ISSN 2225-9309 (Print)
2025. № 2 (33). С. 10–14

Молодежный
Вестник УГАТУ

http://journal.ugatu.su

УДК 004.056.5

doi 10.54708/22259309_2025_23310

Анализ сетевых атак типа MITM: рекомендации по защите сетевой инфраструктуры

М. А. Бакулин[1], А. Ю. Сенцова[2]

[1] bakulinmikhail@mail.ru, [2] sentsova.alina@yandex.ru

[1,2] ФГБОУ ВО «Уфимский университет науки и технологий» (УУНиТ)

Аннотация. Статья посвящена анализу сетевых атак типа MITM. Приводится актуальность как самих сетевых атак в целом, так и атак типа MITM. Дается определение понятию атаки типа MITM. Рассматриваются виды атак типа MITM, которые являются на сегодняшний день наиболее актуальными. Реализуется моделирование атаки DNS-спуфинг. Приводится техника реализации ARP-спуфинга, DHCP-starvation, атаки посредством Captive Portal и mitmproxy. Формируются рекомендации по защите от данного типа атак, которых необходимо придерживаться, относительно сетевой инфраструктуры предприятия.

Ключевые слова: информационная безопасность; сетевая инфраструктура; кибератака; защита информации; MITM; атака посредника; ARP-spoofing; DHCP-starvation; DNS-spoofing; Captive Portal; mitmproxy.

ВВЕДЕНИЕ

Сетевая инфраструктура сегодня является неотъемлемой частью любой организации независимо от ее масштабов. В то же время такая инфраструктура вызывает большой интерес со стороны злоумышленников, что делает ее главной целью таргетированных атак. Число таких атак увеличилось на 18 п. п. относительно показателей предыдущего года [1]. Также текущий квартал показал, что количество инцидентов возросло на 7 %, сравнительно с предыдущим кварталом [2]. Данная статистика подтверждает тот факт, что число сетевых атак неуклонно растет. Все это говорит о том, что необходимо обеспечивать должный уровень защищенности сетевой инфраструктуры каждой организации. В число наиболее популярных сетевых атак относят атаки типа MITM, которые еще также называют атакой посредника. Среди наиболее популярных видов атак данного типа можно выделить следующие: ARP-спуфинг; DNS-спуфинг; DOS и подмена DHCP-сервера; атака посредством Captive Portal; атака посредством mitmproxy.

Атаки типа MITM – это такой тип сетевой атаки, когда злоумышленнику за счет выполнения определенных действий удается логически встать между двумя узлами. В результате чего он сможет прослушивать и модифицировать трафик, который проходит через него. Для реализации данных атак злоумышленнику необходимо иметь подключение к целевой сети.

DNS-спуфинг. Реализуется посредством использования протокола DNS. Данный протокол находится на прикладном уровне. Выделен порт 53 [3]. В качестве протокола транспортного уровня используется UDP. Назначений у протокола несколько, но основным является определение по доменному имени IP-адреса. Протокол DNS работает по архитектуре клиент – сервер в режиме запрос – ответ.

Атака DSN-спуфинг является следующим этапом после того, как злоумышленнику удалось встать посередине путем ARP-спуфинга или путем DOS и подмены DHCP-сервера. В результате выполнения данной атаки злоумышленник сможет перенаправлять обращения жертвы. Например, жертва обращается к веб-странице, где будет скачивать какой-либо файл. При запросе веб-страницы сначала будет осуществляться DNS-запрос. Делается он с целью того, чтобы преобразовать доменное имя, по которому обращается пользователь, в IP-адрес. Проходящие через злоумышленника DNS-пакеты помещаются в очередь, где над ними производятся определенные действия. Суть действий заключается в том, чтобы подменить IP-адрес в DNS-ответе, а также изменить еще несколько полей. В результате чего жертва будет перенаправлена на веб-страницу злоумышленника. В свою очередь злоумышленник может сделать фишинговый сайт, то есть копию оригинального сайта, где файлы для скачивания будут заменены на вредоносные файлы. Или же злоумышленник может сделать копию запрашиваемой страницы авторизации и получать конфиденциальные данные для входа. Вариантов может быть достаточно много. Конечный вариант реализации зависит от целей злоумышленника и исходных данных, которыми он обладает. Обычно сначала злоумышленник прослушивает проходящие через него DNS-запросы, чтобы сформировать список ресурсов, к которым наиболее часто происходит запрос. После этого у злоумышленника будут доменные имена таких страниц, и в зависимости от доменного имени жертва будет перенаправляться на тот или иной ресурс, то есть на соответствующую копию.

