Отчёт по лабораторной работе №4

Захват сервера базы данных

Кроитору Екатерина, Захаренко Анастасия, Щербакова Вероник

Содержание

Список иллюстраций

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)
- Метасплойт-фреймворк
- Bash-скрипт для bruteforce-атаки
- Сетевые утилиты: nmap, proxychains
- 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.

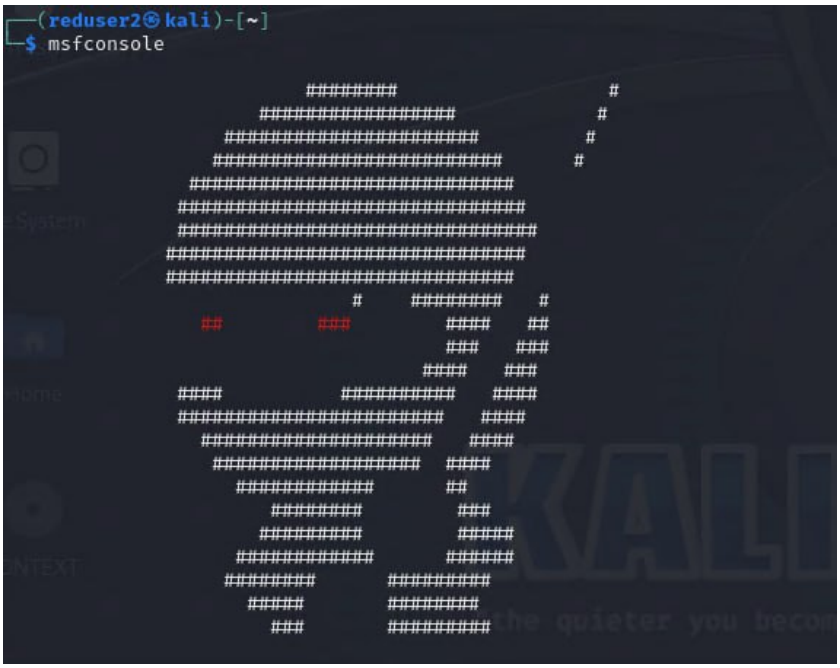

Рис. 3.1: Скрин 1

3.2 2. Установка параметров модуля и запуск атаки

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

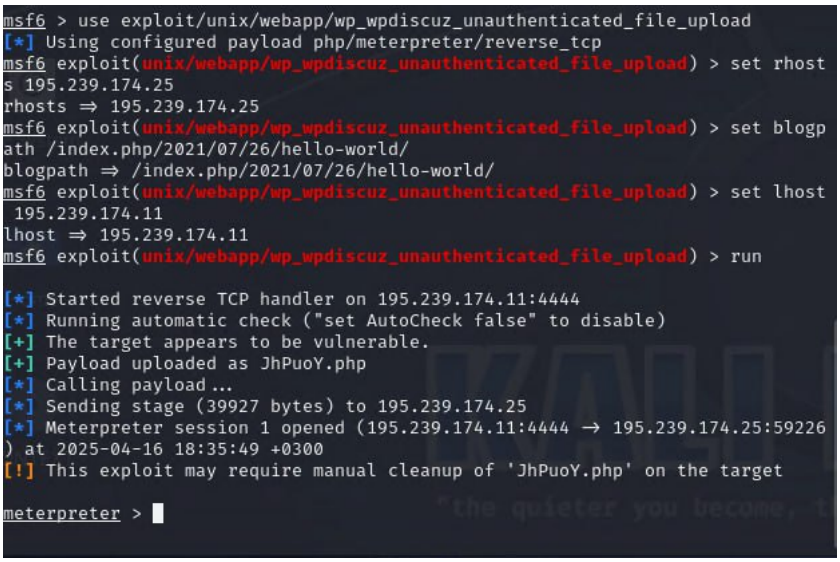

Рис. 3.2: Скрин 2

3.3 3. Успешное получение сессии

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

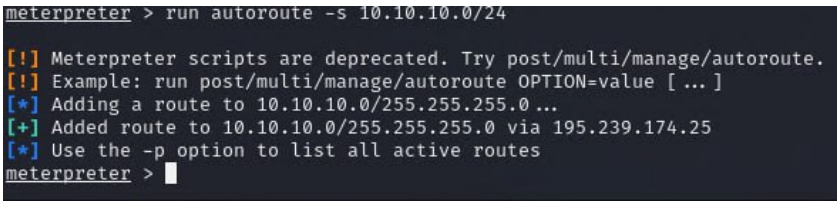

Рис. 3.3: Скрин 3

3.4 4. Определение сетевых интерфейсов

Выполняется просмотр интерфейсов на скомпрометированной машине. Выявлена сеть 10.10.10.0/24.

