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

На внешнем периметре расположен почтовый сервер организации, необходимо получить доступ к флагу, расположенному в папке С:\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. 1).



Рис. 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).

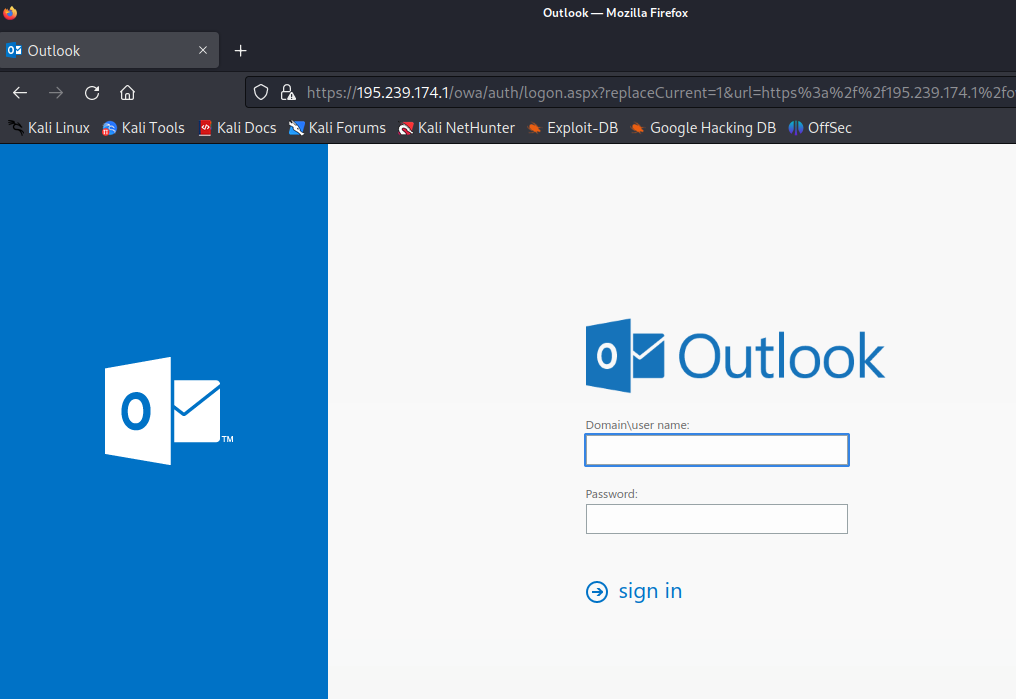


Рис. 2: Exchange Server

Определим версию Exchange Server для поиска уязвимостей (рис. 3, рис. 4).

