Отчёт по лабораторной работе №4

ЗАХВАТ ПОЧТОВОГО СЕРВЕРА

Астраханцева Анастасия
Ибатулина Дарья
Ганина Таисия
Шошина Евгения
Кадирова Мехрубон
Хассан Факи Абакар
(группа НФИбд-01-22)

Содержание

Список иллюстраций

1 Цель работы

Проверить на учебном стенде защищённость почтового сервера Microsoft Exchange методом имитации реальной цепочки атаки: от разведки и фингерпринтинга до валидации наличия известных уязвимостей и подтверждения возможности удалённого выполнения кода (RCE).
В качестве итогового артефакта — получить доказательство проникновения (флаг) и подготовить рекомендации по устранению обнаруженных рисков.

2 Задание

1. Выполнить разведку сети и обнаружить активные хосты в подсети `195.239.174.0/24`. Зафиксировать открытые порты и сервисы, представляющие интерес для почтовой инфраструктуры.

2. Идентифицировать веб-интерфейс OWA / почтовый сервис на целевом хосте (`195.239.174.1`) и собрать информацию, необходимую для фингерпринтинга версии сервера (страницы, ресурсы, заголовки).

3. Сопоставить найденную версию сборки Exchange с публичными базами уязвимостей (CVE, KB, EPSS) и выбрать приоритетные CVE для дальнейшей проверки (фильтр: CVSS $\geqslant 9$, наличие пометок `Public exploit` / `Known exploited`).

4. В лабораторной среде проверить наличие верифицируемых векторов (символически — через готовые модули фреймворков), подтвердить возможность получения интерактивной сессии на целевой системе **только в рамках разрешённого стенда**. Зафиксировать найденный флаг и все артефакты.

5. Подготовить отчёт: выводы по разведке, соответствие сборки уязвимостям, полученные артефакты (скриншоты, логи), оценку риска и практические рекомендации по устранению и предотвращению повторной компромета-

ции.

3 Теоретическое введение

3.1 1. Поверхность атаки Microsoft Exchange

Microsoft Exchange — комплексный почтовый сервер с компонентами, доступными по сети (SMTP, OWA, EWS, Autodiscover и т. д.). Наличие публичного веб-интерфейса (OWA) и сервисов, обрабатывающих удалённые запросы, делает Exchange привлекательной целью: уязвимости в обработке внешних запросов могут привести к обходу аутентификации или удалённому выполнению кода.

3.2 2. Классы уязвимостей, применимых к Exchange

- **SSRF (Server-Side Request Forgery)** — позволяет злоумышленнику вынудить сервер выполнить запросы к внутренним конечным точкам от имени сервера (основной вектор ProxyLogon — CVE-2021-26855).

- **Привилегированная эскалация / подделка контекста** — уязвимости, позволяющие выдавать себя за сервисную учётную запись или переключать контекст (см. CVE-2021-34523 и CVE-2021-31207).

- **Запись произвольного файла / web-shell / RCE** — возможность записать на сервер файл, который затем может выполнить код (CVE-2021-34473 и связанные CVE), обеспечивая полноценную удалённую эксплуатацию.

3.3 3. Оценка риска: CVSS и EPSS

- **CVSS (Common Vulnerability Scoring System)** предоставляет количественную оценку критичности уязвимости (конфиденциальность, целостность, доступность, сложность эксплуатации и т.д.). Значения $\geqslant 9$ указывают на критические уязвимости.

- **EPSS (Exploit Prediction Scoring System)** измеряет вероятность реальной эксплуатации уязвимости в ближайшие 30 дней — высокий EPSS указывает на практическую опасность (наличие публичных PoC/эксплойтов или активность в дикой природе).

3.4 4. Инструменты разведки и фингерпринтинга

- **Сетевое сканирование** (идентификация хостов и открытых портов) — помогает найти сервисы, доступные извне (SMTP, HTTPS и др.).

- **Фингерпринтинг веб-интерфейса** — анализ HTML/ресурсов и HTTP-заголовков для определения версии приложения/сборки; DevTools браузера и заголовки ответа помогают установить соответствие версии с таблицами сборок.

- **Базы уязвимостей** — CVE, CVEdetails, Microsoft Security Bulletins, CISA KEV: используются для поиска известных проблем, дат раскрытия и наличия публичных эксплойтов.

3.5 5. Фреймворки для проверки

- **Metasploit** — фреймворк, содержащий модули для поиска, валидации и (в тестовой среде) эксплуатации уязвимостей. В образовательном и тестовом контексте Metasploit позволяет подтвердить наличие работоспособного вектора и собрать артефакты.
  > Важно: использование эксплойтов и активная эксплуатация допускаются **только** в лабораторных условиях или с явного письменного разрешения владельца инфраструктуры. Незаконное использование — преступление.

3.6 6. Постэксплуатация и артефакты

После успешной эксплуатации атакующий может получить интерактивную сессию (например, Meterpreter), что позволяет: просматривать файловую систему, извлекать конфиденциальные данные, устанавливать постоянные механизмы доступа (backdoor) и выполнять дальнейшее перемещение по сети. Для отчёта важны: логи соединений, снимки экрана, содержимое целевых файлов (флаг), хэши и временные метки действий.

3.7 7. Меры защиты

- Регулярно применять security updates / cumulative updates для Exchange.

- Ограничить доступ к OWA/EWS (WAF, ACL, IP-фильтрация), внедрить MFA для административных аккаунтов.

