УДК 004.056.5

Косинов Артем Александрович, студент кафедры математических методов обеспечения безопасности систем, РГУ нефти и газа (НИУ) имени И.М. Губкина, Россия, г. Москва

Суховеев Денис Владимирович, студент кафедры математических методов обеспечения безопасности систем, РГУ нефти и газа (НИУ) имени И.М. Губкина, Россия, г. Москва

РЕАЛИЗАЦИЯ И АНАЛИЗ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ОТ NETWORK SNIFFING (MITRE ATT&CK T1040) НА БАЗЕ МЕЖСЕТЕВОГО ЭКРАНА

Аннотация

В статье представлены результаты практической реализации атаки Network Sniffing (техника MITRE ATT&CK T1040) в контролируемой лабораторной среде и проверки эффективности защитных мер на базе межсетевого экрана Cisco ASA 5506-X. Эксперимент выполнен на стенде из трех виртуальных машин под управлением ОС «Альт» и аппаратного межсетевого экрана, настроенного в режиме маршрутизации с сегментацией сети на зоны inside и dmz. Атака реализована методом ARP-спуфинга с использованием библиотеки scapy; перехват трафика выполнялся утилитой tcpdump. Проведены два замера: передача учетных данных без шифрования (HTTP) и с шифрованием TLS (HTTPS). В первом случае учетные данные извлечены из дампа в открытом виде (доля читаемых данных – 100 %), во втором – трафик перехвачен, но данные нечитаемы (0 %). Каждый тест воспроизведен в пяти повторениях с идентичным результатом. Дополнительно рассмотрены меры защиты на уровне коммутаторов (DAI, port security), системы IDS/IPS, а также архитектуры VPN и Zero Trust как элементы эшелонированной защиты.

Annotation

The article presents the results of a practical implementation of a Network Sniffing attack (MITRE ATT&CK T1040) in a controlled laboratory environment and verification of protection measures based on a Cisco ASA 5506-X firewall. The experiment was conducted on a testbed of three virtual machines running OS Alt and a hardware firewall configured in routed mode with network segmentation into inside and dmz zones. The attack was implemented using ARP spoofing via the scapy library; traffic capture was performed with tcpdump. Two measurements were taken: credential transmission without encryption (HTTP) and with TLS encryption (HTTPS). In the first case, credentials were extracted from the dump in plaintext (100 % readable); in the second, traffic was captured but data was unreadable (0 %). Each test was reproduced in five repetitions with identical results. Additional protection measures at the switch level (DAI, port security), IDS/IPS systems, as well as VPN and Zero Trust architectures are discussed as elements of defence-in-depth.

Ключевые слова: Network Sniffing, MITRE ATT&CK T1040, ARP-спуфинг, межсетевой экран, Cisco ASA, HTTPS, TLS, сегментация сети, DAI, Zero Trust.

Keywords: Network Sniffing, MITRE ATT&CK T1040, ARP-спуфинг, межсетевой экран, Cisco ASA, HTTPS, TLS, сегментация сети, DAI, Zero Trust.

Введение

Перехват сетевого трафика (Network Sniffing) относится к числу базовых техник разведки и получения учетных данных в современных атаках на корпоративные сети. Согласно матрице MITRE ATT&CK, техника T1040 охватывает тактики Discovery и Credential Access и описывает перехват трафика с целью извлечения конфиденциальной информации, прежде всего паролей, передаваемых в открытом виде. В коммутируемых сетях пассивный перехват невозможен без вмешательства в канальный уровень – наиболее распространенным вектором является ARP-спуфинг, позволяющий атакующему реализовать атаку «человек посередине». По данным Verizon Data Breach Investigations Report 2024, кража учетных данных является

вектором атаки №1: использование похищенных credentials признано наиболее распространенным начальным действием при взломах, а в категории атак на веб-приложения на их долю приходится 77 % инцидентов [11]. Техника T1040 непосредственно направлена на перехват таких данных в сетевом трафике, что подчеркивает практическую значимость исследования эффективных мер противодействия.

Основной мерой противодействия T1040 по классификации MITRE является M1041 «Encrypt Sensitive Information» – шифрование передаваемых данных, делающее перехваченный трафик нечитаемым. Дополнительными мерами выступают сегментация сети и мониторинг трафика, реализуемые средствами межсетевого экрана.