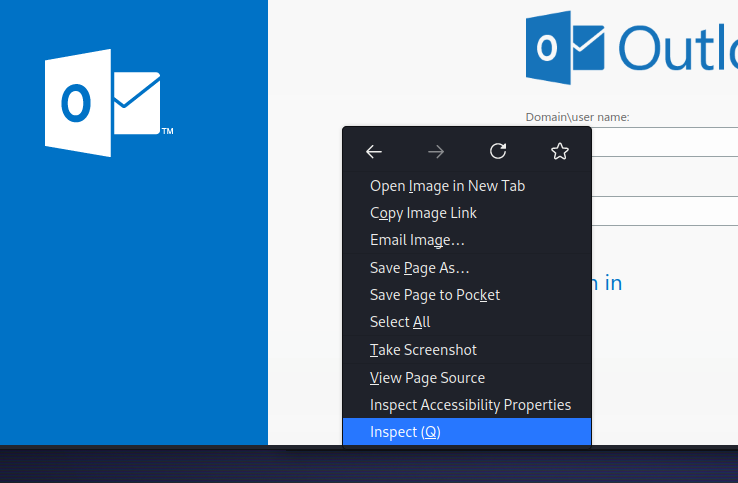


Рис. 3: Определение версии Exchange Server

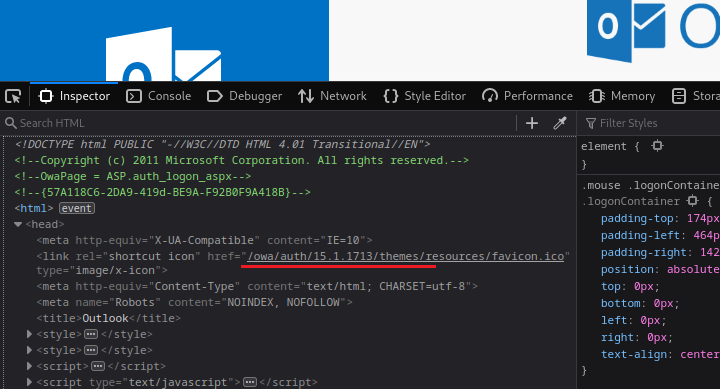


Рис. 4: Определение версии Exchange Server

Ищем нужную сборку в документации Microsoft Exchange (рис. 5).

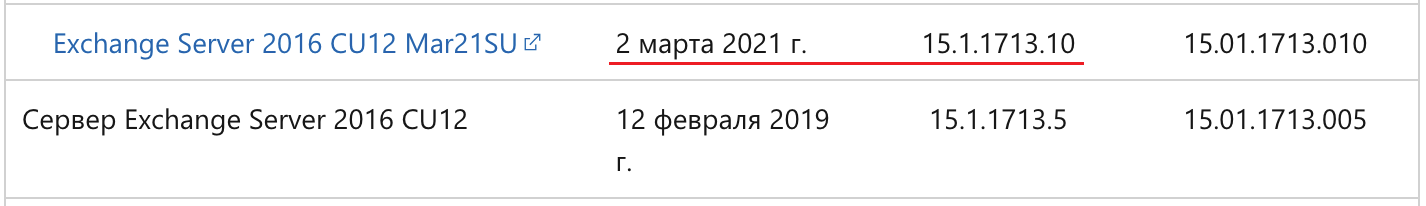


Рис. 5: Дата выпуска сборки Exchange Server

Для дальнейшего планирования атаки, переходим на сайт CVEdetails (рис. 6).