- Мониторинг: IDS/IPS/WAF правила для выявления попыток эксплуатации ProxyLogon/ProxyShell, анализ аномалий в журналах Exchange и IIS.

- Форензика и инцидент-респонс: собрать логи, образ памяти, и провести проверку на web-shells и следы постэксплуатации при подозрениях на компрометацию.

4 Выполнение лабораторной работы

4.1 Описание сценария

На внешнем периметре расположен почтовый сервер организации, необходимо получить доступ к флагу, расположенному в папке `C:Windows\system32\`.

4.2 Разведка на предмет поиска вектора атаки

Для обнаружения потенциальных целей и оценки поверхности атаки выполнены сканирование подсети и анализ веб-интерфейса. В качестве инструментов использовались: `nmap`, веб-браузер с DevTools (режим «Inspect»), поиск по базам уязвимостей (CVEdetails).

Инструменты и фильтры:

`nmap -sS -p- 195.239.174.0/24`, просмотр веб-страниц через HTTPS с включённым режимом разработчика, сверка сборок Exchange с KB и CVE.

4.2.1 Инцидент 1: Обнаружение почтового сервера (Exchange) на `195.239.174.1`

Что произошло:

В результате сканирования подсети `195.239.174.0/24` (утилита `nmap`) был обнаружен хост `195.239.174.1` с открытыми портами **25/tcp (smtp)** и **443/tcp (https)** — признак наличия почтового сервера с веб-интерфейсом OWA (Outlook Web

Access). (рис. fig. 4.1, fig. 4.7)

Что это означает:

Наличие SMTP и HTTPS на одном хосте сильно коррелирует с развёрнутым Microsoft Exchange. Публичный OWA делает сервер потенциальной целью для известных уязвимостей (например, ProxyLogon), что позволяет атакующему получить доступ к почтовым ящикам и выполнить пост-эксплуатационные операции.

Индикаторы и артефакты:

- IP цели: `195.239.174.1`.
- Открытые порты: `25/tcp`, `443/tcp`.
- Инструмент: `nmap` (см. вывод сканирования).
- Веб-интерфейс: `https://195.239.174.1/`.

Рекомендации:

1. Сохранить лог сканирования `nmap`.
2. Ограничить доступ к OWA (ACL/WAF, MFA).
3. Развернуть фронтенд/proxy для OWA и настроить мониторинг HTTPS-доступа. (рис. fig. 4.1)

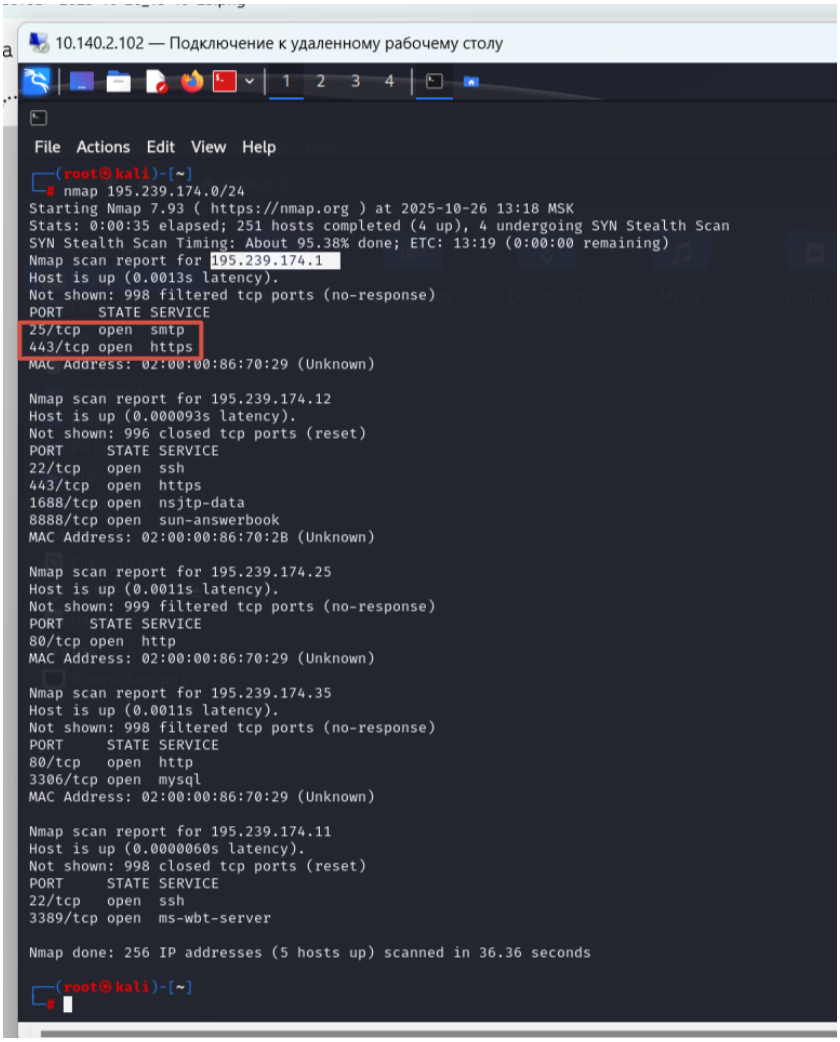

Рис. 4.1: Результат сканирования сети — вывод nmap, обнаружены порты 25 и 443

4.2.2 Инцидент 2: Фингерпринтинг версии Exchange через DevTools

Что произошло:

Через веб-интерфейс OWA открыта панель разработчика (Inspect) и проанализированы HTML/ресурсы страницы — обнаружены маркеры, позволяющие идентифицировать версию/сборку Exchange (атрибуты в `link`/`script`, комментарии). (рис. fig. 4.2, fig. 4.3)

Что это означает:

Определение точной версии (например, `15.1.1713`) позволяет соотнести ин-

сталляцию с известными исправлениями и CVE. Если сборка совпадает с уязвимой (до применения KB5000871 и т.п.), сервер может быть уязвим к эксплойтам ProxyLogon и связанным уязвимостям.