Объектом исследования является сетевая инфраструктура на базе межсетевого экрана Cisco ASA 5506-X, развернутая в контролируемой лабораторной среде. Предметом исследования выступает эффективность защитных мер – шифрования TLS и сегментации сети – против атаки Network Sniffing (T1040). Целью настоящей работы является практическая реализация атаки T1040 и экспериментальная оценка эффективности указанных мер защиты с количественным измерением доли читаемых данных в перехваченном трафике.

Для достижения цели поставлены следующие задачи:

1. Провести анализ техники T1040 и соответствующих мер противодействия по матрице MITRE ATT&CK.

2. Спроектировать и развернуть лабораторный стенд с межсетевым экраном Cisco ASA 5506-X, воспроизводящий реальный сценарий атаки.

3. Реализовать атаку Network Sniffing методом ARP-спуфинга в контролируемой среде.

4. Провести контрольные замеры эффективности перехвата трафика без шифрования (HTTP) и с шифрованием TLS (HTTPS).

5. Проанализировать результаты и сформулировать рекомендации по эшелонированной защите от T1040.

Научная новизна работы состоит в экспериментальной верификации гипотезы о полной нейтрализации практического результата атаки Network Sniffing (T1040) посредством шифрования TLS при сохранении успешности атаки на канальном уровне: впервые получены количественные показатели эффективности защиты в среде на базе отечественной ОС «Альт» с аппаратным межсетевым экраном Cisco ASA 5506-X (доля читаемых данных: 100 % без шифрования против 0 % при применении TLS).

Практическая значимость работы заключается в том, что полученные результаты и сформулированные рекомендации по эшелонированной защите могут быть применены администраторами корпоративных и ведомственных сетей при проектировании защиты от техники T1040, в частности при выборе средств сегментации, настройке политик шифрования трафика, а также при оценке достаточности межсетевого экрана как единственного средства защиты от перехвата данных.

Анализ источников

Нормативную основу работы составляют документы MITRE ATT&CK: карточка техники T1040 «Network Sniffing» [1] и описание меры противодействия M1041 «Encrypt Sensitive Information» [2], определяющие терминологию, тактический контекст атаки и перечень рекомендуемых защитных механизмов. Протокол ARP рассмотрен в соответствии с оригинальной спецификацией RFC 826 [4], а механизм его уязвимости перед спуфингом – на основе классической работы Беллоуина по проблемам безопасности стека TCP/IP [7], сохраняющей актуальность для понимания атак канального уровня.

Криптографическая составляющая эксперимента опирается на спецификацию протокола TLS 1.3 (RFC 8446) [5] и протокола HTTP/1.1 (RFC 7230) [6], задающих условия передачи данных в тестах А и Б соответственно. Конфигурация и поведение межсетевого экрана изучались по официальной документации Cisco ASA [3], в том числе в части интерпретации журнальных событий, включая %ASA-4-405001. Меры защиты на уровне коммутаторов –

Dynamic ARP Inspection и port security – рассмотрены с опорой на руководство по настройке Cisco [8]. Концепция Zero Trust как перспективная архитектурная мера противодействия исследована по публикации NIST SP 800-207 [9].

Большинство доступных практических работ по теме T1040 ограничиваются либо демонстрацией самой атаки без количественной оценки защитных мер, либо рассматривают шифрование и сегментацию раздельно. Отличие настоящей работы состоит в совместном исследовании обеих мер в единой инфраструктуре на базе аппаратного межсетевого экрана и отечественной ОС «Альт», с количественным измерением результата и многократным воспроизведением эксперимента.

Методы исследования

На первом этапе применялся теоретико-аналитический метод: изучены механизм атаки T1040, принципы работы ARP-спуфинга, архитектура межсетевого экрана Cisco ASA и криптографические свойства протоколов TLS и HTTP. Анализ позволил сформулировать проверяемую гипотезу: шифрование на прикладном уровне полностью нейтрализует практическую ценность перехваченного трафика вне зависимости от успешности атаки на канальном уровне.

На втором этапе использовался моделирующий метод: спроектирован лабораторный стенд из трех виртуальных машин и аппаратного межсетевого экрана Cisco ASA 5506-X, воспроизводящий реальный сценарий T1040 – атакующий и жертва находятся в одном широковещательном домене, сервер-получатель изолирован в демилитаризованной зоне. Использование среды Oracle VirtualBox с подключением в режиме сетевого моста обеспечивает воспроизводимость топологии.