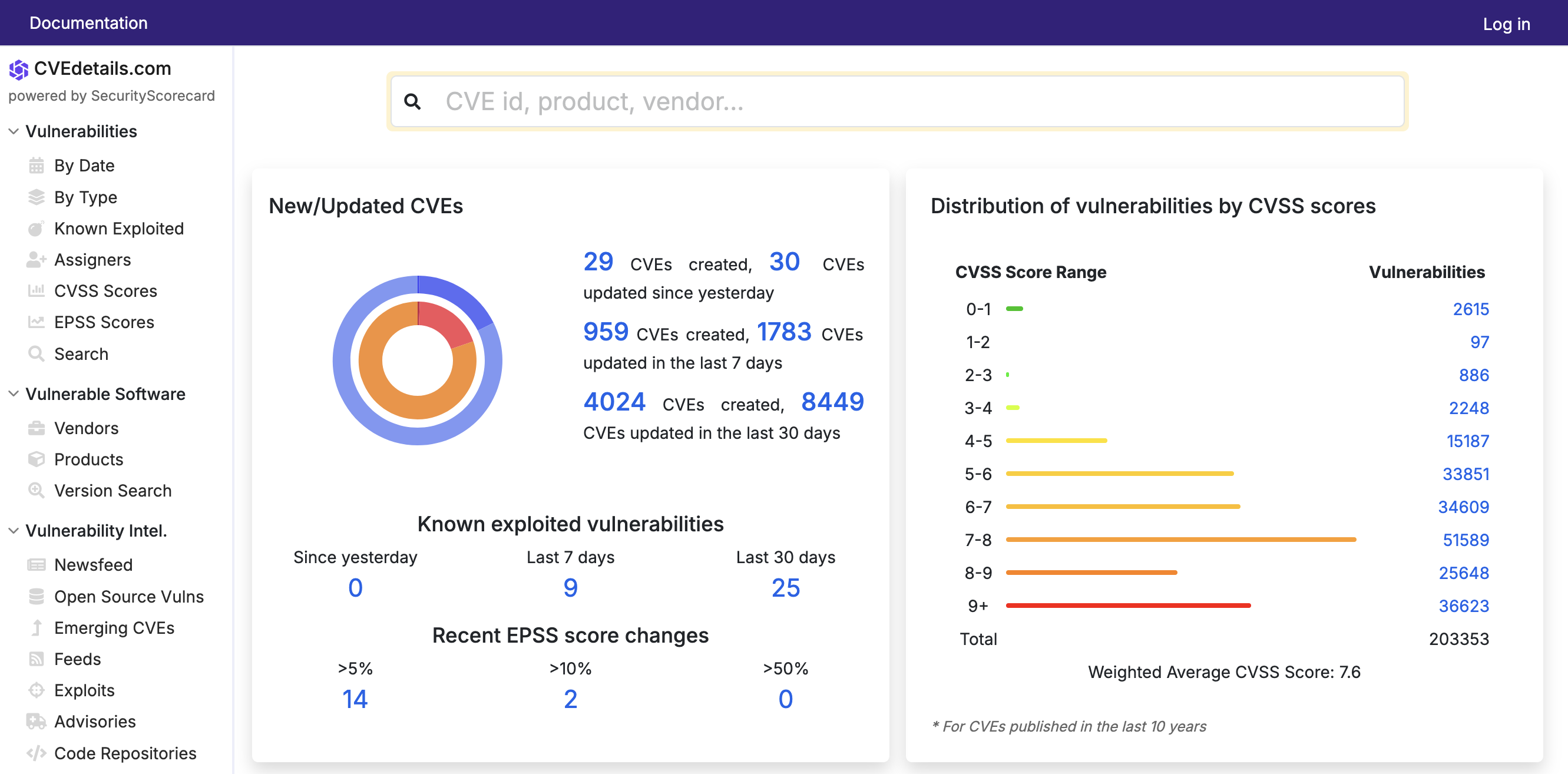


Рис. 6: Сайт CVEdetails

Найдем уязвимости, доступные к эксплуатации (рис. 7).

