий через коммутатор с переполненной *CAM*-таблицей, злоумышленник может прослушивать с помощью анализатора трафика.

Технология *VLAN* позволяет создавать полностью изолированные сегменты сети путем логического конфигурирования коммутаторов, не прибегая к изменению физической структуры [6, С. 364]. Трафик в таких сетях на канальном уровне полностью изолирован от трафика других узлов сети.

VLAN Hopping реализуется злоумышленником путем перенаправления данных из одной *VLAN* в другую. Данная атака возможна только при работе коммутатора в режиме транка. При этом злоумышленнику необходимо создать имитацию транкингового коммутатора и перевести таким образом атакуемый коммутатор в транкинговый режим работы. Другим способом реализации данной атаки является использование двойного тегирования кадра. Злоумышленник добавляет два тега *VLAN* к передаваемому кадру. Кадр, помеченный внешним идентификатором *VLAN*, к которой подключен порт злоумышленника, пересылается без первого тега, поскольку это собственный *VLAN* интерфейса транка. Затем второй тег становится виден коммутатору, и он направляет кадр во вторую *VLAN*, так как считает, что он был создан в ней [7, С. 14-15].

Для коммутаторов, поддерживающих технологию *PVLAN* (в отличие от *VLAN*), порты могут функционировать в одном из трех режимов:

1) *Isolated*;
2) *Promiscuous*;
3) *Community*.

Атака на *PVLAN* возможна только при функционировании портов в режиме *Isolated*. Для этого злоумышленнику необходимо отправить на такой порт пакет с *IP*-адресом назначения атакуемого устройства, а в качестве *MAC*-адреса назначения указать *MAC*-адрес маршрутизатора. При этом маршрутизатор, получив данный пакет, перенаправит его по указанному адресу. Атакуемое устройство в свою очередь сделает то же самое (см. рис. 3).

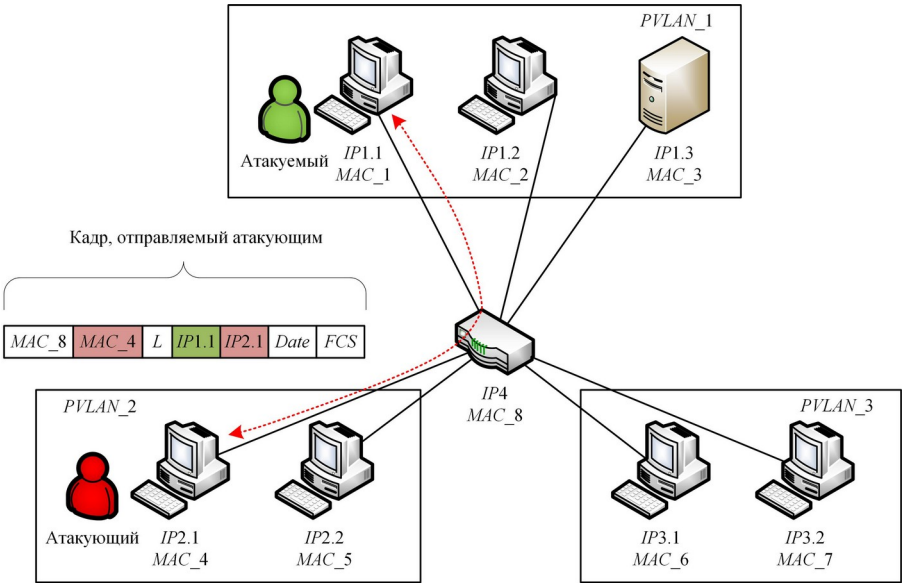

Рисунок 3 - Схема реализации атаки на *PVLAN*
DOI: https://doi.org/10.60797/itech.2025.5.2.3

Протокол *STP* (*Spanning Tree Protocol* – протокол остовного дерева) предназначен для предотвращения зацикливания пакетов в сети при наличии дублирующих маршрутов.

Атака на *STP* реализуется злоумышленником путем подмены подключаемого им устройства как коммутатора и отправления в сторону атакуемого коммутатора *BPDU*-пакета (*Bridge Protocol Data Unit* – блок данных протокола мостового перенаправления), в котором заменен *MAC*-адрес корневого коммутатора. Корневым коммутатором выбирается коммутатор с наименьшим значением идентификатора – *MAC*-адресом. Для того чтобы не быть обнаруженным, злоумышленнику необходимо обеспечить доставку трафика к месту назначения.

*MAC-Spoofing*заключается в подделывании злоумышленником *MAC*-адресов с целью перенаправления трафика и реализации атаки типа «человек посередине». Результатом успешной атаки являются измененные таблицы коммутации коммутаторов сети и перенаправление всех пакетов атакующему. В результате такого воздействия злоумышленник может перехватить трафик между двумя или несколькими устройствами сети. Чтобы оставаться незамеченным, злоумышленнику необходимо произвести подмену нескольких устройств сети (например, сервера для клиента и клиента для сервера, обеспечивая при этом доставку пакетов в оба направления). При использовании злоумышленником двух атакующих устройств они должны быть подключены к разным коммутаторам. При этом атакующее устройство 1 подменяет клиента для сервера, а атакующее устройство 2 – сервер для клиента (см. рис. 4).