Основу эксперимента составил экспериментальный метод с применением контрольных замеров. Каждый тест (HTTP и HTTPS) воспроизводился в пяти независимых повторениях при неизменных условиях стенда. Для реализации ARP-спуфинга применялась библиотека scapy языка Python, для перехвата трафика – утилита tcpdump. Анализ дампов позволил

получить измеримый показатель эффективности защиты – долю читаемых учетных данных в перехваченном трафике. Под читаемыми данными понимается наличие в дампе строки вида user=...&pass=... в открытом тексте, обнаруживаемой командой tcpdump -r capX.pcap -A | grep -i pass: результат «найдено» соответствует 100 %, результат «не найдено» – 0 %. Весь остальной HTTP-трафик в метрику не включался; оценивалась исключительно возможность извлечения учетных данных как целевого объекта атаки T1040.

Блок-схема методологии эксперимента представлена на рисунке 1.

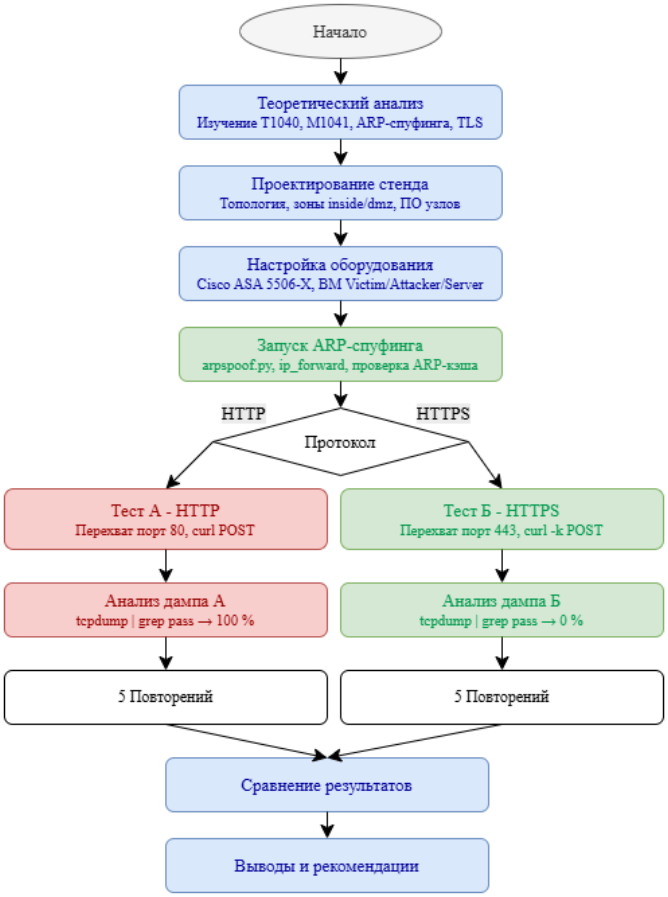

Рисунок 1 – Блок-схема методологии эксперимента

Лабораторный стенд

Стенд включает три виртуальные машины, развернутые в среде Oracle VirtualBox на одном физическом ноутбуке, и аппаратный межсетевой экран Cisco ASA 5506-X. Подключение виртуальных машин к сегментам межсетевого экрана выполнено через два физических Ethernet-адаптера в режиме сетевого моста. Состав стенда приведен в таблице 1.

Таблица 1 – Состав лабораторного стенда

Компонент	Характеристики	Роль
Cisco ASA 5506-X	ASA OS 9.16(3)19, 4096 МБ ОЗУ, 4 ядра	Межсетевой экран, маршрутизация, сегментация
ВМ «Victim»	ОС «Альт» 10.4 (GUI)	Отправитель учетных данных
ВМ «Attacker»	ОС «Альт» 11 (GUI), Python 3, scapy, tcpdump	ARP-спуфинг и перехват трафика
ВМ «Server»	ОС «Альт Сервер» 10.4 (без GUI), Python 3	Веб-ресурс, принимающий учетные данные

Межсетевой экран настроен в режиме маршрутизации. Зона inside (192.168.1.0/24, security-level 100) объединяет узлы Victim (192.168.1.10) и Attacker (192.168.1.6); зона dmz (192.168.2.0/24, security-level 50) содержит узел Server (192.168.2.20). Атакующий размещен в одном широковещательном домене с жертвой, что соответствует реальному сценарию T1040. Топология стенда представлена на рисунке 2.