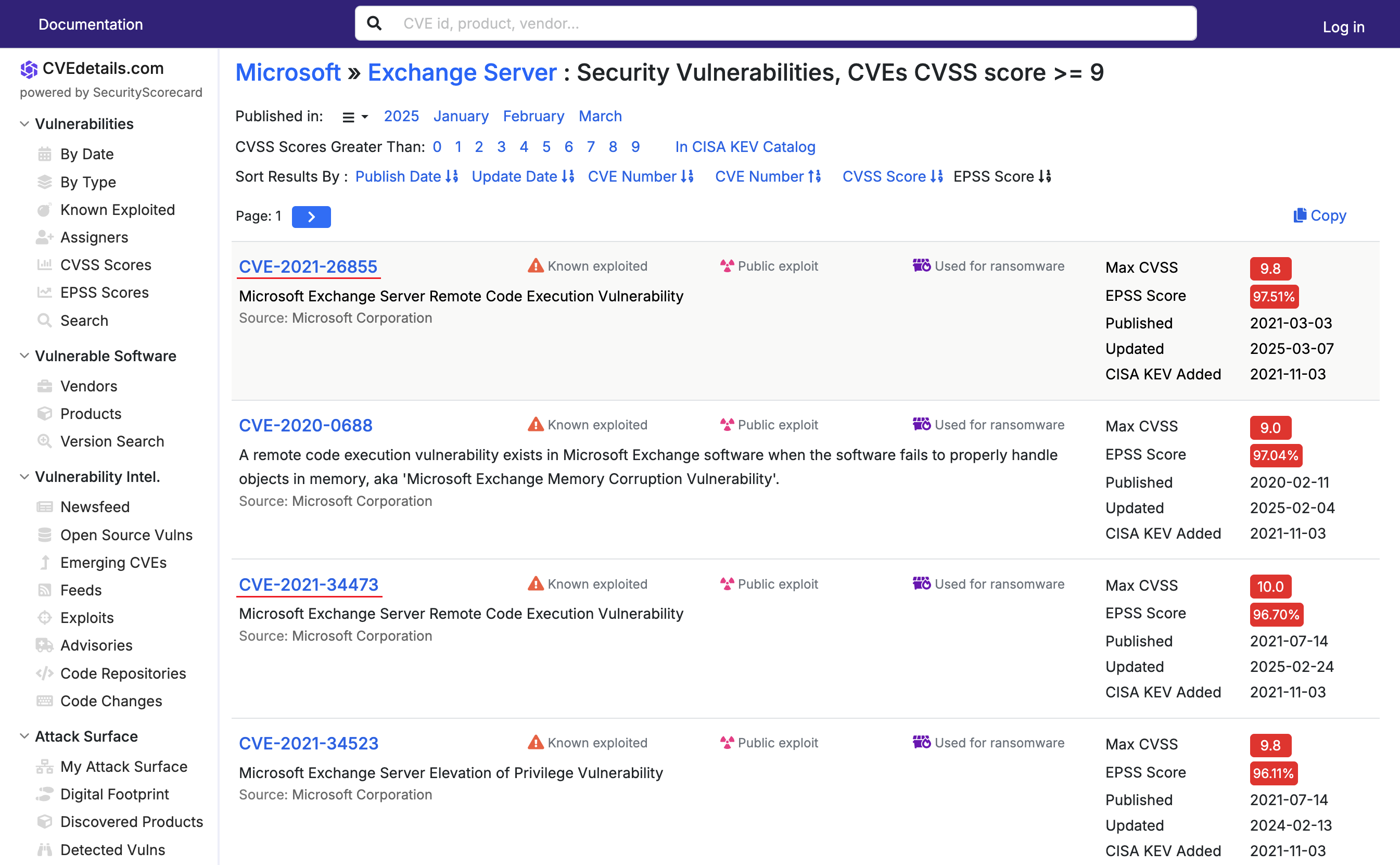


Рис. 7: Приоритетные уязвимости Microsoft Exchange Server

Изучим детальную информацию об уязвимостях (рис. 8, рис. 9).