Для моделирования данной атаки рассматривается ситуация, когда злоумышленник обращается к веб-странице университета, а перенаправляется на веб-сервер, который развернут на рабочей станции (PC) злоумышленника. Схема моделирования данной атаки представлена на рис. 1.

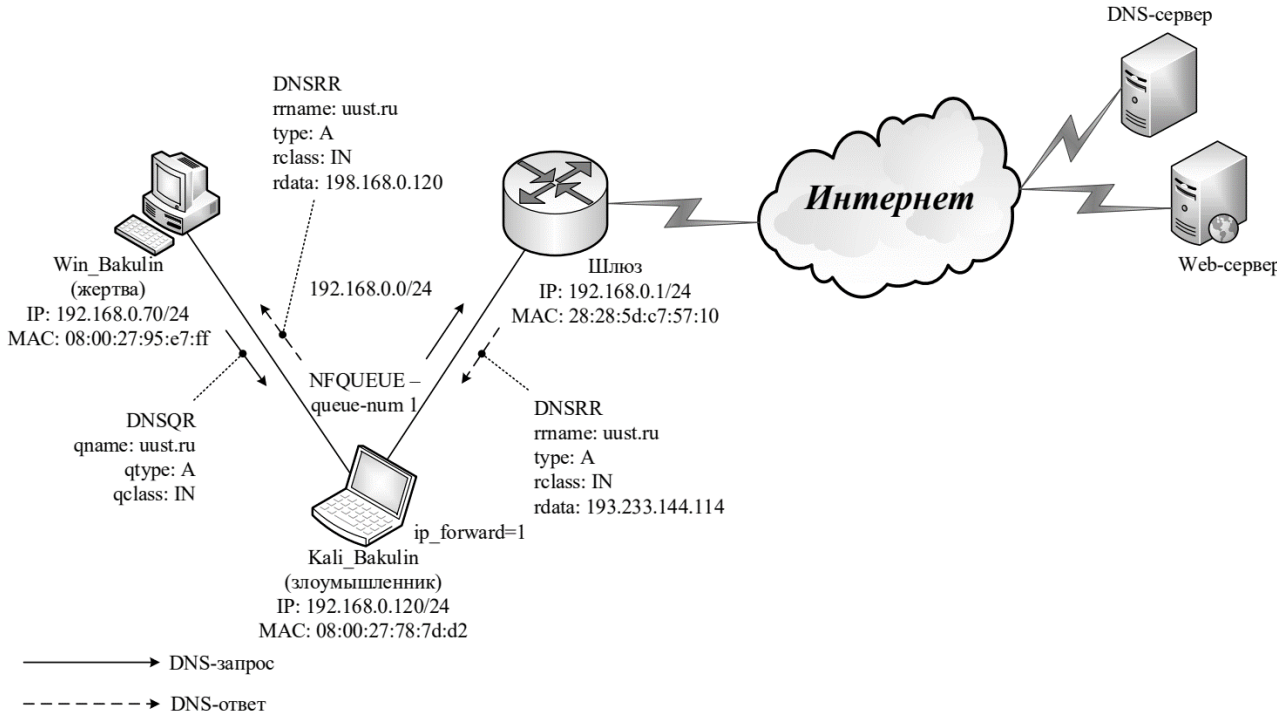

Рис. 1. Схема моделирования атаки – DNS-спуфинг

На рис. 2 представлен процесс моделирования данной атаки.