После этого атакующие устройства, обмениваясь пакетами между собой, устанавливают соединение между клиентом и сервером, а злоумышленник с помощью сниффера наблюдает за клиент-серверным обменом [8].

Рисунок 4 - Схема атаки *MAC-Spoofing* с двумя атакующими устройствами
DOI: https://doi.org/10.60797/itech.2025.5.2.4

ARP-Spoofing – атака, используемая для прослушивания сети, построенной на основе маршрутизаторов. В ходе реализации данной атаки злоумышленник выдает себя за легального пользователя сети посредством подмены *MAC*-адресов в *ARP*-таблицах сетевых узлов. Для этого злоумышленник отправляет поддельный *ARP*-ответ с информацией о том, что его *MAC*-адрес соответствует *IP*-адресу маршрутизатора. Атакуемый компьютер получает поддельный *ARP*-пакет и обновляет информацию в своей *ARP*-таблице. В результате чего трафик перенаправляется не на маршрутизатор, а на компьютер злоумышленника. Для обеспечения прослушивания трафика в обе стороны, злоумышленнику необходимо аналогичным образом изменить *ARP*-таблицу маршрутизатора (см. рис. 5) [9, С. 48-53].

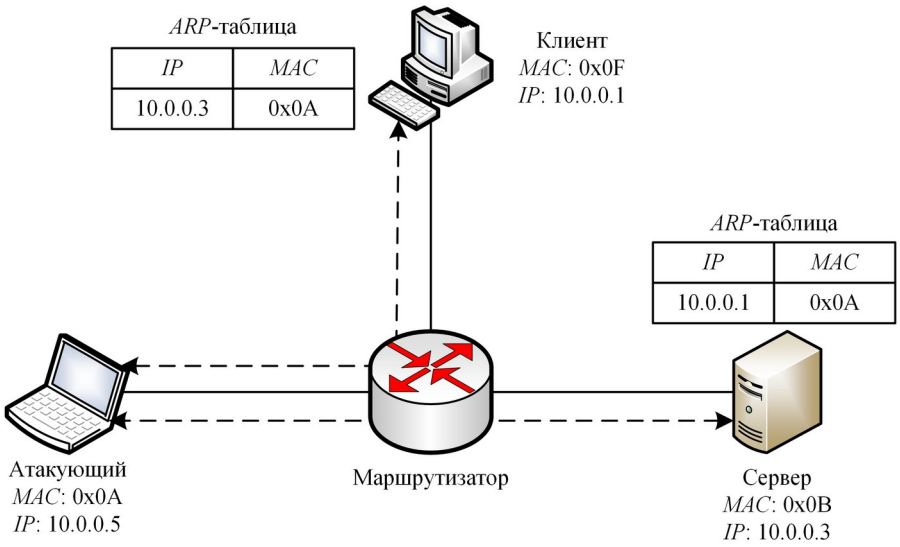

Рисунок 5 - Схема реализации атаки *ARP-Spoofing*
DOI: https://doi.org/10.60797/itech.2025.5.2.5

Атака на *DHCP*-сервер заключается в формировании и отправке на него огромного количества *DHCP*-запросов с разными *MAC*-адресами. Протокол *DHCP* предназначен для назначения *IP*-адреса клиенту. Сервер выделяет *IP*-адреса из пула, рано или поздно они могут закончиться и сервер не сможет обслуживать новых клиентов. Атака на *DHCP* является *DoS*-атакой, так как нарушается работоспособность сети. После того как атакующий вывел из строя легальный *DHCP*-сервер, он может развернуть свой и выдавать настройки пользователям сети, изменяя их для реализации более сложных атак [10, С. 19].

Заключение

Существенным недостатком описанных выше атак является необходимость непосредственного доступа к оборудованию или линии связи, которые, как правило, расположены внутри контролируемой зоны. Данные атаки с большей степенью вероятности могут быть реализованы внутренним нарушителем. В связи с этим существует

необходимость обеспечения защиты данных на нижних уровнях модели *TCP/IP*. Таким образом является актуальной разработка методов криптографической защиты информации, передаваемой на уровне сетевого доступа модели *TCP/IP*.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы / References

1. Иванов Ю.Б. Модель угроз и нарушителя безопасности информации для протоколов уровня сетевого доступа модели TCP/IP / Ю.Б. Иванов, И.А. Чубуткин // Актуальные вопросы науки 2024: сборник статей III международной научно-практической конференции. — Пенза: Наука и Просвещение, 2024. — С. 48–51.

2. Рекомендация по стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения. — Введ. 2006-06-01. — Москва: Стандартинформ, 2006. — 20 с.