Индикаторы и артефакты:

- Метод: правый клик ☒ *Inspect (Q)* ☒ просмотр HTML/ресурсов.
- Найденные маркеры версии: выделенные строки/ресурсы в DevTools (см. рис. fig. 4.3).
- Примеры связанных KB: `KB5000871`.

Рекомендации:

1. Снять снапшот DevTools и сохранить HTML/ресурсы.
2. Получить HTTP-заголовки (`curl --head`) для подтверждения.
3. Сверить сборку с официальной таблицей Microsoft и применить недостающие security updates.

(рис. fig. 4.2, fig. 4.3)

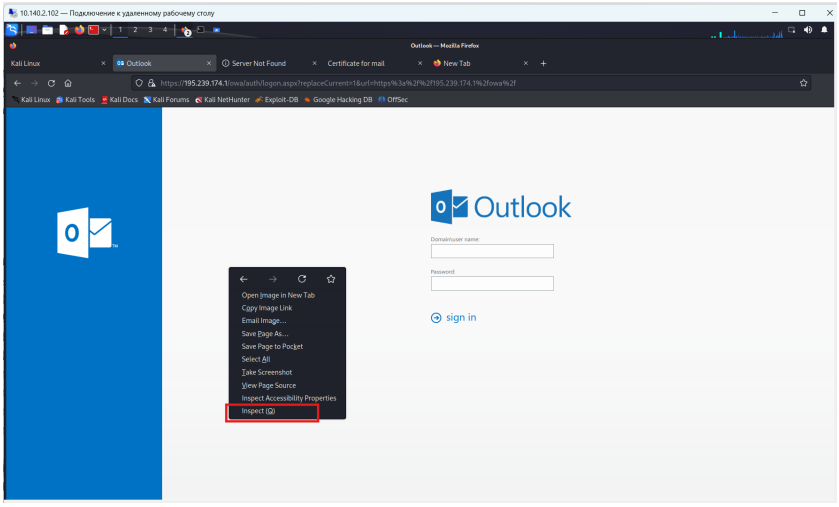

Рис. 4.2: Получение версии Exchange через режим разработчика — «Inspect (Q)»

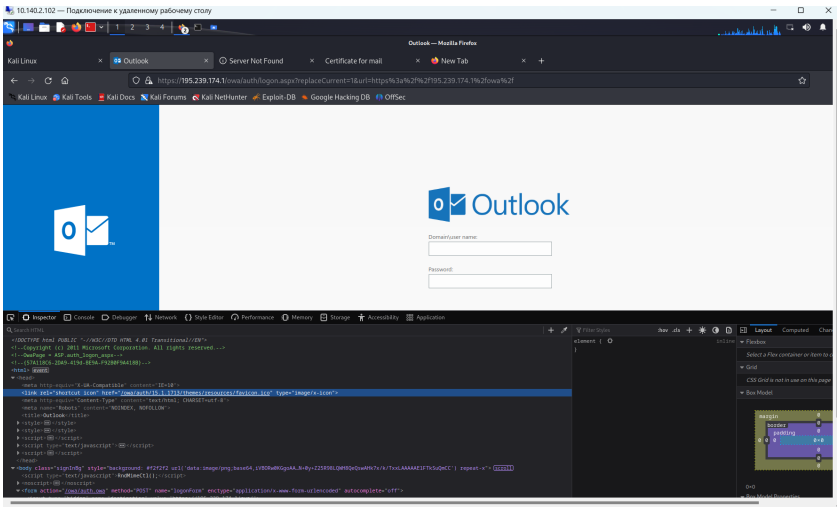

Рис. 4.3: Анализ HTML/ресурсов в DevTools — выделение строки с ресурсом/версией

4.2.3 Инцидент 3: Сопоставление сборки с бюллетенями и CVE

Что произошло:

По найденной сборке произведён поиск в справочных источниках Microsoft и в базе CVE (CVEdetails). На скриншотах видны таблицы сборок Exchange и соответствующие KB (включая `KB5000871` и сборку `15.1.1713`). (рис. fig. 4.4, fig. 4.5, fig. 4.6)

Что это означает:

Если развернутая версия совпадает с небезопасной сборкой, сервер подлежит немедленной проверке и экстренному обновлению. Наличие соответствующих CVE (например, CVE-2021-26855) увеличивает риск эксплуатации.

Индикаторы и артефакты:

- Обнаруженные версии/сборки: `15.1.1713`.
- Сопутствующие KB: `KB5000871`.
- Источники: `cvedetails.com`.

Рекомендации:

1. Проверить установленные обновления на сервере (PowerShell: `Get-ExchangeServer | Format-List Name,AdminDisplayVersion`).