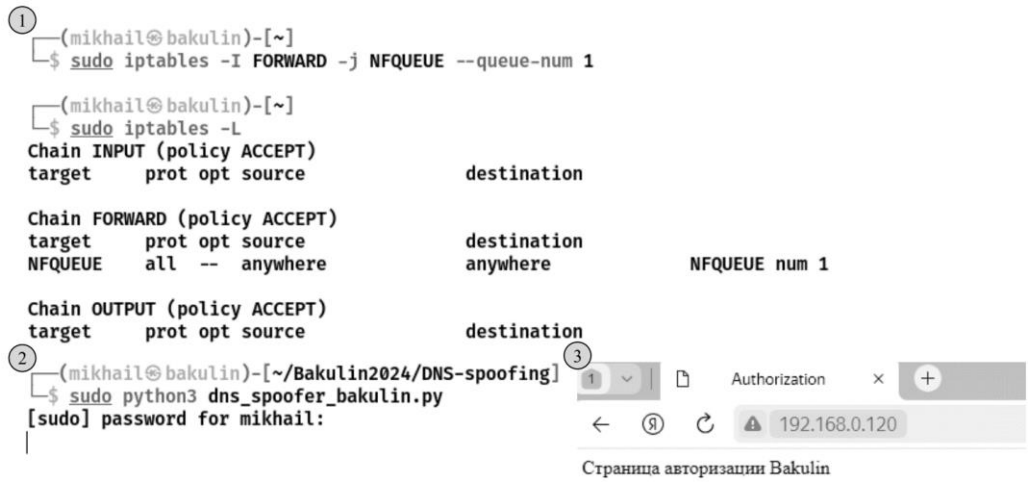

Рис. 2. Создание очереди и результат DNS-спуфинга

На изображении 1 создается очередь под первым номером. На изображении 2 осуществляется запуск DNS-спуфера, а на последнем изображении представлен результат реализации данной атаки, а именно то, что жертва при обращении к веб-странице *uust.ru* была перенаправлена на web-сервер злоумышленника, который развернут посредством Apache.

На рис. 3 представлен процесс подмены соответствующих полей. На изображении 1 показан изначальный запрос и ответ, а на изображении 2 представлен запрос и ответ после внесения соответствующих изменений, которые произошли благодаря DNS-спуферу.

