Отчет по лабораторной работе №5

Дисциплина: «Кибербезопасность предприятия»

Тема: Эксплуатация уязвимостей Microsoft Exchange Server

Выполнили:

Апареев Д.А.

Игнатенкова В.Н.

Демидович Н.М.

Ендонова А.В.

Машковцева К.С.

Шубнякова Д.И.

Задача

На внешнем периметре расположен почтовый сервер организации, необходимо получить доступ к флагу, расположенному в папке C:\Windows\system32\.

Теоретическое введение

Теоретическое введение

Microsoft Exchange Server представляет собой почтовый сервер и сервер совместной работы, обеспечивающий доставку и хранение электронной почты, календарей и других данных пользователей организации. Для доступа к почтовому ящику часто используется веб-интерфейс Outlook Web App (OWA), доступный по протоколу HTTPS и размещаемый на внешнем периметре, что делает его привлекательной целью для злоумышленников.

Критические уязвимости в Microsoft Exchange Server позволяют удалённо выполнять произвольный код (RCE) на уязвимом сервере, обходя стандартные механизмы аутентификации.Одними из наиболее известных являются цепочки ProxyShell и ProxyLogon, которые затрагивают компоненты, обрабатывающие входящие HTTP-запросы и запросы к внутренним службам Exchange.

ProxyShell представляет собой комбинацию нескольких уязвимостей (CVE-2021-31207, CVE-2021-34523, CVE-2021-34473), использование которых даёт возможность обойти аутентификацию, выдать себя за произвольного пользователя и записать файл на сервере, тем самым добившись удалённого выполнения кода. В случае отсутствия установленных обновлений злоумышленник может получить полный контроль над сервером и доступ ко всем данным почтовой системы.

ProxyLogon основан на уязвимости серверной подделки запросов (SSRF) CVE-2021-26855, позволяющей внешнему атакующему формировать HTTP-запросы к внутреннему интерфейсу Exchange от имени машинного аккаунта сервера. В сочетании с уязвимостью CVE-2021-27065 это даёт возможность записывать и запускать произвольные файлы, что также приводит к RCE и компрометации почтового сервера.

Для практической эксплуатации указанных уязвимостей в лабораторной работе применяется программный комплекс Metasploit Framework, содержащий специализированные модули `windows/http/exchange_proxyshell_rce` и `windows/http/exchange_proxylogon_rce`. [1] Данные модули автоматизируют формирование последовательностей запросов к уязвимому серверу Exchange и позволяют получить интерактивную сессию meterpreter на целевой системе.