2. При отсутствии патчей — провести экстренное применение security updates (с резервной копией и тестированием).

3. При признаках компрометации — изолировать сервер, собрать логи (IIS, Application, Security), дампы памяти и запустить IOC-сканирование на web-shells и признаки ProxyLogon.

(рис. fig. 4.4, fig. 4.5, fig. 4.6)

Exchange Server 2016 CU4	13 декабря 2016 г.	15.01.0669.032
Exchange Server 2016 CU5	21 марта 2017 г.	15.01.0845.034
Exchange Server 2016 CU6	27 июня 2017 г.	15.01.1034.026
Exchange Server 2016 CU7	19 сентября 2017 г.	15.01.1261.035
Exchange Server 2016 CU8	19 декабря 2017 г.	15.01.1415.002
Exchange Server 2016 CU9	20 марта 2018 г.	15.01.1466.003
Exchange Server 2016 CU10	19 июня 2018 г.	15.01.1531.003
Exchange Server 2016 CU11	16 октября 2018 г.	15.01.1591.010
Exchange Server 2016 CU12	12 февраля 2019 г.	15.01.1713.005
Exchange Server 2016 CU13	18 июня 2019 г.	15.01.1779.002
Exchange Server 2016 CU14	17 сентября 2019 г.	15.01.1847.003
Exchange Server 2016 CU15	17 декабря 2019 г.	15.01.1913.005
Exchange Server 2016 CU16	17 марта 2020 г.	15.01.1979.003
Exchange Server 2016 CU17	12 июня 2020 г.	15.01.2044.004

Рис. 4.4: Дата выпуска сборки Exchange Server и сопоставление с номерами сборок/KB

2019CU3+KB5000871	15.2.464.15	Mar-21	KB5000871	Download
2019CU2+KB5000871	15.2.397.11	Mar-21	KB5000871	Download
2019CU1+KB5000871	15.2.330.11	Mar-21	KB5000871	Download
2019+KB5000871	15.2.221.18	Mar-21	KB5000871	Download
2016CU17+KB5000871	15.1.2044.13	Mar-21	KB5000871	Download
2016CU16+KB5000871	15.1.1979.8	Mar-21	KB5000871	Download
2016CU15+KB5000871	15.1.1913.12	Mar-21	KB5000871	Download
2016CU14+KB5000871	15.1.1847.12	Mar-21	KB5000871	Download
2016CU13+KB5000871	15.1.1779.8	Mar-21	KB5000871	Download
2016CU12+KB5000871	15.1.1713.10	Mar-21	KB5000871	Download
2016CU11+KB5000871	15.1.1591.18	Mar-21	KB5000871	Download
2016CU10+KB5000871	15.1.1531.12	Mar-21	KB5000871	Download
2016CU9+KB5000871	15.1.1466.16	Mar-21	KB5000871	Download
2016CU8+KB5000871	15.1.1415.10	Mar-21	KB5000871	Download
2013CU22+KB5000871	15.0.1473.6	Mar-21	KB5000871	Download
2013CU21+KB5000871	15.0.1395.12	Mar-21	KB5000871	Download
2010 SP3 RU32	14.3.513.0	Mar-21	KB5000978	Download
2019CU8+KB4602269	15.2.792.5	Feb-21	KB4602269	Download
2019CU7+KB4602269	15.2.721.8	Feb-21	KB4602269	Download

Рис. 4.5: Таблица соответствия Exchange CU ☒ номер сборки (выделено 15.01.1713)

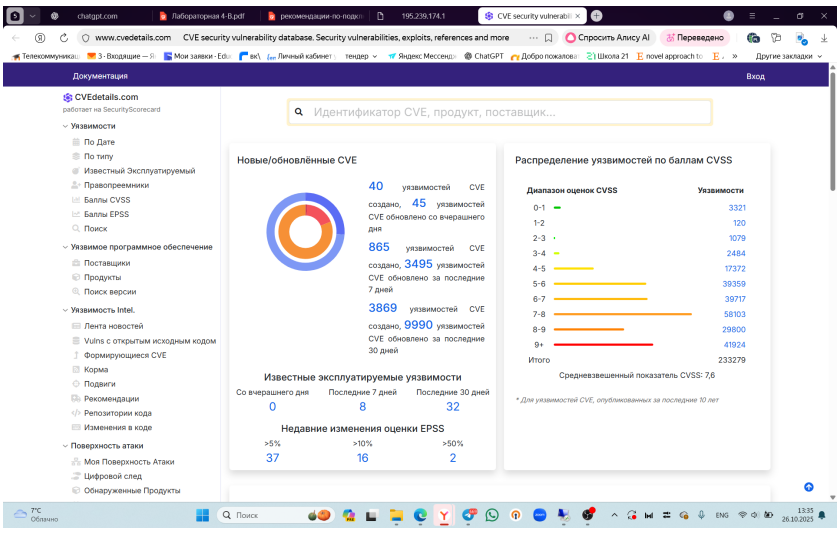

Рис. 4.6: Стартовая страница CVEdetails — поиск и справочные данные по уязвимостям

Для оценки возможности эксплуатации использовалась база CVE (CVEdetails) с фильтром по продукту **Microsoft Exchange Server** и порогом **CVSS >= 9**. Это позволило выделить уязвимости с высокой степенью риска и метками наличия

публичных эксплойтов / фактов эксплуатации в дикой природе (public exploit exists / Known exploited). (рис. fig. 4.7)

- Методика: фильтр CVSS ⩾ 9 ⊠ сортировка по меткам «Public exploit» / «Known exploited» ⊠ просмотр подробностей CVE (дата раскрытия, EPSS, наличие модулей Metasploit).