3. Иванов Ю.Б. Оппортунистическое шифрование данных на уровне сетевого доступа модели TCP/IP / Ю.Б. Иванов, И.А. Чубуткин // Актуальные научные исследования: сборник статей XIII Международной научно-практической конференции. — Пенза: Наука и Просвещение, 2023. — С. 57–61.

4. Жуков А.Н. Хакерство. Физические атаки с использованием хакерских устройств / А.Н. Жуков — Санкт-Петербург: БХВ-Петербург, 2023. — 304 с.

5. Бирюков А.А. Информационная безопасность: защита и нападение / А.А. Бирюков — Москва: ДМК Пресс, 2023. — 440 с.

6. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание / В.Г. Олифер, Н.А. Олифер — Санкт-Петербург: Питер, 2022. — 1008 с.

7. Разруливаем DTP. Как взломать протокол DTP и совершить побег в другую сеть VLAN // Хакер. — 2022. — 274. — С. 39–40.

8. Сафиуллина Л.Х. Компьютерные сети. Лабораторные работы / Л.Х. Сафиуллина // MOODLE - Виртуальная среда обучения КНИТУ (КХТИ). — 2023 — URL: https://moodle.kstu.ru/mod/page/view.php?id=190638 (дата обращения: 05.09.2024)

9. Грэм Дэниел Г. Этичный хаккинг. Практическое руководство по взлому / Г. Грэм Дэниел — Санкт-Петербург: Питер, 2022. — 384 с.

10. Михайлов А. Атаки на DHCP. Разбираем техники DHCP Starvation и DHCP Spoofing и защиту от них / А. Михайлов // Хакер. — 2022. — 284. — С. 34–35.

Список литературы на английском языке / References in English

1. Ivanov Ju.B. Model' ugroz i narushitelja bezopasnosti informatsii dlja protokolov urovnja setevogo dostupa modeli TCP/IP [Threat and Information Security Intruder Model for TCP/IP Model Network Access Layer Protocols] / Ju.B. Ivanov, I.A. Chubutkin // Topical issues of science 2024: collection of articles of the III International Scientific and Practical Conference. — Penza: Nauka i Prosveschenie, 2024. — P. 48–51. [in Russian]

2. Rekomendatsija po standartizatsii R 50.1.056-2005. Tehnicheskaja zaschita informatsii. Osnovnye terminy i opredelenija. [Recommendation on standardization R 50.1.056-2005. Technical information protection. Terms and definitions] — Introduced 2006-06-01. — Moskva: Standartinform, 2006. — 20 p. [in Russian]

3. Ivanov Ju.B.. Opportunisticheskoe shifrovanie dannyh na urovne setevogo dostupa modeli TCP/IP [Opportunistic data encryption at the TCP/IP network access layer] / Ju.B. Ivanov, I.A. Chubutkin // Current scientific research: collection of articles of the XIII International Scientific and Practical Conference. — Penza: Nauka i Prosveschenie, 2023. — P. 57–61. [in Russian]

4. Zhukov A.N. Hakerstvo. Fizicheskie ataki s ispol'zovaniem hakerskih ustrojstv [Hacking. Physical attacks using hacker devices] / A.N. Zhukov — Saint-Petersburg: BHV-Peterburg, 2023. — 304 p. [in Russian]

5. Birjukov A.A. Informatsionnaja bezopasnost': zaschita i napadenie [Information security: Protection and attack] / A.A. Birjukov — Moskva: DMK Press, 2023. — 440 p. [in Russian]

6. Olifer V.G. Komp'juternye seti. Printsipy, tehnologii, protokoly: Jubilejnoe izdanie [Computer networks. Principles, technologies, protocols: Anniversary edition] / V.G. Olifer, N.A. Olifer — Sankt-Peterburg: Piter, 2022. — 1008 p. [in Russian]

7. Razrulivaem DTP. Kak vzlomat' protokol DTP i sovershit' pobeg v druguju set' VLAN [We are resolving the DTP. How to hack the DTP protocol and escape to another VLAN network] // Hacker. — 2022. — 274. — P. 39–40. [in Russian]

8. Safiullina L.H. Komp'juternye seti. Laboratornye raboty [Computer networks. Laboratory work] / L.H. Safiullina // MOODLE - A virtual learning environment for KNITU (KHTI). — 2023 — URL: https://moodle.kstu.ru/mod/page/view.php?id=190638 (accessed: 05.09.2024) [in Russian]

9. Grem Deniel G. Etichnyj hakking. Prakticheskoe rukovodstvo po vzlomu [Ethical hacking. A practical guide to hacking] / G. Grem Deniel — Sankt-Peterburg: Piter, 2022. — 384 p. [in Russian]

10. Mihajlov A. Ataki na DHCP. Razbiraem tehniki DHCP Starvation i DHCP Spoofing i zaschitu ot nih [Attacks on DHCP. We analyze the techniques of DHCP Starvation and DHCP Spoofing and protection against them] / A. Mihajlov // Hacker. — 2022. — 284. — P. 34–35. [in Russian]