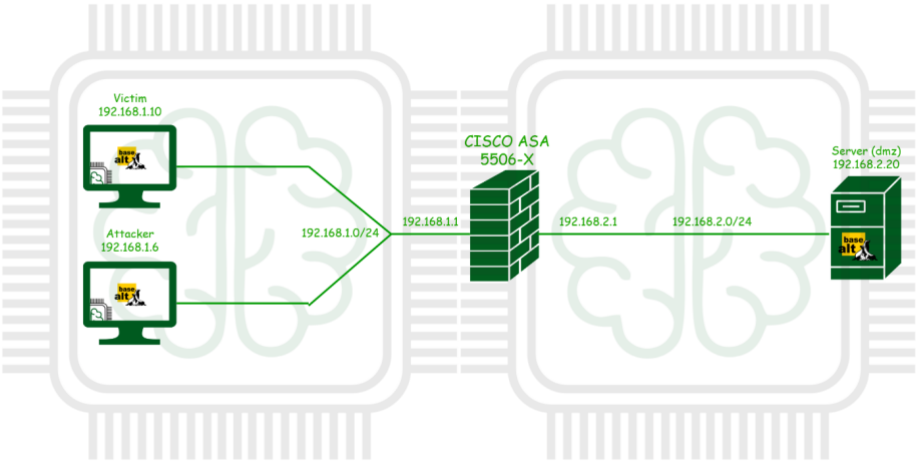

Рисунок 2 – Топология лабораторного стенда

На узле Server развернуты два веб-сервера на Python: HTTP-сервер (порт 80) и HTTPS-сервер (порт 443) с самоподписанным RSA-2048 сертификатом. На узле Attacker для ARP-спуфинга применена библиотека scapy; перехват трафика выполнялся утилитой tcpdump.

Ключевые команды конфигурации межсетевого экрана приведены ниже:

```
interface GigabitEthernet1/2
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 no shutdown

interface GigabitEthernet1/3
 nameif dmz
 security-level 50
 ip address 192.168.2.1 255.255.255.0
 no shutdown

access-list ALLOW extended permit ip any any
access-group ALLOW in interface inside
access-group ALLOW in interface dmz
logging enable
logging buffered informational
```

Формальная модель угроз для рассматриваемого сценария приведена в таблице 2.

Таблица 2 – Модель угроз

Актив	**Угроза**	**Уязвимость**	**Контрмера**
Учетные данные пользователя	Перехват и извлечение из трафика (T1040)	Передача данных в открытом виде по незащищенному каналу	Шифрование TLS (M1041)
Сетевой трафик между зонами	Несанкционированный доступ к межзональному обмену	Отсутствие сегментации сети	Разделение на зоны inside и dmz средствами Cisco ASA
Сетевая инфраструктура	Подмена ARP-записей (спуфинг)	Отсутствие проверки подлинности ARP-ответов на канальном уровне	DAI, port security на коммутаторах

Остаточные риски по каждому из рассмотренных активов распределяются следующим образом. Для учетных данных пользователя: применение TLS нейтрализует практический результат перехвата, однако сам факт ARP-спуфинга на канальном уровне остается технически возможным. Для сетевого трафика между зонами: сегментация на зоны inside и dmz ограничивает область потенциального перехвата, при этом атакующий внутри зоны inside сохраняет доступ к трафику в пределах своего сегмента. Для

сетевой инфраструктуры: в отсутствие DAI подмена ARP-записей остается возможной – данный риск устраняется только при внедрении защиты на уровне коммутаторов.

Необходимо отметить ограничение теста Б: в эксперименте использовался самоподписанный сертификат, а отправка данных выполнялась утилитой curl с параметром -k, отключающим проверку цепочки доверия. В реальных условиях браузер выдает предупреждение о ненадежном сертификате, и пользователь может отказаться от соединения. Тем не менее данное ограничение не влияет на основной вывод работы: при любом валидном TLS-соединении перехваченный трафик остается нечитаемым вне зависимости от типа сертификата.