4.2.3.1 Инцидент 4: Приоритезация уязвимостей через CVE-поисковик

Что произошло:

На сервере/в окружении была сопоставлена версия Exchange с записями CVE. По результатам фильтрации получен список приоритетных уязвимостей, помеченных как **Public exploit** или **Known exploited** — их эксплуатация доказана на практике. (рис. fig. 4.7)

Что это означает:

Если дата раскрытия уязвимости (*Disclosure Date*) позже даты выпуска сборки сервера — значит уязвимость не была исправлена в этой сборке и может быть эксплуатируема против указанного сервера. Наличие публичного эксплойта (и особенно — модуля Metasploit) значительно упрощает автоматизацию атаки и повышает приоритет реагирования. (рис. fig. 4.8, fig. **??**)

Индикаторы и артефакты:

- Источник разведки: `cvedetails.com`.
- Примеры CVE с высокой вероятностью эксплуатации: `CVE-2021-34473`, `CVE-2021-34523`, `CVE-2021-34527` (см. страницы CVE — EPSS/метасплоит-модули). (рис. fig. 4.8, fig. **??**)
- Метки: `Public exploit`, `Known exploited`, EPSS > 90% — повышенный риск. (рис. fig. 4.8)

Рекомендации:

1. Немедленно сверить список CVE с реальной версией сервера (как минимум — календарная дата сборки против даты публикации CVE).
2. Сфокусировать первичную защиту и проверку на уязвимостях с метками

`Public exploit` и `Known exploited`.

3. При обнаружении соответствия — подготовить план экстренного патч-менеджмента и расследования на предмет следов эксплуатации.

(рис. fig. 4.7)

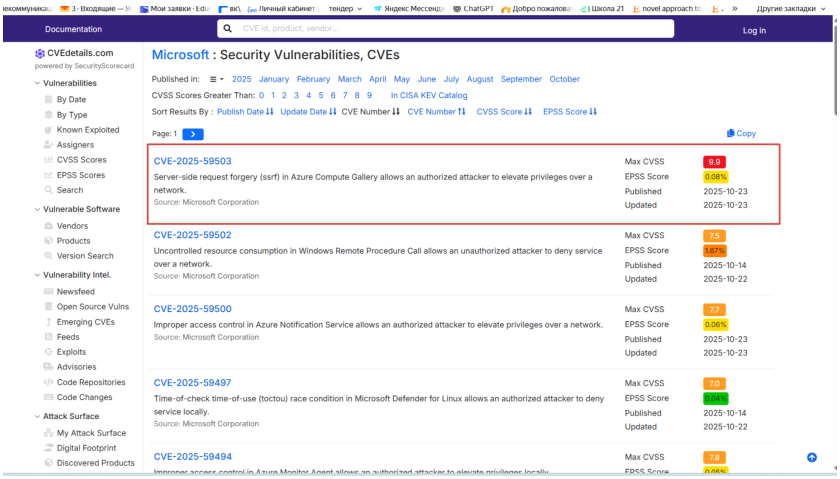

Рис. 4.7: Приоритезация уязвимостей Microsoft Exchange Server (CVSS >= 9)

4.2.3.2 Детальная проверка CVE (пример)

Что просмотрено:

Страницы CVE показывают: EPSS / вероятность эксплуатации, наличие модулей Metasploit и даты — *Disclosure Date* и *First seen* (появление эксплойтов в публичных репозиториях). Это даёт временную корреляцию между выпуском сборки сервера и появлением эксплойтов. (рис. fig. 4.8)

Вывод:

Если *Disclosure Date* (дата раскрытия уязвимости) **позже** даты сборки сервера — уязвимость может быть использована против текущей установки.

(рис. fig. 4.8)

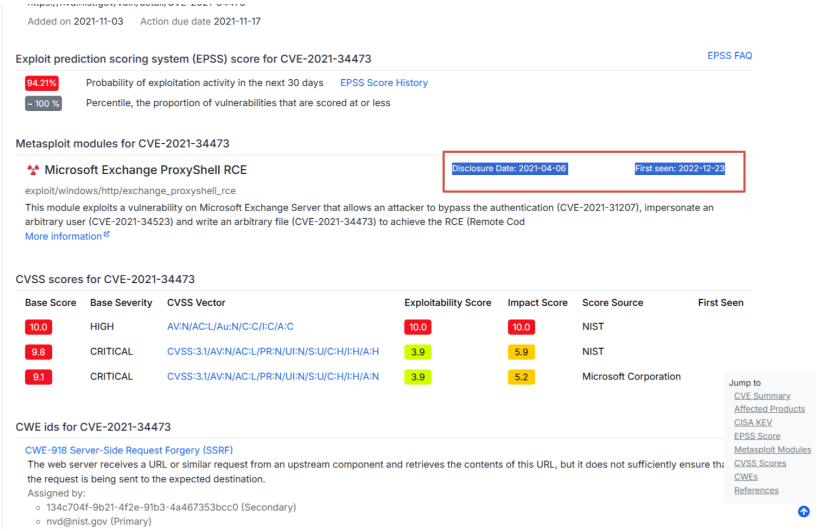

Рис. 4.8: Детальная информация по уязвимости (пример CVE-2021-34473) — EPSS, Metasploit module, Disclosure/First seen

4.2.4 Подготовка и использование Metasploit для поиска векторов

Для практической проверки возможности RCE и получения сессии использовался фреймворк Metasploit:

- Запуск msf6 ☒ `search Exchange` ☒ просмотр доступных модулей (включая `exchange_proxylogon_rce`, `exchange_proxyshell_rce`, `exchange_proxynothell_rce` и т.д.). (рис. fig. 4.9, fig. 4.10)

- Метасплоит-модули подтверждают наличие готовых реализаций эксплойтов для ряда CVE, что облегчает эксплуатацию.