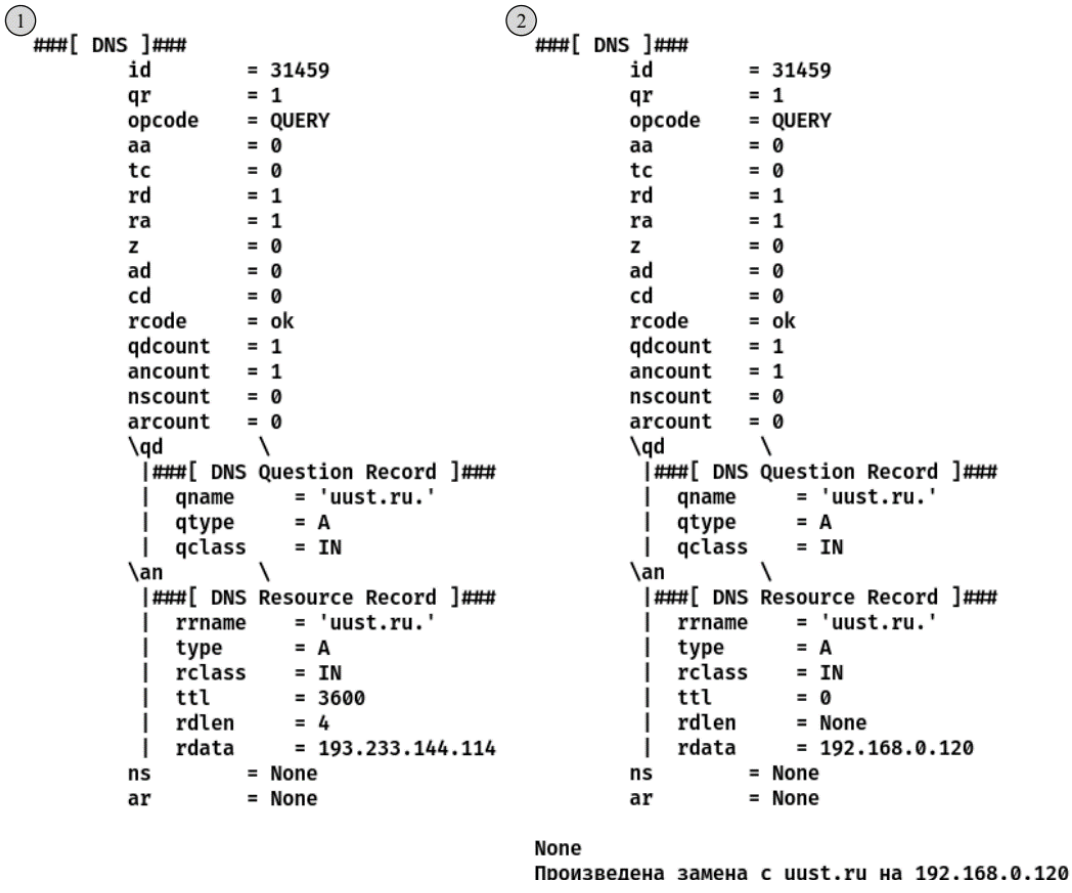

Рис. 3. Результат подмены полей заголовков

ARP-спуфинг. Данная атака реализуется за счет уязвимостей протокола ARP, а именно – за счет следующих аспектов: возможен самопроизвольный ARP; нет механизма проверки подлинности ARP-ответа. Суть атаки заключается в том, чтобы подменить MAC-адрес в ARP-кэше двух узлов. Например, в качестве узлов рассматриваются PC и шлюз. Злоумышленник на PC жертвы подменяет MAC-адрес, который соответствует IP-адресу шлюза на свой, а на шлюзе в записи, которая соответствует IP-адресу жертвы, также подменяет на свой. В результате выполнения данных действий злоумышленнику удастся встать посередине.

DOS и подмена DHCP-сервера. Данную атаку также называют DHCP-starvation. Суть атаки заключается в том, чтобы вызвать отказ в обслуживании исходного DHCP-сервера и развернуть свой, чтобы жертва подключилась к нему. При подключении к серверу злоумышленника PC жертвы будут выданы сетевые параметры, которые сконфигурирует злоумышленник, например, в качестве IP-адреса шлюза будет выдан IP-адрес злоумышленника, в результате чего он встанет посередине.

Атака посредством Captive Portal. Данную атаку злоумышленник обычно использует тогда, когда ему не удалось реализовать ни ARP-спуфинг, ни DHCP-starvation. Злоумышленник развертывает свою точку доступа (ТД), которая является копией исходной ТД. После чего деаутентифицирует жертву от исходной ТД. Жертве ничего не остается как подключиться к копии исходной ТД, где настроена авторизация посредством Captive Portal, за счет которой злоумышленник может получать различную информацию конфиденциального характера, например, логин и пароль исходной ТД.

Атака посредством mitmproxy. Реализовав данную атаку, злоумышленник сможет обойти механизм HSTS [4]. Суть заключается в том, что злоумышленнику нужно добиться выполнения трех аспектов:

– скачать или передать сертификат mitmproxy на PC жертвы;

– импортировать данный сертификат в доверенные корневые центры сертификации;

– сконфигурировать прокси на PC жертвы.

Сделать это он может различными способами, например, добиться того, чтобы жертва скачала исполняемый файл, который реализует выполнение данных аспектов.