Практическая часть

Перед каждым тестом на узле Attacker активировался режим пересылки пакетов, после чего запускался скрипт arpspoof.py, рассылающий поддельные ARP-ответы. Скрипт циклически рассылает поддельные ARP-ответы с интервалом 2 секунды в обоих направлениях: жертве сообщается, что MAC-адрес шлюза принадлежит атакующему, и наоборот. В результате ARP-кэш узла Victim содержал MAC-адрес Attacker вместо MAC-адреса шлюза. Факт отравления кэша подтверждался командой ip neigh show (рисунок 3).

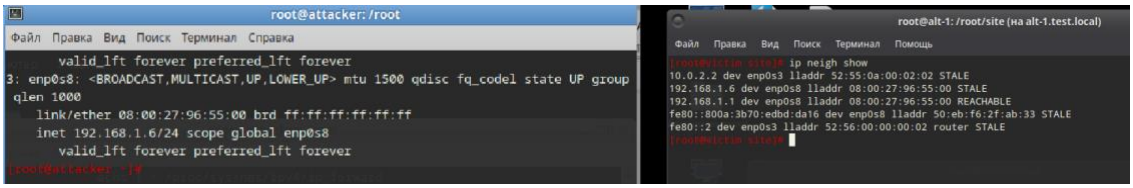

Рисунок 3 – Подтверждение отравления ARP-кэша узла Victim

Тест А (HTTP). На Attacker запускался перехват пакетов на порту 80; с узла Victim отправлялись учетные данные командой curl -d "user=admin&pass=SecretPass123" http://192.168.2.20/login. Данные передавались методом POST в формате application/x-www-form-urlencoded. После остановки перехвата анализ дампа выявил строку с учетными данными в открытом виде (рисунок 4). Доля читаемых данных – 100 %.

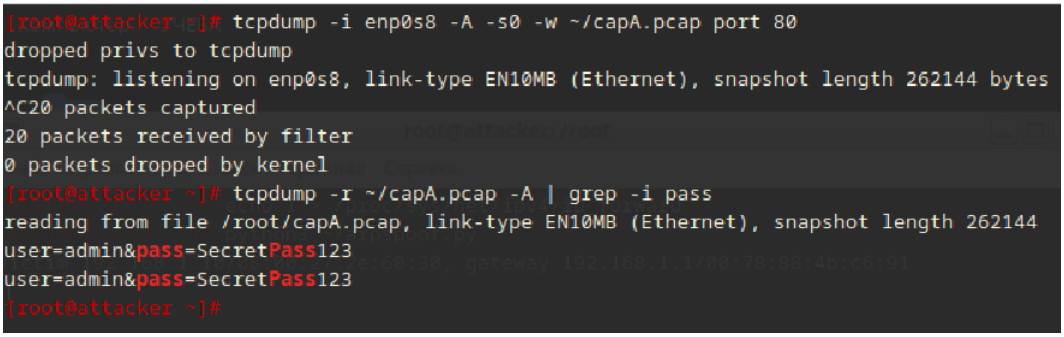

Рисунок 4 – Результат анализа дампа теста А: учетные данные в открытом виде

Тест Б (HTTPS). ARP-спуфинг не прерывался; изменялся только способ передачи данных. Учетные данные отправлялись командой: curl -k -d "user=admin&pass=SecretPass123" https://192.168.2.20/login. Параметр -k отключает проверку сертификата, что необходимо при использовании самоподписанного сертификата в лабораторных условиях. Перехват выполнялся на порту 443. Анализ дампа не вернул ни одной строки с учетными данными – в перехваченном файле присутствовали исключительно зашифрованные данные протокола TLS (рисунок 5). Доля читаемых данных – 0 %.

