Кибербезопасность предприятия

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

Оширова Юлия Николаевна

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

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

Выполнение лабораторной работы

Выполнение лабораторной работы

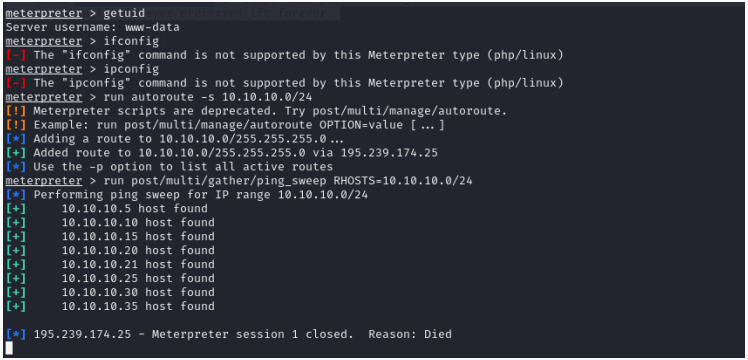

Рис. 1: Результат сканирования nmap для IP 195.239.174.25

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

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.