ЗАКЛЮЧЕНИЕ

Таким образом, на основе моделирования данных атак были сформированы следующие рекомендации, которых стоит придерживаться:

1) выстраивание надежной защиты периметра Сети;

2) использование статических ARP-записей;

3) использование VPN;

4) использование VLAN;

5) использование коммуникационного оборудования с модулями защиты от ARP-спуфинга;

6) использование Security Endpoint Protection на антивирусных средствах защиты;

7) использование Dynamic ARP Inspection (DAI);

8) использование многофакторной аутентификации;

9) использование arpwatch;

10) использование DHCP Snooping;

11) настройка Port Security;

12) использование DHCP Rate Limiting;

13) использование DNSSEC;

14) мониторинг трафика.

Если придерживаться данных рекомендаций, то можно значительно снизить вероятность реализации атаки типа MITM относительно сетевой инфраструктуры предприятия.

СПИСОК ЛИТЕРАТУРЫ

1. Positive Technologies. Актуальные киберугрозы для организаций: итоги 2023 года. [Электронный ресурс]. URL: https://clck.ru/3AcYGu (дата обращения 12.04.2024).

2. Positive Technologies. Актуальные киберугрозы: I квартал 2024 года. [Электронный ресурс]. URL: https://clck.ru/3AdYNi (дата обращения 15.05.2024).

3. Олифер В. Г., Олифер Н. В. Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание. СПб.: Питер, 2020. 1008 с.: ил. (Серия «Учебник для вузов»).

4. Mitmproxy docs. Introduction mitmproxy. [Электронный ресурс]. URL: https://docs.mitmproxy.org/stable/ (дата обращения 18.05.2024).

ОБ АВТОРАХ

БАКУЛИН Михаил Алексеевич, маг. каф. ВТиЗИ. Готовит маг. дис. о методике определения степени уязвимости сетевой инфраструктуры предприятия перед атаками типа MITM.

СЕНЦОВА Алина Юрьевна, доц. каф. ВТиЗИ. Дипл. специалист по информационной безопасности. Канд. техн. наук. Иссл. в обл. экспертного аудита информационной безопасности в системе облачных вычислений.

METADATA

Title: Analysis of network attacks of the MITM type. Recommendations for protecting the network infrastructure.

Authors: M. A. Bakulin[1], A. Y. Sentsova[2]

Affiliation:

[1, 2] Ufa University of Science and Technology (UUST), Russia.

Email: [1] bakulinmikhail@mail.ru, [2] sentsova.alina@yandex.ru.

Language: Russian.

Source: Molodezhnyj Vestnik UGATU (scientific journal of Ufa University of Science and Technology), no. 2 (33), pp. 10-14, 2025. ISSN 2225-9309 (Print).

Abstract: The article is devoted to the analysis of network attacks of the MITM type. The relevance of both network attacks in general and MITM-type attacks is given. The definition of a MITM-type attack is given. The types of MITM-type attacks that are currently the most relevant are considered. DNS spoofing attack simulation is implemented. The technique of implementing ARP spoofing, DHCP-starvation, attacks via Captive Portal and mitmproxy is given. Recommendations for protection against this type of attacks are being formed, which must be followed regarding the enterprise's network infrastructure.

Key words: information security; network infrastructure; cyberattack; information protection; attacks; intermediary attack; ARP spoofing; DHCP server-hunger; DNS spoofing; portal; mitmproxy.

About authors:

BAKULIN, Mikhail Alexeyevich, Graduate student of the Department of Computer Engineering and Information Security. He is preparing a master's thesis on the methodology for determining the degree of vulnerability of an enterprise's network infrastructure to MITM-type attacks.

SENTSOVA, Alina Yurievna, Associate Professor of the Department of Computer Engineering and Information Security. He is a certified information security specialist. Candidate of Technical Sciences. Research in the field of expert audit of information security in the cloud computing system.