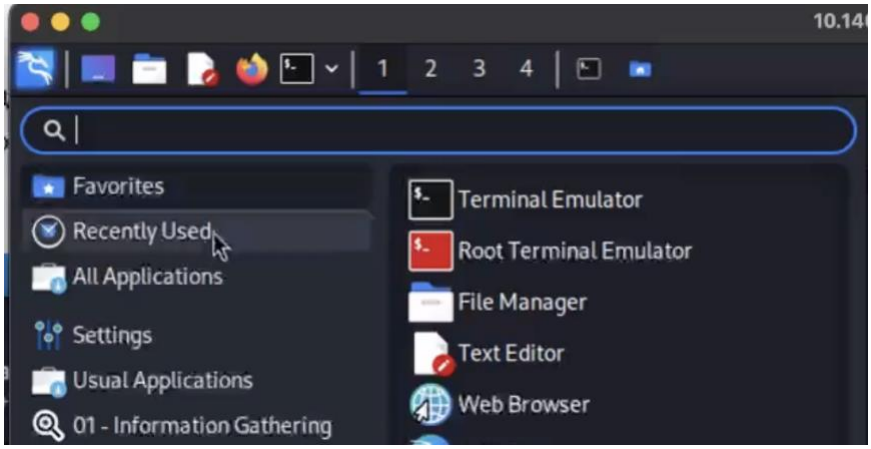
Выполнение лабораторной работы

Способы получения флага

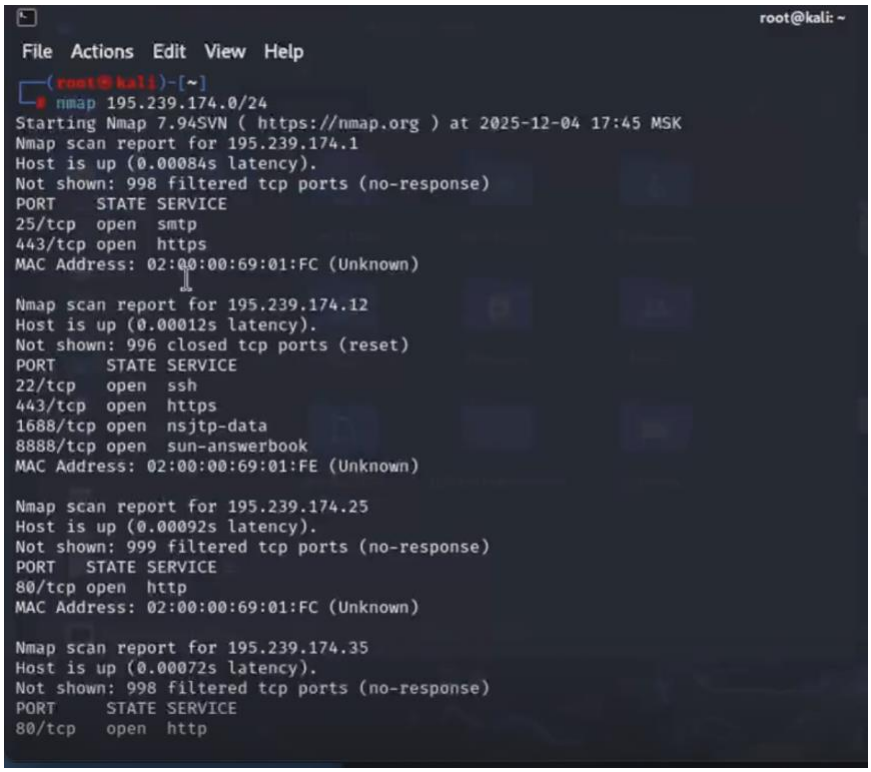
Флаг можно получить различными способами. Предварительно необходимо провести разведку инфраструктуры для обнаружения и дальнейшей эксплуатации уязвимостей.

Разведка на предмет поиска вектора атаки

Запускаем терминал.



Сканируем подсеть 195.239.174.0/24 для поиска открытых портов, которые можно использовать для атаки на инфраструктуру. Сканирование проводим с использованием утилиты nmap.

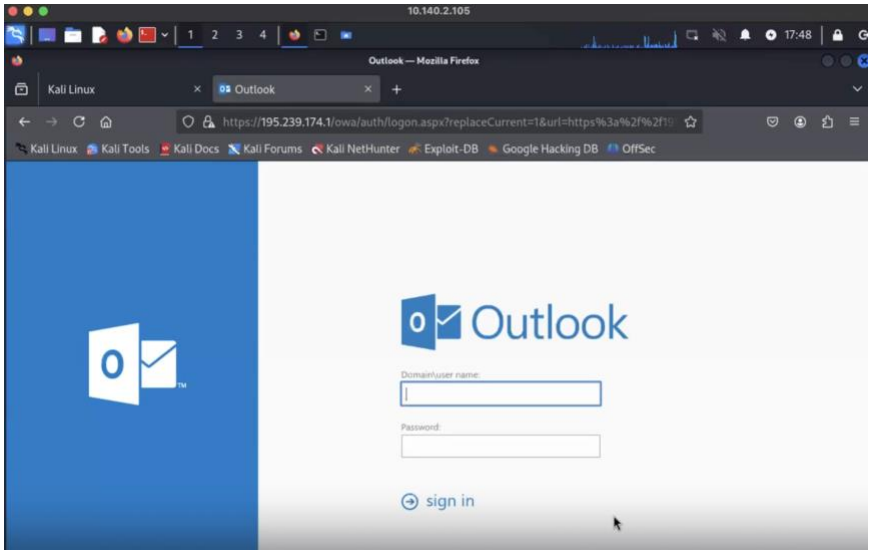


В результате сканирования на хосте 195.239.174.1 получены следующие открытые порты:

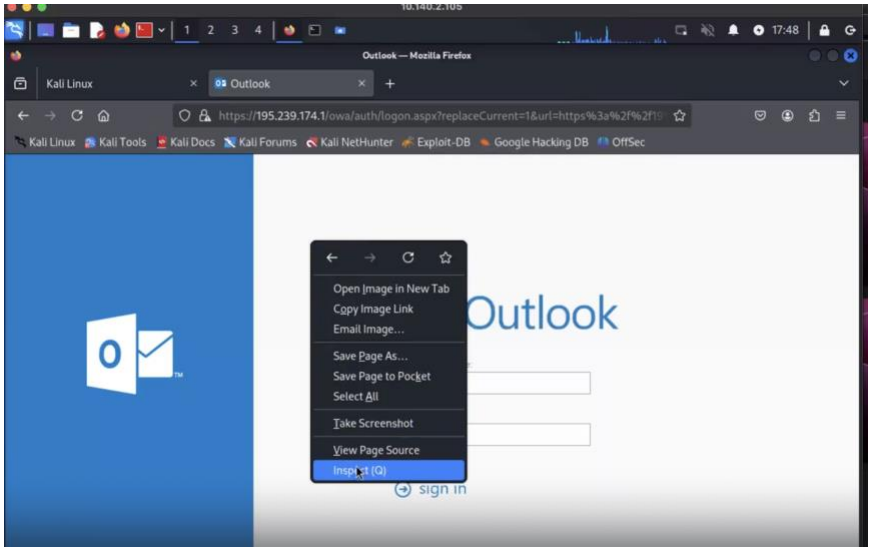
25 порт – стандартный порт, предназначенный для передачи электронных писем между почтовыми сервисами;