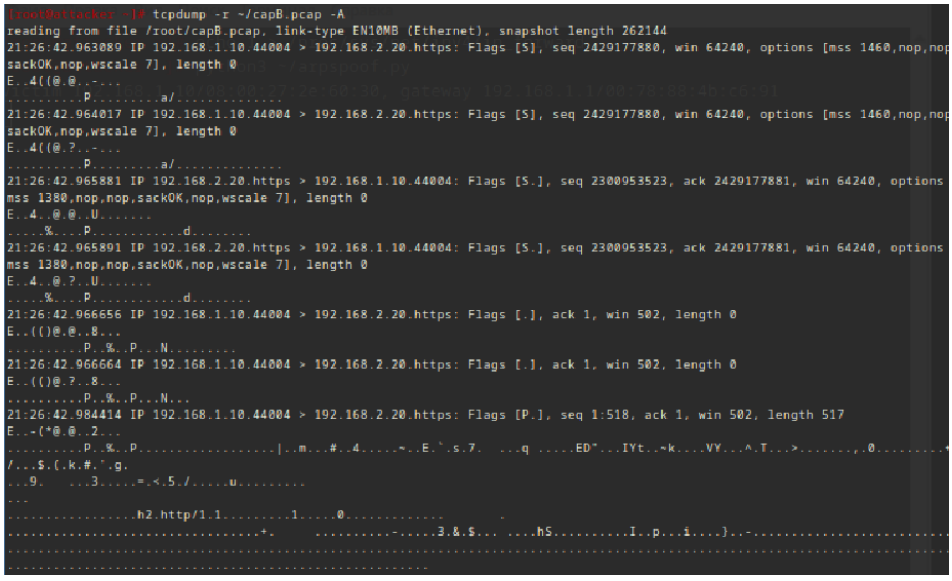

Рисунок 5 – Содержимое дампа теста Б: только зашифрованные данные TLS

Со стороны Cisco ASA журнал зафиксировал построение и завершение TCP-соединений между зонами, а также событие %ASA-4-405001 «Received

ARP response collision» – прямое свидетельство выполняемой атаки (рисунок 6).

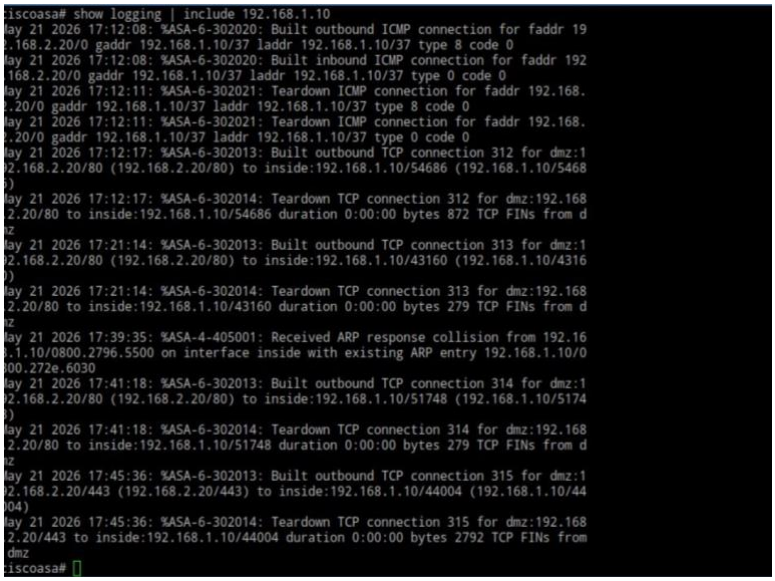

Рисунок 6 – Журнал Cisco ASA: TCP-соединения и событие коллизии ARP (%ASA-4-405001)

Результаты эксперимента

Сводные результаты двух тестов представлены в таблице 3. Воспроизводимость подтверждена пятью независимыми повторениями каждого теста. Выбор числа повторений обусловлен бинарным характером измеряемого показателя: при результате, принимающем только два значения (100 % или 0 %), пять последовательных идентичных исходов достаточны для вывода об отсутствии вариабельности и случайного влияния среды. Вариабельность результата отсутствует.

Таблица 3 – Сравнение результатов замеров

Параметр	**Замер А (HTTP, без защиты)**	**Замер Б (HTTPS, M1041)**
ARP-спуфинг	Выполнен успешно	Выполнен успешно
Трафик перехвачен	Да	Да
Учетные данные читаемы	Да (100 %)	Нет (0 %)
Содержимое перехвата	Открытый текст	Зашифрованные данные TLS
Логин и пароль в дампе	Присутствуют	Отсутствуют

Эксперимент показал, что межсетевой экран не предотвращает ARP-спуфинг: атака реализуется на канальном уровне и не затрагивает уровень маршрутизации, на котором работает Cisco ASA. Вместе с тем межсетевой экран обеспечил сегментацию сети, ограничив область возможного перехвата, и зафиксировал факт атаки в журнале. Применение TLS полностью нейтрализовало практический результат перехвата: атака технически состоялась, однако цели не достигла.

Дополнительные меры противодействия

Для комплексной защиты от T1040 помимо межсетевого экрана и шифрования следует рассматривать следующие механизмы.