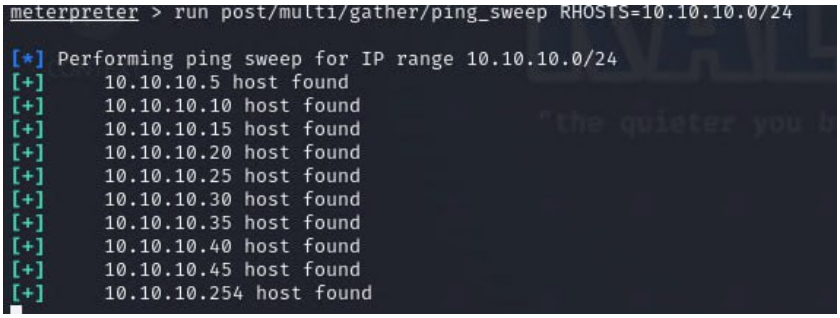

Рис. 3.4: Скрин 4

3.5 5. Добавление маршрута через autoroute

Добавлен маршрут к внутренней сети с помощью команды autoroute.

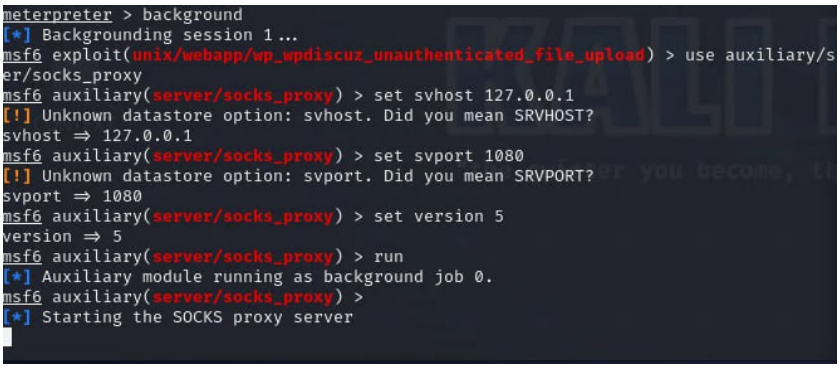

Рис. 3.5: Скрин 5

3.6 6. Сканирование внутренней сети

Запущен модуль multi/gather/ping_sweep для выявления активных хостов.

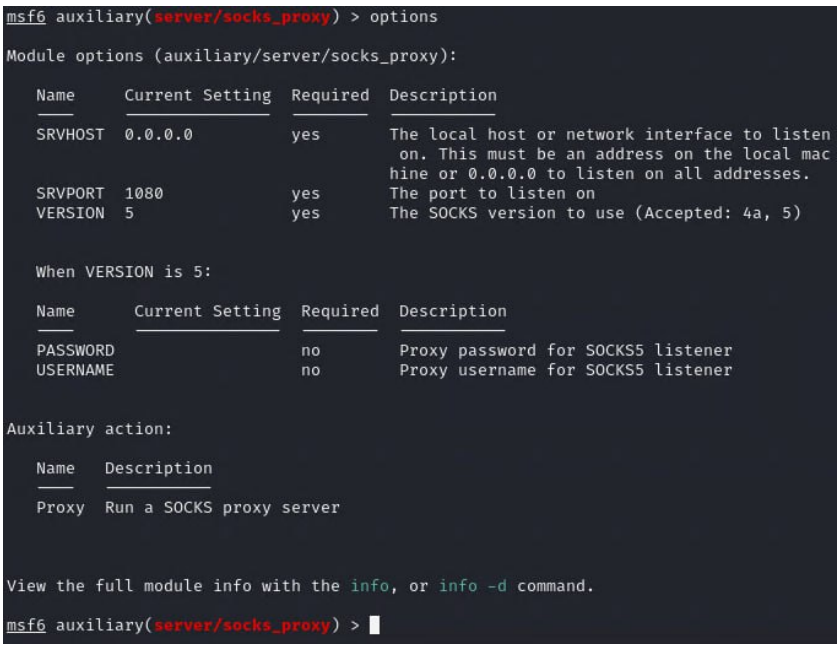

Рис. 3.6: Скрин 6

3.7 7. Просмотр ARP-таблицы

Получена таблица маршрутизации, показывающая IP-адреса активных хостов.

Рис. 3.7: Скрин 7

3.8 8. Настройка SOCKS-прокси

Настроен модуль server/socks_proxy и конфигурация proxychains.

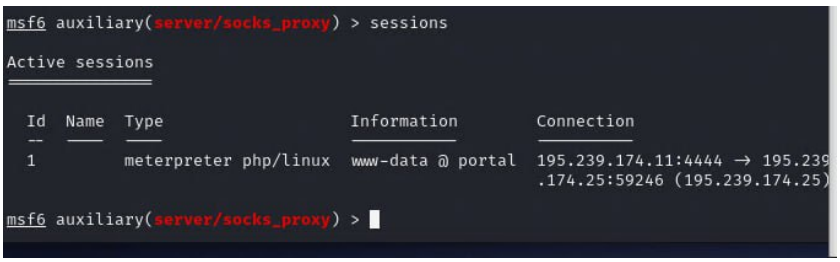

Рис. 3.8: Скрин 8

3.9 9. Сканирование портов с помощью proxychains

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

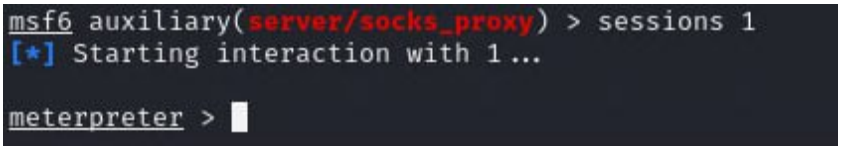

Рис. 3.9: Скрин 9

3.10 10. Обнаружение сервера MySQL

На хосте 10.10.10.30 обнаружен порт 3306 — стандартный для MySQL.