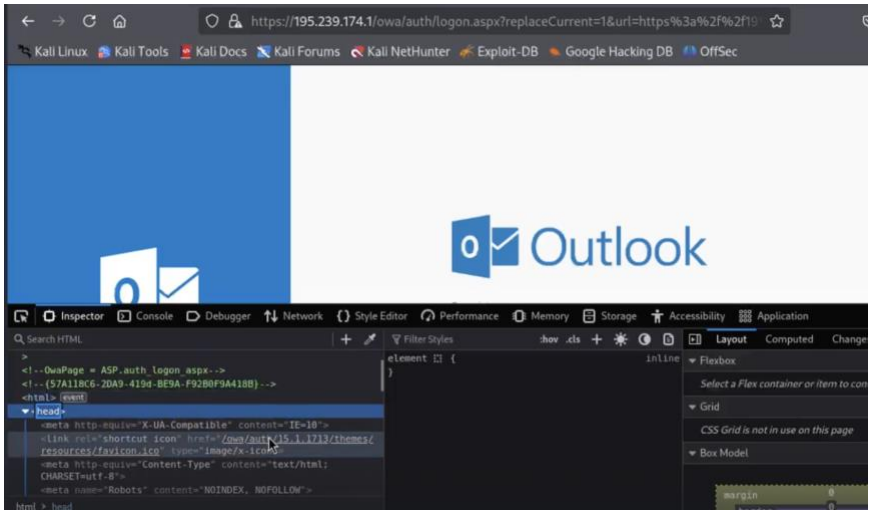
443 порт – стандартный порт для защищенной связи веб-браузера.

Наличие данных портов предполагает, что на хосте 195.239.174.1 установлен почтовый сервер. В наличии почтового сервера можно убедиться по адресу https://195.239.174.1.

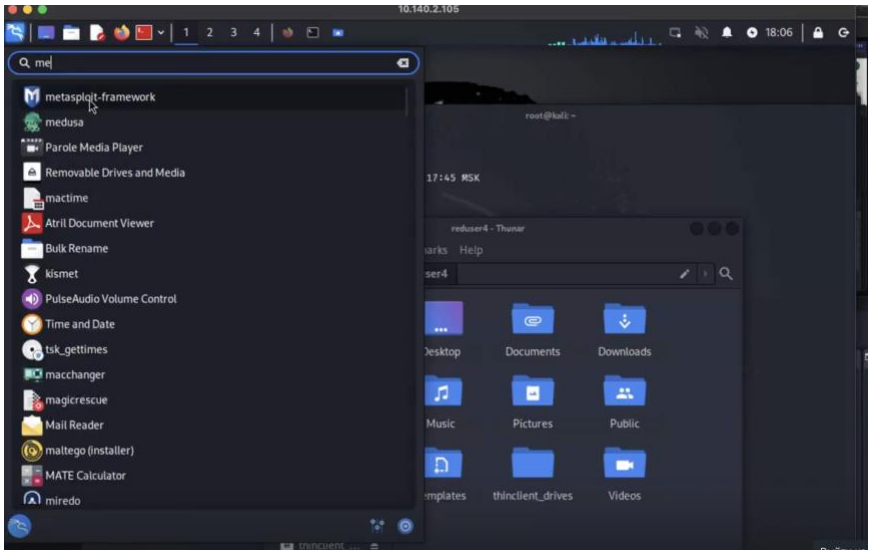


Для поиска уязвимостей предварительно определим версию Exchange Server.

