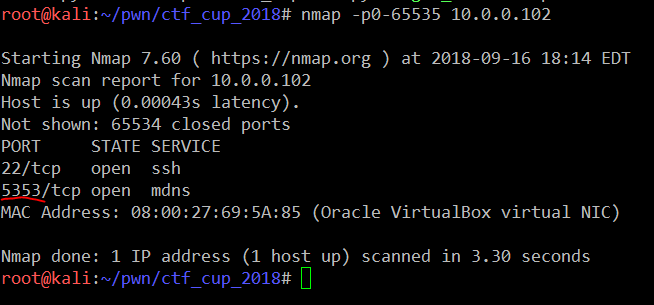
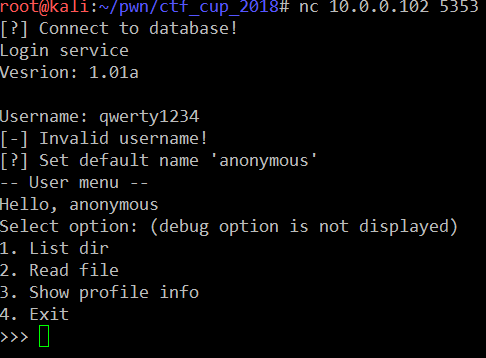
**Решение заданий категории Pwn.**

**Задание №1. «Login panel: Access»**

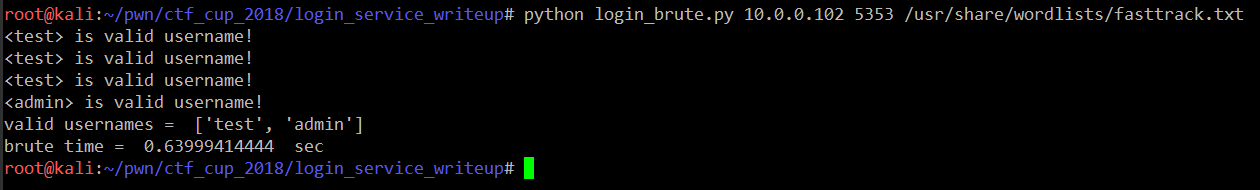
Командам был выдан IP-адрес некоторой машины (у каждой команды своя машина). Первое действие, которое нужно было предпринять – это просканировать порты с помощью nmap.



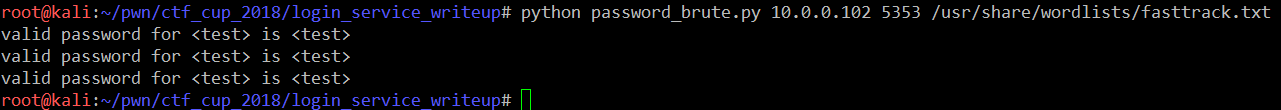
После сканирования команда обнаруживает 2 открытых порта, на одном из них запущен SSH, а на втором некоторый сетевой сервис. Попытки подключения по SSH остаются неудачными, так как подключение осуществляется по ключу. Поэтому, переводим всё внимание на сетевой сервис.



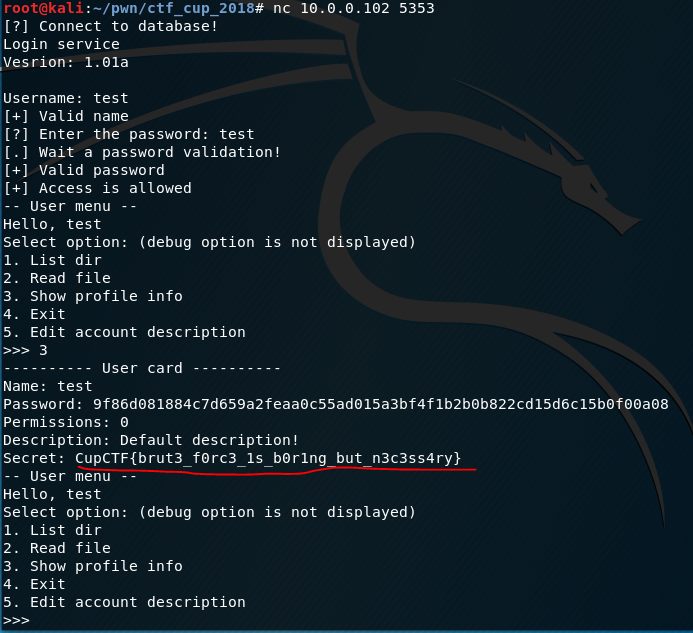
При подключении к сервису, запрашивается имя пользователя, при этом если ввести неверное имя, то будет установлено стандартное имя «anonymous». Для начала команде нужно определить все верные имена. Чтобы решить эту задачу достаточно написать простой брутфорсер по словарю имён пользователей. Пример такого брутфорсера на языке Python представлен в файле «login\_brute.py».



Попробуем перебрать имена пользователей по небольшому словарю и получим 2 верных имени – «test» и «admin». Подтвердим верность находки вручную, и обнаружим, что имена подходят, однако требуется пароль. Для получения пароля также необходимо написать небольшой брутфорсер. Пример такого брутфорсера представлен в файле «password\_brute.py».



После применения скрипта, получаем верный пароль и заходим под учётной записью «test/test».



Смотрим информацию о профиле и получаем первый флаг.