Индикаторы и артефакты:

- Локальный вывод Metasploit: список модулей и их даты/статусы (рис. fig. 4.9).
- Наличие модулей с пометкой `excellent/Yes` (готов к использованию). (рис. fig. 4.9)

Рекомендации:

1. Использовать Metasploit **только** в рамках тестовой/лабораторной среды или с письменного разрешения владельца инфраструктуры.

2. Для проверки уязвимости — сначала выполнить безопасную валидацию без эксплуатации (fingerprinting, запросы HEAD, проверка заголовков, тестирование на тестовом стенде).
3. При подтверждении уязвимости — подготовить план реагирования: сбор логов, резервное копирование, установка патчей, последующий аудит и мониторинг.

(рис. fig. 4.9, fig. 4.10)

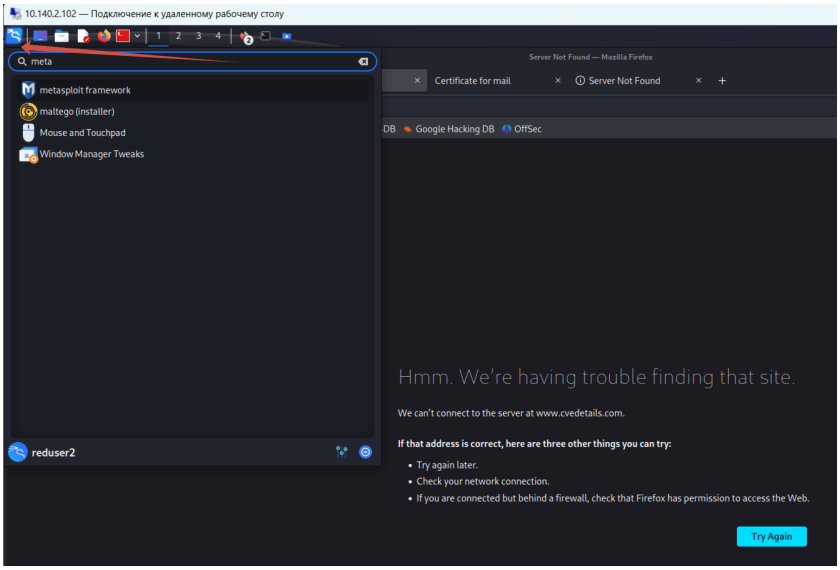

Рис. 4.9: Запуск Metasploit и поиск модулей по Exchange (вывод `search Exchange`)

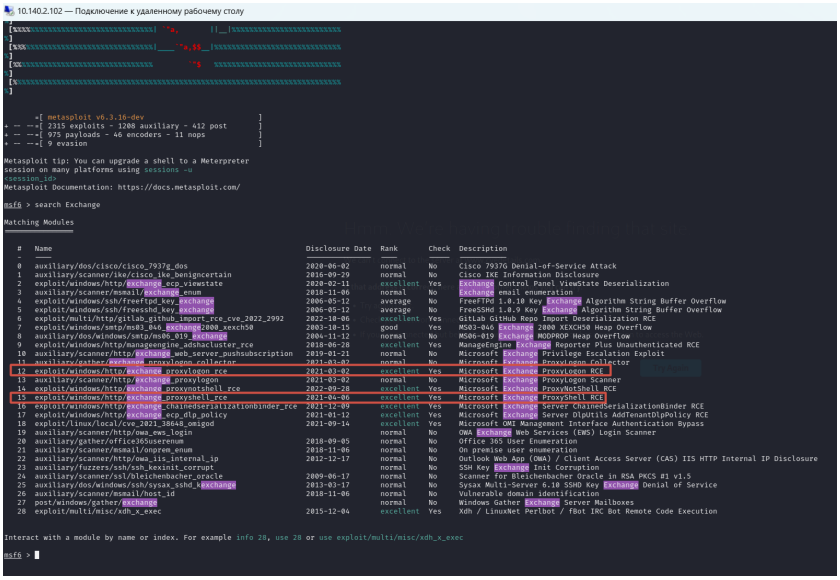

Рис. 4.10: Перечень модулей Metasploit, предназначенных для атак на Exchange (выделены модули RCE/ProxyShell/ProxyLogon)

4.3 Эксплуатация уязвимостей и захват флага (результаты)

В ходе практической работы подтверждена возможность получения RCE на почтовом сервере `195.239.174.1` с применением публичных модулей Metasploit (ProxyShell / ProxyLogon). Ниже — структурированная сводка наблюдений, артефактов и выводов.