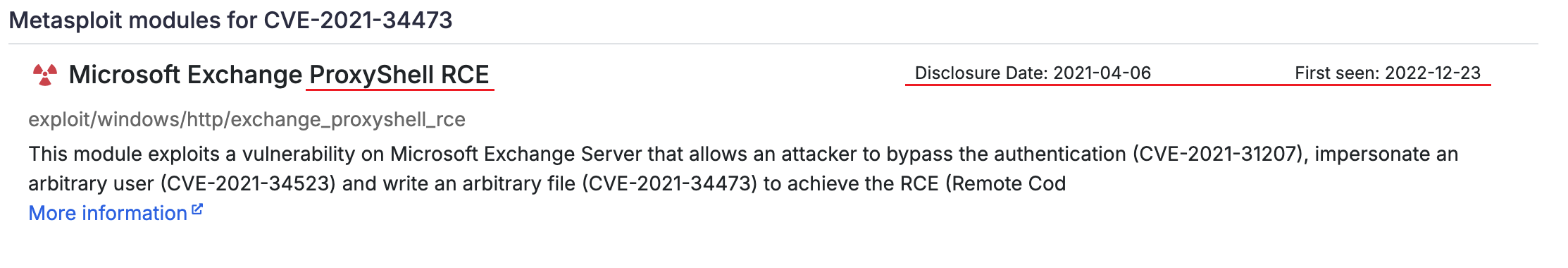


Рис. 8: Детальная информация по уязвимости CVE-2021-34473

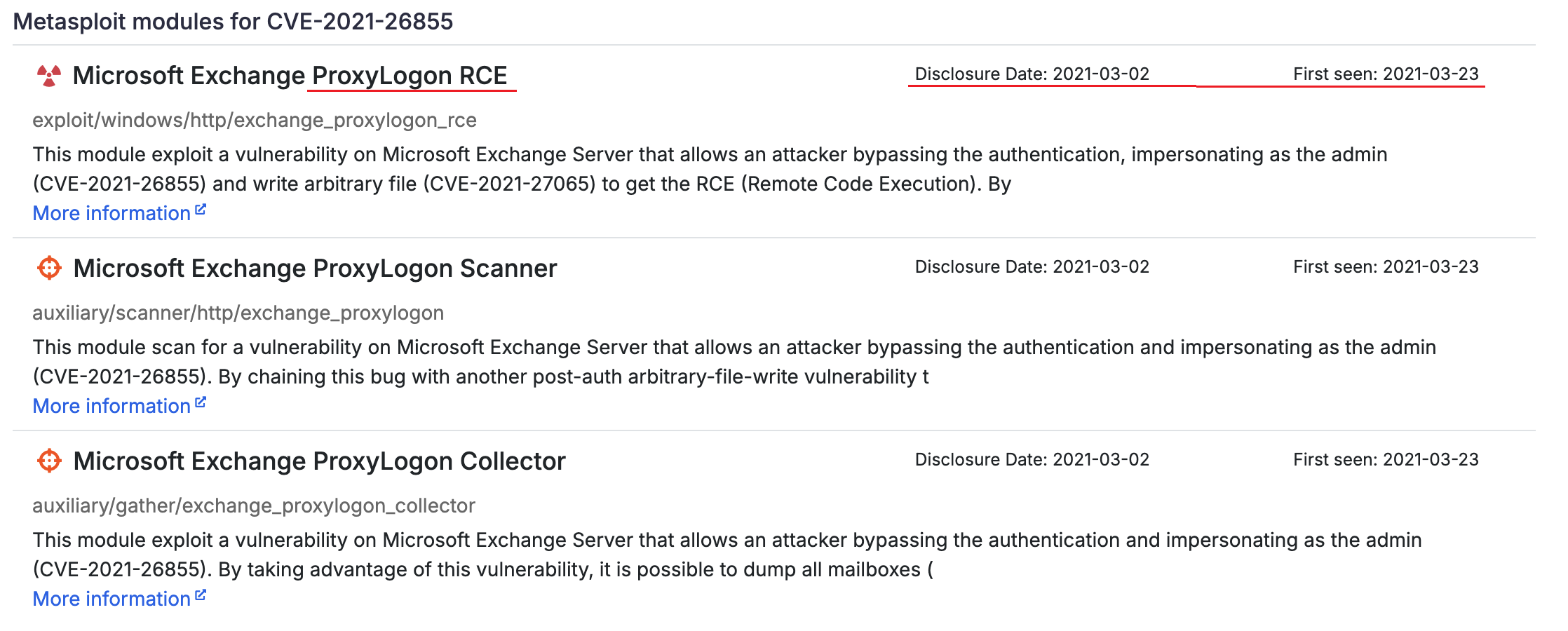


Рис. 9: Детальная информация по уязвимости CVE-2021-26855

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. 10, рис. 11).

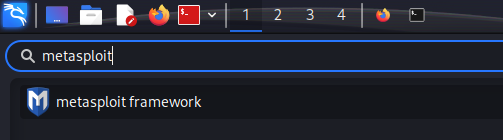


Рис. 10: Запуск модуля Metasploit

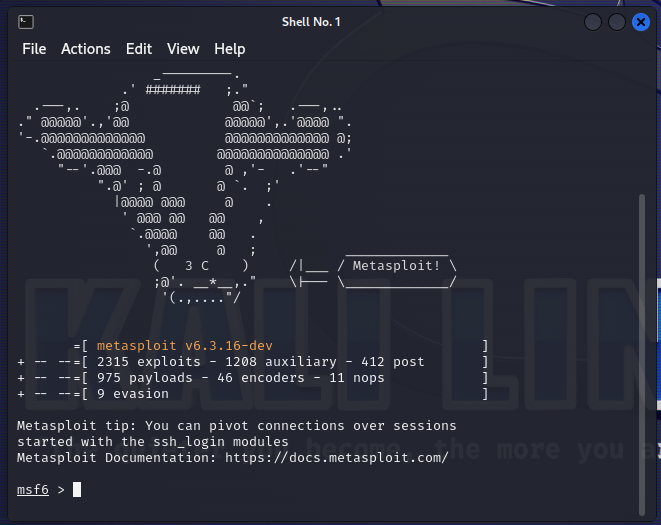


Рис. 11: Запуск модуля Metasploit

Проведем сканирование с помощью данного модуля (рис. 12).