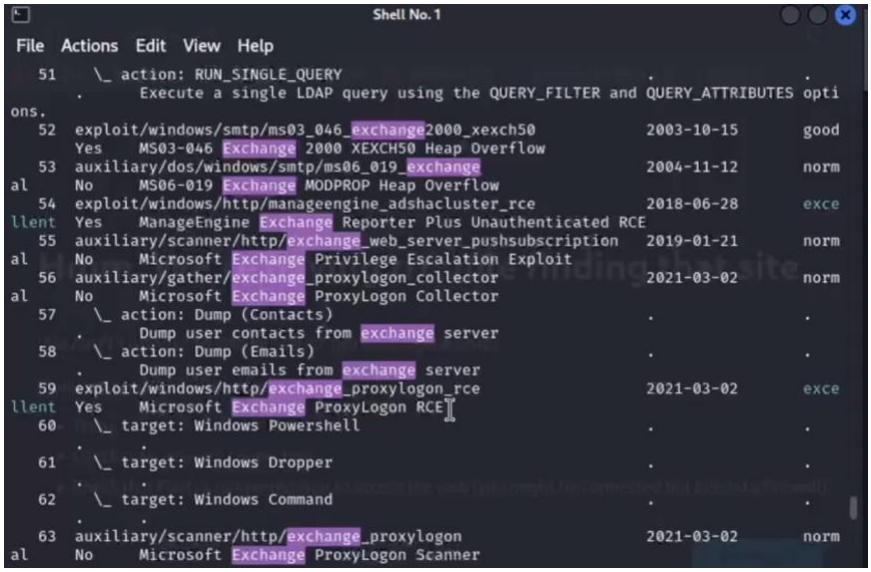




Для атаки необходимо использовать инструмент для создания, тестирования и использования exploit Metasploit. Для поиска возможных векторов атаки провести дальнейшее сканирование с помощью данного модуля.



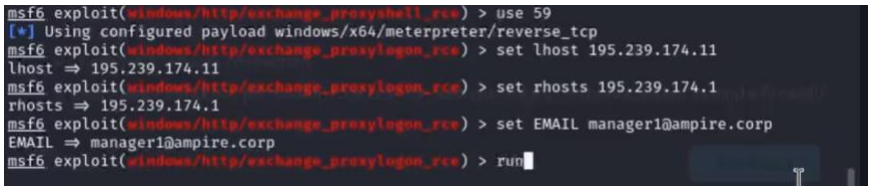
Для захвата флага необходимо получить сессию с удаленным хостом 195.239.174.1 с использованием возможность RCE. Далее произвести захват флага, эксплуатируя возможность RCE двумя модулями.



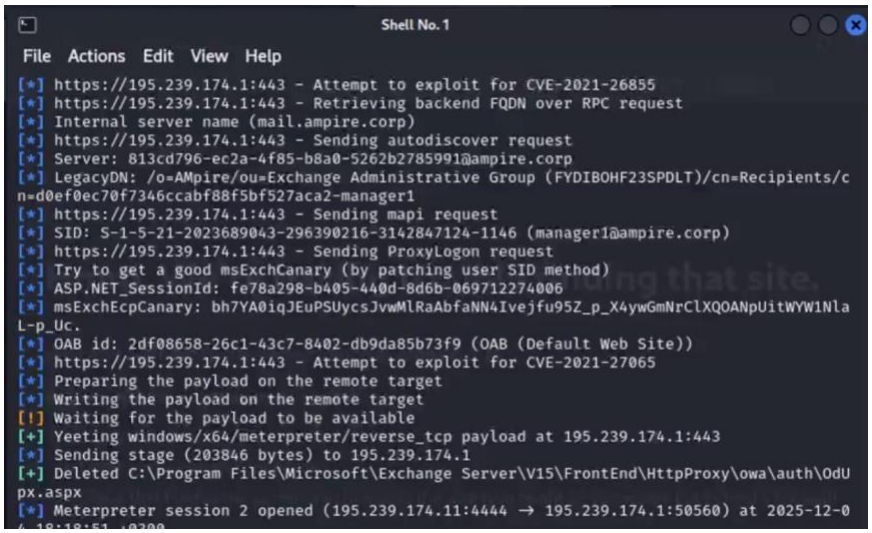
Использование уязвимости ProxyShell

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.

Воспользуемся модулем windows/http/exchange_proxyshell_rce. Выбираем модуль 59 и задаем параметры lhost и rhost.



Далее запустим модуль ProxyShell и получим meterpeter-сессию.



На скриншоте (Рисунок 9) представлено, что в процессе эксплуатации модуля ProxyShell обнаружена и проэксплуатирована уязвимость CVE-2021-34473 – https://www.cvedetails.com/cve/CVE-2021-34473.

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

Выводы

Мы успешно получили доступ к флагу, расположенному в папке C:\Windows\system32\.