4.3.1 Инструменты и условия

- Среда атакующего: Kali Linux с установленным Metasploit (msf6).
- Цель: `195.239.174.1` (Microsoft Exchange — OWA + SMTP).
- Источники артефактов: выводы Metasploit, сессии Meterpreter, снимки экрана DevTools и страницы CVE.

4.3.2 Эксплуатация ProxyShell (итоги)

Описание наблюдаемого процесса:

Модуль для ProxyShell (ProxyShell RCE, связанный с CVE-2021-34473 / CVE-2021-34523 / CVE-2021-31207) был запущен из фреймворка Metasploit. В выводе показано, что модуль успешно отправил полезную нагрузку на целевой сервер, удалённый хост отработал, и была открыта Meterpreter-сессия.

Ключевые наблюдения (логи/вывод):

- Запуск обработчика обратного соединения (reverse TCP handler).
- Сообщение: `The target is vulnerable.`
- Успешные этапы: получение FQDN backend, поиск валидных почтовых ящиков, создание и отправка черновика с webshell-аттачем, ожидание обратного подключения.
- Открыта `Meterpreter session 1` — подтверждение RCE. (рис. fig. 4.11)

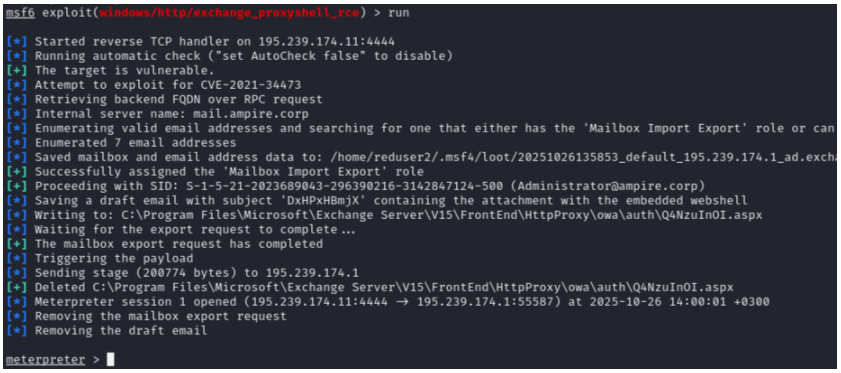

Рис. 4.11: Вывод Metasploit — успешная эксплуатация ProxyShell и открытие Meterpreter-сессии

Полученные артефакты:

- Открытая Meterpreter-сессия (запись в консоли).
- Флаг найден по пути `C:\windows\system32\flag_for_red_team.txt` — содержимое: `81596`. (рис. fig. 4.12)

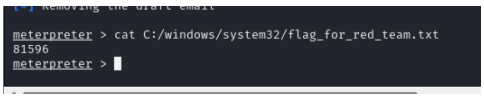

Рис. 4.12: Чтение файла флага в Meterpreter

Вывод: эксплуатация ProxyShell привела к получению интерактивной сессии и извлечению артефакта — флага. Это подтверждает реальную возможность RCE на исследуемом сервере при текущей конфигурации/сборке.

4.3.3 Альтернативная эксплуатация ProxyLogon (итоги)

Описание:

Для проверки альтернативного вектора использовался модуль, реализующий ProxyLogon (CVE-2021-26855 + связанная логика записи файла — CVE-2021-27065). В качестве целевого почтового ящика применялся адрес `manager1@ampire.corp` (легитимная служебная запись, обнаруженная в портале). В выводах также показан успешный цикл эксплуатации и открытие Meterpreter-сессии.

Ключевые наблюдения (логи/вывод):

- Настройка параметров модуля (rhosts, lhost, EMAIL).
- Сообщения модуля: `The target is vulnerable to CVE-2021-26855` / отправка MAPI/ProxyLogon-запросов / подготовка и запись полезной нагрузки.
- Открыта дополнительная Meterpreter-сессия (время/порты видны в выводе).

(рис. fig. 4.13–fig. 4.14)

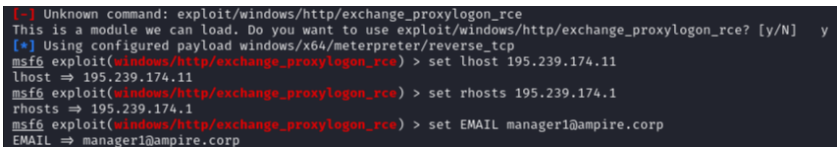

Рис. 4.13: Пример установки параметров модуля и запуска ProxyLogon (вывод Metasploit)

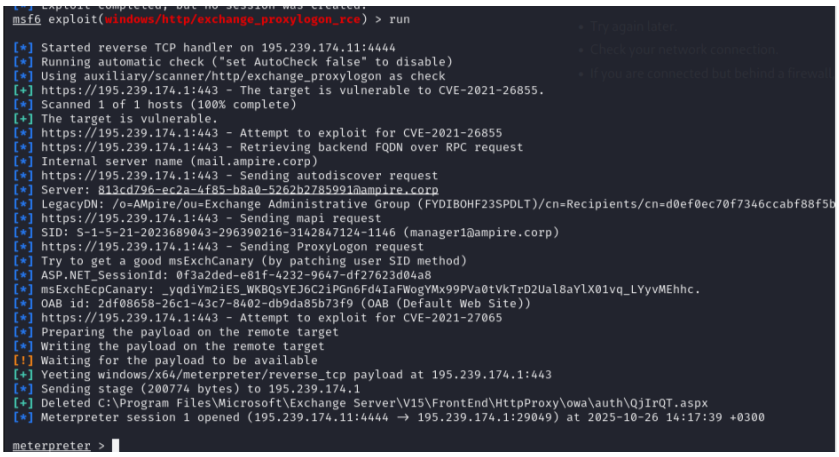

Рис. 4.14: Вывод успешной эксплуатации ProxyLogon — открыта Meterpreter-сессия

Вывод: проксимальные уязвимости ProxyLogon также позволяют получить RCE и доступ к файловой системе сервера; подтверждена возможность извлечения флага через оба канала.