Защита на уровне коммутаторов. Dynamic ARP Inspection (DAI) проверяет соответствие IP- и MAC-адресов в ARP-ответах по привязочной таблице DHCP Snooping и отбрасывает поддельные пакеты, блокируя ARP-спуфинг непосредственно на канальном уровне. Port security ограничивает число допустимых MAC-адресов на порту, затрудняя подключение несанкционированных узлов. Совместное применение DAI и port security устраняет вектор атаки, использованный в эксперименте.

Системы IDS/IPS. Сигнатуры, реагирующие на массовую рассылку ARP-ответов от одного источника, позволяют выявить атаку в реальном времени и автоматически заблокировать атакующий узел. Cisco ASA зафиксировал коллизию ARP в журнале, однако блокировка не выполнялась – интегрированная IPS-подсистема могла бы обеспечить такую реакцию автоматически.

VPN и Zero Trust. VPN обеспечивает шифрование трафика на сетевом уровне вне зависимости от прикладного протокола. Архитектура Zero Trust предполагает взаимную аутентификацию всех участников и непрерывную верификацию прав доступа, что лишает смысла перехват трафика внутри периметра: даже получив данные, атакующий не сможет ими воспользоваться без соответствующей аутентификации [9].

Заключение

В работе практически реализована атака Network Sniffing (MITRE ATT&CK T1040) методом ARP-спуфинга в среде с межсетевым экраном Cisco ASA 5506-X. По результатам двух серий экспериментов (по пять повторений каждая) сформулированы следующие выводы.

- В отсутствие шифрования атака T1040 приводит к полной компрометации передаваемых учетных данных: доля читаемых данных составила 100 % во всех повторениях.
- Применение TLS (HTTPS, мера MITRE M1041) не предотвращает перехват трафика, но полностью исключает возможность извлечения из него полезной информации: доля читаемых данных составила 0 %. Шифрование является решающей мерой противодействия T1040.
- Межсетевой экран не блокирует ARP-спуфинг на канальном уровне, однако обеспечивает сегментацию сети, межзональный контроль трафика и детектирование атаки посредством события %ASA-4-405001.
- Эффективная защита от T1040 достигается только сочетанием мер: сегментации и мониторинга на уровне МЭ, сквозного шифрования, защиты коммутаторов (DAI, port security) и применения IDS/IPS. Ни одна мера в отдельности не закрывает технику полностью, что подтверждает принцип эшелонированной защиты.

Литература

1. MITRE ATT&CK. T1040: Network Sniffing. [Электронный ресурс]. – URL: https://attack.mitre.org/techniques/T1040/ (дата обращения: 20.05.2026).
2. MITRE ATT&CK. M1041: Encrypt Sensitive Information. [Электронный ресурс]. – URL: https://attack.mitre.org/mitigations/M1041/ (дата обращения: 20.05.2026).
3. Cisco Systems. Cisco ASA Series General Operations CLI Configuration Guide, 9.16. – Cisco, 2022.
4. Plummer D. An Ethernet Address Resolution Protocol: RFC 826. – IETF, 1982. [Электронный ресурс]. – URL: https://datatracker.ietf.org/doc/html/rfc826 (дата обращения: 20.05.2026).

5. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3: RFC 8446. – IETF, 2018. [Электронный ресурс]. – URL: https://datatracker.ietf.org/doc/html/rfc8446 (дата обращения: 20.05.2026).
6. Fielding R. et al. Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing: RFC 7230. – IETF, 2014.
7. Bellovin S.M. Security Problems in the TCP/IP Protocol Suite // ACM SIGCOMM Computer Communication Review. – 1989. – Vol. 19, No. 2. – P. 32–48.
8. Cisco Systems. Dynamic ARP Inspection Configuration Guide. – Cisco, 2020. [Электронный ресурс]. – URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_55_se/configuration/guide/scg3750/swdynarp.html (дата обращения: 22.05.2026).
9. Rose S. et al. Zero Trust Architecture: NIST SP 800-207. – NIST, 2020. [Электронный ресурс]. – URL: https://doi.org/10.6028/NIST.SP.800-207 (дата обращения: 22.05.2026).
10. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
11. Verizon. 2024 Data Breach Investigations Report. – Verizon, 2024. [Электронный ресурс]. – URL: https://1password.com/blog/verizon-data-breach-report-2024-analysis (дата обращения: 29.05.2026).