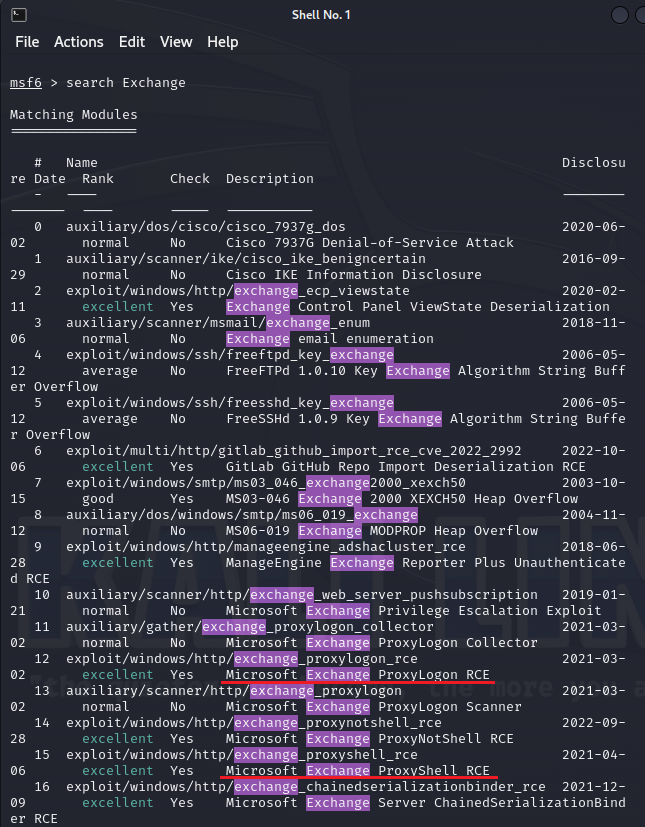


Рис. 12: Модули Metasploit для атаки на Microsoft Exchange Server

Для атаки мы воспользуемся уязвимостью ProxyShell.

## 2.2 Атака с использованием уязвимости ProxyShell

Воспользуемся модулем windows/http/exchange\_proxyshell\_rce (рис. 13).

Рис. 13: Модуль windows/http/exchange_proxyshell_rce

Рис. 13: Модуль windows/http/exchange\_proxyshell\_rce

Зададим параметры lhost и rhosts (рис. 14, рис. 15).

Рис. 14: Установка параметров

Рис. 14: Установка параметров

Рис. 15: Установка параметров

Рис. 15: Установка параметров

Запустим модуль ProxyShell и получим meterpeter-сессию. (рис. 16).

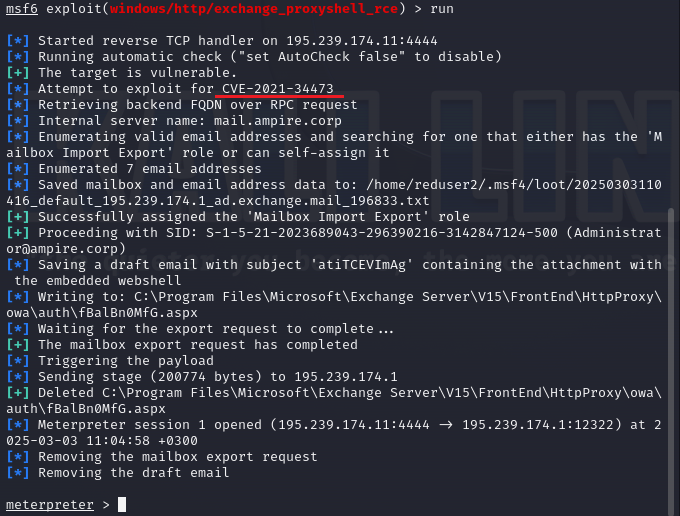


Рис. 16: Процесс эксплуатации уязвимого сервера Microsoft Exchange

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. 17).

Рис. 17: Поиск и чтение содержимого флага

Рис. 17: Поиск и чтение содержимого флага

# 3 Вывод

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