4.3.4 Проблемы и замечания при работе с сессиями

- В некоторых попытках наблюдались сообщения об ошибках доступа к файлам (например, `Operation failed: The system cannot find the file specified.`), однако последующие команды `cat C:\windows\system32\flag_for_red_team.txt` успешно возвращали содержимое флага — `81596`. (рис. fig. 4.15)

- Метки `Disclosure Date / First seen` и наличие модулей Metasploit для соответствующих CVE позволяют объяснить, почему эксплуатация возможна в лабораторных/реальных условиях (см. раздел 2.2).

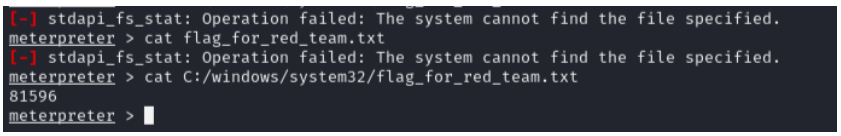

Рис. 4.15: Ошибки доступа и последующее успешное чтение файла флага в Meterpreter

4.3.5 Артефакты для отчёта и дальнейшего расследования

- Выводы `nmap` и скриншоты OWA/DevTools (фингерпринт версии).
- Страницы CVE/CVEdetails с метками «Public exploit / Known exploited» и информацией по модулям Metasploit (см. раздел 2.2).
- Логи Metasploit: полные сессии атак, таймстемпы открытия Meterpreter.
- Содержимое флага `C:\windows\system32\flag_for_red_team.txt` = `81596` (снимок вывода).
- Сохранённые черновики/файлы, которые модуль создавал на сервере (если доступны).

4.3.6 Рекомендации по реагированию

1. **Немедленно изолировать** сервер `195.239.174.1` от сети (VLAN/ACL).
2. **Собрать артефакты**: журналы IIS, Application, Security, Exchange, PowerShell; образ памяти; дампы файлов, созданных в `FrontEnd\HttpProxy\owa\`.
3. **Провести форензик**: поиск web-shell, новых учётных записей, подозрительных задач/служб, изменений в почтовых ящиках.

4. **Применить патчи**: установить все security updates/KB, относящиеся к CVE-2021-26855 / CVE-2021-34523 / CVE-2021-34473 и соответствующие CU для вашей версии Exchange.

5. **Поменять/отозвать** скомпрометированные учётные данные и сертификаты.

6. **Повысить мониторинг**: IDS/WAF правила для OWA/EWS, контроль целевых вызовов EWS/Autodiscover, детектирование массовых экспортов почтовых ящиков.

5 Выводы по работе

В результате выполнения лабораторной работы были успешно реализованы этапы разведки, анализа уязвимостей, их эксплуатации и получения удалённого доступа к почтовому серверу Microsoft Exchange.

1. **Проведена разведка сети.**
   Сканированием подсети `195.239.174.0/24` выявлен активный хост `195.239.174.1` с открытыми портами `25/tcp` (SMTP) и `443/tcp` (HTTPS), что позволило идентифицировать сервер Microsoft Exchange.

2. **Выполнено определение версии Exchange.**
   С помощью инструментов DevTools в браузере получены сведения о сборке сервера (`15.1.1713`), что позволило соотнести её с известными бюллетенями Microsoft и выявить неустановленные обновления безопасности.

3. **Проведён анализ CVE и приоритезация угроз.**
   Используя портал CVEdetails, определены наиболее критические уязвимости (CVSS $\geqslant 9$), имеющие публичные эксплойты и зафиксированные случаи эксплуатации:

   - CVE-2021-26855 (ProxyLogon, SSRF);
   - CVE-2021-34473 (ProxyShell, RCE);
   - CVE-2021-34523, CVE-2021-31207 (связанные компоненты цепочки ProxyShell).

4. **Подтверждено наличие эксплуатационных модулей.**
   В Metasploit обнаружены соответствующие модули (`windows/http/exchange_proxyshell`

`windows/http/exchange_proxylogon_rce`), что подтвердило возможность автоматизации атаки.

5. **Реализована эксплуатация ProxyShell.**
   При запуске модуля ProxyShell подтверждена уязвимость сервера, создан черновик с webshell, и установлена `Meterpreter`-сессия с удалённым сервером. В каталоге `C:\Windows\System32\` найден флаг `flag_for_red_team.txt` с содержимым `81596`.

6. **Реализована эксплуатация ProxyLogon.**
   Аналогичный результат получен при использовании модуля ProxyLogon RCE — также открыта сессия и прочитан тот же флаг, что подтверждает множественные точки входа для RCE.

7. **Проведён анализ результатов и сформулированы меры реагирования.**
   Полученные результаты демонстрируют критическую уязвимость сервера, отсутствие актуальных обновлений безопасности и возможность удалённого исполнения кода с привилегиями администратора.