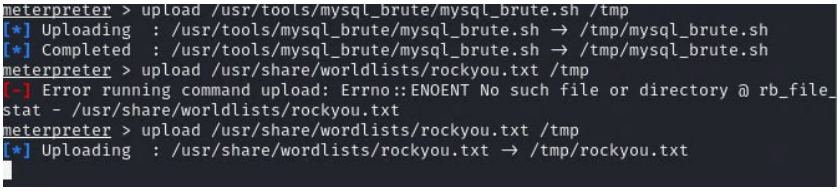

Рис. 3.10: Скрин 10

3.11 11. Загрузка скрипта перебора и словаря

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

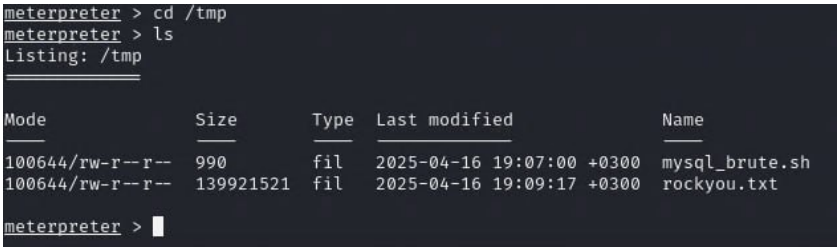

Рис. 3.11: Скрин 11

3.12 12. Проверка загрузки файлов

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

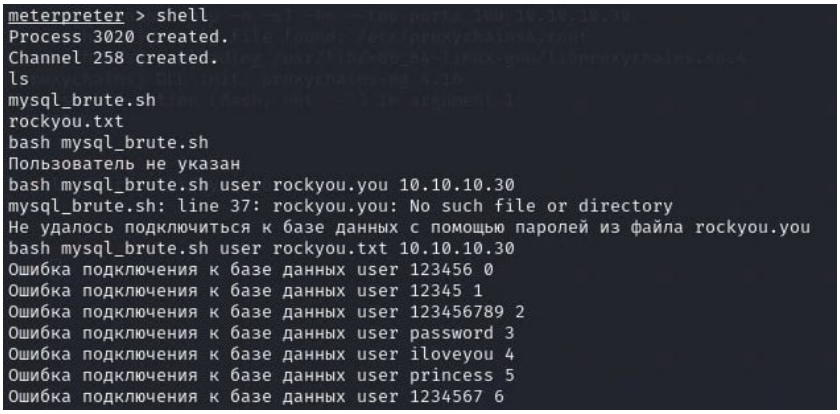

Рис. 3.12: Скрин 12

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.

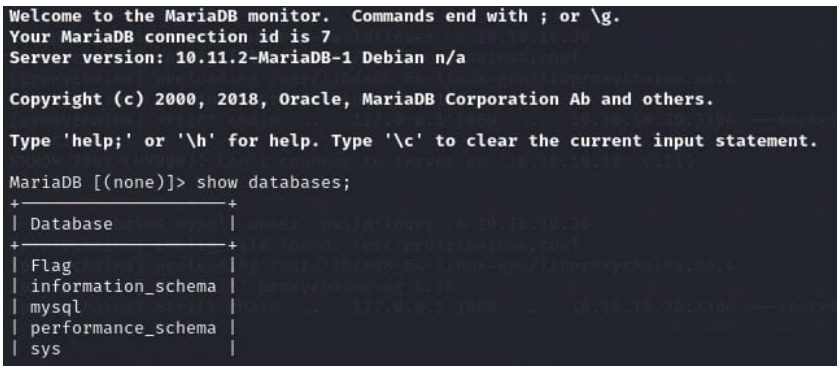

Рис. 3.13: Скрин 13

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.

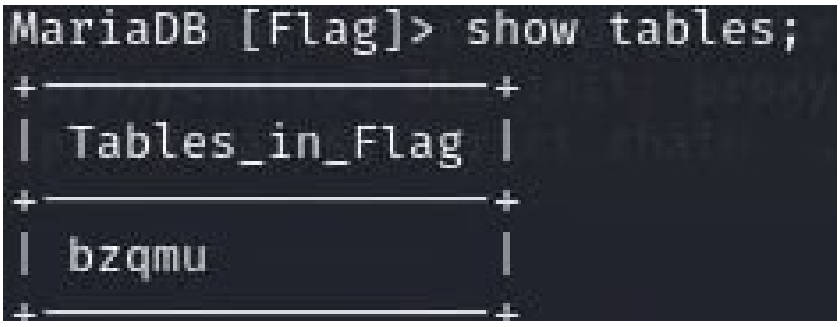

Рис. 3.14: Скрин 14

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.